Ron Porath

Internet, Cyber- und IT-Sicherheit von A-Z

Aktuelle Begriffe kurz und einfach erklärt – Für Beruf, Studium und Privatleben

2. Auflage

EBOOK INSIDE

Springer Vieweg

Internet, Cyber- und IT-Sicherheit von A–Z

Ron Porath

Internet, Cyber- und IT-Sicherheit von A–Z

Aktuelle Begriffe kurz und einfach erklärt – Für Beruf, Studium und Privatleben

2., Auflage

Springer Vieweg

Ron Porath
Wettswil, Schweiz

ISBN 978-3-662-60910-1 ISBN 978-3-662-60911-8 (eBook)
https://doi.org/10.1007/978-3-662-60911-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Die erste Auflage des Buches erschien mit dem Titel „WÖRTERBUCH Cyber- und Informations-Sicherheit: 350 Fachbegriffe übersetzt in Englisch und Deutsch“ 2018 bei Amazon im Selbstverlag.

Planung/Lektorat: Martin Börger
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Falls wir unsere Geräte nicht schützen und unsere Aktivitäten im Internet nicht mit Bedacht ausführen, lautet die Frage nicht ob, sondern wann die eigenen Daten in falsche Hände geraten.

Für all die vielen Menschen, denen Wissen wichtig ist.

Inhaltsverzeichnis

1 Einleitung 1

Teil I Begriffe von 0–9, A–Z

2 0–9 7

3 A 9

4 B 33

5 C 51

6 D 75

7 E 95

8 F 107

9 G 119

10 H 129

11 I 145

12 J 165

13 K 169

14 L 177

15 M 185

16 N 203

17 O 213

18 P 223

19 Q 249

20 R 255
21 S 269
22 T 311
23 U 321
24 V 331
25 W 339
26 X 351
27 Y 353
28 Z 355

Teil II Anhang

29 SPEZIALTHEMA „Der Aufruf einer HTTPS-Internetseite“ 363
30 SPEZIALTHEMA „E-Mail-Verschlüsselung. Kostenlos. Einfach einzurichten und zu benutzen.“ 365
31 Tipps und Tricks für die eigene IT-Sicherheit 369
32 ASCII-Tabelle 375
33 HTTP Status Code Definitionen 379
34 RegEx Übersicht 381
35 Markdown-Übersicht 383

Einleitung

1

Die Digitalisierung schreitet mit großen Schritten voran. Jeder von uns ist Teil davon und wir profitieren in vielen Bereichen unseres Lebens. Angefangen bei Apps auf Handys, die uns mitteilen, wann wir zu Hause ankommen, über persönliche, digitale Assistenten, die scheinbar wissen, wann wir welche Musik hören möchten, bis hin zum Smart Home, welches nur dann Licht einschaltet, wenn Licht benötigt wird. Ist das nicht wunderbar!?

Dieses aktuelle Standardbuch mit über *2600 Begriffen zu Internet, zu IT im Allgemeinen sowie zu Cyber- und IT-Sicherheit* im Besonderen bietet einfache, kurze und verständliche Erklärungen und Zusammenfassungen zu Abkürzungen, Funktionen und Risiken dieser neuen digitalen Möglichkeiten. Es offeriert ein gutes erstes Verständnis für die aktuellen Begriffe des Alltags, beruflich und privat, *ohne lange Texte lesen zu müssen*. Den meisten Lesern dieses Buches werden die darin enthaltenen Erklärungen ausreichen, um ihre eigentliche Tätigkeit weiterführen zu können. Personen, die zusätzliche, detailliertere Informationen benötigen, können diese danach im Internet finden und mit den Erklärungen dieses Buches rascher verstehen.

Neue und zukünftig wichtige Internettechniken wie *HTTPS* und *Wi-Fi6* fanden Einzug in dieses Lexikon, genauso wie Begriffe zu *Quantencomputer* und *künstliche Intelligenz.* Leser werden ebenfalls Details zu *Ransomware, Trojaner* und *Bitcoin* finden, sowie geläufige Abkürzungen, welche in sozialen Medien und Messengers benutzt werden. Experten können auch Erklärungen entdecken zu *Azure Information Protection, scrypt, Markdown, Qubit, Blockchain* und *SChannel.* Dabei erfolgte die Auswahl der in diesem Buch beschriebenen Definitionen stets mit dem Gedanken, dem Leser *die wichtigsten Begriffe seines privaten, universitären, schulischen und beruflichen IT-Alltags* zu erläutern und auf die Gefahren hinzuweisen sowie mögliche Schutzmaßnahmen anzubieten. Dies soll es einerseits dem Anwender an seinem PC zu Hause, andererseits auch dem Mitarbeiter im Unternehmen und dem Profi in einer IT-Funktion ermöglichen, schnell ein Verständnis für relevante Begriffe zu erhalten.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_1

Dieses Buch versucht nicht, eine Konkurrenz zu Online-Lexika, wie dem genialen Wikipedia, zu sein, sondern eine Ergänzung dazu. *Im Gegensatz zu internetbasierten Lexika stellt dieses Buch die Begriffe linear, kurz, ohne Verzettelung und aus einer Hand dar, sodass der Leser innerhalb weniger Sekunden einen Begriff seines Alltags versteht, ohne erst lange Texte lesen oder relevante Internetseiten finden zu müssen.* Dem interessierten Leser, der darüber hinausgehende, zusätzliche, vertiefte Informationen zu den gesuchten Begriffen sucht, wird Wikipedia wärmstens empfohlen, welches auch dem Autor dieses Buches stets weiterhilft.

1.1 Benutzungshinweise

Die Reihenfolge der Begriffe in diesem Buch entspricht dem deutschen Alphabet, wobei Bindestriche, Schrägstiche, Interpunktionen und Leerzeichen nicht als eigene Zeichen gelten. Einige längere, zusammengesetzte Begriffe wurden mittels eines Bindestriches getrennt, um die Lesbarkeit und Auffindbarkeit zu erhöhen, zum Beispiel *„Software-Entwicklung“* anstatt *„Softwareentwicklung“*.

Falls Begriffe mehrere geläufige Bedeutungen besitzen, werden diese mit **1)** …, **2)** … usw. getrennt.

Um den Lesefluss nicht zu unterbrechen, wurde, wie in vielen anderen Lexika, darauf verzichtet, Pfeile für Verweise zu anderen Begriffen darzustellen. Der Leser findet diese Begriffe jedoch mit Leichtigkeit an der entsprechenden Stelle des Buches.

Viele englische Bezeichnungen werden im Internet- und IT-Alltag verwendet und wurden deshalb in diesem Buch mit aufgenommen. Falls deren deutsche Übersetzungen ebenfalls geläufig sind, verweisen die englischen Wörter auf die deutschen ausführlichen Erklärungen, andernfalls enthalten die englischen Bezeichnungen eigene Erklärungen. Siehe Beispiel A.

Beispiel A

HONEYPOT (engl.)
Übsg. Honigtopf

> **HONIGTOPF 1)** Datei mit interessant klingendem Namen, welche Hacker anlocken soll. Greifen Hacker dann auf diese Datei zu, kann im besten Fall die Kontrolle über den Computer des Hackers erlangt werden. **2)** Virtuelle Nachbildung eines realen Netzwerks, bspw. einer Industrieanlage, eines Wasserwerks oder eines Kraftwerks. Bei einem Angriff eines Hackers auf das vermeintliche Netzwerk kann der Angreifer beobachtet und zurückverfolgt werden.

Begriffe, welche einzig ein Synonym oder eine Übersetzung als Erklärung besitzen, werden unter dem Synonym resp. der Übersetzung ausführlicher erklärt. Siehe Beispiel B.

Beispiel B

ONE-WAY FUNCTIONS (engl.)
Übsg. Einweg-Funktionen. **Syn.** zu Falltür-Funktionen

> **EINWEG-FUNKTIONEN** Syn. zu Falltür-Funktionen. Mathematische Berechnungen, die rasch ausgeführt werden können, aber Ergebnisse liefern, welche nur mit viel Aufwand zurückzurechnen sind. Solche Funktionen werden bei der Berechnung von asymm. Verschlüsselungen verwendet. Dabei werden zwei große Primzahlen miteinander multipliziert. Das dadurch erhaltene Produkt lässt sich nur mit sehr großem Rechenaufwand wieder in die zwei Primzahlen zerlegen.

Begriffsabkürzungen verweisen auf die ausführliche Schreibweise, unter welcher detaillierte Begriffserklärungen zu finden sind. Siehe Beispiel C.

Beispiel C

DRM
Abk. für Digital Rights Management

> **DIGITAL RIGHTS MANAGEMENT [DRM] (engl.)** **1)** Ugs. für Programme und Systeme zum Schutz von Informationen. Präziser wird dieser Schutz „Information Rights Management“ (IRM) genannt. **2)** Softwarelösungen zur Vermeidung von Raubkopien digitaler Produkte, wie Software, Bücher, Musik.

Abkürzungen

aba.	auch bekannt als
Abk.	Abkürzung
Aktuell	Zeitpunkt des Drucks dieses Buches
allg.	allgemein
Anz.	Anzahl
App.	Applikation, Software, Programm, System
asymm.	asymmetrisch
bzw.	beziehungsweise
ca.	circa
cm	Zentimeter
engl.	Englisch
etc.	et ceterea (lateinisch), und die übrigen
evtl.	eventuell
insb.	insbesondere

inkl.	inklusiv
mind.	mindestens
Mio.	Millionen
PC	Personal Computer, allg. Computer
resp.	respektive
sog.	sogenannt
symm.	symmetrisch
Syn.	Synonym
System	IT-System, Computer, PC, Gerät, Infrastruktur
Übsg.	Übersetzung
ugs.	umgangssprachlich
usw.	und so weiter
u. a.	unter anderem, und andere(s)
u. Ä.	und Ähnliches
u. u.	und umgekehrt
v. a.	vor allem
z. B.	zum Beispiel
z. T.	zum Teil
z. Z.	zur Zeit

Teil I

Begriffe von 0–9, A–Z

0–9

2

1FA
Abk. für Ein-Faktor-Authentisierung, Ein-Faktor-Authentifizierung

2D
Abk. für Zweidimensional

2FA
Abk. für Zwei-Faktor-Authentisierung, Zwei-Faktor-Authentifizierung

2-FACTOR-AUTHENTICATION [2FA] (engl.)
Übsg. Zwei-Faktor-Authentisierung

2-STEP VERIFICATION [2SV]
Übsg. 2-Schritt-Überprüfung. Syn. zu 2FA

2SV
Abk. für 2-Step Verification

3D
Abk. für Dreidimensional

3DES
Syn. zu Triple-DES, DESede. Verschlüsselungsalgorithmus. Nachfolger von DES. Mathematisch erfolgt dabei eine Verschlüsselung, gefolgt von einer „Entschlüsselung" mit einem anderen Schlüssel und schließlich eine erneute Verschlüsselung mit einem weiteren Schlüssel (Encrypt-Decrypt-Encrypt).

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_2

3-D SECURE
Internationaler Sicherheitsstandard bei Kreditkartentransaktionen. Dabei werden nicht nur Informationen verwendet, die auf der Kreditkarte vermerkt sind, sondern auch geheime Informationen, welche nur dem Besitzer bekannt sind, wie z. B. ein Passwort.

404 NOT FOUND
Einer der Fehlermeldungen des HTTP-Standards. Dieser HTTP-Statuscode bedeutet, dass die Internetseite, die URI oder die Ressource nicht gefunden wurde (siehe Liste der HTTP-Statuscodes im Anhang bei Kap. 33).

4K
Abk. für 4K-Auflösung, d. h. eine horizontale Bildauflösung von ca. 4000 Pixeln. Bei Fernsehern und Computern wird meist eine Auflösung von 3840×2160 („4K UHD“) verwendet.

51-%-ATTACKE
Angriff auf eine Blockchain durch Angreifer, die mehr als 50-%-Rechenleistung aller im Blockchain-Mining Beteiligten besitzen und damit Transaktionen verändern können.

802.11
Abk. für IEEE 802.11

A

3

AAA
Abk. für Automatisierter aktiver Angriff

AAD
Abk. für Azure Active Directory

AADRM
1) Ursprüngliche, inoffizielle Abk. für Microsoft Azure Active Directory Rights Management. **2)** PowerShell-Modul für Microsoft Azure Rights Management.

ABANDONED WEB APPLICATIONS (engl.)
Übsg. Verlassene Websoftware. Alte, noch installierte, aber nicht mehr verwaltete, jedoch evtl. noch erreichbare Webapplikationen und Webseiten. Diese bergen ein Risiko, da oft veraltete, nicht aktuell gehaltene Software enthalten ist, die ein Eingangstor für Hacker sein kann.

ABFRAGE-ANTWORT-AUTHENTIFIKATION
Syn. zu Challenge-Response Authentication. Authentifizierungsmethode eines Benutzers an einem System oder allg. zw. zwei Parteien, basierend auf gemeinsamem Wissen, auch Shared Secret genannt. Dabei gibt die Partei A der Partei B eine Aufgabe zu lösen. Da Partei B die Lösung kennt und antworten kann, kann sich Partei B damit bei Partei A authentisieren.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_3

ABHÖREN
Methode zum Abfangen von sensiblen Daten, um diese mit unehrenhaften Absichten auszunutzen. Die Arten des Abhörens sind vielfältig, meist in Form von Anzapfen von Telefon- oder Internetleitungen, physisch oder digital.

ABNORMES VERHALTEN
Syn. zu Auffälligkeiten. Bezeichnung für Unregelmäßigkeiten beim Betrieb von Systemen. Auffälligkeiten in Logs können ein Hinweis auf Manipulation sein.

ABWEHR VON CYBER-ATTACKEN
Verfahren innerhalb von Firmen, und in kleinerem Maßstab auch bei Privatpersonen, um Cyber-Attacken abzuwehren. Die Abwehr erfolgt meist auf vier Arten:

a) Ständige oder punktuelle Analyse von Systemen, von Software oder von Netzwerk-Traffic zur Erkennung von Auffälligkeiten und Schwachstellen.
b) Fortwährender Schutz von Systemen, z. B. mittels Anti-Viren-Software.
c) Detektion von Angriffen, z. B. durch lückenlose Überwachung der Online-Tätigkeit der Benutzer durch Anti-Malware-Tools.
d) Richtige Reaktion auf Angriffe, z. B. durch Abhängen des angegriffenen Systems vom Netzwerk, um weitere Verbreitung von Malware zu verhindern.

AC
Abk. für Access Control

ACCESS CONTROL [AC] (engl.)
Übsg. Zugriffskontrolle

ACCESS CONTROL LISTS [ACL] (engl.)
Übsg. Zugriffslisten

ACCESS MANAGEMENT (engl.)
Übsg. Zugangsverwaltung

ACCESS REVIEW (engl.)
Übsg. Überprüfung von Zugriffsrechten. Regelmäßig stattfindender Prozess in Firmen mit dem Ziel, die Zugriffsrechte der Mitarbeiter zu den verschiedenen Ressourcen (Computer, Netzwerke, Server, Applikationen usw.) zu überprüfen und daraufhin diese Zugriffsrechte entweder zu verlängern oder zurückzuziehen. Bei größeren Unternehmen wird dabei dem Prinzip des „Need-to-know“ Rechnung getragen und nur die Zugriffsrechte aktiv gehalten, die für die aktuelle Tätigkeit des Mitarbeiters aktuell nötig sind.

ACCESS TOKEN (engl.)
Übsg. Zugriffsobjekt. Hardware oder Software mit enthaltenen Informationen zum Benutzer, wie bspw. seine Identität und seine Zugriffsrechte im aktuellen Kontext, z. B. innerhalb einer Internetseite. In vielen Systemen wird ein Software Access Token erstellt, sobald das Passwort des Benutzers eingegeben und überprüft wurde. Jede vom Benutzer daraufhin im gleichen Kontext aufgerufene Ressource erhält diesen Access Token zur Überprüfung der Benutzerrechte.

ACCIDENTAL DISCLOSURE OF INFORMATION (engl.)
Übsg. Zufällige, unbeabsichtigte Offenlegung von Informationen.

ACCIDENTAL LOSS (engl.)
Übsg. Unbeabsichtigter Verlust, z. B. von Informationen. Dies kann bspw. durch Hardwarefehler auf der Festplatte passieren oder durch Schadsoftware.

ACCOUNT (engl.)
Übsg. Konto

ACCOUNT ACCESS (engl.)
Übsg. Zugriff auf ein Online- oder System-Konto

ACL
Abk. für Access Control Lists

ACTIVE DIRECTORY [AD] (engl.)
Von Microsoft verwendete Bezeichnung für Windows-Server-basierte Personen-, Gruppen- und Infrastrukturverzeichnisse in Netzwerken. Die darin enthaltenen Daten werden zur Authentisierung und Autorisierung von Benutzern und Ressourcen in Windows-Applikationen sowie zur zentralen Administration des Netzwerks verwendet.

ACTIVE DIRECTORY DOMAIN SERVICES [AD DS] (engl.)
Hauptkomponente von Active Directory zur Verwaltung von Domain Controller und Ressourcen.

ACTIVE DIRECTORY FEDERATION SERVICES [ADFS] (engl.)
Software zur Bereitstellung von Single Sign-On bei Windows Server. Dies ermöglicht die Anmeldung und die Applikationssicherheit durch verteilte (verbundene) Identitäten der Benutzer über mehrere Systeme.

ACTIVE DIRECTORY GROUP [AD GROUP] (engl.)
Syn. zu Windows Security Group. Solche Gruppen sind virtuelle Container für Benutzer- oder Computerobjekte. Durch die Zusammenfassung in einer Gruppe können allen darin enthaltenen Benutzern oder Computern die gleichen Zugriffsrechte vergeben werden.

ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES [ADRMS] (engl.)
Client-Server-basierte Softwarelösung von Microsoft, um Information Rights Management anzuwenden, d. h. zur Verschlüsselung und der Einschränkung der Benutzungsrechte bei Dateien und E-Mails. Syn. zu Active Directory Rights Management System

ACTIVE DIRECTORY RIGHTS MANAGEMENT SYSTEM [ADRMS] (engl.)
Von Microsoft entwickelte Server-Client-Lösung zur Verschlüsselung und Entschlüsselung von E-Mails und Office-Dokumenten innerhalb der Windows-Umgebung sowie zur Rechtevergabe bei diesen verschlüsselten E-Mails und Dokumenten. Damit lässt sich erreichen, dass bspw. eine E-Mail nicht weitergeleitet werden kann oder auch, dass ein verschlüsseltes Dokument von niemandem außerhalb der Firma gelesen werden kann, der keinen digitalen Schlüssel und damit keine Berechtigung zur Entschlüsselung vom Server erhalten kann. ADRMS baut auf dem ursprünglichen Rights Management System (RMS) für Windows Server auf. Es wird in großen und kleinen Firmen dazu verwendet, Datenverlust zu verhindern und geistiges Eigentum zu schützen.

ACTIVE SETUP (engl.)
Übsg. Aktives Setup. Methode bei Windows, um während der Anmeldung des Benutzers oder beim Start einer Applikation Werte der Registrierungsdatenbank von HKLM zu HKCU zu kopieren und für den Benutzer bereitzustellen.

ACTIVEX CONTROLS
Software, die innerhalb von Internetbrowsern auf Windows-Systemen nachgeladen und ausgeführt wird und aus kompiliertem Maschinencode besteht, im Gegensatz bspw. zu JavaScript-Programmen, welche in Internetbrowsern zur Laufzeit interpretiert werden.

AD
1) Abk. für Active Directory. **2)** Abk. für Advertisement, Übsg. Werbung.

ADBLOCKER (engl.)
Übsg. Werbeblocker

ADDITIONAL DECRYPTION KEY [ADK] (engl.)
Übsg. Zusätzlicher Entschlüsselungsschlüssel. Notfallschlüssel, um Daten entschlüsseln zu können, falls der Hauptschlüssel verloren ging oder unbrauchbar wurde. Manchmal werden ADK auch als Hintertüren eingebaut, um Zugang zu den Daten zu erhalten, auch ohne den Besitz des Hauptschlüssels.

ADDRESS RESOLUTION PROTOCOL [ARP] (engl.)
Datentransferprotokoll in einem lokalen Netzwerk. Dieses dient der Zuordnung von MAC-Adressen zu den einzelnen Geräten innerhalb des Netzwerks.

AD DS
Abk. für Active Directory Domain Services

ADFS
Abk. für Active Directory Federation Services

AD GROUP
Abk. für Active Directory Group

ADK
1) Abk. für Additional Decryption Key. **2)** Abk. für Windows Assessment and Deployment Kit.

ADMIN ACCESS (engl.)
Übsg. Admin-Zugang

ADMIN ACCOUNT (engl.)
Übsg. Admin-Konto

ADMINISTRATION
Tätigkeiten eines Administrators an Systemen, meist innerhalb eines internen Netzwerks.

ADMINISTRATOR
Person, die einen oder mehrere Computer oder Netzwerke bereitstellt, aktuell hält und pflegt. Dafür benötigt der Administrator einen sicheren Admin-Zugang zu einem speziellen Admin-Konto, welches ihm die benötigten erweiterten Zugriffsrechte auf dem oder den Systemen und darin enthaltenen Dateien und Ressourcen bereitstellt. Ugs. wird jeder berechtigte Benutzer des Admin-Kontos als Administrator bezeichnet.

ADMINISTRATOR GROUP (engl.)
Auf Systemen meist vorhandenes Benutzergruppenkonto, welches bei der Installation des Betriebssystems erstellt wurde und Mitgliedern dieser Gruppe lokale Admin-Rechte für das System gibt.

ADMIN-KONTO
Benutzerkonto eines Systemadministrators. Diesem Konto werden erweiterte Zugriffsrechte zugewiesen, um dem Administrator die Möglichkeit zu geben, die Systeme im Netzwerk zu warten und bereitzustellen.

ADMIN-ZUGANG
Um bei privaten Computern oder in zentral betreuten Computersystemen, bspw. in Firmen, Installationen, Einstellungen oder Wartungen durchzuführen, meldet sich der Administrator am speziell dafür vorhandenen Admin-Konto an und erhält dadurch erweiterte Zugriffs- und Zugangsrechte. Diese Anmeldung ermöglicht ihm erweiterte Änderungsrechte zu benutzen, um den oder die Computer zu verwalten. Aufgrund dieser erweiterten Änderungsrechten, mit denen sich unter anderem auch Schutzmaßnahmen ausschalten lassen, sind die Admin-Passwörter begehrte Angriffsziele von Hackern und müssen bestmöglich geschützt sein.

ADOBE FLASH PLAYER
Software der Firma Adobe zur Wiedergabe von multimedialen Inhalten in Webbrowsern. Aufgrund mancher Attacken über den Flash Player in den letzten Jahren blockieren einige Seiten und Webbrowser die Ausführung von Flash-Inhalten.

ADRMS
Abk. für Active Directory Rights Management System, Active Directory Rights Management Services.

ADVANCED ENCRYPTION STANDARD [AES] (engl.)
Kryptografischer Algorithmus zum Schutz sensibler Informationen. Dieser wird in vielen Produkten verwendet, bspw. in WPA2 bei Wi-Fi, bei SSH sowie bei Skype. AES ist ein symmetrisches Verschlüsselungsverfahren, benutzt demnach denselben Schlüssel für Ver- und Entschlüsselung. Es basiert auf einer Blockchiffre-Berechnung, bei welcher mehrere Zeichen gleichzeitig verschlüsselt werden. CPUs werden inzwischen mit speziellen Funktionen für AES ausgestattet, sodass Ver- und Entschlüsselung schneller durchgeführt werden können. Bei Berücksichtigung der voraussichtlich zu erwartenden Entwicklung von Quantencomputern wird AES für Daten, die bis ca. 2030 erstellt werden, als sicher gegenüber Quantencomputer-Angriffen angesehen, da es auf einem symmetrischen Algorithmus basiert und damit der Schlüssel nicht auf Basis einer Berechnung beruht, die von Quantencomputern schnell möglich sein wird. Dies im Gegensatz zu asymm. Algorithmen, bei denen der Schlüssel aus der Multiplikation von Primfaktoren besteht und deren Faktorisierung mit Quantencomputern bis ca. 2030 schnell möglich sein wird.

ADVANCED PERSISTENT THREAT [APT] (engl.)
Heimlich durchgeführte, umfangreiche und kontinuierliche Hacking-Attacken, die von einer Person oder einer Gruppe von Personen gegen ein System durchgeführt werden. Häufig werden solche APTs von staatlich gelenkten Hackergruppen ausgeübt.

Beispiel

Beispiele von Advanced Persistent Threat-Methoden:
Privilege Escalation, Lateral Movement, Data Exfiltration.

ADVANCED RANSOMWARE INTRUSION (engl.)
Übsg. Umfangreicher Ransomware-Angriff

ADVANCED SPEAR PHISHING ATTACK (engl.)
Betrugsattacke mittels E-Mail oder anderer elektronischer Kommunikation, welche auf Basis gesammelter, persönlicher Informationen über bestimmte Personen, Organisationen oder ausgesuchte Firmen geschieht. Mithilfe dieser persönlichen Daten kann eine Vertrautheit vorgetäuscht und dadurch eine hohe Erfolgsquote beim Phishing erzielt werden, um unautorisierten Zugang zu sensiblen Informationen zu erhalten.

ADWARE (engl.)
Übsg. Software, die Werbung anzeigt.

AES
Abk. für Advanced Encryption Standard

AFAIK
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „As far as I know“, Übsg. „Soweit ich weiß“.

AGENT (engl.)
1) Abk. für Software Agent. **2)** Abk. für Hardware Agent.

AGENTEN-WEITERLEITUNG
In SSH benutzte Methode, um Zugang zu mehr als einem Server aufzubauen, ohne jeweils erneut das Passwort für den geschützten privaten Schlüssel eingeben zu müssen. Die Client- und Server-Authentifizierung zu den zusätzlichen Servern erfolgt dabei aufgrund vorheriger Authentisierung am ersten Server.

AGILE MODEL
Übsg. Agile Projektmethode

AGILE PROJEKTMETHODE
Dynamische Projektvorgehensmethode, bei welcher mehrmals, bspw. einmal alle zwei Wochen oder einmal monatlich, alle Phasen der Entwicklung durchgeführt werden, inkl. Anforderungsdefinition, Design, Entwicklung, Validierung und Implementation. Ziel ist die rasche Lieferung erster Resultate und rasche Einbeziehung von Änderungswünschen der zukünftigen Anwender.

AGILE SOFTWARE-ENTWICKLUNG
Projektmethode, die es erlaubt, raschere Entwicklungszyklen durchzuführen und erste Funktionen frühzeitig den Benutzern anzubieten. Durch die Einbeziehung der Benutzer werden die Risiken im Entwicklungsprozess reduziert und die Benutzerzufriedenheit erhöht.

AGNOSTISCH
Syn. zu unabhängig, nicht wahrnehmbar. Bspw. ist eine browseragnostische Lösung eine Internetseite, welche bei allen Internetbrowsern läuft.

AI
Abk. für Artificial Intelligence

AIA
Abk. für Automatischer Informationsaustausch

AIM
Abk. für AOL Instant Messenger

AIOPS
Abk. für Artificial Intelligence for IT Operations

AIP
Abk. für Azure Information Protection

AI SECURITY (engl.)
Abk. für Artificial Intelligence Security. Verfahren und Softwareprodukte zur Datensicherheit, welche auf Methoden der künstlichen Intelligenz beruhen.

AKTIVER ANGRIFF
Angriff, bei welchem Systeme oder Dateien manipuliert werden.

AKUSTIKKOPPLER
In den 1970er- und 1980er-Jahren benutztes Gerät zur Übertragung von digitalen Daten über den Hörer eines analogen Telefons.

ALERT (engl.)
Übsg. Alarm, Warnung

ALEXA
Amazons virtueller Assistent, welcher in Produkten wie Amazon Echo und Amazon Echo Dot eingesetzt wird. Der Name ist angelehnt an die Bibliothek von Alexandria.

ALGORITHMUS
Abfolge von mathematischen Operationen, angewendet auf Daten. Bspw. beschreiben die auszuführenden Schritte zur Addition zweier Zahlen einen einfachen Algorithmus. Verschlüsselungsalgorithmen verwenden mathematische Verfahren, um Klartext in geheimen Text zu transformieren. In Kombination mit großen Datenmengen werden Algorithmen zur Klimavorhersage, zur Kaufempfehlung und vieles mehr benutzt.

ALIAS (engl.)
Übsg. Pseudonym, Stellvertreter. Beispiel: Um die Server hinter einem Loadbalancer anzusprechen, wird die Adresse des Loadbalancers als Alias für die Adressen der einzelnen Server benutzt.

ALTAVISTA
Suchmaschine für Internetseiten. Sie wurde von Dezember 1995 bis Juli 2013 betrieben.

ALTE, NICHT MEHR VERWALTETE WEBAPPLIKATION
Früher benutzte, möglicherweise durch neuere Applikationen abgelöste Software, die nicht mehr aktuell gehalten wird, aber noch immer auf dem System gespeichert ist und aufgerufen werden kann. Dies stellt ein immer größer werdendes Sicherheitsproblem für Firmen und Hosting-Anbieter dar. Syn. zu App-Leiche.

AMA
Abk. für Authentication Mechanism Assurance

AMAZON WEBSERVICES [AWS] (engl.)
Amazons Cloud-Computing- und Cloud-Service-Angebot. Dieser wird von vielen Firmen für ihre Online-Dienste angemietet.

AMERICAN STANDARD CODE FOR INFORMATION INTERCHANGE [ASCII] (engl.)
Standardisierte Zeichencodierung zur Datenverarbeitung und zum Datenaustausch. Ursprünglich aus 128 unterschiedlichen 7-Bit-Werten definiert, später auf 256 unterschiedlichen 8-Bit-Werten erweitert, um 128 resp. 256 verschiedene, klar definierte Buchstaben, Zahlen und Sonderzeichen in verschiedenen Programmen und Systemen benutzen zu können (siehe ASCII-Tabelle im Anhang bei Tab. 32.1).

ANATOVA
Schadsoftware in Form von Ransomware

ÄNDERUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Abschnitt im Lebenszyklus kryptografischer Schlüssel. Bei der Änderung eines kryptografischen Schlüssels werden Eigenschaften des Schlüssels, bspw. die Schlüssel-

länge, geändert und der öffentliche Schlüssel erneut publiziert. Dies ist nicht bei jeder Schlüsselart möglich, sodass evtl. der aktuelle Schlüssel annulliert werden muss und ein neuer mit den zu ändernden Eigenschaften erstellt werden muss. Siehe zusätzliche Details beim Begriff Schlüssel.

ANFORDERUNG ZUR ZERTIFIKATSSIGNIERUNG
Elektronische Anfrage an eine Zertifizierungsstelle (CA) zur Erstellung eines neuen, signierten Zertifikats. Dazu erzeugt der Antragsteller zuerst ein Paar aus privatem und öffentlichem Schlüssel auf seinem System und daraus eine genau spezifizierte digitale Formulardatei („CRS-Datei"), welche den öffentlichen Schlüssel enthält. Diese wird an die CA gesendet, die die CRS-Datei und damit die Identität des Antragstellers oder des Systems prüft. Bei positiver Prüfung sendet die CA dem Antragsteller sein Zertifikat signiert zurück.

ANGRIFF
Syn. zu Attacke. Methode, um Zugang zu Computer, Handy, Computernetzwerken oder Online-Konten zu erschleichen. Dabei geht es den Angreifern meist um Datendiebstahl, um Identitätsdiebstahl oder um das Lahmlegen von Systemen und Internetseiten, bspw. mittels automatischen Massenanfragen (DDoS-Angriff). Mögliche Angriffsmethoden sind das Hacking und Benutzen von gestohlenen Passwörtern, das Erschleichen der Login-Daten („Phishing") durch Nachahmung echter Internetseiten oder die Einspeisung von Malware bei schwach gesicherten Routern, Webcams oder Temperaturreglern.

ANGRIFF-ERKENNUNGS-SYSTEM
Syn. zu Intrusion Detection System. System zur Erkennung von Angriffen gegen Computer und Netzwerke. Ein solches Erkennungssystem kann auf allen Computern des Netzwerks oder als Sensor innerhalb des Netzwerkverkehrs eingesetzt werden. Auch die Kombination beider Methoden wird verwendet.

ANGRIFFSFLÄCHE
Syn. zu Attack Surface. Gesamtheit aller Angriffsmöglichkeiten, die einem Hacker den Zugriff auf ein System oder dessen Daten erlauben.

ANGRIFFSPUNKT
Syn. zu Attack Vector. Angriffsmöglichkeit, die einem Hacker den Zugriff auf ein System oder auf Daten erlaubt.

ANHANG
Abk. für E-Mail-Anhang. Datei, die mit einem E-Mail-Text verschickt wird. Da E-Mail-Anhänge Makros, Viren und andere Schadsoftware beinhalten können, besteht bei unbedachtem Öffnen des Anhangs die Gefahr, sein System und andere Systeme zu beeinträchtigen, wie bspw. beim Virus „IloveYou".

ANMELDEDATEN
Anmeldedaten werden verwendet, um sich an einem System, einem Programm oder an einem Online-Dienst anzumelden.

Beispiele: Benutzername mit Passwort, digitales Zertifikat u. Ä.

ANMELDEDATENSPEICHER
Syn. zu Tresor und Passwort-Manager. Datenbank auf Betriebssystemen wie Android, Windows und iOS, in welchem Anmeldedaten, also Benutzernamen mit Passwort oder Zertifikate gespeichert werden. Durch die Anmeldung an einem Betriebssystem oder direkt an dem Anmeldedatenspeicher wird dieser Tresor geöffnet und nimmt dem Benutzer nachfolgend die Aufgabe ab, die Anmeldedaten bei jeder Anmeldung an Applikationen und anderen Systemen neu eingeben zu müssen.

ANMELDEVERFAHREN
Methoden, mit denen Benutzer sich an einem System, an einer Applikation oder an einem Online-Dienst anmelden. Die häufigsten Verfahren sind die Eingabe von Benutzername mit Passwort, die Benutzung von Smartcard mit Pin oder die Verwendung einer Authenticator-Applikation mit Master-Passwort.

ANMELDUNG
Aktion eines Benutzers nach dem Starten oder Reaktivieren eines Computers, Handys oder Online-Dienstes, um den Zugriff auf sein Konto oder das System zu erlangen. Dabei wird meist die Kombination aus Benutzername und Passwort verwendet oder auch das sicherere 2FA.

ANNULIERUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Abschnitt im Lebenszyklus kryptografischer Schlüssel. Bei der Annullierung wird ein bisher benutzter Schlüssel als ungültig erklärt. Siehe zusätzliche Details beim Begriff Schlüssel.

ANOMALIES (engl.)
Übsg. Auffälligkeiten und abnormes Verhalten

ANONYMISIERUNG
Abk. für Datenanonymisierung

ANONYMITÄT
Situation und Verhalten, bei der eine Person nicht identifizierbar ist. Das Internet ermöglicht scheinbar anonymes Agieren, jedoch werden meist unbemerkt Daten mitübertragen, wie bspw. die IP-Adresse des Computerbenutzers.

ANONYMIZATION (engl.)
Übsg. Datenanonymisierung

ANONYMIZED DATA (engl.)
Übsg. Anonymisierte Daten

ANONYMOUS (engl.)
Übsg. Anonym. In der IT wird ein Benutzer Anonymous genannt, wenn dieser einen Gast- oder Anonymzugang benutzt und damit seine Identität nicht preisgibt oder preisgeben muss. Dabei werden keine Benutzernamen und Passwörter verwendet und es findet keine Authentifizierung statt. Anonym angemeldeten Benutzern weisen Systeme meist limitierte Gastzugriffe zu, mit denen immerhin öffentliche Informationen, die sich auf dem System befinden oder von diesem aus zugänglich sind, eingesehen oder heruntergeladen werden können. Bspw. können öffentliche Schlüssel anonym heruntergeladen und installiert werden, da diese keine geheimen Daten beinhalten. Auch offerieren Produktanbieter häufig Bedienungsanleitungen für deren Produkte auf ihrer Internetseite an, ohne dass sich der Benutzer anmelden muss.

ANSI
1) Abk. für American National Standards Institute. **2)** Zeichencodes mit 8-Bit pro Zeichen. Die ersten 127 Zeichen entsprechen den ASCII-Zeichen (siehe ASCII-Tabelle im Anhang bei Tab. 32.1). **3)** Abk. für ANSI-Escapesequenzen. Codes basierend auf dem ANSI.SYS-Treiber bei MS-DOS und entsprechenden Implementierungen bei anderen Betriebssystemen, mit denen die Cursorposition und -farbe und andere Darstellungsfunktionen auf textbasierten Darstellungen möglich werden. ANSI-Escapesequenzen wurden häufig in den 1980er-Jahren bei BBS-Mailboxen und heute noch bei Terminal-Emulatoren verwendet.

ANTI-SPAM-FILTER (engl.)
Software auf Servern, Computern, Routern und Handys, um unerwünschte E-Mails, v. a. Werbe-E-Mails, zu blockieren. Meist arbeiten solche Filter mit Algorithmen des maschinellen Lernens, sodass vom Benutzer neue, als Spam gekennzeichnete E-Mails den Algorithmus fortlaufend verbessern.

ANTI-SPYWARE-SOFTWARE (engl.)
Übsg. Anti-Spionage-Software. Programm auf Servern, Computern, Routern und Handys, um verseuchte Apps oder ausführbare Skripte zu blockieren, bevor diese heruntergeladen werden.

ANTI-TAMPERING (engl.)
Übsg. Sabotagenschutz

ANTI-VIREN-SCANNER
Software auf Servern, Computern und Handys, um Dateien im System zu durchsuchen, zu analysieren und darin gefundene Viren zu entfernen.

ANTI-VIRUS SOFTWARE (engl.)
Software auf Servern, Computer und Handys, um Viren fernzuhalten oder zu entfernen. Heutige PCs und Handys sind häufig oder ständig mit dem Internet verbunden und damit laufend den Gefahren von neuen Viren und anderer Schadsoftware ausgesetzt. Viren können sich im eigenen PC durch unterschiedliche Methode einnisten, bspw. beim versehentlichen Anklicken von Links auf verseuchten Internetseiten, beim unbedachten Öffnen von E-Mail-Anhängen oder auch beim automatischen Ausführen von Makros innerhalb von Dokumenten. Auf jedem Gerät, welches persönliche oder wichtige Daten speichert, sollte immer ein Anti-Viren-Programm laufen.

ANTRAG ZUR ZERTIFIZIERUNG
Verfahren, mit denen Internetserverbetreiber ihren öffentlichen Schlüssel des Servers von einer Zertifizierungsstelle signieren lassen können, indem sie dafür ein digitales Zertifikat ausstellen lassen. Ein signiertes Zertifikat ermöglicht bspw. das Anbieten einer HTTPS-Internetseite anstatt nur einer HTTP-Internetseite. Das dazu benötigte Schlüsselpaar wird mit OpenSSL oder ähnlicher Software erzeugt oder direkt mittels eines Webformulars der Zertifizierungsstelle.

ANWENDUNGS-PROGRAMMIERSCHNITTSTELLE
Syn. zu Application Programming Interface (API). Diese Schnittstelle stellt eine Verbindung von einem Programm zu einer Funktionssammlung dar. Darin sind Funktionen, die von einem Softwareprodukt oder Betriebssystem für andere Programme zur Verfügung gestellt werden. Z. B. bietet Microsoft Windows-Funktionen in sog. Bibliotheken an, um Fenster im typischen Windows-Stil erstellen zu können. Bei Online-Diensten, welche meist als Server-Client-Applikationen aufgebaut sind, werden solche API z. T. auch als Webservice bezeichnet.

AOB
Abk. für „Any other Business“, in der Bedeutung von „Irgendwelche anderen Themen zu besprechen?“

AOL
Ursprünglich eine Abk. für America Online. Zeitweise einer der größten Anbieter von Internetdienstleistungen.

AOL INSTANT MESSENGER [AIM] (engl.)
Instant-Messaging-Dienst der Firma AOL. Betrieben zwischen 1997 und 2017.

APACHE STRUTS
Framework zur vereinfachten Entwicklung von Java-Webanwendungen.

APACHE STRUTS BUG (engl.)
2018 entdeckter Softwarefehler, welcher rasch ausgebessert wurde. Aufgrund einer falschen Behandlung von Content-Type Headers innerhalb Apache Struts 2 könnte ein Angreifer Schadsoftware aus der Ferne auf infizierten Systemen ausführen.

API
Abk. für Application Programming Interface, Übsg. Anwendungs-Programmierschnittstelle.

API-ECONOMY
Neuere, unscharf definierte Bezeichnung zum Zusammenspiel von vernetzten Geräten und Diensten. Das Ziel ist „Business-APIs“ also Schnittstellen zw. Benutzer und Systeme anzubieten, um komplizierte Steuerungen zu vereinfachen. Bspw. die Steuerung der Licht- und Raumtemperatur-Schalter über eine App auf dem Handy.

APP
Abk. für Applikation. Syn. zu Software, Programm.

APP-LEICHE
Früher benutzte, möglicherweise durch neuere Applikationen abgelöste, Software, die nicht mehr aktuell gehalten wird, aber noch immer auf dem System gespeichert ist und aufgerufen werden kann. Dies stellt ein immer größer werdendes Sicherheitsproblem für Firmen und Hosting-Anbieter dar.

APPLE MAC OS
Betriebssystem von Apple, welches bspw. auf iMac läuft. Es basiert auf FreeBSD und Mach.

APPLICATION POOL
Software und Konfigurationsmethode innerhalb eines Servers zur Separierung von Applikationen, damit diese sich nicht gegenseitig beeinflussen. Falls eine Applikation auf dem Server stoppt, bspw. aufgrund eines Fehlers, können die anderen Applikationen auf dem gleichen Server unabhängig weiterlaufen.

APPLICATION PROGRAMMING INTERFACE [API] (engl.)
Übsg. Anwendungs-Programmierschnittstelle

APPLICATION SECURITY (engl.)
Teilgebiet der IT-Sicherheit, welches sich mit dem Schutz von (firmenrelevanten) Applikationen befasst, um diese vor internen und externen Attacken, vor Datendiebstahl und vor anderem Missbrauch abzusichern. Application Security wird bspw. erreicht durch die Überprüfung von eingegebenen Daten, durch den Einsatz von 2FA innerhalb der Applikation oder durch die Benutzung von Firewalls, Verschlüsselung u. Ä.

APPLICATION SHARING (engl.)
1) Gemeinsame Programmbenutzung bei Online-Games, Online-Whiteboards u. Ä. **2)** Darstellung einer Applikation auf mehreren Computern gleichzeitig, bspw. bei Videotelefonie.

APPSENSE
Softwareprodukt der Firma Ivanti zur Virtualisierung von Benutzerkonten und Benutzereinstellungen, um diese einfacher bei mehreren Systemen anzuwenden, sodass der Benutzer auf jedem dieser Systeme die gleichen Einstellungen vorfindet.

APP TO APP COMMUNICATION (engl.)
Übsg. Kommunikation zwischen Applikationen, um Daten auszutauschen. Bspw. kann eine Musik-App einer anderen App mitteilen, welche Musik z. Z. gespielt wird, damit die zweite App daraus Statistiken und Musikvorschläge erstellen kann. Die Kommunikation, insbesondere die Input- und Output-Beschreibung, muss dafür einer genau spezifizierten Syntax folgen, die auch als Protokoll bezeichnet wird. Dazu können vom Betriebssystem oder Webserver angebotene API-Funktionen und Bibliotheken dem Programmierer helfen, die Verbindung aufzubauen und Daten zwischen den Apps auszutauschen.

APP TO ENDPOINT COMMUNICATION (engl.)
Übsg. Kommunikation zwischen einer Serverapplikation und zugehörigen Clients.

APP-V
Abk. für Microsoft Application Virtualization

APT
Abk. für Advanced Persistent Threat

ARC4
Syn. zu Arcfour

ARCFOUR
Syn. zu ARC4. Open-Source-Strom-Chiffre und Stromverschlüsselungsalgorithmus, welche auf dem offiziell geheimen RC4 basieren.

ARCHIVIERUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Abschnitt im Lebenszyklus kryptografischer Schlüssel. Eine solche Archivierung ist nötig, um frühere Daten, welche mit diesem Schlüssel verschlüsselt wurden, noch immer validieren oder entschlüsseln zu können, obwohl evtl. bereits neuere Versionen des Schlüssels vorliegen.

ARCHIVIERUNG VON INFORMATION
Abschnitt im Lebenszyklus von Informationen. Für gewisse Informationstypen besteht eine rechtliche Verpflichtung zur Archivierung über eine bestimmte Archivierungsdauer.

ARCHIVING OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Archivierung eines kryptografischen Schlüssels

ARMS RACE SECURITY (engl.)
Sinnbildliches Wettrüsten in der IT Security. Ein Systemdesigner entwirft ein System, bei welchem der Angreifer anschließend eine Schwachstelle findet, welches der Designer danach repariert, woraufhin der Angreifer wieder eine Schwachstelle findet, welches vom Designer wieder repariert wird usw.

ARP
Abk. für Address Resolution Protocol

ARPANET
Abk. für Advanced Research Projects Agency Network. Ende der 1960er-Jahre über Telefonleitungen aufgebautes Computernetzwerk. Vorläufer des Internets.

ARP-PAKET
Zusammenstellung von Daten, die über das Address Resolution Protocol (ARP) im Netzwerk verschickt werden.

ARP REQUEST POISONING (engl.)
Syn. zu ARP-Spoofing

ARP-SPOOFING (engl.)
Syn. zu ARP Request Poisoning. Methode, um ARP-Pakete im Transfer zwischen zwei PCs, bspw. bei einer RDP-Sitzung, zu verändern und zu missbrauchen.

ARTIFICIAL INTELLIGENCE [AI] (engl.)
Übsg. künstliche Intelligenz

ASAP
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „As soon as possible“, Übsg. „So bald wie möglich“.

ASCII
Abk. für American Standard Code for Information Interchange. Ursprünglich 7-Bit, später auf 8-Bit erweiterte Zeichencodierung, für die eindeutige Definition von 128, später 256 Buchstaben, Zahlen und Sonderzeichen (siehe ASCII-Tabelle im Anhang bei Tab. 32.1).

ASCII-TABELLE
Aufstellung der eindeutigen Codierung von Buchstaben, Zahlen und Sonderzeichen (siehe ASCII-Tabelle im Anhang bei Tab. 32.1).

ASMR
Abk. für Autonomous Sensory Meridian Response. Gefühl des Kribbelns auf der Kopfhaut, im Nacken und auf der Wirbelsäule. Kann durch Geräusche ausgelöst werden und ist deswegen ein Trend auf YouTube.

ASN1
Abk. für Abstract Syntax Notation One. Internationaler Standard zur Beschreibung von zu übertragenden Datentypen und -strukturen. Dies findet Verwendung in der Entwicklung von Softwareprodukten oder auch im Mobilfunk. Es erlaubt die Beschreibung der ausgetauschten Informationen unabhängig von der Art der Informationsdarstellung durch die kommunizierenden Systeme.

ASP.NET
Abk. für Active Server Page .NET. Programmierumgebung von Microsoft, die es ermöglicht, unterschiedliche .NET-Sprachen zu benutzen, um Programme auf Servern zu entwickeln und auszuführen und damit dynamische Internetseiten und Apps zu erstellen.

ASPOSE API
Funktionsbibliotheken um Dateiformate zu bearbeiten, umzuwandeln, zu erstellen oder automatisiert auszulesen und zu ändern. Die Funktionen innerhalb dieser Bibliotheken können Microsoft-Office-Formate und andere Formate bearbeiten und bieten auch OCR an.

ASSERTIONS (engl.)
Übsg. Aussage, Behauptung

ASSET CLASSIFICATION (engl.)
Übsg. Klassifizierung von Systemen

ASTAROTH
Schadsoftware in Form eines Trojaners, welche u. a. das Anti-Viren-Programm Avast attackiert und dadurch ermöglicht, Login- und andere Benutzerdaten zu stehlen.

ASYMMETRIC CRYPTOGRAPHY (engl.)
Übsg. Asymmetrische Kryptografie

ASYMMETRIC ENCRYPTION (engl.)
Übsg. Asymmetrische Verschlüsselung. Syn. zu Public-Key-Verschlüsselung.

ASYMMETRISCHE KOMMUNIKATION
Kommunikation zwischen verschiedenartigen Kommunikationsteilnehmern.

Beispiel: Client-Server-System, bei welchem der Server mehrere Clients bedient.

ASYMMETRISCHE KRYPTOGRAFIE
Syn. zu Public-Key-Verschlüsselung. Oberbegriff für Methoden der asymmetrischen Verschlüsselung, bei welcher für die Ver- und Entschlüsselung unterschiedliche Schlüssel verwendet werden.

ASYMMETRISCHE VERSCHLÜSSELUNG
Syn. zu Public-Key-Verschlüsselung. Kryptografische Methode zur verschlüsselten Kommunikation ohne den Bedarf eines gemeinsamen geheimen Schlüssels. Dabei wird von jedem Kommunikationspartner eine Kombination aus privatem Schlüssel und öffentlichem Schlüssel benutzt. Damit wird ein großer Nachteil der symmetrischen Verschlüsselung vermieden, bei welcher derselbe Schlüssel von beiden Parteien zur Ver- und Entschlüsselung verwendet wird und deshalb zuerst vereinbart werden muss.

Prinzip der asymmetrischen Verschlüsselung: Ein Sender A benutzt den öffentlichen Schlüssel des Empfängers B zur Verschlüsselung der Nachricht und kann diese danach über ungesicherte Wege verschicken. Nur der Empfänger B, der im Besitz seines privaten Schlüssels ist, kann die Nachricht entschlüsseln.

ASYNCHRONE KOMMUNIKATION
Kommunikation, welche nicht über ein Taktsignal synchronisiert wird und bei der nicht auf die Antwort der anderen Partei gewartet wird, im Gegensatz zur synchronen Kommunikation.

Beispiel für asynchrone Kommunikation: Gespräch zwischen Menschen, die sich ins Wort fallen.

ATTACHMENT (engl.)
Übsg. E-Mail-Anhang

ATTACK AGAINST CLIENTS (engl.)
Angriff auf PCs der Kunden von ausgesuchten Firmen, bspw. mithilfe von E-Banking-Trojanern oder Phishing. Ziel ist sowohl die Beeinträchtigung der Kunden als auch der ausgesuchten Firmen.

ATTACKE
Angriffe auf Computer und Systeme durch die Ausnutzung von technischen oder sozialen Sicherheitslücken. Häufig ist unsaubere Programmierung die Ursache für technische Sicherheitslücken.

ATTACK SURFACE (engl.)
Übsg. Angriffsfläche

ATTACK SURFACE MODEL (engl.)
Stufenmodell zu möglichen Attacken, um an ein Zielsystem zu gelangen:
1. Stufe: Attacke auf Personen
2. Stufe: Attacke auf das Netzwerk
3. Stufe: Attacke auf das Zielsystem

ATTACK VECTOR (engl.)
Übsg. Angriffspunkt

ATTRIBUTION (engl.)
Übsg. Erkennen und Zuordnung von Merkmalen, bspw. zur Identifikation, Klassifikation und Abwehr von Schadsoftware.

AUDIO DATA ENCODING (engl.)
Verfahren in der Nachrichten- und Tontechnik zur Modulation und Demodulation von Audiodaten, wie Sprache oder Musik, auf einem hochfrequenten Trägersignal. Die Audiodaten werden dabei entweder zur Amplitude hinzuaddiert („AM“) oder die Frequenz des Trägersignals wird entsprechend den Audiodaten verändert („FM“).

AUDIO STREAM ENCRYPTION (engl.)
Übsg. Verschlüsselung eines Audiostroms. Dies wird bspw. zur verschlüsselten Übertragung von Kommunikation bei IP-Telefonie verwendet. Ein häufig benutztes Protokoll ist das Secure Real-Time Transport Protocol (SRTP), basierend auf AES-Verschlüsselung.

AUDIT TRAIL (engl.)
Verfahren und Dokumentation zum Nachweis der Einhaltung von firmeninternen oder regulatorischen Prozessen und Standards. Dabei wird angestrebt, einen lückenlosen Beweis für die richtige Durchführung der Prozesse oder Standards zu dokumentieren.

AUFBEWAHRUNGSDAUER
Angabe, wie lange bestimmte Daten mindestens (z. B. bei Verträgen) oder höchstens (z. B. bei digitalen Zertifikaten) aufbewahrt werden sollen, gemäß regulatorischer oder technischer Vorgaben. Bspw. sollte die Aufbewahrungsdauer eines digitalen Zertifikats möglichst kurz gesetzt sein und das Zertifikat nach Ablauf dieser Zeit erneuert werden, da der technische Fortschritt immer schnellere Hacking-Methoden erlaubt.

AUFFÄLLIGKEITEN
Syn. zu abnormem Verhalten. Bezeichnung für Unregelmäßigkeiten beim Betrieb von Systemen. Auffälligkeiten in Logs können ein Hinweis auf Manipulation sein.

AUSFALLSICHERUNG
Syn. zu Failover. Manuelle oder automatische Aktion, bei welcher die Datenkommunikation zwischen Systemen umgeleitet wird, falls ein Kommunikationspartner ausfällt. Z. B. werden Server häufig zweifach aufgebaut, sodass die Client-Server-Kommunikation zum zweiten Server umgeleitet werden kann, falls der erste Server ausfällt.

AUTH
Abk. für Authentication. Begriff wird u. a. bei User Auth Certificate verwendet.

AUTHENTICATION (engl.)
Übsg. Authentifizierung

AUTHENTICATION ASSURANCE (engl.)
Übsg. Stärke der Authentifizierungsmethode, die ein Benutzer zur Anmeldung an einem System benutzt. Bspw. ist eine Anmeldung mittels Benutzername und Passwort riskanter im Vergleich zur Anmeldung mittels 2FA-Methoden.

AUTHENTICATION DATABASE (engl.)
Datenbank innerhalb eines Handys, Computers oder Servers, oder innerhalb einer Applikation, in welcher der Benutzername zusammen mit den Benutzerberechtigungen gespeichert wird.

AUTHENTICATION MECHANISM ASSURANCE [AMA] (engl.)
Funktion bei Windows Active Directory, um einem Benutzer einen bestimmten Zugriff zu erlauben, basierend auf der Authentifizierungsart, die die Person benutzte. Im Detail erlaubt AMA das Hinzufügen eines Gruppenzugehörigkeitsidentifikators zum Kerberos-Token des Benutzers.

AUTHENTICATION PROCESS (engl.)
Übsg. Verfahren zur Authentifikation.

AUTHENTICATOR (engl.)
Syn. zu Authentisierungs-App

AUTHENTICATOR APP (engl.)
Übsg. Authentisierungs-App

AUTHENTICATOR SECRET CODE (engl.)
Vom Online-Dienst oder System dargestelltes Geheimnis zur Registrierung dieses Online-Dienstes oder Systems in einer Authentisierungs-App. Meist in Form eines QR-Codes oder eines Textes.

AUTHENTICATOR THREATS (engl.)
Angriffe auf Authentisierungs-Apps. Bspw. durch Modifikation oder Erzeugung falscher Bestätigungscodes, durch Diebstahl des Handys, durch Duplikation des Geheimnisses, durch Abhören der Übertragung, durch Brute-Force-Attacke, durch Auslesen des Speichers, durch Phishing oder durch andere Social-Engineering-Methoden.

AUTHENTIFIKATIONSMECHANISMEN
Verfahren zur Authentifizierung von Benutzer oder Systeme unter Benutzung von Protokollen, Signaturen, Tokens u. Ä.

AUTHENTIFIKATION VON NACHRICHTEN
Methode zur Überprüfung der Herkunft von Nachrichten. Dies kann bspw. mittels einer digitalen Signatur der Nachricht geschehen, welche mithilfe des privaten Schlüssels des Senders erstellt wird.

AUTHENTIFIZIERUNG
Syn. zu Authentication. Bei einer Authentifizierung verifiziert eine Partei B die Authentizität der Partei A. Das Resultat ist meist eine Autorisation der Partei A, sodass die Partei A das System oder darin enthaltene Dateien und andere Ressourcen benutzen darf.

Sprachgebrauch:

- Partei A authentisiert sich bei Partei B
- Partei B authentifiziert Partei A

Beispiel

Anwendungsbeispiele zur Authentifizierung:

Partei A kann ein Benutzer sein, der sich an einem Authentifizierungssystem (Partei B) authentisiert, mittels einer Kombination aus:

Benutzername und

a) einem Passwort (durch Eingabe über die Tastatur oder die Bildschirmtastatur),
b) seinem Fingerabdruck oder anderer biometrischer Erkennung,
c) seinem privaten Schlüssel,
d) seiner Position via Geolokationserkennung oder IP-Adresse,
e) einem vertrauenswürdigem Zertifikat,
f) einer App, welche die Programmierschnittstellen (GSSAPI) benutzt,
g) einem Authentifizierungsdienst, der sowohl Partei B als auch Partei A einen Token und eine Session-ID erstellt, die danach für die Transaktion zwischen A und B benutzt werden können und die Authentizität garantieren (Kerberos).

Die meisten dieser genannten Kombinationen (außer Fingerabdruck und anderer biometrischer Erkennung) können auch zur Authentifizierung zwischen zwei Servern benutzt werden.

AUTHENTISIERUNG
Überprüfung der Authentizität einer Partei, bspw. als Vorbereitung einer Kommunikation, oder um auf Dateien auf dem Server zuzugreifen. Ein Benutzer authentisiert sich an einem Server mit Benutzername und Passwort oder mit einem Zertifikat. Der Server authentifiziert die Angaben des Benutzers und erlaubt bei positiver Authentifizierung die weitere Kommunikation zwischen Benutzer und Server.

Sprachgebrauch:

- Partei A authentisiert sich bei Partei B
- Partei B authentifiziert Partei A

AUTHENTISIERUNGS-APP
Handysoftware zur Ermöglichung von Zweistufenauthentisierung (2FA) bei mehreren Systemen oder Online-Diensten mithilfe von Einmal-Kennwörtern. Dazu wird zuerst ein Geheimnis, meist in Form eines QR-Codes vom System oder Online-Dienst dargestellt und mit der Handy-App gescannt. Danach reicht zur Anmeldung jeweils der Benutzername mit Passwort und das synchron erzeugte Einmal-Kennwort beim System oder Online-Dienst und auf der Handy-App um den Benutzer zu authentifizieren. Viele Firmen, die Online-Einkäufe oder -Transaktionen anbieten, lassen sich mit einer solchen Authentisierungs-App koppeln.

Beispiele für Authentisierungs-Apps: a) Google Authenticator, b) Microsoft Authenticator, c) Symantec VIP Access.

AUTHENTIZITÄT
Gesamtheit der drei Eigenschaften Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit von Benutzern, Datenherkunft oder Geräten. Mithilfe von Verschlüsselungs- und Signaturverfahren kann die Authentizität sichergestellt werden und mittels Authentifikationsmethoden jederzeit überprüft werden.

AUTHORIZATION (engl.)
Übsg. Autorisation

AUTOMATISCHER INFORMATIONSAUSTAUSCH [AIA]
Globaler Standard der OECD für den automatischen Informationsaustausch von Finanzkontodaten zwischen beteiligten Staaten.

AUTOMATISCHES LERNEN
Syn. zu Deep Learning

AUTOMATISIERTER AKTIVER ANGRIFF [AAA]
Angriff, der automatisiert werden kann, um mit wenig Aufwand viele Systeme oder Dateien anzugreifen und zu verändern.

AUTONOMER ROBOTER
Syn. zu Hardware Agent. Kombination aus Software Agent, Sensoren und Aktuatoren, die zusammen Aktionen ausführen und die Umgebung verändern.

AUTORISATION
Einem Benutzer oder System erteiltes (digitales) Zugriffsrecht, um einen bestimmten Computer, ein bestimmtes System oder Dateien und andere Ressourcen darauf zu benutzen. Meist geht eine Authentifizierung voraus, um zu prüfen, ob die Authentizität des Benutzers oder Systems gewährleistet ist.

AUTOSPLOIT
Software, welche die Shodan API und Metasploit benutzt, um automatische Attacken auszuführen. Diese Software ist mit 400 Zeilen Python-Code sehr einfach und wird deshalb einerseits als Schadsoftware angesehen, andererseits auch als einfach zu verstehendes Lehrstück gegen Hacking.

AVAILABILITY (engl.)
Übsg. Verfügbarkeit

AVALANCHE
1) Netzwerk von Cyber-Kriminellen, die 2009 bis 2016 mehrere große Phishing-, Spam- und Ransomware-Attacken ausführten. **2)** Name eines Botnets

AVATAR
1) Grafische Repräsentation einer Person, bspw. als Profilbild anstelle des echten Bildes. **2)** Künstliche Person in Filmen, Spielen oder anderen Medien.

AWARENESS (engl.)
Übsg. Sensibilisierung

AWS
Abk. für Amazon Webservices

AZURE
Von Microsoft betriebene Plattform für Cloud-Services.

AZURE ACTIVE DIRECTORY [AAD] (engl.)
Verzeichnis innerhalb der Microsoft Azure Cloud, um Authentisierung und Autorisation von Cloud-Benutzern zu ermöglichen, bspw. für den Gebrauch von Microsoft Azure Information Protection.

AZURE ACTIVE DIRECTORY RIGHTS MANAGEMENT [AADRM] (engl.)
Syn. zu Windows Azure AD Rights Management. Ein Cloud- und AD-basierter Service innerhalb der Microsoft-Azure-Umgebung. Dieser Service wird von Azure Information Protection benutzt, um Verschlüsselung, sowie regel- und labelbasierten Benutzungseinschränkungen auf Daten anzuwenden. Nachfolger von Microsofts ADRMS.

AZURE AD
Abk. für Azure Active Directory

AZURE INFORMATION PROTECTION [AIP] (engl.)
Cloudbasierte Softwarelösung von Microsoft, um Klassifizierung, Verfolgung und Information Rights Management (IRM) bei Dateien und E-Mails anzuwenden. Dabei wird IRM mittels ADRMS- und AzureRMS-Verschlüsselung, Autorisation und Benutzungseinschränkungen umgesetzt. AIP kann mit Office 365-Labeling zu Microsoft Information Protection (MIP) kombiniert werden.

AZURE IP [AIP]
Abk. für Azure Information Protection

AZURE KEY VAULT (engl.)
Microsoft-Produkt zur Verwaltung von digitalen Schlüsseln innerhalb Microsofts Azure Cloud. Die Schlüssel können u. a. in Cloud-HSMs gesichert werden.

AZURE RIGHTS MANAGEMENT SYSTEMS [AZURERMS] (engl.)
Ein cloudbasierter Service innerhalb der Microsoft-Azure-Umgebung. Dieser Service wird von Azure Information Protection benutzt, um Verschlüsselung von Daten und regelbasierten Benutzungseinschränkungen auf Daten anzuwenden. Nachfolger von ADRMS.

AZURERMS
Abk. für Azure Rights Management Systems

B

4

BAAS
Abk. für Blockchain as a Service

BACKDOOR (engl.)
Übsg. Hintertür

BACKEND (engl.)
Übsg. Unterbau, hinteres Ende. Die Serverkomponente und darauf laufende Programme eines Client-Server-Systems.

BACKUP (engl.)
Methode zur Sicherung von Daten, um diese im Falle eines destruktiven Ereignisses wieder herstellen zu können. Für Firmen sind Backups und die Überprüfung der Backups existenziell wichtig. Auch Privatpersonen wird empfohlen ihre Daten, wie z. B. ihre Bilder, ihre Dokumente und ihre digitalen Bankbelege regelmäßig auf externen, nicht ständig angehängten, Festplatten oder auf vertrauenswürdigen Cloud-Speichern zu sichern, um diese nicht für immer zu verlieren.

BADRABBIT
Schadsoftware in Form von Ransomware

BANNER
1) Ein großflächiger Werbebereich auf Webseiten. **2)** Metadaten, die beim Anmelden und dem Zugriff eines Servers, Systems oder Geräts zuerst übertragen werden. Dies kann eine simple technische Begrüßung sein, es können aber auch Informationen sein über die vorhandenen Server-Software-Pakete oder andere Informationen, die für Clients interessant sein könnten.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_4

BASE32 ENCODED BINARY FILE (engl.)
Binärdatei, die in Base32-Kodierung vorliegt.

BASE32-KODIERUNG
Algorithmus zur Umwandlung von beliebig langen Binärdaten (z. B. Bilder, ZIP-Dateien) in eine Zeichenfolge aus ASCII-Zeichen, welche einfacher verarbeitet und gesendet werden können. Dabei werden die Binärdaten jeweils in Fünferpakete umgewandelt. Die Länge der erzeugten ASCII-Zeichenfolge ist dabei nicht fest vorgegeben.

Beispiel

Binärcode „00000“ = Base32 „0“
Binärcode „00001“ = Base32 „1“
Binärcode „00002“ = Base32 „2“
…
Binärcode „11111“ = Base32 „V“

BASE64 ENCODED BINARY FILE (engl.)
Binärdatei, die in Base64-Kodierung vorliegt.

BASE64-KODIERUNG
Algorithmus zur Umwandlung von beliebig langen Binärdaten (z. B. Bilder, ZIP-Dateien) in eine Zeichenfolge aus ASCII-Zeichen, welche einfacher verarbeitet und gesendet werden können. Dabei werden die Binärdaten jeweils in Sechserpakete umgewandelt. Die Länge der erzeugten ASCII-Zeichenfolge ist dabei nicht fest vorgegeben.

Beispiel

Binärcode „000000“ = Base32 „A“
Binärcode „000001“ = Base32 „B“
Binärcode „000002“ = Base32 „C“
…
Binärcode „111111“ = Base32 „/“

BASH BUNNY
Hacking-Tool, welches via USB-Stick auf ein System hineingebracht und ausgeführt wird.

BASIC
Höhere Programmiersprache, welche in vielen Varianten für fast alle Betriebssysteme vorhanden und sehr einfach zu erlernen und einzusetzen ist, da der Befehlssatz aus englischen Wörtern abgeleitet wurde.

Beispiel

Beispiel einer Basic-Programmzeile, die eine einfache Berechnung prüft und ein Resultat anzeigt:

```
IF 1+2=3 THEN PRINT "1+2=3"
```

BASIC-Programme können sowohl komplett in Maschinensprache umgewandelt (kompiliert) werden als auch zur Laufzeit interpretiert werden.

BCM
Abk. für Business Continuity Management

BCMUPNP_HUNTER
IoT Botnet, welcher Router angreift, die eine Schwachstelle in der UPnP-Funktion besitzen. Dadurch werden bspw. große Mengen an Spam-E-Mails verschickt.

BCP
Abk. für Business Continuity Planning

BCRYPT
Kryptografische Hash-Funktion, welche für Passwörter entwickelt wurde. Im Unterschied zu anderen Hash-Funktionen wie MD5 und SHA die mittels Brute-Force-Attacken oder Rainbow-Tabellen erraten werden können, wird bei Bcrypt ein einstellbarer Arbeitsaufwand zur Hashwert-Berechnung eingebaut, sodass die Berechnung künstlich länger dauert, was Angriffen entgegenwirkt.

BEARBEITUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Änderung der Daten eines Schlüssels, z. B. zur Aktualisierung des Verfallsdatums. Abschnitt im Lebenszyklus kryptografischer Schlüssel. Siehe zusätzliche Details beim Begriff Schlüssel.

BEARBEITUNG VON INFORMATION
Jegliche Änderung von Informationen. Abschnitt im Lebenszyklus von Informationen.

BEAST ATTACKE
Abk. für Browser Exploit Against SSL/TLS Attacke. Angriff auf eine Schwachstelle im CBC-Modus des Secure Sockets Layer Protokolls (SSL3.0 und TLS1.0). Dies ermöglicht Man-in-the-Middle-Angreifern, den Authentisierungs-Token oder das HTTP-Cookie abzugreifen und dadurch Zugang auf die übertragenden Daten zwischen dem Webserver und dem Webbrowser zu erhalten.

BEC
Abk. für Business E-Mail Compromise. Eine Social-Engineering-Methode, um Zugang zu Systemen von Firmen zu ergaunern.

BEENDIGUNG EINER BENUTZERBERECHTIGUNG
Eine erteilte Zugangsberechtigung zu einem System oder Onlinedienst wird aufgrund einer Zeitüberschreitung oder aufgrund anderer Gründe zurückgezogen. Der Benutzer muss sich erneut anmelden, falls der Zugang weiterhin verwendet werden soll.

BEGLAUBIGUNGSSTELLE
Syn. zu Zertifizierungsstelle und Certification Authority (CA). Vertrauenswürdige Organisation oder Firma, welche digitale Zertifikate ausstellt oder signiert, um die Authentizität von elektronischen Signaturen und Public-Private-Schlüsselpaaren zu bestätigen.

BEHANDLUNG VON CYBER-BEDROHUNGEN
Überbegriff für Identifizierung, Risikoanalyse, Protokollierung, Überwachung und Entschärfung von Cyber-Bedrohungen.

BENCHMARK (engl.)
Test oder Analyse von Apps, Prozessen, Verfahren oder Firmen bzgl. eines bestimmten Zustands oder einer bestimmten Eigenschaft, mit dem Ziel eines Vergleichs mit anderen, ähnlichen Apps, Prozessen, Verfahren oder Firmen.

BENUTZERKONTO
Daten innerhalb eines Systems oder Online-Dienstes, welche einem registrierten Benutzer eine eindeutige Identität mit Benutzername, Passwort, Zugriffsrechten und evtl. anderen Daten zuweisen.

BENUTZERNAME UND PASSWORT
Syn. zu Username und Passwort. Kombination für die Anmeldung eines Benutzers an einem System oder Online-Dienst, bei welchem er sich bereits registriert hat. Moderne Systeme verlangen zur Anmeldung zusätzlich eine Bestätigung mit einem 2FA-Verfahren, wie bspw. einem SMS-Code oder einem Einmal-Kennwort von einem Authenticator-Programm.

BENUTZER-VIRTUALISIERUNG
Benutzer-Virtualisierungssoftware entkoppelt die Benutzerprofile, -einstellungen und -daten sowie evtl. andere vorhandene benutzerspezifischen Informationen vom Betriebssystem und ermöglicht diese Informationen zentral zu speichern und zu verwalten. Diese Informationen lassen sich danach auf unterschiedliche Desktops anwenden, bspw. auf einem physischen PC oder auf einem virtuellen System in der Cloud.

BENUTZUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Kryptografische Schlüssel werden u. a. zur Anmeldung an einem System und zur Authentisierung eines Benutzers benötigt. Abschnitt im Lebenszyklus kryptografischer Schlüssel. Siehe zusätzliche Details beim Begriff Schlüssel.

BERECHTIGUNG
Syn. zu Bewilligung, Autorisation. Einem Benutzer aufgrund seiner vorher definierten Rechte vergebene Erlaubnis auf Daten, auf ein System oder auf ein Netzwerk zuzugreifen und evtl. Änderungen daran durchzuführen.

BERECHTIGUNGSNACHWEIS
Syn. zu Security Token. Wird vom Betriebssystem oder einem Credential Service Provider als Bestätigung von zuvor authentisierten Anmeldedaten eines Benutzers ausgestellt, und an Systeme oder Apps weitergegeben, damit diese den Benutzer nicht erneut nach seinen Anmeldedaten fragen müssen.

BERECHTIGUNGSSYSTEM
Syn. zu Entitlement Management System. Software zur Verwaltung von Berechtigungen mehrerer Benutzer für verschiedene Daten, Systeme oder Netzwerke. Mit der Anmeldung eines Benutzers an ein System oder Netzwerk werden ihm die mit seinem Benutzerkonto verknüpften Zugriffsrechte bereitgestellt. Mittels Definitionen von Benutzerrollen für gleiche Aufgaben können die Berechtigungen zentral und effizient verwaltet werden sowie JML-Prozesse umgesetzt werden.

BESEITIGUNG VON INFORMATION
Informationsbeseitigung geschieht bspw. durch Datenmaskierung oder durch Löschung von Informationen. Abschnitt im Lebenszyklus von Informationen.

BETAVERSION
Weitestgehend fertiggestellte Software, welche aber noch nicht vollständig getestet und zur Auslieferung bereit ist und somit als experimentelle und riskante Version anzusehen ist. Siehe auch Cutting Edge Technology, Leading Edge Technology.

BETRIEBSKONTINUITÄTSMANAGEMENT
Syn. zu Business Continuity Management (BCM). Strategien und Handlungen, um eine Firma, ein Netzwerk oder ein einzelnes System nach einem Ausfall schnellstmöglich wieder funktionsfähig zu stellen.

BETRIEBSSYSTEM
Syn. zu OS, Operating System. Software, welche beim Starten des Systems geladen wird und zwei Hauptziele verfolgt:

a) Den Benutzern des Systems eine digitale Arbeitsumgebung zu bieten, um mit Daten, Dokumenten, Programmen und verbundenen Geräten, wie bspw. einem Drucker zu arbeiten.
b) Den Speicher, die Festplatten, die Grafikkarte und alle anderen Ressourcen des Systems zu verwalten und anderen Programmen zur Verfügung zu stellen.

BETRIEBSSYSTEM- UND APPLIKATIONSUPDATES
Syn. zu Software-Aktualisierungen

BEWILLIGUNG
Syn. zu Autorisation, Berechtigung. Einem Benutzer aufgrund seiner vorher definierten Rechte vergebene Erlaubnis auf Daten, auf ein System oder auf ein Netzwerk zuzugreifen und evtl. Änderungen daran durchzuführen.

BGP
Abk. für Border Gateway Protocol

BIBLIOTHEK
1) Sammlung von Programmfunktionen (sog. „API“), welche anderen Programmen zur Verfügung gestellt werden. Solche Bibliotheken werden in den Quellcode eines neuen Programms eingebunden und bieten dadurch Funktionen an, um die Entwicklung neuer Software zu vereinfachen und zu beschleunigen, da die Funktionen nicht nochmals entwickelt werden müssen. Bspw. können optimierte Funktionen für kryptografische Berechnungen eingebunden werden, die mehrfach von unterschiedlichen Personen geprüft und auf Geschwindigkeit optimiert wurden. **2)** System, welches systematisch geordnete Informationen bereitstellt.

BIG ENDIANS (engl.)
Übsg. Groß-Endende. Reihenfolge der Bytebenutzung beginnend mit dem höchsten Byte, vergleichbar mit der Uhrzeit in der deutschen Sprache, die mit der größten Angabe beginnt (Stunde – Minute – Sekunde). Gegenteil: Little Endians.

Beispiel

Big Endians 0x23lFE343 wird als 23 1F E3 43 übertragen oder gespeichert
Little Endians 0x23lFE343 wird als 43 E3 1F 23 übertragen oder gespeichert

BILDSCHIRMSCHONER
1) Programm, welches nach einer vordefinierten Dauer, der sog. Timeout-Zeit, die andere Programme verdeckt und das System nur nach Reaktivierung bspw. durch Mausbewegung oder nach der Eingabe der Anmeldedaten wieder zugänglich macht.

Dies ermöglicht Ressourcen zu schonen und die Sicherheit zu erhöhen. Empfohlen wird, Timeouts und Bildschirmschoner bei allen Computern und Handys zu aktivieren und das System nur nach Eingabe der Login-Daten wieder freizugeben. **2)** Programm, welches nach einer vordefinierten Dauer, der sog. Timeout-Zeit, die anderen Programme verdeckt und ständig unterschiedliche Bereiche des Bildschirms einfärbt und damit verhindert, dass Teile der Leuchtschicht des (Kathodenstrahl-) Bildschirms durch dauernde Elektronenbestrahlung „einbrennen", d. h. sich nicht mehr regenerieren können. Diese Gefahr besteht seit Gebrauch von Flachbildschirmen kaum mehr.

BINÄRCODE
Zahlen oder Informationen, die nur mit den Werten „0" und „1" gespeichert oder verwendet werden. Beispiel: Der Buchstabe „A" entspricht im ASCII-Zeichensatz dem Binärcode „0100 0001".

BINÄRDATEI
Datei, deren Inhalt nur Binärcodes beinhaltet und somit nicht von Menschen lesbar ist. Ausführbare Dateien, bspw. mit der Endung „.exe" bei Windows, sind Beispiele von Binärdateien.

BINARY (engl.)
1) Übsg. Binärzahl, Binärcode. Zahlen oder Informationen, die nur mit den Werten „0" und „1" gespeichert oder verwendet werden. Beispiel: Der Buchstabe „A" entspricht im ASCII-Zeichensatz der Zahl „65", welche der Binärzahl „0100 0001" entspricht. **2)** Kompilierter, ausführbarer Programmcode. Auch „Executable" genannt.

BINARY HARDENING (engl.)
Software-Schutzmethode, bei der ausführbare Dateien analysiert und optimiert werden, sodass sie gegen bekannte Angriffe immun werden.

BING.COM
Internetsuchmaschine von Microsoft

BIOMETRIC AUTHENTICATION (engl.)
Übsg. Biometrische Authentisierung

BIOMETRIC IDENTIFICATION (engl.)
Übsg. Biometrische Identifizierung

BIOMETRIC INFORMATION (engl.)
Übsg. Biometrische Informationen

BIOMETRISCHE AUTHENTISIERUNG
Überprüfung der Authentizität einer Person mittels biometrischer Merkmale, wie Fingerabdruck, Irisabbild, Gesichtsform.

BIOMETRISCHE IDENTIFIZIERUNG
Überprüfung der Benutzeridentität mittels biometrischer Merkmale, wie Fingerabdruck, Irisabbild, Gesichtsform.

BIOMETRISCHE INFORMATIONEN
Biometrische Merkmale wie Fingerabdruck, Irisabbild, Gesichtsform, Stimmstruktur usw.

BIOS
Abk. für Basic Input/Output System. Erstes Programm, welches nach dem Einschalten des Computers geladen und ausgeführt wird, um die Konfiguration der Hardwarekomponenten des Computers zu überprüfen, sodass diese danach benutzt werden können.

BIT
Abk. für „Binary Digit“, Übsg. Binäre Ziffer. Kleinste Speichereinheit für Daten. Die Folge von 8 Bit bilden ein 1 Byte und erlauben die Speicherung von 256 unterschiedlicher Werte (siehe zusätzliche Informationen unter dem Begriff „Byte“ sowie in der ASCII-Tabelle Tab. 32.1).

BITCOIN
Bekannteste Kryptowährung

BITHUMB
Südkoreanische Börse für Kryptowährungen.

BITLOCKER
Software zur Festplattenverschlüsselung. Dieses Programm startet vor dem eigentlichen Start des Betriebssystems und benutzt ein Trusted Platform Modul (TPM), um zu validieren, ob Hardware am System verändert wurde.

BITTORRENT
Software und Protokoll, um Dateien zu verteilen und auszutauschen. Bei Benutzung ist darauf zu achten, nicht illegale, copyrightgeschützte oder virenverseuchte Dateien hoch- oder herunterzuladen.

BKA-TROJANER
Schadsoftware, in Form eines Erpressungstrojaners, welche missbräuchlich die Logos der Bundespolizei und des Bundesamts für Sicherheit in der Informationstechnik (BSI) verwendet und weltweite Verbreitung erzielte. Diese Malware behauptet, auf dem infizierten Rechner illegale Inhalte entdeckt zu haben und sperrt den Zugang zu diesen Inhalten bis zur Zahlung eines Betrags. Mithilfe von Informationen, die einfach auf Internetseiten zu finden sind, lässt sich dieser Trojaner umgehen und entfernen.

BLACK HAT HACKERS (engl.)
Übsg. Hacker mit „schwarzen Hüten“. Von Regierungen und Organisationen angestellte Hacker mit kriminellen Absichten.

BLACKHOLE
Toolsammlung in der Hackerszene, mit deren Hilfe Malware und Attacken ausgeführt werden.

BLACKLIST (engl.)
Übsg. Schwarze Liste

BLACKSHEEP
Internetbrowsererweiterung, die vor Mithören durch Firesheep warnt.

BLADE
Ugs. für einen Computer, auf dem virtuelle Maschinen (VMs) betrieben werden.

BLEEDING EDGE TECHNOLOGY (engl.)
Weitestgehend fertiggestellte Software, welche aber noch nicht vollständig getestet und zur Auslieferung bereit ist und somit als experimentelle und riskante Version anzusehen ist. Häufig auch als Syn. zu Betaversion verwendet. Siehe auch Cutting Edge Technology, Leading Edge Technology.

BLEICHENBACHER ATTACKE
Ein Angriff auf eine SSL-/TLS-Verbindung u. Ä., bei der eine Schwachstelle des Paddings bei der Verschlüsselung mit RSA gemäß PKCS#1 (v1.5) ausgenutzt wird.

BLOATWARE (engl.)
Für viele Benutzer unnütze Software, die auf neu gekauften PCs vorinstalliert ist und unnötig Speicherplatz verwendet.

BLOB
Abk. für Binary Large Object. Übsg. Großes binäres Objekt. Bei Datenbanken können große, in Binärcode vorliegende Datenmengen, wie Video-, Bild- oder Audiodateien, komplett als Feldinhalt des Typs BLOB gespeichert werden.

BLOCK
Zusammenstellung aufeinanderfolgender Zeichen zu einer Einheit, die gleichzeitig verarbeitet werden. U. a. bei Blockchiffre-Verfahren verwendet, bei welcher die Nachricht in gleich lange Blöcke aufgeteilt wird, die jeweils als Ganzes verschlüsselt werden, im Gegensatz zu Strom-Chiffre-Verfahren, bei welchen jedes Zeichen einzeln verschlüsselt wird.

BLOCKCHAIN (engl.)
Übsg. Blockkette. Aufbau verteilter Systeme mit verteilter Buchführung (auch Distributed Ledger genannt) zur Sicherstellung von Garantien, z. B. einer Kryptowährung wie Bitcoin. Jede neue Transaktion, z. B. der Kauf eines Bitcoins, wird kryptografisch als neues Kettenglied mit den bestehenden Datenblöcken früherer Transaktionen verknüpft (siehe Blockverkettung, Merkle Tree). Durch die Synchronisation der neuen Kette auf allen verteilten Systemen können Manipulationen erkannt werden, da jede Transaktion mittels Zurückrechnen auf Konsistenz überprüft werden kann. Die Entscheidung, ob eine neue Transaktion an die Blockchain angehängt werden darf, wird durch den verwendeten „Consensus Algorithm“ entschieden. Die Daten einer Transaktion beinhalten grundsätzlich die, mit dem privaten Schlüssel gesicherte, Sendersignatur, einen Transaktionswert, ein Transaktionsdatum, die Empfängeradresse und evtl. andere Informationen.

BLOCKCHAIN AS A SERVICE [BAAS] (engl.)
Von Microsoft, Oracle und anderen Firmen offerierte Lösung, um Blockchain in Firmen aufzubauen, ohne sich um die Grundlagen kümmern zu müssen.

BLOCKCHAIN SECURITY (engl.)
Übsg. Blockchain-Sicherheit. Methoden, um eine Blockchain zu schützen, bspw. durch Verwendung asymmetrischer Kryptografie.

BLOCKCHIFFRE
Syn. zu Block Cipher. Algorithmus in der Kryptografie zur Durchführung von Verschlüsselung und Entschlüsselung, bei der die Nachricht in Blöcke aus Zeichen oder Bits, meist gleichbleibender Anzahl, aufgeteilt wird, die jeweils zusammen verschlüsselt werden. Im Gegensatz zu Strom-Chiffre-Verfahren, bei welchen jedes Zeichen oder Bit einzeln verschlüsselt wird. Siehe auch Cipher.

Beispiel

Beispiele für Blockchiffre-Verfahren sind AES und DES.
Betriebsmodi bei Blockchiffre:

a) Electronic Codebook Mode (ECB)
b) Cipher Block Chaining Mode (CBC)
c) Counter Mode (CTR)
d) Galois/Counter Mode (GCM)
e) Cipher Feedback Mode (CFB)
f) Output Feedback Mode (OFB)

BLOCK CIPHER (engl.)
Übsg. Blockchiffre

BLOCKING (engl.)
Übsg. Blockieren. Ein Beispiel ist das Blockieren von Anfragen an einen Server durch Schließung eines Netzwerkports.

BLOCKING APP (engl.)
Übsg. Blockierende App. Software, die einen Einsatz eines ganzen Systems blockiert.

BLOCKVERKETTUNG
Verfahren bei Verschlüsselungsmodi wie z. B. dem CBC-Modus. Dabei werden die einzelnen Blöcke nicht unabhängig voneinander verschlüsselt, sondern werden mathematisch verkettet.

BLOG
Abk. für Weblog, aus „Web“ für Internet und „Log“ für Tagebuch. Webseite, die von einem Blogger (aba. Weblogger) erstellt und aktualisiert wird, um bspw. seine Gedanken und Erfahrungen zu einem Thema, einem Produkt oder zu einer Reise zu dokumentieren.

BLOWFISH
Cipher und Verschlüsselungsalgorithmus. Empfohlener Algorithmus für Passwort-Hashing, anstatt MD5, SHA1 oder SHA256, da Blowfish den Einbezug von „Salt“ ermöglicht und ausreichend langsam ist, sodass Brute-Force-Attacken sehr lange dauern würden.

BLUEKEEP
Schadsoftware in Form eines Erpressungstrojaners, der ältere Versionen von Windows angreift und nicht nur die Daten auf dem infizierten, sondern auch auf anderen

Windows-PCs im lokalen Netz verschlüsselt und erst nach Zahlung eines Betrags in Bitcoins wieder entschlüsselt, falls überhaupt. Bluekeep basiert auf einer Schwachstelle im Remote-Desktop-Protokoll (RDP). Da Bluekeep eine hohe Gefahr darstellt, stellte Microsoft 2019 auch für die älteren, offiziell nicht mehr unterstützten Windows-Versionen einen Patch bereit.

BOILERPLATE (engl.)
Übsg. Vorformulierter Text

BOOTEN
Starten des Betriebssystems angestoßen durch das BIOS.

BOOTER
Im Deep and Darknet gehandelte Software, um DDoS-Attacken durchführen zu lassen.

BOOTKIT (engl.)
Schadsoftware, welche beim Booten eines Systems aktiv wird und Sicherheitsmechanismen des Computers aushebelt.

BOOTSTRAP/BOOTSTRAPPING (engl.)
Übsg. Stiefelriemen. **1)** Freie Funktionsbibliothek, ursprünglich von Twitter, zur einfacheren HTML-, JavaScript- und CSS-Programmierung von ansprechenden Internetseiten. **2)** Das Entwickeln, Aktivieren oder Starten komplexer Systeme oder Programme auf Basis einfacherer Systeme oder Programme. Beispiel: Starten eines Betriebssystems („Booten“) durch das einfache BIOS. **3)** Aktivieren von Tools auf Clients durch Aufbau einer Kommunikation mit einem Server. **4)** Erster Aktivierungsprozess von Server oder Clients in komplexen Aufbauten und Client-Server-Systemen.

BORDER GATEWAY PROTOCOL [BGP] (engl.)
Routingprotokoll im Internet, bei welchem der Weg von Netzwerk zu Netzwerk definiert wird.

BÖSWILLIGER INSIDER
Syn. zu Malicious Insider. Person, welche offiziell Zugang zu Systemen und Netzwerken hat und diese missbraucht, um Daten zu stehlen, Daten zu manipulieren oder das System anderweitig zu beeinträchtigen. Solche Personen können interne Angestellte, externe Berater, oder andere Personen mit Zugang sein. Ein erfolgreicher Schutz gegen Attacken solch böswilliger Insider ist die Kombination aus rollenbasiertem Zugang („Need-to-know“-Prinzip) und eine Whistleblowerkultur, in welcher verdächtiges Verhalten von Kollegen ohne Angst vor negativen Folgen mitgeteilt werden kann.

BÖSWILLIGER OUTSIDER
Syn. zu Malicious Outsider. Person, die mittels Hacking oder Social Engineering versucht, von außerhalb einer Firma oder von außerhalb eines Systems, auf Computer, Netzwerke oder auf Daten zuzugreifen, für welche diese Person offiziell keinen Zugang hat.

BOT
Software, welche autonom und automatisch repetitive Aufgaben ausführt. Bekannt sind v. a. die Chatbots, welche als künstliche Support- oder Verkaufsansprechkontakte auf Internetseiten von Firmen auftreten und Standardfragen kostengünstig beantworten. Auch Suchbots (aba. Crawler) werden seit Längerem zur Aktualisierung von Suchmaschinen eingesetzt.

BOTNET (engl.)
Übsg. Botnetz

BOTNETZ
Vernetzte Systeme, wie PCs, Routers, Webcams etc., die zusammen, ferngesteuert oder zeitgeschaltet einen DDoS-Angriff auf ein Zielsystem ausführen, oder dieses Zielsystem missbrauchen, um Spam-E-Mails zu verschicken oder Malware zu verbreiten.

Beispiele für Botnetze: Avalanche, Dropperbot, Satori.

BOUNCER
Googles Virencheck bei eingereichten neuen Apps für Google Play.

BRAND ABUSE (engl.)
Übsg. Markenmissbrauch. Cyber-Bedrohung, bei welcher eine Produktmarke mittels eines Angriffs auf die Firmensysteme beeinträchtigt wird.

BREACH (engl.)
Abk. für Security Breach

BREACHED DATA TYPES (engl.)
Übsg. Datentypen, welche bei einer Sicherheitsverletzung beeinträchtigt wurden.

BRI
Abk. für Business Risk Intelligence

BRIDGE (engl.)
Übsg. Brücke. Verbindungsgerät zwischen zwei Netzwerksegmenten, ähnlich einem Switch.

BRING YOUR OWN DEVICE [BYOD] (engl.)
Übsg. Bringe dein eigenes Gerät. Benutzung des eigenen Geräts innerhalb des Firmennetzwerks. Dies wurde in den letzten Jahren in vielen Firmen ermöglicht und akzeptiert, bedeutet jedoch auch ein Risiko für die Firmen.

BRING YOUR OWN KEY [BYOK] (engl.)
Von Firmen mit sensiblen Daten gewählte Konfiguration innerhalb Azure Information Protection, bei welcher der Verschlüsselungshauptschlüssel durch die Firmen selber erzeugt und bewirtschaftet, aber im Gegensatz zu HYOK außerhalb der Firmengrenzen („Off-Premises“) gespeichert und benutzt wird.

BROADCAST (engl.)
Übsg. Kommunikation, die von einer Partei an alle anderen involvierten Parteien erfolgt, im Gegensatz zu Unicast und Multicast (Tab. 4.1).

BROWSER (engl.)
Syn. zu Webbrowser, Internetbrowser. Programm, um Internetseiten anzusehen.

BROWSER COOKIE (engl.)
Vom Internetbrowser auf dem PC des Benutzers gespeicherte Textdateien, welche von Skripts innerhalb der Internetseiten erstellt, geändert und ausgelesen werden. Dadurch werden bspw. die angesehenen Produkte auf Shoppingseiten gespeichert, um diese dem Benutzer nochmals offerieren zu können. Browser Cookies werden auch zur Verfolgung der vom Benutzer besuchten Seiten eingesetzt, sodass zielgerichtete Werbung dargestellt werden kann. Deswegen wird das regelmäßige oder zumindest gelegentliche Löschen der Cookies empfohlen.

BROWSERERWEITERUNG
Programm, das innerhalb eines Internetbrowsers eingebunden wird und zusätzliche Funktionen anbietet, die der Browser in der Standardversion nicht mitbringt. Beispiel: Passwortgenerator, AD-Blocker.

Tab. 4.1 Beispiele für Broadcast, Unicast, Multicast

Beispiel für Broadcast	Fernsehsendung eines öffentlich-rechtlichen Fernsehsenders
Beispiel für Unicast	FTP-Verbindung zwischen zwei Computern
Beispiel für Multicast	Fernsehsendung eines Bezahlsenders

BROWSER-KRIEG
Wettrennen von ca. 1995 bis 2005 zwischen dem Netscape Webbrowser und dem Microsoft Internet Explorer um den Titel des am häufigsten benutzten Webbrowsers. Erst war Netscape deutlich voraus, wurde jedoch aus dem Markt gedrängt und günstig an den Online-Dienst AOL verkauft, da Microsoft den Internet Explorer bei Windows vorinstalliert mitlieferte.

BROWSER WAR
Übsg. Browser-Krieg.

