Studienskript



## Cyber Risk Assessment und Management

DLMCSECRAM01\_E



### Lernziele

###### Einleitung 9



Der Kurs **Cyber Risk Assessment und Management** erklärt zunächst, weshalb Unternehmen nicht auf Risikomanagement verzichten können. Darüber hinaus beschreibt er die Anatomie eines Datendiebstahls. Zudem werden grundlegende Informationen über Cyber-Katastrophen und Cyber-Risiken vermittelt.

Um mit Cyber-Risiken umzugehen, müssen die Bedrohungen gemessen werden. Wie das funktioniert, welche Messverfahren angewendet werden und wie Unternehmen vorgehen können, wird in diesem Studienskript beschrieben. Die Messung von Bedrohungen kann nur erfolgen, wenn die Bedrohung selbst bekannt ist und verstanden wird. Sie werden drei Methoden zur Modellierung von Bedrohungen kennenlernen: Angriffsbäume, STRIDE und LINDDUN. Die Kombination dieser Instrumente und Methoden bilden die Grundlage des Risikobewertungsprozesses. Außerdem liefert der Kurs eine Einführung in Standardisierungen wie das NIST Risk Management Framework, die ISO/IEC 27005 und den BSI-Standard 100-3.

Im letzten Teil des Studienskripts werden die cyber-resiliente Organisation und die Cyber-Versicherung erklärt. Sie lernen, wie man eine cyber-resiliente Organisation mit einer sich ständig ändernden Herangehensweise an Risikomanagement, Incident Response, Krisenmanagement, Resilience Engineering und Sicherheitslösungen aufbaut.

[www.iubh.de](http://www.iubh.de/)



# Lektion 1

## Organisatorisches IT- Risikomanagement

##### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie in der Lage sein, …

… zu verstehen, warum Risikomanagement notwendig ist.

… verschiedene Cyber-Katastrophen zu identifizieren.

… ein Cyber-Risiko zu definieren.

DL-E-DLMCSECRAM01\_E-U01

### Organisatorisches IT-Risikomanagement

#### Einführung

Risiken gehören zum Leben eines jeden Menschen, sei es das Risiko, die Wohnungsschlüssel zu verlieren, oder das Risiko, ausgeraubt zu werden. Nachdem wir ein Risiko bewertet haben, suchen wir eine Strategie, um es einzudämmen: Möglicherweise kaufen wir ein Schlüsselband oder meiden Orte, an denen wir Opfer eines Taschendiebstahls werden könnten. Auch Unternehmen sind Risiken ausgesetzt, mit denen sie umgehen müssen. Diese Risiken sind meist komplexer als der Verlust der Wohnungsschlüssel. Ein Beispiel für ein solches Risiko ist der mögliche Verlust von Daten bei einer Datenpanne, die in den meisten Fällen zu Reputations- oder finanziellen Schäden (beispielsweise dem Verlust von Kunden oder Bußgeldern) führen kann. Aus diesem Grund benötigen Unternehmen ein entsprechendes Risikomanagement, was durch die im Folgenden beschriebenen realen Cyber-Katastrophenfälle untermauert wird. Zudem werden die grundlegenden Ziele des Risikomanagements und dessen Möglichkeiten zur Vorbeugung von Cyberattacken erläutert. Abschließend werden die Begriffe „Risiko“ und „Bedrohung“ definiert.

#### Geschäftliche Notwendigkeit des Risikomanagements

Der Aufbau und die Leitung eines Unternehmens bieten hervorragende Möglichkeiten, etwas Großes zu erreichen. Dies kann jedoch große Risiken mit sich bringen. Die Verantwortlichen eines Unternehmens müssen wissen, worin diese Risiken bestehen und welche Auswirkungen sie haben können. Sich der Risiken bewusst zu sein, ist der erste Schritt; der nächste besteht in der Kenntnis der möglichen Maßnahmen zur Risikominderung. Kann das Risiko reduziert werden oder ist es besser, es auf einen Dritten (z. B. eine Versicherung) auszulagern? Bei einem vernünftigen Risikomanagement sind sich die Entscheidenden über die Risiken und die damit verbundenen Kosten einer bestimmten Entscheidung im Klaren. Das Management kann dann entscheiden, ob es sich lohnt, derlei Maßnahmen umzusetzen, oder ob das Risiko einfach akzeptiert werden kann. Im Folgenden wird mit Hilfe einer Planübung gezeigt, wie ein Risikomanagementprozess aussehen kann. Um diese Simulation durchzuführen, gehen wir von einigen Annahmen aus:

* Das Unternehmen ist ein mittelständischer Konzern
* Das zu erörternde Thema ist die europäische Datenschutz-Grundverordnung (DSGVO).
* Die Firma verarbeitet persönliche Daten in einer Webanwendung.
* Die Website hat einen Konstruktionsfehler, der zu Datenlecks führen kann.

Mit Hilfe dieser Information kann ein mögliches Risiko identifiziert werden. Ein eindeutiges Risiko läge vor, wenn der Konstruktionsfehler der Website genutzt werden könnte, um Unternehmensdaten zu extrahieren. Im schlimmsten Fall würden diese veröffentlicht, was nach der DSGVO eine Geldbuße zur Folge hätte. In diesem Fall bestünde die Risikominderungsstrategie darin, den Konstruktionsfehler der Website zu beheben. Die Kosten der Fehlerbehebung betragen X Euro, und die Kosten für die Geldbuße und die Rufschädigung betragen Y Euro. Mit diesen und anderen detaillierteren Informationen können die Verantwortlichen entscheiden, ob sie das Risiko akzeptieren oder beheben wollen. In diesem Beispiel sollte das Risiko behoben werden, wenn Y>X ist.

Letztlich ist ein Risikomanagement in einem Unternehmen erforderlich, um zu entscheiden, ob es sich lohnt, Geld in die Behebung eines Problems zu investieren. Aus finanzieller Sicht mag es sich nicht lohnen, das Risiko zu beheben, wenn seine Auswirkungen oder die Wahrscheinlichkeit seines Eintretens gering sind. Die Behebung von Problemen mit erheblichen Auswirkungen ist jedoch die Kosten wert. Die Kunst des Risikomanagements besteht darin, Entscheidungsträgern eine faktenbasierte Übersicht aller Risiken und ihrer Berechnung vorzulegen. Diese Risikoliste kann auch dazu beitragen, Unternehmensressourcen zu priorisieren und zu planen. Ein höheres Risiko erfordert dringender Ressourcen und Aufmerksamkeit als ein geringeres Risiko (Siegel & Sweeney, 2020).

Organizational IT Risk Management

#### Anatomie eines Datenangriffs

Datenexfiltrationen stellen ein hohes Risiko für Unternehmen dar. Einige große Konzerne sind Opfer solcher Angriffe geworden (z. B. Facebook im Jahr 2019, Capital One 2019 und Equifax 2017). Bei einem Datenangriff verschafft sich ein arglistiger Akteur Zugang zu internen Daten. Dabei handelt es sich meistens um Kundendaten oder andere sensible Informationen. Die folgenden Beispiele verdeutlichen die Anatomie eines Datenangriffs. Es werden die Ereignisse und die Folgen der Datenexfiltration erläutert.

Equifax-Datenpanne 2017

Im Jahr 2017 kam es bei Equifax, einer Verbraucherkreditauskunftei in den USA, zu einer Datenpanne, bei der sich Unbefugte Zugang zu Kundendaten verschafften (Equifax, 2017). Die Datenpanne betraf die Daten von 143 Millionen US-Kundinnen und -Kunden (Fruhlinger, 2020). Die Daten beinhalteten die folgenden Personenangaben (Electronic Privacy Information Center, 2020):

* Name
* Sozialversicherungsnummer
* Geburtsdatum
* Adresse
* Führerscheinnummer

Das Haupteinfallstor war eine ungepatchte Sicherheitslücke in Apache Struts (CVE-2017-5638). Die Hacker nutzten diese Schwachstelle aus, um auf interne Server des Unternehmensnetzwerks zuzugreifen. Sie sammelten interne Informationen, darunter Anmeldedaten von Mitarbeitenden, und nutzten diese, um sich weiteren Zugang zum Netzwerk zu verschaffen. Dann scannten und exfiltrierten sie 76 Tage lang unentdeckt Informationen. Um ihre Aktivitäten zu verschleiern, verschlüsselten die Eindringlinge die Daten und griffen nur auf kleine Archive zu (Mort, 2017).

**Apache Struts**

Bei Apache Struts handelt es sich um ein Open-Source-Framework für Java EE-Webanwendungen.

Infolge dieser Datenschutzverletzung zahlte Equifax im Rahmen eines Vergleichs mindestens 575 Millionen US-Dollar (Federal Trade Commission, 2019). Doch Equifax verlor durch das Leck nicht nur Geld, sondern auch das Vertrauen vieler und stand in der Öffentlichkeit schlecht da. Brian Krebs, ein bekannter Journalist für Cyberkriminalität, nannte die Reaktion auf die Panne „ein Desaster“ (Krebs, 2017).

Ein interessanter Aspekt dieses Datenverlusts ist, dass keine der exfiltrierten Daten im Darknet verkauft wurden. Dies führte zu der Annahme, dass keine „normalen“ Cyberkriminellen hinter dem Vorfall steckten, sondern ein Staat. Diese Theorie wurde bestätigt, als die USA chinesische Militäroffiziere für den Angriff verantwortlich machten (Benner, 2020). Die chinesische Regierung wies die Anschuldigungen zurück (CBS Interactive, 2020). Letztlich befinden sich die Daten der Opfer nun im Besitz eines unbefugten Dritten (Fazzini, 2019), unabhängig davon, wer dafür verantwortlich war.

**Apache Struts**

Bei Apache Struts handelt es sich um ein Open-Source-Framework für Java EE-Webanwendungen.

Capital One-Datenpanne 2019

Im Jahr 2019 kam es bei Capital One, einer US-amerikanischen Bankenholding, zu einer massiven Datenpanne (Capital One Financial Corporation, 2019). Eine unbefugte Person griff auf mehr als 100 Millionen Benutzerkontodaten von Kundinnen und Kunden zu. Das Datenleck betraf die folgenden personenbezogenen Daten:

* + Namen
  + Adressen
  + Postleitzahlen
  + Telefonnummern
  + E-Mail-Adressen
  + Geburtsdaten
  + Einkommensselbstauskünfte
  + Daten zum Kundenstatus, z. B. Bonität, Kreditlinien, Salden, Zahlungshistorie und Kontaktinformationen
  + Sozialversicherungsnummern
  + verknüpfte Bankkontonummern

Web Application

Firewall

Eine Web Application Firewall ist eine Layer-7-Firewall, die dazu dient, Webanwendungen vor typischen Angriffen zu schützen.

.

AWS Metadatendienst

Der AWS-Metadatendienst ist ein Backend-Service von AWS, der Anmeldeinformationen für Ressourcen liefert.

Der ursprüngliche Angriffsvektor für diesen Datenangriff war eine falsch konfigurierte Web Application Firewall (WAF). Diese falsch konfigurierte WAF wurde ausgenutzt, um an Sicherheitsdaten des AWS-Metadatenservice zu gelangen. Die vom Metadatenservice für die WAF erlangten Daten konnten Daten aus den S3-Buckets von Capital One auflisten und synchronisieren. Über diese Fähigkeit wurden bei dem Angriff fast 30 GB Daten heruntergeladen (Novaes Neto et al., 2020). Capital One wurde für diese Datenschutzverletzung mit einem Bußgeld von 80 Millionen US-Dollar belegt. Die US-Aufsichtsbehörde OCC (Ofﬁce of the Comptroller of the Currency) sagte, „dass die Bank es versäumt hat, im Vorfeld die Risiken des Wechsels zu einer Cloud-Storage-Lösung zu identifizieren und zu managen, und ausreichende Kontrollen für die Netzwerksicherheit und Strategien zur Vermeidung von Datenverlust vermissen lässt“ (zitiert in Schroeder, 2020, Abs. 5, vom Autor übersetzt).

Facebook Datenpanne 2019

Im Jahr 2019 wurde online eine Datenbank mit mehr als 419 Millionen Einträgen gefunden (Holmes, 2021). Facebook dementierte einen Hackingversuch auf seine internen Systeme. Die Datenbank enthielt die folgenden Informationen (Whittaker, 2019):

* Benutzername
* Facebook-ID
* Telefonnummer
* Geschlecht
* Standort nach Land

Organizational IT Risk Management

Dieser Datenverlust wurde nicht durch einen Hack der internen Systeme verursacht, sondern durch den Missbrauch einer „Funktion“. So wurde eine Technik namens Scraping verwendet, um Informationen von Facebook zu erlangen. Web Scraping wird genutzt, um verfügbare Daten von Websites zu sammeln. Im Falle von Facebook wurde die Suchfunktion missbraucht, und Nutzer:innen konnten auf der Plattform Freunde anhand ihrer Telefonnummer ausfindig machen. Arglistige Akteure nutzten dies, um Facebook-Nutzer-IDs zu gewinnen. Höchstwahrscheinlich sammelten sie Telefonnummern und prüften, ob es zu diesen Telefonnummern passende Facebook-Profile gab. Nach einem früheren Vorfall (dem Cambridge Analytica-Skandal) hatte Facebook diese Funktion im April 2018 bereits deaktiviert, jedoch waren die Daten bereits ausgespäht worden (O’Sullivan, 2019).

Im April 2021 wurden die Daten aus der im Jahr 2019 entdeckten Datenbank in einem Untergrundforum veröffentlicht, was erneut ein schlechtes Licht auf die Datensicherheit von Facebook warf. Anfangs wurden die Daten durch den Missbrauch einer rechtmäßigen Funktion des Systems erlangt. Unter Missachtung der Vorschriften wurden die Daten dann ohne die Zustimmung der Nutzerinnen und Nutzer an unbefugte Dritte weitergegeben. Dies stellt eine Verletzung der Datenschutz-Grundverordnung dar und kann zu einer Geldstrafe von bis zu vier Prozent des weltweiten Gesamtumsatzes von Facebook im vorangegangenen Geschäftsjahr führen (Intersoft Consulting, 2018).

Risikomanagement eines Datenangriffs

### Die oben genannten Beispiele verdeutlichen, welch gravierende Auswirkungen Datenschutzverletzungen oder Angriffe auf Daten haben können. Die Folgen reichen von Rufschädigung bis hin zu empfindlichen Geldbußen. Meist ist es günstiger, das Risiko zu beheben, als die Geldstrafen zu bezahlen. Daher sollte das Risikomanagement auch das Risiko einer Datenexfiltration berücksichtigen und Kontrollen vorsehen, um ein solches zu verringern. Wenn sich eine Organisation dem Risiko eines Datenangriffs widmet, ist die Wahrscheinlichkeit niedriger, von Regulierungsbehörden mit einer Geldbuße belegt zu werden.

#### Cyber-Katastrophen

Katastrophen gehören zu unserem Leben auf diesem Planeten dazu. Es gibt Naturkatastrophen (z. B. die Buschbrände in Australien 2020) und menschengemachte Katastrophen (z. B. der Reaktorunfall von Tschernobyl 1986). Dies alles sind große Katastrophen mit schwerwiegenden Auswirkungen, wie dem Verlust von Menschenleben und hohen ökologischen Schäden. Solche Katastrophen können sich auch im Cyberspace ereignen. Beispielsweise griffen Cyberkriminelle im Jahr 2020 eine Wasseraufbereitungsanlage in den USA an und versuchten, dem frischen Wasser Chemikalien beizumischen, um es zu vergiften. Glücklicherweise schaltete sich ein Mitarbeiter ein und machte den Eingriff rückgängig, bevor die Chemikalien hinzugegeben wurden. Wäre der Angriff erfolgreich gewesen, so hätte die Vergiftung bis zu 15.000 Anwohnerinnen und Anwohner betroffen. Der Angriff hätte auf einer Ebene mit den zuvor genannten Katastrophen gestanden (BBC, 2021).

Allgemeine Katastrophen

### Müssen Ereignisse immer so schwerwiegend sein, um als Katastrophe zu gelten? Um diese Frage zu beantworten, sollte die Definition des Begriffs „Katastrophe“ untersucht werden. Das Cambridge Dictionary (o.D., vom Autor übersetzt) beschreibt eine Katastrophe als „ein plötzliches Ereignis, das sehr große Schwierigkeiten oder Zerstörung bewirkt“. Das bedeutet erstens, dass die Zahl der Opfer nicht ausschlaggebend für die Einstufung eines Ereignisses als Katastrophe ist. Zweitens werden „große Schwierigkeiten“ subjektiv wahrgenommen. Dabei kann es sich um Todesfälle handeln oder aber um eine bloße Unterbrechung des „normalen“ Lebens. Schließlich ist das Ausmaß einer Katastrophe von Bedeutung. Ein Ereignis mit geringerer Tragweite mag vielleicht keine Katastrophe für die ganze Welt sein, jedoch kann es für eine kleinere Gruppe von Personen oder ein Unternehmen durchaus eine solche darstellen. Eine weitere Definition stammt von der amerikanischen Aktuarsakademie. Ihr zufolge sind Katastrophen „seltene Ereignisse, die erhebliche Verluste, Verletzungen oder Sachschäden bei einer großen Anzahl Betroffener verursachen“ (American Academy of Actuaries, S. 5, vom Autor übersetzt). Fasst man die Definitionen des Cambridge Dictionary und der amerikanischen Aktuarsakademie zusammen, so sind die folgenden Faktoren entscheidend bei der Frage, ob ein Ereignis eine Katastrophe darstellt:

* + - geringe Eintrittswahrscheinlichkeit
    - schwerwiegende Auswirkungen
    - hohe Gruppenbelastung

Leider lassen sich diese Parameter nicht genau und präzise definieren. Die Schwere einer Katastrophe hängt vom Schaden der Opfer ab, unabhängig davon, ob es sich um Einzelpersonen oder um Organisationen handelt.

Cyber-Katastrophen

### Cyber-Katastrophen müssen keine Auswirkungen auf die „reale“ Welt nach sich ziehen. Eine Cyber-Katastrophe ist ein Cyber-Ereignis, dessen gravierende Folgen einer Organisation schaden. Ein Ereignis kann als Cyber-Katastrophe bezeichnet werden, wenn es die folgenden Eigenschaften aufweist (Bashan & Lo Giudice, 2020):

* + - Ausstrahlungsradius. Eine große Gruppe von Anwender:innen ist vom Ereignis betroffen.
    - Ausfall. Ein für Endnutzer:innen bereitgestellter Dienst fällt aus. Der/die Endnutzer:in kann diesen Dienst nicht nutzen, was die Arbeit das Leben der Person beeinträchtigt.
    - Unkontrollierbarkeit. Die Organisation ist nicht mehr in der Lage, ein Ereignis zu kontrollieren, das sie betrifft. Die einzige Handlungsoption, die der Organisation bleibt, ist, die Katastrophe zu überstehen.

Der Ausstrahlungsradius eines Ereignisses kann ein globaler Radius sein (d.h. das weltweite Internet ist betroffen) oder ein kleinerer Radius, bei dem nur eine (größere) Nutzergruppe betroffen ist. Wir können also zwei Arten von Katastrophen unterscheiden: eine lokale Katastrophe, die ein katastrophales Ereignis für eine Gruppe von Menschen oder eine Organisation darstellt, und eine globale Katastrophe, bei der es zu weltweiten Auswirkungen kommt. In der nachfolgenden Tabelle finden sich aktuelle Beispiele globaler Cyber-Katastrophen.

Organizational IT Risk Management

|  |  |  |
| --- | --- | --- |
| Liste ausgewählter jüngster globaler Cyber-Katastrophen | | |
| Jahr | Ereignis | Beschreibung |
| 2001 | Code Red | Code Red war ein Computerwurm, der Server infiziert hat. Der Wurm führte zu einem Denial of Service sowie zur unberechtigten Veränderung (Defacement) der Systeme der Opfer (Boyce, o.D.). |
| 2008 | Conﬁcker | Conﬁcker war ein Computerwurm, der infizierte Systeme verlangsamte. Der Wurm infizierte Millionen von Computern und errichtete aus diesen Systemen ein Botnetz (Burton, o.D.). |
| 2016 | Dyn DDoS-Angriff | Dyn ist ein DNS-Dienstleister. Ein DDoS-Angriff (Distributed Denial of Service) unterbrach den Dienst und legte große Teile des Internets lahm. Der DDoS-Angriff war so breit angelegt, dass er Probleme bei Internetdienstleistern verursachte (Woolf, 2019). |
| 2017 | WannaCry / Not Petya-Ransomware | Ransomware-Angriffe treten seit 2017 vermehrt auf und führen zu Störungen bei großen Konzernen und nationalen Einrichtungen wie Krankenhäusern. Beim Angriff werden die Daten auf den Geräten verschlüsselt und es wird ein Lösegeld gefordert, um die Daten wieder zu entschlüsseln (Hern, 2017). |

Diese Beispiele zeigen, dass ein globales Ereignis nicht an eine einzige Gruppe gebunden ist. Die meisten Internetnutzer:innen waren von diesen Vorfällen betroffen. Lokale Katastrophen betreffen jedoch kleinere Nutzer:innengruppen, wie die folgende Tabelle zeigt.

|  |  |  |
| --- | --- | --- |
| Liste ausgewählter jüngster lokaler Cyber-Katastrophen | | |
| Jahr | Ereignis | Beschreibung |
| 2019 | Störung der AWS Cloud | Ein Stromausfall und das Versagen der Generatoren verursachte eine Störung im AWS US-EAST-1-Rechenzentrum. Dieser Vorfall führte dazu, dass die EC2- und EBS-Instances nicht verfügbar waren. Nachdem die Stromversorgung wieder hergestellt war, erlitten die Speichervolumen Hardwareschäden und es kam zum Datenverlust. Kunden ohne Backups konnten ihre Daten und Dienste nicht wiederherstellen (Abrams, 2019). |
| 2020 | Garmin-Ransom­ware-Angriff | Ein Ransomware-Angriff verschlüsselte Systeme von Garmin. Es wird vermutet, dass Garmin nicht in der Lage war, die Daten wiederherzustellen und die 10 Millionen Dollar Lösegeld gezahlt hat (BBC, 2020). |
| 2021 | Azure AAD-Ausfall | Eine neue Bereitstellung von Azure AAD führte zu einer Unterbrechung des Dienstes. Aufgrund dieser Unterbrechung fielen wichtige Microsoft-Dienste aus (darunter Office, Teams und das Azure-Portal). Es dauerte zwei Stunden, die Störung zu beheben (Foley, 2021). |

#### Cyber-Risiko

Was ist ein Risiko? Genauer gefragt: Was ist ein Cyber-Risiko? Ein Risiko ist das Ausmaß der Auswirkungen, die eine Bedrohung auf eine Organisation haben kann, verbunden mit der Wahrscheinlichkeit, dass diese Bedrohung eintritt. Cyber-Risiken ergeben sich aus Cyber-Bedrohungen, und Cyber-Bedrohungen beschränken sich auf den Cyberspace. So ist es zum Beispiel keine Cyber-Bedrohung, wenn ein Rechenzentrum abbrennt, sofern dies durch ein Nicht-Cyber-Ereignis ausgelöst wurde. Wenn das Feuer hingegen von einem Cyber-Angriff verursacht wurde, stellt die Bedrohung eine Cyber-Bedrohung dar. Das Risikomanagement in einer Organisation muss beide Risiken berücksichtigen (Refsdal et al., 2015).

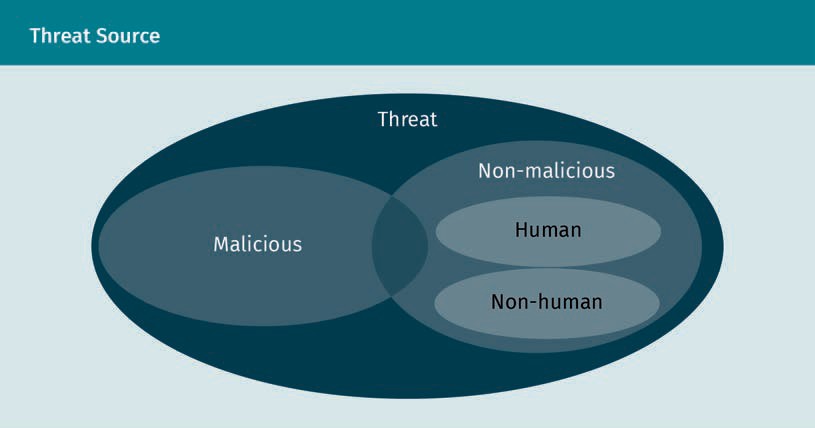
Was ist eine Bedrohung?

Vermögenswert

Ein Vermögenswert ist eine Ressource im Besitz einer Organisation, die wertvoll für ihren Betrieb oder ihre Geschäftstätigkeit ist.

### Eine Bedrohung ist die Quelle eines Risikos. Generell ist eine Bedrohung ein Ereignis mit dem Potenzial, die Organisation zu schädigen. Der daraus resultierende Schaden kann die Organisation selbst oder einen Vermögenswert der Organisation betreffen. Die Bedrohungsquelle kann böswillig (absichtlich) oder nicht böswillig (unbeabsichtigt) sein. Böswillige Bedrohungen sind immer das Resultat menschlichen Handelns. Um das Beispiel des abgebrannten Rechenzentrums wieder aufzugreifen, so ist die Bedrohungsquelle böswillig, wenn ein Bedrohungsakteur dieses absichtlich in Brand setzt. Demgegenüber kann eine nicht böswillige Bedrohung von einem menschlichen oder nicht-menschlichen Ereignis herrühren. Im Beispiel des abgebrannten Rechenzentrums wäre eine menschliche, nicht böswillige Bedrohung ein Brand, der durch den Fehler eines Elektrikers verursacht wurde. Eine nicht menschliche, nicht bösartige Bedrohung wäre es, wenn der Brand von einem Blitzeinschlag ausgelöst worden wäre.

Organizational IT Risk Management

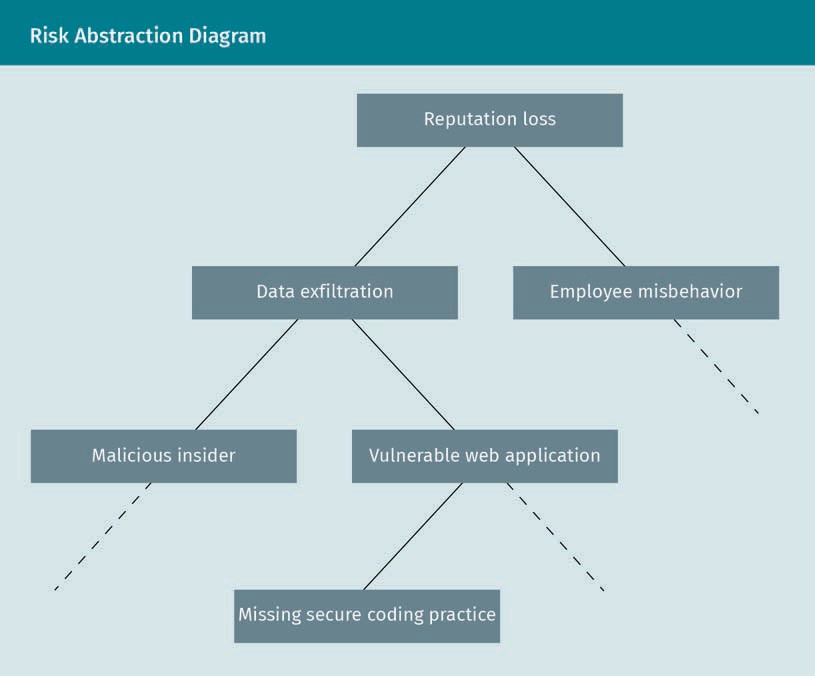


Verbindung zwischen Risiko und Bedrohung

### Wie bereits erwähnt, sind Bedrohung und Risiko nicht gleichzusetzen. Nicht alle Bedrohungen für eine Organisation stellen zugleich Risiken dar, doch alle Risiken beinhalten eine Bedrohung. Eine Bedrohung, die unabhängig von einer Organisation für sich steht, würde keine Probleme verursachen. So ist zum Beispiel ein Exploit für ein spezielles System eine ernste Bedrohung. Falls die Organisation das betreffende System jedoch gar nicht nutzt, stellt es kein Risiko dar, weil es unmöglich ist, dass diese Bedrohung ein Problem verursacht. Im Kern wird eine Bedrohung dann zu einem Risiko für die Organisation, wenn die Wahrscheinlichkeit besteht, dass diese Bedrohung zu Auswirkungen führt.

