|  |
| --- |
| IU Internationale Hochschule |
| Cyber Risk Assessment und Management |
| Kurscode |

# Übergeordnete Lernziele

Der Kurs **Cyber Risk Assessment und Management** beginnt mit einer Erläuterung, warum Risikomanagement für Unternehmen notwendig ist, sowie der Anatomie eines Datendiebstahls. Es werden grundlegende Informationen über Cyberkatastrophen und Cyberrisiken vermittelt.

Um Cyberrisiken zu managen, müssen die Bedrohungen gemessen werden. In diesem Kursbuch wird beschrieben, wie Bedrohungen gemessen werden können, welche Messverfahren angewendet werden können und wie Unternehmen Bedrohungen messen können. 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. Diese Instrumente und Methoden können dann zu einem Risikobewertungsprozess kombiniert werden. Außerdem erhalten Sie in diesem Skript eine Einführung in Standardisierungen wie das NIST Risk Management Framework, die ISO/IEC 27005 und den BSI-Standard 100-3.

Im letzten Teil dieses Skripts werden die cyberresiliente Organisation und die Cyber-Versicherung erklärt. Sie lernen, wie man eine cyberresiliente Organisation mit einer sich ständig ändernden Herangehensweise an Risikomanagement, Vorfallsreaktion, Krisenmanagement, Resilienz-Engineering und Sicherheitslösungen aufbaut.

# Lektion 1 – Organisatorisches IT-Risikomanagement

Lernziele

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

… zu erkennen, warum Risikomanagement notwendig ist.

… verschiedene Cyberkatastrophen zu identifizieren.

… ein Cyberrisiko zu definieren.

# 1. Organisatorisches IT-Risikomanagement

### Einführung

Risiken gehören zum Leben eines jeden Menschen, sei es das Risiko, seine Wohnungsschlüssel zu verlieren, oder das Risiko, ausgeraubt zu werden. Nachdem wir ein Risiko bewertet haben, formulieren 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 irgendwie 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 einem Reputationsschaden oder zu finanziellen Auswirkungen (beispielsweise zum Verlust von Kunden oder zu Geldbußen) führen kann. Genau aus diesem Grund brauchen Unternehmen ein Risikomanagement. In dieser Lektion wird der Bedarf eines Risikomanagements für Unternehmen anhand von realen Beispielen von Cyber-Katastrophen begründet. Zudem werden die grundlegenden Ziele des Risikomanagements und die Möglichkeiten der Vorbeugung von Cyberattacken mit Hilfe eines Risikomanagements erläutert. Abschließend werden die Begriffe „Risiko“ und „Bedrohung“ formal definiert.

## 1.1 Geschäftliche Notwendigkeit eines Risikomanagements

Der Aufbau und die Leitung eines Unternehmens bieten hervorragende Möglichkeiten, etwas Großes zu erreichen. Die Wahrnehmung dieser Möglichkeiten kann jedoch große Risiken mit sich bringen. Die Verantwortlichen eines Unternehmens müssen wissen, worin diese Risiken bestehen und welche Auswirkungen sie haben können. Das Wissen um die Risiken ist der erste Schritt; der nächste Schritt 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 Tatsachen 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 Risiko identifiziert werden. Ein klares 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 zur Zahlung einer Geldbuße führen würde. In diesem Fall bestände die Risikominderungsstrategie darin, den Konstruktionsfehler der Website zu beheben. Die Kosten der Fehlerbehebung betragen X Euro, und die Kosten für die Geldbuße und und die Rufschädigung betragen Y Euro. Mit diesen und anderen, detaillierteren Informationen können die Entscheidungsträger 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. Risikomanagement ist die Kunst, Entscheidungsträgern eine faktenbasierte Liste der 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).

## 1.2 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 böswilliger Akteur Zugang zu internen Daten. Dabei handelt es sich meistens um Kundendaten oder sensible Informationen. Die folgenden Beispiele beleuchten die Anatomie eines Datenangriffs. Beschrieben werden die Ereignisse und die Folgen einiger Fälle von Datenexfiltration.

### 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 Mitarbeitern, 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 nicht nur Geld: Die Firma verlor das Vertrauen der Öffentlichkeit und erhielt nach dem Leck schlechte Publicity. 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 Theorie, dass keine „normalen“ Cyberkriminellen hinter dem Vorfall steckten, sondern ein Nationalstaat. Diese Theorie wurde bestätigt, als die USA chinesische Militäroffiziere der Datenschutzverletzung beschuldigten (Benner, 2020). Die chinesische Regierung wies diese Anschuldigungen zurück (CBS Interactive, 2020). Im Endeffekt befinden sich Opferdaten nun im Besitz eines unbefugten Dritten (Fazzini, 2019), unabhängig davon, wer dafür verantwortlich war.