BRUTE-FORCE (engl.)
Hacking-Methode, bei der alle möglichen Schlüssel oder Passwörter durchprobiert werden, bis der Klartext vorliegt oder der Zugang offen ist. Dabei werden bspw. alle Wörter zahlreicher Wörterbücher durchprobiert, da Passwörter häufig aus echten Wörtern bestehen. Durch die ständig steigende Geschwindigkeit der bezahlbaren PCs können immer größere Brute-Force-Attacken durchgeführt werden. Deshalb sollten Passwörter nicht aus echten Wörtern irgendeiner Sprache bestehen und die Gültigkeitsdauer neuer Zertifikate sollte kleiner gewählt werden als die konservativ gerechnete Zeit, die eine Brute-Force-Attacke benötigen wird, während der Gültigkeitsdauer des Zertifikats.

BSI
Abk. für Bundesamt für Sicherheit in der Informationstechnik. Zivile Bundesbehörde in Deutschland, welche für Themen der IT-Sicherheit zuständig ist und allg. verständliche Tipps anbietet.

BSI 100-1/100-2/100-3/100-4/200-1/200-2/200-3
Vom deutschen Bundesamt für Sicherheit in der Informationstechnik definierte Standards zu

a) Managementsystemen für Informationssicherheit (100-1/200-1),
b) IT-Grundschutz-Vorgehensweise (100-2/200-2),
c) Risikoanalyse auf der Basis von IT-Grundschutz (100-3/200-3),
d) Notfallmanagement (100-4).

BUCKETS AND OBJECTS (engl.)
Der Filehosting-Dienst S3 („Simple Storage Service“) von Amazon basiert auf dem Konzept von Buckets and Objects, welche vergleichbar sind mit Verzeichnissen und Dateien.

BUFFER OVERFLOW (engl.)
Übsg. Pufferüberlauf

BUFFER OVERFLOW ATTACK (engl.)
Übsg. Puffer-Überlauf-Angriff. Hacking-Methode, bei der ein Speicherbereich durch ein Programm überschrieben wird, der nicht vom Programm beschreibbar sein sollte. Dies kann bei Programmiersprachen wie „C“ geschehen, die keine Überprüfung der Adressierung vornehmen. Dadurch wird das System unstabil oder schädlicher Code wird eingefügt und ausgeführt. Moderne Betriebssysteme versuchen, solche Attacken zu verhindern, indem bspw. der Speicher nicht sequenziell an die Programme vergeben wird, sondern zufällig.

BUG (engl.)
Übsg. Käfer, Programmfehler. Die Bezeichnung stammt aus den Zeiten, als elektronische Bauteile so groß waren, dass Käfer darauf Kurzschlüsse erzeugen konnten.

BUG BOUNTY PROGRAM (engl.)
Große Software-Hersteller bieten privaten Personen Geld an, falls diese Sicherheitslücken in der Software finden und melden, bevor diese Lücken von Hackern ausgenutzt werden. Dies verhindert nicht nur Attacken und Exploits, sondern auch Rufschädigung.

BULLETIN BOARD SYSTEM [BBS] (engl.)
Syn. zu Mailbox, elektronisches schwarzes Brett.

BUNDESGESETZ ÜBER DEN DATENSCHUTZ [DSG]
Schweizer Datenschutzgesetz, in weiten Teilen parallel zu GDPR.

BUNDES-TROJANER
Ugs. Bezeichnung für Software in Form von Trojanern, die von deutschen Bundesbehörden entwickelt und zur Strafverfolgung benutzt wird.

BUSINESS CONTINUITY MANAGEMENT [BCM] (engl.)
Übsg. Betriebskontinuitätsmanagement

BUSINESS CONTINUITY PLANNING [BCP] (engl.)
Übsg. Betriebskontinuitätsplanung

BUSINESS E-MAIL COMPROMISE [BEC] (engl.)
Betrugstyp, welcher mit einer E-Mail beginnt und Personen mithilfe von Social Engineering dazu verführt, Geld zu transferieren. Häufig wird in der E-Mail vorgegaukelt,

dass eine Person im höheren Management die Geldüberweisung fordert und diese schnellstmöglich erfolgen soll.

BUSINESS RISK INTELLIGENCE [BRI] (engl.)
Wissen aus vergangenen Cyber- und physischen Attacken. Dieses Wissen kann sowohl für firmeninterne Strategieentscheidungen genutzt werden als auch zur Vorbereitung auf mögliche, zukünftige Cyber-Attacken.

BYOD
Abk. für Bring Your Own Device

BYOK
Abk. für Bring Your Own Key

BYPASS AUTHENTICATION (engl.)
Übsg. Umgehen der Authentisierung.

BYTE
Speicherbedarf für ein Zeichen. Die Folge von 8 Bit bilden ein 1 Byte und erlauben die Speicherung von 256 unterschiedlicher Zeichen (siehe ASCII-Tabelle Tab. 32.1).

Vielfaches von Bytes wurden früher als Faktoren von 1024 angegeben, werden heute jedoch überwiegend als Faktoren von 1000 benutzt (Tab. 4.2).

Tab. 4.2 Vielfaches von Bits and Bytes

Abkürzung	Bezeichnung	In der nächsttieferen Einheit	10er-Potenz
1 B	1 Byte	8 Bit	10^0 Byte
1 kB	1 Kilobyte	1000 B	10^3 Byte
1 MB	1 Megabyte	1000 kB	10^6 Byte
1 GB	1 Gigabyte	1000 MB	10^9 Byte
1 TB	1 Terabyte	1000 GB	10^{12} Byte
1 PB	1 Petabyte	1000 TB	10^{15} Byte
1 EB	1 Exabyte	1000 PB	10^{18} Byte
1 ZB	1 Zettabyte	1000 EB	10^{21} Byte
1 YB	1 Yottabyte	1000 ZB	10^{24} Byte

C

5

C#
Höhere objektorientierte Programmiersprache. Der Name wird als „C-Sharp“ ausgesprochen.

CA
Syn. zu Certification Authority, Certificate Authority. Übsg. Beglaubigungsstelle. Syn. zu Zertifizierungsstelle.

CACHE POISONING (engl.)
Übsg. Speichervergiftung. Angriff auf DNS, bei welchem die Zuordnung von Domainnamen zu IP-Adressen manipuliert wird. Hierbei werden gefälschte Einträge in den DNS-Cache des Benutzers eingeschleust, damit aufgerufene Daten scheinbar vom echten, tatsächlich jedoch von einem anderen Server gesendet werden.

CALLER ID SPOOFING (engl.)
Übsg. Verschleierung der Anruferkennung, v. a. in Voice-over-IP-Telefonnetzwerke.

CALM TECHNOLOGY (engl.)
Übsg. Ruhige Technologie. Geräte, die dem Benutzer nicht Technik und Informationen aufdrängen, sondern ihn nur peripher begleiten, ihm seinen Alltag unbemerkt verbessern und nur die minimalen Informationen anbieten, die wirklich hier und jetzt für ihn wichtig sind.

Beispiel: Ein vernetztes Haus, welches in dem Raum Licht einschaltet, in welches eine Person sich demnächst hineinbewegen wird.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_5

CANDIDACY MODEL (engl.)
Übsg. Kandidatur-Modell. Definition von System-Benutzer-Populationen, bspw. zur Festlegung, wer zu welcher Zeit eine neue Software eingespielt erhalten soll, um das Betriebsrisiko minimal zu halten.

CAPTCHA (engl.)
Abk. für „Completely Automated Public Turing Test to Tell Computers and Humans Apart". Prüfsoftware im Internet zur Sicherstellung, dass ein Formular von einer echten Person und nicht von einem Bot automatisch ausgefüllt wurde. Meist werden dem Benutzer dafür Bilder, einfache Rechnungen oder verzogene Texte zur Erkennung dargestellt und das erkannte Rätsel oder Wort vom Benutzer eingetippt. Die Erkennung oder Lösung des Rätsels ist für Menschen einfach, aber schwierig für maschinelles Erraten. Dadurch kann verhindert werden, dass massenweise, automatisch erzeugte Fake-Formulardaten eingegeben werden (siehe Abb. 5.1).

Durch die Anzeige und Erkennung von gescannten Bildern als CAPTCHA, bspw. handschriftliche Texte aus alten Büchern, werden diese durch die Eingabe oder Markierung von echten Personen katalogisiert und damit wird gleichzeitig Wissen generiert und bspw. für das Trainieren von neuronalen Netzen zugänglich gemacht (siehe Abb. 5.2).

CARBANEK GROUP (engl.)
Hacking-Gruppe

Abb. 5.1 Beispiel eines CAPTCHA-Rätsels, welches für Menschen einfach, für Bots jedoch schwierig zu lösen ist

Abb. 5.2 Beispiel eines CAPTCHA-Rätsels, welches genutzt wird zur Katalogisierung alter Bücher

CARD IDENTIFICATION NUMBER [CID] (engl.)
Übsg. Kartenidentifikationsnummer, Kartenprüfnummer. Zahl auf der Rückseite von Kreditkarten.

Andere Formate: Card Validation Code 2 (CVC2), Card Verification Value (CVV), Card Verification Value 2 (CVV2).

CARD SKIMMING MALWARE (engl.)
Schadsoftware zur Manipulation von Online-Shops, sodass eingegebene Kreditkartendetails in falsche Hände gelangen.

CARD VALIDATION CODE 2 [CVC2] (engl.)
Übsg. Kartenüberprüfungswert, Kartenprüfnummer. Zahl auf der Rückseite von Kreditkarten.

Andere Formate: Card Verification Value (CVV), Card Verification Value 2 (CVV2), Card Identification Number (CID).

CARD VERIFICATION VALUE [CVV] (engl.)
Übsg. Kartenüberprüfungswert, Karteprüfnummer. Zahl auf der Rückseite von Kreditkarten.

Andere Formate: Card Validation Code 2 (CVC2), Card Verification Value 2 (CVV2), Card Identification Number (CID).

CA-ROOT-ZERTIFIKAT
Public-Key-Zertifikat einer Beglaubigungsstelle (CA). Diesem Basiszertifikat muss vertraut werden, damit darauf aufbauenden Zertifikaten in einer Vertrauenskette vertraut werden kann. Viele solche CA-Root-Zertifikate sind in aktuellen Webbrowsern vorinstalliert.

CAS
1) Übsg. Central Authentication Service. **2)** Übsg. Code Access Security. **3)** Übsg. Conditional Access System.

CÄSAR-VERSCHLÜSSELUNG
Kryptografieverfahren, welches angeblich bereits Cäsar angewendet haben soll, um Nachrichten geheim zu halten. Dabei wird eine Nachricht, Buchstabe für Buchstabe, um jeweils einen festen Wert des Alphabets zyklisch verschoben. Trotz der einfachen und damit unsicheren Verschlüsselung wird dieses Verfahren noch immer verwendet.

Beispiel: Cäsar-3-Algorithmus erstellt aus „TEXT“ den Geheimtext „WHAW“.

CASB
Abk. für Cloud Access Security Broker

CAST
Symmetrischer Blockchiffre-Algorithmus, der schnell und aktuell noch ungebrochen ist und u. a. in PGP enthalten ist.

CBA
Abk. für Certificate Based Authentication

CBC
Abk. für Cipher Block Chaining Mode

CENTRAL AUTHENTICATION SERVICE [CAS] (engl.)
Übsg. Identitätsmanagement-Webservice zur Authentifizierung von Kommunikationsparteien, um Daten auszutauschen. Hierbei verbleiben die Parteien und ihre Systeme unabhängig voneinander.

CERT
Abk. für Computer Emergency Response Team

CERT/CC
US-Behörde namens „CERT Coordination Center“ innerhalb des „Computer Emergency Response Teams“ der US-Homeland Security.

CERTIFICATE (engl.)
Übsg. Zertifikat

CERTIFICATE AUTHORITY [CA] (engl.)
Übsg. Zertifizierungsstelle. Syn. zu Certification Authority.

CERTIFICATE BASED AUTHENTICATION [CBA] (engl.)
Übsg. Zertifikatsbasierte Authentifikation. Diese Methode zur Identifikation von Benutzern, Geräten oder Systemen ermöglicht eine präzise Vergabe von Zugriffsrechten auf Daten, Apps, Netzwerken und Computern. Die Zertifikate können in einer Smartcard gespeichert werden oder verschlüsselt als Datei auf einem Gerät. Die Verteilung innerhalb einer Firma geschieht zentral, zunehmend cloudbasiert, und mit geringem Aufwand.

CERTIFICATE CHAIN (engl.)
Übsg. Zertifikatsvertrauenskette

CERTIFICATE ISSUING (engl.)
Übsg. Zertifikatsausstellung

CERTIFICATE MANAGEMENT PROTOCOL [CMP] (engl.)
Übsg. Verwaltungsprotokoll für Zertifikate in einer Public-Key-Infrastruktur, basierend auf dem X.509 Standard. Dieses Protokoll ermöglicht die Kommunikation zw. der Zertifizierungsstelle und dem Benutzer oder einer App.

CERTIFICATE OF TRANSPARENCY LOGS (engl.)
Experimenteller Sicherheitsstandard, um digitale Zertifikate zu überprüfen und zu beobachten. Dieser basiert auf einer öffentlich vorhandenen Liste von Zertifikaten. Damit soll es einfacher werden, Missbrauch von Zertifikaten zu erkennen.

CERTIFICATE PINNING (engl.)
Syn. zu HTTP Public Key Pinning. Methode, bei welcher speziellen Zertifikaten getraut wird, die nicht von einer Zertifizierungsstelle signiert wurden. Dies können bspw. Client- und Server-Zertifikate sein in einem geschlossenen Client-Server-System.

CERTIFICATE REVOCATION (engl.)
Übsg. Zertifikatsannullierung

CERTIFICATE REVOCATION LIST [CRL] (engl.)
Übsg. Zertifikatssperrliste, die beschreibt, welche Zertifikate nicht mehr gültig sind.

CERTIFICATE STORE (engl.)
Übsg. Zertifikatsspeicher. PC- oder Cloud-Datenspeicher für die sichere Aufbewahrung von digitalen Zertifikaten, die vom Anwender benutzt werden. Dies sind bspw. Root-Zertifikate von CAs oder auch self-signed Zertifikate. Im Unterschied zu einem Certificate Trust Store werden in einem Certificate Store beide Schlüssel, d. h. der öffentliche und der private Teil eines Public-Key-Zertifikats gespeichert. Der öffentliche Schlüssel hiervon kann exportiert und weitergegeben werden.

CERTIFICATE TRUST STORE (engl.)
Übsg. Vertrauenswürdiger Zertifikatsspeicher. PC- oder Cloud-Datenspeicher für die sichere Aufbewahrung von digitalen Zertifikaten, die vom Anwender benutzt werden. Dies sind bspw. Root-Zertifikate von CAs oder auch self-signed Zertifikate. Im Unterschied zu einem Certificate Store wird in einem Certificate Trust Store nur der öffentliche Schlüssel der Public-Key-Zertifikate gespeichert. Auf einem Windows-PC können die vorhandenen Zertifikate angesehen werden, indem die Microsoft Management Console via mmc.exe geöffnet und darin die Zertifikate via „Snap-in“-Menü-Eintrag geladen werden.

CERTIFICATION AUTHORITY [CA] (engl.)
Übsg. Beglaubigungsstelle. Syn. zu Certificate Authority.

CERTIFICATION OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Zertifizierung eines kryptografischen Schlüssels

CERTIFICATION REQUEST (engl.)
Übsg. Anforderung zur Zertifikatssignierung. Syn. zu Certification Signing Request.

CERTIFICATION SIGNING REQUEST [CSR] (engl.)
Übsg. Anforderung zur Zertifikatssignierung. Syn. zu Certification Request.

CERTIFIED INFORMATION SECURITY MANAGER [CISM] (engl.)
Zusatzausbildung und Zertifizierung im Bereich Datenschutz und Informationssicherheit, angeboten durch die „Information Systems Audit and Control Association“ (ISACA).

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL [CISSP] (engl.)
Weiterbildung und Zertifizierung im Bereich Datenschutz und Informationssicherheit, welche von $(ISC)^2$ angeboten wird.

CFB
Abk. für Cipher Feedback Mode

CFS
Abk. für Crypto File System

CHAKRACORE
Software innerhalb des Microsoft Edge Webbrowsers, um JavaScript-Zeilen zu interpretieren und auszuführen.

CHALLENGE-RESPONSE AUTHENTICATION (engl.)
Übsg. Abfrage-Antwort-Authentifikation

CHANGE MANAGEMENT (engl.)
Übsg. Veränderungsmanagement

CHANGE OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Änderung eines kryptografischen Schlüssels.

CHARACTER SET (engl.)
Übsg. Zeichensatz. Liste von Zeichencodierungen, d. h. eindeutige Zuordnung von Zeichen zu Werten. Beispiel ASCII, UTF-8 (siehe ASCII-Tabelle im Anhang Tab. 32.1).

CHEATING (engl.)
Übsg. Betrug. Meist im Zusammenhang mit Spielen verwendet.

CHECKSUM
Übsg. Prüfsumme

CHIEF INFORMATION SECURITY OFFICER [CISO] (engl.)
Rolle des Gesamtverantwortlichen für Informationssicherheit in einer Organisation.

CHIFFRE
Syn. zu Cipher. **1)** Ein durch Verschlüsselung erzeugter Geheimtext. **2)** Ein Algorithmus zur Ver- oder Entschlüsselung.

CHROME
Von Google entwickelter Webbrowser für viele Betriebssysteme.

CIA
1) Abk. für die drei Schutzziele der IT-Sicherheit: Confidentiality (Übsg. Vertraulichkeit), Integrity (Übsg. Integrität), Availability (Übsg. Verfügbarkeit). **2)** Abk. für Central Intelligence Agency, eine US-amerikanische Behörde.

CID
Abk. für Card Identification Number

CINCH
Koaxialer Steckertyp für Audio und Video

CIPHER (engl.)
Syn. zu Chiffre. **1)** Ein durch Verschlüsselung erzeugter Geheimtext. **2)** Ein Algorithmus in der Kryptografie zur Durchführung von Ver- und Entschlüsselung. Der Cipher beschreibt die genaue Abfolge der auszuführenden Rechnungen.

Es werden zwei Typen unterschieden:

a) Block Cipher, Übsg. Blockchiffre. Blöcke von Zeichen, meist gleichbleibender Anzahl, werden gleichzeitig und gemeinsam verschlüsselt.
b) Stream Cipher, Übsg. Strom-Chiffre. Einzelne Zeichen werden nacheinander verschlüsselt.

Beispiele für aktuell verwendete Ciphers: AES, 3DES, Blowfish, CAST, Arcfour u. a.

CIPHER BLOCK CHAINING MODE [CBC] (engl.)
Blockchiffre-Modus, welcher Verkettungen von Blöcken bei der Verschlüsselung verwendet und damit Schwachstellen des ECB-Modus umgeht. Der momentane Klartextblock wird dabei jeweils mit dem vorhergehenden Geheimtextblock kombiniert und zu einem weiteren Geheimtextblock verschlüsselt, welcher wiederum als Ausgangspunkt für die nächste Blockverschlüsselung dient usw. Begonnen wird eine solche Verkettung mittels eines Initialwertes („Initialization Vector“).

CIPHER FEEDBACK MODE [CFB] (engl.)
Blockchiffre-Modus, welcher Verkettungen von Blöcken bei der Verschlüsselung verwendet, jedoch den Klartext im Unterschied zu CBC an anderer Position einbindet und damit einer Strom-Chiffre ähnelt. Der erste Klartextblock wird dabei zuerst mit dem verschlüsselten Initialwert („Initialization Vector“) zu einem Geheimtextblock kombiniert. Dieser dient dann als neuer Initialwert, welcher verschlüsselt und mit dem nächsten Klartextblock zu einem weiteren Geheimtextblock kombiniert wird usw.

CIPHER SUITE (engl.)
Übsg. Chiffren-Sammlung. Kombination kryptografischer Verfahren. Bspw. definiert eine Cipher Suite für TLS die zu verwendeten Algorithmen zum Schlüsselaustausch, zur Authentifizierung, zur Verschlüsselung sowie die zu verwendete Hash-Funktion. Dabei erfolgt der Schlüsselaustausch meist mittels asymm. Algorithmus und sichert die Informationen, die für die Erstellung des gemeinsamen Schlüssels benötigt werden. Die Verschlüsselung der Nachricht erfolgt danach mittels symm. Algorithmus und die Hash-Funktion sichert die Integrität der Nachricht.

Die Beschreibung einer Cipher Suite folgt einem standardisierten Format (Tab. 5.1).

CIPR
Abk. für Cyber Incident Planning & Response

CIS
Abk. für Cyber- und Informationssicherheit

Tab. 5.1 Beispiel einer Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Abkürzung	Bedeutung
TLS	Protokoll
ECDHE	Schlüsselaustauschmethode
ECDSA	Signaturmethode
AES_256_GCM	Nachricht-Verschlüsselungsmethode
SHA384	Nachricht-Authentifikations-Hash-Funktion

CISA
Abk. für Cybersecurity Information Sharing Act

CISM
Abk. für Certified Information Security Manager. Zusatzausbildung im Bereich Datenschutz und Informationssicherheit.

CISO
Abk. für Chief Information Security Officer

CISSP
Abk. für Certified Information Systems Security Professional. Weiterbildung und Zertifizierung im Bereich Datenschutz und Informationssicherheit, welche von $(ISC)^2$ angeboten wird.

CITRIX XENAPP
Software auf einem Windows-Terminal-Server, der die Nutzung von zentral angebotenen Applikationen („published Apps“) oder ganzen virtuellen Desktops („published Desktop“) auf einfachen PCs oder Geräten ermöglicht, z. B. auf einem Thin Client oder auf einem Standard-Windows-PC. Die angebotenen Apps laufen dabei auf dem vollständigen, aber für den Benutzer versteckten, Windows-Server-Betriebssystem, werden dem Benutzer auf seinem einfachen PC bloß dargestellt und seine Eingaben zur Verarbeitung an den Server zurückgeschickt.

CLAMAV
Open-Source Anti-Viren-Scanner-Software

CLASSIFICATION (engl.)
Übsg. Datenklassifizierung

CLC
Abk. für Client Licensor Certificate

CLEAR-SKY-STRATEGY (engl.)
Übsg. Klarer-Himmel-Strategie. Ugs. Begriff, um das Gegenteil zur Cloud-Strategie anzudeuten.

CLEARTEXT BLOCK (engl.)
Übsg. Klartextblock

CLIENT (engl.)
Computer, Gerät oder Programm, welches mit einem Server verbunden ist, um Daten auszutauschen oder um Programme oder Dienste des Servers zu benutzen. Meist sind viele Server zentral in Datenzentren zusammengefasst und bedienen eine große Anzahl an Clients. Jeder Server wird für einen oder wenige Services aufgesetzt, z. B. als Webserver, als Windows-Server, als Datenbank etc.

CLIENT AND PERSONAL DATA (engl.)
Übsg. Kunden- und persönliche Daten.

CLIENT CERTIFICATE (engl.)
Digitales Zertifikat eines Clients, bspw. eines normalen PCs, zur Authentisierung gegenüber einem Server. Wird häufig zusammen mit einem User Certificate des Benutzers verwendet.

CLIENT LICENSOR CERTIFICATE [CLC] (engl.)
Bei Microsoft ADRMS benutztes Zertifikat, um den Benutzer zu identifizieren, sodass dieser Dokumente RMS-verschlüsseln kann. Mit dem CLC werden alle Publishing Licenses des Benutzers signiert, damit geprüft werden kann, von wem das Dokument verschlüsselt wurde.

CLIENT TO AUTHENTICATOR PROTOCOL [CTAP] (engl.)
Software zur Benutzung von Geräten, wie Handys oder physischen Security-Tokens, um Authentisierung durchzuführen, bspw. in Webbrowsern, die WebAuthn verwenden, oder in Desktop-Apps und Webdiensten. CTAP2 wird in Kombination mit WebAuthn für FIDO2 verwendet.

CLOSED SOURCE (engl.)
Gegenteil zu Open Source. Aufgrund der unbekannten Implementierung bestehen Risiken bei Closed Source Apps bspw. dadurch, dass die in der App implementierte Kommunikation zwar nachweisbar verschlüsselt wird, jedoch nicht nachgeprüft werden kann, ob nicht zusätzlich eine Hintertür eingebaut wurde.

CLOSED USER GROUP [CUG] (engl.)
Übsg. Eingeschränkter Benutzerkreis

CLOUD (engl.)
Übsg. Wolke. Sinnbild für nicht selber betriebene, ferne Server und Services, die nicht genau lokalisierbar und nicht im Detail bekannt sind und deshalb ähnlich einer Wolke irgendeine Form annehmen können. Derart verteilte Server und Services werden entweder selber von einer Privatperson oder einer Firma aufgesetzt und betrieben („Private

Cloud“), von anderen Firmen angeboten („Public Cloud“) oder kombiniert („Hybrid Cloud“). Siehe auch On-Cloud, Cloud-Computing.

CLOUD ACCESS SECURITY BROKER [CASB] (engl.)
On-Prem oder cloudbasierte Systeme, die Sicherheitsrichtlinien zwischen dem Cloud-Benutzer und dem Cloud-Service-Anbieter ermöglichen und durchsetzen, bspw. Authentisierung, SSO, Malware-Erkennung etc.

CLOUD-COMPUTING
Mietbare Lösungen von Cloud-Anbietern. Zur Auslagerung von Firmensoftware, Systeme und Infrastruktur.

Beispiele: a) Google Cloud Platform, b) Amazon Webservices, c) Microsoft Azure, d) Citrix Cloud

CLOUDHOPPER (engl.)
Hacking-Gruppe.

CLOUD SECURITY (engl.)
Teilbereich der IT-Sicherheit, in welchem der Schutz bei Cloud-Hardware, Cloud-Software, Cloud-Infrastruktur, Cloud-Diensten und anderen Cloud-Lösungen betrachtet und umgesetzt wird.

CLUSTER (engl.)
Mehrere Computer, die zusammenarbeiten und als ein System angesehen werden können. Bspw. werden derart zusammen verbundene Server unter einer einzigen IP-Adresse angesprochen und die Anfragen mittels eines Loadbalancers auf die einzelnen Server verteilt. Dies kann benutzt werden, um den Ausfall eines Servers abzufangen, oder um die Last auf die Server zu verteilen.

CMDLET
Abk. für Commandlets. Kleine, vordefinierte Befehle innerhalb einer PowerShell-Umgebung zur Ausführung einer spezifischen Aufgabe. Bspw. zeigt „Get-Process“ die laufenden Prozesse, „Get-Location“ zeigt das aktuelle Verzeichnis, „Get-Content“ zeigt den Inhalt einer Datei.

CMP
Abk. für Certificate Management Protocol

CMS
Abk. für Content Management System

CN
Abk. Common Name eines Zertifikats

COBINT
Programm, welches Schadsoftware im System installiert und bspw. über verseuchte E-Mail-Anhänge ins System gelangt.

COBIT
International akzeptierte und angewendete Vorgaben zur gesetzeskonformen Umsetzung von IT-Prozessen und IT-Kontrollen innerhalb von Firmen.

CODE ACCESS SECURITY [CAS] (engl.)
Übsg. Codezugriffssicherheit. Schutzmaßnahme im Microsoft .NET-Framework zur Verhinderung von kritischen Aktionen.

CODEBASE (engl.)
Übsg. Codebasis. Sammlung aller Quelltext- und Konfigurationsdateien, die in einem Projekt zusammengehören und beim Kompilieren verwendet oder benötigt werden.

CODEBUCH
Listen von Kombinationen aus Bedeutungen und zugehörigen Codes, die bspw. für Verschlüsselungen, Datenkompression und Datenübertragungen benutzt werden.

Beispiel

Beispiele möglicher Codes in Codebüchern:

a) Der Code „31“ kann eine Verschlüsselung oder geheime Botschaft bedeuten mit:
„1“ = „Treffen am Bahnhof“
„2“ = „Treffen beim Rathaus“
„3“ = „Paris“
„4“ = „Rom“
b) Der Morsecode „SOS“ kann codiert werden durch: o o o – – – o o o

CODE INJECTION (engl.)
Übsg. Einschleusung von Programmbefehlen oder Steuercodes bei Datenbankanwendungen mit dem Ziel, schädliche Datenbankaktionen auszuführen, um Daten zu verändern oder zu löschen, oder um Informationen aus der Datenbank zu erhalten, die nicht offengelegt werden sollten. Bis ca. 2010 war Code Injection möglich durch Missbrauch der Browseradresszeile bei HTTP GET-Aufrufen, die direkt in SQL umgewandelt wurden. Heutige Webserver erkennen Code Injection normalerweise und blockieren diese.

CODE REVIEW (engl.)
Übsg. Durchsicht eines Programmcodes. Methode zur Sicherstellung hoher Qualität bei Programmen und zur Verhinderung des Einbaus von Hintertüren durch den Programmierer.

CODE SIGNING (engl.)
Kryptografisches Verfahren, bei dem ausführbare Dateien oder Applikationen digital signiert werden, um den Entwickler und die Unversehrtheit der Datei oder der App zu bestätigen.

COGNITIVE COMPUTING (engl.)
Übsg. Kognitive Berechnungen. Technologie, die Signalverarbeitung mit künstlicher Intelligenz kombiniert, als Nachahmung des menschlichen Gehirns.

COLD BOOT ATTACK (engl.)
Übsg. Kaltstartattacke

COLLECTION #1
Sammlung mehrerer Mio. Benutzernamen und Passwörter, die aus verschiedenen Diebstählen stammten und als Paket im Internet 2018 frei zugänglich gemacht wurden. Durch Rainbow-Listen und Brute-Force-Kalkulationen wurden viele dieser Passwörter in Klartext umgewandelt und veröffentlicht, wodurch viele weitere Angriffe ermöglicht wurden.

COM
1) Abk. für Component Object Model. **2)** Eine der ersten Top-Level-Domains.

COM+
Teil des Component Object Model von Microsoft.

COMMAND-EXECUTION-EXPLOITS (engl.)
Syn. zu Remote Command Execution Exploits. Angriff eines Systems durch Ausnutzen einer Sicherheitsschwachstelle, mit der das Ausführen von Befehlen per Fernzugriff möglich ist.

COMMIT (engl.)
1) Bestätigung bei Datenbanken nach erfolgreicher Abarbeitung einer Transaktion. **2)** Vorgang des Speicherns und Freigebens von neuem oder geändertem Quelltext und anderen Dateien in einem Versionsverwaltungssystem. Syn. zu Check-in.

COMMODITY MALWARE (engl.)
Übsg. Schadsoftware, die einfach als käufliche oder kostenlose Ware zu erwerben ist und unverändert für viele Attacken eingesetzt werden kann.

COMMON NAME [CN] (engl.)
Zertifikatseintrag, in welchem der Servername oder der Aussteller definiert wird.
Beispiel: CN = www.domain.de

COMMON VULNERABILITIES AND EXPOSURES [CVE] (engl.)
Namenskonvention und Beschreibung für entdeckte Sicherheitslücken. Dabei bedeutet bspw. CVE-2018–1024 die Sicherheitslücke Nr. 1024, entdeckt im Jahr 2018. Die vollständige Liste wird geführt unter cve.mitre.org *(Abgerufen am 22.12.2019)*.

COMPILER (engl.)
Programm, welches einen Quellcode, der in einer Programmiersprache verfasst wurde, in einen maschinenlesbaren Code umwandelt, damit daraus ein ausführbares Programm entsteht. Compiler werden laufend optimiert, sodass nicht optimal programmierte Quellcodeteile automatisch ausgebessert werden. Gute Compiler erkennen auch Programmzeilen, die Sicherheitsrisiken bergen und verbessern solche Teile oder geben dem Programmierer Hinweise darauf.

COMPLIANCE TO REGULATORY REQUIREMENTS (engl.)
Übsg. Einhaltung von regulatorischen Anforderungen.

COMPONENT OBJECT MODEL [COM] (engl.)
Software, welche zur Kommunikation zwischen Prozessen in Windows-Systemen benutzt wird. COM kann als Funktionsbibliothek oder als ausführbares Programm aufgebaut sein.

COMPROMISED DATA (engl.)
Übsg. Kompromittierte Daten. Syn. zu beeinträchtigte, gehackte, unberechtigt benutzte, oder manipulierte Daten.

COMPUTER ACCESS CONTROL (engl.)
Übsg. Zugriffskontrolle zu Computer

COMPUTER CRIME (engl.)
Übsg. Computerkriminalität

COMPUTER EMERGENCY RESPONSE TEAM [CERT] (engl.)
Übsg. Expertengruppen, die Computersicherheitsvorfälle bearbeiten.

COMPUTERKRIMINALITÄT
Teilgebiet der Kriminalistik, die sich mit allen Formen von Angriffen auf Daten, Computer, Netzwerke, Software und Benutzer beschäftigt.

COMPUTER SECURITY (engl.)
1) Teilgebiet der Informatik, welche sich mit dem Schutz und den Attacken auf Computer und allg. auf IT-Infrastruktur beschäftigt. **2)** Gesamtheit aller Maßnahmen, die eingesetzt werden, um einen Computer, ein Computernetzwerk oder allg. IT-Infrastruktur vor Attacken und Schadsoftware geschützt zu halten.

COMPUTER WORM (engl.)
Übsg. Computer-Wurm

COMPUTER-WURM
Schadprogramm, welches sich selbstständig klont und auf andere Systeme im Netzwerk übertägt. Dabei nutzt das Programm Schwachstellen der Computer oder der Netzwerke aus.

CONDITIONAL ACCESS SYSTEM [CAS] (engl.)
System zur Zugangsberechtigung bei PayTV.

CONFIDENTIALITY (engl.)
Übsg. Vertraulichkeit

CONSENSUS ALGORITHM (engl.)
Übsg. Konsens-Algorithmus. Methode, die in der benutzten Blockchain-Variante bestimmt, ob eine neue Transaktion und damit ein neuer Block an die bestehenden Blockchain-Blöcke angehängt werden darf.

Bespiele für Konsens-Algorithmen:

a) Proof of Work, ohne Bestätigung einer zentralen Stelle (z. B. Bitcoin, Ethereum)
b) Proof of Authority, mit zentraler Stelle, die den neuen Block bestätigt
c) Proof of Stake, Akzeptanz eines neuen Blocks bei Zahlung eines Anteils

CONTENT MANAGEMENT SYSTEM [CMS] (engl.)
Übsg. Inhaltsverwaltungssystem. Software zur Erstellung und Aktualisierung von Inhalten für Webseiten. Ein CMS bietet vorprogrammierte Module, sodass die Benutzer sich auf den Inhalt konzentrieren können und keine Programmierkenntnisse benötigen.

Beispiele für ein populäres CMS: WordPress

CONTAINER (engl.)
Sammlung von Dateien, die zusammen in einer einzigen Datei gespeichert sind. Bekanntestes Bsp. sind ZIP-Container. Container können auch komplette virtuelle Computer sein, die damit mühelos als Datei von einem System auf andere Systeme kopiert werden können.

COOKIE (engl.)
Syn. zu Browser Cookie. Kleines Textfile auf dem PC des Webbrowserbenutzers. Darin werden Daten gespeichert, die die Funktionen einer Webseite unterstützen, bspw. durch Speicherung der bisher besuchten Artikel eines E-Shops.

COUNTER MODE [CTR] (engl.)
Blockchiffre-Modus, welcher Blockverkettungen verwendet und ähnlich wie CBC und CFB funktioniert. Bei CTR werden die Initialwerte („Initialization Vectors“) jeweils als fortlaufende Zahl, sog. Zähler oder Counter, gesetzt. Der erste Klartextblock wird dabei zuerst mit dem verschlüsselten ersten Initialwert zu einem Geheimtextblock kombiniert. Danach wird der zweite Initialwert vom Counter verschlüsselt und mit dem nächsten Klartextblock zu einem weiteren Geheimtextblock kombiniert wird usw.

CPU
Abk. für Central Processing Unit. Übsg. Hauptprozessor eines Geräts.

CRA
Abk. für Cyber Risk Assessment

CRAWLER (engl.)
Syn. zu Bot. Programm, welches das Internet nach neuen oder aktualisierten Seiten durchsucht, um den Suchindex einer Suchmaschine aktuell zu halten.

CREATION OF INFORMATION (engl.)
Übsg. Erzeugung von Information

CREDENTIALS (engl.)
Übsg. Berechtigungsnachweis für zuvor authentisierte Anmeldedaten. Allg. wird der Begriff Credential benutzt für Informationen, die den Benutzer identifizieren und die verwendet werden, um Zugang zu lokalen Ressourcen oder Netzwerkressourcen zu erhalten. Die Informationen können aus Benutzername und Passwort bestehen oder von einem Zertifikat bspw. auf einer Smartcard stammen.

CREDENTIAL SERVICE PROVIDER [CSP] (engl.)
Vertrauenswürdige Behörde, Firma oder Online-Stelle, die digitale Berechtigungsnachweise („Security Tokens“) ausstellt und damit die eindeutige Identität eines Benutzers mitsamt seiner Anmeldedaten bei einem Online-Service sicherstellt.

CREDENTIAL STUFFING ATTACK (engl.)
Angriff, bei welchem eine gestohlene oder gefundene Kombination aus Benutzername und Passwort automatisiert bei vielen Portalen eingegeben wird, um unberechtigten

Zugang zu erhalten. Dies ist häufig erfolgreich, da viele Personen die gleichen Kombinationen aus Benutzernamen und Passwort bei mehr als nur einem Portal benutzen.

CREDENTIAL VAULTS (engl.)
Übsg. Daten innerhalb eines Systems oder Geräts, in dem Berechtigungsnachweise, Anmeldedaten, Passwörter und kryptografische Schlüssel gespeichert werden.

CREEPER
Einer der ersten Viren, welcher sich in den 1970er-Jahren eigenständig im ARPANET-Netzwerk von Computer zu Computer fortbewegte, um PCs zu infizieren und daraufhin die Meldung „I'm the creeper: Catch me if you can" zu zeigen. Wurde durch das erste Anti-Viren-Programm „Reaper" eliminiert.

CRIME SYNDICATES (engl.)
Übsg. Organisierte Kriminalität

CRL
Abk. für Certificate Revocation List

CR LF
Abk. für Carriage Return and Line Feed. Standardeinstellung bei vielen Textprogrammen, um bei Drücken der „Enter"-Taste zum Anfang der nächsten Zeile zu gelangen. Einige Betriebssysteme verwenden hierfür keine Kombination, sondern nur CR oder nur LF.

CROSS-BOARDER DATA TRANSFER (engl.)
Übsg. Grenzüberschreitender Datentransfer

CROSS-SITE REQUEST FORGERY [CSRF] (engl.)
Übsg. Abänderung einer Webseitenanfrage im Webbrowser durch webseitenübergreifende Programme. Bsp. für eine solche Fälschungsaktion ist Cross-Site-Scripting.

CROSS-SITE-SCRIPTING [XSS] (engl.)
Übsg. Webseitenübergreifendes Scripting. Angriff auf ein System oder auf Daten eines Benutzers durch Hinzufügen von Schadsoftware bei Webseiten. Bspw. kann eine manipulierte Internetseite versteckt Schadsoftware in Form von JavaScript-Befehlen in die Datenfelder eines Formulars einfügen, die das Opfer daraufhin an einen Server sendet und damit die Schadsoftware ungewollt zur Ausführung bringt.

CRT
Abk. für Cathode Ray Tube, Übsg. Kathodenstrahlröhre. Technik für Kathodenstrahlröhrenbildschirme, welche bis ca. ins Jahr 2000 verwendet wurden. Danach mehrheitlich von Flachbildschirmen abgelöst, bspw. durch LCD-Monitore.

CRYAKL
Typ einer dateiverschlüsselnden Ransomware

CRYPTGENRANDOM
Funktion innerhalb der Win32 Crypto API-Funktionenbibliothek von Windows zur Berechnung von Zufallszahlen.

CRYPTOCURRENCY (engl.)
Übsg. Kryptowährung

CRYPTOCURRENCY ATTACKS (engl.)
Übsg. Angriffe auf eine Kryptowährung.
Beispiele: Front-Running-Attacke, Cryptojacking-Attacke.

CRYPTOCURRENCY EXCHANGES (engl.)
Übsg. Marktplatz für Kryptowährungen. Syn. zu Cryptocurrency Marketplaces.

CRYPTOCURRENCY MARKETPLACES (engl.)
Übsg. Marktplatz für Kryptowährungen. Syn. zu Cryptocurrency Exchanges.

CRYPTOCURRENCY MINING (engl.)
Übsg. Schürfen von Kryptowährung. Mathematische, kryptografische Methode, um mit geeigneter Software neue Kryptowährungseinheiten, wie z. B. neue Bitcoins herzustellen und diese digital, sicher und unveränderlich zu registrieren, bspw. innerhalb einer Blockchain. Das Mining ist eine zeit-, hardware- und energieintensive Berechnung, weshalb die „Miners“ für ihre Tätigkeit einen Anteil der Transaktionsgebühren oder eine Anzahl Einheiten der Kryptowährung erhalten. Um nicht durch den Einsatz von Cryptojacking-Attacken eine große Menge neuer Währungseinheiten zu erzeugen, und somit einfach reich zu werden, wird versucht, die Währung durch eine künstlich limitierte Menge an neu geschaffenen Einheiten jeden Tag stabil zu halten.

CRYPTO FILE SYSTEM [CFS] (engl.)
Übsg. Kryptografisches Dateisystem. Verschlüsseltes Dateisystem bei Unix-ähnlichen Betriebssystemen. Syn. zu Cryptographic File System.

CRYPTOGRAPHIC FILE SYSTEM (engl.)
Syn. zu Crypto File System

CRYPTOGRAPHIC KEY LIFECYCLE (engl.)
Übsg. Lebenszyklus kryptografischer Schlüssel

CRYPTOGRAPHIC SERVICE PROVIDER [CSP] (engl.)
Programmbibliothek, in Windows oder in einem HSM, welche kryptografische Funktionen zum Verschlüsseln, Entschlüsseln, zur Authentifizierung mit digitalen Zertifikaten und zur Erzeugung von (Pseudo-) Zufallszahlen beinhaltet.

CRYPTOGRAPHY (engl.)
Übsg. Kryptografie

CRYPTO-LOCKERS (engl.)
Erpressungsschadprogramm, welches Dateien des infizierten Systems verschlüsselt und nach einem Reboot die Zahlung von Bitcoins verlangt.

CRYPTO-MINERS (engl.)
1) Syn. zu Cryptojacking-Attacke. Auf Internetseiten ausgeführtes Kryptowährungsmining, welches ohne Kenntnis und Einwilligung des Webbrowserbenutzers ausgeführt wird. **2)** Personen, die Crypto-Mining legal ausführen.

CRYPTO-MINING (engl.)
Abk. für Cryptocurrency Mining

CRYPTO-WÄHRUNG
Syn. zu Kryptowährung

CRYPTOJACKING ATTACK (engl.)
Auf Internetseiten ausgeführtes Kryptowährungsmining, welches ohne Kenntnis und Einwilligung des Webbrowserbenutzers ausgeführt wird.

CRYPTOPRO SECURE DISK (engl.)
Software, um eine Authentisierungsfunktion zu BitLocker hinzuzufügen. Dies erlaubt die PreBoot Authentication, bei welcher die Harddiskverschlüsselung von BitLocker und die Benutzerauthentisierung von CryptoPro Secure Disk ausgeführt wird, bevor das System bootet.

CRYSIS
Schadsoftware in Form einer dateiverschlüsselnden Ransomware

CSP
1) Abk. für Credential Service Provider. **2)** Abk. für Cryptographic Service Provider.

CSR
Abk. für Certificate Signing Request

CSRF
Abk. für Cross-Site Request Forgery

CTAP
Abk. für Client to Authenticator Protocol

CTI
Abk. für Cyber Threat Intelligence

CTR
Abk. für Counter Mode

CU
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „See you“, Übsg. „Wir sehen uns“.

CUG
Abk. für Closed User Group

CURVE25519
Konkrete elliptische Kurve der Form

$$y^2 = x^3 + 486662x^2 + mod\left(2^{255} - 19\right)$$

Diese kann vergleichsweise schnell berechnet werden und wird deshalb in populären asymmetrischen Kryptografie-Algorithmen benutzt, bspw. bei WhatsApp, iOS, GPG etc.

CUSTODIAN (engl.)
Übsg. Verwalter, Beschützer. Syn. zu Data Custodian, Data Owner, Übsg. Dateneigentümer.

CUSTOMER EXPERIENCE [CX] (engl.)
Übsg. Kundenerfahrung. Gesamtheit der Interaktionen eines Kunden mit dem Verkäufer, mit dem gekauften Produkt und mit den in Anspruch genommenen Dienstleistungen des Verkäufers. Dies geht über den reinen Produktverkauf hinaus und hat das Ziel, den Kunden loyal an den Verkäufer zu binden und damit weitere Produkte verkaufen zu können.

CUSTOM HARDWARE ATTACK (engl.)
Übsg. Angriff mithilfe spezieller Hardware, welche viele schnelle Prozessoren enthält. Passwörter, digitale Schlüssel, verschlüsselte Nachrichten u. Ä. können mit derart gebauten Geräten schneller geknackt werden.

CUTTING EDGE TECHNOLOGY (engl.)
Beste oder allerneueste Technologie. Siehe auch Bleeding Edge Technology, Leading Edge Technology.

CVC2
Abk. für Card Validation Code 2

CVE
Abk. für Common Vulnerabilities and Exposures

CVV
Abk. für Card Verification Value

CX
Abk. für Customer Experience

CYBER (engl.)
Ugs. für Kybernetic, dem Themenbereich der Steuerung von Maschinen. Oft benutzt als Syn. zu Internet.

CYBER AND INFORMATION SECURITY [CIS] (engl.)
Übsg. Cyber- und Informationssicherheit

CYBER-ANGRIFF
Kriminelle Aktivität mit dem Ziel, Daten zu stehlen, Systeme zu verändern oder andere Beeinträchtigungen der Verfügbarkeit, Vertraulichkeit oder Integrität von Systemen von Firmen, Instituten oder Privatpersonen zu erreichen.

CYBER-ANGRIFFSSZENARIEN
Formen von Cyber-Angriffen. Unterschieden werden u. a. Denial of Service, Insider Data Theft, Hacking, Malware, Sabotage, Social Engineering Attacks, Payment Card Fraud, E-Banking Fraud, Social Media Incidents, Brand Abuse uvm.

CYBER CRIME (engl.)
Übsg. Internetkriminalität

CYBER ESPIONAGE (engl.)
Übsg. Internetspionage

CYBER FRAUD (engl.)
Übsg. Internetbetrug. Allg. Betrug, der mittels Computer, Geräten oder Internetseiten ausgeübt wird.

CYBER-HYGIENE
Maßnahmen, um die Sicherheit bei Internetbenutzung hochzuhalten. Dies beinhaltet u. a. Verwendung sicherer Passwörter, Installation von Updates, kein unbedachtes Öffnen von Links oder E-Mail-Anhängen und allg. aufmerksam bleiben.

CYBER INCIDENT PLANNING & RESPONSE [CIPR] (engl.)
Methoden und Arbeitsprozesse, um mit Cyber-Angriffen korrekt umzugehen und darauf zu reagieren.

CYBER INSURANCE (engl.)
Übsg. Versicherung gegen Schäden durch Internetkriminalität.

CYBER KILL CHAIN (engl.)
Übsg. Internetangriffsablauf. Syn. zu Kill Chain, Intrusion Kill Chain. Beschreibung der Phasen einer Cyber-Attacke.

Diese sind meist:

a) Erkundung eines Ziels
b) Auswahl der Angriffsmethode
c) Eigentlicher gezielter Angriff
d) Einbau eines Backdoors
e) Übernahme des Systems des Opfers

Die Abwehr bei jeder dieser Phasen kann den Angreifer von seinem Ziel abhalten. Somit kann das Bewusstsein dieser Phasen helfen Attacken zu analysieren und zu verhindern.

CYBER-KRIEG
1) Angriffe und Auseinandersetzungen im Internet. Syn. zu Internetkriminalität. **2)** Militärischer Krieg im digitalen Informationszeitalter.

CYBER-RISIKEN
Syn. zu Internetrisiken und Internetkriminalität. Risiken betreffen v. a. Datendiebstahl, Serviceausfall und Internetbetrug.

CYBER RISK ASSESSMENT [CRA] (engl.)
Teilgebiet des Risikomanagements, welches sich mit Internetkriminalität und allg. Cyber-Risiken beschäftigt.

CYBER RISKS (engl.)
Übsg. Cyber-Risiken.

CYBERSECURITY INFORMATION SHARING ACT [CISA] (engl.)
US-Gesetz (2015) zur Verbesserung der Internetsicherheit in den USA mittels verbesserten Austausches von Informationen über Cyber Security Threats. Das Gesetz definiert und erlaubt den Transfer von Internetinformationen zwischen dem US-Government und Firmen.

CYBER-SPACE (engl.)
Syn. zu Internet, virtuelle Welt.

CYBER-SPIONAGE
Spionage durchgeführt im oder mittels des Internets.

CYBER TALENT WAR (engl.)
Übsg. Kampf der Firmen um die besten Cyber-Security-Talente

CYBER THREAT INTELLIGENCE [CTI] (engl.)
Übsg. Cyber-Angriffswissen. Methoden, Tools und Wissen zur Abwehr von Cyber-Angriffen. Dabei wird u. a. das Wissen aus vergangenen Angriffen, aus analysierter Schadsoftware und aus dem Deep and Dark Web verwendet. Anti-Viren-Software kann bspw. als ein CTI-Tool angesehen werden.

CYBER THREAT MANAGEMENT (engl.)
Übsg. Behandlung von Cyber-Angriffen. Dies beinhaltet Tools, Methoden, Prozesse und Personen zur Analyse, Abwehr und Verhinderung von Angriffen.

CYBER THREAT SCENARIOS (engl.)
Übsg. Cyber-Angriffsszenarien

CYBER- UND INFORMATIONSSICHERHEIT
Methoden, Strategien, Algorithmen und Organisationen, die die Absicht verfolgen oder unterstützen, die Sicherheit im Internet, bei IT-Netzwerken, bei einzelnen PCs und bei Geräten zu erhöhen. Das Ziel ist die Aufrechterhaltung der Integrität, der Vertraulichkeit und der Verfügbarkeit von Daten und Systemen. Oft wird dies abgekürzt mit CIA für Confidentiality, Integrity and Availability.

CYBERWAR (engl.)
Übsg. Cyber-Krieg

CYBERWARFARE (engl.)
Übsg. Cyber-Krieg

D

6

Dab+
Abk. für Digital Audio Broadcasting (plus)

DANABOT
Schadsoftware in Form eines Trojaners speziell gegen Banken.

DANE
Abk. für DNS-based Authentication of Named Entities

DAO BUG
Fehler innerhalb einer 2016 aufgesetzten „Decentralized Autonomous Organization" für die Kryptowährung Ether. Dies ermöglichte einen Angriff auf Ether.

DARKNET (engl.)
Syn. zu Deep and Dark Web. Teil des Internets, bei welchem kriminelle Aktivitäten vermutet werden, und auf die man meist nur mittels Einladung Zugriff erhält. Der Inhalt entsprechender Internetseiten kann von Musiktauschbörsen bis zu politisch motivierten Aktivitäten reichen. Die Kommunikation zw. Benutzern des Darknets erfolgt häufig verschlüsselt. Einladungen und Links zum Darknet werden unter der Hand weitergegeben und entsprechende URLs wechseln häufig, da deren längerer Gebrauch die Wahrscheinlichkeit erhöht aufzufliegen.

DAS
Abk. für DB2 Administration Server. Dieser Server legt fest, wie und wo die Authentifizierung eines Benutzers stattfindet.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_6

DAST
Abk. für Dynamic Application Security Testing

DATA ANONYMIZATION (engl.)
Übsg. Datenanonymisierung

DATA BREACH (engl.)
Übsg. Datenverletzung. Syn. zu Data Leak. Absichtlicher, unabsichtlicher oder unbewusster Datenverlust oder Verletzung der Datensicherheit. Ursache kann bspw. eine Phishing-Attacke sein, bei welcher das Opfer unfreiwillig seine Daten preisgibt.

DATA BREACH INCIDENT NOTIFICATION (engl.)
Übsg. Datenverlustmitteilung. Offizielle Bekanntgabe von Datenverlust, bspw. an einen Regulator. In einigen Ländern rechtlich zwingend notwendig.

DATA BREACH TYPES (engl.)
Übsg. Arten von Datenverlust

DATA CENTER (engl.)
Übsg. Datenzentrum, Rechenzentrum. Gebäude, in welchem die zentralen Computer und die Infrastruktur einer Firma oder Institution untergebracht ist.

DATA-CENTRIC SECURITY (engl.)
Übsg. Datenzentrierte Sicherheit. Wird unterschieden von Netzwerksicherheit, Serversicherheit, Anwendungssicherheit etc.

DATA CLASSIFICATION (engl.)
Übsg. Datenklassifizierung

DATA CUSTODIAN (engl.)
Übsg. Datenverwalter, Datenbeschützer. Syn. zu Data Owner, Übsg. Dateneigentümer.

DATA ENCRYPTION STANDARD [DES] (engl.)
Übsg. Datenverschlüsselungsstandard. Kryptografischer Algorithmus aus dem Jahre 1977 zum Schutz sensibler Informationen. Dieses symmetrische Verschlüsselungsverfahren basiert auf einer Blockchiffre mit 56-Bit Schlüssellänge und wurde bereits in den 1990er-Jahre gebrochen. Deswegen wird es heutzutage als unsicher angesehen. Verbesserte Nachfolger sind 3DES, AES.

DATA EXFILTRATION (engl.)
Übsg. (Böswillige) Datenentfernung. Dies kann durch Insider oder Outsider mittels diverser Methoden und Schadsoftware geschehen. Häufig ist die Data Exfiltration ein explizites Ziel von APT-Angriffen.

DATA EXPOSURE (engl.)
Übsg. Datenfreilegung. **1)** Gewollte Erstellung eines Datenzugangs. **2)** Unabsichtliche oder absichtliche Offenlegung von Daten wie bspw. Passwörter.

DATAGRAMM
Syn. zu Nachricht. Daten, die von einem System zu einem anderen System gesendet werden und neben den eigentlichen Informationen (Payload) nur wenige Header-Daten wie bspw. Empfangs- und Absenderadressen beinhalten.

DATA HIGHWAY (engl.)
Übsg. Datenhighway, Datenautobahn.

DATAIKU
Plattform für kollaborative Datenwissenschaft (Data Science) inkl. Algorithmen zur Ausführung von Berechnungen der künstlichen Intelligenz.

DATA INTEGRITY (engl.)
Übsg. Datenintegrität

DATA LAKE (engl.)
Übsg. Datensee

DATA LEAK (engl.)
Übsg. Datenverlust. Syn. zu Data Breach.

DATA LEAKAGE PREVENTION [DLP] (engl.)
Übsg. Datenverlustschutz

DATA LINEAGE (engl.)
Übsg. Datenherkunft. Bestimmung der Herkunft und der Veränderung von Daten in einem Data-Warehouse-System, häufig mit dem Ziel, einen Audit Trail sicherzustellen.

DATA MASKING (engl.)
Übsg. Datenmaskierung

DATA MINIMIZATION (engl.)
Übsg. Minimierung der Daten. Beispiel: Je weniger sensible Daten man mit sich trägt, desto kleiner das Risiko des Datenverlusts.

DATA MINING
Automatisierte und statistische Methoden zur Entdeckung von Merkmalen, Trends, Kategorien, Ausreißer etc. in großen Datenbeständen („Big Data“).

DATA OWNER (engl.)
Übsg. Dateneigentümer.

DATA PROTECTION (engl.)
Übsg. Datenschutz

DATA PROTECTION API [DPAPI] (engl.)
Abk. für Data Protection Application Programming Interface

DATA PROTECTION APPLICATION PROGRAMMING INTERFACE [DPAPI] (engl.)
Programmbibliothek in Windows zur einfachen Umsetzung von kryptografischen Berechnungen. Wird u. a. dazu verwendet, um mithilfe der Benutzer-Login-Daten eine symmetrische Verschlüsselung von asymmetrischen Benutzerschlüsseln zu berechnen, um diese sicher zu speichern.

DATA PROTECTION IMPACT ASSESSMENT [DPIA] (engl.)
Übsg. Datenschutzauswirkungsanalyse. Verpflichtende Anforderung gemäß GDPR §35. Diese beschreibt, dass eine Auswirkungsanalyse erfolgen muss, bevor eine neue Technologie eingeführt werden darf, welche möglicherweise Einfluss auf die Sicherheit von persönlichen Daten haben wird.

DATA PROTECTION OFFICER [DPO] (engl.)
Übsg. Datenschutzbeauftragter. Position und Funktion einer Person innerhalb von Firmen. Gemäß GDPR in definierten Situationen zwingend erforderlich.

DATA REPLICATION ALGORITHM (engl.)
Übsg. Algorithmus zur Vervielfältigung von Daten. Dies wird bspw. benötigt, um Daten auf mehreren Servern zu speichern, synchron und aktuell zu halten, sodass Benutzer die Daten von demjenigen Server herunterladen können, der jeweils am nächsten zu ihrem Standort ist. Ein Backup kann ebenfalls in diesem Sinne als Data Replication Algorithmus angesehen werden.

DATA SECURITY (engl.)
Übsg. Datensicherheit

DATA THEFT (engl.)
Übsg. Datendiebstahl. Eines der Cyberrisiken.

DATEILOSE MALWARE
Schadsoftware, die keine Dateien auf der Festplatte speichert, sondern sich im Arbeitsspeicher des PCs einnistet, sobald sie über einen Link, einen E-Mail-Anhang oder einen Klick auf eine verseuchte Internetseite heruntergeladen wurde. Einmal im Arbeitsspeicher, hat diese dateilose Malware meist die gleichen Rechte auf Daten und Netzwerke zuzugreifen wie der aktuelle Benutzer des PCs. Bei einem kompletten Neustart des PCs wird der Arbeitsspeicher gelöscht und damit auch die dateilose Malware.

DATEN
Gespeicherte Bits und Bytes auf Datenträger wie CDs, Harddisks, USB-Sticks oder Cloud-Server. Durch intelligente Zusammenführung von Daten kann Information und damit Wissen entstehen. Die Bezeichnungen „Daten“ und „Informationen“ werden häufig als Syn. verwendet.

DATENANONYMISIERUNG
Verfahren, um Daten von ihrer Herkunft, von ihrem ursprünglichen Bezug oder von ihrer personenidentifizierenden Form zu lösen. Ziel ist die Weiterverarbeitung der anonymisierten Daten mit geringeren oder gänzlich ohne Datenschutzrisiken. Datenanonymisierung wird eingesetzt bspw. bei der Analyse von Umfrageresultaten, die in ihrer Gesamtheit interessante Aspekte aufzeigen können, die jedoch zum Schutz der Umfrageteilnehmer nicht zurück verfolgbar sein dürfen.

DATENAUTOBAHN
Syn. zu Datenhighway

DATENDIEBSTAHL
Unerlaubte Entwendung von Daten, bspw. durch Insider, die sich bereichern oder rächen möchten, Outsider, die in ein Netzwerk oder ein System einbrechen oder durch Schadsoftware, welche die Daten unerlaubt an einen Hacker schickt.

DATENEIGENTÜMER
Person, welche Daten erstellt oder als Hüter der Daten ernannt wurde.

DATENHIGHWAY
Ugs. für Internet, in welchem zunehmend größere Daten übermittelt werden.

DATENINTEGRITÄT
Unversehrtheit von Daten. Dies ist eines der Ziele der IT-Sicherheit, welche sich grundsätzlich mit der Aufrechterhaltung der Integrität, der Vertraulichkeit und der Verfügbarkeit von Daten und Systeme beschäftigt. Oft wird dies abgekürzt mit „CIA“ für Confidentiality, Integrity and Availability.

DATENKLASSIFIZIERUNG
Gruppierung und Markierung von Daten bzgl. eines Klassifizierungssystems. Bspw. werden Daten anhand ihres Vertraulichkeitsgehalts eingeteilt in a) öffentliche Daten, b) schutzwürdige Daten und c) geheime Daten. Datenklassifizierungen werden auch verwendet, um die gesetzlich nötige Aufbewahrungsdauer der Daten festzulegen und diese entsprechend auf normalen oder Langzeitarchiven zu speichern.

DATENLECK
Versehentlicher oder böswillig herbeigeführter Abfluss von Daten. Absichtlicher Datenabfluss kann mittels einer Schadsoftware oder manuell durch Insider oder Outsider geschehen, um Daten aus einem System und aus einer Firma zu bringen und diese bspw. im Darknet zu verkaufen.

DATENMASKIERUNG
Entfernen von identifizierbaren Inhalten aus Daten.

DATENSAMMLUNG
1) Zusammengehörige Daten bspw. in einer Datenbank. **2)** Von Internetfirmen gespeicherte Informationen über Personen, welche im Internet Datenspuren hinterlassen, bspw. beim Vergeben von Likes und bei der Eingabe von Anfragen in Internetsuchdiensten. Diese Datensammlungen können verkauft und für Profiling verwendet werden, um gezielt Werbung zu platzieren, aber auch, um Social Engineering durchzuführen.

DATENSCHUTZ
Maßnahmen, Verfahren und Systeme zum Schutz von Daten und Informationen innerhalb von PCs, Netzwerken, bei Firmen, Organisationen oder privaten Personen.

DATENSCHUTZBEAUFTRAGTER
Position und Funktion einer Person innerhalb von Firmen. Gemäß GDPR in definierten Situationen zwingend erforderlich.

DATENSCHUTZ-GRUNDVERORDNUNG [DSGVO]
Datenschutzregelwerk der EU zum Schutz der Personendaten von EU-Bürgern, welcher seit 25. Mai 2018 gültig ist. Seit 20. Juli 2018 auch gültig für EEA-Staaten (Island, Norwegen und Lichtenstein).

Ziele:

a) Harmonisierung: Angleichen der Datenschutzgesetze der EU-Staaten
b) Datenschutz: Firmen müssen den Schutz der persönlichen Daten der EU-Bürger sicherstellen und den EU-Bürgern eine Möglichkeit zur Überprüfung anbieten

DATENSEE
Ugs. Bezeichnung für große Mengen an Daten.

DATENSPIONAGE
Ausspähen von Daten, bspw. mithilfe von Spionagesoftware.

DATENVERLUST
Syn. zu Data Leakage. Abhandenkommen von Daten aufgrund von Fehlern, wie bspw. durch Senden einer sensiblen E-Mail an falsche Adressaten oder aufgrund von Hacking von innerhalb oder außerhalb der Firma.

DATENVERLUSTSCHUTZ
System aus Software und Hardware, um das Versenden oder Verlieren von sensiblen Daten zu verhindern. Solche Systeme werden Data Leakage Systems (DLP) genannt und basieren auf Regeln, die Daten blockieren oder durchlassen, je nachdem, wer die Daten, wann, woher, wohin und an wen schickt.

DATENZENTRIERTE SICHERHEIT
Sicherheitsmaßnahmen, wie bspw. Verschlüsselung von Dateien, welche die Daten im Fokus haben, im Unterschied zur Netzwerksicherheit, Serversicherheit, Anwendungssicherheit usw.

DAY ZERO (engl.)
Übsg. Tag null. Der Tag, an dem eine betroffene Firma von einer Schwachstelle in einem ihrer Systeme oder Programmen erfährt, und an dem die Zeitrechnung beginnt, bis die Schwachstelle behoben ist. Diese Schwachstelle könnte bereits für eine Zero-Day-Attacke benutzt worden sein.

DC
1) Abk. für Domain Controller. **2)** Abk. für Data Center.

DDOS-ATTACK (engl.)
Abk. für Distributed Denial of Service Attack

DDW
Abk. für Deep and Dark Web

DECENTRALIZED AUTONOMOUS ORGANIZATION [DAO] (engl.)
Software zur Definition von Regeln und Verträgen („Smart Contracts“), bspw. für Kryptowährungen in Blockchains.

DECOMM (engl.)
Abk. für Decommission, Übsg. Außer Betrieb setzen von veralteten Systemen.

DECOMMISSION (engl.)
Übsg. Außer Betrieb setzen von veralteten Systemen.

DECRYPTION (engl.)
Übsg. Entschlüsselung

DEEP AND DARK WEB [DDW] (engl.)
Teil des Internets, der nicht jedermann zugänglich ist. Dieses grenzt sich gegen das öffentliche „Surface Web“ ab.

Beispiel für Deep and Dark Web: passwortgeschützte Foren, die nur per Einladung zu finden sind.

DEEP FAKE (engl.)
Übsg. Tiefe Fälschung. Programme, die Fake News und Fake Videos mithilfe von künstlicher Intelligenz erzeugen, v. a. durch Deep Learning mit neuronalen Netzen, welche viele Berechnungsstufen beinhalten (sog. tiefe „Hidden Layers“). Dadurch können bspw. Gesichter und Stimmen von Politikern gefälscht und damit das Vertrauen in diese Politiker beeinträchtigt werden. Deep Fake basiert darauf, dass Filmaufnahmen der Zielperson und des Fälschers gespeichert werden und mittels einer digitalen Maske jede Gesichtsregung des Fälschers vom Programm auf die Aufnahmen des Gesichts der Zielperson projiziert werden.

DEEP LEARNING (engl.)
Übsg. Tiefes Lernen. Auch „automatisches Lernen“ genannt. Programmierte Berechnungen zur Bestimmung der optimalsten Einflussgewichte von Eingangswerten, um erwarteten Ausgabewerten bestmöglich nahezukommen. Ziel ist ein mathematisches Modell aus optimalen Einflussgewichten und definierten Berechnungen, welches für neue Eingangswerte eine gute Vorhersage für die Ausgabewerte ermittelt kann (Tab. 6.1).

Deep Learning wird mittels sog. künstlichen „neuronalen Netzen“ umgesetzt, bei welchen mehrere Berechnungsstufen (sog. tiefe „Hidden Layers“) durchgeführt werden. Dabei durchlaufen die Eingangsdaten in der ersten Stufe eine initiale Berechnung zur groben Festlegung der Gewichtung und bilden dadurch aggregierte Eingangsdaten für die nächste Berechnungsstufe usw. Erst die schnellen Computer der letzten Jahre erlaubten den Einsatz vieler umfangreicher Berechnungsstufen, welche die Erkennungsraten neuronaler Netze stark verbesserten. (siehe Abb. 16.1 und 16.2).

Tab. 6.1 Beispiel einer Anwendung von Deep Learning

Eingangswerte	Die einzelnen Pixel mehrerer Katzenbilder
Ausgangswerte	Information darüber, auf welchen Bildern eine Katze enthalten ist
Resultat	Nach der Durchführung aller Berechnungen kann dieses System Katzen auf neuen Bildern mit hoher Wahrscheinlichkeit erkennen

DEEP WEB (engl.)
Syn. zu Deep and Dark Web

DEFACED (engl.)
Übsg. Verunstalten. Defaced bezeichnen Hacker ein von ihnen attackiertes System.

DEFACEMENT (engl.)
Übsg. Verunstaltung. Syn. zu Defacing, Web-Defacing. Internetseite, die unberechtigt manipuliert wurde, um neue Texte oder Bilder darzustellen.

DEFAULT PASSWORD (engl.)
Übsg. Standardpasswort. Geräte, wie Router oder IP-Webcams, werden häufig ab Fabrik mit einem Initial- oder Standardpasswort geschützt, welches jedoch schnell auf Listen im Internet auffindbar ist. Deshalb wird empfohlen, Standardpasswörter sofort bei Inbetriebnahme von Geräten zu ändern.

DEFCON
1) Jährlich in Las Vegas stattfindende, große Hackerkonferenz. **2)** Armeeindikator zum Bedrohungslevel eines Landes.

DEFENSE-IN-DEPTH-STRATEGY (engl.)
Koordinierter, gleichzeitiger oder sequenzieller Einsatz diverser Sicherheitsmaßnahmen, um relevante Güter, wie Daten, Personen, Maschinen usw. in Firmen zu schützen.

DELETE (engl.)
Syn. zu HTTP-DELETE.

DEMILITARISIERTE ZONE [DMZ]
Bereich innerhalb eines Netzwerks, der von anderen Bereichen physisch oder virtuell abgegrenzt ist und in welchem Geräte verbunden sein können, die besondere Zugriffsrechte benötigen.

DEMILITARIZED ZONE [DMZ] (engl.)
Übsg. Demilitarisierte Zone

DENIAL-OF-SERVICE ATTACK [DOS] (engl.)
Übsg. Hacking-Angriff, der zur Beeinflussung oder sogar zum Ausfall eines Online-Dienstes führt. Eine Form von Distributed Denial of Service Attacke

DENIAL-OF-SERVICE-EXPLOIT (engl.)
Software, die eine Schwäche in einem System ausnutzt, um einen DoS-Angriff durchzuführen. Durch regelmäßige Software-Updates lassen sich viele Systemschwächen beheben, bevor diese ausgenutzt werden.

DES
Abk. für Data Encryption Standard

DESEDE
Syn. zu 3DES

DESTRUCTION OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Vernichtung eines kryptografischen Schlüssels.

DETECTION (engl.)
Übsg. Erkennung

DETECTION OF UNAUTHORIZED DEVICES [DOUD] (engl.)
Übsg. Erkennung von unautorisierten Geräten.

DETECTIVE CONTROLS (engl.)
Übsg. Erkennungsmethoden. Diese helfen Risiken oder Schäden zu erkennen, nachdem diese geschehen sind. Mögliche Verfahren sind bspw. die manuelle oder automatische Überprüfung von Netzwerkaktivitäten, Log-Dateien oder versendeten E-Mails oder auch die Analyse der aktuellen Leistung eines Systems. Wird unterschieden von Preventing Controls.

DEVICE IDENTIFICATION (engl.)
Übsg. Geräteidentifikation

DEVOPS
Zusammengesetzter Begriff aus „Dev“+„Ops“. Philosophie, Unternehmenskultur und Prozessverbesserungsansatz innerhalb von Software-Entwicklungsteams, um Software für Kunden rasch, agil, einheitlich, sicher und mit hoher Qualität zu entwickeln („Dev“) und bereitzustellen („Ops“). Konkret werden aufeinander abgestimmte Tools, Prozesse und Infrastruktur angestrebt.

DEVSECOPS
Zusammengesetzter Begriff aus „Dev“+„Sec“+„Ops“. Teilgebiet des DevOps, welcher sich mit der Sicherheit der Systeme und der Infrastruktur beschäftigt.

DFS (engl.)
Abk. für Distributed File System

DH
Abk. für Diffie-Hellman-Schlüsselaustausch

DHARMA
Schadsoftware in Form von Ransomware.

DHCP
Abk. für Dynamic Host Configuration Protocol

DHM
Abk. für Diffie-Hellman-Merkle. Syn. zu Diffie-Hellman-Schlüsselaustausch.

DIFFERENZIELLE KRYPTOANALYSE
Eine Technik der Kryptoanalyse, welche versucht, die Differenzen in Geheimtexten zu ermitteln durch die Kenntnis von Differenzen in den Klartexten.

DIFFIE-HELLMAN-SCHLÜSSELAUSTAUSCH [DH]
Syn. zu Diffie-Hellman-Merkle-Schlüsselaustausch. Verfahren, welches es zwei Parteien erlaubt, einen gemeinsamen Schlüssel (in Form einer Zahl) über einen unsicheren Kommunikationskanal auszutauschen und dieses Geheimnis danach für symm. Verschlüsselung u. Ä. zu verwenden. Dazu erstellen beide Parteien eine eigene geheime Zufallszahl (sog. „privater Schlüssel“). Beide Parteien berechnen nun ihren öffentlichen Schlüssel durch Verrechnung ihrer Geheimzahl mit der vorher gemeinsam definierten nicht geheimen ganzen positiven Zahl und der vorher gemeinsam definierten großen nicht geheimen Primzahl und schicken das Resultat an die jeweils andere Partei. Beide Parteien kalkulieren den gemeinsamen geheimen Schlüssel (sog. „Sitzungsschlüssel“) mit ihrem privaten Schlüssel und der erhaltenen Zahl der Gegenpartei.

Vor dem Austausch der Schlüssel muss auf die Authentisierung der Parteien gegenseitig gesondert Wert gelegt werden, d. h. die teilnehmenden Parteien müssen sicherstellen, dass sie die Schlüssel mit der richtigen Gegenpartei austauschen und nicht mit einem Man-in-the-Middle-Angreifer, der vorgibt eine dieser Parteien zu sein.

DIFFIE-HELLMAN-MERKLE-SCHLÜSSELAUSTAUSCH [DHM]
Syn. zu Diffie-Hellman-Schlüsselaustausch

DIGINOTAR HACK
Angriff auf die Zertifizierungsstelle DigiNotar. Dabei wurde es Angreifern möglich, unbefugt Zertifikate für Domains auszustellen. Dies führte 2011 zur Insolvenz von DigiNotar.

DIGITAL AUDIO BROADCASTING PLUS [DAB+] (engl.)
Digitaler Übertragungsstandard für terrestrischen Empfang bei Digitalradio.

DIGITAL AUTHENTICATION (engl.)
Übsg. Digitale Authentifizierung. Verfahren zur Bestätigung oder Zertifizierung der Identität einer Person oder seiner Werke.

DIGITAL CREDENTIALS (engl.)
Übsg. Digitale Identifikationsdaten eines Benutzers. Auch als Berechtigungsnachweis verwendet.

DIGITALE AUTHENTIFIKATION
Methode zur Bestätigung der Identifizierung eines Benutzers gegenüber einem System oder einer Applikation. Die einfachste, aber nicht mehr sicherste Art einer digitalen Authentifikation ist die Eingabe eines Benutzernamens und des Passworts.

DIGITALE ID
Digitale Form einer Identitätskarte oder einer anderen Art der Identität einer Person. Auch zur Identität von Systemen benutzt.

DIGITALE IDENTITÄT
Eindeutige Repräsentation einer Person oder eines Systems in der digitalen Welt, bspw. bei einem Online-Dienst, einem System oder einer App. Eine Person kann auch mehrere digitale Identitäten bei unterschiedlichen Online-Diensten, Systemen oder Apps besitzen. Folgende Informationen können eine digitale Identität festlegen: Benutzername mit Passwort, PIN-TAN-Kombination, E-Mail-Adresse, Zertifikate usw.

DIGITALER DATENSCHUTZ
Überbegriff für die Bereiche Datensicherheit, Kommunikationssicherheit und Schutz der Privatsphäre.

DIGITALER SCHLÜSSEL
Information, welche in einem kryptografischen Algorithmus verwendet wird, bspw. zur Verschlüsselung eines Textes und zur Entschlüsselung eines Geheimtextes.

DIGITALER ZWILLING
Digitale Repräsentation eines physischen Objekts. Wird bspw. in der Produktionstechnik benutzt, um die zukünftige Produktion vorher digital zu simulieren.

DIGITALE SIGNATUR
Elektronische Äquivalenz zur persönlichen Unterschrift. Dazu wird der eigene private Schlüssel benutzt, um Daten oder Transaktionen zu signieren. Eine solche digitale Signatur kann danach mit dem zugehörigen öffentlichen Schlüssel des Senders geprüft werden, um zu validieren, ob die Daten oder die Transaktion vom richtigen Sender kamen und unverändert sind.

DIGITALE TRANSFORMATION
Wandel in der Gesellschaft, Wirtschaft und anderen Lebensbereichen, ausgelöst und beeinflusst durch die rasante Entwicklung von neuen digitalen Technologien.

DIGITAL IDENTITY (engl.)
Übsg. Digitale Identität

DIGITALISIERUNG
1) Umwandlung analoger Tätigkeiten und Objekte in elektronische Formate. **2)** Wandel in der Gesellschaft, Wirtschaft und anderen Lebensbereichen, ausgelöst und beeinflusst durch die rasante Entwicklung von neuen digitalen Technologien. Syn. zu Digitale Transformation.

DIGITALIZATION (engl.)
Übsg. Digitalisierung

DIGITAL PRIVACY (engl.)
Übsg. Digitaler Datenschutz, digitale Privatsphäre.

DIGITAL RIGHTS MANAGEMENT [DRM] (engl.)
1) Ugs. für Programme und Systeme zum Schutz von Informationen. Präziser wird dieser Schutz „Information Rights Management“ (IRM) genannt. **2)** Software-Lösungen zur Vermeidung von Raubkopien digitaler Produkte, wie Software, Bücher, Musik.

DIGITAL SIGNATURE (engl.)
Übsg. Digitale Signatur

DIGITAL SIGNATURE ALGORITHM [DSA] (engl.)
Definierter Algorithmus zur Erstellung digitaler Signaturen. Von NIST empfohlen, obwohl teilweise Zweifel vorhanden sind.

DIGITAL TWINS (engl.)
Übsg. Digitaler Zwilling

DISASTER RECOVERY [DR] (engl.)
Übsg. Wiederherstellung nach einer Katastrophe. Prozess- und Methodenbeschreibungen sowie eigentliche Durchführung von Maßnahmen, um Systeme nach einem Desaster, bspw. einem DDoS-Angriff oder einem Stromausfall, wieder in Betrieb zu nehmen.

DISCLOSURE OF INFORMATION (ACCIDENTIALLY OR UNAUTHORIZED) (engl.)
Übsg. Offenlegung von Information (unabsichtlich oder unerlaubt).

DISCOVERY (engl.)
Übsg. Entdeckung. Methoden zur Entdeckung von Anomalitäten, spezifischen Strings oder spezifischen Dateien, bspw. in E-Mails, auf einem USB-Stick oder auf verteilten Systemen. Dadurch lassen sich z. B. Dateien finden, welche, auf der Basis ihres Inhalts, automatisch verschlüsselt werden sollten.

DISK (engl.)
Syn. zu Diskette.

DISKETTE
Syn. zu Floppy Disk. Magnetischer Datenträger, welcher zw. ca. 1970 und 2015 verwendet wurde, bevor USB-Sticks, CDs, DVDs, portable Festplatten und Downloads die Übertragung von einem System zu einem anderen und die Speicherung von Daten in großen Mengen ermöglichten. Die Speichermengen lagen zw. ca. 180 kB (bei 8-Zoll Disketten) und ca. 3.5 MB (bei 3.5-Zoll Disketten).

DISK OPERATING SYSTEM [DOS] (engl.)
Betriebssystem, welches Dateien auf Speichermedien verwaltet. Beispiel: MS-DOS.

DISLIKEN
Ugs. für das Abgeben negativer Bewertung bei sozialen Medien.

DISNEY+
Video-Streaming-Angebot

DISPOSAL AND DESTRUCTION OF INFORMATION (engl.)
Übsg. Beseitigung und Vernichtung von Information

DISRUPTION OF SERVICE (engl.)
Übsg. Unterbruch eines Dienstes. Ein Unterbruch eines Online-Dienstes wird bei vielen Firmen und Großanlagen als eines der größten Cyberrisiken angesehen und interne Abteilungen führen entsprechende Gegenmaßnahmen aus, um dies bestmöglich zu verhindern.

DISTRIBUTED DENIAL OF SERVICE ATTACK [DDOS] (engl.)
Übsg. Verteilte Attacke, die zum Ausfall oder Unterbruch eines Online-Dienstes führt. Angreifer versuchen, eine ans Internet angeschlossene Maschine oder ein Computernetz temporär oder dauerhaft zu überlasten und damit in einen unerreichbaren Zustand für seine eigentlichen Benutzer zu versetzen. Die Überlastung geschieht dabei durch „Überfluten" der Systeme mittels einer großen Anzahl an Anfragen, bspw. HTTP-Anfragen. Diese Überflutung wird häufig dadurch erreicht, dass sich Malware auf nicht oder schlecht geschützten Webcams, Routern u. Ä. hineinbringen lässt und von dort zu einem bestimmten Zeitpunkt aktiv wird. Dramatisch sind solche DDoS-Attacken v. a. für E-Banking-, Energie-, Transport-, oder Spitalversorgungssysteme.

DISTRIBUTED FILE SYSTEM [DFS] (engl.)
Übsg. Verteiltes Dateisystem zur Bereitstellung von Festplatten und anderen Datenspeichern für mehrere authentisierte Benutzer.

DISTRIBUTED LEDGER TECHNOLOGY [DLT] (engl.)
Übsg. Technologie für verteilte Buchführung bei verteilten Systemen. Vor Inbetriebnahme wird definiert, durch welchen „Consensus Algorithmus" neue Transaktionen aufgenommen werden. DLT wird u. a. für Blockchain-Anwendungen benutzt.

DISTRIBUTION LIST [DL] (engl.)
Übsg. Verteilungsliste. Zusammenfassung von E-Mail-Adressen als adressierbare Liste.

DISTRIBUTION OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Verteilung eines kryptografischen Schlüssels.

DIVULGED (engl.)
Übsg. Enthüllt, bekannt gemacht.

DIY
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „Do-it-yourself", Übsg. „Mache es selber".

DL
Abk. für Distribution List

DLL
Abk. für Dynamik Link Library. In Windows benutztes Dateiformat für Programmbibliotheken.

DLL-HIJACKING (engl.)
Übsg. Entführen, Missbrauchen, Übernehmen von DLLs. Angriff, bei der eine bestehende DLL des Betriebssystems oder eines Programms durch eine neue mit gleichem Namen ersetzt wird, welche beim nächsten Start des Systems oder des Programms anstatt der richtigen DLL geladen wird. Dadurch kann Schadsoftware ins System hineingebracht und ausgeführt werden.

DLP
Abk. für Data Leakage Prevention

DLT
Abk. für Distributed Ledger Technology

DMARC
Abk. für Domain-based Message Authentication, Reporting and Conformance.

DMS
Abk. für Document Management System

DMZ
Abk. für Demilitarisierte Zone

DNR
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „Do not Respond“, Übsg. „Keine Antwort nötig“.

DNS
Abk. für Domain Name System

DNS-BASED AUTHENTICATION OF NAMED ENTITIES [DANE] (engl.)
Netzwerkprotokoll zur Erweiterung der TLS/SSL-Transport-Verschlüsselung, sodass Zertifikate nicht unbemerkt ausgetauscht werden können. Dies erhöht die Sicherheit bei E-Mails und beim Aufruf von Internetseiten, und kann auch dazu verwendet werden, eigene Zertifikate auszustellen, ohne den Einbezug einer Zertifizierungsstelle.

DNS-CACHE POISONING (engl.)
Übsg. DNS-Speicher-Vergiftung. Angriff auf DNS, bei welchem die Zuordnung von Domain-Namen zu IP-Adressen manipuliert wird. Hierbei werden gefälschte Einträge in

den DNS-Cache des Benutzers eingeschleust, damit aufgerufene Daten scheinbar vom echten, tatsächlich jedoch von einem anderen Server gesendet werden.

DNS HIJACKING ATTACK (engl.)
Übsg. Angriff durch DNS-Übernahme. Attacke, bei welcher DNS-Einträge manipuliert werden, um Besucher dieser betroffenen Internetseiten auf ähnliche Seiten zu führen und dort die Login-Daten zu stehlen.

DNS-OVER-TLS [DOT]
Protokoll zur TLS-verschlüsselten Auflösung von Hostnamen aus IP-Adressen.

DNSSEC
Abk. für Domain Name System Security Extensions. Zusätzliche Methoden bei DNS zur Sicherstellung der Integrität und Authentizität. Damit soll die Manipulation der Zuordnung von Domain-Namen und IP-Adresse, bspw. durch Cache Poisoning, verhindert werden. Dies wird erreicht durch Übertragung von digitalen Signaturen auf Basis von asymmetrischer Kryptografie.

DOCKER
Open-Source-Virtualisierungssoftware, bspw. um Software-Produkte in einem virtuellen System zu isolieren oder um Software mitsamt allen benötigten Paketen als einen Container für den Transport und die Installation bereitzustellen.

DOCUMENT MANAGEMENT SYSTEM [DMS] (engl.)
Übsg. Dokumentenmanagementsysteme. Software zur Verwaltung von physischen oder elektronischen Dokumenten.

DOMAIN
1) Teilbereich des Internets mit eindeutigem und weltweit einmaligem Namen. Bsp. „domain.com“. Eine Domain erlaubt dadurch die eindeutige Adressierung eines Objekts, bspw. des Servers, auf welchem die Internetseite für „domain.com“ gespeichert wurde. Domains sind verknüpft mit ihrer darüberliegenden Top-Level-Domain, im Bsp. oben „.com“, und können selber Subdomains besitzen, z. B. „info.domain.com“. Jedem Domain- oder Subdomain-Namen entspricht dabei eine IP-Adresse. Die Zugehörigkeit zwischen Namen und IP-Adressen wird in Listen geführt und von DNS weltweit verbreitet. **2)** Abk. für Netzwerk Domain. Gemeinsam über einen Domain Controller administrierte Gruppe von Computern innerhalb eines Netzwerks.

DOMAIN ADMIN
Benutzer, der Admin-Rechte für die ganze Domain besitzt.

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE [DMARC] (engl.)
Von mehreren Internetkonzernen vorgeschlagene und teilweise umgesetzte Technologie bei E-Mails zur Verhinderung von Phishing- und Spam-Attacken. Dabei wird bspw. festgelegt, wie ein Empfänger die Authentifizierung durchführen soll und wie IP-Adressen abgeglichen und wie die E-Mail-Struktur analysiert werden sollen.

DOMAIN CONTROLLER [DC] (engl.)
Server, der Active-Directory-Funktionen anbietet, um zentral die Authentifizierung von Benutzern und Computern in einem Netzwerk zu ermöglichen. Außerdem bietet ein Domain Controller Funktionen für DNS.

DOMAINKEY IDENTIFIED MAIL [DKIM] (engl.)
Übsg. Domainschlüssel-identifizierte E-Mail. Beispiel eines Identifikationsprotokolls.

DOMAIN NAME SYSTEM [DNS] (engl.)
Dezentrales System, welches IP-Adressen und zugehörige Domain-Namen von Systemen eines Netzwerks und des Internets in Listen führt, sodass jeder Aufruf, bspw. einer Internetseite, zur richtigen IP-Adresse und damit zum richtigen Server führt. Diese Listen werden weltweit zw. den Domain-Name-Systemen ausgetauscht und aktuell gehalten.

DORKBOT
Schadsoftware, um Daten zu stehlen und DDoS-Angriffe durchzuführen.

DOS
Abk. für Disk Operating System

DOT
Abk. für DNS-Over-TLS

DOT.NET
Syn. zu.NET Framework

DOTNET
Syn. zu.NET Framework

DOUD
Abk. für Detection of Unauthorized Devices

DOWNGRADE ATTACK (engl.)
Übsg. Runterstufungsattacke für TLS/SSL, bei welcher es aufgrund von Implementierungsfehlern möglich ist, eine eigentlich sichere Verschlüsselung auf einen unsicheren alten Versionsstand zurückzusetzen. Bspw. kann dadurch eine Serververbindung, die mit TLS1.2 begonnen wurde, absichtlich auf TLS1.0/SSL 3.0 runtergestuft werden, sodass Sicherheitslücken ausgenutzt werden können, die bei TLS1.2 nicht mehr vorliegen.

DOWNLOAD (engl.)
Übsg. Herunterladen. Ein Programm, ein Text, eine Tabelle oder allg. eine Datei, die von einem anderen Computer im gleichen Raum, im gleichen Netzwerk oder irgendwo im Internet auf den Computer des Benutzers transferiert wird. Häufig geschieht dies in einem Webbrowser, im Windows Explorer, im Finder des Mac oder via FTP. Ein Download kann auch verschlüsselt übertragen werden, via HTTPS oder FTPS. Eine verschlüsselte Übertragung schützt jedoch nicht vor Schadsoftware, die man potenziell herunterlädt. Deswegen sollte ein Download nur via Internetseiten von seriösen Firmen und Personen erfolgen, bei welchen die Wahrscheinlichkeit für Malware geringer ist.

DPAPI
Abk. für Data Protection Application Programming Interface

DPIA
Abk. für Data Protection Impact Assessment. Begriff wird bei den Gesetzen der GDPR verwendet.

DPO
Abk. für Data Protection Officer

DPOD
Abk. für Data Protection On-Demand der Firma SafeNet

DR
Abk. für Disaster Recovery

DRAGONFLY 2.0
Hacker-Gruppe

DRIVE-BY-DOWNLOAD (engl.)
Übsg. Herunterladen beim Vorbeikommen. Schadsoftwareinfektion eines Systems durch den Aufruf einer „verseuchten“ Internetseite, also einer Internetseite, bei der automatisch Malware heruntergeladen wird, sobald die Seite aufgerufen wird.

DRIVE-BY-INFECTION (engl.)
Übsg. Infektion beim Vorbeikommen. Syn. zu Drive-by-Download.

DRIVE ENCRYPTION (engl.)
Übsg. Laufwerksverschlüsselung

DRM
Abk. für Digital Rights Management

DROPPERBOT
Botnetz

DSA
Abk. für Digital Signature Algorithm

DSG
Abk. für (Schweizer) Bundesgesetz über den Datenschutz. Konkret: Datenschutzgesetz.

DSGVO
Abk. für Datenschutz-Grundverordnung. Syn. zu General Data Protection Regulation (GDPR).

DTLS
Abk. für Datagram Transport Layer Security. Ein auf TLS basierendes Protokoll, welches UDP statt TCP benutzen kann.

DUCKDUCKGO.COM
Internetsuchmaschine, die gemäß Selbstaussage weder Suchanfragen noch andere Daten des Benutzers speichert oder verfolgt. Außerdem zeigt diese keine zielgerichtete Werbung und respektiert die Privatsphäre des Benutzers.

DYNAMIC APPLICATION SECURITY TESTING [DAST] (engl.)
Software zum Testen von Internetanfragen bei laufenden Programmen, d. h. es werden Anfragen über HTTP, HTTPS und HTML auf Sicherheitsfehler analysiert.

DYNAMIC HOST CONFIGURATION PROTOCOL [DHCP] (engl.)
Protokoll, um Geräte automatisch in ein bestehendes Netz einzubinden, ohne manuelle Konfiguration. Dazu wird jedem Gerät eine IP-Adresse u. a. vergeben.

E

7

E.164
Formatsdefinition von Telefonnummern und Festlegung der internationalen Vorwahlen.

E-2-E
Abk. für End-to-End. Häufig benutzt für End-to-End Encryption.

E2E ENCRYPTION
Abk. für End-to-End Encryption

EAS
Abk. für Microsoft Exchange ActiveSync

EASY GPG (engl.)
Übsg. Einfaches GNU Privacy Guard. Projekt der BSI im Rahmen der E-Mail-Verschlüsselung zur Validierung von öffentlichen Schlüsseln. Dabei wird das „Web-Key Directory-(WKD)"-Protokoll verwendet, um die Zusammengehörigkeit registrierter E-Mail-Adressen und hochgeladener öffentlicher Schlüssel beim E-Mail-Anbieter zu überprüfen.

EAVESDROPPER (engl.)
Übsg. Lauscher. Im Bereich des Datenschutzes ist dies eine Person oder ein System, welche/welches eine Kommunikation zw. zwei Parteien unbemerkt mithört. Dies kann durch Verschlüsselung der Kommunikation verhindert werden.

EAVESDROPPING (engl.)
Übsg. Abhören, Lauschen.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_7

E-BANKING
Abk. für elektronisches Bankgeschäft. Syn. zu E-Banking, Online-Banking. Software zur Abwicklung von Bankgeschäften mittels PC oder Handy. Bei einigen Anbietern wird das E-Banking mittels Handys als Mobile-Banking bezeichnet.

EBCDIC
Abk. für Extended Binary Coded Decimal Interchange Code

ECB
Abk. für Electronic Codebook Mode

ECC
Abk. für Elliptic Curve Cryptography

ECDSA-SCHLÜSSEL
Abk. für Schlüssel, welche auf „Elliptic Curve Digital Signature Algorithm“ basieren. Die Kryptografie im Zusammenhang mit solchen Schlüsseln bedient sich der Mathematik der elliptischen Kurven und des DSA-Verfahrens zur Berechnung der digitalen Signatur.

EDGE COMPUTING (engl.)
Übsg. Berechnungen und Datenverarbeitung am „Rand“ einer Cloud, d. h. direkt bei IoT-Sensoren u. Ä. Vorteile liegen bspw. in der möglichen Vorverarbeitung gemessener Sensordaten, sodass nur relevante, aggregierte Daten in die Cloud transferiert werden. Dies reduziert den Speicher- und Bandbreitenbedarf beim Transfer und im Netzwerk.

