|  |
| --- |
| IU |
| Threat Modelling (Bedrohungsmodellierung) |
|  |

# Übergeordnete Lernziele

Das gesamte Kursbuch ist in sieben Lektionen unterteilt. In der ersten Lektion werden die drei Hauptsäulen der Informationssicherheit, nämlich Vertraulichkeit, Integrität und Verfügbarkeit, sowie deren Bewahrung erörtert. In der zweiten Lektion schauen wir uns genauer an, wie sich Bedrohungen messen lassen, sodass im Voraus die notwendigen Vorkehrungen gegen eine potenzielle Bedrohung getroffen werden können, wenn diese eine Schwachstelle ausnutzt.

Die dritte Lektion ist das Herzstück dieses Kursbuchs, in der wir die bekannten Bedrohungsmodelle im Detail erläutern werden. Nach Abschluss dieser Lektion sind Sie in der Lage, eine Bedrohung mit Hilfe eines der erläuterten Bedrohungsmodelle zu modellieren. Die vierte Lektion ist dann der Diskussion von Angriffsbibliotheken gewidmet. Diese werden hauptsächlich für offensive Operationen genutzt. Das eigentliche Ziel dieser Lektion ist jedoch, herauszufinden, wie wir diese Bibliotheken für defensive Operationen nutzen können, und zwar bevor Angreifende sie zur Gefährdung eines Opfers ausnutzen können.

Ein gründliches Verständnis der Gesetzgebung und Strafverfolgung von Cyberkriminalität ist für alle Personen notwendig, die sich mit Cybersicherheit beschäftigen, was in Lektion fünf behandelt wird. Da es nicht ausreicht, eine Bedrohung nur zu modellieren, müssen wir für den Umgang damit auch Methoden des Risikomanagements einsetzen. Dies wird in Lektion sechs erläutert. Dort erhalten wir einen tiefen Einblick in alle im Rahmen des Risikomanagementprozesses durchgeführten Teilprozesse. In der siebten Lektion lernen wir schließlich einige bewährte Vorgehensweisen („Best Practices“) kennen, die zur Abwehr einer Bedrohung oder Gefahr genutzt werden sollten.

# Lektion 1 – CIA und noch mehr

**Lernziele**

Nach Abschluss dieser Lektion werden Sie in der Lage sein,

… die drei wichtigsten Grundpfeiler der Informationssicherheit zu verstehen: Vertraulichkeit, Integrität und Verfügbarkeit (*CIA = Confidentiality, Integrity, Availability*).

… CIA-Konzepte in vorgegebenen Szenarien zu nutzen.

… die wichtigsten Unterschiede zwischen den einzelnen Bestandteilen von CIA zu erkennen.

… zu erkennen, welcher Grundpfeiler von CIA in einer bestimmten Situation gefährdet ist.

… sich an die notwendigen Sicherheitsmaßnahmen zu erinnern, die zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Informationen ergriffen werden müssen.

… allgemeine Fragen der Informationssicherheit zu bewerten.

# 1. CIA und noch mehr

## Einführung

Beim Schutz und bei der Sicherung von Netzwerken, Systemen, Anwendungen und Informationen vor unbefugten Manipulationen, Nutzungen oder Zugriffen geht es im Grunde um das Thema Informationssicherheit. Informationssicherheit umfasst die Sicherheit in allen ihren Aspekten. Der wichtigste Begriff hierbei ist natürlich „Sicherheit“, also dass etwas geschützt oder gesichert werden soll. Die Begriffe Sicherheit und Schutz sollten nicht verwechselt werden. Schutz bedeutet, dass weder vorsätzlich noch fahrlässig Schaden verursacht wird. Sicherheit hingegen bezieht sich nur auf vorsätzliche Schäden, die von einem Angriff stammen könnten. Die zentrale Frage dabei ist, woher wir wissen können, welcher wichtige Aspekt von Informationen gesichert werden muss.

Zum Verständnis von Informationssicherheit wird ein Verständnis der Schlüsselaspekte Vertraulichkeit, Integrität und Verfügbarkeit (*CIA = Confidentiality, Integrity, Availability*) benötigt. Schutz bedeutet Sicherheit, und Sicherheit bedeutet CIA – deshalb ist es unerlässlich, diese Schlüsselaspekte zu verstehen. Diese drei Konzepte, auch als CIA-Triade oder CIA-Dreiklang bekannt, bilden zusammen die Säulen der Informationssicherheit, die in den folgenden Lernzyklen behandelt werden (Deane & Kraus, 2021, S. 4).

**Datenpanne**

(auch Datensicherheitsverletzung) Die Offenlegung von vertraulichen oder sensiblen Informationen an Unbefugte.

Alle drei dieser Schlüsselaspekte wirken zusammen und sind voneinander abhängig. Studierende, Hochschulabsolvent:innen und sogar Sicherheitsprofis, die im Bereich Informationssicherheit tätig sind, müssen diese drei Aspekte und die entsprechenden Gegenmaßnahmen verstehen, um ihre Informationen vor einer **Datenpanne** zu schützen.

In den folgenden Lernzyklen werden wir die grundlegenden und fortgeschrittenen CIA-Konzepte sowie deren Umsetzung im Detail besprechen. Anschließend werden wir die häufigsten Sicherheitsbedrohungen und ‑probleme analysieren, mit denen jedes Unternehmen bzw. seine Vermögensgüter (oder Ressourcen) im Tagesgeschäft konfrontiert sind. Ein Vermögensgut (engl. *Asset*) ist alles, was einen gewissen Wert für seine:n Besitzer:in hat. Hierbei ist zu beachten, dass wir zwei Arten von Vermögensgütern betrachten: primäre und sekundäre. Primäre Vermögensgüter umfassen die wichtigsten Informationen, Prozesse oder Aktivitäten, wie z. B. Geld oder der gute Ruf (Reputation). Die sekundären Vermögensgüter Netzwerk, Software und Hardware können hingegen zur Manipulation bzw. Gefährdung der primären Vermögensgüter ausgenutzt werden.

**Cyberangriff**

Ein Angriff durch Cyberkriminelle, mit dem sie versuchen, unbefugten Zugriff auf Daten zu erhalten und Systemressourcen zu stören.

Laut dem von Cisco veröffentlichten jährlichen Bericht zur Cybersicherheit zielen Cyberkriminelle vor allem auf Menschen mit einem begrenzten Wissen über Cyberkriminalität begrenzt ab. Sie können häufig nicht mit Situationen umgehen, in denen es zu einer Datenverletzung oder einem **Cyberangriff** kommt. Daher ist es wichtig, sich ein gutes Verständnis der grundlegenden Begriffe im Bereich der Cybersicherheit anzueignen, um das Risiko in diesen Situationen wirkungsvoll zu senken (Ng et al., 2021, S. 1).

## 1.1 Vertraulichkeit

**Personenbezogene Daten**

Alle Informationen, die zur Identifizierung einer Person dienen, wie Name, Geburtsdatum, Adresse, Kreditkartennummer usw.

Vertraulichkeit bedeutet den Schutz geheimer Informationen vor unbefugter oder illegaler Offenlegung. Viele Organisationen werden von Cyberkriminellen gefährdet, was zu Datenschutzverletzungen führt. Dazu gehört auch der Verlust von **personenbezogenen Daten** (engl. PII = *personally identifiable information*), einem der Vermögensgüter, die das Ziel der Angreifenden darstellen. Viele Unternehmen führen Schulungen durch, um die Mitarbeitenden mit den grundlegenden Begriffen von Cyber- und Informationsbedrohungen vertraut zu machen. Da der Mensch das schwächste Glied bei Cyberangriffen ist, ist es unerlässlich, die Menschen mit den grundlegenden Begriffen aus dem Cyberbereich vertraut zu machen.

Im Hinblick auf diese Gedanken könnte sich die folgende Frage stellen: Wo sollten wir anfangen, diese Konzepte zu **Cyber-Bedrohungen** zu lernen? In diesem Lernzyklus werden wir uns auf die Vertraulichkeit konzentrieren, die eines der wichtigsten Konzepte der CIA-Triade ist.

**Cyber-Bedrohung**

Jede Handlung, die potenziell die CIA von Daten durch Diebstahl oder Beschädigung gefährdet oder ihre Verfügbarkeit bedroht.

Die Vertraulichkeit ist die erste Säule der CIA-Triade. Nach diesem Konzept haben nur befugte Nutzende Zugang zu Daten und Systemen, wohingegen unbefugte Nutzende daran gehindert werden. Einfach ausgedrückt meint Vertraulichkeit, dass nur die dafür vorgesehenen Personen Zugang zu Ressourcen und Informationen haben. Der Zweck der Vertraulichkeit besteht also darin, den unbefugten und illegalen Zugriff auf private und nicht-private Informationen und Daten zu beschränken. Wichtig ist hierbei, dass sich Vertraulichkeit auf das Betrachten oder Lesen von Daten bezieht. Das bedeutet, dass die Vertraulichkeit dann gewahrt ist, wenn Personen, die zum Betrachten oder Lesen bestimmter Daten befugt und berechtigt sind, diese Daten lesen oder betrachten – aber niemand sonst. Wenn also jemand, der nicht zum Lesen der Daten befugt ist, es irgendwie geschafft hat, auf diese Daten zuzugreifen und sie zu lesen, dann ist die Vertraulichkeit der Daten gefährdet.

Organisationen oder Unternehmen, die sich nicht an die gesetzlichen und vertraglichen Verpflichtungen zum Schutz vertraulicher Daten halten, riskieren geschäftsschädigende Datenschutzverletzungen. Dies sind einige der Hauptkonsequenzen, die ein Unternehmen aufgrund mangelnder Sicherheitsüberprüfungen erleiden kann.

Der Begriff der Vertraulichkeit steht im Zusammenhang mit einer der bewährten Vorgehensweisen, die Least-Privilege-Prinzip (Prinzip der geringsten Rechte) genannt wird. Least Privilege ist ein Konzept, bei dem der Zugriff auf sensible Daten oder Informationen nur bei Bedarf gewährt werden darf. Nach dieser Regel wird den Nutzenden nur ein angemessener Zugang gewährt, damit sie ihre beabsichtigten Aufgaben ausführen können.

Ein weiterer wichtiger Aspekt der Vertraulichkeit ist die Privatsphäre bzw. der Datenschutz. Wenn wir im Zusammenhang mit der Sicherheit von Privatsphäre oder Datenschutz sprechen, geht es um persönliche Daten. Informationen oder Details, die zur eindeutigen Erkennung einer Person genutzt werden können, sind personenbezogene Daten (PII). Diese müssen von jeder Einrichtung oder Organisation vertraulich behandelt werden, um die Datenschutzgesetze des jeweiligen Landes einzuhalten.

Verschiedene böswillige Akteure haben es darauf abgesehen, die Vertraulichkeit der Daten durch Social Engineering (soziale Manipulation) und Phishing-Techniken zu gefährden. Abgesehen von böswilligen Handlungen kann die Vertraulichkeit auch durch menschliche Nachlässigkeit oder Fehler gefährdet werden. Zu solchen Situationen gehört das Versagen der Datenverschlüsselung oder die Anzeige hochsensibler Informationen auf Computerbildschirmen, während sich unbefugte Mitarbeitende, Vorgesetzte oder andere Nutzende in der Nähe befinden.

### Bewährte Vorgehensweisen zur Sicherung der Vertraulichkeit von Daten

Für Datenbesitzer:innen ist die Wahrung der Vertraulichkeit oft eines der wichtigsten Sicherheitskonzepte. Es gibt viele Sicherheitsmaßnahmen, die Datenbesitzer:innen helfen, die Vertraulichkeit ihrer Daten zu gewährleisten. Diese Kontrollen umfassen unter anderem die folgenden Punkte (Security Operations Center, o. D.):

* Verschlüsselung: Eine Technik zur Umwandlung von Klartextdaten in verschlüsselten Text.
* Multi-Faktor-Authentifizierung: Die Nutzung von Token (Marken) zur starken Authentifizierung.
* Die Verwendung eines Passwortmanagers zur Verwaltung von Passwörtern für mehrere Konten.
* Passwortlose Authentifizierung.
* Einrichtung von Sicherheitsmaßnahmen zur Verhinderung eines unbefugten physischen Zugriffs, wenn die Daten nicht aus der Ferne abgerufen werden können.
* Nutzung einer Passphrase (auch Passsatz genannt).
* Nutzung eines langen und komplexen Passworts, das Buchstaben, Zahlen und Sonderzeichen enthält.
* Verwendung unterschiedlicher Passwörter für unterschiedliche Konten anstatt des gleichen Passworts für alle Konten.

Abgesehen von den oben genannten Sicherheitsmaßnahmen ist jedoch eine umfassende Schulung des Personals zur Vermeidung menschlichen Versagens ebenso unerlässlich, weil dies zu Datenschutzverletzungen führen kann und somit die Vertraulichkeit der Daten gefährdet (Deane & Kraus, 2021, S. 4-5).

#### Besseres Verständnis für die Gefährdung der Vertraulichkeit anhand von Beispielszenarien

Zum besseren Verständnis des Prinzips der Vertraulichkeit führen wir hier einige beispielhafte Szenarien auf:

* Ein Laptop oder ein Handy, das nicht verschlüsselt oder passwortgeschützt ist und persönliche oder sensible Daten enthält, wird gestohlen.
* Persönliche Informationen werden unbeabsichtigt auf einer Website oder einer Plattform für soziale Medien veröffentlicht.
* Das Posten von Aktivitäten des täglichen Lebens wie Geburtstagsfeiern, Hochzeitsbildern und ähnliches in den sozialen Medien kann Angreifenden zusätzliche Details über ein anvisiertes Opfer offenbaren.
* Ein Keylogger wird auf dem Rechner des Opfers installiert und zeichnet jede getippte Taste auf. So kann es zu Datenlecks (Passwörter, Kreditkarten-PINs usw.) kommen.
* Ein Text-Chat zwischen befugten Personen wird von einer dritten, unbefugten Person aufgezeichnet und eingesehen.

### Fragen zur Selbstkontrolle

1. Nennen Sie drei Hauptgründe, warum Unternehmen die Vertraulichkeit von Daten sicherstellen müssen.

*Zum Schutz der personenbezogenen Daten (PII) der Nutzenden.*

*Zum Schutz der Privatsphäre der Nutzenden.*

*Zur Verhinderung der durch eine Datenverletzung möglicherweise entstehenden wirtschaftlichen Schäden und Rufschädigungen für das Unternehmen.*

*Zur Einhaltung der Gesetze und Vorschriften des Landes.*

1. Kreuzen Sie die richtige(n) Aussage(n) an.

* *Vertraulichkeit ist ein Teil der bekannten CIA-Triade.*
* Vertraulichkeit der Daten bedeutet, dass nur befugte Personen Zugriff auf die Daten haben.
* *Vertraulichkeit bedeutet, dass geheime Daten nur von dazu befugten Personen gelesen werden können.*
* Unternehmen müssen vertrauliche Daten nur zu ihrer eigenen Zufriedenheit schützen.

1. Vervollständigen Sie den folgenden Satz:

Umfassende Schulungen des *Personals* werden empfohlen, um *menschliches* Versagen zu vermeiden.

## 1.2 Integrität

Bei der Informationssicherheit ist die Integrität nach der Vertraulichkeit das zweite bedeutende Konzept. Integrität bezieht sich auf die Korrektheit und Fehlerfreiheit der Daten, Informationen und Systeme (Lundgren et al., 2019, S. 421). Diese Eigenschaft der Informationssicherheit stellt sicher, dass nur befugte Personen mit den Daten umgehen und dass diese korrekt sind. Das bedeutet, dass die Person, die auf die Daten zugreifen darf, diese auch für korrekt hält. Das Hauptziel der Integrität ist die Garantie, dass die Daten völlig unverändert, zuverlässig und korrekt bleiben. Wenn eine unbefugte Änderung in den Daten festgestellt wird, würde dies als Beeinträchtigung der Integrität der Daten insgesamt wahrgenommen werden. Wird die Integrität der Daten nicht geschützt, kann dies zu falschen Entscheidungen oder nachteiligen Handlungen führen, weil die zugrundeliegenden Daten manipuliert wurden (Deane & Kraus, 2021, S. 5–6).

Die Integrität der Daten, Informationen oder Systeme kann aus den folgenden Gründen gefährdet sein:

* Von Softwareentwickler:innen schlecht geschriebener Code,
* Viren,

**Superuser**

In der Informatik ist der Superuser ein spezielles Benutzerkonto zur Systemverwaltung.

* ein **Superuser** oder Systemadministrator hat den falschen Befehl für eine Datenbank ausgeführt,
* Computerviren,
* ein Administrator hat den falschen Teil einer Konfigurationsdatei geändert,
* auf ein System heruntergeladene Schadsoftware, nachdem ein Nutzender auf einen bösartigen Link in einer E-Mail geklickt hat (Phishing-Angriff),
* verfälschte finanzielle Dokumente (Finanzbetrug),
* menschliche Fahrlässigkeit oder Fehler,
* böswillige Aktivitäten eines Mitarbeitenden mit potenzieller Datenmanipulation.

### Bewährte Vorgehensweisen zur Sicherung der Datenintegrität

Wir haben bereits das Konzept der Integrität und die wichtigsten Gründe für eine Beeinträchtigung der Integrität der Daten erörtert. Zur Gewährleistung der Datenintegrität müssen angemessene Sicherheitsmaßnahmen vorhanden sein (Deane & Kraus, 2021, S. 6).

Einige der wichtigsten Sicherheitsmaßnahmen sind nachstehend aufgelistet. Durch die Berücksichtigung dieser Maßnahmen können die Integrität der Daten gewährleistet und unbefugte Änderungen begrenzt werden:

* Kontinuierliche Erstellung von Sicherungskopien der Daten auf einem externen Gerät, so dass die Originaldaten bei Verlust wiederhergestellt werden können.

**Versionskontrolle**

Ein zentrales System zur Verfolgung von Änderungen am Softwarecode.

* Einrichtung eines geeigneten **Software-Versionskontrollsystems**.
* Einführung strikter Berechtigungen, damit nur befugte Personen auf die Daten zugreifen können.
* Kryptographisches **Hashing**.
* Die Einführung einer Aufgabentrennung. Dies bedeutet, dass mehr als eine Person für die Ausführung und Fertigstellung einer Aufgabe verantwortlich ist, anstatt dass nur eine Person die volle Kontrolle über die gesamte Aufgabe erhält (geeks for geeks, 2022).

**Hashing**

Eine Methode zur Überprüfung der Integrität der vom Empfänger empfangenen Daten.

* Einführung einer Aufgabenrotation, bei der die Nutzenden, die eine bestimmte Aufgabe erledigen, immer wieder wechseln. Dadurch wird verhindert, dass einzelne Nutzende die vollständige Kontrolle haben.
* Zielgerichtete und kontinuierliche Schulung der Nutzenden.

An dieser Stelle sei darauf hingewiesen, dass zwei wichtige Konzepte der Informationssicherheit direkt oder indirekt mit der Integrität zusammenhängen, nämlich die Authentifizierung und die Unleugbarkeit (auch: Unverfälschbarkeit). In diesem Lernzyklus geht es um das Verständnis des Konzepts Integrität, wir sollten aber auch kurz auf das Konzept der Authentifizierung und Unleugbarkeit eingehen. Authentizität oder Authentifizierung bezieht sich auf die Garantie, dass alle Teilnehmer:innen die sind, die sie vorgeben zu sein, und dass die empfangenen Daten original und echt sind. Unleugbarkeit hingegen bedeutet, dass kein:e Teilnehmer:in seine:ihre Handlungen nachträglich verfälschen oder abstreiten kann (z. B. Daten löschen, neu erstellen oder verändern). Digitale Signaturen sind Methoden, die zum Schutz der Authentizität und der Unleugbarkeit von Daten eingesetzt werden (Deane & Kraus, 2021, S. 6).

#### Beispielszenarien zum Verständnis von Integritätsverletzungen

Wir geben nachstehend einige praxisnahe Beispiele für Verletzungen der Datenintegrität (Fruhlinger, 2020):

* Manipulation von Geschäftsdaten, die möglicherweise zu schlechten Entscheidungen führen können.
* Illegaler Zugriff auf ein Finanzsystem zum Aufblähen von Aktienwerten.
* sich in ein Bankkonto hacken und dann den Zugang sperren
* Änderung des HTML-Codes einer Website durch Hacker aus Spaß oder Rache.

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Zwei wichtige Sicherheitskonzepte, die nicht Teil der CIA-Triade sind, aber mit der Integrität in Zusammenhang stehen, sind *Authentifizierung* und *Unleugbarkeit (bzw. Unverfälschbarkeit)*.

1. Die Integrität der CIA-Triade bezieht sich auf …

* befugtes Lesen von Daten.
* befugtes Einsehen von Daten.
* Korrektheit der Daten

1. Welche Art von Nutzenden hat besondere Berechtigungen gegenüber normalen Nutzenden?

*Superuser oder Administrator*

1. Nennen Sie drei Sicherheitsmaßnahmen für die Datenintegrität.

*Nutzung eines Versionskontrollsystems*

*Hashing*

*Schulung zur Sensibilisierung der Nutzenden*

*Aufgabenrotation*

*Starke Berechtigungen*

## 1.3 Verfügbarkeit

Die dritte und letzte Säule der CIA-Triade ist die Verfügbarkeit. Verfügbarkeit bedeutet, dass befugte Nutzende bei Bedarf Zugriff auf die Daten oder einen Dienst haben. Im Hinblick auf **Unternehmensnetzwerke** oder ‑umgebungen bezieht sich der Begriff Verfügbarkeit auf die Gewährleistung des ununterbrochenen und zügigen Zugriffs durch befugte Nutzende und Dienste auf die Daten und Systeme, die sie zur Erfüllung ihrer Aufgaben benötigen. Bedrohungen, die auf die Verfügbarkeit abzielen, können die Geschäftsabläufe des Unternehmens empfindlich stören. Wenn dies geschieht, kommt es möglicherweise zur Unterbrechung eines kritischen Geschäftssystems, was zu weiteren Rufschädigungen, Einkommens- oder Kundenverlusten führen kann (Deane & Kraus, 2021, S. 6–7).

**Unternehmensnetzwerk**

Das Netzwerk bzw. die IT-Infrastruktur einer Organisation.

Im Folgenden finden Sie die Konzepte, die im Zusammenhang mit der Verfügbarkeit berücksichtigt werden sollten:

* **Zugänglichkeit** bezieht sich auf die Einfachheit und Möglichkeit der Nutzenden, bei Bedarf auf Daten zuzugreifen oder eine Ressource zu nutzen. Dazu gehört auch die Aufhebung von Einschränkungen für Nutzende, die zum Zugriff auf die Daten und Ressourcen befugt sind. Nehmen wir zum Beispiel an, es gibt eine Datei, die auf der internen Festplatte eines Unternehmens gespeichert ist. Diese Datei gilt als verfügbar, wenn sie dort verbleibt und die Festplatte in Betrieb ist. Wenn jedoch dieselbe Datei in einen anderen Ordner auf einer gemeinsam genutzten Festplatte verschoben werden muss, lässt sich dort vielleicht nicht auf die Datei zugreifen – die Datei ist aber dennoch verfügbar. Das bedeutet, dass die Daten in diesem Szenario zwar noch vorhanden, aber nicht zugänglich sind.
* **Benutzerfreundlichkeit** bedeutet, dass Nutzende in der Lage sein sollten, die verfügbaren und zugänglichen Daten so zu nutzen, dass sie ihren Anforderungen für die Erfüllung einer Aufgabe entsprechen. Wenn wir zum Beispiel ein über Google Drive freigegebenes Dokument zu bearbeiten versuchen, stellen wir möglicherweise fest, dass es trotz Freigabe nicht bearbeitbar ist, weil wir nur zum Lesezugriff berechtigt sind. In diesem Szenario ist die Datei zwar verfügbar und zugänglich, aber aufgrund der strengen Berechtigungen nicht nutzbar.

**Service Level Agreement**

Ein umfassendes Dokument, in dem die Leistungen aufgeführt sind, die der Dienstleister für die Kund:innen erbringen muss. (Auf Deutsch häufig auch Dienstgütevereinbarung oder Leistungsschein.)

* **Aktualität** ist die Zeitspanne zwischen dem Zeitpunkt, an dem die Informationen angefordert werden, und dem Zeitpunkt, an dem sie für befugte Nutzende zugänglich und verfügbar sind. Um die Aktualität zu gewährleisten, müssen die Daten innerhalb einer bestimmten Zeitspanne für befugte Nutzende verfügbar sein. In Situationen, in denen ein Drittanbieter die Daten verwaltet, wie z. B. Cloud-Anbieter, ist Aktualität die entscheidende Komponente, die in **Service Level Agreements** (SLAs), auf Deutsch Dienstgütevereinbarungen oder Leistungsscheine, erwähnt werden muss.

### Häufig vorkommende Bedrohungen der Verfügbarkeit

Die Verfügbarkeit von Daten, Informationen oder Systemen kann aus folgenden Gründen beeinträchtigt sein (Deane & Kraus, 2021, S. 6–7):

* **Denial-of-Service-Angriffe (DoS-Angriffe)** sind Cyberangriffe, bei denen Angreifende (Hacker) versuchen, ein Netzwerk oder einen Computer auszuschalten oder zu stören, so dass dieser für befugte Nutzende oder andere Dienste nicht mehr verfügbar und zugänglich ist. Dies geschieht durch die Überflutung des Angriffsziels mit unnötigem Datenverkehr.
* **Distributed-Denial-of-Service-Angriffe (DDoS)** ähneln DoS-Angriffen in dem Sinne, dass Angreifende versuche, ein System oder Netzwerk lahmzulegen und den Datenzugriff durch befugte Nutzende zu verhindern. Der Unterschied besteht darin, dass bei DDoS mehrere manipulierte Systeme genutzt werden, um das Angriffsziel mit unnötigem Datenverkehr zu stören.
* **Naturkatastrophen** wie Tornados, Stürme und Erdbeben können zur Zerstörung und Unterbrechung des Systems führen, so dass es nicht mehr verfügbar ist.
* Das **Löschen sensibler Daten** aus dem System macht sie für die befugten Nutzenden unzugänglich.

**Verschlüsselung**

Ein Vorgang, bei dem lesbare Daten in eine Form umgewandelt werden, die nicht lesbar ist.

* Bei **Ransomware-Angriffen** **verschlüsselt** ein Angreifender die Systemdaten des Opfers und verlangt dann ein Lösegeld in Bitcoins für die Entschlüsselung der Daten.
* **Nicht bösartige Bedrohungen** beziehen sich auf Software-Konfigurationsfehler oder Bedrohungen durch die Umwelt, die zu einer Unterbrechung der Stromversorgung führen.
* **Bösartige Bedrohungen** beziehen sich auf alle Bedrohungen, die potenziell von Cyberkriminellen mit bösartigen Absichten initiiert werden. Zu diesen Bedrohungen gehören u. a. Angriffe wie Ransomware, DoS und DDoS.

### Bewährte Vorgehensweisen zur Sicherung der Verfügbarkeit

Wir haben uns kurz das Konzept der Verfügbarkeit angesehen. Wir haben auch einige der wichtigsten Gründe für die Beeinträchtigung der Verfügbarkeit von Systemen erörtert. Wir besprechen nun einige der Sicherheitspraktiken, die berücksichtigt werden müssen, um eine Beeinträchtigung der Verfügbarkeit zu verhindern.

Im Folgenden sind die wichtigsten Sicherheitsmaßnahmen aufgeführt, mit denen die Verfügbarkeit der Daten, Systeme oder Netzwerke sichergestellt werden kann (Deane & Kraus, 2021, S. 6–7):

**Datenredundanz**

Die Praxis, Daten an zwei oder mehr Orten zu speichern, um auf sie zugreifen zu können, wenn sie am Hauptspeicherort nicht mehr verfügbar sind.

* Kontinuierliche Datensicherung (Backup) von kritischen Systemen zur Gewährleistung von **Datenredundanz**.
* Nutzung von Multi-Faktor-Authentifizierung.
* Nutzung von mehr als einem Datenspeicher.
* Einsatz von Ersatz-Stromversorgung.
* Implementierung von Web Application Firewalls (WAFs) zum Schutz der Systeme vor DoS- und DDoS-Angriffen.

**Cloud-Computing**

Ein Konzept, bei dem eine dritte Partei wie Amazon oder Google mit der Verwaltung der IT-Infrastruktur eines Unternehmens beauftragt wird.

* Nutzung von **Cloud Computing** für Systeme, die eine Verfügbarkeit von 99,99 % erfordern.

#### Praxisnahes Beispiel zum Verständnis der Beeinträchtigung der Verfügbarkeit

Die meisten Cyberangriffe beeinträchtigen die Verfügbarkeit von Systemen. Wir beschreiben hier kurz den Ransomware-Angriff auf Colonial Pipeline, durch den die Verfügbarkeit von Flugzeugtreibstoffen und Benzin unterbrochen wurde (Wilkie, 2021):

Der Ransomware-Angriff auf Colonial Pipeline war ein ausgeklügelter Cyberangriff, der im Jahr 2021 stattfand. Colonial Pipeline ist das größte Ölpipelinesystem in den USA und besteht aus mehr als 8.800 km an Pipelines. Am 7. Mai 2021, kurz vor 5 Uhr morgens, stellte ein Mitarbeitender fest, dass sein Unternehmen angegriffen worden war, weil er eine Lösegeldforderung auf einem System der IT-Infrastruktur von Colonial fand. Die Daten des Unternehmens waren gehackt worden, und die Angreifenden forderten ein Lösegeld von 5.000.000 $ für die Freigabe der Daten.

Die Pipeline wurde sofort abgeschaltet, um den Angriff einzudämmen und die Ausbreitung der Schadsoftware über andere Teile des operativen Netzwerks, das den Betrieb der Pipeline steuerte, zu verhindern. Diese sofortige Abschaltung führte zu erheblichen Unterbrechungen der Gaslieferungen an die Ostküste, und an den Zapfsäulen bildeten sich lange Schlangen von Lastwagen. Auch der Flugbetrieb wurde unterbrochen (Wilkie, 2021).

Das oben beschriebene Szenario ist ein Beispiel für die verheerenden Auswirkungen einer Beeinträchtigung der Verfügbarkeit kritischer Infrastrukturen.

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Das dritte wichtige Konzept der CIA-Triade ist *Verfügbarkeit*.

1. SLA ist ein schriftliches Dokument und beschreibt die …

* Dienstleistungen, welche die Kund:innen für den Dienstanbieter erbringen.
* *Dienstleistungen, die der Dienstleister für die Kund:innen erbringt.*
* Dienstleistungen, die von einem Kunden für einen anderen Kunden erbracht werden.
* Dienstleistungen, die von einem Dienstleister für einen anderen Dienstleister erbracht werden.

1. Was sind die möglichen Folgen von DoS-Angriffen?

Veröffentlichung vertraulicher Daten

Rufschädigung (Reputationsverlust)

*Nicht verfügbarer Dienst*

1. Nennen Sie zwei gängige Bedrohungen für die Verfügbarkeit von Systemen.

*DoS-Angriffe.*

*DDoS-Angriffe.*

*Ransomware-Angriffe.*

*Unterbrechung der Stromversorgung.*

*Stürme.*

*Löschung sensibler Daten.*

## 1.4 Bekannte IT-Sicherheitsprobleme

Jede Web-Anwendung – egal ob es sich um eine große Bank handelt, die täglich Millionen und Milliarden von Dollar an Transaktionen abwickelt, oder um die Homepage eines mittelständischen Unternehmens – könnte ein lohnendes Ziel für bösartige Akteure sein. Hacker oder Cyberkriminelle suchen sich ihre Opfer gerne nach Schwachstellen aus. Systeme, die kleiner sind und vielleicht nicht einmal sensible Daten enthalten, könnten attraktivere Ziele sein, weil sie viel leichter zu manipulieren oder zu hacken sind. Dies kann auch als Kosten-Nutzen-Ansatz bezeichnet werden.

Außerdem könnten Beauftragte für die IT-Sicherheit der Meinung sein, dass die Sicherung einer Web-Anwendung oder einer Website bereits eine starke Schutzmaßnahme für einen Server darstellt. Ein professionellerer Ansatz besteht darin, jede Sicherheitsmaßnahme oder Gegenmaßnahme im Bereich der Cybersicherheit als zusätzliche Schutzschicht zu betrachten. Mit jeder zusätzlichen Schicht werden die Daten auf ein akzeptables Sicherheitsniveau gebracht. Die Zwei- oder Mehrfaktor-Authentifizierung bietet beispielsweise eine zusätzliche Authentifizierungsebene, falls jemandem das Hauptpasswort eines Tages gestohlen wird. In diesem Beispiel haben wir zwei Sicherheitsebenen, das Passwort sowie die Multi-Faktor-Authentifizierung, die den **Work Factor** (Arbeitsfaktor) des Hackers erhöhen würde (Escobedo, 2021).

**Work Factor**

Zeit und Aufwand, die ein Hacker für die Manipulation eines Systems benötigt.

### Verständnis von Sicherheitsproblemen

Ein Sicherheitsproblem ist eine nicht behobene **Schwachstelle** in einem Netzwerk, einem System oder einer Anwendung, die ein Hacker ausnutzen kann, um Schaden anzurichten. Dazu können Schwachstellen in den Produktionsservern und den Anwendungen gehören, welche die Kund:innen mit dem Unternehmen verbinden. Web-Sicherheitsprobleme müssen berücksichtigt werden, sobald sie aufgedeckt werden, denn Web-Anwendungen gelten als das erste Ziel von Angreifenden und als Einstiegspunkt in das interne Netzwerk eines Unternehmens (Escobedo, 2021).

**Schwachstelle**

Eine Schwäche, die ein Hacker zur Manipulation eines Systems ausnutzt, z. B. ein schwaches Passwort.

Wenn Unbefugte auf Kundendaten zugreifen können, verlieren Unternehmen das Ansehen und das Vertrauen ihrer Kund:innen. Daher nehmen Unternehmen die Cyber- und Informationssicherheit ernst. Datenschutzverletzungen nehmen trotz der Bedeutung der Sicherung von Kundendaten exponentiell zu. Diese Datenschutzverletzungen sind sowohl auf unzureichende Sicherheitsmaßnahmen als auch auf technisch versierte Cyberkriminelle zurückzuführen (Lumen, o. D.).

In den folgenden Absätzen wollen wir die wichtigsten Sicherheitsprobleme sowie einige Maßnahmen zum Schutz von Daten und Unternehmen erörtern (Escobedo, 2021).

#### Ransomware-Angriff

Das Ziel von Hackern bei diesem Angriff ist es, die vollständige Kontrolle über die Daten des Opfers zu erlangen. Die Angreifenden erreichen dies, indem sie die Daten verschlüsseln und dann ein Lösegeld (Zahlung) in Bitcoin im Austausch für die Entschlüsselung der Daten verlangen. Hacker drohen Unternehmen oder Nutzenden manchmal auch damit, ihre sensiblen Daten an die Öffentlichkeit zu geben, wenn sie nicht bis zum Fälligkeitstermin zahlen.

Häufige Sicherungen (Backups) der Systemdaten stellen eine der besten Schutzmaßnahmen gegen einen Ransomware-Angriff dar.

#### Entfernte Code-Ausführung (RCE = Remote Code Execution) oder Code-Injektion

Durch RCE versuchen Angreifende, sich die Rechte zur Ausführung ihres bösartigen Codes zu verschaffen. Bei RCE suchen Hacker nach den Teilen der Web-Anwendung, die Eingaben der Nutzenden aufnehmen, wie z. B. ein Zulassungs- oder Registrierungsformular, Suchfelder usw. Die Hacker versuchen dann, ihren bösartigen Code in diese Eingabeformulare einzuschleusen und so die Anwendung schließlich zu manipulieren.

Die Eingabebereinigung ist eine Sicherheitsmaßnahme, die bösartigen Code in den Eingaben sucht und für die geregelte Weiterverarbeitung ausfiltert.

#### Malware-Angriff

Schadsoftware wird auch als bösartige Software bezeichnet, ein Überbegriff für Viren, Trojanische Pferde, Rootkits, Spyware usw. Sie alle werden für ein gemeinsames Ziel eingesetzt, nämlich die Manipulation von Systemen oder Datenschutzverletzungen. Bei Schadsoftware handelt es sich um bösartigen Code, der auf dem Zielsystem ausgeführt wird und alle Daten für Ransomware verschlüsselt oder sich dort versteckt und die Aktivitäten des Zielsystems (z. B. eingegebene Passwörter) erfasst. Abgesehen von diesen beiden Beispielen kann Schadsoftware auch andere bösartige Aktivitäten durchführen.