### Capital One-Datenpanne 2019

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

Der ursprüngliche Angriffsvektor für diesen Datenangriff war eine falsch konfigurierte Web Application Firewall (WAF). Diese falsch konfigurierte WAF wurde verwendet, 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. Mit dieser Fähigkeit lud der Angreifer fast 30 GB Daten herunter (Novaes Neto et al., 2020). Capital One wurde für diese Datenschutzverletzung mit einer 80 Millionen Dollar-Geldstrafe belegt. Die US-Aufsichtsbehörde OCC (Ofﬁce of the Comptroller of the Currency) sagte, „dass die Bank es versäumt hat, die Risiken im Vorfeld 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).

Web Application Firewall

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

AWS Metadatendienst

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

### Facebook-Datenpanne 2019

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

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

Dieser Datenverlust wurde nicht durch einen Hack der internen Systeme verursacht, sondern durch den Missbrauch einer „Funktion“. Eine Technik namens Scraping wurde 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 konnten auf der Plattform Freunde anhand ihrer Telefonnummer ausfindig machen. Böswillige Akteure nutzten dies, um Facebook-Nutzer-IDs zu extrahieren. Höchstwahrscheinlich sammelten sie Telefonnummern und überprüften, ob es zu diesen Telefonnummern passende Facebook-Profile gab. Nach einem früheren Vorfall (dem Cambridge Analytica-Skandal) hatte Facebook diese Funktion im April 2018 deaktiviert, aber die Daten waren bereits ausgespäht worden (O’Sullivan, 2019).

Im April 2021 wurden die Daten aus der 2019 gefundenen Datenbank in einem Untergrundforum veröffentlicht, was erneut ein schlechtes Licht auf die Datensicherheitspraktiken bei Facebook warf. Anfangs wurden die Daten durch den Missbrauch einer legitimen Funktion des Systems erlangt. Unter Missachtung der Vorschriften wurden die Daten ohne Zustimmung der Nutzerinnen und Nutzer an einen unbefugten Dritten weitergegeben. Dies stellt eine Verletzung der Datenschutz-Grundverordnung dar und kann zu einer Geldbuße von bis zu vier Prozent des weltweiten Gesamtumsatzes von Facebook im vorangegangen Geschäftsjahr führen (Intersoft Consulting, 2018).

### Risikomanagement eines Datenangriffs

### Wie man an den den obigen Beispielen sieht, können Datenschutzverletzungen oder Datenangriffe gravierende Auswirkungen haben. Die Folgen reichen von Rufschädigung bis hin zu empfindlichen Geldbußen. Meist ist es günstiger, das Risiko zu beheben, als die Geldbußen zu bezahlen. Daher muss das Risikomanagement das Risiko einer Datenexfiltration berücksichtigen und Kontrollen vorsehen, um ein solches Risiko zu vermindern. Wenn eine Organisation das Risiko eines Datenangriffs angeht, läuft sie ein geringeres Risiko, von Regulierungsbehörden mit einer Geldbuße belegt zu werden.

## 1.3 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. So griffen Cyberkriminelle 2020 beispielsweise 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 das vergiftete Wasser bis zu 15.000 Anwohnerinnen und Anwohner betroffen. Der Angriff hätte auf einer Stufe mit den zuvor genannten Katastrophen stehen können (BBC, 2021).

### Allgemeine Katastrophen

### Müssen Ereignisse immer so schwerwiegend sein, um als Katastrophe zu gelten? Um diese Frage zu beantworten, muss die Definition des Begriffs „Katastrophe“ untersucht werden. Das Cambridge Dictionary (o.J.) 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 bezeichnet „große Schwierigkeiten“ eine subjektive Wahrnehmung. Dabei kann es sich natürlich um Todesfälle handeln oder aber um eine bloße Unterbrechung des „normalen“ Lebens. Schließlich ist das Ausmaß einer Katastrophe von Bedeutung. Ein kleines Ereignis mag vielleicht keine Katastrophe für die ganze Welt sein, aber für eine kleinere Gruppe von Menschen oder ein Unternehmen kann es durchaus eine solche darstellen. Eine andere Definition einer Katastrophe 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). 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 einer Katastrophe nicht genau und präzise definieren. Die Schwere einer Katastrophe hängt von dem Schaden der Opfer ab, seien es Einzelpersonen oder Organisationen.