Abstraktion von Risiken

### Nicht alle Risiken sind für die verschiedenen Management- oder Berichtsebenen relevant. Manchmal ist es hilfreich, die Risiken zu abstrahieren oder zusammenzufassen, wie es die folgende Abbildung zeigt. Zu sehen ist an oberster Stelle das abstrakte Risiko des „Reputationsverlusts“. Es gliedert sich in mehrere Teilrisiken, die dem Ruf der Organisation schaden könnten. Als Beispiele hierfür sind „Datenexfiltration“ und das „Fehlverhalten von Mitarbeitenden“ (unziemliches Verhalten in der Öffentlichkeit) zu nennen. Diese Risiken beinhalten wiederum spezifische Unterkategorien. Der Vorgang der Abstraktion kann so lange fortgesetzt werden, wie es Risiken gibt, die sich konkretisieren lassen.



Zusammenfassung

### Das Risikomanagement stellt eine geschäftliche Notwendigkeit dar. Es hilft Unternehmen dabei, darüber zu entscheiden, wie durch Geldinvestitionen die Widerstandsfähigkeit der Organisation verbessert werden kann. Es bietet den verantwortlichen Personen faktenbasierte Unterstützung, um Investition zu priorisieren und zu planen und so Schwachstellen zu beheben.

### Für viele Organisationen sind Datenexfiltrationsangriffe ein ernstes Risiko. Bei einem erfolgreichen Datenangriff (auch als Datenpanne bezeichnet) werden sensible oder vertrauliche Daten einer Organisation gestohlen. Dabei kann es sich um Kundendaten oder das geistige Eigentum des Unternehmens handeln. In den meisten Fällen hat eine Datenpanne große Auswirkungen auf das Unternehmen. Diese können finanzieller Art (z.B. Geldbußen oder Vergleichszahlungen) oder rufschädigend sein (z.B. schlechte Presse und Kundenverlust).

### Cyber-Katastrophen sind Ereignisse mit den größtmöglichen Auswirkungen auf eine Organisation. Eine Katastrophe kann globale oder lokale Auswirkungen haben. Katastrophen sind stets schwerwiegend. Sie haben einen Ausstrahlungsradius von betroffenen Einzelpersonen oder Organisationen. Kommt es beispielsweise zu einem Ausfall und der betroffene Dienst kann nicht zur Verfügung gestellt werden oder ist schwer gestört, hat es die betroffene Organisation nicht geschafft, das Ereignis einzudämmen, und kann nun nur noch versuchen, die Katastrophe zu überstehen.

Organizational IT Risk Management

### Ein Risiko ist das Ausmaß der Auswirkungen, die eine Bedrohung auf eine Organisation hat, verbunden mit der Wahrscheinlichkeit, dass diese Bedrohung die Organisation betrifft. Ein Cyber-Risiko ist das Ergebnis einer Bedrohung, die allein im Cyberspace existiert (z.B. ein Malware-Angriff). Ein Risiko für ein Cyber-Gerät stellt nicht immer ein Cyber-Risiko dar (z.B. bei einem Hardware-Ausfall eines Servers). Eine Bedrohung ist ein Vorfall, der eine Organisation oder einen ihrer Vermögenswerte schädigen könnte. Die Bedrohungsquelle kann böswillig oder nicht böswillig sein. Eine böswillige Bedrohung ist immer menschlich verursacht, während eine nicht böswillige Bedrohung auf einem menschlichen oder einem nicht-menschlichen Ereignis (natürlichen Ursachen) beruhen kann. Eine Bedrohung kann mehrstufig abstrahiert werden, um das Verständnis der darin enthaltenen Bedrohungen zu erleichtern.

.



# Lektion 2

## Eine Cyber-Bedrohung messen

##### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie in der Lage sein, …

… zu verstehen, wie Cyber-Bedrohungen gemessen werden.

… die Messzahlen eines Risikos zu berechnen.

… den Unterschied zwischen einer Katastrophe und einem „schwarzen Schwan“ zu benennen.

… die Eintrittswahrscheinlichkeit schwerer Cyber-Vorfälle zu erklären.

DL-E-DLMCSECRAM01\_E-U02

### Eine Cyber-Bedrohung messen

#### Einführung

In einer Organisation bestehen meist unterschiedliche Risiken. Die Herausforderung liegt darin, ihr Eintreten anhand von Fakten und messbaren Werten zu berechnen. In unserem Privatleben können wir ein Risiko anhand einfacher Messwerte kalkulieren. Wird beispielsweise ein Fahrrad ohne Schloss zurückgelassen, besteht das Risiko, dass es gestohlen wird. Dabei sind zwei Faktoren zu berücksichtigen: die Auswirkung des Risikos und die Wahrscheinlichkeit, dass es eintritt. In diesem Beispiel wäre die Auswirkung des Risikos der Geldwert, den wir verlieren, wenn das Fahrrad gestohlen wird. Die Eintrittswahrscheinlichkeit des Diebstahls ließe sich mit den folgenden Fragen ermitteln: „Befindet sich das Fahrrad auf einem Privatgrundstück? Ist es so alt, dass es niemand mehr haben möchte?“

Unternehmen müssen mögliche Bedrohungen und Risiken für ihre Organisation messen. Als Entscheidungsgrundlage bedarf es messbarer und vergleichbarer Daten. Dafür können Risiken in gesonderte Werte unterteilt und es kann ein Risikograd berechnet werden. Anhand dieser kann das Management entscheiden, ob es ein Risiko in Angriff nimmt (z. B.: Liegen die Behebungskosten unter den Kosten des Risikos?). Dabei geht es vor allem um die Frage, wie Risiken berechnet und gehandhabt werden können. In dieser Lektion wird eine Methode zur Risikobemessung vorgestellt. Zudem werden Kennzahlen verwendet, um die Eintrittswahrscheinlichkeit von Faktoren realer Ereignisse zu berechnen.

#### Messung und Management

Risikomanagement kann nicht aus dem Bauch heraus erfolgen. Um mit Risiken umgehen zu können, müssen diese korrekt gemessen werden.

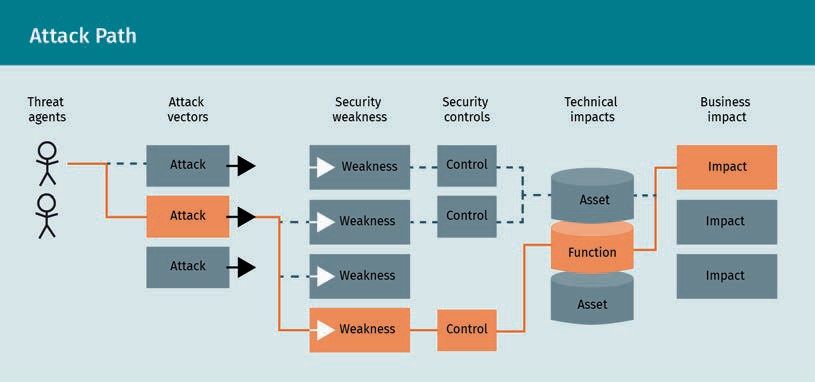
Messung

Um das Risiko einer Bedrohung zu messen, bedarf es einer Methode, welche die Risiken mit Hilfe von messbaren Parametern klassifiziert. Ein Risiko ist die Wahrscheinlichkeit, dass etwas Schlimmes passiert. Das beinhaltet die Möglichkeit, dass sich eine Bedrohung negativ auf eine Organisation auswirkt. Diese Definition kann nun genutzt werden, um eine einfache Formel zu formulieren, mit der sich das Risiko einer Bedrohung berechnen lässt:

Risiko = Auswirkung · Eintrittswahrscheinlichkeit

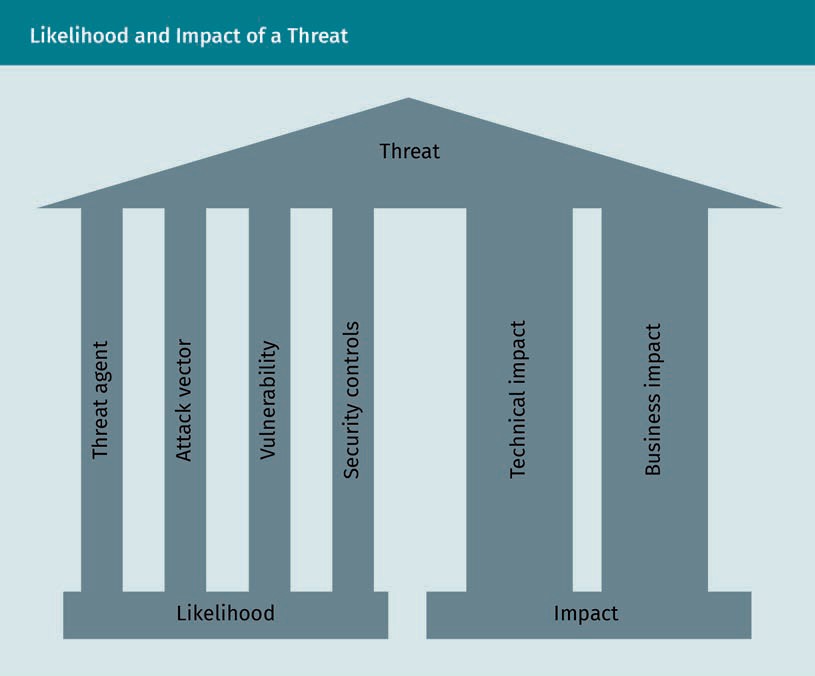
Um einen tatsächlichen Wert zu erhalten, müssen Eintrittswahrscheinlichkeit und Auswirkung messbar sein. Dazu ist es notwendig, sie in genauere und leichter zu definierende Messzahlen zu unterteilen. Die folgende Abbildung beschreibt eine Möglichkeit, dies zu tun.

Measuring the Cyber Threat



Die Abbildung zeigt den Weg eines Bedrohungsakteurs (oder Bedrohungsagenten), der dabei ist, einem Unternehmen zu schaden. Die Auswirkungen der Bedrohung lassen sich als technische und geschäftliche Auswirkungen beschreiben, wobei sich erstere auf ein IT-System und letztere auf das Unternehmen auswirken. Für eine geschäftliche Auswirkung muss immer eine technische Auswirkung vorliegen. Keine Bedrohung eines Cyber-Systems wirkt sich direkt auf das Unternehmen aus: Zunächst muss es eine Auswirkung auf das System selbst geben.

Ein System kann von einem Bedrohungsakteur ausgenutzt werden. In manchen Systemen ist dies leicht möglich, andere sind sicherer und erfordern ein spezielles Wissen des Bedrohungsakteurs. Bevor dieser Einfluss auf ein System nehmen kann, muss er eine Möglichkeit dazu finden. Dies kann als Eintrittswahrscheinlichkeit beschrieben werden: Wie wahrscheinlich ist es, dass Bedrohungsakteure diese Möglichkeit finden? Zunächst benötigt der Bedrohungsakteur einen Angriffsvektor, der auf eine Schwachstelle in den Systemen oder Verfahren der Organisation abzielt. Solche sind normalerweise durch Sicherheitskontrollen geschützt. Diese Kontrollen verhindern üblicherweise, dass eine Schwachstelle ausgenutzt werden kann, um auf das System einzuwirken. Angreifende müssen also eine Schwachstelle finden, für die es entweder keine Sicherheitskontrolle gibt oder die den Angriffsvektor nicht erkennt. Zusammenfassend lassen sich die Eintrittswahrscheinlichkeit und die Auswirkungen einer Bedrohung wie in der folgenden Abbildung darstellen (Williams, 2020).



Management

Nachdem ein Risiko erfolgreich gemessen wurde, muss es bewältigt werden. Dazu muss die verantwortliche Person entscheiden, wie das Risiko einzudämmen ist. Normalerweise kommen dafür die folgenden Möglichkeiten in Frage (Niedbala, 2021):

1. das Risiko vermeiden
2. das Risiko verringern oder abschwächen
3. das Risiko übertragen
4. das Risiko akzeptieren

**Risikoeigner:in**

Als Risikoeigner:in wird die

Person oder Gruppe bezeichnet, die für die Handhabung des Risikos verantwortlich ist.

All diese Maßnahmen sind mit Kosten verbunden. Im Risikomanagementprozess muss der oder die Risikoeigner:in entscheiden, welche Maßnahme praktikabel und im Falle eines Angriffs günstiger als die tatsächlichen Kosten des Risikos ist.

Das Risiko vermeiden

Measuring the Cyber Threat

Um das Risiko zu vermeiden, muss die verantwortliche Person Schritte definieren, die das Eintreten der Bedrohung unmöglich machen. Dies kann durch die Neugestaltung von technischen Aspekten eines Systems oder von Designprozessen erfolgen, die die Handhabung des Systems verändern. Das folgende Szenario veranschaulicht diese Maßnahme.

Angenommen, ein System verarbeitet vertrauliche Informationen für eine Organisation und der Zugriff auf dieses System erfolgt über die Frontend-Website der Organisation. Das Frontend weist eine kritische und einfach auszunutzende Sicherheitslücke auf. Dies birgt nun das Risiko, dass die vertraulichen Daten über das Frontend gestohlen werden. Um zu vermeiden, dass Dritte auf diese Weise Zugang zu den Daten erhalten, kann das System in zwei getrennte Systeme unterteilt werden. Das öffentliche System wird auf einen Drittanbieter übertragen und der Zugang zum Unternehmensnetzwerk wird abgeschaltet. Dieses Vorgehen bezweckt, das Risiko des Diebstahls der vertraulichen Daten über das öffentlich zugängliche Frontend zu verhindern. Das Frontend ist zwar weiterhin angreifbar, aber die Daten sind sicherer

Das Risiko verringern oder eindämmen

Das Risiko zu verringern bedeutet, die Schwachstellen einzudämmen oder zusätzliche Maßnahmen zur Verringerung des Risikos zu ergreifen. Eine Risikominderung oder -eindämmung beinhaltet immer eine Maßnahme, die entweder die Eintrittswahrscheinlichkeit oder die Auswirkungen verringert. Es existieren unterschiedliche Methoden zur Risikominderung, die einerseits von der Bedrohung durch das Risiko und andererseits von den Mitteln der Organisation abhängen. Einige dieser Maßnahmen zur Risikominderung sind:

* die Behebung von Schwachstellen,
* die Verstärkung von Sicherheitskontrollen,
* die Verringerung von Sicherheitslücken,
* die Veränderung des Designs und
* die Nutzung von Präventions- und Erkennungsmechanismen.

Zur Veranschaulichung dieser Maßnahme kann das vorige Beispiel dienen. In diesem Szenario liegt das Risiko in der Angreifbarkeit der Webanwendung eines Unternehmens. Um dieses Risiko zu mindern oder einzudämmen, müssen die Verantwortlichen die Eintrittswahrscheinlichkeit verringern, dass dieser Fall eintreten kann. Die naheliegende Methode wäre es, die Sicherheitslücke in der Anwendung zu beheben. Eine andere Möglichkeit ist die Installation eines IDPS-Systems (Intrusion Detection and Prevention System, IDPS), welches den Zugriff auf die vertraulichen Daten entdeckt und verhindert. Mit diesen Maßnahmen wird die Eintrittswahrscheinlichkeit verringert, dass die Daten durch die Schwachstelle im Frontend kompromittiert werden.

Das Risiko übertragen

Es besteht die Möglichkeit, das Risiko auf eine dritte Partei zu übertragen, die daraufhin als Risikoeigner:in das Risiko trägt. Eine solche Übertragung erfolgt häufig durch rechtlich bindende Verträge. Bei sogenannten Dritten kann es sich um eine Versicherung oder ein Dienstleistungsunternehmen handeln. Im besagten Beispiel könnte sich das Unternehmen zum Beispiel an eine Cyber-Versicherung wenden, um den Diebstahl ihrer vertraulichen Daten abzusichern. Eine weitere Möglichkeit besteht darin, einen Betreiberlösungsanbieter mit der Betreuung des Systems zu beauftragen und vertraglich festzulegen, dass die Sicherheit der vertraulichen Daten von diesem Anbieter gewährleistet werden muss.

Intrusion Detection and Prevention Sys- tem (IDPS)

Ein IDPS überwacht das Netzwerk oder die Systeme, um verdächtigen Datenverkehr oder verdächtige Aktionen zu erkennen. Wenn das System solche Aktivitäten entdeckt, kann es sie automatisch blockieren.

Das Risiko akzeptieren

In der Theorie erscheint die Akzeptanz eines Risikos als die einfachste Maßnahme, die Risikoeigner:innen ergreifen können. Bei näherer Betrachtung erweist sich dies jedoch als nicht mehr so einfach. Denn Risikoakzeptanz bedeutet nicht, das Risiko zu ignorieren. Wer ein Risiko akzeptiert, sollte wissen, was es kosten würde, wenn dieses Risiko eintritt, und wie oft dies passieren könnte. Das Risiko muss zudem beobachtet werden und darf nicht in Vergessenheit geraten. Die Beobachtung des Risikos ist notwendig, damit sich das Unternehmen darauf einstellen kann. Dies kann durch eine Änderung der Sicherheitslücke oder eine Änderung des Geschäftsbetriebs erfolgen.

Das Risiko zu akzeptieren, stellt also keine einfache Lösung dar. Manchmal besteht nicht die Möglichkeit, das Risiko zu vermeiden, zu verringern oder zu übertragen. Manche Risiken müssen bei der Gründung oder Optimierung eines Unternehmens in Kauf genommen werden. Es ist wichtig, eine Balance zwischen dem Eingehen von Risiken und ihrer Vermeidung oder Eindämmung zu finden, wozu gute Risikomanagementprozesse in der Lage sind.

Im vorgestellten Beispiel akzeptiert der oder die Risikoeigner:in das Risiko eines Datendiebstahls über das anfällige Frontend. Im Rahmen des Risikomanagements der Organisation wird ein Risikomanagementplan erstellt, um das Risiko zu beobachten und später eine bessere Lösung zu finden.

#### Metriken für Cyber-Bedrohungen

Das Open Web Applica tion Security Project

Das OWASP ist eine gemeinnützige Organisation mit dem Ziel der Verbesserung von Softwaresicherheit.

Eine Messzahl ist die einfachste Möglichkeit, ein bestimmtes Thema zu quantifizieren. Im Risikomanagement ist die Quantifizierung der Schlüssel zum Erfolg. Allerdings lassen sich „Eintrittswahrscheinlichkeit“ und „Auswirkungen“ nicht so leicht quantifizieren, was jedoch notwendig ist, um das Risiko für eine Organisation zu berechnen. Das Open Web Application Security Project (OWASP) hat messbare Faktoren für die Elemente „Auswirkungen“ und „Eintrittswahrscheinlichkeit“ veröffentlicht. Um diese Faktoren zu quantifizieren, wird jeder Stufe des Faktors ein Wert von null bis neun hinzugefügt. Mit diesen Werten lassen sich geeignete Metriken erstellen. Im Folgenden wird eine mögliche Quantiﬁzierung der Eintrittswahrscheinlichkeit und der Auswirkungen eines Risikos beschrieben. Diese Kennzahlen sind allgemeine Werte und müssen möglicherweise an den spezifischen Bedarf eines Unternehmens angepasst werden.

Eintrittswahrscheinlichkeit

Wie bereits erläutert, lässt sich die Eintrittswahrscheinlichkeit in verschiedene Metriken unterteilen. Diese bilden die Grundlage für die quantiﬁzierte Eintrittswahrscheinlichkeit.

Bedrohungsakteur

Der Bedrohungsakteur stellt den ersten Faktor der Eintrittswahrscheinlichkeit dar. Dieser Faktor beschreibt die Parameter, die die Person benötigt, um eine Schwachstelle auszunutzen. Für die Kalkulation sollte der ungünstigste Bedrohungsakteur verwendet werden. Die folgenden Faktoren können für die Beschreibung herangezogen werden (Williams, 2020, Abschnitt Bedrohungsakteur).

Measuring the Cyber Threat

|  |  |  |
| --- | --- | --- |
| Faktoren für den Bedrohungsakteur | | |
| Kompetenzniveau | Über welche Kompetenzen verfügen die Bedrohungsakteure? | (1) keine technischen Fähigkeiten  (3) gewisse technische Fähigkeiten  (5) fortgeschrittene Computeranwender:innen  (6) Netzwerk- und Programmierkenntnisse  (9) Fähigkeit zum Eindringen in Sicherheitsbereiche |
| Motiv | Wie hoch ist die Motivation der Bedrohungsakteure? | (1) geringe oder keine Belohnung  (5) mögliche Belohnung  (9) hohe Belohnung |
| Gelegenheit | Welche Ressourcen und welcher Zugang sind erforderlich? | (0) vollständiger Zugang oder erhebliche Ressourcen erforderlich  (4) besonderer Zugang oder besondere Ressourcen erforderlich  (7) gewisser Zugang oder Ressourcen erforderlich  (9) kein Zugang oder keine Ressourcen erforderlich |
| Größe | Wie groß ist die Gruppe der Bedrohungsakteure? | (2) Entwickler:innen  (2) Systemadministratoren und -administratorinnen   1. Intranetnutzer:innen 2. Partner:innen 3. authentifizierte Benutzer:innen   (9) anonyme Internetnutzer:innen |

Risikoanfälligkeit

Nach der Bestimmung des Faktors für den Bedrohungsakteur wird auf dieselbe Weise die Risikoanfälligkeit ermittelt. Zur Beschreibung der Vulnerabilität können die folgenden Faktoren angewendet werden (Williams, 2020, Abschnitt Vulnerabilitätsfaktoren).

|  |  |  |
| --- | --- | --- |
| Faktoren für die Risikoanfälligkeit | | |
| Einfachheit der Entdeckung | Wie leicht können Bedrohungsakteure die Schwachstelle finden? | (1) praktisch unmöglich  (3) schwer  (7) leicht  (9) automatisierte Werkzeuge verfügbar |
| Einfachheit der Ausnutzung | Wie leicht kann die Schwachstelle vom Bedrohungsakteur ausgenutzt werden? | (1) theoretisch  (3) schwer  (5) leicht  (9) automatisierte Werkzeuge verfügbar |
| Bekanntheit | Wie verbreitet ist das Wissen um die Schwachstelle unter Bedrohungsakteuren? | (1) unbekannt  (4) versteckt  (6) offensichtlich  (9) öffentlich bekannt |
| Entdeckung des Eindringens | Wie leicht kann der Exploit entdeckt werden? | (1) aktive Erkennung in der Anwendung  (3) erfasst und überprüft   1. ohne Überprüfung erfasst 2. nicht erfasst |

Auswirkungen

Nachdem die Faktoren der Eintrittswahrscheinlichkeit bestimmt wurden, sollen nun die Faktoren der Auswirkungen definiert werden. Normalerweise lassen sich diese weiter unterteilen: Die technischen Auswirkungen bezeichnen die unmittelbaren Folgen der Bedrohung auf das technische System (z. B. den Server oder die Datenbank). Die geschäftlichen Auswirkungen hingegen beziehen sich auf eine Bedrohung des Geschäfts, d.h. auf die Verluste, die die Organisation erleidet, falls sich die Bedrohung realisiert; dieser ist der wichtigere der beiden Faktoren.

Technische Auswirkungen

Die technischen Auswirkungen stellen den Faktor dar, der beschreibt, was mit dem angegriffenen System passiert, wenn die Bedrohung umgesetzt wird. Sie können mit den Prinzipien Vertraulichkeit, Integrität und Verfügbarkeit beschrieben werden. Um die Faktoren der technischen Auswirkungen zu komplettieren, kann zudem Verantwortlichkeit hinzugefügt werden (Williams, 2020, Abschnitt Faktoren technischer Auswirkungen).

Measuring the Cyber Threat

|  |  |  |
| --- | --- | --- |
| Faktoren der technischen Auswirkungen | | |
| Verlust der Vertraulichkeit | Wie sensibel sind die Daten und wie viele davon können offengelegt werden? | (1) minimale Offenlegung nicht sensibler Daten  (6) minimale Offenlegung wichtiger Daten   1. umfangreiche Offenlegung nicht sensibler Daten 2. umfangreiche Offenlegung kritischer Daten   (9) Offenlegung aller Daten |
| Verlust der Integrität | Wie groß kann der Schaden der korrumpierten Daten sein? | (1) minimal, leicht beschädigte Daten  (3) minimal, schwer beschädigte Daten  (5) umfangreich, leicht beschädigte Daten  (7) umfangreich, schwer beschädigte Daten  (9) schwere Beschädigung aller Daten |
| Verlust der Verfügbarkeit | Wie erheblich kann der Dienst unterbrochen werden? | (1) minimale Unterbrechung der sekundären Dienste  (5) minimale Unterbrechung der primären Dienste  (5) umfangreiche Unterbrechung der sekundären Dienste  (7) umfangreiche Unterbrechung der primären Dienste  (9) vollständiger Verlust aller Dienste |
| Verlust der Verantwortlichkeit | Kann der Bedrohungsakteur auf eine Einzelperson zurückgeführt werden? | (1) vollständig rückverfolgbar  (7) möglicherweise rückverfolgbar  (9) vollständig anonym |

Geschäftliche Auswirkungen

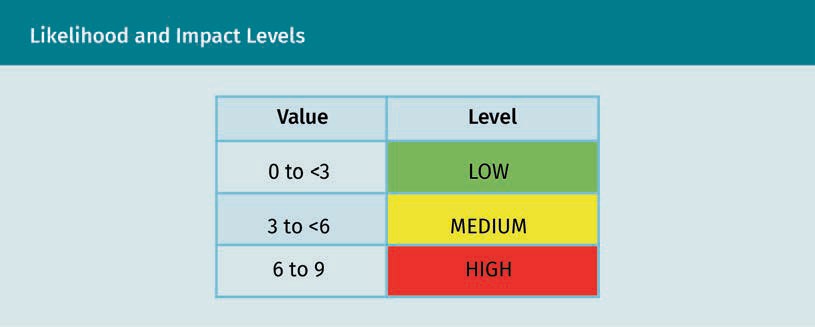
Die geschäftlichen Auswirkungen bilden den wichtigsten Faktor des Risikos, da alle Bemühungen des Risikomanagements darauf abzielen, das Risiko für das Unternehmen zu minimieren. Dieser Faktor rechtfertigt die Maßnahmen zur Behebung eines Risikos. Gemeinsame Faktoren sind in der nachfolgenden Tabelle aufgelistet (Williams, 2020, Abschnitt Faktoren geschäftlicher Auswirkungen).

|  |  |  |
| --- | --- | --- |
| Faktoren für die geschäftlichen Auswirkungen | | |
| Finanzieller Schaden | Wie hoch ist der finanzielle Schaden, den die Bedrohung verursachen könnte? | (1) weniger als die Kosten zur Behebung der Schwachstelle  (3) geringe Auswirkungen auf Jahresgewinn  (7) erhebliche Auswirkungen auf Jahresgewinn  (9) Insolvenz |
| Reputationsschaden | Wie sehr würde der Ruf leiden? | (1) minimaler Schaden   1. Verlust von Großkunden 2. Verlust des Unternehmenswerts   (9) Schädigung der Marke |
| Non-Compliance | Wie sehr verletzt die Bedrohung die Compliance? | (2) geringe Verletzung  (5) klare Verletzung  (7) schwerwiegende Verletzung |
| Verletzung der Privatsphäre | Könnte die Bedrohung zu einer Verletzung der Privatsphäre führen und wie viele Personen wären betroffen? | (3) eine Person  (5) Hunderte Personen  (7) Tausende Personen  (9) Millionen Personen |

#### Die Bedrohung einer Organisation messen

## Um eine Bedrohung zu messen, benötigt eine Organisation eine festgelegte Metrik. Die Messgrößen dienen der Berechnung des Gesamtrisikos anhand der Formel Risiko = Auswirkung × Eintrittswahrscheinlichkeit. Die Methode kann wiederholt werden, um mit den Messgrößen sowohl die Auswirkungen als auch die Eintrittswahrscheinlichkeit zu berechnen. Die Faktoren werden daraufhin multipliziert, um das Risiko zu ermitteln. Für eine visuelle Darstellung des Risikos kann eine einfache Ampelgrafik verwendet werden. Bei dieser Übersicht wird jedem Wert eine Farbe zugewiesen.

