Cyber-Glossar – Do you speak “Cyber”?

Wichtige Begriffe aus der Cyber-Welt verständlich erklärt

Die in diesem Glossar verwendeten Beispiele dienen lediglich der Verdeutlichung der einzelnen Begrifflichkeiten. Sie sollen demnach nur eine Orientierungshilfe bieten und stellen keine rechtlich bindenden Aussagen dar. Die Inhalte dieses Dokuments wurden mit größtmöglicher Sorgfalt recherchiert. Eine Haftung für die Richtigkeit, Vollständigkeit und Aktualität kann jedoch nicht übernommen werden.

Inhalt

A

Ad Blocker:

Eine **Browsererweiterung** (Plugin/Extension), die verhindern soll, dass Werbung auf Websites angezeigt wird. Einige Ad Blocker beinhalten jedoch auch Spyware, umgehen somit den Datenschutz der Nutzer und werten gesammelte Daten aus.

Anonymizer:

Sammelbegriff für Lösungen, die Personen die unerkannte Nutzung von Online-Diensten ermöglichen. Häufig wird die Anonymität gewährleistet, indem zwischen besuchter Website und Nutzer ein weiterer Umweg (Server) in die Verbindung eingebaut wird. Jedoch werden auf diesen zwischengeschalteten Servern oft Verbindungsdaten protokolliert. Dann ist keine komplette Anonymität gewährleistet. Wichtig ist in jedem Fall die Verschlüsselung (SSL/TLS), damit das Abhören der Verbindung zwischen Nutzer und Proxy verhindert wird.

Application Programming Interface (API):

Die Abkürzung für „**Application Programming Interface**“. Übersetzt bedeutet das „**Programmschnittstelle**“. Über ein API können Entwickler auf die Funktionen einer Anwendung zugreifen. So könnte man es vereinfacht ausdrücken: Wenn Software B automatisch Informationen von Software A abrufen und nutzen kann, dann handelt es sich bei der dafür notwendigen Schnittstelle um die sogenannte API.

Advanced Persistent Thread (APT):

„Advanced Persistent Threats“ (APT) sind **zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen,** bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen auf weitere Systeme ausweitet. Hierzu sind hohe Ressourceneinsätze und erhebliche technische Fähigkeiten aufseiten der Angreifer nötig.

Antivirus Software:

Antivirus Software ist ein **wichtiger Bestandteil der Informationssicherheit** und soll Computersysteme vor schädlicher Software wie Viren, Würmern und Trojanern schützen. Die Software arbeitet in der Regel, indem sie schädlichen Code auf einem Computersystem erkennt und entfernt. Es ist wichtig, Antiviren Software regelmäßig zu aktualisieren und zu überprüfen, um einen umfassenden Schutz zu gewährleisten.

Authentifizierung:

Bei der Authentifizierung wird **die Identität eines Benutzers oder einer Anwendung überprüft**. Dies kann durch Passwörter, biometrische Identifikation oder andere Identifikationsmethoden erfolgen. Eine effektive Authentifizierung ist wichtig, um unbefugten Zugriff auf Computersysteme oder vertrauliche Daten zu verhindern.

B

Botnetze:

Als „Botnetz“ bezeichnet man einen **Verbund von Rechnern (Systemen), die von einem fernsteuerbaren Schadprogramm (Bot)** befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert. Oft bestehen diese Botnets aus tausenden gekaperten Geräten (dabei muss es sich nicht um Computer handeln). Auch andere Geräte wie Kameras, Smartphones, Netzwerkdrucker sowie IoT-Geräte können zu Bots werden.

Backdoor:

Bildlich gesprochen: Eine **Hintertür, um sich Zugang zu einem geschützten Bereich zu verschaffen**. Man geht also nicht durch die gesicherte und verschlossene Haustür, sondern geht einmal um das Haus herum und kommt herein beziehungsweise bricht ein.

Black Had Hacker

Black Hat Hacker sind Kriminelle, die in böser Absicht in Computernetzwerke eindringen. Gelegentlich bringen sie auch Malware in Umlauf, die Dateien zerstört, Computer als Geiseln nimmt oder Passwörter, Kreditkarten- und andere personenbezogenen Daten stiehlt.

Dabei handeln Black Hats aus reinem Eigennutzen, streben nach finanziellem Gewinn, leben Rachegelüste aus oder wollen einfach nur Chaos verursachen. In manchen Fällen ist ihr Handeln auch ideologisch motiviert und richtet sich gegen Andersdenkende.

Browser:

Webbrowser oder allgemein auch **Browser** (engl. „*to browse*“ = „stöbern, schmökern, umsehen“, auch „abgrasen“) sind spezielle Computerprogramme zur Darstellung von Webseiten im World Wide Web oder allgemein von Dokumenten und Daten.

Brute-Force-Angriff:

Bei einem Brute-Force-Angriff **versuchen Hacker mittels Software ein Passwort zu entschlüsseln**. Es handelt sich dabei um einen sehr einfachen Algorithmus, der in schneller Abfolge möglichst viele verschiedene Zeichenkombinationen ausprobiert. Man spricht deshalb auch von der „erschöpfenden Suche“. Ein Hochleistungsrechner führt sehr viele Berechnungen pro Sekunde aus und kann so eine entsprechend hohe Anzahl an Kombinationen in kürzester Zeit austesten. Je nach Länge und Komplexität eines Passworts kann das Knacken des Passworts nur ein paar Sekunden dauern oder viele Jahre.