Aktualisierte Antivirenprogramme stellen die wichtigste Sicherheitsmaßnahme zum Schutz vor einer Schadsoftware-Infektion von bösartigen Websites dar.

#### Distributed-Denial-of-Service-Angriff (DDoS-Angriff)

Das Hauptziel von Angreifenden ist hierbei nicht der Diebstahl von Daten, sondern die Störung des Dienstes. Wenn zum Beispiel unnötiger Datenverkehr initiiert wird, wird der Server überlastet und ist nicht mehr in der Lage, legitime Anfragen von befugten Nutzenden zu bearbeiten.

Richtig konfigurierte Firewalls können die erste Verteidigungslinie gegen DDoS-Angriffe sein.

#### Credential-Stuffing-Angriff (Ausfüllen von Zugangsdaten)

Die Wiederverwendung eines aufgedeckten E-Mail-Kontos und Passworts wird als Credential Stuffing bezeichnet. Dies ist eine Art von Brute-Force-Angriff. Wenn es Hackern gelingt, eines Ihrer E-Mail-Konten mit Passwort auszuspähen, können sie versuchen, damit in weitere Konten einzudringen, bei denen möglicherweise die gleiche E-Mail und das gleiche Passwort genutzt werden.

Die beste Sicherheitsmaßnahme gegen diesen Angriff besteht darin, niemals dieselbe Kombination aus Benutzernamen und Passwort oder zumindest andere Passwörter für sonstige Konten zu verwenden. Außerdem verhindert die Zwei-Faktor-Authentifizierung diesen Angriff, selbst wenn ein schwaches Passwort verwendet wird.

#### Brute-Force-Angriff

Bei diesem Angriff versuchen Hacker, das Passwort eines bestimmten Kontos herauszufinden, indem sie alle möglichen Kombinationen für dieses E-Mail-Konto ausprobieren. Dazu nutzen sie Hacking-Werkzeuge, mit denen dieser Prozess automatisiert wird. Für ein bestimmtes Konto könnten zum Beispiel 1 Million Passwörter ausprobiert werden, bis das richtige gefunden wird.

Dies kann über eine Richtlinie verhindert werden, die eine Kontosperrung nach einer bestimmten Anzahl fehlerhafter Anmeldeversuche erzwingt. Heute wird bei den meisten Websites eine Sicherheitsfunktion genutzt, die diesen Angriffsvektor verhindert.

#### Probleme mit schwachen Passwörtern

Es liegt in der menschlichen Natur, leicht zu merkende Passwörter zu nutzen, wie z. B. das Geburtsdatum, den Namen eines Elternteils usw. Solche schwachen Passwörter sind Schwachstellen, die von Hackern zum Eindringen in ein System ausgenutzt werden können. Dazu nutzen sie Hacking-Werkzeuge mit Datenbanken aus häufig verwendeten Passwörtern.

Zur Verteidigung gegen solche Angriffe muss für die Authentifizierung ein sicheres Passwort verwendet werden, das mindestens 18 Zeichen enthält. Eine Kombination aus Sonderzeichen, Buchstaben und Zahlen in einem Passwort wird als komplex bezeichnet. So gilt beispielsweise „2@abc!dgc“ als komplexes Passwort, während „OnceUponaTimeinFloridaCity“ zwar ein starkes, aber kein komplexes Passwort darstellt, weil es nicht mehrere Zeichenarten enthält. Ein starkes Passwort ist für Hacker viel schwieriger zu knacken als ein komplexes Passwort (Escobedo, 2021).

#### Social Engineering (soziale Manipulation)

Social Engineering bezieht sich auf alle nicht-technischen Methoden, mit denen Hacker Daten oder Systeme ihrer Opfer gefährden können. Der primäre Angriffsvektor beim Social Engineering sind die sozialen Medien, wo die persönlichen Daten eines Opfers aufgedeckt werden können. Im nächsten Schritt versuchen die Hacker, durch bewusste Manipulation mit falschen Informationen das Vertrauen des Opfers zu gewinnen. Zum Beispiel tarnen sie sich als Dienstleister oder Bankangestellte. Der Hauptzweck eines solchen Angriffs ist es, wichtige Informationen zu erlangen oder einen befugten Nutzenden zu ungewollten, aber katastrophalen Aktivitäten zu verleiten. Beim Social Engineering geht es um das Sammeln von frei zugänglichen Informationen **(Open Source Intelligence)**.

**Open Source Intelligence (OSINT)**

Aufklärung von Informationen über ein Opfer aus sozialen Medien und anderen Online-Plattformen mit Hilfe kostenloser Werkzeuge und Ressourcen.

Rigorose Schulungen zum Sicherheitsbewusstsein sind die beste Vorbeugung gegen Social Engineering.

#### Phishing und Spear-Phishing

Bei einem Phishing-Angriff verschicken Hacker gefälschte E-Mails an Tausende oder sogar Millionen von Zielpersonen. Diese E-Mails scheinen von einer offiziellen Quelle zu stammen und enthalten Links, die den Empfänger dazu verleiten, darauf zu klicken. Nach dem Klick auf diesen Link lädt sich die Schadsoftware auf das System des Opfers herunter und manipuliert es.

Spear-Phishing ist im Grunde dasselbe wie Phishing, zielt aber direkter auf einen oder ein paar hochrangige Mitarbeitende wie den Geschäftsleiter eines Unternehmens ab.

Solche Angriffe lassen sich am besten durch monatliche Schulungen zum Sicherheitsbewusstsein der Mitarbeitenden abwehren. Nach jeder Schulung sollte ein solcher Phishing-Angriff simuliert werden, um die Reaktionen der Nutzenden darauf zu analysieren.

#### Mangelnde Patches oder Aktualisierungen

Die Verwendung veralteter, nicht aktualisierter oder nicht gepatchter Programme stellt eines der häufigsten Sicherheitsprobleme dar. Wenn ein Programm nicht laufend gepatcht oder aktualisiert wird, können Angreifende diese Schwachstelle nutzen und sich in ein System hacken.

Die einfachste Möglichkeit zur Verhinderung solcher Sicherheitsprobleme besteht darin, die gesamte Software des Systems regelmäßig auf die neuesten Versionen zu aktualisieren.

#### Insider-Bedrohungen

Ein sehr gebräuchlicher Begriff im Bereich der Informations- und Cybersicherheit ist Insider-Bedrohung. Jede Person, der wie einem Mitarbeitenden vertraut wird, könnte eine Insider-Bedrohung sein, die ein Unternehmen von innen heraus schädigen könnte.

Um dies zu verhindern, müssen neue Mitarbeitende einer strengen Überprüfung unterzogen werden. Darüber hinaus können solche Bedrohungen durch Insider oder befugte Mitarbeitende eingedämmt werden, indem ihre Zugriffsrechte auf die Erfüllung der zugewiesenen Aufgabe begrenzt werden.

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Die Wiederverwendung eines aufgedeckten E-Mail-Kontos und Passworts durch Hacker wird als *Credential Stuffing* bezeichnet.

1. Welcher Begriff wird für „die Zeit und den Aufwand, die ein Hacker für die Manipulation eines Systems benötigt“ verwendet?

*Work Factor.*

1. Nennen Sie zwei gängige Probleme in der Informationssicherheit.

*Phishing.*

*Spear-Phishing.*

*Ransomware-Angriffe.*

*Insider-Bedrohungen.*

*Ungepatchte Software.*

*Schwache Passwörter.*

Zusammenfassung

Beim Studium der Informationssicherheit (z. B. Cyber-Abwehr, Penetrationstests und Bedrohungsjagd) sollten wir uns mit den drei Hauptsäulen der Informationssicherheit auseinandersetzen: Vertraulichkeit, Integrität und Verfügbarkeit, auch bekannt als CIA-Triade (*confidentiality*, *integrity* und *availability*). Für Studierende oder Fachleute der IT-Sicherheit ist das gründliche Verständnis dieser drei Schlüsselaspekte unerlässlich.

In einem gegebenen Szenario müssen Studierende der Cybersicherheit bewerten, welcher Aspekt beeinträchtigt wird. Wenn ein unbefugter Zugriff auf die Daten erfolgt, ist die Vertraulichkeit gefährdet. Wenn Unbefugte Daten schreiben oder verändern, ist die Datenintegrität gefährdet. Wenn ein Dienst, z. B. eine Website, unterbrochen wird, ist ihre Verfügbarkeit beeinträchtigt. Alle drei Aspekte der Sicherheit sind wichtig, aber ihre spezifische Bedeutung hängt vom jeweiligen Szenario ab. So spielt zum Beispiel die Vertraulichkeit eine wichtige Rolle für personenbezogene Daten, wohingegen die Verfügbarkeit wichtig für Notfallalarme ist.

Dennoch kommt es immer wieder zu Sicherheitsproblemen und Sicherheitslücken. Zum Schutz von Vermögensgütern vor Hackern oder Cyberangriffen ist ein gutes Verständnis der bekannten Sicherheitsprobleme unerlässlich. Deshalb müssen sowohl technische als auch nicht-technische Mitarbeitende regelmäßig zum Thema IT-Sicherheit geschult werden.

# Lektion 2 – Messung von Cyber-Bedrohungen

**Lernziele**

Nach Abschluss dieser Lektion werden Sie in der Lage sein,

… das Konzept der Messung im Allgemeinen und insbesondere im Zusammenhang mit Cyber-Bedrohungen zu verstehen.

… das Konzept der Metriken und die Gründe für Messungen zu analysieren.

… Methoden zur Messung von Bedrohungen anhand einer Bedrohungsmatrix für ein bestimmtes Szenario zu nutzen.

… die Wahrscheinlichkeit für die häufigsten Cyberangriffe zu kennen.

… das Konzept der schwarzen Schwäne (*Black Swans*) im Allgemeinen und insbesondere im Kontext der Cybersicherheit zu bewerten.

# 2. Messung von Cyber-Bedrohungen

## Einführung

Für fast alle Unternehmen und Organisationen auf der Welt ist die Informationstechnologie (IT) mittlerweile die wichtigste Voraussetzung für den Erfolg. Die IT sorgt dafür, dass die verschiedenen Geschäftsbereiche wie z. B. Vertrieb, Telekommunikation, Öl und Gas sowie Finanzen eine hohe Wirkung und Effizienz aufweisen. Die Technologiegiganten wie Meta, Google und Amazon verlassen sich für den täglichen Geschäftsbetrieb auf ihre großen IT-Infrastrukturen. Aber das eigentliche Problem ist, dass Menschen unvollkommen sind und daher unvollkommene Technologien erfinden – Technologien, die anfällig für Cyber-Bedrohungen sind. Diese Bedrohungen können zu Cyberangriffen und Datenschutzverletzungen führen (Leirvik, 2022, S. 3).

Cyber-Bedrohungen haben die konventionellen Bedrohungen wie z. B. terroristische Aktivitäten überholt. Jedes mit dem Internet verbundene Unternehmen ist anfällig für Cyber-Bedrohungen, wenn nicht die notwendigen Maßnahmen getroffen werden. Für die Bewertung der Widerstandsfähigkeit einer Organisation gegenüber einem Cyberangriff ist eine starke Strategie zwingend erforderlich. Eine solche Bewertung ist jedoch nicht möglich, ohne die Konzepte und Strategien zu lernen, mit denen Cyberbedrohungen und Risiken gemessen werden (Hubbard & Seiersen, 2016, S. 7–8).

In dieser Lektion werden einige der wichtigsten Konzepte zur Messung von Cyber-Bedrohungen eingehend erörtert. Wir wollen lernen, wie Angreifende zu denken und die Auswirkungen einer Cyber-Bedrohung einzuschätzen, die zu einem Cyberangriff mit potenziellem wirtschaftlichen Schaden und Rufschädigung (Reputationsverlust) führen kann. Wir werden erörtern, wie sich eine Bedrohung messen lässt – dazu besprechen wir die wichtigsten Methoden wie z. B. die Bedrohungsmatrix. Die Messung von Cyber-Bedrohungen ermöglicht es Sicherheitsfachleuten, die potenziellen bösartigen Aktivitäten von Cyberkriminellen und deren Auswirkungen zu bewerten.

## 2.1 Konzept der Bedrohungsmessung

Wenn wir über die Messung von Bedrohungen oder Risiken im Bereich der Cybersicherheit sprechen, müssen wir zunächst das Konzept der Messung erläutern und verstehen. Wir müssen auch über den Mythos sprechen, dass manche Dinge in der Cybersicherheit nicht messbar sind.

Es gibt drei missverstandene Begriffe, aufgrund derer Cybersicherheit für nicht messbar gehalten werden kann. Eine falsche Interpretation dieser drei Begriffe könnte zu dem Missverständnis führen, Cybersicherheit sei nicht messbar. Diese Begriffe sind Konzept, Objekt und Methode. Wir betrachten diese drei Begriffe nachstehend im Überblick (Hubbard & Seiersen, 2016, S. 20–21):

1. Das Konzept der Messung kann leicht falsch verstanden werden. Wenn wir klar verstehen, was Messung bedeutet, verstehen wir auch, dass in der Cybersicherheit alles analysiert werden kann.
2. Das zu messende Objekt muss genau betrachtet werden. Ohne eine klare Definition des zu messenden Objekts kann niemand mit der Messung des Objekts beginnen.

**Materiell und immateriell**

Güter oder Vermögenswerte, die sich anfassen lassen, sind greifbar oder materiell. Solche, die nicht anzufassen sind, heißen nicht greifbar oder immateriell.

1. Die Methoden und Verfahren müssen genau definiert werden. Wenn die zur Messung verwendeten Methoden gut bekannt und klar definiert sind, lassen sich problemlos sowohl **materielle als auch immaterielle** Güter messen.

Um sich diese drei Elemente zu merken, lässt sich die Eselsbrücke „.com“ aus den englischen Anfangsbuchstaben verwenden: „c“ für das Konzept (*concept*), „o“ für ein Objekt und „m“ für eine falsche Vorstellung (*misconception*). Wenn wir unsere Vorstellungen von diesen drei gemeinsamen Begriffen klären, wird klar, dass alles messbar ist.

### Das Konzept der Messung

Wenn Cybersicherheitsfachleute zum Begriff der Messung gefragt werden, könnten dies mögliche Antworten sein: „auf eine Zahl reduzieren“, „quantifizieren“ oder „einen genauen Wert berechnen“. Aus all diesen Antworten lässt sich explizit oder implizit folgern, dass bei der Messung kein Fehler zulässig ist und es sich um eine präzise Zahl handeln sollte.

Vielleicht haben wir alle schon einmal Sätze wie die folgenden gesagt oder gehört:

* Wenn wir die genauen Umstände eines Cyberangriffs oder einer Datenschutzverletzung nicht kennen, wie können wir dann die genauen Auswirkungen messen?
* Aufgrund der hohen Unsicherheit können wir die Wahrscheinlichkeit, dass ein Opfer durch einen verteilten Denial-of-Service-Angriff beeinträchtigt wird, nicht berechnen.

Aussagen oder Vorstellungen wie diese zeigen eine hypothetische Definition oder ein Konzept, das unwissenschaftlich ist und nichts mit den tatsächlichen Entscheidungsprozessen zu tun hat. Wenn also nur nach Zahlen gemessen wird, ist es schwierig, diese Methoden in der Cybersicherheit einzuführen (Hubbard & Seiersen, 2016, S. 21).

### Definition der Messung

Für praktische Entscheidungsprozesse müssen Messungen als Beobachtungen oder Meinungen behandelt werden, die **Unsicherheit** oder Zweifel quantitativ abschwächen. Für die Messung würde weniger Unsicherheit schon reichen, wenn die Unsicherheit nicht vollständig beseitigt werden kann. Für manche Wissenschaftler:innen ist eine Messung ein probabilistisches Verfahren. Messung kann definiert werden als die quantitative Verringerung der bei Beobachtungen festgestellten Unsicherheiten. Zum besseren Verständnis dieser Definition werfen wir einen Blick auf eine beispielhafte Aussage zu Ergebnissen auf der Grundlage einer Messung: „Mit 80-prozentiger Wahrscheinlichkeit wird ein Schadsoftware-Angriff auf einen Webserver diesen zwischen 2 und 9 Stunden für die Nutzenden unzugänglich machen.“ Die Aussage ist zwar immer noch mit einer gewissen Unsicherheit behaftet, aber zumindest wurde diese durch die Angabe der Wahrscheinlichkeit und möglichen Folgen eines Angriffs etwas verringert. Damit können Cyber-Abwehrteams die notwendigen Sicherheitsmaßnahmen ergreifen, bevor ein Angriff erfolgt. Ohne ein Verständnis des Konzepts der Messung im Bereich der Cybersicherheit wäre dies nicht möglich. Solche Messergebnisse gelten gemäß gängiger Sicherheitsstandards als annehmbar. Sie liefern Ergebnisse mit einer gewissen Unsicherheit (Hubbard & Seiersen, 2016, S. 21).

**Unsicherheit**

Wenn die Wahrscheinlichkeit eines Ereignisses (wie z. B. eines Cyberangriffs) nicht bekannt ist, sprechen wir von Unsicherheit.

### Klassifizierung von Messskalen

In diesem Teil des Lernzyklus wollen wir uns auf verschiedene Messskalen konzentrieren. Damit können wir unsere Messkonzepte im Bereich der Cybersicherheit verbessern. Wenn wir über Messungen sprechen, denken wir an bestimmte Maßeinheiten, wie z. B. die Dauer des Netzwerkausfalls in Stunden oder den Verlust von Geld in Dollar pro Monat.

Im Gegensatz dazu nutzen Fachleute für Cybersicherheit Skalen wie hoch, mittel oder niedrig, um Bedrohungen und Risiken zu messen. Diese Skalen sind in der Cybersicherheitsbranche, bei internationalen Standards und bei bewährten Vorgehensweisen für Risikobewertungen üblich. In der Cybersicherheit sehen wir oft Begriffe wie „Wahrscheinlichkeit“ und „Auswirkung“. Dies sind subjektive Einschätzungen und werden auf einer Skala von 1 bis 5 bewertet. Diese Skalen werden dann für weitere Risikobewertungen kombiniert und ergeben eine Skala von niedrig über mittel bis hoch.

An dieser Stelle sei angemerkt, dass auch im Bereich der Cybersicherheit Messungen nicht ganz ohne quantitative Angaben auskommen. Zumindest muss die Unsicherheit in Zahlen angegeben, d. h. quantifiziert werden. Allerdings muss die zu beurteilende Größe nicht unbedingt quantitativ sein, sondern sie kann auch rein qualitativer Natur sein. Hier sind einige Beispiele für solche qualitativen Messungen:

* Ein Thema, das nur mit „Ja“ oder „Nein“ zu bewerten ist.
* Die Frage, ob es wahrscheinlich ist, dass es Ende dieses Jahres zu einem Cyberangriff oder einer Datenschutzverletzung kommen wird.
* Die Frage, ob wir eine Cyberversicherung in Anspruch nehmen werden.

Aber was ist mit dem quantitativen Maß, das für die Unsicherheit unserer obigen Analyse angegeben werden soll? Dies muss noch in Zahlen ausgedrückt werden. Die folgenden Beispiele zeigen qualitative Maße an:

* Es besteht eine 60-prozentige Chance, dass Ende dieses Jahres ein Cyberangriff stattfindet.
* Die Wahrscheinlichkeit, dass eine Cyberversicherung in Anspruch genommen wird, liegt bei 25 %.

Die oben betrachteten Konzepte zur Messung sind wichtig und enthalten viele wichtige Lektionen für Cybersicherheitsspezialist:innen und ‑manager:innen. Der weit verbreitete Eindruck, dass Messungen immer präzise Größen sind, berücksichtigt nicht den Nutzen einer Verringerung der Unsicherheit, wenn deren vollständige Beseitigung nicht machbar oder zu kostspielig ist. Und keineswegs müssen alle Messungen eine traditionelle Größe darstellen.

Zum Abschluss unserer Diskussion über Messungen geht es um diskrete Werte von Interesse, wie z. B. „Wird es zu einem schrecklichen Cyberangriff kommen?“, sowie um kontinuierliche Werte oder Größen, wie z. B. „Wie viel würde uns eine Datenschutzverletzung kosten?“. Entscheidungsträger in der Wirtschaft treffen ihre Entscheidungen mit einer gewissen Unsicherheit (Hubbard & Seiersen, 2016, S. 22–24).

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

In der Cybersicherheit gibt es den Mythos, dass manche Dinge nicht *messbar* seien.

1. Die Eselsbrücke für die drei falschen Vorstellungen zu Messungen lautet *.com.*
2. Nennen Sie zwei missverstandene Begriffe zu Messungen im Bereich der Cybersicherheit.

*Konzept*

*Objekt*

*Methode*

## 2.2 Metriken zur Cyber-Bedrohung

Jede Organisation oder Person mit der Absicht, Schaden anzurichten, stellt eine Bedrohung dar. Es ist viel einfacher, die Bedrohungen aufzuzählen, als zu erklären, was Bedrohungen letztendlich sind. Außerdem sind Erklärungen einfacher als Messungen. Daher bevorzugen die meisten Unternehmen die Auflistung von Bedrohungen. Nur wenige Organisationen können sie sinnvoll erklären, und noch weniger können sie sinnvoll messen. Dies führt zu vagen Beschreibungen von Cyber-Bedrohungen. Solche Bereiche lassen keine mühelosen Messungen zu. Die Unternehmen und Führungskräfte sind für das Bedrohungsmanagement verantwortlich, weil sie ihr Budget erst nach einem ordnungsgemäßen Bedrohungsmanagement genehmigen können.

Die Messung von Cyber-Bedrohungen ist ein Bereich, der sich einfachen Messungen widersetzt. Das ist der Grund, warum es leider an Verständnis für die Anwendung und Definition von Bedrohungsmetriken mangelt und warum die Messung von Bedrohungen meistens übergangen wird.

Die präzise und konsequente Messung von Bedrohungen hat viele Vorteile. Eine genaue Messung der Bedrohung hilft zum Beispiel, eine bestimmte Situation besser zu analysieren. Dies kann auch helfen, die potenziellen Auswirkungen zu analysieren oder die Gefährlichkeit von Bedrohungen zu bestimmen. Kurz gesagt, gute und konsistente Bedrohungsmessungen unterstützen ein vernünftiges Risikomanagement.

Um all diese wichtigen Konzepte zu verstehen und diese Probleme im Bereich der Cyber-Bedrohungen anzugehen, erörtern und erklären wir Bedrohungsmetriken für die klare und konsistente Charakterisierung und Beschreibung von Bedrohungen (U.S. Department of Energy et al., 2017, S. 3, 7). Bevor wir jedoch Bedrohungsmetriken und Bedrohungsmatrizen analysieren, wollen wir in den folgenden Unterlernzyklen zunächst das Konzept der Metrik erörtern (U. S. Department U. S. Department of Energy et al., 2017, S. 9–10).

### Was ist eine Metrik?

Im Allgemeinen ist eine Metrik definiert als „ein Messstandard“. Im Bereich der Sicherheit wird er jedoch als „konsistenter Messstandard“ bezeichnet, der die Messung bedeutsamer Verhaltensweisen und Attribute ermöglicht. Zum Beispiel wird ein *Kilogramm* als Einheit in einer Metrik zur Messung des Gewichts bzw. der Masse verwendet, und die *Anzahl der bestandenen Prüfungen* ist eine Metrik, mit der die Gesamtqualität der Studierenden und ihrer Studien gemessen werden kann (U.S. Department of Energy et al., 2017, S. 9).

Die Begriffe „Metrik“ und „Maß“ sollten nicht verwechselt werden. Zur Verdeutlichung: „Metrik“ ist eine Einheit, die uns beim Messen hilft, wohingegen ein „Maß“ die genaue Charakterisierung einer Leistung beschreibt. Wenn also die Anzahl der Cyberangriffe pro Jahr die Metrik ist, wäre das Maß der beobachtete Wert, zum Beispiel 12.

### Warum werden Metriken verwendet?

Wenn etwas mit Hilfe konsistenter Metriken gemessen wird, verbessern wir unsere Fähigkeit, es zu steuern, zu verwalten, zu verstehen, zu vergleichen – und im Falle einer Bedrohung uns davor zu schützen und es abzuwehren. Laut dem Leistungstechniker H. James Harrington (U.S. Department of Energy et al., 2017, S. 9) gilt: „Wenn wir etwas nicht messen können, können wir es nicht verstehen. Wenn wir es nicht verstehen können, können wir es nicht steuern. Wenn wir es nicht steuern können, können wir es auch nicht verbessern.“

### Was macht eine gute Metrik aus?

Eine gute Metrik weist in der Regel verschiedene traditionelle Merkmale auf, von denen wir hier die wichtigsten wiedergeben:

* Eine Qualitätsmetrik ist klar, eindeutig und unmissverständlich.
* Eine gute Metrik unterstützt eine vernünftige Entscheidungsfindung und verhindert subjektive Interpretationen.
* Gute Metriken helfen z. B. bei der Umsetzung quantitativer statt qualitativer Skalen.
* Eine gute Metrik ermöglicht es uns, Ergebnisse in Zahlen auszudrücken (quantitativ) und nicht in Bewertungen wie niedrig, mittel und hoch (qualitativ).
* Eine gute Metrik hilft dabei, auch immateriellen (nicht greifbaren) Vermögensgütern eine Zahl zuzuweisen.

### Was macht eine gute Bedrohungsmetrik aus?

Eine gute und hochwertige Bedrohungsmetrik ist effizient, eindeutig und klar. Außerdem kann sie, wie im vorigen Unterlernzyklus erwähnt, eine qualitativ hochwertige und vernünftige Entscheidungsfindung unterstützen.

### Verstehen einer Bedrohungsmatrix

Bei einer Bedrohungsmatrix geht es um das Verständnis von Bedrohungsmetriken. Eine Metrik ist nicht mit einer Matrix gleichzusetzen; vielmehr werden mehrere Metriken zu einer Matrix kombiniert. Zum besseren Verständnis einer Bedrohungsmetrik müssen wir zunächst das grundlegende Konzept einer Bedrohungsmatrix verstehen, wie in der folgenden Tabelle dargestellt. Da die Messung von Bedrohungen den Rahmen dieses Unterlernzyklus sprengen würde, geben wir hier nur einen Überblick über diese Bedrohungsmatrix. Das Hauptziel einer allgemeinen Bedrohungsmatrix besteht darin, die Attribute zu erkennen, die Bedrohungsanalysten bei der Charakterisierung moderner Bedrohungen anhand ihrer Fähigkeiten unterstützen (U.S. Department of Energy et al., 2017, S. 13).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Allgemeine Bedrohungsmatrix | | | | | | | | |
| **Bedrohungsstufe** | **Bedrohungsprofil** | | | | | | | |
| **Verpflichtung** | | | **Ressourcen** | | | | |
| **Intensität** | **Heimlichkeit** | **Dauer** | **Technisches**  **Personal** | **Wissen** | | | **Zugriff** |
| **Cyber** | **Kinetisch** | |
| 1 | H | H | Jahre bis Jahrzehnte | Hunderte | H | | H | H |
| 2 | H | H | Jahre bis Jahrzehnte | Mehrere Dutzend | M | | H | M |
| 3 | H | H | Monate bis Jahre | Mehrere Dutzend | H | | M | M |
| 4 | M | H | Wochen bis Monate | Dutzende | H | | M | M |
| 5 | H | M | Wochen bis Monate | Dutzende | M | | M | M |
| 6 | M | M | Wochen bis Monate | Einzelne | M | | M | L |
| 7 | M | M | Monate bis Jahre | Dutzende | L | | L | L |
| 8 | L | L | Tage bis Wochen | Einzelne | L | | L | L |

Quelle: U.S. Department of Energy et al. (2017).

Die Charakterisierung von Bedrohungen ermöglicht es Analysten, eine spezifische Bedrohung vollständig zu definieren. Da es jedoch nicht möglich ist, jede spezifische Bedrohung einheitlich zu identifizieren, ermöglicht die allgemeine Bedrohungsmatrix den Behörden und Nachrichtendiensten, Bedrohungen mit einer gemeinsamen Terminologie zu klassifizieren.

Wie in der obigen Tabelle dargestellt, definieren die Spalten in einer Bedrohungsmatrix die potenziellen Attribute einer Bedrohung, während in den Zeilen die Fähigkeit der Bedrohung beschrieben wird. Warum sprechen wir hier von Attributen und Fähigkeiten, und welchen Zusammenhang haben sie mit der Metrik? Die Antwort ist, dass jedes Attribut durch eine einzigartige und spezifische Metrik bestimmt wird. Manche Metriken liefern qualitative Ergebnissen (z. B. hoch, mittel und niedrig), während der Rest quantitative Ergebnisse erzeugen (z. B. die jährlichen Kosten). Da es diese beiden Arten von Metriken in der Bedrohungsmodellierung gibt, brauchen wir einen umfassenden Rahmen, der sie an einer Stelle zusammenführt. Kurz gesagt, eine Matrix ist ein Modell oder ein Rahmen zur Organisation von Metriken (U.S. Department of Energy et al., 2017, S. 13–14).

Bis jetzt haben wir die Grundlagen einer Bedrohungsmatrix im Zusammenhang mit Bedrohungsmetriken und ‑attributen besprochen. Aber was ist mit dem Konzept der Fähigkeiten? Da Fähigkeiten mit den Beobachtungen und Messungen zusammenhängen, die auf der Grundlage von Metriken oder Attributen gemacht werden, würde eine genauere Betrachtung den Rahmen dieses Lernzyklus sprengen. Wir werden den Begriff der Fähigkeiten jedoch später im Zusammenhang mit der Messung von Bedrohungen ausführlicher behandeln.

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Es ist viel einfacher, Bedrohungen aufzulisten, als sie *zu erklären*.

1. Alles, was einen Schaden verursachen kann ist …

* ein Angriff.
* ein Risiko.
* *eine Bedrohung*.
* eine Schwachstelle.

1. Welcher Bereich der Cybersicherheit lässt sich nicht einfach messen?

*Der Bereich der Cyber-Bedrohungen.*

1. Nennen Sie zwei Merkmale einer Qualitätsmetrik.

*Klar*

*Kurz und bündig*

*Eindeutig*

*Unterstützt eine gute Entscheidungsfindung*

*Quantitative Messungen*

## 2.3 Messung der Bedrohung für eine Organisation

Das Konzept der Messung einer Bedrohung für eine Organisation lässt sich mit Hilfe der Tabelle „Allgemeine Bedrohungsmatrix“ illustrieren, die wir in Lernzyklus 2.2 bereits kurz besprochen haben. Bevor wir auf die Details der Matrix eingehen, sollten wir uns zunächst vergegenwärtigen, was Messung im Zusammenhang mit einer Bedrohung bedeutet. Eine Messung ist nichts anderes als eine Beobachtung auf der Grundlage einer Metrik. Wenn wir diese Konzepte der Messung und Metrik auf eine Tabelle wie die „Allgemeine Bedrohungsmatrix“ übertragen, dann sind die Spalten die Metriken oder Attribute, auf deren Grundlage die Beobachtungen gemacht und als Zeilen bzw. Fähigkeiten dargestellt werden. Das bedeutet, dass wir eine Bedrohung leicht messen können, wenn es uns gelingt, eine Bedrohungsmatrix für bestimmte Attribute einer Organisation zu erstellen.

### Bedrohungsattribute

Ein Bedrohungsattribut ist ein bestimmtes Merkmal einer Bedrohung. Die Merkmale einer Bedrohung legen in der Summe die Fähigkeit und Bereitschaft einer Bedrohung zum Erreichen ihres Ziels fest. Dennoch basieren sowohl die Fähigkeit als auch die Bereitschaft auf vielen separaten und vielfältigen Attributen. Daher ist jedes Attribut einer Bedrohung unverwechselbar, und keine zwei Attribute sind voneinander abhängig.

Bedrohungsattribute werden in zwei Gruppen unterteilt: Verpflichtungsattribute und Ressourcenattribute (U.S. Department of Energy et al., 2017, S. 14–15).

#### Verpflichtungsattribute

Verpflichtungsattribute sind die Merkmale, welche die Bereitschaft einer Bedrohung zur Erreichung des Ziels festlegen. Diese Merkmale zeigen die Fähigkeit einer Bedrohung an, denn sie veranschaulichen die Stärke einer Bedrohung zur Erreichung ihres Ziels. Bedrohungen, die sich stärker bemühen, werden ihr Ziel um jeden Preis erreichen, während Bedrohungen, die sich weniger bemühen, nicht so viel Antrieb zur Erreichung des Ziels haben.

Die Gruppe der Verpflichtungsattribute besteht aus drei verschiedenen Attributen:

1. **Intensität**: Sie ist definiert als die starke Entschlossenheit und Ausdauer einer Bedrohung bei der Verfolgung ihres Ziels. Es ist das Maß, wie weit eine Bedrohung zur Erreichung ihres Ziels gehen will und was sie zu riskieren bereit ist. Daher werden Bedrohungen mit höherer Intensität als gefährlicher und fataler angesehen, weil sie ihr Ziel so intensiv verfolgen.
2. **Heimlichkeit:** Während des Angriffs kann eine Bedrohung sich tarnen und so verborgen bleiben. Um die Geheimhaltung aufrechtzuerhalten, kann eine Bedrohung die Details über ihr Ziel, die Organisation der Bedrohung und ihre internen Operationen verschleiern. Eine getarnt vorgehende Bedrohung wird dafür sorgen, dass ihre internen Operationen und Strukturen vor der Außenwelt verborgen bleiben. Das Konzept der Open Source Intelligence (**OSINT**) ist hier von Bedeutung.

**OSINT**

Aufklärung von Informationen über ein Opfer aus sozialen Medien und anderen Online-Plattformen mit Hilfe kostenloser Werkzeuge und Ressourcen.

1. **Zeit:** Dies bezieht sich auf die Zeitdauer, in der ein Angreifender die Methoden zur Erreichung des Ziels plant, entwickelt und umsetzt. Im Zusammenhang mit einem Cyberangriff ist hier die benötigte Zeitdauer von der Planungsphase bis zur Umsetzung und Ausführung gemeint. Je mehr Zeit eine Bedrohung in die Verfolgung ihres Ziels investiert, desto größer ist ihre Fähigkeit zum Anrichten von Schaden.

#### Ressourcenattribute

Die Ressourcenattribute umfassen den Zugang, die Personen und das Wissen, die Angreifenden zur Erreichung ihres Ziels zur Verfügung stehen. Wir beschreiben diese drei Ressourcenmerkmale im Folgenden (U.S. Department of Energy et al., 2017, S. 15–16):

1. **Wissen:** Dazu gehören die praktischen und theoretischen Fähigkeiten von Angreifenden und wie diese Fähigkeiten zur Zielerreichung eingesetzt werden. Zum Wissen gehört auch die Fähigkeit der Angreifenden, sich in einem bestimmten Bereich weiterzubilden, Informationen auszutauschen und sich über die aktuellen Werkzeuge und Methoden auf dem Laufenden zu halten. Eine Bedrohung benötigt zur Erreichung ihres Ziels weniger Ressourcen und Zeit, wenn sie über umfassende Kenntnisse sowohl der **defensiven als auch der offensiven** Gegebenheiten verfügt. Wissen kann in zwei Kategorien aufgeteilt werden. Die erste ist das Cyber-Wissen, d. h. das praktische und theoretische Fachwissen über Netzwerke, Computersysteme und Anwendungen. Das zweite ist kinetisches Wissen über cyber-physische Systeme wie die Öl- und Gasindustrie, die Fertigung, die Energieerzeugung usw.

**Defensiv und offensiv**

Der Schutz eines Vermögensguts meint die Verteidigung, also die Defensive, während der Angriff auf ein Vermögensgut der Offensive entspricht.

1. **Technisches Personal:** Dies ist die Personengruppe, die eine Bedrohung für ein bestimmtes Ziel einsetzt. Diese Leute sind in ihren jeweiligen Bereichen hochqualifiziert und können neue Taktiken und Methoden entwickeln, die es in der Vergangenheit vielleicht noch nicht gab.
2. **Zugang:** Die Fähigkeit einer Bedrohung, eine ihrer Personen innerhalb eines eingeschränkten Systems zu platzieren. Auf ein zugangsbeschränktes System kann ohne höhere Berechtigungen nicht zugegriffen werden. Dieses Merkmal beschreibt die Fähigkeit einer Bedrohung, in ein zugangsbeschränktes und gesichertes System einzudringen. Je größer die Zugangsmöglichkeiten einer Bedrohung sind, desto mehr Sicherheitsmaßnahmen müssen für den Schutz des Systems ergriffen werden.