### Cyber-Katastrophen

### Cyber-Katastrophen müssen nicht zu Auswirkungen in der „realen“ Welt führen. Eine Cyber-Katastrophe ist ein Cyber-Ereignis, dessen gravierende Auswirkungen zu schweren Schäden für eine Organisation führen. Ein Ereignis kann als Cyber-Katastrophe bezeichnet werden, wenn es die folgenden Eigenschaften aufweist (Bashan & Lo Giudice, 2020):

* Ausstrahlungsradius. Eine große Gruppe von Anwendern ist vom Ereignis betroffen.
* Ausfall. Ein für Endnutzer bereitgestellter Dienst fällt aus. Der Endnutzer kann diesen Dienst nicht nutzen, was seine Arbeit oder sein Leben 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 globale 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.

|  |  |  |
| --- | --- | --- |
| 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.J.). |
| 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.J.). |
| 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. Der Angreifer verschlüsselt die Daten auf den Geräten und fordert ein Lösegeld, um die Daten wieder zu entschlüsseln (Hern, 2017). |

Diese Beispiele zeigen, dass ein globales Ereignis nicht an eine einzige Gruppe gebunden ist. Die meisten Internetnutzerinnen und -nutzer waren von diesen Vorfällen betroffen. Lokale Katastrophen betreffen jedoch kleinere Nutzergruppen, 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). |

Wie man an den den obigen Beispiel sieht, können Datenschutzverletzungen oder Datenangriffe gravierende Auswirkungen haben. Die Folgen reichen von Rufschädigung bis hin zu empfindlichen Geldbußen. Meist ist es günstiger, das Risiko zu beheben, als die Geldbußen zu bezahlen. Daher muss das Risikomanagement das Risiko einer Datenexfiltration berücksichtigen und Kontrollen vorsehen, um ein solches Risiko abzumildern. Wenn eine Organisation das Risiko eines Datenangriffs angeht, läuft sie ein geringeres Risiko, von Regulierungsbehörden mit einer Geldbuße belegt zu werden.

## 1.4 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).

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. So griffen 2020 beispielsweise Cyberkriminelle eine Wasseraufbereitungsanlage in den USA an und versuchten, dem frischen Wasser Chemikalien beizumischen, um es zu vergiften.

### Was ist eine Bedrohung?

### 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.

Vermögenswert

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

### 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, Risiken zu abstrahieren oder zusammenzufassen, wie in der folgenden Grafik gezeigt. Die oberste Stufe ist das abstrakte Risiko des „Reputationsverlusts“. Das Risiko besteht aus mehreren kleineren Risiken, die den Ruf der Organisation schädigen könnten. Zwei Beispiele hierfür sind „Datenexfiltration“ und „Mitarbeiter-Fehlverhalten“ (unziemliches Verhalten in der Öffentlichkeit). Diese Risiken bestehen wiederum aus noch spezielleren Risiken. Diese Abstraktion kann so lange fortgesetzt werden, wie es zu konkretisierende Risiken gibt.

### Zusammenfassung

### Ein Risikomanagement ist eine geschäftliche Notwendigkeit. Das Risikomanagement stellt Unternehmen Instrumente zur Verfügung, mit denen sie entscheiden können, wo sie Geld investieren, um die Widerstandsfähigkeit der Organisation zu verbessern. Es bietet Entscheiderinnen und Entscheidern faktenbasierte Unterstützung, um Investition zu priorisieren und zu planen und so Schwachstellen zu beheben.

### Für viele Organisationen stellt ein Datenexfiltrationsangriff ein ernsthaftes Risiko dar. Bei einem erfolgreichen Datenangriff (auch als Datenpanne bezeichnet) stiehlt ein Angreifer sensible oder vertrauliche Daten einer Organisation. 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. Dies können finanzielle Auswirkungen (z.B. Geldbußen oder Vergleichszahlungen) oder eine Rufschädigung sein (z.B. schlechte Presse und Kundenverlust).

### Cyber-Katastrophen sind Ereignisse mit größtmöglichen Auswirkungen auf eine Organisation. Eine Katastrophe kann globale oder lokale Auswirkungen haben. Katastrophen sind immer 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.

### 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.