C

CEO Fraud:

Beim CEO Fraud (= **CEO-Betrug**) handelt es sich um eine **Variante des so genannten Social Engineerings, das die Schwachstelle Mensch ausnutzt**. Bei dieser Betrugsmasche gibt sich der Täter zum Beispiel in einer E-Mail als Vorgesetzter aus und veranlasst einen entscheidungsbefugten Mitarbeiter des Unternehmens dazu, hohe Geldbeträge (ins Ausland) zu überweisen. Die Täter täuschen vor, der Auftrag käme unmittelbar vom Chef des Unternehmens (z. B. vom CEO = Chief Executive Officer).

CSRF:

„Cross-Site Request Forgery“ ist eine weitere Angriffsform, die sich gegen Benutzer von Webanwendungen richtet. Mit dieser Vorgehensweise lassen sich Funktionen einer Webanwendung von einem Angreifer im Namen des Opfers nutzen. Ein Beispiel ist die Versendung einer gefälschten Statusnachricht in einem sozialen Netzwerk: Ein Angreifer formuliert die Nachricht und schiebt sie dem Opfer beim Abruf einer Webseite unter. Wenn der Angriff gelingt und das Opfer während des Angriffs parallel im betreffenden sozialen Netzwerk angemeldet ist, wird die Nachricht des Angreifers im Namen des Opfers veröffentlicht.

Cookie:

Ein Cookie ist eine **kleine, von einem Webserver auf einem lokalen Rechner abgelegte Textdatei**, die Daten über das Surf-Verhalten des Nutzers enthält (z.B. Spracheinstellungen oder Artikel im Warenkorb). Cookies

helfen dabei, die User Experience zu verbessern, aber sie können auch Nutzerverhalten aufzeichnen und Informationen an Webseiten von Dritten ohne das Einverständnis des Users weitergeben.

Chosen-Plaintext-Attacke:

Kryptografischer Angriff, in dem der Angreifer Zugriff auf Chiffrate zu von ihm gewählten Klartexten erhalten kann.

Cyber War:

Cyber War, oft auch als Cyber Warfare oder **Cyber-Krieg** bezeichnet, beinhaltet alle Tätigkeiten, welche **von einem Staat oder einer Organisation** ausgeführt werden, um Systeme oder Informationsnetzwerke einer anderen Nation oder Organisation anzugreifen oder in diese einzudringen. Verbreitete Techniken, um dies zu erreichen, sind **Denial-of-Service**-Angriffe oder ferngesteuerte Malware.

Cyber-Raum:

Der Cyber-Raum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyber-Raum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.

Cyber security:

Computersicherheit beziehungsweise Computerkriminalität stehen in einem engen Zusammenhang zueinander. Ist der Computer geschützt, kann der Kriminelle nicht an die Daten heran. Wird ein nicht hinreichend gesicherter Computer angegriffen, kann ein großer Schaden entstehen. Cyber-Kriminelle fangen Daten ab und verschaffen sich Zugang zu Systemen. Häufig werden Zahlungssysteme kompromittiert, so dass der Nutzer zudem noch finanziellen Schaden erleidet.

Cyber crime as a Service

Cyber crime as a Service (CaaS)“ ist ertragreich und ein **etabliertes Geschäftsmodell**. Über **CaaS-Plattformen im „Darknet“** werden die Schritte, die für einen erfolgreichen Angriff notwendig sind, von spezialisierten und unabhängigen Tätergruppen erbracht. Der Trend zur arbeitsteiligen Professionalisierung cyber-krimineller Dienstleistungen hält an. Kriminelle Gruppen betreiben straff geführte Organisationen und Affiliate-Programme haben sich als Hauptgeschäftsform etabliert.

Der Erfolg eines Angriffs hängt wesentlich von der Qualität dieser Orchestrierung ab. Der erleichterte und kostengünstige Zugang zu hochwertigen Cyber-crime-Dienstleistungen in Form von „Rundum-Sorglos-Paketen“ führt zu einer beschleunigten **Demokratisierung von** Cyber-Angriffen. **„CaaS“-Pakete sind für niedrige zweistellige US-Dollarbeträge pro Monat erhältlich.**

D

Denial-of-Service-(DoS)- und Distributed-Denial-of-Service-(DDoS)-Attacke:

Eine künstlich herbeigeführte Überlastung eines Webservers oder Datennetzes – gesteuert von Cyber-Kriminellen. Im Gegensatz zu einer einfachen **Denial-of-Service-Attacke (DoS)** haben **Distributed-Denial-of-Service-Attacken (DDoS)** eine immense Schlagkraft. Mehrere Computer greifen dabei gleichzeitig und im Verbund (Botnetze) eine Webseite oder eine ganze Netzinfrastruktur an. Dies kann sehr schnell zum Ausfall der Server führen, da das Zielsystem überlastet ist und zusammenbricht.

Datensicherung:

Bei einer Datensicherung werden **zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt**. Sie umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung

der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

Datenmissbrauch:

Viele Unternehmen verarbeiten und speichern Kunden-/Besucherdaten. Kommen diese in falsche Hände und/oder werden die dort dokumentierten Daten zu kriminellen Zwecken missbraucht, löst dies ebenfalls ein Cyber-Schadenereignis aus. Hier ist mit **Kosten wegen der Verletzung der Vertraulichkeit oder des Datenschutzes** zu rechnen.