EDM
Abk. für Exact Data Matching

EDP
Abk. für Enterprise Data Protection

EFS
Abk. für Encryption File System

E-ID
Abk. für elektronische Identifizierungsdienste, bspw. in der Schweiz. Personen können sich mit ihrer E-ID digital identifizieren, ähnlich wie mit einem Reisepass. Somit kann die E-ID nicht nur für Käufe und Transaktionen im Internet benutzt werden, sondern auch für Aktionen, die eine staatlich anerkannte Identifikation benötigen, bspw. den Abschluss eines Versicherungsvertrags.

EIN-FAKTOR-AUTHENTIFIZIERUNG [1FA]
Syn. zu Ein-Faktor-Authentisierung

EIN-FAKTOR-AUTHENTISIERUNG [1FA]
Simple und ursprüngliche Art der Authentifizierung, meist mittels Benutzername und Passwort. Heutzutage wird empfohlen, wo immer möglich, Zwei-Faktor-Authentisierung (2FA) zu wählen, bei welcher die Qualität der Authentifizierung durch weitere „Faktoren", wie bspw. Fingerabdruck, PIN, SmartCard, Authenticator-App u. Ä. erhöht wird.

EINDRINGLING
Syn. zu Hacker, Angreifer. Eine Person, eine Gruppe von Personen oder auch ein System, welche/welches sich unrechtmäßig Zugang zu einer App, einem Computer oder einem Netzwerk verschafft.

EINGESCHRÄNKTER BENUTZERKREIS
Gewollte Einschränkung einer App oder eines Systems, sodass nur ausgewählte Benutzer Zugang dazu erhalten. Syn. zu Closed User Group.

EINMAL-BLOCK
Syn. zu Einmal-Schlüssel, One-Time-Pad (OTP).

EINMAL-KENNWORT
Syn. zu One-Time-Password (OTP). Für jede Session oder jede erneute Anmeldung bei einer App, einem System oder einem Online-Dienst neu von einem Kennwortgenerator erzeugtes Passwort, welches sich meist automatisch nach einer Zeitspanne, bspw. einer Minute, ändert und somit einem Hacker kaum Zeit lässt, das Passwort zu erraten. Auch vordefinierte Kennwortlisten anstatt Kennwortgeneratoren werden verwendet. OTP werden auf Papier, per SMS, Token und Mobile Phone App (z. B. Google Authenticator) zur Verfügung gestellt. Einmal-Kennwörter gelten als sicher, jedoch werden diese im „Deep and Dark Web" gehackt, bspw. mittels einer SIM-Karten-Kopie, mithilfe deren das per SMS geschickte neue Passwort abgefangen werden kann.

EINMAL-PASSWORT
Syn. zu Einmal-Kennwort

EINMAL-SCHLÜSSEL
Syn. zu One-Time-Pad (OTP). Einmalig verwendeter, zufälliger Schlüssel (z. B. in Form einer Zahlenreihe) für die sichere symmetrische Verschlüsselung. Dieser Schlüssel ist mind. gleich lang wie die zu verschlüsselnde Nachricht. Bspw. kann eine Vigenère-Verschlüsselung mit Nachricht und Codewort gleicher Länge benutzt werden. Die Sicherheit ist dabei jedoch nur dann gewährleistet, wenn der Schlüssel immer, heute und in Zukunft, geheim bleibt und geheim dem Empfänger der Nachricht zugänglich

gemacht wird. Dies ist jedoch schwierig, da der Schlüssel zufällig gewählte Werte enthält und damit nicht memorisiert, sondern gespeichert oder aufgeschrieben werden muss und damit physisch oder elektronisch auffindbar wird.

EINTRAGUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Ein erzeugter und evtl. signierter Schlüssel wird auf einem Schlüsselserver registriert. Abschnitt im Lebenszyklus kryptografischer Schlüssel. Siehe zusätzliche Details beim Begriff Schlüssel.

EINWEG-FUNKTIONEN
Syn. zu Falltür-Funktionen. Mathematische Berechnungen, die rasch ausgeführt werden können, aber Ergebnisse liefern, welche nur mit viel Aufwand zurückzurechnen sind. Solche Funktionen werden bei der Berechnung von asymm. Verschlüsselungen verwendet. Dabei werden zwei große Primzahlen miteinander multipliziert. Das dadurch erhaltene Produkt lässt sich nur mit sehr großem Rechenaufwand wieder in die zwei Primzahlen zerlegen.

EINWEG-PASSWORT
Syn. zu Einmal-Kennwort

ELASTICSEARCH (engl.)
Häufig eingesetzte Software zur Suche in Daten. Auf den verwendeten Servern werden die einzelnen Einträge und Abfragen in NoSQL-Format (sog. „JSON-Dokumente“) verteilt gespeichert. Die Kommunikation von ElasticSearch mit Clients geschieht via einem RESTful-WebInterface.

ELECTRONIC CODEBOOK MODE [ECB] (engl.)
Einfachster Betriebsmodus bei Blockchiffre-Verschlüsselungsverfahren. Dabei werden Klartextblöcke unabhängig voneinander mit einem Schlüssel verschlüsselt. Ein Nachteil davon ist, dass gleiche Klartextblöcke, die mit gleichem Schlüssel verschlüsselt werden, immer gleiche Geheimtextblöcke erzeugen.

Beispiel: Bundes-Trojaner unter Verwendung von AES mit hartcodiertem Schlüssel.

ELECTRONIC IDENTIFICATION, AUTHENTICATION AND TRUST SERVICES [EIDAS] (engl.)
Übsg. Elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Eine seit 2014 gültige Regelung der EU, welche als Basis für viele Landesgesetze diente, bspw. das Vertrauensdienstgesetz von Deutschland und das Bundesgesetz ZertES der Schweiz.

ELEKTRONISCHE SICHERHEITSMASSNAHMEN
Software zum Schutz von Computersystemen. Diese können ergänzt werden durch physische Sicherheitsmaßnahmen, wie das Anketten der Geräte.

Beispiele elektronischer Sicherheitsmaßnahmen: Firewalls, Anti-Viren-Programme, 2FA.

ELEKTRONISCHES SCHWARZES BRETT
Syn. zu Mailbox, Bulletin Board System (BBS). In den 1980er- bis Anfang der 1990er-Jahre populäre textbasierte Form der Kommunikation, der Informations- und Newsverbreitung und des Datenaustauschs. Ein PC diente dabei als Host mit der Mailbox-Software und war meist über den Telefonanschluss mit Modem resp. Akustikkoppler erreichbar.

ELEVATED CHANGE RIGHTS (engl.)
Übsg. Erweiterte Änderungsrechte

ELEVATED COMMAND PROMPT (engl.)
Übsg. Erweiterter Befehlssatz durch Öffnen einer Windows-Eingabeaufforderung (CMD-Fensters) mit Administratorrechten.

ELGAMAL-KRYPTOSYSTEM
Verschlüsselungs- und Signaturverfahren für asymmetrische Kryptografie basierend auf Diffie-Hellman-Schlüsselaustausch.

ELLIPTIC CURVE CRYPTOGRAPHY [ECC] (engl.)
Übsg. Elliptische-Kurven-Kryptografie.

ELLIPTIC CURVE DIFFIE-HELLMAN [ECDH] (engl.)
Auf elliptischen Kurven basierende Modifikation des Diffie-Hellman-Schlüsselaustauschverfahrens.

ELLIPTISCHE KURVEN
Mathematische Funktionen mit einer definierten geometrischen Addition. Für reelle Zahlen entspricht dies einer kubischen Gleichung der Form:

$$y^2 = x^3 + ax + b$$

wobei die rechte Seite der Gleichung nur eine einzige Nullstelle besitzen darf. Wie der Name andeutet, stammen solche Funktionen ursprünglich aus Berechnungen an Ellipsen, werden aber in vielen anderen Gebieten der Mathematik verwendet.

ELLIPTISCHE-KURVEN-KRYPTOGRAFIE
Syn. zu Elliptic Curve Cryptography (ECC). Mathematische Methoden für asymmetrische Kryptografie. Dabei werden die Multiplikation und Potenzierung der üblichen Kryptografieberechnungen durch Addition und Skalarmultiplikation auf elliptischen Kurven ausgetauscht. Durch die Verwendung von elliptischen Kurven anstatt einfacheren mathematischen Berechnungen können kürzere Schlüssel eingesetzt werden als bspw. bei RSA bei vergleichbarer Sicherheit.

EMAIL ADDRESS GUESSING (engl.)
Übsg. Erraten von E-Mail-Adressen.

E-MAIL-ANHANG
Datei als Teil einer E-Mail. Der Inhalt der Datei kann ein Bild, eine Textdatei, ein Video oder ein beliebiges anderes, auch verschlüsseltes Format haben. Risiken bestehen bei ankommenden E-Mails mit Anhängen, da diese Malware beinhalten können, die beim Öffnen und Anzeigen des Anhangs in den Computer oder das Handy gelangen.

E-MAIL-DIENSTANBIETER [EMDA]
Firma, die gratis oder gegen Gebühr E-Mail-Adressen vergibt und meist noch weitere Zusatzdienste, wie Kalender oder Datentransfer.

EMDA
Abk. für E-Mail-Dienstanbieter

EMOJI
Syn. zu Bildschriftzeichen, Piktogramme. Werden in E-Mails, SMS und Chats benutzt, um einfach und rasch Gefühle, Objekte oder andere Begriffe darzustellen. Ursprünglich wurden in Texten Zeichenkombinationen geschrieben, welche gesichtsähnliche Form hatten, wenn der Leser seinen Kopf zur linken Seite neigte, z. B. :-) Werden solche gesichtsähnlichen Zeichenkombinationen heutzutage eingetippt, erkennen dies viele Programme automatisch und ersetzen diese durch grafische Emoji-Piktogramme.

EMOTET
Schadsoftware-Familie in Form von Computerwürmern. Diese zielen speziell auf Online-Banking.

EMULATION
1) Software- oder hardwarebasierte Nachahmung eines Computerverhaltens auf einem anderen System. Bspw. kann der in den 1980er-Jahren populäre C64 auf Windows emuliert und benutzt werden. 2) Abk. für Terminal-Emulation, welches ein textbasiertes Terminal auf einer grafischen Benutzeroberfläche nachbildet. Syn. zu Konsole, Terminal.

EMV CHIP
Elektrischer Chip auf Bankkarten und Kreditkarten von Europay, MasterCard und Visa.

ENCODING (engl.)
1) Übsg. Verschlüsselung 2) Übsg. Codierung. Verwendet zur Beschreibung von Zeichencodierungen, d. h. zur eindeutigen Zuordnung von Zeichen zu Werten innerhalb eines Zeichensatzes. Beispiel ASCII, UTF-8 (siehe ASCII-Tabelle im Anhang Tab. 32.1).

ENCRYPT-DECRYPT-ENCRYPT [EDE] (engl.)
Methode beim 3DES-Verschlüsselungsalgorithmus.

ENCRYPTION (engl.)
Übsg. Verschlüsselung

ENCRYPTION AT REST (engl.)
Übsg. Verschlüsselung gespeicherter Daten. Syn. zu Protection at Rest. Wird unterschieden von „Encryption on Transit".

ENCRYPTION FILE SYSTEM [EFS] (engl.)
Übsg. Verschlüsselungsdateisystem

ENCRYPTION ON TRANSIT (engl.)
Übsg. Verschlüsselung von Daten während der Kommunikation. Syn. zu Protection on Transit. Wird unterschieden von „Encryption at Rest".

ENDE-ZU-ENDE-VERSCHLÜSSELUNG [E2E]
Kryptografisches Verfahren, welches eine Nachricht zusätzlich zur Transportverschlüsselung, bspw. mittels TLS, auch bereits eine Verschlüsselung innerhalb der Applikation anwendet, in der die Nachricht entstand und von der aus diese geschickt wird. Erst die Empfänger-Applikation kann diese Nachricht entschlüsseln. Damit wird gewährleistet, dass auch die Serviceanbieter der Applikation die Nachricht nur verschlüsselt verarbeiten und nicht einsehen können. Heutige Chat-Applikationen wie Threema und WhatsApp bauen auf E2E-Verschlüsselung auf.

END OF LIFE [EOL] (engl.)
Übsg. Lebensende. Systeme, Hardware oder Software, welche veraltet oder nicht mehr aktuell sind und häufig nicht mehr aktualisiert werden können. Dies stellt ein akutes Risiko für Firmen und Privatpersonen dar, da fehlende Updates die Systeme, Hardware oder Software angreifbar werden lassen.

ENDPOINT (engl.)
Übsg. Systeme in der Nähe des Benutzers, bspw. PCs, Handys.

END-TO-END ENCRYPTION [E2E ENCRYPTION] (engl.)
Übsg. Ende-Zu-Ende-Verschlüsselung.

ENFORCING 2FA (engl.)
Übsg. Durchsetzung und Forderung von 2FA.

ENFORCING INFORMATION SECURITY (engl.)
Übsg. Durchsetzung und Forderung von Datenschutz.

ENFORCING PRIVILEGED ACCESS MANAGEMENT (engl.)
Übsg. Durchsetzung und Aufforderung zur Verwaltung eines privilegierten Zugangs.

ENISA
Abk. für European Network and Information Security Agency. EU-Agentur zur Verbesserung und Unterstützung der Netz- und Informationssicherheit innerhalb der EU für Privatpersonen, Organisationen und Firmen der EU.

ENTANGLEMENT (engl.)
Übsg. Verschränkung. Siehe Quantenverschränkung.

ENTERPRISE DATA PROTECTION [EDP] (engl.)
Übsg. Schutz von Firmendaten. Ursprüngliche Bezeichnung für Windows Information Protection (WIP).

ENTERPRISE RIGHTS MANAGEMENT [ERM] (engl.)
Generelle Bezeichnung für Software-Lösungen und Produkte, welche eingesetzt werden, um sensible Daten mittels Verschlüsselung u. Ä. zu schützen.

ENTITLEMENT (engl.)
Übsg. Berechtigung

ENTITLEMENT MANAGEMENT SYSTEM (engl.)
Übsg. Berechtigungssystem

ENTROPIE
Maß für die Unordnung in einem System. Je höher die Entropie, desto höher die Unordnung. Der Begriff Entropie wird auch im Zusammenhang mit starker und schwacher Verschlüsselung verwendet, wobei eine große Entropie, bspw. durch Eingabe eines Passworts oder durch Erzeugung von Zufallswerten mittels manueller Mausbewegungen, zu einer stärkeren Verschlüsselung führt.

ENTROPY (engl.)
Übsg. Entropie

ENTRY OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Eintragung eines kryptografischen Schlüssels.

ENTSCHÄRFUNG VON CYBER-BEDROHUNGEN
Phase bei der Behandlung von Cyber-Bedrohungen.

ENTSCHLÜSSELUNG
Umkehraktion einer Verschlüsselung. Bei symmetrischer Verschlüsselung wird der gleiche Schlüssel für die Ver- wie für die Entschlüsselung eingesetzt. Bei asymmetrischer Verschlüsselung werden die Daten mit einem öffentlichen Schlüssel verschlüsselt und mit dem zugehörigen privaten Schlüssel entschlüsselt.

EOL
Abk. für End of Life

EREIGNISPROTOKOLLIERUNG UND -ÜBERWACHUNG
Syn. zu Event Logging and Monitoring. Methoden und Tools zur automatischen und manuellen Detektion von Ereignissen wie bspw. Cyber-Attacken. Größere Firmen führen solche Tätigkeiten in eigens dafür eingesetzten Teams aus, um schnell auf Angriffe reagieren zu können.

ERM
Abk. für Enterprise Rights Management

ERPRESSUNGSTROJANER
Schadsoftware, welche sich dem Benutzer als nützliche Anwendung oder lustige App präsentiert, aber versteckt auf dem PC oder dem Handy die Daten verschlüsselt oder vorgibt, diese verschlüsselt zu haben, um ein Lösegeld in Form von Bitcoins u. Ä. zu erpressen. Anstatt die Daten zu verschlüsseln, drohen manche solcher Trojaner mit Offenlegung von persönlichen Daten im Internet. Bei Zahlung des Lösegeldes erhält das Opfer evtl. den Code zur Entschlüsselung der Daten, jedoch werden dadurch solche kriminellen Aktivitäten für Nachahmer lukrativ und weitere Attacken mitfinanziert. Der beste Schutz vor Schäden durch Trojaner und anderer Malware ist ein aktuelles Virenschutzprogramm und ein regelmäßiges Backup des Computers oder Handys auf einem nicht dauernd angehängten Backup-System bspw. einer externen Festplatte, sowie die Installation der von seriösen Firmen angebotenen Software-Updates der Geräte.

ERRATEN VON E-MAIL-ADRESSEN
Dies ist seit Jahrzehnten einfach möglich und stellt ein Risiko für Hacking via Social Engineering dar, da Firmen meist jedem Mitarbeiter eine E-Mail-Adresse der Form „Vorname.Nachname@Firma.com“ vergibt. Auch Spam-Attacken benutzen häufig einfaches Erraten von E-Mail-Adressen, indem sie Vor- und Nachnahme mit Domainnamen kombinieren.

ERWEITERTE ÄNDERUNGSRECHTE
Speziell vergebene technische Möglichkeiten, um Geräte, Software oder Daten zu ändern. Bspw. können IT-Administratoren erweiterte Änderungsrechte erhalten, falls sie Installationen von Software auf Firmen-PCs durchführen müssen.

ERWEITERTE ZUGRIFFSRECHTE
Speziell vergebene technische Möglichkeiten, um zusätzlichen Zugang zu Geräten, Software oder Daten zu erhalten. Bspw. besitzen nur Mitglieder des Topmanagements erweiterte Zugriffsrechte auf streng geheime interne Firmendaten.

ERZEUGUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Abschnitt im Lebenszyklus kryptografischer Schlüssel. Siehe zusätzliche Details beim Begriff Schlüssel.

ERZEUGUNG VON INFORMATION
Abschnitt im Lebenszyklus von Informationen.

ESCAPE-SEQUENZ
Zeichenfolge, welche mit dem ESC-Zeichen (^ oder \) beginnt und eine Anweisung für den PC beinhaltet. Dies kann bspw. der Befehl zum Anzeigen eines Spezialzeichens sein, oder der Befehl, den Cursor in einem Terminal zu bewegen und umzufärben. Auch beim Ansteuern mancher Drucker kommen Escape-Sequenzen vor.

Beispiel

Mit \n springt der Cursor zur nächsten Linie
Mit \r springt der Cursor zum Anfang der Zeile
mit \t springt der Cursor zur nächsten Tabulatorposition

ETERNALBLUE
Schadsoftware, welche u. a. bei den Erpressungsprogrammen WannaCry und WannaMine einen Programmfehler in der SMB-Implementation von Windows ausnutzte.

ETHER
Kryptowährung, abgekürzt mit dem Kürzel ETH.

ETHERDELTA
Dezentrale Börse für Kryptowährungen. Bei einer dezentralen Börse kann der Handel von Rechner zu Rechner (Peer-to-Peer) erfolgen. Dies reduziert das Risiko von Kryptowährungsdiebstahl.

ETHEREUM
Auf Blockchain-Technologie basierende Kryptowährung und zugleich verteiltes System zum Anlegen, zum Verwalten und zur Ausführung von Programmen (Smart Contracts), bspw. für E-Voting-Systeme.

ETHERNET
Protokolle und Hardware in einem lokalen, geschlossenen Datennetz (LAN), um Daten untereinander kabelgebunden und seriell auszutauschen. Dafür wird jeder Netzwerkschnittstelle die eindeutige 48-Bit-lange MAC-Adresse zugewiesen, über die die Hardware angesprochen werden kann. Heimnetzwerke mit einem Router und LAN-Kabel bilden ein Ethernet-Netz.

EU GDPR
Abk. für EU General Data Protection Regulation. Syn. zu Datenschutz-Grundverordnung (DSGVO). Seit Mai 2018 gültige Gesetze zum Schutz von persönlichen Daten, welche von Firmen verarbeitet werden, die in der EU tätig sind.

EVENT LOGGING AND MONITORING (engl.)
Übsg. Ereignisprotokollierung und -überwachung

EXACT DATA MATCHING [EDM] (engl.)
Übsg. Vergleich exakter Daten

EX-ANTE
Übsg. Vornherein, vorab, erwartet. Begriff wird bspw. verwendet zur Beschreibung einer Analyse von Daten, bevor diese Daten die Firma verlassen. Gegenteil zu „ex-post“.

EXCHANGE ONLINE [EXO] (engl.)
Microsoft Exchange Server, welcher nicht „On-Prem“, also innerhalb des Firmengebäudes, sondern in der Microsoft Cloud betrieben wird. Teil der Microsoft-Office-365-Produktsuite.

EXCHANGE SERVER (engl.)
Abk. für Microsoft Exchange Server. System basierend auf Microsoft-Windows-Software zur Verwaltung von E-Mails, Terminen und anderen Daten für mehrere Benutzer im Netzwerk.

EXISTENTIAL DATA (engl.)
Übsg. Existenzielle Daten, bspw. sensible Firmenwerte wie geistiges Eigentum.

EXO
Abk. für Exchange Online

EXPLOIT (engl.)
Übsg. Ausnutzung einer Schwachstelle in einem System oder in einem Programm, um Zugang zu Daten, Systemen oder Netzwerken zu erhalten.

EXPOSING (engl.)
Übsg. Freilegen, offenlegen. Bspw. die unbeabsichtigte Offenlegung von Datenbankdaten über einen ungeschützten Internetzugang.

EX-POST
Übsg. Nachträglich, im Nachhinein. Begriff wird bspw. verwendet zur Beschreibung einer nachträglichen Erkennung von Cyber-Attacken. Gegenteil zu „ex-ante“.

EXTENDED BINARY CODED DECIMAL INTERCHANGE CODE [EBCDIC] (engl.)
Übsg. Erweiterter binärcodierter Dezimalcode für die Kommunikation. Von IBM 1964 entwickelte 8-Bit Zeichencodierung.

EXTENSION (engl.)
1) Abk. für Webbrowsererweiterung. 2) Abk. für Software-Erweiterungen. Syn. zu Plug-in. 3) Übsg. Endung eines Dateinamens. Letzte 1 bis 3 Zeichen bei Dateinamen, bspw. „exe“ beim Taschenrechnerprogramm „calc.exe“. Diese 1 bis 3 Zeichen beim Dateinamen können einen Hinweis zum Typ und Format der enthaltenen Daten geben. Diese Art der Dateibeschreibung wurde in den ersten DOS-Versionen eingeführt, da aus Speicherplatzgründen die Dateilängen auf acht Zeichen, gefolgt von einem Punkt und einer Dateiendung mit drei Zeichen, limitiert werden mussten.

F

8

FACEBOOK
Populärer Online-Dienst im Bereich der sozialen Medien, bei dem jeder Benutzer eigene Bilder, Texte und Videos zur Veröffentlichung hochladen kann, sowie die hochgeladenen Bilder, Texte und Videos von anderen bewerten („liken“) und mit anderen teilen kann.

FACE ID (engl.)
Biometrische Login-Methode, die auf der Gesichtserkennung basiert. Zunehmend zur Anmeldung bei Handys und PCs verwendet.

FACE RECOGNITION (engl.)
Übsg. Gesichtserkennung. Software, die das Gesicht einer Person aufnimmt und die Gesichtsformen und -details mit vorher gespeicherten Gesichtsdaten vergleicht. Wurden in der Vergangenheit nur 2D-Bilder aufgenommen und zur Erkennung verwendet, erlauben aktuelle Techniken die Aufnahme eines Gesichts in 3D und sind deshalb sicherer, da diese Systeme nicht mithilfe eines Fotos überlistet werden können.

FAILOVER (engl.)
Übsg. Wechsel bei Ausfall. Manuelle oder automatische Aktion, bei welcher die Datenkommunikation zu Ersatzsystemen umgeleitet wird, falls ein Kommunikationspartner ausfällt. Z. B. werden Server jeweils zweifach aufgestellt, sodass die Client-Server-Kommunikation zum zweiten Server umgeleitet werden kann, falls der erste Server ausfällt.

FAILOVER CLUSTER (engl.)
Übsg. Verbund von Failover-Systemen zur Ausfallsicherung. Syn. zu High-Availability (HA) Cluster. Diese Systeme bilden ein eigenes Netzwerk und sind jeweils gleich

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_8

aufgebaut und konfiguriert, sodass das aktive System durch einen Side Selector u. Ä. manuell oder automatisch innerhalb kurzer Zeit durch ein anderes System des Clusters ersetzt werden kann, falls ein Problem auftritt. Dadurch wird ein Service-Unterbruch auf ein Minimum reduziert.

FAKE NEWS (engl.)
Übsg. Gefälschte Nachrichten

FAKESHOP (engl.)
Übsg. Gefälschter Shop. Hacker betreiben falsche Online-Shops, in denen sie Produkte zu sehr günstigen Preisen anbieten, aber nach Zahlung der Kaufsumme die Produkte nicht an den Käufer schicken, und sogar die Käuferdaten missbrauchen oder weiterverkaufen.

FAKTOR
Objekt, Verfahren oder Wissen, welches für die Authentifizierung benutzt wird. Dies sind bspw. Passwort, SMS, TAN, Muster, Fingerabdruck, Smartcard, Token, QR-Code, Zertifikat oder Authenticator-App. Bei Ein-Faktor-Authentisierung (1FA) wird einer dieser Faktoren zur Anmeldung benutzt, entsprechend zwei oder mehreren Faktoren für 2FA und MFA. Faktoren werden auch als „Something you know", „Something you do", „Something you are" bezeichnet.

Beispiel

Faktoren können

a. „etwas sein, das man besitzt", z. B. Bankkarte, Smartcard,
b. „etwas sein, das man weiß", z. B. PIN, Passwort,
c. „etwas sein, das darauf beruht, wo man ist", z. B. das Anmelden am WLAN innerhalb des Firmengebäudes,
d. „etwas sein, das darauf beruht, wer man ist", z. B. Fingerabdruck, Gesichtsform,
e. „etwas sein, was man tut", z. B. die Art des Tippens, die Häufigkeit der App-Benutzung.

FALLTÜR-FUNKTIONEN
Syn. zu Einweg-Funktionen

FALSE-FLAG-OPERATION (engl.)
Übsg. Unter anderer Flagge agieren. Um die eigene Herkunft zu verschleiern, verwenden einige Angreifer dieselben Methoden wie andere bekannte Hacker und lenken damit den Verdacht auf diese.

FAQ
Abk. für Frequently Asked Questions

FAS
Abk. für Federated Authentication Service

FAST IDENTITY ONLINE [FIDO] (engl.)
Standardisierte Spezifikationen eines großen Industriekonsortiums vieler führender IT-Firmen für eine normierte und einfache Methode der Authentisierung im Internet. Diese darf von Software- und Hardware-Anbietern in deren Produkten umgesetzt werden. Dies basiert darauf, dass für jede Anmeldung bei einem Online-Dienst ein privater und ein öffentlicher Schlüssel erzeugt wird und der private Schlüssel immer nur beim Benutzer im sog. FIDO-Authenticator bspw. in seinem Handy gespeichert bleibt. Von da an kann der Benutzer sich eindeutig bei diesem Online-Dienst mithilfe seines Handys anmelden, da nur dort der private Schlüssel vorhanden ist. Für die Authentifizierung können dabei drei Faktoren kombiniert werden:

1. Etwas, das der Benutzer weiß, z. B. Kennwort oder PIN.
2. Etwas, das der Benutzer besitzt, z. B. ein Handy oder ein Security Token.
3. Etwas, das typisch für den Benutzer ist, z. B. sein Fingerabdruck oder seine Stimme.

FAT CLIENT (engl.)
PC, der seine Aufgaben als Einzelplatzrechner auch ohne Server ausführen kann, da er mit entsprechender Hard- und Software ausgestattet ist. Syn. zu Thick Client.

FAVICON
Abk. für „Favorite“ und „Icon“. Ein 16 x 16 oder 32 x 32 Pixel kleines Bildchen, welches vom Internetseitendesigner hochgeladen und im Webbrowser direkt neben dem Titel der Internetseite dargestellt wird. Dies kann ein Wiedererkennungszeichen für die Internetseite oder auch ein Firmenlogo darstellen.

FCM
Abk. für Firebase Cloud Messaging

FCM API KEY
Um Push-Benachrichtigungen mittels Firebase Cloud Messaging innerhalb Android zu schicken, benötigt man eine Sender-ID und einen FCM Server API Key.

FDD
1) Abk. für Frequency Division Duplex, ein Frequenzduplexverfahren in der Funktechnik zur Trennung der Funkkanäle von Uplink und Downlink zwischen Empfangs- und Basisstation. 2) Abk. für Floppy Disk Drive, Übsg. Diskettenlaufwerk.

FEDERATED AUTHENTICATION SERVICE [FAS] (engl.)
Windows-Dienst in einem Netzwerk, welcher dynamisch Zertifikate für bereits authentisierte Benutzern ausstellt, sodass diese sich an einem Active Directory anmelden können, wie wenn sie bspw. eine SmartCard mit Zertifikat zur Anmeldung benutzen würden.

FEDERATED IDENTITY (engl.)
Übsg. Digitale Identität, die mittels FIM den Zugriff auf Apps und Diensten in anderen Domänen erhält.

FEDERATED IDENTITY MANAGER [FIM] (engl.)
Software, die eine Verbindung zw. zwei oder mehr vertrauenswürdigen Domänen herstellt, sodass Personen, die sich an einer dieser Domänen authentisiert haben, Apps und Dienste der anderen Domänen mit derselben (föderierten) digitalen Identität benutzen können.

FEDERATION (engl.)
Übsg. Föderation, Zusammenschluss. Software, Methoden und Protokolle, um Benutzeridentitäten über verschiedene Identitätsdienstleister von Organisationen („Identity Provider“) oder über Sicherheitsdomänen hinweg zu verwalten und zugänglich zu machen. Eine solche Federation basiert auf Vertrauensbeziehungen zw. den Entitäten, bspw. mittels digitaler Signaturen, PKI und Verschlüsselung.

FEHLMANIPULATIONEN
Unsachgemäße Benutzung von Systemen, Maschinen, Programmen und Sicherheitsmaßnahmen durch Personen. Fehlmanipulationen gelten heute als eines der größten IT-Sicherheitsrisiken, die mittels Automatisation und Validierung von Benutzereingaben reduziert werden.

FERNZUGRIFF
Anmeldung und Ausführung von Codes oder von Programmen auf einem nicht lokal vorhandenen System. Bspw. kann ein Thin Client oder auch ein Terminalfenster innerhalb eines einfachen PCs den Fernzugang zu einem Server oder Host ermöglichen. Auch Remote Desktop zur Darstellung eines Windows-Systems auf einem anderen PC ist ein Fernzugriff. Um die Anmeldung und den Datentransfer verschlüsselt auszuführen, werden meist Secure Shell (SSH) oder VPN eingesetzt. Großen Wert sollte auf die Verwaltung der Zugriffsberechtigungen und des SSH-Schlüssels gelegt werden, da ansonsten Angreifer den Fernzugriff missbrauchen könnten.

FESTPLATTENVERSCHLÜSSELUNG
Software, welche die ganze Festplatte oder andere Speichermedien wie z. B. SD-Karte verschlüsselt, sodass die enthaltenen Daten bei einem Diebstahl nicht in

Klartext zugänglich sind. In modernen Versionen wird nebst einem Passwort, einem Fingerabdruck oder einer SmartCard auch der Sicherheitschip TPM des Systems mitberücksichtigt, sodass die Festplatte nur innerhalb dieses Systems entschlüsselt werden kann.

FIDO
Abk. für Fast Identity Online

FIDO2
Authentisierungsprotokoll. Weiterentwicklung von FIDO und FIDO U2F. Neu ermöglicht dieser Standard eine Authentisierung mittels eines Geräts des Benutzers, bspw. einem Android-Handy oder Windows-PCs, um die Anmeldung bei Web-Apps ohne Passwort zu ermöglichen. Dabei wird die neue Web-API „WebAuthn“ des W3C mit dem neuen Client-to-Authenticator-Protokoll „CTAP2“ des FIDO-Konsortiums kombiniert.

FIDO-AUTHENTICATOR
Speicher innerhalb des Systems des Benutzers, in welchem seine privaten Schlüssel für FIDO gespeichert werden.

FIDO U2F
Abk. für FIDO Universal 2nd Factor. Spezifikation zur einfachen Zwei-Faktor-Authentifizierung basierend auf der Verschlüsselung mit öffentlichen Schlüsseln und einem Hardware Token beim Benutzer gemäß den FIDO-Spezifikationen. Ein explizites Ziel dieses Standards ist die Anonymität des Benutzers.

FILE EXCHANGE (engl.)
Übsg. Austausch von Dateien

FILE EXCHANGE PROTOCOL [FXP] (engl.)
Übsg. Datei-Austausch-Protokoll. Verfahren in FTP, um Dateien mittels direkter (sog. Site-to-Site-) Übertragung zwischen zwei Servern auszutauschen.

FILELESS MALWARE (engl.)
Übsg. Dateilose Schadsoftware. Dies sind bspw. Programme, die nicht auf die Festplatte, sondern in den RAM-Speicher heruntergeladen und von dort ausgeführt werden. Sie überleben einen Neustart zwar nicht, werden dafür jedoch von einem Anti-Viren-Scanner, der nur die Dateien auf der Festplatte durchsucht, nicht entdeckt.

FILE-LEVEL ENCRYPTION (engl.)
Übsg. Verschlüsselung auf Dateiebene. Hierbei werden einzelne oder alle Dateien einzeln verschlüsselt, im Unterschied zur Festplattenverschlüsselung, bei welcher die ganze Festplatte als Einheit verschlüsselt wird.

FILESLOCKER
Schadsoftware in Form eines Erpressungstrojaners, für den es eine im Internet frei herunterladbare Entschlüsselungssoftware namens FilesLockerDecryptor gibt.

FILESLOCKERDECRYPTOR
Entschlüsselungssoftware für den Erpressungstrojaner FilesLocker.

FILE TRANFER PROTOCOL [FTP] (engl.)
Übsg. Protokoll zur Übertragung von Daten. Mit FTP-Software lassen sich Dateien von einem Gerät zum anderen hochladen und herunterladen. Außerdem können Dateien und Verzeichnisse auf den Geräten erstellt, umbenannt und gelöscht werden. FTP-Software ist in Webbrowsern standardmäßig integriert, sodass Dateien über den Webbrowser heruntergeladen werden können.

FILEVAULT
Programm auf MacOS, um Daten automatisch auf der Festplatte zu verschlüsseln.

FIM
1) Abk. für Federated Identity Manager. 2) Abk. für Forefront Identity Manager

FIN7
Hacking-Gruppe

FINANCIAL ACCESS (engl.)
Übsg. Zugang zu Finanzen, Finanzsystemen und Finanzprodukten. Viele Schadprogramme zielen heutzutage nicht nur auf die Benutzer, sondern vermehrt auf Finanzdatensysteme, wie das Beispiel der attackierten SWIFT-Software einer Bank in Bangladesch im Jahre 2016 zeigte.

FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER [FS-ISAC]
Industrieforum zur gegenseitigen Alarmierung und zur gemeinsamen Zusammenarbeit bei kritischen Sicherheitsangriffen auf den globalen Finanzsektor.

FINGERABDRUCK
1) Jedem Menschen charakteristisches Rillenmuster in der Fingerkuppel, welches für biometrische Authentisierung benutzt werden kann. 2) Hash-Wert von Daten. 3) Identifikationsmerkmal eines Schlüsselpaars. Ein Schlüsselpaar ist eindeutig bestimmt durch eine Schlüssel-ID und einen digitalen Fingerabdruck als Prüfsumme der Schlüsseldaten in hexadezimaler Form, wie z. B. E5DF91164A73A7FF730B73DF3F1130A897B359FD. Der digitale Fingerabdruck ist keine geheime Angabe und kann deshalb bei E-Mails mitgeteilt

werden, sodass der Empfänger die Echtheit des von ihm benutzten öffentlichen Schlüssels des Absenders prüfen kann.

FINGERPRINT (engl.)
Übsg. Fingerabdruck

FIPS
Abk. für Federal Information Processing Standard. Öffentliche Normen der Vereinigten Staaten.

FIPS 140-2
Normierte Anforderungen an kryptografische Module.

FIREBASE CLOUD MESSAGING [FCM] (engl.)
Dienst, um Nachrichten und Benachrichtigungen zwischen Web Apps, Mobile Apps (unter iOS und Android) und Server-Anwendungen zu schicken. Nachfolder von Google Cloud Messaging (GCM).

FIREBUG
Firefox-Erweiterung zur Analyse und Fehlersuche bei Internetseiten.

FIREEYE EX
Sicherheitsprogramm, welches automatisch eingehende E-Mails auf Bedrohungen überprüft und somit vor Schadsoftware und Attacken schützen kann. Insb. versucht diese Lösung vor Spear-Phishing-Attacken zu schützen, die bei Anti-Spam-Programmen häufig nicht entdeckt werden und die den Benutzer dazu verleiten sollen, einen gefährlichen Link oder einen E-Mail-Anhang zu öffnen.

FIREFOX
Von Mozilla entwickelter Webbrowser für viele Plattformen.

FIRESHEEP
Webbrowsererweiterung, mit dem sich übermittelte Daten bei ungeschützten WLAN-Verbindungen mitlesen lassen. Die Webbrowsererweiterung Blacksheep kann davor warnen.

FIREWALL (engl.)
Übsg. Feuerwand (sinnbildlich). Gerät oder Software zw. zwei Netzwerken oder Systemen, um nur die Daten durchzulassen, die bestimmten vordefinierten Kriterien entsprechen. Falls das eine Netzwerk oder System angegriffen wird, verhindert die Firewall im besten Fall einen Angriff auf das andere verbundene Netzwerk oder System.

FIRMWARE (engl.)
Übsg. Firmen-Ware. Von Geräteherstellern in ihren Geräten eingespeicherte Software, die benötigt wird, um das Gerät zu betreiben, ähnlich einem Betriebssystem. Es wird empfohlen, Updates für Firmware zeitnah zu installieren, falls möglich und vom Hersteller angeboten.

FIRMWARE-UPDATES (engl.)
Software-Aktualisierungen für die Firmware eines Geräts. Firmware-Updates müssen meist manuell installiert oder gestartet werden, und ermöglichen nicht nur verbesserte und erweiterte Funktionen, sondern helfen auch, bekannte Attacken zu verhindern.

FLASH
Abk. für Adobe Flash. Plattform zur Programmierung und Darstellung multimedialer Inhalte. Bekannt sind Flashinhalte bspw. von Internet-Games, die im Webbrowser laufen. Flash war revolutionär zur Darstellung von dynamischen Webseiten, wurde jedoch im Laufe der Jahre auch zur Ausführung von Schadsoftware missbraucht, weswegen Flashinhalte in Webbrowsern z. T. blockiert werden.

FLAWS (engl.)
Übsg. Software-Defekte, Software-Fehler, Schwachstellen.

FLEECEWARE-APP (engl.)
App oder Webbrowser-Plug-in, welche scheinbar nützliche Funktionen gratis oder günstig anbietet, dabei jedoch dem Benutzer ein kostspieliges Abonnement unterjubelt, falls er sich nicht aktiv dagegen ausspricht (Opt-Out). Auch eine Deinstallation der App oder des Plug-ins stoppt das Abonnement nicht.

FOOTPRINT (engl.)
Übsg. Fußabdruck

FORCE TLS1.2 (engl.)
Übsg. Erzwingen von TLS1.2

FOREFRONT IDENTITY MANAGER [FIM] (engl.)
Microsoft-Produkt zur Ausübung von Identity Management, um die digitalen Identitäten, Anmeldedaten und Gruppenzugehörigkeiten der Benutzer zu bearbeiten, unter Einbezug von Verbindungen zu Active Directory und Exchange Servern. Wurde durch Microsoft Identity Manager (MIM) abgelöst.

FORENSIC INVESTIGATIONS (engl.)
Übsg. Forensische Analyse.

FORENSISCHE ANALYSE
Kriminaltechnische Untersuchung, bspw. im Zusammenhang mit Betrug durch interne Mitarbeiter.

FOREST (engl.)
Syn. zu Active Directory Forest, AD Forest. Konfiguration innerhalb Active Directory, bei welcher mehrere Domains zusammengehängt werden.

FORGERY (engl.)
Übsg. Fälschung, Verfälschung.

FORGOT-PASSWORD EMAIL (engl.)
Übsg. Passwort-vergessen-E-Mail

FORM (engl.)
Übsg. Formular

FORMBOOK
Schadsoftware in Form eines „Infostealer"-Trojaners.

FORMJACKING
Schadsoftware, die Eingaben des Benutzers bei Webshops mitlesen kann und an Hacker weiterleitet.

FORMULAR
Früher ein Frageblatt auf Papier, heute meist in digitaler Form angebotene Eingabemaske für Daten.

FORTIFY
Abk. für Fortify Static Code Analyzer. Software zur Analyse von Sicherheitsproblemen im Quellcode mit dem Ziel der Vermeidung von Fehlern und zukünftiger Angriffe auf die daraus erstellte Applikation. Bspw. wird auf Codezeilen hingewiesen, bei welchen Cross-Site-Scripting möglich wäre.

FORWARD PROXY (engl.)
Übsg. Vorwärtsgerichtetes Stellvertretersystem. Meist abgekürzt durch „Proxy". System, welches zwischen PCs eines Netzwerkbereichs und PCs eines anderen Netzwerkbereichs steht und u. a. Zwischenspeicherung und Blockieren des Datenverkehrs ermöglicht. Bspw. wird der Aufruf einer Internetseite vom PC des Benutzers nicht direkt zur Internet-Domain geschickt, sondern erst zum Proxy, welcher diese Anfrage nur dann an die Internet-Domain weiterleitet. wenn diese Internetseite nicht bereits kürzlich zuvor abgefragt und auf dem Proxy zwischengespeichert wurde.

FORWARD SECRECY (engl.)
Abk. für Perfect Forward Secrecy

FRAUD (engl.)
Übsg. Rechtlicher Begriff für Betrug. Syn. zu Scam (ugs.).

FREEBSD
Open-Source Unix-kompatibles Betriebssystem

FREIE SOFTWARE
Programme, welche ohne Lizenz oder Einschränkung benutzt, verändert oder weitergegeben werden dürfen. Häufig, aber nicht immer deckungsgleich mit quelloffener Software, bei welcher der Programmcode öffentlich von jedermann im Detail eingesehen, geändert, angepasst und genutzt werden kann, wobei die Autoren die Benutzung jedoch auch einschränken können.

FREQUENZDUPLEXVERFAHREN
Übertragungsform bei 5G Mobilfunk

FRONTEND (engl.)
Übsg. Vorbau, vorderes Ende. Dem Benutzer angezeigter Teil eines Systems, bspw. ein Programm auf einem Client eines Client-Server-Systems.

FRONT RUNNING ATTACK (engl.)
Übsg. Insidergeschäfte durch Kenntnis kommender Käufe. Mit traditionellem Geld platzieren Händler Kaufaufträge, kurz bevor große Kursschwankungen durch große Käufe, von denen sie Kenntnis hatten, entstehen. Bei Kryptowährungen nutzen Angreifer die Situation aus, dass neue Blöcke einer Blockchain erst geschürft werden müssen (sog. Mining), bevor sie registriert sind, und können damit im Namen eines Opfers gefälschte Beträge zuerst registrieren.

FS-ISAC
Abk. für Financial Services Information Sharing and Analysis Center

FTP
Abk. für File Transfer Protocol

FTPS
Abk. für FTP über SSL/TLS

FTP ÜBER SSH [SFTP]
Typ von Secure File Transfer. Kombination von FTP mit Secure Shell (SSH), um Dateien in einer Secure Shell zu übertragen und zu verwalten.

FTP ÜBER SSL/TLS [FTPS]
Typ von Secure File Transfer. Kombination von FTP mit SSL/TLS-Verschlüsselung. Dies erlaubt die Authentisierung des Benutzers und die verschlüsselte Kommunikation.

FULL CONTROL (engl.)
Übsg. Volle Kontrolle. Bspw. kann ein Benutzer volle Kontrolle über ein verschlüsseltes Dokument besitzen und dieses entschlüsseln, ändern, weiterschicken usw.

FULL DISK ENCRYPTION (engl.)
Übsg. Verschlüsselung der ganzen Festplatte anstatt einzelner Dateien.

FULLY QUALIFIED DOMAIN NAME [FQDN] (engl.)
Vollständiger Name einer Domain. Dieser ist zusammengesetzt als Lokalteil.Domain. Top-Level-Domain. Beispiel für FQDN: mail.exampledomain.com.

FUNCTIONAL TESTING (engl.)
Übsg. Überprüfung der Funktionen einer Software. Alle Funktionen, Einstellungen, Berechnungen, Eingaben und Ausgaben einer Software werden entlang eines für diese Software erstellten Testplans im Detail und sowohl mit normalen als auch mit extremen Werten und Eingaben überprüft und mit erwarteten Resultaten verglichen. Jede Abweichung vom erwarteten Verhalten wird als Defect (aba. Bug) notiert und dem Entwickler zur Korrektur übergeben. Das Functional Testing folgt meist nach dem Smoke Testing und dem Sanity Testing.

FYI
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „For your Information“, Übsg. „Zur Information“.

G

9

GALOIS/COUNTER MODE [GCM] (engl.)
Berechnungsmethode, bei welcher ein Zähler (Counter), eine Blockchiffre und Blockverkettungen verwendet werden, um Verschlüsselung und Authentisierung von Daten zu ermöglichen. Dabei wird der Initialwert („Initialization Vector“) mit dem ersten Counter kombiniert und mit einer Blockchiffre, meist AES, verschlüsselt. Dies bildet den Authentisierungs-Tag. Für die Datenverschlüsselung des Klartextes wird **1)** der Counter jeweils hochgezählt, **2)** das Resultat mit der Blockchiffre verschlüsselt, **3)** danach mit dem neuen Klartextteil kombiniert und **4)** mit dem vorherigen Geheimtextteil verbunden.

Auf GCM basierend wird der Galois Message Authentication Code (GMAC) berechnet.

GALOIS MESSAGE AUTHENTICATION CODE [GMAC] (engl.)
Datenauthentisierung mittels GCM-Berechnungen.

GAMEOVER ZEUS
Im Jahre 2014 stark verbreitete Bankenerpressungssoftware, welche bis zu einer Million PCs infizierte.

GAMIFICATION (engl.)
Methoden, um eine Tätigkeit wie ein Spiel aussehen zu lassen, mit dem Ziel, Menschen zu bewegen, sich eher und sofort damit zu beschäftigen. Wird häufig bei Sport-Apps verwendet, um die Benutzer anzuspornen, besser zu sein als die anderen.

GANDCRAB
Typ von dateiverschlüsselnder Ransomware, welcher seit 2018 sein Unwesen auf Windows-Systemen treibt und im Darkweb angeboten wird. Diese Malware nutzt wie

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_9

WannaCry den SMB-Exploit aus, besitzt aber zusätzlich neuere Methoden, um Windows XP und Windows Server 2003 anzugreifen und benutzt mit Salsa20 eine schnellere Verschlüsselungsfunktion als die in WannaCry eingesetzte RSA-2048, wodurch nach der Infektion schneller großer Schaden angerichtet wird. Seit Februar 2019 wird online ein Entschlüsselungstool angeboten.

GATEWAY (engl.)
Übsg. Durchgangsstelle, Übergangsstelle. Gerät oder Software innerhalb eines Netzwerks, welches den Verbindungspunkt zwischen diesem Netzwerk und einem anderen Netzwerk oder zw. einer Applikation und dem Netzwerk darstellt. Bspw. kann ein Firmennetzwerk an einen Router angehängt sein, welcher den Zugang zum Internet kontrolliert. Dabei agiert der Router als Gateway. Auf dem Gateway können die Anfragen auf Manipulation überprüft werden.

GATEWAY-PORT (engl.)
Konfigurierte Ports, welche für die Verbindung zwischen zwei Netzwerken geöffnet oder geschlossen wurden, um nur bestimmten Datentransfer zu erlauben. Bspw. kann eine Firma dadurch verhindern, dass FTP von innerhalb der Firma zum Internet benutzt wird.

GCM
Abk. für Galois/Counter Mode

GDPR
Abk. für EU General Data Protection Regulation. Syn. zu Datenschutz-Grundverordnung (DSGVO). Seit Mai 2018 gültige Gesetze zum Schutz von persönlichen Daten, welche von Firmen verarbeitet werden, die in der EU tätig sind.

GEBURTSTAGSPARADOXON
Intuitiv scheint die Wahrscheinlichkeit, dass zwei Personen in einem Raum am gleichen Tag Geburtstag haben, zu hoch. Dieses scheinbare Paradoxon folgt aus der Unfähigkeit der Menschen, bestimmte Wahrscheinlichkeiten richtig zu schätzen.

GEHACKT
System, Netzwerk, Software oder Gerät, zu welchem unerlaubt Zutritt verschafft wurde und welches absichtlich geschädigt, ausspioniert, mit Schadsoftware infiziert oder anderweitig beeinträchtigt wurde. Dabei werden meist Schwachstellen von Hardware oder Software ausgenutzt oder Hintertüren, die der Software-Programmierer mutwillig oder in guter Absicht eingebaut hat. Auch werden Methoden verwendet, um an ein Passwort zu gelangen, welches dann Zugang zu einem System ermöglicht.

GEHEIMDIENST
Team, welches verdeckt für das eigene Land operiert, um die Sicherheit der Bewohner dieses Landes zu erhöhen.

GEHEIMER SCHLÜSSEL
Informationen, die nicht öffentlich, sondern nur einer Person oder einer kleinen Anzahl Personen bekannt sind und dazu verwendet werden können, um Daten zu verschlüsseln oder zu entschlüsseln, oder um signieren, sodass deren Herkunft klar nachvollziehbar bleibt. **1)** Syn. zu Privatem Schlüssel. Bei asymmetrischer Verschlüsselung werden Daten mit einem öffentlichen Schlüssel verschlüsselt und mit dem zugehörigen geheimen Schlüssel des Schlüsselpaars entschlüsselt. **2)** Bei symmetrischer Verschlüsselung wird der gleiche geheime Schlüssel sowohl für die Ver- als auch für die Entschlüsselung verwendet.

GEHEIMTEXT
Syn. zu Chiffre, Cipher. Daten, wie bspw. eine Textnachricht, welche verschlüsselt vorliegen, nachdem sie mit einem geheimen Schlüssel kryptografisch aus einem Klartext umgewandelt wurden.

GEHEIMTEXTBLOCK
Syn. zu Blockchiffre, Block Cipher. Daten spezifischer Länge, wie bspw. eine Textnachricht, die verschlüsselt vorliegen, nachdem sie als Block mit einem geheimen Schlüssel kryptografisch aus einem Klartext vorgegebener Länge umgewandelt wurden.

GENERAL DATA PROTECTION REGULATION [GDPR] (engl.)
Abk. für EU General Data Protection Regulation. Syn. zu Datenschutz-Grundverordnung (DSGVO). Seit Mai 2018 gültige Gesetze zum Schutz von persönlichen Daten, welche von Firmen verarbeitet werden, die in der EU tätig sind.

GENERATION OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Erzeugung eines kryptografischen Schlüssels

GENERIC SECURITY SERVICE APPLICATION PROGRAM INTERFACE [GSSAPI] (engl.)
Übsg. Anwendungs-Programmierschnittstelle für allgemeinen Sicherheitsdienst. Funktionsbibliotheken zum Einbau in Programme, um auf Sicherheitsdienste und -geräte zuzugreifen. Dabei werden Token benutzt, die auch über unsichere Netzwerke ausgetauscht werden können. Dies wird v. a. für die Authentifizierung von Benutzern verwendet, bspw. bei Kerberos.

GEOBLOCKING (engl.)
Übsg. Ausschluss von Internetnutzern aufgrund ihrer IP-Adresse.

GEO-LOCATION AWARENESS (engl.)
Übsg. Positionsabhängigkeit. Erkennen der Position eines Geräts und Anwenden darauf basierender, positionsabhängiger Regeln. Bspw. kann der Zugriff auf Firmendaten für private Geräte eingeschränkt werden, sobald diese sich nicht mehr innerhalb des Firmengebäudes befinden.

GERMANWIPER
Schadsoftware in Form einer Ransomware, welche Daten dauerhaft zerstört.

GESICHTSERKENNUNG
Syn. zu Face Recognition. Software, die das Gesicht einer Person aufnimmt und die Gesichtsformen und -details mit vorher gespeicherten Gesichtsdaten vergleicht. Wurden in der Vergangenheit nur 2D-Bilder aufgenommen und zur Erkennung verwendet, erlauben aktuelle Techniken die Aufnahme eines Gesichts in 3D und sind deshalb sicherer, da diese Systeme nicht mithilfe eines Fotos überlistet werden können.

GESICHTSSCANNER
Syn. zu Gesichtserkennung, Face-ID. Gerät und Software zur Erkennung der Form und der Details des Gesichts einer Person. Die damit aufgenommenen Bilddaten können mit zuvor registrierten Gesichtsinformationen verglichen werden und damit als biometrische Anmeldemethode benutzt werden.

GET
Syn. zu HTTP-GET.

GH0STRAT
Trojaner-Schadsoftware auf Windows-Systemen zur Cyber-Spionage. Die enthaltene Software „RAT“ ist das in Trojanern häufig eingesetzte Remote Administration Tool.

GHOSTDNS
Schadsoftware, welche böswillig in Routern hineingebracht wird, um DNS-Abfragen zu ändern und damit Webaufrufe auf Phishingseiten umzuleiten, welche vorgeben, Startseiten von Banken und anderen Firmen zu sein, sodass der Benutzer in die Irre geführt wird und sein Passwort eingibt.

GIC
Abk. für Group Identity Certificate

GITHUB
Online-Dienst zur gemeinsamen Erstellung und Bearbeitung von Software mit Funktionen zur Versionsverwaltung.

GLÄSERNER MENSCH
Ugs. benutzter, negativ behafteter Begriff zur Empfindung von Personen, die sich durch Überwachungskameras, Software und Behörden verfolgt und wie „durchsichtig“ fühlen.

GLOBALLY UNIQUE IDENTIFIER [GUID] (engl.)
Eindeutige, maschinenlesbare Identifikationsnummer für Funktionen, Einstellungen oder Lizenzen innerhalb eines Programms oder eines Systems. Basierend auf UUID.

Beispiel: {8D5197F5-AB1B-4877-BAAE-C1242FEFB118}

GLOBAL POSITIONING SYSTEM [GPS] (engl.)
Übsg. Globales Positionsbestimmungssystem. Kombination von Satelliten, welche ständig ihre aktuelle Position und die genaue Uhrzeit mittels codierten Radiosignalen senden. Über Signallaufzeiten kann damit die genaue Position des Empfängers bestimmt und bspw. für die Navigation benutzt werden.

GLOBAL SIDE SELECTOR (engl.)
Übsg. Globaler Systemwähler. Gerät zur automatischen Auswahl des aktiven Servers in einem Failover-Cluster, damit die Datenkommunikation zwischen Client und Server ununterbrochen aufrechterhalten bleibt, auch bei Ausfall eines der Server im Cluster.

GLOBALTIME [GT] (engl.)
International diskutierter Vorschlag[1] zur einfacheren Darstellung der Zeit in elektronischen Systemen, unabhängig von Zeitzonen. Der Wert der „GlobalTime“ ist weltweit derselbe und verhindert umständliche Angaben wie „14 Uhr (UTC-4)“. Die Zählung der Stunden beginnt bei 170 und endet bei 194, um Verwechslungen mit anderen Zeit- und Datumsangaben zu verhindern. Damit bedeutet GT170 = 0 h GMT, dann GT171 = 1 h GMT, dann GT172 = 2 h GMT usw.

Beispiel: Die an jedem Punkt der Erde gleiche Zeitangabe GT175:30:17 entspricht 5 Uhr 30min 17s in London und 12 Uhr 30min 17s in Singapore

GMAC
Abk. für Galois Message Authentication Code

GMT
Abk. für Greenwich Mean Time. Übsg. Mittlere Greenwich-Zeit. Zeitzone, welche sich an der UTC orientiert.

[1] globaltime.relativität.ch *(Abgerufen am 22.12.2019)*.

GNU
1) Projektname zur Entwicklung eines freien Betriebssystems. **2)** Abk. für GNU General Public License (GNU GPL), einer Lizenzvariante, welche häufig für freie Software verwendet wird und es erlaubt, die Software auszuführen, anzupassen und weiterzugeben.

GNU GENERAL PUBLIC LICENSE [GNU GPL] (engl.)
Lizenzvariante, welche häufig für freie Software verwendet wird und es erlaubt, die Software auszuführen, anzupassen und weiterzugeben.

GNU GPL
Abk. für GNU General Public License. Syn. zu GNU, GPL.

GNUPG
Abk. für GNU Privacy Guard

GNUPG FÜR OUTLOOK [GPGOL]
Abk. für GNU Privacy Guard für Outlook. Erweiterungsprogramm innerhalb Microsoft Outlook, um PGP- oder S/MIME-Verschlüsselung für E-Mails anzuwenden.

GNU PRIVACY ASSISTENT [GPA] (engl.)
Übsg. GNU-Privatsphärenassistent. Programm zur Verwaltung von Zertifikaten.

GNU PRIVACY GUARD [GNUPG] (engl.)
Übsg. GNU-Privatsphärenschutz. Freie Kryptografie-Software zum Verschlüsseln und Signieren von Dateien. Die Implementation basiert auf OpenPGP, einer PGP-Variante.

GNU PRIVACY GUARD FOR WINDOWS [GPG4WIN] (engl.)
Übsg. GNU-Privatsphärenschutz für Windows. Freie Kryptografie-Software zum Verschlüsseln und Signieren von E-Mails, Dateien und Ordnern unter Microsoft Windows.

GO
1) Open-Source-Programmiersprache, die das Ziel verfolgt, rasch einfache, aber effiziente Software zu schreiben. **2)** Strategienbrettspiel.

GOLANG
Syn. zur Programmiersprache GO.

GOLDEN TICKET (engl.)
Übsg. Goldenes Ticket. Kerberos-Schlüssel, der einem Benutzer zeitlich unlimitierten Domain-Admin-Zugang ermöglicht.

GO-LIVE (engl.)
Übsg. In Produktion bringen, den Anwendern zur Verfügung zu stellen.

GOOGLE.COM
Internetsuchmaschine

GOOGLE AUTHENTICATOR
Authentisierungs-App für 2FA.

GOOTKIT
Schadsoftware in der Form eines Trojaners, welcher vertrauliche Informationen stiehlt. Es öffnet zudem eine Hintertür, um weitere Schadprogramme nachzuladen. Der Trojaner gelangt auf den PC des Opfers über angeklickte Links in E-Mails oder über den Besuch von verseuchten Internetseiten.

GOPHER
Informationsdienst und Protokoll, welcher im Jahre 1991 quasi als Vorgänger des WWW entstand und das Verteilen, Suchen und Laden von Dokumenten vereinfachte.

GOST
Blockchiffre mit 64-Bit-Blöcken und 256-Bit-Schlüsseln.

GPA
Abk. für GNU Privacy Assistent. Programm zur Verwaltung von Zertifikaten.

GPG
Abk. für GNU Privacy Guard. Syn. zu GNUPG

GPG4WIN
Abk. für GNU Privacy Guard for Windows

GPGEX
Erweiterung für den Windows Explorer, um Dateien mit GPG zu verschlüsseln.

GPGOL
Abk. für GnuPG für Outlook

GPG SHELL EXTENSION [GPGEX] (engl.)
Erweiterungsprogramm für den Windows Explorer innerhalb Microsoft Windows, um Verschlüsselung via Kontextmenü auf Dateien anzuwenden.

GPL
Abk. für GNU General Public License. Syn. zu GNU GPL, GNU.

GPO
Abk. für Group Policy Object.

GPS
Abk. für Global Positioning System.

GPU
Abk. für Graphics Processing Unit. Übsg. Grafikprozessor.

GRÖSSTE CYBER- UND IT-SECURITY-GEFAHREN
Firmen sind angreifbar, u. a. aufgrund der Top-3-Risiken:

a) Nicht aktuell gehaltene Systeme
b) Schwache oder nicht geänderte Standardpasswörter
c) Mitarbeiterfehler durch Social Engineering oder Phishing

GROUP IDENTITY CERTIFICATE [GIC] (engl.)
Übsg. Zertifikat zur Identität eines Clients in der Gruppe. Bei ADRMS wurde GIC durch Rights Account Certificate (RAC) ersetzt.

GROUP POLICY OBJECT [GPO] (engl.)
Übsg. Gruppenrichtlinienobjekt

GRUNDSCHUTZHANDBUCH [GSHB]
Von der BSI herausgegebenes Handbuch zur systematischen Identifikation und Umsetzung notwendiger Sicherheitsmaßnahmen in Firmen und Behörden. Heute eher IT-Grundschutz genannt.

GRUPPENRICHTLINIENOBJEKT
Syn. zu GPO. Funktion innerhalb Windows, um Einstellungen, bspw. Registry-Werte, zentral zu definieren und automatisiert anzuwenden. IT-Admins können durch die Ausbreitung von GPOs in der Firma einheitliche Einstellungen auf den von ihnen verwalteten PCs setzen.

GSHB
Abk. für Grundschutzhandbuch

GT
Abk. für GlobalTime

GSSAPI
Abk. für Generic Security Service Application Program Interface

GUI
Abk. für Graphical User Interface

GUID
Abk. für Globally Unique IDentifier

H

10

HACKBACK (engl.)
Zurückschlagen von Cyber-Abwehrgruppen gegen Hacker.

HACKER HERO (engl.)
Hacker mit positiven Absichten, welcher Firmen hilft, sich gegen andere Hacker zu schützen.

HACKING (engl.)
Eindringen in Systeme, Netzwerke, Programme oder Geräte, für die der Eindringling keine Berechtigung hat. Dabei werden meist Schwachstellen von Hardware oder Software ausgenutzt oder Hintertüren, die der Software-Programmierer mutwillig oder mit guter Absicht eingebaut hat. Auch werden Methoden verwendet, um an ein Passwort zu gelangen, welches den Zugang zu einem System ermöglicht.

HACK-PROOFED (engl.)
Übsg. Hacking-sicher. Geheime oder sensible Daten, wie bspw. medizinische Dokumente u. Ä., die weder heute noch in absehbarer Zeit von unbefugten Personen gelesen werden können. Hierbei muss bedacht werden, dass Computer und insb. Quantencomputer rapide leistungsstärker werden und die Daten auch gegen diese geschützt sein müssen.

HACKTIVIST
Person, die ihren politischen Zielen mittels Hacking Gehör verschafft.

HA CLUSTER (engl.)
Abk. für High-Availability Cluster

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_10

HAKAI
IoT Botnetz, welches v. a. Router von D-Link und Huawei missbraucht.

HALBDUPLEX
Kommunikation, die in beide Richtungen abwechslungsweise stattfindet. Bspw. ein Gespräch mit einem Freund über Funk, bei welchem das Ende des Satzes vom Freund abgewartet wird, bevor man selber spricht. Grenzt sich gegen simplexe und vollduplexe Kommunikation ab.

HAN
Abk. für Home Area Network

HANDLING OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Bearbeitung eines kryptografischen Schlüssels.

HANDLING OF INFORMATION (engl.)
Übsg. Bearbeitung von Information.

HANDSHAKE (engl.)
Übsg. Händeschütteln. Beginn einer Kommunikation zwischen zwei Systemen. Dabei werden bspw. kryptografische Schlüssel oder Session IDs ausgetauscht, um diese im weiteren Verlauf der Kommunikation beidseitig zu verwenden.

HARD DISK DRIVE [HDD] (engl.)
Übsg. Festplattenlaufwerk

HARDENING (engl.)
Übsg. Härtung. Verfahren, um ein System sicherer und damit weniger anfällig für Hacking zu machen. Dies geschieht mittels unterschiedlicher Methoden und Tools, wie bspw. Schließung von Netzwerkports, Patching der Software, Aktivierung von Firewalls oder Einsetzen eines Anti-Viren-Programms.

HARDENING OF APPLICATIONS AND INFRASTRUCTURE (engl.)
Übsg. Härtung von Applikationen und Infrastruktur. Verfahren, um Apps und Infrastruktur sicherer und damit weniger anfällig für Hacking zu machen. Dies geschieht mittels unterschiedlicher Methoden und Tools, wie bspw. Schließung von Netzwerkports, Patching der Software, Aktivierung von Firewalls oder Einsetzen eines Anti-Viren-Programms.

HARDWARE (engl.)
Übsg. Geräte. Teile eines Computers oder anderer Geräte, die physisch vorhanden sind und sich berühren lassen. Bspw. Monitor, Tastatur, Maus, Netzwerkkabel, Drucker, CPU etc.

HARDWARE AGENT (engl.)
Übsg. Autonomer Roboter. Kombination aus Software Agent, Sensoren und Aktuatoren, die zusammen Aktionen ausführen und die Umgebung verändern.

HARDWARE SECURITY MODULE [HSM] (engl.)
Übsg. Hardware-Sicherheitsmodul

HARDWARE-SICHERHEITSMODUL [HSM]
Gerät, dessen Hauptfunktionen die sichere Schlüsselerzeugung und -verwaltung ist. Dies wird erreicht durch

a. ein Gehäuse, welches Eingriffe von außen detektieren kann (sog. Tampering-Erkennung),
b. die Möglichkeit, Authentisierung nur unter Verwendung von Hardware Token zu erlauben,
c. Schutz vor Zugriff durch Einfordern des Mehr-Augen-Prinzips, d. h. ein Zugriffscode wird auf „n“ Personen aufgeteilt und der Zugriff danach nur mit „k-von-n“ Personen erlaubt,
d. sichere HSM-Backups,
e. implementierte, optimierte Kryptoalgorithmen zur symm. und asymm. Verschlüsselung, zur Erstellung von Signaturen sowie zur Erzeugung von Hash-Werten, Zufallszahlen, Schlüsseln und PINs.

Gängige HSMs basieren häufig auf eigens dafür erstellten Unix-Betriebssystemen.

HARDWARE TOKEN
Syn. zu Security Token. Hardwarebasierter und damit physischer Berechtigungsnachweis. Beispiele sind Symantec VIP Security Card, RSA SecurID u. Ä.

HARTKODIERTER SCHLÜSSEL
Für AES-Blockverschlüsselung und andere kryptografische Methoden verwendeter Schlüssel, der direkt in die Codezeilen des Verschlüsselungsprogramms eingetippt wurde und damit unveränderlich ist.

HARVEST FROM ATM (engl.)
Übsg. Ernten bei einem Geldautomaten. Bezeichnung für das Auslesen von Karten- und evtl. anderer Daten bei Geldautomaten.

HASH
Abk. für Hash-Wert. Resultat einer Hash-Funktion, welche Daten beliebiger Länge in einen Hash-Wert festgelegter Länge umwandelt. Hash-Werte werden bspw. als Index für die effiziente Suche in großen Daten benutzt oder auch zur Sicherstellung der Integrität von Daten. Hash-Werte werden auch als Fingerabdruck von Ursprungsdaten benutzt, da sie die Daten eindeutig beschreiben.

HASH-ALGORITHMUS
Syn. zu Hash-Funktion

HASHEN
Syn. zu „Hash-Funktion anwenden“

HASH-FUNKTION
Algorithmus, um Daten beliebiger Länge in Hash-Werte festgelegter Länge umzuwandeln. Kryptografische Hash-Funktionen sind darauf ausgelegt, keine Kollisionen zu enthalten, d. h. keine zwei Eingabedaten sollen auffindbar sein, die die gleichen Hash-Werte erzeugen. Nur kollisionsfreie Hash-Funktionen erlauben die Sicherstellung der Integrität von Daten und damit die sichere Speicherung von Passwörtern u. Ä.

Beispiele für kryptografische Hash-Funktionen: MD5, SHA, Blowfish.

HASHING (engl.)
Übsg. Anwenden eines Hash-Algorithmus.

HASH MESSAGE AUTHENTICATION CODE [HMAC] (engl.)
Berechnung zur Erzeugung eines Message Authentication Codes (MAC). Diese Prüfsumme wird durch Kombination der Daten mit einem Schlüssel und einer kryptografischen HASH-Funktion erstellt. Dies erlaubt die Validierung der Datenintegrität und Datenherkunft. HMAC wird u. a. für TLS und für HMAC-SHA1 eingesetzt.

HASHTAG (engl.)
Begriff gebildet aus dem engl. Wort „Hash“ für Doppelkreuz (#) und dem engl. Wort „Tag“ für Markierung. Wird seit ca. 2007 in Kurznachrichten, sozialen Medien und in der physischen Welt benutzt, um einen Begriff als Schlagwort, Leitwort oder Motto zu markieren. Andere Personen können denselben Hashtag benutzen, um zum gleichen Thema Stellung zu nehmen.

Beispiel

Beispiele für Hashtags:
#Springer #IT-Security #2020

HAVE I BEEN PWNED? (engl.)
Übsg. Wurde ich erwischt? Online-Service[1], welcher öffentlich zugängliche Daten aus Datenlecks und Hackings benutzt, um festzustellen, ob eine E-Mail-Adresse oder ein Passwort bereits Opfer solcher Datenlecks wurde und damit als unsicher anzusehen ist. Das Wort „Pwned" ist durch einen Tippfehler aus „owned" entstanden.

HAWKEYE
Schadsoftware in Form eines „Infostealer"-Trojaners.

HDD
Abk. für Hard Disk Drive, Übsg. Festplattenlaufwerk.

HDF
Abk. für Hierarchical Data Format. Format zur Speicherung großer Datenmengen.

HDMI
Abk. für High Definition Multimedia Interface. Schnittstelle für digitale Bild- und Tonübertragung. Neueste Version HDMI 2.1 kann bis zu 38 Gbit/s Daten übertragen.

HDR
Abk. für High Dynamic Range. Ein Videoformat.

HEARTBEAT (engl.)
Übsg. Herzschlag. Funktion bei Server-Clustern, um regelmäßig zu prüfen, welche Server des Clusters noch funktionsfähig sind. Heartbeats werden auch bei anderen Systemen verwendet, um zu prüfen, ob diese noch am Netz angehängt und in Betrieb sind.

HEARTBLEED BUG
Einer der schwerwiegendsten Sicherheitslücken im Internet- und Computerumfeld in den Jahren 2012 bis 2014. Dieser ließ sich auf OpenSSL zurückführen und ermöglichte aufgrund eines Programmierfehlers Teile des Arbeitsspeichers der beteiligten Clients und Servern auszulesen, trotz verschlüsselter TLS-Verbindungen. Daten, wie private Schlüssel oder Passwörter konnten dadurch missbräuchlich kopiert werden. Aufgrund der weltweiten Verbreitung von OpenSSL waren viele große und kleine Anbieter von Online-Diensten, aber auch Router, Netzwerkdrucker und andere Ressourcen für solche Angriffe anfällig. Sicherheitsupdates und Patches von Software-Anbietern lösten das Problem weitestgehend.

[1] https://haveibeenpwdned.com *(Abgerufen am 22.12.2019).*

HEIF
Abk. für High Efficiency Image File Format. Ein neueres Format zur Speicherung von Bildern.

HEIMNETZWERK
Verbund von vernetzten Geräten innerhalb eines Gebäudes oder Raums mit dem Ziel der gemeinsamen Nutzung von Datenspeicher, Drucker und Internetzugang.

HEIST (engl.)
Übsg. Raub

HELLO WORLD (engl.)
Zwei-Wort-Satz, welcher häufig als Resultat eines ersten einfachen Programms in einer neuen oder neu installierten Programmiersprache ausgegeben wird, um zu prüfen, ob die Programmiersprache richtig läuft und der Programmierer die Syntax dieser Sprache versteht.

HERUNTERLADEN
Syn. zu Download

HEURISTICS (engl.)
Übsg. Heuristiken

HEURISTIKEN
Abkürzungen in Algorithmen. Bei Programmen oder bei einer Entscheidungsfindung müssen nicht alle Möglichkeiten analysiert werden, da die Erfahrung zeigt, dass einige davon nicht relevant oder nicht möglich sind. Nur mit solchen Abkürzungen ist es bspw. einem Schachcomputer möglich, einen nächsten Zug auszuwählen, ohne jahrelang alle noch möglichen Züge durchzutesten.

HEXADEZIMALE ZAHL
Darstellung von Zahlen im 16er-System mit den Ziffern 0–9 und A–F, welche den Dezimalzahlen 0–15 entsprechen. Häufig werden hexadezimale Zahlen zur Verdeutlichung mit einem zusätzlichen „h“ oder „0x“ gekennzeichnet, z. B. 20h, 20H, 0x20.

Beispiel: die hexadezimale Zahl 0x6AC36 entspricht der Dezimalzahl 437302.

HEX-EDITOR
Software zur Darstellung und Bearbeitung von Dateien. Dabei wird der Inhalt einer Datei als Folge von Hexadezimalzahlen statt als Text dargestellt.

HEXSPEAK
Zahlen in hexadezimaler Schreibweise, die scheinbar Wörter beinhalten. Bei einigen Software-Produkten als Rückgabe- oder Fehlerwert zufällig oder bewusst gewählt.

Beispiel

0x**BADCAB1E** „BAD CABLE“ = „Schlechtes Kabel“
0x**BADC0DED** „BAD CODED“ = „Schlecht Programmiert“

HIDDEN VECTOR ENCRYPTION [HVE] (engl.)
Übsg. Verschlüsselung versteckter Attribute. Kryptografische Methode, bei welcher ein spezieller Schlüssel zu einem privaten und öffentlichen Schlüsselpaar hinzuerzeugt wird, und mit welchem Teile einer verschlüsselten Nachricht entschlüsselt werden können, ohne den ganzen Text entschlüsseln zu müssen. Dies kann benutzt werden, um bspw. in einer verschlüsselten E-Mail nach einem bestimmten Stichwort (sog. Attribut oder Prädikat) zu suchen. Verwandt mit homomorpher Verschlüsselung.

HIDS
Abk. für Host Intrusion Detection System

HIERARCHICAL DATA FORMAT [HDF] (engl.)
Übsg. Hierarchisches Datenformat. V. a. in wissenschaftlichen Anwendungen benutztes Format zur Speicherung großer Datenmengen. Dabei können die Daten in beliebiger Verzeichnisstruktur effizient gespeichert und ausgelesen werden. HDF-Dateien besitzen die Endung „.H5“.

HIGH-AVAILABILITY CLUSTER [HA CLUSTER] (engl.)
Übsg. Cluster mit hoher Verfügbarkeit. Syn. zu Failover Cluster. Gruppe von Servern mit gleicher Konfiguration, die sich Datenbanken und Ressourcen teilen. Bei Ausfall eines Servers (eines sog. „Node“) werden Client-Anfragen in kurzer Zeit zu einem anderen Server umgeleitet, um die hohe Erreichbarkeit der Anwendung zu garantieren. Im laufenden Betrieb kann regelmäßig geprüft werden, welche Server noch funktionsfähig sind, durch den Einsatz einer sog. „Heartbeat“-Abfrage.

HIGH EFFICIENCY IMAGE FILE FORMAT [HEIF] (engl.)
Neueres Bildspeicherformat, welches im Gegensatz zu JPG und GIF eine effizientere Komprimierung durchführt und weitere Vorteile bietet. HEIF wird bei neueren Apple-Betriebssystemversionen eingesetzt und ebenso bei Windows 10 ab Herbst 2018.

HIGHLY PRIVILEGED USERS [HPU] (engl.)
Systembenutzer mit zusätzlichen Zugangs- oder Änderungsrechten. Oft werden solche erweiterten Rechte an IT-Admins vergeben, um das Firmennetzwerk oder die

Firmen-PCs zu administrieren. Damit einzelne Personen nicht ständig über solche Rechte verfügen („Standing Access“) und dabei aus Versehen oder absichtlich großen Schaden anrichten, werden solche Rechte nicht dem Standardaccount der IT-Admins zugewiesen, sondern an strenger kontrollierte und überwachte zusätzliche IT-Admin-Accounts („Secondary Account“) mit eigenen Zugangsdaten.

HIJACKING (engl.)
Übsg. Entführung, auch im Sinne von Hacking, Übernahme und Missbrauch eines Systems.

HINTERTÜR
Geheimer Zugang zu einem System oder Programm oder eine Geheimfunktion innerhalb eines Programms, um versteckte, häufig weitreichende Einflussmöglichkeiten zu erhalten. Gutmütige Programmierer bauen solche Hintertüren ein, um bspw. ihre eigenen Softwareteile einzeln zu testen. Ein Spieleprogrammierer kann sich mit solchen Hintertüren bspw. unendlich viele Punkte vergeben und kann damit verhindern, sein Spiel ständig von vorne beginnen zu müssen, um es zu testen. Weniger gutmütige Programmierer integrieren solche Hintertüren, um in Zukunft die Möglichkeit zu haben, in das System einzudringen, ohne offiziell die entsprechenden Rechte und ohne die Autorisation zu besitzen.

HITRUST
Organisation, welche Datenschutzstandards entwickelt und zertifiziert. Das von HITRUST erstellte HITRUST CSF Framework ermöglicht es Firmen und Behörden, ihre Datenschutz-, Compliance- und regulatorischen Maßnahmen risikobasiert zu identifizieren, zu beschreiben und zu bearbeiten.

HIVE
Bereich in der Windows-Registrierungsdatenbank und dessen Repräsentation als Datei.

HKCC
Abk. für HKEY_CURRENT_CONFIG. Ein Bereich (Hive) innerhalb der Windows-Registrierungsdatenbank.

HKCR
Abk. für HKEY_CLASSES_ROOT. Ein Bereich (Hive) innerhalb der Windows-Registrierungsdatenbank.

HKCU
Abk. für HKEY_CURRENT_USER. Ein Bereich (Hive) innerhalb der Windows-Registrierungsdatenbank.

HKLM
Abk. für HKEY_LOCAL_MACHINE. Ein Bereich (Hive) innerhalb der Windows-Registrierungsdatenbank.

HLD
Abk. für High-Level-Design. Dokument, welches das geplante Design für ein Produkt grob beschreibt.

HMAC
Abk. für Hash Message Authentication Code

HOCHLADEN
Syn. zu Upload. Transferieren eines Programms, einer Datei, eines Texts, einer Tabelle u. Ä. vom benutzten Computer auf einen anderen Computer, der sich im gleichen Raum, im gleichen Netzwerk oder irgendwo im Internet befindet. Häufig geschieht dies im Webbrowser, im Windows Explorer, im Finder des Mac oder via FTP.

HODL
Durch einen Tippfehler entstandenes Synonym für „HOLD“. Besitzer von Bitcoins und anderer Kryptowährungen deuten mit einem solchen Slogan in sozialen Medien an, dass sie aktuell ihren Bitcoin-Bestand nicht verkaufen werden, sondern weiterhin halten.

HOLD YOUR OWN KEY [HYOK] (engl.)
Übsg. Halte deinen eigenen Schlüssel. Von Firmen mit sensiblen Daten gewählte Konfiguration innerhalb Azure Information Protection (AIP), bei welcher der Hauptschlüssel durch die Firma selber erzeugt, bewirtschaftet, innerhalb der Firmengrenzen („On-Premise“) gespeichert und benutzt wird, im Gegensatz zu BYOK.

HOME AREA NETWORK [HAN] (engl.)
Übsg. Heimnetzwerk. Syn. zu Lokales Netzwerk (LAN). Verbund von Systemen, bei welchem die Geräte über Netzwerkadressen angesprochen werden und untereinander kommunizieren können. Bspw. können kabelgebundene und kabelfreie (wireless) Geräte mit einem Router verbunden werden und von diesem jeweils eine IP-Adresse im gleichen IP-Netzwerk erhalten. Dadurch bilden diese Geräte ein HAN und können untereinander kommunizieren. Um mit anderen Geräten im Internet zu kommunizieren, kann der Router als Modem über einen Breitbandanschluss die Verbindung des HAN zum Internet herstellen.

HOME NETWORK DEVICES (engl.)
Übsg. Heimnetzwerkgeräte. Gesamtheit aller Geräte zu Hause oder in einem Büro, die sich mit dem Heimnetzwerk oder direkt mit dem Internet verbinden können. Dazu zählen u. a. Modem, Router, IP-Webcams, Computer, WLAN-Verstärker, TVs, Handys, Radios usw.

HOMEPAGE (engl.)
Syn. zu Hauptinternetseite einer Firma, einer Familie, eines Vereins etc.

HOMOMORPHE VERSCHLÜSSELUNG
Kryptografisches Verfahren, welches Möglichkeiten bietet, um Berechnungen auf verschlüsselten Daten auszuführen, ohne die Daten zu entschlüsseln. Dazu werden Algorithmen auf den ursprünglichen, unverschlüsselten Daten definiert, die danach angepassten Algorithmen auf den verschlüsselten Daten entsprechen. Dies kann bspw. dazu verwendet werden, um Berechnungen an Daten auszuführen, die verschlüsselt und verteilt in der Cloud gespeichert sind, ohne dass der Cloud-Besitzer Zugang zu entschlüsselten Daten oder Berechnungsresultaten erhält.

HOMOMORPIC ENCRYPTION (engl.)
Übsg. Homomorphe Verschlüsselung

HONEYPOT (engl.)
Übsg. Honigtopf

HONIGTOPF
1) Datei mit interessant klingendem Namen, die Hacker anlocken soll. Greifen Hacker dann auf diese Datei zu, kann im besten Fall die Kontrolle über den Computer des Hackers erlangt werden. 2) Virtuelle Nachbildung eines realen Netzwerks, bspw. einer Industrieanlage, eines Wasserwerks oder eines Kraftwerks. Bei einem Angriff eines Hackers gegen das vermeintliche Netzwerk kann der Angreifer beobachtet und zurückverfolgt werden.

HORIZONTAL SCALING (engl.)
Syn. zu Scaling Out. Übsg. Horizontale Skalierung. Methoden zur Steigerung der Gesamtleistung durch Hinzufügen von zusätzlichen Systemen.

HOST
1) Ursprünglich ein zentraler Großrechner. Seit dem massiven Aufkommen der Arbeitsplatz-PCs bieten HOSTs v. a. Dienste und Rechenzeit für schwächere Systeme im Netzwerk an. 2) Syn. zu System, Computer.

HOSTING (engl.)
Bereitstellung von Infrastruktur, Software und Dienste, um Internetdomains und Internetseiten speichern und online anbieten zu können.

HOST INTRUSION DETECTION SYSTEM [HIDS] (engl.)
Übsg. Angrifferkennungssystem. Software oder Hardware in einem Netzwerk oder auf einem Computer, um Angriffe zu erkennen, damit diese entweder verhindert, gestoppt oder zumindest in einem Log registriert werden.

HOSTNAME
Eindeutige Kennung eines Computers in einem Netzwerk. Die Verbindung zw. Hostname und IP-Adresse geschieht über DNS. Der Hostname kann meist willkürlich gewählt werden, bspw. „MeinPC“, häufig wird jedoch der „Fully Qualified Domain Name“ (FQDN) als Hostname gesetzt, welcher zusammengesetzt wird als „Lokalteil“. „Domain“.„Top-Level-Domain“.

Beispiel: mail.exampledomain.com.

HOST SECURITY (engl.)
Übsg. Gerätesicherheit. Maßnahmen, um die Sicherheit von Geräten in einem Netzwerk zu erhöhen, bspw. durch Hinzufügen von Firewalls, Installation von Anti-Viren-Programmen u. Ä.

HOT WALLET (engl.)
Übsg. Heißes Portemonnaie. Kryptowährungsadresse, die regelmäßig benutzt wird, so, wie man Geld in einem Portemonnaie bei sich trägt und häufig benutzt.

HPKP
Abk. für HTTP Public Key Pinning

HPU
Abk. für Highly Privileged User

HSM
Abk. für Hardware Security Module, Übsg. Hardwaresicherheitsmodul.

HSM BASED CERTIFICATE (engl.)
Übsg. HSM-basiertes Zertifikat. Zertifikat, welches auf einem HSM erstellt und gespeichert wird.

HSTS
Abk. für HTTP Strict Transport Security

HTML
Abk. für Hypertext Markup Language. Grundlegende Programmiersprache für Internetseiten, welche auf Webbrowsern dargestellt werden. HTML erlaubt u. a. die Darstellung

von Text, von Grafik- und von Audioobjekten sowie das Definieren des Layouts und die Verlinkung zu anderen Internetseiten. Aktuelle Version ist HTML5.

HTTP
Abk. für Hypertext Transfer Protocol. Ab Anfang der 1990er-Jahre benutzte Strukturbeschreibung und Software zur Kommunikation im Internet. Bei diesem Protokoll werden Nachrichten zwischen Client und Server verschickt, welche aus Metadaten („HTTP-Header“) und eigentlichen Daten („HTTP-Body“) bestehen. Der Client schickt dafür eine HTTP-GET- oder HTTP-POST-Anfrage („Request“) an den Webserver, welcher eine Antwort („Response“) in Form einer Internetseite zurückschickt. Im Unterschied zu HTTPS, wird bei HTTP der Datentransport ohne Verschlüsselung vorgenommen. Dadurch werden Daten im Klartext und damit für alle mit Zugriff darauf lesbar übertragen, vergleichbar mit Postkarten, die der Briefträger auch lesen könnte. Mit Einführung der EU GDPR am 25. Mai 2018 wird die Verwendung von HTTP für die Übertragung von Formular- und anderen Daten noch toleriert, aber HTTPS erwartet. Eine HTTP-Verbindung erkennt man im Webbrowser an der URL, welche entweder mit „http://www“, nur mit „www“ oder direkt mit dem Domainnamen beginnt, und bei modernen Webbrowsern außerdem an einem fehlenden oder durchgestrichenen Schlüssel- oder Schlösschensymbol neben der Internetadresszeile. Außerdem wird bei vielen modernen Webbrowsern ein kleines „Info“-Symbol in Form eines von einem Kreis umrandeten „i“ dargestellt, um dem interessierten Benutzer mehr über die Sicherheit und Unsicherheit der angezeigten Internetseite anzuzeigen. Der Standard-Port für HTTP-Verbindungen ist 80.

HTTP-DELETE
Standardisierte Anfrageart innerhalb der Internetkommunikation zwischen Internetbrowser und Webseitenserver, bei welcher der Server aufgefordert wird, bestehende Dateien zu löschen.

HTTP-GET
Standardisierte Anfrageart innerhalb der Internetkommunikation zwischen Internetbrowser und Webseitenserver, bei welcher dynamische Werte übergeben werden können. Dabei wird die Webseiten-URL ergänzt mit einem Fragezeichen „?“ und anschließender Parameterlisten in Form von „Parameter-Name“ & „Parameter-Wert“. Allfällige Sonderzeichen werden mit „%“ angegeben sowie Leerzeichen mit „+“.

Beispiel: http://www.UnsereFamilie.com/Ferien1990?Tag=Montag&Ort=Zentrum+von+Rom

Neben den Vorteilen der einfachen Parameterübergabe und des einfachen Kopierens der ganzen URL bestehen auch Risiken, denn sensible Daten könnten ungeschützt in der URL sichtbar sein und schlecht programmierte Internetseiten nehmen jedes Parameterpaar ohne Überprüfung an und öffnen Hackern damit eine Möglichkeit, gefährliche Codezeilen einzuspeisen (siehe auch SQL-Injection).

HTTP-POST
Standardisierte Anfrageart innerhalb der Internetkommunikation zwischen Internetbrowser und Webseitenserver, bei welcher dynamische Werte übergeben werden können. Dabei werden die Parameter versteckt im HTTP-Nachrichtenbody übertragen. Diese Parameter stammen meist aus Benutzereingaben innerhalb eines sichtbaren Formulars oder sind vordefinierte Werte in einem für den Benutzer nicht sichtbaren Formular. HTTP-POST wird auch benutzt, um Uploads von Bildern u. Ä. auf dem Server zu speichern. Da die Daten und Parameter im Unterschied zu HTTP-GET nicht in der URL stehen, reicht ein simples Kopieren der URL für zukünftige gleiche Internetseitenaufrufe nicht aus. Der Vorteil von HTTP-POST liegt darin, dass sensible Daten in der URL nicht sichtbar und bei einem HTTPS-Aufruf zusätzlich verschlüsselt sind.

Beispiel

Beispiel eines HTTP-POST-Headers mit 4 Zeilen gefolgt von einer Zeile HTTP-Body mit sensiblen Daten, die jedoch für Benutzer nicht sichtbar wären, da sie üblicherweise in Variablen gespeichert sind:

```
POST /path/script.php HTTP/1.0
Host: localhost
Content-Type: multipart/form-data
Content-Length: 38
username=benutzer1&pass=pwd_ben1_ABYZ
```

HTTP PUBLIC KEY PINNING [HPKP] (engl.)
Syn. zu Certificate Pinning. Methode, die charakteristische IDs (sog. PINs) von signierten Zertifikaten benutzt, um die Zertifikate wiederzuerkennen und Man-in-the-Middle-Angriffe zu verhindern.

HTTP-PUT
Standardisierte Anfrageart innerhalb der Internetkommunikation zwischen Internetbrowser und Webseitenserver, bei welcher Daten übergeben werden, die vom Server abgespeichert werden sollen. Dies wird meist bei Uploads benutzt, um vorherige Daten auf dem Server zu überschreiben. Dabei werden die Daten wie bei HTTP-POST versteckt im HTTP-Nachrichtenbody übertragen.

HTTPS
Abk. für Hypertext Transfer Protocol Secure. Strukturbeschreibung und Software zur Kommunikation im Internet. HTTPS wurde 1994 von Netscape entwickelt und basiert auf HTTP mit TCP. Die Verschlüsselung geschieht dabei mittels SSL/TLS. Bei HTTPS werden, wie bei HTTP, Nachrichten zwischen Client und Server verschickt, welche

grundsätzlich aus Metadaten („HTTP-Header“) und eigentlichen Daten („HTTP-Body“) bestehen. Der Client schickt eine HTTP-GET- oder HTTP-POST-Anfrage („Request“) an den Webserver, welcher eine Antwort („Response“) in Form einer Internetseite zurückschickt. Bei Internetseiten, welche Formulardaten oder andere sensible Daten übertragen, oder auch bei Verwendung von offenen, passwortfreien, also unsicheren WLANs, kann HTTPS die übertragenen Daten bei der Kommunikation verschlüsseln. Eine HTTPS-Verbindung erkennt man im Internetbrowser an der URL, welche mit „https://“ beginnt, und bei modernen Browsern außerdem an einem weißen oder grünen Schlüssel- oder Schlösschensymbol in der Internetadresszeile. Die Details der HTTPS-Kommunikation werden im ausführlicheren Spezialthema „Der Aufruf einer HTTPS-Internetseite“ in Kap. 29 erklärt. Der Standard-Port für HTTPS-Verbindungen ist 443.

HTTP STATUS CODE
Antwort vom Webserver an einen Client, bspw. einem Internetbrowser, der angibt, ob die Anfrage erfolgreich war oder ein Fehler auftrat (siehe Liste der HTTP Status Codes im Anhang Kap. 33).

HTTP STRICT TRANSPORT SECURITY [HSTS] (engl.)
Webserver-Einstellung, die die Webbrowser auffordert, immer verschlüsselte Verbindungen für diese Domain einzusetzen.

HUMAN ERRORS (engl.)
Übsg. Menschliche Fehler. Solche Fehler sind häufig Ursache für Datenverlust und für angreifbare Systeme. Sie geschehen unabsichtlich, bedeuten jedoch für Firmen und Privatpersonen ein großes Risiko, da sie, wenn überhaupt, erst nach einer gewissen Dauer erkannt werden. Beispiele solcher Fehler sind die zeitweise Abschaltung von TLS zwischen Client- und Server-Applikationen oder das unverschlüsselte Hochladen von Passwortlisten in die Cloud.

HVE
Abk. für Hidden Vector Encryption

HYBRID CLOUD (engl.)
Gleichzeitige Benutzung von Servern innerhalb einer Firma („On-Prem“) und Servern in einer Cloud. Gründe für die Weiterbenutzung eigener Server „On-Prem“ können Sicherheitsbedenken sein, sodass die wertvollsten Daten oder die wichtigsten Verschlüsselungsschlüssel darauf, anstatt in der Cloud gespeichert werden.

HYBRIDE BEDROHUNG
Kombination verschiedenartiger Angriffe. Bspw. physischer Militäreinsatz, unterstützt durch Cyber-Angriffe gegen den Gegner.