### Fähigkeiten und Profil einer Bedrohung

Die Messung der Bedrohung resultiert aus den Beobachtungen, die bei der Analyse und Überprüfung der allgemeinen Bedrohungsmatrix gemacht werden. Zur Beobachtung einer Bedrohungsmatrix sollten die Attribute, die wir zuvor im Detail besprochen haben, sehr gut verstanden werden. Wir wollen nun die Attribute mit ihren Fähigkeiten erörtern, was uns die Analyse, Beobachtung oder Messung einer Bedrohung ermöglicht. Zur Erstellung eines starken Bedrohungsprofils müssen vor allem zwei Randbedingungen berücksichtigt werden (U.S. Department of Energy et al., 2017, S. 16–17):

* Bedrohungen mit einem Profil der Stufe 1 werden bei jedem Attribut mit der höchsten Fähigkeit berücksichtigt.
* Bedrohungen der Stufe 8 sind diejenigen, die bei jedem Attribut die geringsten Fähigkeiten aufweisen.

Zweitens kann das technische Personal bei der Messung und Beobachtung einer Bedrohung dabei helfen, die Eigenschaften einer anderen Bedrohung zu verstehen und abzuleiten:

* Eine Bedrohung mit starkem technischem Personal wird sicherlich mehr Zugang, Wissen und Intensität aufweisen. Erfahrene Bedrohungsanalysten oder ‑forschende können solche Annahmen treffen und damit die Fähigkeiten anderer Attribute ableiten (U.S. Department of Energy et al., 2017, S. 16).
* Bedrohungen, die in der Kategorie „Technisches Personal“ nur eine „1“ aufweisen, verfügen beispielsweise nicht über so viel Wissen wie die der Kategorie „10“. Das liegt daran, dass Bedrohungen mit geringen personellen Ressourcen nicht in der Lage sind, sich Wissen anzueignen und es zu teilen.
* Eine Bedrohung braucht besseres technisches Personal für ein Attribut mit hoher Intensität. Technischem Personal auf der Stufe „1“ fehlt es an hoher Intensität, weil es keine Ausdauer und Entschlossenheit aufweist (U.S. Department of Energy et al., 2017, S. 16).

Anhand des Wissens einer Bedrohungsorganisation lassen sich auch Messungen und Beobachtungen durchführen: Bedrohungen mit großem Wissen werden dem Angriffsziel immer einen Schritt voraus sein, wenn dieses nicht auf dem neuesten Stand der aktuellen Cybersicherheitstrends ist. Hohes Cyberwissen einer Bedrohung meint sowohl theoretisches als auch praktisches Wissen.

Das letzte Attribut, das zur Messung einer Bedrohung hilfreich sein könnte, sind ihre Zugangsfähigkeiten und ‑möglichkeiten: Eine Bedrohung mit umfangreichem kinetischen Wissen und Cyber-Wissen wird in der Lage sein, ihren Zugang aufrechtzuerhalten, nachdem sie bereits in ihr Ziel eindringen konnte. Ein Angriffsziel kann ein Netzwerk, ein System oder eine Anwendung sein. Angreifende können ihren Zugang z. B. aufrechterhalten, indem sie ihre Berechtigungen von niedrig auf hoch ausweiten, wie z. B. auf „Root“ im Falle von Linux oder „Administrator“ beim Windows-Betriebssystem.

Zusammenfassung: In diesem Lernzyklus haben wir untersucht, wie wir eine allgemeine Bedrohungsmatrix für unsere Beobachtungen analysieren und eine Bedrohung auf der Grundlage ihrer Eigenschaften und Fähigkeiten messen können. Die in diesem Lernzyklus betrachtete Matrix ist sehr allgemein und kann deshalb als Bezugsgröße dienen. Zur Messung der konkreten Bedrohung einer Organisation können wir die Werte für jedes Attribut dann in diese Matrix eintragen. Wenn wir ein Profil einer Bedrohung erstellen können, d. h. sie auf der Grundlage der gegebenen Attribute und ihrer Fähigkeiten in einer Bedrohungsmatrix als Stufe 1 oder Stufe 2 (usw.) einstufen können, dann können wir die Bedrohung damit messen.

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Wir müssen die *allgemeine Bedrohungsmatrix* zur Messung einer Bedrohung heranziehen.

1. Eine Messung steht in engem Zusammenhang mit …

* einem Angriff.
* einem Attribut.
* einer Fähigkeit.
* *einer Beobachtung*.

1. Welcher Begriff definiert ein bestimmtes Merkmal einer Bedrohung?

*Attribut*

1. Nennen Sie drei Attribute einer Bedrohung aus einer Bedrohungsmatrix.

*Intensität*

*Zeit*

*Heimlichkeit*

*Wissen*

*Technisches Personal*

*Zugang*

## 2.4 Große Cyberangriffe und ihre Auswirkungen

Das Jahr 2021 gilt als eines der kritischsten Jahre im Hinblick auf massive Datenschutzverletzungen und Cyberangriffe, die kritische Infrastrukturen in Mitleidenschaft gezogen haben. Zu diesen Infrastrukturen gehörten Colonial Pipeline, Solar Winds und viele andere, bei denen es nach dem Angriff große Auswirkungen auf die Sicherheit und die Wirtschaft gab. Angreifende betrachteten Ransomware als ihr primäres Werkzeug für den Angriff auf mittelständische Unternehmen und kritische Infrastrukturen. Wenn wir über die Wahrscheinlichkeit von Cyberangriffen sprechen, müssen wir sie in Zahlen oder Prozentsätzen quantifizieren, um die Auswirkungen eines potenziellen Angriffs besser zu verstehen und die notwendigen Sicherheitsmaßnahmen zu treffen. Ohne die Wahrscheinlichkeit eines Angriffs zu kennen, lässt sich nicht festlegen, wie viel Geld in die Implementierung von Sicherheitsmaßnahmen zur Verhinderung und Erkennung eines potenziellen Cyberangriffs investiert werden sollte. In den folgenden Unterlernzyklen werden wir die wichtigsten Trends der gängigen Cyberangriffe in verschiedenen Sektoren der Branche erörtern. Dadurch können wir unser Verständnis der Landschaft großer Cyberangriffe und deren Wahrscheinlichkeit verbessern (Brooks, 2022).

### Unternehmen und Cyberangriffe

Obwohl auch Großunternehmen von massiven Datenschutzverletzungen betroffen sind, waren gerade mittelständische Unternehmen aufgrund des Mangels an angemessenen Sicherheitsmaßnahmen und technischem Fachwissen schon immer das einfachste Ziel für Hacker. Fast 43 % der Angriffe zielen auf kleine Unternehmen ab, von denen jedoch nur 14 % über die notwendigen Sicherheitsmaßnahmen zur Abwehr dieser Angriffe verfügen. Die Wahrscheinlichkeit eines Cyberangriffs steigt, wenn keine angemessenen Sicherheitsmaßnahmen implementiert sind. Aus diesem Grund tun sich mittelständische Unternehmen immer schwer mit einer angemessenen Verteidigung.

Die drei häufigsten Cyberangriffe und ihre prozentuale Wahrscheinlichkeit für mittelständische Unternehmen sind wie folgt (Brooks, 2022):

1. Social Engineering bzw. Phishing: 57 %
2. Gestohlene oder manipulierte Geräte: 33 %
3. Aufgedeckte oder manipulierte Anmeldedaten: 30 %

### Cyberangriffe im Gesundheitswesen

Laut einer kürzlich durchgeführten Umfrage im Gesundheitswesen berichteten 70 % der Befragten, dass sie mit Ransomware-Angriffen konfrontiert waren. Diese haben zu Verzögerungen bei Untersuchungen und Verfahren geführt, die schwerwiegende Folgen hatten, darunter auch ein Anstieg der Todesfälle bei Patient:innen. Mehr als die Hälfte der internetfähigen Geräte in Krankenhäusern weisen ausnutzbare Schwachstellen auf, wodurch die Daten und die Sicherheit der Patient:innen gefährdet würden (Brooks, 2022).

### Internet der Dinge (*IoT = Internet of Things*) und Cyberangriffe

Wie Semantic berichtet, sind IoT-Geräte im Durchschnitt 5.200 Angriffen pro Monat ausgesetzt. Tatsächlich befinden sich die meisten IoT-Geräte in der Anfangsphase, was die Angriffsfläche für Angreifende zur Ausnutzung der Schwachstellen dieser Geräte stark vergrößert (Brooks, 2022). Cyberangriffe auf ein IoT-Gerät beeinträchtigen die Benutzerfreundlichkeit des Geräts, die Leistung und die von dem Gerät angebotenen Dienste. Die Manipulation eines IoT-Geräts könnte beispielsweise dazu führen, dass sich der Akku entleert, das Gerät ausgeschaltet wird und somit der vom IoT-Gerät angebotene Dienst nicht mehr verfügbar ist.

Zur Minimierung des Cyberangriffsrisikos sollte jede Branche die bewährten Vorgehensweisen in Sachen Sicherheit befolgen. So muss der Gesundheitssektor in den USA beispielsweise den *Health Insurance Portability and Accountability Act* (HIPAA) einhalten, ein Gesetz, das die Sicherheit der Patientendaten durchsetzt und verhindert, dass diese ohne das Wissen und die Zustimmung der Patient:innen weitergegeben werden. In ähnlicher Weise müssen Unternehmen und Organisationen Sicherheitsmaßnahmen gemäß den Anforderungen der Norm ISO 27001 implementieren, einem internationalen Standard für Informationssicherheits-Managementsysteme (ISMS). Darüber hinaus können IoT-Geräte durch Befolgen der in der ISO-Norm 27400 genannten bewährten Vorgehensweisen zur Sicherheit geschützt werden.

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Die von Hackern im Gesundheitswesen am häufigsten eingesetzte Methode ist *Ransomware*.

1. Welche Unternehmen sind im Hinblick auf ihre Größe am ehesten das Ziel von Cyberangriffen?

*Kleine Betriebe*

## 2.5 Black-Swan-Ereignisse

Ein „Black Swan“ (schwarzer Schwan) ist ein ungewisses Ereignis mit potenziell schwerwiegenden Folgen, das die normale Situation übersteigt und schwer vorherzusagen ist. Ereignisse wie der 11. September 2001, der Erste Weltkrieg, die Finanzkrise von 2008 und COVID-19 sind Beispiele für schwarze Schwäne.

Es besteht kein Zweifel daran, dass Cyberangriffe und Sicherheitsverletzungen immer häufiger vorkommen und dass die Angreifenden immer geschickter und raffinierter in ihren Werkzeugen und Methoden werden. Von Phishing-Kampagnen bis hin zu Schadsoftware, von Aufklärungsangriffen bis hin zu Denial-of-Service-Angriffen – die Angreifenden werden mit jedem Tag entschlossener und dreister. Im Kampf gegen Hacktivisten und Cyberkriminelle müssen sich Unternehmen auf die Stärkung ihrer Sicherheitsmaßnahmen konzentrieren, um dadurch die Widerstandsfähigkeit gegen Datenschutzverletzungen zu erhöhen (Financier Worldwide, 2017).

Nichtsdestotrotz müssen Unternehmen über die traditionelle Sicherheitsplanung für einen Cyberangriff hinaus denken und andere Verteidigungsstrategien für ungewöhnliche Bedrohungen, wie z. B. einen Black-Swan-Cyberangriff, einrichten.

Im Bereich der Cybersicherheit werden Ereignisse mit schwarzem Schwan als „Black-Swan-Cyber-Events“ bezeichnet. Black-Swan-Cyber-Events können im Gegensatz zu herkömmlichen Cyberangriffen andere Methoden und Ansätze nutzen. Die Motivation hinter den meisten Cyberangriffen ist finanzieller Gewinn, sei es durch böswillige Mitarbeitende oder durch das Hacken von Organisationen. Das Netzwerk eines Unternehmens oder die kritische Infrastruktur von Branchen wie Öl und Gas, Fertigung und Telekommunikation werden am stärksten durch Cyberkriminelle bedroht (Financier Worldwide, 2017).

Die folgenden Punkte fassen das Konzept der schwarzen Schwäne sehr gut zusammen (Investopedia, 2022):

* Ein schwarzer Schwan ist ein äußerst seltenes Ereignis, das jedoch schwerwiegenden Auswirkungen haben kann.
* Black-Swan-Events sind unberechenbar.
* Diese Ereignisse können sich negativ auf Investitionen und Märkte auswirken sowie katastrophale Schäden für die Volkswirtschaften verursachen.
* Selbst mit Hilfe starker Modellierungsmethoden lassen sich schwarze Schwäne nicht vorhersagen.
* Auch Prognosemethoden und ‑instrumente können solche Ereignisse nicht vorhersagen.

### Fragen zur Selbstkontrolle

1. Nennen Sie zwei Merkmale eines schwarzen Schwans.

*Selten*

*Unvorhersehbar*

*Starke Auswirkungen auf die Wirtschaft*

Zusammenfassung

In dieser Lektion haben wir das Konzept der Messung erörtert. Außerdem haben wir untersucht, wie Bedrohungen für eine Organisation gemessen und bewertet werden können und wie sich eine Bedrohungsmatrix für die Analyse der gesamten Bedrohungslage einer Organisation nutzen lässt. Wir sind kurz auf einige der wesentlichen Begriffe eingegangen, die in Bedrohungsmatrizen genutzt werden, darunter Metriken, Messungen, Beobachtungen, Attribute, Fähigkeiten und Bedrohungsprofile bzw. Profilierung.

Wir haben auch die Wahrscheinlichkeiten und Auswirkungen größerer Cyberangriffe auf kritische Infrastrukturen und mittelständische Unternehmen betrachtet. Zum Verständnis des Konzepts unvorhersehbarer oder unvorhersagbarer Ereignisse oder Angriffe haben wir kurz den Begriff „Black Swan“ bzw. schwarzer Schwan und dessen Manifestation im Cyberspace besprochen.

# Lektion 3 – Bedrohungsmodellierung

**Lernziele**

Nach Abschluss dieser Lektion werden Sie in der Lage sein,

… das Konzept der Bedrohungsmodellierung zu verstehen.

… die Art der Bedrohungen zu identifizieren, die Systeme, Netzwerke und Anwendungen beeinträchtigen können.

… Angriffsbaumdiagramme zur Beschreibung von Angriffen auf ein System zu erstellen.

… das von Softwareentwickler:innen verwendete STRIDE-Modell zu bewerten.

… die DREAD-Modellierungsmethode zur Priorisierung und Bewertung der Intensität von Bedrohungen zu analysieren.

… das konzeptionelle Modell der Schmerzpyramide für die effektive Nutzung von Bedrohungsdaten anzuwenden.

# 3. Bedrohungsmodellierung

## Einführung

In dieser Lektion wollen wir verschiedene wertvolle Modelle zur Analyse und Eindämmung von potenziellen Bedrohungen ausgiebig erörtern und erklären. Menschen oder Organisationen, die Netzwerke, Systeme, Software oder Anwendungen aufgebaut haben, müssen sich mit verschiedenen Bedrohungen auseinandersetzen, denen ihre Infrastruktur ausgesetzt sein könnte (Shostack, 2014, S. xxi).

Bedrohungsmodellierung ist ein Begriff, der für verschiedene Handlungen verwendet werden kann, die wir alle intuitiv in unserem täglichen Leben ausführen. Wenn die Bedrohung für ein Haus modelliert werden soll, wird meist nur an die Vermögensgüter darin gedacht, also Erbstücke, Familienfotos oder andere Wertgegenstände. Oder es wird an die verschiedenen Möglichkeiten gedacht, wie jemand einbrechen könnte, z. B. durch offene Türen und Fenster. Vielleicht wird auch darüber nachgedacht, wer einbrechen könnte, wie zum Beispiel echte Kriminelle, Stalker oder vielleicht jemand aus der Nachbarschaft.

Jedes der oben genannten Beispiele für den Denkprozess einer Person, die eine Bedrohungsmodellierung für ihr Haus erstellt, ist der Cyberwelt sehr ähnlich. Der Grund dafür ist, dass der gleiche Denkprozess bei der Modellierung von Bedrohungen in der Cybersicherheit angewandt wird. Diese Fragen sind genau die, die einem als Analyst in den Sinn kommen. Wie sieht es mit den anschließend zu implementierenden Prozessen aus, um diese Fragen zu klären und die potenziellen Bedrohungen abzuschwächen? Dies erfordert die richtigen Fähigkeiten und Methoden, die wir in den Lernzyklen dieser Lektion besprechen werden. Bei diesen Methoden handelt es sich um verschiedene Bedrohungsmodelle, die einem Bedrohungsanalysten dabei helfen, nicht nur über die notwendigen Fragen zu einer potenziellen Bedrohung nachzudenken, sondern sie auch zu beantworten (Shostack, 2014, S. xxi).

Der Begriff „Bedrohung“ kann auf viele Arten interpretiert werden. Er kann auf einen verärgerten Mitarbeitenden zutreffen, der als „Insider-Bedrohung“ gilt. Er kann auch für ein Ereignis stehen, z. B. „Am Ende dieses Monats droht ein Tornado“. Oder er definiert Schadsoftware und Viren oder die Möglichkeit eines bestimmten Cyberangriffs.

Ebenso lässt sich die Bedrohungsmodellierung auf unterschiedliche Weise beschreiben, aber im Allgemeinen werden die folgenden zwei Konzepte betrachtet (Shostack, 2014, S. xxii-xxiii):

1. Durchführung des Analyseprozesses, um die möglichen Folgen einer Bedrohung für eine Schwachstelle zu erkennen.

**Risiko**

Der potenzielle Schaden oder Verlust, wenn eine Bedrohung eine Schwachstelle ausnutzt.

1. Einsatz von Abstraktionen, die beim Nachdenken über **Risiken** helfen.

Bedrohungsmodellierung ist eine der wichtigsten Methoden einer stärkeren Verteidigung. In den folgenden Lernzyklen wollen wir verschiedene Bedrohungsmodelle wie Angriffsbaumdiagramme, STRIDE, DREAD und die Schmerzpyramide behandeln.

Es gibt echte Fachleute im Bereich der Informationssicherheit. Softwareentwickler:innen sind zwar IT-Fachleute, haben aber häufig keine Kenntnisse der Informationssicherheit. Deshalb sehen sie die Entwicklung einer Anwendung in der Regel nicht aus der Sicht von Angreifenden. Es ist wichtig zu verstehen, dass es im Bereich der Cybersicherheit keine Sicherheitsmaßnahme gibt, die nicht umgangen werden könnte, und in der Regel geschieht dies auf eine Art und Weise, die sich die Software-Entwicklungsfachleute nie hätte vorstellen können. Da jeden Tag in den Zeitungen und Berichten über Sicherheitslücken berichtet wird, ist es offensichtlich, dass das Konzept der „Sicherheit“ keine Bedeutung hat, solange wir keine Antworten auf Fragen wie „Sicherheit vor wem und für wie lange?“ finden.

**Netzwerkinfrastruktur**

Die Bezeichnung für eine Kombination aus Hardware, Netzwerkdiensten und Software.

Natürlich benötigen wir bestimmte Methoden zur Modellierung von Bedrohungen gegen die **Netzwerkinfrastruktur**. Wenn wir die verschiedenen Methoden erkennen, die für Angriffe auf die Netzwerkinfrastruktur genutzt werden können, lassen sich möglicherweise Gegenmaßnahmen zur Verhinderung dieser Angriffe planen. Diese Gegenmaßnahmen lassen sich dann zur Bekämpfung von realen Bedrohungen umsetzen (Schneier, 1999).

## 3.1 Angriffsbaum-Methodik

Ein nützlicher Weg zur Verdeutlichung der Angriffsbaum-Methodik ist die Analyse von Beispielen aus der Praxis.

### Praxisnahe Beispiele für Angriffsbäume

Angriffsbäume sind eine Methode zur Bedrohungsmodellierung, die von Bruce Schneier (1999) entwickelt wurde. Diese Methode bietet einen strukturierten Ansatz, der die unterschiedlichen Arten von Angriffen berücksichtigt. Der Angriff auf ein Ziel wird in einer hierarchischen Baumstruktur dargestellt. Der Wurzelknoten stellt das Hauptziel dar, und die Blätter und Äste beschreiben die Wege zur Erreichung dieses Ziels. Die Angriffsbaum-Methode erlaubt die Modellierung verschiedener Wege, über die in ein Ziel eingedrungen werden kann, und das resultierende Diagramm hilft Sicherheitsfachleuten bei der besseren Analyse potenzieller Sicherheitsbedrohungen. In den folgenden Abschnitten werden die Angriffsbäume aus Schneier (1999) detailliert erläutert. Parallel zum Text in diesem Lernzyklus können die Studierenden die Angriffsbaummodelle auf der Website der Quelle betrachten.

Der erste Angriffsbaum von Schneier modelliert einen Angriff auf einen physischen Tresor (1999). Das Angriffsziel ist der Einbruch in den Tresor. Dazu könnten Angreifende das Schloss knacken, die Kombination herausfinden, den Tresor mit dem Schneidbrenner öffnen, oder den Tresor vorab unvorschriftsmäßig einbauen, so dass sie ihn anschließend leicht knacken können. Die Kombination müssen sie entweder aus einer versteckten Niederschrift oder direkt vom Besitzer des Tresors erhalten. Jeder Knoten beschreibt ein Unterziel, und jeder untergeordnete Knoten repräsentiert den Ansatz zur Erreichung dieses Unterziels. Der hier beschriebene Angriffsbaum ist natürlich subjektiv. Je nach Fähigkeiten und Fachkenntnissen kann man verschiedene andere potenzielle Angriffe hinzufügen, die zum Erreichen des Ziels eingesetzt werden können.

Zu beachten ist, dass es sich hier um ODER- und UND-Knoten (OR bzw. AND) handelt. Ein Knoten, der nicht als UND-Knoten gekennzeichnet ist, gilt als ODER-Knoten. ODER-Knoten stellen eine Option dar. Es gibt zum Beispiel vier verschiedene Möglichkeiten, ein Ziel zu erreichen (z. B. in einen Tresor einzudringen). Mit jeder der vier Möglichkeiten kann der Tresor geknackt werden. Im Gegensatz dazu stehen AND-Knoten für verschiedene Schritte, die zur Erreichung des Ziels zusammen ausgeführt werden müssen. Um die Kombination eines Tresors zu erfahren, müssen Angreifende laut der ersten Abbildung von Schneier (1999) ein Gespräch belauschen UND den Besitzer des Tresors irgendwie dazu bringen, die Kombination preiszugeben. In diesem Beispiel würden Angreifende das Ziel (d. h. den erfolgreichen **Lauschangriff**) nicht erreichen, wenn eine (oder beide) der Bedingungen nicht erfüllt sind.

**Lauschangriff**

Unbefugtes Abhören einer vertraulichen Kommunikation.

Nach der Erstellung des Angriffsbaums können den Knoten zur Durchführung weiterer Analysen und Berechnungen zwei weitere Werte zugewiesen werden, nämlich P (*possible* = möglich) und I (*impossible* = unmöglich). Nach Zuweisung dieser Werte wird die Prognose der Sicherheit des Wurzelknotens viel einfacher. ODER-Knoten werden mit P markiert, wenn mindestens einer ihrer untergeordneten Knoten mit P markiert ist, bzw. mit I, wenn alle untergeordneten Knoten mit I markiert sind. UND-Knoten werden mit P markiert, wenn alle untergeordneten Knoten P sind, und mit I, wenn mindestens einer der untergeordneten Knoten I ist, wie in der zweiten Abbildung von Schneier (1999) gezeigt.

In der zweiten Abbildung von Schneier (1999) werden alle erzielbaren Angriffe mit gestrichelten Linien hierarchisch von den Blattknoten zum Ziel (dem Wurzelknoten) dargestellt. Diesem Modell zufolge kann ein Ziel durch zwei mögliche Angriffsmethoden erreicht werden: Der Tresor wird mit dem Schneidbrenner geöffnet, oder der:die Tresorbesitzer:in wird zur Herausgabe der Kombination gebracht. Mit diesem Wissen aus einem Angriffsbaummodell lassen sich die geeigneten Sicherheitsmaßnahmen implementieren, um die Infrastruktur gegen den potenziellen, zuvor modellierten Angriff zu schützen. Die Beauftragung eines Sicherheitsdienstes, der den Tresor in regelmäßigen Abständen überprüft, ist ein Beispiel für die Umsetzung einer Sicherheitsmaßnahme in diesem Szenario.

Die Zuweisung von „P“- und „I“-Werten zu den Knoten ist nur eine Möglichkeit der Modellierung eines Angriffs über einen Angriffsbaum. Den Knoten können beliebige andere Werte zugewiesen werden, z. B. „schwierig und leicht“, „billig und teuer“, „illegal und legal“, „keine spezielle Ausrüstung oder spezielle Ausrüstung erforderlich“ usw. Die dritte Abbildung von Schneier (1999) zeigt den Angriffsbaum mit demselben Ziel, aber mit anderen Werten. Die Zuweisung von Werten wie „billig“ und „teuer“ wäre ebenfalls von Vorteil, jedoch lassen sich die Modelle mit Zahlenangaben besser analysieren. Die vierte Abbildung von Schneier (1999) zeigt einen Angriffsbaum, bei dem den Knoten unterschiedliche Kosten als Werte zugeordnet sind. Einem übergeordneten ODER-Knoten werden die Kosten des billigsten untergeordneten Knotens zugewiesen, wohingegen einem UND-Knoten die Summe der Kosten aller untergeordneten Knoten zugewiesen wird. Angreifende versuchen immer, die günstigsten Methoden einzusetzen. Der Angriff mit den geringsten Kosten ist daher in der vierten Abbildung dargestellt (Schneier, 1999).

Anhand der vierten Abbildung des Angriffsbaums von Schneier (1999) lässt sich die Schwachstelle des Systems identifizieren. Wenn Bedrohungsanalysten nur die weniger kostspieligen Angriffe modellieren wollen, dann sollten auch nur diese Angriffe im Angriffsbaum berücksichtigt werden, wie in der fünften Abbildung von Schneier (1999) gezeigt. Angenommen, in einem Tresor lägen 100.000 $. Dann werden nur die Angriffe angezeigt, welche die Angreifenden potenziell weniger als 100.000 $ kosten. Das Motiv hinter diesem Modell ist, dass Angreifende ihr Ziel nicht erreichen wollen, wenn es sie mehr kostet als der mögliche Profit.

Neben dem in Schneiers fünfter Abbildung gezeigten Wert könnten auch andere stetige Werte an den Knoten verwendet werden, wie z. B. die Erfolgswahrscheinlichkeit des Angriffs oder die Wahrscheinlichkeit, dass Angreifende einen Angriff versuchen, und so weiter.

In jedem realen Szenario erfolgt die Modellierung von Bedrohungen über Angriffsbäume meist dadurch, dass den Knoten mehr als ein Wert zugewiesen wird. Dadurch lassen sich die Schwachstellen des Systems noch besser erkennen. Die sechste Abbildung von Schneier (1999) modelliert beispielsweise den billigsten Angriff, der keine besondere Ausrüstung erfordert.

Ein Angriffsbaum-Bedrohungsmodell hilft bei der Implementierung der geeigneten Sicherheitsmaßnahmen. In der sechsten Abbildung von Schneier (1999) zum Beispiel würde es Angreifende 20.000 $ kosten, ihr Ziel zu erreichen. In diesem Modell wird davon ausgegangen, dass die Angreifenden den billigsten Angriff ohne besondere Ausrüstung versuchen würden, nämlich die Bestechung einer Person, welche die Kombination des Tresors kennt. Gemäß dieser Analyse könnten wir als Gegenmaßnahme dieser Person mehr bezahlen, um sie weniger anfällig für Bestechungsversuche zu machen. Wenn wir zum Beispiel annehmen, dass die Bestechung die Angreifenden 60.000 $ kosten würde, dann steigen deren Kosten um 40.000 $. Wahrscheinlich könnte eine dritte Partei beauftragt werden, um die Widerstandsfähigkeit dieser Person gegen Bestechungsversuche zu überprüfen.

Es sei darauf hingewiesen, dass dies nur Beispiele sind und die Modellierung der Angriffe sowie die Zuordnung von Werten zu Knoten von der jeweiligen Situation abhängt. Diese praxisnahen Beispiele sollen es den Studierenden ermöglichen, die Methode der Angriffsbäume für die Modellierung von Bedrohungen in einem bestimmten Szenario zu nutzen. Kurz gesagt, Sicherheit ist ein fließender Prozess und kein Produkt. Angriffsbäume ermöglichen es uns das Verständnis dieses Prozesses (Schneier, 1999).

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Eine Bedrohung kann auf *viele* Arten interpretiert werden.

1. Wählen Sie die richtige Antwort: Ein Angriffsbaum ist eine …

* Modellierungsmethode für die Verteidigung.
* *Modellierungsmethode für Bedrohungen.*
* Modellierungsmethode für offensives Vorgehen.

## 3.2 STRIDE

Das Akronym STRIDE steht für Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service und Elevation of Privilege. STRIDE ist eine Methode zur Bedrohungsmodellierung, die 1999 von Praerit Garg und Loren Kohnfelder entwickelt wurde. Die Technik wurde für Softwareentwickler:innen entworfen, um ihnen zu helfen, potenzielle Angriffe auf die Software zu erkennen (Shostack, 2014, S. 61).

Die in STRIDE genannten Bedrohungen sind im Grunde das Gegenteil der Sicherheitsaspekte, die man sich für seine Infrastruktur wünschen würde, nämlich Authentifizierung, Integrität, Unleugbarkeit, Vertraulichkeit, Verfügbarkeit und Autorisierung. Die Tabelle „STRIDE-Bedrohungsmodell“ enthält eine Liste von STRIDE-Bedrohungen, die entsprechende zu bewahrende Sicherheitseigenschaft, die Beschreibung und Definition der Bedrohung sowie einige Beispiele (Shostack, 2014, S. 62).

Es sei darauf hingewiesen, dass das STRIDE-Modell nicht dazu dient, Bedrohungen zu kategorisieren, sondern diejenigen zu identifizieren und aufzulisten, die zu Cyberangriffen führen könnten. In den folgenden Lernzyklen wollen wir die einzelnen STRIDE-Bedrohungen erläutern.

### Spoofing

Spoofing bedeutet Identitätsverschleierung, also eine Person, die sich für eine andere ausgibt. In der folgenden Tabelle sehen wir als Beispiele Elon Musk, system32.dll, einen Polizisten, amazon.com oder einen Betrugsbekämpfer. Jeder dieser Fälle gehört zu einer anderen Unterkategorie des Spoofing. In den Beispielen mit amazon.com handelt es sich um Spoofing mit einer sehr bekannten Person. In diesem Fall gibt es keine zwischengeschaltete Behörde, welche die Authentizität der Website überprüft. Das Beispiel mit system32.dll ist anders. Dabei handelt es sich um eine Windows-Registry-Datei, bei der das Betriebssystem zwischen dem Nutzenden und den Dateien steht und deren Authentizität sicherstellt. Angreifende könnten eine neue .dll-Datei einschleusen, die authentisch scheint, aber bösartigen Code enthält. Dies ist ein Beispiel für das Spoofing über eine Datei oder einen Systemprozess. Das Beispiel mit Elon Musk zeigt, wie sich jemand als eine andere Person ausgibt, meist eine berühmte Persönlichkeit oder ein Mitarbeitender einer Organisation. Wenn jemand vorgibt, Betrugsbekämpfer, Polizist oder der Premierminister eines Landes zu sein, fallen diese Beispiele unter die Kategorie der Vortäuschung einer bestimmten Rolle (Shostack, 2014, S. 64–65).

|  |  |  |  |
| --- | --- | --- | --- |
| STRIDE-Bedrohungsmodell | | | |
| **Bedrohung** | **Sicherheitsverletzung** | **Beschreibung der Bedrohung** | **Beispiele** |
| Spoofing | Authentifizierung | Identitätsverschleierung, also sich für eine andere Person ausgeben | Sich fälschlicherweise als Elon Musk, system32.dll, amazon.com, Polizist oder Betrugsbekämpfer ausgeben |
| Tampering | Integrität | Etwas im Speicher oder auf einer Festplatte ändern | Ändern der Binärdatei eines wichtigen Programms, einer Tabellenkalkulation oder der Datenbank auf der Festplatte |
| Repudiation | Unleugbarkeit | Leugnen einer Handlung | Eine Person behauptet, keine E-Mail geschickt zu haben, obwohl sie in Wirklichkeit am Vortag eine E-Mail geschickt hat |
| Information disclosure | Vertraulichkeit | Weitergabe von Informationen an eine unbefugte Person | Gewährung von Zugang zu privaten E-Mails, Datenbanken oder Dateien |
| Denial of Service | Verfügbarkeit | Beeinträchtigung der für den Betrieb des Dienstes erforderlichen Ressourcen | Austricksen eines Webservers, um alle Systemressourcen wie Festplatte, Speicher und Netzwerkbandbreite zu nutzen |
| Elevation of Privilege | Autorisierung | Zugriff auf Ressourcen, für die jemand nicht befugt ist | Erlaubnis für einen normalen Nutzenden zum Ausführen der administrativen Befehle als Superuser |

Quelle: Adam Shostack (2014).

### Tampering

Im STRIDE-Modell bezieht sich der Begriff Tampering (Manipulation) auf eine Bedrohung, durch die etwas im Speicher oder auf einer Festplatte verändert wird. Wie in der obigen Tabelle angegeben, sind Beispiele für Manipulationen das Ändern von Daten in Tabellenkalkulationen wie Microsoft Excel oder einem anderen Editor, das Ändern des Inhalts einer Datenbank auf einer Festplatte oder das Ändern von Konfigurationen und Binärdateien auf einer Festplatte. Pakete, die über das Netzwerk laufen, könnten auch durch Hinzufügen zusätzlicher und unnötiger Pakete verändert werden und dann die Kommunikation beeinträchtigen (Shostack, 2014, S. 67). Die Implementierung von starken Hash-Algorithmen kann Manipulationsbedrohungen verhindern.

### Repudiation

Repudiation bedeutet, eine Handlung oder die Verantwortung für eine Handlung zu verleugnen oder abzustreiten. Wie im Beispiel in der obigen Tabelle könnte jemand, der am Vortag eine E-Mail verschickt hat, dies später abstreiten. **Protokollsysteme** und ‑prozesse sind ebenfalls eng mit Verleugnungsbedrohungen verbunden. Wenn Protokolle für die Netzwerkinfrastruktur nicht aktiviert sind, Protokolle nicht gespeichert werden oder man nicht in der Lage ist, die Protokolle zu analysieren, lassen sich Bedrohungen durch Verleugnung nur schwer bekämpfen (Shostack, 2014, S. 68–69). Starke Protokollierungssysteme in Unternehmen ermöglichen den Sicherheitsteams hingegen die Verhinderung von Bedrohungen durch Ableugnung.

**Protokollieren**

Die Aufzeichnung von Ereignissen im Netzwerk und in den Systemen einer Organisation.

### Information Disclosure

Die Offenlegung von Informationen ist eine Art von Bedrohung, bei der Unbefugte Zugang zu vertraulichen Informationen erhalten. Dazu gehört auch die unbeabsichtigte Preisgabe von Informationen über die Architektur der Anwendung, mit denen Angreifende das System angreifen können.

Einige bekannte Beispiele für die Offenlegung von Informationen (Bauernfreund, 2022) betrachten wir im Folgenden:

* Die von den Softwareentwickler:innen geschriebenen Kommentare können Informationen über die Anwendung offenlegen.
* Fehler können entscheidende Angaben preisgeben.
* Der Quellcode einer Anwendung kann Informationen zu den Parametern oder technische Informationen zur Infrastruktur der Anwendung preisgeben.

Da das STRIDE-Bedrohungsmodell für Softwareentwickler:innen konzipiert ist, können sie am ehesten Schwachstellen durch Offenlegung von Informationen verhindern. Im Folgenden betrachten wir die bewährten Vorgehensweisen im Bereich der Sicherheit, die eine Offenlegung von Informationen verhindern können, sofern sie von den Entwickler:innen befolgt werden (Bauernfreund, 2022):

* Informationen über die Anwendung wie Antwort-Header, Fehlermeldungen und sensible Hintergrundinformationen müssen allgemein gehalten werden, damit keine Hinweise auf das Verhalten der Anwendung preisgegeben werden.
* Zur Verhinderung unbefugten Zugriffs müssen geeignete Autorisierungsmechanismen und Zugriffskontrollen konfiguriert werden.
* Die Anwendung muss aus der Sicht der Nutzenden überprüft werden, um sicherzustellen, dass keine sensiblen Informationen und Kommentare des Entwicklers offengelegt werden. Dazu können **Penetrationstests für Web-Anwendungen** gemäß den bewährten Vorgehensweisen und Standards der IT-Branche eingesetzt werden.

**Penetrationstests für Web-Anwendungen**

Legale Angriffe auf eine Web-Anwendung, um so ihre Schwachstellen zu erkennen und sie rechtzeitig zu beseitigen.