Datenverschlüsselung:

Datenverschlüsselung ist eine **Methode zum Schutz von Daten durch Umwandlung der Daten in eine unlesbare Form**, die nur mit einem speziellen Schlüssel entschlüsselt werden kann. Eine wirksame Datenverschlüsselung kann dazu beitragen, die Vertraulichkeit von Daten zu gewährleisten und die Datenintegrität zu schützen.

Disaster Recovery:

Disaster Recovery meint Maßnahmen zum **Wiederherstellen gelöschter Dateien oder anderer IT-Dienste**, die durch eine Katastrophe wie Brände, Überschwemmungen, Stromausfälle oder Cyber-Angriffe (zum Beispiel durch Erpressertrojaner) gelöscht, verschlüsselt oder unbrauchbar geworden sind.

DNS-Spoofing

DNS ist das „Domain Name System“, bei dem eine Website mit der IP-Adresse des Webservers verknüpft wird. Mit DNS-Spoofing (dt. DNS-Täuschung) manipulieren Angreifende die IP-Adresse, die zu einer Website gehört. Nutzende besuchen dann eine vermeintlich vertrauenswürdige Internetseite, werden aber auf eine gefälschte weitergeleitet. Dabei können sensible Daten abgegriffen oder schädliche Programme heruntergeladen werden.

Digital Trust

Digital Trust bezeichnet das Vertrauen in die Sicherheit und Zuverlässigkeit digitaler Technologien und Dienstleistungen. Es ist die Grundlage der digitalen Wirtschaft.

Was umfasst Digital Trust?

- Datenschutz
- Cyber-Sicherheit
- Datenintegrität
- Ethische Nutzung von Technologien
- Rechenschafts- und Aufsichtspflicht
- Inklusive, ethische und verantwortungsvolle Nutzung

Wie wird Digital Trust sichergestellt?

- Durch die Implementierung von technischen und organisatorischen Maßnahmen
- Durch die Einhaltung von Branchen- und Technologie-Standards

- Durch die Einhaltung von Compliance- und Betriebsvorschriften
- Durch die Nutzung von Software, die das Management von Vertrauen innerhalb einer Organisation ermöglicht
- Durch die Erweiterung des Vertrauens über Ökosysteme

Herausfordernd für Digital Trust sind unter anderem: Informationssicherheit, Datenschutz, Digitalisierung hin zu Künstlicher Intelligenz und Roboterisierung.

E

Entschlüsselung:

Vorgang, bei dem unter Verwendung mathematischer Algorithmen und privater oder geheimer Schlüssel **elektronische Daten wieder les- bzw. verarbeitbar gemacht werden**. In verschlüsselter Form sind die Daten von unbefugten Dritten nicht einsehbar. Die Daten können nur vom Besitzer des entsprechenden privaten oder geheimen Schlüssels wieder in die Originalform überführt werden.

E-Mail Spoofing:

E-Mail Spoofing bezeichnet das **Erstellen und Versenden von E-Mails mit gefälschtem Absender**.

F

Fuzzing:

„Fuzzing“ ist eine **automatisierte Testmethode für Software**, bei der ein Programm eine Vielzahl automatisch generierter Eingabedaten verarbeiten muss, ohne dabei eine Fehlfunktion zu zeigen. Findet ein Hacker durch Fuzzing ein Eingabemuster, das eine Fehlfunktion erzeugt, muss überprüft werden, ob sich der gefundene Fehler als Sicherheitslücke ausnutzen lässt.

Fake President:

Bezeichnet eine Betrugsmethode **(„Enkeltrick“)**, bei der E-Mails mit angeblichen Transaktionsanordnungen bzw. **Aufforderung zu bestimmten Handlungen im Namen des Firmenchefs an Mitarbeiter des Unternehmens** geschickt werden. Diese Betrugsmethode kommt sehr häufig vor, weil die E-Mail-Adressen im Internet öffentlich zugänglich sind.

Face Swapping:

„Face Swapping“ – wird zu einem wichtigen Werkzeug für Cyber-Kriminelle. So werden beispielsweise KI-generierte Avatare von realen Entscheidungsträgern eines Unternehmens während eines Videotelefonats von Angreifern gesteuert und die angerufenen ahnungslosen Mitarbeitenden zu schädlichen Handlungen überredet.

Fake Invoice:

Fake-Rechnungen. Manchmal macht man alles richtig, und dennoch schlagen die Hacker zu. So erging es einem Handwerksbetrieb aus Berlin: In seinem Namen wurden Rechnungen an Kunden geschickt, die diese auch umgehend beglichen. Misstrauen entstand nicht, denn die Kunden hatten tatsächlich mit diesem Dienstleister in der jüngsten Vergangenheit zusammengearbeitet.

Firewall:

Eine Firewall ist eine **Schutzbarriere zwischen einem Computersystem oder Netzwerk und dem Internet**. Sie kontrolliert den Zugriff auf das System oder Netzwerk und blockiert unerwünschten Netzwerkverkehr. Eine effektive Firewall sollte regelmäßig aktualisiert und überwacht werden, um potenzielle Schwachstellen zu erkennen und zu beheben.

G

Geheimer Schlüssel:

Geheime Schlüssel werden im **Zusammenhang mit symmetrischen Krypto-Algorithmen** verwendet. Im Gegensatz zu den asymmetrischen Krypto-Algorithmen eingesetzten privaten Schlüsseln ist das gesamte Schlüsselmaterial bekannt.