Measuring the Cyber Threat



## Es ist wichtig, für die Variablendefinition ein wiederholbares Verfahren anzuwenden. Dies trägt zur Nachvollziehbarkeit der Berechnung des Risikos bei und erhöht die Glaubwürdigkeit des Risikomanagementprozesses. Dennoch beruhen viele der definierten Werte auf Annahmen. So wird beispielsweise häufig davon ausgegangen, dass die Angestellten stets zugunsten des Unternehmens (nicht böswillig) handeln und die zugrunde liegende Infrastruktur über keine bekannten Schwachstellen verfügt. Bei diesem Prozess ist es wichtig, die ausgewählten Werte zu begründen. Daher sollte die Frage „Warum beträgt diese Bewertung X?“ stets beantwortet werden können.

Messung der Eintrittswahrscheinlichkeit

Die Messung der Eintrittswahrscheinlichkeit erfolgt anhand der zuvor deﬁnierten Messgrößen. Hier müssen die Fragen zur Bestimmung der Faktoren für die Risikowahrscheinlichkeit (Bedrohungsakteur und Risikoanfälligkeit) beantwortet werden.

|  |  |
| --- | --- |
| Bedrohungsakteur | Risikoanfälligkeit |
| Kompetenzniveau: Wie kompetent sind die Bedrohungsakteure? | Einfachheit der Entdeckung: Wie leicht kann die Schwachstelle durch den Bedrohungsakteur entdeckt werden? |
| Motiv: Wie groß ist die Motivation der Bedrohungsakteure? | Einfachheit der Ausnutzung: Wie einfach lässt sich die Schwachstelle durch den Bedrohungsakteur ausnutzen? |
| Gelegenheit: Welche Ressourcen und welcher Zugang sind erforderlich? | Bekanntheit: Wie verbreitet ist das Wissen um die Schwachstelle? |
| Größe: Wie groß ist die Gruppe der Bedrohungsakteure? | Entdeckung des Eindringens: Wie leicht kann der Exploit entdeckt werden? |

## Die Antworten auf diese Fragen sollten in eine Tabelle oder ein Formular eingetragen werden. Die Werte werden daraufhin addiert und anschließend durch die Anzahl der Werte geteilt, um den Durchschnitt zu ermitteln. Die folgenden Tabellen zeigen dies beispielhaft.

|  |  |  |  |
| --- | --- | --- | --- |
| Beispiel: Faktor des Bedrohungsakteurs | | | |
| Kompetenzniveau | Motiv | Gelegenheit | Größe |
| 6 | 9 | 7 | 6 |
| = 7 (HOCH) | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Beispiel: Faktor der Risikoanfälligkeit | | | |
| Einfachheit der Entdeckung | Einfachheit der Ausnutzung | Bekanntheit | Entdeckung des Eindringens |
| 3 | 1 | 4 | 9 |
| = 4,25 (MITTEL) | | | |

## Mit diesen beiden Werten lässt sich nun die Eintrittswahrscheinlichkeit berechnen. Dies erfolgt anhand der Summe des Faktors des Bedrohungsakteurs und des Faktors der Risikoanfälligkeit. Diese wird daraufhin durch zwei geteilt, um die Eintrittswahrscheinlichkeit zu ermitteln. In diesem Fall beträgt die Eintrittswahrscheinlichkeit also = (7 + 4,25) / 2 = 5.625 (mittel).

Die Auswirkungen messen

Die Messung der Auswirkungen erfolgt auf die gleiche Weise wie die der Eintrittswahrscheinlichkeit. Zunächst müssen Fragen zur Bestimmung der Messgrößen beantwortet werden.

|  |  |
| --- | --- |
| Technische Auswirkungen | Geschäftliche Auswirkungen |
| Verlust der Vertraulichkeit: Wie sensibel sind die Daten und wie viele davon können offengelegt werden? | Finanzieller Schaden: Wie hoch ist der finanzielle Schaden, den die Bedrohung verursachen könnte? |
| Verlust der Integrität: Wie groß kann der Schaden der korrumpierten Daten sein? | Reputationsschaden: Wie sehr würde der Ruf leiden? |
| Verlust der Verfügbarkeit: Wie erheblich kann der Dienst unterbrochen werden? | Non-Compliance: Wie sehr verletzt die Bedrohung die Compliance? |
| Verlust der Verantwortlichkeit: Kann der Bedrohungsakteur auf eine Einzelperson zurückgeführt werden? | Verletzung der Privatsphäre: Könnte die Bedrohung zu einer Verletzung der Privatsphäre führen und wie viele Personen wären betroffen? |

Auch hier wird der Durchschnitt aus den Werten der Antworten auf diese Fragen berechnet. Die folgenden Tabellen zeigen ein Beispiel.

|  |  |  |  |
| --- | --- | --- | --- |
| Beispiel: technische Auswirkungen | | | |
| Verlust der Vertraulichkeit | Verlust der Integrität | Verlust der Verfügbarkeit | Verlust der Verantwortlichkeit |
| 9 | 5 | 1 | 7 |
| = 5,5 (MITTEL) | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Beispiel: geschäftliche Auswirkungen | | | |
| Finanzieller Schaden | Reputations­schaden | Non-Compliance | Verletzung der Privatsphäre |
| 7 | 9 | 5 | 3 |
| = 6 (MITTEL) | | | |

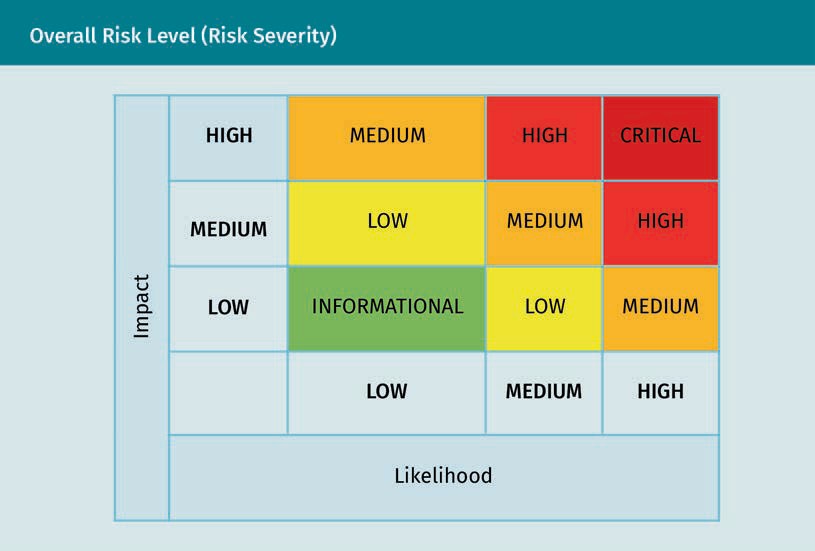
Measuring the Cyber Threat

Nachdem die Faktoren für die Auswirkungen ermittelt wurden, können die Gesamtauswirkungen berechnet werden. Dies erfolgt ebenfalls durch Berechnung des arithmetischen Mittels von technischen und geschäftlichen Auswirkungen. In diesem Fall entspricht der Wert der Auswirkungen = (5,5+6) / 2 = 5,75 (mittel).

Da die geschäftlichen Auswirkungen in der Regel entscheidender sind als die technischen, kann die Berechnung höher gewichtet werden. Das bedeutet, dass der Faktor für die geschäftlichen Auswirkungen stärker gewertet wird als der Faktor für die technischen Auswirkungen. Es ist zudem möglich, nur die technischen Auswirkungen als Faktor für das resultierende Risiko zu verwenden.

Berechnung des Gesamtrisikos

Nachdem sowohl die Eintrittswahrscheinlichkeit als auch die Auswirkungen berechnet wurden, kann das Gesamtrisiko ermittelt werden. Dies kann mit Hilfe einer Matrix der berechneten Eintrittswahrscheinlichkeit und der Auswirkungen geschehen. In diese Matrix werden die jeweiligen Grade der beiden Faktoren (niedrig, mittel oder hoch) eingetragen. Die folgende Abbildung zeigt eine solche Matrix und den resultierenden Risikograd.



In diesem Beispiel ergaben sowohl die Eintrittswahrscheinlichkeit als auch die Auswirkungen einen mittleren Wert. Der daraus resultierende Risikograd wäre daher ebenfalls mittel.

#### Die Eintrittswahrscheinlichkeit schwerwiegender Cyber-Angriffe

## Die oben dargestellten Eintrittswahrscheinlichkeitskennzahlen können auch zur Kategorisierung der Eintrittswahrscheinlichkeit schwerwiegender Cyberattacken dienen. Dies ist nützlich, um zu verstehen, wie die Kategorisierung funktioniert. Dafür muss der Angriffsvektor bekannt sein. Öffentliche Cyberangriffe werden häufig im Nachhinein analysiert. Die Analyse kann dazu dienen, die Eintrittswahrscheinlichkeit des Vorfalls zu ermitteln. Das nachfolgende Beispiel zeigt, wie ein solcher Angriff analysiert werden kann.

Equifax-Datenleck 2017

Im Jahr 2017 wurde bei der US-amerikanischen Verbraucherkreditauskunftei Equifax eine Sicherheitslücke festgestellt, bei der sich Unbefugte Zugang zu Kundendaten verschafften. Der Datenklau betraf 143 Millionen US-Kundinnen und -Kunden (Equifax, 2017).

Szenario

Das Haupteinfallstor für den Datenklau war eine ungepatchte Sicherheitslücke in Apache Struts (CVE-2017-5638). Die Hacker:innen nutzten diese Schwachstelle aus, um sich Zugang zu internen Servern des Equifax-Unternehmensnetzwerks zu verschaffen. Sie sammelten interne Informationen, einschließlich der Anmeldedaten von Mitarbeitenden und nutzten diese, um auf das Netzwerk zuzugreifen. Anschließend scannten und exfiltrierten sie 76 Tage lang unentdeckt Informationen. Um ihre Aktivitäten zu verschleiern, verschlüsselten die Eindringlinge die Daten und griffen nur auf kleine Archive zu (Equifax, 2017).

Wahrscheinlichkeitsanalyse

Um diesen Cyberangriff zu analysieren wird der Wahrscheinlichkeitswert des Bedrohungsakteurs ermittelt.

Kompetenzniveau

Wie kompetent sind die Bedrohungsakteure? Im oben beschriebenen Szenario haben die Eindringlinge eine bekannte Sicherheitslücke ausgenutzt und das Netzwerk gescannt. Die Tatsache, dass sie die Daten daraufhin verschlüsselten, um unentdeckt zu bleiben, deutet darauf hin, dass sie über Netzwerkwissen verfügten und wussten, wie Erkennungsmechanismen umgangen werden können. Es handelt sich um Bedrohungsakteure, die sich damit auskennen, in Sicherheitssysteme einzudringen (9).

Motiv

Wie hoch ist die Motivation der Bedrohungsakteure? Equifax verarbeitet die persönlichen Daten zahlreicher Personen, die im Darknet verkauft werden können. Bei einem erfolgreichen Angriff ist eine hohe Belohnung zu erwarten (9).

Gelegenheit

Welche Ressourcen und welcher Zugang sind erforderlich? Die Website war über das Internet zugänglich und somit anfällig für einen Angriff. Dazu war kein Zugang notwendig. Da die Daten nicht direkt auf dem Server, sondern im Netzwerk gespeichert waren, bedurfte es zusätzlicher Ressourcen, um auf diese Daten zuzugreifen. Dafür waren sowohl ein Zugang als auch Ressourcen erforderlich (7).

Größe

Wie groß ist die Gruppe der Bedrohungsakteure? Der Datendiebstahl wurde anonym durchgeführt, das heißt, von einer anonymen Gruppe von Internetnutzern und -Nutzerinnen (9).

Die ausgewählten Werte für die Eigenschaften des Bedrohungsakteurs können nun zur Berechnung in eine Tabelle eingetragen werden. Das Ergebnis ist eine Gesamtwahrscheinlichkeit von *8,5*.

|  |  |  |  |
| --- | --- | --- | --- |
| Faktor für den Equifax-Bedrohungsakteur | | | |
| Kompetenzniveau | Motiv | Gelegenheit | Größe |
| 9 | 9 | 7 | 9 |
| = 8,5 (HOCH) | | | |

Nach der Berechnung des Faktors für den Bedrohungsakteur kann der Faktor für die Risikoanfälligkeit berechnet werden. Dies geschieht wiederum durch die Beantwortung der Frage nach der untersuchten Schwachstelle.

Einfachheit der Entdeckung

Wie leicht kann die Schwachstelle vom Bedrohungsakteur entdeckt werden? Die ausgenutzte Schwachstelle ist bekannt und es gab bereits Scan- oder ungezielte Angriffe. Das bedeutet, dass automatisierte Tools zur Verfügung stehen, um die Schwachstelle zu erkennen (9).

Einfachheit der Ausnutzung

Wie leicht lässt sich die Schwachstelle ausnutzen? Exploits für diese Sicherheitslücke waren im Internet verfügbar. Die Ausnutzung des internen Netzwerks erforderte jedoch manuelle Eingaben. Diese Schwachstelle zum Exfiltrieren von Daten auszunutzen, bringt gewisse Schwierigkeiten mit sich (3).

Bekanntheit

Wie verbreitet ist das Wissen um die Schwachstelle? Dieser Schwachstelle war ein CVE (Common Vulnerabilities and Exposures – häufige Sicherheitsrisiken und Sicherheitslücken) zugewiesen worden und es waren Patches verfügbar. Man kann also davon ausgehen, dass die Sicherheitslücke weithin bekannt war (9).

Feststellen des Eindringens

Wie leicht kann der Angriff festgestellt werden? Das Sicherheitsteam von Equifax bemerkte den schädlichen Datenverkehr im Netzwerk und begann daraufhin zu ermitteln. Die Trafﬁc-Protokolle hatten sie darauf aufmerksam gemacht. Das bedeutet, dass es keine Anwendungsprotokolle gab. Das Eindringen wurde erfasst und überprüft (3).

Angesichts dieser Werte ergibt sich ein Risikoanfälligkeitsfaktor von (6).

|  |  |  |  |
| --- | --- | --- | --- |
| Faktor für die Equifax-Risikoanfälligkeit | | | |
| Einfachheit der Entdeckung | Einfachheit der Ausnutzung | Bekanntheit | Entdeckung des Eindringens |
| 9 | 3 | 9 | 3 |
| = 6 (HOCH) | | | |

Nach der Berechnung der Wahrscheinlichkeitsfaktoren kann die Gesamtwahrscheinlichkeit berechnet werden. Diese beträgt 7,25 (HOCH). Dieser Wahrscheinlichkeitswert hätte das Risikomanagement alarmieren müssen, denn es war dringend angeraten, das System zu patchen. Warum dies nicht geschehen ist, ist nicht bekannt.

#### Schwarze Schwäne

Früher war es nicht bekannt, dass schwarze Schwäne in freier Wildbahn vorkommen. Als zum ersten Mal ein solcher gesichtet wurde, stellte dies eine große Überraschung dar. In der Tat war dieses Ereignis für die Menschen verheerend, da es ihr Naturverständnis auf den Kopf stellte (Taleb, 2007). Dieses Phänomen lässt sich auch auf das Risikomanagement übertragen. Dort wird ein Ereignis mit verheerenden Auswirkungen und einer Eintrittswahrscheinlichkeit nahe Null als schwarzer Schwan bezeichnet, der die Betroffenen überrascht. In den USA können die Ereignisse vom 11. September 2001 als schwarzer Schwan bezeichnet werden. Niemand hätte sich zu dieser Zeit vorstellen können, dass ein terroristischer Anschlag dieses Ausmaßes verübt werden könnte. Die Auswirkungen des Anschlags, bei dem Tausende starben oder verletzt wurden, waren bekanntermaßen dramatisch. Die USA begannen daraufhin den „Krieg gegen den Terror“, der viele weitere Opfer und noch höhere finanzielle Kosten erforderte. Der Anschlag hatte erhebliche wirtschaftliche Auswirkungen, da die Börse vorübergehend geschlossen wurde und an Wert verlor.

Auch im Cyber-Risikomanagement sind schwarze Schwäne möglich. Einige Ereignisse können so schwerwiegende Auswirkungen haben wie ein schwarzer Schwan, werden jedoch nicht als ein solcher eingestuft, da die Eintrittswahrscheinlichkeit des jeweiligen Ereignisses höher ist. Dies ist der Hauptunterschied zwischen einem schwarzen Schwan und einer Cyber-Katastrophe. Wie auch ein schwarzer Schwan hat eine Cyber-Katastrophe ebenfalls große Auswirkungen auf die betroffenen Parteien, jedoch beträgt die Eintrittswahrscheinlichkeit nicht nahezu Null. Die Ransomware-Angriffe von WannaCry gelten beispielsweise als Cyber-Katastrophe, da sie im Jahr 2017 gehäuft auftraten und großen Unternehmen und nationalen Einrichtungen schadeten (Hern, 2017). Die Angreifenden verschlüsselten die Daten auf den Geräten und forderten ein Lösegeld, um diese wieder zu entschlüsseln. Für die Opfer ist ein solcher Angriff verheerend und durchaus nicht unwahrscheinlich. WannaCry griff auf das Betriebssystem zu, um sich auszubreiten und weitere Daten zu verschlüsseln. Diese Schwachstellen bestanden bereits vorher und es war abzusehen, dass jemand sie ausnutzen würde (Microsoft, 2017).

Cyber-Ereignisse als schwarze Schwäne einzuordnen, erweist sich als kompliziert, da die meisten Katastrophen als Möglichkeit bekannt sind. Ein Beispiel hierfür ist der Angriff auf die Lieferkette von SolarWinds, dessen Auswirkungen als verheerend eingestuft werden können. Die Angreifenden verschafften sich Zugriff auf den Update-Server von SolarWinds und infizierten die Updates mit Malware. Die infizierten Updates wurden daraufhin an Organisationen verteilt und öffneten den Angreifenden Hintertüren (FireEye, 2020). Zuvor zeigten Machbarkeitsnachweise, dass Angriffe auf die Lieferkette möglich sind und Sicherheitsexperten hatten ebenfalls davor gewarnt. Nach der Untersuchung des Vorfalls stand fest, dass das Risikomanagement von SolarWinds versagt hatte. Es gab keine verbindlichen Passwortrichtlinien für den Server und laut der offiziellen Erklärung war ein Praktikant für die mangelhafte Sicherheit verantwortlich (Moore, 2021).

Warum sollte ein solch verheerender Vorfall nicht als schwarzer Schwan bezeichnet werden? Ein Ereignis wie dieses kann als Planübung skizziert werden. Die Finanzbranche stellt dafür ein beispielhaftes Ziel dar, welches weltweite Auswirkungen zur Folge hätte, die vermutlich zu einer Wirtschaftskrise führen würden. Denkbar wäre ein Szenario, in dem Angreifer:innen die Software, die im globalen Bankennetzwerk oder den Aktienmärkten der Welt verwendet wird, ausnutzen.

Vorbereitung auf einen schwarzen Schwan

Das Risikomanagement einer Organisation muss sich auch auf schwarze Schwäne vorbereiten. Die Schwierigkeit der Planung liegt darin, dass diese Ereignisse so unerwartet auftreten, dass sich die Eintrittswahrscheinlichkeit kaum berechnen lässt. Die beste Vorbereitung auf einen schwarzen Schwan besteht darin, dessen mögliche Folgen abzumildern. Dies erfordert eine effektive Cybersicherheitsstrategie. Zudem erweist sich die Reaktionsplanung in der Bewältigung solcher Ereignisse als entscheidend.

Zusammenfassung

Beim Risikomanagement ist es wichtig, die Risiken und Bedrohungen zu messen und zu quantifizieren. Zu diesem Zweck kann die einfache Formel Risiko = Auswirkungen · Eintrittswahrscheinlichkeit verwendet werden. Demnach ist das Risiko ein Produkt von Eintrittswahrscheinlichkeit und Auswirkungen.

### Sowohl die Eintrittswahrscheinlichkeit als auch die Auswirkungen lassen sich mit Hilfe von Faktoren messen. Die Faktoren der Eintrittswahrscheinlichkeit sind der Bedrohungsakteur und der Risikoanfälligkeitswert der Bedrohung. Die technischen und die geschäftlichen Folgen stellen Faktoren für die Auswirkungen dar.

### Zur Berechnung der Gesamtwahrscheinlichkeit und -auswirkungen kann jedem dieser Faktoren ein Wert zugewiesen werden. Diese Werte bewegen sich auf einer Skala von Null bis Neun. Der numerische Wert lässt sich mit den Werten anderer Risiken vergleichen. Zur besseren Lesbarkeit können die numerischen Werte auch in die Schweregrade niedrig, mittel und hoch umgewandelt werden. Für das sich daraus ergebende Risiko lauten die Kategorien informationshalber, niedrig, mittel, hoch und kritisch.

### Diese Kriterien können zur Klassifizierung größerer Cyber-Ereignisse verwendet werden. Dabei handelt es sich im Grunde um ein Reverse Engineering des Ereignisses. Bei dieser Vorgehensweise können die bekannten Faktoren eines Ereignisses verwendet werden, um dessen Eintrittswahrscheinlichkeit zu berechnen. Dies kann dazu dienen, die Kriterien zu verbessern oder die Klassifizierung eines ähnlichen Ereignisses zu überprüfen.

### Schwarze Schwäne sind besondere Ereignisse. Sie sind verheerend wie eine Katastrophe, treten aber so unerwartet auf, dass es schwierig ist, sie einzuplanen. Der beste Ansatz, sich auf solche vorzubereiten, besteht darin, ihre Auswirkungen zu verringern und sie durch eine Reaktionsplanung zu bewältigen.



# Lektion 3

## Threat Modeling

##### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie in der Lage sein, …

… Angriffsbäume zu zeichnen.

… Bedrohungen mit STRIDE zu beschreiben.

… Bedrohungen mit LINDDUN zu bewerten.

DL-E-DLMCSECRAM01\_E-U03

### Threat Modeling

#### Einführung

Um Risiken erfolgreich identifizieren und managen zu können, muss eine Organisation zunächst die zugrunde liegenden Bedrohungen erkennen. Threat Modeling, also das Ermitteln und Suchen von Bedrohungen, stellt in gewisser Weise eine Kunst dar. Ähnlich wie ein/e Künstler:in zahlreiche Werkzeuge nutzen kann, verwendet ein/e Bedrohungsanalyst:in verschiedene Werkzeuge und Methoden, um Bedrohungen zu modellieren. Diese Werkzeuge können von einfachen Anforderungskatalogen und Fragen, die vom Analysierenden zu berücksichtigen sind, bis hin zu komplexen Methoden der Bedrohungsanalyse reichen. Die Auswahl des richtigen Werkzeugs ist entscheidend, um den Prozess möglichst einfach zu gestalten. In dieser Lektion werden verschiedene Methoden zur Bedrohungsmodellierung vorgestellt und ihre Anwendung erklärt.

#### Attack-Tree-Methode

Die Attack-Tree-Methodik ist eine der umfassenderen Methoden zur Modellierung von Bedrohungen. Attack-Trees sind grafische Darstellungen, die Bedrohungen hierarchisch veranschaulichen und die Eintrittswahrscheinlichkeit ermitteln, dass Angriffe erfolgreich sein könnten. Bruce Schneier (1999) definierte Attack-Trees als „formalen, methodischen Weg zur Beschreibung der Sicherheit von Systemen, beruhend auf verschiedenen Angriffen […] stellen Angriffe auf ein System in einer Baumstruktur dar, wobei das Ziel den Wurzelknoten darstellt und die verschiedenen Wege zur Erreichung dieses Ziels die Blattknoten“ (Abschnitt Enter Attack Tree).

Verschiedene Formen von Attack-Trees

Attack-Trees können verschiedene Formen aufweisen, wobei Listen und Graphen die gängigsten sind. Bei der ersten Form wird ein Attack-Tree als Liste mit Indizes dargestellt. Jeder Index steht für einen Angriff auf das Zielsystem. Das Wurzelelement ist das Gesamtziel des Angreifers, wie die folgende Liste zeigt.

Beispiel für einen Attack-Tree

1. Safe öffnen

* Tresortür öffnen

Passwortkombination ausspionieren Tresorschloss aufbrechen

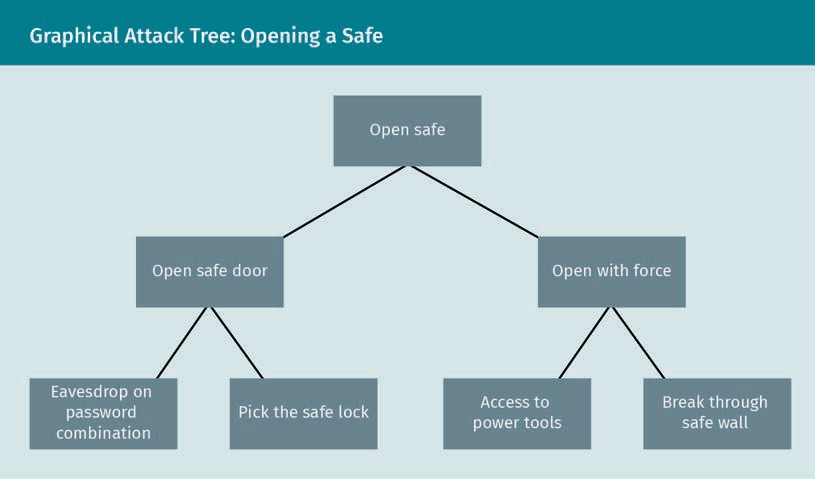
1. Unter Anwendung von Gewalt öffnen (&)

•

* + Zugang zu elektrischem Werkzeug
  + Aufbrechen der Tresorwand

Threat Modeling

Ein Attack-Tree kann auch die Form einer Grafik mit einem Wurzelknoten und einer unbestimmten Anzahl von Unterknoten haben. In dieser Form beschreibt der Graph den Hauptangriff und die Schritte, die erforderlich sind, damit der konkrete Angriff erfolgreich ist (siehe Grafik unten).

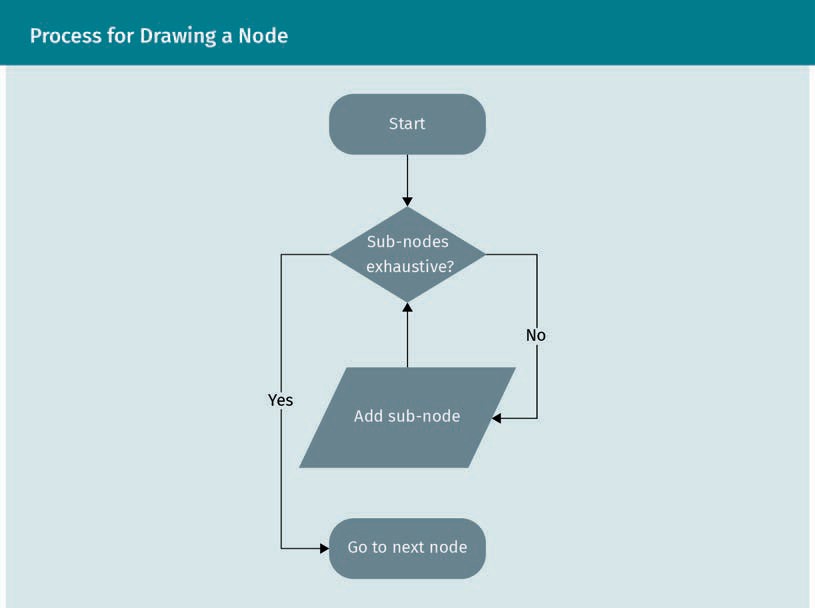


Obgleich Struktur und Informationen beider Versionen identisch sind, bietet der Graph eine umfassendere und besser lesbare Darstellung. Die Listenversion kann leicht in den Graph umgewandelt werden und umgekehrt.