### Denial-of-Service-Angriffe

Denial-of-Service-Angriffe (DoS) fallen unter die Denial-of-Service-Bedrohungen des STRIDE-Modells und die Verfügbarkeit als zugehörige Sicherheitsverletzungsklasse. Solche Angriffe überschwemmen den Zielserver mit unnötigem Datenverkehr, führen zu einem Absturz und machen ihn für legitimen Datenverkehr unerreichbar. Diese Angriffe kosten ihre Opfer in der Regel Geld und Zeit, sowie ihren guten Ruf im Hinblick auf die Zuverlässigkeit. Eines der bekanntesten Beispiele für DoS-Angriffe ist ein Pufferüberlauf. Dabei wird der reservierte Speicherpuffer durch Einschleusung zu vieler Daten überlastet, was schließlich die Anwendung zum Absturz bringt.

**Web Application Firewall (WAF)**

Schutz einer Web-Anwendung durch die Filterung des HTTP-Verkehrs zwischen dem Internet und der Web-Anwendung.

Durch die Konfiguration einer **Web Application Firewall** **(WAF**) könnte eine solche Anwendung vor DoS-Angriffen geschützt werden. Diese blockiert den eingehenden Datenverkehr von verdächtigen IP-Adressen oder begrenzt die Paketrate zur besseren Datenverkehrssteuerung (Bauernfreund, 2022).

### Elevation of Privilege

Elevation of Privilege (Rechteausweitung) ist ein Angriff, bei dem Fehlkonfigurationen, meist in der Web-Anwendung, ausgenutzt werden, um Angreifenden illegal Zugang zu privilegierten Zugriffsrechten zu verschaffen. Diese Angriffe können Authentifizierungs- und Anmeldungsprozesse oder Fehlkonfigurationen im Design und Code ausnutzen, oder über Social Engineering und Schadsoftware-Methoden privilegierten Zugriff erhalten. Nachdem Angreifende privilegierten Zugriff erlangt haben, können sie Befehle auf Administrator- oder Root-Ebene ausführen und damit Schaden anrichten. Es sei angemerkt, dass der Zugriff auf ein höher privilegiertes Konto als vertikale Privilegieneskalation bezeichnet wird (z. B. der Zugriff von einem normalen Nutzenden auf ein Root-Benutzerkonto). Der Zugriff auf ein Konto, das die gleiche Berechtigungsstufe wie das eigene hat, wird jedoch als horizontale Privilegieneskalation bezeichnet (z. B. der Zugriff auf ein Studierendenkonto von einem anderen Studierendenkonto aus).

Der Schutz vor diesen Bedrohungen muss bereits in der Entwicklungsphase der Software eingebaut werden. Dazu gehören Härtungsmechanismen wie Least Privilege, das Schließen unnötiger offener Ports, die Löschung nicht benötigter Zugänge und Rechte usw. (Bauernfreund, 2022).

### Vorteile der STRIDE-Bedrohungsmodellierung

Viele bekannte Methoden werden während oder nach der Entwicklung der Web-Anwendung zur Identifizierung von Schwachstellen eingesetzt (Penetrationstests, **Code-Reviews** usw.). Es ist jedoch viel einfacher und billiger, die Fehler zu beheben, während sich die Anwendung noch in der Entwicklungsphase befindet, als wenn die Anwendung bereits in Betrieb ist. STRIDE ist eine Methode der Bedrohungsmodellierung, die den Entwickler:innen dabei hilft, potenzielle Schwachstellen frühzeitig in der Entwicklungsphase zu erkennen, also wenn ihre Beseitigung noch relativ einfach und kostengünstig ist (Bauernfreund, 2022).

**Code-Review**

Bewertung eines Quellcodes zur Ermittlung von Fehlern.

### Fragen zur Selbstkontrolle

1. Nennen Sie zwei Bedrohungen des STRIDE-Modells.

*Spoofing (Identitätsverschleierung)*

*Tampering (Manipulationen)*

*Repudiation (Verleugnung)*

*Information Disclosure (Offenlegung von Informationen)*

*Denial of Service (Verweigerung des Dienstes)*

*Elevation of Privilege (Rechteausweitung)*

## 3.3 DREAD

Die zuvor betrachteten Methoden Angriffsbäume und STRIDE werden eher zur Identifizierung von Bedrohungen verwendet. DREAD hingegen ist eine Methode zur Bewertung von Bedrohungen, mit der sich Bedrohungen priorisieren lassen. Die Priorisierung basiert auf den potenziellen Auswirkungen der Bedrohung auf eine Web-Anwendung oder ein Softwaresystem, der Wahrscheinlichkeit ihres Auftretens und den Methoden, mit denen sie potenziell ausgenutzt werden können. Diese Priorisierung erfolgt nach der Identifizierung der Bedrohungen, wie in den Lernzyklen 3.1 und 3.2 beschrieben. Mit diesen Merkmalen kann zur Bedrohungspriorisierung eine qualitative Einstufung wie niedrig, mittel und hoch vorgenommen werden.

Die zur Bedrohungspriorisierung genutzten Methoden basieren in der Regel auf einer Bedrohungs-Risiko-Einstufung. (Zu beachten: Die Begriffe Bewertung und Einstufung werden in diesem Lernzyklus synonym verwendet.) Das DREAD-Modell ist ein Beispiel für ein Bedrohungs-Risiko-Bewertungsmodell, das Bedrohungen auf der Grundlage ihrer Einstufung priorisiert (Ingeno, 2018, S. 363–364).

DREAD ist ein Modell zur Priorisierung von Sicherheitsbedrohungen auf der Grundlage eines **Risikobewertung**.Ebenso wie das STRIDE-Modell wurde es von Microsoft entwickelt. DREAD ist eine Abkürzung für die folgenden Risikokomponenten:

**Risikobewertung**

Ein Verfahren zur Identifizierung von Bedrohungen mit hoher Priorität, die den Vermögensgütern schaden könnten.

* Damage potential (Schadenspotenzial)
* Reproducibility (Reproduzierbarkeit)
* Exploitability (Ausnutzbarkeit)
* Affected users (betroffene Nutzende)
* Discoverability (Entdeckbarkeit)

Mit dem DREAD-Modell von Microsoft wird das Risiko berechnet. Wir stellen Fragen, die auf den oben genannten Risikofaktoren des DREAD-Modells basieren, und bewerten so das Risiko einer bestimmten Bedrohung. Wir wollen zunächst die einzelnen Risikofaktoren des DREAD-Modells erörtern und dann einige Beispiele untersuchen, um zu verstehen, wie eine Bedrohung auf der Grundlage der Risikobewertungsfaktoren des DREAD-Modells priorisiert und eingestuft werden kann (Microsoft Corporation, 2003, S. 63).

### Damage potential (Schadenspotenzial)

Das Schadenspotenzial bezieht sich auf das Ausmaß des Schadens, der einer Organisation oder einzelnen Nutzenden bei einem erfolgreichen Angriff entstehen könnte. Zum Beispiel wäre die Bewertung für Schäden an Benutzerdaten niedriger als bei einem Cyberangriff, der das gesamte System lahmlegen kann. Die Bewertung des Schadens hängt von der Art des Cyberangriffs und den angegriffenen Vermögensgütern ab, z. B. von der Rufschädigung oder der finanziellen Haftung eines Unternehmens (Ingeno, 2018, S. 364).

### Reproducibility (Reproduzierbarkeit)

Reproduzierbarkeit bedeutet, wie einfach es ist, einen bestimmten Cyberangriff zu wiederholen. Ein Cyberangriff, der leicht und zuverlässig reproduziert werden kann, wird höher bewertet als ein Angriff, der nicht leicht reproduziert werden kann (Ingeno, 2018, S. 364).

**Exploit**

Eine Software oder Methode, mit der eine Sicherheitslücke ausgenutzt wird, um in ein System einzudringen.

### Exploitability (Ausnutzbarkeit)

Die Ausnutzbarkeit ist ein Risikofaktor zur Beurteilung, wie schwer es für eine Bedrohung ist, ein Vermögensgut durch Ausnutzung einer Schwachstelle zu beschädigen. Einige **Exploits** (also Methoden zur Ausnutzung von Schwachstellen) sind leicht zu verstehen und können sogar von nicht authentifizierten Nutzenden ausgeführt werden, während andere mehr technische Fähigkeiten zur Ausführung fortgeschrittener Werkzeuge und **Skripte** erfordern (Ingeno, 2018, S. 365).

**Skript**

Spezielle Anweisungen zur Automatisierung eines Prozesses.

### Affected users (betroffene Nutzende)

Dieser Risikofaktor gibt den Prozentsatz der Nutzenden an, die von einer bestimmten Bedrohung betroffen wären. Manche Cyberangriffe können alle Nutzenden betreffen, während andere sich nur auf wenige Nutzende auswirken. Dieser Risikofaktor sollte höher eingestuft werden, wenn die Anzahl der Nutzenden, die von einer Bedrohung betroffen sein könnten, höher ist (Ingeno, 2018, S. 365).

### Discoverability (Entdeckbarkeit)

Die Entdeckbarkeit gibt an, wie einfach es ist, eine Sicherheitslücke zu finden. Eine Bedrohung, die bereits öffentlich bekannt ist, wird eher entdeckt als eine, die schwer zu finden ist. Hier sei erwähnt, dass manche Sicherheitsfachleute und Organisationen der Meinung sind, dass der Risikofaktor Entdeckbarkeit nicht berücksichtigt werden sollte, weil er eine Sicherheitskontrolle namens **Security through Obscurity** (Sicherheit durch Unklarheit) berücksichtigt. Sie glauben, es sei unklug, eine Schwachstelle als weniger riskant zu betrachten, nur weil sie nicht leicht zu entdecken ist. Daher nutzen viele Sicherheitsfachleute ein DREAD–D-Modell (DREAD ohne das letzte D) oder geben für alle Bedrohungen die maximale Entdeckbarkeit an (Ingeno, 2018, S. 365). Da wir uns in diesem Lernzyklus auf die Diskussion von DREAD konzentrieren, bewerten wir diesen Faktor nicht anhand von DREAD–D.

**Security through Obscurity**

(Sicherheit durch Unklarheit) Der Vorgang, ein System sicher zu halten, indem das Wissen darüber geheim gehalten wird, wie z. B. das Verstecken eines Schlüssels für eine verschlossene Tür unter einer Fußmatte.

Die betrachteten fünf Risikofaktoren des DREAD-Modells sind im Grunde die zu stellenden Fragen, wenn die Risikoeinstufung für eine bestimmte Bedrohung ermittelt werden soll. Diese fünf Fragen könnten wie folgt gestellt werden:

1. **Damage potential (Schadenspotenzial):** Wie hoch ist der potenzielle Schaden an einem Vermögensgut?
2. **Reproducibility (Reproduzierbarkeit):** Wie einfach lässt sich ein Cyberangriff reproduzieren?
3. **Exploitability (Ausnutzbarkeit):** Wie einfach kann ein Cyberangriff durchgeführt werden?
4. **Affected users (betroffene Nutzende):** Wie viele Nutzende wären davon betroffen?
5. **Discoverability (Entdeckbarkeit):** Wie einfach kann eine Schwachstelle entdeckt werden?

Die oben genannten Fragen können mittels der Skalen niedrig (1), mittel (2) und hoch (3) für die Bewertung der Bedrohungen verwendet werden. Wenn jeder Wert des Bewertungssystems klar definiert ist, ist es einfacher, eine bestimmte Bedrohung zu bewerten, indem man sie mit einer geeigneten Skala in Beziehung setzt. Die nachstehende Tabelle „Bedrohungsbewertung und Priorisierung“ zeigt eine Bewertungstabelle, die bei der Priorisierung der Bedrohungen hilft (Microsoft Corporation, 2003, S. 63–64).

Nachdem die oben genannten Fragen für eine bestimmte Bedrohung gestellt wurden, werden die Bewertungen von 1 bis 3 für jede Kategorie von DREAD angekreuzt und addiert. Das Ergebnis liegt dann im Bereich von 5–15. Eine Bedrohung mit einer Bewertung von 5–7 würde dann als geringes Risiko eingestuft werden, von 8–11 als mittleres Risiko und von 12–15 als hohes Risiko (Microsoft Corporation, 2003, S. 64). Der vollständige Ablauf der Bewertung einer bestimmten Bedrohung ist in der nachstehenden Tabelle „DREAD-Bewertungen“ dargestellt

Wir betrachten zwei Bedrohungen, um den Ablauf der DREAD-Bewertungen besser zu verstehen:

1. Bösartige SQL-Befehle werden in eine Anwendung eingeschleust.
2. Die Angreifenden verschaffen sich durch die Überwachung des Netzwerks Zugang zu den Authentifizierungsdaten.

Nach der Ermittlung der Risikoeinstufung für jede Bedrohung sollte diese in der Tabelle „DREAD Ratings“ für die beiden als „hoch“ eingestuften Bedrohungen eingetragen werden.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bedrohungsbewertung und Priorisierung | | | | |
|  | **Einstufungen** | **Niedrig (1)** | **Mittel (2)** | **Hoch (3)** |
| **D** | Schadenspotenzial | Triviale Informationen sind durchgesickert. | Sensible Informationen sind durchgesickert. | Die Angreifenden können administrative Befehle ausführen. |
| **R** | Reproduzierbarkeit | Die Reproduktion eines Angriffs ist extrem schwierig, selbst wenn die Angreifenden eine Schwachstelle gut kennen. | Der Angriff kann nur in einer bestimmten Situation reproduziert werden. | Der Angriff kann in jeder Situation leicht reproduziert werden. |
| **E** | Ausnutzbarkeit | Um einen Cyberangriff zu starten, braucht man eine hochqualifizierte und gut informierte Person. | Gute Programmierfachleute können mit etwas Geschick und Wissen einen Angriff starten. | Auch Programmierfachleute, die am Anfang stehen, können einen Angriff starten. |
| **A** | Betroffene Nutzende | Nur sehr wenige Nutzende wären davon betroffen. | Einige Gruppen von Nutzenden wären davon betroffen. | Alle Nutzenden wären davon betroffen. |
| **D** | Entdeckbarkeit | Die Schwachstelle ist ziemlich versteckt, und die Wahrscheinlichkeit, sie zu finden, ist für die Nutzenden sehr gering. | Die Schwachstelle wird nur selten genutzt und zu ihrer Ausnutzung ist einige Knobelarbeit erforderlich. | Die Sicherheitslücke ist öffentlich zugänglich und könnte leicht ausgenutzt werden. |

Quelle: Microsoft Corporation (2003).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DREAD-Bewertungen | | | | | | | | |
| **Bedrohungen** | **D** | **R** | **E** | **A** | **D** | **Gesamt** | **Einstufung** |
| Bösartige SQL-Befehle werden in eine Anwendung eingeschleust. | 3 | 3 | 3 | 3 | 2 | 14 | Hoch |
| Die Angreifenden verschaffen sich durch die Überwachung des Netzwerks Zugang zu den Authentifizierungsdaten. | 3 | 3 | 2 | 2 | 2 | 12 | Hoch |

Quelle: Microsoft Corporation (2003).

Die folgende Tabelle zeigt beispielhaft eine so dokumentierte Bedrohung.

|  |  |
| --- | --- |
| Eine vollständig dokumentierte Bedrohung |  |
| **Beschreibung der Bedrohung** | Die Angreifenden verschaffen sich durch die Überwachung des Netzwerks Zugang zu den Authentifizierungsdaten. |
| **Ziel der Bedrohung** | Authentifizierungsprozess |
| **Risikobewertung** | Hoch |
| **Angriffsmethode** | Netzwerküberwachung |
| **Gegenmaßnahme** | Verschlüsselung zur Wahrung der Vertraulichkeit |

Quelle: Microsoft Corporation (2003).

Die in der obigen Tabelle genannte Gegenmaßnahme ist die Sicherheitsmaßnahme, die für ein Vermögensgut vorgesehen werden sollte. Wie wir in dieser Tabelle sehen, wird die Entscheidungsfindung zur Auswahl geeigneter Sicherheitsmaßnahmen zur Sicherung eines Vermögensguts erleichtert, wenn eine Bedrohung mit ihren Risikoeinstufungen und anderen Details ordnungsgemäß dokumentiert ist.

### Fragen zur Selbstkontrolle

1. Nennen Sie zwei beliebige DREAD-Attribute.

*Damage potential (Schadenspotenzial)*

*Reproducibility (Reproduzierbarkeit)*

*Exploitability (Ausnutzbarkeit)*

*Affected users (betroffene Nutzende)*

*Discoverability (Entdeckbarkeit)*

## 3.4 Schmerzpyramide

Der Sicherheitsfachmann David J. Bianco hat das Konzept der Schmerzpyramide erstmals im Jahr 2013 präsentiert. Es handelt sich um ein konzeptionelles Modell zur Erkennung von Bedrohungen, wobei der Schwerpunkt darauf liegt, die Kosten für die Angreifenden zu erhöhen. Das Hauptziel der Einführung dieser Methode war die Unterstützung bei der Identifizierung potenzieller Angriffsindikatoren oder Bedrohungen, und so eine Bedrohung zu modellieren. Ein vollständiges Modell der Schmerzpyramide ist unten abgebildet.

Schmerzpyramide

Ein Bild mit Text, Visitenkarte

Beschreibung automatisch generiert

Quelle: Zohaib Hassan (2023), nach Bianco (2013).

### Verstehen der Angriffsindikatoren

In der obigen Grafik ist eine Pyramide mit sechs Ebenen dargestellt. Jede Ebene repräsentiert verschiedene Formen von Angriffsindikatoren. Die Ebene, auf der ein bestimmter Indikator liegt, legt den entsprechenden Schmerz fest. Angenommen, Angreifende setzen zur Infektion eines Systems **Schadsoftware** ein, und wir nutzen zur Erkennung dieses Verhaltens Hashes. Dann könnten die Angreifenden diese Schadsoftware ganz einfach mit einem anderen Hash-Wert als dem, den wir für die Erkennung nutzen, neu kompilieren, wodurch unser Hash-Wert relativ nutzlos wird (Chenette, 2019).

**Schadsoftware (Malware)**

Eine bösartige Software, die in einem Netzwerk, in einem System oder in einer Anwendung Schaden anrichten soll.

Nachstehend definieren wir kurz alle acht Indikatoren, auf denen die Pyramide aufgebaut ist (Bianco, 2013):

1. **Hashes:** Dies sind die Hash-Werte zu einer bestimmten Schadsoftware. MD5 oder SHA1 sind Beispiele für Hashes einer bestimmten bösartigen Datei, auf deren Grundlage die Erkennung durchgeführt wird.
2. **IP-Adressen:** Dies ist eine Adresse oder Adressgruppe, die einen Rechner im Netzwerk oder Internet eindeutig identifizieren. 15.2.1.2 ist ein Beispiel für eine IPv4-Adresse.
3. **Domain-Namen:** Eine Domain bezieht sich auf eine Webseite wie google.com oder eine Sub-Domain wie sites.google.com. Sie kann sich auch auf eine Sub-Sub-Domain wie site1.sites.google.com beziehen.

**Artefakt**

Ein Beleg oder Nachweis, der nach einem Vorfall für weitere Untersuchungen vorgelegt wird.

1. **Netzwerk-Artefakte:** Nachweisbare Spuren oder die **Artefakte**, die nach einer Manipulation von den Angreifenden im Netzwerk hinterlassen werden. Die IP-Adressinformationen der Angreifenden finden sich beispielsweise in den Netzwerkprotokollen.
2. **Host-Artefakte:** Nachweisbare Spuren oder die Artefakte, die nach einer Manipulation von den Angreifenden im Host-Server hinterlassen werden. Zum Beispiel können bösartige .dll-Dateien an bestimmten Stellen unter legitimen Namen abgelegt werden.
3. **Werkzeuge:** Dies umfasst beispielsweise Software oder Dienstprogramme, die von den Angreifenden zur Erreichung ihres Ziels eingesetzt werden. So nutzen Angreifende zum Beispiel meist eine Linux-Distribution namens Kali Linux für ihre bösartigen Aktivitäten.
4. **Taktiken, Methoden und Verfahren (TTPs = Tactics, Techniques, Procedures):** Eine vollständige, von Angreifenden verfolgte Strategie zum Angriff auf ein Netzwerk, System oder eine Anwendung. Spear-Phishing ist eines der Beispiele für TTPs, bei denen bösartige Anhänge, meist als .zip- oder .pdf-Dateien, verwendet werden. TTPs beziehen sich auf die Methoden und Verfahren zur Durchführung bösartiger Aktivitäten und sind nicht auf ein bestimmtes Werkzeug bezogen. Dies führt zu erheblichen Schmerzen für die Angreifenden, weil wir nicht nur die Aktivitäten der Angreifenden aufdecken, sondern auch die Angreifenden selbst.

Wir haben uns jetzt die grundlegenden Details zu jedem der Indikatoren angesehen. Nun wollen wir die Pyramide im Einzelnen besprechen. Die breitesten Teile der Pyramide sind grün, und die Spitze ist rot. Sowohl Farbe als auch Breite haben ihre Bedeutung bei der Bewertung der einzelnen Indikatoren. Indikatoren am unteren Ende bereiten den Gegnern nur geringe Schmerzen, während der Indikator an der Spitze enorme Auswirkungen hätte. Seine Aufdeckung erfordert einen immensen Aufwand für die Sicherheitsanalysten (Panhalkar, 2020).

Am unteren Ende der Pyramide befinden sich die Hashes. Der Grund dafür ist, dass die Offenlegung der Hashes keine signifikanten Auswirkungen auf die Gegner hat. Außerdem müssen Hashes zur Analyse einer Bedrohung wie Schadsoftware genau sein. Das bedeutet, dass die Aufnahme unnötiger Bits Hashes für weitere Analysen unbrauchbar machen würde. Außerdem ist für Analysten weniger Aufwand erforderlich, um die Hashes zu berechnen.

**The Onion Router**

Eine Open-Source-Software, die Dienste für anonyme Kommunikation bietet.

Oberhalb der Hashes befinden sich die IP-Adressen. IP-Adressen nehmen einen großen Bereich der Pyramide ein, da riesige Datenbanken mit IP-Adressen zur Verfügung stehen, die Angreifende benötigen, um eine Verbindung mit dem Opfer herzustellen. Angreifende können ihre ursprüngliche IP-Adresse mithilfe von Proxy-Diensten wie dem **The Onion Router** (TOR) leicht verbergen und so unentdeckt bleiben. Wenn die gefälschte IP-Adresse irgendwie blockiert wird, können sie den Angriff fortsetzen, indem sie die IP-Adresse sofort in eine neue gefälschte IP-Adresse ändern. Daher wird dieser Indikator in grüner Farbe angezeigt.

Ebene drei von unten nach oben ist den Domain-Namen gewidmet. Da für die Gegner der Kauf eines Domain-Namens zur Etablierung im Internet Kosten verursacht, wird dies in hellgrüner Farbe dargestellt, was auf größere Schmerzen im Vergleich zu den beiden unteren Ebenen hinweist.

In der Pyramide stehen in der Ebene oberhalb der Domain-Namen die Host- und Netzwerk-Artefakte. Diese Ebene ist in hellgelber Farbe dargestellt, was den Beginn der schmerzhaften Auswirkungen auf die Angreifenden anzeigt, da Sicherheitsanalysten mehr Mühe haben, diesen Indikator zu entdecken. Für Analysten ist es immer ein größerer Aufwand, einen gut strukturierten Angriff zu verstehen und zu erkennen. Sobald sie diesen entdecken, müssen die Angreifenden ihren Angriff umstrukturieren, um nicht erneut entdeckt zu werden. Die Angreifenden erleiden also Schmerzen, wenn sie den Angriff umstrukturieren und dabei berücksichtigen müssen, wie dieser zuvor entdeckt wurde. Außerdem müssen sie durch Nachforschungen herausfinden, welche Methoden die Analysten zur Erkennung einsetzen. Diese Entdeckung der Host- und Netzwerk-Artefakte würde die Angreifenden dazu bringen, das Werkzeug umzubauen und dabei das bereits aufgedeckte Artefakt zu berücksichtigen. Solche Hindernisse zu entdecken, zu beheben und zu überwinden, erfordert bei den Gegnern große Anstrengungen und viel Zeit.

Die Werkzeuge weiter oben in der Pyramide sind in gelber Farbe dargestellt. Wenn Sicherheitsanalysten ein Werkzeug entdecken, würde dies die Gegner dazu veranlassen, für einen weiteren Angriff mehr Zeit in die Suche nach einem neuen und effizienteren Werkzeug zu stecken. Dies würde die Leistung der Angreifenden verringern und die Zeit, die sie für ihren Angriff benötigen, verlängern.

An der Spitze der Pyramide schließlich stehen die TTPs. Wenn sie identifiziert und aufgedeckt werden, hat dies die schlimmsten Auswirkungen auf den Gegner. Dies würde die Gegner dazu zwingen, den gesamten Angriffsprozess neu zu starten. Zu diesem Zeitpunkt kennen die Sicherheitsanalysten die komplette Vorgehensweise der Gegner.

### Fragen zur Selbstkontrolle

1. Nennen Sie drei beliebige Ebenen des Modells der Schmerzpyramide.

*Domain-Namen*

*IP-Adressen*

*Hash-Werte*

*TTPs*

*Werkzeuge*

*Netzwerk- bzw. Host-Artefakte*

Zusammenfassung

In dieser Lektion wurde das Konzept der Bedrohungsmodellierung mit seinen bekanntesten Methoden besprochen. Wir haben die Methode der Angriffsbäume erörtert, die bei der Identifizierung einer Bedrohung hilft, indem sie diese in einer hierarchischen Struktur in Form von Knoten modelliert. Wir haben auch die Methode der STRIDE-Bedrohungsmodellierung besprochen, die von Software-Entwicklungsfachleuten zur Identifizierung von Bedrohungen eingesetzt wird. Anschließend haben wir das DREAD-Modell im Detail betrachtet. Dieses Modell beschreibt die Priorisierung einer Bedrohung nach ihrer Identifizierung. Schließlich wurde das Modell der Schmerzpyramide erläutert. Dabei werden verschiedene Bedrohungsebenen bezüglich der Auswirkungen (oder dem verursachten Schmerz) modelliert, die Gegnern entstehen, wenn diese Bedrohung von Analysten entdeckt wird.

# Lektion 4 – Angriffsbibliotheken

**Lernziele**

Nach Abschluss dieser Lektion werden Sie in der Lage sein,

… öffentlich verfügbare Angriffsmethoden mit Hilfe der CAPEC-Angriffsbibliothek zu erkennen.

… Verstöße gegen die Privatsphäre und ihre Schäden anhand der Taxonomie der Privatsphäre nach Solove zu verstehen.

… mittels des MITRE-ATT&CK-Frameworks die fortgeschrittenen Methoden und Taktiken der Angreifenden zu entdecken.

… neue Angriffsarten auf der Grundlage aktueller Bedrohungen zu identifizieren.

# 4. Angriffsbibliotheken

## Einführung

Im Bereich der Cybersicherheit müssen sich Sicherheitsfachleute über die aktuelle Bedrohungslandschaft und die Angriffsvektoren stets auf dem Laufenden halten. Um Sicherheitsfachleuten eine aktuelle, zentralisierte und sich ständig weiterentwickelnde Wissensdatenbank zur Verfügung zu stellen, wurde das Konzept der Angriffsbibliotheken entwickelt. Eine Angriffsbibliothek bezieht sich auf verschiedene zentralisierte Datenbanken, die berücksichtigt und konsultiert werden, um die aktuellen Methoden der Angreifenden zu bewerten und zu verstehen. In dieser Lektion werden verschiedene bekannte Angriffsbibliotheken besprochen.

Der CAPEC-Katalog (*Common Attack Pattern Enumeration and Classification*) wird im Detail besprochen, um gegnerische Operationen zu verstehen. Dies ist auch bei der Implementierung eines starken Cybersicherheitsprogramms nützlich. CAPEC ist ein umfangreiches Wörterbuch mit den bekannten Methoden, die Angreifende zum Ausnutzen von Schwachstellen in der Netzwerkinfrastruktur einsetzen.

Anschließend erörtern wir ausführlich das Konzept der Privatsphäre und die verschiedenen Schäden und Folgen, die sich aus deren Beeinträchtigung ergeben können. Anhand von Soloves Taxonomie der Privatsphäre (2006) untersuchen wir die Diskussion zu den Themen Datenschutz und Privatsphäre. Dies hilft uns, die Probleme im Zusammenhang mit der Privatsphäre zu identifizieren und die Schäden zu kategorisieren, die durch deren Gefährdung entstehen könnten.

Im Anschluss daran werden wir das MITRE-ATT&CK-Framework untersuchen und erörtern. Dabei handelt es sich um eine der bekannten, weltweit zugänglichen Datenbanken, die vor allem von Bedrohungsanalysten genutzt wird, um die gegnerischen Taktiken, Methoden und Ansätze zur Durchführung eines Cyberangriffs auf ein Opfer zu identifizieren. Da es sich bei MITRE ATT&CK um eine ständig aktualisierte Datenbank handelt, hilft sie auch bei der Modellierung und Identifizierung von Cyberangriffen. Dies ermöglicht Organisationen dann, geeignete Sicherheitsmaßnahmen entsprechend der aktuellen Bedrohungslage zu implementieren.

## 4.1 CAPEC

CAPEC (*Common Attack Pattern Enumeration and Classification*) ist eine Angriffsbibliothek von MITRE, die einen öffentlich zugänglichen, zentralisierten Katalog für Sicherheitsfachleute bietet. Sie wurde vom U.S. Department of Homeland Security vorgeschlagen, erstellt und erstmals 2007 veröffentlicht (CAPEC™, 2019).

CAPEC enthält bekannte Angriffsmuster, die Fachleuten helfen, das Verhalten von **Gegnern** (Angreifenden) bei der Ausnutzung von Schwachstellen in Anwendungen zu verstehen. Die Bibliothek wird ständig durch die Beiträge und Eingaben der Öffentlichkeit aktualisiert. Dies schafft ein Standardverfahren für die Identifizierung, Sammlung, Verbesserung und den Austausch von Angriffsmustern innerhalb der Cybersicherheitsgemeinschaft. Auf den Begriff „Angriffsmuster“ muss genauer eingegangen werden. Damit sind die Beschreibungen und Erklärungen der Methoden und Ansätze gemeint, mit denen Angreifende Schwachstellen auszunutzen versuchen, was zu einer Gefährdung führt. Angriffsmuster beschreiben außerdem die Schwierigkeiten und Herausforderungen, denen Angreifende gegenüberstehen und wie sie diese überwinden könnten. Ein Angriffsmuster vermittelt uns umfassende Kenntnisse über den Entwurf und die Ausführung eines Angriffs und gibt uns Hinweise und Anleitungen, wie wir die Auswirkungen eines potenziellen Angriffs durch die Auswahl geeigneter Sicherheitsmaßnahmen abschwächen können. Hier ist anzumerken, dass sich CAPEC im Gegensatz zu MITRE ATT&CK auf die Anwendungssicherheit konzentriert (CAPEC™, 2019). MITRE ATT&CK wird in Lernzyklus 4.3 ausführlicher behandelt.

**Gegner**

Personen oder Organisationen, die bösartige Operationen durchführen.

Die wichtigsten Vorteile und Verwendungsmöglichkeiten von CAPEC-Angriffsvektoren sind die folgenden:

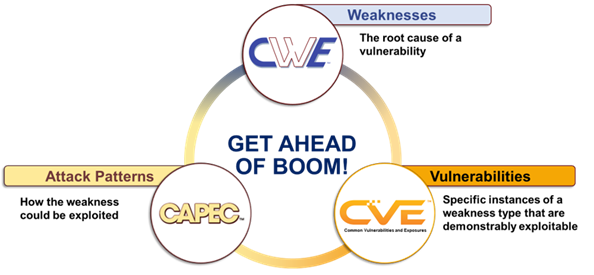
* Penetrationstests,
* die Ausbildung und Schulung von Softwareentwickler:innen,
* die Bedrohungsmodellierung von Anwendungen,
* die Definition von potenziellen Bedrohungen und

**Pufferüberlaufangriff**

Bei dieser Art Angriff übersteigt die Größe der Daten die Kapazität des Speichers.

* die Risikoanalyse der Anwendungsarchitektur.

Die CAPEC-Listen enthalten bekannte Schwachstellen und Anfälligkeiten (*CVE = Common Vulnerabilities and Exposures*) und die Aufzählung allgemeiner Schwachstellen (*CWE = Common Weakness Enumeration*). CWE stellt die Ausgangsbasis für die Identifizierung von Schwachstellen und die Bemühungen zur Abschwächung und Vorbeugung dar. CVE hingegen steht für eine spezifische Schwachstelle in einem System oder Produkt, die ausgenutzt werden kann. Ein **Pufferüberlaufangriff** (Buffer Overflow) ist also ein CWE, wohingegen der Entwicklungsfehler in einem Anwendungscode, mit dem Angreifende eine Anwendung durch Pufferüberlauf manipulieren, als CVE bezeichnet wird. Das CAPEC-Angriffsmuster nutzt einen CWE für einen Angriff, wie in der Abbildung unten dargestellt. Daher enthalten die CAPEC-Angriffsmuster einen vollständigen „Ausführungsablauf“, also vollständige Anweisungen für Angreifende zur Manipulation eines Ziels. Ein Beispiel für die Durchführung des Angriffsmusters von CAPEC wird im nächsten Unterlernzyklus erläutert.

Zusammenhang zwischen CAPEC, CWE und CVE

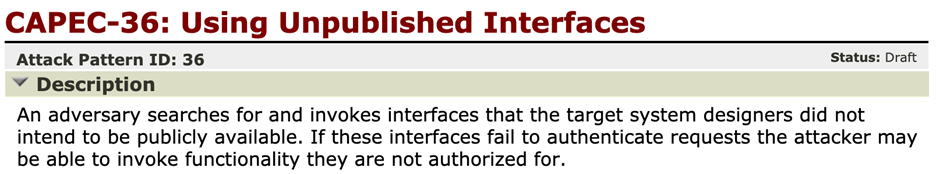
Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

### Beispiel zum Verständnis des CAPEC-Angriffsmusters

Um das Konzept der Angriffsmuster im Detail zu verstehen, wollen wir eines der bekannten Angriffsmuster von CAPEC, nämlich die „Verwendung unveröffentlichter Schnittstellen“, im Detail besprechen und erkennen, welche Vorteile die verschiedenen Merkmale von Angriffsmustern bieten.

Jedem CAPEC-Eintrag ist eine ID zugeordnet. Diese numerische ID enthält keine besonderen Informationen, außer das Datum des Eintrags in die Datenbank. Jeder Eintrag hat einen Namen und eine Beschreibung. Die Beschreibung ist eine vollständige Zusammenfassung eines Angriffsmusters und worum es dabei geht. Diese Informationen sind in der folgenden Abbildung dargestellt. Die Zahl 36 ist die ID, und „Using Unpublished Interfaces“ ist der Name des Angriffsmusters des Beispiels der nachstehenden Abbildung.

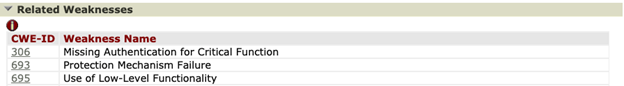
Name, ID und Beschreibung des CAPEC-Angriffsmusters



Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

Die Schwachstellen für jedes Angriffsmuster finden sich im Abschnitt „Verwandte Schwachstellen“ (*Related Weaknesses*), die Angreifende ausnutzen könnten. Der Abschnitt „Verwandte Schwachstellen“ für CAPEC-36 ist in der folgenden Abbildung dargestellt.

Verwandte Schwachstellen für CAPEC-36

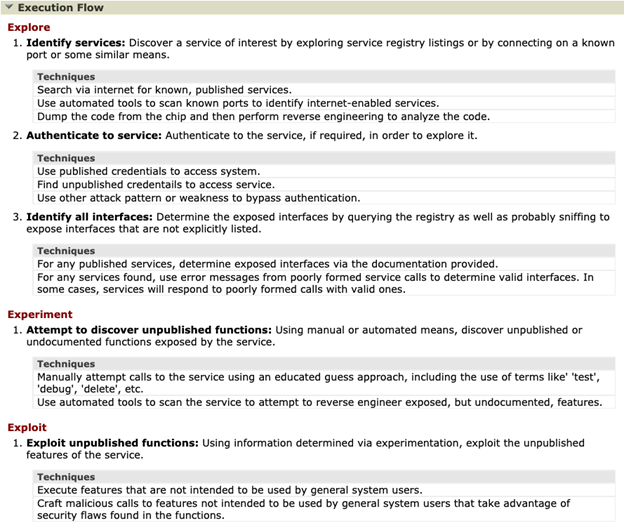


Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

Wenn wir die beiden obigen Abbildungen analysieren, können wir feststellen, dass das Angriffsmuster und die Schwachstellen scheinbar nicht miteinander zusammenhängen, und dass es nicht unbedingt eine Eins-zu-Eins-Beziehung geben muss. Das Angriffsmuster muss für einen Angriff diese Schwachstellen ausnutzen.