Grey Had Hacker

Ein Gray Hat Hacker ist ein Computer-Experte, der sich zwischen legalen und illegalen Handlungen bewegt. Er bricht in Systeme ein, um Schwachstellen zu finden, ohne dabei böse Absichten zu verfolgen.

H

HTTPS:

Hyper Text Transfer Protocol Secure (HTTPS, englisch für **„sicheres Hypertext-Übertragungsprotokoll“**) ist ein Protokoll im World Wide Web, um Daten abhörsicher zu übertragen.

HTTP:

Das **„Hyper Text Transfer Protocol“** HTTP ist im Gegensatz zu HTTPS **nicht verschlüsselt**. Daten, die mit diesem Protokoll übertragen werden, können leicht von Dritten gelesen oder manipuliert werden. Wenn Sie schützenswerte Informationen über das Internet austauschen, ist eine verschlüsselte Verbindung wie z. B. HTTPS sehr empfehlenswert.

HTML:

Hyper Text Markup Language (HTML) ist eine **Auszeichnungssprache zur Erstellung von Webseiten**. Es ist eine Kerntechnologie des Internets. HTML-Dokumente enthalten Informationen für den Benutzer und auch Instruktionen für den Browser zur Darstellung dieser Informationen.

Hacker:

Beschäftigen sich mit Sicherheitsmechanismen und deren Schwachstellen. Während der Begriff auch diejenigen beinhaltet, die Sicherheitslücken suchen, um sie aufzuzeigen oder zu korrigieren, wird er von den Massenmedien und in der allgemeinen Öffentlichkeit häufiger für Personen benutzt, die unerlaubt in fremden Systemen solche Lücken ausnutzen.

Hardware:

Ist der Oberbegriff für die **physischen Komponenten** (die elektronischen und mechanischen Bestandteile) **eines datenverarbeitenden Systems**.

IT-Forensik:

Die „IT-Forensik“ befasst sich mit der **Untersuchung, Analyse und Aufklärung von Sicherheitsvorfällen im Zusammenhang mit IT-Systemen.**

Informationssicherheit:

Die Informationssicherheit befasst sich mit der **Erhaltung von Vertraulichkeit, Integrität und Verfügbarkeit von Information**. Außerdem können auch andere Eigenschaften wie Echtheit, Zurechenbarkeit, Nachweisbarkeit und Zuverlässigkeit abgedeckt werden (ISO/IEC 27000). Information kann dabei z.B. in elektronischer, gedruckter oder gesprochener Form vorliegen. Die IT-Sicherheit stellt eine Unterkategorie der Informationssicherheit dar.

IT-Security Roadmap:

Eine IT Security Roadmap oder Information Security Roadmap) **definiert einen Fahrplan und zugehörige Informationssicherheitsaktivitäten**, um kontinuierlich und nachhaltig die Sicherheit im Unternehmen zu erhöhen.

Identitätsdiebstahl:

Beim Identitätsdiebstahl werden **gestohlene oder betrügerisch erlangt Identitätsinformationen** verwendet, um sich als eine andere Person auszugeben. Dies kann **schwerwiegende finanzielle Folgen** haben, da die Täter häufig auf den Namen der Opfer Kredite aufnehmen oder andere betrügerische Aktivitäten durchführen. Um sich vor Identitätsdiebstahl zu schützen, sollten Unternehmen und Privatpersonen starke Passwörter verwenden und sensible Informationen nicht frei zugänglich machen. Darüber hinaus sollten sie ihre Kredit- und Finanzinformationen regelmäßig überprüfen, um mögliche Fälle von Identitätsdiebstahl zu erkennen.

Incident Response (Plan):

Incident Response bezieht sich auf die **Reaktion auf einen Sicherheitsvorfall oder einen Cyber-Angriff**. Ein effektiver Incident-Response-Plan sollte die Schritte enthalten, die ergriffen werden müssen, um den Angriff zu stoppen, den Schaden zu minimieren und das System wiederherzustellen. Dieser sollte auch klare Verfahren für die Kommunikation und Zusammenarbeit mit relevanten Parteien wie Kunden, Behörden und anderen betroffenen Parteien enthalten.

IDS/IPS-Programme:

Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS) **überwachen kontinuierlich ein Netzwerk**, erkennen potenzielle Vorfälle und protokollieren die dazugehörigen Informationen, stoppen Vorfälle und melden diese den Sicherheitsadministratoren.

K

Keylogger:

Als „Keylogger“ wird **Hard- oder Software zum Mitschneiden von Tastatureingaben** bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern, filtern.

Kumulationseffekt im IT-Grundschutz:

Der Kumulationseffekt beschreibt, dass sich der **Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden**

entstehen kann. Ein Auslöser kann auch sein, dass mehrere IT-Anwendungen bzw. eine Vielzahl sensitiver Informationen auf einem IT-System verarbeitet werden, sodass durch Kumulation von Schäden der Gesamtschaden höher sein kann.

M

Malware:

Als Malware bezeichnet man **Computerprogramme, die entwickelt wurden, um unerwünschte und gegebenenfalls schädliche Funktionen auszuführen**. Malware ist damit ein Oberbegriff, der u. a. das Computervirus umfasst. Der Begriff des Virus ist älter und häufig nicht klar abgegrenzt. So ist die Rede von *Virenschutz*, womit viel allgemeiner der Schutz vor Schadsoftware jeglicher Art gemeint ist. Ein typischer Virus verbreitet sich, während die heute gängigen Schadprogramme die Struktur von Trojanischen Pferden zeigen, deren primärer Zweck nicht die Verbreitung, sondern die Fernsteuerbarkeit ist. Malware ist ein Kunstwort, welches von Malicious Software (dt. schadhafte Software) abgeleitet wird.