HYBRIDE VERSCHLÜSSELUNG
Kombination aus symmetrischer und asymmetrischer Verschlüsselung mit dem Ziel, das Schlüsseltauschproblem zu lösen. Dabei wird erst ein symm. Schlüssel (Session-Key) erstellt. Danach wird der Session-Key mit dem öffentlichen Schlüssel des Empfängers asymm. verschlüsselt und kann nun für Datenverschlüsselung benutzt werden.

HYBRID EXCHANGE (engl.)
Kombination von firmeninternen Exchange Servern („On-Prem“) und Exchange Online von Office 365 („on-cloud“). Für den Benutzer erscheint diese Kombination als ein System („hybrid“).

HYOK
Abk. für Hold Your Own Key

HYPERLINK
Syn. zu Link

HYPERTEXT MARKUP LANGUAGE [HTML] (engl.)
Programmiersprache, welche für Internetseiten benutzt wird und hauptsächlich das Erscheinungsbild, d. h. das Layout, und den Text der Internetseite definiert. Diese Programmiersprache wurde Anfang der 1990er-Jahren erfunden und wird seither weiterentwickelt. Die aktuell offizielle Version ist HTML5. Eine der ersten und noch immer wichtigste Funktion innerhalb HTML sind Verweise (engl. Links) zu anderen Internetseiten. HTML lässt sich durch eingebundene und hinzugeladene Programmiersprachen und Tools erweitern, so z. B. durch JavaScript und Java-Applets innerhalb des Internetbrowsers oder auch durch PHP-Programme auf dem Webserver.

HYPERTEXT TRANSFER PROTOCOL [HTTP] (engl.)
Siehe HTTP und HTTPS

I

11

IAAS
Abk. für Infrastructure As a Service

IAC
Abk. für Infrastructure As Code

IAM
Abk. für Identity and Access Management

IAST
Abk. für Interactive Application Security Testing

ICANN
Abk. für Internet Corporation for Assigned Names and Numbers

ICEID
Schadsoftware in Form eines Trojaners, der ursprünglich gegen Banken betrieben wurde, danach aber auch gegen Einzelhändler.

ICQ
Sofortnachrichtendienst. Der Name entstand aus dem Text „I seek you“, Übsg. „Ich suche dich“.

ICS
Abk. für Industrial Control Systems

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_11

ICT
Abk. für Information and Communications Technology. Übsg. Informations- und Kommunikationstechnik.

ID
Abk. für Identifikation

IDENTIFICATION OF CYBER THREATS (engl.)
Übsg. Identifizierung von Cyber-Bedrohungen

IDENTIFIKATION [ID]
1) Verfahren, um eine Person oder ein Objekt anhand von Merkmalen eindeutig zu bestimmen. 2) Eindeutige Bezeichnung, Nummer oder Name, welche einen Benutzer innerhalb eines Systems oder eines Netzwerks von Systemen identifiziert. Diese ID wird verwendet, um dem Benutzer Zugangs- und Benutzungsrechte an Software, Applikationen, Systemen oder anderen Ressourcen zu erteilen. Zur Authentifizierung eines Benutzers an einem System wird meist neben der ID noch ein Passwort benötigt. Aufgrund der eindeutigen ID können auch Aktivitäten von Benutzern gezielt verfolgt werden („Profiling"). 3) Eindeutige Kennzeichnung für Ressourcen, wie PC, Monitor oder Docking-Station innerhalb von Netzwerken. Ein Ressourcen-Repository wird verwendet, um wichtige Eigenschaften jeder Ressource zu speichern.

IDENTIFIKATIONSPROTOKOLL
Methode zur Authentifizierung von E-Mail-Sende-Servern für die Verhinderung von Man-in-the-Middle-Attacken beim E-Mail-Versand. Dabei wird der öffentliche Serverschlüssel in der DNS der Domain gespeichert und eine digitale Signatur der zu sendenden E-Mail mithilfe des privaten Serverschlüssels erstellt, um diese im Header der E-Mail mitzuschicken. Diese Signatur kann beim Empfänger mithilfe des öffentlichen Serverschlüssels entschlüsselt und zur Validierung der Integrität und Herkunft der E-Mail verwendet werden. Ein Bsp. eines solchen Protokolls ist DomainKey Identified Mail (DKIM).

IDENTIFIZIERUNG VON CYBER-BEDROHUNG
Phase bei der Behandlung von Cyber-Bedrohungen.

IDENTITÄT
Eigenschaften einer Person oder eines Objekts, die in der Gesamtheit das Individuum eindeutig beschreiben. Im Internet reichen meist ein Benutzername und ein Passwort, um die digitale Identität zu definieren und einem Online-Account zuzuschreiben. Kommen jedoch Benutzername und Passwort in fremde Hände, kann die digitale Identität missbraucht werden.

IDENTITÄTSDETAILS
Eigenschaften einer physischen oder digitalen Identität. Beispiele sind Name, Alter, Geburtsdatum und Passwort.

IDENTITÄTSDIEBSTAHL
Aktion eines Diebes oder Hackers mit dem Ziel, die physische oder digitale Identität eines anderen anzunehmen und sich als diesen auszugeben. Dadurch ergaunert sich der Dieb die Rechte der bestohlenen Person oder des bestohlenen Benutzers und erhält damit Zugang zu sensiblen Daten, E-Mails, E-Banking-Kontos u. Ä. Häufig bemerken die bestohlenen Personen und Benutzer den Diebstahl erst, nachdem bereits Missbrauch mit ihrer Identität begangen wurde. Wenn Systeme oder IT-Admins einen Identitätsdiebstahl verdächtigen, sperren sie den Zugang, die Kreditkarte u. Ä. und es kostet den Bestohlenen viel Aufwand, seine Identität und damit seine Rechte wieder vollständig herzustellen. Je mehr Identitätsdaten über eine Person veröffentlicht werden und online sichtbar oder auffindbar sind, desto leichter kann die Identität missbraucht werden.

IDENTITÄTSVERLUST
Ereignis, bei welchem der Benutzername und das Passwort, oder andere identitätsbeschreibende Eigenschaften einer Person in falsche Hände geraten und die digitale Identität missbraucht wird.

IDENTITY AND ACCESS MANAGEMENT [IAM] (engl.)
Übsg. Identitäts- und Zugangsmanagement. Methoden, Prozesse, Maßnahmen und Programme, um digitale Identitäten zu verwalten und zugehörige Berechtigungen zu vergeben und zu gewährleisten.

IDENTITY BROKER (engl.)
Dienstleistungsfirma oder Dienstleistungssoftware, welche die Zugangsberechtigungen zwischen mehreren Identitätsdienstleistern ermöglicht.

IDENTITY LEAK (engl.)
Übsg. Abhandengekommene, gestohlene oder unrechtmäßig veröffentlichte Identitätsdaten.

IDENTITY LIFE-CYCLE MANAGEMENT [ILM] (engl.)
Übsg. Management des Identitätslebenszyklus. Erstellung, Bearbeitung und Benutzung von Identitäten, zur Verwendung in Netzwerken und Systemen, inkl. der Möglichkeit zur Anonymität.

IDENTITY PROOFING (engl.)
Übsg. Bestätigung der Identität einer Person durch Überprüfung offizieller Dokumente oder ähnlich vertraulicher Daten.

IDENTITY PROOFING PROCESS (engl.)
Übsg. Verfahren, um die Identität einer Person zu überprüfen und bestätigen, bevor ein Konto für diese Person erstellt wird, oder dieser Person Zugangsrechte vergeben werden.

IDENTITY PROVIDER (engl.)
Übsg. Identitätsdienstleister. Dieser agiert bspw. zw. einer Firma und einer externen Cloud und vermittelt Identitäts- und Zugangsmanagement (IAM) zw. beiden Parteien.

IDENTITY THEFT (engl.)
Übsg. Identitätsdiebstahl

IDENTITY TOKEN (engl.)
Übsg. Identitätsmerkmal. Physisches, elektronisches oder geistiges Merkmal, welches als Identität einer Person verwendet werden kann.

IDK
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „I don't know", Übsg. „Ich weiß nicht".

IDLE SESSION (engl.)
Übsg. Unbenutzte Sitzung

IDN
Abk. für Internationalized Domain Name. Domain-Namen mit Sonderzeichen, wie Umlaute.

IDNA
Abk. für Internationalizing Domain Names in Applications. 2003 definierte Methoden zur Verarbeitung von Nicht-ASCII-Zeichen in Domain-Namen. IDNA-fähige Software kann einen Domain-Namen mit Nicht-ASCII-Zeichen in die entsprechende ASCII-Repräsentation des Domain-Namens umwandeln. Siehe auch Punycode.

IDS
Abk. für Intrusion Detection Systems

IEC
Abk. für International Electrotechnical Commission.

IEEE
Abk. für Institute of Electrical and Electronics Engineers

IEEE 802.11
Norm für Kommunikation in Funknetzwerken. Syn. zu Wireless-LAN, WLAN, Wi-Fi. Es wurden mehrere Versionen definiert (siehe Tab. 11.1).

IE ESC
Abk. für Internet Explorer Enhanced Security Configuration

IIS
Abk. für Internet Information Services

IKE
Abk. für Internet Key Exchange

IKT
Abk. für Informations- und Telekommunikationstechnik

Tab. 11.1 Spezifikationen und Vergleich der Wi-Fi-Typen

Bezeichnung	Technische Bezeichnung	Maximale Geschwindigkeiten (Mbit/s)	Kanalbreite (MHz)	Frequenz (GHz)
Wi-Fi1	802.11	2	22	2.4
–	802.11a	13	5/10	5
–	802.11a	27	20	5
Wi-Fi2	802.11b	11	22	2.4
Wi-Fi3	802.11g	13	5 und 10	2.4
	802.11g	27	20	2.4
Wi-Fi4	802.11n	72	20	2.4
	802.11n	150	40	5
	802.11n	600	20 (Kombination von Antennen)	
–	802.11p	13	5 und 10	5.9
–	802.11p	27	20	5.9
Wi-Fi5	802.11ac	347	20	5
	802.11ac	800	40	5
	802.11ac	1733	80	5
	802.11ac	3466	160	5
–	802.11ad	6700		4 x 60
–	802.11ah	9		0.9
Wi-Fi6	802.11ax	9600	20–160	2.4 und 5

Quelle: https://www.wi-fi.org *(Abgerufen am 22.12.2019)*

IKT-INFRASTRUKTUR
Abk. für Informations- und Telekommunikationstechnik-Infrastruktur. Alle Computer, Netzwerke, Firewalls, Rechenzentren, Handys etc., die innerhalb der Firma oder eines Industriebetriebs benutzt werden.

IKT-STRATEGIE
Abk. für Informations- und Telekommunikationstechnik-Strategie

ILM
Abk. für Identity Life-Cycle Management

ILOVEYOU
Schadsoftware in Form eines Trojaner-Virus, welcher im Jahr 2000 Mio. von Windows-PCs weltweit über E-Mails infizierte, Dateien überschrieb und sich dadurch selber vervielfältigte.

IMAGE (engl.)
Übsg. Abbild. Harddisks, Verzeichnisse oder ganze Systeme können gesamthaft als ein Image (d. h. als eine Datei) abgebildet und gespeichert werden. Dieses Abbild kann mit geeigneter Software jederzeit wie das ursprüngliche Original benutzt, kopiert und geklont werden.

IMAGETRAGICK
Schwachstelle im Programm ImageMagick, durch welche ein RCE-Angriff („Remote Command Execution“) möglich war.

IMAP
Abk. für Internet Message Access Protocol

IMAPS
Abk. für Internet Message Access Protocol Secure. TLS-verschlüsselte Variante von IMAP.

IMEI
Abk. für International Mobile Station Equipment Identity.

IMHO
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „In my Humble Opinion“, Übsg. „Meiner unbedeutenden Meinung nach“.

IMPERSONIEREN
Methode, um die Rechte eines anderen Benutzers anzunehmen.

IMSI
Abk. für International Mobile Subscriber Identity

IMSI CATCHER
Gerät, welches vorgibt, ein Sendemast zu sein und dadurch ein Man-in-the-Middle-Angriff auf Verbindungen zwischen Handys und echten Sendemasten ermöglicht.

INCIDENT (engl.)
Übsg. Vorfall im Bereich der Cyber- und IT-Sicherheit, bspw. eine DDoS-Attacke. Allg. ist ein Incident ein Ereignis, welcher zu Verlusten, zu Unerreichbarkeit von Systemen oder zur Beeinträchtigung des Betriebs führt.

INCIDENT FORENSICS (engl.)
Übsg. Vorfallsanalyse. Methoden zur Analyse eines Cyber- und IT-Sicherheitsvorfalls.

INCIDENT MANAGEMENT (engl.)
Übsg. Vorfallsmanagement. Methoden und Prozesse zur Verhinderung von und Reaktion auf Cyber- und IT-Sicherheitsvorfälle.

INCIDENT RECOVERY (engl.)
Prozess- und Methodenbeschreibungen sowie eigentliche Durchführung von Maßnahmen, um bei einem Incident, bspw. einem DDoS-Angriff, diesen zu beheben und volle Funktionsfähigkeit der Systeme wiederherzustellen.

INCIDENT RESPONSE (engl.)
Übsg. Vorfallsreaktion. Tätigkeiten, die in einer Firma unternommen werden als Folge eines Cyber- und IT-Security-Vorfalls, mit dem Ziel, die negativen Folgen zu minimieren und zukünftige Vorfälle zu verhindern.

INCOGNITO BROWSER
Privater Modus eines Internetbrowsers. Dabei werden keine Cookies und kein Verlauf gespeichert. Downloads hingegen bleiben auf dem System bestehen. Auch kann der Benutzer anhand seiner IP-Adresse oder anderer Daten identifiziert werden und ist somit nicht „inkognito“ im Internet.

INDICATORS OF COMPROMISE [IOCS] (engl.)
Übsg. Merkmale von Attacken und Schadsoftware. Solche Merkmale befinden sich in einem Netzwerk oder in einem System während oder nach einer Attacke und können bspw. Dateien sein, die eindeutige Hinweise auf die Verursacher oder die Schadsoftware darstellen. Anti-Viren-Programme werden laufend erweitert, um neuere solcher Merkmale zu erkennen.

INDUSTRIAL CONTROL SYSTEMS [ICS] (engl.)
Übsg. Industrielle Kontrollsysteme

INDUSTRIELLE KONTROLLSYSTEME
Systeme zur Kontrolle und Steuerung von Großanlagen wie AKWs.

INDUSTROYER
Schadsoftware gegen industrielle Kontrollsysteme, speziell in Hochspannungsanlagen.

INFECTION (engl.)
Übsg. Infektion

INFEKTION
Am gleichnamigen, medizinischen Vorgang angelehnter Begriff, der beschreibt, dass Schadsoftware, wie (digitale) Viren in ein elektronisches Gerät, z. B. PC, Handy, Smart-TV, Webcam u. Ä. hineingelangt. Diese Schadsoftware kann daraufhin bspw. Webcambilder an Diebe schicken, Gespräche aufzeichnen oder den infizierten Rauchmelder für DDoS-Attacken missbrauchen.

INFINEON TPM VULNERABILITY (engl.)
Sicherheitslücke in einer veralteten TPM-Firmware, bei welcher der implementierte Algorithmus, der zur Erstellung von RSA-Schlüssel benutzt wurde, anfällig ist.

INFORMATION
Durch intelligente Zusammenführung von Daten entstandenes Wissen. Häufig ungenau als Syn. zu Daten verwendet.

INFORMATION BUBBLE (engl.)
Übsg. Informationsblase. Durch das Sammeln und Analysieren von Likes, besuchten Internetseiten und Videos versuchen Algorithmen in einigen Programmen zu bestimmen, welche Themen für den Benutzer wichtig sind. Die Gefahr dabei ist, dass dies zu einseitiger Information führen kann und dadurch für den Benutzer die Meinung einer Gruppe mehr Gewicht erhält, als objektiv angebracht wäre.

INFORMATION CORRUPTION (engl.)
Übsg. Informationsverfälschung

INFORMATION LIFE-CYCLE (engl.)
Übsg. Informationslebenszyklus

INFORMATION OWNER (engl.)
Übsg. Informationsbesitzer

INFORMATION PROTECTION (engl.)
Übsg. Schutz von Informationen

INFORMATION RIGHTS MANAGEMENT [IRM] (engl.)
Übsg. Informationsrechteverwaltung. Microsoft-Office-Implementation von Microsofts ADRMS (lokale Version) und AzureRMS (cloudbasiert).

INFORMATIONSBESITZER
Person oder Gruppe von Personen, die für bestimmte Informationen zuständig sind und Kriterien für Erstellung, Sammlung, Verarbeitung, Verbreitung und Entsorgung dieser Informationen festlegen.

INFORMATION SECURITY (engl.)
Übsg. Informationssicherheit

INFORMATIONSLEBENSZYKLUS
Überbegriff für die Erzeugung, die Bearbeitung, den Transport, die Speicherung, die Archivierung, die Beseitigung und die Vernichtung von Informationen.

INFORMATION SOCIETY (engl.)
Übsg. Informationsgesellschaft

INFORMATIONSSICHERHEIT
Themenkreis, der sich mit dem Schutz von Daten vor unberechtigtem Zugriff, mit den Zugriffskontrollen und mit der Privatsphäre in Computersystemen beschäftigt. Syn. zu Sicherheit in der Informationstechnik.

INFORMATIONSVERFÄLSCHUNG
Absichtliche oder unabsichtliche Änderung von Informationen.

INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY [ITIL] (engl.)
Beschreibung von Erfolgsrezepten im Bereich IT-Service-Management mit dem Ziel einer messbaren Verbesserung des aktuellen Zustands der IT-Infrastruktur, die typischerweise in mittleren und großen Unternehmen vorkommen. Diese Beschreibungen beinhalten Vorschläge für optimale Prozesse, Funktionen und Rollen, welche im Lebenszyklus von IT-Services vorkommen.

INFORMATION THEORETIC SECURITY (engl.)
Übsg. Informationstheoretische Sicherheit. System, welches nicht gebrochen werden kann, auch wenn genug Zeit und Computerleistung vorhanden ist.

INFOSTEALER (engl.)
Übsg. Informationsdieb. Schadsoftware, welche Login-Informationen oder sensible private Daten stiehlt und an einen vordefinierten Ort schickt.

INFRASTRUCTURE AS A SERVICE [IAAS] (engl.)
Übsg. Infrastruktur, welche als Dienstleistung angeboten wird. Vorwiegend im Zusammenhang mit virtuellen PCs (VMs) benutzt, welche einfach bereitgestellt und verwaltet werden können.

INFRASTRUCTURE AS CODE [IAC] (engl.)
Übsg. Programmierte Infrastruktur. Konfiguration und Administration von physischen und v. a. virtuellen Computern mittels Programmen und Skripten.

INHERITANCE (engl.)
1) Übsg. Vererbung von Dateneigenschaften. Bspw. gibt es Software, mit welcher beim Kopieren von Teilen einer klassifizierten Datei in eine andere hinein die Klassifizierung mitvererbt wird. 2) Übsg. Vererbung von Objekteigenschaften bei objektorientierter Programmierung.

INITIALIZATION VECTOR [IV] (engl.)
Übsg. Initialisierungswert. Zufälliger oder berechneter Anfangswert bei Verschlüsselungsmethoden, bspw. bei Blockchiffre-Methoden. Der Anfangswert sorgt dafür, dass die Verschlüsselung gleicher Texte nicht gleiche Resultate erzeugt.

Beispiel: Bei SSL 2.0 wurde der letzte Geheimtextblock als neuer Initialization Vector für die nächste zu verschlüsselnde Nachricht verwendet, was jedoch unsicher war.

INNER SOURCE (engl.)
Übsg. Firmeninterner Open-Source

INSIDER DATA THEFT (engl.)
Übsg. Datendiebstahl durch Insider. Heutzutage eine der größten Risiken und häufigsten Diebstahlarten bei Firmen. Durch Insiderwissen oder -zugang gelangen Mitarbeiter an Daten, die aus der Firma gebracht und verkauft oder veröffentlicht werden.

INSIDER SABOTAGE (engl.)
Übsg. Absichtliche Manipulation von Daten, Geräten oder Infrastruktur durch Mitarbeiter, welche Insiderwissen und oder -zugang besitzen.

INSTAGRAM
Online-Dienst zum Teilen von Fotos und Videos.

INSTANT MESSAGING [IM] (engl.)
Übsg. Sofortnachrichten. Mithilfe von Apps können Personen ohne Zeitverzögerung miteinander kommunizieren. Beispiele sind SMS, Twitter, ICQ, WhatsApp, Skype.

INSTANZIIERUNG
1) Erzeugung eines Objekts als Instanz einer vordefinierten Klasse in objektorientierter Programmierung. Dabei wird ein entsprechender Speicherbedarf für die Instanz angelegt sowie Attribute und Initialwerte belegt. 2) Bereitstellung einer Applikation auf einem System. 3) Bereitstellung eines Systems.

INTEGRATED WINDOWS AUTHENTICATION [IWA] (engl.)
Methode auf Windows-Systemen, um den angemeldeten Benutzer ohne erneute Passwortabfrage in Webbrowsern und anderen Apps zu authentisieren. Dies wird dadurch erreicht, dass der Benutzer sich am Windows-System und damit am Domain-Server und Active Directory authentisiert und anmeldet. Ein ebenfalls in der gleichen Domäne eingesetzter Webserver („IIS“) kann anschließend mittels dieser erfolgten Anmeldung des Benutzers automatisch authentisierte Verbindungen zum Webbrowser oder zu Apps herstellen.

INTEGRITÄT
Unversehrtheit von Daten, d. h. die Daten sind vollständig und in der richtigen Reihenfolge. Dies ist eines der Ziele der IT-Sicherheit, welche sich grundsätzlich mit der Aufrechterhaltung der Integrität, der Vertraulichkeit und der Verfügbarkeit von Daten und Systemen beschäftigt. Oft wird dies abgekürzt mit CIA für Confidentiality, Integrity and Availability.

INTEGRITY (engl.)
Übsg. Integrität. Syn. zu Datenintegrität.

INTELLECTUAL PROPERTY THEFT (engl.)
Übsg. Diebstahl geistigen Eigentums

INTEL TXT FEATURE (engl.)
Abk. für Intel Trusted Execution Technology Feature. Eine hardwarebasierte Sicherheitseinstellung, mit deren Hilfe eine Vertrauenskette gebildet wird, um damit Informationen vor softwarebasierten Angriffen zu schützen.

INTERACTIVE APPLICATION SECURITY TESTING [IAST] (engl.)
Überprüfung einer laufenden Applikation zur Entdeckung und Behebung von Sicherheitsschwachstellen. Im Vergleich zu statischen Sicherheitsüberprüfungen von Programmzeilen (Static Code Analysis) wird bei IAST die Applikation ausgeführt, bspw. während

funktionale Tests durchgeführt werden. Dabei arbeitet IAST im Unterschied zu Dynamic Application Security Testing innerhalb der zu überprüfenden Applikation.

INTERAKTIVE TASTATURAUTHENTIFIZIERUNG
Authentifizierungsmethode, bei welcher der Benutzer seinen Benutzernamen und sein Passwort über eine eingeblendete Tastatur eintippt.

INTERCEPTORS (engl.)
Übsg. Abfänger. Personen oder Systeme, welche zw. zwei Parteien stehen, bspw. zw. PCs, Netzwerken, Telefonen etc., und die übermittelten Nachrichten oder Daten abfangen, um diese zu lesen, zu verändern oder zu missbrauchen.

INTERMEDIATE CA CERTIFICATE (engl.)
Übsg. Public-Key-Zertifikat einer Zwischenzertifizierungsstelle. Dieses Zertifikat wird von der Hauptzertifizierungsstelle (Root-CA) ausgestellt und wird dadurch vertrauenswürdig. Durch die Vertrauenskette von der Root-CA zur Zwischenzertifizierungsstelle kann diese Zwischenzertifizierungsstelle selber weitere vertrauenswürdige Zertifikate ausstellen und damit weitere Zwischenzertifizierungsstellen zertifizieren.

INTERMEDIATE CERTIFICATE (engl.)
Syn. zu Subordinated Certificate, untergeordnetes Zertifikat.

INTERNAL FRAUD (engl.)
Übsg. Interner Betrug

INTERNATIONAL ELECTROTECHNICAL COMMISSION [IEC] (engl.)
Internationale Organisation zur Definition von Normen im Bereich der Elektrotechnik und Elektronik.

INTERNATIONAL MOBILE STATION EQUIPMENT IDENTITY [IMEI] (engl.)
Übsg. Internationale Mobilfunkgerätekennung. Die IMEI-Nummer ist eine eindeutige Kennung eines Mobilfunkgeräts.

INTERNATIONAL MOBILE SUBSCRIBER IDENTITY [IMSI] (engl.)
Übsg. Internationale Mobilfunkteilnehmerkennung. Die IMSI-Nummer ist eine eindeutige Kennung eines Mobilfunkteilnehmers, genauer der SIM-Karte des Teilnehmers.

INTERNET
Syn. zu WWW, World Wide Web, Cyberspace. Gesamtheit aller Computer und Geräte, welche über das standardisierte Internet-Protokoll kommunizieren und Daten austauschen können. Aus dem in den 1970er- und 1980er-Jahren unter Universitäten betriebenem ARPANET entstandenes und ab ca. 1990 öffentliches Netzwerk, welches

zunehmende Popularität erlangte, als grafikfähige Webbrowser (NCSA Mosaic, Netscape und weitere) zur Verfügung standen.

INTERNETADRESSE
Syn. zu URL, WebURL.

INTERNETBROWSER (engl.)
Syn. zu Webbrowser. Programm, um Internetseiten darzustellen.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS [ICANN] (engl.)
Organisation, welche die einmaligen Namen und Adressen von Internet-Domains vergibt.

INTERNETDATENVERKEHR
1) Syn. zu Daten, die über das Internet gesendet werden. 2) Abk. für das Gesamtvolumen der total übertragenen Daten.

INTERNET DER DINGE
Syn. zu Internet of Things (IOT). Gesamtheit aller internetfähigen Geräte, wie Computer, Glühbirnen, Kühlschränke, Autos und viele andere.

INTERNET EXPLORER ENHANCED SECURITY CONFIGURATION [IE ESC] (engl.)
Sicherheitsmechanismus im Microsoft Internet Explorer Webbrowser auf Windows-Server 2003, um Aufrufe schädlicher Internetseiten zu verhindern.

INTERNET HIJACKER (engl.)
Übsg. Missbraucher des Internets. Bspw. können Hacker IP-Adressen durch Manipulation des Border Gateway Protocol übernehmen und missbräuchlich verwenden.

INTERNET INFORMATION SERVICES [IIS] (engl.)
Webservice auf Windows-PCs und -Servern, welches Dienste für HTTP, für HTTPS, für FTP, für SMTP, für POP3 und weitere bereitstellt.

INTERNET KEY EXCHANGE [IKE] (engl.)
aÜbsg. Internetschlüsselaustausch. Protokoll zur Beschreibung des automatischen Schlüsselaustauschs bei IPsec-Verbindungen. Es basiert auf dem Diffie-Hellman-Schlüsselaustausch, um einen sicheren Austausch von Schlüsseln über ein unsicheres Rechnernetz zu ermöglichen. Nach der gegenseitigen Authentisierung beim Aufbau einer IPSec-Verbindung einigen sich beide Systeme mit IKE auf die zu verwendenden Schlüssel-Algorithmen.

INTERNET-KRIEG
Syn. zu Cyber-Krieg.

INTERNET-KRIMINALITÄT
Verbrechen, die hauptsächlich im oder mittels des Internets ausgeführt werden. Beispiele sind DDoS-Attacken, Cryptocurrency-Attacken oder auch illegale Musikuploads.

INTERNET MESSAGE ACCESS PROTOCOL [IMAP] (engl.)
Übsg. Internetnachricht Abrufprotokoll. Textbasiertes Verfahren aufbauend auf POP3, zum Abrufen, Auflisten, Ordnen und Speichern von E-Mails. Dabei bleiben im Vergleich zu POP3 die E-Mails und die Ordnerstruktur auf dem Server und können mit mehreren Clients abgerufen werden, bspw. mit Handy, PC und Tablet. Heutzutage kann und sollte der Transport des Benutzernamens und Passworts zum Server und die E-Mails vom Server zum Empfänger mit SSL/TLS verschlüsselt werden. Dies wird durch den Befehl STARTTLS vom Client an den Server auf Port 143 oder ohne Befehl durch implizites TLS via IMAPS auf Port 993 angestoßen.

INTERNET OF THINGS [IOT] (engl.)
Übsg. Internet der Dinge. Gesamtheit aller Geräte, Gebäude und digitaler Objekte, welche mit Elektronik, Sensoren, Software und Internetverbindung ausgestattet sind, um Daten zu sammeln und auszutauschen. Beispiele sind internetfähige Kühlschränke, die selber Milch nachbestellen oder auch vernetzte Rauchmelder, die andere Rauchmelder im Haus warnen, wenn in einer Wohnung ein Brand ausgebrochen ist. Auch Fahrzeuge werden vermehrt an IoT angeschlossen, was bei Bus, Zug, Tram usw. sinnvoll ist, um den Verkehr zu optimieren, aber bei privaten Autos auch Gefahren mit sich bringt, da diese dann durch Hacker angreifbar sind sowie ein Tracking und Profiling erstellt werden kann.

INTERNET PROTOCOL [IP] (engl.)
Übsg. Internet-Protokoll. Standardisiertes Verfahren zur Kommunikation zwischen Computern, welche IP-Adressen besitzen.

INTERNET PROTOCOL SECURITY [IPSEC] (engl.)
Methode, um Daten innerhalb des Computers umzuleiten, damit diese verschlüsselt werden können, bevor sie über sichere oder unsichere IP-basierte Rechnernetzen, bspw. über das Internet, kommuniziert werden. Die Kommunikation wird dabei über eigene IPSec-Ports der Systeme geleitet, sodass damit eine Art Tunnel zwischen den Systemen entsteht. Auch virtuelle private Netzwerke (VPN) werden damit möglich. IPSec kann derart konfiguriert werden, dass Systeme nur dann kommunizieren dürfen, wenn sich diese gegenseitig via Kerberos, Zertifikate, NTLM-Anmeldedaten oder vorher definierten Schlüssel („Preshared Key“) authentifiziert haben. Durch die

IPSEC-Möglichkeit zur Authentifikation und Verschlüsselung können auch Apps davon profitieren, die diese Funktionen nicht selber mitbringen.

INTERNETPROTOKOLL
Protokoll zur Kommunikation zw. Computern, welche IP-Adressen besitzen und damit eindeutig adressierbar sind. Seit ca. 1981 werden IP-Adressen in der IPv4-Variante des Internetprotokolls als 4 Bytes in der 4 x 3 Darstellung mit Werten zw. 0 und 255 definiert, bspw. 192.168.0.1. Seit 1998 werden Geräte zudem mit IPv6 adressiert, wobei die verwendeten 16 Bytes nicht in der langen 16 x 3 Darstellung mit Werten zw. 0 und 255 gebraucht werden, sondern als 16 x 2 Werte zw. 00 und FF in hexadezimaler Form und zusätzlich mit Abkürzungen zu einem Wert wie 1354:8d2a:12ab:234:5dbb::534:aab4 zusammengefasst werden.

INTERNET RELAY CHAT [IRC] (engl.)
Textbasiertes Chatsystem mit beliebiger Anzahl von Teilnehmern. Zur Teilnahme wird ein IRC-Client-Programm verwendet, bspw. ChatZilla, Instantbird, Opera etc., welches sich mit den Servern, dem sog. Relais, verbindet.

INTERNET SECURITY (engl.)
Übsg. Internetsicherheit

INTERNETSEITE
Dokument, welches von einem Datenträger geladen oder von einem Webserver angeboten und in einem Webbrowser dargestellt wird. Hauptmerkmal von Internetseiten war ursprünglich die Möglichkeit, diese untereinander zu verlinken. Neuere Internetseiten können dynamisch erstellt werden und bieten viele Layoutelemente. Auch komplette Apps können als dynamische Internetseiten betrieben werden, die lokal und eigenständig arbeiten oder bei Bedarf Daten über eine Serververbindung erhalten.

INTERNETSICHERHEIT
Teilgebiet der Cyber- und IT-Sicherheit. Ziel ist die Verhinderung von Angriffen, von Missbrauch und von Datenverlust über Webbrowser, Internetnetzwerke oder allg. über das Internet.

INTERPRETER
Software, welche einen Quellcode, der in einer Programmiersprache verfasst wurde, zur Laufzeit Zeile für Zeile in einen maschinenlesbaren Code umwandelt und diesen direkt ausführt. Dies erlaubt einerseits schnelles Prototyping von Ideen, andererseits auch die Erstellung kompletter Programme. Derart entwickelte Programme können zusätzlich von einem Compiler vollständig in ein maschinenlesbares Programm umgewandelt werden, sodass sie auch ohne Interpreter lauffähig sind.

INTRUDERS (engl.)
Übsg. Eindringling in ein System

INTRUSION (engl.)
Übsg. Einbruch in ein System

INTRUSION DETECTION SYSTEMS [IDS] (engl.)
Übsg. Einbruchserkennungssystem. Software oder Hardware in einem Netzwerk oder auf einem Computer, welche Angriffe zu erkennen versuchen, damit diese entweder verhindert, gestoppt oder zumindest in einem Log registriert werden.

INTRUSION KILL CHAIN (engl.)
Übsg. Angriffsablauf. Beschreibung der Phasen einer Cyber-Attacke. Diese sind

a. Erkundung eines Ziels,
b. Auswahl der Angriffsmethode,
c. Eigentlicher gezielter Angriff,
d. Einbau eines Backdoors,
e. Übernahme des Systems des Opfers.

Die Abwehr bei jeder dieser Phasen kann den Angreifer von seinem Ziel abhalten. Somit kann bereits das Bewusstsein dieser Phasen helfen, Attacken zu analysieren und zu verhindern.

Syn. zu Kill Chain, Cyber Kill Chain.

INTRUSION PREVENTATION (engl.)
Übsg. Einbruchsvorbeugung. Betreiben von Methoden, Prozesse, Software und Hardware, um das unberechtigte Eindringen in Systeme oder Netzwerke zu verhindern.

INTRUSION PROTECTION (engl.)
Übsg. Einbruchsschutz. Betreiben von Methoden, Prozessen, Software und Hardware, welche vor dem unberechtigten Eindringen in Systeme oder Netzwerke schützen.

INTUNE
Abk. für Microsoft Intune. Programm zum Cloud-Computing und zur Verwaltung von Windows-PCs und anderer Geräte mit Windows-Betriebssystem über das Internet. In einem Webbrowser lassen sich damit bspw. Updates auf den Geräten einspielen und Virenccans ausführen. Außerdem bietet Intune Zugriffskontrolle und Datenschutz in der Cloud.

INUNDATING (engl.)
Übsg. Überschwemmen. Attacke, die das Zielsystem mit sehr vielen Anfragen überschwemmt und damit überlastet. Beispiel: DDoS-Attacke.

INVENTORY (engl.)
Übsg. Bestände, Vorrat, Inventar. U. a. benutzt als „Inventory of Keys“ im Zusammenhang mit digitalen Schlüsseln.

IOCS
Abk. für Indicators of Compromise

IOT
Abk. für Internet of Things

IOT SECURITY (engl.)
Übsg. Sicherheit für Internet der Dinge. Themenkreis, der sich mit der Sicherheit und dem Schutz von IoT-Daten und IoT-Geräten beschäftigt.

IP
Abk. für Internet Protocol

IP-ADRESSE
Eindeutige, numerische Kennzeichnung der Geräte, welche am Internet oder einem anderen IP-Netzwerk angeschlossen sind und über das Internet-Protokoll kommunizieren können. Damit werden diese Geräte eindeutig adressierbar und Datenpakete können gezielt von Gerät zu Gerät geschickt werden. Seit ca. 1981 werden IP-Adressen in der IPv4-Variante des Internet-Protokolls als 4 Bytes in der 4 x 3 Darstellung mit Werten zw. 0 und 255 definiert, bspw. 192.168.0.1. Seit 1998 werden Geräte zudem mit IPv6 adressiert, wobei die verwendeten 16 Bytes nicht in der langen 16 x 3 Darstellung mit Werten zw. 0 und 255 gebraucht werden, sondern als 16 x 2 Werte zw. 00 und FF in hexadezimaler Form und zusätzlich mit Abkürzungen zu einem Wert wie 1354:8d2a:1 2ab:234:5dbb::534:aab4 zusammengefasst werden. Domain-Name-Systeme (DNS) verbinden IP-Adressen mit Domain-Namen und erlauben damit die Adressierung einer Internetseite bspw. als „www.domain.com“ anstatt einer reinen numerischen IP-Adresse „18.221.195.49“. Die eigene IP-Adresse lässt sich unter Windows in einem CMD-Fenster mit dem Befehl „ipconfig“ auslesen.

IP-PAKET
Grundelement der Datenkommunikation im Internet. Jede Anfrage oder Antwort im Internet wird als IP-Paket gesendet und besitzt Kopfdaten und Nutzdaten. Der Kopfteil beinhaltet Angaben zur Quelle, zum Ziel, zum Status, usw. und ist 60 Byte (IPv4) oder 40 Byte (IPv6) lang. Die Nutzdaten enthalten die eigentlichen Daten. In IP-Telefone wird das akustische Signal der Sprache digitalisiert und als IP-Pakete geschickt, z. T. sogar verschlüsselt.

IPSEC
Abk. für Internet Protocol Security

IRC
Abk. für Internet Relay Chat

IRIS-SCANNER
Elektronische Funktion innerhalb eines PCs oder Handys oder als eigenständiges Gerät, um die Regenbogenhaut („Iris“) eines Auges zu scannen. Das gescannte Bild der Iris kann benutzt werden, um die gescannte Person zu identifizieren, zu autorisieren oder zu authentifizieren, und damit bspw. Zugang zu einem Gebäude oder einem PC zu erlauben (siehe auch Biometrische Identifikation).

IRM
Abk. für Information Rights Management von Microsoft

ISA
Abk. für International Society of Automation

ISA-62443-3-3
Ein von International Society of Automation (ISA) herausgegebener Standard für den Bereich Sicherheit bei Industrieautomation und Steuerungssystemen, im Speziellen betreffend die Sicherheitsanforderungen und Sicherheitsniveaus.

(ISC)²
Abk. für International Information Systems Security Certification Consortium. Internationale Non-Profit-Organisation für Personen im Bereich der Informationssicherheit.

ISDN
Abk. für Integriertes Sprach- und Datennetz. Ab ca. 1980 benutzter Standard für digitale Telekommunikationsnetze.

ISO
Abk. für Organization for Standardization

ISO 27K
Von der International Organization for Standardization (ISO) publizierte Sammlung an Standards zur Informationssicherheit.

ISO 27000–27035
Einzelne Sammlungen innerhalb ISO 27k.

ISSUER OF CERTIFICATES (engl.)
Übsg. Emittent von Zertifikaten

IT
Abk. für Informationstechnologie

IT-GRUNDSCHUTZ
Von der BSI publiziertes Handbuch zur systematischen Identifikation und Umsetzung notwendiger Sicherheitsmaßnahmen in Firmen und Behörden.

ITIL
Abk. für Information Technology Infrastructure Library

IT PROFESSIONAL (engl.)
Person, welche Hardware oder Software in komplexen Systemen weltweit testet, aufbaut, installiert, repariert oder betreibt.

IT SECURITY (engl.)
Übsg. IT-Sicherheit. Schutz von Computersystemen, Netzwerken, Programmen oder Daten vor Diebstahl, Manipulation oder Zerstörung.

IT-SICHERHEITSGESETZ [IT-SIG]
Vom deutschen Bundestag seit Juli 2015 publiziertes Gesetz mit dem offiziellen Titel „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“. Dieses soll u. a. dazu beitragen, Ausfälle bei kritischen Infrastrukturen (KRITIS) zu verhindern.

IT-SIG
Abk. für IT-Sicherheitsgesetz

IV
Abk. für Initialization Vector

J

12

JACK
Steckertyp für den Anschluss von kleinen Audiogeräten. Ugs. Kopfhörerstecker.

JACKPOTTING (engl.)
Hacker-Methode, um Geld aus einem Geldautomaten zu stehlen. Dabei bohren die Angreifer ein kleines Loch in den Geldautomaten, entkoppeln die interne Festplatte und koppeln stattdessen eine externe Festplatte an, von der sie dann das System nach einem Reset neu booten und nach Belieben manipulieren können.

JAILBREAK (engl.)
Syn. zu Rooted device. Handy, bei welchem der SuperUser-Zugang freigeschaltet wurde und damit alle Einstellungen inkl. der Sicherheitseinstellungen verändert werden können. Auch können Standard-Apps gelöscht und ersetzt werden. Apps, die einen bestimmten Level an Sicherheit benötigen, bspw. Online-Banking-Apps, werden bewusst so programmiert, dass sie nur auf Handys laufen, bei denen kein Jailbreak durchgeführt wurde.

JAVA
1) Höhere objektorientierte Programmiersprache mit Ähnlichkeiten zur Programmiersprache „C++“. Java läuft auf Milliarden von Geräten, weswegen Sicherheitslücken gravierend sein können und rasch beseitigt werden. 2) Indonesische Insel mit der Hauptstadt Jakarta.

JAVA APPLET (engl.)
In Java programmierte Applikation, welche innerhalb einer Laufzeitumgebung bspw. einem Internetbrowser ausgeführt wird. Java-Applets waren weitverbreitet in den

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_12

1990er- und 2000er-Jahren, wurden seither jedoch von anderen Techniken und neueren HTML-Funktionen abgelöst.

JAVA DEVELOPMENT KIT [JDK]
Programmierumgebung mit Java-APIs

JAVA PLATFORM, STANDARD EDITION [JSE]
Sammlung von Java-APIs (JDK) sowie der Java-Laufzeit-Umgebung (JRE).

JAVA RUNTIME ENVIRONMENT [JRE]
Übsg. Java-Laufzeit-Umgebung

JAVASCRIPT
Einfach zu erlernende Programmiersprache, mit laufend erweitertem Befehlsumfang, welche innerhalb eines Internetbrowsers abgearbeitet (interpretiert) wird. Da der Code direkt zwischen die HTML-Zeilen der Internetseite eingefügt wird, ermöglicht JavaScript viele Automatisationen und damit dynamische Internetseiten, wie bspw. das Vorschlagen von Suchresultaten bereits während der Eingabe einer Suche.

JAVASCRIPT OBJECT NOTATION [JSON] (engl.)
Dateiformat in lesbarer Textform, welches zum Datenaustausch zw. Anwendungen und zur Speicherung benutzt wird.

JAVA VIRTUAL MACHINE [JVM] (engl.)
Interpreter für kompilierten JAVA-Code, wobei die JVM eine Schnittstelle zwischen dem JAVA-Code und der Maschine bzw. dem Betriebssystem darstellt, sodass derselbe JAVA-Code auf unterschiedlichen Betriebssystemen ohne Anpassung lauffähig ist. Außerdem überwacht die JVM die Ausführung des JAVA-Codes und verhindert damit Puffer Overflow u. Ä.

JML
Abk. für Joiner-Mover-Leaver

JOINER-MOVER-LEAVER [JML] (engl.)
Benutzer, welche neu zu einem System hinzukommen (Joiner), zu einem anderen System oder einer anderen Rolle innerhalb des Systems wechseln (Mover) oder vom System weggehen (Leaver).

JONDO
Software, welche den eigenen Internetdatenverkehr verschlüsseln und die eigene IP-Adresse verstecken kann.

JPM COIN
2019 gestartete Kryptowährung von JP Morgan.

JSON
Abk. für JavaScript Object Notation

JUNK MAIL (engl.)
Übsg. Unerwünschte Werbe-E-Mail

JVM
Abk. für Java Virtual Machine

K

13

KALTSTARTATTACKE
Im Jahr 2008 von Wissenschaftlern vorgestellte Angriffsmöglichkeit, welche „Kaltstartattacke“ genannt wird, und dazu verwendet werden könnte, um das Bitlocker-Passwort oder andere sensible Daten aus dem Speicher (RAM) auszulesen. Beim noch eingeloggten Gerät wird dafür die Batterie heraus- und schnell wieder hineingesetzt, sodass zwar das System neu bootet, aber das RAM noch nicht gelöscht ist. Dies wird zusätzlich durch Kühlung des RAM mit flüssigem Stickstoff oder einem Kältespray verbessert. Dann wird der Laptop mit einem kleinen Betriebssystem auf einem USB-Stick gebootet und das Passwort mit geeigneten Tools aus dem RAM ausgelesen.

KANAL
Konkreter Frequenzbereich des elektromagnetischen Spektrums, der benutzt wird, um Daten zu transferieren, bspw. bei WLAN-Routern.

KANBAN
Software-Entwicklungsmethode

KEEPASS PASSWORD SAFE
Kostenloser Passwort-Manager, der in vielen Tests empfohlen wird.

KENNWORT
Syn. zu Passwort

KERBERIZED FTP (engl.)
Sichere Authentifikationsmethode von FTP-Sessions, ohne das Kerberos-Passwort im Klartext übers Internet senden zu müssen. Dazu wird Kerberos auf dem Client und

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_13

dem Server verwendet. Kerberized FTP wird heutzutage meist durch SSH File Transfer Protocol (SFTP) abgelöst.

KERBEROS
Methode der Authentifizierung, welche auch in ungesicherten TCP/IP-Netzwerken möglich ist, dadurch, dass ein vertrauenswürdiger, geschützter Kerberos-Netzwerkdienst als dritte Partei (Trusted Third Party), meist ein Domain Controller, beteiligt ist.

KERCKHOFF-PRINZIP
Aussage in der Informations- und Kryptografietheorie zur Sicherheit eines kryptografischen Systems. Das Prinzip sagt aus, dass die Sicherheit eines kryptografischen Systems nur von der Geheimhaltung des Schlüssels, jedoch nicht vom kryptografischen Algorithmus abhängig sein sollte.

KERNEL PANIC (engl.)
Fehlerzustand im Hauptteil eines Betriebssystems. Dieses befindet sich damit in einem undefinierten Zustand und das System kann nicht mehr kontrolliert weiterbetrieben werden.

KEYCHAIN (engl.)
Übsg. Schlüsselbund. Passwort-Management-Software bei MacOS. Darin können Passwörter, private Schlüssel, Zertifikate und Notizen sicher gespeichert werden.

KEY DISTRIBUTION PROBLEM (engl.)
Übsg. Schlüsseltauschproblem. Um symmetrische Verschlüsselung durchführen zu können, muss ein gemeinsamer Schlüssel vereinbart werden. Diese Vereinbarung muss jedoch ebenfalls geheim geschehen, was ein Problem darstellt. Das Diffie-Hellman-Schlüsselaustauschverfahren löst dieses Problem.

KEY ESCROW (engl.)
Übsg. Schlüsselhinterlegung. Um verschlüsselte Daten auch bei Verlust des Schlüssels wieder entschlüsseln zu können, können Schlüsselkopien hergestellt und an einem sicheren Ort hinterlegt werden.

KEY EXCHANGE (engl.)
Übsg. Schlüsselaustausch

KEY GENERATION (engl.)
Übsg. Schlüsselerzeugung

KEY INJECTION (engl.)
Übsg. Schlüsseleinspeicherung

KEY LENGTH (engl.)
Übsg. Schlüssellänge. Siehe Liste der empfohlenen Schlüssellängen auf Keylength.com *(Abgerufen am 22.12.2019)* und einen Vergleich weiter unten beim Begriff „Sicherheitsniveau".

KEY LIFETIME (engl.)
Übsg. Schlüssellebensdauer. Siehe Liste der empfohlenen Schlüssellebensdauern auf Keylength.com *(Abgerufen am 22.12.2019).*

KEYLOGGER (engl.)
Übsg. Tastenprotokollierer. Schadsoftware oder Schadhardware, welche die Eingaben des Benutzers auf seiner Tastatur aufzeichnet und damit Hackern den Zugang zu Passwörtern und anderen sensiblen Daten ermöglicht.

KEY MANAGEMENT (engl.)
Übsg. Schlüsselverwaltung. Prozesse und Systeme, mit denen Schlüssel sicher gespeichert und archiviert werden, ohne die Möglichkeit zu verlieren, diese zur Entschlüsselung von Daten zu verwenden, und ohne das Risiko einzugehen, diese in falsche Hände geraten zu lassen.

KEY PERFORMANCE INDICATORS [KPI] (engl.)
Übsg. Hauptleistungsindikatoren. Kennzahlen eines Prozesses oder Systems, welche Aussagen machen darüber, wie weit der aktuelle Istzustand vom Sollzustand entfernt ist.

KEY ROTATION (engl.)
Übsg. Schlüsselwechsel. Verfahren, um Schlüssel regelmäßig automatisch zu ändern und damit die Zeit zu limitieren, in welcher ein Angreifer einen Schlüssel erraten oder benutzen kann.

KEY SIGNING (engl.)
Übsg. Signieren von Schlüsseln. Mathematische Verbindung zw. einem Schlüssel und Eigenschaften des Besitzers oder des Systems, auf dem dieser Schlüssel erzeugt wurde. Durch die Möglichkeit der Überprüfung dieser Verbindung wird ein Vertrauen aufgebaut oder erhöht, da damit sichergestellt werden kann, dass der Schlüssel auch wirklich zum richtigen Besitzer gehört oder vom richtigen System stammt.

Es werden zwei Verfahren unterschieden:

a. In hierarchischen Verfahren muss ein Schlüssel von einer höheren Beglaubigungsstelle signiert werden, damit der Signatur vertraut werden kann.
b. Bei Web-of-Trust-Verfahren können andere Benutzer den Schlüssel einer Person signieren, wenn sie die Person kennen, ihm vertrauen oder sogar seine physische Identität überprüft haben.

KEY SIGNING KEY [KSK] (engl.)
Übsg. Schlüssel für das Signieren eines Schlüssels.

KEY SIZE (engl.)
Übsg. Schlüssellänge

KEYSTROKE LOGGING (engl.)
Syn. zu Keylogger

KI
Abk. für künstliche Intelligenz

KILL CHAIN (engl.)
Übsg. Angriffsablauf. Beschreibung der Phasen einer Cyber-Attacke.

Diese sind

a. Erkundung eines Ziels,
b. Auswahl der Angriffsmethode,
c. eigentlicher gezielter Angriff,
d. Einbau eines Backdoors,
e. Übernahme des Systems des Opfers.

Die Abwehr bei jeder dieser Phasen kann den Angreifer von seinem Ziel abhalten. Somit kann das Bewusstsein dieser Phasen helfen, Attacken zu analysieren und zu verhindern. Syn. zu Intrusion Kill Chain, Cyber Kill Chain.

KILL SWITCH (engl.)
Übsg. Notausschalter. Wird auch im übertragenen Sinn verwendet. Bspw. beinhaltete WannaCry einen Kill Switch, sodass sich die Malware verbreitete, bis eine bestimmte Internetdomain erreichbar war und damit als Notausschalter agierte.

KIMSUKY
Schadsoftware einer APT-Gruppe, welche mittels Advanced Spear Phishing eine Google Chrome Extension verteilte, um Passwörter und Cookies zu stehlen.

KLARTEXT
Daten oder Informationen, die nicht verschlüsselt sind, unabhängig davon, ob sie jemals verschlüsselt waren.

KLARTEXT-BLOCK
Syn. zu Cleartext Block. Nachricht oder allg. Daten vordefinierter Länge, die unverschlüsselt vorliegen. Jede Nachricht kann grundsätzlich in gleich lange Blöcke aufgeteilt werden, wobei evtl. beim letzten Block ein Auffüllen („Padding“) mit Nullen oder Leerzeichen stattfinden muss, um die definierte Länge zu erreichen.

KLASSIFIKATION
Syn. zu Datenklassifizierung

KLEOPATRA
Software mit intuitiver Benutzeroberfläche zur Verwaltung, Bearbeitung und Benutzung von OpenPGP- und S/MIME (X.509)-Zertifikaten.

KNOWN PLAINTEXT ATTACK (engl.)
Übsg. Angriff durch Kenntnis des Klartexts. Methode, bei welcher mittels Kenntnis vieler Paare von Klartext und zugehörigem Geheimtext Rückschlüsse auf den Schlüssel und das Verschlüsselungsverfahren möglich werden.

KOLLABORATIVES FILTERN
Methode zur Vorhersage des wahrscheinlichen Nutzerverhaltens basierend auf dem Nutzerverhalten anderer mit gleicher Benutzungshistorie. Dies wird bspw. angewendet, um einer Person ein Buch oder einen Film vorzuschlagen, basierend auf ihren bisherigen Büchern und Filmen und ähnlichem Verhalten anderer Personen.

KOLLISION BEI HASH-FUNKTION
Bei einer Kollision besitzen zwei unterschiedliche Texte den gleichen Hash-Wert als Resultat einer Hash-Funktionsberechnung. Die verwendete Hash-Funktion ist damit „nicht kollisionsresistent“ und die damit erzeugten Signaturen etc. angreifbar.

KOMPROMITTIERTE DATEN, PASSWÖRTER, KONTEN, E-MAIL-ADRESSEN
Syn. zu beeinträchtigte, gehackte, unberechtigt benutzte, manipulierte Daten, Passwörter, Konten, E-Mail-Adressen.

KOMPROMITTIERUNG
Syn. zu Manipulation von Daten oder Systemen

KONSOLE
1) Gerät für Videospiele. Dieses wird meist an einen Fernseher oder Monitor angeschlossen. 2) Programm, aba. Terminal oder Terminal-Emulation, um Systembefehle und Systemausgaben textbasiert auszuführen und darzustellen. Bevor grafische Benutzeroberflächen und Computermäuse Ende 1970er-, Anfang 1980er-Jahren auf allen Computersystemen verfügbar waren, wurden Computer textbasiert benutzt, bspw. unter DOS oder Unix. Heutige

Systeme erlauben eine solche textbasierte Benutzung mit Programmen wie „CMD.exe“ (unter Windows) und „Terminal“ (unter Linux und Mac).

KONTO
1) Sammlung an Daten einer echten oder juristischen Person innerhalb einer Datenbank eines Finanzinstitutes. Diese Daten beinhalten v. a. Angaben zu den Geldwerten des Kontobesitzers. 2) Persönlicher Daten- und Zugriffsbereich bei einem PC oder in einem Online-Dienst. Ein registriertes und eingerichtetes Konto erlaubt die eindeutige Anmeldung und damit die Identifikation des Benutzers und seiner Rechte. Damit erhält der Benutzer bspw. Lese-/Schreibrechte auf Dateien, Rechte zur Bestellung von Waren usw. Der Zugang zu Konten wird mittels Benutzername und Passwort oder durch andere Login-Methoden wie PIN, 2FA usw. geschützt. Innerhalb eines Kontos gibt es meist die Möglichkeit, seine Identitätsdetails wie Name, Alter, E-Mail-Adresse sowie die eigene Sichtbarkeit für andere Benutzer einzustellen.

KPI
Syn. zu Key Performance Indicator

KREDITKARTENDATEN
Kombination der Kreditkartennummer, des Besitzernamens, des Ablaufdatums und der Kartenidentifikationsnummer. Erhält ein Dieb Kenntnis dieser Daten, kann er im Namen des Opfers Waren bestellen. Deshalb erweiterten viele Kreditkartenherausgeber den Schutz durch zusätzliche Abfrage eines Passworts oder eines Codes.

KRITIS
Abk. für kritische Infrastruktur

KRITISCHE INFRASTRUKTUR [KRITIS]
IT- oder Infrastruktursysteme, welche grundlegende Bereiche der Bevölkerung unterstützen und somit besonderen IT-Sicherheitsschutz benötigen. Beispiele sind Systeme der Stromversorgung, der Finanzen, der Wasserversorgung oder der Ernährung.

KRYPTOANALYSE
Methoden und Verfahren zur Bestimmung des Klartextes oder des Schlüssels aus dem Geheimtext. Benutzte Techniken sind bspw. a) lineare Kryptoanalyse, welche mittels direkter „Known-Plaintext“-Berechnungen versucht, blockbasierte, symmetrische Verfahren zu knacken sowie b) die differenzielle Kryptoanalyse, welche versucht, die Differenzen in Geheimtexten zu ermitteln durch die Kenntnis von Differenzen in den Klartexten.

KRYPTOGRAFIE
Teilgebiet der Mathematik und der IT. Die Kryptografie beschäftigt sich mit der Wissenschaft und der Anwendung der Verschlüsselung, Entschlüsselung und allg. der Informationssicherheit. Auch als Syn. zu Kryptologie verwendet.

KRYPTOGRAFISCHE METHODEN
Mathematische Algorithmen zur Verschlüsselung, Entschlüsselung, Signierung und Zertifikatserzeugung mit dem Ziel der Geheimhaltung und der Übermittlung von Daten sowie der Sicherstellung und der Validierung der Datenintegrität, der Datenvertraulichkeit, der Datenauthentizität sowie der Datenverfügbarkeit.

KRYPTOLOGIE
Teilgebiet der Mathematik und der IT. Die Kryptologie beschäftigt sich mit der Lehre der Verschlüsselung, Entschlüsselung und allg. der Informationssicherheit. Auch als Syn. zu Kryptografie verwendet.

KRYPTOMECHANISMUS
Syn. zu Verschlüsselungsmechanismus

KRYPTOPROTOKOLLE
Verschlüsselungsstrukturdefinitionen und -software, bspw. für sichere Datenübertragung. Meist aufgebaut als Kombination aus Funktionen für den Schlüsselaustausch und Funktionen für die Kryptografie zur Sicherstellung der Vertraulichkeit und Integrität der Nachricht.

Beispiele für Kryptoprotokolle: TLS, SSL, SSH, WPA2.

KRYPTO-TROJANER
Schadsoftware, welche Dateien im infizierten PC verschlüsselt. Erpressungstrojaner (aba. Ransomware) können in Form von Krypto-Trojanern vorkommen und Lösegeld verlangen zur Entschlüsselung der Dateien.

KRYPTOWÄHRUNG
Digitale Geldwährung und digitales Zahlungsmittel, welches gehandelt werden kann, und mit welchem sich digitale und physische Objekte kaufen und verkaufen lassen. Kryptowährungen basieren auf kryptografischen Algorithmen, durch welche die Transaktionen nachvollziehbar und gegen Manipulation geschützt werden und mit welchen zusätzliche Geldeinheiten dieser Währung erzeugt und kontrolliert werden. Viele Kryptowährungen basieren auf der Blockchain-Technologie.

Beispiele für Kryptowährungen: Bitcoin, Ether, XRP, Litecoin, Monero

KSK
Abk. für Key Signing Key

KÜNSTLICHE INTELLIGENZ [KI]
Themengebiet innerhalb der Datenwissenschaften (Data Science). Methoden und Algorithmen, um mithilfe großer Datenmengen und großer Computerleistung spezifische Probleme zu lösen.

Häufig eingesetzte Techniken sind:

Neuronale Netze, Deep Learning, Natural Language Processing (NLP), Reinforcement Learning, Pattern Recognition, Supervised Learning, Un-Supervised Learning u. a.

K-VON-N
Methode zur Sicherstellung, dass ein Systemzugriff zwingend durch mehrere Personen bestätigt werden muss. Dabei wird ein Zugriffscode oder Passwort mathematisch auf „n Personen“ aufgeteilt, sodass der Systemzugriff danach nur mit mind. „k von n Personen“ möglich ist.

KYBERNETIC
Teilgebiet der Technik, welches sich mit der Steuerung von Maschinen beschäftigt.

L

14

LAAR
Abk. für Location Aware Access Control

LAN
Abk. für Local Area Network

LATERAL MOVEMENT (engl.)
Übsg. Seitwärtsbewegung. Technik von Angreifer, bei welcher der Hacker sich systematisch durch das Netzwerk bewegt, um Daten und Informationen zu finden, welche es ihm erlauben, Zugang und Kontrolle über ferngesteuerte Systeme im Netzwerk zu erhalten.

LAUFWERKSVERSCHLÜSSELUNG
Methode, um ganze Laufwerke anstatt einzelner Dateien zu verschlüsseln. Dies hat den Vorteil, dass ein Dieb weder die Dateinamen noch die Verzeichnisstruktur erkennen kann. Entsprechende Software, bspw. BitLocker, verknüpft die automatische Laufwerksverschlüsselung und -entschlüsselung mit einem Benutzerpasswort, einem Zertifikat auf einer SmartCard, einem Fingerabdruck oder bspw. der Windows-Anmeldung.

LAUFZEITUMGEBUNG
Syn. zu Runtime Environment. Software, in welcher Programme geladen und ausgeführt werden können, die dabei verwaltet und geschützt werden, bspw. vor verbotenem Speicherzugriff. Laufzeitumgebungen ermöglichen auch die Ausführung der gleichen Software auf unterschiedlichen Betriebssystemen. Beispiel: Java Runtime Environment.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_14

LAUSCHANGRIFF
Syn. zu Abhören

LAUSCHEN
Syn. zu Abhören von Daten oder Gesprächen.

LAZARUS GROUP
Hacking-Gruppe

LCD
Abk. für Liquid Crystal Display, Übsg. Flüssigkristallanzeige. Technik für Displays und Bildschirme zur Darstellung des Inhalts.

LDAP
Abk. für Lightweight Directory Access Protocol

LEADING EDGE TECHNOLOGY (engl.)
Übsg. Spitzentechnologie. Siehe auch Bleeding Edge Technology, Cutting Edge Technology.

LEAK (engl.)
Übsg. Undichte Stelle. Datenverlust aufgrund von Fehlfunktionen in Systemen, über welche sensible Daten ungeschützt verschickt werden, oder aufgrund von Personen, die Zugriff auf sensible Daten besitzen und diese bewusst oder unbewusst aus der Firma bringen.

LEAST PRIVILEGED (engl.)
Übsg. Geringste Berechtigung. Prinzip, nach welcher eine Software, ein System oder ein Benutzer nur die Zugangsrechte erhält, die für die Aufgabe aktuell erforderlich sind.

LEBENSZYKLUS KRYPTOGRAFISCHER SCHLÜSSEL
Digitale Schlüssel durchleben mehrere unterschiedliche Phasen innerhalb ihrer Existenzdauer. Die Reihenfolge und Häufigkeit dieser Phasen sind nicht strikt vorgegeben, sondern abhängig vom Einsatz der Schlüssel. Die wichtigsten Phasen im Lebenszyklus kryptografischer Schlüssel sind: 1) Erzeugung, 2) Bearbeitung, 3) Speicherung, 4) Zertifizierung, 5) Eintragung, 6) Verteilung, 7) Benutzung, 8) Änderung, 9) Übertragung, 10) Annullierung, 11) Archivierung, 12) Wiederherstellung, 13) Vernichtung.

LEBENSZYKLUS VON INFORMATIONEN
Informationen durchleben mehrere unterschiedliche Phasen innerhalb ihrer Existenzdauer. Die Reihenfolge und Häufigkeit dieser Phasen sind nicht strikt vorgegeben, sondern abhängig vom Einsatz der Informationen.

Die wichtigsten Phasen im Lebenszyklus von Informationen sind: 1) Erzeugung, 2) Bearbeitung, 3) Transport, 4) Speicherung, 5) Archivierung, 6) Beseitigung und 7) Vernichtung.

LEDGER (engl.)
Übsg. Grundbuch, Kassenbuch, Wertverzeichnis

LEETSPEAK
Methode, um Buchstaben durch ähnlich aussehende oder ähnlich klingende Zahlen zu ersetzen. Leet entstammt dem Wort „Elite“ und deutet an, dass nur ein Experte solche Worte oder Texte verstehen kann.

Beispiele für Texte in einem Leetspeak-Format:

Original-Text	Text im Leetspeak-Format
«IT Security A-Z»	«17-53cur17y 4-z»
«someone»	«sum1»
«me, too»	«m1 2»
«you are too late»	«u r 2 l8»

LEGACY SYSTEM (engl.)
Übsg. Altsystem. Computer, Handy oder anderes Gerät mit alter, nicht mehr zeitgemäßer Hardware oder Software. Das Risiko für Malware, Attacken, fehlender Sicherheitsfunktionen u. Ä. steigt bei diesen Systemen zunehmend, da Hersteller der Hardware und Software häufig Sicherheitsupdates überhaupt nicht oder nur mit Verzögerung bereitstellen. Auch kann die fehlende aktive Überprüfung der Zugriffe bei Altsystemen Personen weiterhin einen Zugriff auf diese Systeme oder auf Daten ermöglichen, obwohl sie längst in anderen Bereichen oder für andere Firmen tätig sind.

LET’S ENCRYPT (engl.)
Übsg. Lasst uns verschlüsseln. Zertifizierungsstelle, die ab 2015 kostenlos Zertifikate für TLS anbietet, damit mehr Internetseiten über das Protokoll HTTPS anstatt HTTP angeboten und abgerufen werden können.

LIBRARY (engl.)
Übsg. Bibliothek. Bei Programmiersprachen bieten Bibliotheken zusätzliche, optimierte Funktionen an, die im Grundumfang der Programmiersprache nicht vorhanden sind. Dies können bspw. Funktionen sein, um ein Fenster zu erstellen, einen Text in ein Fenster zu schreiben, einen Text zu verschlüsseln oder eine Person zu authentisieren. Die Einbindung solcher Funktionen erleichtert, beschleunigt und vereinheitlicht die Software-Entwicklung und erzeugt einen sichereren Code.

LIBSSH
Bibliothek für die Programmiersprache C. LibSSH bietet Funktionen, um SSHv2-Protokolle auf Server und Client zu implementieren.

LIBSSH FLAW (engl.)
Im Jahr 2018 gefundene Schwachstelle in LibSSH, die es einem Hacker erlaubt, die Serverauthentisierung zu umgehen.

LIFECYCLE MANAGEMENT (engl.)
Übsg. Lebenszyklusbewirtschaftung. Alle Maßnahmen der Bewirtschaftung von Systemen, Produkten oder Prozessen während deren Einsatzdauer.

LIFELOGGING (engl.)
Übsg. Lebensaufzeichnung. Syn. zu „Quantified Self Movement“. Methoden und Tools, um das ganze Leben ständig aufzuzeichnen.

LIGHTNING
Schnittstelle und Steckertyp von Apple.

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL [LDAP] (engl.)
Netzwerkprotokoll zur Abfrage und Änderung von Informationen, wie Personendaten oder Rechnerkonfigurationen, welche auf verteilten Verzeichnisdiensten gespeichert sind.

LIKE-BUTTON (engl.)
Übsg. Zustimmungsknopf. Funktion bei sozialen Medien, um seine Zustimmung zu einem Text, Bild oder Video zu äußern und damit nachfolgenden Personen einen Entscheidungshinweis zu geben.

LIKEN
Ugs. für positive Bewertung abgeben bei sozialen Medien.

LINEARE KRYPTOANALYSE
Eine Technik der Kryptoanalyse, welche mittels direkter „Known-Plaintext“-Berechnungen versucht, blockbasierte, symmetrische Verfahren zu knacken.

LINK (engl.)
Übsg. Verknüpfung. Syn. zu Hyperlink, Weblink. Objekt, meist Text oder ein Bild auf einer Internetseite, welche den Benutzer durch Anklicken zu einem anderen Bereich dieser Internetseite oder zu einer anderen Internetseite weiterleitet.

LINUX
Kostenlose, Unix-ähnliche Betriebssysteme. Linux erreichte innerhalb der letzten 30 Jahren große Verbreitung auf privaten PCs, Firmen-PCs, auf wissenschaftlichen Rechnern, Servern, Handys usw. Es werden verschiedene Linux-Varianten, sog. Distributionen von mehreren Organisationen und Firmen bereitgestellt. Viele davon werden basierend auf der freien GPL-Lizenz bereitgestellt.

LINUX-KONSOLE
System-Konsole in Linux, mit dessen Hilfe der Kernel und andere Prozesse Textmeldungen zum Benutzer senden und Eingaben vom Benutzer empfangen kann.

LITECOIN
Kryptowährung

LITTLE ENDIANS (engl.)
Übsg. Klein-Endende. Reihenfolge der Bytebenutzung beginnend mit dem kleinsten Byte, vergleichbar mit dem Datum in der deutschen Sprache, welches auch mit der kleinsten Angabe beginnt (Tag – Monat – Jahr). Gegenteil: Big Endians.

Beispiel

Little Endians	0x23lFE343 wird als 43 E3 1F 23 übertragen oder gespeichert.
Big Endians	0x23lFE343 wird als 23 1F E3 43 übertragen oder gespeichert.

LLD
Abk. für Low-Level-Design. Dokument, welches das geplante Design für ein Produkt genau beschreibt.

LOADBALANCER (engl.)
Übsg. Lastverteiler. Gerät oder Software, welche Anfragen von Clients erhält und an gleichwertige Server verteilt, sodass alle Server gleich ausgelastet sind und möglichst viele Anfragen gleichzeitig abgearbeitet werden können. Es werden zwei Betriebsmodi unterschieden:

a. Anfragen aller Clients werden rundum auf den jeweils nächsten Server verteilt (sog. „Round Robin“)
b. Anfragen jedes Clients (genauer: jeder Session) werden immer zum gleichen Server geleitet (sog. „Sticky“)

LOAD TEST (engl.)
Übsg. Lasttest. Überprüfung des Verhaltens einer neuen Software oder eines neuen Systems bei hoher Belastung, bspw. durch Simulation vieler gleichzeitig agierender Benutzer.

LOC
Abk. für Line of Code, Übsg. Anzahl programmierter Zeilen.

LOCAL ADMINSTRATION RIGHTS [LAR] (engl.)
Übsg. Lokale Administratorrechte

LOCAL AREA NETWORK [LAN] (engl.)
Übsg. Lokales Netzwerk. Verbund von Systemen, die untereinander kommunizieren können. Typisches Beispiel ist WLAN im privaten Haushalt, bei welchem die Geräte mit einem Router kabellos verbunden sind und über ihre IP-Adressen gegenseitig angesprochen werden können.

LOCATION AWARE ACCESS CONTROL [LAAR] (engl.)
Übsg. Positionsabhängige Zugangskontrolle.

LOCKBOX (engl.)
Übsg. Schließfach. Speicher für private Schlüssel des Benutzers.

LOCKHEED MARTIN KILL CHAIN
Typ von Kill Chain.

LOCK SCREEN (engl.)
Übsg. Sperrbildschirm. Bildschirmdarstellung bei PCs, Handys und anderen Geräten, welche den Zugang zum Gerät erst freigibt, wenn ein Code, ein Passwort, ein Fingerabdruck u. Ä. korrekt eingegeben wurde.

LOCKY
Schadsoftware in Form eines Krypto-Trojaners.

LOG
Syn. zu Protokollierung. Eintrag in einer Textdatei oder einer Datenbank zur Protokollierung von Ereignissen, bspw. dem Zeitpunkt der Anmeldung eines Benutzers an einem PC.

LOGCAT
Tool zur Analyse von Protokolldateien.

LOGGING OF CYBER THREATS (engl.)
Übsg. Protokollierung von Cyber-Bedrohungen.

LOGIC BOMBS (engl.)
Übsg. Logik-Bombe

LOGIK-BOMBE
Schadsoftware, welche erst dann ausgeführt wird, wenn eine bestimmte Triggerbedingung erfüllt ist, bspw. ein vordefinierter Kalendertag.

LOGIN (engl.)
Übsg. Anmeldung

LOGIN CREDENTIALS (engl.)
Übsg. Anmeldedaten

LOGIN DOMAIN (engl.)
Übsg. Anmeldedomäne. Active Directory Domäne, welche speziell für die Anmeldung von Benutzern an ihren PCs aufgesetzt wurde.

LOJACK FÜR LAPTOPS
Software, die im BIOS vieler Laptophersteller vorinstalliert ist und einmal pro Tag eine Verbindung zu einem Server der Firma „Absolute Software" herstellt, um zu prüfen, ob der Laptop als gestohlen gemeldet wurde. Falls ja, kann der Laptop aus der Ferne gesteuert werden, um Daten zu sichern, Daten zu löschen und weitere Software zu installieren, die helfen kann, den Laptop zu orten. Da LoJack sich wie ein UEFI Rootkit einnisten muss, wird dieses Tool von Anti-Viren-Programmen ignoriert, was jedoch bei Attacken auf LoJack zum Risiko wird.

LOKALE ADMINISTRATORRECHTE
Zeitlich limitierte oder unlimitierte Administratorzugriffs- und -änderungsrechte auf einem System.

LOKALE EXPLOITS
Ausnutzung von Schwachstellen in Anwendungen lokaler Geräte. Bspw. können Schwachstellen bei Foto-Apps oder bei PDF-Viewer beim Öffnen manipulierter Foto- oder PDF-Dateien ausgenutzt werden.

LOKIBOT
Android Erpressungsprogramm. Schadsoftware in Form eines „Infostealer"-Trojaners.

LOL
1) In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „Loughing out Loud", Übsg. „Laut herauslachen". 2) Seltener in SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „Lots of Love", Übsg. „Liebe Grüße". Da „Lots of Love" auch in traurigen Zusammenhängen benutzt wird, sollte es nicht mit LOL abgekürzt werden, da Missverständnisse bei den Empfängern entstehen könnten, welche dies als „Loughing out Loud" interpretieren.

LONG TERM EVOLUTION [LTE] (engl.)
Mobilfunktechnologie der vierten Generation (4G).

LOOK-UP SECRETS AUTHENTICATOR (engl.)
Übsg. Geheimnisse, die sich nachsehen lassen. Physisch vorliegende oder elektronisch gespeicherte Geheimnisse, welche zuvor vereinbart wurden oder vor Benutzung, bspw. in einem Authenticator, erzeugt werden. Dies können z. B. Schlüsselwiederherstellungscodes oder TANs für E-Banking sein.

LOOPHOLE (engl.)
Übsg. Sicherheitslücke

LOSS OF PROPRIETARY INFORMATION (engl.)
Übsg. Verlust geschützter oder geheimer Informationen.

LOW ENTROPY PASSWORD (engl.)
Übsg. Passwort mit wenig Entropie. Syn. zu schwaches Passwort.

LTE
Abk. für Long Term Evolution, einer Mobilfunktechnologie der vierten Generation (4G)

LUCKY 13 ATTACKE
Angriff auf TLS und DTLS durch Ausnutzung eines Fehlers in der TLS-Spezifikation, insb. bei der Berechnung des Message Authentication Codes (MAC). Angewendet auf OpenSSL, konnte der komplette Klartext von CBC-verschlüsselten Daten ermittelt werden.

LUNINOSITYLINK
Schadsoftware in Form eines Trojaners, der ferngesteuert wird. Aba. „Remote Access Trojan“.

M 15

MAC
1) Abk. für Message Authentication Code. 2) Abk. für MAC-Adresse. 3) Abk. für Macintosh. Geräte der Firma Apple.

MAC-ADRESSE
Eindeutige Adresse jedes Geräts in einem Netzwerk. 48-Bit langer, hexadezimaler Wert der Art 00:23:ae:33:18:6d

MACH
Mikrokernel für Unix-kompatible Betriebssysteme, auf welchem u. a. Apple MacOS basiert.

MACHINE LEARNING (engl.)
Übsg. Maschinenlernen. Fähigkeit von Software, Informationen zu verarbeiten, einzuordnen und für die weitere Optimierung der Berechnungen zu verwenden und dadurch im übertragenen Sinn zu lernen. Diese neu gelernten, zusätzlichen Informationen können danach eingesetzt werden, um komplexere oder vorher noch nicht gelernte Informationen in die Ordnungsstruktur einzufügen oder zu analysieren. Siehe auch Abb. 16.1 und 16.2.

Beispiel: Neuronale Netze mit mehreren Berechnungsstufen (sog. „Hidden Layers“) benutzen Machine Learning Algorithmen, aba. Deep Learning, und ermöglichen es, Texte, Sprache oder Bilder immer genauer und schneller zu erkennen und damit bspw. autonomes Fahren zu ermöglichen.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_15

MACHINE LEARNING SYSTEM (engl.)
Übsg. Maschinenlernsystem. System aus Software und evtl. auch Hardware, um Machine Learning Algorithmen und Routinen auszuführen.

MACRO (engl.)
Übsg. Makro

MAGECART
Programm, welches von Hacking-Gruppen benutzt wird, um Schadsoftware in Internetshops hineinzubringen und damit Zahlungsdetails zu stehlen.

MAILBOX (engl.)
Übsg. Postkasten. 1) Bis ca. 1990 wurde ein Computer als Mailbox oder Bulletin Board System (BBS) bezeichnet, falls er privat betrieben und zur Kommunikation und zum Datenaustausch benutzt wurde. 2) Ab ca. 1990 wird ein E-Mail-Konto Mailbox genannt.

MAINFRAME (engl.)
Großrechner bei Firmen, wie Banken und Versicherungen sowie bei der öffentlichen Verwaltung. Mainframes werden v. a. auf Zuverlässigkeit und hohen Datendurchsatz getrimmt.

MAKRO
Software innerhalb von Microsoft Office, in Mathematik-Tools und in vielen anderen Applikationen. Makros können hilfreich sein, bspw. zur Automatisation regelmäßiger Berechnungen, die jeweils nur leicht unterschiedlich sind. Ebenso lassen sich damit auch rasch und einfach Aktionen auf dem PC programmieren. Als Programmiersprache werden meist interpretierbare, d. h. als Einzelschritte ausgeführte Skriptsprachen benutzt, wie z. B. Basic, Perl, DOS etc. Die Möglichkeit, Makros automatisch beim Öffnen von Microsoft Excel, Microsoft Word oder anderen Produkten auszuführen, in Kombination mit der Möglichkeit, dem Makro tief greifende Rechte im PC zu erteilen, erhöht die Gefahr, dass Makros innerhalb von E-Mail-Anhängen oder von heruntergeladenen Programmen schwerwiegende Schäden am PC anrichten.

MALICIOUS ACTOR (engl.)
Übsg. Böswilliger Akteur. Person oder Gruppe von Personen, welche verantwortlich ist für einen ausgeübten oder geplanten Hacker-Angriff.

MALICIOUS INSIDER (engl.)
Übsg. Böswilliger interner Mitarbeiter

MALICIOUS OUTSIDER (engl.)
Übsg. Böswillige Person, die nicht Mitarbeiter der attackierten Firma ist.

MALICIOUS SOFTWARE (engl.)
Übsg. Schadsoftware, welche zum Ziel hat, Computer oder Geräte zu zerstören, unbrauchbar zu machen, zu manipulieren, sensible Informationen zu stehlen, Zugang zu privaten PCs zu erlangen u. Ä.

MALVERTISEMENT (engl.)
Übsg. Internetwerbung, in welcher sich Schadsoftware versteckt, die durch das Anklicken oder automatisch aktiviert wird.

MALVERTISING CAMPAIGN (engl.)
Übsg. Angriffskampagne basierend auf schädlichem Code, der sich durch Internetwerbung verbreitet. Dieser injizierte Code wird entweder beim Anklicken der Werbung aktiv oder bereits beim Laden der Internetseite („Drive-by-Download“) ohne Zutun des Benutzers.

MALWARE (engl.)
Übsg. Schadsoftware, welche zum Ziel hat, Computer oder Geräte zu zerstören, unbrauchbar zu machen, zu manipulieren, sensible Informationen zu stehlen, Zugang zu privaten PCs zu erlangen u. Ä.

MAN
Abk. für Metropolitan Area Network

MANAGED CODE (engl.)
Übsg. Verwalteter Code. Software, für welche die Laufzeitumgebung oder der Compiler die Speicherverwaltung kontrolliert. Beispiele sind: Java Runtime Environment und .NET.

MANAGED FILE TRANSFER [MFT] (engl.)
Übsg. Geregelte Dateiübertragung. Eine Methode zur Dateiübertragung ohne die Limitationen und (Sicherheits-) Risiken von FTP. Dies erlaubt es, hohe Datenmengen sicher und zuverlässig zu übertragen. Bspw. sind Funktionen enthalten für Multi-Faktor-Authentisierung, Verschlüsselung der Daten am Ort, bevor sie versendet werden, Wiederherstellung nach einer Panne usw.

MANAGED POE SWITCH (engl.)
Syn. zu PoE Switch

MANDANTEN-SCHLÜSSEL
Aba. Server Licensor Certificate (SLC). Der digitale Hauptschlüssel für kryptografische Funktionen innerhalb einer firmenweiten Microsoft-Rights-Management-Installation.

MAN-IN-THE-EMAIL-SCAM (engl.)
Übsg. Betrug durch gefälschte E-Mails. Personen in höheren Firmenpositionen erhalten scheinbar echte E-Mails von bekannten Partnern mit der Bitte um Bezahlung einer vereinbarten Rechnung. Dabei benutzen die böswilligen Sender E-Mail-Adressen, die den bekannten E-Mail-Adressen ähneln, sodass diese nicht sofort als falsch angesehen werden.

MAN-IN-THE-MIDDLE [MITM] (engl.)
Übsg. Betrug durch Mithören oder Verändern der Kommunikation zw. zwei Parteien. Dabei täuscht der Angreifer jeweils vor, die andere Partei zu sein.

MARKDOWN (engl.)
Methode zur Formatierung und Strukturierung von Texten durch einfache Befehle innerhalb des Textes. Derart formatierte Texte können danach meist auch als HTML-Code exportiert werden, wobei die HTML-Befehle automatisch aus den Markdown-Befehlen erstellt werden (siehe Kap. 35).

Beispiele: Text, der kursiv dargestellt werden soll, wird *zwischen Sternchen* gesetzt

MARKENMISSBRAUCH
Cyber-Bedrohung, bei welcher eine Produktmarke durch Angriff auf die Firmensysteme beeinträchtigt wird.

MARKET DATA (engl.)
Übsg. Marktdaten

MASKIEREN VON DATEN
Entfernen von identifizierbaren Inhalten aus Daten.

MASSIVE OPEN ONLINE COURSE [MOOC] (engl.)
Meist kostenlose Online-Kurse, welche von Hochschulen, Institutionen und Privatpersonen angeboten werden, mit dem Ziel, den Zugang zu Wissen für alle Personen zu ermöglichen.

MASTER BOOT RECORD [MBR] (engl.)
Syn. zu Master Boot Sector. Software in festdefinierten Bereichen der Festplatte. Diese Software wird beim Start eines PCs als Erstes ausgeführt, um BIOS-Werte auszulesen und bereit zu stellen, sodass ein Betriebssystem geladen und gestartet werden kann.

MASTER BOOT SECTOR (engl.)
Syn. zu Master Boot Record

MASTER-PASSWORT
Kennwort zur Anmeldung an einem Passwort-Manager. Mit einem Passwort-Manager können die eigenen Logins und Passwörter zu Online-Diensten und Apps gespeichert werden, ohne dass man sich diese merken oder aufschreiben muss. Dadurch können diese Kennwörter komplex gewählt werden, was die Sicherheit und den Schutz der eigenen Konten erhöht. Das Speichern dieser Kennwörter im Passwort-Manager bedarf eines gut gewählten Master-Passworts. Passwort-Manager und Master-Passwörter können direkt in einem Webbrowser, in einer Browser-Erweiterung oder in einer separaten App benutzt werden. In vielen Tests wurde der kostenlose Passwort-Manager KeePass Password Safe empfohlen.

MASTER SECRET KEY [MSK] (engl.)
Übsg. Geheimer Hauptschlüssel. Bei einigen kryptografischen Funktionen erzeugter und benutzter Hauptschlüssel, mit welchem andere geheime Schlüssel erzeugt werden können.

MASVS
Abk. für Mobile App Security Verification Standard

MAYHAM
Erster Computer, der einen Hackerwettbewerb gegen andere Hackercomputer gewann (2017).

MBR
Abk. für Master Boot Record

MCAS
Abk. für Microsoft Cloud App Security. Ein Microsoft Office365 Service.

MD5-HASH
Abk. für Message-Digest Algorithm 5. Kryptografische Funktion, um Passwörter und Nachrichten vor der Speicherung in einer Datenbank zu verschleiern. Der zu verschleiernde Text wird dabei in einen 128-Bit langen Hash-Wert umgerechnet. Sowohl MD5 als auch SHA1 und SHA256 werden nicht mehr für Passwort-Hashing empfohlen, denn sie sind u. a. schnell zu berechnen und deswegen auf Brute-Force-Angriffe anfällig. Der meistempfohlene Algorithmus zum Hashen von Passwörtern ist aktuell Blowfish.

MDNS
Abk. für Multicast DNS

MELANI
Abk. für Melde- und Analysestelle Informationssicherung. Organisation der Schweizerischen Bundesverwaltung. Hauptaufgabe ist der Schutz der nationalen kritischen Infrastrukturen, sowie der Schutz der Schweiz vor Cyber-Risiken.

MELTDOWN
Im Jahre 2017 gefundene und 2018 publizierte Hardware-Sicherheitslücke in sehr vielen Mikroprozessoren, welche den Zugriff auf Speicherbereiche anderer Prozesse ermöglicht (sog. Seitenkanalattacke). Meltdown wurde Anfang 2018 zeitgleich mit der Prozessorsicherheitslücke Spectre veröffentlicht.

MEME
Mehrzahl des Begriffs „Mem“. Physisch oder digital ausbreitende Gedanken oder Bilder, meist amüsanter Art.

MEMORIZED SECRET AUTHENTICATOR (engl.)
Übsg. Geheimnis, welches nur als Erinnerung vorhanden ist, bspw. ein Passwort oder ein PIN. Dieses Geheimnis muss ausreichend komplex und sicher sein, sodass es nicht erraten und missbräuchlich verwendet werden kann.

MEMORY ANALYSIS
Übsg. Speicheranalyse. Methoden und Tools zur Bestimmung von Viren-Signaturen oder von dateiloser Schadsoftware, welche nur im Speicher vorhanden ist. Durch die Speicheranalyse lassen sich Anti-Viren-Programme verbessern, sodass gleichartige Angriffe in Zukunft verhindert werden.

MERKLE-BAUM
Eine Datenbaumstruktur, welche durch Kombination von Hashes die Richtigkeit der Daten sicherstellt und damit die Überprüfung der Unversehrtheit der Daten erlaubt. Dies wird bspw. bei Blockchain-Transaktionen verwendet, bei welchen jeweils der Transaktions-Hash berechnet wird und dieser zusammen mit anderen Transaktions-Hashes einen neuen Hash bildet, der danach als neuer Blockchain-Block eingebunden werden kann. Auch die Unversehrtheit von Daten in Archiven kann in ähnlicher Weise mit einem Merkle-Baum bewiesen werden.

MERKLE TREE (engl.)
Übsg. Merkle-Baum

MESSAGE AUTHENTICATION CODE [MAC] (engl.)
Verfahren, welches Daten mit einem Schlüssel zu einer Prüfsumme kombiniert, und damit die Überprüfung der Integrität und der korrekten Herkunft der Daten ermöglicht.

Bspw. wird für TLS eine kryptografische Hash-Funktion benutzt, um den MAC zu berechnen. Häufig verwendete Algorithmen sind GMAC und HMAC.

METADATA
Syn. zu Metadaten

METADATEN
Daten, die nicht die eigentlichen Nutzdaten darstellen, sondern Angaben beinhalten zur Steuerung oder Verfolgung der Nutzdaten. Bspw. beinhalten E-Mails nicht nur den geschriebenen E-Mail-Text (im E-Mail-Body), sondern auch Metadaten (im E-Mail-Header), die den Weg der E-Mail von einem Server zum anderen beinhalten, sowie Angaben über den Absender, Empfänger, Sendedatum, Sendezeit etc.

METASPLOIT
1) Pentesting-Software, um Systeme gegen bekannte Exploits zu testen. 2) Software, welche zur Entwicklung und Ausführung von Attacken gegen Exploits eingesetzt wird.

MFA
Abk. für Multi-Factor Authentication, Übsg. Multi-Faktor-Authentisierung, Multi-Faktor-Authentifizierung

MFT
Abk. für Managed File Transfer

MICIUS
Erster Satellit, der speziell für wissenschaftliche Experimente im Bereich der Quantenkommunikation ins Weltall gebracht wurde. Damit wurde u. a. gezeigt, dass die Verteilung von Quantenschlüsseln (sog. Quantum-Key-Distribution) via Satellit-zu-Boden-Kommunikation über 1200 km möglich ist.

MICROCODE
Die Art, wie Befehle in der CPU ausgeführt werden, ist bei bestimmten Prozessortypen nicht fest eingebrannt (hartcodiert), sondern dynamisch mittels Microcodes implementiert. Microcodes sind somit Übersetzer von Anweisungen, die an die CPU geschickt werden, um als physikalische Vorgänge innerhalb der CPU ausgeführt zu werden.

MICROCODE-UPDATE
Verbesserungen, Optimierungen und Fehlerbehebungen der Microcode-Anweisungen eines Prozessors. Die Möglichkeit, Microcode-Updates einzuspielen, ist ein Vorteil der nicht hartcodierten Befehle bei bestimmten Prozessortypen.

MICROSERVICES (engl.)
Übsg. Mikrodienste. Designwahl bei der Erstellung von Software. Dabei werden komplexe Applikationen in kleinere, unabhängige Applikationen oder Module aufgeteilt, die jeweils eine kleine Aufgabe, einen sog. Dienst, erledigen. Eine Anfrage des Benutzers oder einer anderen Software an die Gesamtapplikation wird dann aufgeteilt in verschiedene Anfragen für die Microservices, und deren Resultate werden zusammengefasst als gemeinsame Antwort zurückgegeben. Durch die Aufteilung in kleinere Module entstehen schlanke, einfach zu optimierende und aktuell zu haltende Teile, anstatt einer großen „monolithischen" Applikation. Die Module können dabei eigene Datenkonzepte und eigene Frontends haben und in unterschiedlichen Programmiersprachen entwickelt werden.

MICROSOFT APPLICATION VIRTUALIZATION [APP-V] (engl.)
Programm zur Virtualisierung von Applikationen. Die Apps werden nicht auf den Clients installiert, sondern vom Server an eine virtuelle Umgebung auf dem Client geliefert und in einer Sandbox auf dem Client ausgeführt.

MICROSOFT AUTHENTICATION APP (engl.)
Authentisierungs-App für 2FA.

MICROSOFT CLOUD APP SECURITY [MCAS] (engl.)
Cloud Access Security Broker (CASB)-Lösung. On-Prem oder cloudbasiertes System, welches Sicherheitsrichtlinien zwischen dem Cloud-Benutzer und dem Cloud-Service-Anbieter ermöglicht und durchsetzt, inkl. Discovery, Verhaltensanalysen, Risikobewertung und Daten- und Bedrohungsschutz. Ein Microsoft Office365 Service.

MICROSOFT EDGE
Webbrowser von Microsoft.

MICROSOFT EXCHANGE ACTIVESYNC [EAS] (engl.)
Protokoll zur Kommunikation über HTTP und HTTPS, um Synchronisation von E-Mails, Kontakten, Kalendern, Aufgaben und Notizen zw. Exchange-Nachrichten-Server und mobilem Gerät zu ermöglichen.

MICROSOFT IDENTITY MANAGER [MIM] (engl.)
Software, um mehrere „On-Prem"-Authentifikationsspeicher, wie Active Directory, LDAP u. a. mit Azure Active Directory zu verbinden. Dies ermöglicht den Benutzern eine einheitliche Erfahrung bei „On-Prem"-Apps und SaaS-Lösungen.

MICROSOFT INFORMATION PROTECTION [MIP] (engl.)
Kombination von Azure Information Protection (AIP) und Office365-Labeling.

MICROSOFT.NET
Syn. zu .NET Framework

MICROSOFT RIGHTS MANAGEMENT (engl.)
Oberbegriff für Microsofts ADRMS (lokale Version) und AzureRMS (cloudbasierend).

MIDDLEWARE (engl.)
Applikation oder System, welches zw. Anwendungen vermittelt. Beispiel: Managed File Transfer (MFT).

MIM
Abk. für Microsoft Identity Manager

MIMIKATZ
Open-Source-Software, welche ursprünglich aufzeigen sollte, wie die Authentisierungsprotokolle von Windows angreifbar sind. Die Software wurde danach aber auch für Attacken wie WannaCry missbraucht. Gleichzeitig bietet diese Software Programmierern die Möglichkeit, ihre Systeme gegen mögliche Attacken zu testen und zu härten.

MINECRAFT
Programm, um spielerisch Landschaften und Objekte dreidimensional aufzubauen.