Deﬁnition eines Attack-Trees

Um einen Attack-Tree für eine bestimmte Bedrohung erstellen zu können, müssen wir zunächst das Grundprinzip von Attack-Trees verstehen. Grundsätzlich besteht ein Attack-Tree aus zwei Elementen: Knoten und Kanten. Knoten sind die Angriffsaktionen des Baums (z. B. Öffnen der Tresortür). Die Knoten sind mit Kanten verbunden, die verschiedene Verbindungen darstellen. Ein einfacher Baum kann zwei verschiedene Verknüpfungen aufweisen: ODER oder UND. Diese Verbindungen veranschaulichen die Beziehung zwischen den Kindern eines Knotens. In den folgenden Beispielen wird die ODER-Verbindung durch eine normale Kante zwischen zwei Knoten dargestellt. Die UND-Verbindung wird durch einen Punkt am Anfang der Kante zwischen zwei Knoten in der Graph-Darstellung oder durch ein Kaufsmanns-Und (&) in der Listendarstellung dargestellt.

Einen Attack-Tree zeichnen

Beim Zeichnen eines Graphen entscheiden wir zunächst, welcher Angriffspfad oder welche Bedrohung für ein bestimmtes System zu modellieren ist. Diese Bedrohung bildet den Wurzelknoten des Attack-Trees. Alle weiteren Knoten sind dann Unterknoten des Wurzelknotens. Jeder Attack-Tree kann nur einen Wurzelknoten haben. Wenn verschiedene Angriffsziele modelliert werden sollen, müssen unterschiedliche Attack-Trees gezeichnet werden. Die Entwicklung von Attack-Trees wiederholt sich für jeden Knoten. Sobald ein Knoten gezeichnet ist, identifizieren die Analysten dessen Unterknoten und gehen dann zum nächsten über.

Oft ist es schwierig, die Unterknoten für jeden Knoten zu identifizieren. In diesem Fall können verschiedene Fragen genutzt werden, um weitere Unterknoten zu ermitteln. Einige Fragen lauten z. B.:

* Was ist erforderlich, um den beschriebenen Angriff erfolgreich auszuführen?
* Unterliegt der Angriff bestimmten Einschränkungen?
* Kann der Angriff auf verschiedene Weise ausgeführt werden?

Nach einer gewissen Anzahl von Unterknoten könnte der Attack-Tree als vollständig angesehen werden. Tatsächlich ist ein Attack-Tree jedoch niemals wirklich vollständig; Analysten können immer noch mehr Details zu einem Knoten hinzufügen oder sich neue Wege überlegen, das Hauptziel zu erreichen. Daher ist es wichtig, dass ein ausreichendes Vollständigkeitsniveau des Attack-Trees für den konkreten Fall bestimmt wird. So muss ein Attack-Tree auf hoher Ebene für eine gesamte Organisation keine technischen Details darüber enthalten, wie ein konkretes System kompromittiert werden könnte. In der Regel sollte ein Attack-Tree immer auf eine Seite passen, damit er lesbar und übersichtlich bleibt.

Sobald der Attack-Tree für vollständig gehalten wird, können die Analysten damit beginnen, die Verzweigungen zu beschneiden, d. h. die Knoten durchzugehen und sie auf Doppelungen zu überprüfen. Auch Angriffe, die im Rahmen des Attack-Trees als unmöglich eingestuft werden, müssen markiert werden. Sie dürfen nicht gelöscht werden, damit der Attack-Tree vollständig bleibt.

Threat Modeling

Erweiterung der Attack-Trees

Der oben erwähnte Attack-Tree umfasst die Grundform eines Baumes. Ein Attack-Tree kann jedoch auch funktional erweitert und um Bedrohungen ergänzt werden. Er lässt sich zudem zu einem Attack-Defense-Tree umwandeln.

Hinzufügen von Bedrohungskennzahlen

Bedrohungskennzahlen können genutzt werden, um das Angriffsszenario (den Knoten) quantitativ zu beschreiben. Diese Kennzahlen können Blattknoten zugewiesen und anschließend auf die verbleibenden Knoten weiterverbreitet werden. Die Analysten können entscheiden, welche Bedrohungskennzahlen verwendet werden, wobei sie in der Regel mit Kennzahlen beginnen, die zur Bestimmung der Angriffswahrscheinlichkeit und der potenziellen Auswirkungen dienen. Die Eintrittswahrscheinlichkeit bezeichnet die Chance, dass dieser Angriff auf den betreffenden Knoten erfolgreich sein könnte, und die Auswirkungen beschreiben den Effekt auf das System, falls der Angriff erfolgreich ist.

Attack-Defense-Trees

Attack-Defense-Trees erweitern das Konzept der Attack-Trees, indem die Knoten um Verteidigungs- oder Gegenmaßnahmen ergänzt werden. Diese Verteidigungsknoten bieten Schutz gegen die Bedrohung, die durch den jeweiligen Angriffsknoten dargestellt wird. Sobald der Attack-Defense-Tree vollständig ist, sollte jeder Angriffsknoten eine Gegenmaßnahme haben oder im Teilbaum gemindert werden. So ist das System ist gegen alle identiﬁzierten Angriffe geschützt. Es besteht Handlungsbedarf, wenn in einem Teilbaum keine Gegen- oder Abwehrmaßnahmen vorhanden sind.

#### STRIDE

Eine weitere Methode zur Modellierung von Bedrohungen ist STRIDE. Von den beiden Microsoft-Ingenieuren Loren Kohnfelder und Praerit Garg entwickelt, wurde STRIDE ursprünglich genutzt, um Bedrohungen innerhalb von Microsoft-Produkten zu entdecken (Kohnfelder & Garg, 1999). Der Begriff setzt sich aus den Anfangsbuchstaben der folgenden Bedrohungen zusammen (Shostack, 2014).

* Spoofing (Identitätsverschleierung) bedeutet vorzugeben, jemand oder etwas anderes zu sein, als man in Wirklichkeit ist.
* Tampering (Manipulation) bedeutet, etwas zu verändern, das man nicht verändern darf.
* Repudiation (Verleugnung) bedeutet zu behaupten, dass man etwas nicht getan hat (unabhängig davon, ob man es getan hat oder nicht).
* Information Disclosure (Offenlegung von Informationen) bedeutet, Informationen an Personen weiterzugeben, die nicht berechtigt sind, diese zu sehen.
* Denial-of-Service-Angriffe (Verweigerung des Dienstes) zielen darauf ab, ein System an der Erbringung von Diensten zu hindern, es beispielsweise zum Absturz zu bringen, unbrauchbar langsam zu machen oder seinen gesamten Speicher zu füllen.
* Elevation of Privilege (Rechteausweitung) liegt vor, wenn ein Programm oder ein:e Benutzer:in technisch in der Lage ist, Dinge zu tun, die eigentlich unzulässig sind.

Jede der STRIDE-Bedrohungen ist das direkte Gegenteil einer zentralen Eigenschaft, die eine Software oder ein System haben sollte. Die Paarungen lauten:

* + Spoofing ←→ Authentifizierung: Ein System sollte Benutzereingaben authentifizieren und Benutzer:innen validieren.
  + Tampering ←→ Integrität: Ein System sollte die unbefugte Manipulation von Daten verhindern und die Integrität seiner Daten schützen.
  + Repudiation ←→ Nachweisbarkeit: Ein System sollte in der Lage sein, seine Benutzer:innen und Administrator:innen zu tracken, so dass sie gegebenenfalls zurückverfolgt oder validiert werden können.
  + Information Disclosure ←→ Vertraulichkeit: Ein System sollte in der Lage sein, seine Daten vor unbefugtem Zugriff zu schützen.
  + Denial of Service ←→ Verfügbarkeit: Ein System muss so konzipiert sein, dass bösartige Benutzerinteraktionen seine Leistungsfähigkeit nicht beeinträchtigen können.
  + Elevation of Privilege ←→ Autorisierung: Ein System sollte immer überprüfen, ob Benutzer:innen berechtigt sind, die angeforderte Aktion auszuführen. Unbefugte Benutzer:innen müssen an der Ausführung von Aktionen gehindert werden.

Die Verwendung von STRIDE zur Identifikation von Bedrohungen

Um Bedrohungen mit Hilfe von STRIDE zu identifizieren, müssen die Analysten alle Bedrohungen berücksichtigen, die das System gefährden könnten. Auf welche Weise sie im Einzelnen eine Bedrohung für das System darstellen, kann später bestimmt werden, beispielsweise „könnte sich jemand als Administrator ausgeben“. Dies mag zunächst nach einem berechtigten Risiko klingen, es bleibt jedoch vage. Um diese Bedrohung näher zu untersuchen, können die Analysten die Systemarchitekten oder -entwickler befragen. Wenn niemand in der Lage ist, zu erklären, warum dieser Vorfall nicht eintreten wird, haben die Analysten eine verifizierte Bedrohung gefunden. Mitunter erhalten die Analysten vielleicht die Rückmeldung: „Nein, das kann nicht passieren, weil wir die Benutzerauthentifizierung stets überprüfen.“ Das heißt, dass es an Stelle des Risikos eine Maßnahme gibt, die überprüft werden kann und sollte, um diese Aussage zu bestätigen.

UML

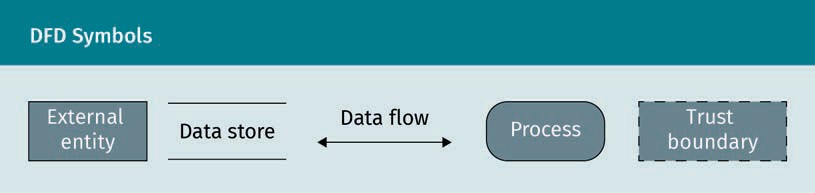
Die Uniﬁed Modeling Language ist eine allgemeine Modellierungssprachefür die Systemvisualisierung in der Softwareentwicklung.

Threat-Modeling-Diagramme

Es kann schwierig sein, Bedrohungen zu identifizieren, ohne einen Überblick über die gesamte Systemumgebung zu haben. Dabei dienen Diagramme oft als hilfreiche Modellierungswerkzeuge. UML-Diagramme (Unified Modeling Language), wie z. B. Swimlane- oder Zustandsdiagramme, können uns dabei helfen, ein Verständnis für die Funktionsweise eines Systems zu gewinnen (Booch et al., 2005). Das für die Bedrohungsmodellierung wichtigste Diagramm ist das Datenflussdiagramm (DFD). Dieses Diagramm enthält alle Informationen über Entitäten und ihre Beziehungen innerhalb des Systems. Das DFD hilft den Analysten, Verbindungen und Bedrohungen aller im System verwendeter Entitäten zu identifizieren. Ein Datenflussdiagramm besteht aus den folgenden Elementen:

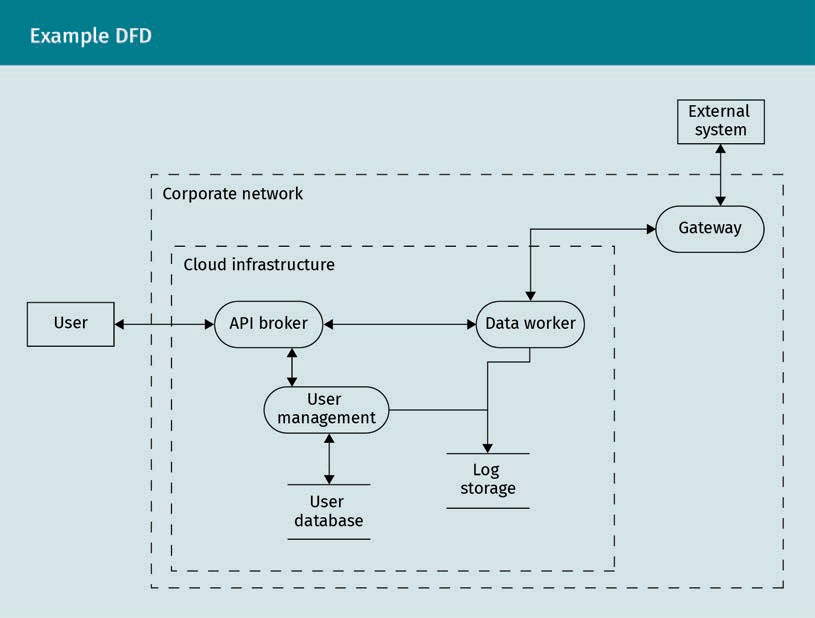
Threat Modeling

* Prozess, also jeder ausgeführte Code, der vom System kontrolliert wird.
* Datenfluss, also jeder Datenfluss zwischen Prozessen, Datenspeichern oder externen Entitäten.
* Datenspeicher, also jedes Teilsystem, das vom System kontrollierte Daten speichert.
* externe Entität, also jede externe Entität (Benutzer:in oder System), die mit dem System interagiert, aber nicht vom System selbst kontrolliert wird.
* Vertrauensgrenze, also eine Grenze zwischen zwei Entitäten, die einen Vertrauenswechsel kennzeichnet (z. B. vom Firmennetzwerk zum Internet)



Ein DFD muss alles enthalten, was für das System relevant ist und was auf relevante Weise mit ihm interagiert. Im Grunde beschreibt das DFD, wie das System funktioniert, mit wem es interagiert und wie die gesamte Kommunikation und die Datenspeicherung ablaufen. Um sicherzustellen, dass ein DFD zur Modellierung von Bedrohungen verwendet werden kann, müssen bei der Erstellung des DFD die folgenden Regeln beachtet werden (Howard & LeBlanc, 2009):

* + Ein Prozess muss mit mindestens einem Datenfluss verbunden sein.
  + Ein Datenfluss muss bei einem Prozess beginnen oder enden.
  + Ein Datenspeicher muss mit einem Prozess mit Datenfluss verbunden sein.
  + Datenspeicher können sich nur mit einem Prozess verbinden.



Spooﬁng

Als Spoofing wird das Vortäuschen, jemand oder etwas anderes zu sein, bezeichnet, d. h. der Angreifer stellt die Frage: „Kann ich das System dazu bringen, mich für jemand anderen zu halten?“ Im Beispiel-DFD entsteht eine Bedrohung möglicherweise durch eine/n Benutzer:in, der/die seine/ihre Identität verschleiert, um die Benutzerverwaltung zu unterlaufen. Auch könnte das externe System das Gateway davon überzeugen, ein anderes System zu sein. Zu den technischen Schwachstellen gehören:

* + - Die Benutzer-ID ist Teil der Anfrage und kann geändert werden.
    - Ein externes System wird über eine Subdomain kontaktiert, die gekapert werden kann.

Tampering

Beim Tampering kommt es zur Änderung oder Modifikation von Daten, die von den Benutzern nicht geändert oder modifiziert werden sollten, d.h. der Angreifer stellt die Frage: „Kann ich das System dazu bringen, spezielle Dateien zu modifizieren, oder kann ich sie selbst modifizieren?“ Im Beispiel-DFD könnten folgende Bedrohungen aufgrund von Tampering vorliegen:

* + - Manipulation des Data Workers, um Zugang zu verschiedenen externen Systemen zu erhalten
    - Modifikation der Benutzerdatenbank, um Werte zu ändern.

Repudiation

Bei der Repudiation geht es um die Übernahme oder Ablehnung der Verantwortung bestimmter Benutzer:innen oder Systeme hinsichtlich der Durchführung bestimmter Aktionen. Das Ziel des Angreifers ist es, die Rückverfolgbarkeit dieser Aktionen zu verhindern, d. h. er stellt die Frage: „Kann ich das System dazu bringen anzunehmen, dass ich etwas getan bzw. nicht getan habe?“ In diesem Beispiel könnte zu den Bedrohungen aufgrund von Repudiation Folgendes gehören:

* + - Die Benutzeraufzeichnung wird manipuliert, um das Aufzeichnen gewisser Aktionen zu verhindern.
    - Ein/e Benutzer:in kann Aufzeichnungsereignisse auslösen, ohne die eigentliche Aktion durchzuführen.
    - Es ist nicht möglich nachzuvollziehen, welche Benutzer:innen auf welche Programmierschnittstelle (API) zugegriffen haben.

Information Disclosure

Die Information Disclosure beinhaltet die Extraktion von Information, für die ein/e Benutzer:in keine Zugriffsberechtigung hat, d.h. der Angreifer stellt die Frage: „Welche Daten kann ich extrahieren und wie?“ Im Beispiel-DFD können sich Bedrohungen aufgrund von Information Disclosure ergeben durch:

* + - das Auffinden eines Fehlers in der Programmierschnittstelle, um Benutzerdaten zu extrahieren.
    - das Erhalten von Fehlermeldungen, die Anmeldedaten oder andere sensible Informationen offenlegen könnten.

Denial of Service

Ein Denial-of-Service-Angriff (DoS) ist eine Form des Cyberangriffs, bei dem der Angreifer Ressourcen nutzt, um die Verfügbarkeit oder die Kosten des Systems zu stören, d.h. der Angreifer stellt die Frage: „Wie kann ich das System überlasten?“ Im Beispiel-DFD können sich Bedrohungen ergeben durch:

* + - die Überlastung des API-Brokers mit einem Netzwerk-DoS.
    - Erzeugung unnötiger Aufzeichnungen, um den Logspeicher zu füllen und unnötige Cloud-Ressourcen zu verbrauchen.

Threat Modeling

Elevation of Privilege

Als Elevation of Privilege wird ein Vorgang bezeichnet, bei dem ein System ausgenutzt wird, um einem/r bestimmten Benutzer:in oder einer Anwendung erweiterten Zugriff zu gewähren. Berechtigungen werden in der Regel durch die Aufhebung der Authentifizierung und Zugriffskontrolle oder durch die Unterbrechung und Beschädigung von Prozessen erweitert, d. h. der Angreifer stellt die Frage: „Was kann ich manipulieren, um mehr Rechte zu erhalten?“ Im Beispiel-DFD könnten Bedrohungen auftreten durch

* + die Ausnutzung von Schwachstellen in der Benutzerverwaltung, um Berechtigungen auszuweiten.
  + Ausbrechen aus dem Data-Worker-Ablauf zwecks Ausführung von beliebigem Code.

STRIDE-Varianten

STRIDE kann auf eine große Bandbreite an Bedrohungen angewandt werden und stellt eine wichtige Merkhilfe für die Modellierung von Bedrohungen dar. Die Grundvariante von STRIDE hat keine Einschränkungen bei der Identifikation von Bedrohungen, was für Bedrohungsanalysten und andere Stakeholder oftmals eine Herausforderung darstellt. Aufgrund dessen wurden mehrere STRIDE-Varianten entwickelt, die einen einfacheren Ansatz zum Threat Modeling bieten. Wir werden nun zwei dieser Varianten untersuchen: STRIDE-per-Element und STRIDE-per-Interaction

STRIDE-per-Element

STRIDE-per-Element folgt jedem Element im Datenflussdiagramm mit dem Fokus darauf, welche Bedrohungen für jedes Element vorherrschend sind. Die folgende Tabelle veranschaulicht die Entitäten, die durch die beschriebenen Angriffe unterwandert werden können. Das Fragezeichen in der Zeile des Datenspeichers weist darauf hin, dass Datenspeicher angegriffen werden können, wenn sie Protokolle speichern. Die Tabelle zeigt, dass die externe Entität Opfer von Spooﬁng werden kann, aber beispielsweise nicht von Denial-of-Service-Angriffen.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| STRIDE-per-Element | | | | | | |
|  | S | T | R | I | D | E |
| Externe Entität | X |  | X |  |  |  |
| Prozess | X | X | X | X | X | X |
| Datenfluss |  | X |  | X | X |  |
| Datenspeicher |  | X | ? | X | X |  |

Eine Schwachstelle von STRIDE-per-Element, wie in der Tabelle dargestellt, besteht darin, dass es keine vollständige Darstellung des Anwendungsfalles mit dem erforderlichen Geltungsbereich bietet. Dies lässt sich darauf zurückführen, dass STRIDE-per-Element von Microsoft entwickelt wurde und in erster Linie auf dessen Bedürfnisse ausgerichtet ist (Shostack, 2014). Die STRIDE-per-Element-Tabelle muss daher möglicherweise an die Bedürfnisse der Organisation angepasst werden.

STRIDE-per-Interaction

STRIDE-per-Interaction konzentriert sich auf die Interaktion zwischen Entitäten und weniger auf jedes einzelne Element. Dennoch ermitteln beide STRIDE-Varianten die gleiche Anzahl von Bedrohungen. STRIDE-per-Interaction verwendet ebenfalls eine Tabelle, um Bedrohungen für jede Interaktion zu identifizieren. Diese enthält die folgenden Zeilen:

* + - Referenznummer
    - Entität
    - Entitätsinteraktion
    - STRIDE-Bedrohungen für diese Interaktion

Die nachfolgende STRIDE-per-Interaction-Tabelle enthält Beispiele aus dem zuvor verwendeten DFD. Mit einem X werden potenzielle Bedrohungen den Interaktionen zugeordnet. Das folgende Beispiel verwendet nur die Entitäten Gateway, Data Worker und Log-Speicher.

Threat Modeling

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| STRIDE-per-Interaction | | | | | | | | |
|  | Element | Interaktion | S | T | R | I | D | E |
| 1 | Prozess (Gate­way) | Der Prozess sendet ausgehende Datenströme an eine externe Entität. |  |  | X |  |  |  |
| 2 |  | Der Prozess empfängt Daten von einer externen Entität. | X |  |  |  | X | X |
| 3 |  | Der Prozess sendet Daten an einen anderen Prozess (Data Worker). | X |  | X | X | X | X |
| 4 |  | Der Prozess empfängt Daten von einem anderen Prozess (Data Worker). | X |  | X |  | X | X |
| 5 | Prozess (Data Worker) | Der Prozess sendet Daten an einen anderen Prozess (Gateway). | X |  | X | X | X | X |
| 6 |  | Der Prozess empfängt Daten von einem anderen Prozess (Gateway). | X |  | X |  | X | X |
| 7 |  | Der Prozess sendet Daten an einen anderen Prozess (API-Broker). | X |  | X | X | X | X |
| 8 |  | Der Prozess empfängt Daten von einem anderen Prozess (API-Broker). | X |  | X |  | X | X |
| 9 |  | Der Prozess sendet Daten an einen Daten­speicher (Log-Speicher). | X |  |  | X |  |  |
| 10 | Daten­fluss (Gate­way/ extern) | Überschreitet die Umgebungsgrenze |  | X |  | X | X |  |
| 11 | Datenfluss (Gateway/ Data Worker) | Überschreitet die Umgebungsgrenze |  | X |  | X | X |  |
| 12 | Daten­speicher (Log-Speicher) | Der Datenspeicher hat einen ein­gehenden Da­tenfluss. |  | X | X | X | X |  |
| 13 | Externer Interaktor (externes System) | Der externe Interaktor wandelt Eingaben in Prozesse um. | X |  | X | X |  |  |
| 14 |  | Der externe Interaktor emp­fängt Eingaben von Prozessen. | X |  |  |  |  |  |

#### LINDDUN

LINDDUN ist eine Methode zur Modellierung von Datenschutzaspekten in einem System (DistriNet Research Group, 2020d). LINDDUN konzentriert sich auf die systematische Ermittlung und Minderung von Datenschutzbedrohungen in einem System. Ähnlich wie STRIDE ist auch LINDDUN eine Merkhilfe für die Kategorien der Datenschutzbedrohungen, die es unterstützt (Sion et al., 2018, S. 2).

|  |  |
| --- | --- |
| Linkability (Verknüpfbarkeit) | Ein Kontrahent ist in der Lage, zwei Objekte von Interesse miteinander zu verknüpfen, ohne die Identität der betroffenen Datensubjekte zu kennen. |
| Identiﬁability (Identifizierbarkeit) | Ein Kontrahent ist in der Lage, ein Datensubjekt aus einer Reihe von Datensubjekten anhand eines Objekts von Interesse zu identifizieren. |
| Non-repudiation (Nachweisbarkeit) | Das Datensubjekt ist nicht in der Lage, eine Behauptung zu leugnen (z. B. eine Aktion durchgeführt oder eine Anfrage gestellt zu haben). |
| Detectability (Erkennbarkeit) | Ein Kontrahent ist in der Lage festzustellen, ob ein Objekt von Interesse über ein Datensubjekt existiert, unabhängig davon, ob er den Inhalt lesen kann. |
| Disclosure of information (Offenlegung von Informationen) | Ein Kontrahent ist in der Lage, den Inhalt eines Objekts von Interesse über ein Datensubjekt zu erfahren. |
| Unawareness (Unkenntnis) | Das Datensubjekt hat keine Kenntnis von der Erhebung, Verarbeitung, Speicherung oder Weitergabe (und den entsprechenden Zwecken) seiner personenbezogenen Daten. |
| Non-compliance (Nichtkonformität) | Die Verarbeitung, Speicherung oder Handhabung personenbezogener Daten entspricht nicht den Gesetzen, Vorschriften und/oder Richtlinien. |

Threat Modeling

Unterschied zwischen der Modellierung von Datenschutz- und Sicherheitsbedrohungen

Items of interest (IOI)

Ein Objekt von Interesse (IOI) ist ein Datenelement, das durch das Datenschutzrecht geschützt ist und mit einer Person zusammenhängt.

Sicherheitsbedrohungsmodelle konzentrieren sich auf Assets und ihren Schutz vor (externen) Bedrohungen. Datenschutzbedrohungsmodelle verfolgen jedoch einen anderen Ansatz. Anstatt sich auf die Systemwerte zu konzentrieren, fokussieren sie sich auf die Daten des Datensubjekts, um die Objekte von Interesse („items of interest“, IOI) und nicht das System zu schützen. Die Privatsphäre der Nutzerinnen und Nutzer ist sowohl durch (externe) Angriffe als auch durch das System selbst gefährdet, wenn es sich falsch verhält.

Verwendung von LINDDUN zur Identifizierung von Bedrohungen

Mit LINDDUN lassen sich Bedrohungen umfassender modellieren als mit anderen Methoden wie STRIDE, das keine Datenschutzbedrohungen erfasst. Die LINDDUN-Methode besteht aus drei Hauptschritten:

1. Systemmodellierung (Modellierung des Systems und Erstellung eines DFD als Grundlage für die Bedrohungsermittlung)
2. Bedrohungsermittlung (Verwendung der LINDDUN-Mnemonik, um Bedrohungen zu identifizieren)
3. Bedrohungsmanagement (Finden von geeigneten Minderungsmaßnahmen für die gefundenen Bedrohungen)

Systemmodellierung

Der erste Schritt des LINDDUN-Threat-Modelings besteht darin, das System zu verstehen, um es zu analysieren. Hierfür wird wie bei STRIDE vorgegangen, d. h. ein DFD erstellt. Das DFD bietet dann die Grundlage für den Umfang der Analyse und der Bedrohungsidentifizierung.

Bedrohungsermittlung

Sobald das DFD erstellt wurde, müssen die Bedrohungen identifiziert werden. Ähnlich wie bei STRIDE bietet auch LINDDUN eine Tabelle, um die potenziellen Bedrohungen den einzelnen DFD-Elementen zuzuordnen (in der nachfolgenden Tabelle mit X markiert).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| LINDDUN Bedrohungen für jedes Element | | | | | | | |
|  | L | I | N | D | D | U | N |
| Externe Entität | X | X |  |  |  | X |  |
| Prozess | X | X | X | X | X |  | X |
| Datenfluss | X | X | X | X | X |  | X |
| Datenspeicher | X | X | X | X | X |  | X |

Einwirkungsaktionen

(Impact

actions)

Eine Aktion, die die Situation verbessert [+] oder verschlechtert [-], ist eine Einwirkungsaktion.

Anhand der Tabelle können Analysten nun feststellen, ob diese eine Bedrohung für das DFD-Element darstellen. LINDDUN bietet auch einen nach Bedrohungskategorien strukturierten Katalog von Bedrohungsbäumen, der die verbreitetsten Angriffspfade für die einzelnen Bedrohungskategorien und die jeweilige Verbindung zu jedem DFD-Element enthält. Die folgende Tabelle veranschaulicht die Folgen und die vom LINDDUN-Framework für jede Bedrohung deﬁnierten Einwirkungsaktionen. Die Informationen in den folgenden Tabellen können auf der LINDDUN-Website abgerufen werden.