Man-in-the-middle-Angriff:

Ziel bei einem „Man-in-the-Middle-Angriff“ ist es, sich **unbemerkt in eine Kommunikation zwischen zwei oder mehreren Partnern einzuschleichen**, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte“ der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt. So können sensible Daten wie Passwörter, Kontodaten oder Ähnliches direkt in die Hände des Angreifers gelangen.

MDR:

Bei MDR (Managed Detection and Response) handelt es sich um eine **ausgelagerte Sicherheitsdienstleistung: Ein externer Anbieter übernimmt im Auftrag eines Unternehmens die Überwachung von Netzwerkaktivitäten, um Cyber-Bedrohungen frühzeitig zu erkennen**. Wird ein Angriff oder eine Bedrohung entdeckt, leitet er geeignete Maßnahmen als Reaktion ein. Dazu gehören z. B. das Blockieren von Angriffen, die Isolation betroffener Systeme sowie Disaster-Recovery-Maßnahmen. Ein MDR-Dienstleister hilft, interne Ressourcen zu minimieren und verfügt häufig über mehr Fachwissen und Erfahrung im Bereich Cyber Security.

Multi-Faktor-Authentifizierung:

Multi-Faktor-Authentifizierung (MFA) ist eine **Authentifizierungsmethode, bei der der Benutzer zwei oder mehr Verifizierungsfaktoren** angeben muss, um Zugang zu einer Ressource wie einer Anwendung, einem Online-Konto oder einem VPN zu erhalten.

N

Nicknapping:

Personen treten im Internet mit ihrem realen Namen oder unter der Verwendung eines Pseudonyms oder Nicknames auf. Als „Nicknapping“ bezeichnet man einen **Cyber-Angriff, bei dem der Angreifer unter einem bekannten Namen oder Pseudonym** auftritt. Dadurch versucht der Angreifer, gegenüber Dritten den Eindruck zu erwecken, er sei der eigentliche ursprüngliche Inhaber des Namens oder des Pseudonyms. Gelingt dies, kann der Angreifer in begrenztem Maße als der eigentliche/ursprüngliche Inhaber agieren.

Next Generation Firewall (NGFW):

Im Vergleich zu einer klassischen Firewall, die Sicherheitsmaßnahmen auf Protokoll- und Port-Ebene umsetzt, bezieht die **Next Generation Firewall (NGFW)** zusätzlich auch die Anwendungsebene mit ein. Eine NGFW **analysiert den Inhalt des Datenstroms, erkennt ungewöhnliches Verhalten und filtert infizierte Dateien heraus**. Neben der Paketfilterung bieten NGFW zusätzliche Features wie spezielle Intrusion-Detection-and-

Prevention-Systeme (IPS), Application Awareness, Deep Packet Inspection (DPI), Content-Filter, Malware-Erkennung und Virenschutz.

O

Online-Händler versus Online-Handelsplattform:

Eine **Online-Handelsplattform (nicht versicherbar)** im Bereich des E-Commerce kann zum besseren Verständnis mit einem klassischen, uns bekannten realen Marktplatz verglichen werden. An einem zentralen Ort werden unterschiedliche, ähnliche, aber auch komplett gleiche Produkte von verschiedenen Händlern angeboten und dem Käufer präsentiert. Wie auf realen Marktplätzen haben Käufer die Möglichkeit, zu stöbern und zu vergleichen, ohne den tatsächlichen Ort verlassen zu müssen.

Ein **Online-Shop hingegen (versicherbar, wenn über den Online-Absatz weniger als 30 % des Gesamtumsatzes generiert werden)**, stellt in der realen Welt ein eher klassisches Einzelhandelsgeschäft dar, in dem die Produkte gezielt, von einem einzigen Händler angepriesen, vermarket und verkauft werden.

P

Phishing:

Phishing bezeichnet die illegale Methode, **über gefälschte Webseiten, per E-Mail oder Kurznachrichten persönliche Daten oder Anmeldedaten von Internetnutzern abzugreifen**. Die Daten eines Benutzers werden dann für betrügerische Aktionen genutzt (Identitätsdiebstahl, Kontoplünderung, usw.).

Was ist Payment Diversion?

Kriminelle geben sich als Mitarbeitende, Lieferanten oder Geschäftspartner, mit denen das Unternehmen zusammenarbeitet, aus und erreichen durch manipulierte Mitteilungen oder Rechnungen, dass die Bezahlung für erbrachte Dienstleistungen oder Waren auf abweichende Konten erfolgt (Umleitung von Zahlungsströmen / Bestellerbetrug).

Personenbezogene / Personenidentifizierbare Daten

Nach europäischem Recht und Bundesdatenschutzgesetz (BDSG) und im Sinne der **Datenschutzgrundverordnung (DSGVO)** sind personenbezogene Daten alle Daten, die sich **einer bestimmten oder bestimmbaren natürlichen Person** zuordnen lassen und so Rückschlüsse auf deren Persönlichkeit erlauben. **Personenbezogene Daten** sind zum Beispiel:

- Name,
- Geburtsdatum und Alter,
- Geburtsort,
- Anschrift,
- E-Mail-Adresse,
- Telefonnummer,
- Kennnummern,
- Bankdaten,
- Online-Daten,
- Kundendaten (Bestellungen, Adressdaten, Kontodaten usw.)