Als nächstes folgt der Teil „Ausführungsablauf“, der eine vollständige Schritt-für-Schritt-Anleitung für die Ausführung eines Angriffs enthält. Der Teil „Ausführungsablauf“ für CAPEC-36 ist in der folgenden Abbildung dargestellt.

Ausführungsablauf von CAPEC-36



Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

Der Ausführungsablauf ist in drei Phasen unterteilt:

1. **Erkunden:** In dieser Phase werden mehrere Möglichkeiten beschrieben, um ein potenzielles Opfer für einen Angriff zu entdecken. In jeder der drei Phasen gibt es mindestens einen Schritt. Jeder Schritt beschreibt mehrere Methoden zur Durchführung dieses Schritts.
2. **Experimentieren:** Sobald ein Opfer oder ein Ziel entdeckt wurde, werden die in der Experimentierphase vorgestellten Methoden eingesetzt, um festzustellen, ob das Ziel Schwachstellen aufweist, die dieser spezielle CAPEC ausnutzen könnte.
3. **Ausnutzen:** In dieser Phase des Ausführungsablaufs werden Methoden zur Ausführung des eigentlichen Angriffs vorgeschlagen.

Hier sei angemerkt, dass der Ausführungsablauf eines CAPEC-Angriffsmusters nicht nur bei der Ausführung eines Angriffs hilft, sondern auch bei der Feststellung, ob das Opfer dafür anfällig ist.

Anschließend gibt es einen Abschnitt mit der Bezeichnung „Folgen“, der die möglichen Auswirkungen nach der erfolgreichen Ausführung des Angriffs nach diesem Angriffsmuster aufzeigt. Die nachstehende Abbildung zeigt zum Beispiel den Abschnitt „Folgen“ für CAPEC-36.

Folgen von CAPEC-36



Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

Ein wichtiger Punkt dabei ist, dass die in CAPEC aufgeführten Einträge nicht die Folgen des Angriffs betreffen. Sie basieren vielmehr darauf, wie man erfolgreich die Schwäche eines Ziels ausnutzt, das diese Folgen verursacht. Für DoS-Angriffe (Denial-of-Service) gibt es zum Beispiel keinen CAPEC-Eintrag. Es gibt jedoch verschiedene Angriffsmuster, die einen DoS verursachen. Hier ist DoS eine Folge, kein Angriffsmuster.

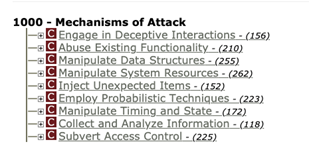
Außerdem können CAPEC-Einträge mit zwei **Ansichten** betrachtet werden. Die CAPEC-Einträge sind vordefiniert und je nach Ansicht angeordnet. Die beiden Ansichten sind:

**Ansichten**

Bei CAPEC stellen Ansichten eine Perspektive dar, aus der die verschiedenen Sammlungen von Angriffsmustern innerhalb von CAPEC betrachtet werden können.

* **Angriffsmechanismus:** Bei dieser Ansicht werden die unterschiedlichen, für Angriffe auf verschiedene Bereiche der Cybersicherheit auszunutzenden CAPEC-Einträge hervorgehoben. Die nachstehende Abbildung zeigt ein Beispiel für die Ansicht „Angriffsmechanismus“.
* **Angriffsbereiche:** In dieser Ansicht werden ähnliche Angriffe gruppiert dargestellt. Ein Beispiel für diese Ansicht findet sich in der nachfolgenden Abbildung.

Ansicht: Angriffsmechanismen



Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

Ansicht: Angriffsbereiche



Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

In den beiden obigen Abbildungen lässt sich die nächste Ebene des Teilbaums durch Klicken auf das „+“-Zeichen öffnen.

### Nutzung der CAPEC-Website

In diesem Unterlernzyklus erläutern wir, wie sich die CAPEC-Website für Recherchen nutzen lässt, also z. B., wenn der Chief Information Security Officer (CISO) von uns wissen möchte, ob das neue System für SQL-Injektionen anfällig ist. Dafür können wir uns zwei gängige Navigationsmethoden auf der CAPEC-Website zunutze machen und die angeforderten Informationen extrahieren.

#### Stichwort-Suche

Die CAPEC-Website stellt eine Suchfunktion zur Verfügung, wie in der Abbildung unten dargestellt.

CAPEC-Stichwortsuche – I



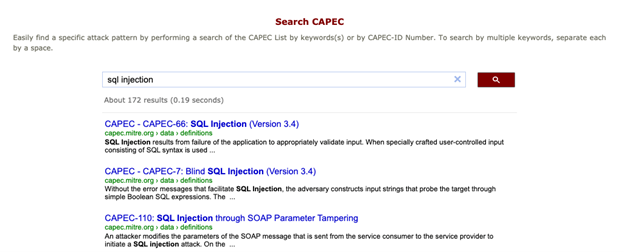
Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

Es kann nach beliebigen Stichwörtern, IDs oder allgemeinen Begriffen gesucht werden. Angenommen wir möchten nach Informationen im Zusammenhang mit einer **SQL-Einschleusung** (*Structured Query Language Injection*) suchen. Das zu befolgende Verfahren ist in der folgenden Abbildung dargestellt: Nach Eingabe von „sql injection“ in die Suchleiste erhalten wir mehrere Ergebnisse.

**SQL-Einschleusung**

Es handelt sich um eine Sicherheitslücke in einer Web-Anwendung, die von Angreifenden ausgenutzt wird, um über die Web-Anwendung bösartige Befehle an die Datenbank zu schicken.

CAPEC-Stichwortsuche – II

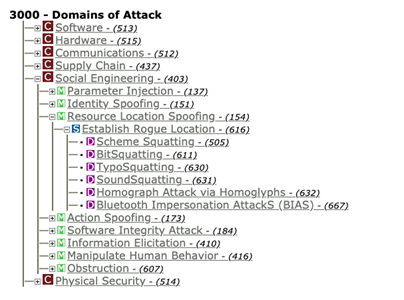


Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

#### Verwendung der Ansichten

Wir haben bereits gesehen, dass CAPEC-Einträge in Ansichten organisiert sind. Wir können jede beliebige Ansicht durchlaufen, je nach Bereich, für den wir uns interessieren. Wenn wir uns zum Beispiel für die Angriffsmuster der sozialen Manipulation (Social Engineering) interessieren, sehen wir uns in der Ansicht „Angriffsdomänen“ die CAPEC-Einträge zu diesem Bereich an (siehe unten).

CAPEC-Nutzung mit Ansichten



Quelle: MITRE (2021b). © 2023 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Im Bereich der *Cybersicherheit* müssen Sicherheitsfachleute ständig über die aktuelle *Bedrohungslandschaft* informiert sein.

## 4.2 Taxonomie der Privatsphäre nach Solove

„Datenschutz“ und „Privatsphäre“ sind weit gefasste Begriffe, die sich auf eine Vielzahl zusammenhängender Dinge beziehen. Solche Begriffe können manchmal sehr hilfreich sein, in anderen Fällen jedoch weniger. Nehmen wir zum Beispiel das Wort „Tier“. Der Begriff „Tier“ umfasst eine große Gruppe von Lebewesen wie Reptilien, Säugetiere, Fische, Vögel usw. Innerhalb jeder dieser Gruppen gibt es dann Untergruppen. In manchen Szenarien reicht der Begriff „Tier“ aus. Angenommen, Alice fragt John: „Wie viele Tiere gibt es genau in diesem Zoo?“. Dann muss John für die Beantwortung dieser Frage keine Details kennen, denn die Verwendung des Wortes „Tier“ in der Frage ist in diesem Zusammenhang eindeutig. Nehmen wir nun an, Alice möchte eine Katze haben und fragt John danach. In diesem Zusammenhang reicht es nicht aus, den Begriff „Tier“ zu verwenden, da sie die Art des gewünschten Tieres angeben muss. Ähnlich wie beim weiter gefassten Begriff „Tier“ können wir auch den Begriff „Privatsphäre“ ganz allgemein gebrauchen. Manchmal kann die Verwendung des Begriffs „Privatsphäre“ allein jedoch zu Verwirrung führen, z. B. bei politischen Entscheidungsträgern und Gerichten.

Diese Taxonomie (Klassifikationsschema) veranschaulicht die Zusammenhänge zwischen verschiedenen Problemen und Schäden. Es ist nicht ungewöhnlich, dass unterschiedliche Probleme aufgrund ihrer Ähnlichkeit als Verletzung der Privatsphäre bezeichnet werden. Aber wir müssen auch verstehen, worin sich diese Dinge unterscheiden. Ziel ist es, ein Problem entsprechend dem Kontext klar zu benennen, also seine Einzigartigkeit, die Unterschiede sowie die Zusammenhänge mit anderen Problemen der Privatsphäre zu bestimmen.

In der Regel fügen diese Probleme den Menschen Schaden zu. Schäden wie Verletzungen sind leicht zu verstehen, aber Verletzungen der Privatsphäre sind ein schwieriger Fall. Die Privatsphäre sollten wir als etwas Immaterielles oder nicht Greifbares betrachten und nicht als eine physische Verletzung. Die Sicherheitsforschenden und Autoren Warren und Brandeis vertreten die Ansicht, dass die Verletzung der Privatsphäre eines Individuumszu einer Verletzung von Emotionen und Gefühlen führt (nachzulesen in Solove, 2006).

Brandeis und Warren sprechen über den Schaden für die Würde einer Person, und Rufschädigung ist ein klassisches Beispiel für einen solchen Schaden. Sie haben damit gut zum Ausdruck gebracht, dass diese Arten von Schäden faktisch und rechtlich anzuerkennen sind (Solove, 2006, S. 485–487).

In dieser Taxonomie werden die schädlichen Aktivitäten in vier Gruppen unterteilt (Solove, 2006, S. 488):

1. Informationssammlung
2. Informationsverarbeitung
3. Informationsverbreitung
4. Eindringen

Diese vier Gruppen sind um ein Modell herum angeordnet, das mit einer betroffenen Person (Subjekt) anfängt. Eine betroffene Person ist eine Person, auf die sich die in dieser Taxonomie aufgeführten Ereignisse und Aktivitäten direkt auswirken. Verschiedene Entitäten wie Regierungen, Unternehmen und Privatpersonen sammeln Informationen von solchen Personen. Die Entitäten, welche die Daten sammeln, speichern, bearbeiten, kombinieren, suchen und nutzen, werden Dateninhaber genannt. All diese Aktivitäten werden in der Solove-Taxonomie der Privatsphäre als „Informationsverarbeitung“ bezeichnet. Nach der Verarbeitung der Informationen können die Dateninhaber die Informationen mit anderen teilen, freigeben oder übertragen. Dieser Schritt wird in der Taxonomie als „Informationsverbreitung“ bezeichnet. Das Modell der Taxonomie zeigt, dass sich die Daten bei ihrer Anhäufung, Sammlung, Verarbeitung und Verbreitung von der Macht und Kontrolle des Einzelnen entfernen. Die letzte Aktivität wird als „Eindringen“ (*Invasion*) bezeichnet und wirkt sich direkt auf den Einzelnen aus (Solove, 2006, S. 488, 489).

Die Informationssammlung bezeichnet die Hauptgruppe der Aktivitäten, die sich auf die Privatsphäre einer Person auswirken. Diese Aktivitäten sind die folgenden:

* **Überwachung**: Bei dieser Aktivität werden die Aktivitäten der Testperson aufgezeichnet, abgehört oder beobachtet.
* **Befragung**: Mehrere Möglichkeiten der Abfrage und Informationserfassung fallen unter diese Kategorie.

Die zweite Gruppe bezieht sich auf die Aktivitäten und Methoden, mit denen Informationen manipuliert, gespeichert und verwendet werden, was als Informationsverarbeitung bezeichnet wird. Zu den Aktivitäten in dieser Gruppe gehören die folgenden:

* **Aggregation (Anhäufung):** Der Prozess der Kombination mehrerer Datensätze über eine Person.
* **Identifikation:** Dies ist der Prozess der Verknüpfung der Informationen mit bestimmten Personen.
* **Unsicherheit:** Dies ist der mangelnde Schutz der gesammelten Informationen vor unbefugtem Zugriff und Lecks.
* **Sekundärnutzung:** Dies ist die Nutzung der gesammelten Informationen für einen anderen Zweck als den, für den sie gesammelt wurden, und ohne die Zustimmung der betroffenen Person.
* **Ausschluss:** Dies bedeutet, dass die betroffene Person keine Möglichkeit hat, zu wissen, welche Informationen andere über sie haben und an deren Verwendung und Handhabung teilzuhaben.

Bei den vorgenannten Aktivitäten der zweiten Gruppe geht es um den Umgang, die Nutzung und die Pflege der Daten, und nicht um das Sammeln der Daten, was Teil der ersten Gruppe von Aktivitäten ist (Solove, 2006, S. 490).

Bei der dritten Gruppe geht es um die Informationsverbreitung und die folgenden Aktivitäten:

* **Verletzung der Vertraulichkeit:** Dies bedeutet, dassdie persönlichen Informationen einer betroffenen Person nicht vertraulich behandelt wurden.
* **Offenlegung:** Dies bezeichnet die Preisgabe echter Informationen über eine Person, was das Urteil anderer über sie beeinflussen könnte.
* **Bloßstellung:** Dies beinhaltet die Enthüllung des Kummers, der Körperfunktionen oder der Nacktheit eines anderen.
* **Verbesserte Zugänglichkeit:** Dies bezeichnet die Erweiterung des Zugangs zu Informationen.
* **Erpressung:** Dies ist die Drohung der Preisgabe persönlicher Informationen.
* **Aneignung:** Dies bezeichnet die Nutzung der Identität einer Person zur Unterstützung der Interessen und Ziele eines anderen.
* **Verzerrung:** Dies ist die Verbreitung irreführender und gefälschter Informationen über betroffene Personen.

Bei allen oben genannten Aktivitäten geht es um die Weitergabe oder Verbreitung von Personendaten (Solove, 2006, S. 491).

Die letzte Gruppe umfasst Aktivitäten, die darauf abzielen, in die Privatangelegenheiten von Personen einzudringen. Zu den Aktivitäten in dieser Gruppe gehören die folgenden:

* **Eindringen:** Der Akt der Störung der Zurückgezogenheit oder Ruhe einer Person.
* **Einflussnahme auf Entscheidungen:** Die Einmischung staatlicher Stellen in die Entscheidungen des Einzelnen zu dessen privaten Angelegenheiten.

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Privatsphäre und Datenschutz sind *weit gefasste (breite)* Begriffe.

## 4.3 Mitre ATT&CK®

MITRE ATT&CK wurde 2013 entwickelt, und ATT&CK ist ein Akronym, das für *Adversarial Tactics, Techniques, and Common Knowledge* steht (auf Deutsch etwa: Gegnerische Taktiken, Methoden und allgemeines Wissen). Es wurde von den Forschenden des Fort Meade Experiment (FMX) bei MITRE entwickelt. Sie emulierten das verteidigende und gegnerische Verhalten, um durch Verhaltensanalyse die Erkennung von Bedrohungen nach einer Gefährdung zu verbessern. Die entscheidende Frage der Forschenden lautete: „Wie effizient erkennen wir gegnerisches Verhalten über Dokumentation?“ Zur Beantwortung dieser Frage entwickelten die Forschenden das ATT&CK-Framework, das seither als nützliches Werkzeug zur Klassifizierung gegnerischen Verhaltens eingesetzt wird (Trellix, o. D.).

Das MITRE-ATT&CK-Framework zeigt die verschiedenen Phasen eines gegnerischen Angriffs sowie die anvisierten Opfer und Plattformen. Das im Modell dargestellte Konzept der Taktiken und Methoden bietet eine allgemeine Klassifizierung gegnerischer Aktivitäten, die sowohl von defensiven als auch offensiven Cybersicherheit-Teams leicht verstanden werden kann (Trellix, o. D.).

Das Verhaltensmodell nach ATT&CK enthält die folgenden Hauptkomponenten (Strom et al., 2018):

* **Taktik**: Die kurzfristigen Ziele des Gegners während des Angriffs (Darstellung in Spalten).
* **Methoden**: Die wesentlichen Wege, mit denen Angreifende ihre taktischen Ziele erreichen (Darstellung in einzelnen Zellen).
* **Untermethoden**:Spezifischere gegnerische Methoden zur Erreichung der taktischen Ziele.

Bei MITRE ATT&CK können auch drei Hauptiterationen betrachtet werden, die ebenfalls als Matrizen bekannt sind:

|  |  |  |  |
| --- | --- | --- | --- |
| MITRE-ATT&CK-ANSICHTEN | | | |
| **ATT&CK for ENTERPRISE (UNTERNEHMEN)** | **ATT&CK for MOBILE (MOBILGERÄTE)** | **ATT&CK für ICS** |
| Diese Matrix zeigt das gegnerische Verhalten in Linux-, Mac-, Windows- und Cloud-Umgebungen. | Diese Matrix zeigt das gegnerische Verhalten auf den Betriebssystemen Android und iOS. | Diese Matrix konzentriert sich auf potenzielle gegnerische Aktionen bei einem Angriff auf ein industrielles Kontrollsystem (ICS). |

Quelle: Zohaib Hassan (2023), nach Trellix (o. D.).

MITRE ATT&CK wird weltweit in verschiedenen Bereichen wie z. B. Red-Teaming, Eindringlingserkennung, Sicherheitstechnik, Threat-Hunting und Risikomanagement eingesetzt (Strom et al., 2018).

### Die MITRE-ATT&CK-Matrix

Das MITRE ATT&CK-Framework bzw. ‑Modell wird in Form einer Matrix dargestellt. Sie enthält eine Sammlung von Methoden, die von Angreifenden zur Erreichung eines bestimmten Ziels eingesetzt werden. Diese Ziele werden in der ATT&CK-Matrix kategorisiert und Taktiken genannt. Die Ziele werden linear dargestellt, beginnend mit „Erkennung“ und bis zum letzten Ziel „Auswirkung“. Bei der umfangreichen Version von ATT&CK for Enterprise (die Linux, macOS, Windows, Office 365, Azure AD und Cloud Networks umfasst) sind die folgenden vierzehn gegnerischen Taktiken gruppiert und kategorisiert (Trellix, o. D.):

1. **Erkennung**: Dazu gehört das Sammeln von Informationen, um zukünftige gegnerische Operationen vorherzusehen, z. B. Informationen über die Zielorganisation.
2. **Ressourcenentwicklung**: Dies betrifft die Einrichtung von Ressourcen zur Unterstützung von Operationen wie der Einrichtung einer Steuerungs- und Kontrollinfrastruktur.

**Spear-Phishing**

Eine Methode zum Anvisieren herausgehobener Personen durch ein E-Mail-Betrugsschema oder auf andere Weise über das Internet.

1. **Erster Zugriff:** Ein Vorgang zum Herstellen des Anfangszugriffs auf das Netzwerk des Opfers, z. B. über **Spear-Phishing**.
2. **Ausführung:** Dabei wird versucht, den bösartigen Code im Netzwerk oder auf dem System des Opfers auszuführen, d. h. ein Werkzeug zur Fernsteuerung.
3. **Beharrlichkeit:** Dabei geht es um den Versuch, den Zugang aufrechtzuerhalten, zum Beispiel durch Manipulation der Konfigurationen des Angriffsziels.
4. **Privilegieneskalation:** Der Versuch, Zugang zu hochprivilegierten Konten wie Root-Benutzerkonten unter Linux oder Administratorkonten unter Windows zu erhalten. Dies kann durch Ausnutzung einer Sicherheitslücke in einem beeinträchtigten System geschehen. In diesem Stadium könnten die Angreifenden bereits Zugriff auf das manipulierte System haben, allerdings nur auf die Berechtigungen der Nutzenden auf der unteren Ebene.
5. **Umgehung der Verteidigung:** In diesem Fall versuchen die Angreifenden, nicht erwischt oder entdeckt zu werden, beispielsweise durch Nutzung eines vertrauenswürdigen Prozesses als Versteck für Schadsoftware.
6. **Zugang zu Anmeldeinformationen:** Hierbei versuchen die Angreifenden, Passwörter, Namen und Konten zu stehlen. Dies kann zum Beispiel über Keylogger geschehen.
7. **Ausforschen:** Der Versuch der Angreifenden, die Umgebung des Ziels zu erkunden, um herauszufinden was kontrolliert werden könnte.

**Pivoting**

Ausnutzung eines manipulierten Systems zum Angriff auf ein anderes System.

1. **Seitliche Fortbewegung:** Sobald die Angreifenden die befugten Anmeldeinformationen haben, bewegen sie sich durch **Pivoting** legitim durch benachbarte Systeme.
2. **Sammeln:** Das Sammeln von Daten, die im Interesse der gegnerischen Zielverfolgung sind. Dies könnte zum Beispiel bedeuten, dass die Gegner sich Zugang zu den Daten in der Cloud verschaffen.
3. **Kommando und Kontrolle:** Die Phase, in der ein beeinträchtigtes System oder Netzwerk von den Angreifenden kontrolliert und mit ihm kommuniziert wird, d. h. sie imitieren den legitimen Web-Datenverkehr, um mit dem Netzwerk des Opfers zu kommunizieren und es zu steuern.

**Ransomware**

Eine spezielle Schadsoftware, durch die den Organisationen und Nutzenden der Zugriff auf ihre Computerdateien verhindert wird. Dazu verschlüsseln die Angreifenden die Daten und verlangen ein Lösegeld zur Datenentschlüsselung.

1. **Exfiltration:** Dies steht für den Diebstahl und die Ausschleusung der Daten des Opfers.
2. **Auswirkung:** Hierzu gehören die Unterbrechung, Manipulation und Zerstörung von Daten und Systemen, beispielsweise die Verschlüsselung der Daten des Opfers durch **Ransomware**.

Die eigentliche gegnerische Handlung wird durch die Methoden nach den obigen Taktiken beschrieben. Einige Methoden sind in Untermethoden unterteilt, die beschreiben, wie eine bestimmte Methode von den Angreifenden ausgeführt wird. Die nachstehend verkleinert abgebildete vollständige Matrix von ATT&CK for Enterprise 2021 zeigt alle Taktiken mit den dazugehörigen Methoden. Dieselbe Matrix kann auf der MITRE-ATT&CK-Website genauer betrachtet werden.

### Nutzung einer MITRE-ATT&CK-Matrix

**Advanced Persistent Threat (APT)**

(Fortgeschrittene anhaltende Bedrohung) Hierbei handelt es sich um einen speziellen Cyberangriff, der auch als staatlich gesponsert oder nationalstaatlich bezeichnet wird, und bei dem sich die Angreifenden sehr lange auf einem kompromittierten System verstecken können und unentdeckt bleiben.

Unternehmen und Sicherheitsfachleute können die ATT&CK-Matrix auf vielfältige Weise nutzen. Die häufigsten Vorteile der Verwendung der Matrix sind die folgenden (Trellix, o. D.):

#### Red-Teaming

Dabei handelt es sich um einen vollständigen Angriff, der innerhalb einer Organisation aus der gegnerischen Perspektive nachgestellt wird, um die möglichen Auswirkungen nach einem Eindringen zu ermitteln. Man könnte diesen Prozess auch als „Emulation der Gegner“ bezeichnen. Anhand dieses Vorgangs können auch die Sicherheitsvorkehrungen des Unternehmens überprüft werden. Für die Organisation und Durchführung von Red-Team-Operationen kann ebenfalls die ATT&CK-Matrix genutzt werden.

Gruppierung der Aktivitäten in der Solove-Taxonomie der Privatsphäre

Tabelle

Automatisch generierte Beschreibung

Quelle: MITRE (2021a). © 2022 The MITRE Corporation. Die Vervielfältigung und Verbreitung dieses Diagramms wurde von The MITRE Corporation genehmigt.

#### Bedrohungsinformationen

ATT&CK kann von Bedrohungsanalysten als umfangreiche Informationsquelle genutzt werden, um über die neuesten Cyberangriffe und die Bedrohungslandschaft auf dem Laufenden zu bleiben. Durch die Bewertung ihrer Sicherheitsmaßnahmen gegen **fortgeschrittene anhaltende Bedrohungen** (APTs = Advanced Persistent Threats) können die Verteidigungsteams damit beurteilen, wie widerstandsfähig sie gegen einen solchen Cyberangriff sind.

#### SOC-Bewertung

Das Security Operations Center (SOC) ist eine spezielle Umgebung innerhalb einer Organisation, deren Aufgabe es ist, Cyberangriffe zu erkennen, zu überwachen, zu untersuchen, zu entdecken und darauf zu reagieren. Da Angriffe anhand der ATT&CK-Matrix emuliert werden, würde diese Emulation auch die Bewertung der Effektivität des SOC bei der Erkennung des Angriffs unterstützen.

Die Implementierung von MITRE ATT&CK erfolgt in der Regel durch manuelle Kartierung der Bedrohungen oder durch die Integration mit Cyber-Sicherheitswerkzeugen. Das hierfür am häufigsten verwendete Werkzeug ist das Security Information and Event Management (SIEM). Die Integration von SIEM mit MITRE ATT&CK umfasst die Sammlung von **Protokollen** aus dem Unternehmensnetzwerk, die Identifizierung der Bedrohungen und deren Zuordnung zur ATT&CK-Matrix.

**Protokolle (Logs)**

Automatisch erzeugte, detaillierte Informationen über Ereignisse.

Neben der Nutzung von MITRE ATT&CK für die oben genannten und allgemeinen Aktivitäten könnte dieses Framework auch für andere Cyberabwehroperationen genutzt werden, z. B. für die Cyberforensik und die Bedrohungsjagd (Threat Hunting).

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

ATT&CK wurde im Jahr *2013* von der *MITRE*-Organisation entwickelt.

## 4.4 Identifizierung neuer Cyberangriffe

Sicherheitsfachleute, Mitarbeitende, Studierende oder auch normale Internetnutzende sollten zumindest über Grundkenntnisse verfügen, um einen Cyberangriff oder bösartige Aktivitäten, die zu einem Cyberangriff führen könnten, zu erkennen. Dies ist unbedingt erforderlich, da Angreifende in der Regel versuchen, das Vertrauen von Menschen zu gewinnen, um sie dann zu illegalen Aktivitäten wie der Weitergabe vertraulicher Unternehmensdaten zu zwingen. Wenn Menschen geschult sind und die verschiedenen Methoden der Angreifenden kennen, wird es viel schwieriger, sie zu manipulieren.

In diesem Lernzyklus werden wir erörtern, wie sich ein Cyberangriff oder eine bösartige Aktivität anhand einiger wichtiger Anzeichen erkennen lässt. Wir erörtern im Folgenden die häufigsten Cyberangriffe, die zu massiven Datenschutzverletzungen führen können (Stanfield, 2022):

### Gehacktes E-Mail-Konto

Die folgenden Anzeichen deuten darauf hin, dass ein E-Mail-Konto aufgedeckt worden ist:

* Das Passwort wurde geändert.
* Im Posteingang und unter den gesendeten E-Mails sind ungewöhnliche Aktivitäten zu beobachten.
* Im Posteingang erscheinen E-Mails von anderen Websites zum Zurücksetzen von Passwörtern.
* Der Zugriff auf das E-Mail-Konto erfolgt von einem ungewöhnlichen Ort und einer fremden IP-Adresse.
* Nachrichten von E-Mail-Kontakten, die ständig seltsame E-Mails von dem betreffenden E-Mail-Konto erhalten.

### Gehacktes Systemkonto

Die folgenden Anzeichen weisen darauf hin, dass ein Systemkonto und seine Informationen manipuliert wurden.

**Add-on**

Ein kleines Programm, das die Funktionen eines Browsers erweitert.

* Die Geschwindigkeit des Computers nimmt deutlich ab.
* Das Antivirenprogramm des Systems wurde manipuliert oder automatisch deaktiviert.
* Verdächtige **Add-ons** erscheinen in Ihrem Browser.
* Es kommt zu zufälligen Neustarts und Abschaltungen.
* Verlust des Zugriffs auf das Systemkonto.
* Ungewöhnliche Aktivitäten wie eine automatische Bewegung des Mauszeigers oder der Bildschirmanzeige.

### Gehacktes Cloud-Speicher-Konto

In Cloud-Speicher-Konten speichern Nutzende ihre Daten online. Beispiele für Cloud-Speicher-Konten sind OneDrive, DropBox, Google Drive und iCloud. Zu den häufigsten Anzeichen dafür, dass ein Online-Konto gehackt wurde, gehören die folgenden:

* Ungewöhnliche Inhalte werden auf das Online-Konto hochgeladen.
* Auf das Konto kann nicht zugegriffen werden.
* Daten fehlen oder sind verändert worden.
* Seltsamer Datenverkehr geht vom Netzwerk über das Konto aus.
* Benachrichtigungen über Kontozugriffe von mehreren Standorten aus.
* Es gibt enorme Lesevorgänge auf dem Online-Konto.
* Die Kontaktpersonen erhalten gefälschte E-Mails mit bösartigen Anhängen und Links vom manipulierten Konto.

### Gehacktes Social-Media-Konto

Konten auf sozialen Medien wie Facebook, Instagram, Twitter und TikTok werden im heutigen digitalen Zeitalter von Milliarden von Menschen genutzt. Das Hacken eines Social-Media-Kontos ist ein lukratives Ziel für Angreifende, weil sie so weiteren Zugang zu sensiblen Informationen erhalten und größeren Schaden anrichten können. Die wichtigsten Anzeichen für ein gehacktes Social-Media-Konto sind die folgenden:

* Änderungen in der Anzahl der Follower.
* Vom manipulierten Konto gehen sehr viele ungewollte Freundschaftsanfragen aus.
* Frühere Beiträge werden gelöscht.
* Das Passwort ändert sich plötzlich.
* Benachrichtigungen, dass von mehreren Standorten aus auf das Konto zugegriffen wird.

### Gehacktes Netzwerk

Ein Netzwerk besteht aus zwei oder mehr elektronischen Geräten (z. B. Computern), die miteinander verbunden sind und so Daten und Informationen austauschen. Wenn das Netzwerk eines mittelständischen oder sogar großen Unternehmens gehackt wird, kann dies zu einer massiven Datenverletzung führen, weil in den Systemen des Netzwerks vertrauliche Informationen gespeichert sind. Die häufigsten Anzeichen für ein gehacktes Netzwerk sind die folgenden:

* Die Dateien wurden verschlüsselt.
* Das Netzwerk wird ungewöhnlich langsam.
* Die Netzwerkauslastung wird sehr hoch.
* Die Programme stürzen ständig ab.
* Die Systeme arbeiten von selbst, ohne jeglichen Input.
* Nutzende erhalten Ransomware-Meldungen auf ihren Computerbildschirmen.

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Normalerweise versucht der Hacker zunächst, das menschliche *Vertrauen* auszunutzen.

Zusammenfassung

In dieser Lektion haben wir explizit CAPEC besprochen, einen Katalog, der die beliebtesten Methoden von Angreifenden enthält. Wir haben gelernt, wie wir das Cyberabwehrprogramm eines Unternehmens verbessern können. Dazu müssen wir herausfinden, was der nächste gegnerische Schritt sein könnte und im Vorfeld geeignete Sicherheitsmaßnahmen ergreifen. Anschließend haben wir uns mit Forschungsarbeiten zum Datenschutz befasst, in denen das Konzept der Privatsphäre als eine Taxonomie betrachtet wird. Wir haben erörtert, wie wir dieses Konzept nutzen können, um die Probleme im Zusammenhang mit der Privatsphäre sowie die potenziellen Folgen einer Beeinträchtigung dieser Privatsphäre zu verstehen.

Außerdem wurde das MITRE-ATT&CK-Framework im Detail behandelt. Diese Datenbank wird ständig mit den neuesten gegnerischen Taktiken und Methoden aktualisiert. Wir haben gesehen, wie Analysten diese Datenbank für Bedrohungsinformationen nutzen können, um den Gegnern einen Schritt voraus zu sein: Dazu modellieren sie Bedrohungen mit den im Framework genannten Taktiken und Methoden. Schließlich haben wir einige der wichtigsten Anzeichen für Hackerangriffe und manipulierte Konten erörtert, die auch normalen Internetnutzenden bei der Erkennung und Behebung von Cyberangriffen helfen können.

# Lektion 5 – Regeln, Vorschriften und Strafverfolgung

**Lernziele**

Nach Abschluss dieser Lektion werden Sie in der Lage sein,

… das Konzept des Internetrechts zu verstehen.

… das Konzept der Compliance und der regulatorischen Anforderungen zu erklären.

… das Konzept und die Notwendigkeit der Strafverfolgung im Cyberspace zu identifizieren.

# 5. Regeln, Vorschriften und Strafverfolgung

## Einführung

Im Bereich der Cybersicherheit verwenden wir oft das Wort „Cyberspace“. Dieser Begriff wurde erstmals von William Gibson in den frühen 1980er Jahren in seinem Science-Fiction-Roman Neuromancer geprägt (Bussell, 2013). Gibson veranschaulichte den Cyberspace als eine virtuelle, von Computernetzwerken geschaffene Landschaft. Heute gilt der Cyberspace als eine Umgebung, in der die Kommunikation über ein Computernetzwerk stattfindet. Der Cyberspace könnte auch als virtuelles Medium bezeichnet werden, weil die Kommunikation über das Internet zwischen elektronischen Geräten ohne physische Grenzen stattfindet. Bei der Erörterung der Gesetze und Vorschriften zur Cybersicherheit ist das Verständnis des Begriffs Cyberspace unerlässlich, da dieser Begriff in der Literatur häufig verwendet wird.

Bei der Entwicklung des Internets war den Fachleuten aus Forschung und Entwicklung klar, dass es sich zu einer Bestie entwickeln würde, die für verschiedene unmoralische und illegale Aktivitäten ausgenutzt werden könnte, und dass zur Kontrolle seiner Nutzung schließlich strenge Gesetze erforderlich sein würden. Im Cyberspace finden verschiedene besorgniserregende Aktivitäten wie Geldwäsche, Terrorismus und Identitätsdiebstahl statt. Dies sind Grauzonen, die das Internetrecht notwendig gemacht haben.

**Einhaltung gesetzlicher Bestimmungen**

Regeln, die von Organisationen befolgt werden müssen, um kritische Informationen und Personen vor Cyberkriminellen zu schützen.

In dieser Lektion wird das Internetrecht erörtert und Gesetze erklärt, die bei der Kommunikation im Cyberspace befolgt werden müssen. Anschließend wird das Konzept der Compliance erörtert, also die Frage, wie eine Organisation internationale Standards befolgen sollte, um die **Einhaltung gesetzlicher Bestimmungen** oder die Sicherheit der Informationen vor einem Cyberangriff zu gewährleisten. Darüber hinaus wird das Konzept der Strafverfolgung im Zusammenhang mit dem Cyberspace diskutiert, sowie die Frage, wie Organisationen durch den Austausch von Bedrohungsdaten mit den Behörden Unterstützung bei der Bekämpfung von Cyberkriminellen erhalten.

## 5.1 Internetrecht

Im heutigen digitalen Zeitalter ist das Internet zu einem wesentlichen Aspekt des täglichen Lebens geworden, von der einfachen Kommunikation bis hin zum Einkaufen im Web. Fast jedes Unternehmen nutzt das Internet für seine täglichen Aktivitäten. Dies hat zum Anwachsen des **eCommerce** geführt. Unterschiedliche Vorgänge bei staatlichen Behörden werden ebenfalls online abgewickelt, und auch **eFinance** ist auf dem Vormarsch. Mit der rasanten Zunahme der Internetnutzung haben auch die damit verbundenen Bedrohungen zugenommen. Das Internetrecht (auch Online-Recht oder Cyber-Recht) dient als Schutz für die Kommunikation im Cyberspace und verhindert in gewissem Maße auch Cyberkriminalität. Auch wenn die Gesetzgebung im Bereich des Internetrechts für den Gesetzgeber schwierig ist, wird ständig daran gearbeitet, entsprechende Gesetze zu entwerfen, zu aktualisieren und zu erlassen, um illegale und fragwürdige Aktivitäten einzuschränken, die online oder im Cyberspace stattfinden (UNext-Redaktion, 2020).

**eCommerce**

Auch bekannt als elektronischer Handel. Der Begriff bezieht sich auf den Kauf und Verkauf von Dienstleistungen und Waren über das Internet.