Threat Modeling

|  |  |
| --- | --- |
| Linkability (Verknüpfbarkeit) | |
| Folgen | * „Kann zu Identifizierbarkeit führen (siehe Identifizierbarkeitsbäume), wenn zu viele verknüpfbare Informationen kombiniert werden“ * „Kann zu Rückschlüssen führen: Wenn „Gruppendaten“ verknüpfbar sind, kann dies zu gesellschaftlichen Schäden wie Diskriminierung führen“ |
| Beeinflusst durch | + „Datenminimierung: Je weniger Informationen verfügbar sind, desto besser“  - „Identifizierbarkeit: Wenn die Identität des Subjekts bekannt ist, können alle damit zusammenhängenden Daten eindeutig verknüpft werden“ (DistriNet Research Group, 2020e) |

|  |  |
| --- | --- |
| Identifiability (Identifizierbarkeit) | |
| Folgen | * „Kann zu schweren Datenschutzverletzungen führen (wenn Subjekt annimmt, dass es anonym ist)“ |
| Beeinflusst durch | + „Datenminimierung: Je weniger Infos verfügbar sind, desto besser“  - Verknüpfbarkeit: „Je mehr Informationen verknüpft sind, desto höher ist die Wahrscheinlichkeit, dass die kombinierten Daten identifizierbar sind (je mehr Attribute bekannt sein, desto kleiner ist die Anonymitätsmenge)“ (DistriNet Research Group, 2020c) |

|  |  |
| --- | --- |
| Non-Repudiation (Nachweisbarkeit) | |
| Folgen | * „Verantwortlichkeit: Wenn eine Person nicht in der Lage ist, eine Handlung oder Information zu widerlegen, kann sie zur Rechenschaft gezogen werden.“ |
| Beeinflusst durch | - „Identifizierbarkeit: Wenn Daten identifizierbar sein, ist es schwer, sie zu widerlegen“  (DistriNet Research Group, 2020g) |

|  |  |
| --- | --- |
| Detectability (Erkennbarkeit) | |
| Folgen | * „Inferenz: Durch die Feststellung, ob ein Objekt von Interesse existiert, kann man auf gewisse Informationen schließen, selbst ohne tatsächlich hierzu Zugang zu haben“ (DistriNet Research Group, 2020a) |
| Beeinflusst durch |  |

|  |  |
| --- | --- |
| Disclosure of Information (Offenlegung von Informationen) | |
| Folgen | * Kann zu schweren Datenschutz­verletzungen führen (wenn persön­liche Daten an die Öffentlichkeit gelangen) |
| Beeinflusst durch | + Wenn das System gut gesichert ist, ist es schwieriger, Daten zu leaken (DistriNet Research Group, 2020b) |

|  |  |
| --- | --- |
| Unawareness (Unkenntnis) | |
| Folgen | * „Verknüpfbarkeit/Identifizierbarkeit: je mehr Informationen verfügbar sein, desto leichter können sie verknüpft (und identifiziert) werden“ (DistriNet Research Group, 2020h) |
| Beeinflusst durch |  |

|  |  |
| --- | --- |
| Non-Compliance (Nichtkonformität) | |
| Folgen | * Kann zu Geldbußen führen (bei Verletzungen des Gesetzes oder der mitgeteilten Unternehmensrichtlinien)“ * Kann zu Verlust an Image und Glaubwürdigkeit etc. führen“ |
| Beeinflusst durch | + „Sicherheitsbeauftragter/ Rechtsaudit/ […]: eine Person, die für die Compliance des Systems verantwortlich ist“  - „Manipulation des Richtlinien­datenspeichers: Wenn die Richt­liniendatenbank nicht manipulationssicher ist, können Angreifer die Zugangs­kontrollrichtlinien und Nutzereinwilligungen des Systems ändern“ (DistriNet Research Group, 2020f) |

Threat Modeling

Jede identifizierte Bedrohung muss in den vom Framework bereitgestellten Attack-Trees dokumentiert werden. Auch andere Tools, z. B. Datenbanken, können hierfür verwendet werden.

Bedrohungsmanagement

Sobald alle Bedrohungen identifiziert wurden, müssen sie bewertet und priorisiert werden. LINDDUN bietet kein spezielles Risikobewertungsmodell zur Bewertung von Bedrohungen. Die Risikobewertungsmethode des Open Web Application Security Project (OWASP) kann genutzt werden, um das Risiko jeder Bedrohung zu bewerten, wobei es möglicherweise an Datenschutzbedrohungen angepasst werden muss. Sobald die Risiken bewertet und priorisiert wurden, können Minderungsmaßnahmen geplant werden. LINDDUN bietet eine Reihe von Minderungsstrategien und -lösungen.

Das System bietet zwei Strategien zur Risikominderung. Die erste Strategie ist der proaktive Ansatz, bei dem die Zuordnungen zwischen Benutzern und ihren Aktionen und persönlichen Informationen überprüft werden, um sicherzustellen, dass die Benutzer:innen so wenige Informationen wie möglich mit dem System teilen. Dies folgt dem Grundsatz, dass „nicht geteilte Daten nicht bedroht sein können“.

Die zweite Risikominderungsstrategie ist reaktiv. Die Daten werden hierbei geschützt, indem die Zuordnung von Daten zu Einzelpersonen nach ihrer Offenlegung auf ein Minimum beschränkt werden, indem

* + unnötige Daten entfernt werden,
  + Daten durch nicht verknüpfbare Objekte ersetzt werden,
  + Daten generalisiert werden und
  + Verbindungen zwischen Objekten von Interesse verborgen werden.

Objekte von Interesse (IOIs) können sowohl auf Datenebene als auch auf technischer oder Systemebene geschützt werden. Dies unterstreicht die enge Verbindung zwischen Datenschutz und Systemsicherheit, denn Daten können ohne ein sicheres System nicht geschützt werden.

Zusammenfassung

### Das Threat Modeling wird dazu eingesetzt, Bedrohungen für Assets in einem bestimmten Bereich zu ermitteln. Für die Modellierung von Bedrohungen können verschiedene Tools und Verfahren verwendet werden.

Eines davon, der Attack-Tree, ist eine ausführliche Methode zur hierarchischen Darstellung von Bedrohungen und zur Bestimmung der Eintrittswahrscheinlichkeit erfolgreicher Angriffe. Ein Attack-Tree besteht aus einem Wurzelknoten, der das Ziel des Angreifers beschreibt. Die Unterknoten des Wurzelknotens untergliedern das Ziel des Angreifers weiter in Teilziele. Verschiedene Konjunktionen können verwendet werden, um Kindknoten mit ihren Eltern zu verbinden. Der Attack-Tree kann als Liste mit Indizes oder als Graph dargestellt werden. Er kann auch durch das Hinzufügen von Verteidigungsknoten erweitert werden, um einen Attack-Defense-Tree aufzubauen, der Verteidigungsmaßnahmen enthält, die zur Minderung von Angriffen ergriffen werden können.

Eine weitere Methode des Threat Modelings ist STRIDE, benannt nach den Anfangsbuchstaben der folgenden Bedrohungskategorien: Spooﬁng, Tampering, Repudiation, Information Disclosure, Denial of Service und Elevation of Privileges. Der STRIDE-Ansatz verwendet Datenflussdiagramme (DFDs), um Bedrohungen zu identifizieren. DFDs stellen den logischen Datenfluss im Anwendungsbereich dar. Analysten verwenden DFDs, um Bedrohungen für jede Entität zu identifizieren und sie anschließend den STRIDE-Bedrohungskategorien zuzuordnen.

Das LINDDUN-Framework kann zur Modellierung von Datenschutzbedrohungen verwendet werden. Auch LINDDUN ist nach den Anfangsbuchstaben der Bedrohungskategorien für den Datenschutz benannt: Linkability, Identiﬁability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness und Non-Compliance.

Bei dieser Methode werden ebenfalls DFDs zur Ermittlung von Bedrohungen eingesetzt. Darüber hinaus bietet LINDDUN eine Reihe von Strategien und Lösungen zur Eindämmung der ermittelten Bedrohungen.

# Lektion 4

## Standardisierung und Compliance

##### LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie in der Lage sein, …

… den Prozess des NIST-Risikomanagement-Frameworks zu beschreiben.

… den Inhalt der ISO/IEC 27005 zu verstehen.

… die Ziele des BSI-Standards 100-3 zu erläutern.

DL-E-DLMCSECRAM01\_E-U04

### Standardisierung und Compliance

#### Einführung

Entscheidungsträger benötigen ein wiederholbares und standardisiertes Framework, auf das sie sich verlassen können. Die Standardisierung bietet ein einheitliches Konzept für Produkte und Prozesse. Das Konzept der Standardisierung begegnet uns in der modernen Welt täglich. Standardisierte Objekte und Vorschriften sind überall um uns herum zu finden, z. B. Steckdosen und Verkehrsregeln. Sie tragen dazu bei, unser Leben leichter zu gestalten. Auch im IT-Bereich gibt es eine Reihe von Risikomanagement- und Risikobewertungsstandards, welche die notwendigen Prozesse und Maßnahmen festlegen, die eine Organisation zur Einhaltung der jeweiligen Standards ergreifen muss. Die meisten Standards bieten einen Gesamtüberblick und definieren die generellen Prozesse, die von Organisationen in Übereinstimmung mit dem Standard umgesetzt werden müssen. Drei der gängigsten Standards sind ISO/IEC 27005, NIST SP 800-37 und in Deutschland der BSI-Standard 100-3.

#### Das NIST Risikomanagement-Framework

NIST

Das National Institute of Standards and Technology (NIST) ist eine nicht-regulatorische Behörde des US-amerikanischen Handelsministeriums. Diese Behörde stellt öffentliche Standards und Richtlinien bereit (z.B. für die Cybersicherheit).

Die Sonderveröffentlichung SP (Special Publication) 800-37 des National Institute of Standards and Technology (NIST) bietet ein Risikomanagement-Framework für Informationssysteme und Organisationen. Die aktuelle Version dieses Frameworks, Revision 2, wurde im Jahr 2018 veröffentlicht (NIST, 2018). Die Veröffentlichung wurde mit dem Ziel entwickelt, einen praktischen Leitfaden für das Risikomanagement in Organisationen zur Verfügung zu stellen. Sie enthält umfassende Informationen darüber, wie ein Risikomanagement-Framework (RMF) anzuwenden ist, und untersucht Risikomanagementverfahren. Die folgenden Abschnitte geben einen Überblick über das Dokument NIST SP 800-37.

Grundlagen

In diesem Abschnitt werden die grundlegenden Konzepte des Risikomanagements für Cybersicherheit und Datenschutz beschrieben, wobei der Schwerpunkt auf den folgenden Themen liegt (NIST, 2018, Table of Contents):

* Organisationsweites Risikomanagement
* Schritte und Struktur des Risikomanagement-Frameworks,
* Informationssicherheit und Datenschutz im RMF,
* System und Systemelemente,
* Berechtigungsgrenzen,
* Anforderungen und Maßnahmen
* Sicherheits- und Datenschutzstatus und
* Supply-Chain-Risikomanagement.

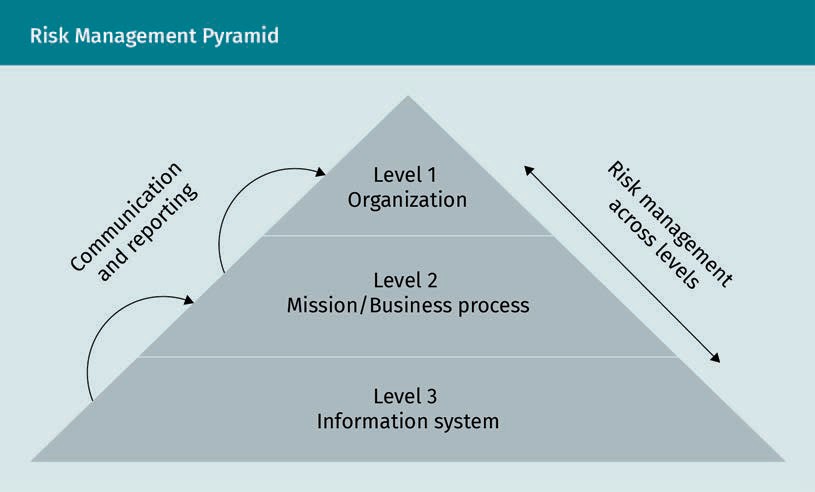
Organisationsweites Risikomanagement

Risikomanagement stellt eine organisationsweite Aufgabe dar. Es beginnt auf der höchsten Ebene einer Organisation und reicht hinunter bis zur Systementwicklung. Der Risikomanagementprozess kann in drei Ebenen unterteilt werden:

Standardization and Compliance

1. Organisation. Die Organisationsebene stellt die höchste Ebene dar. Auf dieser Ebene werden die organisationsweiten Risikomanagementprozesse verwaltet.
2. Mission/Geschäftsprozess. Die auf dieser Ebene durchgeführten Aktivitäten beziehen sich nicht auf technische Risiken, sondern konzentrieren sich auf das Management von Produkt- oder Projektrisiken.
3. Informationssystem. Diese Ebene befasst sich mit Risiken aus der Perspektive des Informationssystems, wobei der Schwerpunkt auf den technischen und organisatorischen Risiken liegt, denen ein Informationssystem ausgesetzt ist.

Alle drei Ebenen sind miteinander verbunden; Risiken werden zwischen ihnen kommuniziert und berichtet und das Risikomanagement erfolgt auf allen Ebenen.



Die Aktivitäten auf Ebene 3 beruhen auf den Vorbereitungsaktivitäten der Ebenen 1 und 2. Ohne eine organisationsweite Risikomanagementstrategie ist das Risikomanagement auf der Informationssystemebene für die Organisation nicht sehr nützlich. Risikomanagement ist keine isolierte Aktivität und erfordert die Zusammenarbeit auf allen Ebenen.

Die Sonderveröffentlichung NIST SP 800-37 führt drei Aktivitäten der Ebenen 1 und 2 auf, die die Organisation auf die Durchführung des RMF vorbereiten (NIST, 2018, S. 7):

* + „Zuweisung von Rollen und Verantwortlichkeiten für organisatorische Risikomanagementverfahren“
  + „Festlegung einer Risikomanagementstrategie und einer organisatorischen Risikotoleranz“
  + „Identifizierung der Geschäftszwecke, Geschäftsfunktionen und Mission/Geschäftsverfahren, die das Informationssystem unterstützen soll“
  + „Identifizierung der wichtigsten Stakeholder (innerhalb und außerhalb der Organisation), die ein Interesse am Informationssystem haben“
  + „Identifizierung und Priorisierung der Assets (einschließlich Informations-Assets)“

Schritte und Struktur des Risikomanagement-Frameworks

Ein Management-Framework verlangt nach einem festgelegten Prozess, um messbare Ergebnisse zu erzielen. NIST SP 800-37 deﬁniert sieben Schritte für den Risikomanagementprozess (NIST, 2018, S. 8- 9):

* 1. „Bereiten Sie sich darauf vor, das RMF aus einer Organisations- und einer Systemperspektive auszuführen, indem Sie einen Kontext und Prioritäten für das Management der Sicherheits- und Datenschutzrisiken schaffen.“
  2. „Kategorisieren Sie das System und die vom System verarbeiteten, gespeicherten und übertragenen Informationen auf der Grundlage einer Analyse der Auswirkungen eines Verlusts.“
  3. „Wählen Sie einen ersten Maßnahmensatz für das System aus und passen Sie die Maßnahmen nach Bedarf an, um das Risiko auf der Grundlage einer Risikobewertung auf ein akzeptables Niveau zu reduzieren.“
  4. „Führen Sie die Maßnahmen durch und beschreiben Sie, wie die Maßnahmen innerhalb des Systems und seiner Betriebsumgebung angewandt werden.“
  5. „Bewerten Sie die Maßnahmen, um zu entscheiden, ob diese korrekt durchgeführt werden, wie beabsichtigt funktionieren und die erwünschten Ergebnisse in Bezug auf die Erfüllung der Sicherheits- und Datenschutzanforderungen liefern.“
  6. „Genehmigen Sie das System oder die gemeinsamen Maßnahmen auf Grundlage der Feststellung, dass das Risiko für den Betrieb und die Assets der Organisation, für Einzelpersonen, andere Organisationen und die Nation akzeptabel ist.“
  7. „Überwachen Sie das System und die zugehörigen Maßnahmen fortlaufend, um die Wirksamkeit der Maßnahmen zu bewerten, Änderungen am System und an der Betriebsumgebung zu dokumentieren, Risikobewertungen und Auswirkungsanalysen durchzuführen und über die Sicherheits- und Datenschutzlage des Systems zu berichten.“

Informationssicherheit und Datenschutz im RMF

Maßnahmen zum Schutz der Privatsphäre und zur Informationssicherheit stehen oft im Widerspruch zueinander. So muss beispielsweise die Dauer der Datenaufbewahrung so kurz wie möglich gehalten werden, um die Privatsphäre der Log-Daten zu schützen, während die Informationssicherheit wiederum eine möglichst lange Speicherung erfordert. Eine Organisation muss ein Risikomanagement einführen, um sicherzustellen, dass beide Aspekte den einschlägigen Anforderungen entsprechen.

Das Risikomanagement-Framework des NIST SP 800-37 ist sowohl auf Sicherheits- als auch auf Datenschutzrisiken anwendbar. Dennoch muss eine Organisation die Erfordernisse beider Aspekte und ihr Verhältnis zueinander verstehen.

SDLC

Der Softwareentwicklungszyklus (Software Development Life Cycle, SDLC) definiert Prozesse zur Verwaltung des Lebenszyklus der Softwareentwicklung.

.

System und Systemelemente

Informationssysteme lassen sich in Systeme und Systemelemente untergliedern. ISO 15288 definiert ein System als eine Reihe von interagierenden Elementen, die so aufgebaut sind, dass sie einen oder mehrere angegebene Zwecke erfüllen (ISO/IEC/IEEE, 2015). Jedes dieser Systeme hat spezifische Fähigkeiten und Anforderungen, die von den Systemelementen erfüllt werden. Das RMF stellt sicher, dass die Anforderungen an Sicherheit und Datenschutz während des gesamten Softwareentwicklungszyklus von Informationssystemen durch die Ermittlung der Risiken für jedes System erfüllt werden.

Standardization and Compliance

Berechtigungsgrenzen

Berechtigungsgrenzen legen den Schutzbereich für ein Informationssystem fest. Gruppen von Systemelementen, die als Berechtigungsgrenzen deﬁniert sind, können direkt von einem System verwaltet werden, da die in der Berechtigungsgrenze enthaltenen Elemente im Allgemeinen ähnliche Risiken beinhalten. Die Berechtigungsgrenzen werden durch den Umfang der Systeme bestimmt. Laut NIST SP 800-37 sollten Systemelemente innerhalb der gleichen Berechtigungsgrenze folgende Merkmale aufweisen (NIST, 2018, S. 17):

* + „die gleichen Missions- oder Geschäftsfunktionen unterstützen“
  + „ähnliche Betriebseigenschaften und Sicherheits- und Datenschutzanforderungen haben“
  + „ähnliche Arten von Informationen verarbeiten, speichern und übertragen“
  + „sich in der gleichen Betriebsumgebung befinden“

Anforderungen und Maßnahmen

Anforderungen und Maßnahmen sind entscheidend für das Risikomanagement, was das Verständnis der Sicherheits- und Datenschutzanforderungen für Informationssysteme angeht. Zu den Anforderungen gehören Vorschriften oder Gesetze, die zu befolgen sind (z.B. DSGVO) und Richtlinien über den Schutz von Assets und Systemen. Maßnahmen hingegen beziehen sich auf Sicherheits- und Schutzmechanismen, die umgesetzt werden können, um die Sicherheits- und Datenschutzziele einer Organisation zu erreichen.

Sicherheits- und Datenschutzstatus

Das Ziel des RMF ist es, die befugten Stellen mit genauen Informationen über den Sicherheits- und Datenschutzstatus der Informationssysteme der Organisation zu versorgen, um risikobasierte Entscheidungen zu erleichtern. Daher muss der Sicherheits- und Datenschutzstatus den Status des Informationssystems beschreiben, den Umgang mit erkannten Risiken skizzieren und definieren, wie die Organisation auf Veränderungen innerhalb der Organisation oder Systeme reagieren wird.

Supply-Chain-Risikomanagement

Angesichts der stetig zunehmenden Angriffe auf Lieferketten und/oder Bedrohungen der Lieferkette, wie etwa die Blockade des Suezkanals im Jahr 2021, wird das Management dieser Risiken immer wichtiger. Daher stellen die Sicherheitsvorkehrungen der Lieferanten einen Schlüsselaspekt des Risikomanagements dar. Die Strategie des Supply-Chain-Risikomanagements (SCRM) muss alle potenziellen Risiken abdecken, die sich auf die Organisation auswirken könnten.

Prozess

Die NIST-RMF-Aufgaben können zeitgleich mit den Prozessen des Softwareentwicklungszyklus durchgeführt werden, da die jeweiligen Managementrollen und Prozessschritte ähnlich sind. Die gleichzeitige Durchführung von RMF-Aufgaben und SDLC-Prozessen trägt dazu bei, die Effizienz in Bezug auf das Management von Sicherheits- und Datenschutzrisiken zu optimieren. Zudem können die für das RMF erforderlichen Ergebnisse wie Risikobewertungen, Pläne zur Risikominderung und Datenschutzkonzepte aus dem SDLC-Prozess gewonnen werden. Weitere Informationen über den gesamten Prozess sind in NIST SP 800-37 zu finden.

#### ISO/IEC 27005

ISO/IEC 27005 ist ein von der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) veröffentlichter Standard für das Risikomanagement von Informationssicherheit. Sein offizieller Name lautet „Management von Informationssicherheitsrisiken“. Er ist ein Kernbestandteil der ISO/IEC 27000-Reihe, die gemeinhin als ISO27k bezeichnet wird. Die aktuelle Version dieser Norm ist die dritte Version, die im Jahr 2018 veröffentlicht wurde (ISO/IEC, 2018).

ISO/IEC 27005 führt die folgenden Ziele auf, die Risikomanagementprozesse erreichen müssen (ISO/IEC, 2008, S. 4):

* + - „Risiken werden erkannt“
    - „Risiken werden im Hinblick auf ihre Folgen für die Organisation und die Wahrscheinlichkeit ihres Eintretens bewertet“
    - „die Eintrittswahrscheinlichkeit und Folgen dieser Risiken werden kommuniziert und verstanden“
    - „eine Rangfolge für die Risikobehandlung wird festgelegt“
    - „Maßnahmen, die den Eintritt des Risikos vermindern, werden priorisiert“
    - „Beteiligte werden in Entscheidungen zum Risikomanagement einbezogen und über den Stand des Risikomanagements auf dem Laufenden gehalten“
    - „die Wirksamkeit der Risikobehandlung wird überprüft“
    - „die Risiken und der Risikomanagementprozess werden regelmäßig kontrolliert und überarbeitet“
    - „Informationen werden erfasst, um den Ansatz des Risikomanagements zu verbessern“
    - „Manager:in und Personal werden über die Risiken und die Maßnahmen zu ihrer Minderung aufgeklärt“

Maßnahmen des Sicherheitsrisikomanagements

Um die festgelegten Ziele zu erreichen, unterteilt ISO/IEC 27005 die Maßnahmen des Sicherheitsrisikomanagements in sechs Aufgaben (ISO/IEC, 2008, S. 3):

1. „Ermittlung des Kontexts“
2. „Risikobewertung“
3. „Risikobehandlung“
4. „Risikoakzeptanz“
5. „Risikokommunikation“
6. „Risikoüberwachung und -überprüfung“

Da das Risikomanagement in ein Informationssicherheitsmanagement­system (ISMS) integriert werden muss, können die Aktivitäten wie folgt auf den Plan-Do-Check-Act-Zyklus (PDCA) eines ISMS abgestimmt werden.

Standardization and Compliance

|  |  |
| --- | --- |
| Abgleich von ISMS und Informationssicherheits-Risikomanagementprozessen | |
| ISMS-Prozess | Informationssicherheit-Risikomanagementprozess |
| Plan | * Festlegung des Kontexts * Risiko-Assessment * Entwicklung eines Risikomanagementplans * Risikoakzeptanz |
| Do | * Umsetzung des Risikomanagementplans |
| Check | * Kontinuierliche Überwachung und Überprüfung von Risiken |
| Act | * Aufrechterhaltung und Verbesserung des Informationssicherheits-Risikomanagementprozesses (ISO/IEC, 2018) |

Ermittlung des Kontexts

Das erste Ziel des Standards besteht darin, den Kontext des Informationssicherheits-Risikomanagements zu ermitteln. Dazu gehören die Festlegung der grundlegenden Kriterien für diesen Prozess, die Bestimmung des Geltungsbereichs und die Einrichtung einer Organisation, die den Risikomanagementprozess durchführt. Zu den grundlegenden Kriterien für diesen Prozess gehören die Bewertung des Risikos, die Bestimmung der Auswirkungen bestimmter Risiken und die Festlegung des Risikoniveaus, das die Organisation zu akzeptieren bereit ist, d. h. die Risikobewertungskriterien, Auswirkungskriterien und Risikoakzeptanzkriterien. Die Festlegung des Geltungsbereichs bezieht sich auf die Bestimmung des Geltungsbereichs und der Grenzen des Informationssicherheits-Risikomanagementansatzes. Diese Aspekte müssen definiert werden, um sicherzustellen, dass alle relevanten Assets bei der Risikobewertung berücksichtigt werden.

Risikobewertung

Der Risikobewertungsprozess legt fest, wie Risiken beurteilt werden sollten. ISO/IEC 27005 spezifiziert dazu die folgenden Schritte:

* + Bei der Risikoidentifikation werden potenzielle Risiken für die Organisation im Hinblick auf mögliche Verluste gefunden und eingestuft. Dazu gehören die folgenden Schritte (ISO/IEC, 2008, S. 10—14):

Informationssicherheitsmanagement­system Ein ISMS ist ein System aus Richtlinien und Verfahren zum Verwalten von sicherheitsrelevanten Assets.

* + „Identifikation von Assets“
  + „Identifikation von Bedrohungen“
  + „Identifikation bestehender Maßnahmen“
  + „Identifikation von Schwachstellen“
  + „Identifikation der Folgen“
* Eine Risikoanalyse ist erforderlich, um Aktionen und Maßnahmen zur Risikominderung für eine Organisation zu planen und zu bewerten. Die folgenden Schritte dienen der Beurteilung von identiﬁzierten Risiken (ISO/IEC, 2008, S. 14-15):
  + „Einschätzung der Folgen“
  + „Einschätzung der Häufigkeit des Vorfalls“
* Die Risikobewertung umfasst den Vergleich des Risikoniveaus mit den im Rahmen der Kontextermittlung festgelegten Akzeptanzkriterien.

Risikobehandlung

Nach der Identifikation und Bewertung kann mit einem Risiko auf vielfältige Weise umgegangen werden. Die folgenden Möglichkeiten werden in ISO/IEC 27005 spezifiziert:

* Risikominderung. Das Risikoniveau sollte durch die Auswahl von Maßnahmen so weit reduziert werden, dass das Restrisiko wiederum als akzeptabel eingestuft werden kann.
* Risikoakzeptanz. Die Entscheidung, das Risiko ohne weitere Maßnahmen zu akzeptieren, sollte in Abhängigkeit von der Risikobewertung getroffen werden.
* Risikovermeidung. Die Tätigkeit oder Bedingung, die das betreffende Risiko auslöst, sollte vermieden werden.
* Risikoübertragung. Abhängig von der Risikobewertung sollte das Risiko auf Dritte übertragen werden, die das betreffende Risiko effizienter managen können.

Risikoakzeptanz

Nachdem die ermittelten Risiken mit den gewünschten Minderungsmaßnahmen behandelt wurden, muss eine formale Entscheidung erfolgen, ob das Restrisiko von der Organisation akzeptiert werden kann, und diese muss dokumentiert werden.