Daneben existieren auch noch **besondere personenbezogene Daten**, die **eines erhöhten Schutzes** bedürfen. Die Vorschriften zur Sammlung und Verarbeitung solcher Daten sind wesentlich strenger.

Besondere personenbezogene Daten sind zum Beispiel:

- rassische oder ethnische Herkunft,

- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit,
- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung.

Betroffene haben vor allem das Recht auf informationelle Selbstbestimmung. Das Speichern und Verarbeiten von personenbezogenen Daten ist mithin nur unter Zustimmung des Betroffenen zulässig. Unternehmen und öffentliche Stellen, die derlei "Datenschätze" sammeln, speichern und verarbeiten, müssen diese entsprechend **vor unbefugten Zugriffen schützen**. Zudem dürfen auch **nicht alle Daten zu jedwedem Zweck verarbeitet oder gespeichert – und schon gar nicht weitergegeben** – werden.

Plug-in:

Ein **Plug-in** (von englisch „*to plug in*“, „einstöpseln, anschließen“, auch **Software-Erweiterung** oder **Zusatzmodul**) ist eine **optionale Software-Komponente, die eine bestehende Software erweitert bzw. verändert.** Der Begriff wird teilweise auch als Synonym zu „Add-on“ und „Add-in“ benutzt. Plug-ins werden meist vom Benutzer installiert und dann von der entsprechenden Hauptanwendung während der Laufzeit eingebunden. Plug-ins können nicht ohne die Hauptanwendung ausgeführt werden.

PCI DSS:

Payment Card Industry Data Security Standard, ist ein Regelwerk im Zahlungsverkehr, das sich auf die Abwicklung von Kreditkartentransaktionen bezieht.

Proxy:

Ein Proxy ist **eine Kommunikationsschnittstelle in einem Netzwerk**. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.

Pharming:

Ist eine **Betrugsmethode**, die auf der Grundidee des Phishings beruht. Dabei wird der Benutzer durch die Nutzung von **Systemmanipulationen auf gezielt gefälschte** Webseiten umgeleitet, ohne dass er dies bemerkt. Dadurch ist es möglich, an persönliche Informationen wie z. B. Bankdaten zu gelangen.

Penetrationstest:

Bei der Durchführung eines **Penetrationstests (kurz: Pen-Test)** wenden IT-Experten gezielt Mittel und Methoden an, mit denen Hacker üblicherweise versuchen würden, unautorisiert in ein System einzudringen (es zu „penetrieren“). Der Pen-Test zeigt, wie empfindlich das System auf solche Cyber-Angriffe reagiert, deckt Gefährdungspotentiale auf und ermöglicht es, Schwachstellen zu beheben.

Patching:

Das Einspielen von **Software-Patches**, welche Fehler oder andere Probleme, wie z.B. Effizienzprobleme beheben.

R

Ransomware:

Ein **Angriff auf den eigenen Computer per schädlicher Software (Malware)**, die bösartig eingeschleust wurde. Die Malware sorgt dafür, dass der Computer infiziert wird und die Dateien auf der Festplatte und auf beschreibbaren Laufwerken verschlüsselt werden. **Der Cyber-Kriminelle verlangt Geld (BitCoins) bzw. ein**

Lösegeld (englisch: *„ransom“*) dafür, dass dieser Vorgang von ihm rückgängig gemacht wird (Erpressungssoftware). Wird das Lösegeld nicht gezahlt, besteht die Gefahr, wichtige Daten zu verlieren.

Replay-Angriffe:

„Replay-Angriffe“ beschreiben allgemein Angriffe, bei denen ein Informationsaustausch zuerst aufgezeichnet wird und die gewonnenen Informationen im Anschluss daran missbräuchlich wiederverwendet werden. Anhand eines aufgezeichneten Login-Vorgangs kann ein Angreifer beispielsweise versuchen, sich selbst unberechtigt Zugang zu dem jeweiligen System zu verschaffen.

Redirection-Angriff:

Eine Redirection-Schwachstelle liegt dann vor, wenn eine Web-Anwendung Daten von einem Benutzer verwendet, um ihn auf eine in den Daten spezifizierten URL weiterzuleiten. Ein Angreifer hat dadurch die Möglichkeit, einen Angriff hinter einem vertrauenswürdigen Domain-Namen zu verstecken. Für einen direkten Angriff auf eine Web-Anwendung ist ein Redirection-Angriff uninteressant. In den Händen eines Phishers kann sie wiederum “bares Geld” bedeuten.

Rootkit:

Ein Rootkit ist eine Art Malware, die dazu dient, einem Angreifer Zugang zu einem System oder Netzwerk zu verschaffen und seine Aktivitäten zu verbergen. Es ist schwer zu erkennen und zu entfernen, da es oft tief in das System integriert ist. Eine Möglichkeit, sich vor Rootkits zu schützen, besteht darin, regelmäßig Virenscans durchzuführen und sicherzustellen, dass das Betriebssystem und andere Anwendungen mit den neuesten Sicherheits-Updates und -Patches aktualisiert werden.

S

Software:

Ist ein Sammelbegriff für Programme und die zugehörigen Daten. Software bestimmt, was ein programmgesteuertes Gerät tut und wie es das tut (in etwa vergleichbar mit einem Manuskript). Die Hardware (das Gerät selbst) führt Software aus (arbeitet sie ab) und setzt sie so in die Tat um. Software ist die Gesamtheit von Informationen, die man der Hardware hinzufügen muss, damit ein Software-gesteuertes Gerät für ein definiertes Aufgabenspektrum nutzbar wird.