**eFinance**

Über das Internet erbrachte Finanzdienstleistungen.

### Was bedeutet Internetrecht?

Das Internetrecht ist auch als Online-Recht, Cyber-Recht oder IT-Recht bekannt. Es ist definiert als eine rechtliche Struktur, die zur Regulierung der Kommunikation über das Internet und der damit verbundenen rechtlichen Fragen geschaffen wurde. Da wir über Gesetze sprechen, die sich mit einer Umgebung ohne physische Grenzen befassen, kann das Internetrecht auch als „Papier“-Gesetz für eine „papierlose“ Welt bezeichnet werden (UNext-Redaktion, 2020).

Das Internetrecht umfasst Aspekte des Vertragsrechts, des geistigen Eigentums, des Datenschutzes, der Gerichtsbarkeit, der Rede- und Meinungsfreiheit und der Privatsphäre. Es lenkt und gewährleistet die folgenden Dinge (UNext-Redaktion, 2020):

* Die Details zur digitalen Verbreitung von Informationen,
* die Bereitstellung einer rechtssicheren Identifizierung und die Akzeptanz von eDokumenten und
* die Schaffung und Etablierung eines rechtlichen Rahmens für Online-Transaktionen.

Kurz gesagt könnte man das Internetrecht als eine Infrastruktur betrachten, die eine rechtliche Grundlage für die Bekämpfung von Cyberkriminalität bietet (UNext-Redaktion, 2020).

Das für die Cybersicherheit geltende Internetrecht unterscheidet sich von Gerichtsbarkeit zu Gerichtsbarkeit und von Land zu Land. Auch die Strafen variieren von Geld- bis hin zu Gefängnisstrafen, je nach Art des begangenen Cyberverbrechens. Daher müssen die Bürger:innen das in ihren Ländern geltende Internetrecht verstehen. An dieser Stelle sei darauf hingewiesen, dass der amerikanische Computer Fraud and Abuse Act das erste Gesetz war, das 1986 im Cyberspace eingeführt wurde und den unbefugten und illegalen Zugriff auf digitale Vermögensgüter (wie Computer) und die unrechtmäßige Nutzung digitaler Informationen einschränkte (UNext-Redaktion, 2020).

### Bedeutung des Internetrechts

Das Internetrecht umfasst Regeln und Vorschriften, die Personen, Unternehmen und Organisationen vorschreiben, wie das Internet zu nutzen ist. Manche Bestimmungen davon schützen die Menschen vor Cyberkriminalität, also Vergehen und Verbrechen, die von Cyberkriminellen über das Internet verübt werden. Das Internetrecht lässt sich anhand der unten aufgeführten Punkte umreißen (UNext-Redaktion, 2020):

* Es bestimmt die Nachverfolgung aller elektronischen Aufzeichnungen.
* Es schreibt vor, welche Aktionen und Reaktionen im Cyberspace durchgeführt werden sollen.
* Es regelt jede Online-Aktivität.
* Es bietet Sicherheit für die digitalen Informationen von Organisationen, der Regierung und Einzelpersonen.
* Es fordert die Einhaltung von **detaillierten Überprüfungen** und der **Sorgfaltspflicht**.

**Detaillierte Überprüfung**

(Engl.: *Due diligence*) Gründliche Nachforschungen zur Entdeckung von Schwachstellen.

* Es hilft bei der Einrichtung einer elektronischen Verwaltung.

### Warum brauchen wir ein Internetrecht?

Mehr als 4,6 Milliarden Menschen weltweit nutzen das Internet nicht nur für ihre tägliche Kommunikation, sondern auch für Online-Transaktionen und eCommerce-Aktivitäten (UNext Editorial Team, 2020). Angesichts der rasanten Zunahme der Nutzung des Cyberspace trägt die Durchsetzung strenger Cyber-Regeln zur Schaffung einer sicheren Umgebung im Internet bei. Das Internetrecht dient der Abschreckung, weil Opfer gegen Personen vorgehen können, die gegen das Internetrecht verstoßen. Das wäre nicht möglich, wenn es kein Internetrecht gäbe (UNext Editorial Team, 2020).

**Sorgfaltspflicht**

Die Umsetzung geeigneter Sicherheitsmaßnahmen nach der Identifizierung von Schwachstellen.

### Die verschiedenen Elemente bzw. Artikel des Internetrechts

Innerhalb des Internetrechts gibt es verschiedene Artikel zum Schutz digitaler Informationen, deren wichtigste wir hier erörtern (UNext Editorial Team, 2020):

* **Schutz der Privatsphäre und der Daten**:Zu Einhaltung des Internetrechts müssen Unternehmen den Schutz von Daten und privaten Informationen vor Cyberkriminellen sicherstellen. Die entsprechenden Gesetze dienen der Abschreckung potenzieller Täter:innen in der digitalen Umgebung und verhindern den Missbrauch privater Informationen eines Nutzenden.
* **Cyberkriminalität**:Als Cyberkriminalität (Internetkriminalität) werden alle illegalen Aktivitäten bezeichnet, die über das Internet ausgeführt werden. Beispiele für solche Verbrechen sind Hackerangriffe, Erpressung, Geldwäsche und Cybermobbing, um nur einige zu nennen. Das in einem Land geltende Internetrecht sieht vor, dass Täter:innen für solche Handlungen zur Rechenschaft gezogen werden können.
* **Geistiges Eigentum**: Jedes Werk einer Gruppe oder eines Einzelnen, darunter Erfindungen, Designs, Symbole sowie jedes immaterielle, urheberrechtlich geschützte Element, wird als geistiges Eigentum der betreffenden Personen bezeichnet. Das Internetrecht bietet Schutz vor der illegalen Nutzung oder dem Diebstahl geistigen Eigentums.

### Arten von Cyberkriminalität

Cyberkriminalität wird meist in die folgenden drei Kategorien eingeteilt (UNext-Redaktion, 2020):

1. **Eigentum**:Der illegale Besitz und die Nutzung digitaler Informationen, die Übertragung und Nutzung bösartiger Programme, der Diebstahl von Finanzdaten usw. sind Beispiele für Eigentums-Cyberkriminalität.
2. **Einzelperson**: Der Diebstahl persönlicher Daten, Online-Belästigung, die Weitergabe von Kinderpornografie und die Verwendung vulgärer und obszöner Daten sind die häufigsten Beispiele für Cyberkriminalität, die sich gegen Einzelpersonen richtet.
3. **Regierung**: Cyberkriminalität, die Regierungen bzw. Staaten gegen andere ausüben, fällt unter diese Kategorie. Diese Verbrechen werden auch als *Advanced Persistent Threat* (APT; deutsch „fortgeschrittene andauernde Bedrohung“) bezeichnet und von einer Gruppe von Fachleuten ausgeführt.

**Digitale Signatur**

Eine mathematische Berechnungsmethode, mit Hilfe derer Integrität und Authentizität eines digitalen Dokuments, einer Software oder einer elektronischen Nachricht bestätigt werden kann.

### Ziele des Internetrechts

Das Hauptziel des Internetrechts ist die Kontrolle und Aufrechterhaltung der Rechtsstaatlichkeit bei jeder Art von Online-Aktivität und die Eindämmung der Cyberkriminalität. Die wichtigsten Ziele, die durch das Internetrecht erreicht werden sollen, sind hier zum besseren Verständnis aufgeführt (UNext Editorial Team, 2020):

* Im Gegensatz zu papierbasierten Transaktionen und Kommunikationen erfolgt die rechtliche Authentifizierung und Anerkennung von Online-Transaktionen durch das Internetrecht.
* Aufgrund des Internetrechts hat sich das Konzept und die Implementierung **digitaler Signaturen** weit verbreitet.
* Das Internetrecht fördert die elektronische Einreichung von Dokumenten bei Behörden und Ministerien, wie z. B. dem sog. **eFiling**.

**eFiling**

Die Einreichung von Steuererklärungen über das Internet im englischen Sprachraum.

* Es ermöglicht Geldtransfers über das Internet, d. h. elektronische Überweisungen zwischen Banken, Finanzinstituten, Personen und so weiter.
* Es erlaubt den Banken rechtlich, Kontoinformationen elektronisch zu speichern.

### Arten von illegalen Online-Aktivitäten, die durch das Internetrecht abgedeckt werden

Wir wollen hier die wichtigsten Arten illegaler Online-Aktivitäten erörtern, die vom Internetrecht abgedeckt werden (UNext-Redaktion, 2020):

* **Urheberrecht (Copyright):** Der Schutz der Rechte von Einzelpersonen und Unternehmen, Einnahmen aus den von ihnen geschaffenen Originalwerken zu erzielen. Der Missbrauch von urheberrechtlich geschütztem Material ist indirekt ein Verstoß gegen das Internetrecht des betreffenden Landes oder der Gerichtsbarkeit. Aufgrund des Internetrechts wird die Verletzung von urheberrechtlich geschütztem Online-Material heute streng verfolgt und geahndet.
* **Verleumdung**: Die Verbreitung falscher Behauptungen im Internet oder in den sozialen Medien über Persönlichkeiten des öffentlichen Lebens, Unternehmen oder Einzelpersonen. Solche Vergehen werden durch entsprechende Bestimmungen abgedeckt und ermöglichen betroffenen Internetnutzenden, gerichtlich gegen die Täter:innen vorzugehen. Die jeweiligen Internetnutzenden können hierbei professionell oder privat agieren, denn die Verbreitung von Falschaussagen könnte sogar durch die Erstellung eines gefälschten Social-Media-Kontos im Namen des Opfers erfolgen, wofür keine besonderen technischen Kenntnisse erforderlich sind.
* **Betrug**: Das Internetrecht schützt Personen vor Betrug im Internet. Online-Betrug umfasst unter anderem illegale Internet-Aktivitäten im Zusammenhang mit Geld sowie **Identitätsdiebstahl** und Diebstahl von Kreditkartendaten. Menschen werden strafrechtlich belangt, wenn sie Online-Betrug begehen.

**Identitätsdiebstahl**

Betrug unter Verwendung einer gestohlenen Identität wird als Identitätsdiebstahl bezeichnet.

* **Stalking und Belästigung**: Stalking und Belästigung bedeuten die Veröffentlichung bedrohlicher oder einschüchternder Aussagen über eine unschuldige Person in sozialen Medien. Dies ist eine böswillige Handlung und verstößt gegen zivil- und strafrechtliche Gesetze, auf die wir später eingehen werden.
* **Meinungsfreiheit**: Das Internet ist ein Medium, das seinen Nutzenden erlaubt, sich frei auszudrücken. Es gibt jedoch bestimmte Grenzen, deren Überschreitung zu einem Verstoß gegen das Internetrecht führen würde.
* **Geschäftsgeheimnisse:** Geschäftsgeheimnisse sind eine Art geistiges Eigentum, z. B. eine Methode eines Unternehmens zur Herstellung seiner Produkte. Der Diebstahl von Geschäftsgeheimnissen ist ebenfalls ein Verstoß gegen das Internetrecht. Daher bietet das Internetrecht den Unternehmen auch Schutz, indem es ihnen rechtliche Schritte gegen die verdächtige Organisation ermöglicht.
* **Arbeits- und Vertragsrecht:** Auf Websites oder beim Herunterladen von Software wird immer wieder darauf hingewiesen, dass vor Betrachtung oder Nutzung der Inhalte den Geschäftsbedingungen zuzustimmen ist. Normalerweise nehmen die meisten Menschen das nicht ernst. Trotzdem fällt auch dies unter das Internetrecht zum Schutz der Online-Privatsphäre.

Bei der Diskussion von Gesetzen im Cyberspace ist es wichtig, den Unterschied zwischen Strafrecht und Zivilrecht zu kennen und zu verstehen, da dieser auch bei der Diskussion des Internetrechts ausführlich erörtert wird. Im folgenden Lernzyklus wird ausdrücklich auf das Straf- und Zivilrecht eingegangen.

### Unterschiede zwischen Straf- und Zivilrecht

Es gibt einige Unterschiede zwischen dem Straf- und dem Zivilrecht, die wir hier erläutern.

#### Strafrecht

Das Strafrecht bezieht sich auf bestimmte Verhaltensweisen, die als Straftaten bezeichnet und entsprechend bestraft werden. Das Strafrecht wird in der Regel von staatlichen Behörden durchgesetzt, z. B. Verbote von Computer-Hacking und Bankbetrug. Das Strafrecht kann als Kombination der folgenden Punkte beschrieben werden (Rashid et al., 2019, S. 55):

* **Abschreckung**:Die Menschen sollen vor strafrechtlichem Verhalten abgeschreckt werden. Dies gilt für Kriminelle genauso wie für andere Mitglieder der Gesellschaft.
* **Unfähigmachung**: Einschränkung der Möglichkeiten von Kriminellen, der Gesellschaft weiter zu schaden.
* **Bestrafung**:Den Kriminellen soll ein Schaden zugefügt werden, damit sie für die von ihnen begangenen Verbrechen leiden.
* **Wiedergutmachung**:Die Kriminellen müssen ihren Opfern bestimmte Entschädigungsleistungen erbringen.
* **Resozialisierung**:Hierdurch soll das Verhalten von Kriminellen dauerhaft gebessert werden.

Begriffe wie „unschuldig“ und „schuldig“ sind in der Regel die Ergebnisse (Urteile) in Strafverfahren. Daher sollten diese Formulierungen bei Urteilen in Zivilprozessen nicht verwendet werden (Rashid et al., 2019, S. 55). Zu den möglichen Bestrafungen nach dem Strafrecht gehören Geldstrafen, die in der Regel an den Staat gezahlt werden, die Beschlagnahme von Erträgen aus Straftaten, finanzielle oder sonstige Entschädigungen an die Opfer sowie Gefängnisstrafen (Rashid et al., 2019, S. 55).

#### Zivilrecht

#### Das Zivilrecht regelt die privaten Beziehungen zwischen verschiedenen Personen. Dazu gehören zum Beispiel Bestimmungen zur Fahrlässigkeit und das Vertragsrecht. Rechtsverletzungen nach dem Zivilrecht können zu Gerichtsverfahren gegen die schuldige Partei führen (Rashid et al., 2019, S. 55).

Die Rechtsmittel nach dem Zivilrecht enthalten in der Regel eine Kombinationen der folgenden Punkte:

* Die haftende Partei zahlt eine Entschädigung an die geschädigte Partei.
* Die Rechtsbeziehungen zwischen den Parteien sind beendet.
* Eine haftende Partei muss ihre schädlichen Aktivitäten einstellen.
* Eine haftende Partei muss eine positive Handlung vornehmen, wie z. B. die Übertragung des Eigentums an einem Vermögen.

Zivilrechtliche Bestimmungen werden in der Regel in dem Bemühen geschaffen, die negativen Folgen des Verhaltens in der Gesellschaft zu korrigieren. Außerdem sollten Menschen, die sich der Gesetze bewusst sind, verantwortungsbewusster handeln und letztlich ihr Verhalten in Bezug auf die Cybersicherheit ändern (Rashid et al., 2019, S. 55, 56).

### Fragen zur Selbstkontrolle

1. Nennen Sie zwei wichtige Aktivitäten, die Unternehmen oder Personen bei ihren täglichen Aktivitäten im Internet durchführen.

*eCommerce*

*eFinance*

*Online-Transaktionen*

*Einkaufen im Internet*

*Kommunikation*

## 5.2 Einhaltung von Bestimmungen (Compliance) und Strafverfolgung

Die Umsetzung von Cybersicherheit in einem Unternehmen ist eine komplexe Aufgabe. Dazu gehört eine auf Resilienz ausgerichtete Strategie für dem Internet ausgesetzte Hardware- und Software-Infrastrukturen, um potenzielle Schwachstellen zu beseitigen, die sich auf Kund:innen, Unternehmen und betroffene **Akteure** auswirken könnten. Die Einhaltung gesetzlicher Vorschriften unterstützt und erzwingt die Umsetzung dieser Widerstandsfähigkeit gegen Cyberangriffe durch die Unternehmen (NordLayer, 2022).

**Akteur (engl. Stakeholder)**

Eine Organisation oder Person, mit einem Recht, einem Anspruch, einem Interesse oder einem Anteil an einem Rechtsgut, der ihren Erwartungen und Bedürfnissen entspricht.

### Was bedeutet Compliance in der Cybersicherheit?

Die Einhaltung der Cybersicherheit bedeutet die Implementierung von Sicherheitsmaßnahmen, die Branchenstandards wie ISO 27001 erfüllen. Das **Managementsystem für Informationssicherheit** (ISMS = Information Security Management System) eines Unternehmens, das die gesetzlichen Anforderungen erfüllt, ermöglicht dem Unternehmen, die notwendigen Sicherheitsmaßnahmen zu ergreifen, mit denen die Wahrscheinlichkeit eines Datenschutzverstoßes verringert wird. Die Unternehmen können damit auch Pläne für den Fall eines Verstoßes aufstellen, wie z. B. die Mitteilung der Fakten und Auswirkungen eines Verstoßes an die betroffenen Parteien (NordLayer, 2022).

**Managementsystem für Informationssicherheit**

Ein System aus Kontrollen und Richtlinien, das Risiken und Sicherheit methodisch in einer gesamten Organisation verwaltet.

### Bedeutung der Einhaltung von Cybersicherheitsvorschriften

Die Einhaltung von Cybersicherheitsvorschriften umfasst natürlich nicht nur eine Reihe von verbindlichen und strengen Anforderungen einer Aufsichtsbehörde, sondern beeinflusst auch den Gesamterfolg des Unternehmens.

Jede Organisation, die im Cyberspace existiert, ist ein potenzielles Ziel für einen Cyberangriff. Datenschutzverstöße können sich zu einer komplexen Situation ausweiten, die sich auf die Finanzen und den Ruf eines Unternehmens auswirken und zu Streitigkeiten und Gerichtsverfahren führen könnte. Ein Unternehmen, das die Anforderungen und Standards für die Compliance in der Cybersicherheit erfüllt, verringert damit auch das Risiko eines Cyberangriffs (NordLayer, 2022). Die Einhaltung von Cybersicherheitsvorschriften hat unter anderem die folgenden Vorteile:

* Vermeidung schwerer Sanktionen und Geldstrafen.
* Schutz des Prestiges der Organisation durch Verhinderung nicht konformer Aktivitäten.
* Unterstützung und Gewährleistung des Rechts der Kund:innen auf Privatsphäre, also auf Zugriff, Änderung oder Löschung ihrer Daten, was letztendlich die Geschäftsfunktionen stärkt.
* Vergrößert das Vertrauen bei den Akteuren, weil sie sehen können, dass die Organisation ihre Sorgfaltspflicht zum Schutz der gesammelten Daten erfüllt hat.
* Hilft Unternehmen, durch Einrichtung der notwendigen Sicherheitsmaßnahmen die Anforderungen der einschlägigen Gesetze und Vorschriften zu erfüllen.
* Fördert die Verantwortlichkeit und Transparenz innerhalb einer Organisation.

#### Branchenstandards

Die Anpassung von Sicherheitsstandards in Unternehmen hilft Sicherheitsfachleuten, Fehlinterpretationen zwischen den Unternehmen zu vermeiden, und unterstützt die Koordination bei der Einhaltung von Cybersicherheitsbestimmungen. Wenn ein Unternehmen beispielsweise sagt, es sei ISO-27001-konform, dann wissen alle, die diese Norm kennen, dass das Unternehmen die strengen Sicherheitsmaßnahmen dieser Norm einhält (NordLayer, 2022). Es gibt mehrere Normen, die Organisationen je nach ihren Anforderungen befolgen können, darunter ISO 27001, PCI-DSS und der deutsche IT-Grundschutz. Im nächsten Lernzyklus erläutern wir einige davon.

#### Vermeidung von Bußgeldern

Durch die Implementierung bewährter Sicherheitspraktiken und ‑maßnahmen gemäß den gesetzlichen Anforderungen können sich Unternehmen vor Bußgeldern und Strafen nach einer Datenverletzung schützen (NordLayer, 2022). So muss beispielsweise eine Bank, die über die Kreditkartendaten ihrer Kund:innen verfügt, diese gemäß dem Payment Card Industry Data Security Standard (PCI-DSS) schützen, und im Falle eines Verstoßes drohen der Bank hohe Strafen. Die in der Sicherheitsbranche gängigsten internationalen Sicherheitsstandards werden im nächsten Lernzyklus erläutert.

### Allgemeine Anforderungen an die Cybersicherheit

**Verordnungen**

Richtlinien oder Vorschriften für Organisationen zum Schutz der Daten vor Cyberangriffen.

Die Standards für die **Einhaltung** der Cybersicherheit (Compliance) werden durch die entsprechenden **Verordnungen** festgelegt. Obwohl die in den einzelnen Standards beschriebenen Methoden unterschiedlich sind, ist das Ziel das gleiche, nämlich die Entwicklung von Regeln, die in einer Organisation zum Schutz sensibler Informationen leicht befolgt und umgesetzt werden können.

**Einhaltung (Compliance)**

Die Einhaltung staatlicher oder internationaler Vorschriften und Gesetze wird auch als Compliance (Konformität) bezeichnet.

Die Compliance-Anforderungen hängen vom Standort des Unternehmens und dem Markt ab, in dem es die Daten verarbeitet und betreibt. Das Hauptziel ist die Implementierung eines ISMS (*Information Security Management System*), das den Schutz der Daten vor Cyberangriffen gewährleistet. Organisationen, die Zugang zu vertraulichen Daten haben, sind das häufigste Opfer von Cyberangriffen (NordLayer, 2022). Einige der gängigsten Sicherheitsstandards und gesetzlichen Anforderungen werden im Folgenden erläutert:

#### ISO/IEC 27001

Eine der gängigsten internationalen Normen für die Einführung eines ISMS ist ISO/IEC 27001. Diese Norm stammt von der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC).

Jedes Unternehmen, das nach ISO 27001 zertifiziert ist, zeigt damit, dass es alle in der Norm ISO 27001 genannten Kontrollen einhält. Der Standard beschreibt die bewährten Vorgehensweisen zur Einrichtung eines zuverlässigen und widerstandsfähigen Cybersicherheitsprogramms in einer Organisation (NordLayer, 2022).

#### PCI-DSS

PCI-DSS ist ein Informationssicherheitsstandard, der zum Schutz der Daten von Kreditkarten und deren Inhaber:innen umgesetzt werden muss. Der Standard gilt für alle Händler, die Kreditkartenzahlungen abwickeln. Unternehmen, die PCI-DSS nicht einhalten, laufen Gefahr, ihre Händlerlizenz zu verlieren Der Verlust der Händlerlizenz bedeutet, dass sie zukünftig keine Zahlungen mit Kreditkarten mehr abwickeln können. Unternehmen, die nicht nach PCI-DSS arbeiten, riskieren Cyberangriffe (und dadurch eine Rufschädigung) und müssen außerdem mit hohen Geldstrafen von den Aufsichtsbehörden rechnen (NordLayer, 2022).

#### DSGVO

Die Datenschutz-Grundverordnung (DSGVO oder engl. *GDPR = General Data Protection Regulation*) ist ein Gesetz zum Schutz der Privatsphäre und des Datenschutzes, das 2016 veröffentlicht wurde und 2018 in Kraft getreten ist. Sie gilt für den Europäischen Wirtschaftsraum (EWR) und die Länder der Europäischen Union (EU). Die DSGVO bietet eine rechtliche Struktur, die den Schutz der personenbezogenen Daten von in der EU und im EWR ansässigen Personen gewährleistet.

Die DSGVO verpflichtet Unternehmen dazu, klare und präzise Geschäftsbedingungen zu erstellen, aus denen hervorgeht, wie genau die Kundendaten verarbeitet werden. Zur Einhaltung der DSGVO müssen Unternehmen daher die Zustimmung jedes Einzelnen einholen, bevor sie deren personenbezogene Daten verarbeiten. Gleichzeitig garantieren sie die Vertraulichkeit der Daten und verpflichten sich, die betreffenden Personen im Falle einer Datenschutzverletzung zu benachrichtigen (NordLayer, 2022).

#### HIPAA

Der Health Insurance Portability and Accountability Act (HIPAA) ist ein 1996 von den USA erlassenes Bundesgesetz zum Schutz gesundheitsbezogener Informationen. Alle Einrichtungen, die für die Verarbeitung und Speicherung von gesundheitsbezogenen Informationen im Internet verantwortlich sind, müssen den HIPAA einhalten. Die HIPAA-Bestimmungen unterstützen Einrichtungen im Gesundheitssektor (wie Krankenhäuser und Gesundheitsdienstleister) durch Empfehlungen, z. B. zu den notwendigen Sicherheitsmaßnahmen zum Schutz persönlicher Daten vor einer Datenschutzverletzung. Außerdem verpflichtet HIPAA die Einrichtungen dazu, Daten nicht ohne die Zustimmung der betreffenden Person weiterzugeben. Die HIPAA-Bestimmungen gelten nur für Einrichtungen innerhalb der USA. (NordLayer, 2022).

#### FISMA

Der Federal Information Security Management Act (FISMA) ist ein US-amerikanisches Gesetz aus dem Jahr 2002. Es handelt sich um ein umfassendes Rahmenwerk, das die Anforderungen an die Sicherheit von US-Bundessystemen oder Systemen, die hochvertrauliche Daten im nationalen Interesse des Landes enthalten, festlegt. Das Gesetz ist mit anderen gültigen Gesetzen und Durchführungsverordnungen des Landes abgestimmt, um die Einhaltung der Cybersicherheit zu gewährleisten (NordLayer, 2022).

### Strafverfolgung

Für die Cybersicherheit müssen Cyberkriminelle verhaftet und ihre illegalen Aktivitäten gestoppt werden. Cyberkriminelle können davon abgehalten werden, weiterhin Verbrechen zu begehen, indem die von ihnen genutzte Infrastruktur zur Ausführung von Cyberangriffen entfernt wird. Durch Strafverfolgung lassen sich Cyberangriffe auch vereiteln, Vorfälle nachverfolgen und strafrechtlich ahnden. Die Strafverfolgung stellt nicht nur eine Reaktion auf Vorfälle dar, sondern auch eine Vorbeugung, weil sie Cyberkriminelle abschreckt (U.S. Department of Justice, o. D.).

Die Strafverfolgungsbehörden unterbrechen und beenden laufende cyberkriminelle Tatbestände durch Gerichtsverfahren oder Verhaftungen und hindern andere daran, sich an solchen Aktivitäten zu beteiligen. Diese Behörden sind auf die Methoden und Taktiken der Akteure im Bereich Cyberangriffe spezialisiert und entsprechend geschult. Da sie außerdem Zugang zu speziellen Ressourcen und Aufklärungsdaten zu Bedrohungen haben, verfügen sie über einen umfassenden Einblick in **ausgeklügelte Angriffe**. Beispielsweise könnte die Untersuchung einer kriminellen Organisation wertvolle Informationen über die Methoden und die Infrastruktur anderer krimineller Organisationen liefern. Zur Bekämpfung von internationalen kriminellen Organisationen sind diese Behörden auch auf internationale Beziehungen und Ressourcen angewiesen. Die internationale Vernetzung der Behörden ist unerlässlich, um gegen Cyberangriffe vorzugehen, die von kriminellen Organisationen in anderen Ländern ausgeführt und gesteuert werden (U.S. Department of Justice, o. D.).

**Ausgeklügelter Angriff**

Ein Cyberangriff, der von hochqualifizierten Fachleuten auf eine Organisation gerichtet ist.

Geschädigte Organisationen oder Kund:innen melden die Tatbestände den Strafverfolgungsbehörden, die dann Ermittlungen gegen die Cyberkriminellen einleiten. Die Behörde kann ihre Ermittlungen erst dann aufnehmen, wenn sie darüber informiert wurde, dass ein Vorfall auf einen Cyberangriff zurückzuführen ist. Daher sollten die Opfer in solchen Situationen die Vorfälle und böswilligen Aktivitäten den Strafverfolgungsbehörden melden. Dies ermutigt Organisationen zur Entwicklung einer starken Kommunikationskultur und zum Austausch genauer Informationen zu den Bedrohungen mit den Strafverfolgungsbehörden, denn eine wirksame Bestrafung von Cyberkriminellen erfordert intensive Unterstützung durch die Opfer. Nachdem die Opfer den Strafverfolgungsbehörden einen Cyberangriff gemeldet haben, sichern diese schnell die digitalen Beweise. Die rechtzeitige Kontaktaufnahme mit den Strafverfolgungsbehörden stellt daher sicher, dass die Beweise für die Cyberkriminalität ordnungsgemäß gesichert werden und der Tatort für Ermittlungen zur Verfügung steht, um schließlich die Täter:innen zur Verantwortung zu ziehen (U.S. Department of Justice, o. D.).

Bei der Bekämpfung von Cyberkriminalität ist eine starke Koordination zwischen betroffenen Organisationen und Strafverfolgungsbehörden erforderlich. Das Wissen und die Informationen der Organisation unterstützen die Strafverfolgungsbehörden bei der Durchführung von Ermittlungen, die strafrechtliche Sanktionen nach sich ziehen können. Dies könnte eine entscheidende Abschreckung für Kriminelle darstellen und sie dazu bringen, sich einen Angriff sehr genau zu überlegen (U.S. Department of Justice, o. D.).

### Fragen zur Selbstkontrolle

1. Nennen Sie zwei internationale Normen oder Vorschriften, die Organisationen im Bereich Datenschutz und Schutz vor Cyberangriffen einhalten sollten (Compliance).

*ISO 27001*

*FISMA*

*DSGVO (GDPR)*

*HIPAA*

*PCI-DSS*

Zusammenfassung

In dieser Lektion haben wir das Konzept des Internetrechts besprochen und erklärt, wie zivil- und strafrechtliche Gesetze bei Verstößen gegen das Internetrecht eingesetzt werden können. Außerdem haben wir untersucht, mit welchen Konsequenzen Cyberkriminelle rechnen müssen, wenn sie gegen diese Gesetze verstoßen. Darüber hinaus wurde das Konzept der Einhaltung gesetzlicher Vorschriften erörtert. Dabei haben wir erläutert, wie Unternehmen verschiedene internationale Normen einhalten müssen, um die Daten ihrer Kund:innen vor Cyberangriffen zu schützen und sie vor Geldstrafen zu bewahren. Schließlich haben wir die Rolle der Strafverfolgungsbehörden bei der Cybersicherheit besprochen und gesehen, wie sie ein abschreckendes Umfeld für Cyberkriminelle schaffen können.

# Lektion 6 – Risikomanagement

**Lernziele**

Nach Abschluss dieser Lektion werden Sie in der Lage sein,

… die Konzepte von Risiko, Risikomanagement, Risikobewertung und Risikominderung zu verstehen.

… die Begriffe Vorfallmanagement und Krisenmanagement zu begreifen.

… das Konzept der kontinuierlichen Überwachung und Neubewertung des Risikomanagementprozesses zu definieren.

… das Konzept der schwarzen Schwäne zu identifizieren und zu analysieren.

# 6. Risikomanagement

## Einführung

Unternehmen sind zur Erreichung ihrer Geschäftsziele in hohem Maße von technologischen Ressourcen abhängig. Wenn die Informationstechnologie (IT) eines Unternehmens oder einer Organisation ausfällt, hat dies negative Folgen: Der normale Geschäftsbetrieb wird unterbrochen, die Ziele können nicht erreicht werden und somit entsteht ein erheblicher wirtschaftlicher Verlust für das Unternehmen selbst und darüber hinaus. Der **Cyberspace** stellt eine ständig wachsende Bedrohung für Unternehmen und ihre IT-Infrastruktur dar, die es ihnen erschwert, ihre Geschäftsziele zu erreichen und ihre Kernfunktionen zu erfüllen. Daher liegt die Verantwortung für die Cybersicherheit sowohl bei den IT-Fachleuten als auch bei der Geschäftsleitung. Zur Umsetzung eines wirksamen Cybersicherheitsprogramms in einem Unternehmen ist ein umfassender Ansatz für das Risikomanagement im Bereich der Cybersicherheit erforderlich.

**Cyberspace**

Eine virtuelle Welt, in der die Kommunikation über das Internet stattfindet.

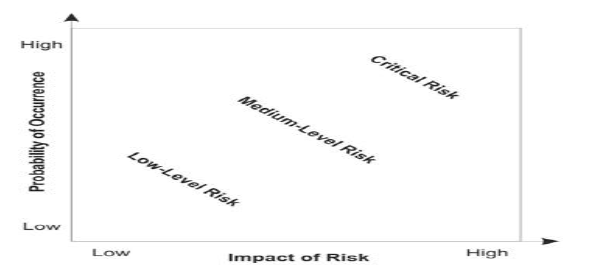
In dieser Lektion besprechen wir ausführlich das Konzept und die Umsetzung des Risikomanagements in der Cybersicherheit. Das Konzept und die Prozesse der Risikobewertung, der Risikominderung sowie der kontinuierlichen Überwachung und Neubewertung, die unter den Begriff des Risikomanagements fallen, werden ebenfalls besprochen. Darüber hinaus werden die Themen Vorfallmanagement und Krisenmanagement behandelt. Diese kommen zum Tragen, wenn in einer Organisation ein Vorfall, der zu einer Krise führen könnte, trotz eines robusten Risikomanagementprozesses eintritt. Zum Schluss beschreiben wir kurz schwarze Schwäne und ihre Auswirkungen auf den Markt.

## 6.1 Risikomanagement: Ein Überblick

Ein Risiko ist die Wahrscheinlichkeit des Auftretens eines Ereignisses, das sich auf die Erreichung der Ziele einer Organisation auswirken würde. Risiko kann mathematisch wie folgt definiert werden:

Die folgende Abbildung zeigt, wie das Risiko in einer Matrix als Kombination aus Auswirkung und Wahrscheinlichkeit dargestellt werden kann.

Die Wahrscheinlichkeits-Auswirkungs-Risiko-Matrix



Quelle: Verma et al. (2016, S. 152) CC BY-SA 4.0.

Es gibt viele verschiedene Arten von Risiken: Finanz-, IT-, Personal- und Betriebsrisiken sind nur einige der Möglichkeiten. Zur effizienten Risikobewältigung setzen Unternehmen eine Risikomanagementmethode ein, mit der sie diese Risiken identifizieren, bewerten und eindämmen können. Die Risiken, die in Unternehmen möglicherweise auftreten können, lassen sich nach ihrem Schweregrad kategorisieren. Sie reichen von banalen Unannehmlichkeiten bis hin zu Risiken, welche die kritischen Geschäftsabläufe des gesamten Unternehmens bedrohen können. Das Risiko in der Cybersicherheit ist eine Funktion aus der Wahrscheinlichkeit, dass eine Bedrohungsquelle eine Schwachstelle ausnutzt, und der aus diesem schädlichen Ereignis resultierenden Auswirkungen auf das Gesamtsystem und die Aufgaben einer Organisation. Unternehmen müssen strenge Risikomanagementprozesse entwickeln und umsetzen, um sich vor Cyberangriffen zu schützen und ihre Geschäftsziele zu erreichen. Häufig sind diese Prozesse auch gesetzlich vorgeschrieben (Verma et al., 2016, S. 152–153).

Risikomanagement bezeichnet den Prozess der Risikobewertung und der Ergreifung geeigneter Maßnahmen, um die Risiken auf ein akzeptables Niveau zu verringern oder sie zu vermeiden. Die Schritte im Prozess des Risikomanagements sind in der Regel Risikobewertung und Risikominderung.

## Risikobewertung

Bei der Risikobewertung wird versucht, Bedrohungen für Informationssysteme oder Informationen zu identifizieren, ihre Wahrscheinlichkeit zu bestimmen und die potenziell ausnutzbaren Schwachstellen in Netzwerken, Systemen und Anwendungen zu ermitteln. Der erste Schritt im Prozess des Risikomanagements ist die Risikobewertung. Risiken werden bewertet oder abgeschätzt, indem zunächst die Schwachstellen und Bedrohungen identifiziert und anschließend die Auswirkungen und die Wahrscheinlichkeit des Risikos bestimmt werden. Im Folgenden wird ein typischer Risikobewertungsvorgang beschrieben (Verma et al., 2016, S. 153):

1. Identifizierung und Klassifizierung von Vermögensgütern (Ressourcen),
2. Identifizierung der Bedrohungen,
3. Identifizierung der Schwachstellen,
4. Analyse des Risikos,
5. Auswahl einer Methodik zur Risikobewertung.

#### Identifizierung und Klassifizierung von Vermögensgütern

Der erste Schritt im Prozess der Risikobewertung ist die Identifizierung und Klassifizierung von IT-Vermögensgütern oder Ressourcen. Bei der Klassifizierung wird einem Vermögensgut anhand einer vordefinierten Skala und abhängig von seiner Bedeutung eine Kategorie oder Kennzeichnung zugewiesen.IT-Vermögensgüter umfassen alle Formen von Informationen, wie Datenbanken, Dateien oder spezifische digitale und nicht-digitale Vermögensgüter. Organisationen sind für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von IT-Vermögensgütern verantwortlich.