Risikokommunikation

Da Risiken ein zentraler Bestandteil der Entscheidungsfindung in Organisationen sind, ist es wichtig, dass sie zwischen den Entscheidungsträgern und den Beteiligten kommuniziert werden. ISO/IEC 27005 führt für diese Kommunikationsanforderung eine Reihe von Gründen auf (ISO/IEC, 2008, S. 22):

* „um Gewissheit für das Ergebnis des Risikomanagements der Organisation zu erlangen“
* „um Risikoinformationen zu sammeln“
* „um die Ergebnisse der Risikobewertung zu übermitteln und den Risikobedrohungsplan vorzustellen“
* „um das Auftreten und die Folgen von Verstößen gegen die Informationssicherheit, die auf einem mangelnden gegenseitigen Verständnis der Entscheidungsträger und Beteiligten beruhen, zu vermeiden oder zu reduzieren“
* „um die Entscheidungsfindung zu verbessern“
* „um neue Kenntnisse über die Informationssicherheit zu gewinnen“
* „um sich mit anderen Parteien zu koordinieren und Reaktionen zur Verringerung der Folgen eines Vorfalls zu planen“
* „um Entscheidungsträgern und Beteiligten ein Gefühl der Verantwortlichkeit für die Risiken zu vermitteln“
* „um das Bewusstsein zu schärfen“

Standardization and Compliance

Risikoüberwachung und -überprüfung

Das Risikomanagement ist niemals abgeschlossen, denn es handelt sich dabei um einen andauernden Prozess, der die fortlaufende Überwachung und Überprüfung der Systeme und Risiken erfordert. ISO/IEC 27005 legt fest, dass nach jeder der folgenden Systemänderungen eine Risikoüberprüfung durchgeführt werden muss (ISO/IEC, 2008, S. 22-23):

* + „Aufnahme neuer Assets in den Bereich des Risikomanagements“
  + „erforderliche Modifikation von Assets, z. B. aufgrund geänderter Geschäftsanforderungen“
  + „neue Bedrohungen, die sowohl außerhalb als auch innerhalb der Organisation auftreten könnten und noch nicht bewertet wurden“
  + „die Möglichkeit, dass neue oder schwerwiegendere Schwachstellen es den Bedrohungen möglich machen könnten, diese neuen oder veränderten Schwachstellen auszunutzen“
  + „identiﬁzierte Schwachstellen, um diejenigen zu ermitteln, die neuen oder wiederholt auftretenden Bedrohungen ausgesetzt sind“
  + „erhöhte Auswirkungen oder Folgen der bewerteten Bedrohungen, Schwachstellen und Risiken, die in ihrer Gesamtheit zu einem inakzeptablen Risikoniveau führen“
  + „Vorfälle in Bezug auf die Informationssicherheit“

#### BSI-Standard 100-3

Beim BSI-Standard 100-3 handelt sich um einen deutschen Standard, der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) publiziert wird. Er ist Teil des vom BSI herausgegebenen ganzheitlichen Ansatzes eines IT-Grundschutzes zur Informationssicherheit. IT-Grundschutz-Standards helfen privaten und öffentlichen Organisationen dabei, IT-Risiken zu minimieren. Ferner verlangen bestimmte öffentliche Ausschreibungen die Einhaltung des IT-Grundschutzes als Voraussetzung für die Angebotsabgabe. Der BSI-Standard 100-3 beschreibt, wie eine Risikoanalyse auf der Grundlage von IT-Grundschutz-Standards durchgeführt werden kann (BSI, 2008). Das Dokument ist in sieben Abschnitte gegliedert (BSI, 2008, S. 3):

1. Vorarbeiten
2. Erstellung der Gefährdungsübersicht
3. Ermittlung zusätzlicher Gefährdungen
4. Behandlung von Risiken
5. Gefährdungsbewertung
6. Konsolidierung des IT-Sicherheitskonzepts
7. Rückführung in den IT-Sicherheitsprozess

Vorarbeiten

Der erste Abschnitt beschreibt die Arbeit, die vor einer Risikobewertung abgeschlossen sein muss. Gemäß dem Standard gibt es die folgenden Schritte (BSI, 2008, S. 7):

* + „Ein systematischer IT-Sicherheitsprozess muss initiiert worden sein.“
  + „Ein Rahmen für das Sicherheitskonzept muss festgelegt worden sein.“
  + „Für den IT-Verbund muss eine Strukturanalyse durchgeführt worden sein.“
  + „Eine Schutzbedarfsfeststellung muss durchgeführt worden sein.“
  + „Es muss eine Modellierung durchgeführt worden sein.“
  + „Vor der Sicherheitsanalyse muss ein Basissicherheitscheck durchgeführt werden.“
  + „Es muss eine ergänzende Sicherheitsanalyse durchgeführt worden sein.“

Erstellung der Gefährdungsübersicht

Um sich einen Überblick über die Bedrohungen zu verschaffen, sehen sich Entscheidungsträger zunächst die Gefährdungsübersicht an. Dementsprechend muss diese informativ sein und einen Überblick über den Sicherheitsstatus des untersuchten Systems bieten. Der Standard enthält die nötigen Arbeitsschritte zur Erstellung einer Gefährdungsübersicht.

Ermittlung zusätzlicher Gefährdungen

Das IT-Grundschutz-Modell enthält eine festgelegte Menge von Gefährdungen für Systeme. Unter bestimmten Umständen können jedoch zusätzliche isolierte Bedrohungen für ein System auftreten, die über die im IT-Grundschutz-Modell aufgeführten Gefährdungen hinausgehen. Auch diese Gefährdungen müssen analysiert werden.

Der BSI-Standard 100-3 nennt eine Reihe von Fragen, die bei der Ermittlung zusätzlicher Gefährdungen berücksichtigt werden sollten (BSI, 2008, D. 12-13):

* + - „Welche möglichen Ereignisse aus dem Bereich *höhere Gewalt* stellen besondere Bedrohungen für den IT-Bereich dar?“
    - „Welche organisatorischen Mängel müssen vermieden werden […], um die Informationssicherheit zu gewährleisten?“
    - „Welche menschlichen Fehlhandlungen beeinträchtigen die Sicherheit der Informationen und Anwendungen?“
    - „Welche speziellen Sicherheitsprobleme können beim jeweils betrachteten Zielobjekt durch technisches Versagen entstehen?“
    - „Welche besondere Gefahr droht durch vorsätzliche Angriffe von Außentätern?“
    - „Wie können Innentäter durch vorsätzliche Handlungen den ordnungsgemäßen, sicheren Betrieb des zu prüfenden Zielobjekts beeinträchtigen?“
    - „Gibt es Objekte außerhalb des zu untersuchenden IT-Bereichs, die besondere Bedrohungen darstellen?“

Gefährdungsbewertung

Der BSI-Standard 100-3 beschreibt die Prüfung, ob die bereits umgesetzten oder im Sicherheitskonzept vorgesehenen Maßnahmen, in der Regel Standard-Sicherheitsmaßnahmen aus den IT-Grundschutz-Katalogen, für jede Bedrohung einen ausreichenden Schutz bieten oder ob es Lücken gibt. Der Standard definiert die folgenden Prüfkriterien (BSI, 2008, S. 15):

Standardization and Compliance

* + „Vollständigkeit. Bieten die Standard-Sicherheitsmaßnahmen Schutz gegen alle Aspekte der jeweiligen Gefährdung?“
  + „Mechanismenstärke. Wirken die in den Standard-Sicherheitsmaßnahmen empfohlenen Schutzmechanismen der jeweiligen Gefährdung ausreichend stark entgegen?“
  + „Zuverlässigkeit. Wie schwer ist es, die vorgesehenen Sicherheitsmechanismen zu umgehen?“

Handling Risks

In der Regel werden bei der Gefährdungsbewertung eine Reihe von Risiken identiﬁziert, denen die Sicherheitsmaßnahmen aus den IT-Grundschutz-Katalogen nicht ausreichend entgegenwirken. Der Standard sieht für den Umgang mit einem Risiko die folgenden Strategien vor (BSI, 2008):

* + Risikoreduktion durch weitere Sicherheitsmaßnahmen
  + Risikovermeidung durch Umstrukturierung
  + Risikoübernahme
  + Risikotransfer

Konsolidierung des Sicherheitskonzepts

Falls zu den Standard-Sicherheitsmaßnahmen zusätzliche Maßnahmen hinzugefügt wurden, muss das Sicherheitskonzept konsolidiert werden. Darüber hinaus müssen alle Risiken im Sicherheitskonzept dokumentiert werden, zusammen mit der Risikobehandlungsstrategie. Der Standard enthält die folgenden Kriterien für die Konsolidierung des Sicherheitskonzepts (BSI, 2008, S. 21):

* + „Ungeeignete Sicherheitsmaßnahmen sollten verworfen und nach eingehender Analyse durch wirksame Maßnahmen ersetzt werden.“
  + „Widersprüche oder Inkonsistenzen bei den Sicherheitsmaßnahmen sollten aufgelöst und durch einheitliche, aufeinander abgestimmte Mechanismen ersetzt werden.“
  + „Sicherheitsmaßnahmen, die von den Benutzern und Benutzerinnen nicht akzeptiert werden, sind wirkungslos. Es sollten praktikable Lösungen gefunden werden, die die Benutzer:innen möglichst wenig einschränken oder behindern.“
  + „Zu aufwändige oder zu teure Sicherheitsmaßnahmen sollten überarbeitet oder verworfen und durch angemessene Schutzmaßnahmen ersetzt werden. […] Zu schwache Maßnahmen gefährden die IT-Sicherheit […] und sollten ebenfalls überarbeitet oder ersetzt werden.“

Rückführung in den Sicherheitsprozess

Nach erfolgreicher Risikoanalyse können die Ergebnisse der Analyse und des Sicherheitskonzepts zur Anpassung des Sicherheitsprozesses genutzt werden. Die Analyse bildet die Basis für die folgenden Arbeitsschritte (BSI, 2008, S. 23):

* + Umsetzung des Sicherheitskonzepts;
  + Überprüfung des IT-Sicherheitsprozesses auf allen Ebenen und
  + Informationsfluss im IT-Sicherheitsprozess.

Wenn die Einhaltung des IT-Grundschutzes erforderlich ist, kann auch eine ISO 27001-Zertifizierung erworben werden. Die „ISO 27001-Zertifizierung auf Basis von IT-Grundschutz“ kann zudem von einem Auditor attestiert werden.

Zusammenfassung

Die Sonderveröffentlichung NIST SP 800-37 stellt einen Standard für das Risikomanagement in Organisationen dar. Sie beschreibt den Aufbau eines Risikomanagement-Frameworks. Der erste Teil beschreibt die Grundlagen des Risikomanagements, während der zweite Teil den Risikomanagementprozess wie folgt bestimmt: vorbereiten, kategorisieren, auswählen, durchführen, bewerten, genehmigen und überwachen.

ISO/IEC 27005 ist eine Veröffentlichung aus der ISO27k-Normenfamilie, die sich mit dem Risikomanagement in der Informationssicherheit befasst. ISO/IEC 27005 gliedert den Prozess des Sicherheitsrisikomanagements in sechs Phasen: Ermittlung des Kontexts, Risikobewertung, Risikobehandlung, Risikoakzeptanz, Risikokommunikation sowie Risikoüberwachung und -überprüfung.

Der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte BSI-Standard 100-3 bietet ein Framework für die Risikoanalyse. Er beschreibt, wie das Risikomanagement in Übereinstimmung mit den BSI IT-Grundschutz-Katalogen durchgeführt werden sollte. Der Prozess nach BSI-Standard 100-3 umfasst sieben Schritte: Vorarbeiten, Erstellung der Gefährdungsübersicht, Ermittlung zusätzlicher Gefährdungen, Gefährdungsbewertung, Behandlung von Risiken, Konsolidierung des Sicherheitskonzepts und Rückführung in den Sicherheitsprozess. Der Schwerpunkt dieses Prozesses liegt auf der Einhaltung des BSI IT-Grundschutzes. Ist eine Organisation mit der BSI 100er-Reihe konform, kann die Konformität mit ISO 27001 durch einen Auditor bescheinigt werden.

# Lektion 5

## Risikobewertung

##### LERNZIELE

Nach der Bearbeitung dieser Lektion wissen Sie, …

… wie eine Risikobewertung durchgeführt wird.

… wie eine Risikobewertung geplant wird.

… wie Black-Swan-Ereignisse bei der Risikobewertung einbezogen werden.

… was unter kontinuierlicher Neubewertung zu verstehen ist.

DL-E-DLMCSECRAM01\_E-U05

### Risikobewertung

#### Einführung

Unter dem Risikomanagement wird der Prozess des Managements bekannter oder unbekannter Risiken für eine Organisation verstanden. So ist es meist einfacher, ein Problem zu bewältigen, wenn man über ausreichende Informationen verfügt, die für eine fundierte Entscheidung nötig sind. Wenn wir zum Beispiel zu einem Freund oder Familienmitglied fahren, geben wir eine ungefähre Ankunftszeit an. Nun könnte es aber auf unserem Weg einen Unfall oder Stau geben, und ohne weitere Informationen lässt sich unsere Ankunftszeit nicht mehr genau bestimmen. Wir rufen also unsere bevorzugte Navigations-App auf oder hören uns die Verkehrsmeldungen im Radio an, um die Situation besser einschätzen zu können. Mit Hilfe dieser neuen Informationen können wir die Ankunftszeit wesentlich genauer angeben.

Im Risikomanagementprozess einer Organisation erfüllen Risikobewertungen genau diesen Zweck. Eine Risikobewertung kombiniert das Threat Modeling mit einem umfassenderen Prozess, um genaue und nützliche Informationen über die Risiken des Projekts oder der Organisation zu erhalten. Mithilfe dieses Prozesses können die Entscheidungsträger bestimmen, wie sie mit Risiken umgehen wollen.

#### Methoden

Bei einer Risikobewertung sucht ein Analyst oder ein Sicherheitsexperte nach Risiken in einer definierten Umgebung. Die ausgemachten Risiken werden anschließend klassifiziert und kategorisiert, um den Entscheidungsträgern bei ihrer Risikomanagementstrategie zu helfen. Eine Risikobewertung sollte einer klar definierten Methode folgen, damit sämtliche Bewertungen und die daraus resultierenden Risiken verglichen werden können. Schließlich sollte der gesamte Prozess dokumentiert werden. Da Risiken nicht statisch sind, kann auch der Risikomanagementprozess nicht statisch sein. Die Risikobewertung muss somit auf eine sich entwickelnde Art und Weise durchgeführt werden. Ein einfaches Framework für einen Risikobewertungsprozess sollte die folgenden Schritte enthalten: Bewertungsvorbereitung, Threat Modeling, Risikobewertung und Vorschläge zur Risikominderung.

Bewertungsvorbereitung

In der Vorbereitungsphase wird das Fundament für die Risikobewertung gelegt. In dieser Phase wird der Geltungsbereich der Bewertung festgelegt, es werden Annahmen getroffen und die dem Geltungsbereich entsprechenden Assets aufgelistet.

Den Geltungsbereich definieren

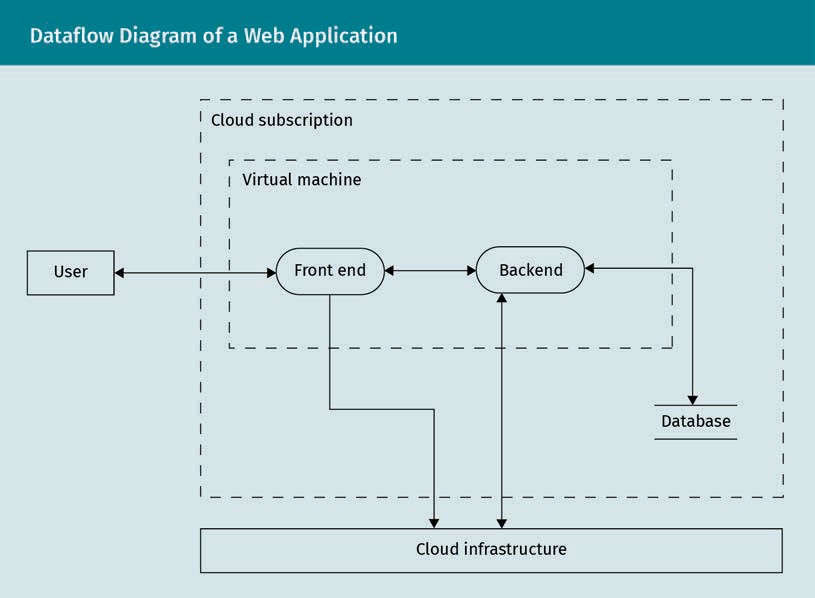
Den Geltungsbereich der Bewertung zu definieren, ist ein entscheidender Bestandteil der Analyse. Denn der Geltungsbereich bestimmt, was analysiert werden soll und was nicht (White, 2014). Ein geeigneter Geltungsbereich ist so eng gefasst, dass er keine Systeme einschließt, die nicht unter der Kontrolle des Projektteams stehen, aber gleichzeitig so weit gefasst, dass alle Verbindungen zu und von den Systemen im Geltungsbereich enthalten sind. Alle Systeme, für die das Projektteam verantwortlich ist oder die von ihm betrieben werden, sowie alle Verbindungen zu und von diesen Systemen sollten in den Geltungsbereich einbezogen werden. In diesem Fall ist ein Projektteam das Team, das den Kern der im Geltungsbereich enthaltenen Systeme betreibt oder entwickelt. Mit dieser Projektdefinition ist es möglich, die Risikobewertung in verschiedene Projekte zu unterteilen. Meist enthält die Definition des Geltungsbereichs nur den technischen Teil eines Projekts. Es ist zudem wichtig, einen Blick auf die

Risikobewertung

umgebenden Prozesse des zu analysierenden Systems zu werfen. Es gibt Fälle, in denen das technische System zwar korrekt implementiert zu sein scheint, die damit verbundenen Prozesse jedoch eine große Bedrohung für die Organisation darstellen können (z. B. fehlendes Patch-Management oder fehlende Lebenszyklusprozesse).

Ein Beispiel dafür ist eine normale dreistufige Webanwendung, die auf einem beliebten öffentlichen Cloud-Anbieter läuft. Das Frontend und die Anwendungsdienste werden auf einer virtuellen Maschine (VM) ausgeführt, und für die Datenbank wird eine Platform-as-a-Service (PaaS) verwendet, wie sie in der folgenden Abbildung zu sehen ist.

Zunächst werden die Elemente, die nicht zum Geltungsbereich zählen, identiﬁziert. In diesem Fall gehören Benutzer:innen nicht zum Geltungsbereich, da das Projektteam sie nicht kontrollieren kann. Mitunter kann das Risiko für die Benutzer:innen z. B. nur durch Sensibilisierungsprogramme gemanagt werden. Außerdem fällt die Cloud-Infrastruktur nicht in den Geltungsbereich, da der Cloud-Anbieter diese Infrastruktur verwaltet. Die virtuelle Maschine ist der Bereich, in dem der Frontend- und der Backend-Service arbeiten. Die Datenbank als Datenspeicher sollte ebenfalls zum Geltungsbereich gehören. Der Datenbankserver selbst wird nicht berücksichtigt, da der Cloud-Anbieter diesen verwaltet. Nur die für die Cloud-Kunden bestimmte Konfiguration könnte in den Geltungsbereich fallen. Normalerweise sollten alle Verbindungen zu oder von zum Geltungsbereich gehörigen Elementen ebenfalls zum Geltungsbereich gehören. Im Beispielfall handelt es sich um alle eingezeichneten Verbindungen.



Deﬁnieren der Annahmen

Nachdem der Geltungsbereich definiert wurde, werden Annahmen über das Projekt getroffen. Diese Annahmen bilden die Grundlage für die Risikoanalyse und engen den Geltungsbereich ein. Ohne Annahmen kann der Umfang der Analyse unkontrollierbar werden. Zu den üblichen Annahmen gehören die folgenden:

Platform-as-a-Service (PaaS)

Platform-as-a-Service ist ein Servicemodell im Cloud Computing, das einen vollständig verwalteten Computing-Service als Plattform für den/die Benutzer:in zur Erstellung seiner Anwendung bereitstellt.

* „Die Mitarbeiter:innen der Organisation sind vertrauenswürdig.“
* „Der Cloud-Anbieter handelt nicht böswillig.“
* „Die verwendete Hardware hat keine bekannten Schwachstellen.“
* „Die physische Sicherheit ist gewährleistet.“
* „Die Cloud-Infrastruktur funktioniert wie beschrieben.“

Annahmen helfen Analysten dabei, sich auf den relevanten Teil des Projekts zu konzentrieren und keine Zeit mit uninteressanten Fragen zu verschwenden. Wenn wir beispielsweise davon ausgehen, dass die physische Sicherheit gewährleistet ist, können Analysten alle Bedrohungen, die auf das Rechenzentrum abzielen, direkt überspringen und bei den Netzwerkbedrohungen eines Servers beginnen.

Auflistung der Assets

Sobald der Geltungsbereich und die Annahmen festgelegt sind, können die Analysten damit beginnen, die für diese Analyse relevanten Assets zu suchen und aufzulisten. Assets sind Dinge, die für Angreifer interessant sind und daher geschützt werden müssen (z. B. geistiges Eigentum). Diese Assets können in zwei Kategorien unterteilt werden: primäre und sekundäre oder unterstützende Assets (International Organization for Standardization [ISO]/International Electrotechnical Commision [IEC], 2018). Primäre Assets beziehen sich auf die Organisation und die Angreifer. Diese Assets „verdienen das Geld“. Geschäftsaktivitäten und Informationen sind die wichtigsten Assets. Beispiele :

* geistiges Eigentum,
* Geschäftspläne,
* Kundenkontakte,
* Kundendaten und
* persönliche identifizierbare Informationen (PII).

Die sekundären Assets unterstützen die primären Assets und sind nur relevant, wenn ein primäres Asset von ihnen beeinträchtigt wird. Ein Server kann z. B. als unterstützendes Asset klassifiziert werden, wenn Kundendaten darauf gespeichert sind. Wenn der Server kein primäres Asset beherbergt, dann ist er für den Geltungsbereich nicht relevant, da kein Risiko besteht. Zu den unterstützenden Assets gehören

* Server,
* Netzwerk,
* kryptografisches Material,
* Geheimnisse,
* Prozesse, und
* Personal.

Die wichtigsten Assets sind die in der Datenbank gespeicherten Daten und die Informationen der Benutzer:innen. Logging-Daten können ebenfalls als primäres Asset klassifiziert werden. Bei den unterstützenden Assets handelt es sich um die virtuelle Maschine, die Cloud-Prozesse, die für das Verfahren verwendeten Schlüssel und Anmeldeinformationen sowie den Quellcode für den Frontend- und Backend-Server.

Im Rahmen einer Risikobewertung sollte die Ermittlung von Assets gemeinsam mit dem Projektteam durchgeführt werden. Mit unterstützenden Fragen der Analysten kann das Team die wichtigen Assets identifizieren und herausfinden, wo diese gespeichert oder verarbeitet werden. Mit diesen Informationen können die Analysten daraufhin die primären und unterstützenden Assets beschreiben.

Risikobewertung

Threat Modeling

Nach der Vorbereitungsphase des Bewertungsprozesses kann das Threat Modeling (Bedrohungsmodellierung) beginnen. In der Threat-Modeling-Phase suchen Analysten nach Bedrohungen im definierten Geltungsbereich (Shostack, 2014). Die Bedrohungen zielen alle indirekt auf eines der genannten Assets ab. Das Threat Modeling sollte aus Gründen der Konsistenz im gesamten Projekt mit einer einzigen Methode durchgeführt werden. Daher müssen die Analysten entscheiden, welche Methode sie verwenden möchten. Es gibt u.a. folgende Methoden:

* STRIDE
* LINDDUN
* Attack-Trees
* Process for Attack Simulation and Threat Analysis (PASTA)
* Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
* Visual, Agile, and Simple Threat modeling (VAST)

Diese Methoden des Threat Modelings verfügen über unterschiedliche Vor- und Nachteile. So ist STRIDE zum Beispiel sehr ausgereift und einfach zu bedienen, und die Attack-Trees sind ausdrucksstark und leicht wiederholbar.

Das Threat Modeling sollte mit dem Zeichnen eines Datenflussdiagramms (DFD) für den Geltungsbereich beginnen. Dieses Diagramm zeigt den logischen Datenfluss und enthält alle Informationen über die Entitäten und deren Beziehungen im System. Ein Datenflussdiagramm hilft den Analysten bei einem besseren Verständnis der Datenflüsse und der Prozesse des Geltungsbereichs. Ein DFD zeigt zudem, ob der Geltungsbereich vollständig ist und nichts vergessen wurde. Das DFD kann daraufhin als Grundlage für das Threat Modeling verwendet werden. Für den Threat-Modeling-Prozess sollten weitere unterstützende Materialien verwendet werden. Ein Gespräch mit den Architekten und den zuständigen Projektmanagern und -managerinnen ist stets ein guter Anfang. Dies kann in Form von Workshops geschehen, bei denen sich alle Beteiligten in einem Raum befinden und das Projekt besprechen. Einzelgespräche stellen ebenfalls eine sinnvolle Option dar, dabei kann in Erfahrung gebracht werden, ob die verschiedenen Stakeholder das gleiche Verständnis vom Geltungsbereich und vom Projekt haben.

Anfangs mag es schwierig erscheinen, die richtigen Fragen zu stellen. Mit wachsender Erfahrung fällt es mitunter leichter, einzuschätzen, welche Fragen zur Ermittlung von Bedrohungen gestellt werden müssen. Um diesen Punkt zu erreichen, werden Dokumente wie Anforderungskataloge (z. B. OWASP Application Security Veriﬁcation Standard), Best Practices oder Compliance-Standards (z. B. Health Insurance Portability and Accountability Act [HIPAA]) benötigt. Meistens ist es nicht möglich, alle potenziellen Risiken zu ermitteln, da Informationen fehlen oder sich die Bedrohungslandschaft verändert hat. Folglich muss das Bedrohungsmodell zu einem bestimmten Zeitpunkt als vollständig deﬁniert werden.

Risikobewertung

Sobald das Bedrohungsmodell als vollständig deﬁniert wurde, kann die Bewertung dieser Bedrohungen beginnen. Die Risikobewertung betrachtet die Bedrohungen und berechnet ein Risiko für die Organisation. Bedrohungen, die kein Risiko für die Organisation darstellen, können dabei ignoriert werden. Die Risikoklassifizierung kann mithilfe der Formel Risiko = Wahrscheinlichkeit × Auswirkungen erfolgen. Diese Formel beschreibt das Risiko als ein

Vielfaches der Wahrscheinlichkeit der Bedrohung und ihres Schadenspotenzials. Das Ergebnis unterstützt das Management dabei, eine fundierte Entscheidung zu treffen. Damit die Risikobewertung ein wiederholbares Ergebnis liefert, sollte ein geeignetes Framework gewählt werden. Solche Frameworks (z. B. die OWASP-Risikobewertungsmethode) beschreiben die Komponenten der einzelnen Faktoren und wie diese zu bewerten sind (Williams, 2020).

Risikominderungsvorschlag

Risikominderungsmaßnahmen sind auf die Bedrohungen ausgerichtet und sollen das Risiko verringern (Shostack, 2014). In der Regel verringern diese Maßnahmen lediglich die Eintrittswahrscheinlichkeit, da sich die Auswirkungen meist nicht reduzieren lassen. So wären die Auswirkungen eines Diebstahls von Kundendaten beispielsweise schwerwiegend und nicht veränderbar, jedoch können entsprechende Risikominderungsmaßnahmen den Diebstahl verhindern.

Es sind verschiedene Arten von Maßnahmen zur Risikominderung möglich. Diese können sich auf Prozesse (z. B. in Bezug auf den Softwareentwicklungsprozess oder das Änderungsmanagement) oder auf technische Maßnahmen (z. B. Änderungen der Architektur oder spezifische technische Anforderungen, wie die Installation einer Anti-Malware-Lösung) beziehen. Da sich alle Risikominderungsmaßnahmen direkt auf die Risikoeinstufung auswirken, sollte ein Restrisiko berechnet werden, um eine Gesamtrisikoeinstufung zu erhalten, nachdem die Risikominderungsmaßnahmen umgesetzt wurden. Dies hilft dabei, die Prioritäten für die Umsetzung der Risikominderungsmaßnahmen festzulegen.

Dokumentation und Berichterstattung

Die Dokumentation und Berichterstattung der Risikobewertung ist für eine gute Risikobewertung unerlässlich. Einen einfachen und formellen Weg stellt das Verfassen eines Berichts dar. Dieser sollte die Vorbereitungsschritte, die Ergebnisse und eine Erklärung der durchgeführten Maßnahmen enthalten. So könnte ein beispielhaftes Inhaltsverzeichnis aussehen:

1. Zusammenfassende Darstellung
2. Geltungsbereich und Voraussetzungen
   1. Annahmen
   2. Geltungsbereich
   3. Assets
   4. Diagramme
3. Architekturdiagramm
4. Datenflussdiagramm (DFD)
5. Bedrohungsmodell
   1. Bedrohung-01
   2. Bedrohung-02
6. Risikobewertung
7. Anhang

Alternativ können die Ergebnisse und die Abhilfemaßnahmen auch direkt in einem Ticket- oder Tracking-System des Projekts dokumentiert werden. In ein solches System kann das Projektteam die notwendigen Aufgaben in seinen Entwicklungsprozess aufnehmen.