Spyware:

Spähprogramm oder Spionagesoftware, die Daten eines Computernutzers ohne dessen Wissen oder Zustimmung an den Hersteller der Software oder an Dritte sendet oder dazu genutzt wird, dem Benutzer über Werbeeinblendungen Produkte anzubieten. Die ungewollte Installation der Spyware wird oft durch aktive Inhalte (wie Flash, Java und Active X) beziehungsweise über die Installation von befallenen Browser-Plug-ins begünstigt. Ein erstes Spyware-Symptom ist die Langsamkeit des Rechners. Weitere Anzeichen können die Änderung der Browserstartseite sein, neue Einträge im Lesezeichenmenü oder absurderweise die Empfehlung, ein Anti-Sypware-Programm zu installieren. Spyware überträgt – bei aktiver Internetverbindung – bestimmte Daten des Nutzers, die vom Sypware-Anbieter kommerziell ausgewertet werden.

Schadfunktion:

Mit Schadfunktion wird eine vom Anwender ungewünschte Funktion bezeichnet, die die Informationssicherheit unbeabsichtigt oder bewusst gesteuert gefährden kann.

Scareware:

„Scareware“ ist eine Form von Schad-Software, die der Nutzer selbst auf seinem System installiert. In den meisten Fällen wird dem Nutzer beim Surfen im Internet durch Täuschung oder Ausnutzen von technischem Unverständnis suggeriert, dass ein Problem mit seinem Computer besteht. Häufig wird dazu eine Infektion mit Schad-Software gemeldet, eine angebliche Fehlfunktion des Betriebssystems erkannt oder mit einem

wichtigen Sicherheits-Update geworben. Vertraut ein Anwender auf diese Meldungen und installiert die angebotene Software, hat er selbst dadurch das System im ungünstigsten Fall mit einer Schad-Software infiziert.

SIEM:

SIEM (Security Incident and Event Management) ist eine Methode der Cyber Security, die in Echtzeit Sicherheitsereignisse sammelt, korreliert und auswertet. Auf diese Weise werden außergewöhnliche Muster oder gefährliche Trends sichtbar und Unternehmen können schnell und gezielt auf Bedrohungen reagieren. SIEM ermöglicht einen ganzheitlichen Blick auf die IT-Sicherheit und nutzt Verfahren des maschinellen Lernens sowie der künstlichen Intelligenz (KI).

SOC:

Das SOC (Security Operations Center) ist eine Art Kommandozentrale zum Schutz der IT-Infrastruktur eines Unternehmens. Hier werden die einzelnen IT-Elemente überwacht, der aktuelle Zustand analysiert, mögliche Bedrohungslagen identifiziert und im Bedarfsfall mit geeigneten Maßnahmen darauf reagiert.

SASE:

SASE (Secure Access Service Edge) kombiniert modernes SD-WAN mit Sicherheitsfunktionen aus der Cloud. Das Besondere: SASE trifft sichere Zugriffsentscheidungen auf Unternehmensdaten bereits am Service Edge (Netzwerkrand) bzw. an der jeweiligen Quelle der Verbindung (Nutzer, Gerät, Standort). Denn der Zugriff erfolgt immer öfter dezentral, am Rand des Unternehmensnetzwerks. Zu den Security-Komponenten von SASE zählen z. B. Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), Firewall as a Service (FaaS), Cloud Access Security Broker (CASB) u.a. SASE ist eine moderne und dynamische Lösung, die den neuen Anforderungen von Unternehmen an ihre Netzwerksicherheit gerecht wird.

Security Incident:

Als Security Incident zählt jeder absichtlich herbeigeführte oder unbeabsichtigte Vorfall, der zu einer erhöhten Bedrohung der Informationssicherheit führt wie zum Beispiel der Ausfall eines Intrusion Detection Systems oder das Erkennen von Angriffsmustern wie Port Scans.

Security Scan:

Ein Security Scan ist eine automatisierte, technische, unprivilegierte Sicherheitsüberprüfung mit manueller Verifikation der detektierten Sicherheitslücken.

Session Hijacking:

Bei Session Hijacking übernimmt ein Angreifer die Sitzung seines Opfers. Dadurch kann dieser auf die Daten des Opfers zugreifen und Befehle in dessen Namen ausführen.

Social Engeneering:

Social Engineering bezeichnet die Manipulation von Menschen, um Zugang zu vertraulichen Informationen oder Systemen zu erhalten. Durch z.B. Erzeugung von Stress, Zeitdruck oder das Ausnutzen von Vertrauen, werden Betroffene dazu gebracht, bestimmt Handlungen auszuführen oder sensible Daten preiszugeben. Ein Beispiel wäre ein Angreifer, der sich als IT-Administrator ausgibt und einen Mitarbeiter auffordert, seine Zugangsdaten preiszugeben. Unternehmen sollten ihre Mitarbeiterinnen und Mitarbeiter in Schulungen über Social-Engineering-Methoden informieren und ihnen beibringen, wie sie solche Angriffe erkennen und vermeiden können.

Spam:

Als Spam werden unerwünschte E-Mails bezeichnet, die in großen Mengen versendet werden und oft betrügerische oder schädliche Absichten verfolgen. Um sich vor Spam zu schützen, sollten Unternehmen

Spam-Filter und Antiviren-Software einsetzen. Wichtig ist auch, die Mitarbeiterinnen und Mitarbeiter über die Gefahren von Spam zu informieren und sie daran zu erinnern, keine unbekannten Links oder Anhänge zu öffnen.