MINIMUM VIABLE PRODUCT [MVP] (engl.)
Übsg. Minimales Produkt, welches die Anforderungen erfüllt. Bei Software häufig mit der Versionsnummer v1.0 bezeichnet

MINING OF DIGITAL CURRENCY (engl.)
Übsg. Schürfen von digitaler Währung. Berechnen spezieller kryptografischer Algorithmen, um Zahlungen und Transaktionen, die in der digitalen Währung ausgeführt werden, mathematisch zu signieren. Bei Kryptowährungen, welche auf der Blockchain-Technologie basieren, wird durch das Schürfen die Verlinkung der Zahlung mit der bisherigen Hash-Kette („Merkle-Tree“) durchgeführt. Diese Berechnungen werden gleichzeitig von vielen Personen ausgeführt und der schnellste jedes Minings erhält als Gegenleistung für die eingesetzte Arbeit einen Teilbetrag der transferierten und signierten Zahlung.

MIP
Abk. für Microsoft Information Protection

MIRAI
Schadsoftware, welche Linux-Systeme in Webcams, Routers u. Ä. manipuliert, sodass diese ferngesteuert werden können, um bspw. Teil eines Botnetzes zu werden.

MITIGATION OF CYBER THREATS (engl.)
Übsg. Entschärfung von Cyber-Bedrohungen.

MIT-LIZENZ (engl.)
Am Massachusetts Institute of Technology (MIT) entworfene freizügige Open-Source-Lizenz, welche von vielen Programmierern für ihre Software angewendet wird.

MITM
Abk. für Man-in-the-Middle

MITRE ATT&CK
Abk. für Mitre Adversarial Tactics, Techniques and Common Knowledge. Wissensdatenbank über vergangene Angriffstaktiken und -techniken. Dies hilft Firmen, Organisationen und privaten Personen, eigene Abwehrmodelle und -methoden für ihre Systeme und Apps zu entwickeln.

MMC
Abk. für Microsoft Management Console. Tool in Windows, um Details zu vorhandenen Netzwerken, Computern, Diensten oder andere Komponenten aufzuzeigen, bspw. zur Darstellung der festgelegten Group Policy Objects (GPO). Einzelne Zusatzfunktionen, sog. Snap-Ins, können hinzugeladen werden. Gestartet werden kann MMC durch die Angabe von „mmc.exe“ für das allgemeine Tool und bspw. „gpmc.mmc“ für GPOs.

MMS
Abk. für Multimedia Messaging Service

MNIST
Datenbank mit handgeschriebenen Zahlen, die benutzt werden kann, um ein neues Schrifterkennungssystem zu testen. Es beinhaltet 60.000 Trainingsbilder und 10.000 Testbilder, die es zu erkennen gilt.

MOBILE APP (engl.)
Software, welche speziell für mobile Geräte, wie Handy oder Tablet entwickelt wurde.

MOBILE APP SECURITY VERIFICATION STANDARD [MASVS] (engl.)
Richtlinien zur Entwicklung von sicheren Mobile Apps.

MOBILE-BANKING (engl.)
Software zur Abwicklung von Bankgeschäften mittels Handys oder Tablets. Bei einigen Anbietern auch als E-Banking oder Online-Banking bezeichnet.

MOBILE DATEN
Zugang zum Internet über das Mobilfunknetz. Syn. zu Datendienst.

MOBILE SECURE GATEWAY [MSG] (engl.)
Software oder Hardware zur Bereitstellung sicherer Kommunikation über ein Netzwerk zw. einer mobilen App und dem zugehörigen Dienst auf einem Server. Auf dem Gateway können die Anfragen der mobilen App auf Manipulation überprüft werden.

MOBILE SECURITY (engl.)
Teilgebiet der Cyber- und IT-Sicherheit. Ziel ist die Verhinderung von Angriffen, von Missbrauch und von Datenverlust auf oder über mobile Geräte.

MOBILE SECURITY TESTING GUIDE [MSTG] (engl.)
Umfangreiche Anleitung von OWASP für das Testen von Sicherheitsaspekten bei mobilen Apps sowie für das Reverse Engineering von iOS- und Android-Sicherheitsaspekten.

MOBILE TAN VIA SMS [MTAN] (engl.)
Authentisierungsmethode, bei welcher eine TAN per SMS an den Benutzer geschickt wird.

MODEM
Abk. für Modulator und Demodulator. Nicht mehr häufig benutzte Bezeichnung für ein Gerät zw. zwei Computern zur Übertragung von Daten. Dabei werden die Daten beim Senden auf eine Trägerfrequenz aufmoduliert und beim Empfangen demoduliert.

MODS
Abk. für Modifikationen. Kleine Anpassungen von Systemen oder Programmen.

MODSEC
Abk. für Modsecurity

MODSECURITY
Syn. zu „ModSec“. Open-Source-Firewall für Web-Applikationen, mit welcher HTTP-Anfragen und -Antworten auf Risiken überprüft werden können. Geprüft wird bspw. auf

a. das Ausnützen von Schwachstellen, wie Cross-Site-Scripting, SQL-Injection, Command-Injection,
b. verdächtige Stichworte und URLs,
c. misslungene Logins.

MODULE-PROTECTED KEYS (engl.)
Übsg. Modulgeschützte Schlüssel. Einer von drei Arten der Autorisation für den Gebrauch von Schlüsseln in HSMs. Bei Module-Protected Keys werden für den Gebrauch der Schlüssel keine weiteren Autorisationen benötigt. Die anderen zwei Arten sind: Softcard-Protected Keys und Token-Protected Keys.

MONERO
Kryptowährung

MONEY LAUNDRY (engl.)
Übsg. Geldwäscherei. In Umlauf bringen von illegal erhaltenem Geld.

MONEY MULE (engl.)
Übsg. Geldesel. Person, die ihr Bankkonto zur Verfügung stellt, um Geld für jemand anderen darüber zu transferieren und auszuzahlen. Methode der Geldwäscherei.

MONITORING (engl.)
Übsg. Überwachung

MONITORING OF CYBER THREATS (engl.)
Übsg. Überwachen von Cyber-Bedrohungen.

MOOC
Abk. für Massive Open Online Course

MOONSHOT
1) Forschungsabteilung von Google. 2) Serversysteme on Hewlett Packard Enterprise.

MOORE'S GESETZ DER CYBER-ATTACKEN
Die Kosten für eine bestimmte Attacke halbieren sich alle 18 bis 24 Monate, basierend auf der Verdoppelung der Rechengeschwindigkeit in dieser Periode. Durch Fortschritte in der Mathematik können sich die Kosten zusätzlich reduzieren.

MOSAIC
Abk. für NCSA Mosaic. Einer der ersten grafischen Webbrowser aus dem Jahre 1993. Wurde bis 1997 weiterentwickelt und danach durch Netscape Navigator und andere Webbrowser abgelöst.

MQTT
Abk. für Message-Queuing Telemetry Transport. Ein leichtgewichtiges, offenes, einfach zu implementierendes Client-Server-Protokoll für Nachrichtentransport bei Maschine-zu-Maschine-Verbindungen sowie bei Internet der Dinge (IoT)-Netzwerken

mit sparsamer Hardwareausstattung, bei denen keine hohen Datenraten und Geschwindigkeiten benötigt werden. Dabei kommunizieren die Clients und Server nicht direkt, sondern senden und erhalten abonnierte Mitteilungen über eine dritte Partei (sog. Broker).

MS-DOS
Abk. für Microsoft Disk Operating System

MSDRM
Microsofts RMS Client 1.0, welcher Information-Rights-Management-Lösungen ermöglicht, die mit RMS SDK 1.0 entwickelt wurden. MSDRM wurde durch MSIPC (aba. RMS Client 2.0) abgelöst.

MSG
Abk. für Mobile Secure Gateway

MSIPC
Microsofts RMS Client 2.0, welcher Information-Rights-Management-Lösungen ermöglicht, die mit RMS SDK 2.0 entwickelt wurden. MSIPC löste MSDRM (aba. RMS Client 1.0) ab.

MSK
Abk. für Master Secret Key

MSTG
Abk. für Mobile Security Testing Guide

MTAN
Abk. für Mobile TAN via SMS

MTA-STS
Abk. für SMTP MTA Strict Transport Security. Neueres Protokoll zur standardmäßigen Benutzung von TLS-gesicherten Verbindungen bei E-Mail-Transport via SMTP. Zusätzlich erlaubt dieses Protokoll Maßnahmen gegen Manipulation der verschlüsselten SMTP-Verbindung.

MTLS
Abk. für Mutual TLS Authentication

MULTICAST
Kommunikation, die von einem Sender an mehrere Empfänger erfolgt, nachdem sich diese beim Sender angemeldet haben, im Gegensatz zu Unicast und Broadcast (siehe Tab. 15.1).

MULTICAST DNS [MDNS]
Verfahren, bei dem Geräte DNS-Anfragen statt an eine zentrale DNS-Stelle an Multicast-Adressen senden. Geräte im Netzwerk können diese Anfrage beantworten.

MULTI-FACTOR AUTHENTICATION [MFA] (engl.)
Übsg. Multi-Faktor-Authentisierung

MULTI-FACTOR CRYPTOGRAPHIC DEVICE (engl.)
Übsg. Multi-Faktor-Kryptografiegerät. Gerät oder Hardware, welches/welche einen geschützten kryptografischen Schlüssel beinhaltet und nach Aktivierung mittels eines zweiten Authentifizierungsfaktors kryptografische Operationen ausführt. Die Authentisierung des Benutzers wird durch den Besitz des Geräts und des Schlüssels sichergestellt.

Beispiel: Smartcard, YubiKey.

MULTI-FACTOR OTP DEVICE (engl.)
Übsg. Multi-Faktor-Einmal-Passwortgerät. Gerät oder Hardware, welches/welche nach Aktivierung mittels eines zweiten Authentifizierungsfaktors, ein Einmal-Passwort für die Authentisierung des Benutzers erstellt.

Beispiele: Handy mit Authenticator-App, YubiKey.

MULTI-FACTOR SOFTWARE CRYPTOGRAPHIC AUTHENTICATOR (engl.)
Übsg. Multi-Faktor-Software-Kryptografiegerät. Schlüssel, welcher auf einer Festplatte, auf einem USB-Stick u. Ä. gespeichert ist und nach Aktivierung mittels eines zweiten Authentifizierungsfaktors den Benutzer authentisiert.

MULTI-FAKTOR-AUTHENTIFIZIERUNG [MFA]
Syn. zu Multi-Faktor-Authentisierung

Tab. 15.1 Beispiele für Multicast, Broadcast, Unicast

Beispiel für Multicast	Fernsehsendung eines Bezahlsenders
Beispiel für Broadcast	Fernsehsendung eines öffentlich-rechtlichen Fernsehsenders
Beispiel für Unicast	FTP-Verbindung zwischen zwei Computern

MULTI-FAKTOR-AUTHENTISIERUNG [MFA]
Verfahren zur sichereren Anmeldung an Systemen, Online-Diensten, Netzwerken oder Bankautomaten. Dabei wird mehr als ein Faktor („Geheimnis“) verwendet.

Beispiele:

I. Bankkarte und PIN bei Bankautomaten.
II. Username mit Passwort und zusätzlich dem Fingerabdruck zur Anmeldung an einem System.

Viele Online-Dienste bieten Zwei-Faktor-Authentisierung an, welche verwendet werden sollte, wann immer möglich.

Beispiel

Kombinierbare Faktoren für Multi-Faktor-Authentisierung:

a. „Etwas, das man besitzt“, z. B. Bankkarte, Smartcard.
b. „Etwas, das man weiß“, z. B. PIN, Passwort.
c. „Etwas, das darauf beruht, wo man ist“, z. B. das Anmelden am WLAN im Firmengebäude.
d. „Etwas, das darauf beruht, wer man ist“, z. B. Fingerabdruck, Gesichtsform.
e. „Etwas, was man tut“, z. B. die Art des Tippens, die Häufigkeit der App-Benutzung.

MULTI-HOP
1) Datenpaket, welches mehrere Netzwerkrouter durchläuft. Jeder Durchgang durch einen Router entspricht einem Hop. Ein-Time-to-Live (TTL)-Wert bei einer Anfrage, bspw. bei Ping, gibt an, wie viele Router das Paket durchlaufen darf, bevor es als nicht zustellbar erklärt wird. 2) Wechsel eines Benutzers (bspw. Admin) von einem System zum anderen, um das Zielsystem zu erreichen. Bei kritischen Systemen können zur Sicherstellung der Zugriffsrechte Einschränkungen konfiguriert werden, die Zugriffsanfragen nur von bestimmten Systemen aus erlauben. Deshalb muss ein Admin zuerst mit richtigen Anmeldedaten über mehrere Hops von System zu System springen, bis er das System erreicht, von wo der Zugriff auf das Zielsystem erlaubt ist.

MULTIMEDIA MESSAGING SERVICE [MMS] (engl.)
Anfang 2000er-Jahre eingeführter Kurznachrichtendienst, mit welchem im Vergleich zum textbasierten SMS auch Bilder, Videos und andere multimediale Inhalte von Handy zu Handy und zu E-Mail-Adressen versendet werden können.

MULTIPLEXING (engl.)
Fähigkeit eines physischen Quantensystems zur Speicherung mehrerer Photonen als Qubits.

MULTI-SIG SCHEME (engl.)
Übsg. Multisignaturenschema. Ein System, welches mehrere kryptografische Schlüssel zur Authentifikation verlangt. Bei Kryptowährungen können Multisignaturenschemata eingesetzt werden, um zwingend mehrere Schlüssel für eine Transaktion einsetzen zu müssen.

MULTI-TENANT (engl.)
Übsg. Mehrere Mieter. Bei mandantenfähigen Software- oder Cloud-Lösungen bezieht eine Gruppe von Personen einen Tenant zum gemeinsamen Zugriff.

MULTI-TIER ARCHITECTURE (engl.)
Übsg. Mehrschichtige Architektur. Separate Betrachtung und Bearbeitung einzelner gleicher oder gleichwertiger Teile („Schichten“) eines Systems. Bspw. spricht man von einer 3-Tier-Architektur, wenn die Anwendungsschicht, die Domänenschicht und die Datenschicht einzeln bearbeitet werden.

MURAENA
Schadsoftware zur Ausführung von automatischen Phishing-Attacken.

MUSTER
1) Darstellungs-, Speicherungs- oder Klassifizierungsart von Objekten. 2) Fingerbewegungen auf einem Touchbildschirm als „Geheimnis“ bei der Anmeldung an Handys und PCs. Diese Anmeldeform kann zusätzlich oder anstatt eines PINs oder Passworts gewählt werden. Dabei wird die Bewegung des Fingers über einem Bild oder über einem Buchstaben- oder Zahlenfeld verglichen mit einem gespeicherten Muster im Benutzerkonto. Das Login mittels Muster gilt als unsicher, da auf dem Handydisplay leicht zu erkennen ist, wo häufig getippt wird, und die Bewegungen des Fingers auch von weitem noch einfach auszuspähen sind.

MUTUAL AUTHENTICATION (engl.)
Übsg. Gegenseitige Authentisierung. Wird bei einigen Verfahren der Kommunikation zwischen zwei Parteien eingesetzt, z. B. PC-zu-PC oder Client zu Server. Bei TLS ist Mutual Authentication optional möglich, aber eher selten verwendet, sodass meist nur der Server sich mit seinem Zertifikat gegen die Clients authentisiert, aber der Aufwand groß wäre, für alle Clients ebenso ein Zertifikat bereitzustellen, um sich gegenüber dem Server zu authentisieren. Bei Verbindungen zwischen zwei Firmen über TLS oder bei Verbindungen über SSH wird Mutual Authentication meist als Standardverfahren eingesetzt.

MUTUAL CLIENT AUTHENTICATION (engl.)
Übsg. Gegenseitige Authentisierung zwischen Client und Server. Beide Parteien authentisieren sich gegenseitig durch ihr Zertifikat.

MUTUAL TLS AUTHENTICATION [MTLS] (engl.)
Übsg. Gegenseitige TLS-Authentisierung. Beide Parteien kommunizieren dabei verschlüsselt über TLS und authentisieren sich gegenseitig durch ihr Zertifikat. Eher für Business-zu-Business-Applikationen eingesetzt als für Client-Server-Verbindungen, wo meist nur der Server sich mit seinem Zertifikat gegen die Clients authentisiert, aber der Aufwand groß wäre, für alle Clients ebenso ein Zertifikat bereitzustellen, um sich gegenüber dem Server zu authentisieren.

MVP
Abk. für Minimum Viable Product

MYDOOM
Computer-Wurm, der 2004 entdeckt wurde und Microsoft Windows PCs angreift. Diese Schadsoftware wird meist via ausführbaren E-Mail-Anhang übertragen und sendet nach der Infektion des PCs eine weitere verseuchte E-Mail an alle E-Mail-Adressen des Adressbuchs. Mydoom installiert außerdem ein Backdoor, um die PCs fernzusteuern, und verhindert das Einspielen von Updates für Microsoft Windows und für Anti-Viren-Programme.

MYSPACE
Soziales Netzwerk, welches 2003 entstand.

N

16

NACHRICHT
Jede Form von Daten, die für einen oder mehrere Empfänger vorbereitet und mit geeigneten Mitteln transportiert werden.

NACL
1) Abk. für Networking and Cryptography Library. 2) Abk. für Natriumchlorid, aba. Kochsalz.

NAE
Abk. für Network Assurance Engine von Cisco

NAS
Abk. für Network Attached Storage

NAT
Abk. für Network Address Translation, Übsg. Netzwerkadressübersetzung. NAT wird zur gewollten Maskierung und Änderung von IP-Adressen verwendet mit dem Ziel der Trennung von internen und externen Netzen. Bspw. werden die IP-Adressen eines privaten WLAN-Netzes übersetzt, damit eine Adressierung und Kommunikation über einen Router zum Internet erfolgen kann.

NATIONAL CYBER SECURITY CENTRE [NCSC] (engl.)
Übsg. Nationales Cyber-Sicherheitszentrum. Mehrere Länder betreiben nationale Organisationen zur Beratung und Unterstützung von öffentlichen und privaten Institutionen und Firmen mit dem Ziel der Verhinderung von Cyber- und IT-Sicherheitsattacken. Solche

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z*,
https://doi.org/10.1007/978-3-662-60911-8_16

Sicherheitszentren werden u. a. betrieben in Großbritannien, Niederlande, Irland, Deutschland, Litauen u. a.

NATIONALE STRATEGIE ZUM SCHUTZ DER SCHWEIZ VOR CYBER-RISIKEN [NCS]
Von Schweizer Bundesdepartementen und -amtsstellen dezentral bereitgestellte Empfehlungen zu Cyber- und IT-Sicherheitsanforderungen und -Implementationen.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [NIST] (engl.)
Bundesbehörde der USA zur Festlegung von Standards, Richtlinien und anderen Vorgaben, wie bspw. die Verschlüsselungsalgorithmen DES und AES sowie die SHA-Hash-Funktionen.

NATIONAL SECURITY AGENCY [NSA] (engl.)
Übsg. Nationale Sicherheitsbehörde. Größter Auslandsgeheimdienst der Vereinigten Staaten.

NATION STATE ACTOR (engl.)
Hacker, der seine Aktivitäten im Auftrag oder zugunsten eines Staates durchführt.

NATURAL LANGUAGE PROCESSING [NLP] (engl.)
Übsg. Verarbeitung natürlicher Sprache. Eine Anwendung der künstlichen Intelligenz.

NAVIGATOR GROUP
Hacking-Gruppe

NCIPHER NSHIELD
HSM-Produktreihe der Firma nCipher. Damit lassen sich sichere Schlüssel erzeugen, speichern und schützen und bspw. im Zusammenspiel mit Azure Key Vault verwenden.

NCS
Abk. für nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken.

NCSC
Abk. für National Cyber Security Centre

NEAR FIELD COMMUNICATION [NFC] (engl.)
Übsg. Nahfeldkommunikation. Datenübertragung auf kurze Distanzen mittels elektromagnetischer Induktion. Viele Handys, Bank- und Kreditkarten sowie Bezahlsysteme wurden in den 2010er-Jahren mit NFC ausgestattet, sodass Kleinbeträge bis ca. 80 CHF / 50 € ohne PIN und kontaktlos über NFC bezahlt werden können. Andere

Anwendungen sind die kontaktlose Zwei-Faktor-Authentisierung oder die Zugangskontrolle bei Gebäuden.

NEED TO KNOW (engl.)
Übsg. Nötig-zu-wissen. Prinzip bei der Vergabe von Zugriffsrechten, sodass die Zugriffe einer Person auf eine bestimmte Ressource nur dann erteilt werden, wenn dies für deren aktuelle Tätigkeit nötig oder wichtig ist.

.NET
1) Syn. zu dot.Net, Microsoft.NET. Software-Entwicklungsplattform und -tools für Microsoft-Produkte und Windows-Apps. 2) Eine der ersten Top-Level-Domains. Diese wurde 1985 erstellt und war ursprünglich als Abkürzung für „Network“ gedacht.

NETBIOS
Abk. für Network Basic Input Output System

NETBIOS OVER TCP/IP (engl.)
Netzwerkprotokoll zur Verwendung von NetBIOS über TCP/IP.

NETFLIX
Video-Streaming-Dienst

NET KEY V3
Zertifikatstyp basierend auf Smartcards.

NETSCAPE
Abk. für Netscape Navigator. Einer der ersten grafischen Webbrowser, welcher als Nachfolger von Mosaic erstellt und zwischen 1994 und 2008 weiterentwickelt wurde. Zeitweise erreichte dieser Webbrowser einen Marktanteil von fast 80 Prozent.

NETWORK ASSURANCE ENGINE [NAE] (engl.)
Von Cisco entwickeltes System, welches den aktuellen oder zukünftigen Zustand eines Netzwerks mathematisch überprüft, sodass Ausfälle oder Angriffe verhindert werden können und das Netzwerk in der erwarteten Weise funktioniert.

NETWORK ATTACHED STORAGE [NAS] (engl.)
Übsg. am Netzwerk angehängter Speicher. Syn. zu Netzwerkspeicher.

NETWORK BASIC INPUT OUTPUT SYSTEM [NETBIOS] (engl.)
Programmfunktionen (API) zur Kommunikation zw. Programmen in einem lokalen Netzwerk.

NETWORK FILE SYSTEM [NFS] (engl.)
Übsg. Netzwerkdateisystem. Protokoll auf Unix-Systemen, um den Zugriff auf Dateien in Speichermedien über ein Netzwerk zu ermöglichen, sodass die Speichermedien bei den Computern der Benutzer wie lokale Festplatten erscheinen. Bei Windows-Systemen kann dafür SMB (Server Message Block) verwendet werden.

NETWORK HARDENING (engl.)
Übsg. Netzwerkhärtung. Methoden, Systeme und Software zur Erhöhung der Sicherheit des Netzwerks. Dies kann bspw. mithilfe von Firewalls, VPN, Schließung von Netzwerk-Ports u. Ä. erfolgen.

NETWORK HSM (engl.)
Netzwerk-HSM, welches nicht direkt mit einem physischen Kabel an einen Server angeschlossen ist, sondern vom Server über das Netzwerk angesprochen wird.

NETWORK LEVEL AUTHENTICATION [NLA] (engl.)
Übsg. Authentisierung auf dem Netzwerklevel. Sicherheitsmethode für den Fernzugriff auf andere Systeme (via RDS, RDP). Bei dieser Methode erfolgt die Authentisierung vor dem Aufbau der Verbindung mit dem entfernten System und kann damit bspw. DoS-Attacken verhindern.

NETWORKING AND CRYPTOGRAPHY LIBRARY [NACL] (engl.)
Übsg. Netzwerk und kryptografische Bibliothek. Funktionen zur Programmierung schneller kryptografischer Berechnungen für Netzwerkkommunikation, Verschlüsselung, Entschlüsselung und Signatur. Ziel von NaCl ist jede Netzwerkverbindung kryptografisch zu schützen und so eine starke Vertraulichkeit, Integrität und Verfügbarkeit auf dem neuesten Stand der Technik zu gewährleisten, damit Angreifer keine Netzwerkpakete abfangen oder ändern können.

NETWORK PERIMETER SECURITY (engl.)
Übsg. Netzwerksicherheitsbereich. Schutzmaßnahmen, die nicht direkt im System ansetzen, sondern in der Peripherie oder Umgebung des Systems.

Beispiele sind Firewalls, Jump-Server, Fernzugriff.

NETWORK SECURITY (engl.)
Übsg. Netzwerksicherheit. Teilgebiet der Cyber- und IT-Sicherheit. Ziel ist die Verhinderung von Angriffen und der Missbrauch des Netzwerks und somit der Schutz vor Schädigung angehängter Systeme und enthaltener Daten.

NETWORK SNIFFER (engl.)
Übsg. Netzwerkschnüffler. Syn. zu Packet Sniffer. Hardware oder Software, mithilfe dessen die Netzwerkkommunikation mitgehört, aufgezeichnet und analysiert werden

kann. Dies kann zur Überprüfung des eigenen Netzwerks oder Systems eingesetzt werden, wird jedoch auch von Hackern missbraucht.

NETZWERK
Syn. zu Netz. Zusammenschluss von Einheiten, wie PCs, Telefonen, Funknetzantennen, Sensoren, elektrischen Bauteilen usw., welche miteinander verbunden sind und sich mithilfe von Regeln organisieren lassen. Die Elemente eines Netzwerks werden Knoten, Knotenpunkte, oder Verzweigungen genannt. Eine Kante eines Netzwerks ist die Verbindung zw. zwei Knoten. Ein geschlossener Kreis, gebildet aus Kanten und Knoten, wird als Masche bezeichnet.

NETZWERKSPEICHER
Am Netzwerk angehängter Speicher, welcher eigenständig, d. h. ohne zusätzlichen Steuerungs-PC, im Netzwerk arbeitet und kommuniziert und welcher verschiedenen Teilnehmern des Netzwerks zur Verfügung gestellt wird, sodass dieser Speicher von den Benutzern wie eine lokale Festplatte verwendet werden kann.

NEURAL NETWORKS (engl.)
Übsg. Neuronale Netze

NEURONALE NETZE
Abk. für Künstliche Neuronale Netze. Eine mathematische Berechnungsmethode im Themenkreis der künstlichen Intelligenz, angelehnt an biologische neuronale Netze im Gehirn. Das Ziel eines neuronalen Netzes ist die Lösung einer vorgegebenen Aufgabe mithilfe vorher erlernter Daten, bspw. das Erkennen einer Katze in einem Bild. Alle Eingangssignale (Eingabewerte) an einem sog. Neuron (Knotenpunkt) des Netzes werden mittels Berechnungen zu einem Ausgangssignal dieses Neurons. Dieses Ausgangssignal dient wiederum als Eingangssignale für andere verbundene Neuronen. Einige Teile der Berechnungen (die sog. Gewichte) sind dabei nicht starr vorgegeben, sondern veränderbar. Mithilfe von Trainingsdaten, welche als Eingangssignale dienen und bei denen die Ausgangssignale nach allen Berechnungen innerhalb des Netzes bewertet werden, können die dynamischen Gewichte festgelegt werden (sog. „Lernen“), und damit kann erreicht werden, dass die vorgegebene Aufgabe auch bei neuen Daten als Eingangssignale die optimalsten Ausgangswerte liefert.

Beispiel: Die Farbwerte jedes Pixels von vorliegenden Bildern mit und ohne Katzen können als Trainingsdaten in das neuronale Netz eingegeben werden. Die Ausgangswerte der Berechnungen jedes Bildes lassen sich gegen die Kenntnis, ob eine Katze darauf abgebildet ist oder nicht, vergleichen und die Gewichte der Berechnungen entsprechend anpassen, sodass die Trainingsdaten möglichst häufig richtig erkannt werden. Danach kann dieses trainierte neuronale Netz benutzt werden, um bei neuen Bildern automatisch zu entscheiden, ob eine Katze abgebildet ist oder nicht (siehe Abb. 16.1 und 16.2).

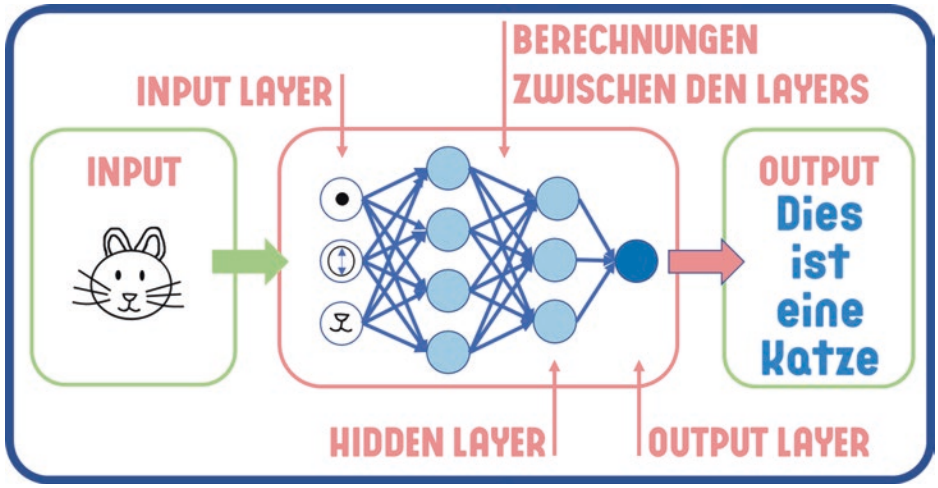

Abb. 16.1 Begriffe im Zusammenhang mit neuronalen Netzen

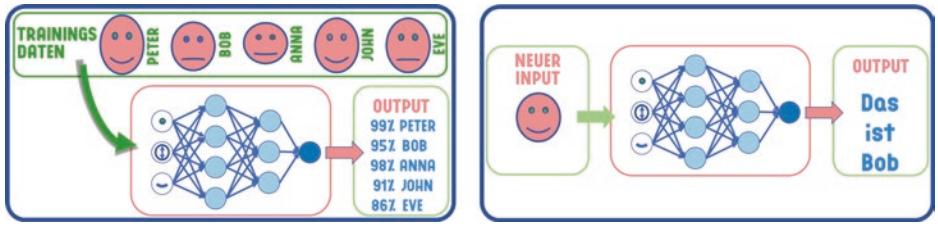

Abb. 16.2 Lernverfahren bei neuronalen Netzen

NFC
Übsg. Near Field Communication

NFR
Abk. für Non-Functional-Requirement. Übsg. Nicht-funktionale Anforderung an ein System. Bspw. die Reaktionszeit des Systems auf eine Aktion des Benutzers.

NFS
Abk. für Network File System

NIC
Abk. für Network Information Center. Vergabestelle von Domainnamen.

NICEHASH
Marktplatz, um Kryptowährungsminer (Übsg. Kryptowährungsschürfer) und Kryptowährungskäufer zusammenzubringen.

NICKNAME (engl.)
Übsg. Spitzname, Kurzname. In Online-Diensten verwendeter Name für einen Benutzer, um die Bekanntgabe des echten Namens zu umgehen.

NIST
Abk. für National Institute of Standards and Technology

NIST CYBERSECURITY FRAMEWORK (engl.)
Von NIST publiziertes Dokument, welches Firmen mit Vorgaben, guten Beispielen und Analysetools unterstützen kann, um die Cybersecurity-Risiken zu managen und damit die Firma nicht nur auf angemessene Reaktionen nach Cyber-Attacken vorzubereiten, sondern solche zu verhindern.

NIST FRAMEWORK CORE (engl.)
Für Firmen bereitgestellte Analysevorgaben und Empfehlungen zur Umsetzung von Cybersecurity gemäß dem „NIST Cybersecurity Framework".

NIST FRAMEWORK PROFILE (engl.)
Aktueller Stand und Pläne einer Firma bzgl. der Umsetzung der Cybersecurity-Empfehlungen gemäß „NIST Cybersecurity Framework".

NIST FRAMEWORK TIER (engl.)
Maturitätslevel einer Firma bzgl. des Risikomanagements und Cybersecurity-Schutzes gemäß „NIST Cybersecurity Framework".

NIST-SP-800-53
NIST-Sonderpublikation, welche einen Katalog von Sicherheitskontrollen für Informationssysteme bietet, insb. bzgl. des Risikomanagements. Diese Kontrollen sind die für ein Informationssystem empfohlenen verwaltungs-, betrieblichen und technischen Schutzmaßnahmen zum Erhalt der Vertraulichkeit, Integrität und Verfügbarkeit des Systems und seiner Informationen.

NODE (engl.)
Übsg. Knoten. Ein Server innerhalb eines Clusters von Servern.

NODE.JS
Programmierumgebung, mit deren Hilfe Programme auf Servern entwickelt und ausgeführt werden können. Die Programme werden dabei in der JavaScript-Laufzeitumgebung betrieben. U. a. lassen sich damit einfach Webserver entwickeln.

NONCE
Nummer, die nur einmal verwendet wird. Meist ist dies eine Zufallszahl und wird für kryptografische Berechnungen benutzt.

NOSQL
Abk. für „Not only SQL“. Datenbankstruktur, die nicht relational aufgesetzt ist. Wird auch „strukturierter Datenspeicher“ genannt. Im Gegensatz zu relationalen Datenbanken mit Tabellen nutzen NoSQL-Datenbanken Wertepaare, Objekte, Dokumente und Listen.

NOTPETYA
Familie von verschlüsselnder Erpressungsschadsoftware (Ransomware), die Microsoft-Windows-Systeme scheinbar ähnlich angreifen wie der Petya Erpressungstrojaner, jedoch eher zum Ziel haben, Chaos zu verursachen als eine Erpressung. Entdeckt 2017.

NSA
Abk. für National Security Agency

NSA-CHIFFRE SPECK
Eine Blockchiffre, welche von NSA entwickelt wurde und auch bei schwachen CPUs effizient implementiert werden kann.

N-TIER ARCHITECTURE (engl.)
Abk. für Multi-Tier Architecture, Übsg. Mehrschichtige Architektur.

NTLM
Abk. für NT LAN Manager. Authentisierungsverfahren, ursprünglich von Microsoft. Dabei wird der Benutzername vom Client an den Server geschickt, auf dem sich der Benutzer früher bereits registriert hat. Der Server schickt daraufhin eine Zufallszahl zum Client. Nun kann der Client das Passwort des Benutzers verwenden, um diese Zufallszahl zu verschlüsseln und zum Server zu schicken. Schließlich vergleicht der Server diesen Wert mit demjenigen, den dieser selber mit dem früher gespeicherten Passwort des Benutzers und der Zufallszahl berechnet.

NUISANCE (engl.)
Übsg. Belästigung, Missstand, Beeinträchtigung.

NUTZDATEN

Syn. zu Payload. Teil eines transportierten Datenpakets bei einer Kommunikation zw. zwei Parteien, welcher die eigentlichen Daten enthält. Die Nutzdaten werden unterschieden von Metadaten, welche Steuer- und Protokollinformationen beinhalten und gleichzeitig mitgeschickt werden.

O

17

O365
Abk. für Office365

OATH
Abk. für Open Authentication

OAUTH
Abk. für Open Authorization

OBFUSCATION (engl.)
Übsg. Verschleierung, Verwirrung. Bei vielen Software-Entwicklungsplattformen kann Obfuscation gewählt werden, sodass vor dem Kompilieren die für Menschen verständlichen Variablen- und Methodennamen in Bezeichnungen umgewandelt werden, die für Menschen nicht mehr verständlich sind, um damit das Reverse Engineering der Software zu erschweren.

OBJECT LINKING AND EMBEDDING [OLE] (engl.)
Methode innerhalb Windows, um die Zusammenarbeit zwischen OLE-fähigen Programmen zu ermöglichen, sodass bspw. eine Excel-Tabelle mittels Copy & Paste in ein Word-Dokument übernommen werden kann. Dabei wird entweder eine Verknüpfung (Linking) zur Original-Excel-Datei erstellt oder die Excel-Tabelle vollständig eingebettet (Embedding).

OBJEKTORIENTIERTE PROGRAMMIERUNG [OOP]
Methode der Software-Entwicklung, bei der das Programm nicht rein prozedural, d. h. durch Hintereinanderreihung von Befehlen erstellt wird, sondern mithilfe von sog.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_17

Klassen, Objekten und Vererbung strukturiert wird. Dies entspricht häufig eher der Realität, wenn bspw. in einem Spiel Autos vorkommen sollen und dafür die Klasse „Auto“ programmiert wird, mit Eigenschaften wie Farbe, Größe, Anzahl der Räder, maximaler Geschwindigkeit usw., sodass danach jedes im Spiel benötigte (instanziierte) Auto als neues Objekt dieser Autoklasse erstellt werden kann, welches dieselben Eigenschaften, Methoden und Funktionen dieser „Auto“-Klasse erbt.

Beispiele für objektorientierte Programmiersprachen: Java, C++

OCR
Abk. für Optical Character Recognition

OCSP
Abk. für Online Certificate Status Protocol

OCS-PROTECTED
Abk. für Operator Cardset Protected. Methode zum Schutz und zur Bereitstellung von HSM-Schlüsseln, bei welcher es Apps erlaubt ist, auf die HSM-Schlüssel zuzugreifen, auch nachdem das Operator Cardset aus dem HSM-Kartenleser entfernt wurde. Dies wird v. a. bei netzwerkbasierten HSMs konfiguriert, damit mehrere Apps damit arbeiten können.

ODFB
Abk. für OneDrive for Business. Ein Microsoft Office365-Service.

OEM
Abk. für Original Equipment Manufacturer. Übsg. Originalausrüstungshersteller.

OFB
Abk. für Output Feedback Mode. Ein Blockchiffre-Modus.

OFFENLEGUNG VON INFORMATION
Syn. zu Disclosure of Information. Übergabe, Freigabe oder Publikation von Informationen aufgrund richterlicher Anordnung oder anderer Gründe.

ÖFFENTLICHER SCHLÜSSEL
Einer der zwei Schlüssel eines asymmetrischen Kryptosystems, bei welchem ein öffentlicher und ein mathematisch zugehöriger privater Schlüssel gleichzeitig erzeugt werden. Der öffentliche Schlüssel kann auf öffentlich zugänglichen Servern gespeichert werden und zur Verschlüsselung von Informationen für den Besitzer des privaten Schlüssels verwendet werden.

OFFICE365 [O365]
Produkt der Firma Microsoft, welches je nach eingesetzter Lizenz die Applikationen Word, Excel, PowerPoint, Outlook, MS Access u. a. beinhaltet und ein Konto bei Microsoft voraussetzt. Sicherheits- und Funktionsupdates werden regelmäßig eingespielt.

OFFICE365-LABELING
Funktion in Office365, um Dokumente und E-Mails mit bestimmten Attributen zu kennzeichnen und darauf aufbauend Aktionen an den Dokumenten und E-Mails auszuführen. Dies kann bspw. eine Aufbewahrungsfrist sein oder ein zukünftiges Datum, an welchem die Datei automatisch gelöscht wird.

OFFICE MACRO (engl.)
Übsg. Office Makro. Software zur Automatisation innerhalb von Microsoft Office und anderer Office-Produkten. Makros können hilfreich sein, bspw. zur wiederholten Ausführung ähnlicher Berechnungen oder zur Ergänzung der bereits vorhandenen Funktionen. Ebenso lassen sich damit rasch und einfach Aktionen auf dem PC programmieren. Bei Microsoft Office Makros wird Visual Basic als Programmiersprache eingesetzt. Aufgrund der weitreichenden Möglichkeiten und Systemrechte werden Office Makros auch für Schadsoftware missbraucht.

OFFICE MESSAGE ENCRYPTION (engl.)
Übsg. Office-Nachrichtenverschlüsselung. Eine Funktion für Azure Rights Management innerhalb Office365 zur Verschlüsselung von Nachrichten für interne und externe E-Mail-Empfänger.

OFF-PREM (engl.)
Abk. für „Off-Premise“, „Off the Premises“. Übsg. Außerhalb des Hauses.

OFF-PREMISE (engl.)
Abk. für „Off the Premises“. Übsg. Außerhalb des Hauses. Firmensysteme, wie Firmenhandy, Firmen-PCs oder Cloud-Systeme, die außerhalb der Firmengebäude benutzt werden. Off-Prem-Systeme werden als unsicherer angesehen im Vergleich zu On-Prem-Systemen, da Benutzer unsichere Geräte und ungeschützte Netzwerke für die Verbindung zur Firma verwenden, und somit Man-in-the-Middle-Attacken u. Ä. möglich sind.

OIDC
Abk. für OpenID Connect

OLE
Abk. für Object Linking and Embedding

OMG
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „Oh my God“, Übsg. „Oh, mein Gott“.

ON-CLOUD (engl.)
Abk. für „On the Cloud“. Systeme, die in der Cloud, also auf verteilten, oft firmenfremden Systemen benutzt werden. Eine firmeninterne Cloud kann sorgfältig überwacht und geschützt werden, wohingegen externe Clouds neben vielen Vorteilen immer auch Risiken besitzen, da der Datenschutz, die Zugriffsbeschränkung, die Ausfallwahrscheinlichkeit u. Ä. dem Cloud-Provider anvertraut werden muss. Um das Risiko zu vermindern, können die Daten vor dem Hochladen zur Cloud verschlüsselt werden, wobei der Schlüssel in der eigenen Firma geheim und geschützt aufbewahrt werden kann.

ONEDRIVE
Abk. für Microsoft OneDrive. Ein Online-Datenspeicherdienst, um Dateien via Webbrowser oder Apps von verschiedenen Geräten aus hochzuladen, zu bearbeiten und darauf zuzugreifen.

ONEDRIVE FOR BUSINESS [ODFB] (engl.)
Ein Microsoft Office365-Service zur zentralen Speicherung von Daten in der Cloud.

ONE-TIME-PAD [OTP] (engl.)
Übsg. Einmal-Schlüssel, Einmal-Block. Schlüssel, der gleich lang ist wie die Nachricht und nur einmal benutzt wird. Zu unterscheiden von One-Time-Password, welches auch mit OTP abgekürzt wird.

ONE-TIME-PASSWORD [OTP] (engl.)
Übsg. Einmal-Kennwort. Zu unterscheiden von One-Time-Pad, welches auch mit OTP abgekürzt wird.

ONE-WAY FUNCTIONS (engl.)
Übsg. Einweg-Funktionen. Syn. zu Falltürfunktionen, Trapdoor Functions. Mathematische Berechnungen, die einfach auszuführen sind, aber Ergebnisse liefern, welche schwierig zurückzurechnen sind. Solche Funktionen werden bei der Berechnung von asymm. Verschlüsselungen verwendet. Dabei werden zwei große Primzahlen miteinander multipliziert. Das dadurch erhaltene Produkt lässt sich nur mit sehr großem Aufwand wieder in die zwei Primzahlen zerlegen.

ONLINE-BANKING (engl.)
Abk. für Bankgeschäfte über das Internet. Syn. zu E-Banking, eBanking, Mobile-Banking.

ONLINE CERTIFICATE STATUS PROTOCOL [OCSP] (engl.)
Spezifikationen und Verfahren zur Prüfung von X.509-Zertifikaten bei Validierungsstellen, bevor diese Zertifikate für TLS, Verschlüsselung von E-Mails oder zur Identifizierung von Kommunikationspartnern benutzt werden.

ONLINE-GAMES (engl.)
Spielprogramme, die Benutzer weltweit über das Internet gemeinsam, als Verbündete oder Gegner, spielen. Die Benutzer haben häufig auch die Möglichkeit, gegenseitig Chatnachrichten zu senden, oder mit Mitspielern via Mikrofon und Kopfhörer zu sprechen.

ON-PREM (engl.)
Abk. für „On-Premise“, „On the Premises“. Übsg. Innerhalb des Hauses.

ON-PREMISE (engl.)
Abk. für „On the Premises“. Übsg. Innerhalb des Hauses. Firmensysteme, die innerhalb der Firmengebäude benutzt werden. On-Premise ist die sicherere Methode im Vergleich zu Off-Premise, da hauseigene Geräte und Netzwerke benutzt werden, die man sorgfältig überwachen und schützen kann.

OOB
Abk. für Out-of-Band. Übsg. Aus der Reihe fallend, gesondert betrachtet.

OOBA
Abk. für Out-of-Band Authentication

OOO
In SMS, Internet-Kommentaren, Internet-Foren, E-Mails und in sozialen Medien benutzte Abk. für „Out-of-Office“, Übsg. „Nicht im Büro“.

OOP
Abk. für Objektorientierte Programmierung

OPCODE
Codierung der Prozessorbefehle als Nummern.

OPEN AUTHENTICATION [OATH] (engl.)
Initiative zur Vereinfachung der Implementation und Verwendung von Zwei-Faktor-Authentisierung, ähnlich wie U2F.

OPEN AUTHORIZATION [OAUTH] (engl.)
Offener Standard für API-Autorisierung. Dabei kann ein Autorisierungscode (Token) bei einer App A erstellt werden, welcher verwendet werden kann, um Benutzern einer App B den Zugriff auf Daten der App A zu erlauben, ohne die Notwendigkeit, die Passwörter mitschicken zu müssen.

OPENID CONNECT [OIDC] (engl.)
API für REST-Applikationen, zur Authentifizierung von Identitäten aufbauend auf dem Autorisierungsprotokoll OAuth2.0. OpenID Connect ermöglicht es Clients, die Identität des Benutzers anhand der von einem Autorisierungsserver durchgeführten Authentifizierung zu überprüfen und grundlegende Profilinformationen über den Benutzer abzurufen.

OPENPGP
Kryptografiefunktionen und standardisiertes Datenformat für verschlüsselte und digital signierte Daten, welches von PGP eingeführt wurde und in RFC4880 spezifiziert ist.

OPEN-SOURCE (engl.)
Übsg. Quelloffene Software. Meist kostenlose Software, bei welcher der Programmcode (sog. Quelltext) öffentlich von jedermann im Detail eingesehen, geändert, angepasst und genutzt werden kann. Autoren von Open-Source Software können die Benutzung jedoch auch einschränken. Häufig, aber nicht immer ist Open-Source deckungsgleich mit „freier Software“, bei welcher Programme ohne Lizenz und Einschränkung benutzt, verändert oder weitergegeben werden dürfen. Open-Source-Software gibt es bereits, seit es Computer gibt (ca. 1940) und wurde in den 1990er-Jahren häufig als „Public Domain“ Software bezeichnet, z. T. mit leicht anderen Benutzungsrechten. Da bei Open-Source jede Codezeile öffentlich ist und deshalb mehrfach unabhängig geprüft wird, werden Hintertüren und Überwachungsalgorithmen schnell erkannt, wodurch Open-Source-Programme bzgl. Datensicherheit als sicherer gelten als (proprietäre) Software, die von Firmen bereitgestellt oder verkauft wird, ohne Möglichkeit der genauen Einsichtnahme. Andererseits bedarf der Einsatz von Open-Source-Software vielfach IT-Kenntnisse, die über die reine Benutzung hinausgehen, da bei solchen Programmen keine Firma mit ihrem guten Ruf dahintersteht und den Benutzern einen guten Service und eine gute Bedienbarkeit ermöglichen möchte. Auch muss die Open-Source-Software meist im Internet besorgt werden, wobei dubiose Internetseitenbetreiber den Personen, die Open-Source-Software herunterladen möchten, Malware oder kostenpflichtige Services unterjubeln können. Open-Source-Software ist heutzutage bei Firmen und Privatpersonen weitverbreitet und etabliert. Beispiele sind Internetbrowser, Programmiersprachen, Verschlüsselungsprogramme, Bürosoftware, Betriebssysteme usw.

OPENSSH
Programme für Fernzugriff und Dateiübertragung basierend auf Secure Shell (SSH).

OPENSSL
Open-Source-Software, die auf vielen Servern zum Standard wurde, um SSL/TLS-Protokolle umzusetzen, um Verschlüsselungs- und Entschlüsselungsfunktionen anzubieten, um X.509-Zertifikate zu erstellen und zu verwalten, sowie zur Erzeugung von privaten und öffentlichen Schlüsseln. Auch lassen sich damit S/MIME-verschlüsselte oder -signierte E-Mails bearbeiten sowie RSA benutzen. Viele OpenSSL-Funktionen werden ohne grafische Benutzeroberfläche in einer Konsole durchgeführt. Auch in vielen kommerziellen Softwareprodukten wird auf OpenSSL aufgebaut. Aufgrund der weltweiten Verbreitung von OpenSSL können Sicherheitslücken darin folgenschwere Konsequenzen haben, wie dies beim Heartbleed Bug in den Jahren 2012 bis 2014 der Fall war.

OPERA
Von Opera Software entwickelter Webbrowser für viele Plattformen.

OPERATING SYSTEM [OS] (engl.)
Übsg. Betriebssystem

OPTICAL CHARACTER RECOGNITION [OCR] (engl.)
Übsg. Optische Zeichenerkennung. Methoden und Programme zur Erkennung von Zeichen, Texten und Bildern in einem Bild. OCR wird bspw. für gescannte Dokumente eingesetzt, um Texte herauszulesen.

OPT-IN (engl.)
Übsg. Ausdrückliche Zustimmung. Beispiel: Einige Online-Dienste und Webbrowser bieten die Möglichkeit an, gezielte Werbung anzuzeigen, sofern der Benutzer dieser Einstellung ausdrücklich zustimmt.

OPT-OUT (engl.)
Übsg. Ausdrückliche Ablehnung. Beispiel: Einige Online-Dienste und Webbrowser bieten die Möglichkeit an, weniger Daten des Benutzers zu sammeln, sofern der Benutzer diese Datensammelfunktion ausdrücklich ablehnt.

ORACLE JROCKIT JVM
Java Virtual Machine innerhalb der Oracle Fusion Middleware.

ORIGINAL EQUIPMENT MANUFACTURER [OEM]
Übsg. Originalausrüstungshersteller

OS
Abk. für Operating System

OSI-SCHICHTENMODELL
Abk. für Open Systems Interconnection Model. Beschreibung der verschiedenen technischen Schichten bei der Kommunikation zwischen Systemen, wobei jede Schicht eine bestimmte Aufgabe erfüllt und eigene Funktionen und Protokolle besitzt (siehe Tab. 17.1).

OS SECURITY (engl.)
Abk. für Operating System Security. Übsg. Betriebssystemsicherheit. Teilgebiet der Cyber- und IT-Sicherheit. Ziel ist die Verhinderung von Angriffen, Missbrauch und Datenverlust, welche aufgrund von Schwächen im Betriebssystem möglich wären.

OTP
1) Abk. für One-Time-Password. 2) Abk. für One-Time-Pad.

OUTLOOK WEB ACCESS [OWA]
Microsoft-Produkt, mit welchem ein Outlook-Konto über einen Webbrowser statt in der Outlook-App angezeigt und benutzt wird.

OUT-OF-BAND AUTHENTICATION [OOBA] (engl.)
Übsg. Gesonderte Authentisierung. 2FA-Methode, bei der für die Authentifizierung eines Benutzers zwei verschiedene Validierungen über zwei verschiedene Kanäle durchgeführt werden. Ziel ist es, dadurch viele Arten von Betrug und Hacking zu verhindern. Mögliche Authentifizierungsverfahren dafür sind bspw. Benutzername und Passwort zusammen mit einem One-Time-Password in einem Authenticator, mit einer Sicherheitszahl via E-Mail oder mit einem per SMS zugeschickten Code.

Tab. 17.1 OSI-Schichtenmodell

Schicht	Bereich	Funktion, die in der Schicht ausgeführt wird
1. Schicht	Bit-Übertragung	Umwandlung der Bits in ein Signal und physikalische Übertragung
2. Schicht	Sicherung	Paketesegmentierung in Frames und Hinzufügen von Prüfsummen
3. Schicht	Vermittlung	Routing der Datenpakete zum nächsten Knoten
4. Schicht	Transport	Zuordnung der Datenpakete zu einer Anwendung
5. Schicht	Sitzung	Steuerung der Verbindungen und des Datenaustauschs
6. Schicht	Darstellung	Umwandlung der systemabhängigen Daten in unabhängiges Format
7. Schicht	Anwendung	Anbieten und Ausführung von Anwendungsfunktionen sowie Dateneingabe und -ausgabe
8. Schicht	Benutzer	(Inoffiziell) Benutzung der Systeme durch Menschen

OUTPUT FEEDBACK MODE [OFB] (engl.)
Blockchiffre-Modus, welcher Verkettungen von Zeichenblöcken bei Verschlüsselungen verwendet und ähnlich wie CBC und CFB funktioniert. Der erste Klartextblock wird dabei zuerst mit dem verschlüsselten Initialwert (Initialization Vector) zu einem Geheimtextblock kombiniert. Danach wird der benutzte verschlüsselte Initialwert als neuen Initialwert gesetzt, verschlüsselt und mit dem nächsten Klartextblock zu einem weiteren Geheimtextblock kombiniert wird usw.

OWA
Abk. für Outlook Web Access

OWASP
Abk. für Open Web Application Security Project. Eine Non-Profit-Organisation, die Checklisten, Anleitungen und Standards für Sicherheitsüberprüfungen sowie Sicherheitsanforderungen und Testanleitungen zur Verfügung stellt.

OWASP TOP 10
Beschreibung der 10 kritischsten Sicherheitsrisiken bei Web-Applikation.

P 18

P2P NETWORK
Abk. für Peer-to-Peer Network. Übsg. Rechner-zu-Rechner-Verbindung.

P7C
Dateiendung von S/MIME Zertifikaten.

P7M
Dateiendung von S/MIME signierten und verschlüsselten Daten.

P7S
Dateiendung bei S/MIME Signaturen.

PAAS
Abk. für Platform as a Service

PACKET SNIFFER (engl.)
Übsg. Paket-Schnüffler. Syn. zu Network Sniffer.

PACKET SNIFFING (engl.)
Übsg. Paketschnüffeln. Attacke mithilfe von Tools, die kaum detektiert werden können und dem Angreifer erlauben, den Benutzernamen, Passwörter und andere übermittelte Daten im Netzwerk mitzuhören.

PACKETS PER SECOND [PPS] (engl.)
Übsg. Anzahl Datenpakete pro Sekunde.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_18

PADDING (engl.)
Übsg. Auffüllen. Hinzufügen von Nullen oder Leerzeichen am Ende eines Textes oder von Daten. Dies wird bspw. bei Blockverschlüsselung benötigt, um eine Nachricht in Blöcke gleicher Länge aufteilen zu können.

PAM MODULES (engl.)
Abk. für Pluggable Authentication Modules. Übsg. Hinzufügbare Authentisierungsmodule. Standardisierter Dienst von Linux-Systemen, der Apps und Diensten zur Authentisierung von Benutzern bereitgestellt wird. Dadurch brauchen bestehende Apps und Dienste keine eigenen Updates, wenn neue Authentisierungsverfahren im Linux-System eingesetzt werden.

PANAMA PAPERS (engl.)
Sammlung Mio. geheimer, aber 2016 anonym veröffentlichter Finanzdokumente.

PANOPTICLICK
Online-Tool, um zu prüfen wie trackingsicher der benutzte Internetbrowser und darin enthaltene Add-ins sind. Damit kann geprüft werden, ob das benutzte System eine seltene oder einmalige Konfigurationskombination besitzt und somit identifizierbar und verfolgbar ist. Siehe https://panopticlick.eff.org *(Abgerufen am 01.05.2020).*

PASSIVER ANGRIFF
Angriff, bei welchem Systeme oder Dateien nicht manipuliert werden.

PASSPHRASE (engl.)
Übsg. Passwortsatz. Ein Satz als Passwort, anstatt nur eines Wortes.

PASSWORD (engl.)
Übsg. Passwort

PASSWORD HASH FUNCTION (engl.)
Übsg. Passwort-Hash-Funktion. Kryptografische Berechnung, welche auf Passwörter angewendet wird, damit diese nicht als Klartexte gespeichert werden. Zur Vermeidung von Brute-Force-Attacken werden Hash-Funktionen künstlich verlangsamt und die Hash-Werte häufig mit mitgespeicherten zufälligen sog. „Salt"-Werten kombiniert, damit gleiche Passwörter nicht gleiche Hash-Werte ergeben.

Beispiele für Password Hash Function: Blowfish, PBKDF2, SCRYPT.

PASSWORD PROTECTED OFFICE DOCUMENT (engl.)
Übsg. Passwortgeschütztes Office-Dokument. Verschlüsselungsfunktion in Microsoft Office (Word, Excel, PowerPoint). Durch die Verwendung dieser Funktion und der Eingabe eines Passworts wird das ganze Dokument verschlüsselt.

PASSWORD PROTECTED ZIP [PPZIP] (engl.)
Übsg. Passwortgeschütztes ZIP-Dokument. Eine Funktion innerhalb von WinZIP ermöglicht die Verschlüsselung einer ZIP-Datei mithilfe eines Passworts.

PASSWORD RECYCLING (engl.)
Übsg. Benutzung gleicher Passwörter in verschiedenen Diensten. Dies stellt ein beträchtliches Risiko dar, denn wird einer der Dienste gehackt, sind auch die anderen Dienste in Gefahr.

PASSWORD-SPRAYING ATTACK (engl.)
Übsg. Passwort-Versprühungsangriff. Attacke, bei der anstatt vieler Passwörter gegen ein Konto wenige Passwörter gegen viele Konten ausprobiert werden. Dies funktioniert häufig erfolgreich, da es in einer Organisation meist noch immer Benutzer gibt, die einfache Passwörter verwenden. Ein Schutz gegen solche Angriffe sind 2FA und strenge Passwortregeln (Siehe auch Abschn. 31.2.3).

PASSWORD WALLET (engl.)
Syn. zu Password Manager

PASSWORT
Geheimnis, welches benutzt wird, um Daten oder den Zugang zu einem System zu schützen. Nur, wer das richtige Geheimnis kennt, erhält Zugang zu den Daten und dem System.

PASSWORT GEHACKT
Syn. zu Passwort herausgefunden.

PASSWORT GEKNACKT
Syn. zu Passwort herausgefunden.

PASSWORT GENERATOR
Software zur automatischen Erstellung von neuen Passwörtern, damit diese zufällig, komplex und damit sicherer sind, als wenn diese von Menschen ausgedacht werden. Solche Passwörter können in einem Passwort-Manager gespeichert werden, sodass man sich diese nicht merken muss.

PASSWORT-MANAGER
Syn. zu Tresor und Anmeldedatenspeicher. Software zur Speicherung eigener Logins und Passwörter zu Online-Diensten und Apps. Damit verhindert man die Notwendigkeit, sich diese Angaben merken oder aufschreiben zu müssen und ermöglicht dadurch die Benutzung von komplexen Passwörtern, um die Sicherheit und den Schutz der eigenen Konten zu erhöhen. Um die Logins und Kennwörter im Passwort-Manager

sicher zu halten, muss dieser mit einem gut gewählten Master-Passwort geschützt sein. Passwort-Manager werden in modernen Internetbrowsern angeboten oder auch als Internetbrowsererweiterung. Außerdem können separate Passwort-Manager-Apps benutzt werden. In vielen Tests wurde der kostenlose Passwort-Manager KeePass Password Safe empfohlen.

PASSWORTSATZ
Syn. zu Passphrase. Ein Satz als Passwort, anstatt nur eines einfachen Wortes. Vorteil davon ist, dass man sich den Passwortsatz besser merken kann, auch wenn der Passwortsatz lang gewählt wird. Dabei wird empfohlen, keinen bekannten Satz aus Liedern oder Literatur zu verwenden, sondern die darin enthaltenen Wörter zufällig zu wählen und sich den Passwortsatz mit einer Eselsbrücke zu merken.

PASSWORT-VERGESSEN-E-MAIL
Häufig bieten Online-Dienste eine Funktion an, um vergessene Passwörter neu setzen zu können. Dafür muss vorher vom Benutzer eine Notfall-E-Mail-Adresse beim Online-Dienst registriert werden. Da viele Benutzer jedoch dieselbe Notfall-E-Mail-Adresse bei mehreren Diensten benutzen, kann ein Angreifer, welcher Zugang zu diesem einen Notfall-E-Mail-Konto erlangt, folglich Zugang zu vielen anderen Konten des Benutzers bei diversen Online-Diensten erhalten und diese plündern oder missbrauchen.

PATCH (engl.)
Übsg. Flicken. Kleinere Software-Aktualisierungen, bspw. zum Schutz vor neu entdeckten Sicherheitslücken.

PATCHING OF OPERATING SYSTEMS (engl.)
Übsg. Flicken des Betriebssystems. Kleinere Betriebssystemaktualisierungen, bspw. zum Schutz vor neu entdeckten Sicherheitslücken.

PATCH KABEL
Netzwerkkabel. Syn. zu RJ45-Kabel.

PATCH-MANAGEMENT
Bearbeitung und Planung von kleineren Updates für Systeme, um z. B. neue Sicherheitslücken sofort zu schließen. Patch-Management wird häufig unabhängig zu Release-Management durchgeführt, bei welchem große Teile oder ganze Software-Produkte aktualisiert werden.

PATTERN (engl.)
Übsg. Muster

PATTERN MATCHING (engl.)
Übsg. Übereinstimmung von Mustern.

PATTERN RECOGNITION (engl.)
Übsg. Erkennen von Mustern. Teil des Themenkreises der künstlichen Intelligenz.

PAYLOAD (engl.)
Übsg. Nutzdaten

PAYMENT CARD FRAUD (engl.)
Übsg. Zahlungskartenbetrug

PAYMENT FRAUD DETECTION (engl.)
Übsg. Erkennung von Zahlungsbetrug.

PAY WALL (engl.)
Übsg. Zahlungsmauer. Internetseiten, die nur nach Zahlung sichtbar sind. Dies wird nicht nur für pikante Seiten eingerichtet, sondern auch für kostenpflichtige Seiten bei Zeitschriften usw.

PBA
Abk. für PreBoot Authentication

PBKDF2
Abk. für Password-Based Key Derivation Function. Eine Password Hash Function, d. h. eine kryptografische Hash-Funktion, welche auf Passwörter angewendet wird, damit diese nicht als Klartexte gespeichert werden. Zur Vermeidung von Brute-Force-Attacken werden Hash-Funktionen künstlich verlangsamt und die Hash-Werte häufig mit mitgespeicherten zufälligen sog. „Salt"-Werten kombiniert, damit gleiche Passwörter nicht gleiche Hash-Werte ergeben.

PE
Abk. für Portable Executable. Dateiformat für ausführbare Binärdateien auf Windows, bspw. alle Dateien mit der Endung „.exe".

PEER-TO-PEER (engl.)
Übsg. Gerät-zu-Gerät. Kommunikation unter gleichberechtigten Kommunikationsteilnehmern. Syn. zu symmetrischer Kommunikation.

PEER-TO-PEER CONNECTION (engl.)
Übsg. Gerät-zu-Gerät-Verbindung zwischen gleichberechtigten Systemen, bspw. zwei Telefone. Syn. zu symmetrischer Kommunikation.

PEER-TO-PEER-NETZWERK
Übsg. Gerät-zu-Gerät-Netzwerk. Syn. zu Punkt-zu-Punkt-Netzwerk. Netz zwischen Systemen, die, mit oder ohne Kabel, direkt verbunden sind und deshalb nicht über einen zentralen Hub oder Router kommunizieren. Bspw. können die in einem Heimnetzwerk eingebundenen Heim-PCs mit Mac, Windows, Linux usw. als Peer-to-Peer-Netzwerk angesehen werden, falls alle Systeme miteinander verbunden sind und auf Ressourcen wie Drucker und Festplatte der anderen zugreifen können. Befindet sich ein Router im Heimnetzwerk, welcher den Heim-PCs jeweils eine IP-Adresse vergibt, stellt dieser einen Server dar, der von den Heim-PCs als Clients für Verbindungen zu den anderen Heim-PCs benutzt wird, wodurch eine asymmetrische, Nicht-Peer-to-Peer-Kommunikation im Heimnetzwerk entsteht.

PENETRATION TESTING (engl.)
Methode des Software-Testens zur Reduzierung des Cybersecurity-Risikos. Dabei werden Hacker-Angriffe auf eine interne oder auf eine von außen erreichbare Software simuliert, um Schwachstellen zu erkennen und diese vor dem Go-Live der Software eliminieren zu können.

PEN TESTING (engl.)
Abk. für Penetration Testing

PERFECT FORWARD SECRECY [PFS] (engl.)
Übsg. Perfekte vorwärts gerichtete Geheimhaltung. Protokoll zur Erzeugung und zum Austausch kryptografischer Schlüssel für jede einzelne Sitzung, basierend auf einem vorher vereinbarten Langzeitschlüssel. Die Session-Schlüssel dürfen nach Beendigung der Sitzungen nie mehr mittels des Langzeitschlüssels rekonstruierbar sein.

PERFECT SECRECY (engl.)
Übsg. Perfekte Geheimhaltung, perfekte Sicherheit. Kryptografiemethoden, bei welchen die verschlüsselte Nachricht keine Informationen über den ursprünglichen Klartext bietet, außer evtl. die maximal mögliche Länge.

PERFEKTE SICHERHEIT
Begriff aus der Kryptografie- und Informationstheorie. Eine Verschlüsselungsmethode gilt dann als perfekt sicher, wenn aus dem Geheimtext keine Rückschlüsse auf den Klartext möglich sind.

PERMISSION (engl.)
Übsg. Erlaubnis, Zulassung.

PERMUTATIONS-CHIFFREN
Verschlüsselungsmethoden, bei welchen der Geheimtext durch Ändern der Reihenfolge des Alphabets erzeugt wird, sodass bspw. bei einer einfachen linearen Permutations-Chiffre „A“ im Klartext zu „D“ im Geheimtext wird, „B“ zu „E“, „C“ zu „F“ usw.

Beispiel einer Permutations-Chiffre

Aus dem Klartext „HAUS“ wird bei einer Verschiebung des Alphabets um 3 Zeichen der Geheimtext „KDXG“.

PERSONAL CERTIFICATE STORE (engl.)
Teil des Certificate Store.

PERSONAL DATA (engl.)
Übsg. Persönliche Daten

PERSONAL IDENTIFICATION NUMBER [PIN] (engl.)
Übsg. Persönliche Geheimzahl. Kann als Passwort angesehen werden, welches nur aus Zahlen besteht. Verwendungszwecke sind Bankkarten-PIN, Login-PIN, Smartcard-PIN, SIM-Karten-PIN u. Ä. Zu beachten ist, dass entgegen der häufigen Meinung der PIN für die SIM-Karte in Handys zwar vor Netzzugriff (Anrufe, Internet) schützt, jedoch nicht vor der Benutzung anderer Apps und Handy-Funktionen, und damit nicht vor Datendiebstahl.

PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT [PIPEDA] (engl.)
Kanadisches Recht zum Datenschutz, eingeführt im Jahr 2000.

PERSONALLY IDENTIFIABLE INFORMATION [PII] (engl.)
Übsg. Informationen, die eine Person identifizieren. Häufig als Syn. zu „Persönliche Daten“ verwendet. Definiert als:

> „Jegliche Information über eine Person, die von einer Agentur oder Firma verwaltet wird, einschließlich 1) jeglicher Information, die zur Unterscheidung oder Rückverfolgung der Identität einer Person verwendet werden kann, wie Name, Sozialversicherungsnummer, Geburtsdatum und -ort, Mädchenname der Mutter oder biometrische Aufzeichnungen; und 2) sonstige Information, die mit einer Person verknüpft ist oder verknüpft werden kann, wie z. B. medizinische, Bildungs-, Finanz- und Beschäftigungsinformationen.“ (Quelle: NIST, frei übersetzt).

PERSONAL SECURITY ENVIRONMENT [PSE] (engl.)
Übsg. Persönliche Sicherheitsumgebung

PERSÖNLICHE DATEN
Syn. zu Personally Identifiable Information (PII). Das Datenschutz-Gesetz „EU GDPR“ definiert persönliche Daten als alle Informationen, die sich auf eine natürliche Person beziehen und es erlauben, die Person direkt oder indirekt zu identifizieren. Dies können Merkmale sein wie der Name und der Wohnort, aber auch genetische, mentale, physische, psychologische, ökonomische, kulturelle oder soziale Details.

PERSÖNLICHE SICHERHEITSUMGEBUNG [PSU]
Bereich in einem Speichermedium, in welchem kryptografische Schlüssel gespeichert werden. Ein Software-PSU kann als eine symm. verschlüsselte Datei erstellt werden, sodass nur der Ersteller ein Passwort zur Entschlüsselung besitzt. Ein Hardware-PSU kann als spezielles Gerät vorliegen, bspw. eine Smartcard oder ein USB-Stick.

PERVASIVE ENCRYPTION (engl.)
Übsg. Allgegenwärtige Verschlüsselung. Prinzip, in dem alle Daten verschlüsselt werden, ungeachtet ihrer Wichtigkeit. Im Unterschied zu „Selektive Encryption“, bei welcher nur die wichtigsten Daten verschlüsselt werden.

PETNA
Schadsoftware. Variante der Petya-Ransomware. Verschlüsselt die Daten auf den erreichbaren Festplatten und verlangt ein Erpressungsgeld.

PETYA
Familie von verschlüsselnden Ransomware-Varianten, die Microsoft-Windows-basierte Systeme angreifen und ein Erpressungsgeld verlangen. Erstmals entdeckt im Jahr 2016. Für die ersten Varianten gab es eine Entschlüsselung, die jedoch für spätere Varianten nicht mehr funktionierte.

PFA
In E-Mails, SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „Please find attached“, Übsg. „Bitte finde angehängt“.

PFB
In E-Mails, SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „Please find below“, Übsg. „Bitte finde unten“.

PFILE
Von Microsoft Information Rights Management (RMS) benutzte Dateierweiterung für Dateitypen, die nicht standardmäßig mit RMS verschlüsselt werden können, wie z. B. JPG, TXT, CSV und bei welchen der Inhalt deshalb als eingebetteter Teil einer neuen Datei (eines sog. „Wrapper“) verschlüsselt wird. Windows vergibt einem solchen File

eine neue Dateierweiterung, welche weiterhin mit der korrekten Anwendung geöffnet werden kann, falls RMS installiert ist. Die derart erstellten und verschlüsselten Dateien erlauben jedoch nur noch den Lesezugriff.

Beispiel eines PFILE: Eine Datei.txt wird durch RMS-Verschlüsselung zu Datei.ptxt.

PFS
Abk. für Perfect Forward Secrecy

PGP
Abk. für Pretty Good Privacy (siehe Spezialthema im Kap. 30).

PHISHING (engl.)
Kombiniertes Kunstwort aus „Password“ und „Fishing“. Hacker-Methode mit dem Ziel, das Passwort zu „fischen“. Dabei wird bspw. eine scheinbar korrekte E-Banking-Seite gezeigt, die jedoch nur eine Imitation ist und benutzt wird, um die vom nichts ahnenden Benutzer eingegebenen Login-Daten zu sammeln und danach zu missbrauchen.

PHOTON
Syn. zu Lichtteilchen. Das Licht kann je nach Anwendung als Welle oder als Lichtteilchen modelliert werden.

PHP
Abk. für PHP: Hypertext Preprocessor. Freie Programmiersprache, welche auf Servern interpretiert wird und dynamische Internetseiten ermöglicht.

PHPMYADMIN
Populäre Weboberfläche zur Administration von MySQL-Datenbanken.

PHYSICAL SECURITY (engl.)
Übsg. Physische Sicherheit

PHYSISCHE SICHERHEIT
Maßnahmen, wie Videoüberwachung, Zugangskontrollen und Anketten von Geräten. Diese Maßnahmen können ergänzt werden durch digitale Sicherheitsmaßnahmen.

PII
Abk. für Personally Identifiable Information

PIN
Abk. für Personal Identification Number

PING
Programm zur Prüfung der Erreichbarkeit eines Systems. Durch die Eingabe von *ping* + IP-Adresse in einer Konsole erhält man als Antwort die Angabe, ob Daten mit dem Gerät an dieser IP-Adresse ausgetauscht werden können, oder ob gesendete Testdaten als unzustellbar erklärt wurden.
Beispiel: ping 192.168.0.20

PIPEDA
Abk. für Personal Information Protection and Electronic Documents Act.

PIPELINE
1) Abfolge von Datenverarbeitungsprozessen. 2) Rohrleitungssystem.

PIT
Abk. für Public Intrusion Test

PKC
Abk. für Public Key Cryptography

PKCS#1–PKCS#15
Abk. für Public-Key Cryptography Standards. Von RSA Security initiierte Standards für asymmetrische Kryptografie.

PKCS#1
Beschreibung des Formats der RSA-Verschlüsselung. Syn. zu RFC8017. Empfohlener Standard zur Implementation von Public-Key Kryptografie basierend auf RSA.

PKCS#2
Nicht mehr benutzt. Wurde in PKCS#1 eingebaut.

PKCS#3
Beschreibung des Diffie-Hellman-Schlüsselaustauschs.

PKCS#4
Nicht mehr benutzt. Wurde in PKCS#1 eingebaut.

PKCS#5
Beschreibung der passwortbasierten Verschlüsselung. Syn. zu RFC2898.

PKCS#6
Veraltete Beschreibung der ersten Version des v1-X.509-Zertifikats. Durch PKCS#7 ersetzt.

PKCS#7
Beschreibung der Syntax einer kryptografischen Nachricht. Dies wird u. a. für das Signieren, Authentisieren und Verschlüsseln von Nachrichten verwendet, bspw. bei S/MIME. Syn. zu RFC5652.

Folgende Dateiendungen werden hierfür verwendet: *.p7b und *.p7c für Zertifikate, *.p7m für MIME-Nachrichten, *.p7s für Signaturen.

PKCS#8
Beschreibung der Syntax für private Schlüssel. Syn. zu RFC5208.

PKCS#9
Beschreibung von bestimmten Attributklassen für andere PKCS. Syn. zu RFC2985.

PKCS#10
Beschreibung des Formats der Nachricht, welche an eine Zertifizierungsstelle (CA) gesendet wird. Syn. zu RFC2986.

PKCS#11
Beschreibung einer API für kryptografische Tokens, bspw. um private Schlüssel für das Signieren von Daten zu verwenden.

PKCS#12
Beschreibung der Art, wie private Schlüssel mit entsprechendem Zertifikat passwortgeschützt gespeichert werden. Syn. zu RFC7292.

PKCS#13
Beschreibung einer neueren Verschlüsselung, welche auf elliptischen Kurven basiert.

PKCS#14
Beschreibung einer Methode zur Pseudozufallszahlerzeugung.

PKCS#15
Nicht mehr benutzt.

PKI
Abk. für Public Key Infrastructure

PL
Abk. für Publishing License

PLAGIARISM (engl.)
Übsg. Plagiat. Syn. zu Diebstahl geistigen Eigentums.

PLAIN TEXT (engl.)
Übsg. Einfacher Text. Reine Daten, wie z. B. Buchstaben ohne Verschlüsselung und ohne Formatierung.

PLAY STORE (engl.)
Googles Online-Warenhaus für Android Apps, Bücher und andere Medien.

PLUG-IN
Syn. zu Erweiterung, Extension. Software, welche in ein Produkt hinzugeladen werden kann, um zusätzliche Funktionen anzubieten. Bspw. können Webbrowser-Plug-ins sicherstellen, dass Aufrufe standardmäßig via HTTPS anstatt HTTP erfolgen, falls der adressierte Server dies anbietet.

PM
1) Abk. für Private Message. 2) Abk. für Projekt-Management. 3) Abk. für Projekt-Manager. 4) Abk. für Programm-Manager. 5) Abk. für Produkt-Manager.

POC
Abk. für Proof of Concept

POE SWITCH
Abk. für Power over Ethernet Switch. Gerät, welches sowohl Strom als auch Daten über ein Ethernet-Kabel erhält.

POINT OF SALE [POS] (engl.)
Übsg. Verkaufsort

POLICY (engl.)
Übsg. Strategie, Grundsatz. 1) Dokumentation und Regeln, welche festlegen, wie firmeninterne oder regulatorische Weisungen von Firmenmitarbeitern eingehalten werden müssen. 2) Set von programmierten Konfigurationen oder Regeln, die auf Systeme verteilt werden, um automatische Aktionen durchzuführen, wie bspw. Verschlüsselung oder Klassifizierung von Daten, die durch Datenscanner gefunden werden.

POLY1305-AES
Eine Variante von Message Authentication Code (MAC), welcher die Überprüfung der Datenintegrität und der Authentizität einer Nachricht ermöglicht. Google adaptierte Poly1305 für TLS.

POLYRANDOM
Schadsoftware in Form einer dateiverschlüsselnden Ransomware.

POODLE ATTACKE
Abk. für Padding Oracle On Downgraded Legacy Encryption Attacke. Eine Sicherheitslücke im CBC-Blockchiffre-Modus von SSL3.0. Mittels JavaScript-Code auf einer Internetseite wird diese Sicherheitslücke dadurch ausgenutzt, dass Verbindungen mit aktuellem TLS bewusst abgelehnt werden und damit erreicht wird, dass der Webbrowser auf SSL3.0 zurückwechselt. Danach können verschlüsselt übertragene Daten durch mehrfaches Senden einzelner, veränderter Bytes an den Server entschlüsselt werden.

POP3
Abk. für Post Office Protocol

POP3S
Abk. für Post Office Protocol Secure. TLS-verschlüsselte Variante von POP3.

POP SOCKET (engl.)
An der Rückseite von Handys und Tablets angeklebte Halterung, die sich 1 bis 2 cm herausziehen lässt, um das Gerät dadurch gut mit den darum herum gehaltenen Fingern zu halten.

POP-UP (engl.)
Übsg. Erscheinen, Aufspringen. Häufig als Abk. für Pop-up-Window, Pop-up-Fenster verwendet zur Beschreibung eines Programmfensters, welches erscheint, um den Benutzer auf einen Fehler hinzuweisen oder ihm eine Eingabemaske anzubieten.

PORT
Unterscheidungsnummer zur Bezeichnung einer angebotenen oder möglichen Verbindung zwischen einem Paar von Systemen. Bspw. werden bei einem Webserver meist die Ports 80 für unverschlüsselte HTTP-Verbindungen und 443 für TLS/SSL verschlüsselte HTTPS-Verbindungen angeboten, sodass Webbrowser Downloads über diese Ports durchführen können. Ein Webbrowser kann auch mehrere Downloads vom gleichen Webserver über den gleichen (Eingangs-) Port 80 durchführen, da der Webbrowser selber unterschiedliche (Ausgangs-) Ports verwenden kann (siehe Tab. 18.1).

PORTAL
Abk. für Webportal. Internetseite, welche andere Internetseiten in Verzeichnissen mit direkten Links auflistet.

PORT FORWARDING (engl.)
Übsg. Port-Weiterleitung. Funktion, um von einem Netzwerk A über ein Gateway zu einem System innerhalb eines anderen Netzwerks B zu gelangen.

Tab. 18.1 Netzwerkprotokolle verwenden meist vordefinierte Portnummern

Portnummer	Netzwerkprotokoll
Port 20	FTP
Port 22	SSH
Port 23	Telnet
Port 25	SMTP
Port 80	HTTP
Port 110	POP3
Port 143	IMAP
Port 443	HTTPS
Port 465	SMTPS (SMTP über SSL/TLS)
Port 587	SMTP
Port 993	IMAPS (IMAP über SSL/TLS)
Port 995	POP3S (POP3 über SSL/TLS)

PORTLET
Syn. zu Kacheln. Programme, die als Komponenten einer Benutzeroberfläche genau definierte Inhalte, meist in Kachelform, anzeigen. Die Inhalte werden von einem Portalserver geliefert. Bspw. Kacheln für News-Ticker, Wettervorhersage, Chat.

PORT SECURITY (engl.)
Teilgebiet der Cyber- und IT-Sicherheit. Ziel ist die Verhinderung von Angriffen, von Missbrauch und von Datenverlust durch offene Ports.

PORT-WEITERLEITUNG
Funktion, um von einem Netzwerk A über ein Gateway zu einem System innerhalb eines anderen Netzwerks B zu gelangen. Syn. zu Port Forwarding.

POS
Abk. für Point of Sale

POSIX
Abk. für Portable Operating System Interface. Eine Funktionsbibliothek (API) für App-Entwickler auf Unix als Schnittstelle zum Betriebssystem.

POST
Syn. zu HTTP-POST

POST OFFICE PROTOCOL [POP3] (engl.)
Übsg. Postfachprotokoll. Textbasiertes Verfahren für das Auflisten, Abrufen und Löschen von E-Mails vom E-Mail-Server. Bei den meisten POP3-Servern können der Transport des Benutzernamens und des Passworts zum Server und die E-Mails vom Server zum Empfänger mit SSL/TLS verschlüsselt werden. Dies wird durch den Befehl STARTTLS vom Client an den Server auf Port 110 oder ohne STARTTLS-Befehl durch implizites TLS via POP3S auf Port 995 angestoßen. Das Senden von E-Mails geschieht nicht über POP3, sondern über SMTP.

POTENZIELL UNERWÜNSCHTE APPS [PUA]
Apps oder Webbrowser-Plug-ins, die neben der eigentlichen Funktion zusätzlich Werbung anzeigen, andere Webbrowser-Plug-ins oder Webbrowser-Toolbars installieren oder anderweitig unklare Ziele verfolgen.

POWER BLACKOUT (engl.)
Übsg. Stromausfall

PPS
Abk. für Packets Per Second

PPZIP
Abk. für Password Protected Zip

PRANK (engl.)
Übsg. Streich

PREBOOT AUTHENTICATION [PBA] (engl.)
Übsg. Authentisierung vor dem Booten. Software, die noch vor dem Betriebssystem gestartet wird und eine Authentisierung durchführt. Ohne eine erfolgreiche Authentisierung wird das Betriebssystem nicht gestartet. PBA kann bspw. durch das Zusammenspiel von BitLocker und CryptoPro Secure Disk erreicht werden.

PREMISE (engl.)
Übsg. Haus, Räume. Oft im Zusammenhang mit „On-Premise“, „Off-Premise“ verwendet.

PREPARED STATEMENTS (engl.)
Übsg. Vorbereitete Abfragen. SQL-Datenbankabfragen, die vorher mit Platzhaltern vordefiniert wurden. Mittels Überprüfung dieser Abfragen durch das Datenbanksystem vor der eigentlichen Benutzung unterstützen Prepared Statements den Schutz vor Attacken, wie bspw. SQL Injection.

PRE-SHARED-KEY [PSK] (engl.)
Übsg. Vorher ausgetauschter Schlüssel. Schlüssel für kryptografische Verfahren, welcher zuvor zwischen den Teilnehmern vereinbart wurde.

Beispiel: Die Benutzung desselben Passworts durch alle teilnehmenden Geräte bei der Verwendung eines WLAN-Netzes mit WPA2-PSK.

PRE-SHARED-SECRETS (engl.)
Übsg. Vorher ausgetauschtes Geheimnis. Unter Teilnehmern vereinbartes Geheimnis, wie Schlüssel, Passwort oder Passphrase, welches für kryptografische Verfahren benutzt wird. Ein solches Geheimnis kann bei entsprechender Authentisierung auch von einem Dienst auf einen anderen weitergereicht werden, bspw. bei Single Sign-On (SSO).

PRETTY GOOD PRIVACY [PGP] (engl.)
Übsg. Ziemlich gute Privatsphäre. Programm zur Verschlüsselung und zum Signieren von Daten und E-Mails. Dieses benutzt ein hybrides kryptografisches Verfahren mit symm. und asymm. Verschlüsselung, wobei letztere eine Kombination aus privatem und öffentlichem Schlüssel verwendet, aba. Public-Key-Verschlüsselung. PGP basiert auf dem „Web of Trust“. Die quelloffene Variante OpenPGP kann in vielen Betriebssystemen und E-Mail-Programmen hinzugeladen werden (siehe auch Spezialthema im Kap. 30).

PREVENTING CONTROLS (engl.)
Übsg. Verhinderungsmethoden. Diese helfen Risiken oder Schäden zu verhindern, bevor diese geschehen. Mögliche Verfahren sind bspw. die Kontrolle von Zugriffsrechten, die Schulung von Mitarbeitern und die Verschlüsselung von E-Mails. Wird unterschieden von Detective Controls.

PRINCIPLE OF LEAST PRIVILEGED (engl.)
Übsg. Prinzip der geringsten Rechte.

PRINZIP DER GERINGSTEN RECHTE
Zum Schutz von Daten, Systemen und Netzwerken soll jeder Benutzer von Systemen nur so viele Zugriffsrechte erhalten, wie er für seine jetzige Tätigkeit benötigt.

PRIVACY (engl.)
Übsg. Privatsphäre

PRIVATE BROWSING (engl.)
Übsg. Privates Browsen. Fenster oder Tab innerhalb eines Webbrowsers, bei welchem keine Cookies und keine Chronik gespeichert werden. Dadurch wird die Verfolgung des Benutzers über mehrere Internetseiten erschwert. Downloads werden jedoch trotzdem

gespeichert und die Systemkonfiguration kann weiterhin einmalig sein und ist dadurch erkennbar und verfolgbar (siehe Panopticlick).

PRIVATE CLOUD (engl.)
Cloud-Installation, die komplett in den eigenen Firmengebäuden oder in der eigenen Wohnung läuft.

PRIVATE KEY (engl.)
Übsg. Privater Schlüssel

PRIVATE KEY SEARCHABLE ENCRYPTION (engl.)
Übsg. Durchsuchbare Verschlüsselung basierend auf dem privaten Schlüssel. Eine Nachricht und eine spezielle dazugehörige Datenstruktur werden vor dem Hochladen auf einen Server mit dem privaten Schlüssel verschlüsselt. Durch Besitz des privaten Schlüssels und Kenntnis der Datenstruktur kann die geheime Nachricht auch in verschlüsselter Form durchsucht werden, ohne die Nachricht komplett entschlüsseln zu müssen und damit im Server offenzulegen. Verwandt mit homomorpher Verschlüsselung und Hidden Vector Encryption (HVE).

PRIVATE MESSAGE [PM] (engl.)
Mitteilung innerhalb eines Online-Diskussionsforums, welches nicht für alle sichtbar, sondern nur an eine bestimmte Person gerichtet und nur für diese Person sichtbar ist.

PRIVATER SCHLÜSSEL
Einer der beiden Teile eines asymm. kryptografischen Schlüsselpaars. Der private Schlüssel muss geheim bleiben und sicher gespeichert werden, bspw. in einer Smartcard oder einer anderen „persönlichen Sicherheitsumgebung“. Nur der Besitzer des privaten Schlüssels kann eine mit dem entsprechenden öffentlichen Schlüssel verschlüsselte Nachricht entschlüsseln. Der private Schlüssel kann auch benutzt werden zur digitalen Signatur von E-Mails, um damit dem Empfänger die Möglichkeit der Überprüfung zu geben, wer der Absender war und ob die Nachricht unversehrt ankam.

PRIVILEGED ACCESS (engl.)
Übsg. Privilegierter Zugang

PRIVILEGED ACCESS MANAGEMENT (engl.)
Übsg. Verwaltung der Rechteausweitung. Software und Prozesse, mit denen der privilegierte Zugriff auf kritische bzw. sensible Daten oder Systeme verwaltet und überwacht wird. Benutzer, die privilegierten Zugriff erhalten müssen, verwenden im optimalen Fall dazu ein spezielles Konto und spezielle Anmeldedaten, damit das Risiko des versehentlichen Schadens und des Diebstahls verringert werden kann.

PRIVILEGE ESCALATION (engl.)
Übsg. Rechteausweitung durch Ausnutzung von Fehlern in Programmen und Betriebssystemen. In ordentlich konfigurierten Systemen hat ein Benutzer oder eine App nur beschränkte Zugriffsrechte und kann in Ausnahmefällen via Privileged Access Management die Admin-Rechte erhalten. Bei Prozess- oder Konfigurationsfehlern kann sich im Gegensatz dazu der Benutzer oder die App weitergehende Zugriffsrechte vergeben, um noch tiefere Änderungen am System vorzunehmen.

PRIVILEGIEN
Syn. zu Benutzerrechte

PRIVILEGIERTER ZUGANG
Besondere, weitergehende Zugangsrechte von Benutzern an einem System. Beispiel: Administratoren erhalten privilegierte Zugangsberechtigungen, um Systemaktualisierungen durchzuführen.

PROACTIVE DEFENSE (engl.)
Übsg. Proaktive Abwehr. Maßnahmen zur Vorbereitung und Verhinderung von Angriffen.

PROCESS HOLLOWING (engl.)
Übsg. Prozessaushöhlung. Angriffsmethode, um eine Schadsoftware bzw. den zugehörigen Betriebssystemprozess unbemerkt zu starten. Erst wird ein Prozess ordentlich gestartet und in einen angehaltenen Zustand gebracht. Danach kann die Schadsoftware in den für den angehaltenen Prozess benutzten Speicherbereich geschrieben werden. Bei Wiederstarten des Prozesses wird nun die Schadsoftware ausgeführt.

PROFILING (engl.)
Automatische Verarbeitung von Personendaten, um gewisse Aspekte der verfolgten Person zu untersuchen und damit ein Benutzerprofil zu erstellen. Dabei können sowohl das Verhalten als auch die Aktivitäten der Person am System aufgezeichnet und verwendet werden. Dies kann daraufhin missbraucht werden, um diese Person eindeutig zu bestimmen und ihr gezielte Werbung zu offerieren o. Ä. Profiling geschieht in Internetbrowsers bspw. durch Verfolgen von Cookies über verschiedene Internetseiten hinweg, durch Verfolgung der IP-Adresse, durch die Analyse angeklickter Facebook-Likes oder durch die Analyse angesehener YouTube-Filme.

PROGRAMMIERSCHNITTSTELLE
Syn. zu Anwendungs-Programmierschnittstelle

PROGRAMMIERSPRACHE
Vordefinierte Computerbefehle, die von einem Programmierer in strukturierter Form als sog. Quellcode hintereinander geschrieben werden, um ein Programm zu erstellen, welches danach von einem System ein oder mehrere Male ausgeführt wird. Meist steht ein Compiler- oder ein Interpreterprogramm zwischen dem Quellcode und dem maschinenlesbaren Code, sodass der Programmierer nicht selber einen maschinenlesbaren Code schreiben muss. Auch gibt es grafische Programmiersprachen, die fast komplett ohne textbasierte Befehle auskommen und damit leichter zu erlernen sind. Einige Programmiersprachen, wie C++ und Java, erlauben die Benutzung objektorientierter Programmierung im Vergleich zur rein prozeduralen Hintereinanderreihung von Befehlen bei anderen Programmiersprachen wie bei Basic und Assembler.

Beispiel

Die wohl am häufigsten eingesetzte Programmiersprache ist Java, welche auf über 3 Milliarden Geräte zum Einsatz kommt. Einige weitere populäre Programmiersprachen werden in Tab. 18.2 aufgelistet.

PROOF OF AUTHORITY (engl.)
Übsg. Autoritätsbeweis. Typ eines Konsens-Algorithmus bei Blockchain-Systemen, bei welchem eine zentrale Stelle jeden neuen Block bestätigt. Andere Beweistypen sind: Proof of Stake, Proof of Work.

PROOF OF CONCEPT [POC] (engl.)
Übsg. Konzeptbeweis. Methode, um ein Konzept oder eine Idee als einfachen Prototyp zu entwickeln, um zu prüfen, ob das Konzept oder die Idee umsetzbar ist.

PROOF OF CONCEPT EXPLOIT (engl.)
Übsg. Nachweis einer Schwachstelle. Von Forschern bewusst ausgenutzte Schwachstelle in einem System, um zu beweisen, dass diese auch von Hackern ausgenutzt werden könnte.

PROOF OF STAKE (engl.)
Übsg. Teilnehmerbeweis. Typ eines Konsens-Algorithmus bei Blockchain-Systemen, bei welchem ein neuer Block bei Zahlung eines Anteils akzeptiert wird. Andere Beweistypen sind: Proof of Authority, Proof of Work.

Tab. 18.2 Beispiele einiger Programmiersprachen

Basic	Python	VBA
C#	Assembler	C++
Java	Ruby	HTML
JavaScript	PHP	SCALA

PROOF OF WORK (engl.)
Übsg. Arbeitsbeweis. Typ eines Konsens-Algorithmus bei Blockchain-Systemen, bei welchem ein neuer Block ohne Bestätigung einer zentralen Stelle akzeptiert wird (z. B. bei Bitcoin, Ethereum). Andere Beweistypen sind: Proof of Authority, Proof of Stake.

PROPRITÄRE SOFTWARE
Syn. zu „in Eigentum befindliche" Software. Programme, bei welchem die Verwendung oder der Vertrieb eingeschränkt wurde.