Risikobewertung

#### Berücksichtigung von Black-Swan-Ereignissen

Black-Swan-Ereignisse sind durch ihre weitreichenden Auswirkungen neben einer geringen Eintrittswahrscheinlichkeit gekennzeichnet. Es kann deshalb der Eindruck entstehen, dass diese Ereignisse bei der Risikobewertung nicht so wichtig seien. Dies mag zutreffen, wenn nur kleine Teile einer Organisation analysiert werden, aber tatsächlich können Black-Swan-Ereignisse eine Organisation in den Ruin treiben (Taleb, 2007).

Aus Analystensicht ist es am einfachsten, Black-Swan-Ereignisse zu berücksichtigen, indem man Annahmen trifft, die diese Ereignisse ausschließen. Diese Methode kann notwendig sein, um die Risikobewertung in einem engen Rahmen zu halten und zu verhindern, sich in Details zu verlieren. Wenn andererseits das Risiko für die Organisation als Ganzes bewertet werden muss, müssen auch Black-Swan-Ereignisse in die Bewertung einfließen. Es gibt zwei Strategien, um Black-Swan-Ereignisse zu ermitteln und ihr Risiko zu bewerten: 1) Bewertung von Ereignissen und Ermitteln von Risiken für Assets sowie

2) Bewertung von Bedrohungen für Assets und Ermitteln von Ereignissen.

Bewerten von Ereignissen

Die erste Bewertungsstrategie für Black-Swan-Ereignisse besteht darin, die Ereignisse zu bewerten und zu analysieren, was mit dem Geltungsbereich passieren würde. Bei diesen Ereignissen kann es sich um frühere Black-Swan-Ereignisse und Katastrophen handeln (z. B. der Anschlag vom 11. September 2001 in den USA). Auch Planspiel-Ereignisse, d. h. solche, die sich die Analysten vorstellen, können durchgespielt und die daraus resultierenden Risiken für die Assets analysiert werden.

Bewertung von Bedrohungen

Die zweite Bewertungsstrategie ist im Grunde die Umkehrung der ersten. Bei dieser Strategie werden die Bedrohungen für die Assets bewertet und Ereignisse ermittelt, die zu Risiken führen könnten. Diese Risiken können das Ergebnis bekannter Bedrohungen aus Bedrohungsmodellstrategien sein (z. B. die Bedrohungen aus STRIDE). So könnten zum Beispiel Kundendaten zu schützende Assets sein. Eine Bedrohung könnte der Verlust dieser Daten darstellen (Denial of Service im Sinne von STRIDE). Mit dieser Bedrohung im Hinterkopf könnten entsprechende Szenarien ermittelt werden. Darüber hinaus könnten Naturereignisse eine weitere Möglichkeit sein; So könnte beispielsweise eine Überflutung oder ein Hurrikan das Rechenzentrum, in dem die Live-Daten gehostet werden, und das Backup-Rechenzentrum zerstören.

Risikominderungsmaßnahmen für Black-Swan-Ereignisse

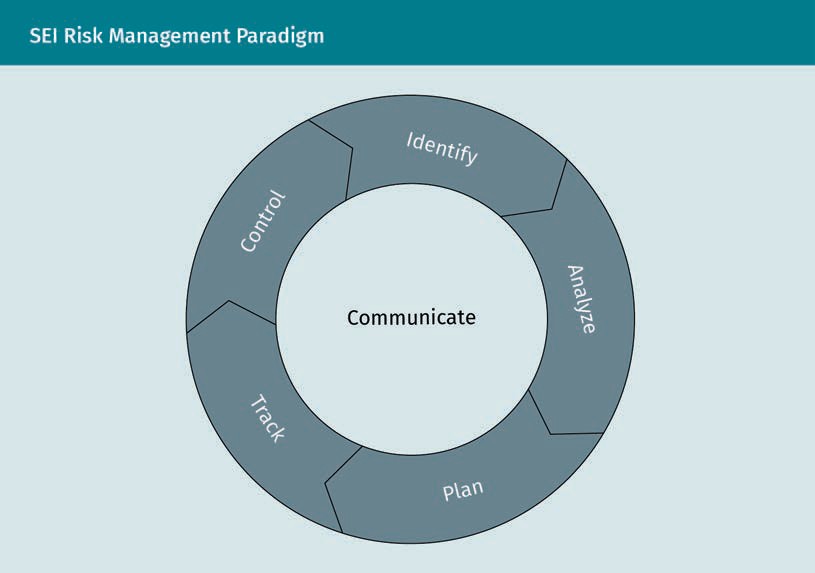
Da die Eintrittswahrscheinlichkeit von Black-Swan-Ereignissen relativ gering ist, müssen die Auswirkungen eines solchen Ereignisses durch Minderungsmaßnahmen angegangen werden. Durch technische Maßnahmen kann das Risiko verringert werden. Im Beispiel des Naturereignisses könnten die Daten auf mehrere Rechenzentren in der ganzen Welt verteilt werden. Eine weitere Möglichkeit besteht darin, das Risiko zu vermeiden. Dies geschieht durch Maßnahmen und Kontrollelemente, welche die Umgebung so verändern, dass die Bedrohung nicht mehr möglich ist. Eine dritte Möglichkeit ist die Übertragung des Risikos durch entsprechende Versicherungen. So kann eine Organisation gegen Bedrohungen oder Katastrophenfälle versichert werden. Dadurch wird die Bedrohung zwar nicht verhindert, aber die Auswirkungen werden abgemildert, da die Versicherung den finanziellen Schaden erstattet.

#### Kontinuierliche Neubewertung

Da sich die Risikolandschaft einer Organisation im Laufe der Zeit wandeln kann und wird, sind sowohl das Risikomanagement als auch die -bewertung keine einmaligen Prozesse. So ist eine kontinuierliche Neubewertung notwendig, um mit den potenziellen Risiken Schritt zu halten. Die Neubewertung kann jährlich durchgeführt werden, um die offenen Risiken neu zu bewerten oder unbekannte Risiken zu ermitteln. Wenn sich der Geltungsbereich verändert, ist möglicherweise eine neue Risikobewertung erforderlich, um die Abweichung zwischen der ursprünglichen Implementierung und der Änderung zu bewerten.

SEI-Risikomanagementparadigma

PDCA

Die Managementmethode Plan-Do-Check-Act wird verwendet, um ein Produkt oder einen Prozess kontinuierlich zu managen und zu verbessern.

Die kontinuierliche Neubewertung kann Bestandteil des standardmäßigen kontinuierlichen Managementprozesses Plan-Do-Check-Act (PDCA) sein (Tague, 2005). Das Software Engineering Institute der Carnegie Mellon University (CMU/SEI) ist noch einen Schritt weiter gegangen und hat ein Risikomanagementparadigma entwickelt, um Risiken kontinuierlich zu managen. Dieser Managementprozess ist in sechs Schritte unterteilt: identifizieren, analysieren, planen, verfolgen, kontrollieren und kommunizieren (Van Scoy, 1992).

Identifizieren

Risiken werden entdeckt und identiﬁziert. Dies geschieht in der Regel im Rahmen der Risikobewertung.

Risikobewertung

|  |  |
| --- | --- |
| Analysieren | Die Analyse der Risiken umfasst die Evaluation, d. h. die Ermittlung der Eintrittswahrscheinlichkeit und der Auswirkungen der Risiken für die Organisation. Dies ist wichtig, damit sich die Entscheidungsträger auf die entscheidenden Risiken konzentrieren können |
| Planen | Für jedes Risiko muss ein Plan zur Risikominderung erstellt werden, der die Maßnahmen und den Zeitrahmen für die Umsetzung enthält. Bei den möglichen Maßnahmen handelt es sich um die üblichen Maßnahmen des Risikomanagements (z. B. gemäß ISO/IEC 27005): Risikominderung, Risikoakzeptanz, Risikovermeidung und Risikotransfer. |
| Verfolgen | Wir verfolgen die Umsetzung der Maßnahme und stellen fest, ob sie die geplante Wirkung erzielt hat. Die Verfolgung kann mit auslösenden Ereignissen oder Meilensteinen erfolgen. |
| Kontrollieren | Die festgelegte Verfolgung muss kontrolliert werden, um sicherzustellen, dass das Risiko ordnungsgemäß gemanagt wird. Das Risiko und die Maßnahmen sollten dahingehend kontrolliert werden, ob sie das gewünschte Ziel erreichen. Das Risikocontrolling sollte sich in den normalen Projektmanagementprozess einfügen und keine unerwünschte Nebenaktivität sein. |
| Kommunizieren | Kommunikation ist der Schlüssel zum Risikomanagementprozess und steht im Mittelpunkt des Paradigmas. Die Ergebnisse aller Schritte müssen den entsprechenden Teams und Entscheidungsträgern mitgeteilt werden. |

Tools für die kontinuierliche Neubewertung

Geeignete Tools können den Prozess der Neubewertung unterstützen. Bei diesen Tools kann es sich um einfache Listen mit allen Risiken und Auslösern für die Nachverfolgung sowie um den Umsetzungsplan handeln. Für die Dokumentation der Evaluation können bereits verwendete Tracking-Tools (z. B. Atlassian Jira) verwendet werden. Einige Anbieter haben spezielle Risikomanagement-Tools entwickelt, die Organisationen bei der Durchführung des Risikomanagements helfen (z. B. SimpleRisk). Letztendlich hängt es von den Anforderungen der Organisation ab, wie sie den Neubewertungsprozess mit Tools unterstützen möchte.

Ein Bild, das Tisch enthält.

Automatisch generierte Beschreibung

Zusammenfassung

Risikobewertungen sind notwendig, um über einen definierten Prozess zur Festlegung eines bestimmten Geltungsbereichs und zur Bewertung der ermittelten Risiken zu verfügen. Dieser Prozess der Risikobewertung setzt sich zusammen aus der Vorbereitung der Bewertung, dem Threat Modeling, der Risikobewertung und dem Vorschlag zur Risikominderung. Die Vorbereitung der Bewertung lässt sich in die Definition des Geltungsbereichs, die Definition der Annahmen und die Auflistung der Assets unterteilen. Die Definition des Geltungsbereichs beschreibt einen konkreten Bereich, in dem die Risikobewertung durchgeführt werden soll. Zur Eingrenzung des Geltungsbereichs dienen die Annahmen als Aussagen, die von den Analysten als wahr deﬁniert werden.

Unter Assets werden Dinge verstanden, auf die Bedrohungen abzielen können. Sie lassen sich in primäre und unterstützende Assets unterteilen. Erstere sind geschäftsrelevant, wie z. B. geistiges Eigentum oder Daten von Kundinnen und Kunden. Bei den unterstützenden Assets handelt es sich wiederum um Systeme, die zur Verarbeitung oder Speicherung der primären Assets benötigt werden (z. B. Server oder Software). Sobald all diese Punkte definiert sind, kann das Threat Modeling mit einem Framework für die Modellierung beginnen. Anschließend werden die Bedrohungen aus dem Bedrohungsmodell bewertet und die Risiken identiﬁziert und ebenfalls bewertet. Ausgehend von diesen Risiken können die Analysten Maßnahmen zur Risikominderung vorschlagen. Für die Entscheidungsträger:innen wird all dies dokumentiert.

Bei einer Risikobewertung sollten außerdem Black-Swan-Ereignisse berücksichtigt werden. Da die Wahrscheinlichkeit für diese Ereignisse gegen Null geht, müssen die Auswirkungen und die Möglichkeiten zur Abschwächung dieser analysiert werden. Assets können analysiert und es können potenzielle Schadensereignisse ermittelt werden, oder umgekehrt, und die Auswirkungen für die Assets können mit einer Auswahl an katastrophalen Ereignissen ermittelt werden.

Da die Risikolandschaft einem stetigen Wandel unterliegt, ist eine kontinuierliche Neubewertung erforderlich, um mit diesen neuen Risiken Schritt zu halten. Das Software Engineering Institute hat ein Risikomanagement-Paradigma entwickelt, um dieses Problem anzugehen und ein kontinuierliches Risikomanagement durchzuführen. Die einzelnen Schritte des Paradigmas sind: Identifizieren, Analysieren, Planen, Verfolgen, Kontrollieren und Kommunizieren.



# Lektion 6

## Die cyber-resiliente Organisation

##### LERNZIELE

Nach der Bearbeitung dieser Lektion können Sie …

... beschreiben, inwiefern sich das Risikomanagement einer agilen Umgebung anpassen muss.

... nachvollziehen, warum Krisenmanagement und Incident Response Bestandteile des Risikomanagements sind.

... erklären, warum Resilience Engineering und Sicherheitstools für eine cyber-resiliente Organisation nötig sind.

DL-E-DLMCSECRAM01\_E-U06

### Die cyber-resiliente Organisation

#### Einführung

Umgebungen und Infrastrukturen werden zunehmend komplexer, und damit auch die Bedrohungen, denen eine Organisation ausgesetzt ist. Deshalb sind Organisationen gezwungen, entsprechende Maßnahmen zu planen und umzusetzen, um gegen derlei Bedrohungen gewappnet zu sein. Ein einfaches Beispiel verdeutlicht dies: Wenn wir in einer Gegend mit einer höheren Kriminalitätsrate wohnen, können bessere Schlösser oder Überwachungskameras dem Schutz dienlich sein. Selbstverständlich können wir auch die Türen abschließen, um Eindringlinge abzuhalten. Das Gleiche gilt für eine Organisation, die sich gegen Cyber-Bedrohungen zur Wehr setzen will. Wenn sich die Bedrohungen oder die Umgebung ändern, passen sich Organisationen an und verändern ihre Risikomanagementstrategie, indem sie diese um Maßnahmen und Richtlinien erweitern, die der Organisation bei einem Vorfall helfen könnten, oder überdenken die Art und Weise, wie Software oder Systeme entwickelt werden.

#### Veränderung der Ansätze im Risikomanagement

Wenn Organisationen ihre Entwicklungsprozesse von einem eher statischen Entwicklungsprozess (z. B. dem Wasserfallmodell) auf einen agilen Prozess (z. B. Scrum) umstellen, muss sich auch der Risikomanagementansatz entsprechend ändern. In agilen Projekten kann der Risikomanagementprozess kein statischer Prozess sein. Außerdem müssen Risikobewertungen häufiger durchgeführt werden, da sich der Geltungsbereich mit jeder Software-Iteration oder Umgebungsänderung verändert (Brunton-Spall et al., 2017). Für diesen Kulturwandel muss sich der gesamte Ansatz des Risikomanagements ändern. Dies betrifft die Bereiche Governance, Entscheidungsfindung, Ausbildung und Tools (Deloitte, 2019).

Governance

In einer agilen Umgebung sind die Governance-Teams nicht in der Lage, alle Risiken zu bewerten und Maßnahmen zur Risikominderung für jedes einzelne Risiko zu beschließen. Daher müssen die Governance-Teams klare Richtlinien für das Delivery-Team erarbeiten, in denen festgelegt ist, wie die Risiken gemanagt werden sollen. So kann die Entscheidung über die Risikostrategie von den Governance-Teams auf ein führendes Mitglied des Delivery-Teams verlagert werden.

Diese Richtlinien oder Leitlinien sollten Folgendes beinhalten:

Risikobereitschaft Die Risikobereitschaft bestimmt den Grad des Risikos, den eine Organisation bereit ist, ohne weitere Konsequenzen zu akzeptieren. Die Minderung dieser Risiken wird als Verschwendung

von Ressourcen betrachtet.

* Wie hoch ist die Risikobereitschaft der Organisation?
* Wie hoch ist die Risikotoleranz der Organisation?
* Wie hoch ist die Risikokapazität der Organisation?
* Auf welcher Ebene kann das Projekt über Risiken entscheiden?
* Wie sollten die Risiken eingestuft werden (d. h. wie werden die Auswirkungen und die Eintrittswahrscheinlichkeit bewertet)?
* Wie sollten Risiken in einem agilen Team gemanagt werden?

Die cyber-resiliente Organisation

Entscheidungsfindung

Die Entscheidung darüber, wie mit Risiken umgegangen wird, muss im agilen Team getroffen werden (so kann z. B. der Project Owner oder Product Owner der Risk Owner sein). Dies ist in sich wandelnden Umgebungen notwendig. Wenn sich das Design in einer Iteration ändert, werden sich auch die Risiken schnell verändern. In einem solchen Szenario müssen die Risiken neu bewertet und es müssen neuerliche Entscheidungen getroffen werden. Um hierbei mit der Entwicklung Schritt zu halten, sollten Entscheidungen schnell und in Zusammenarbeit mit den Entwicklerinnen erfolgen. Risikominderungsmaßnahmen lassen sich leicht innerhalb des agilen Frameworks planen. Beispielsweise bietet Scrum verschiedene Möglichkeiten, die für das Risikomanagement genutzt werden können. In der Sprintplanung können Risiken überprüft und gewichtet werden. Während des Sprint Storywritings kann der Schwerpunkt auf die Umsetzung der Maßnahme zur Risikominderung verlagert werden. In der Designphase können Risiken durch Threat Modeling identifiziert werden. Während der Nachbetrachtungen können die Umsetzung der Risikominderungsmaßnahmen bewertet und die Prozesse verbessert werden.

Ausbildung

Die meisten Entwickler:innen sind entweder nicht im Bereich Risikomanagement ausgebildet oder sie verfügen über keine tieferen Kenntnisse in der Anwendungssicherheit. Sicherheitsexperten und -expertinnen sind schwieriger zu finden als Entwickler:innen. Für dieses Problem hat die Sicherheitsgemeinschaft das Security Champion Programm entwickelt (SAFECode, 2019). Ein Security Champion ist Bestandteil eines Entwicklerteams, z. B. als Entwickler:in, Produktmanager:in oder Tester:in. Die Security Champions unterstützen ihr Team bei der Implementierung und Verbesserung der Sicherheit. Die Aufgaben des Security Champions können von Team zu Team variieren. Einige grundlegende Aufgaben sind

* + Ausführung des Risikomanagements
    - Threat Modeling
    - Risikobewertung
    - Risikoverfolgung
  + Aufklärungsarbeit
    - Motivation des Teams zur Einhaltung der Sicherheitsmaßnahmen
    - Überprüfung oder Erstellung von Best Practices im Bereich Sicherheit
    - Erstellung von Richtlinien des sicheren Programmierens für das Projektteam
  + Überprüfung der Umsetzung
    - Sicherheitsüberprüfungen
    - Implementierung von automatischen Sicherheitsscannern

Da es sich bei den Security Champions um Entwickler:innen handelt, die für diese zusätzliche Aufgaben verantwortlich sind, sollte die Ausübung freiwillig sein. Denn wenn Mitarbeitende dazu gedrängt werden, sich für die Sicherheit einzusetzen, so würden sie die Sicherheit vermutlich nur als eine zusätzliche, unnötige Aufgabe betrachten (d. h. sie wären keine große Hilfe). Haben sie sich hingegen freiwillig bereit erklärt, ist ihre Motivation größer, die Aufgaben zu erledigen. Auf diese Weise kann eine größere Wirkung und ein besseres Ergebnis erzielt werden.

Risikotoleranz Die Risikotoleranz bestimmt das Risikoniveau,

das eine Organisation akzeptieren kann. Die Minderung des Risikos wird gegen die Kosten des Risikos und der Minderung abgewogen.

Risikokapazität Die Risikokapazität

definiert das Risikoniveau, das eine Organisation tolerieren kann. Die Minderung von Risiken oberhalb dieses Niveaus ist zwingend erforderlich, da diese Risiken der Organisation erheblich schaden können.

Tools

Tools und Automatisierung stellen einen wichtigen Faktor bei der agilen Entwicklung dar. Sie unterstützen die Projektteams dabei, die gewünschten Aufgaben schnell und efﬁzient zu erledigen, damit sie sich auf die Entwicklung ihres Produkts konzentrieren können. Sicherheit und Risikomanagement sind hierbei keine Ausnahme. So können Tools den Sicherheitsexperten oder Champions dabei helfen, Tests oder Bedrohungsmodelle einfacher durchzuführen. Dies können Tools sein, die Risiken verfolgen und bewerten. Checklisten stellen zusätzliche Hilfsmittel dar, die verwendet werden können, um Standardprobleme im Design oder in der Software zu finden. Eine solche Checkliste ist der Open Web Application Security Project Application Security Verﬁcation Standard (OWASP ASVS), der Anforderungen für die sichere Softwareentwicklung enthält (OWASP, 2021).

Mithilfe von Automatisierung lassen sich z. B. Datenflussdiagramme oder andere Diagramme erstellen. So können beim Threat Modeling Änderungen im Design oder im System schnell modelliert werden. Darüber hinaus kann die Automatisierung dazu genutzt werden, zu überprüfen, ob die Risikominderungsmaßnahmen korrekt umgesetzt wurden.

#### Incident Response und Krisenmanagement

Für eine cyber-resiliente Organisation ist das Risikomanagement im Bereich der Entwicklung unverzichtbar, ferner sind proaktive Maßnahmen und die Planung dessen, was im schlimmsten Fall passieren kann, entscheidend. Meist stellt sich nicht die Frage, „ob“ eine Organisation von einer Cyberattacke oder einem größeren Vorfall betroffen sein wird, sondern vielmehr „wann“. Zur Vorbereitung müssen Organisationen sowohl Incident Response als auch Krisenmanagement einsetzen.

Krisenmanagement

Das Krisenmanagement dient dazu, unerwartete und für die Organisation gefährliche Situationen zu bewältigen. Es lässt sich in drei Schritte unterteilen, die von der Krisenkommunikation begleitet werden (Deloitte, 2016): Bereitschaft, Reaktion und Erholung. Die Kommunikation ist wichtig, um alle Beteiligten über die Situation auf dem Laufenden zu halten.

Bereitschaft

Dieser erste Schritt beinhaltet die Vorbereitung einer Organisation auf mögliche Szenarien und auf Krisen im Allgemeinen. Die Vorbereitung beginnt mit einer Krisenstrategie und der Entscheidung, wer am Krisenmanagement beteiligt sein soll. Die Vorbereitung kann zudem Playbooks für bestimmte Ereignisse oder eine Checkliste mit allen wichtigen Punkten einer Krise umfassen. Weiterhin sollten die Instrumente zur Krisenbewältigung gut vorbereitet werden. Dazu gehört die Einrichtung von Kommunikationskanälen und die Festlegung dessen, wie bestimmte Dinge kommuniziert werden müssen und mit wem. Eine Krise zu trainieren bzw. zu simulieren kann ebenfalls einen wichtigen Schritt in dieser Phase darstellen. Denn Planspiele oder Simulationen können dem Krisenteam dabei helfen, Probleme im Krisenmanagement zu erkennen und sich im Umgang mit solchen Situationen zu üben.

Die cyber-resiliente Organisation

Reaktion

In dieser Phase wird eine reale Krise bewältigt. Dafür tritt das Krisenteam zusammen und wendet die Strategien aus dem ersten Schritt an. Zudem übermittelt es die Krisenmeldung an die zuständigen Stellen, damit das Problem schnellstmöglich behoben werden kann.

Erholung

Sobald die Krise bewältigt wurde, müssen Maßnahmen eingeleitet werden, um zu einem normalen Betriebsablauf zurückzukehren. Dazu gehören die Bewertung des Schadens und die Ausarbeitung einer Schadensbehebungsstrategie. Ferner muss die Ursache des Vorfalls ermittelt und beseitigt werden. Abschließend sollte der Krisenprozess im Rahmen einer „Lessons-Learned“-Besprechung reflektiert werden. In dieser Besprechung definiert das Krisenteam Schritte zur Verbesserung des Prozesses, um zukünftige Krisen besser bewältigen zu können.

Incident Response

Der Incident-Response-Prozess ähnelt dem Prozess des Krisenmanagements, unterscheidet sich jedoch insofern von diesem, als dass der Incident-Response-Prozess auch kleinere Ereignisse berücksichtigt, die den normalen Betriebsablauf der Organisation stören, während das Krisenmanagement nur tatsächliche Krisen behandelt (Cichonski et al., 2012). Der IT-Incident-Response-Prozess behandelt zudem mehr technische Probleme als der Krisenmanagementprozess (z. B. Systemausfälle oder Cyberangriffe). Der Incident-Response-Prozess für Cybervorfälle kann in vier wesentliche Bestandteile unterteilt werden: 1) organisatorische Vorbereitung, 2) technische Vorbereitung, 3) Behandlung und 4) Nachbearbeitung.

Organisatorische Vorbereitung

Die Incident-Response-Strategie und -Prozesse müssen von einer Organisation sorgfältig geplant und vorbereitet werden. Dabei werden die Anforderungen für den gesamten Incident-Response-Prozess festgelegt. Die folgenden Bereiche sollten bei der organisatorischen Vorbereitung berücksichtigt werden (Cichonski et al., 2012):

* + Asset-Management. Das Asset-Management speichert jegliche Informationen über alle möglichen Assets einer Organisation. Dies können primäre oder unterstützende Assets sein.
  + Rollen und Zuständigkeiten. Die Rollen und Zuständigkeiten bestimmen, wer beim Incident-Response-Prozess für welche Aufgaben verantwortlich ist. Zu den Rollen gehören das Bereitschaftsteam, der Incident Investigator, der Incident Manager und die IT-Abteilung.
  + Zugriffskonzept. Das Zugriffskonzept beschreibt, wie das Incident-Response-Team auf Systeme oder Assets zugreifen kann. Dazu gehört ein normaler Lesezugriff, z. B. zur Überwachung und Protokollierung, oder ein vollständiger administrativer Zugriff im Falle eines Vorfalls.
  + Kommunikation. Eine Definition der Kommunikation ist erforderlich, da bei einem Vorfall unverzüglich die Kommunikation hergestellt werden muss. Dazu gehört die interne Kommunikation, die Kommunikation mit Kunden und Kundinnen und die Kommunikation mit den Strafverfolgungsbehörden.
  + Prozessdokumentation. Jegliche Aufgaben des Incident-Response-Managements müssen in festen Prozessen geregelt werden. So erhalten die Teams einen Leitfaden für die Vorbereitung und den Umgang mit einem Vorfall.
* Governance und Richtlinien. Das Incident-Response-Management muss in der Organisation einheitlich gestaltet werden, daher sollte dieser Prozess mit Hilfe von Governance und genauen Richtlinien definiert werden. Letztere können eine Definition von Cybervorfällen, die allgemeine Berichterstattung über solche Ereignisse, den Eskalationsprozess oder die Bewertung und Priorisierung von Vorfällen umfassen.
* Schulung. Es muss vermittelt werden, wie auf Vorfälle reagiert wird. Das ist wichtig, damit die Incident-Response-Teams stets auf dem Laufenden sind, was neue Technologien, die Umgebung und die Prozesse der Organisation betrifft.

Technische Vorbereitung

Im Rahmen der technischen Vorbereitung plant das Incident-Response-Team seine technischen Hilfsmittel für die Bewältigung von Vorfällen und bereitet diese vor. Dies schließt auch die Planung und Implementierung der folgenden Erkennungsmechanismen ein:

* Logging ist eine wichtige Informationsquelle. Logs können Spuren des Angreifers und eine Liste von Ereignissen enthalten, die zu dem Vorfall führen könnten.
* Per Monitoring kann der Asset-Zustand verfolgt werden, und bei Anomalien können Alarme an die Incident-Response-Teams gesendet werden.
* Der Zugriff muss so eingerichtet werden, dass das Incident-Response-Team schnell auf die Systeme zugreifen kann, in denen sich der Vorfall ereignet.
* Es sollten nützliche Incident-Response-Tools zusammengetragen werden.

Behandlung

Die Behandlung eines Vorfalls kann knifflig sein. Die folgenden Schritte sollten befolgt werden, um angemessen mit einem Vorfall umzugehen:

1. Klassifizierung. Das Ereignis, das zu dem Vorfall geführt hat, wird analysiert und als echt oder falsch-positiv eingestuft.
2. Triage. Die Auswirkungen des Vorfalls werden analysiert. Hier müssen die betroffenen Assets ermittelt werden. Bei neuen Informationen wird die Triage im Behandlungsprozess wiederholt.
3. Eindämmung. Nachdem die betroffenen Assets gefunden wurden, müssen die Auswirkungen des Vorfalls eingedämmt werden. Dies kann beispielsweise durch das Herunterfahren von Servern, den Entzug von Zugriffsrechten oder die Unterbrechung der Netzwerkverbindung zu Systemen geschehen.
4. Beseitigung oder Wiederherstellung. Nachdem der Vorfall eingedämmt ist, müssen die Umgebung gesäubert und alle Spuren des Vorfalls beseitigt oder repariert werden. In diesem Schritt können auch kurzfristige Minderungsmaßnahmen angewandt werden.
5. Rekonstruktion oder Ursachenanalyse. Wenn der Vorfall eingedämmt und unter Kontrolle ist, kann die Ursachenanalyse beginnen. In diesem Analyseschritt werden die Beweise analysiert, um festzustellen, wie der Vorfall passieren konnte.