Spear Phishing:

Während Phishing nach dem Gießkannenprinzip funktioniert, **ist Spear Phishing** ein gezielter Phishing-Angriff, bei dem der Angreifer gezielt Personen oder Unternehmen auswählt, um an vertrauliche Informationen oder Systeme zu gelangen. Um sich vor Spear Phishing zu schützen, sollten Unternehmen ihre Mitarbeiterinnen und Mitarbeiter in Schulungen über die Gefahren von Spear Phishing aufklären und sicherstellen, dass ihre Systeme mit den neuesten Sicherheits-Updates und -Patches aktualisiert sind.

SQL-Injektion

SQL ist eine Programmiersprache für Datenbanken. Bei der SQL Injection (dt. SQL-Einschleusung) wird eine Schwachstelle im Zusammenhang mit SQL-Datenbanken ausgenutzt. Dabei werden SQL-Befehle eingeschleust und die Einträge in der Datenbank so manipuliert, dass Daten verändert, gelöscht oder gelesen werden können.

T

TLS:

Transport Layer Security (TLS, deutsch Transportschichtsicherheit) ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.

Trojaner:

Als „Trojanisches Pferd“ (oft auch fälschlicherweise kurz „Trojaner“ genannt) bezeichnet man ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt. Mittels Trojanern werden schädliche Programme installiert, mit denen Nutzende z.B. ausspioniert oder erpresst werden können. Trojaner zählen zu den unerwünschten bzw. schädlichen Programmen, der sogenannten Malware.

V

Viren:

Klassische Form von Schad-Software, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (keine Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte). „Viren“ treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.

Verschlüsselung:

Verschlüsselung ist der Prozess der Umwandlung von Daten in eine unlesbare Form, um ihre Vertraulichkeit und Integrität zu schützen. Unternehmen sollten ihre Daten verschlüsseln, um sicherzustellen, dass ihre vertraulichen Informationen vor unbefugtem Zugriff geschützt sind.

Virtuelles Privates Netzwerk (VPN):

Ein virtuelles privates Netzwerk ist ein sicherer Tunnel, der es Benutzern ermöglicht, sicher auf ein IT-System oder Netzwerk zuzugreifen, indem ihre Internetverbindung verschlüsselt und anonymisiert wird. Unternehmen sollten sicherstellen, dass sie ein VPN verwenden, um ihre Systeme und Netzwerke vor potenziellen Bedrohungen zu schützen.

Vulnerability:

Eine Vulnerability ist eine Schwachstelle oder ein Fehler in einem IT-System oder Netzwerk, die von einem Angreifer ausgenutzt werden kann, um Zugriff auf das System oder Netzwerk zu erlangen oder Daten zu stehlen. Unternehmen sollten ihre Systeme regelmäßig auf Schwachstellen überprüfen und geeignete Maßnahmen ergreifen, um potenzielle Schwachstellen zu minimieren.

W

World Wild Web (WWW):

Das World Wide Web ist ein Informationssystem aus verknüpften Dokumenten, die Webseiten genannt werden. Auf das System kann über das Internet mittels eines Browsers zugegriffen werden. Das System enthält unterschiedliche Inhalte wie Text, Bilder, Musik und Videos. Das Web wurde 1989 von Tim Berners-Lee erfunden.

Wurm:

Ein Wurm ist bösartige Software, welche sich selbständig dupliziert und auf andere Computer verbreitet (diese infiziert). Dies geschieht häufig unter Benutzung von Computer-Netzwerken.

White Hat Hacker:

Ist ein IT-Sicherheitsexperte, der Schwachstellen in Systemen entdeckt, um Unternehmen vor Cyber-Angriffen zu schützen. White Hat Hacker werden auch als ethische Hacker bezeichnet.

Z

Zero Day Exploit:

Die Ausnutzung einer Schwachstelle, die nur dem Entdecker bekannt ist, charakterisiert man mit dem Begriff „Zero Day Exploit“. Die Öffentlichkeit und der Hersteller des betroffenen Produkts merken in der Regel erst dann die Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Der Hersteller hat keine Zeit, die Nutzer vor den ersten Angriffen zu schützen.

Zugriff:

Bezeichnet die Nutzung von Informationen bzw. Daten. Über Zugriffsberechtigungen wird geregelt, welche Personen oder IT-Anwendungen bevollmächtigt sind, Informationen oder Daten zu nutzen oder Transaktionen auszuführen.

ZTNA:

ZTNA (Zero Trust Network Access) verweigert grundsätzlich jeden Zugriff auf das Unternehmensnetzwerk, es sei denn, er ist ausdrücklich erlaubt. Das Prinzip des Sicherheitskonzepts lautet „never trust, always verify“. ZTNA betrachtet keinen Benutzer, kein Gerät und keine Anwendung automatisch als sicher. Jeglicher Datenverkehr und alle Zugriffsquellen müssen erst authentifiziert werden, bevor sie Zugriff auf das Netzwerk erhalten. Dieser Zugriff wird nur gewährt, wenn er erforderlich ist und erfolgt mit minimaler Rechtevergabe. Zero Trust Network Access ist das Gegenteil traditioneller Netzwerksicherheitsansätze, die Benutzer, Geräte und Anwendungen als sicher einstufen, allein deshalb, weil sie sich innerhalb des definierten Netzwerks befinden.