PROTECTION (engl.)
Übsg. (Daten-) Schutz. Häufig auch als Syn. zu Verschlüsselung verwendet.

PROTECTION AT COMPUTATION (engl.)
Übsg. Verschlüsselung während der Berechnung. Bei homomorpher Verschlüsselung kann die Verschlüsselung von Daten bestehen bleiben, während ein Teil der geheimen Daten für Berechnungen benutzt werden kann.

PROTECTION AT REST (engl.)
Übsg. Schutz gespeicherter Daten. Wird unterschieden von „Protection on Transit", Übsg. Schutz übermittelter Daten.

Beispiele für Protection at Rest

a) Passwortschutz bei Microsoft-Office-Dokumenten
b) RMS-Verschlüsselung bei Dateien
c) PGP-Verschlüsselung bei Dateien

PROTECTION OF SENSITIVE KEY MATERIAL (engl.)
Übsg. Schutz von sensiblen Schlüsseln und Zertifikaten.

PROTECTION ON TRANSIT (engl.)
Übsg. Schutz übermittelter Daten. Wird unterschieden von „Protection at Rest", Übsg. Schutz gespeicherter Daten.

Beispiel für Protection on Transit: Verschlüsselte Übermittlung von Formulardaten bei Internetseiten, falls die Verbindung über HTTPS ausgeführt wird.

PROTECTIVE TECHNOLOGY (engl.)
Übsg. Schutztechnologie

PROTOCOL (engl.)
Übsg. Protokoll

PROTOKOLL
Definierte Vereinbarungen, Regeln, Strukturen oder Algorithmen, welche bspw. die Kommunikation oder die Verschlüsselung während der Kommunikation zw. zwei Parteien beschreiben. Die Protokolldetails beschreiben u. a. Regeln zur Kontrolle des Datenflusses, Syntaxdefinitionen einer Nachricht, Syntaxdefinitionen der Daten-Header, Fehlertoleranz u. Ä.

Wichtige Protokolle:

a) Internet Protocol (IP)
b) Transmission Control Protocol (TCP)
c) Hypertext Transfer Protocol (HTTP)
d) Post Office Protocol (POP)
e) Transport Layer Security (TLS)

PROTOKOLLIERUNG VON CYBER-BEDROHUNG
Phase bei der Behandlung von Cyber-Bedrohungen.

PROVABLE SECURITY (engl.)
Übsg. Beweisbare Sicherheit. Verfahren zur Gewährleistung der IT-Sicherheit bei Systemen. Diese beruht überwiegend auf der Modularität der Teilsysteme, die jede für sich selber geprüft und als sicher garantiert werden können.

Beispiel: Das TLS-Protokoll ist zusammengesetzt aus den zwei geprüften Teilen „Schlüsselaustausch“ und „Verschlüsselung“.

PROXY (engl.)
Abk. für Proxy Server. Übsg. Stellvertretersystem oder -programm. Ein Proxy erhält Anfragen von PCs im Netzwerk und leitet diese an andere Systeme innerhalb oder außerhalb des Netzwerks weiter. Ein Proxy kann als Server oder auch als einfaches Programm auf dem PC des Benutzers aufgesetzt werden. Ein wichtiger Vorteil eines Proxys ist die Zwischenspeicherung von gesendeten Daten, sodass diese beim nächsten Aufruf direkt vom Proxy bereitgestellt werden anstatt vom entfernten Server. Dabei wird der Aufruf einer Internetseite vom PC des Benutzers nicht direkt zur Internet-Domain geschickt, sondern erst zum Proxy, welcher diese Anfrage nur dann an die Internet-Domain weiterleitet, wenn diese Internetseite nicht bereits kürzlich zuvor abgefragt und auf dem Proxy zwischengespeichert wurde.

PROXY-TUNNEL
Verbindung eines Webbrowsers oder Terminals zu einem bestimmten Proxy-Server (Zwischenserver), von wo aus eine Internetadresse über weitere Proxy-Server aufgerufen wird. Damit bleibt die eigene IP-Adresse verschleiert.

PSD2
Abk. für Payment Services Directive 2. Übsg. Zahlungsdiensterichtlinie. Weisung des Europäischen Parlaments, um Zahlungsverkehr auch für Nichtbanken im EU-Raum zu öffnen, um damit Innovation und Wettbewerb zu fördern und den Verbraucherschutz zu erhöhen. Gültig seit 2018.

PSE
Abk. für Personal Security Environment

PSU
Abk. für Persönliche Sicherheitsumgebung

PUA
Abk. für Potenziell unerwünschte Apps

PUBLIC (engl.)
Übsg. Öffentlich, Öffentlichkeit

PUBLIC CA (engl.)
Abk. für Public Certification Authority. Übsg. Öffentliche Zertifizierungsstelle.

PUBLIC DISCLOSURE (engl.)
Übsg. Öffentliche Offenlegung

PUBLIC DOMAIN (engl.)
Übsg. Öffentlicher Bereich im Sinne von „frei von Urheberrechten“. Software wird als Public Domain angeboten, wenn diese mehrheitlich frei kopiert und weiterverwendet werden kann. Häufig als Syn. zu Open Source oder freier Software.

PUBLIC INTRUSION TEST [PIT] (engl.)
Übsg. Öffentlicher Einbruchstest

PUBLIC KEY (engl.)
Übsg. Öffentlicher Schlüssel

PUBLIC KEY AUTHENTIFICATION (engl.)
Übsg. Authentifikation, basierend auf einem öffentlichen Schlüssel. Bei dieser Authentifikationsmethode erhält oder erstellt der Benutzer ein Paar aus privaten und öffentlichen Schlüsseln, speichert den privaten Schlüssel auf seinem PC und übermittelt den öffentlichen Schlüssel auf einen Server, auf den er von nun an durch den Besitz des privaten Schlüssels. bspw. mittels SSH, zugreifen kann, ohne ein Passwort zu benötigen. Auch kann dem Besitzer des privaten Schlüssels eine verschlüsselte E-Mail geschickt

werden, indem der Absender den öffentlichen Schlüssel des Empfängers vom Server herunterlädt und zur Verschlüsselung verwendet und damit verhindert, dass ein Betrüger ihm seinen öffentlichen Schlüssel unterjubeln könnte anstatt des öffentlichen Schlüssels des echten E-Mail-Empfängers. Der öffentliche Schlüssel eines Benutzers gilt als vertrauenswürdig, falls dieser mit einem Zertifikat einer PKI verbunden ist oder durch eine vertrauenswürdige Zertifikationsstelle (CA) signiert wurde.

PUBLIC KEY CERTIFICATE (engl.)
Übsg. Digitales Zertifikat für öffentliche Schlüssel. Dieses Zertifikat bestätigt die Richtigkeit eines öffentlichen Schlüssels und seiner Herkunft, sodass dieser Schlüssel für eine sichere Kommunikation mit dem Schlüsselbesitzer benutzt werden kann.

PUBLIC KEY CRYPTOGRAPHY [PKC] (engl.)
Übsg. Asymmetrisches Kryptosystem. Verfahren zur Verschlüsselung, zur Authentifikation sowie zur Erstellung und Benutzung digitaler Signaturen. Bei asymm. Kryptografie wird jeweils für eine Person oder ein System ein Paar aus zwei mathematisch zusammengehörigen Schlüsseln erstellt: ein öffentlicher Schlüssel („Public Key“) und ein privater Schlüssel („Private Key“). Zur Verschlüsselung einer Nachricht kann danach der öffentliche Schlüssel von jedermann verwendet werden. Die Entschlüsselung gelingt nur dem Besitzer des zugehörigen privaten, geheimen Schlüssels.

PUBLIC KEY DISTRIBUTION (engl.)
Übsg. Verteilung öffentlicher Schlüssel

PUBLIC KEY INFRASTRUCTURE [PKI] (engl.)
Übsg. Infrastruktur für asymm. Kryptografie. Software und Hardware zur Erstellung, Herausgabe, Bearbeitung, Verteilung, Benutzung, Speicherung und Löschung von vertrauenswürdigen digitalen Zertifikaten. Eine PKI verbindet öffentliche Schlüssel mit den zugehörigen Identitäten. Von einer PKI erstellte und herausgegebene Zertifikate werden mit einem Root-Zertifikat verbunden und einer Identität, bspw. einer Person, zugewiesen. Damit ist das Zertifikat rückverfolgbar vertrauenswürdig und die Gültigkeit der mit diesem Zertifikat verbundenen Schlüssel kann bestätigt werden. Dies verhindert auch das Problem, dass es ansonsten einem Betrüger möglich wäre, seinen öffentlichen Schlüssel anstatt des öffentlichen Schlüssels des echten Empfängers den Sendern von Nachrichten unterzujubeln, sodass der Betrüger die gesendete, verschlüsselte Nachricht mit seinem zugehörigen privaten Schlüssel entschlüsseln könnte.

PUBLIC KEY SEARCHABLE ENCRYPTION (engl.)
Übsg. Durchsuchbare Verschlüsselung, basierend auf dem öffentlichen Schlüssel. Ein Benutzer bereitet eine geheime Nachricht und eine bestimmte Datenstruktur vor, bevor er beides mit seinem öffentlichen Schlüssel oder dem öffentlichen Schlüssel einer anderen Person verschlüsselt und auf einen Server hochlädt. Nur die Person, die

Kenntnis des privaten Schlüssels und der Datenstruktur hat, kann die geheime Nachricht auch in verschlüsselter Form durchsuchen, ohne einen großen Teil davon im Server offenlegen zu müssen. Verwandt mit homomorpher Verschlüsselung und Hidden Vector Encryption (HVE).

PUBLIC-KEY-VERSCHLÜSSELUNG
Übsg. Verschlüsselung, basierend auf einem öffentlichen Schlüssel. Syn. zu asymmetrischer Verschlüsselung. Für eine Person oder System wird ein Paar aus zwei mathematisch zusammengehörigen Schlüsseln erstellt: ein öffentlicher Schlüssel („Public Key“) und ein privater Schlüssel („Private Key“). Zur Verschlüsselung einer Nachricht kann danach der öffentliche Schlüssel von jedermann verwendet werden. Die Entschlüsselung gelingt nur dem Besitzer des zugehörigen privaten, geheimen Schlüssels. Mit einem Zertifikat für den öffentlichen Schlüssel, ausgestellt oder signiert von einer Zertifizierungsstelle (CA) oder einer PKI, kann auch sichergestellt werden, dass der öffentliche Schlüssel wirklich von der richtigen Person stammt.

PUBLIC NETWORK (engl.)
Übsg. Öffentliches Netzwerk. Beispiel: Internet.

PUBLISHED APPS (engl.)
Übsg. Veröffentlichte Applikation. Bei Citrix-Lösungen können Applikationen zentral auf einem Server installiert und konfiguriert werden, um diese dann Benutzern, welche den Citrix-Client auf ihren Geräten verwenden, auf ihrem üblicherweise benutzten Desktop anzubieten.

PUBLISHED DESKTOP (engl.)
Übsg. Veröffentlichte Benutzeroberfläche. Bei Citrix-Lösungen können ganze Desktops auf einem Server zentral installiert und konfiguriert werden, um diese dann Benutzern anzubieten, welche den Citrix-Client auf ihren Geräten verwenden. Damit lässt sich bspw. ein Linux-Desktop virtuell auf einem Windows-PC bereitstellen ohne eine Installation durch den Anwender.

PUBLISHING LICENSE [PL] (engl.)
Übsg. Lizenz zur Veröffentlichung. Bei Microsoft ADRMS benutztes Zertifikat, welches eingesetzt werden kann, um bei einer RMS-verschlüsselten Nachricht Zugriffsrechte vorzugeben, wie bspw. das Recht, die Nachricht anzusehen, zu bearbeiten, zu drucken, zu kopieren usw. Diese PL wird mit dem verschlüsselten Dokument kombiniert, mit dem „Client Licensor Certificate“ (CLC) des Senders signiert, und mit dem öffentlichen Schlüssel des „Server Licensor Certificate“ (SLC) verschlüsselt, sodass nur der RMS-Server und der Sender diese Nachricht komplett entschlüsseln können. Empfänger der verschlüsselten Nachricht können diese lesen, drucken, kopieren usw., falls die

entsprechenden vom Sender vorgegebenen Zugriffsrechte in der Publishing License definiert wurden.

PUFFER-ÜBERLAUF
Ereignis bei der Speicherung von Daten in einen zu kleinen Speicherbereich.

PUK
Abk. für Personal Unblocking Key. Übsg. Persönlicher Entsperrungsschlüssel. Code vom Mobilfunkanbieter, mit dem sich eine SIM-Karte in einem Handy wieder entsperren lässt.

PUNKT-ZU-PUNKT-SICHERHEIT
Gesicherte Kommunikation zw. Systemen. Ein Beispiel ist der Versand von E-Mails mittels eingestellter TLS-Verschlüsselung vom und zu den Mail-Servern. Ergänzt werden kann dies durch Endpoint-Verschlüsselung, wodurch eine End-to-End-Sicherheit entsteht.

PUNYCODE
Verfahren zur Umwandlung von Domain-Namen aus Unicode (UTF-8) zu Domain-Namen aus ASCII-Code mit dem eingeschränkten Zeichensatz aus den 37 Zeichen a–z, 0–9 und –. Siehe auch IDNA.

Beispiel: Der Domain-Name „bücherverlag.ch“ wird im Webbrowser umgewandelt in „xn--bcherverlag-thb.ch“.

PUSH RELAY (engl.)
Übsg. Anfrageweiterleitung

PUT
Syn. zu HTTP-PUT

PUTTY
Freies, Open-Source Terminal-Emulator-Programm. Dieses bietet viele Authentisierungsmöglichkeiten an, um verschlüsselte Verbindungen aufzubauen, sodass PuTTY als SecureShell (SSH)-Client-Applikation benutzt werden kann.

PVP
Abk. für Player Versus Player. Spielmodus bei Computerspielen.

PWD
Abk. für Password

PWGRAB
Modul innerhalb der TrickBot-Schadsoftware, welches wahrscheinlich Login-Daten und Passwörter aus Internet Explorer, Firefox, Chrome, Edge, Outlook, Filezilla und WinSCP stiehlt.

PYTHON
Umfangreiche, höhere Programmiersprache, die einfach zu erlernen ist und mithilfe von Funktionsbibliotheken in vielen Bereichen eingesetzt wird, bspw. in Data Science und künstlicher Intelligenz.

Q

19

QKD
Abk. für Quantum Key Distribution

QNX
Unix-kompatibles Betriebssystem für eingebettete Systeme.

QOS
Abk. für Quality of Service

QRA
Abk. für Quantum-Resistant Algorithms

QR-CODE
Abk. für Quick Response, Übsg. Schnelle Antwort. Viereckige Grafik, deren Struktur einer Datencodierung entspricht. Haupteinsatzbereich ist der direkte Zugang zur Internetseite durch das Abscannen des QR-Codes mit einer entsprechenden App bspw. vom Bildschirm, von einem Plakat oder von einer Werbungsbroschüre. Außer Internetadressen können ebenso Texte, auch verschlüsselte, in QR codiert werden. QR-Codes werden ebenfalls von Banken und anderen Firmen benutzt, um die Sicherheit beim Login durch einen weiteren Faktor zu erhöhen, dadurch, dass bspw. die E-Banking-App eine eigene sichere Verbindung aufbaut und mit dem speziell für diese Session erzeugten und auf der E-Banking-Seite angezeigten QR-Code verifiziert. Risiken bestehen bei QR-Codes durch unprofessionelle Apps, welche die codierten, allenfalls verseuchten Internetseiten sofort öffnen, ohne die Internetadresse vom Benutzer vorher bestätigen zu lassen (siehe Abb. 19.1).

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z*,
https://doi.org/10.1007/978-3-662-60911-8_19

Abb. 19.1 Beispiel eines QR-Codes, welcher den Text „IT Security A-Z“ codiert beinhaltet

QRNG
Abk. für Quantum Random Number Generation

QUALITY OF SERVICE [QOS] (engl.)
Übsg. Qualitätsgüte. Dies kann bspw. eine Beschreibung von Anforderungen an einen Kommunikationsdienst sein, um sicherzustellen, dass die Kommunikation rasch aufgebaut, stabil und zuletzt sicher getrennt wird.

QUANT
1) Quantenmechanisches Objekt, bspw. ein Lichtteilchen (sog. „Photon“), ein Elektron, ein Atom usw. 2) Berufsbezeichnung für Mathematiker

QUANTENKOMMUNIKATION
Austausch von Informationen, die in Quantensystemen gespeichert sind. Mögliche Verfahren zur sicheren Kommunikation über weite Entfernungen sind:

a) Quantentransport, z. B. Transport eines Lichtteilchens (sog. „Photon“) durch eine Glasfaser.
   Die Naturgesetze der Quantenphysik verbieten die Teilung eines Lichtteilchens. Deshalb kann ein Hacker nicht einfach die Hälfte eines Lichtteilchens abzwacken und abhören. Das Lichtteilchen würde dadurch komplett zerstört. Auch kann er nicht einfach ein anderes Lichtteilchen senden, da er die Lichtpolarisation des ursprünglichen Lichtteilchens aufgrund der Quantenphysik nicht mit einer Messung eindeutig bestimmen kann und somit sein neu verschicktes Lichtteilchen eine andere Polarisation hätte als dasjenige des ursprünglich gesendeten. Beides kann vom Empfänger der Quantenkommunikation entdeckt werden und damit die Kommunikation als ungültig erkennen.
b) Quantenteleportation durch Replikation des Quantenzustands. Die Korrelation (sog. „Quantenverschränkung“) zweier Quantenteilchen ermöglicht die Übertragung des Quantenzustands, d. h. der Information, des einen Quants zum korrelierten Quant an einem anderen Ort. Jeder Manipulationsversuch würde die Quantenverschränkung aufbrechen und die Kommunikation als ungültig erkannt werden. Quantenteleportation kann jedoch nicht schneller als mit Lichtgeschwindigkeit erfolgen und es bestehen Limiten bei der Informationsübertragung.

QUANTENKOMMUNIKATIONSPROTOKOLL
Regeln zur Form und Art der Quantenkommunikation zwischen zwei Parteien. Dieses Protokoll wird u. a. dazu verwendet, um einen sicheren Austausch von privaten Schlüsseln zwischen zwei Parteien zu ermöglichen, wobei der Schutz der Schlüssel durch die Quantenphysik garantiert ist. Das häufigste Protokoll („BB84“) benutzt definierte Polarisationsrichtungen von Lichtteilchen. Beim Sender werden Lichtteilchen mit zufällig bestimmten Polarisationen erzeugt. Die Lichtteilchen werden über einen Quantenkanal gesendet und die Polarisationen klassisch gespeichert. Der Empfänger setzt Polarisationsfilter mit zufällig bestimmten Richtungen ein. Der Vergleich der Resultate zwischen ursprünglicher Polarisation und beim Empfänger detektierten Lichtteilchen nach den Polarisationsfiltern würde eine Man-in-the-Middle-Attacke erkennen lassen.

QUANTENTELEPORTATION
Übermittlung von Informationen mittels Qubits, bspw. mittels Lichtteilchen. Dazu werden verschränkte, d. h. quantenphysikalisch gekoppelte Qubits vorbereitet und die Qubit-Paare aufgeteilt auf Sender und Empfänger. Danach kann der Sender die zu sendende Nachricht als Quantenzustände seiner Qubits codieren, wodurch zeitgleich ohne aktive Kommunikation die verschränkten Qubits beim Empfänger die gleichen Quantenzustände einnehmen.

QUANTENVERSCHRÄNKUNG
Syn. zu Quantenkorrelation, Quantum Entanglement. Mögliche Eigenschaft von einzelnen Quanten in einem System von Quanten, bei welchen die Quanten quantenphysikalisch gekoppelt sind. Auch bei großer Distanz wirkt sich eine Änderung eines Quants gleichzeitig an einem anderen, verschränkten Quant aus, jedoch nicht mit Überlichtgeschwindigkeit.

QUANTENVOLUMEN
Maß für die Leistungsfähigkeit von Quantenchips, unter Berücksichtigung von signifikanten Fehlerraten.

QUANTIFIED SELF MOVEMENT (engl.)
Übsg. Quantifizierte Eigenbewegung. Syn. zu Lifelogging

QUANTUM CHANNEL (engl.)
Übsg. Quantenkanal. Kombination von Lichtleiter, z. B. Glasfaser und Übertragungsinfrastruktur beim Sender und Empfänger.

QUANTUM COMMUNICATION PROTOCOL (engl.)
Übsg. Quantenkommunikationsprotokoll

QUANTUM COMPUTER (engl.)
Übsg. Quantencomputer. Angestrebtes Gerät, welches statt mit klassischen Bits mit quantenmechanischen Qubits rechnet und dadurch Rechnungen um ein Vielfaches schneller lösen kann, da Qubits nicht nur die Werte „0“ oder „1“ annehmen können wie klassische Bits, sondern mit allen Überlagerungswerten dazwischen gleichzeitig rechnen. Im Jahre 2018 wurde erstmals ein Quantencomputer mit 72 Qubits aufgebaut. Man geht davon aus, dass Tausende Qubits in einem Quantencomputer benötigt werden, um schneller zu sein als klassische Computer.

Beispiel der Vorteile eines Quantencomputers: Bei der klassischen Suche nach Daten in einer Datenbank werden alle Einträge in Indexlisten nacheinander geprüft. Mit Quantencomputern könnten mehrere oder sogar alle Einträge in den Indexlisten gleichzeitig untersucht werden.

QUANTUM CRYPTOGRAPHY (engl.)
Übsg. Quantenkryptografie. Technologie zur sicheren Verteilung von symm. Schlüsseln zwischen zwei Parteien. Die Sicherheit des Schlüsselaustauschs ist durch die Gesetze der Quantenphysik garantiert.

QUANTUM ENTANGLEMENT (engl.)
Übsg. Quantenverschränkung

QUANTUM INTERNET (engl.)
Verbund von Systemen, die Daten mittels Quantenkommunikation austauschen.

QUANTUM KEY DISTRIBUTION [QKD] (engl.)
Übsg. Schlüsselaustausch basierend auf quantenphysikalischen Eigenschaften von Quantenteilchen, sog. Qubits, bspw. Lichtteilchen. Dies soll das klassische Schlüsseltauschproblem verhindern. Dabei ist die Idee, die Unversehrtheit des Schlüsselaustauschs durch die Gesetze der Quantenphysik zu schützen, sodass die mit diesen symm. Schlüssel verschlüsselten Informationen auch in den nächsten Jahrzehnten noch sicher sind. Die Sicherheit während des Schlüsselaustauschs ist dabei dadurch gegeben, dass die Zustände von Qubits bei jedem Versuch eines Angriffs durch eine Man-in-the-Middle-Attacke verändert würden. Dies kann beim Empfänger des Schlüssels eindeutig detektiert werden. Falls die Qubit-Zustände korrekt ankommen, kann der Schlüssel für die Verschlüsselung von Informationen benutzt werden, da nur die zwei Parteien diesen Schlüssel kennen.

QUANTUM KEY RATE (engl.)
Übsg. Quantenschlüsselrate. Anzahl der Qubits pro Sekunde, die kommuniziert werden.

QUANTUM MEMORY (engl.)
Gerät, welches ein Lichtteilchen (sog. Photon, aba. Qubit) über eine gewisse Zeit speichern und wieder mit gleichen Eigenschaften emittieren kann. Dies wird bspw. dadurch erreicht, dass das Photon seine Energie an ein hochkohärentes, atomares System abgibt, dieses System dann diese zusätzliche Energie behält und erst nach einer Weile in Form einer Photonemission wieder abgibt.

QUANTUM RANDOM NUMBER GENERATION [QRNG] (engl.)
Übsg. Zufallszahlerzeugung mittels Quantenphysik. Beim Durchgang eines Lichtteilchens durch einen halbdurchlässigen Spiegel ist es aufgrund der quantenphysikalischen Eigenschaften des Lichtteilchens statistisch zufällig, ob das Lichtteilchen am Spiegel reflektiert oder durch diesen hindurch transmittiert wird. Dies lässt sich zur Erzeugung von perfekt zufälligen Binärzahlen benutzen.

QUANTUM REPEATER (engl.)
Übsg. Quantenwiederholer. Methode, um die Absorptionsverluste bei direkter Punkt-zu-Punkt-Quanten-Kommunikation innerhalb einer Glasfaser zu beheben.

Möglichkeiten der Implementation von Quantum Repeater sind:

a) Nutzung der Korrelationseigenschaft zweier Qubits, welche über sehr große Distanzen erhalten bleibt.
b) Zwischenspeicherung in Quantum Memory.

QUANTUM-RESISTANT ALGORITHMS [QRA] (engl.)
Übsg. Quantenresistente Algorithmen. Syn. zu Quantum-Safe Cryptography. Berechnungsmethoden, wie bspw. Verschlüsselung, welche auch mittels Quantencomputer in absehbarer Zeit nicht geknackt oder manipuliert werden können.

QUANTUM-SAFE CRYPTOGRAPHY (engl.)
Übsg. Quantensichere Kryptografie. Syn. zu Quantum-Resistant Algorithms. Kryptografische Algorithmen wie bspw. Verschlüsselung, welche in absehbarer Zeit auch mit Quantencomputer nicht in vernünftiger Zeit geknackt werden können.

QUANTUM SECURITY (engl.)
Übsg. Quantensicherheit. Teilgebiet der Cyber- und IT-Sicherheit. Ziel ist die Verhinderung von Angriffen, Missbrauch und Datenverlust bei oder mittels Quantensystemen.

QUANTUM SUPREMACY (engl.)
Übsg. Quantenüberlegenheit. Zeitpunkt, an welchem ein Quantencomputer eine Berechnung oder Aufgabe schneller lösen kann als ein klassischer Computer.

QUANTUM TELEPORTATION (engl.)
Übsg. Quantenteleportation

QUARANTINING (engl.)
1) Anpassung von Daten, sodass diese zwar noch immer eine Person identifizieren könnten, die jedoch keinen Kontext mehr besitzen und somit nicht für die Identifizierung von Personen benutzt werden können. Beispiel: der Name „Peter". 2) Wegspeichern von Dateien, die evtl. von Schadsoftware verändert wurden, oder die evtl. selber Schadsoftware beinhalten.

QUBIT
Abk. für „Quanten"+„Bit". Quantenmechanische Objekte, wie Photon, Elektron usw., die viele Zustände annehmen können, und erst bei der Messung genau einen von zwei Zuständen annehmen. Dies erlaubt, Qubits als kleinste Speichereinheit in Quantencomputern zu benutzen, analog zur Einheit „Bit" klassischer Computer. Da jedes Qubit eines Systems von verschränkten, d. h. gekoppelten Qubits unendlich viele Zustände annehmen kann, kann dieses System gleichzeitig eine große Zahl an Totalzuständen einnehmen und für Berechnungen benutzt werden.

Anwendungsbeispiel für Qubits

Ein Lichtteilchen („Photon") als Qubit kann in alle Richtungen polarisiert sein und somit grundsätzlich viele Zustände annehmen. Erst eine Messung der Polarisation erlaubt die Bestimmung der Polarisationsstärke in horizontaler und vertikaler Richtung, entsprechend der Information „0" und „1". Drei solcher Qubits können als verschränktes System somit gleichzeitig alle Kombinationen 000, 001, 010, 011, 100, 101, 110, 110 einnehmen und bei Berechnungen mitberücksichtigen. Dies ermöglicht Quantencomputern, Berechnungen schneller auszuführen im Vergleich zu klassischen Computern. ◀

QUELLOFFENE SOFTWARE
Syn. zu Open Source. Meist kostenlose Software, bei welcher der Programmcode (sog. Quelltext) öffentlich von jedermann im Detail eingesehen, geändert, angepasst und genutzt werden kann. Autoren von Open-Source-Software können die Benutzung jedoch auch einschränken.

QUORUM
1) Beschlussfähige, minimale Anzahl von Mitgliedern einer Gruppe. 2) Methode bei Server-Clustern, um die Datenintegrität im Fall eines Teilausfalls sicherzustellen. Bspw. werden drei Server in einem Cluster zu einem Quorum zusammengefasst, sodass immer mind. zwei davon aktiv sind.

R

20

R45J KABEL
Syn. zu Patch-Kabel

RABBIT
Strom-Chiffre

RAC
Abk. für Rights Account Certificates

RADIUS
Abk. für Remote Authentication Dial-In User Service

RAID
Abk. für Redundant Array of Independent Disks

RAINBOW TABLE (engl.)
Übsg. Regenbogen-Tabelle. Liste von vorberechneten Paaren von Passwörtern und deren Hash-Werten. Gestohlene Hash-Werte können mit einer Rainbow-Liste verglichen werden, um dadurch die ursprünglichen Passwörter zu bestimmen, falls die gestohlenen Hash-Werte kein Salt enthalten.

RAMNIT
Schadsoftware aus dem Jahr 2011. Diese infiziert interne Speicher, USB-Sticks und andere Wechselspeicher dadurch, dass sie sich im Master Boot Record (MBR) versteckt.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_20

RANDOM
Funktion in Linux und Max OS X zur Generierung von Zufallszahlen. Genauer Ort: „/dev/random“

RANDOM NUMBER (engl.)
Übsg. Zufallszahl

RANSOM DEMAND THREATENING (engl.)
Übsg. Bedrohung durch Lösegeldforderung.

RANSOMWARE (engl.)
Übsg. Erpressungssoftware. Schadsoftware, die sich versteckt auf dem Computer oder Handy einnistet, bspw. durch einen versehentlichen oder im Hintergrund versteckt ablaufenden Download von einer verseuchten Internetseite. Sobald diese Malware startet oder aus dem Internet ferngesteuert gestartet wird, verschlüsselt sie alle erreichbaren Daten oder gibt vor, diese verschlüsselt zu haben, und verlangt ein Lösegeld in Form von Bitcoins u. Ä., um die Daten wieder zugänglich zu machen. Statt Verschlüsselung wird z. T. auch eine Offenlegung der persönlichen Daten im Internet angedroht. Bei Zahlung des Lösegeldes erhält das Opfer im besten Fall den Code zur Entschlüsselung der Daten, jedoch werden dadurch solche kriminellen Aktivitäten lukrativ und weitere Attacken mitfinanziert. Der beste Schutz vor Ransomware ist ein regelmäßiges Backup des Computers oder Handys, auf einem nicht dauernd angehängten Backupsystem, z. B. einer externen Festplatte.

RASP
Abk. für Runtime Application Self-Protection

RAT
Abk. für Remote Access Trojan

RBAC
Abk. für Role-Based Access Control

RC4
Weitverbreitete Strom-Chiffre und Verschlüsselungsalgorithmus. Diese wurde u. a. in SSL und WEP eingesetzt. Kern des Algorithmus ist die Benutzung einer zufälligen Permutation des Alphabets, die mit dem Nachrichtenstrom XOR-verknüpft wird. Die Entschlüsselung geschieht auf gleiche Weise mit der gleichen Alphabetpermutation. Seit 2015 für TLS verboten aufgrund von Sicherheitsmängeln. Das BSI und andere Institutionen raten grundsätzlich davon ab, RC4 zu verwenden, da Angriffe auf Teile bereits erfolgreich waren. ARC4 basiert auf RC4 und ist im Vergleich dazu Open-Source.

RCE
Abk. für Remote Command Execution, Remote Code Execution.

RCE FLAW
Abk. für Remote Code Execution Flaw. Fehler in einer Software, durch welchen aus der Ferne ein Programm auf einem PC ausgeführt werden kann.

RCP
Abk. für Remote Control Protocol

RCS
Abk. für Rich Communication Services

REAPER
Erstes Anti-Viren-Programm in den 1970er-Jahren, welches den ersten Virus „Creeper" eliminierte.

RECHTE
Abk. für Zugriffsrechte, Benutzungsrechte, Zugangsrechte.

RECOVERY OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Wiederherstellung eines kryptografischen Schlüssels.

RED TEAM
Hacker-Gruppe mit positiven Absichten, die Firmen helfen sich, vor Angriffen anderer Hacker zu schützen, bspw. dadurch, dass das RED-Team durch erlaubten Versuch, die Firma anzugreifen, Schwachstellen aufzeigt.

RED TEAM TESTERS
Tester, die ein neues System oder eine neue Software von außerhalb der Gruppe oder der Firma auf Schwachstellen überprüfen.

REDUNDANT ARRAY OF INDEPENDENT DISKS [RAID] (engl.)
Übsg. Gruppe von redundanten, unabhängigen Festplatten. Methode, um Festplatten in redundanter Form zusammenzufügen, um Datenverlust bei Ausfall einer Festplatte zu verhindern.

REGEDIT.EXE
Programm zur Bearbeitung von Konfigurationsdaten innerhalb Microsoft Windows Versionen seit 1992 (Windows 3.1). Diese Daten werden in der Windows-Registrierungsdatenbank gespeichert, Syn. zu Registry.

REGELN
Viele Systeme und Programme sind konfigurierbar und bieten die Möglichkeit, Regeln zu konfigurieren, welche Inputs oder Trigger auswerten, mit Bedingungen verknüpfen und Aktionen ausführen. Bspw. bieten viele moderne E-Mail-Programme die Möglichkeit, ankommende E-Mails von bestimmten Personen oder mit bestimmten Texten direkt als wichtig zu markieren und in einen Ordner zu verschieben.

REGEX
Abk. für Regular Expression. Zeichenkette, die definiert, welche Daten eines Textes herausgefiltert oder markiert werden sollen (siehe auch eine RegEx-Zusammenstellung im Anhang bei Kap. 34).

RegEx-Beispiele

a) Ein „x“ filtert oder markiert alle „x“ eines Textes.
b) Der Ausdruck „[A-Za-z0-9]“ filtert oder markiert einen beliebigen lateinischen Buchstaben von A bis Z oder eine beliebige Ziffer.

REGISTRIERUNGSDATENBANK
Konfigurationsdaten innerhalb Microsoft-Windows-Versionen seit 1992 (Windows 3.1). Syn. zu Registry.

REGISTRY (engl.)
Übsg. Registrierungsdatenbank

REGRESSION TESTING
Software-Tests, welche wiederholt ausgeführt werden, um grundlegende Funktionen nochmals zu überprüfen, bspw. nach der Modifikation von Komponenten.

REGULATORISCHE VORGABEN
Gesetze und Vorschriften, die von lokalen oder globalen Regulatoren und Behörden vorgegeben werden und eingehalten werden müssen, um Geschäfte in regulierten Märkten tätigen zu dürfen. Ein Beispiel ist die Verordnung „EU GDPR“, die seit Mai 2018 für den Datenschutz von persönlichen Daten eingehalten werden muss.

REINFORCEMENT LEARNING (engl.)
Übsg. Lernen durch Verstärkung. Algorithmus des maschinellen Lernens innerhalb der künstlichen Intelligenz, bei welchem das System die jeweils nächste Aktion aus allen möglichen Aktionen anhand von positiven und negativen Belohnungen erlernt und dadurch seine totale Belohnung mit jeder Aktion maximiert. Reinforcement Learning ist eine von drei grundlegenden Lernmethoden des maschinellen Lernens neben Supervised und Unsupervised Learning.

REKALL
Offene und freie Sammlung von Speicher-Analyse-Techniken.

RELATIVE IDENTIFIER [RID] (engl.)
Letzte drei Stellen der SID eines Windows-User-Konto. Diese beschreiben codiert die Berechtigungen des Nutzers, bspw. ob der Benutzer Admin-Rechte besitzt.

RELEASE-MANAGEMENT (engl.)
Übsg. Veröffentlichungsmanagement. Bearbeitung und Planung von größeren Software-Updates für Systeme. Geht einher mit Patch-Management, bei welchem kleinere Teile aktualisiert werden zwischen den großen Releases.

REMEDIATION (engl.)
Übsg. Mängelbeseitigung

REMOTE ACCESS (engl.)
Übsg. Fernzugriff

REMOTE ACCESS TROJAN [RAT] (engl.)
Übsg. Fernzugriffstrojaner. Schadsoftware, welche es Hackern erlaubt, die infizierten PCs aus der Ferne zu kontrollieren.
Beispiel: LuninosityLink

REMOTE AUTHENTICATION DIAL-IN USER SERVICE [RADIUS] (engl.)
Übsg. Fernauthentisierungsdienst für sich einwählende Benutzer. Sicherheitsprotokoll für Client-Server-Systeme (wie z. B. Internet, Intranet u. a.) zur Authentifizierung, Autorisation und Verrechnung (Accounting) und zur Kontrolle der Zugriffsberechtigung.

REMOTE CODE EXECUTION [RCE] (engl.)
Syn. zu Remote Command Execution

REMOTE COMMAND EXECUTION [RCE]
Übsg. Ausführen von Befehlen mittels Fernzugriff.

REMOTE CONTROL PROTOCOL [RCP] (engl.)
Übsg. Fernsteuerungsprotokoll. Programm und Definitionen zur Übertragung von Daten zwischen PCs in einem Netzwerk. Von RCP wird abgeraten, da die Daten nicht verschlüsselt übertragen werden. SCP gilt als Nachfolger und bietet den sicheren Transfer via SSH.

REMOTE DESKTOP PROTOCOL [RDP] (engl.)
Übsg. Desktop-Fernsteuerungsprotokoll. Netzwerkprotokoll für den Fernzugriff von PCs. Bildschirmausgaben, Maus- und Tastatureingaben werden übertragen, um die Ausgaben des fernen PCs darzustellen und zu steuern. Mittels TLS können RDP-Verbindungen gesichert werden.

REMOTE DESKTOP SERVICES [RDS] (engl.)
Übsg. Desktopfernsteuerungsdienste. Komponente von Microsoft Windows Servern, die den Benutzern sowohl ganze Windows-Desktops als auch einzelne Apps in einem „Kiosk-Modus“ über eine Netzwerkverbindung anbietet, wobei diese auf dem Server ausgeführt werden und auf dem vom Benutzer eingesetzten System dargestellt werden, wie bspw. auf einem Thin Client.

REMOTE-EXPLOITS (engl.)
Übsg. Fernsteuerungsschwachstellen. Fehler in Programmen oder Netzwerken, die ausgenutzt werden, um diese aus der Ferne zu attackieren.

REMOTE SHELL [RSH] (engl.)
Übsg. Fernsteuerungsumgebung. Software unter Unix, um mittels Fernzugriff auf einem anderen PC Programme auszuführen. Es wird empfohlen, stattdessen SSH zu nutzen.

REMOTE-ZUGRIFF
Benutzung eines Computers aus der Ferne von einem anderen Computer aus. Es stehen Programme zur Verfügung, die diesen Zugriff unverschlüsselt oder verschlüsselt ermöglichen, wie z. B. RDP und PuTTY, früher Telnet. Gründe für solche Remote-Zugriffe sind bspw. die Administration von Servern und die Benutzung eines schnellen Computers von einem einfacheren PC aus.

REQUEST (engl.)
Übsg. Anfrage. Begriff wird bspw. im Zusammenhang mit „Request and Response“ verwendet.

REQUEST AND RESPONSE (engl.)
Übsg. Anfrage und Antwort. Kommunikation, bei dem ein Client eine Anfrage („Request“) an einen Server schickt und daraufhin eine Antwort („Response“) vom Server erhält. Bspw. sendet ein Internetbrowser eine Anfrage und erhält die Antwort in Form einer Internetseite. Damit sich Client und Server verstehen, bedarf es einer strukturierten Kommunikation, welche in einem Protokoll definiert ist.

REQUEST FOR COMMENTS [RFC] (engl.)
Übsg. Anfrage für Kommentare. Sammlung detaillierter Beschreibungen und Definitionen zu Internet- und Netzwerkthemen, begonnen 1969. Jede dieser Beschreibungen erhält eine eindeutige Nummer.

Bespiel: RFC8017 beschreibt das Format der RSA-Verschlüsselung. Syn. zu PKCS#1.

RESILIENCE (engl.)
Übsg. Widerstandsfähigkeit

RESILIENCE AGAINST MALICIOUS CYBER INCIDENTS (engl.)
Übsg. Widerstandsfähigkeit gegen böswillige Cyber-Vorfälle.

RESILIENT
Syn. zu belastbar

RESILIENZ
Syn. zu Widerstandsfähigkeit

RESPONSE (engl.)
Übsg. Antwort. Wird bspw. im Zusammenhang mit „Request and Response“ verwendet.

RESSOURCEN
Festplatten, Dateien, CD-Laufwerke, CPUs, Computersystems usw.

RESSOURCEN-REPOSITORY
Datenbank, in der wichtige Eigenschaften jeder Ressource einer Firma oder eines Netzwerks gespeichert sind. Dies ermöglicht die eindeutige, korrekte und sichere Identifikation jeder Ressource über deren ganzen Lebenszyklus hinweg.

REST/RESTFUL
Abk. für Representational State Transfer. Übsg. Repräsentative Zustandsübertragung. Strukturdefinitionen und Bereitstellung grundlegender Strukturvorlagen für Webservices mit dem Ziel einheitlicher Schnittstellen für Maschinen-zu-Maschinen-Kommunikation. Alternative zum älteren SOAP.

RESTRICTED DOMAIN (engl.)
Übsg. Eingeschränkte Domäne

RETENTION PERIOD (engl.)
Übsg. Aufbewahrungsdauer

REVERSE ENGINEERING (engl.)
Verfahren und Tools, um die Programmzeilen (den Quellcode) einer Software, die nur als ausführbarer Code vorliegt, zurückzugewinnen. Dies wird bspw. benutzt, um Viren oder Ransomware zu verstehen und dadurch geeignete Gegenmaßnahmen zu entwickeln.

REVERSE PROXY (engl.)
Übsg. Umgekehrtes Stellvertretersystem. System, welches sich zwischen einem Client und mehr als einem Server steht. Dabei muss der Client die Adressen der Server nicht kennen, sondern nur des Reverse Proxy. Dies erlaubt v. a. eine Lastverteilung (Loadbalancing) zwischen den Servern. Außerdem ermöglicht dies die Zwischenspeicherung von transferierten Daten, die Authentisierung des Benutzers gegenüber den Servern und die Verschlüsselung des Transfers.

REVOCATION OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Annullierung eines kryptografischen Schlüssels.

REVOKE (engl.)
Übsg. Widerrufen. Beispiel: Ein Zertifikat kann widerrufen werden, damit es nicht mehr benutzt werden kann, falls es kompromittiert wurde.

RFC
Abk. für Request for Comments

RFID
Abk. für Radio-Frequency Identification. Übsg. Identifikation mittels Radiofrequenz. Automatische und berührungslose Identifikation und Lokalisierung von Objekten mithilfe von elektromagnetischen Wellen. Eingesetzt werden RFID-Transponder bei Kreditkarten, verschickten Paketen, Haustierimplantaten, Kleidern in Geschäften usw. Neben aktiven RFID-Transpondern, welche batteriebetrieben sind, erhalten passive RFID-Transponder die benötigte Energie zum Betrieb aus den elektromagnetischen Wellen des Senders.

RFID BLOCKER (engl.)
Hülle für Kreditkarten, um zu verhindern, dass Daten der Kreditkarte über RFID kontaktlos gestohlen werden oder sogar Geld abgebucht wird.

RHEL
Abk. für Red Hat Enterprise Linux

RICH COMMUNICATION SERVICES [RCS] (engl.)
Vom Industrieverband der internationalen Mobilfunkanbieter (GSM Association) als Nachfolger von SMS als Sofortnachrichtendienst geplant und in Handys von Samsung,

Google und anderen bereits integriert. Damit lassen sich bspw. Nachrichten, Bilder, Videos und Audiodateien versenden und der Sender kann erkennen, ob die Nachricht gelesen wurde. Weitere Funktionen werden laufend hinzugefügt mit dem Ziel, eine Alternative zu WhatsApp und ähnlichen Apps zu bieten.

RICH TEXT FORMAT [RTF]
Dateiformat für Texte. Zusammen mit den eigentlichen Textzeichen werden auch Metadaten wie Schriftart, Schriftgröße und andere Formatierungsdetails in der Datei gespeichert.

RID
Abk. für Relative Identifier

RID HIJACKING
2017 gefundene Angriffsmöglichkeit durch Ausnutzung der SID in Windows, um mehr Rechte auf dem Windows-System zu erlangen, indem die RID manuell verändert wird.

RIGHTS ACCOUNT CERTIFICATE [RAC] (engl.)
Übsg. Rechte-Konto-Zertifikat. Früher „Group Identity Certificate“ (GIC) genannt. Bei Microsoft ADRMS benutztes Zertifikat zur Identifikation des Benutzers. Bei der erstmaligen Authentifikation des Benutzers gegenüber dem Zertifizierungsserver einer ADRMS-Installation erhält der Benutzer eine RAC oder GIC, welche er danach für seine erneute Identifikation gegenüber dem ADRMS-Server benutzt. Die RAC wird ebenfalls verwendet, um andere Lizenzen zu verschlüsseln, bevor diese an diesen Benutzer geschickt werden.

RIGHTS MANAGEMENT CONNECTOR (engl.)
Von Microsoft Information Rights Management benutzte, ausgehende Schnittstelle zu anderen Produkten, um diesen Produkten Datenverschlüsselungsservices bereitzustellen.

RIGHTS MANAGEMENT SYSTEM [RMS] (engl.)
Auch Windows Rights Management System genannt. Vorgänger von Active Directory Rights Management System (ADRMS). Von Microsoft entwickelte Server-Client-Lösung zur Verschlüsselung und Entschlüsselung von E-Mails und Office-Dokumenten innerhalb der Windows-Umgebung sowie zur Rechtevergabe bei diesen verschlüsselten E-Mails und Dokumenten. Damit lässt sich erreichen, dass bspw. eine E-Mail nicht weitergeleitet werden kann oder auch, dass ein derart verschlüsseltes Dokument von niemandem außerhalb der Firma gelesen werden kann, der keinen Schlüssel und damit keine Berechtigung zur Entschlüsselung vom Server erhalten kann. Es wird in großen und kleinen Firmen dazu verwendet, Datenverlust zu verhindern und geistiges Eigentum zu schützen.

RIGHT TO BE FORGOTTEN (engl.)
Übsg. Recht, vergessen zu werden. Jede Person soll selber bestimmen können, welche Daten gespeichert werden und wie lange. Syn. zu Right to Erasure.

RIGHT TO ERASURE (engl.)
Syn. zu Right to be Forgotten.

RING FENCING (engl.)
Übsg. Abschirmung

RIPEMD-160
Abk. für RACE Integrity Primitives Evaluation Message Digest. Kryptografische Hash-Funktion, welche 160-Bit lange Hash-Werte erzeugt und bzgl. Stärke und Geschwindigkeit mit SHA-1 vergleichbar ist.

RIPPLE
Kryptowährung

RISIKOANALYSE VON CYBER-BEDROHUNG
Teil der Behandlung von Cyber-Bedrohungen.

RISIKOAPPETIT
Qualitative oder quantitative Angabe zur Akzeptanz einer Person, Gruppe oder Firma Risiken einzugehen. Bspw. zeigt ein risikoscheuer Aktienanleger einen kleineren Risikoappetit und wird eher sicherere Aktien kaufen.

RISK APPETITE (engl.)
Übsg. Risikoappetit

RISK ASSESSMENT OF CYBER THREATS (engl.)
Übsg. Risikoanalyse von Cyber-Bedrohungen.

RISKWARE (engl.)
Software, die unabsichtlich sicherheitskritische Funktionen beinhaltet, welche für Attacken missbraucht werden können.

RLOGIN
Abk. für Remote Login. Software für den Fernzugriff von einem PC auf einen anderen über ein Netzwerk oder über das Internet. Die ursprüngliche Version übermittelte Benutzername, Passwort und Inhalt unverschlüsselt. In Kombination mit Kerberos-Authentisierung kann die Kommunikation heutzutage verschlüsselt geschehen. Bessere Alternative ist das sicherere Secure Shell (SSH).

RMS
Abk. für Rights Management System, Active Directory Rights Management System.

ROBOT
Syn. zu Bot

ROBOTER-GESETZE
Von I. Asimov 1942 erstmals postulierte Gesetze für Roboter. In seiner überarbeiteten Version von 1983 lauten seine Roboter-Gesetze:

0. Ein Roboter darf die Menschheit nicht verletzen oder durch Passivität zulassen, dass die Menschheit zu Schaden kommt.
1. Ein Roboter darf keinen Menschen verletzen oder durch Untätigkeit zu Schaden kommen lassen, außer er verstieße damit gegen das nullte Gesetz.
2. Ein Roboter muss den Befehlen der Menschen gehorchen – es sei denn, solche Befehle stehen im Widerspruch zum nullten oder ersten Gesetz.
3. Ein Roboter muss seine eigene Existenz schützen, solange sein Handeln nicht dem nullten, ersten oder zweiten Gesetz widerspricht.

(Deutsche Übersetzung von Wikipedia, *Abgerufen am 22.12.2019)*

ROBOTIC PROCESS AUTOMATION SOFTWARE (engl.)
Übsg. Prozessautomatisierungsprogramm. Software, welche als technischer Benutzer automatisch Aktionen für Benutzer ausführt und damit den Benutzern aufwendige, repetitive Arbeiten abnimmt und schneller ausführt. Dies können bspw. Benutzereingaben, Mausklicks, Kopieren, Löschen, Internetseitenaufrufe, Auslesen von Bildschirmbereichen usw. sein. Syn. zu Bot.

ROBUST SECURITY NETWORK [RSN] (engl.)
Netzwerkprotokoll zur Erstellung und Aufrechterhaltung von sicherer Kommunikation über kabellose Datennetzwerke wie bspw. beim WLAN-Standard IEEE 802.11.

ROCA
Abk. für Return Of Coppersmith's Attack. Sicherheitslücke in der Software-Bibliothek RSALib von Infineon, welche bspw. in Chipkarten, TPMs und Yubikey 4 verwendet wird. Dabei kann ein privater Schlüssel mit weniger Aufwand anhand der Daten des öffentlichen Schlüssels gehackt werden.

ROGUEROBIN
Dateilose Schadsoftware, entdeckt 2018. Über eine Phishing-E-Mail, welche schädlichen Microsoft Excel Code beinhaltet, wird ein PowerShell-Skript ausgeführt, welches dem

Angreifer eine Hintertür zum PC öffnet. Obwohl die Schadsoftware zu Beginn ohne Datei startet, bleibt die Hintertür auch nach dem Ausschalten des PCs im System.

ROLE-BASED ACCESS CONTROL [RBAC] (engl.)
Übsg. Rollenbasierte Zugangskontrolle. Applikationen und Systeme erlauben häufig die Konfiguration von virtuellen Benutzergruppen. Benutzer mit ähnlichen Aufgaben in einer oder mehrerer solcher Applikationen und Systemen können zu diesen virtuellen Benutzergruppen hinzugefügt werden und erhalten dadurch automatisch die damit definierten Zugangsrechte.

ROMANCE SCAM (engl.)
Übsg. Romanzenbetrug. Betrug an einer Person, die den Betrüger über ein Dating-Portal kennenlernte. Häufig verlangt der Betrüger Geld vom Opfer mit dem Hinweis kurzfristiger Geldprobleme.

ROOT (engl.)
Übsg. Wurzel. 1) Abk. für Root Directory. Übsg. Wurzelverzeichnis. Höchstes Verzeichnis in einem Dateisystem. 2) Abk. für Root-Konto. Syn. zu SuperUser-Konto. Admin-Benutzerkonto, welches bei der Installation des PC-Betriebssystems angelegt wird.

ROOT-CA (engl.)
Übsg. Hauptzertifizierungsstelle

ROOTED DEVICE (engl.)
Syn. zu Jailbreaked Device. Handy, bei welchem der SuperUser-Zugang freigeschaltet wurde und damit alle Einstellungen, inkl. der Sicherheitseinstellungen, verändert werden können. Auch können Standard-Apps gelöscht und ersetzt werden. Apps, die einen bestimmten Level an Sicherheit benötigen, bspw. E-Banking Apps, werden bewusst so programmiert, dass sie nur auf Handys laufen, bei denen kein Jailbreak durchgeführt wurde.

ROOTEN
Syn. zu Jailbreak. Aufheben der eingeschränkten, üblichen Zugriffsrechte auf linuxbasierten Systemen, wie bspw. Android- oder iOS-Handys. Damit ist es möglich, vorinstallierte Software zu entfernen und andere, normalerweise eingeschränkte Änderungen durchzuführen. Auch lässt sich damit ein anderes und neueres Betriebssystem (sog. Custom-ROM) einspielen. Bei vielen Handy-Herstellern verliert man durch das Rooten die Gerätegarantie.

ROOTKIT
Programme, welche in einem attackierten System installiert werden, damit der Hacker sich zukünftig an diesem System anmelden kann, ohne entdeckt zu werden.

ROOT SHELL (engl.)
Kommandozeileninterpreter-Fenster auf Unix-PCs, welches via „sudo bash“ gestartet wird, und in welchem der Benutzer SuperUser-Rechte besitzt.

ROOT-TRUST-ANCHOR (engl.)
Übsg. Hauptvertrauensursprung. Digitale Zertifikate werden entlang einer Vertrauenskette bis zurück zum Root-Zertifikat, dem Hauptvertrauensursprung überprüft, bevor sie verwendet werden. Dem Root-Zertifikat muss vertraut werden und es muss deshalb von einer vertrauenswürdigen Beglaubigungsstelle ausgestellt worden sein. Auch Betriebssysteme und Webbrowser bieten eingebaute (selbstsignierte) Root-Zertifikate, um als Root-Trust-Anchor für Applikationen zu agieren.

ROOT-ZERTIFIKAT
Public-Key-Zertifikat einer Beglaubigungsstelle (CA). Diesem Basiszertifikat muss vertraut werden, damit darauf aufbauenden Zertifikaten in einer Vertrauenskette vertraut werden kann. Viele solche CA-Root-Zertifikate sind in aktuellen Webbrowser vorinstalliert.

ROUND ROBIN (engl.)
Übsg. Rundlaufverfahren. Methode zur Lastverteilung bei Ressourcen, wie z. B. Servern, bei welcher der Loadbalancer mehrere gleichartige Ressourcen gleichmäßig bedient. Andere Lastverteilungsmethode: Sticky.

ROUTER
Abk. für Netzwerkrouter. Gerät, welches Netzwerkpakete zwischen Rechnern innerhalb eines Netzwerks und über Netzwerkgrenzen hinaus weiterleitet. Bspw. verbindet ein Router den Heim-PC mit dem Internet.

RS-232
Abk. für Recommended Standard 232. Beschreibung und Steckertyp für die Kommunikation bei seriellen Computer-Ports, bspw. beim DB-25-Anschluss der für Drucker, Computermäuse etc. benutzt wurde.

RSA
Asymmetrisches kryptografisches Verfahren, erfunden von R. Rivest, A. Shamir und L. Adleman im Jahr 1977. RSA benutzt einen privaten und einen öffentlichen Schlüssel als Paar zusammengehörender Schlüssel und umgeht damit das Schlüsseltauschproblem, d. h. das unsichere Austauschen eines gemeinsamen Schlüssels.

Beispiel

Anwendungen von RSA sind bspw.:

a) Digitales Signieren. Dabei wird eine Nachricht mit dem geheimen, privaten Schlüssel verrechnet und kann von jedem mit dem öffentlichen Schlüssel überprüft werden.
b) Verschlüsselung. Dabei wird der öffentliche Schlüssel des Empfängers verwendet, sodass die verschlüsselte Nachricht nur vom Empfänger mit seinem dazugehörigen privaten Schlüssel entschlüsseln kann.

RSA SECUREID
Syn. zu „Authenticator Stick" der Firma RSA Security. Kleines Gerät, welches jede Minute einen Einmal-PIN erstellt und mit einer Applikation oder einem System synchronisiert ist, sodass dieser Einmal-PIN als 2FA eingesetzt werden kann.

RSH
Abk. für Remote Shell

RSN
Abk. für Robust Security Network

RTF
Abk. für Rich Text Format

RUBY
Höhere objektorientierte Programmiersprache. Ruby-Programme werden nicht komplett in Maschinensprache umgewandelt (kompiliert), sondern zur Laufzeit interpretiert.

RULE SET (engl.)
Übsg. Regeln

RUNTIME APPLICATION SELF-PROTECTION [RASP] (engl.)
Übsg. Eigenschutz von Applikationen zur Laufzeit. Sicherheitssoftware, welche während der Ausführung einer Applikation die Aufrufe und Befehle innerhalb der App überprüft und vor Attacken schützt, indem die App bspw. beendet wird.

RUP
Abk. für Rational Unified Process. Übsg. Rationaler, einheitlicher Prozess. Vorgehensmodell und Tools zur Software-Entwicklung. Wird auch als Grundlage für Projekte verwendet, bei denen keine Software erstellt wird, sondern bspw. Prozesse optimiert oder Produkte erstellt werden.

21

S3
Abk. für Simple Storage Service. Übsg. Einfacher Speicherdienst. Von Amazon eingeführter Filehosting-Dienst, basierend auf dem Konzept von Buckets und Objects, welche vergleichbar sind mit Verzeichnissen und Dateien.

SAAS
Abk. für Software as a Service

SABOTAGE
Tätigkeit, bei der absichtlich Maschinen, Computer, Software oder Prozesse gestört werden, um Personen, Firmen, Organisationen oder Infrastrukturen zu schaden. Dies stellt ein Risiko dar für Stromnetze, für Atomkraftwerke oder für Firmencomputernetzwerke. In der IT wird Sabotage häufig mittels eines eingeschleusten Virus, einem Trojaner (bspw. Stuxnet), einer DDoS-Attacke oder durch interne oder externe Firmenmitarbeiter durchgeführt.

SABOTAGENSCHUTZ
Methoden, Tools, Prozesse zum Schutz vor Sabotagen. Dies beinhaltet u. a. die Risikoanalyse, die Berücksichtigung von Sicherheitsanforderungen bereits ab Beginn der Systementwicklung („Security by Design"), ein verlässliches Identity Management sowie Schulung und Sensibilisierungskampagnen.

SAFARI
Von Apple entwickelter Webbrowser für MacOS und iOS.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_21

SAFE HARBOUR
Abk. für Safe-Harbor-Pakt. Übsg. „Sicherer-Hafen"-Abkommen. Ein Vertrag zwischen der Europäischen Kommission und den USA. Damit war es Firmen zwischen den Jahren 2000 und 2015 erlaubt, personenbezogene Daten aus der EU in die USA zu übermitteln.

SALESFORCE
Anbieter von Cloud-Computing für Firmen.

SALSA20
Stromverschlüsselung, die schneller berechnet werden kann als bspw. RSA-2048. Dieser Geschwindigkeitsvorteil war ein Grund für die Verwendung von Salsa20 in Ransomware wie Petya und GandCrab.

SALT (engl.)
Übsg. Salzen

SALTED SIGNATURE HASH (engl.)
Übsg. Gesalzener Signatur-Hash-Wert. Einbeziehung von zusätzlichen zufälligen Werten bei der Berechnung von Hash-Werten für Signaturen.

SALTYRTC PROTOCOL
Protokoll, welches eine Ende-zu-Ende-Verschlüsselung für WebRTC und andere Anwendungen ermöglicht, bei der einem Server zwischen den zwei Parteien nicht vertraut werden muss, da die Clients die Authentisierung selber gegenseitig durchführen und die Kommunikation verschlüsseln.

SALZEN
Zufälliger Wert, der beim Hashing von Passwörtern miteinbezogen wird, um unterschiedliche Hash-Werte für gleiche Passwörter zu erhalten und damit Angriffe mit Rainbow-Tabellen zu verhindern. Neben den so erzeugten Hash-Werten der Passwörter müssen die zufälligen Salzwerte für jeden Benutzer gespeichert werden, sodass ein bei der Anmeldung eingegebenes Passwort gegenüber den gespeicherten gesalzenen Hash-Werten überprüft werden kann.

SAML
Abk. für Security Assertion Markup Language

SAMSAM
Schadsoftware in Form eines Erpressungstrojaners, der Dateien verschlüsselt und ein Lösegeld zur Entschlüsselung verlangt.

SAN
Abk. für Storage Area Network

SANDBOX MODEL (engl.)
Übsg. Sandkastenmodell. Ausführung von Apps innerhalb einer Umgebung, die abgegrenzt ist von anderen Apps. Dies stellt sicher, dass Apps nicht auf die Daten anderer Apps auf dem gleichen Gerät zugreifen können.

SANITY TESTING (engl.)
Übsg. Plausibilitätstesting, welches früh in einer Software-Testing-Phase durchgeführt wird, um zu prüfen, ob die Software grundsätzlich funktioniert. Meist erfolgt das Sanity Testing nach dem Smoke Testing, bei welchem geprüft wird, ob sich die Software starten und bedienen lässt, und vor dem Functional Testing, welches die Funktionen im Detail überprüft.

SAST
Abk. für Static Application Security Testing

SATORI
Botnetz, welches die Malware Mirai benutzt und Angriffe auf nicht aktualisierte Router ausführt.

SCADA
Abk. für Supervisory Control and Data Acquisition

SCALA
Objektorientierte Programmiersprache, die JAVA-Bibliotheken benutzen kann.

SCALING DOWN (engl.)
Übsg. Herunterskalieren. Syn. zu Horizontal Scaling. Erweiterung eines Systems durch Hinzufügen gleicher Systeme. Bspw. werden VMs zu einem virtuellen Gesamtsystem hinzugefügt, um schnellere Antwortzeiten für mehr Anfragen zu bieten.

SCALING OUT (engl.)
Übsg. Herausskalieren. Syn. zu Horizontal Scaling. Erweiterung eines Systems durch Hinzufügen gleicher Systeme. Bspw. werden VMs zu einem virtuellen Gesamtsystem hinzugefügt, um schnellere Antwortzeiten für mehr Anfragen zu bieten.

SCALING UP (engl.)
Übsg. Hochskalieren. Syn. zu Vertical Scaling. Methode, um die Netzwerkbandbreite, die Anzahl CPUs, die Größe des Speichers oder die Größe der Harddisk innerhalb eines

Systems zu vergrößern, um damit die Gesamtleistung zu erhöhen. Bei VMs geht dies online, bei physischen Computern muss dafür die Hardware ersetzt werden.

SCAM (engl.)
Ugs. Betrug. Beispiel: Ein Produkt wird angeboten, jedoch bei Zahlung des Preises nicht geliefert.

SCANNER
1) Software zur Entdeckung, Klassifizierung und evtl. Verschlüsselung von Daten auf lokalen oder vernetzten Speicher. 2) Hardware zur digitalen Ablichtung und Speicherung von Informationen.

SCAR
Schadsoftware in Form eines Trojaners.

SCHADSOFTWARE
Syn. zu Malware. Computerprogramm, welches nicht eines guten Zwecks wegen entwickelt wird, sondern um Schaden anzurichten. Schadsoftware kam bereits mit der zunehmenden Verbreitung von PCs, C64, AMIGA, ATARI usw. in den 1980er-Jahren auf. Damals war es sehr einfach, einen Computer eines Nichtexperten lahmzulegen, da Disketten unter der Hand ausgetauscht wurden und diese ohne Überprüfung in den Computer gesteckt und automatisch geladen wurden. Schadsoftware-Herstellung wurde in den letzten Jahren zunehmend als Gewerbe betrieben und erzeugt Schäden in Milliardenhöhe pro Jahr. Es werden große Anstrengungen im Bereich IT-Security unternommen, um Gegenmittel zu entwickeln und dadurch mit den Schadsoftware-Herstellern auf Augenhöhe zu sein. Schadsoftware kommt in Form von Viren, Würmern, (Erpressungs-) Trojaner, Makros usw. vor, und für jeden Typ von Schadsoftware gibt es teils gute, teils weniger gute Schutzmaßnahmen. Als Schutz und Gegenmittel wird empfohlen, regelmäßig Backups zu erstellen, bedachtes Downloaden von Dateien, ständiger Betrieb von aktuellen Anti-Viren-Programmen und rasche Einspielung von Betriebssystem- und Applikationsupdates.

SCHANNEL
Abk. für Windows Secure Channel. Funktionsbibliothek für die Implementation von SSL/TLS-Verschlüsselung, bspw. bei Internet-Apps, die HTTPS benutzen. SChannel beinhaltet Funktionen zur Authentifikation und zur sicheren, privaten Kommunikation mittels Verschlüsselung.

SCHLÜSSEL
Geheime Daten in Form von Zahlen, Strings, Text u. Ä., die bei kryptografischen Berechnungen eingesetzt werden und das Resultat dieser Berechnungen beeinflussen. Bspw. transformiert ein Schlüssel bei einer Verschlüsselung einen Klartext in einen

Geheimtext. Da Schlüssel geheime Daten sind, benötigen sie eine aktive Verwaltung (sog. Key Management) über den gesamten Lebenszyklus hinweg, d. h. die sichere Erstellung, Übertragung, Verteilung, Vernichtung usw.

SCHLÜSSELAUSTAUSCH
Verfahren, welches es zwei Parteien erlaubt, einen gemeinsamen Schlüssel für die Ver- und Entschlüsselung zu benutzen. Beim Diffie-Hellman-Schlüsselaustausch kann dies auch über einen unsicheren Kommunikationskanal geschehen und der Schlüssel danach für symm. Verschlüsselung u. Ä. verwendet werden.

SCHLÜSSELAUTHENTISIERUNG
Methode zur Sicherstellung, dass öffentliche Schlüssel von der richtigen Person stammen und nicht durch einen Man-in-the-Middle-Angriff ausgetauscht wurden.

Beispiele zur Schlüsselauthentisierung

a) Treffen der Person und Vergleichen des Schlüsselfingerabdrucks,
b) Vorlesen des Schlüsselfingerabdrucks durch das Telefon,
c) Nachsehen des Schlüsselfingerabdrucks auf gedruckten Dokumenten, wie Visitenkarten, handschriftlich unterzeichneten Briefe, Zeitschriften u. Ä.

SCHLÜSSELEINSPEICHERUNG
Syn. zu Key Injection. Methode, um digitale Schlüssel außerhalb eines Servers oder HSMs zu erzeugen und danach in diesen hineinzubringen. Dies wird verwendet, falls der Algorithmus zur Schlüsselerzeugung und die sichere Verwaltung des Schlüssels (sog. Key Management) in der Hand der Firmenmitarbeiter bleiben soll und nicht den Herstellern der Server oder HSMs überlassen wird. Dies bedingt, dass das gesamte Key Management, also alle Phasen des Lebenszyklus der Schlüssel, durch firmeninterne Prozesse und Personen durchgeführt und abgedeckt wird.

SCHLÜSSELERZEUGUNG
Verfahren und Software, um mittels Algorithmen neue digitale Schlüssel für Server, Clients, Systeme, Geräte, Personen u. Ä. zu generieren. Dabei kann sowohl ein einzelner Schlüssel für symmetrische, kryptografische Verfahren erzeugt werden als auch zwei zusammenhängende, in Form eines privaten und eines öffentlichen Schlüssels, für asymmetrische, kryptografische Verfahren. Die Erzeugung von Schlüsseln geschieht meist innerhalb des Zielgeräts, kann jedoch auch außerhalb des Zielgeräts geschehen und danach durch Schlüsseleinspeisung (Key Injection) ins Zielgerät gebracht werden. In vielen Fällen werden Schlüssel mit zusätzlichen Angaben und Daten zu sog. digitalen Zertifikaten kombiniert (z. B. Public-Key-Zertifikate), sodass damit die Authentizität und Identität des Schlüssels und des Schlüsselbesitzers überprüft und bestätigt werden kann.

Tab. 21.1 Beispiele für Schlüssellängen und Schlüsselanzahl bei symm. Verfahren

Symmetrisches, kryptografisches Verfahren	Schlüssellänge S_L	Schlüsselanzahl S_A
Cäsar	5-Bit	$2^{25} \approx 3 \cdot 10^7$
DES	56-Bit	$2^{56} \approx 7 \cdot 10^{16}$
AES	256-Bit	$2^{256} \approx 1 \cdot 10^{77}$

SCHLÜSSELLÄNGE

Bei symmetrischen, kryptografischen Verfahren entspricht die Schlüssellänge einem Maß für das Sicherheitsniveau des kryptografischen Verfahrens. Mathematisch entspricht die Schlüssellänge dem Logarithmus der Anzahl möglicher Schlüssel des angewendeten, symmetrischen, kryptografischen Verfahrens:

Schlüssellänge [in Bit] $S_L = \log_2 S_A$
Anz. möglicher Schlüssel $S_A = 2^{S_L}$

Für symmetrische Verfahren werden heutzutage Schlüssellängen von mind. 128-Bit empfohlen (siehe Tab. 21.1).

Bei asymmetrischen kryptografischen Verfahren entspricht die Schlüssellänge der Anzahl Bits der für die Berechnung benutzten Primfaktoren, d. h. Primfaktoren p und q, welche für einen Schlüssel n mit $n = p \cdot q$ verwendet werden, werden mit Schlüssellängen $S_L = 2^{Anzahl\ Bits}$ gewählt. Diese Schlüssellängen sind jedoch nicht direkt ein Maß für das Sicherheitsniveau, da asymmetrische, kryptografische Verfahren Primzahlen benutzen und deswegen nicht mit jedem Wert arbeiten können, und außerdem Angriffsmöglichkeiten bieten, die bei symmetrischen Schlüsseln nicht vorliegen. Bspw. entspricht 1024-Bit RSA einem theoretischen Sicherheitsniveau von ca. 73-Bit, also nur wenig sicherer als DES.

Die Schlüssellänge sollte für neue Schlüssel vorausschauend und konservativ gewählt werden, sodass entsprechende Schlüssel auch mehrere Jahre über deren geplanten Einsatzzeitraum noch sicher sind. Empfehlungen sind zu finden auf NIST.gov[1] und keylength.com *(Abgerufen am 22.12.2019)*.

Beispielsweise wird zum Zeitpunkt der Erstellung dieses Buches (2019) erwartet, dass

2048-Bit RSA bis ca. 2030 sicher ist,
4096-Bit RSA bis ca. 2060 sicher ist.

[1]https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf, NIST Special Publication 800-57 Part 1Revision 4 *(Abgerufen am 22.12.2019)*.

SCHLÜSSELLEBENSDAUER
Angabe für die erlaubte Benutzungsdauer eines Schlüssels. Nach Ablauf dieser Dauer wird der Schlüssel für ungültig erklärt, d. h. widerrufen („revoked"), und kann nicht mehr für Verschlüsselungen u. Ä. verwendet werden. Schlüssellebensdauern sollten klein genug gewählt werden, damit der Schlüssel nicht innerhalb dieser Dauer durch neue Methoden geknackt werden kann.

SCHLÜSSELPAAR
Bei asymmetrischer Verschlüsselung und allg. bei Public-Key-Kryptografie wird eine Kombination zweier Schlüssel verwendet. Diese werden öffentlicher und privater Schlüssel genannt und hängen mathematisch voneinander ab. Der öffentliche Schlüssel kann von jedermann eingesehen und benutzt werden, um geheime Botschaften oder verschlüsselte Dateien an den Besitzer des privaten Schlüssels zu schicken, die nur dieser entschlüsseln kann.

SCHLÜSSELTAUSCHPROBLEM
Eines der Grundprobleme der Kryptografie, bei welcher ein geheimer Schlüssel über einen, potenziell unsicheren Kommunikationskanal ausgetauscht werden muss. Dieses Problem wird u. a. durch das Diffie-Hellman-Schlüsselaustauschverfahren gelöst, wobei die Authentisierung stets zusätzlich durchzuführen ist, d. h. die teilnehmenden Parteien müssen sicherstellen, dass sie die Schlüssel miteinander austauschen und nicht ein Man-in-the-Middle-Angreifer, der vorgibt, eine dieser Parteien zu sein.

SCHLÜSSELVERTEILUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Abschnitt im Lebenszyklus kryptografischer Schlüssel. Siehe zusätzliche Details beim Begriff Schlüssel.

SCHNÜFFEL-SOFTWARE
Syn. zu Spionage-Software

SCHUTZMASSNAHMEN
Prozesse, Verfahren, Programme und Geräte zum Schutz von Daten, Systemen, Netzwerken oder Infrastruktur.

SCHUTZTECHNOLOGIE
Programme und Geräte zum Schutz von Daten, Systemen, Netzwerken oder Infrastruktur.

SCHWARZE LISTE
Syn. zu Blacklist. Informationen oder Daten, die nicht erwünscht sind. Bspw. können E-Mail-Adressen von Spamversendern auf schwarze Listen gesetzt werden, damit solche Spam-E-Mails automatisch abgewiesen werden.

SCP
Abk. für Secure Copy Protocol

SCREEN SCRAPER (engl.)
Übsg. Bildschirmableser. Programm, das Text auf einem Bildschirm erkennt und speichert. Dies wird u. a. verwendet, um alte terminalbasierte Programme weiterbetreiben und dem Benutzer trotzdem eine neue Benutzeroberfläche zeigen zu können. Dazu erkennt ein Screen Scraper die dem Benutzer nicht gezeigte Terminalausgabe und baut den erkannten Text in die moderne Benutzeroberfläche ein.

SCREENSHOTTING (engl.)
Übsg. Abfotografieren des kompletten aktuellen Bildschirminhalts oder eines Teils davon. Dies kann manuell mit einem Fotoapparat oder mittels Software auf dem PC durchgeführt werden. Das resultierende Bild liegt dann entweder im Zwischenspeicher oder als Datei vor. Bei Windows, MacOS, iOS, Android und anderen Betriebssystemen ist diese Funktion ohne Zusatzsoftware vorhanden. Bei Windows via Taste „Print Screen“. Bei MacOS via Tastenkombination „Cmd“+„Ctrl“+„Shift“+„3“ (u. Ä.).

SCRUM
Vorgehensmodell und Tools zur agilen Software-Entwicklung. Wird auch als Grundlage für andere Projekte verwendet, bei denen keine Software erstellt wird. Der Name stammt aus dem Rugby, bei welchem auch nur eine Richtung vorgegeben wird und die Teams schnell und selbstorganisiert das Ziel erreichen.

SCRUTINY (engl.)
Übsg. Genaue Prüfung

SCRYPT
Password Hash Function, d. h. eine kryptografische Hash-Funktion, welche auf Passwörter angewendet wird, damit diese nicht als Klartext gespeichert werden. Zur Vermeidung von Brute-Force-Attacken werden Hash-Funktionen künstlich verlangsamt und die Hash-Werte häufig mit mitgespeicherten zufälligen „Salt“-Werten kombiniert, damit gleiche Passwörter nicht gleiche Hash-Werte ergeben.

SDL
Abk. für Supplemental Downlink

SDLC
1) Abk. für Secure Development Life Cycle. 2) Abk. für Software Development Life Cycle

SECONDARY ACCOUNT (engl.)
Zweitaccount eines Benutzers, bspw. eines IT-Admins, mit anderen Berechtigungen und Zugangsdaten im Vergleich zum Standardaccount. Eine solche Separation von Accounts für einen Benutzer kann helfen, das „Need-to-know"-Prinzip einzuhalten.

SECOND LIFE [SL] (engl.)
Übsg. Zweites Leben, Parallelwelt. Spielsoftware, bei welcher Benutzer als Avatare virtuell und dreidimensional interagieren, Handel betreiben und kommunizieren.

SECRET-KEY CRYPTOLOGY [SKC] (engl.)
Übsg. Verschlüsselung mithilfe eines Geheimschlüssels. Der geheime Schlüssel wird sowohl zum Verschlüsseln als auch zum Entschlüsseln benutzt.

SECURE BOOT (engl.)
Übsg. Sicheres Starten. Möglichkeit in UEFI, um nur signierte Bootloader zu erlauben.

SECURE BY DESIGN (engl.)
Übsg. Sicherheit während des Designs. Sicherheitsaspekte sollten bereits während der Planung neuer Software berücksichtigt werden.

SECURE BY DEFAULT (engl.)
Übsg. Sicherheit standardmäßig. Von Sicherheitslücken muss bei der Erstellung neuer Software ausgegangen werden und deshalb sollten Standardeinstellungen restriktiv sein und kaum benutzte Funktionen standardmäßig deaktiviert werden.

SECURE CODING (engl.)
Übsg. Sicheres Programmieren

SECURE COLLABORATION (engl.)
Übsg. Sichere Zusammenarbeit

SECURE CONNECTION (engl.)
Übsg. Sichere Verbindung. Eine direkte Verbindung von PCs in einem Netzwerk, bei welcher sichere Protokolle zum Datentransfer benutzt werden. Das wichtigste Protokoll im Datenverkehr des Internets ist das kryptografische Transport Layer Security (TLS)-Protokoll, welches zur sicheren HTTPS-Verbindung eingesetzt wird.

SECURE COPY (engl.)
Syn. zu Secure Copy Protocol

SECURE COPY PROTOCOL [SCP] (engl.)
Übsg. Sicheres Kopierprotokoll. Auf SSH basierendes Programm und Protokoll zur verschlüsselten Übertragung von Daten zwischen PCs in einem Netzwerk.

SECURE DEVELOPMENT LIFE CYCLE [SDLC] (engl.)
Übsg. Lebensphasen zur sicheren Entwicklung. Software-Entwicklungsprozess, welcher aufbauend auf Standardprojektvorgehensmethoden Sicherheitschecks in allen Phasen berücksichtigt, d. h. bereits bei der Planung, Programmierung, Validierung und der Implementation. Dies beinhaltet bspw. Simulation von Angriffen, Benutzung von bewährten und geprüften Codezeilen, Durchführung von Sicherheitstests oder auch Analyse des Quellcodes. Syn. zu Secure Software Development Life Cycle (SSDLC), Secure SLDC.

SECURE FILE TRANSFER (engl.)
Übsg. Sichere Dateiübermittlung. Programme und Protokolle, bei welchen der Transport der Daten verschlüsselt durchgeführt wird.

Beispiele: SFTP, FTP über SSH, FTP über SSL/TLS, Kerberized FTP.

SECURE FTP
Programm, welches FTP über SSL/TLS anbietet.

SECURE HASH ALGORITHM [SHA] (engl.)
Übsg. Sicherer Hash-Algorithmus. Gruppe standardisierter kryptografischer Hash-Funktionen. Damit können Prüfwerte für digitale Daten berechnet werden, sodass die Integrität der Daten jederzeit überprüft werden kann. Dies wird bspw. bei digitalen Signaturen verwendet.

SECURE OPERATING SYSTEM (engl.)
Übsg. Sicheres Betriebssystem

SECURE PASSWORD AUTHENTICATION (engl.)
Übsg. Sichere Passwort Authentisierung. Authentisierung für E-Mail-Abruf und E-Mail-Versand über NTLM für Microsoft Exchange Server.

SECURE REAL-TIME TRANSPORT PROTOCOL [SRTP] (engl.)
Protokoll zur sicheren Verschlüsselung von Daten in Echtzeit. Wird u. a. für Audio Stream Encryption verwendet.

SECURE REMOTE STORAGE (engl.)
Übsg. Sicherer Speicherplatz in einer Cloud, bei der Wert auf IT-Schutzmaßnahmen gelegt wurde.

SECURE SHELL [SSH] (engl.)
Übsg. Sichere Umgebung. Kryptografisches Netzwerkprotokoll und kryptografische Software, welche Funktionen in einer Shell (aba. Terminal) anbieten, um Kommandos verschlüsselt über ein potenziell ungeschütztes Netzwerk auf einem anderen Computer auszuführen. Dazu bietet SSH einen sicheren Kanal zwischen einer authentifizierten, verschlüsselten Client-Applikation und einem SSH-Server. Manche Anwender bevorzugen SSH in der Kommandozeile, andere benutzen grafische Oberflächen. Bekannte SSH-Client-Applikationen sind WinSCP, OpenSSH und PuTTY. SSH wird heutzutage als Ersatz für die veralteten Tools Telnet, RemoteShell und rlogin eingesetzt. Die 1995 entwickelte erste Version SSH-1 wurde wegen Sicherheitsschwachstellen 1996 durch SSH-2 ersetzt, welche heute noch als sicher gilt.

SECURE SLDC [SSDLC] (engl.)
Syn. zu Secure Development Life Cycle

SECURE SOCKETS LAYER [SSL] (engl.)
Protokoll zur Serverauthentifizierung und Datenverschlüsselung bei Internetverbindungen. SSL basiert auf einer Kombination von öffentlichem und privatem Schlüssel und kann von Applikationen wie E-Mail-Programmen oder Internetbrowsern benutzt werden, um E-Mails oder vertrauliche Daten gesichert von und zu einem Server zu schicken. Dies kann bspw. der verschlüsselte Aufruf von E-Mails von einem POP3-Server oder der verschlüsselte Aufruf einer HTTPS-Seite sein. Dabei geht es v. a. darum, die Echtheit (Authentizität) des kontaktierten Servers durch ein Zertifikat zu bestätigen und die Verbindung zwischen Client und Server zu verschlüsseln.

SSL1.0 wurde in den 1990er-Jahren von Netscape entwickelt und bis SSL3.0 weiterentwickelt. Ab Version SSL3.1 (1999) wird es als TLS1.0 bezeichnet (siehe Tab. 22.1).

Die exemplarische Verwendung von SSL/TLS wird im ausführlichen Spezialthema „Der Aufruf einer HTTPS-Internetseite“ im Kap. 29 erklärt.

SECURE SOFTWARE DEVELOPMENT (engl.)
Übsg. Sichere Software-Entwicklung. Syn. zu sicheres Programmieren.

SECURE SOFTWARE DEVELOPMENT LIFE CYCLE [SSDLC] (engl.)
Syn. zu Secure Development Life Cycle (SDLC)

SECURE WEB GATEWAY (engl.)
Übsg. Sicherer Webdurchgang. Software und Hardware, um a) unerwünschte Schadsoftware aus dem Internetverkehr des Benutzers herauszufiltern oder b) Unternehmensrichtlinien und gesetzliche Bestimmungen durchzusetzen. Angewendete Methoden sind bspw. URL-Filter, Filterung von schädlichem Code und Blockierung von Chat und sozialen Medien.

SECURING DATABASES (engl.)
Übsg. Sicherheit von Datenbanken erhöhen.
Einige mögliche Methoden, um Datenbanken zu schützen:

a) Vorsetzen einer Firewall
b) Physische Platzierung der Datenbankserver in einem gesicherten Raum
c) Aktuell gehaltene Datenbanksoftware
d) Entfernen von nicht benötigten Accounts
e) Code-Review
f) Systemdokumentation

SECURITY ASSERTION MARKUP LANGUAGE [SAML] (engl.)
Übsg. Auszeichnungssprache für Sicherheitshinweise. Protokoll für den XML-Transfer von a) Benutzerautorisierung, b) Benutzerauthentifizierung, c) Berechtigungen, d) Attributinformationen und e) Benutzerföderation. SAML erlaubt bspw. Web-SSO, bei welchem der Benutzer sich bei einer Webadresse authentisiert und danach ohne zusätzliche Authentifizierung auf andere Ressourcen zugreifen kann. Dies wird dadurch erreicht, dass die Authentifizierungsbestätigung von der ersten zu jeder weiteren Webadresse übermittelt wird.

SECURITY AWARENESS PROGRAM (engl.)
Schulung der Mitarbeiter und regelmäßige Information an Mitarbeiter, um sie für Aspekte der IT-Sicherheit zu sensibilisieren.

SECURITY BREACH (engl.)
Übsg. Sicherheitsverletzung

SECURITYBSIDES.ORG
Internetseiten, die Informationen und Support bieten, um eigene sogenannte „Security BSides Events“ zu organisieren. Solche finden bereits weltweit statt und erlauben sowohl Information-Security-Experten als auch Interessierten, gemeinsam Themen der IT-Sicherheit zu diskutieren.

SECURITY BY DESIGN (engl.)
Übsg. Sicherheit durch Design. Grundsatz, der besagt, dass Sicherheitsanforderungen bereits ab Beginn der Entwicklung eines Systems oder einer Software berücksichtigt werden sollen.

SECURITY BY OBSCURITY (engl.)
Prinzip in der IT-Sicherheit, welches aussagt, dass bereits die Geheimhaltung eines Systems oder eines Verfahrens eine gewisse Sicherheit bietet.

SECURITY CONSOLE (engl.)
Abk. für Microsoft Cloud App Security Console. Oberfläche der Cloud-App-Security-Umgebung von Azure.

SECURITY CONTROLS (engl.)
Übsg. Sicherheitsmaßnahmen

SECURITY DOMAIN (engl.)
Übsg. Sicherheitsbereich, Sicherheitsdomäne. Systeme oder Applikationen, welchen alle den gleichen Sicherheitsrichtlinien einer zentralen Stelle folgen.

SECURITY GAP (engl.)
Übsg. Sicherheitslücke

SECURITY HARDENING (engl.)
Übsg. Verstärkung der Sicherheit, Erhöhung der Sicherheit.

SECURITY IDENTIFIER [SID] (engl.)
Übsg. Sicherheitskennung. Eindeutige Nummer zu jedem Benutzerkonto in Windows. Diese SID wird in der Registry gespeichert. Der Unterschied zwischen den Rechten der Benutzer zeigt sich in den letzten 3 Stellen (sog. RID), die bspw. beschreiben, ob der Benutzer Admin-Rechte besitzt.

SECURITY INCIDENT MANAGEMENT (engl.)
Übsg. Behandlung von Sicherheitsvorfällen. Software und Prozesse zur Detektion und Behandlung von Sicherheitsvorfällen.

SECURITY INFORMATION AND EVENT MGMT [SIEM] (engl.)
Übsg. Behandlung der Informationssicherheit und der Sicherheitsvorfälle. Software und Prozesse zur ständigen Analyse und Behandlung von Sicherheitsvorfällen.

SECURITY PATCHES (engl.)
Übsg. Sicherheitsaktualisierungen bei Software.

SECURITY PROCESSOR CERTIFICATE [SPC] (engl.)
Übsg. Sicherheitsprozesszertifikat. Bei Microsoft ADRMS benutztes Zertifikat innerhalb des Client-Computers. Dieses identifiziert den Computer und ermöglicht die Verschlüsselung anderer Elemente, welche lokal im Computer gespeichert sind.

SECURITY QUESTIONS (engl.)
Übsg. Sicherheitsfragen

SECURITY SUPPORT PROVIDER INTERFACE [SSPI] (engl.)
Windows-Funktionen für Authentisierung. Apps und Infrastruktur benutzen SSPI zur einheitlichen Anwendung von Authentisierung. Dabei bietet SSPI Mechanismen, um Authentisierungs-Tokens über existierende Kommunikationskanäle zw. Client und Server zu übermitteln.

SECURITY THROUGH OBSCURITY (engl.)
Übsg. Sicherheit durch Geheimhaltung. Prinzip, die Sicherheit eines Systems oder einer Berechnung aufrechtzuerhalten durch Geheimhaltung der inneren Funktionsweise.

SECURITY TOKEN (engl.)
Übsg. Berechtigungsnachweis. Dieser kann elektronisch oder physisch vorliegen.

SEEDS (engl.)
Startwerte für Berechnungen, die auf Zufallszahlen basieren. Gleiche Startwerte erzeugen gleiche Folgen von Zufallszahlen. Bei der Erzeugung von Schlüsseln für Verschlüsselungen wird darauf geachtet, keine gleichen Startwerte zu benutzen, damit keine zwei Schlüssel gleich sind. Bei 3D-Spielen wie Minecraft startet jede Welt an einem Seed-Punkt. Dieser Seed-Punkt kann anderen Personen mitgeteilt werden, damit diese die gleiche Welt starten können.

SEGREGATION OF DUTIES [SOD] (engl.)
Übsg. Aufgabentrennung. Maßnahme zur Erhöhung der Sicherheit durch bewusste Aufteilung der Aufgaben auf verschiedene Personen. Dies reduziert die Möglichkeiten jedes Einzelnen zur Manipulation oder zum Diebstahl. Ähnlicher Grundgedanke wie beim „Vier-Augen-Prinzip“.

SEITENKANAL-ATTACKE
Absichtlicher Zugriff auf Speicherbereiche anderer Prozesse. Die Sicherheitslücke Meltdown ermöglichte solche Seitenkanalattacken.

SELECTIVE ENCRYPTION (engl.)
Übsg. Selektive Verschlüsselung. Nur die wichtigsten Daten werden verschlüsselt, um die Kosten, den Aufwand und die Einschränkungen für Benutzer gering zu halten. Der Trend geht heutzutage mehr in Richtung „Pervasive Encryption“, also der Verschlüsselung aller Daten.

SELF-SIGNED CERTIFICATE (engl.)
Übsg. Selbstsigniertes Zertifikat. Digitales Zertifikat, welches einen öffentlichen Schlüssel enthält, und welches mit dem korrespondierenden privaten Schlüssel signiert wird. Solche selbstsignierten Zertifikate reichen in einigen Anwendungsfällen aus, wie

bspw. im eigenen kleinen Heimnetzwerk, und können im Vergleich zu CA-signierten Zertifikaten kostenlos mit Tools wie OpenSSL oder Apples Keychain erstellt werden.

SEMANTIC (engl.)
Übsg. Semantik, Wortbedeutung.

SEMANTIC SECURITY (engl.)
Übsg. Semantische, d. h. textbasierte Sicherheit. Als Verschärfung des Prinzips der „Perfect Secrecy“, besagt „Semantic Security“, dass ein Angreifer, welcher den Geheimtext abfängt, auch mit allen verfügbaren Ressourcen in endlicher Zeit keine Informationen zusätzlich daraus ablesen kann. Der Angreifer hätte auch ohne Abfragen des Geheimtexts gleich viele Informationen über den ursprünglichen Klartext gehabt.

SENSIBLE DATEN
Syn. zu wichtigen Daten. Diese müssen besonders verlässlich und sicher behandelt, gespeichert und transferiert werden, da deren Verlust die Firma oder die Person beeinträchtigen würde.

SENSITIVE DATA (engl.)
Übsg. Sensible Daten

SENSITIVITY (engl.)
Übsg. Sensibilität, Wichtigkeit, Verletzbarkeit.

SEPARATES NETZWERKSEGMENT
Syn. zu Demilitarisierte Zone (DMZ). Teil eines Computernetzwerks, welches durch Firewalls oder physisch vom Rest des Netzwerks separiert ist, um die Sicherheit der Computer in diesem Segment besonders zu schützen.

SERVER (engl.)
Übsg. Diener. Computer, der Daten oder Programme von anderen Computern (sog. Clients) empfängt oder für andere Computer bereitstellt. Meist sind viele Server zentral in Datenzentren zusammengefasst und bedienen eine große Anzahl an Clients. Jeder Server wird für einen oder für wenige Dienste (sog. Services) aufgesetzt, bspw. als Webserver, als Windows-Server, als Datenbank usw. Die Betreuung, Verwaltung und Pflege der Server unterliegen den Administratoren, welche erhöhte Admin-Rechte dafür benötigen. Auch der Zutritt zu den Datenzentren benötigt spezielle Schlüssel oder Zutrittsrechte, da die Server wichtige Daten der Firma oder der Nutzer oder auch der Schlüssel für die Verschlüsselung speichern.

SERVER-AUTHENTIFIZIERUNG
Verfahren innerhalb einer Client-Server-Abfrage zur Sicherstellung der Verbindung mit dem richtigen Server. Der Server, bspw. ein Webserver, von dem ein Benutzer im Webbrowser eine Internetseite ansehen möchte, besitzt ein signiertes Serverzertifikat, meist im Format X.509, welches zum Client geschickt wird und auf Vertrauenswürdigkeit geprüft wird, bevor weitere Kommunikation stattfindet.

SERVER CERTIFICATE (engl.)
Übsg. Serverzertifikat

SERVER-FARM
Ansammlung von Servern, die meist im gleichen Data Center installiert sind.

SERVER LICENSOR CERTIFICATE [SLC] (engl.)
Syn. zu Mandantenschlüssel. Bei Microsoft ADRMS benutztes selbstsigniertes Zertifikat eines ADRMS Server Clusters. Der korrespondierende private Schlüssel wird vom Server verwendet, um andere Zertifikate zu signieren, und der korrespondierende öffentliche Schlüssel wird von Clients verwendet, um Daten für den Server zu verschlüsseln.