Nachbearbeitung

Die Nachbearbeitung des Vorfalls schließt das gesamte Ereignis ab. Dies geschieht in den folgenden Schritten:

Die cyber-resiliente Organisation

1. Gewonnene Erkenntnisse. Die Besprechung der gewonnenen Erkenntnisse wird zur Verbesserung und zum Lernen genutzt. In dieser Besprechung lässt das Team das Ereignis Revue passieren und identiﬁziert Verbesserungsmöglichkeiten.
2. Dokumentation. Die Dokumentation ist der Schlüssel zu einem sinnvollen Incident-Response-Prozess. Sie ist besonders dann hilfreich, wenn ähnliche Ereignisse stattfinden.
3. Verbesserung der Organisation. Ausgehend von der identifizierten Ursache bzw. den identifizierten Problemen kann die Organisation verbessert werden. Dies kann in Form von Empfehlungen oder neuen Richtlinien für die Organisation geschehen.

#### Resilience Engineering, Sicherheitslösungen und Finanzen

Eine cyber-resiliente Organisation zu sein bedeutet, dass auch die darin eingesetzten Systeme und Dienste cyber-resilient sind. Um dieses Ziel zu erreichen, müssen die Systeme bereits mit Blick auf ihre Resilienz entwickelt werden. Darüber hinaus ist es möglich, die Umgebung um gewisse Sicherheitslösungen zu erweitern, um Cybervorfälle erkennen und verhindern zu können.

Resilience Engineering

Das sogenannte Resilience Engineering umfasst die Entwicklung und Implementierung von Systemen, die den Fokus auf die Sicherheit legen (Brunton-Spall et al., 2017). Der Grad der Sicherheit hängt vom jeweiligen Bedrohungsmodell der Organisation und ihrer Risikobereitschaft ab. Daher können bei verschiedenen Systemen unterschiedliche Sicherheitsmaßnahmen im Vordergrund stehen. Die Systeme sollten so konzipiert sein, dass sie einem Angriff standhalten können. Das bedeutet, dass Angriffe, die schwerwiegender sind als der Schwellenwert der Risikobereitschaft, fehlschlagen und das System gegen solche Angriffe resilient ist. In diesem Zusammenhang wird häufig davon ausgegangen, dass Sicherheit und Benutzerfreundlichkeit entgegengesetzte Ziele verfolgen. Tatsächlich sollte dies jedoch nicht der Fall sein, denn die Organisation muss ihren Benutzerinnen Systeme zur Verfügung stellen, die sich als benutzbar und sicher erweisen. Ein zu kompliziertes System, das sich ausschließlich auf die Sicherheit konzentriert, verringert letztendlich die Gesamtsicherheit, da die Benutzer:innen Wege finden werden, die Sicherheitsmaßnahmen zu umgehen, um ihre Arbeit zu erledigen. Die Entwicklung sicherer und resilienter Systeme erfordert daher einen ganzheitlichen Blick auf die Sicherheit. Das System sollte so sicher wie möglich sein, ohne dabei die Benutzerfreundlichkeit zu beeinträchtigen. Zu diesem Zweck wurden allgemeine Kontrollmaßnahmen entwickelt, die von der Organisation durch technische oder prozessuale Maßnahmen deﬁniert werden müssen. Eine Implementierung sollte Folgendes enthalten:

* + Widerstandsmaßnahmen werden als „erste Hürde“ eingesetzt, um den Angriff zu verlangsamen und die Angreifenden zu frustrieren. Dieser Maßnahmenkatalog enthält u. a. Bandbreitenbeschränkungen oder Verschleierung.
  + Schutzmaßnahmen dienen der Verhinderung von Angriffen, z. B. Firewall-Zugriffskontrolllisten.
  + Erkennungsmaßnahmen sollten Mittel zur Erkennung eines Angriffs oder eines bösartigen Ereignisses enthalten. Dazu gehören Protokollierungs- und Prüfungsmaßnahmen.
  + Kompensationsmaßnahmen stellen eine zweite Verteidigungslinie dar, wenn eine erste Verteidigungslinie nicht möglich ist; wenn es z. B. nicht möglich ist, einen Dienst auf das interne Netzwerk zu beschränken, müssen andere Maßnahmen ergriffen werden. Zu diesen Maßnahmen gehören die Aktivierung der Multifaktor-Authentifizierung oder das Hinzufügen einer Webanwendungs-Firewall.

Sicherheitslösungen und Finanzen

Um die Cyber-Resilienz der Organisation zu verbessern, ist es außerdem möglich, Sicherheitslösungen zu kaufen. Bei diesen Lösungen kann es sich um Appliances oder Software handeln, die das allgemeine Sicherheitsniveau der Organisation steigern. Derlei Lösungen sollten sorgfältig geplant und entworfen werden, damit sie den Bedürfnissen der Organisation entsprechen. Einige dieser Lösungen umfassen

* Firewalls
* IDS/IPS-Systeme (Intrusion Detection/Intrusion Prevention)
* Spam-Schutz
* EDR-Lösungen (Endpoint Protection and Response)
* SIEM-Lösungen (Security Information and Event Management)

Firewalls

Firewalls sind Geräte oder Software, die den ein- und ausgehenden Datenverkehr gemäß verschiedener definierter Regeln überprüfen. Moderne Firewalls (auch Next Generation Firewall [NGFW] genannt) verfügen über weitere integrierte Funktionen. Dabei handelt es sich um Hardware-Geräte oder virtuelle Maschinen, die Anwendungskontrolle, Funktionen zur Bedrohungserkennung und -abwehr oder Deep-Packet-Inspection bieten können (Brook, 2020).

IDS/IPS-Systeme

Wie es der Name bereits sagt, erkennen Intrusion-Detection-/Intrusion-Prevention-Systeme (IDS/IPS) Eindringlinge im Netzwerk oder Host. Diese Systeme können Eindringlinge auf der Basis von Mustern oder mit Machine Learning und Anomalieerkennung entdecken (Barracuda, 2021).

Spam-Schutz

Spam-Schutz ﬁltert unerwünschte Spam- oder Phishing-E-Mails heraus. Dadurch wird die Wahrscheinlichkeit, dass Mitarbeitende auf eine bösartige E-Mail klicken, drastisch reduziert (DuoCircle, 2021).

EDR-Lösungen

Eine EDR-Lösung (Endpoint Protection and Response) wird dazu eingesetzt, die Endpunkte (z. B. PCs oder Server) einer Organisation vor Malware oder anderen Bedrohungen zu schützen. EDRs sammeln Daten auf dem Endpunkt und verhindern die Ausführung von Malware. Zudem bieten sie Reaktionsfunktionen wie Audit-Logging oder Ausführungsspuren von Binärdateien (Malwarebytes, 2021).

SIEM-Lösungen

Eine SIEM-Lösung (Security Information and Event Management) wird verwendet, um alle Sicherheitsereignisse in einem zentralen Tool zu verwalten. Dazu gehören Logging, Korrelation und die automatische Benachrichtigung. Solche Lösungen helfen dabei, schnell auf Sicherheitsvorfälle zu reagieren und bieten einen umfassenden Überblick über das Geschehen (impreva, 2021).

Die cyber-resiliente Organisation

#### Cyber-Versicherung

Cyber-Versicherungen werden genutzt, um das identiﬁzierte Risiko auf eine Versicherung zu verlagern. Damit werden die anderen Maßnahmen zur Schaffung einer cyber-resilienten Organisation ergänzt. Cyber-Versicherungen sind in großer Vielfalt erhältlich und decken zahlreiche Serviceleistungen und Schutzmaßnahmen ab. Eine Cyber-Versicherung kann die folgenden Ereignisse abdecken (AXA, 2021):

* + Malware-Angriffe
  + Hackerangriffe
  + Datenmissbrauch
  + Datenmanipulation
  + Offenlegung von Daten
  + Datenverlust
  + Systemausfall
  + Zweckentfremdung des Systems

Die meisten Cyber-Versicherungen enthalten eine Klausel, die besagt, dass die versicherte Partei bestimmte Schutzmaßnahmen ergreifen muss. Wenn dies nicht getan wird, kann die Versicherung die Zahlung verweigern oder den Auszahlungsbetrag verringern. AXA (2020) nennt das folgende Beispiel: „Werden Sorgfaltspflichten, Sicherheitsbestimmungen oder andere Pflichten schuldhaft verletzt, kann die Entschädigung in dem Maße gekürzt werden, in dem die Verletzung den Schaden verursacht oder beeinflusst hat“ (S. 5). Das bedeutet, dass die Versicherungsnehmer weiterhin Sicherheitsmaßnahmen durchführen müssen und sich nicht allein auf die Versicherung verlassen dürfen. Daher sollte eine Cyberversicherung zur Deckung potenzieller Verluste abgeschlossen werden, selbst wenn alle nötigen Maßnahmen zur Schadensbegrenzung und die entsprechenden Sicherheitsmaßnahmen vorhanden sind.

Zusammenfassung

Um eine cyber-resiliente Organisation zu sein, müssen gewisse Änderungen der Vorgehensweise umgesetzt werden. Zunächst wird sich der Ansatz für das Risikomanagement ändern, da Organisationen bei der Software- oder Systementwicklung zunehmend nach agilen Ansätzen arbeiten. Denn der klassische Risikomanagement-Ansatz ist nicht geeignet, um mit der sich rasch wandelnden agilen Umgebung Schritt zu halten. Entscheidungen müssen in den Entwicklungsteams getroffen werden, und die Governance-Abteilung muss Leitlinien und Richtlinien bereitstellen, um diese Projektteams zu steuern. Den nächsten Schritt im veränderten Risikomanagement-Ansatz stellt die Bereitstellung von Schulungen und Tools für die Entwicklungsteams dar. Dies hilft ihnen dabei, Risikobewertungen unabhängiger von den zentralen Sicherheitsteams durchzuführen.

Die Organisation muss ihre Software und Systeme so gestalten, dass sie eine höhere Resilienz erreichen. Dies kann mit Hilfe verschiedener Maßnahmen geschehen, die festlegen, wie die sichere Entwicklung von Software erfolgt. Dabei handelt es sich um Widerstandsmaßnahmen, Schutzmaßnahmen, Erkennungsmaßnahmen und Kompensationsmaßnahmen. Außerdem können Sicherheitslösungen implementiert werden, um die Cyber-Resilienz der Organisation weiter zu stärken. Reaktive Maßnahmen müssen geplant werden. Hier sind sowohl das Krisenmanagement als auch das Incident-Response-Management wichtig. Cyber-Resilienz kann zudem

durch eine Cyber-Versicherung abgesichert werden, wobei das Restrisiko auf eine Versicherungsgesellschaft übertragen wird. Diese Versicherungen decken eine Vielzahl von Cyber-Ereignissen ab.



# Anhang 1

## Literaturverzeichnis

### Literaturverzeichnis

Abrams, L. (2019, September 5). *Amazon AWS outage shows data in the cloud is not always safe* [Amazon-AWS-Ausfall zeigt, dass Daten in der Cloud nicht immer sicher sind]. Bleepingcomputer. https://[www.bleepingcomputer.com/news/technology/](http://www.bleepingcomputer.com/news/technology/) amazon-aws-outage-shows-data-in-the-cloud-is-not-always-safe/

American Academy of Actuaries. (o. D.). What is a catastrophe? *Catastrophe exposures and insurance industry catastrophe management practices* [Was ist eine Katastrophe? Katastrophenrisiken und Katastrophenmanagementpraktiken der Versicherungsbranche].

AXA. (2020). Duty of care and other obligations. *General Insurance Conditions (GIC) Cyber Insurance Companies* [Sorgfaltspflicht und andere Verpflichtungen. Allgemeine Versicherungsbedingungen (AVB) Cyber-Versicherungsgesellschaften].

AXA. (2021). Cyber insurance for companies [Cyber-Versicherung für Unternehmen]. https://[www.axa.ch/en/corporate-custom-](http://www.axa.ch/en/corporate-custom-) ers/offers/liability-property/cyber-insurance.html

Barracuda. (2021). What is a intrusion detection system? [Was ist ein Intrusion Detection System?] https://[www.barracuda.com/](http://www.barracuda.com/) glossary/intrusion-detection-system

Bashan, A., & Lo Giudice, M. (November 2020). *Deﬁning cyber catastrophes* [Bewältigung von Cyber-Katastrophen]. Kovrr Inc.

BBC. (27. Juli 2020). *Garmin begins recovery from ransomware attack* [Garmin beginnt mit Wiederherstellung nach Ransomware-Angriff]. https:// [www.bbc.com/news/technology-53553576](http://www.bbc.com/news/technology-53553576)

BBC. (8. Februar 2021). *Hacker tries to poison water supply of Florida city* [Hacker versucht, die Wasserversorgung einer Stadt in Florida zu vergiften]. https:// [www.bbc.com/news/world-us-canada-55989843](http://www.bbc.com/news/world-us-canada-55989843)

Benner, K. (10. Februar 2020). U.S. charges Chinese military ofﬁcers in 2017 Equifax hacking [Die USA beschuldigen chinesische Militärs des Equifax-Hackings von 2017]. *The New York Times.* https://[www.nytimes.com/2020/02/10/us/politics/equi-](http://www.nytimes.com/2020/02/10/us/politics/equi-) fax-hack-china.html

Booch, G., Jacobson Booch, I., & Rumbaugh, J. (2005). *The uniﬁed modeling language user guide* [Das UML-Benutzerhandbuch]*.* Addison-Wesley Professional.

Boyce, R. (o. D.). *Malware FAQ: Code red ISS buffer overﬂow* [Code Red ISS Buffer Überlauf]. https://[www.sans.org/secur-](http://www.sans.org/secur-) ity-resources/malwarefaq/code-red

Brook, C. (2020). What is a next generation ﬁrewall? Learn about the differences between NGFW and traditional ﬁrewalls [Was ist eine Firewall der nächsten Generation? Erfahren Sie mehr über die Unterschiede zwischen NGFW und traditionellen Firewalls]. Digitalguardian. https://digitalguardian.com/ blog/what-next-generation-ﬁrewall-learn-about-differences-between-ngfw-and-tradi- tional-ﬁrewalls

Brunton-Spall, M., Smith, R., Bird, J., & Bell, L. (2017). *Agile application security* [Agile Anwendungssicherheit]*.* OʼReilly Media.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2008). *BSI Standard 100-3: Risk analysis based on IT-Grundschutz* [Risikoanalyse auf der Grundlage des IT-Grundschutzes]*.* BSI.

Literaturverzeichnis

Burton, K. (o. D.). *The conﬁcker worm* [Der conficker-Wurm]. SANS. https://[www.sans.org/security-resources/](http://www.sans.org/security-resources/) malwarefaq/conﬁcker-worm

CBS Interactive. (11. Februar 2020). *Data from Equifax credit hack could* “*end up on the black market,*” *expert warns* [Experte warnt: Daten aus Equifax-Hack könnten auf dem Schwarzmarkt landen]. https://[www.cbsnews.com/news/china-denies-responsi-](http://www.cbsnews.com/news/china-denies-responsi-) bility-in-equifax-breach-after-doj-charges-four-military-members/

Cambridge Dictionary. (o. D.). Catastrophe [Katastrophe]. In *Cambridge dictionary*. Abgerufen am 1. Oktober 2021 von https://dictionary.cambridge.org/dictionary/english/catastrophe

Capital One Financial Corporation. (29. Juli 2019). *Capital One announces data security incident* [Capital One gibt Datensicherheitsvorfall bekannt]. https://[www.capitalone.com/about/newsroom/capital-one-announces](http://www.capitalone.com/about/newsroom/capital-one-announces)

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident han- dling guide [Leitfaden für den Umgang mit Computer-Sicherheitsvorfällen]. NIST.

Deloitte. (2016). *Cyber crisis management: Readiness, response, and recovery* [Cyber-Krisenmanagement: Bereitschaft, Reaktion und Wiederherstellung]. Deloitte. (2019). *Future of risk management* [Die Zukunft des Risikomanagements]*.*

DistriNet Research Group. (2020a). *Detectability* [Erkennbarkeit]*.* https://[www.linddun.org/detectability](http://www.linddun.org/detectability)

DistriNet Research Group. (2020b). *Disclosure of information* [Offenlegung von Informationen]. https://[www.linddun.org/](http://www.linddun.org/) disclosure-of-information

DistriNet Research Group. (2020c). *Identiﬁability* [Identiﬁzierbarkeit]. https://[www.linddun.org/identiﬁabil-](http://www.linddun.org/identiﬁabil-) ity-1

DistriNet Research Group. (2020d). LINDDUN framework [LINDDUN-Framework]. https://[www.linddun.org/lind-](http://www.linddun.org/lind-) dun

DistriNet Research Group. (2020e). *Linkability* [Verknüpfbarkeit]. https://[www.linddun.org/linkability](http://www.linddun.org/linkability)

DistriNet Research Group. (2020f). *Non-compliance* [Nicht-Konformität]. https://[www.linddun.org/non-com-](http://www.linddun.org/non-com-) pliance

DistriNet Research Group. (2020g). *Non-repudiation* [Nichtabstreitbarkeit]. https://[www.linddun.org/non-](http://www.linddun.org/non-) repudiation

DistriNet Research Group. (2020h). *Unawareness* [Unkenntnis]. https://[www.linddun.org/unaware-](http://www.linddun.org/unaware-) ness

DuoCircle. (2021). *How can you ensure your email security with anti-spam measures?* [Wie können Sie Ihre E-Mail-Sicherheit mit Anti-Spam-Maßnahmen gewährleisten?]

https://[www.duocircle.com/content/email-ﬁltering-service/anti-spam](http://www.duocircle.com/content/email-ﬁltering-service/anti-spam)

Electronic Privacy Information Center. (2020). *Electronic privacy information center*. https://epic.org/privacy/data-breach/equifax/

Equifax. (15. September 2017). *Equifax releases details on cybersecurity incident, announces personnel changes* [Equifax veröffentlicht Details zum Cybersecurity-Vorfall und kündigt personelle Veränderungen an]. https://investor.equifax.com/news-and-events/press- releases/2017/09-15-2017-224018832

Fazzini, K. (13. Februar 2019). *The great Equifax mystery: 17 months later, the stolen data has never been found, and experts are starting to suspect a spy scheme* [Das große Equifax-Rätsel: 17 Monate später wurden die gestohlenen Daten noch immer nicht gefunden, und Experten vermuten ein Spionageprogramm]. CNBC. https:// [www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html](http://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html)

Federal Trade Commission. (22. Juli 2019). *Federal Trade Commission*. https:// [www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settle-](http://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settle-) ment-ftc-cfpb-states-related

FireEye. (13. Dezember 2020). *Highly evasive attacker leverages solarwinds supply chain to compromise multiple global victims with SUNBURST backdoor* [Äußerst raffinierter Angreifer nutzt die Lieferkette von Solarwinds, um mehrere Opfer weltweit mit der SUNBURST-Backdoor zu kompromittieren]. https://www.ﬁre- eye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply- chain-compromises-with-sunburst-backdoor.html

Foley, M. J. (16. März 2021). *Azure Active Directory issue takes down Teams, Ofﬁce, Dynamics and more for some users* [Azure-Active-Directory-Problem legt Teams, Ofﬁce, Dynamics und mehr für einige Benutzer lahm]. https://[www.zdnet.com/article/azure-active-direc-](http://www.zdnet.com/article/azure-active-direc-) tory-issue-takes-down-teams-ofﬁce-dynamics-and-more-for-some-users/

Fruhlinger, J. (12. Februar 2020). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* [FAQ zum Datenverlust bei Equifax: Was ist passiert, wer war betroffen, was waren die Auswirkungen?] https://[www.csoonline.com/article/3444488/equifax-](http://www.csoonline.com/article/3444488/equifax-) data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Hern, A. (30. Dezember 2017). WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017 [WannaCry, Petya, NotPetya: Wie Ransomware im Jahr 2017 groß rauskam]. *The Guardian.* https://[www.theguardian.com/technology/2017/dec/30/](http://www.theguardian.com/technology/2017/dec/30/) wannacry-petya-notpetya-ransomware

Holmes, A. (3. April 2021). 533 million Facebook users” phone numbers and personal data have been leaked online [Die Telefonnummern und persönlichen Daten von 533 Millionen Facebook-Nutzern sind im Internet aufgetaucht]. *Business Insider*. https://[www.businessinsider.com/](http://www.businessinsider.com/) stolen-data-of-533-million-facebook-users-leaked-online-2021-4

Howard, M., & LeBlanc, D. (2009). *Writing secure code* [Sicheren Code schreiben](2. Aufl.). Microsoft Press.

impreva. (2021). Security information and event management (SIEM). https:// [www.imperva.com/learn/application-security/siem/](http://www.imperva.com/learn/application-security/siem/)

Intersoft consulting. (2018). *GDPR Consent* [DSGVO-Einwilligung]. https://gdpr-info.eu/issues/consent/

intersoft consulting. (25. Mai 2018). *GDPR: Fines/Penalties* [DSGVO: Bußgelder/Strafzahlungen]. https://gdpr-info.eu/issues/ ﬁnes-penalties/

International Organization for Standardization, & International Electrotechnical Com- mission (ISO/IEC). (2008). *Information technology*—*Security techniques*—*Information security risk management* [Informationstechnologie - Sicherheitstechniken - Risikomanagement in der Informationssicherheit]. https://[www.iso.org/standard/42107.html](http://www.iso.org/standard/42107.html)

Literaturverzeichnis

International Organization for Standardization & International Electrotechnical Com- mission (ISO/IEC). (2018). Information technology: Security techniques information security risk management [Informationstechnologie: Sicherheitstechniken Risikomanagement in der Informationssicherheit].

International Organization for Standardization, International Electrotechnical Commis- sion, & Institute of Electrical and Electronics Engineers (ISO/IEC/IEEE). (2015). *Systems and software engineering—System life cycle processes* [System- und Softwaretechnik - Lebenszyklusprozesse]. ISO. https://[www.iso.org/stand-](http://www.iso.org/stand-) ard/63711.html

Kohnfelder, L., & Garg, P. (1999). *The threats to our products* [Die Bedrohungen für unsere Produkte]. Microsoft. https:// adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx

Krebs, B. (8. September 2017). *Krebs on security* [Krebs zum Thema Sicherheit]. https://krebsonsecurity.com/2017/09/ equifax-breach-response-turns-dump

Malwarebytes. (2021). What is EDR? [Was ist EDR?] https://[www.malwarebytes.com/what-is-edr](http://www.malwarebytes.com/what-is-edr) ster- ﬁre/

Microsoft. (12. Mai 2017). *Customer guidance for WannaCrypt attacks* [Kundenleitfaden für WannaCrypt-Angriffe]. R Microsoft Security Response Center. https://msrc-blog.microsoft.com/2017/05/12/customer-guidance- for-wannacrypt-attacks/

Moore, M. (1. März 2021). *SolarWinds blames intern for weak passwords breach* [SolarWinds macht Praktikant für Passwortverletzung verantwortlich]. Techradar. https://[www.techradar.com/news/solarwinds-blames-intern-for-weak-passwords-](http://www.techradar.com/news/solarwinds-blames-intern-for-weak-passwords-) breach

Mort, S. (14. September 2017). *CVE-2017-5638: The Apache Struts vulnerability explained* [Die Apache-Struts-Schwachstelle erklärt]. Synopsys. https://[www.synopsys.com/blogs/software-security/cve-2017-5638-apache-](http://www.synopsys.com/blogs/software-security/cve-2017-5638-apache-) struts-vulnerability-explained/

Niedbala, C. (8. September 2021). *Risk management: Avoid, reduce, transfer or accept?* [Risikomanagement: Vermeiden, verringern, übertragen oder akzeptieren?]

Founder Shield. https://foundershield.com/blog/risk-management/

National Institute of Standards and Technology (NIST). (2018). *Risk management frame- work for information systems and organizations* [Risikomanagement-Framework für Informationssysteme und Organisationen]. https://[www.nist.gov/publications/](http://www.nist.gov/publications/) risk-management-framework-information-systems-and-organizations-system-life-cycle

Novaes Neto, N., Madnick, S., Moraes G. de Paula, A., & Malara Borges, N. (2020). *A case study of the Capital One data breach* [Eine Fallstudie über die Datenpanne bei Capital One]*.* Massachusetts Institute of Technology.

OʼSullivan, D. (5. September 2019). *Hundreds of millions of phone numbers once tied to Facebook accounts posted online* [Hunderte von Millionen Telefonnummern, die einmal mit Facebook-Konten verbunden waren, online veröffentlicht]. CNN Business. https://edition.cnn.com/2019/09/04/ tech/facebook-phone-numbers-exposed

Open Web Application Security Project (OWASP). (2021). *OWASP application security ver- iﬁcation standard* [OWASP-Standard zur Verifizierung der Anwendungssicherheit]. https://owasp.org/www-project-application-security-veriﬁcation- standard/

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-risk management* [Cyberrisiko-Management]*.* Springer. SAFECode. (2019). *Software security takes a champion* [Software-Sicherheit braucht einen Fürsprecher]. SAFECode.

Schneier, B. (Dezember 1999). *Attack trees* [Attack-Trees]. Schneier on Security. https://www.schne- ier.com/academic/archives/1999/12/attack\_trees.html

Schroeder, P. (6. August 2020). Capital One to pay $80 million ﬁne after data breach [Capital One zahlt nach Datenpanne 80 Millionen US-Dollar Strafe].

*Reuters.* https://[www.reuters.com/article/us-usa-banks-capital-one-ﬁn-idUSKCN2522DA](http://www.reuters.com/article/us-usa-banks-capital-one-ﬁn-idUSKCN2522DA) Shostack, A. (2014). *Threat modeling: Designing for security* [Threat Modeling: Entwerfen für die Sicherheit]*.* Wiley.

Siegel, C., & Sweeney, M. (2020). *Cyber strategy: Risk-driven security and resiliency* [Cyber-Strategie: Risikoorientierte Sicherheit und Resilienz]*.* CRC Press.

Sion, L., Wuyts, K., Yskout, K., Van Landuyt, D., & Joosen, W. (2018). *Interaction-based pri- vacy threat elicitation* [Interaktionsbasierte Erkennung von Datenschutzbedrohungen]. IEEE. https://sion.info/assets/pdf/IWPE2018/ e87bde5187d64311aac53ddd31ad30ee.pdf

Tague, N. R. (2005). *Quality toolbo*x [Instrumente für eine höhere Qualität]. American Society for Quality (ASQ). Taleb, N. N. (2007). *The black swan [Der schwarze Schwan].* Random House.

Van Scoy, R. (1992). *Software development risk: Opportunity, not problem* [Risiko in der Softwareentwicklung: Chance, nicht Problem]. Carnegie Mel- lon University.

White, J. M. (2014). *Security risk assessmen*t [Sicherheitsrisikobewertung]. Butterworth-Heinemann.

Whittaker, Z. (4. September 2019). *A huge database of Facebook users’ phone numbers found online* [Eine riesige Datenbank mit Telefonnummern von Facebook-Benutzern wurde online gefunden]. TechCrunch. https://techcrunch.com/2019/09/04/facebook-phone-num- bers-exposed/?guccounter=1

Williams, J. (2020, April 24). *OWASP risk rating methodology* [OWASP-Risikobewertungsmethode]. Open Web Application Security Project. https://owasp.org/www-community/OWASP\_Risk\_Rating\_Methodology

Woolf, N. (26. Oktober 2019). DDoS attack that disrupted internet was largest of its kind in history, experts say [Der DDoS-Angriff, der das Internet lahmlegte, war laut Experten der größte seiner Art in der Geschichte]. *The Guardian.* https://[www.theguardian.com/technology/](http://www.theguardian.com/technology/) 2016/oct/26/ddos-attack-dyn-mirai-botnet