Sie sind Eigentümer der Informationen, die den Wert eines Vermögensguts bestimmen. Der Wert von IT-Vermögensgütern für ein Unternehmen hängt von dessen Zielen ab. Daher müssen alle IT-Vermögensgüter identifiziert werden. Am besten sollte eine vollständige Liste der IT-Vermögensgüter erstellt und einzeln als öffentlich, eingeschränkt oder vertraulich klassifiziert werden. Die Informationen über die Klassifizierung der einzelnen Vermögensgüter sollten ebenfalls in einer zentralen Liste enthalten sein (Verma et al., 2016, S. 154).

#### Identifizierung von Bedrohungen

Eine Bedrohung kann eine Person, eine Organisation oder eine Kraft sein, die darauf abzielt, Informationen zu manipulieren oder darauf zuzugreifen. Durch die Analyse der Fähigkeiten und Ressourcen einer Bedrohung kann man im Rahmen der Risikobewertung die Wahrscheinlichkeit ihres Auftretens ermitteln. Die Bedrohung kann in Bezug auf die Wahrscheinlichkeit eines Angriffs bewertet werden. Bedrohungen im Bereich der Informationssicherheit können wie folgt eingeteilt werden:

* Social Engineering (soziale Manipulation),
* Naturkatastrophen wie Tornados, Überschwemmungen, Erdbeben und Brände,
* Schadsoftware wie Viren, Würmer und Trojanische Pferde,
* Insider-Bedrohungen wie verärgerte Mitarbeitende,
* Netzwerkangriffe wie Routing-Angriffe, Man-in-the-Middle-Angriffe und Denial-of-Service-Angriffe.

#### Bewertung und Identifizierung von Schwachstellen

Schwachstellen sind Schwächen im Netzwerk, im System oder in den Anwendungen, die Angreifende ausnutzen könnten. Schwachstellen können alles sein, was einen Cyberangriff erfolgreich machen könnte. Einige Beispiele für Schwachstellen sind die folgenden:

* Ungepatchte Software,
* unsichere Anwendungen,
* Weitergabe vertraulicher Informationen an unbefugte Personen,
* Verwendung von einfachen und gleichen Passwörtern für mehrere Konten,
* fehlende Multi-Faktor-Authentifizierung.

#### Risikoanalyse

Die Übertragung und Aufbewahrung von Informationen birgt einige Risiken in sich. Informationen können unbeabsichtigten und beabsichtigten Handlungen unterliegen. Zum Beispiel könnte es sein, dass Unbefugte, wie verärgerte Mitarbeitende oder Konkurrenten, auf vertrauliche Informationen zugreifen und diese einsehen möchten. Hacker könnten auch versuchen, in Systeme einzudringen, die sensible Informationen enthalten, oder diese während der Übertragung abzufangen. Sie könnten auch ganz zufällig an vertrauliche und sensible Informationen gelangen. Außerdem könnten Informationssysteme versehentlich oder absichtlich beschädigt werden. Solche Verstöße gegen die Informationssicherheit können ein Unternehmen ernsthaft schädigen. Im Allgemeinen kann das Risiko für ein Vermögensgut wie folgt beschrieben werden:

*Risiko =   
(Wahrscheinlichkeit des Auftretens einer Bedrohung für ein Vermögensgut)   
x (Wert des Vermögensguts)*

Einfach ausgedrückt: Je größer die Wahrscheinlichkeit, dass sich eine Bedrohung auf das Vermögensgut auswirkt und je höher der Wert des Vermögensguts ist, desto größer ist das Risiko. Wenn die Wahrscheinlichkeit des Auftretens einer Bedrohung null oder sehr gering ist, oder wenn ein Vermögensgut (fast) keinen Wert hat, wäre das Risiko entsprechend null oder sehr niedrig (Verma et al., 2016, S. 155).

#### Methodik für die Risikobewertung

Unternehmen müssen Methoden zur Quantifizierung und Messung von Risiken entwickeln, damit die Ergebnisse der Risikobewertung leicht kommuniziert werden können. Es gibt verschiedene Methoden zur Risikobewertung, von denen einige im nächsten Unterlernzyklus beschrieben werden. Jedes Unternehmen muss diejenige auswählen, die sich am besten für seine Compliance-Anforderungen eignet. Die Werte der Vermögensgüter und der Grad des Risikos variieren von Unternehmen zu Unternehmen.

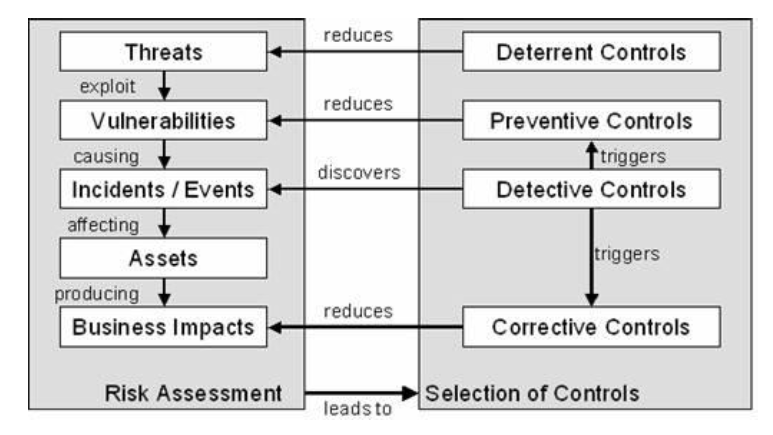
### Risikominderung

Das Ergreifen notwendiger Maßnahmen zur Verringerung der Wahrscheinlichkeit einer Bedrohung auf ein akzeptables Niveau wird als Risikominderung bezeichnet. In der Wirtschaft bedeutet Risikominderung die Implementierung von Sicherheitsmaßnahmen und Maßnahmen gegen potenzielle Bedrohungen. Die Maßnahmen können nach ihrer Art wie folgt eingeteilt werden:

* Abschreckende Maßnahmen – zur Abschwächung einer Bedrohung,
* Vorbeugende Maßnahmen – zur Entschärfung einer Schwachstelle,
* Erkennende Maßnahmen – zur Aufdeckung eingetretener Vorfälle,
* Korrektive Maßnahmen – zur Verringerung der Auswirkungen eines Vorfalls.

Die folgende Abbildung zeigt die Beziehung zwischen den Sicherheitsmaßnahmen und dem Risikobewertungsprozess.

Zusammenhang zwischen Auswahl der Maßnahmen und Risikobewertung



Quelle: Verma et al. (2016, S. 156). CC BY-SA 4.0.

Nach der Risikobewertung wird die Risikominderung in der Regel in drei Schritten durchgeführt: Identifizierung, Auswahl und Implementierung der Kontrollen und Maßnahmen (Verma et al., 2016, S. 156).

Nachdem das Risiko bewertet wurde, muss sich eine Organisation für eine der vier unten aufgeführten Optionen entscheiden:

1. Akzeptieren des Risikos. Unternehmen können sich dafür entscheiden, das Risiko zu akzeptieren, wenn es als sehr gering eingeschätzt wird oder die Folgekosten der Risikoakzeptanz geringer sind als die Kosten für die Begrenzung oder Übertragung des Risikos.
2. Übertragen des Risikos. Dies meint die Inanspruchnahme von Versicherungen über Drittanbieter. Gegen Bezahlung entschädigen diese Drittanbieter den Eigentümer des Vermögensguts für den möglichen Schaden, falls dieser eintritt.
3. Begrenzen des Risikos. Dies bezieht sich auf den Einsatz geeigneter Sicherheitsmaßnahmen wie z. B. die Installation von Antivirenlösungen, Systemen zu Eindringlingserkennung und ‑vorbeugung, Firewalls sowie Sensibilisierung und Schulung der Nutzenden.
4. Vermeiden des Risikos. Dies kommt in der Regel zum Tragen, wenn keine Sicherheitsmaßnahmen eingerichtet werden können. Es kann an hohen Kosten liegen oder daran, dass die Bedrohungen der Vermögensgüter natürlich oder unkontrollierbar sind. Beispiele hierfür sind der Bau eines Gebäudes nahe einer Erdbebenzone, oder wenn eine Organisation eine bestimmte Lösung nicht installieren will, weil sie in anderen Organisationen ständig manipuliert wird.

#### Auswahl und Umsetzung von Optionen zur Risikominderung

Nachdem ein Unternehmen verschiedene Optionen zur Risikominderung festgelegt hat, muss eine davon ausgewählt und in die Tat umgesetzt werden. Jedem Vermögensgut wurde ein bestimmtes Risiko zugeordnet, und eine Option zur Risikominderung wurde gewählt. Die Umsetzung der gewählten Option bedeutet, dass bestimmte Verfahren befolgt und neue Kontrollmaßnahmen eingeführt werden müssen. Üblicherweise setzen Unternehmen zum Schutz ihrer Informationssysteme und Vermögensgüter Kontrollmaßnahmen zur Risikobegrenzung ein (Verma et al., 2016, S. 157).

### Methoden der Risikobewertung und des Risikomanagements

Es gibt verschiedene Methoden des Risikomanagements und der Risikobewertung. Die Geschäftsleitung eines Unternehmens entscheidet und wählt einen Rahmen für das Risikomanagement und die Bewertungsmethoden. Bei der Auswahl der Risikobewertungsmethode können Unternehmen den Umfang eines Projekts, die Kosten und die Angemessenheit der erforderlichen Ressourcen berücksichtigen. Jede Organisation wählt eine Risikobewertungsmethode entsprechend ihren Anforderungen aus und schneidet die Methode auf ihre Bedürfnisse zu (Verma et al., 2016, S. 158). In diesem Unterlernzyklus sehen wir uns einige übliche Methoden zur Risikobewertung an:

* ISO/IEC 27005
* NIST SP 800-30 und SP 800-39
* OCTAVE
* COBIT

#### ISO/IEC 27005

ISO 27005 ist die internationale Norm, die Richtlinien und Anweisungen für das Risikomanagement enthält. Diese Norm ist Teil der Familie der ISO-27000-Normen. ISO 27005 wird von Organisationen als eine der Hauptanforderungen für die Umsetzung von ISO 27001 verwendet, einer Norm für die Implementierung eines Informationssicherheitsmanagementsystems (ISMS; Verma et al., 2016, S. 158).

**Geltungsbereich**

Die zu schützenden IT-Vermögensgüter.

Die Hauptanforderung bei der Risikobewertung gemäß ISO 27005 ist die Berücksichtigung von Schwachstellen, Bedrohungen und Auswirkungen. Diese Faktoren müssen für das Unternehmen kontextualisiert und bei der Risikobewertung berücksichtigt werden, was den Entscheidungsträgern bei der Bewältigung der Risiken hilft. Die Grundsätze des ISO-27005-Rahmenwerks können auf verschiedene Größen und Arten von Organisationen angewendet werden. Da die in diesem Rahmenwerk bereitgestellten Anleitungen allgemein und breit gefächert sind, werden qualifizierte Ressourcen für die maßgeschneiderte Umsetzung entsprechend den Geschäftsanforderungen benötigt (Verma et al., 2016, S. 158).

#### NIST SP 800-30 und SP 800-39

Die Normen *SP 800-30 Guide for Conducting Risk Assessments* und *NIST SP 800-39 Managing Information Security Risk* des amerikanischen National Institute of Standards and Technology (NIST) sind die von der US-Regierung bevorzugten Methoden zur Durchführung von Risikobewertungen. Diese Normen bieten einen detaillierten und schrittweisen Prozess, der von den ersten Phasen der Planung einer Bewertung über die Verwaltung und Durchführung bis hin zur Übermittlung der Ergebnisse und einer Neubewertung zur Beibehaltung der ursprünglichen Bewertungen reicht. Diese Normen sind kostenlos auf der offiziellen NIST-Website erhältlich. Öffentliche und private Organisationen jeder Größe können diese Normen nutzen. Außerdem sind sie so konzipiert, dass sie zusammen mit verschiedenen anderen ISO-Rahmennormen gesehen werden können (Verma et al., 2016, S. 158–159).

Die in SP 800-30 beschriebenen Schritte zur Durchführung der Risikobewertung sind folgende:

1. Festlegen des **Geltungsbereichs** (Umfangs).

**Auswirkungen**

Der Verlust von Vertraulichkeit, Integrität und Verfügbarkeit sowie Einbußen wie Rufschädigung und Einkommensverluste.

1. Bestimmung der **Auswirkungen**, der Wahrscheinlichkeit und des Risikos anhand der identifizierten Schwachstellen und Bedrohungen.
2. Kommunikation der Ergebnisse an die Beteiligten.
3. Überwachen der Wirksamkeit der Sicherheitsmaßnahmen.

#### OCTAVE

Die Bewertungsmethode *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)* wurde von der Carnegie Mellon University in den USA entwickelt. Sie bietet eine strukturierte Methode zur Bewertung des Risikos und umfasst die bewährten Vorgehensweisen im Bereich der Sicherheit, das **Betriebsrisiko** und die zur Verringerung des identifizierten Risikos eingesetzte Technologie. Dieser Ansatz unterscheidet sich von den anderen insofern, als er eher strategisch als taktisch ausgerichtet ist. Unternehmen können diese Methode auch ohne Sicherheitsfachleute erlernen und anwenden. OCTAVE ist so konzipiert, dass es als Workshop mit Teilnehmer:innen aus den IT- und Betriebsabteilungen des Unternehmens und ohne umfassende Fachkenntnisse durchgeführt werden kann. Die OCTAVE-Ressourcen zur Durchführung von Risikobewertungen können kostenlos heruntergeladen werden (Verma et al., 2016, S. 159).

**Betriebsrisiko**

Das Risiko von Verlusten aufgrund von Betriebsstörungen, z. B. durch menschliche oder technische Fehler.

Die einzelnen Schritte von OCTAVE sind die folgenden:

1. Festlegen der Kriterien zur Messung des Risikos entsprechend den Unternehmenszielen.
2. Identifizieren der Vermögensgüter.
3. Berücksichtigung der Bedrohungen und ihrer möglichen Auswirkungen entsprechend der aktuellen Bedrohungslage.
4. Identifizieren der Risiken.
5. Priorisieren der Risiken auf der Grundlage der für die Risikomessung festgelegten Kriterien.

#### COBIT

Die Methode Control Objectives for Information and Related Technologies (COBIT) wurde von ISACA entwickelt. ISACA ist ein internationaler Berufsverband, der sich auf **IT-Governance** spezialisiert hat. COBIT ist ein bindender und gründlicher Rahmen, der eine Risikobewertung beinhaltet. ISACA-Mitglieder haben direkten Zugang zu diesem Standard, während Nicht-Mitglieder ihn erwerben können. Die Umsetzung dieses Standards erfordert meist eine erhebliche Investition an Fachpersonal und Zeit. COBIT eignet sich am besten für Organisationen, in denen die Einhaltung von Vorschriften (Compliance) von größter Bedeutung ist. COBIT orientiert sich nach einigen bekannten Risikomanagementstandards wie ISO 27005 (Verma et al., 2016, S. 159, 160). Zur Implementierung von COBIT müssen Organisationen die folgenden Aspekte berücksichtigen:

**IT-Governance**

(Auf Deutsch etwa: IT-Unternehmensführung) Dieses Konzept definiert diejenigen Prozesse in einer Organisation, welche die effiziente und effektive Nutzung der IT gewährleisten.

* Identifizierung von Bedrohungen und Schwachstellen,
* Identifizierung der potenziellen Auswirkungen,
* Notwendigkeit von Fachpersonal.

|  |  |  |  |
| --- | --- | --- | --- |
| Zusammenfassung der Unterschiede zwischen den Risikomanagement-Methoden | | |  |
| **ISO 27005** | **NIST SP 800-30** | **OCTAVE** | **COBIT** |
| Teil der ISO-27000-Familie | Teil der NIST-Sonderveröffentlichungen | Carnegie Mellon Universität (USA) | Entwickelt von ISACA |
| Nutzung durch Organisationen, die dies als eine der Hauptanforderungen für die Implementierung von ISO 27001 betrachten | Bevorzugt von der US-Regierung für die Durchführung von Risikobewertungen | Nutzbar durch jede Organisation und ohne Sicherheitsfachleute | Am besten geeignet für Unternehmen, bei denen die Einhaltung von Vorschriften von größter Bedeutung ist und die in qualifizierte Mitarbeitende investieren müssen |
| Nicht kostenlos verfügbar | Kostenlos verfügbar | Kostenlos verfügbar | Kostenlos verfügbar für ISACA-Mitglieder |

Quelle: Zohaib Hassan (2023)

### Fragen zur Selbstkontrolle

1. Nennen Sie zwei bekannte internationale Rahmenwerke, die von Organisationen für das Risikomanagement verwendet werden.

*ISO 27005, NIST SP 800-30, NIST SP 800-39, OCTAVE, COBIT*

## 6.2 Reaktion auf Vorfälle und Krisenmanagement

Eine Bedrohung der Cybersicherheit kann verschiedene Formen annehmen, sich negativ auf den Ruf der Marke und den Geschäftsbetrieb auswirken und sogar zu rechtlichen Schritten führen. Unternehmen müssen darauf vorbereitet sein, die Auswirkungen erfolgreicher Angriffe zu bewältigen und zu verringern sowie die Wiederherstellung des Betriebs zu beschleunigen (Gorecki & Sullivan, 2020).

### Widerstandsfähigkeit (Resilienz)

Im Geschäftsalltag sind kleinere Zwischenfälle unvermeidlich, wie z. B. ein vorübergehendes Problem mit der Internetverbindung. Unternehmen müssen schnell handeln, um einen Umstand zu bewerten und darauf zu reagieren. „Krise“ und „Vorfall“ werden häufig synonym verwendet, was aber nicht zutrifft.

### Vorfall

Ein Vorfall ist ein Cyber-Ereignis und bezieht sich auf eine Situation, die zunächst ein geringes Ausmaß hat, jedoch zu einer Krise führen kann, die weitaus größere Verluste nach sich zieht, wie z. B. die Unterbrechung des Geschäftsbetriebs. Vorfälle wie der Absturz eines Computers oder Laptops, eine schlechte WIFI-Verbindung, der Absturz einer Website oder ein Druckerproblem stören den täglichen Geschäftsbetrieb. Vorfälle sind in der Regel von geringem Ausmaß und durch schnelles Handeln zu bewältigen (Shahane, 2021).

### Krise

Eine Krise ist viel ernster. Eine Krise kann entscheidende Aktivitäten eines Unternehmens stören und zu größerer Verunsicherung führen. Vorfälle, die nicht oder nicht richtig gelöst werden, können sich zu Krisen ausweiten, die ein strategisches Eingreifen erfordern. Eine Kette von nacheinander auftretenden Vorfällen oder ein Vorfall, der einen anderen auslöst, kann zu einer Krise führen.

Beispiele für solche Krisen sind schwerwiegende Datenschutzverletzungen und Cyberangriffe, **Finanzstraftaten**, Diebstahl kritischer Geschäftsgüter oder andere Ereignisse, welche die Stabilität eines Unternehmens gefährden könnten (Shahane, 2021).

**Finanzstraftaten**

Aktivitäten wie z. B. unbefugter Zugriff auf Finanzkonten oder Diebstahl von Kreditkarteninformationen zur Durchführung unrechtmäßiger Transaktionen.

Die folgenden Fragen können bei der Unterscheidung zwischen einem Vorfall und einer Krise helfen:

* Entsteht durch die Situation ein erheblicher Druck?
* Stellt das Ereignis eine erhebliche Bedrohung für eine Organisation dar?
* Hat die Situation ein Überraschungs- oder Schockelement?

Wenn die Antworten auf die Fragen „ja“ lauten, ist die Situation eine Krise (Shahane, 2021).

Situationen wie die oben beschriebenen können die Unternehmen hart treffen, wenn sie nicht vorbereitet sind. Unternehmen müssen die Unterschiede zwischen einem Vorfall und einer Krise verstehen. Viele Organisationen gehen fälschlicherweise davon aus, dass sie auf einen Vorfall oder eine Krise gut vorbereitet sind (Shahane, 2021). Um beide Situationen gut zu lösen und zu bewältigen, ist es daher unerlässlich, zunächst ihre Natur zu erkennen. Dies führt uns zur Diskussion über das Krisenmanagement und das Vorfallmanagement.

### Vorfallmanagement

**Ereignisse**

Alles was in einer IT-Umgebung eintritt, ist ein Ereignis. Alle Vorfälle sind Ereignisse, aber nicht alle Ereignisse sind Vorfälle. Ein Vorfall ist ein Ereignis, das sich negativ auf die Daten des Unternehmens auswirkt, indem es ihre Vertraulichkeit, Integrität und Verfügbarkeit gefährdet.

Vorfallmanagement ist ein Ansatz für den Umgang mit Ereignissen, die den alltäglichen, normalen Betrieb einer Organisation oder eines Unternehmens stören. Es umfasst die Identifizierung des Ereignisses, das die normalen Aktivitäten eines Unternehmens gestört hat, seine Bewertung und die anschließende Reaktion darauf. Das Vorfallmanagement ermöglicht es Unternehmen, nach einer Störung zum normalen Betrieb zurückzukehren.

Das Vorfallmanagement kann durch die Ausarbeitung eines geeigneten Plans zur Bewältigung aller potenziellen Vorfälle erreicht werden, die den normalen Betrieb stören und Verluste oder Schäden verursachen könnten. **Ereignisse**, die zu einem Vorfall führen, können in jeder kleinen bis großen Organisation auftreten und den normalen Arbeitsablauf beeinträchtigen (Shahane, 2021). Daher ist die Planung des Vorfallmanagements von Vorteil und ermöglicht einer Organisation die folgenden Punkte:

* Unternehmen von entscheidenden Schritten für eine rasche Erholung,
* Sofortige Information der von einem Vorfall betroffenen Personen,
* Erkennen der potenziellen Risiken, um ihnen mit gezielter Planung zu begegnen,
* Erhalt eines Überblicks über alle potenziellen Vorfälle,
* Verbesserte Produktivität und Effizienz der täglichen Arbeit.

### Krisenmanagement

Wie wir bereits besprochen haben, ist eine Krise eine Situation, die ein größeres Ausmaß als ein Vorfall hat und den guten Ruf des Unternehmens stark beeinträchtigen kann. Zur Bewältigung einer Krise muss es in einer Organisation ein spezielles Krisenmanagement-Team geben, dessen Aufgabe es ist, die notwendigen Schritte zur Eingrenzung der Auswirkungen zu unternehmen. Unternehmen, die das Krisenmanagement nicht ernst nehmen, könnten schwerwiegende Auswirkungen auf verschiedene Aspekte des Betriebs verspüren, wie z. B. die Moral der Mitarbeitenden, den Umsatz, den Ruf des Unternehmens, das Ansehen der Führungskräfte und die Produktivität (Shahane, 2021). Ein geeigneter Plan für das Krisenmanagement kann dem Unternehmen folgende Vorteile verschaffen:

* Verringerung der Ausfallzeiten des normalen Geschäftsbetriebs,
* Verringerung der negativen Auswirkungen,
* Unterstützung von Organisationen bei der Vermeidung von Rufschädigung und finanziellen Verlusten,
* Vermeidung rechtlicher Konsequenzen.

Zum besseren Verständnis der Unterschiede zwischen Vorfall- und Krisenmanagement sind einige wichtige Punkte in der folgenden Tabelle zusammengefasst.

|  |  |
| --- | --- |
| Vorfallmanagement und Krisenmanagement | |
| **Vorfallmanagement** | **Krisenmanagement** |
| Kleine und schnelle Aktionen | Größere Schritte zur Bewältigung der Lage notwendig |
| Beteiligung der obersten Führungsebene des Unternehmens möglicherweise nicht erforderlich | Beteiligung der oberen Führungsebene wahrscheinlich erforderlich |
| Kann meist innerhalb von Tagen, Stunden oder Minuten erledigt werden | Kann Tage, Wochen oder Monate dauern |
| Kann nur wenige Personen oder Teams betreffen | Kann die gesamte Organisation betreffen |

Quelle: Renuka Shahane (2021).

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Eine *Bedrohung* kann für eine Organisation in verschiedenenFormen auftreten.

## 6.3 Unvorhersehbare Ereignisse (Schwarzer Schwan)

Ein schwarzer Schwan (Black Swan) ist ein unvorhersehbares und seltenes Ereignis, das schwerwiegende Auswirkungen hat, und es ist fast unmöglich, solche Ereignisse vorherzusehen. Schwarze Schwäne können zu großen Verlusten und Schäden für die Märkte und die Wirtschaft führen. Ereignisse wie die Finanzkrise 2008, der 11. September 2001 und die COVID-19-Pandemie können als schwarze Schwäne eingestuft werden.

### Vorbereitung auf Cyber-Ereignisse des Typs Schwarzer Schwan

Große Unternehmen implementieren Managementsysteme für die Informationssicherheit, um Cyberangriffe abzuwehren. Aber da Cyberangriffe auf Versorgungsunternehmen, Behörden, Krankenhäuser und Unternehmen immer stärker werden, wird es offensichtlich, dass Organisationen jetzt zwei **Drehbücher** haben müssen, eines für die Abwehr bekannter Cyber-Bedrohungen wie Denial-of-Service-Angriffe, Phishing und Schadsoftware, und ein anderes, das durch Resilienz (Widerstandsfähigkeit) noch viel schlimmeren Bedrohungen entgegenwirkt. Unternehmen müssen sowohl auf Cyber-Krisen vorbereitet sein, die ihren eigenen Geschäftsbetrieb lahmlegen und stören, als auch auf solche, die eine gesamte Branche betreffen (Herbolzheimer, 2016).

**Drehbuch**

(Engl. *Playbook*) Als Schlüsselkomponente für den IT-Betrieb und das Vorfallmanagement sollte ein Drehbuch Übungen und Schulungen enthalten, um die Notfallteams auf den nächsten potenziellen Vorfall vorzubereiten.

Daher müssen Unternehmen die Zeit dafür investieren, die Arten potenzieller Cyber-Katastrophen zu analysieren. Wie andere Katastrophen auch, kann ein Cyberangriff plötzlich auftreten. Sie können aber auch langsam und schleichend entstehen, wie eine Seuche oder Pandemie, die sich mit der Zeit immer weiter ausbreitet, bevor sie zu einer globalen Krise wird. Daher müssen Unternehmen wirksame Pläne und Strategien in Betracht ziehen und durchsetzen, z. B. den Aufbau von Redundanzen, um sowohl bekannten Cyber-Bedrohungen als auch Black-Swan-Cyber-Ereignissen zu begegnen (Herbolzheimer, 2016).

Unternehmen müssen auch prüfen, ob sie Cyberangriffe des Typs schwarzer Schwan eindämmen und überleben können, oder ob diese sich wie eine Infektion innerhalb der Branche und vielleicht darüber hinaus verbreiten könnten. Viele Unternehmen haben bereits extreme Eindämmungs- und Notfallpläne ausgearbeitet, wie z. B. die Vorbereitung auf einen Offline-Betrieb im Falle eines schwarzen Schwans. So haben beispielsweise Krankenhäuser und Gesundheitsdienstleister, die von Ransomware-Angriffen in Deutschland und den Vereinigten Staaten betroffen waren, ihre kritischen Infrastruktursysteme teilweise offline genommen und sich darauf vorbereitet, ihren Betrieb wieder manuell mit Papier und Stift aufzunehmen, falls ein Vorfall ihren täglichen digitalen Betrieb beeinträchtigt (Herbolzheimer, 2016).

Auch die Einrichtung branchenweiter SWAT-Teams (Special Weapons and Tactics) kann in Erwägung gezogen werden, um Cyber-Bedrohungen regelmäßig zu überwachen und zu bekämpfen. Diese Teams können dann festlegen, ab wann ein Ereignis als Cyber-Krise eingestuft wird, welche Art von Daten und Diensten sie sich zu verlieren leisten könnten, und welcher Daten- und Dienstverlust sie in eine vollständige Katastrophe führen würde (Herbolzheimer, 2016).

Zusammenfassend lässt sich sagen, dass schwarze Schwäne durch ihre schwerwiegenden Auswirkungen, ihre Folgen und durch extreme Seltenheit definiert sind. Schwarze Schwäne sind höchst ungewöhnlich und haben meist schwerwiegende Auswirkungen. Sie wirken sich negativ auf die Märkte aus, indem sie verheerende Umsatzverluste verursachen. Selbst durch die Nutzung von starken Bedrohungsmodellen und Risikomanagementmethoden können schwarze Schwäne nicht durch Prognosewerkzeuge vorhergesagt werden (Investopedia, 2022).

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Schwarzer-Schwan-Ereignisse haben *schwere* Auswirkungen auf Unternehmen.

## 6.4 Kontinuierliche Neubewertung

Der Plan zur Risikobewertung muss von den Organisationen regelmäßig und kontinuierlich neu bewertet und geprüft werden. Der Neubewertungsvorgang wird in Unternehmen durchgeführt, um sicherzustellen, dass die eingerichteten Kontrollmaßnahmen für einen bestimmten Vermögenswert noch praktikabel und funktionsfähig sind und gemäß den Sicherheitsrichtlinien des Unternehmens umgesetzt werden.

### Restrisiko

Restrisiko bezeichnet eine Bedrohung, die auch dann noch besteht, wenn alle Versuche und Bemühungen zur Beseitigung des Risikos unternommen worden sind. Wie wir bereits erörtert haben, gibt es vier Möglichkeiten, mit Risiken umzugehen: Vermeidung, Begrenzung, Übertragung oder Akzeptanz. Da das Restrisiko unbekannt ist, ziehen es die meisten Unternehmen vor, das Restrisiko entweder zu übertragen oder zu akzeptieren (Verma et al., 2016, S. 157–158)

Zusammenfassung

In dieser Lektion haben wir den Gesamtprozess des Risikomanagements und die Art und Weise, wie er üblicherweise in Unternehmen umgesetzt wird, eingehend erläutert. Die Prozesse Risikobewertung, Risikominderung und kontinuierliche Neubewertung wurden im Rahmen der Diskussion über das Risikomanagement erläutert. Die Teilprozesse der Risikobewertung, der Risikominderung und der Neubewertung wurden im Detail analysiert. Danach haben wir die Gegenstrategien untersucht, die Unternehmen in Betracht ziehen müssen, falls es trotz eines robusten Risikomanagementprozesses zu einem Cyberangriff kommt (z. B. das Vorfall- und Krisenmanagement). Schließlich haben wir das Phänomen und das Konzept der Schwarzen Schwäne und ihre Auswirkungen betrachtet.

# Lektion 7 – Bedrohungsabwehr

**Lernziele**

Nach Abschluss dieser Lektion werden Sie in der Lage sein,

… die verschiedenen Strategien und Methoden zu verstehen, die zur Stärkung der Cyberabwehr und Risikominderung in einem Unternehmen eingesetzt werden.

… zu erkennen, wie die Sicherheitsmaßnahmen bei der Cyberabwehr bewertet und validiert werden.

… das Konzept der eingebauten Sicherheit und des eingebauten Datenschutzes zu identifizieren.

… Strategien zur Bedrohungsabwehr in einer Organisation anzuwenden.

# 7. Bedrohungsabwehr

## Einführung

**Digitaler Wandel**

Die Integration digitaler Technologien in allen Unternehmensbereichen.

Die ständige Weiterentwicklung der Technologie ermöglicht es Unternehmen, ihre angestrebten Ziele und Zielgruppen zu erreichen, Daten zu sammeln, Daten zu analysieren und vieles mehr. Doch mit dem rasanten **digitalen Wandel**, den Unternehmen und Organisationen vollziehen, wächst auch die Gefahr, von Cyberkriminellen angegriffen zu werden. Laut dem Internet Crime Report 2021 des amerikanischen Federal Bureau of Investigation (FBI) übersteigen die potenziellen Verluste durch Cyberkriminalität im Jahr 2021 6,9 Milliarden $ (Acrisure, 2022). Ein erfolgreiches Unternehmen muss daher eine Strategie entwickeln und umsetzen, die diesen Bedrohungen entgegenwirkt und die Intensität einer möglichen Datenverletzung durch einen Cyberangriff verringert. Diese Strategie wird als Bedrohungsabwehr oder Bedrohungseindämmung (engl.: *Threat Mitigation*) bezeichnet.

In dieser Lektion werden die unterschiedlichen Konzepte der Bedrohungsabwehr im Detail erläutert. Unternehmen müssen verschiedene Methoden und Strategien anwenden, um ihre Cyberabwehrlandschaft zu verbessern. Die Stärkung der Cyberabwehr hängt mit der Risikominderung zusammen, und Taktiken und Methoden helfen Unternehmen bei der Risikominderung.

Darüber hinaus ist es unerlässlich, die Wirksamkeit der implementierten Sicherheitsmaßnahmen zu validieren, indem sie nach einer angemessenen Zeitspanne überprüft werden. Wir werden ausführlich erläutern, wie die Kontrollmaßnahmen validiert und geprüft werden können, um sicherzustellen, dass sie aktuell und regelkonform sind. Darüber hinaus ist es notwendig, die Sicherheit bereits bei der Entwicklung der Software anderen Lösungen zu berücksichtigen. Dies bringt uns zum Konzept des Einbaus von Sicherheit und Datenschutz schon bei der Entwicklung. Dies ist einer der wichtigsten Aspekte bei der Bedrohungsabwehr. Schließlich werden wir uns mit den bewährten Vorgehensweisen und Methoden zur Bedrohungsabwehr befassen.

## 7.1 Taktiken und Methoden zur Cyberabwehr

Cyberabwehr (auch: Cyberverteidigung) ist ein Begriff aus dem Bereich der Cybersicherheit. Er meint die Fähigkeit, Cyberangriffe an ihrem Ziel zu hindern, ein Netzwerk, ein System oder eine Anwendung zu manipulieren oder in sie einzudringen. Dazu gehören auch proaktive Schritte, um böswillige Aktionen von Cyberkriminellen vorherzusehen und sie zu bekämpfen. Alle Taktiken, Methoden oder Strategien, die eine Organisation zur Stärkung ihrer Cyberabwehr einsetzt, haben das Ziel, Cyberangriffe zu verhindern, zu stören und auf sie zu reagieren (CyberTalk, o. D.).

Cyber-Bedrohungen zielen weiterhin auf Unternehmen ab und führen zu Rufschädigung, kostspieligen Reparaturen und aufgedeckten Informationen. Durch den Einsatz einer Vielzahl von Taktiken und Methoden können Cyberkriminelle verschiedene Teile der Netzwerkinfrastruktur eines Unternehmens angreifen. Kurz gesagt, unsere Abhängigkeit von Technologie oder digitalen Lösungen macht uns anfällig für Cyberangriffe (CyberDefenses, 2019). Daher muss ein Unternehmen, das für seinen täglichen Betrieb auf Technologie angewiesen ist, eine starke Cyberabwehrlandschaft einrichten. Im Folgenden finden Sie einige der gängigsten Taktiken und Methoden zur Stärkung der Cyberabwehr.

### Starke Passwörter

Die Verwendung von sicheren Passwörtern ist bei jeder Art von Konto von großem Vorteil. Es liegt in der menschlichen Natur, dass wir bei der Erstellung eines neuen Passworts oder bei der Aktualisierung eines älteren Passworts dieses lieber einfach halten, damit wir es uns leicht merken können, oder dass wir ein Passwort auch für andere Konten nutzen. Laut dem Untersuchungsbericht von Verizon über die Datenschutzverletzungen 2019 waren 80 Prozent der Datenschutzverletzungen und gehackten Konten das Ergebnis von schwachen Passwörtern (ADKtechs, 2020).

Ein gutes und sicheres Passwort ist lang, zufällig und wird häufig geändert. Die Komplexität eines Passworts bringt oft den Drang mit sich, es aufzuschreiben. Dies kann jedoch zu weiteren Angriffen führen und verringert den Nutzen komplexer Passwörter. Daher ist ein Passwortmanager eine gute Lösung. Man kann ihn nutzen, um alle Passwörter in der virtuellen Brieftasche in verschlüsselter Form, und mit einem Master-Passwort geschützt, zu speichern. Ein langer Satz, der als Passwort verwendet wird, wird Passphrase genannt und ist ebenfalls eine gute Alternative. Eine Passphrase ist eine Art Passwort aus einem langen Satz, der mit eigenen Erinnerungen zu tun hat und für Angreifende fast unmöglich zu knacken ist.

### Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) ist eine der robustesten und einfachsten Methoden zur Stärkung der Cyberabwehr eines Unternehmens. Die Multi-Faktor-Authentifizierung, auch bekannt als Zwei-Faktor-Authentifizierung (2FA), verstärkt den normalen Passwortmechanismus um ein zusätzliches Schutzschild. MFA ist eine Kombination aus mindestens zwei der folgenden Elemente:

* Ein Standard-Passwort, das auch als „etwas, das wir wissen“ bezeichnet wird,
* ein einmaliger Code oder Token (Marke), der nach dem Zufallsprinzip über die Software eines Drittanbieters auf dem persönlichen Mobiltelefon generiert wird, was auch bekannt ist als „etwas, das wir haben“,
* biometrische Daten, Unterschrift oder Stimme, auch „etwas, das wir sind“ genannt. Diese Methode verstärkt die Cyberabwehr so, dass Angreifende im Falle der Aufdeckung eines Faktors nicht in der Lage ist, ein solches physisches Merkmale des Opfers zu erbringen.

### Firewalls

Eine Firewall (Brandmauer) ist ein physisches Hardware-Gerät oder eine Software, die zwischen einem internen und einem externen Netzwerk eingesetzt wird. Eine Firewall fungiert als Hindernis für den Datenverkehr, der aus externen Netzwerken (d. h. dem Internet) in das interne Netzwerk eines Unternehmens gelangt, oder umgekehrt für den Datenverkehr vom internen in das externe Netzwerk. Dies geschieht durch eine Filterung auf der Grundlage von Regeln, die in der Firewall konfiguriert werden. Firewalls sind wichtige Schutzschilde für mittelständische und große Unternehmen ebenso wie für Heimnetzwerke.

### Gepatchte oder aktualisierte Software

Hier sei darauf hingewiesen, dass das kontinuierliche Patchen oder Aktualisieren von Software zu den wichtigsten bewährten Vorgehensweisen der Cyberabwehr gehört. Jede Softwarelösung, die ein Unternehmen einsetzt, sollte ständig auf die neueste Version aktualisiert werden. Ungepatchte Software ist anfälliger und könnte zu massiven Datenverletzungen führen, wenn sie gehackt wird, und es Angreifenden ermöglichen, sich im kritischen Netzwerk des Unternehmens zu bewegen. Das routinemäßige Patchen von Software kann also einen der wichtigsten Einbruchswege eliminieren, über die Cyberkriminelle ein gesamtes Unternehmensnetzwerk gefährden können.

### Verschlüsselung

Verschlüsselung ist eine Methode, mit der lesbare Daten (Klartextdaten) in eine Form umgewandelt werden, die für Unbefugte nicht verständlich ist. Der Einsatz von Verschlüsselung ist für alle Unternehmen, die das Internet für ihre tägliche Kommunikation nutzen, zwingend erforderlich. Zum Beispiel finden Banktransaktionen über das Internet statt, das ein nicht vertrauenswürdiges Netzwerk ist. Daher müssen die Banken die entsprechenden Sicherheitsmaßnahmen durchsetzen, um sichere Kreditkartenzahlungen und ‑transaktionen zu gewährleisten. Die Verwendung von Verschlüsselung im Heimnetzwerk ist ebenfalls empfehlenswert und sorgt dafür, dass unsere gespeicherten Daten sicherer sind, wenn wir unser Speichermedium verlieren oder ausgeraubt werden. Die Verschlüsselungsmethode sollte jedoch auf dem neuesten Stand sein, damit sie nicht mit Hilfe von Hacking-Werkzeugen geknackt werden kann. Mehrere Organisationen veröffentlichen regelmäßig Listen mit starken kryptographischen Algorithmen, z. B. BSI TR-02102 (Bundesamt für Sicherheit in der Informationstechnik, o. D.).

### Antivirus

Eine der grundlegenden, aber unerlässlichen Sicherheitsmaßnahmen in jedem Unternehmen ist die Verwendung von aktuellen Antivirenlösungen. Eine solche Software hilft beim Scannen, Erkennen, Verhindern und Löschen von Viren auf einem Computer. Jedes Unternehmen genauso wie alle privaten Nutzenden müssen die aktuellsten Antivirenlösungen einsetzen, um die neuesten Bedrohungen zu erkennen und zu verhindern. Es ist ratsam, solche Programme nicht von unbekannten Websites herunterzuladen, sondern sie von einer bekannten Quelle zu kaufen und sie regelmäßig zu aktualisieren.

### VPN

Ein virtuelles privates Netzwerk (VPN) ist eine technische Methode, mit der sicher über ein öffentliches Netzwerk wie dem Internet kommuniziert werden kann. Zum Beispiel müssen Mitarbeitende, die von zu Hause aus arbeiten, manchmal sicher über das Internet mit ihrem Unternehmen kommunizieren. Dafür ist ein VPN die beste Wahl, weil es einen sicheren verschlüsselten Tunnel über das Internet schafft, durch den beide Parteien ihre Daten senden können.

### Datensicherungen (Backups)

Die Erstellung von Backups bedeutet, dass regelmäßig eine Kopie aller wichtigen digitalen Geschäftsdokumente erzeugt und gespeichert wird. Für den eigenen Schutz müssen Unternehmen kontinuierliche Backups ihrer digitalen Vermögensgüter wie Tabellenkalkulationen, Personaldateien, Datenbanken und Finanzdateien erstellen, damit bei einem Vorfall alle Daten aus dem sekundären Speicher wiederhergestellt werden können. Kritische Daten sollten mindestens auf zwei unabhängigen Geräten oder Medien gespeichert werden, die sich physisch an verschiedenen Orten befinden, wodurch eine starke Redundanz entsteht.

### Schulungen zur Sicherheit und Sensibilisierung der Mitarbeitenden

Keine Sicherheitslösung kann ein Unternehmen jemals vor Cyberangriffen schützen, wenn es nicht über geschulte und gut informierte Mitarbeitende verfügt, welche die aktuellen Herausforderungen und Bedrohungen im Bereich der Cybersicherheit kennen. Cyberkriminelle versuchen immer, Menschen zu täuschen, weil diese das schwächste Glied in der Kette darstellen. Die Durchführung von Schulungen zum Sicherheitsbewusstsein ist einfach und kostengünstig, hat aber eine immense Wirkung. Im Hinblick auf die Stärkung der Cyberabwehr sind sicherheitsbewusste Mitarbeitende der erste Verteidigungspfeiler gegen Cyberbedrohungen in jeder Organisation. Eine solche Schulung sollte eine Erläuterung der Sicherheitsrichtlinien des Unternehmens beinhalten, ebenso wie die Informationen zur Meldung verdächtiger Aktivitäten, die Unterrichtung über gefährliche Links in E-Mails, die nicht angeklickt werden dürfen, und vieles mehr.

### Fragen zur Selbstkontrolle

1. Nennen Sie zwei wichtige Infrastrukturelemente, die von Cyberkriminellen in einem Unternehmen ins Visier genommen werden können.

*Netzwerk, Systeme, Anwendungen*

## 7.2 Strategien zur Risikominderung

Risikominderung ist ein Vorgang, bei dem wichtige Maßnahmen ergriffen werden, um die Wahrscheinlichkeit einer durch einen Angriff ausgenutzten Schwachstelle abzuschwächen. Zur Risikominderung werden in Unternehmen die notwendigen Sicherheitsmaßnahmen umgesetzt. Dies geschieht in der Regel nach einer Risikobewertung im Rahmen des umfassenden Risikomanagements. Zu den gängigen Strategien gehören die folgenden:

* Risikoakzeptanz,
* Risikotransfer,
* Risikobegrenzung,
* Risikovermeidung.

### Risikoakzeptanz

Risikoakzeptanz, Risikoübernahme oder Risikoselbstbehalt bedeutet, dass die identifizierten Risiken akzeptiert werden, ohne dass Sicherheitsmaßnahmen zur Vermeidung von Verlusten durch Risiken ergriffen werden. Eine solche Entscheidung wird von der Unternehmensleitung getroffen, wenn sie der Meinung ist, dass die Kosten für die Implementierung der notwendigen Sicherheitsmaßnahmen höher sind als der tatsächliche Wert des betreffenden Vermögensguts.

### Risikotransfer

Der Risikotransfer ist ein Ansatz, bei dem der potenzielle Verlust aus einem Cyberangriff einer Organisation über eine Versicherung an ein Drittunternehmen weitergegeben wird. Diese Unternehmen erstatten den geschädigten Unternehmen eine Zahlung als Schadensersatz.

### Risikobegrenzung

Risikobegrenzung, auch bekannt als Risikoverringerung, bedeutet die Einrichtung von Sicherheitsmaßnahmen. Bei diesem Ansatz wird versucht, das Risiko durch die Einrichtung von Sicherheitsmaßnahmen wie aktualisierte Firewalls, Passwortrichtlinien, Planung der Notfallreaktion nach Vorfällen, Multi-Faktor-Authentifizierungen und VPN für entfernte Mitarbeitende zu verringern.

### Risikovermeidung

Die Risikovermeidung ist ein Ansatz zur Minimierung des Risikos, indem als riskant angesehene Vorgänge nicht durchgeführt werden. Ein Beispiel ist ein Unternehmen, das im Falle eines Cyberangriffs die Speicherung von Kundendaten auf seinen Servern einschränkt. Ein anderes Beispiel ist ein Produktionsunternehmen, das aufgrund der Risiken bei der Lagerung und Handhabung von schädlichen Chemikalien oder Materialien auf deren Verwendung verzichtet. Die Überwachung und Überprüfung der implementierten Lösungen stellt ebenfalls eine Möglichkeit der Risikovermeidung dar.

### Fragen zur Selbstkontrolle

1. Nennen Sie zwei Strategien, die im Rahmen der Risikominderung durchgeführt werden.

*Risikoakzeptanz, Risikotransfer, Risikobegrenzung, Risikovermeidung*

## 7.3 Validierung der Abwehr

Eine wichtige Voraussetzung für ein erfolgreiches Cyber-Abwehrprogramm in jedem Unternehmen ist die Bewertung und Validierung der Wirksamkeit der eingerichteten Sicherheitsmaßnahmen. Unternehmen sollten dies in regelmäßigen Abständen durchführen, um zu überprüfen, ob die Sicherheitsmaßnahmen wie vorgesehen funktionieren (Bakertilly, 2017). Die gängigsten Methoden, die von Unternehmen zur Überwachung und Bewertung der Wirksamkeit von Sicherheitsmaßnahmen eingesetzt werden, sind Penetrationstests, Red Teaming, Schwachstellenanalysen und Audits.

### Penetrationstests und Bewertungen der Schwachstellen

**Sicherheits-Patches**

Korrekturen, die im Softwarecode vorgenommen und von den Software-Unternehmen veröffentlicht werden, um das Risiko von Schwachstellen zu entschärfen.

Um die Wirksamkeit der Sicherheitsmaßnahmen zu überprüfen und zu bewerten, müssen alle Organisationen Schwachstellenbewertungen und Penetrationstests durchführen. Schwachstellenbewertungen werden durchgeführt, um mangelhafte Sicherheitskonfigurationen eines Unternehmens oder **Sicherheits-Patches** zu identifizieren, die ein Unternehmen möglicherweise übersehen hat. Organisation setzen unterschiedliche Werkzeuge zum Scannen von Schwachstellen ein, um die aktuellen Systemkonfigurationen mit den bekannten veröffentlichten Listen von Schwachstellen zu vergleichen (Bakertilly, 2017).

Wenn wir beim Scannen von Schwachstellen einen Schritt weiter gehen, kommen wir zum nächsten Schritt, den Penetrationstests. Erfahrene und professionelle **ethische Hacker** nutzen die beim Schwachstellen-Scan gefundenen Schwachstellen und simulieren dann reale Angriffe. So können sie herausfinden, ob diese Schwachstellen von echten Cyberkriminellen für einen Einbruch ausgenutzt werden könnten. Die Unternehmen nutzen dann die Ergebnisse von Schwachstellen-Scans und Penetrationstests, um Sicherheitslücken zu ermitteln und den Hauptgrund dafür zu finden, wie diese Schwachstellen in das Unternehmen gelangen konnten (Bakertilly, 2017).

**Ethische Hacker**

Erfahrene Fachleute, die mit Genehmigung reale Angriffe simulieren, um die Schwachstellen im Netzwerk, im System und in den Anwendungen zu finden.

### Audits zur Cybersicherheit

Ein Audit im Bereich der Cybersicherheit ist eine umfassende Prüfung und Bewertung der Informationssysteme eines Unternehmens, um die Einhaltung der Sicherheitsrichtlinien zu beurteilen und Lücken in der Umsetzung der Sicherheitsrichtlinien zu ermitteln. Bei dieser Prüfung werden die Sicherheitsmaßnahmen des Unternehmens und die digitalen Assets sorgfältig überprüft, um sicherzustellen, dass sie den Compliance-Anforderungen entsprechen. Cybersicherheits-Audits werden unterteilt in interne oder externe Audits (Sengupta, 2022).

#### Interne Audits

**Cybersicherheitsprozesse**

Methoden oder Strategien innerhalb einer Organisation zur Anleitung von Cybersicherheitsfachleuten.

Ein spezielles Team einer Organisation führt interne Audits durch, um die **Cybersicherheitsprozesse** zu bewerten. Ein starkes internes Audit hilft einer Organisation und dem Audit-Team, die Schwachstellen in den Sicherheitsmaßnahmen zu erkennen. Dies ermöglicht es den Unternehmen auch, Lücken zu schließen, d. h. herauszufinden, welche Sicherheitsmaßnahmen vorhanden sein sollten, aber nicht eingerichtet wurden.

#### Externe Audits

**Lückenanalyse**

Diese detaillierte Überprüfung hilft Unternehmen dabei, den Unterschied zwischen ihrem derzeitigen Stand der Informationssicherheit und den Anforderungen der Branche zu erkennen.

Bei externen Audits untersuchen externe Cybersicherheitsfachleute die Einhaltung von Vorschriften, Sicherheitsmaßnahmen und Sicherheitslücken im Unternehmensnetzwerk eines Unternehmens. Externe Audit-Fachleute sind hochqualifiziert und darin geschult, sensible Daten, Netzwerkressourcen und Schwachstellen zu identifizieren. Dadurch gewährleisten sie, dass der Auditprozess eine Organisation bei der Erreichung ihrer Ziele unterstützt, insbesondere durch eine gründliche **Lückenanalyse**. Ein starkes Audit bewertet die folgenden fünf Schlüsselaspekte der Sicherheit (Sengupta, 2022).

#### Betriebliche Sicherheit

Die betriebliche Sicherheit umfasst die Cybersicherheitsrichtlinien des Unternehmens, die Sicherheitsmaßnahmen und die bewährten Vorgehensweisen im Bereich der Sicherheit. Zur betrieblichen Sicherheit gehören umfassende Schutzmaßnahmen für die Verwaltung der verschiedenen Infrastrukturressourcen.

#### Netzwerksicherheit

Eine Prüfung der Netzwerksicherheit beinhaltet die Bewertung der Sicherheitslage von Netzwerksystemen und Ressourcen, auf die über das Internet zugegriffen werden kann. Bei einer umfassenden Prüfung der Netzwerksicherheit werden die Verfügbarkeit des Netzwerks und der gesamte Betrieb von Netzwerkgeräten wie Firewalls, Switches und Routern untersucht.

#### Datensicherheit

Die Datensicherheit umfasst Kontrollen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Daten innerhalb des Unternehmens. Zu den Sicherheitsmaßnahmen, die in der Regel für die Datensicherheit implementiert werden, gehören Authentifizierung, Autorisierung, Verschlüsselung und bewährte Vorgehensweisen bei der Sicherheit zum Schutz wichtiger Geschäftsdaten im **Ruhezustand und im Transit**.

**Ruhezustand und Transit**

(Engl.: Rest and Transit) Daten im Ruhezustand sind gespeicherte Daten, z. B. auf einer Festplatte. Daten im Transit, also bei der Übertragung, sind in Bewegung, z. B. bei der Eingabe der Anmeldedaten für das Benutzerkonto auf einer Website.

#### Systemsicherheit

Zur Systemsicherheit gehören Sicherheitsmaßnahmen auf Hardware und Betriebssystemen. Die Prüfung der Systemsicherheit umfasst die Überprüfung der Verwaltung **erhöhter Berechtigungen**, der Gerätezugriffsverwaltung, des Patching-Prozesses usw.

**Erhöhte Berechtigungen**

Die Tatsache, dass normale Nutzende nicht auf die administrativen Kontorechte zugreifen und keine Befehle ausführen können.

#### Physische Sicherheit

Implementierung von vorbeugenden Kontrollmaßnahmen zur Kontrolle des physischen Zugriffs auf Software- und Hardware-Ressourcen sowie Anwendungsdaten. Physische Sicherheitsmaßnahmen schützen die Mitarbeitenden des Unternehmens auch vor potenziellen Bedrohungen, die zur Beeinträchtigung wichtiger Geschäftssysteme führen können. Bei einem Audit der Cybersicherheit werden verschiedene Aspekte der physischen Sicherheit bewertet, z. B. Zugangs- und Zugriffskontrolle, physische Laufwerkssicherungen und Überwachungsverfahren.

### Fragen zur Selbstkontrolle

1. Nennen Sie eine Methode, mit der die Sicherheitsmaßnahmen in einer Organisation validiert werden kann.

*Schwachstellenbewertung, Penetrationstests, interne Audits, externe Audits, Erstellung von Sicherheitsmetriken*

## 7.4 Sicherheit und Datenschutz bei der Entwicklung

In diesem Lernzyklus erörtern wir die Konzepte Sicherheit und Privatsphäre. Obwohl sie eng miteinander zusammenhängen, sind sie sich nicht besonders ähnlich. Die Informationssicherheit gewährleistet den Schutz von Vermögensgütern und Aktivitäten sowohl der Organisationen als auch der Öffentlichkeit, während der Schutz der Privatsphäre (Datenschutz) darauf abzielt, persönlich identifizierbare Informationen zu schützen und zu respektieren. Dazu werden Privatpersonen in die Lage versetzt, die Kontrolle über deren Verwendung, Sammlung und Offenlegung zu behalten (Cavoukian & Dixon, 2013).

### Datenschutz bei der Entwicklung (engl. *Privacy by Design*)

Auch wenn der Datenschutz den Schutz personenbezogener Daten vor unbefugtem Zugriff fordert, und starke Sicherheitsmaßnahmen für die Erreichung eines solchen Schutzniveaus unerlässlich sind, muss man sich darüber im Klaren sein, dass der Datenschutz weit mehr umfasst als nur die Gewährleistung eines sicheren und befugten Zugriffs auf die Daten. Kurz gesagt: Datenschutz bedeutet Kontrolle, d. h., dass der Einzelne die persönliche Kontrolle über die Sammlung, Verwendung und Offenlegung seiner personenbezogenen Daten behält. Dieser Begriff des Datenschutzes lässt sich am besten als „informationelle Selbstbestimmung“ ausdrücken, ein Begriff, der ursprünglich in der Entscheidung des deutschen Verfassungsschutzes über die Sammlung bzw. Erhebung personenbezogener Daten bei der Volkszählung 1983 in Deutschland verwendet wurde (Cavoukian & Dixon, 2013).

Mit der Ausweitung der vernetzten digitalen Systeme wachsen auch die Herausforderungen für die gewünschte Privatsphäre. Die Datenschutzgesetze versuchen, sich an die sich ständig verändernde digitale Landschaft anzupassen, die durch den raschen technologischen Wandel verursacht wird. Doch trotz der zunehmenden Herausforderungen durch Cloud-Computing, soziale Medien und mobile Geräte ist die Wahrung der Privatsphäre nicht nur machbar, sondern auch äußerst wünschenswert für Unternehmen, die das Vertrauen ihrer Kund:innen aufrechterhalten wollen (Cavoukian & Dixon, 2013).

Das Konzept des Datenschutzes bei der Entwicklung („Privacy by Design“) bietet einen ganzheitlichen Ansatz in dieser sich ständig weiterentwickelnden Ära des digitalen Wandels. Es geht um die gesamte und durchgängige Struktur („End-to-End“) einer Organisation oder eines Unternehmens, einschließlich der Netzwerkinfrastruktur, der Geschäftspraktiken und der Informationstechnologie. Ein Unternehmen kann also den vollen Nutzen aus der Technologie ziehen, indem es den Datenschutz in jeder seiner Einheiten umsetzt (Cavoukian & Dixon, 2013).

Datenschutz bei der Entwicklung umfasst die folgenden sieben Grundprinzipien:

1. Proaktiv und nicht reaktiv – präventiv und nicht heilend,
2. Datenschutz als Standardeinstellung,
3. Datenschutz schon im Design integriert,
4. Volle Funktionalität – Doppelsieg-Strategie (*Positive Sum*),
5. End-to-End-Sicherheit – Schutz über den gesamten Lebenszyklus,
6. Transparenz und Sichtbarkeit,
7. Respekt für die Privatsphäre der Nutzenden.

### Sicherheit bei der Entwicklung (engl. *Security by Design*)

Wie bereits erwähnt, bezieht sich die Informationssicherheit auf den Schutz der Vermögensgüter und Aktivitäten von Unternehmen und Menschen. Das NIST definiert „Informationssicherheit“ in seinem Glossar der wichtigsten Begriffe der Informationssicherheit als Schutz von Informationen und Informationssystemen vor unbefugtem Zugriff, unbefugter Nutzung, Offenlegung, Unterbrechung, Änderung oder Zerstörung zum Schutz der folgenden Werte:

* **Vertraulichkeit** – die Einhaltung genehmigter Beschränkungen der Offenlegung und des Zugriffs.
* **Integrität –** der Schutz vor unbefugter Zerstörung oder Veränderung von Informationen.
* **Verfügbarkeit –** die Gewährleistung eines zuverlässigen und rechtzeitigen Zugangs zu Informationen.

Ein gründliches und robustes Informationssicherheitsprogramm bietet nicht nur eine starke Abwehrlandschaft in einem Unternehmen, sondern kann auch dazu beitragen, dass Unternehmen ihre Geschäftsziele erreichen. Wenn beispielsweise die Steigerung des Umsatzes durch die Verbesserung der Kundenzufriedenheit das oberste Ziel eines Unternehmens ist, dann kann das Angebot einer sicheren Umgebung für die Verwaltung und den Empfang von Kundendaten zusammen mit der Gewährung des Zugangs zu diesen Daten das Vertrauen der Kund:innen in das Unternehmen stärken und so zu höheren Umsätzen führen. Das Gleiche gilt auch für den Umgang mit Verkäufern oder Geschäftspartnern (Cavoukian & Dixon, 2013).

Im Bereich der Informationssicherheit ist die Sicherheit bei der Entwicklung („Security by Design“) ein robuster und ganzheitlicher Ansatz, der von Anfang an in die Systeme oder Produkte integriert wird. Hier sei darauf hingewiesen, dass das Konzept der Sicherheit bei der Entwicklung im Gegensatz zur „Sicherheit durch Unklarheit“ („Security through Obscurity“) steht, bei der die Sicherheit aus der Perspektive der Komplexität, Geheimhaltung und Unverständlichkeit betrachtet wird (Cavoukian & Dixon, 2013).

### Einklang von Datenschutz und Sicherheit bei der Entwicklung

In der nachstehenden Tabelle wird erläutert, wie die Grundsätze des „eingebauten Datenschutzes“ mit den Grundsätzen der „eingebauten Sicherheit“ in Einklang gebracht werden können.

|  |  |  |
| --- | --- | --- |
| Datenschutz bei der Entwicklung und Sicherheit bei der Entwicklung | | |
| **Grundprinzipien des eingebauten Datenschutzes** | **Datenschutz** | **Sicherheit** |
| Schutz von und Respekt vor persönlicher Informationen | Schutz von Vermögensgütern und Aktivitäten von Unternehmen und Menschen |
| Proaktiv statt reaktiv | Vorhersagen und Beenden von Datenschutzvorfällen bevor sie auftreten | Implementieren präventiver Kontrollmaßnahmen wie IPS und Firewalls |
| Standardeinstellung | Integrieren von Datenschutz-Kontrollmaßnahmen direkt in Geschäftspraktiken oder IKT-Systeme (Informations- und Kommunikationstechnik) | Implementieren von „standardmäßig sicheren“ Richtlinien wie Need-to-know, Least Privilege und Aufgabentrennung |
| Einbettung in die Planung und Entwicklung | Implementierung des Datenschutzes in die Architektur und die Gestaltung von Geschäftsprozessen und IKT-Systemen | Verwendung von Hardware-Sicherheitslösungen, z. B. den speziellen TPM-Chips (Trusted Platform Module) |
| Doppelsieg-Strategie bzw. Win-win-Situation (*Positive Sum*) | Anpassen aller gültigen Ziele und Interessen in einer positiven „Win-Win-Situation“ und Vermeidung einer Nullsummen-Technik mit nutzlosen Kompromissen | Unterstützen von Interessengruppen und Lösen von Streitigkeiten für eine Win-Win-Situation |
| Durchgängige Sicherheit („End-to-End“) | Gewährleistung eines lebenslangen sicheren Managements von Informationen | Sicherstellung des Schutzes der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen |
| Transparenz und Sichtbarkeit | Teile der IKT-Systeme und der täglichen Geschäftsaktivitäten transparent und für die Nutzenden sichtbar halten | Verbessern der Sicherheit eines Unternehmens durch Industriestandards und robuste Audits |
| Respekt für die Nutzenden | Schutz und Respekt vor allem der Interessen jedes Einzelnen – sie stehen im Mittelpunkt | Schutz und Respekt der Interessen aller Informationseigentümer; Sicherheit muss sowohl organisatorische als auch individuelle Interessen berücksichtigen |

Quelle: Cavoukian & Dixon (2013).

#### Proaktiv statt reaktiv

Die Vorbereitung auf einen Vorfall, bevor er passiert, erfordert eine Änderung der Einstellungen der Geschäftsleitung und der gesamten Unternehmenskultur. Es geht dabei um einen strategischen Ansatz und nicht um einen taktischen Ansatz, bei dem die Bedrohungen erst bei ihrem Auftreten angegangen werden (Cavoukian & Dixon, 2013). Wie in der obigen Tabelle aufgeführt, sind Kontrollmaßnahmen wie Firewalls und IPS Beispiele für proaktive oder strategische Ansätze, bei denen unbefugter oder bösartiger Datenverkehr am Eindringen in das Unternehmensnetzwerk gehindert wird. Dies steht im Gegensatz zum reaktiven Ansatz, bei dem bösartiger Datenverkehr erst beim Eindringen in ein Unternehmensnetzwerk bekämpft wird.

#### Sicherheit als Standard

Dieses Prinzip bezieht sich auf die Durchsetzung der Richtlinien für die Implementierung der Sicherheitsmaßnahmen und auf spezielle Methoden für die Konfiguration und Installation der Software. Das Hauptziel dieses Prinzips besteht darin, standardmäßig sichere Konfigurationen von Informationssystemen zu gewährleisten, anstatt dass die Nutzenden dies separat tun oder, noch schlimmer, dass die Sicherheit erst nach einer Beeinträchtigung verschärft wird (Cavoukian & Dixon, 2013).

#### Einbettung in die Planung und Entwicklung

Zu Schaffung sicherer Systeme ist es unerlässlich, die Sicherheit schon in das Design der Systeme zu integrieren, also bei der Planung und Entwicklung. Dies kann durch Software oder Hardware erreicht werden. Das TPM (Trusted Platform Module) ist, wie in der Tabelle oben erwähnt, ein Beispiel für die Einbettung von Sicherheit bei der Entwicklung der Hardware. TPMs bieten Unterstützung bei der Schlüsselverwaltung durch die Hardware. Es handelt sich um Mikrocontroller (Computerchips) mit begrenztem Speicherplatz zur sicheren Speicherung von Zertifikaten und Schlüsselmaterial auf einer Hauptplatine. Die Einbettung von Zertifizierungs- und Schlüsselmaterial in die Hardware des Systems ermöglicht das Signieren und Hashing der Daten, ohne dass der Verschlüsselungsschlüssel den TPM verlässt. Dadurch wird verhindert, dass ein Schlüssel gestohlen oder durch Schadsoftware verändert wird, wodurch die Authentifizierung und die **kryptografischen Dienste** des Systems zusätzlich abgesichert werden (Cavoukian & Dixon, 2013).

**Kryptografische Dienste**

Den Prozess der Verschlüsselung und Entschlüsselung.

#### Doppelsieg-Strategie (Positive Sum)

Bei diesem Ansatz werden die Interessen aller beteiligten Akteure respektiert, so dass alle ein gemeinsames Ziel erreichen können, das die Entwicklung und Umsetzung von Technologien und Geschäftsinitiativen vorantreibt. Dies führt zu einem strategischen Impuls in Richtung mehr Nachhaltigkeit und Effektivität.

#### Durchgängige Sicherheit („End-to-End“)

Das Hauptziel der Informationssicherheit eines Unternehmens ist die Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit. Bei einem solchen Ansatz werden Schwachstellen im gesamten Unternehmen angegangen, anstatt nur die Außengrenzen des Unternehmens zu schützen. Datenbanksicherheit, Netzwerksicherheit, Identitäts- und Zugriffsverwaltung sowie Privilegien-Zugriffsverwaltung sind einige Beispiele, die bei der Implementierung von End-to-End-Sicherheit in einem Unternehmen berücksichtigt werden (Cavoukian & Dixon, 2013).

#### Transparenz und Sichtbarkeit

Transparenz und Sichtbarkeit sind herausragende Sicherheitsprinzipien, die das Vertrauen von Lieferanten und Kund:innen in die in einem Unternehmen implementierte Informationssicherheit stärken. Unternehmen können dies durch die Umsetzung der Informationssicherheit nach internationalen Normen für Informationssicherheit wie ISO 27001 erreichen. Wenn dieser bekannte internationale Standard sauber umgesetzt wird, können Organisationen nach einer vorschriftsmäßigen externen Prüfung nach ISO 27001 zertifiziert werden. Dies gibt den Kund:innen und Lieferanten die Gewissheit, dass die von der Organisation vorgehaltenen Informationen sicher sind (Cavoukian & Dixon, 2013).

#### Respekt für die Nutzenden

Eine Grundregel des bei der Entwicklung eingebetteten Datenschutzes besteht darin, den Einzelnen und seine Datenschutzrechte zu respektieren. Sicherheit betrifft jedoch noch weitere Aspekte. Sie muss die Belange der Informationseigentümer schützen und respektieren, was sowohl Unternehmensressourcen als auch Einzelpersonen einschließt. Bei Cyberangriffen, deren Hauptziel der Diebstahl von geistigem Eigentum und nicht von personenbezogenen Daten ist, ist der Schutz der Unternehmensdaten beispielsweise genauso wichtig (Cavoukian & Dixon, 2013).

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Die Konzepte Sicherheit und Datenschutz sind einander *wenig ähnlich*.

## 7.5 Umsetzung der Bedrohungsabwehr in einer Organisation

Die durchschnittlichen Kosten einer Datenschutzverletzung betrugen im Jahr 2022 4,35 Millionen $, ein Anstieg von 2,6 Prozent gegenüber 2021 (Tunggal, 2022). Können sich Organisationen das leisten? Nein, natürlich nicht. Cybersicherheit ist heute für jedes Unternehmen von entscheidender Bedeutung, insbesondere in unserem digitalen Zeitalter, in dem Daten das neue Erdöl sind. Aber die Umsetzung des Schutzes ist nicht billig. Die wirksame Umsetzung der Bedrohungsabwehr umfasst Werkzeuge und Lösungen sowie die im Geschäftsbetrieb durchgesetzten Strategien (Usiagwu, 2021). Im Folgenden erläutern wir einige der gängigsten Taktiken zur Bedrohungsabwehr im Bereich der Cybersicherheit.

### Risikobewertung

Die Risikobewertung ist der erste Schritt der Bedrohungsabwehr. Unternehmen müssen ein vollständiges Inventar ihrer Vermögensgüter erstellen und die Schwachstellen in Bezug auf jedes einzelne dieser Vermögensgüter dokumentieren. Dann wird eine Risikobewertung durchgeführt. Zum besseren Verständnis des Prozesses der Risikobewertung werden hier einige wichtige, bei diesem Prozess zu stellende Fragen im Überblick aufgeführt (Usiagwu, 2021).

* Welche Art von Informationen und Daten werden von uns gesammelt und gespeichert?
* Wie kritisch und wichtig sind diese Daten? Unternehmen müssen ihren Handlungsspielraum definieren, um ihre Strategien auf die Bedrohungen und Risiken zuzuschneiden. Organisationen im Gesundheits- und Finanzwesen verarbeiten zum Beispiel besonders sensible Daten, die deshalb strenger geschützt werden müssen.
* Wie speichern wir die Daten?
* Wer hat Zugang zu diesen Daten?

### Schaffung einer robusten Kultur der Cybersicherheit

Der Mensch ist das schwächste Glied und das angreifbarste Element in jeder Organisation. Die besten Cybersicherheitslösungen werden versagen, wenn die Menschen nicht in den bewährten Vorgehensweisen der Cybersicherheit und der aktuellen Bedrohungslandschaft geschult sind. Ein Unternehmen kann keine stringente Cybersicherheitskultur erreichen, wenn sie nicht in den Mitarbeitenden verankert ist. Daher ist die Förderung konsistenter und bewährter Vorgehensweisen für die Cybersicherheit durch regelmäßige Schulungen zur Sensibilisierung der Nutzenden von größter Bedeutung (Usiagwu, 2021).

### Reaktion auf Vorfälle

Die Reaktion auf Vorfälle ist für die Bedrohungsabwehr von entscheidender Bedeutung, denn wenn ein Vorfall in einem Unternehmen eintritt, können die Auswirkungen eines Cyberangriffs durch frühzeitige Erkennung und sofortige Einleitung der erforderlichen Maßnahmen begrenzt werden. Die Organisation muss über eine Strategie für die Reaktion auf Vorfälle verfügen. Es müssen auch Richtlinien vorhanden sein, die das Verhalten im Falle eines Cyberangriffs vorschreiben. Wann genau würde das Cybersicherheitsteam die Geräte der Mitarbeitenden übernehmen? Welche Angriffe erfordern eine vollständige Abschaltung des Netzwerks? All diese Fragen sind entscheidend. Für den Fall einer Datenpanne müssen Unternehmen auch kontinuierliche Datensicherungen (Backups) in Betracht ziehen (Usiagwu, 2021).

### Netzwerküberwachung

Unternehmen müssen eine Netzwerküberwachung einführen, um Jagd auf Bedrohungen zu machen. Ein Unternehmen, genauer gesagt ein Netzwerk, kann mehrere Tage oder sogar Monate lang beeinträchtigt sein, ohne dass die Informationssicherheitsteams davon etwas mitbekommen. Hier kommt also die Überwachung ins Spiel. Der Netzwerk-Datenverkehr eines Unternehmens sollte ständig von den Informationssicherheitsteams überwacht werden, um ungewöhnliche und verdächtige Aktivitäten zu erkennen und zu melden. Dies betrifft insbesondere von Mitarbeitenden durchgeführte Aktivitäten, welche die Ein- und Ausgangspunkte gefährden könnten. Dies könnte durch den Einsatz von Überwachungssystemen wie *Security Information and Event Monitoring* (SIEM) mit künstlicher Intelligenz und maschinellem Lernen erreicht werden, die den Netzwerk-Datenverkehr in Echtzeit überwachen (Usiagwu, 2021).

### Fragen zur Selbstkontrolle

1. Vervollständigen Sie den folgenden Satz:

Die durchschnittlichen Kosten einer Datenpanne *steigen* jedes Jahr.

Zusammenfassung

In dieser Lektion haben wir die verschiedenen Strategien und Methoden, die zur Stärkung der Cyberabwehr eines Unternehmens eingesetzt werden können, im Detail erläutert. Da die Cyberabwehr ohne Verständnis und Umsetzung der Risikominderung nicht gestärkt werden kann, haben wir auch unterschiedliche Methoden zur Risikominderung analysiert, die Unternehmen letztendlich zu einer stärkeren Cyberabwehr verhelfen würden. Darüber hinaus haben wir geprüft, wie die Wirksamkeit der Sicherheitsmaßnahmen sichergestellt werden kann. Zu diesem Zweck haben wir das Konzept von Audits in der Cybersicherheit vorgestellt und erörtert, wie und wann Organisationen zur Validierung ihrer implementierten Sicherheitsmaßnahmen Audits durchführen sollten. Darüber hinaus haben wir gelernt, wie Sicherheit in jeden Aspekt einer Organisation oder eines Produkts eingebettet werden kann, indem Datenschutz und Sicherheit bereits in die Planung und Entwicklung einbezogen werden. Schließlich haben wir die verschiedenen Strategien betrachtet, die zur Bedrohungsabwehr genutzt werden können.