SERVER MESSAGE BLOCK [SMB] (engl.)
Übsg. Server-Nachrichtenblock. Protokoll auf Windows-Systemen, um den Zugriff auf gemeinsame Dateien in Speichermedien über ein Netzwerk zu ermöglichen, sodass die Speichermedien bei den Computern der Benutzer wie lokale Festplatten erscheinen. Auch die gemeinsame Benutzung von Druckern kann damit umgesetzt werden. Aufgrund von Sicherheitslücken bei SMB1.0, die bspw. durch WannaCry ausgenutzt wurden, wird SMB1.0 bei aktuellen Windows10-Versionen nicht mehr standardmäßig installiert oder aktiviert. Stattdessen wird empfohlen, die aktuelle Version SMB3.0 zu verwenden, welche viele Sicherheits- und Performanceverbesserungen beinhaltet. Bei Unix-Systemen u. Ä. bietet NFS (Network File System) ein ähnliches Protokoll wie SMB.

SERVER-ZERTIFIKAT
Digitale Datei auf einem Server, welche den Server eindeutig identifiziert und gegenüber anderen Systemen authentifiziert. Eines der häufigsten Zertifikatformate ist X.509. Dieses kann selbstsigniert oder von einer Zertifizierungsstelle (CA) signiert sein. Es enthält den öffentlichen Schlüssel, welcher für die Verschlüsselung von Daten an diesen Server verwendet werden kann. Für den Aufruf einer HTTPS-Internetseite von einem Server wird TLS zur Verschlüsselung der Daten benutzt, und TLS verlangt zu Beginn der Kommunikation zwingend ein Zertifikat des Servers dieser Internetseite.

SERVICE (engl.)
Übsg. Dienst, Dienstprogramm. Durch ein Betriebssystem bereitgestellte oder auf einem System zusätzlich installierte Software, um anderen Programmen erweiterte Funktionen anzubieten, wie z. B. eine Datenbankabfrage, Festplattenverwaltung, WLAN-Erkennung, automatische Suche nach Updates usw.

SERVICE ACCOUNT (engl.)
Übsg. Dienstkonto, Konto eines technischen Benutzers. Spezielles Konto, welches von einer Applikation oder einem Service benutzt wird, um mit dem Betriebssystem zu interagieren. Dabei können dem Service Account Rechte vergeben werden, die die Applikation benötigt, die jedoch den normalen Benutzern der Applikation nicht vergeben werden sollen.

SERVICE LEVEL AGREEMENT [SLA] (engl.)
Übsg. Vereinbarung über Qualität, Preis, Lieferzeit und Verfügbarkeit einer Dienstleistung.

SERVICE-ORIENTED ARCHITECTURE [SOA] (engl.)
Übsg. Serviceorientierte Architektur. Software, welche Dienste wie Datenbanken und Server als abgeschlossene Einheiten über ein Netzwerk anbietet, sodass diese Dienste wie Module oder Blackboxes verwendet werden können. Auch wenn ein Produkt in einem dieser Dienste ausgetauscht wird, muss kein Benutzer dieses Dienstes Änderungen durchführen, da der Dienst die bestehende Kommunikation unverändert weiterhin anbietet.

SERVLET
Programme, genauer Java-Klassen, die innerhalb eines Webservers Anfragen von Clients entgegennehmen und beantworten.

SESSION ENTROPY (engl.)
Übsg. Sitzungsunordnung. Methode, um Session-IDs zu erstellen, die nicht einfach zu erraten sind. Bspw. werden, anstatt jeder neuen Session-ID einfach den nächsthöheren Wert zuzuweisen, Zufallszahlen benutzt.

SESSION HIJACKING (engl.)
Übsg. Sitzungsmissbrauch. Hacking-Methode, um eine Internetbrowser-Session zu manipulieren, bspw. durch Mithören bei unverschlüsselten WLAN-Verbindungen oder durch Erraten einfach gestrickter Session-IDs.

SESSION ID (engl.)
Übsg. Sitzungskennung. Bei der ersten Abfrage einer Internetseite vom Server erstellte Nummer, welche zum Webbrowser geschickt wird, damit dieser bei jeder weiteren

Abfrage an diese Internetseite diese Session-ID mitschicken kann. Damit kann der Webserver erkennen, welche Anfragen vom gleichen Benutzer kommen. Die Session-ID wird gelöscht, sobald sich der Benutzer abmeldet oder eine vordefinierte Zeit keinen Kontakt mit dem Server hatte.

SESSION KEY (engl.)
Übsg. Sitzungsschlüssel

SFTP
Abk. für FTP über SSH. Syn. zu SSH File Transfer Protocol.

SHA
Abk. für Secure Hash Algorithm. Kryptografische Hash-Funktion, welche u. a. verwendet werden kann für das Signieren von Zertifikaten und die Erstellung von Passwort-Hashs (siehe Tab. 21.2).

Tab. 21.2 SHA-Versionen

Version	Akzeptiert von – bis	Beschreibung
SHA-0	1993–1995	Ursprünglicher Secure Hash Algorithm (SHA) mit 160-Bit Hash-Wert-Länge, von der NSA im Jahr 1993 entwickelt 1995 durch SHA-1 ersetzt
SHA-1	1995–2005	Von 1995 bis 2005 der NIST-Standard für Secure Hash Algorithm (SHA) mit 160-Bit Hash-Wert-Länge Seit 2005 wird der Nachfolger SHA-2 empfohlen
SHA-2 SHA-224 SHA-256 SHA-384 SHA-512	2005–	Ab 2005 als NIST-Standard für Secure Hash Algorithm (SHA) empfohlen SHA-2 ist die Bezeichnung für eine Gruppe von vier Secure Hash Algorithmen: SHA-224, SHA-256, SHA-384 und SHA-512, welche im Vergleich zu SHA-1 längere Hash-Werte erzeugen, wobei der Zahlenwert in den SHA-Namen der Länge des Hash-Wertes in Bit entspricht SHA-2 wird in vielen Programmen und Protokollen verwendet, bspw. TLS, SSL, PGP, SSH, S/MIME und IPsec
SHA-3 SHA3-224 SHA3-256 SHA3-384 SHA3-512	2015–	Seit 2015 von NIST, zusätzlich zu SHA-2 empfohlener Secure Hash Algorithm (SHA). Dieser entstammt einem Wettbewerb und benutzt eine andere Berechnung als SHA-0, SHA-1, SHA-2 SHA-3 soll SHA-2 vorerst nicht ersetzen, sondern soll als Alternative eingesetzt werden. Sollte SHA-2 in Zukunft geknackt werden, kann ohne großen Aufwand zu SHA-3 gewechselt werden

SHADE
Schadsoftware in Form einer dateiverschlüsselnden Ransomware. Wird über Spam-Mails mit einem angehängten ZIP-Archiv versendet.

SHADER
Funktionen in Grafikchips oder in Programmen, die eingesetzt werden, um Schatteneffekte u. Ä. in 3D-Grafiken und 3D-Spielen umzusetzen.

SHARED SECRET (engl.)
Übsg. gemeinsames Geheimnis. Wird bspw. bei der Abfrage-Antwort-Authentifikation verwendet.

SHAREPOINT ONLINE [SPO] (engl.)
Ein Microsoft Office365-Service, der in der Cloud bereitgestellt wird, und als Hauptfunktion die Zusammenarbeit von Personen und Teams bietet.

SHELLCODE
Programmcode zur Ausnutzung einer Systemschwäche. Häufig in codierter Form als Opcode geschrieben, um die Lesbarkeit und Erkennbarkeit zu reduzieren.

SHELL EXTENSION (engl.)
Erweiterung von Windows Explorer, um zusätzliche Funktionen anzubieten, bspw. ermöglicht die Shell Extension GpgEX ein zusätzliches Menü für Dateiverschlüsselung.

SHITSTORM (engl.)
Schimpftiraden und Beleidigungen in Internet-Foren und sozialen Medien, meist aufgrund eines unbedachten oder unpopulären Kommentars oder Tweets.

SHODAN
Suchmaschine für das Finden von öffentlich erreichbaren Geräten und Datenbanken im Internet.

SHORT MESSAGE SERVICE [SMS] (engl.)
Übsg. Kurztextdienst. Funktion in Handys, um kurze Textnachrichten an andere Handys zu versenden. Die Längenlimitation von ursprünglich 160 Zeichen wird bei neueren Handys durch automatisches Versenden mehrerer SMS hintereinander aufgehoben, ohne dass der Benutzer sich darum kümmern muss. Über Gateways im Internet lassen sich solche Textnachrichten auch von und zu Computer verschicken. SMS wird noch häufig als ein zweiter Sicherheitsfaktor einer Zwei-Faktor-Authentifikation verwendet, was jedoch nicht mehr als sicher angesehen wird, da eine SMS abgefangen werden kann und Handys gestohlen werden können.

SICHERER HASH-ALGORITHMUS [SHA]
Syn. zu Secure Hash Algorithm. Gruppe standardisierter kryptografischer Hash-Funktionen. Damit können Prüfwerte für digitale Daten berechnet werden, sodass die Integrität dieser Daten jederzeit überprüft werden kann. Dies wird bspw. bei digitalen Signaturen verwendet.

SICHERES PROGRAMMIEREN
Syn. zu Secure Coding. Durch Schulung der Software-Entwickler sowie durch den Einsatz geeigneter Code-Testing- und Analyse-Tools können viele Programmierfehler verhindert werden, die zu Sicherheitsproblemen und Schwachstellen führen könnten.

SICHERE SYSTEMENTWICKLUNG
Methoden und Tools, die beim Aufbau eines Systems eingesetzt werden, um die Wahrscheinlichkeit eines zukünftigen Komponentenfehlers auf ein Minimum zu reduzieren.

SICHERHEIT IN DER INFORMATIONSTECHNIK
Syn. zu Informationssicherheit, IT-Sicherheit. Themenkreis, der sich mit dem Schutz von Daten vor unberechtigtem Zugriff, mit Zugriffskontrollen und mit der Privatsphäre in Computersystemen beschäftigt.

SICHERHEITSAKTUALISIERUNGEN
Verbesserungen an Software und Hardware zur Reduktion des Risikos eines Angriffs auf Daten und Systeme. Sobald neue Exploits, Softwareschwachstellen oder Hacker-Angriffe bekannt werden, versuchen Software- und Hardware-Hersteller diese Angriffsmöglichkeiten durch Verbesserungen und Aktualisierungen ihrer Produkte zu verhindern. Die Benutzer von Geräten und Software, bei welchen Aktualisierungen durchgeführt werden können, sollten die von den Herstellern bereitgestellten Updates zeitnah übernehmen. Viele Betriebssysteme und Software-Produkte, wie Windows, Android, iOS, MacOS u. Ä., bieten die Funktion einer automatischen Einspielung von Aktualisierungen an. Diese Funktion sollte aktiviert sein, damit die neuesten Aktualisierungen sofort installiert werden, sobald die Hersteller diese ausrollen. Auch Router, Autos, Webcams. vernetzte Kühlschränke, BIOS u. Ä. besitzen Software, die Fehler oder Schwächen beinhalten können, weswegen auf den Herstellerseiten regelmäßig nach Sicherheitsaktualisierungen Ausschau gehalten werden sollte.

SICHERHEITSDOMÄNE
Syn. zu Sicherheitsbereich. Systeme oder Applikationen, welchen alle den gleichen Sicherheitsrichtlinien einer zentralen Stelle folgen.

Tab. 21.3 Vergleich der Sicherheitsniveaus beim symmetrischen, kryptografischen Verfahren AES und asymmetrischen, kryptografischen Verfahren RSA

Schlüssellänge beim asymmetrischen, kryptografischen Verfahren RSA		Schlüssellänge beim symmetrischen, kryptografischen Verfahren AES
1024-Bit asymm. RSA	Sicherheitsniveau entspricht ca.	73-Bit symm. AES
2048-Bit asymm. RSA	Sicherheitsniveau entspricht ca.	112-Bit symm. AES
15360-Bit asymm. RSA	Sicherheitsniveau entspricht ca.	256-Bit symm. AES

Quelle: NIST.gov (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf, NIST Special Publication 800-57 Part 1Revision 4 [*Abgerufen am 22.12.2019*])

SICHERHEITSFRAGEN

Um das Passwort für Online-Profile oder -Konten zurückzusetzen, werden bei einigen Online-Diensten Details zum Benutzer abgefragt, welche dieser bei der Einrichtung des Kontos gespeichert hatte.

Beispiele: Ort der ersten Schule, Name des ersten Haustiers, Anzahl Geschwister u. Ä.

Da die korrekten Antworten auf viele solcher Fragen einfach im Internet und auf sozialen Medien gefunden werden können, wird empfohlen, die Antworten bei der Einrichtung des Accounts bewusst falsch einzutragen und diese falschen Angaben in einem Passwort-Manager u. Ä. zu speichern. Auch kann häufig darauf verzichtet und stattdessen eine andere 2FA-Methode verwendet werden.

SICHERHEITSLÜCKE

Fehler, Defekt oder Schwäche einer Software, eines Geräts, eines Netzwerks u. Ä., welche zu einem erhöhten Risiko eines Hacker-Angriffs führen kann.

SICHERHEITSNIVEAU [SN] (engl.)

Bei einem vertrauenswürdigen kryptografischen Verfahren für symmetrische Schlüssel gibt das Sicherheitsniveau den Aufwand in „Anzahl Versuchen“ an, der benötigt wird, um einen Schlüssel mit einer bestimmten Schlüssellänge zu brechen. Bspw. galt das kryptografische Verfahren DES mit 56-Bit Schlüssellänge bis vor wenigen Jahren als sicher, ist jedoch seit 2008 mit seinen ca. $7 \cdot 10^{16}$ möglichen Schlüssel innerhalb weniger Stunden zu knacken. Für symmetrische Verfahren werden heutzutage Schlüssellängen von mind. 128-Bit empfohlen.

Bei asymmetrischen kryptografischen Verfahren lässt sich das Sicherheitsniveau nicht direkt aus der Schlüssellänge ermitteln, sondern liegt tiefer, da asymmetrische Schlüssel Angriffsmöglichkeiten bieten, die bei symmetrischen Schlüsseln nicht vorliegen.

Beispielsweise entspricht ein RSA-Schlüssel mit 1024-Bit einem theoretischen Sicherheitsniveau von ca. 73-Bit (siehe Tab. 21.3).

Mit elliptischer Kurvenkryptografie (ECC) lassen sich höhere Sicherheitsniveaus erzielen. Bspw. lässt sich eine 255-Bit ECC-basierte Verschlüsselung vergleichen mit 2048- bis 3072-Bit asymm. RSA und ca. 128-Bit symm. AES.

SICHERHEITS-UPDATE
Syn. zu Sicherheitsaktualisierung

SICHERHEITSVERLETZUNG
Beeinträchtigung eines Systems, eines Programms, eines Netzwerks oder von Daten, durch Eingriff oder Manipulation von nicht berechtigten Personen.

SICHERHEITSVORGABEN
Vorschriften zur Sicherstellung der Sicherheit von Systemen, Betrieben, Software, Gebäuden usw. Oft sind dies regulatorische oder betriebsinterne Vorgaben.

SICHTBARKEIT
1) Einstellung innerhalb von Online-Diensten, der festlegt, wer welche Daten des Benutzers ansehen darf. 2) Geräteeinstellungen, bspw. für WLAN und Bluetooth bei Handys, zur Festlegung, ob dieses Gerät durch andere Geräte in der Nähe auffindbar sein soll und für den Aufbau einer Kommunikation angezeigt werden darf.

SID
Abk. für Security Identifier

SIDE-SELECTOR (engl.)
Übsg. Systemwähler. Gerät oder Software zur automatischen Auswahl des aktiven Servers in einem Failover-Cluster, damit die Datenkommunikation zwischen Client und Server stets aufrechterhalten bleibt, auch bei Ausfall eines der Server im Cluster.

SIEM
Abk. für Security Incident and Event Mgmt

SIGNALLING (engl.)
Austausch von Metadaten bei einer Kommunikation zw. Systemen. Dieses Signalling kann über den gleichen Kanal wie die eigentliche Datenkommunikation erfolgen oder über einen separaten Kanal.

SIGNATUR
Syn. zu digitale Signatur

SIGNATURE (engl.)
Übsg. Signatur

SIGNATURE HASH FUNCTION (engl.)
Übsg. Algorithmus zur Berechnung des Hash-Wertes eines Zertifikats. Syn. zu Hash-Algorithmus. Siehe auch Password Hash Function.

Beispiele: SHA256, WHIRLPOOL.

SIGNIEREN
Syn. zu digital unterschreiben. Methode, um mit einem privaten Schlüssel einen Prüfwert für einen Text, eine E-Mail oder eine Datei zu erzeugen, mit der eindeutig der Urheber und die Integrität nachvollziehbar sind. Damit kann bspw. sichergestellt werden, dass eine empfangene E-Mail vom richtigen Sender und ohne Veränderung angekommen ist. Der Algorithmus zur Erzeugung der Signatur bildet als Erstes einen Hash-Wert der Daten (z. B. mittels SHA-1) und wendet dann den privaten Schlüssel auf diesen Hash-Wert an. Dies ist keine Verschlüsselung, kann jedoch mit dem eindeutigen öffentlichen Schlüssel des Senders überprüft werden (siehe auch Spezialthema zur E-Mail-Verschlüsselung in Kap. 30).

SILVER TICKET (engl.)
Übsg. Silbernes Ticket. Gefälschter Kerberos-Schlüssel, der einem Benutzer Zugang zu allen Diensten im Netzwerk ermöglicht.

SIM CARD (engl.)
Abk. für Subscriber Identity Module. Übsg. Teilnehmeridentitätsmodul. Chipkarte zur eindeutigen Identifizierung eines Handys im Mobilfunknetz. Kann durch eine PIN geschützt werden, die beim Starten eines Handys abgefragt wird.

SIM CARD SWAP (engl.)
Übsg. SIM-Kartenaustausch. Syn. zu SIM Intercept Attack. Hacker-Angriff, bei dem einem zweiten Handy die gleiche Nummer zugewiesen wird und der Hacker dadurch die Identität und die Möglichkeiten des ursprünglichen SIM-Kartenbesitzers erhält.

SIM INTERCEPT ATTACK (engl.)
Syn. zu SIM Card Swap

SIMON
Schnelle Blockverschlüsselung, entwickelt 2013 durch die NSA. Die Methode ist auf Hardwareimplementationen optimiert, sodass diese bspw. auf IoT-Geräten eingesetzt werden kann. Es unterstützt die Blocklängen 32- bis 128-Bit und korrespondierende Schlüssel von 64- bis 256-Bit. Die gleichzeitig entwickelte Blockverschlüsselung Speck wurde auf Software-Implementationen optimiert.

SIMPLE MAIL TRANSFER PROTOCOL [SMTP] (engl.)
Übsg. Einfaches E-Mail-Transportprotokoll. Textbasiertes Verfahren für das Senden von E-Mails und das Weiterleiten von Server zu Server. Heutzutage wird der Transport vom Sender zum Server und zwischen den Servern meist mit TCP verschlüsselt. Dies wird in den E-Mail-Programmeinstellungen durch den Befehl STARTTLS vom Client an den Server auf Port 25 bzw. 587 oder ohne Befehl durch implizites TLS mittels SMTPS auf Port 465 angestoßen. Das Abholen von E-Mails vom Server geschieht über andere Protokolle wie POP3 und IMAP.

SIMPLE OBJECT ACCESS PROTOCOL [SOAP] (engl.)
XML-basiertes Netzwerk-Framework zur Kommunikation von Daten zw. Systemen, meist via HTTP mit TCP. SOAP definiert Regeln für das Design von Nachrichten und für die Interpretation der Daten innerhalb der Nachrichten. Dies erlaubt den Apps, beliebige, aber klar interpretierbare Informationen zu übertragen. Bspw. können Suchanfragen an Datenbanken via SOAP umgesetzt werden.

SIMPLEX
Kommunikation, die nur in eine Richtung stattfindet. Bspw. frühere Drucker, die nur Befehle empfingen, aber keine zurückgaben. Siehe auch halbduplexe und vollduplexe Kommunikation.

SIM SWAP FRAUD (engl.)
Übsg. Betrug durch SIM-Austausch. Siehe SIM Card Swap.

SINGLE-FACTOR CRYPTOGRAPHIC DEVICE (engl.)
Übsg. Ein-Faktor-kryptografisches Gerät. Ein solches Gerät führt kryptografische Operationen basierend auf darin sicher gespeicherten Schlüsseln durch. Je nach Einsatzgebiet verlangt dieses Gerät ein Passwort vor der Ausführung der kryptografischen Berechnungen.

SINGLE-FACTOR OTP DEVICE (engl.)
Übsg. Ein-Faktor One-Time-Password-Gerät. Spezielles Gerät oder Handy-App, welches ein Einmal-Kennwort erzeugt. Durch den Besitz des Geräts und zusätzlich entweder einem sicher darin gespeicherten Schlüssel oder einer vorher durchgeführten Anmeldung am Gerät wird kein zusätzliches Passwort benötigt, um ein Einmal-Kennwort zu erzeugen.

SINGLE-FACTOR SOFTWARE CRYPTOGRAPHIC AUTHENTICATOR (engl.)
Übsg. Ein-Faktor-kryptografischer Authenticator basierend auf Software. Kryptografischer Schlüssel, welcher auf einem Speichermedium gespeichert ist. Die Authentisierung basiert auf dem Besitz und der Kontrolle des Schlüssels.

SINGLE PAGE APPLICATION [SPA] (engl.)
Übsg. Einzelseiten-Web-Applikation. Internetauftritt, welcher nur aus einer Seite besteht und dynamisch aktualisiert wird, im Gegensatz zum klassischen Internetauftritt mit Hauptseiten und verlinkten Unterseiten. Vorteile von Single Page Apps liegen v. a. darin, dass die Last auf dem Webserver auch bei großen Benutzerzahlen niedrig gehalten wird, da jeweils nur ein Teil einer Seite gesendet werden muss. Auch für die Benutzer ist das Erlebnis angenehmer, da nicht zwischen Seiten gewechselt werden muss, was jeweils mit Wartezeit und Unterbruch der Interaktion einhergeht.

Beispiele für Single Page Apps: Facebook, Twitter, Spiele im Webbrowser, Produktvorstellungen.

SINGLE-SIGN-ON [SSO] (engl.)
Methode in Computersystemen, um Mehrfachauthentifizierungen zu vermeiden. Durch die Anmeldung eines Benutzers, bspw. an einem Windows-PC, authentifiziert er sich, und braucht nun sein Passwort nicht wieder einzugeben, wenn er sich an diesem PC bei SSO-angebundenen Applikationen oder über eine Terminal-Emulation an einem anderen System einwählen möchte. Die Applikation oder das zweite System erkundigt sich beim ersten System, ob der Benutzer bereits erfolgreich authentifiziert wurde und falls positiv, lässt es den Benutzer die Applikation gebrauchen oder auf Ressourcen des zweiten Systems zugreifen. Bei Windows-Systemen wird SSO via Kerberos in Kombination mit Active Directory umgesetzt.

SITE-TO-SITE ÜBERTRAGUNG ZWISCHEN SERVERN
Funktion in FTP, um Dateien direkt zwischen zwei Servern zu senden, ohne diese zuerst auf den Client herunter und auf den zweiten Server hochzuladen. Dafür wird das File Exchange Protocol (FXP) benutzt.

SITZUNGSSCHLÜSSEL
Syn. zu Session Key. Von zwei Systemen ausgehandelter Schlüssel für eine bevorstehende Verbindung, bspw. zw. Webserver und Webbrowser. Sobald die zwei Systeme erfolgreich eine sichere Verbindung aufgebaut haben, z. B. mittels TLS, können sie den beim Verbindungsaufbau gemeinsam vereinbarten, kürzeren Sitzungsschlüssel verwenden, um Daten symmetrisch und damit schneller zu verschlüsseln und zu übermitteln.

SKALIERBARKEIT
Möglichkeit bei Systemen zur einfachen Erhöhung der Leistung oder Speichermenge, falls sich der Bedarf erhöht.

SKC
Abk. für Secret-Key Cryptology

SKIMMING
Übsg. Abschöpfen, abschneiden.

SKIMMING-DATENKLAU
Datendiebstahl bei mobilen Geräten oder Geldautomaten durch das Auslesen von RFID oder Bankkartenmagnetstreifen und des PINs. Dazu werden bei Bankautomaten manipulierte Tastaturen vor die richtige Tastatur geklebt und Kartenleser vor dem Karteneinschubschacht angebracht.

SKYPE
Sofortnachrichten- und Videochatdienst.

SL
Abk. für Second Life

SLA
Abk. für Service Level Agreement

SLC
Abk. für Server Licensor Certificate

SMALL OFFICE AND HOME OFFICE [SOHO] (engl.)
Umgebungen, wie Büros und Wohnungen, in denen ein Home Area Network (HAN) aufgebaut und eingesetzt werden kann.

SMARTCARD
Karte im Kreditkartenformat, welche mit einem Chip, manchmal zusätzlich mit einer Antenne und weiteren Funktionen, wie Display, Batterie, Speicher und Prozessor ausgestattet ist. Die Smartcard kann ein digitales Benutzerzertifikat mit privatem Schlüssel speichern und mit einer PIN das sichere Login an einem PC ermöglichen. Dabei nimmt die Smartcard die Rolle eines physischen Tokens ein, der zusammen mit dem PIN eine Zwei-Faktor-Authentisierung (2FA) ermöglicht. Sobald der Benutzer des Computers den Smartcard-PIN eingegeben hat, wird dieser mittels kryptografischer Berechnungen und z. T. von Hinzuziehen von Schlüsselmaterial aus einer PKI mit dem auf der Karte gespeicherten Schlüssel verglichen und die Anmeldung am PC erlaubt oder geblockt. Falls Single Sign-On (SSO) im System oder Firmennetzwerk eingerichtet ist, kann der authentifizierte Benutzer weitere Dienste nutzen ohne nochmalige Anmeldung.

SMARTCARD AUTHENTICATION (engl.)
Übsg. Anmeldung und Authentifikation an einem System mittels Smartcard. Hierfür wird der auf der Smartcard gespeicherte Schlüssel zusammen mit einem Smartcard-PIN

benutzt. Bei größeren Firmen und Institutionen wird hierzu auch eine Abfrage bei der PKI durchgeführt, um die Identität des Benutzers zu prüfen.

SMART CONTRACT (engl.)
Übsg. Smarter Vertrag. Protokoll und Software, um einfache Verträge zw. zwei Parteien zu vereinbaren und automatisch auszuführen, ohne eine Person, welche diese Ausführung überprüfen oder regeln muss. Hierfür kann die Blockchain-Technologie eingesetzt werden, sodass Smart Contracts auf den Blockchain Nodes ausgeführt werden können, welche von anderen Nodes überprüft werden. Smart Contracts werden auch innerhalb von Kryptowährungen eingesetzt, um bspw. Auszahlungsregeln für Transaktionen umzusetzen.

SMART CONTRACT SECURITY (engl.)
Übsg. Sicherheitsaspekte bei Smart Contracts.

SMART HOME (engl.)
Übsg. Intelligentes Haus. Oberbegriff für Automatisierungen von Geräten und deren Vernetzung in Wohnräumen.

SMB
Abk. für Server Message Block

S/MIME
Abk. für Secure/Multipurpose Internet Mail Extensions. Verfahren zur asymm. Verschlüsselung und zur digitalen Signatur von E-Mails, basierend auf X.509-Zertifikaten. Definiert in PKCS#7.

Kostenpflichtige und für den Privatgebrauch kostenlose S/MIME-Zertifikate sind bei mehreren Firmen über das Internet erhältlich.

SMOKE TESTING (engl.)
Übsg. Rauchtests. Erste Tests bei einem neuen System oder einer neuen Software, um zu prüfen, ob sich das System oder die Software starten und bedienen lässt. Der Begriff stammt aus dem Bereich der Elektronik, bei der manchmal Rauch auftritt, wenn ein neues Gerät einen Kurzschluss enthält, überhitzt oder noch nicht ganz ausgereift ist.

SMS
Abk. für Short Message Service

SMS BASED AUTHENTICATION (engl.)
Bei vielen Online-Diensten wird zur Anmeldung ein Benutzername mit Passwort und zusätzlich ein Einmal-Kennwort benötigt, welches per SMS an den Benutzer geschickt wird.

SMTP
Abk. für Simple Mail Transfer Protocol

SMTP ENCRYPTION (engl.)
Übsg. SMTP-Verschlüsselung. Dies wird in den E-Mail-Programmeinstellungen durch den Befehl STARTTLS vom Client an den Server auf Port 25 bzw. 587 oder ohne Befehl durch implizites TLS mittels SMTPS auf Port 465 angestoßen.

SMTPS
Abk. für Simple Mail Transfer Protocol Secure. TLS-verschlüsselte Variante von SMTP.

SN
Abk. für Sicherheitsniveau

SNAKE
Name einer Hacker-Gruppe.

SNAPCHAT
Instant-Messaging-Dienst, bei welchem der Inhalt nach kurzer Zeit bei den Empfängern wieder verschwindet.

SNIFFER (engl.)
Übsg. Schnüffler. Software zum Auslesen der Netzwerkkommunikation. Dies wird einerseits zur Analyse verwendet, um Hacker-Angriffe zu detektieren, andererseits aber auch für Datendiebstahl.

SNIPPET (engl.)
Teil eines Quellcodes, der zu Schulungszwecken, zur Veranschaulichung oder zur Wiederverwendung in anderen Programmen bereitgestellt wird, der jedoch nicht ein ganzes Modul oder lauffähiges Programm sein muss.

SOA
Abk. für Service-Oriented Architecture

SOAK TEST (engl.)
Übsg. Dauerbelastungstest. Methode beim Testen von neuen oder veränderten Software- oder Hardware-Komponenten. Dabei wird das System mit ähnlich hoher Auslastung betrieben, wie später in der produktiven Umgebung.

SOAP
Abk. für Simple Object Access Protocol. Heutzutage wird SOAP jedoch nicht mehr als Abk. verwendet, sondern als eigenständiger Name.

SOCIAL ENGINEERING (engl.)
Übsg. Soziale Manipulation

SOCIAL MEDIA ANALYSIS (engl.)
Übsg. Analyse sozialer Medien. Methoden zur Analyse gesammelter Daten aus sozialen Medien. Die Resultate dieser Analysen können für Marketingzwecke verwendet werden.

SOCIAL MEDIA INCIDENTS (engl.)
Übsg. Vorfälle bei sozialen Medien. Neben dem Zeitverlust durch übermäßigen Konsum von sozialen Medien am Arbeitsplatz verursacht der Verlust und die Weitergabe vertraulicher Informationen mittels sozialen Medien großen Schaden für Firmen.

SOCIAL PROOF (engl.)
Übsg. Sozialer Beweis. Beeinflussung der Entscheidung einer Person davon, ob andere dieselbe Entscheidung auch bereits getroffen haben. Die Verhaltensforschung fand heraus, dass Personen sich besser fühlen, wenn sie Tätigkeiten ausführen, die ähnliche Menschen ebenfalls bereits ausgeführt haben. Dies wird bei Like-Buttons ausgenutzt.

SOCKET (engl.)
Übsg. Steckverbindung, Sockel. Verbindungsstelle zwischen Programmen in einem Computer oder über das Internet. Ein Programm kann bspw. einen Socket vom Betriebssystem via API anfordern, an welchen Daten geschickt und von welchem Daten empfangen werden können. Ein anderes Programm kann sich an diesen Socket anknüpfen, sodass Daten von beiden Programmen in beide Richtungen gesendet und empfangen werden können.

SOD
Abk. für Segregation of Duties

SOFORTNACHRICHTEN
Texte, die innerhalb von Chat-Applikationen in Echtzeit von einem Chatbenutzer zu einem anderen gesendet werden. Diese Texte besitzen keine oder nur wenige Metadaten im Unterschied zu E-Mails, die zeitversetzt und mit vielen Metadaten beim Empfänger ankommen. Einige Chat-Applikationen verschlüsseln die Texte, bevor diese verschickt werden, und helfen damit, dem Identitäts- und Datendiebstahl vorzubeugen und die Privatsphäre zu schützen.

SOFTCARD-PROTECTED KEYS (engl.)
Übsg. Softcardgeschützte Schlüssel. Einer von drei Arten der Autorisation für den Gebrauch von Schlüsseln in HSMs. Bei Softcard-Protected Keys wird eine Passphrase für den Gebrauch der Schlüssel benötigt. Die anderen zwei Arten sind: Module-Protected Keys und Token-Protected Keys.

SOFT TOKEN (engl.)
Abk. für Software Token. Softwarebasiertes Objekt, wie bspw. ein digitales Zertifikat, welches die Identität einer Person bestätigt oder für 2FA benutzt wird. Dieses softwarebasierte Objekt wird geschützt in einem digitalen Tresor auf einem PC, Handy u. Ä. gespeichert.

SOFTWARE AGENT (engl.)
1) Programm, welches nach Benutzereingabe Aktionen ausführt und ein Ergebnis für den Benutzer oder für ein anderes Programm liefert. 2) Client-Software eines Client-Server-Systems.

SOFTWARE-AKTUALISIERUNG
Verfahren, um Betriebssysteme, Applikationen und allgemein Software aktuell zu halten. Dabei werden Dateien oder Programme durch neuere Versionen ersetzt. Auf internetfähigen PCs und Handys sollte regelmäßig automatisch oder manuell nach Aktualisierungen gesucht und diese installiert werden, damit neue Sicherheitsbedrohungen sofort behoben werden können. Die meisten Betriebssysteme und viele Programme bieten eine entsprechende Updatefunktion an. Für ältere Geräte ohne eigenen Internetzugang oder ohne eine automatische Updatefunktion (z. B. USB-Drucker oder Router) sollte auch regelmäßig nach Aktualisierungen, aba. Firmware-Updates, gesucht und diese eingespielt werden, da diese Geräte ansonsten möglicherweise Hintertüren für Attacken wie DDoS bieten und missbraucht werden könnten.

SOFTWARE AS A SERVICE [SAAS] (engl.)
Service innerhalb eines Cloud-Angebots, bei welchem Software und dazugehörige Infrastruktur vom Cloud-Anbieter angeboten und von Kunden gemietet wird. Die Kunden ersparen sich den Aufwand und die Organisation des Installierens und der Updates.

SOFTWARE DEVELOPMENT LIFE CYCLE [SDLC] (engl.)
Strukturierte Projektvorgehensmethode zur Erstellung von Software. Anforderungen an die Software werden von der Entwicklungsphase bis zur Fertigstellung mithilfe von zahlreichen bewährten Standardmethoden, -vorlagen und -tools unterstützt und vereinheitlicht, mit dem Ziel ein Produkt hoher Qualität effizient erstellen zu können.

SOFTWARE RESTRICTION POLICIES [SRP] (engl.)
Sicherheitsfunktion in Windows, um das Ausführen von Programmen zu verhindern. Dies kann dazu beitragen, das Ausführen von Schadsoftware zu verhindern. Über Regeln lässt sich definieren, dass nur Programme aus einer zuvor festgelegten Liste ausgeführt werden können.

SOFTWARE SECURITY MODUL [SSM] (engl.)
Software, um Schlüssel sicher im RAM zu speichern, ähnlich wie ein hardwarebasiertes HSM.

SOHO
Abk. für Small-Office and Home-Office.

SOLARIS
Unix-Betriebssysteme von Sun Microsystems. Syn. zu SunOS, jedoch mit anderer Versionsnummer.

SOMETHING DETERMINING WHERE YOU ARE (engl.)
Übsg. Etwas, das darauf beruht, wo du bist. Ein möglicher Faktor bei Multi-Faktor-Authentisierung (MFA). Bspw. das Anmelden am WLAN innerhalb des Firmengebäudes.

SOMETHING DETERMINING WHO YOU ARE (engl.)
Übsg. Etwas, das darauf beruht, wer du bist. Ein möglicher Faktor bei Multi-Faktor-Authentisierung (MFA). Bspw. Fingerabdruck, Gesichtsform usw.

SOMETHING YOU DO (engl.)
Übsg. Etwas, das darauf beruht, was du tust. Ein möglicher Faktor bei Multi-Faktor-Authentisierung (MFA). Bspw. die installierten Apps, die Art des Tippens, die Häufigkeit der App-Benutzung usw.

SOMETHING YOU HOLD (engl.)
Übsg. Etwas, das darauf beruht, was du besitzt. Ein möglicher Faktor bei Multi-Faktor-Authentisierung (MFA). Bspw. eine Smartcard.

SOMETHING YOU KNOW (engl.)
Übsg. Etwas, das darauf beruht, was du weißt. Ein möglicher Faktor bei Multi-Faktor-Authentisierung (MFA). Bspw. ein Passwort.

SOZIALE MANIPULATION
Ausnutzen der Hilfsbereitschaft, des Vertrauens oder der Neugier von Opfern, um sich Zugang zu privaten oder geschäftlichen Bereichen und Informationen zu beschaffen.

SPA
1) Abk. für Single Page Application. 2) Abk. für Secure Password Authentication

SPAM
Unerwünschte Werbe-E-Mails oder Einträge in Foren und Kommentaren.

SPAM FILTER (engl.)
Abk. für Anti-Spamfilter

SPAMMER (engl.)
Hacker-Tool, um automatisch Spameinträge in Foren und Kommentarfeldern einzufügen. Auch für Fake News und politische Propaganda eingesetzt.

SPAN PORT (engl.)
Abk. für Switched Port Analyzer Port. Funktion in einem Switch, um Datenpakete eines Ports am Switch auf einem anderen Port zu duplizieren. Dies erlaubt die Beobachtung der Daten, bspw. zur Erkennung von Angriffen.

SPÄHPROGRAMM
Syn. zu Spionagesoftware

SPC
Abk. für Security Processor Certificate

SPEAR PHISHING ATTACK (engl.)
Syn. zu Advanced Spear Phishing Attack

SPECK
Schnelle Blockverschlüsselung, entwickelt 2013 durch die NSA. Die Methode ist auf Software-Implementationen optimiert, sodass diese bspw. auf schwachen Handys eingesetzt werden kann. Es unterstützt die Blocklängen 32- bis 128-Bit mit korrespondierenden Schlüsseln von 64- bis 256-Bit. Die gleichzeitig entwickelte Blockverschlüsselung Simon wurde auf Hardware-Implementationen optimiert.

SPECTRE
Im Jahre 2017 gefundene und 2018 publizierte Hardwaresicherheitslücke in sehr vielen Mikroprozessoren, welche den Zugriff auf Speicherbereiche anderer Prozesse ermöglicht, aba. Seitenkanalattacke. Spectre wurde Anfang 2018 zeitgleich mit der Prozessorsicherheitslücke Meltdown veröffentlicht.

SPEICHERUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Abschnitt im Lebenszyklus kryptografischer Schlüssel. Siehe zusätzliche Details beim Begriff Schlüssel.

SPEICHERUNG VON INFORMATION
Abschnitt im Lebenszyklus von Informationen.

SPERREN
Aktion bei Computern und Handys, um diese in einen Zustand zu bringen, von dem nur mit einer erneuten Anmeldung mit PIN, Face-ID, Benutzername und Passwort u. Ä. das Gerät entsperrt wird und die Benutzung wieder möglich ist. Damit ist dies eine wichtige Schutzmaßnahme für die Datensicherheit. Die Aktion des Sperrens wird entweder bewusst durch den Benutzer ausgelöst oder nach einer gewissen Timeout-Zeit automatisch gestartet. Auf dem Sperrbildschirm können Informationen eingeblendet, andere Benutzerkonten gewählt, das Gerät neu gestartet und bei Handys eine Notfallnummer angerufen werden.

SPERRZERTIFIKAT
Syn. zu Widerrufszertifikat. Zertifikat, welches für ein Schlüsselpaar aus öffentlichem und privatem Schlüssel erstellt werden kann. Falls das Schlüsselpaar kompromittiert wird, kann dieses Sperrzertifikat aktiviert werden, indem es auf Public Key Servern veröffentlicht wird. Damit wird das zugehörige Schlüsselpaar gesperrt. Ein gesperrtes Schlüsselpaar kann weiterhin verwendet werden, um alte Signaturen zu verifizieren und Daten zu entschlüsseln, solange der private Schlüssel noch immer im Besitz der ursprünglichen Person ist.

SPIDER (engl.)
Übsg. Spinne. Syn. zu Bot, Robot, WebCrawler, Searchbot. Programm, welches im Internet Verlinkungen folgt, um neue Internetseiten zu finden und diese zu indexieren. Indexierte Seiten können bei Suchanfrage durch Benutzer durchsucht und angezeigt werden.

SPIONAGE-SOFTWARE
Syn. zu Spyware. Programme in Form von Malware, wie z. B. Keylogger, die unbemerkt auf Computer oder Netzwerke hineingebracht werden und es Kriminellen, Überwachungsinstitutionen, Konkurrenten, Kriegsgegnern oder dem Hersteller der Computer erlauben, die Aktivitäten der Benutzer aufzuzeichnen, zu analysieren oder persönliche Daten, geheime Pläne, Dokumente und Passwörter zu übermitteln. Häufig gelangen solche Spionageprogramme mittels vorinstallierter Software mittels Social Engineering, bspw. gratis abgegebener USB-Sticks, mittels Downloads einer scheinbar sinnvollen Browsererweiterung, wie bspw. eine zusätzliche Symbolleiste, oder durch Insider auf Firmencomputer oder auf privat genutzte Computer. Aktuelle Anti-Viren-Programme schützen teilweise gut vor Spyware, wobei diese als „potenziell unerwünschte Software“ gekennzeichnet und behandelt wird, da Spyware nicht immer eindeutig als solche klassifizierbar ist.

SPLUNK
System zur Beobachtung, Analyse und Darstellung von Log-Dateien.

SPO
Abk. für SharePoint Online, ein Microsoft Office365 Service.

SPOOFING (engl.)
Übsg. Verschleierung

SPRITZ
2014 vorgeschlagene, verbesserte Variante von RC4. Kann als Strom-Chiffre und Hash-Algorithmus verwendet werden.

SPYWARE (engl.)
Übsg. Spionage-Software

SQLCIPHER
Erweiterung für SQLite, um Datenbankdateien mit AES 256-Bit zu verschlüsseln.

SQL-INJECTION
Ausnutzen einer Sicherheitslücke bei SQL-Datenbanken. Dabei werden SQL-Anfragen durch direkte Übernahme von Benutzereingaben oder durch manipulierte URL-Veränderungen direkt ohne weitere Prüfung zur Datenbank geschickt. Dadurch können Daten in der Datenbank geändert, abgefragt oder gelöscht werden. Auch Betriebssystemfunktionen auf dem Datenbankserver können ausgeführt werden. Neuere Webserver erkennen und blockieren solche Attacken.

SQLITE
Einfache Datenbank, welche innerhalb von Programmen eingebaut wird, anstatt eines separaten Client-Server-Dienstes. Diese wird bspw. bei Handy-Apps verwendet.

SRANDOM
Funktion in Linux und Max OS X zur Generierung von Zufallszahlen. Genauer Ort: /dev/srandom.

SRP
Abk. für Software Restriction Policies

SRTP
Abk. für Secure Real-Time Transport Protocol

SS7
Abk. für Signalisierungssystem Nummer 7. Telekommunikationsprotokoll. Eine Schwachstelle in SS7 wurde mehrfach ausgenutzt, um Multi-Faktor-Autorisierung zu umgehen.

SSDLC
Abk. für Secure Software Development Life Cycle, Secure SLDC.

SSH
Abk. für Secure Shell

SSH-1/SSH-2
Versionen von Secure Shell (SSH). Die 1995 entwickelte erste Version SSH-1 wurde wegen Sicherheitsschwachstellen 1996 durch SSH-2 ersetzt, welche heute noch als sicher gilt.

SSH FILE TRANSFER PROTOCOL [SFTP]
Abk. für FTP über SSH.

SSL
Abk. für Secure Sockets Layer, die veraltete Variante von Transport Layer Security (TLS) (siehe Tab. 22.1).

SSL-HANDSHAKE
Start einer SSL-verschlüsselten Kommunikation. Dabei werden eine sichere Authentifizierung und eine Identifikation der Kommunikationsparteien durchgeführt.

SSO
Abk. für Single Sign-On

SSPI
Abk. für Security Support Provider Interface

STAATS-TROJANER
Ugs. Software zur Beobachtung und zum Ausspähen von Verdächtigen, eingesetzt durch die Polizei oder andere Behörden.

STACK
1) Übsg. Stapelspeicher. Eine dynamische Datenstruktur, bei der nur jeweils das zuletzt hinzugefügte Element gelesen wird („Last in, First out“). 2) Abk. für Software Stack. Übsg. Software-Stapel. Syn. zu Full-Stack. Beschreibung der einem Software-Produkt zugrunde liegenden Technologien.

Beispiele für Software-Stacks

a) LAMP-Stack als Abk. für Linux, Apache, MySQL und PHP.
b) WIMP-Stack als Abk. für Windows, IIS, MySQL, Perl.

STACK OVERFLOW (engl.)
1) Übsg. Stapelüberlauf. Programmfehler bei Benutzung von mehr Speicher als zugewiesen oder verfügbar. 2) Online-Dienst für Software-Entwickler. Darin können Fragen gestellt und von jedermann beantwortet werden.

STANDARD-PASSWORT
Geräte, wie Router oder IP-Webcams werden häufig mit einem Initial- oder Standardpasswort geschützt, welches jedoch bei allen Geräten gleichen Typs gleich ist und deshalb schnell im Internet auffindbar ist. Deshalb ist es wichtig, Standardpasswörter sofort vor Inbetriebnahme von Geräten zu ändern.

STANDING ACCESS (engl.)
Übsg. Stehender, ständiger Zugang.

STARTPAGE.COM
Internetsuchmaschine, die weder Suchanfragen noch andere Daten des Benutzers speichert oder verfolgt. Außerdem zeigt diese keine zielgerichtete Werbung und respektiert die Privatsphäre des Benutzers.

STARTTLS
Befehl zum Starten der Kommunikationsverschlüsselung mittels Transport Layer Security (TLS), insb. beim Versand und Empfang von E-Mails mit SMTP, POP3 und IMAP. Da der Verbindungsaufbau bis zum Befehl StartTLS unverschlüsselt geschieht und danach bei Kommunikationsfehlern aus Kompatibilitätsgründen auf unverschlüsselte Kommunikation zurückgewechselt werden kann, ohne den Benutzer zu informieren, wird der direkte Einsatz von TLS via SMTPS, POP3S und IMAPS auf den entsprechenden Ports 465, 995, 993 empfohlen.

STATELESS/STATEFUL (engl.)
Übsg. Zustandslos/zustandsbehaftet. Adjektive, die beschreiben, ob ein PC oder eine App nachfolgende Interaktionen des Benutzers mit dem System oder Interaktionen von Systemen untereinander speichert bzw. nicht speichert.

STATE SPONSORED (engl.)
Übsg. Finanziert durch den Staat.

STATIC APPLICATION SECURITY TESTING [SAST] (engl.)
Software zur Analyse von Quellcode und kompiliertem Code bzgl. Sicherheitsschwachstellen. Dabei wird der Code im nicht laufenden Betrieb analysiert, im Gegensatz zu Dynamic Application Security Testing.

STATIC CODE ANALYSIS (engl.)
Übsg. Statische Codeprüfung. Software und Verfahren zur frühzeitigen Erkennung von Sicherheitsrisiken während der Entwicklung neuer Applikationen. Dabei wird der Quellcode nach möglichen Schwachstellen durchsucht, sodass solche Probleme frühzeitig und effizient behoben werden können, und das finale Produkt möglichst wenige Angriffsziele bietet.

STATIC CODE SCANNING (engl.)
Übsg. Statische Codedurchsicht. Verfahren innerhalb einer Static Code Analysis.

STICKY (engl.)
Übsg. Klebend. Methode zur Lastverteilung bei Ressourcen, wie z. B. Servern, bei welcher der Loadbalancer die Anfragen von Clients (genauer: der aufgebauten Client/Server-Sessions) von immer dem gleichen Server bedienen lässt. Andere Lastverteilungsmethode: Round Robin.

STIMMABDRUCK
Audioaufnahme und Audioprofil der Stimme einer Person, bspw. während eines Anrufs oder bei Ansprechen eines persönlichen Agenten wie Alexa, Siri usw. Die Stimme einer Person gibt Hinweise zur Persönlichkeit, Stimmung, Krankheiten und Motivation der Person und muss deshalb als schutzwürdiger persönlicher Datenwert angesehen werden.

STOP THE BLEEDING (engl.)
Übsg. Stoppen des Ausblutens. Pläne oder Aktionen, um schnellstmöglich den weiteren Datenverlust zu stoppen.

STORAGE AREA NETWORK [SAN] (engl.)
Übsg. Speichernetzwerk. Hardware und Software, welche ein eigenes Netzwerk bilden zur Übertragung von Daten von und zu Computersystemen auf Speichermedien in diesem SAN und in anderen Netzwerken. Ein SAN besitzt neben der Infrastruktur zur Kommunikation auch eine Verwaltungsebene, die die Verbindungen, Speicherelemente und Computersysteme so organisiert, dass die Datenübertragung sicher und robust ist.

STORAGE OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Speicherung eines kryptografischen Schlüssels.

STORING AND ARCHIVING OF INFORMATION (engl.)
Übsg. Speicherung und Archivierung von Information.

STRANDHOGG
Sicherheitslücke in allen Versionen von Android bis Android 10. Zur Ausnutzung der Sicherheitslücke lenkt eine Schadsoftware den Start einer richtigen App so um, dass die

Schadsoftware zusätzliche Berechtigungen erfragen kann und erst danach die richtige App geladen wird. Damit erhält die Schadsoftware Zugriff auf Mikrofon, Kamera, GPS und SMS und kann zum Aushorchen oder zur Spionage verwendet werden.

STREAM CIPHER (engl.)
Übsg. Strom-Chiffre

STREAMING (engl.)
Begriff für Video- und Audiodatenübertragungen von einem Computer über ein Netzwerk an einen anderen Computer. Dies sind bspw. Radiosendungen, Musikstücke oder TV-Sendungen. Dabei werden die gestreamten Daten auf dem Zielsystem meist nicht dauerhaft gespeichert, sondern direkt abgespielt und danach wieder gelöscht. Steaming wurde Anfang der 2000er-Jahren möglich und populär, als Datenkompressionsmethoden und schnellere Internetleitungen zur Verfügung standen.

STROMAUSFALL
Eines der Ziele von Cyber-Attacken auf Industrieanlagen und Staaten. Ein Stromausfall im Osten von Europa 2015 geschah wahrscheinlich aufgrund einer Cyber-Attacke, welche via verseuchten E-Mail-Anhängen auf die Steuer-PCs der Anlagen gelangte.

STROM-CHIFFRE
Syn. zu Stream Cipher. Algorithmus in der Kryptografie zur Durchführung von symm. Verschlüsselung und Entschlüsselung, bei der ein kontinuierlicher Strom von Zeichen als sog. Schlüssel verwendet wird, um jedes Zeichen des Klartextes nacheinander umzuwandeln. Der benutzte Zeichenstrom kann aus einem Passwort bestehen, welches ständig wiederholt wird, oder bspw. aus einem zufällig gewählten Text eines Buches. Solche Algorithmen für Strom-Chiffre können in Hardware schnell mittels Schieberegister implementiert werden und werden deshalb u. a. im Mobilfunknetz GSM benutzt. Sie sind jedoch angreifbar, falls sowohl der Klartext als auch der verschlüsselte Geheimtext abgehört werden, wie dies bei WLAN-Verschlüsselungsverfahren WEP möglich ist. Siehe auch Cipher.

STRONG-2FA (engl.)
Übsg. Starke 2FA. Einsatz von sicheren Faktoren innerhalb einer Zwei-Faktor-Authentifikation. Physische Token, wie Smartcards oder biometrische Methoden, wie Iris-Scanner, sind stärker als vierstellige PINs, welche über SMS zugeschickt werden.

STRUKTURIERTE DATEN
Daten, mit geordneter, innerer, bekannter Struktur. Bspw. Datenbanken, Listen mit Kreditkartennummern usw. E-Mails besitzen sowohl strukturierte Daten wie Absender, Empfänger, Betreffzeile etc., als auch unstrukturierte Daten wie Bilder. Die maschinelle

Analyse strukturierter Daten kann meinst mit wenig Aufwand geschehen, im Gegenteil zu unstrukturierten Daten, wie bspw. Filme oder Audioaufnahmen.

STUXNET
Schadsoftware in Form eines Computer-Wurms. Dieser wurde 2010 entdeckt, aber entstand wahrscheinlich bereits 2005. Diese Malware zielte auf große Industrieanlagen und erlaubte destruktive Attacken.

SU
1) Abk. für SuperUser. 2) Abk. für Substitute User, Übsg. Benutzerwechsel. Dieses Kommando erlaubt bei Unix-kompatiblen Betriebssystemen, Befehle unter einem anderen Benutzer auszuführen, nachdem das Passwort des anderen Accounts eingegeben wurde. SU ist ähnlich zum Befehl „sudo“, bei dem jedoch das eigene Passwort eingegeben werden muss, damit man als SuperUser Befehle ausführen kann, sofern die Berechtigung in der Datei /etc/sudoers eingetragen ist.

SUBNET
Abgeschlossenes Netzwerk mit eigenen IP-Adressen. Dies erlaubt die lokale Kommunikation zwischen den PCs im Netzwerk. Ein Router ermöglicht den darin enthaltenen PCs zusätzlich die Verbindung zu einem größeren Netzwerk und dem Internet.

SUBNET MASK (engl.)
Übsg. Subnetzmaske. Eine elektronische Schablone, die definiert, welche und wie viel IP-Adressen im Subnetz für Geräte verwendet werden können. In Heimnetzwerken wird häufig die 24-Bit Subnetzmaske 255.255.255.0 mit den privaten IP-Adressen 192.168.0.x benutzt (zusammengefasst bezeichnet als: 192.168.0.0/24) und damit festgelegt, dass die letzte Ziffer, d. h. 192.168.0.0–192.168.0.255 für die Geräte im Heimnetzwerk benutzt werden können, wobei 192.168.0.0 und 192.168.0.255 nicht verwendet werden dürfen, da diese bereits vorbesetzt sind.

SUBORDINATED CERTIFICATE (engl.)
Übsg. Untergeordnetes Zertifikat. Syn. zu Intermediate Certificate. Zertifikat, welches zwischen CA-Root-Zertifikat und anderen, bspw. normalen Userzertifikaten steht und verwendet werden kann, um weitere Zertifikate zu signieren. Da es zurückverfolgt werden kann bis zum CA-Root-Zertifikat, ist es auch vertrauenswürdig und kann bspw. in Browser eingetragen werden. Vorteil eines Subordinated Certificate ist, dass die Root-CA dieses Zertifikat jederzeit als ungültig erklären kann, falls es kompromittiert wurde.

SUBSTITUTIONSCHIFFREN
Verschlüsselungsmethode, welche auf der Substitution von Buchstaben basiert.

SUCHMASCHINE
Software zur Suche von Daten in Systemen. Bekanntestes Bsp. sind Suchmaschinen, wie Bing.com, Google.com, Startpage.com usw. zur Suche nach Internetseiten, welche bestimmte Stichworte beinhalten.

SUDO
Abk. für SuperUser Do. Kommando bei Unix-kompatiblen Betriebssystemen. Dieses erlaubt nach Eingabe des eigenen Passworts, Befehle als Admin-Benutzer auszuführen, sofern die Berechtigung in der Datei „/etc/sudoers“ eingetragen ist.

SUNOS
Unix-Betriebssysteme von Sun Microsystems. Syn. zu Solaris, jedoch mit anderer Versionsnummer.

SUPERUSER-KONTO
Syn. zu Root-Konto. Admin-Benutzerkonto, welches bei der Installation des PC-Betriebssystems angelegt wird und über umfangreiche Rechte verfügt und deswegen nicht im Alltag verwendet werden sollte. Auf Unix-Maschinen kann sich ein Benutzer mit dem Befehl „su“ und der Eingabe des SuperUser-Passworts im laufenden Betrieb als SuperUser anmelden.

SUPERUSER-ZUGANG
Syn. zu Admin-Zugang. Auf Windows-PCs wählt man das „Administrator“-Konto zur Anmeldung. Auf Unix-PCs kann sich ein Benutzer mit dem Befehl „su“ und der Eingabe des SuperUser-Passworts im laufenden Betrieb als SuperUser anmelden. Um nur einzelne Befehle auszuführen, kann auch der String „sudo“ vor dem Befehl eingetippt werden, bspw. „sudo cd /tmp“ oder man öffnet eine Root Shell mittels „sudo bash“ und arbeitet darin als SuperUser.

SUPERVISED LEARNING (engl.)
Übsg. Überwachtes Lernen. Methode der künstlichen Intelligenz. Hierbei werden Daten benutzt, um ein Modell zu optimieren („zu trainieren“), in dem bspw. die Differenz zwischen der Vorhersage des Modells und des erwarteten Resultats verglichen („überwacht“) wird und als Maß zur weiteren Anpassung der Modellparameter benutzt wird. Das Ziel ist häufig, ein Modell zu erstellen, mit dem zukünftige Daten richtig klassifiziert werden können. Supervised Learning ist eine von drei grundlegenden Lernmethoden des maschinellen Lernens neben Reinforcement und Unsupervised Learning.

Beispiel für Supervised Learning

Von einem vollen Obstkorb sollen jeweils gleiche Früchte in kleinere Körbe verteilt werden. Dem Modell wird nun für jede mit einer Kamera aufgenommenen und mit einem Roboter bewegten Frucht mitgeteilt, ob es sich um eine Banane, einen Äpfel

oder eine Kirsche handelt. Das System passt nach jeder so bestimmten Frucht die Parameter an, sodass es neue Früchte zunehmend besser anhand von Farbe, Größe und Form vorhersagen kann.

SUPERVISORY CONTROL AND DATA ACQUISITION [SCADA] (engl.)
Übsg. Überwachungssteuerung und Datenerfassung. System aus Software und Hardware zur Überwachung von großen Industrieanlagen.

SUPPLEMENTAL DOWNLINK [SDL] (engl.)
Übertragungsform bei 5G Mobilfunk, bei welcher für eine Verbindung drei Funkkanäle verwendet werden.

SURFACE WEB (engl.)
Öffentlich zugänglicher Teil des Internets. Grenzt sich gegen das „Deep and Dark Web" ab.

SWIFT
Abk. für Society for Worldwide Interbank Financial Telecommunication. Ein standardisiertes Zahlungsverkehr-Datensystem.

SWIFT ATTACK
Angriff auf das SWIFT-Zahlungsverkehrdatensystem im Jahre 2016. Dabei wurde eine Bank in Bangladesch attackiert und ca. 80 Mio. US$ erbeutet.

SWISS DPA
Abk. für Swiss Federal Data Protection Act. Übsg. Schweizerisches Bundesgesetz über den Datenschutz (DSG).

SWISSID
USB-Stick oder Chipkarte zur eindeutigen Identifizierung von Personen in der Schweiz. Die SwissID bietet einen standardisierten, elektronischen Identitätsnachweis, welcher für Einkäufe online oder auch als rechtsgültige elektronische Signatur verwendet werden kann. Bereitgestellt wird die SwissID von SwissSign Group AG und drei anderen Anbietern.

SWISSSIGN
Abk. für SwissSign Group AG. Im Jahr 2018 gegründete Gruppe aus 17 schweizerischen Firmen mit dem Ziel der Erstellung und Bereitstellung der SwissID.

SWITCH
Gerät, welches mehrere Computer miteinander verbindet, ähnlich wie Router, aber mit kleinerem Funktionsumfang.

SYMMETRIC CRYPTOGRAPHY (engl.)
Übsg. Symmetrische Verschlüsselung, und allg. symm. Kryptografie.

SYMMETRIC ENCRYPTION (engl.)
Übsg. Symmetrische Verschlüsselung

SYMMETRISCHE KOMMUNIKATION
Syn. zu Peer-to-Peer-Kommunikation. Datenaustausch unter gleichberechtigten Kommunikationsteilnehmern.

SYMMETRISCHE VERSCHLÜSSELUNG
Kryptografische Methode zur Verschlüsselung von Nachrichten und Daten. Dabei wird von jedem Kommunikationspartner der gleiche geheime Schlüssel zur Ver- und Entschlüsselung verwendet, welcher vorweg sicher ausgetauscht werden muss.

SYNCHRONE KOMMUNIKATION
Kommunikation, die auf Antwort oder auf ein Taktsignal wartet bevor die Kommunikation fortgesetzt wird. Beispiel: HTTP-Anfragen, oder auch Personen die miteinander sprechen und sich nicht ins Wort fallen.

SYNTAX
Syn. zu Schreibweise

SYSADMIN
Abk. für Systemadministrator. Person, welche IT-Systeme und Netzwerke installieren, konfigurieren, bearbeiten, aktualisieren und betreiben. Der SysAdmin besitzt erhöhte Zugangsrechte, um die Tätigkeiten auszuführen.

SYSTEMATIC MONITORING (engl.)
Übsg. Systematische Überwachung. Dies kann bspw. eine Überwachung der Benutzereingaben in einem Webbrowser sein, um die angeklickten Links aufzuzeichnen und für Marketingzwecken zu verwenden.

SYSTEMATIC RISK (engl.)
Übsg. Systematisches Risiko. Risiko, welches im System oder Verfahren vorhanden ist. In der Finanzmathematik beschreibt es den Anteil, der auch bei optimaler Zusammensetzung eines Portfolios nicht diversifiziert werden kann.

SYSTEM-PRIVILEGIEN
Syn. zu Administratorrechte

T 22

TALKTALK ATTACK
SQL-Injektion-Attacke auf die Kommunikationsfirma TalkTalk im Jahr 2015.

TAMPERING (engl.)
Übsg. Sabotage, Verfälschung.

TAMPER-RESISTANT HARDWARE (engl.)
Übsg. Manipulationssichere Hardware, die eine hohe Sicherheit gegen Eindringlinge und Sabotage bietet. Beispiel: HSM, Smartcard, speziell gehärteter USB-Stick.

TAN
Abk. für Transaktionsnummer

TCP
Abk. für Transmission Control Protocol

TCP/IP
Abk. für Transmission Control Protocol/Internet Protocol. Verwendung von TCP bei IP-Netzwerken.

TCP PORT-WEITERLEITUNG
Funktion, um unter Benutzung des Kommunikationsprotokolls TCP von einem Netzwerk A, über ein Gateway zu einem System innerhalb eines anderen Netzwerks B zu gelangen. Dies wird bspw. für Tunneling verwendet.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_22

TECHNOLOGIE-LEBENSZYKLUS
Vierstufiges Lebenszyklusmodell für Technologien. Dabei wird unterschieden zwischen der

a) Entstehungsphase, ausgeführt als Forschung und Entwicklung,
b) Wachstumsphase nach Einführung der Technologie,
c) Reifephase als etablierte Technologie,
d) Phase der Alterung, bei welcher bereits mögliche Ablösetechnologien entstehen.

TECH-STACK
Syn. zu Stack. Beschreibung der Tools, die zur Entwicklung von Software benutzt werden.

TELETRUST
Bezeichnung für den Bundesverband IT-Sicherheit e. V. Ein Verein zur Stärkung der IT-Sicherheit in Deutschland.

TELNET
Abk. für Teletype Network. Netzwerkprotokoll und Software zum Datenaustausch zw. Clients und Servern über das Internet. Benutzt wird Telnet hauptsächlich zur Fernsteuerung von Systemen innerhalb eines Kommandozeileninterpreterfensters. Da bei Telnet eine unverschlüsselte Verbindung aufgebaut und das Passwort im Klartext übertragen wird, wird heutzutage das sicherere Secure Shell (SSH) empfohlen.

TENANT (engl.)
Übsg. Mieter, Mandant, Auftraggeber, Bereich. Bei mandantenfähigen Software- oder Cloud-Lösungen verwendet eine Gruppe von Personen einen Tenant, d. h. einen eigenen Bereich zum gemeinsamen Zugriff. Dieser Bereich ist abgetrennt von anderen Tenants. Bspw. sind auf Hostingsystemen mehrere Domains unterschiedlicher Firmen vorhanden, die jeweils als unterschiedliche Tenants behandelt werden.

TENANT KEY (engl.)
Übsg. Mandantenschlüssel zur gemeinsamen Nutzung von Software- oder Cloud-Lösungen.

TENSORFLOW
Open-Source Maschine Learning. Umgebung zur Entwicklung von Anwendungen und Funktionen in der Programmiersprache Python.

TERMINAL
Syn. zu Konsole. Programm, um Systembefehle und Systemausgaben textbasiert auszuführen und darzustellen. Bevor grafische Benutzeroberflächen und Computermäuse Ende

1970er-, Anfang 1980er-Jahren auf allen Computersystemen verfügbar waren, wurden Computer textbasiert benutzt, bspw. unter DOS oder Unix. Moderne Systeme erlauben eine solche textbasierte Benutzung mit Programmen wie „CMD.exe“ (unter Windows) und „Terminal“ (unter Linux und Mac). Heutzutage werden auch andere Geräte Terminal genannt, wenn Personen daran Eingaben machen können.

TERMINAL-EMULATION
Software zur Darstellung eines Terminals in einem Fenster innerhalb einer grafischen Benutzeroberfläche.

TERMINATION OF ACCESS (engl.)
Übsg. Beendigung des Zugriffs.

TERMINATION OF USER ENTITLEMENT (engl.)
Übsg. Beendigung einer Benutzerberechtigung.

TEXT MINING (engl.)
Übsg. Text-Schürfen. Automatisierte Methoden zur Entdeckung von Wissen in Texten, ähnlich zu Data-Mining, jedoch sind die Inhalte und die Informationen in Texten meist weniger strukturiert als bei reinen (strukturierten) Daten und die Bestimmung der Bedeutung deswegen aufwendiger.

THEFT (engl.)
Übsg. Diebstahl, bspw. Datendiebstahl

THICK CLIENT (engl.)
Syn. zu Fat Client

THIN CLIENT (engl.)
System oder Programm, welches einen Server benötigt, um Aufgaben zu erledigen. Häufig sind Thin Clients einfache PCs, welche die Benutzereingaben an den Server schicken und nur zur Darstellung der Ausgabe des Servers benötigt wird. Gegenteil von Fat Client.

THINKPHP
Web-App-Entwicklungsumgebung. 2018 wurde eine Schwachstelle gefunden, die via Remote Code Execution (RCE) augenutzt werden konnte und ein hohes Risiko darstellte.

THREAT ACTOR (engl.)
Übsg. Bedrohungsakteur. Person oder Gruppe von Personen, welche verantwortlich ist für einen ausgeübten oder geplanten Hacker-Angriff.

THREAT HUNTING (engl.)
Übsg. Bedrohungsjäger. Person oder Gruppe von Personen, welche aktiv nach möglichen Bedrohungen fahnden, um diese zu verhindern.

THREAT INTELLIGENCE (engl.)
Abk. für Cyber Threat Intelligence. Übsg. Cyber-Angriffswissen.

THREAT-LED PENETRATION TESTING (engl.)
Übsg. Angriffsgeleitetes Penetration Testing. Prüfen der potenziellen Angriffe und deren Erfolgschancen, um diese zu verhindern.

THREAT MODELING (engl.)
Übsg. Bedrohungsmodellierung. Methoden und Tools zur Identifikation und systematischer Bewertung und Behandlung von möglichen Bedrohungsszenarien. Ziel ist der effiziente Einsatz von Geld- und personellen Aufwänden bei den größten Risiken.

THREEMA
Sofortnachrichtendienst, der die Datensicherheit und Privatsphäre durch Verschlüsselung schützt.

THUNDERSTRIKE-ATTACKE
Über physischen Zugang zum Thunderbolt-Eingang von Mac-PCs konnten Hacker eigenen Code in den Flash-ROM schreiben und damit eine neue Firmware-Bootroutine ausführen lassen.

TIMEOUT (engl.)
Übsg. Auszeit. Ereignis bei Software, welches nach einer vordefinierten Zeitspanne eintrifft und Verbindungen oder Systeme in einen vordefinierten Zustand bringt. Dies ermöglicht Ressourcen zu schonen und die Sicherheit zu erhöhen. Bspw. gehen Bildschirmschoner und Internetverbindungen (speziell Sessions) in Timeouts und benötigen danach eine Reaktivierung oder eine erneute Anmeldung.

TIME STAMP (engl.)
Übsg. Datumsstempel. Das Hinzufügen des aktuellen Datums und der aktuellen Zeit in eine Log-Datei für eine soeben ausgeführte Aktivität oder für einen neuen Eintrag in einer Datenbank.

TIME TO LIVE [TTL] (engl.)
Maximale Anzahl von Server- oder Router-Hops, die ein Datenpaket vom Startsystem zum Zielsystem durchführen darf, bevor es verworfen wird, bspw. TTL = 128.

TLA
Abk. für Three Letter Acronym. Negativ behafteter Ausdruck für die Tendenz, viele Fachbegriffe nur als Abkürzung mit drei Buchstaben zu verwenden, sodass nur Fachpersonen wissen, wovon die Rede ist.

TLD
Abk. für Top-Level-Domain

TLS
Abk. für Transport Layer Security

TLS HANDSHAKE (engl.)
Startaktion einer TLS-verschlüsselten Kommunikation. Dabei wird eine sichere Authentifikation und Identifikation basierend auf asymm. Kryptografie durchgeführt, bei dem sich der Server gegenüber dem Client authentisiert, bei einigen Anwendungsfällen auch umgekehrt. Danach einigen sich Client und Server auf einen einmaligen Session Key, der fortan für die symm. Ver- und Entschlüsselung der Daten verwendet wird.

TLS INTERCEPTION (engl.)
Übsg. TLS-Abfangen. Methode, um eine TLS-Kommunikation zu unterbrechen, die Daten zu entschlüsseln und zu analysieren, die Daten wieder zu verschlüsseln und weiter an das Zielsystem zu schicken. Dies geschieht bspw. bei einer Kommunikation, welche über einen Proxy aufgebaut wird. TLS Interception ist ein bewährtes Verfahren, um die Kommunikation auf Schadsoftware zu prüfen. Da Daten dabei jedoch zeitweise unverschlüsselt vorliegen, stellt dies ein Risiko dar.

TLS PROTOCOL (engl.)
Übsg. TLS-Protokoll. Siehe TLS.

TOGAF
Abk. für The Open Group Architecture Framework. Methode zur einheitlichen Durchführung der Phasen Entwurf, Planung, Implementierung und Wartung für Systemarchitekturen.

TO ISSUE CERTIFICATE (engl.)
Syn. zu Certification Issuing

TOKEN
Ein Objekt, das eine Person besitzt und kontrolliert, bspw. ein kryptografisches Gerät wie Smartcard oder ein Passwort. Ein Token kann die Identität der Person bestätigen.

TOKENISIERUNG
Aufteilung eines Objekts in kleinere Teile. Beispiel: Aufsplittung eines Texts in Wörter.

TOKENIZATION
Übsg. Tokenisierung

TOKEN-PROTECTED KEYS (engl.)
Übsg. Sicherheitsmerkmalgeschützte Schlüssel. Einer von drei Arten der Autorisation für den Gebrauch von Schlüsseln in HSMs. Bei Token-Protected Keys wird für den Gebrauch der Schlüssel ein Token, bspw. spezielle Smartcards, und eine Passphrase benötigt. Die anderen zwei Arten sind: Softcard-Protected Keys und Module-Protected Keys.

TOLLGATE (engl.)
Übsg. Entscheidungspunkte

TOMCAT
Abk. für Apache Tomcat Webserver. Ein weitverbreiteter Open-Source-Webserver, der Java-Web-Anwendungen ausführen kann.

TOP-LEVEL-DOMAIN [TLD] (engl.)
Höchster Level bei der hierarchischen Struktur von Domainnamen im Internet. Beispiele: „.com“, „.ch“, „.de“, „.org“. Jede Domain, bspw. info.domain.com, ist verlinkt mit ihrer Top-Level-Domain, hier „.com“. Jedem Domainnamen und auch jedem TLD entspricht dabei eine IP-Adresse. Die Zugehörigkeit zwischen Namen und IP-Adresse wird in Listen geführt und von DNS weltweit verbreitet.

TOR BROWSER
Webbrowser, der die eigene IP-Adresse verschleiert durch Adressierung eines Proxy-Servers, der über weitere Proxy-Server im Tor-Netzwerk die angefragte Internetseite aufruft.

TPD
Abk. für Trusted Publishing Domain. Diese wird u. a. bei Microsofts ADRMS benutzt.

TPM
Abk. für Trusted Platform Module

TRACKING (engl.)
Übsg. Verfolgung. Methoden, Software und Hardware zur Verfolgung von Objekten und Personen. Bspw. werden Klicks auf Links und Like-Buttons verfolgt, um gezielte Werbung anzuzeigen.

TRANSAKTIONSNUMMER [TAN]
Einmal-Kennwort meist aus 4 bis 6 Ziffern für Online-Banking. Benutzer erhalten TANs entweder als Listen auf Papier, einzeln als SMS oder in einer App auf dem Handy.

TRANSMISSION CONTROL PROTOCOL [TCP] (engl.)
Übsg. Übertragungssteuerungsprotokoll. Definition und Implementierung von vollduplexer Netzwerkkommunikation zwischen zwei Endpunkten einer Netzverbindung. TCP wird häufig mit dem Internetprotokoll (IP) kombiniert und als TCP/IP bezeichnet. Eine TCP-Verbindung baut immer auf vier Angaben auf: Netzwerkadresse und Port des ersten PCs sowie Netzwerkadresse und Port des zweiten PCs.

TRANSMITTAL OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Übertragung eines kryptografischen Schlüssels.

TRANSPORT
Übertragung von Daten zwischen Geräten.

TRANSPORT ENCRYPTION (engl.)
Syn. zu Protection on Transit

TRANSPORT LAYER SECURITY [TLS] (engl.)
Übsg. Transportschichtsicherheit. Sammlung von Internetprotokollen, welche durch Verschlüsselung den Schutz der Vertraulichkeit und Integrität von übermittelten Daten durch unsichere Netzwerke ermöglichen. Wird bei HTTPS-Verbindungen benutzt sowie bei FTPS, IMAPS, POP3S u. A. Gestartet wird eine TLS-Verbindung durch einen Handshake basierend auf asymm. Kryptografie, bei dem sich der Server gegenüber dem Client authentisiert, bei einigen Anwendungsfällen auch umgekehrt. Danach einigen sich Client und Server auf einen einmaligen Session Key, der fortan für die symm. Ver- und Entschlüsselung der Daten verwendet wird. TLS ersetzte Secure Sockets Layer (SSL). SSL1.0 wurde in den 1990er-Jahren von Netscape entwickelt und bis SSL3.0 weiterentwickelt. Ab Version SSL3.1 (1999) wird es als TLS1.0 bezeichnet (siehe Tab. 22.1).

Die exemplarische Verwendung von SSL/TLS wird im ausführlichen Spezialthema „Der Aufruf einer HTTPS-Internetseite“ im Kap. 29 erklärt.

TRANSPORT OF INFORMATION (engl.)
Übsg. Übermittlung von Information.

TRANSPORT VON INFORMATION
Übertragung von Daten zwischen zwei oder mehreren Parteien. Abschnitt im Lebenszyklus von Informationen.

Tab. 22.1 SSL/TLS-Versionen

Version	Akzeptiert von – bis	Kommentar
SSL1.0	1994–1995	Erste Version, die nur kurz verwendet wurde
SSL2.0	1995–2011	Hat bekannte Protokollschwächen, wie z. B. Gebrauch von unsicheren MD5-Hashes, und bietet Angriffsziele für Man-in-the-Middle-Attacken. Wird deshalb nicht mehr als sicher angesehen
SSL3.0	1996–2015	Ist angreifbar für Poodle und andere Attacken. Wird deshalb nicht mehr als sicher angesehen
SSL3.1 TLS1.0	1999–	Ist angreifbar für Beast und andere Attacken, wird aber z. T. noch als akzeptierbar angesehen und verwendet
TLS1.1	2006–	Ist angreifbar für Lucky13 und andere Attacken, wird aber noch als akzeptierbar angesehen und verwendet
TLS1.2	2008–	Gilt aktuell als sicher
TLS1.3	2018–	Neueste Version

TRAPDOOR FUNCTIONS (engl.)
Übsg. Falltür-Funktionen, Einweg-Funktionen.

TRESOR
Syn. zu Anmeldedatenspeicher

TRICKBOT
Schadsoftware. Beinhaltet das Modul pwgrab, welches wahrscheinlich Login und Passwörter aus Internet Explorer, Firefox, Chrome, Edge, Outlook, Filezilla und WinSCP stiehlt.

TRIPLE-DES
Syn. zu 3DES

TROJANER
Scheinbar nützliches Programm oder interessante Datei, die jedoch Schadsoftware beinhaltet, welche sich via E-Mail oder Download im PC einnistet und selbstständig Funktionen ausführt und sich weiterverbreitet. Bspw. kann ein Trojaner Geld von E-Banking-Konten der Opfer umleiten.

TROJANISCHES PFERD
Syn. zu Trojaner

TRUST (engl.)
Übsg. Vertrauen

TRUSTED PLATFORM MODULE [TPM] (engl.)
Übsg. Vertrauenswürdiges Plattformmodul. Chip in PCs, Handys und anderen Geräten, welcher Sicherheitsfunktionen anbietet.

TRUSTED PUBLISHING DOMAIN [TPD] (engl.)
Übsg. Vertrauenswürdige Lizenz zur Veröffentlichung. Bei Microsoft ADRMS eingetragene Domäne zur Verifizierung der Publishing License (PL) von zuvor publiziertem verschlüsseltem Inhalt.

TRUSTED USER DOMAIN [TUD] (engl.)
Übsg. Vertrauenswürdige Benutzerdomäne.

TRUST RELATIONSHIP (engl.)
Übsg. Vertrauensbeziehung

TTL
Abk. für Time to Live

TUD
Abk. für Trusted User Domain

TUNNELING (engl.)
Übertragung einer Datenkommunikation über spezielle Verbindungen. Bspw. können unverschlüsselte Applikationsdaten über definierte Ports umgeleitet werden, sodass diese Daten durch IPSec in verschlüsselte Pakete eingebettet und versendet werden können.

TWITTER
Sofortnachrichtendienst

TWO DISTINCT AUTHENTICATION FACTORS (engl.)
Übsg. Zwei unterscheidbare Authentisierungsfaktoren. Syn. zu 2FA.

TWO FACTOR AUTHENTICATION [2FA] (engl.)
Übsg. Zwei-Faktor-Authentisierung

U

23

U2
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „You too“, Übsg. „Du auch“.

U2F
Abk. für Universal Second Factor

UAC
Abk. für User Account Control

ÜBERNAHME DER IDENTITÄT
Syn. zu Identitätsverlust. Missbrauch einer elektronischen Identität einer anderen Person. Dies kann bspw. geschehen, wenn Benutzername und Passwort gestohlen und missbräuchlich verwendet werden. 2FA bietet hierbei Schutz durch die zusätzliche Sicherheitshürde.

ÜBERSCHWEMMEN
Senden vieler Anfragen an ein Gerät, um dieses durch Überlastung außer Gefecht zu setzen oder in einen Zustand zu bringen, in dem Sicherheitsmaßnahmen nicht mehr ausgeführt werden können.

ÜBERTRAGUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Transport eines Schlüssels von einem System zu einem anderen. Abschnitt im Lebenszyklus kryptografischer Schlüssel. Siehe zusätzliche Details beim Begriff Schlüssel.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_23

ÜBERWACHEN VON CYBER-BEDROHUNGEN
Phase bei der Behandlung von Cyber-Bedrohungen.

UCE
Abk. für Unsolicited Commercial E-Mail

UDP
Abk. für User Datagram Protocol

UEFI
Abk. für Unified Extensible Firmware Interface

UEM
Abk. für User Environment Management. Software, mit welcher Regeln und Einstellungsdaten für und von den Benutzern zentral gespeichert und verwaltet werden können, unabhängig vom Betriebssystem und von Apps.

UG
Abk. für Universal Group

UL
Abk. für User License

UNAUTHORIZED ACCESS (engl.)
Übsg. Unberechtigter Zugang

UNAUTHORIZED DISCLOSURE OF INFORMATION (engl.)
Übsg. Unberechtigte Offenlegung von Information

UNAUTHORIZED INTRUSION (engl.)
Übsg. Unerlaubter Eingriff

UNAUTHORIZED RECIPIENTS (engl.)
Übsg. Unberechtigter Empfänger. 1) Empfänger von Nachrichten oder E-Mails, die technisch keine Berechtigung erhalten, den Inhalt zu öffnen. Dies kann bspw. mittels Verschlüsselung geschehen. 2) Empfänger von Nachrichten oder E-Mails, die keine Empfänger sein dürften, jedoch die Nachricht oder E-Mail aus Versehen oder mit Absicht erhielten.

UNBERECHTIGTER ZUGANG
1) Eintreten einer Person in einen physischen oder digitalen Bereich, für den diese Person keine Berechtigung hat. 2) Aufbau einer Verbindung zu einem System oder Teil eines Systems, für die keine Berechtigung gegeben wurde.

UNC
Abk. für Universal Naming Convention, Übsg. Universelle Namensvergabe. Eine UNC-Adresse ist ein Netzwerkpfad, über den man Verzeichnisse und Laufwerke anderer Systeme im Netzwerk nutzen kann.

Struktur einer UNC-Adresse:

- Windows: \\Servername\Freigabename\Pfad
- MacOS, Unix: //Servername/Freigabename/Pfad

(Servername kann auch IP-Adresse sein)

UNENCRYPTED (engl.)
Übsg. Unverschlüsselt. Daten, die weder jetzt verschlüsselt sind noch in der Vergangenheit verschlüsselt waren. Bei Daten, welche bereits verschlüsselt waren, wird der unverschlüsselte Zustand „decrypted“ genannt.

UNERWÜNSCHTE WERBE-E-MAIL
Syn. zu Spam, Unsolicited Commercial E-Mail (UCE).

UNICAST
Kommunikation, die von einem Sender zu einem Empfänger erfolgt, im Gegensatz zu Multicast und Broadcast, siehe Tab. 23.1.

Tab. 23.1 Beispiele für Unicast, Broadcast, Multicast

Beispiel für Unicast	FTP-Verbindung zwischen zwei Computern
Beispiel für Broadcast	Fernsehsendung eines öffentlich-rechtlichen Fernsehsenders
Beispiel für Multicast	Fernsehsendung eines Bezahlsenders

UNICODE
Definition von Zahlenwerten für internationale Buchstaben, Schriftzeichen, Bildschriftzeichen und Emojis. Neue Codes werden laufend ergänzt mit dem Ziel, Unicode weltweit benutzen zu können. Bis 2019 wurden bereits ca. 140.000 Zeichen aufgenommen.

UNIFIED EXTENSIBLE FIRMWARE INTERFACE [UEFI] (engl.)
Übsg. Vereinheitlichte, erweiterbare Firmware-Schnittstelle. Verbindung zw. der Firmware, Hardware und dem Betriebssystem. Ersetzt das veraltete BIOS und bietet u. a. eine Möglichkeit, nur signierte Bootloader zu erlauben, sog. „Secure Boot".

UNIFORM RESOURCE IDENTIFIER [URI] (engl.)
Eindeutige Bezeichnung für Ressourcen im Internet, wie Daten, Computer u. Ä. URIs werden unterteilt in URLs und URNs, wobei eine URL die „Location" (Übsg. Ort) einer Ressource oder die Zugriffsart auf diesen Ort bezeichnet, und URN den „Namen" der Ressource darstellt.

Aufbau einer URI:
Protokoll „:" Instanz „/" Pfad „?" Abfrage „#" Fragment
(Nicht alle Teile müssen vorkommen, und Teile können auch mehrfach vorkommen)

Beispiele für URI:

http://name@example.com:8080/some/where/script.php?action=submit&param1=wert1#teil_1
ftp://example.com/seite.txt
news://example.com/heute.pdf
mailto:Hans.Muster@example.com
file:///C:/temp/datei.txt
urn:isbn:1-2345-6789-0

UNIFORM RESOURCE LOCATION [URL] (engl.)
Syn. zu Internetadresse. Einer der zwei URI-Typen, welcher den Ort („Location") der Ressource (Daten, Computer etc.) oder die Zugriffsart auf diesen Ort darstellt. Häufig werden URL und URI ungenau als Synonyme verwendet.

Beispiel für URL: http://example.com/seite.html

UNIFORM RESOURCE NAME [URN] (engl.)
Einer der zwei URI-Typen, welcher einer Ressource (Daten, Computer etc.) einen eindeutigen Namen zuweist. URNs können mit URLs kombiniert werden, um zusätzlich zu beschreiben, wo sich die Ressource befindet. Ohne zugehöriger URL können URNs somit nicht in einem Internetbrowser direkt angeklickt und geöffnet werden.

Beispiel für URN: urn:isbn:1-2345-6789-0

UNIVERSAL GROUP [UG] (engl.)
Typ von Security Groups in Microsoft Active Directory. UGs können Benutzer und andere Gruppen von jeder Domain oder Forest beinhalten. Dabei wird kein Vertrauen („Trust“) zw. diesen Domains und Forest vorausgesetzt.

UNIVERSAL PLUG AND PLAY [UPNP] (engl.)
Netzwerkprotokoll, welches es Geräten erlaubt, einander automatisch zu erkennen, um untereinander zu kommunizieren.

UNIVERSAL SECOND FACTOR [U2F] (engl.)
Initiative zur allg. Verwendung von Zwei-Faktor-Authentisierung, ähnlich wie UATH. Für U2F wird die Spezifikation durch das FIDO-Gremium festgelegt.

UNPUBLISHED PUBLIC INFORMATION [UPI] (engl.)
Übsg. Nicht publizierte, öffentliche Information.

UNSOLICITED COMMERCIAL E-MAIL [UCE]
Syn. zu Spam, unerwünschte Werbe-E-Mail.

UNSTRUCTURED DATA (engl.)
Übsg. Unstrukturierte Daten

UNSTRUKTURIERTE DATEN
Digital vorliegende Informationen, die keine oder nur eine eingeschränkte innere Struktur aufweisen. Bspw. E-Mail-Inhalte, gescannte Dokumente, Audioaufnahmen, geschriebene Dokumente, Fotos. Die maschinelle Analyse dieser Daten kann nur mit viel Aufwand geschehen, im Gegenteil zu strukturierten Daten, wie bspw. in Datenbanken.

UNSUPERVISED LEARNING (engl.)
Übsg. Unüberwachtes Lernen. Methode der künstlichen Intelligenz. Hierbei wird ein Modell ohne eine klare Struktur der Daten trainiert und ohne klar definierte, erwartete Resultate. Das Modell lässt sich demnach „nicht überwachen“. Das Ziel ist meist eine Analyse der Daten oder das Finden von Besonderheiten und Häufigkeiten in den Daten. Unsupervised Learning ist eine von drei grundlegenden Lernmethoden des maschinellen Lernens, neben Reinforcement und Supervised Learning.

Beispiel für Unsupervised Learning

Von einem vollen Obstkorb sollen jeweils gleiche Früchte in kleinere Körbe verteilt werden. Das System muss nun also Gemeinsamkeiten wie Farbe, Größe und Form selbstständig entdecken und zur Klassifizierung benutzen.

UNVERSCHLÜSSELTE INFORMATION
Syn. zu Klartext. Jede nicht verschlüsselte Information, unabhängig davon, ob sie jemals verschlüsselt war.

UPDATE MANAGEMENT (engl.)
Übsg. Verwaltung und Installation von Sicherheitsaktualisierungen.

UPDATES (engl.)
Übsg. Software-Aktualisierungen

UPGRADES (engl.)
Übsg. Hardware- oder große Software-Aktualisierungen.

UPI
Abk. für Unpublished Public Information

UPLOAD (engl.)
Übsg. Hochladen

UPLOAD FILTER (engl.)
Software auf Servern, die einschränkt, welche Daten hochgeladen werden dürfen. Die Gründe für solche Filter sind Copyright-Limitationen, Größenlimitationen, Dateiformatlimitationen usw.

UPN
Abk. für User Principle Name

UPNP
Abk. für Universal Plug and Play

UR2L8
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „You are too late“, Übsg. „Du bist zu spät“.

URANDOM
Funktion in Linux und Max OS X zur Generierung von Zufallszahlen. Genauer Ort: /dev/urandom

URI
Abk. für Uniform Resource Identifier

URL
Abk. für Uniform Resource Location

URL-SHORTENER (engl.)
Übsg. Funktion zur Erzeugung von kurzen URLs. Dies kann vorteilhaft sein, damit Benutzer sich diese besser merken können und sich seltener vertippen beim Eintippen der URL. Auch können die Aufrufe dieser Kurz-URL beim Anbieter dieser Funktion registriert werden, um ein Klicktracking zu ermöglichen.

URN
Abk. für Uniform Resource Name

URSNIF
Schadsoftware in Form eines Trojaners, welcher sich meist durch Hacker-Tools, E-Mail-Anhänge und verseuchte Links im System einnistet.

USB-C
24-pin USB-Steckertyp.

USB SHIELD
Kleines USB-Gerät, welches zwischen USB-Kabel und USB-Anschluss angeschlossen wird, um zu verhindern, dass Daten gestohlen oder Viren übertragen werden, wenn ein USB-Gerät über dieses Kabel zum Aufladen angeschlossen wird.

USB-TOKEN
Sicherheitsschlüssel in Form eines USB-Sticks, der in ein USB-Anschluss gesteckt und durch den physischen Besitz als Authentisierungsfaktor dienen kann.

USE LICENSE [UL] (engl.)
Innerhalb einer Microsoft-Rights-Management-Installation erhalten Benutzer, falls sie berechtigt sind, vom RMS-Server eine Use License für das Öffnen eines verschlüsselten Dokuments oder einer E-Mail. Innerhalb der Use License ist festgelegt, welche Funktionen der Benutzer des entschlüsselten Dokuments anwenden darf, wie bspw. Drucken, Weiterleiten, Editieren. Solche Rechteeinschränkungen wurden durch den Dokumentenersteller bei der Speicherung des Dokuments oder der E-Mail festgelegt und zusammen mit dem Inhalt mitverschlüsselt. Sie werden durch die RMS-fähigen Applikationen, in denen das Dokument geöffnet wird, durchgesetzt.

USE OF A CRYPTOGRAPHIC KEY (engl.)
Übsg. Benutzung eines kryptografischen Schlüssels.

USER ACCESS PERIMETER (engl.)
Übsg. Benutzerzugangsbereich

USER ACCOUNT CONTROL [AUC] (engl.)
Übsg. Benutzerkontokontrolle. Windows-Sicherheitsmaßnahme seit Windows Vista, die ermöglicht, dass PC-Benutzer mit eingeschränkten Benutzerrechten arbeiten, auch wenn sie als Administrator angemeldet sind.

USER AUTHENTICATION CERTIFICATE (engl.)
Übsg. Zertifikat zur Authentisierung eines Benutzers gegenüber einem System, einer Software oder einem Netzwerk. Dies kann bspw. ein X.509-Zertifikat sein, in welchem der öffentliche Schlüssel des Benutzers enthalten ist und welches durch eine Zertifizierungsstelle signiert ist.

USER CERTIFICATE (engl.)
Übsg. Benutzerzertifikat. Zertifikat zur Authentisierung eines Benutzers gegenüber einem System zur Verschlüsselung von Daten und zum Signieren von E-Mails. Dies kann bspw. ein X.509-Zertifikat sein, in welchem der öffentliche Schlüssel des Benutzers enthalten ist und welches durch eine Zertifizierungsstelle signiert wurde.

USER DATAGRAM PROTOCOL [UDP] (engl.)
Übsg. Benutzer-Datagramm-Protokoll. Einfaches Netzwerkprotokoll zum Versand von Datagrammen durch Apps in IP-basierten Rechnernetzen. Das Protokoll garantiert nicht, dass die versendeten Pakete richtig und unverfälscht ankommen.

USER EXPERIENCE [UX] (engl.)
Übsg. Benutzererlebnis. Ziel der Software-Entwicklung ist u. a. eine gute User Experience, d. h. eine möglichst optimierte, intuitive Interaktion der Software mit dem Benutzer.

USERNAME (engl.)
Übsg. Benutzername

USERNAME UND PASSWORT
Häufigster und seit Jahrzehnten benutzter Berechtigungsnachweis von Personen, um sich an einem Programm, einem PC oder einem Netzwerk anzumelden und Zugang zu erhalten. Damit bei einem Diebstahl des Passworts nicht auch die Daten im Programm, im PC oder im Netzwerk in Gefahr zu bringen, wird empfohlen, wo möglich, zusätzlich 2FA zu verwenden.

USER PRINCIPAL NAME [UPN] (engl.)
Übsg. Benutzer-Prinzipal-Name. Aliasname für den Benutzer innerhalb des Active Directory Accounts.

UTC
Abk. für Coordinated Universal Time. Übsg. Koordinierte Weltzeit. Zeitstandard für die Berechnung von Ortszeiten in Zeitzonen weltweit.

UTF-8
Abk. für 8-Bit Universal Coded Character Set Transformation Format. Codierung für Unicode-Zeichen. Die ersten 128 Zeichen entsprechen den ASCII-Zeichen, alle anderen (mehrere Hunderttausend) möglichen Zeichen beinhalten u. a. sprachenspezifische Zeichen.

UUID
Abk. für Universally Unique Identifier. Nummer zur eindeutigen Identifikation eines Objekts. Besteht aus fünf Gruppen mit je 16-Byte-Zahlen in hexadezimaler Form. Die von Microsoft in vielen Bereichen eingesetzte GUID ist ein Beispiel einer UUID.

UX (engl.)
Abk. für User Experience

UX MONITORING (engl.)
Abk. für User Experience Monitoring. Übsg. Überwachung der Benutzererfahrung. Methoden zur Überwachung und Analyse der Interaktion von Personen mit Programmen oder Systemen. Ziel ist die Optimierung der Bedienbarkeit.

VALIDIERUNG KRYPTOGRAFISCHER BIBLIOTHEKEN
Zur Sicherstellung der Korrektheit kryptografischer Bibliotheken werden diese gegen allg. akzeptierte Standards geprüft, wie bspw. FIPS 140-2 Level 1.

VDI
Abk. für Virtual Desktop Infrastructure

VERÄNDERUNGSMANAGEMENT
Syn. zu Change Management. Methoden, Prozesse und Organisation, um Änderungen an IT-Systemen und IT-Infrastruktur kontrolliert, effizient und mit minimalem Risiko umzusetzen.

VERERBUNG
Funktion innerhalb von Applikationen und Datenbanken zur Erstellung von Kopien einzelner oder aller Eigenschaften eines Datensatzes.

VERFÜGBARKEIT
Zustand von Netzwerken und Systemen, die nicht manipuliert sind und wie erwartet arbeiten. Dies ist eines der Ziele der IT-Sicherheit, welche sich grundsätzlich mit der Aufrechterhaltung der Integrität, der Vertraulichkeit und der Verfügbarkeit von Daten und Systeme beschäftigt. Oft wird dies abgekürzt mit CIA für Confidentiality, Integrity and Availability.

VERGLEICH EXAKTER DATEN
DLP-Methode, die es ermöglicht, sensible Daten in E-Mails zu erkennen, bevor diese aus der Firma gelangen. Diese Art der Datenüberwachung wird gewählt, wenn die Daten

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_24

unterschiedlich sind und keinem Muster folgen. Dabei werden die sensiblen Daten direkt oder als Hash-Wert verwendet. Beispiel: Kundendaten.

VERGLEICH VON MUSTERN
DLP-Methode, die es ermöglicht, sensible Daten in E-Mails zu erkennen, bevor diese aus der Firma gelangen. Obwohl die Daten unterschiedlich sind, lassen sich diese aufgrund der strukturierten Datenmuster erkennen. Beispiel: Kreditkartennummern.

VERNICHTUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Vorgang am Ende der Lebensdauer eines Schlüssels oder nach Bekanntwerden eines Missbrauchs dieses Schlüssels. Abschnitt im Lebenszyklus kryptografischer Schlüssel (siehe zusätzliche Details beim Begriff Schlüssel).

VERNICHTUNG VON INFORMATION
Abschnitt im Lebenszyklus von Informationen.

VERSCHLÜSSELTE KOMMUNIKATION
Datenübermittlung zw. zwei Parteien, bei welcher die Daten vor der Übermittlung mit einem Verschlüsselungsalgorithmus umgewandelt werden. Dadurch kann verhindert werden, dass der Inhalt der Daten während der Kommunikation erkannt werden kann, auch wenn die übermittelten Daten mitgehört werden. Am Zielsystem werden die verschlüsselten Daten empfangen und mit dem benötigten geheimen Schlüssel entschlüsselt und verwendet.

Beispiel für verschlüsselte Kommunikation: Übertragung einer HTTPS-Internetseite.

VERSCHLÜSSELUNG
Algorithmus zur Umwandlung eines Textes (sog. „Klartext“) in einen Geheimtext mithilfe eines Geheimnisses (sog. „Schlüssel“), damit nur bestimmte Personen oder Systeme diesen Geheimtext in den Klartext zurückwandeln können. Bei einer symm. Verschlüsselung wird das gleiche Geheimnis zur Ver- und Entschlüsselung benutzt und muss vorher den beteiligten Parteien bekannt sein. Bei der asymm. Verschlüsselung wird der Text mit einem öffentlichen Schlüssel verschlüsselt und mit einem privaten, geheimen Schlüssel entschlüsselt. Dabei sind der öffentliche und private Schlüssel mathematisch verknüpft.

Beispiel einer Cäsar-3-Verschlüsselung

Der Klartext „TEXT“ wird zum Geheimtext „WHAW“.

VERSCHLÜSSELUNGSALGORITHMUS
Berechnungsmethode zur Verschlüsselung von Daten. Einfache Algorithmen können auf Papier ausgerechnet werden, kompliziertere werden in Software oder Hardware

implementiert. Da Verfahren und Computerleistung zum Brechen eines Verschlüsselungsalgorithmus laufend besser werden, werden auch die Verschlüsselungsalgorithmen ständig verbessert und ersetzt.

Beispiele für Verschlüsselungsalgorithmen: AES, 3DES, Blowfish, CAST, Arcfour, Vigenère, Cäsar.

VERSCHLÜSSELUNGSDATEISYSTEM
Dateisystem bei Unix-ähnlichen Betriebssystemen, bei welchem die Dateien automatisch ver- und entschlüsselt werden. Syn. zu Cryptografik File System, Crypto File System.

VERSCHRÄNKTE QUANTEN
Syn. zu Quantum Entanglement. Mögliche Eigenschaft von Quanten oder Gruppen von Quanten, bspw. Lichtteilchen, Elektronenspins usw., bei welcher zwei solcher Partikel quantenphysikalisch gekoppelt sind und damit eine Änderung an einem Partikel auch eine Änderung am anderen Partikel erzeugt, und dies auch bei großer Distanz. Hierbei können Informationen jedoch nicht mit Überlichtgeschwindigkeit übertragen werden.

VERSEUCHTE INTERNETSEITEN
Internetseiten im „Deep and Dark Web“ und im normalen Internet, welche manipuliert wurden, sodass Besucher dieser Seite automatisch und unbewusst eine Schadsoftware herunterladen oder starten und damit ihren PC und ihre Daten beinträchtigen. Die Schadsoftware kann bspw. als JavaScript-Programm implementiert sein oder in verseuchten Werbebannern lauern.

VERSEUCHTE WERBEBANNER
Manipulierte Werbebanner können Schadsoftware auf den PC bringen oder automatisch starten. Dies ist eine Form von verseuchten Internetseiten.

VERTEILUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Abschnitt im Lebenszyklus kryptografischer Schlüssel. Siehe zusätzliche Details beim Begriff Schlüssel.

VERTICAL SCALING (engl.)
Übsg. Vertikales Skalieren. Syn. zu Scaling Up. Methoden, um die Gesamtleistung eines Systems zu erhöhen durch Austausch von Komponenten wie CPUs, Festplatten usw.

VERTRAUEN
Grundlage, auf welcher Cyber- und IT-Security basiert, da 100-Prozent-Sicherheit unbezahlbar ist und nicht erreicht werden kann. Vertrauen muss bestehen zwischen Businesspartner, zwischen Privatpersonen und zwischen Arbeitgeber und Arbeitnehmer, um Geschäfte zu tätigen, Verträge abzuschließen oder um miteinander zu kommunizieren.

VERTRAUENSBEZIEHUNG
Durch Authentisierung hergestelltes Vertrauen zwischen zwei Systemen, bspw. zw. zwei Sicherheitsdomänen.

VERTRAUENSKETTE
Eindeutig nachvollziehbare und überprüfbare Kette von Public-Key-Zertifikaten, angefangen beim Root-Zertifikat einer offiziellen Beglaubigungsstelle über Zertifikate von Zwischenzertifizierungsstellen bis hin zum Benutzerzertifikat.

VERTRAUENSWÜRDIGE BENUTZERDOMÄNE
Syn. zu Trusted User Domain. Methode, um RMS-verschlüsselte Informationen zwischen zwei Forests zu teilen, wenn bei beiden Forests ADRMS-Cluster vorhanden sind. Dadurch können Benutzer von beiden ADRMS-Installationen die ADRMS Use License erhalten, um verschlüsselte Dateien öffnen zu können.

VERTRAUENSWÜRDIGES KRYPTOGRAFISCHES VERFAHREN
Für symmetrische Schlüssel wird bei einem anerkannten, vertrauenswürdigen kryptografischen Verfahren verlangt, dass darauf kein Angriff möglich ist, der schneller zum Ziel führt als die „Brute-Force"-Methode, d. h. das reine Durchtesten aller Schlüssel.

VERTRAULICHE DATEN
Daten wie Fotos, Videos, Kundenadressen usw., die Privatpersonen oder Firmen wichtig sind, und deswegen geschützt werden müssen.

VERTRAULICHKEIT
1) Gewährleistung, dass Daten vom richtigen Absender kommen. 2) Definition der Wichtigkeit der Daten und wer diese sehen darf. 3) Eines der Ziele der IT-Sicherheit, welche sich grundsätzlich mit der Aufrechterhaltung der Integrität, der Vertraulichkeit und der Verfügbarkeit von Daten und Systeme beschäftigt. Oft abgekürzt mit CIA für Confidentiality, Integrity and Availability.

VERWUNDBARKEIT VON SYSTEMEN
Jedes System bietet unbekannte oder bekannte Angriffsmöglichkeiten, bspw. aufgrund veralteter Software oder durch Fehlmanipulationen. Deswegen muss darauf geachtet werden, dass Geräte, welche online oder physisch zugänglich sind, geschützt werden, falls das System oder die darin enthaltenen Daten wichtig sind.

VICTIM OF CYBER-RELATED FRAUD (engl.)
Übsg. Opfer von Cyber-Betrug.

VIGENÈRE-VERSCHLÜSSELUNG
Kryptografieverfahren, das auf der Cäsar-Verschlüsselung basiert, wobei jedoch die Buchstaben nicht um jeweils den gleichen Wert im Alphabet zyklisch verschoben werden. Für die Vigenère-Verschlüsselung wird ein Codewort („Schlüssel“) benutzt. Damit wird für jede Buchstabenposition der Nachricht eine Verschiebung um die Schlüsselbuchstabenposition durchgeführt. Eine Attacke dieses Verfahrens kann bei langen Codeworten zwar aufwendig sein, aber das Verfahren gilt heute nicht mehr als sicher, da dieses mittels Brute Force geknackt werden kann. Das Hauptproblem dabei ist die periodische Wiederverwendung des Codeworts bei längeren Texten.

Beispiel einer Vigenère-Verschlüsselung

Der Klartext „TEXT“ wird mit Codewort „SAFE“ zum Geheimtext „LECX“.

VIRTUALBOX
Virtual Machine (VM)-Software von Oracle.

VIRTUAL CREDIT CARD (engl.)
Übsg. Virtuelle Kreditkarte. Von einigen Kreditkarteninstituten oder Banken offeriertes Produkt. Die virtuellen Kreditkarten sind mit dem gleichen Konto verbunden wie die eigenen physischen Kreditkarten, besitzen jedoch eine zufällig generierte Kartennummer, ein Ablaufdatum und einen Sicherheitscode. Diese virtuellen Kreditkarten können für Käufe im Internet benutzt werden und verfallen nach einer Anwendung. Dies schützt vor Kreditkartenmissbrauch.

VIRTUAL DESKTOP INFRASTRUCTURE [VDI] (engl.)
Virtualisierung kompletter PC-Systeme auf Servern im Rechenzentrum. Ein Server kann dabei mehrere VDIs gleichzeitig betreiben und sowohl den Speicher als auch die zugewiesenen Prozessoren dynamisch dem Bedarf anpassen. Benutzer arbeiten an leistungsschwachen Geräten („Thin Client“), die ein Abbild der leistungsstarken VDIs darstellen und nur die Benutzereingaben übertragen. Die Vorteile sind reduzierte Hardwarekosten sowie einfaches Patch-Management.

VIRTUALISIERUNGSSOFTWARE
Programme, um virtuelle Computer auf physischem Computer zu ermöglichen. Damit lässt sich bspw. MacOS auf Windows PCs betreiben oder es lassen sich alte Systeme wie AMIGA, C64 etc. auf modernen PCs wiederbeleben. Großer Vorteil ist, dass diese virtuellen Systeme neben der Software, um sie zu betreiben, nur aus einer Datei bestehen und somit schnell vervielfältigt oder gesichert werden können.

VIRTUAL KEY MANAGEMENT (engl.)
Übsg. Virtuelle Schlüsselverwaltung. Methoden, um eine virtuelle Zentralisierung der kryptografischen Verfahren und der Schlüsselverwaltung in einer ausgelagerten Cloud-Infrastruktur zu ermöglichen.

VIRTUAL LAN [VLAN] (engl.)
Abk. für Virtual Local Area Network. Segment (aba. logisches Teilnetz) innerhalb eines physischen Netzwerks.

VIRTUAL MACHINE [VM] (engl.)
Übsg. Virtuelle Maschine. Virtueller Computer, welcher in einem physischen Computer ausgeführt wird. Dieser benutzt die Hardware und Virtualisierungsfunktionen des Prozessors des physischen Computers, im Gegensatz zu Emulationen, die rein auf Software basieren.

VIRTUAL PRIVATE NETWORK [VPN] (engl.)
Übsg. Virtuelles privates Netzwerk. Direkte, geschützte Netzwerkverbindung zweier Computer über das Internet.

VIRUS
1) Computerprogramm, welches sich in den Speicher, in den Startbereich des Systems oder in andere Software einnistet und dadurch erreicht, dass es immer wieder gestartet und kopiert wird und sich damit weiter ausbreitet. 2) Ugs. für Schadsoftware.

VIRUSSCANNER
Syn. zu Anti-Viren-Scanner

VIRUSTOTAL
Online-Verzeichnis für Beispiele von Schadsoftware.

VISHING
Abk. für Voice Phishing, Übsg. Sprachphishing. Mithilfe eines verwirrenden Anrufs wird versucht, Passwörter zu „fischen“ oder auch Kreditkartendaten und andere sensible Daten.

VLAN
Abk. für Virtual LAN

VM
Abk. für Virtual Machine

VMWARE
Softwareunternehmen, welches Virtualisierungssoftware offeriert, bspw. VMware ESXi, VMware Workstation, VMware Fusion, VMware vSphere.

VOICE OTP ATTACK (engl.)
Übsg. Sprach-Einmal-Kennwort-Attacke. Hacker lassen das über Sprache mitgeteilte Einmal-Kennwort auf den Anrufbeantworter aufzeichnen, indem sie die Leitung des Opfers besetzen. Falls der Standard-PIN des Anrufbeantworters noch immer der vom Hersteller eingegebenen Standardnummer entspricht, kann der Angreifer nun dieses Einmal-Kennwort abhören und missbrauchen.

VOICE OVER IP [VOIP] (engl.)
Übsg. IP-Telefonie. Telefongespräche werden in digitale Datenpakete umgewandelt und über die Internetverbindung übermittelt. Beim Empfänger wandelt ein Adapter diese digitalen Daten in hörbare Sprache zurück.

VOIP
Abk. für Voice Over IP

VOLATILITY FOUNDATION (engl.)
Unabhängige Non-Profit-Organisation, welche Speicher-Analyse-Tools anbietet.

VOLLDUPLEX
Kommunikation, die in beide Richtungen gleichzeitig stattfindet. Bspw. bei heutigen Breitbandinternetanschlüssen, bei denen Daten gleichzeitig hochgeladen und heruntergeladen werden können. Siehe auch simplexe und halbduplexe Kommunikation.

VORFALLSANALYSE
Methoden zur Analyse eines Cyber- und IT-Sicherheitsvorfalls.

VORFALLSREAKTIONEN
Aktionen, die im Fall einer Cyber-Attacke unternommen werden. Jede Firma sollte sich ihre eigenen Vorfallreaktionen vor dem ersten Angriff überlegen und für alle Mitarbeiter zugänglich ablegen.

Bei den meisten Firmen beinhaltet dies u. a. folgende Aktionen:

a) Information an betroffene Kunden,
b) Information an das Führungsteam,
c) Information an andere Stakeholder und Shareholder,
d) Information evtl. an Regulatoren,
e) Analyse des Vorfalls zur Vermeidung zukünftiger Attacken vom gleichen Typ.

VPN
Abk. für Virtual Private Network

VT100, VT220, VT320
Computerterminal aus den 1970er- und 1980er-Jahren. Diese benutzten bereits ANSI-Escape-Sequenzen bspw. für die Cursorposition und -farben. Heutzutage ermöglichen viele Terminal-Emulationen die Verwendung der Befehlsätze vom VT100, VT220 usw.

VULNERABILITY (engl.)
Übsg. Sicherheitslücke, Verletzlichkeit. Schwachstelle eines IT-Systems, eines Netzwerks oder eines Programms.

VULNERABILITY OF SYSTEMS (engl.)
Übsg. Verwundbarkeit von Systemen

W

25

W3C
Abk. für World Wide Web Consortium

WAAS
Abk. für Windows as a Service. Microsoft liefert Windows10-Funktionsaktualisierungen als halbjährliche Updates aus, anstatt wie früher als vollständige, neue Betriebssysteme. Ein Updatezyklus beinhaltet Vorbereitungsphase, Rollout und Support.

WAF
Abk. für Web-Application-Firewall

WAN
Abk. für Wide Area Network

WANNACRY
Erster Vertreter eines neuen Schadsoftwaretyps in Form eines Erpressungstrojaners, der nicht nur die Daten auf dem infizierten, sondern auch auf anderen Windows-PCs im lokalen Netz verschlüsselt und erst nach Zahlung eines Betrags in Bitcoins wieder entschlüsselt, falls überhaupt. Bis zum Druck dieses Buches gibt es noch kein zuverlässiges Entschlüsselungsprogramm, und so bleibt bei wichtigen Daten bloß ein Backup einzuspielen, falls ein solches besteht. Es wird abgeraten, den Erpressungsbetrag zu zahlen und zu hoffen, dass der Entschlüsselungscode auch wirklich zugesendet wird, denn dies ist ungewiss und weitere solche Angriffe werden dadurch lukrativ. WannaCry basiert auf dem Exploit EternalBlue.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_25

WANNAMINE
Nachfolger von WannaCry, der keine Bitcoins erpresst, sondern Mining (Übsg. Schürfen) betreibt für die Kryptowährung Monero. WannaMine basiert auf dem Exploit EternalBlue.

WASSERFALL-MODELL
Lineare Projektvorgehensmethode, bei welcher in jeder Projektphase definierte Ziele und Tätigkeiten fertiggestellt werden, bevor die nächste Phase startet. Dies erlaubt die einfachere und bewährte Durchführung eines Projekts, bietet jedoch im Gegensatz zu agilen Projektmethoden weniger Änderungsmöglichkeiten nach dem Beginn der Entwicklungsphase des Projekts.

WATERFALL MODEL (engl.)
Übsg. Wasserfall-Modell

WATERING HOLE (engl.)
Übsg. Wasserloch. Präparierte populäre Websites, die wie die Originale aussehen, jedoch gefälschte und manipulierte Versionen sind, bei deren Besuch unbewusst Schadsoftware heruntergeladen wird.

WBT
Abk. für Web Based Training

WEAK AUTHENTICATION (engl.)
Übsg. Schwache Authentifikation. Benutzung von Passwort, PIN, Face-ID oder Fingerabdruck als alleiniger „Faktor“ zur Anmeldung an einem System oder Programm, in welchem wichtige Daten gespeichert sind, entspricht nicht mehr heutigem Standard und wird als schwache Authentifikation angesehen, da die Daten einfach gestohlen werden können. Wenn immer möglich, sollte auf 2FA gewechselt und Passwörter sollten komplex und lange gewählt werden.

WEB2.0
Unscharf definiertes Schlagwort in Nachrichten zur Verdeutlichung des Wandels vom Internet als Informationsquelle zum Internet, bei welchem eine große Anzahl von Personen gleichzeitig Inhalt generieren und zusammenarbeiten.

WEB-APP (engl.)
Übsg. Webanwendung. Software, die in einem Webbrowser ausgeführt wird und dabei Daten an einen Webserver schickt und von diesem erhält.

WEB-APPLICATION-FIREWALL [WAF] (engl.)
Software, welche bei Webservern und Proxys eingesetzt werden kann, um eingehende und ausgehende Daten zu analysieren und bei verdächtigen Inhalten zu blockieren.

WEBAUTHN
Web-API des World Wide Web Consortium (W3C) zur einfacheren und sicheren Authentisierung. Dies ermöglicht es Benutzern, ihr bevorzugtes Gerät, wie bspw. ein Android-Handy oder ein Windows-PC, zu verwenden, um sich ohne Passwort bei Internetkonten anzumelden, falls sie sich bereits bei ihrem Gerät erfolgreich angemeldet oder authentisiert haben. Die Anmeldung bei den Internetkonten basiert somit auf Login-Methoden wie biometrischer Erkennung oder einem Security Token. WebAuthn wird in Kombination mit CTAP in FIDO2 verwendet.

WEB BASED TRAINING [WBT] (engl.)
Übsg. Online-Training. Schulungsfilme und -übungen. Große Firmen gehen dazu über, ihre Mitarbeiter über WBTs zu schulen anstatt in teure Kurse zu schicken.

WEBBROWSER (engl.)
Syn. zu Internetbrowser. Programm, um Internetseiten anzusehen.

WEB CRAWLING (engl.)
Übsg. Web-Raupe. Syn. zu Bot, Robot, Spider, Searchbot. Programm, welches im Internet Verlinkungen folgt, um neue Internetseiten zu finden und diese zu indexieren. Indexierte Seiten können bei Suchanfrage durch Benutzer durchsucht und angezeigt werden.

WEB-DEFACEMENT (engl.)
Übsg. Verunstaltung. Syn. zu Defacement. Internetseite, die unberechtigt manipuliert wurde, um neue Texte oder Bilder darzustellen.

WEBINAR
Abk. für Webseminar. Seminar, Vortrag oder Weiterbildung, welche über das Internet durchgeführt werden.

WEB KEY DIRECTORY [WKD] (engl.)
Übsg. Webschlüsselverzeichnis. Vom Projekt „Easy GPG“ initiiertes Protokoll, um die Zusammengehörigkeit registrierter E-Mail-Adressen und hochgeladener öffentlicher Schlüssel beim E-Mail-Anbieter zu überprüfen.

WEBMAIL (engl.)
Internetseite, welche die E-Mails des eigenen E-Mail-Kontos darstellt sowie einfache E-Mail-Funktionen, wie Lesen, Schreiben und Weiterleiten von E-Mails anbietet. Damit

kann auch unterwegs auf die eigenen E-Mails zugegriffen werden, wenn man nicht an seinem PC arbeitet. Beim Aufruf des Webmails auf einem fremden PC bspw. in einem Internetcafé muss darauf geachtet werden, sich zuletzt abzumelden und den Browserverlauf sowie die Browser-Cookies zu löschen, sonst könnten die nächsten Benutzer dieses PCs auf die E-Mails zugreifen.

WEB OF TRUST [WOT] (engl.)
Übsg. Netz des Vertrauens. Methode, um die Authentizität von öffentlichen Schlüsseln und dazugehörigen Zertifikaten zu bestätigen. Hierbei wird ein Zertifikat einer Person nicht von einer Beglaubigungsstelle (CA) oder durch eine zentrale Public-Key-Infrastruktur signiert, sondern durch andere Personen, die den Besitzer des öffentlichen Schlüssels persönlich kennen. Dies soll verhindern, dass Hacker sich als Besitzer dieses öffentlichen Schlüssels ausgeben, indem sie ihr Zertifikat unterjubeln.

WEBRTC
Abk. für Web Real-Time Communication. Übsg. Web-Echtzeitkommunikation. Protokolle und APIs zur Echtzeitkommunikation zwischen PCs. Dies wird bspw. für Videotelefonie und Chats verwendet.

WEBSEITE
Syn. zu Internetseite

WEBSERVER
Computer, welcher Anfragen von Clients über das Internet empfangen kann und Dateien oder Daten zurückschickt, bspw. Internetseiten, welche danach im Webbrowser des Benutzers angezeigt werden.

Beispiele: Microsoft Internet Information Services (IIS), Apache HTTP Server, nginx.

WEBSERVICE (engl.)
Übsg. Webdienst. System und Software, welche Apps oder anderen Systemen eine Möglichkeit anbieten, Daten einer Datenbank abzufragen oder andere rechen- oder datenintensive Funktionen aufzurufen. Meist ist das Resultat eine strukturierte, maschinenlesbare Antwort in den Formaten XML oder JSON.

WEBSITE (engl.)
Übsg. Webseite, Internetseite.

WEBSITE HACK (engl.)
Übsg. Angriff auf Internetseiten

WEBSOCKET
Auf TCP basierendes Netzwerkprotokoll zur Verbindung zw. einer Web-App und einem Webserver. Dabei wird, im Unterschied zu HTTP bei dem jeweils eine Anfrage und eine zugehörige Antwort verschickt wird, eine Verbindung offen gehalten, damit Daten ohne erneute Verbindungseröffnung an die Web-App geschickt werden können.

WEB-SSO
Abk. für Web-Single-Sign-On. Methode in Online-Systemen, um Mehrfachauthentifizierungen zu vermeiden. Durch die Verwendung des Protokolls SAML erlaubt Web-SSO einem Benutzer, sich bei einem Webdienst zu authentisieren und danach ohne zusätzliche Authentifizierung auf andere Ressourcen zuzugreifen. Dies wird dadurch erreicht, dass die Authentifizierungsbestätigung von der ersten zu jeder weiteren Webadresse übermittelt wird.

WEBTRAFFIC (engl.)
Übsg. Internetdatenverkehr

WEBURL (engl.)
Syn. zu URL, Internetadresse.

WEGWERF-E-MAIL-ADRESSE
Zeitlich begrenzte E-Mail-Adresse, die im Internet kostenlos eingerichtet und benutzt wird. Solche E-Mail-Adressen können jederzeit gelöscht werden, wenn bspw. zu viele Spam-E-Mails ankommen. Wer einen eigenen Webauftritt besitzt, kann meist selber E-Mail-Adressen aufsetzen und somit selber „Wegwerf- E-Mail-Adressen“ erzeugen.

WEISSE LISTE
Syn. zu Whitelist. Informationen oder Daten, die explizit akzeptiert werden. Bspw. können E-Mail-Adressen von Freunden auf weiße Listen gesetzt werden, damit E-Mails von ihnen nicht als Spam gekennzeichnet werden.

WEISUNG
Regeln, bspw. firmenintern, um Prozesse einheitlich auszuführen. Auch Verbote werden als Weisung formuliert.

WEP
Abk. für Wired Equivalent Privacy

WERBEBLOCKER
Zusatzsoftware innerhalb von Webbrowser, als Plug-in oder Extension, die besuchte Internetseiten analysiert, bevor oder nachdem diese angezeigt werden, und versucht, Werbung darin zu erkennen und aus den Seiten zu entfernen. Die Werbeblocker benutzen

dafür Blacklists und Heuristiken. Manche Werbeblockerhersteller lassen Firmen einen Eintrag auf Whitelists bezahlen, damit deren Seiten nicht geblockt werden. Mehrere Internetbetreiber verhindern die Anzeige ihrer Internetseite vollständig, falls ihre Webseite den Einfluss von Werbeblockern erkennt. Werbeblocker werden empfohlen, da damit auch verseuchte Werbebanner verhindert werden.

WERBE-E-MAILS
Syn. zu Spam

WESENTLICHE SCHUTZZIELE DER IT-SICHERHEIT
Bei IT-Sicherheit geht es grundsätzlich um die Aufrechterhaltung der Integrität, der Vertraulichkeit und der Verfügbarkeit von Daten und Systemen. Oft abgekürzt mit CIA für Confidentiality, Integrity and Availability.

WHALING
Gezielter Angriff auf Manager. Hergeleitet vom engl. Wort „Whale“, im Sinne von „große Fische“.

WHATSAPP
Sofortnachrichtendienst

WHIRLPOOL
Kryptografische Hash-Funktion, welche Hash-Werte von 512-Bit Länge erstellt.

WHISTLEBLOWER (engl.)
Übsg. Geheimer Informant. Whistleblower nutzen Insiderwissen und -zugang, falls sie keine andere Möglichkeit sehen, um über Missstände zu informieren. Sie tun dies mit guten Absichten aus ihrer Sicht, auch wenn dies möglicherweise nicht im Sinne der Firma oder Organisation ist.

WHITE HAT HACKERS (engl.)
Übsg. Hacker mit „weißen Hüten“. Von Firmen angestellte Hacker mit guten Absichten, die den Firmen helfen sollen, Schwachstellen in deren IT-Systemen aufzudecken.

WHITELIST (engl.)
Übsg. Weiße Liste

WHOAMI
Befehl, der in vielen Betriebssystemen in einer Konsole eingegeben werden kann, um den Benutzernamen und andere Informationen des Benutzers auszugeben.

WIDERRUFSZERTIFIKAT
Syn. zu Sperrzertifikat

WIEDERHERSTELLUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Seltene Aktion, um einen Schlüssel wieder als gültig zu definieren oder um einen verlorenen bzw. zerstörten Schlüssel aus einem Backup wiederherzustellen. Abschnitt im Lebenszyklus kryptografischer Schlüssel (siehe zusätzliche Details beim Begriff Schlüssel).

WI-FI
Ursprüngliche Abk. für Wireless Fidelity, Übsg. Kabellose Wiedergabetreue, in Anlehnung an Hi-Fi. Syn. zu WLAN. Für Spezifikation siehe Details unter IEEE 802.11.

WI-FI PROTECTED ACCESS [WPA] (engl.)
Übsg. Wi-Fi geschützter Zugriff. Kommunikationsprotokoll zur Sicherung von drahtlosen Netzwerken (Wireless-LAN), basierend auf der Strom-Chiffre RC4 zur Verschlüsselung der Kommunikation. Ab 2003 verfügbar. WPA wurde aufgrund von Sicherheitslücken durch WPA2 abgelöst, welches eine AES-Verschlüsselung benutzt.

WI-FI PROTECTED ACCESS 2 [WPA2] (engl.)
Übsg. Wi-Fi geschützter Zugriff 2. Kommunikationsprotokoll zur Sicherung von drahtlosen Netzwerken (Wireless-LAN). Ab 2004 verfügbar. Dieses basiert auf dem Advanced Encryption Standard (AES) mit 128-Bit und ist ein Nachfolger von WPA, welches nur auf dem Strom-Chiffre RC4 beruhte. Aufgrund vieler bekannt gewordener Passwort-Attacken gegen WPA2 sollte das eingesetzte Passwort stark gewählt werden, d. h. eine lange Kombination aus Groß- und Kleinbuchstaben mit Zahlen und Sonderzeichen und ohne Wörter, die in Wörterbüchern vorkommen.

WI-FI PROTECTED ACCESS 3 [WPA3] (engl.)
Übsg. Wi-Fi geschützter Zugriff 3. Kommunikationsprotokoll zur Sicherung von drahtlosen Netzwerken (Wireless-LAN). Ab 2018 verfügbar. Nachfolger von WPA2. Aufbauend auf 128- bis 192-Bit-Verschlüsselung, Forward Secrecy und zusätzlichen Funktionen.

WIKI
Internetinformationsseiten, die von Benutzern im Internet erstellt, veröffentlicht, geändert und ergänzt werden können, im Sinne von Web 2.0.

WIKIPEDIA
Freie Online-Enzyklopädie, die jeder ergänzen und ändern darf, gemäß dem Prinzip von Wiki.

WIN32 CRYPTO API
Funktionenbibliothek in Microsoft Windows zur Ausführung von kryptografischen Berechnungen. Bspw. CryptGenRandom zur Generierung von Zufallszahlen.

WINDOWS ADK
Abk. für Windows Assessment and Deployment Kit

WINDOWS ASSESSMENT AND DEPLOYMENT KIT [WINDOWS ADK] (engl.)
Programme von Microsoft, um Windows-Installationen anzupassen und um die Qualität und Leistung des PCs zu testen.

WINDOWS AUTHENTICATION (engl.)
Abk. für Integrated Windows Authentication (IWA)

WINDOWS AZURE ACTIVE DIRECTORY RIGHTS MANAGEMENT (engl.)
Syn. zu Azure Active Directory Rights Management

WINDOWS DEFENDER (engl.)
Abk. für Windows Defender Antivirus. Programm in Windows-Systemen zur Detektion von Schadsoftware wie bspw. Viren. Dazu werden Dateien durch die Software überprüft, bevor der Benutzer damit arbeitet. Falls kein anderes Anti-Viren-Programm installiert ist, sollte Windows Defender aktiviert werden.

WINDOWS INFORMATION PROTECTION [WIP] (engl.)
Trennung von persönlichen Daten und Firmendaten und Schutzfunktionen auf Windows10-Geräten. Nachfolger von Enterprise Data Protection (EDP).

WINDOWS INTERNET NAMING SERVICE [WINS] (engl.)
Microsofts Implementation des NetBIOS über TCP/IP zur Namensauflösung in Local Area Networks, ähnlich zu DNS.

WINDOWS RIGHTS MANAGEMENT SYSTEM [WINDOWS RMS] (engl.)
Syn. zu Rights Management System (RMS). Produkt der Firma Microsoft zur Verschlüsselung von Dokumenten und E-Mails. Vorgänger von Active Directory Rights Management System (ADRMS).

WINDOWS RMS
Abk. für Windows Rights Management System

WINDOWS SECURITY GROUP (engl.)
Syn. zu Active Directory Group

WINDOWS TERMINAL SERVER
Syn. zu Remote Desktop Services (RDS)

WINPE
Abk. für Microsoft Windows Preinstallation Environment. Minimales Windows-Betriebssystem, welches auf einer CD oder einem USB-Stick Platz findet und eine manuelle oder automatische Installation von Windows auf einem neuen Computer ermöglicht.

WINS
Abk. für Windows Internet Naming Service

WINSCP
SSH-Client-Applikationen (siehe Secure Shell)

WINTEL
Abk. für Systeme, welche auf der Kombination von Windows-Betriebssystem und Intel Prozessor betrieben werden.

WIP
Abk. für Windows Information Protection

WIPER MALWARE
Schadsoftware, die den Master Boot Sector löscht. Dies wird von Hackern als Ablenkungsaktion benutzt, oder um Beweise zu löschen.

WIRED EQUIVALENT PRIVACY [WEP] (engl.)
Veralteter Sicherheitsalgorithmus für drahtlose Netzwerke (Wireless-LAN). Ab 1997 verfügbar. Dieser benutzt die Strom-Chiffre RC4 für die Datenvertraulichkeit und CRC-32 Prüfsumme für die Datenintegrität. Wurde 2003 durch WPA und danach durch WPA2 abgelöst. WEP sollte für das Heimnetzwerk nicht mehr verwendet werden.

WIRELESS LOCAL AREA NETWORK [WLAN] (engl.)
Übsg. Drahtloses lokales Netzwerk. Syn. zu Wi-Fi, Funknetzwerk (siehe Details unter IEEE 802.11).

WKD
Abk. für Web Key Directory

WLAN
Abk. für Wireless Local Area Network. Syn. zu Wi-Fi. Für Spezifikation und Details siehe IEEE 802.11.

WORDPRESS
Beliebte CMS-Plattform zur einfachen Erstellung und Verwaltung von Blogs und Internetseiten.

WORLDWIDEWEB
Ursprünglicher Name des ersten Browsers, der 1990 am Forschungszentrum Cern in der Schweiz entwickelt wurde. Danach als Nexus bezeichnet, um den Unterschied zum Internet zu verdeutlichen, welches „World Wide Web“ bezeichnet wird.

WORLD WIDE WEB [WWW] (engl.)
Übsg. Weltweites Netz. Früher wurde der Begriff häufig als Syn. zu Internet benutzt. Ursprünglich ein Begriff nur für HTML-Webseiten, heute für alle onlineverfügbaren Dienste, Informationen und Seiten und allg. die weltweite Vernetzung von Computern.

WORLD WIDE WEB CONSORTIUM [W3C] (engl.)
Organisation zur Festlegung und Standardisierung von Techniken und Spezifikationen im Internet.

WORM (engl.)
Übsg. Computer-Wurm

WÖRTERBUCH-ANGRIFF
Erraten eines Passworts mittels Durchtestens der Wörter mehrerer Wörterbücher als Eingabe in ein Passwortfeld.

WOSD PROTECTION
Wordpress Schutzfunktion

WOT
Abk. für Web of Trust

WOW6432
Eintrag in der Windows-Registrierungsdatenbank, der für 32-Bit-Programme benutzt wird, welche auf 64-Bit-Versionen von Windows betrieben werden. Der Eintrag befindet sich in der Registrierungsdatenbank unter „HKLM\Software\Wow6432“.

WPA
Abk. für Wi-Fi Protected Access

WPA2
Abk. für Wi-Fi Protected Access 2

WPA3
Abk. für Wi-Fi Protected Access 3

WPML PLUG-IN
Abk. für WordPress Multilingual Plugin. Dies erlaubt die Mehrsprachigkeit bei Wordpress.

WS-FEDERATION
Abk. für Webservices Federation. Protokoll für die Federation von Identitäten innerhalb der SOAP-Erweiterung WS-Security. WS-Federation erweitert WS-Trust um eine flexible verteilte Identitätsarchitektur mit klaren Unterscheidungen zwischen Vertrauensmechanismen, Formaten von Security Tokens und dem Protokoll zum Abrufen von Token. Es kann durch Webservices und SOAP-Clients benutzt werden.

WS-SECURITY
Abk. für Webservices Security. Erweiterung für SOAP, um Sicherheitsaspekte bei Webservices anzuwenden. Es definiert, wie SOAP-Nachrichten signiert und verschlüsselt werden können und wie Security Tokens an SOAP-Nachrichten angehängt werden können, um den Sender zu identifizieren.

WS-TRUST
Abk. für Webservices Trust. Teil von WS-Security. Beinhaltet Spezifikationen und Implementationen für Webservices, zur Erstellung von Security Tokens, zur Ermöglichung von Security-Token-Aufrufen, und zur Durchführung von Schlüsselaustausch. Diese werden im Betrieb von Trust-Domänen verwendet.

WURM
Syn. zu Computer-Wurm

WWW
1) Abk. für World Wide Web. Syn. zu Internet. Gesamtheit aller Internetseiten, die speziell für Webbrowser erstellt wurden und über eine URL aufrufbar sind, bspw. www.domain.com. 2) Die Bezeichnung „WWW“ wurde in den 1990er-Jahren (belustigend) auch als „World Wide Wait“ verwendet, oder auch (seriöser) als „Work Where you Want“.

X

26

X.509-ZERTIFIKAT
Digital signierte Datei, die eine vordefinierte Struktur hat und u. a. den Namen des Besitzers, den öffentlichen Schlüssel des Besitzers und die signierende Zertifizierungsstelle angibt, wobei der Schlüssel ein Teil ist eines Schlüsselpaars aus öffentlichem und privatem Schlüssel. Damit kann eine Person oder ein System identifiziert werden, können E-Mails oder Internetverbindungen verschlüsselt werden, kann ein programmierter Code signiert werden oder der Aufruf einer HTTPS-Internetseite erfolgreich und sicher durchgeführt werden. X.509 ist eine Bezeichnung der Struktur des Zertifikats.

X-HEADER
Metadaten innerhalb einer E-Mail. Solche werden häufig verwendet, um die E-Mail zu beschreiben, umzuleiten oder um versteckte, nicht geheime Daten mit der E-Mail mitzuschicken.

XML-GATEWAYS
Hardware oder Software zur Umsetzung von Identitäts- und Sicherheitsfunktionen für SOAP-, XML- und REST-basierte Webservices im Kontext von Sicherheitsaspekten bei Service-Oriented Architecture (SOA). XML-Gateways bieten u. a. PKI, digitale Signatur, Verschlüsselung, XML-Schemavalidierung, Virenschutz und Mustererkennung.

XRP
Kryptowährung

XSALSA20
Erweiterung der Salsa20 Stromverschlüsselung. Hierbei wird eine Einmalzahl von 192-Bit Länge mitverrechnet.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_26

XSS
Abk. für Cross-Site-Scripting

XSS VULNERABILITIES (engl.)
Übsg. Anfälligkeiten für Cross-Site-Scripting.

XTERM
Terminal-Emulator für Unix oder Unix-ähnliche X Window-Systeme.

Y

27

Y2K
Abk. für Year 2000, Übsg. Jahr 2000. Syn. zu Jahr-2000-Problem, Millennium-Bug. Begriff der 1990er-Jahren zur Beschreibung eines weltweiten Typs von (vermuteten) Softwareproblemen in Geräten, PCs, Anzeigetafeln, Geldautomaten etc. Viele der damals verwendeten Programme wurden in den 1960er- bis 1990er-Jahren entwickelt und benutzten aus Speicherplatzgründen zweistellige Datumswerte, z. B. „95“ anstatt „1995“. Es wurde erkannt, dass mit dem damalig bevorstehenden Wechsel des Jahrtausends diese Programme mit dem Datum „00“ (für „2000“) rechnen würden, was zu Fehler führen könnte, da bspw. ein Eintrag „80“ für das Geburtsdatum zu einer Lebensalterberechnung führen könnte, welche kleiner null wäre. Deshalb wurden viel Geld und Aufwand eingesetzt, um die Programme erfolgreich vor dem Jahr 2000 anzupassen.

YABA
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „Yet another Bloody Acronym!“, Übsg. „Wieder eine Abkürzung!“

YAHOO!
Anbieter von Webservices, wie bspw. Internetportal und Suchmaschine.

YAML
Abk. für YAML Ain’t Markup Language. Von Menschen lesbare Datenbeschreibung für alle Programmiersprachen, angelehnt an XML. Grundgedanke ist, dass alle Daten und Datenstrukturen immer als Listen, Arrays und Einzelwerte geschrieben werden können.

YOLO
In SMS, Internet-Kommentaren, Internet-Foren und in sozialen Medien benutzte Abk. für „You only live once“, Übsg. „Du lebst nur einmal“.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_27

YOUBIT
Bitcoinbörse, welche 2017 aufgrund einer Attacke durch Hacker schließen musste.

YOUTUBE
Videoportal

YOWAI
Typ von Botnet

YUBICLOUD
Webservice der Firma Yubico zur Verifizierung von One-Time-Passwörter, die mit YubiKeys erzeugt werden.

YUBIKEY
Hardwarebasierter Authentisierungsstick von Yubico.

Z

28

ZEICHENSATZ
Liste von Zeichenkodierungen, d. h. eindeutige Zuordnung von Zeichen zu Werten. Beispiele: UTF-8, ASCII (siehe auch ASCII-Tabelle im Anhang Tab. 32.1).

ZERO-DAY ATTACK (engl.)
Übsg. Null-Tage-Attacke. Syn. zu Zero-Day Exploit. Angriff, der eine Schwachstelle ausnutzt, bevor sie dem Opfer bekannt wurde. Die Opfer und Hersteller der Systeme haben demnach „null Tage" Zeit, diese Schwachstelle zu beheben.

ZERO-DAY EXPLOIT (engl.)
Übsg. Null-Tage-Schwachstelle. Ausnutzen einer Schwachstelle, bevor Softwarehersteller eine Chance haben, ihr Produkt dagegen zu schützen. Die Softwarehersteller erfahren zu spät davon und haben „null Tage" Zeit, sich darauf vorzubereiten. Solche Zero-Day Exploit werden im Darknet gehandelt, da sie für Hacker wertvoll sind, solange die Softwarehersteller noch nichts davon wissen. Große Softwarehersteller versuchen, solchen Attacken zuvorzukommen, indem sie „Finderlohn" („Bug Bounty") anbieten für die Suche und Mitteilung von Sicherheitslücken in ihren Systemen und Programmen.

ZERO-DAY VULNERABILITY (engl.)
Syn. zu Zero-Day Exploit

ZERO-KNOWLEDGE PROOF [ZKP] (engl.)
Übsg. Kenntnisfreier Beweis. Verfahren zur Authentisierung, bei welcher eine Partei der anderen glaubhaft beweisen kann, dass sie (und meist nur sie) ein Geheimnis kennt, ohne das Geheimnis mitteilen oder anwenden zu müssen. Anstatt Zero-Knowledge Proof werden heutzutage häufiger digitale Signaturen zur einfacheren Authentisierung verwendet.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_28

ZERTIFIKAT
Digital signierte Datei, die eine vordefinierte Struktur hat und u. a. den Namen des Besitzers, den öffentlichen Schlüssel des Besitzers und die Zertifizierungsstelle angibt, wobei der Schlüssel Teil ist eines Schlüsselpaars aus öffentlichem und privatem Schlüssel. Damit kann eine Person oder ein System identifiziert werden, können E-Mail-Verbindungen verschlüsselt werden, kann ein programmierter Code signiert werden oder der Aufruf einer Internetseite gesichert erfolgen. Die Struktur des Zertifikats kann bspw. durch X.509 definiert sein (siehe Abb. 28.1).

ZERTIFIKAT EINER ZWISCHEN-CA
Syn. zu Zertifikat einer Zwischenzertifizierungsstelle. Zwischenzertifizierungsstellen stehen zw. der Hauptzertifizierungsstelle (Root-CA) und dem Benutzer oder weiteren Zwischen-CAs und können Zertifikate signieren, falls diese Zwischen-CA von der Root-CA als vertrauenswürdig angesehen wird, und damit ein signiertes Zertifikat erhält. Damit lässt sich eine Vertrauenskette bis zur Root-CA aufbauen.

ZERTIFIKATSANNULIERUNG
Falls ein privater Schlüssel oder ein Zertifikat kompromittiert wurde, kann das zugehörige Sperrzertifikat aktiviert werden, indem es auf Public-Key-Servern veröffentlicht wird. Damit wird das zugehörige Schlüsselpaar gesperrt und das entsprechende Zertifikat annulliert. Ein gesperrtes Schlüsselpaar kann weiterhin verwendet werden, um alte Signaturen zu verifizieren und Daten zu entschlüsseln, solange der private Schlüssel noch vorhanden und nicht kompromittiert ist.

ZERTIFIKATSAUSSTELLUNG
1) Verfahren zur Erstellung eines Zertifikats. 2) Signieren eines Zertifikats durch eine Zertifizierungsstelle.

ZERTIFIKATSSPERRLISTE
Liste der Zertifikate, die mittels eines Widerrufszertifikats annulliert wurden und damit ungültig sind. Applikationen prüfen, ob ein Zertifikat annulliert, gesperrt oder widerrufen wurde, bevor sie es verwenden.

ZERTIFIKATSWIDERRUFSLISTE
Syn. zu Zertifikatssperrliste

ZERTIFIZIERUNG EINES KRYPTOGRAFISCHEN SCHLÜSSELS
Erstellung und digitales Signieren von Schlüsseln auf Anfrage an eine CA. Abschnitt im Lebenszyklus kryptografischer Schlüssel. Siehe zusätzliche Details beim Begriff Schlüssel.

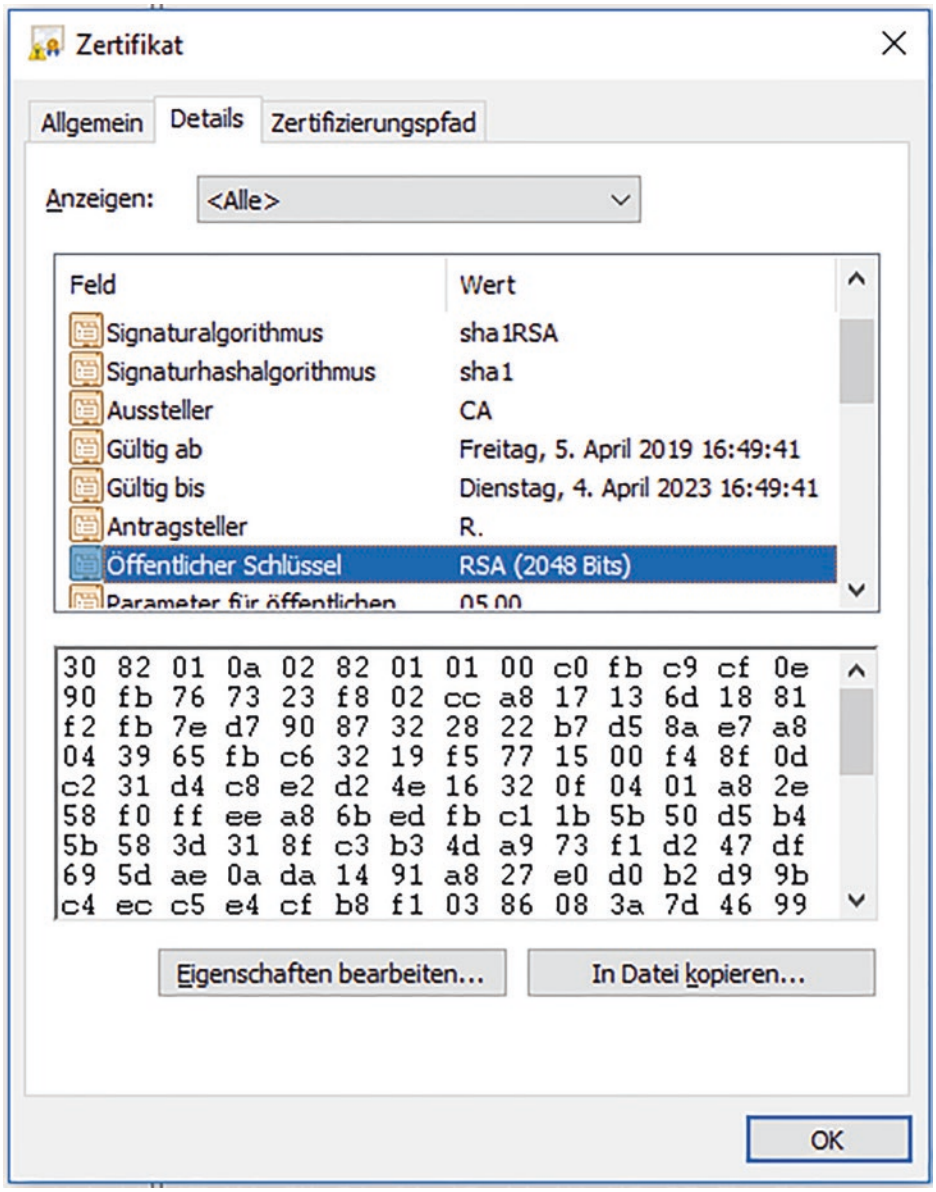

Abb. 28.1 Beispiel eines Zertifikats (in Windows)

ZERTIFIZIERUNGSSTELLE

Syn. zu Beglaubigungsstelle, Certification Authority (CA). Vertrauenswürdige Organisation oder Firma, welche digitale Zertifikate ausstellt oder signiert, und damit die Authentizität von elektronischen Signaturen und Public-Private-Schlüsselpaare bestätigt. Internetbetreiber können mittels eines „Certificate Signing Request“ (CSR) bei einer

Zertifizierungsstelle ein Zertifikat signieren lassen, welches Details beinhaltet, wie den Servernamen, den öffentlichen Serverschlüssel, ein Ablaufdatum und den Namen der Stelle, die die Vertrauenswürdigkeit bestätigt. Solche signierten Zertifikate werden dann auf dem Internetserver gespeichert und garantieren den Zusammenhang zw. öffentlichem Serverschlüssel und der Serveridentität. Mehrere Hundert Zertifizierungsstellen sind weltweit tätig und bilden eine wichtige Stütze für die Internetsicherheit, da sie die Echtheit von digitalen Schlüsseln und Signaturen bestätigen. Viele solcher CAs sind mit ihren eigenen Root-Zertifikaten bei den Internetbrowsern standardmäßig als vertrauenswürdige Stellen hinterlegt und sie unternehmen alles, damit ihnen bedingungslos vertraut werden kann.

ZKP
Abk. für Zero-Knowledge Proof

ZONE SIGNING KEY [ZSK] (engl.)
Signaturschlüssel für eine Zone. Bei Domain Name System (DNS) ist jeder Nameserver für eine bestimmte Zone, d. h. für einen Teil des Domänenbaums verantwortlich und besitzt die entsprechenden DNS-Daten. Diese Daten werden mit dem privaten Schlüssel des Nameservers signiert und können mit dem öffentlichen Schlüssel des Nameservers überprüft werden. Die Authentizität des Nameservers und der benutzten Schlüssel können mit dem Zone Signing Key validiert und garantiert werden.

ZSK
Abk. für Zone Signing Key

ZUFALLSZAHLEN
Per Software oder Hardware erzeugte zufällige Zahlenwerte. Eine statistisch möglichst gleichmäßige Verteilung von Zufallszahlen ist eine Voraussetzung für sichere Verschlüsselung und andere kryptografische Algorithmen.

ZUGANG
Benutzung von Systemen, Netzwerken, Dateien oder physischen Eingangstüren.

ZUGANGSBESCHRÄNKUNG
Teil der Zugriffskontrolle. Einschränkungen von Personen oder Systemen beim Zugang zu Computern, Netzwerken, Dateien oder Gebäuden. Diese Einschränkungen können benutzerspezifisch eingerichtet werden oder für Gruppen, in die die Benutzer eingeteilt werden. Ziel ist meist nur, den Zugang zu erlauben, der für die aktuelle Funktion des Benutzers nötig ist und damit die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen.

ZUGANGSDATEN
Syn. zu Anmeldedaten, Credentials. Benutzername und Passwort oder Zertifikate, die benutzt werden und ausreichen, um sich an einem System, einem Programm oder an einem Onlinedienst anzumelden und damit den Zugang zu erhalten.

ZUGANGSVERWALTUNG
Syn. zu Access Management. Verwaltung und Bereitstellung von Zugriffsrechten, Single Sign-On (SSO) und Sicherheitsregeln.

ZUGRIFF
Benutzung von Systemen, Netzwerken oder Dateien.

ZUGRIFFSKONTROLLE
Überwachung, Verwaltung und Steuerung des Zugriffs auf bestimmte Computer, Netzwerke oder Dateien. Das Ziel der Zugriffskontrolle ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und Systemen. Ein wichtiger Teil der Zugriffskontrolle ist die Zugangsbeschränkung.

ZUGRIFFSLISTEN
Syn. zu Access Control Lists (ACL). Die Zugriffskontrolle von Benutzer an einem System geschieht häufig über Zugriffslisten. Dabei wird für Dateien oder andere Ressourcen im System festgelegt, wer zu welcher Zeit und in welcher Art und Weise diese Dateien und Ressourcen benutzen oder bearbeiten darf. Nicht explizit erteilte Zugriffsrechte sind grundsätzlich verboten, d. h. bspw. ein erlaubtes „Nur-Lesen“-Recht ist indirekt auch ein „Speichern-verboten“-Recht, auch wenn dies nicht explizit erteilt wurde.

ZUGRIFFSRECHT
Zeitlich oder örtlich vergebene Erlaubnis an Benutzer oder Systeme, um die in Zugriffslisten definierten Dateien, Systeme oder Systemressourcen zu benutzen. Dafür muss dieser Benutzer oder das System vorweg genau identifiziert sein, bspw. durch Authentifizierung.

ZWEI-FAKTOR-AUTHENTIFIZIERUNG [2FA]
Syn. zu Zwei-Faktor-Authentisierung

ZWEI-FAKTOR-AUTHENTISIERUNG [2FA]
Authentisierungsmethode zur Anmeldung bei Apps, Systemen oder Online-Diensten oder bspw. zur Durchführung von Zahlungen. Dabei werden zwei Sicherheitsmethoden (sog. „Faktoren“) nacheinander oder gleichzeitig eingesetzt, wie z. B. Passwort und zusätzlich Codes per SMS. Ziel ist das Verhindern und Blockieren von Angriffen zum Schutz vor Identitäts- und Datendiebstahl. Nur falls beide Faktoren vorhanden

und korrekt bestätigt werden, wird die Zahlung ausgeführt, das Produkt bestellt, die Online-Transaktion durchgeführt oder der Zugang zum Konto ermöglicht. Andere Methoden, die bei 2FA verwendet werden, sind TAN, Muster, Fingerabdruck, Smartcard, Token, QR-Code, Autorisierungs-Apps usw.

ZWEI-SCHRITT-VERIFIZIERUNG
Syn. zu Zwei-Faktor-Authentisierung. Methode, um den Zugriff auf ein Online-Konto oder Online-Dienst sicherer zu machen. Dabei wird nicht nur ein Benutzername und Passwort abgefragt, sondern zusätzlich eine zweite Bestätigung (sog. „Faktor“), welche bspw. in Form eines Codes per SMS geschickt wurde.

Teil II

Anhang

SPEZIALTHEMA „Der Aufruf einer HTTPS-Internetseite“

29

29.1 Einführung

Die sichere Kommunikation im Internet wird zunehmend wichtiger, je mehr im Internet eingekauft wird, Online-Banking durchgeführt wird oder persönliche Daten übermittelt werden. Der geschützte Abruf einer Internetseite basiert heutzutage meist auf HTTPS. Man erkennt dies im Internetbrowser an einem geschlossenen Schlösschen oder einem Schlüsselsymbol. Für die dabei benötigte verschlüsselte Übertragung werden drei Schritte ausgeführt (siehe auch Abb. 29.1):

1. Der Internetseitenbetreiber muss seinen Webserver zertifizieren und erhält dafür ein Zertifikat.
2. Der Internetbrowser prüft die Echtheit des Webservers, d. h. führt eine Authentifizierung des Webservers mittels Zertifikats durch.
3. Die zu sendenden Internetdaten werden mit einem gemeinsamen Client-Server-Session-Schlüssel verschlüsselt.

29.2 Schritt 1: Zertifikat des Webservers

Damit dem Webserver einer Firma vertraut wird, lässt sich diese ein digitales Zertifikat für diesen Webserver ausstellen. Dazu wird auf dem Webserver ein Paar aus öffentlichem und privatem Schlüssel erstellt (z. B. mittels OpenSSL) und ein signiertes X.509-Zertifikat bei einer Zertifizierungsstelle (CA) beantragt. Dieses beinhaltet Details, wie den Namen der Webadresse, den erstellten öffentlichen Schlüssel, Ablaufdatum und den Namen der Stelle, die die Vertrauenswürdigkeit bestätigt. Dieses signierte Zertifikat wird dann auf dem Webserver gespeichert und verknüpft dadurch den öffentlichen Webserverschlüssel mit dem

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z*,
https://doi.org/10.1007/978-3-662-60911-8_29

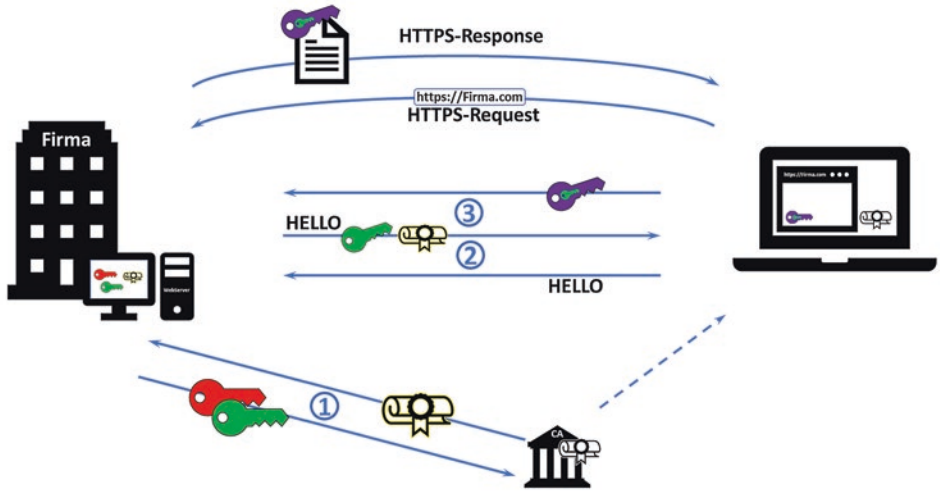

Abb. 29.1 Der Aufruf einer HTTPS-Internetseite

Webserver. Der private Schlüssel wird geheim gehalten und ebenfalls auf dem Webserver oder einem angehängten Token, z. B. einem Hardware Security Module (HSM) gespeichert.

29.3 Schritt 2: Prüfung der Echtheit durch Internetbrowser

Beim ersten Aufruf einer HTTPS-Seite von einem Webserver findet ein sog. TLS-Handshake statt, bei welchem der Internetbrowser eine unverschlüsselte Anfrage an den Webserver sendet („Client HELLO“). Der Server schickt daraufhin zur Authentisierung unverschlüsselt seinen öffentlichen Schlüssel sowie sein Zertifikat („Server HELLO“). Der Internetbrowser validiert, ob ihm die im Zertifikat angegebene Zertifizierungsstelle und deren Root-Zertifikat bekannt ist, sowie weitere Daten des Webserverzertifikats und entscheidet, ob diesem vertraut werden kann.

29.4 Schritt 3: Senden der verschlüsselten Internetdaten

Nach erfolgreicher Authentifizierung des Webservers erzeugt der Internetbrowser mit SSL/TLS einen symmetrischen Sitzungsschlüssel (sog. „Session Key“), den er mit dem öffentlichen Schlüssel des Webservers verschlüsselt und als Paket an diesen Webserver schickt („Client Key Exchange“). Nur dieser Webserver kann das vom Internetbrowser kommende Paket mit dem eigenen privaten Schlüssel entschlüsseln. Damit besitzen der Internetbrowser und der Webserver ein gemeinsames Geheimnis, welches nur ihnen bekannt ist. Dieses kann fortan für diese Verbindung benutzt werden, um eine sichere Übertragung von HTTPS-Daten durchzuführen. Der Webserver schickt dabei die mit dem gemeinsamen Geheimnis verschlüsselten Internetdaten der HTTPS-Seite an den Internetbrowser, der diese anschließend entschlüsseln und dem Benutzer anzeigen kann („HTTPS-Request“ und „HTTPS-Response“).

SPEZIALTHEMA „E-Mail-Verschlüsselung. Kostenlos. Einfach einzurichten und zu benutzen.“

30

30.1 Wozu E-Mails verschlüsseln?

E-Mail-Verschlüsselung scheint nur wichtig für Whistleblower und Agenten, ist es jedoch längst nicht mehr. Es müsste zum Standard für uns alle werden, auch wenn man „nichts zu verbergen hat“. E-Mails lassen sich mit Postkarten vergleichen. Jeder, der diese zwischen dem Absender und dem Empfänger in die Hände kriegt, kann die Postkarte und die E-Mail lesen, auch wenn SSL/TLS auf dem Transport der E-Mail vom Sender zum Mail-Server und vom Mail-Server zum Empfänger eingerichtet ist. Dadurch können private Informationen, die scheinbar harmlos sind, kombiniert werden mit anderen öffentlichen Datenquellen und bieten Möglichkeiten des Missbrauchs. Auch könnten Daten, wie z. B. eigene Bilder, die heute harmlos scheinen, bei einer zukünftigen Jobbewerbung oder einer Wohnungssuche ein negatives Bild abgeben, und letztlich kann man auch nie sicher sein, ob der Empfänger der E-Mail die zugeschickten Informationen unverschlüsselt erhalten möchte.

Erfreulicherweise ist es in den letzten Jahren sehr einfach geworden, E-Mail-Verschlüsselung einzurichten. Es bedarf lediglich ca. 15 min Zeit und kann danach mit einem Klick auf private oder berufliche E-Mails angewendet werden.

Die Einrichtung der E-Mail-Verschlüsselung ist ähnlich für die meisten Systeme (Windows, MAC, Linux). Auf jedem System besteht die Einrichtung aus den folgenden drei Schritten:

1. Download der freien, kostenlosen Software „GnuPG“ (GNU Privacy Guard).
2. Erstellen eines persönlichen Schlüsselpaars für die eigene E-Mail-Adresse.
3. Anwenden der Verschlüsselung auf E-Mails.

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z*,
https://doi.org/10.1007/978-3-662-60911-8_30

(Zum aktuellen Zeitpunkt könnte das von Ihnen benutzte E-Mail-Programm bereits eine einfachere Methode zur Benützung von „GnuPG“ anbieten. Auf https://www.gpg4win.org *[Abgerufen am 22.12.2019]* finden Sie Installations- und Benützungstipps.)

30.2 Schritt 1: Installation

Das Programm „GnuPG“ von https://www.gpg4win.org/ *(Abgerufen am 22.12.2019)* herunterladen und die vordefinierten Komponenten installieren.

Zusätzlich lässt sich in Apple Mail und Thunderbold ein Add-on namens „Enigmail“ herunterladen und gemäß dem darin enthaltenen „Enigmail Einrichtungsassistent“ installieren.

30.3 Schritt 2: Eigenes Schlüsselpaar erstellen

Das soeben mitinstallierte „Kleopatra“ öffnen, falls es nicht bereits automatisch nach der Installation gestartet wurde, und entweder „Persönliches OpenPGP-Schlüsselpaar erzeugen“ oder „Neues Schlüsselpaar“ wählen.

Nach der Eingabe des eigenen Namens und der eigenen E-Mail-Adresse kann bereits das persönliche Schlüsselpaar erzeugt werden. Dazu wird noch eine Passphrase oder ein Passwort eingegeben, das man sich gut merken sollte, denn dieses wird verwendet, um seine digitalen Schlüssel zu schützen. Nun werden das Schlüsselpaar und der zugehörige sog. Fingerabdruck erzeugt. Die Sicherheitskopie des Schlüsselpaars sollte unbedingt an einem sicheren Ort gespeichert werden.

Damit andere Personen den so erzeugten öffentlichen Schlüssel zur Verschlüsselung von E-Mails benutzen können, muss dieser noch abschließend an einen Verzeichnisdienst übermittelt werden. Dafür einfach den entsprechenden Knopf oder das entsprechende Menü wählen.

30.4 Schritt 3: E-Mails verschlüsseln

Um verschlüsselte E-Mails austauschen zu können, müssen beide, Sender und Empfänger, GnuPG installiert haben. Dann ist alles bereit und kann zur E-Mail-Verschlüsselung und -Entschlüsselung benutzt werden. Der Sender wählt hierzu in seinem E-Mail-Programm den öffentlichen Schlüssel des Empfängers. Der Empfänger kann daraufhin die verschlüsselte E-Mail mit seinem privaten Schlüssel entschlüsseln.

Konkret beginnt man zur Verschlüsselung einer E-Mail diese wie üblich zu erstellen und wählt vor dem Senden noch den Knopf mit der Bezeichnung „Verschlüsseln“ (siehe Abb. 30.1).

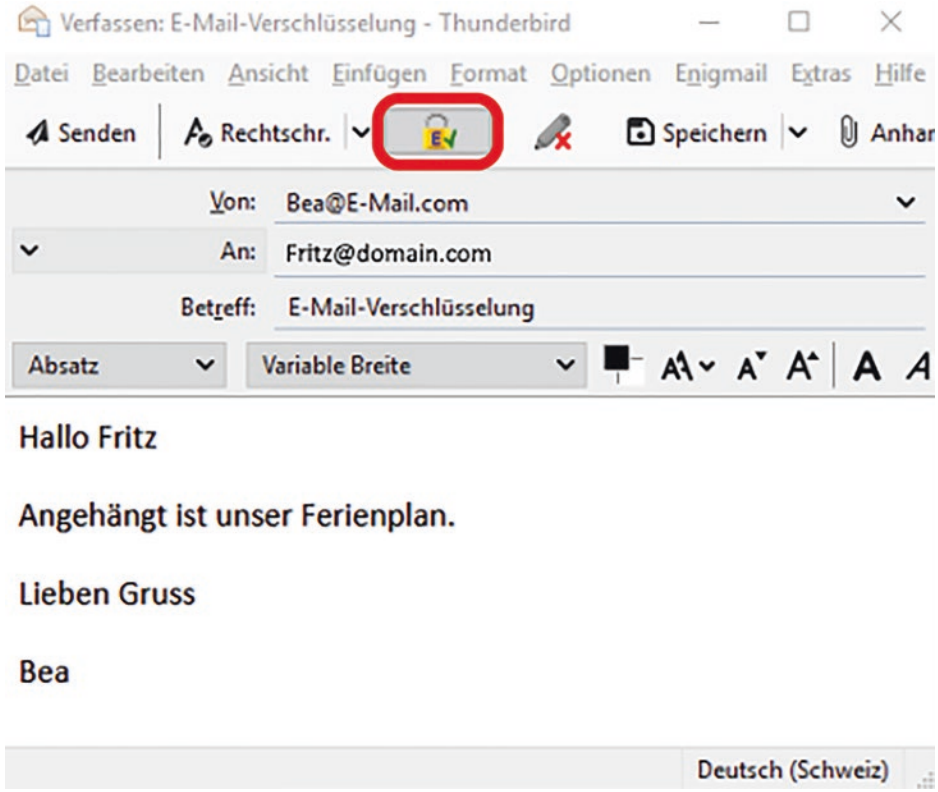

Abb. 30.1 E-Mail-Verschlüsselung am Beispiel des E-Mail-Programms Thunderbird

Falls man einem Empfänger noch nie eine verschlüsselte Nachricht geschickt hat, kennt das eigene E-Mail-Programm dessen öffentlichen Schlüssel noch nicht und schlägt vor, die E-Mail unverschlüsselt zu senden. Hier lohnt es sich, auf „Kleopatra“ oder in „Enigmail“ mittels „Auf Server suchen“ den öffentlichen Schlüssel des Empfängers zu suchen und wenn vorhanden, durch „Importieren“ herunterzuladen. Danach kann die E-Mail an diesen Empfänger verschlüsselt verschickt werden.

Wichtige Zusatzfunktion: Eine weitere mitinstallierte Funktion, die separat oder zusammen mit der Verschlüsselung angewendet werden kann, ist das sog. „Signieren“. Dadurch wird mit dem eigenen privaten Schlüssel ein Hashwert der E-Mail erzeugt und mit der E-Mail mitgeschickt. Der Empfänger kann dadurch mithilfe des öffentlichen Schlüssels prüfen, ob die erhaltene E-Mail unverändert und vom richtigen Sender bei ihm angekommen ist.

Tipps und Tricks für die eigene IT-Sicherheit

31

▶ **Trailer**

In den letzte`n 30 Jahren wurden wir aufgefordert, zunehmend komplexere Passwörter zu wählen. Für uns Menschen ist dies eine Herausforderung. Für Computer hingegen wurde die Enträtselung der Passwörter eine immer einfachere Aufgabe.

Bedachtes Handeln, aktuelle Systeme und Programme, ein Passwort-Manager und Zwei-Faktor-Authentifizierung helfen unsere Daten und uns zu schützen!

31.1 Warum soll ich meine Daten schützen?

Im Alltag begegnet man vielen Situationen, in denen die eigenen Daten oder die Firmendaten in Gefahr sind. Sei es durch einen Virus, der als E-Mail-Anhang auf den PC kommt, oder durch Schadsoftware, welche mittels eines vermeintlich interessanten USB-Stick eingeschleust wurde.

Die folgenden drei Erklärungen sollen aufzeigen, warum man sich schützen soll, auch wenn man „unwichtig für Gauner" scheint:

a) Wer Zahlungen im E-Banking am Computer erledigt, möchte seinen Zugang zum E-Banking-Konto nicht in fremden Händen sehen.
b) Wer Bilder und Videos von sich oder seinen Kindern auf dem Computer speichert, möchte diese Aufnahmen nicht unverändert oder manipuliert auf Social Media oder auf verbotenen Internetseiten sehen oder dort vermuten. Auch können diese Aufnahmen für Social Engineering, also zur Erschleichung von Vertrauen, z. B. bei den eigenen Kindern,

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_31

missbraucht werden. Außerdem können Daten, die heute gestohlen werden, in naher oder ferner Zukunft für Erpressungen und andere Missbräuche verwendet werden.

c) Der Diebstahl von Daten eines PCs oder eines Kontos bietet häufig Möglichkeiten, auch andere PCs oder Konten zu missbrauchen.

31.2 Tipps zum Schutz der Daten und der eigenen Identität

Unterschiedliche Datentypen besitzen unterschiedliche Schutzanforderungen. Sind die Daten nicht oder kaum persönlich oder sensitiv, dann braucht der Schutz nicht stark zu sein. Bei persönlich oder sensitiven Daten hingegen, z. B. bei privaten Fotos, sollte auf möglichst hohen Schutz Wert gelegt werden.

31.2.1 TOP-5-Datenschutztipps für jedermann

1. UPDATES!
   Betriebssystem und Apps von PC, Handy, Router und anderen Geräten aktuell halten durch die zeitnahe Installation der Updates der Hersteller. Auch Anti-Viren-Programm installieren und aktuell halten (Abb. 31.1).
2. BACKUPS!
   Backups von wichtigen Daten regelmäßig erstellen und nicht am PC angeschlossen lassen (Abb. 31.2).

Abb. 31.1 Updates bei Betriebssystem und Apps durchführen

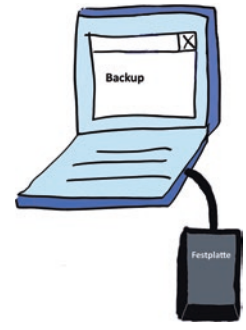

Abb. 31.2 Regelmäßig Backups erstellen

3. NICHTS UNBEDACHT ÖFFNEN ODER ANKLICKEN!
   Keine Links und keine E-Mail-Anhänge unbedacht anklicken und öffnen. Je stärker der Reiz einen Anhang zu öffnen, desto misstrauischer sollte man sein. Auch geschenkte USB-Sticks oder CDs sind potenziell gefährlich (Abb. 31.3).
4. ZWEI-FAKTOR-AUTHENTIFIZIERUNG!
   Zwei-Faktor-Authentifizierung einsetzen, wo immer möglich (Abb. 31.4).
5. VERSCHIEDENE PASSWÖRTER!
   Vertrauen ist gut, mehrere Passwörter sind besser! Jedes Passwort nur bei einem Online-Account oder Programm verwenden, und Passwörter kompliziert wählen. Passwort-Manager mit einem guten Master-Passwort können helfen, komplizierte Passwörter zu erzeugen und zu speichern. Webbrowser sollten Passwörter nicht speichern, da sonst auch Schadsoftware darauf zugreifen kann. Wer Passwörter doch in Webbrowsern gespeichert werden, dann nur mit Master-Passwort und eingestellter Verschlüsselung der Passwörter (Abb. 31.5).

Abb. 31.3 Nicht unbedacht auf Links und Anhänge klicken

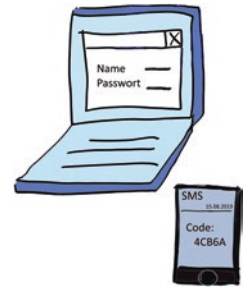

Abb. 31.4 2FA verwenden

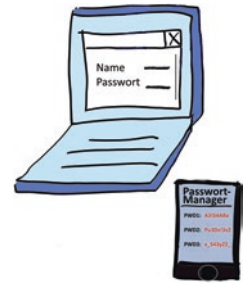

Abb. 31.5 Unterschiedliche Passwörter benutzen

31.2.2 Weitere Datenschutztipps

6. E-MAIL-ABRUF VERSCHLÜSSELN:
   Wenn E-Mails benutzt werden zum Erhalt von Links oder PINs, um sich bei einem Online-Account anzumelden oder das Passwort neu zu setzen, sollte das Passwort zum Abruf von E-Mails komplex gewählt sein und der Abruf der E-Mail verschlüsselt geschehen.
7. SICHERHEITSFRAGEN FALSCH BEANTWORTEN:
   Sicherheitsfragen für Online-Accounts besser umgehen oder falsche Angaben machen, die man sich merkt, aufschreibt oder im Passwort-Manager speichert.
8. WLAN NUR MIT PASSWORT:
   Keine WLAN-Verbindungen nutzen, die ohne Passwort eingerichtet sind. Eigenes WLAN-Netz zu Hause oder im Büro mit einem starken Passwort schützen.
9. NICHT ALS ADMIN ARBEITEN:
   Nicht ständig mit dem Administrator-Konto arbeiten.
10. UNGEWÖHNLICHES BEMERKEN:
    Unübliches Verhalten des PCs oder des Handys kann auf Hacking oder Viren hindeuten.
11. GESUNDER MENSCHENVERSTAND:
    Vorsichtig sein mit seinen Daten, seinen Passwörtern und seinen Aktionen im Internet.

31.2.3 Passwort-Empfehlungen

1. MEHR ALS EIN PASSWORT:
   Unterschiedliche Konten brauchen unterschiedliche Passwörter.
2. BEI VERDACHT WECHSELN:
   Regelmäßig bei https://haveibeenpwdned.com (22.12.2019) prüfen, ob die eigenen E-Mail-Adressen bei großen Hackingfällen gestohlen wurden. Bei Verdacht auf Missbrauch wird empfohlen, das Passwort zu ändern. Auch wenn man das Passwort bereits mehrere Monate oder Jahre benutzte, lohnt sich ein Wechsel.
3. LANGE PASSWÖRTER:
   Mind. 8 Zeichen lang, 12 und mehr werden empfohlen. Vorteilhaft sind Passphrasen, Anfangsbuchstaben eines Satzes oder künstlich erzeugte Passwörter mit Zahlen, Sonderzeichen sowie Groß- und Kleinbuchstaben.
4. SCHWIERIGE PASSWÖRTER VERWENDEN:
   Keine häufig benutzten Passwörter benutzen, wie z. B. Hallo, Password, Passwort, 123456, 12345678, 1234, 12345, qwertz, abc123, 111111, Urlaub, hallo123, passwort1, Schatz etc. Auch keine echten Daten für das Passwort benutzen, wie z. B. Name des Partners, Geburtsdatum, Name der Katze oder ein Wort, welches in Lexika vorkommt. Nach den meist benutzten Passwörtern im Internet suchen und keine davon benutzen.

Tab. 31.1 Beispiele für starke und schwache Passwörter und Passwortsätze im Vergleich

Schwaches Passwort	Ferien2020	Wort aus dem Wörterbuch zusammen mit einer Zahl
Starkes Passwort	Ig3xnB,udS2020zg!	Abkürzung des Satzes „Ich gehe dreimal nach Berlin, um den Sommer 2020 zu genießen!“
Schwacher Passwortsatz	Sein oder Nichtsein, das ist hier die Frage	Bekannter Satz aus W. Shakespeares Hamlet
Starker Passwortsatz	Hund auf Mond war lachender Igel	Zufällig gewählte Wörter, die einen komischen Satz bilden

5. PASSWÖRTER GEHEIM HALTEN:
   Niemals ein eigenes Passwort mitteilen. Das eigene Passwort nie in eine Suchmaschine eintippen, um zu prüfen, ob dieses bereits verwendet wurde (Tab. 31.1).

ASCII-Tabelle

32

Zeichen	Dez	Hex	Oct	Bin
(Steuercode)	001	1	1	1
(Steuercode)	002	2	2	10
(Steuercode)	003	3	3	11
(Steuercode)	004	4	4	100
(Steuercode)	005	5	5	101
(Steuercode)	006	6	6	110
Ton	007	7	7	111
Backspace	008	8	10	1000
Horiz. Tab	009	9	11	1001
Nächste Zeile	010	A	12	1010
Vert. Tab	011	B	13	1011
Seitenvorschub	012	C	14	1100
Zeilen-Anfang	013	D	15	1101
(Steuercode)	014	E	16	1110
(Steuercode)	015	F	17	1111
(Steuercode)	016	10	20	10000
(Steuercode)	017	11	21	10001
(Steuercode)	018	12	22	10010
(Steuercode)	019	13	23	10011
(Steuercode)	020	14	24	10100
(Steuercode)	021	15	25	10101
(Steuercode)	022	16	26	10110
(Steuercode)	023	17	27	10111
(Steuercode)	024	18	30	11000
(Steuercode)	025	19	31	11001
(Steuercode)	026	1A	32	11010
ESC	027	1B	33	11011
(Steuercode)	028	1C	34	11100
(Steuercode)	029	1D	35	11101
(Steuercode)	030	1E	36	11110
(Steuercode)	031	1F	37	11111

Zeichen	Dez	Hex	Oct	Bin
Leertaste	032	20	40	100000
!	033	21	41	100001
"	034	22	42	100010
#	035	23	43	100011
$	036	24	44	100100
%	037	25	45	100101
&	038	26	46	100110
'	039	27	47	100111
(	040	28	50	101000
)	041	29	51	101001
*	042	2A	52	101010
+	043	2B	53	101011
,	044	2C	54	101100
-	045	2D	55	101101
.	046	2E	56	101110
/	047	2F	57	101111
0	048	30	60	110000
1	049	31	61	110001
2	050	32	62	110010
3	051	33	63	110011
4	052	34	64	110100
5	053	35	65	110101
6	054	36	66	110110
7	055	37	67	110111
8	056	38	70	111000
9	057	39	71	111001
:	058	3A	72	111010
;	059	3B	73	111011
<	060	3C	74	111100
=	061	3D	75	111101
>	062	3E	76	111110
?	063	3F	77	111111

Abb. 32.1 ASCII-Zeichen und Umrechnungen von Dezimal zu Hexadezimal zu Oktal und zu Binär (Windows-Version)

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z*,
https://doi.org/10.1007/978-3-662-60911-8_32

Zeichen	Dez	Hex	Oct	Bin
@	064	40	100	1000000
A	065	41	101	1000001
B	066	42	102	1000010
C	067	43	103	1000011
D	068	44	104	1000100
E	069	45	105	1000101
F	070	46	106	1000110
G	071	47	107	1000111
H	072	48	110	1001000
I	073	49	111	1001001
J	074	4A	112	1001010
K	075	4B	113	1001011
L	076	4C	114	1001100
M	077	4D	115	1001101
N	078	4E	116	1001110
O	079	4F	117	1001111
P	080	50	120	1010000
Q	081	51	121	1010001
R	082	52	122	1010010
S	083	53	123	1010011
T	084	54	124	1010100
U	085	55	125	1010101
V	086	56	126	1010110
W	087	57	127	1010111
X	088	58	130	1011000
Y	089	59	131	1011001
Z	090	5A	132	1011010
[	091	5B	133	1011011
\	092	5C	134	1011100
]	093	5D	135	1011101
^	094	5E	136	1011110
_	095	5F	137	1011111

Zeichen	Dez	Hex	Oct	Bin
`	096	60	140	1100000
a	097	61	141	1100001
b	098	62	142	1100010
c	099	63	143	1100011
d	100	64	144	1100100
e	101	65	145	1100101
f	102	66	146	1100110
g	103	67	147	1100111
h	104	68	150	1101000
i	105	69	151	1101001
j	106	6A	152	1101010
k	107	6B	153	1101011
l	108	6C	154	1101100
m	109	6D	155	1101101
n	110	6E	156	1101110
o	111	6F	157	1101111
p	112	70	160	1110000
q	113	71	161	1110001
r	114	72	162	1110010
s	115	73	163	1110011
t	116	74	164	1110100
u	117	75	165	1110101
v	118	76	166	1110110
w	119	77	167	1110111
x	120	78	170	1111000
y	121	79	171	1111001
z	122	7A	172	1111010
{	123	7B	173	1111011
|	124	7C	174	1111100
}	125	7D	175	1111101
~	126	7E	176	1111110
Löschen	127	7F	177	1111111

Abb. 32.2 ASCII-Zeichen und Umrechnungen von Dezimal zu Hexadezimal zu Oktal und zu Binär (Windows-Version)

Zeichen	Dez	Hex	Oct	Bin
Ç	128	80	200	10000000
ü	129	81	201	10000001
é	130	82	202	10000010
â	131	83	203	10000011
ä	132	84	204	10000100
à	133	85	205	10000101
ă	134	86	206	10000110
ç	135	87	207	10000111
ê	136	88	210	10001000
ë	137	89	211	10001001
è	138	8A	212	10001010
ï	139	8B	213	10001011
î	140	8C	214	10001100
ì	141	8D	215	10001101
Ä	142	8E	216	10001110
Å	143	8F	217	10001111
É	144	90	220	10010000
æ	145	91	221	10010001
Æ	146	92	222	10010010
ô	147	93	223	10010011
ö	148	94	224	10010100
ò	149	95	225	10010101
û	150	96	226	10010110
ù	151	97	227	10010111
ÿ	152	98	230	10011000
Ö	153	99	231	10011001
Ü	154	9A	232	10011010
ø	155	9B	233	10011011
£	156	9C	234	10011100
Ø	157	9D	235	10011101
×	158	9E	236	10011110
ƒ	159	9F	237	10011111

Zeichen	Dez	Hex	Oct	Bin
á	160	A0	240	10100000
í	161	A1	241	10100001
ó	162	A2	242	10100010
ú	163	A3	243	10100011
ñ	164	A4	244	10100100
Ñ	165	A5	245	10100101
ª	166	A6	246	10100110
º	167	A7	247	10100111
¿	168	A8	250	10101000
®	169	A9	251	10101001
¬	170	AA	252	10101010
½	171	AB	253	10101011
¼	172	AC	254	10101100
¡	173	AD	255	10101101
«	174	AE	256	10101110
»	175	AF	257	10101111
▒	176	B0	260	10110000
▒	177	B1	261	10110001
▓	178	B2	262	10110010
▏	179	B3	263	10110011
┤	180	B4	264	10110100
Á	181	B5	265	10110101
Â	182	B6	266	10110110
À	183	B7	267	10110111
©	184	B8	270	10111000
╣	185	B9	271	10111001
▌	186	BA	272	10111010
╗	187	BB	273	10111011
╝	188	BC	274	10111100
¢	189	BD	275	10111101
¥	190	BE	276	10111110
┐	191	BF	277	10111111

Abb. 32.3 ASCII-Zeichen und Umrechnungen von Dezimal zu Hexadezimal zu Oktal und zu Binär (Windows-Version)

Zeichen	Dez	Hex	Oct	Bin
└	192	C0	300	11000000
┴	193	C1	301	11000001
┬	194	C2	302	11000010
├	195	C3	303	11000011
─	196	C4	304	11000100
┼	197	C5	305	11000101
ã	198	C6	306	11000110
Ã	199	C7	307	11000111
╚	200	C8	310	11001000
╔	201	C9	311	11001001
╩	202	CA	312	11001010
╦	203	CB	313	11001011
╠	204	CC	314	11001100
═	205	CD	315	11001101
╬	206	CE	316	11001110
¤	207	CF	317	11001111
ð	208	D0	320	11010000
Ð	209	D1	321	11010001
Ê	210	D2	322	11010010
Ë	211	D3	323	11010011
È	212	D4	324	11010100
ı	213	D5	325	11010101
Í	214	D6	326	11010110
Î	215	D7	327	11010111
Ï	216	D8	330	11011000
┘	217	D9	331	11011001
┌	218	DA	332	11011010
█	219	DB	333	11011011
▄	220	DC	334	11011100
¦	221	DD	335	11011101
Ì	222	DE	336	11011110
▀	223	DF	337	11011111

Zeichen	Dez	Hex	Oct	Bin
Ó	224	E0	340	11100000
ß	225	E1	341	11100001
Ô	226	E2	342	11100010
Ò	227	E3	343	11100011
õ	228	E4	344	11100100
Õ	229	E5	345	11100101
µ	230	E6	346	11100110
þ	231	E7	347	11100111
Þ	232	E8	350	11101000
Ú	233	E9	351	11101001
Û	234	EA	352	11101010
Ù	235	EB	353	11101011
ý	236	EC	354	11101100
Ý	237	ED	355	11101101
¯	238	EE	356	11101110
´	239	EF	357	11101111
-	240	F0	360	11110000
±	241	F1	361	11110001
‗	242	F2	362	11110010
¾	243	F3	363	11110011
¶	244	F4	364	11110100
§	245	F5	365	11110101
÷	246	F6	366	11110110
¸	247	F7	367	11110111
°	248	F8	370	11111000
¨	249	F9	371	11111001
·	250	FA	372	11111010
¹	251	FB	373	11111011
³	252	FC	374	11111100
²	253	FD	375	11111101
■	254	FE	376	11111110
	255	FF	377	11111111

Abb. 32.4 ASCII-Zeichen und Umrechnungen von Dezimal zu Hexadezimal zu Oktal und zu Binär (Windows-Version)

HTTP Status Code Definitionen

33

Tab. 33.1 Liste der HTTP-Status-Codes

Informational 1xx	
100	Continue
101	Switching Protocols
Successful 2xx	
200	OK
201	Created
202	Accepted
203	Non-Authoritative Information
204	No Content
205	Reset Content
206	Partial Content
Redirection 3xx	
300	Multiple Choices
301	Moved Permanently
302	Found
303	See Other
304	Not Modified
305	Use Proxy
306	(Unused)
307	Temporary Redirect

(Fortsetzung)

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z*,
https://doi.org/10.1007/978-3-662-60911-8_33

Tab. 33.1 (Fortsetzung)

Client Error 4xx	
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Request Entity Too Large
414	Request-URI Too Long
415	Unsupported Media Type
416	Requested Range Not Satisfiable
417	Expectation Failed
Server Error 5xx	
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version Not Supported

Quelle: w3.org *(Abgerufen am 22.12.2019)*

RegEx Übersicht

34

Tab. 34.1 RegEx Übersicht

RegEx String	Erklärung		RegEx String	Erklärung
.	Alle Zeichen außer Codes für „nächste Zeile“		(?:abc)	Gruppe, die nicht vorhanden sein darf
a	Zeichen a		\1	Referenz zur Gruppe 1
xy	String xy		a* b+ c?	0 oder mehr Mal a, 1 oder mehr Mal b, 0- oder 1-mal c
\w \d \s	Ein Wort, eine Zahl, ein Space		a{5} b{3;}	Genau fünf Mal a, drei oder mehr Mal b
\W \D \S	Kein Wort, keine Zahl, kein Space		a{1;3}	Zwischen ein und drei Mal a
[abc]	Eines der Zeichen a, b, oder c		a|b	a oder b
[^abc]	Keines der Zeichen a, b, oder c		ab|yz	ab oder yz
[^ax-z]	Ein Zeichen ohne a, x, y, z		i	Groß-/Kleinschreibung ignorieren
[a-k]	Ein Zeichen zwischen a und k		^ $	Start und Ende einer Zeile
[ab-e]	Entweder a, b, c, d oder e		a.b	a gefolgt von einem anderen Buchstaben gefolgt von b
^abc$	Start und Ende des Strings abc		a.*b	a gefolgt von mehreren Buchstaben gefolgt von b
\. * \\	Eingabe von Spezial-Zeichen		[ab]+	a, b, aa, ab, aaaba, abab, etc.
\b \t \n \r	Backspace, Tabulator, nächste Zeile, Zeilenvorschub		(abc)	Gruppieren

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_34

Markdown-Übersicht

35

Tab. 35.1 Markdown-Übersicht

Eine Leerzeile ergibt einen neuen Absatz		Horizontale Linie: - - -
Zwei Leerzeichen am Ende der Zeile ␣␣ ergeben einen Zeilenumbruch		* Listeneintrag * Listeneintrag ␣␣␣␣* Eingerückter Listeneintrag
␣␣␣␣Vier Leerzeichen am Anfang der Zeile ergeben eine Einrückung des Absatzes		1. Geordneter Listeneintrag 2. Geordneter Listeneintrag ␣␣␣␣1. Eingerückter, geordneter Listeneintrag
Kursiv		> Zitat
Fett		`Code-Block`
Fett und kursiv		*Text zwischen Sternchen*
~~Durchstreichen~~		Tabelle mit Spaltenüberschriften, links-, zentriert-, rechtsbündigen Spalten sowie verbundene Zellen: |Spalte 1|Spalte 2|Spalte 3| |:- - - - - - |:- - - - - - -:|- - - - - - -:| |Zeile 1|Zeile 1|Zeile 1| |Verbundene Zeile 2||Zeile 2|
Link: [Link-Text](URL „Optionaler Titel“)		
Bild: ![Alt-Text](URL „Optionaler Titel“)		
# Überschrift 1 ## Überschrift 2 ### Überschrift 3		

R. Porath, *Internet, Cyber- und IT-Sicherheit von A–Z,*
https://doi.org/10.1007/978-3-662-60911-8_35