IN DIESEM KAPITEL

- erfahren Sie etwas über Gefahren im Internet
- lernen Sie grundlegende Maßnahmen für mehr digitale Sicherheit kennen
- lernen Sie die Grundzüge der Risikoeinschätzung kennen

Kapitel 1
Zurück in die Zukunft? Bedrohungen im Wandel der Zeit

Digitale Bedrohungen haben in den letzten Jahrzehnten rapide zugenommen und sind zu einer ernsthaften Gefahr für Unternehmen, Organisationen und Einzelpersonen weltweit geworden. Die Bedrohungen reichen von Viren und Malware bis hin zu Phishing und Ransomware und haben sich im Laufe der Zeit ständig weiterentwickelt und verändert.

Die Geschichte des Internets

Die ersten Schritte in Richtung einer vernetzten Welt gab es in den 1960er-Jahren, als das amerikanische Verteidigungsministerium mit der Entwicklung des »Advanced Research Projects Agency Network (ARPANET)« begann. 1969 wurde das erste Datenpaket der Welt zwischen der University of California, Los Angeles (UCLA) und der Stanford University ausgetauscht.

Doch bis das Internet annähernd die Form hatte, wie wir sie heute kennen, sollten noch Jahrzehnte vergehen. So gab es beispielsweise Anfang 1994 ungefähr 700 Internetseiten. Heutzutage gibt es allein 172 Millionen ».com«- und ».net«-Domains (Stand: 25.03.2023).

Das ARPANET

Das World Wide Web ist zweifellos eine der bahnbrechendsten Innovationen im Bereich der Informationsvermittlung. Es hat eine so signifikante Auswirkung auf unseren Alltag, dass man es oft mit der Erfindung des Druckens vergleicht. Bevor das Internet jedoch zu einem praktischen Werkzeug wurde, mussten zahlreiche Grundlagen gelegt werden. Dabei sticht das ARPANET als einer der Wegbereiter des Internets hervor.

ARPANET, die Kurzform für »Advanced Research Projects Agency Network«, entstand durch die Zusammenarbeit des MIT und des US-Verteidigungsministeriums. Das Hauptziel war die Verknüpfung amerikanischer Universitäten, die für das Verteidigungsministerium forschen. Im Jahr 1969 wurden das Stanford Research Institute, die University of Utah, die University of California, Los Angeles und die University of California, Santa Barbara, miteinander vernetzt. Am 29. Oktober 1969 um 22:30 Uhr Ortszeit wurde die erste Verbindung von Host zu Host zwischen dem Stanford Research Institute und der University of California, Los Angeles, aufgebaut. Der erste Befehl »login« wurde gesendet, allerdings brach der Host-Computer während der Eingabe der ersten beiden Buchstaben zusammen, sodass die ersten übertragenen Buchstaben »lo« waren. Ab 1970 wurde die Kommunikation durch das Network Control Protocol sichergestellt.

Bis zum 5. Dezember 1969 wurden alle vier Universitäten durch das Netzwerk miteinander verbunden. Seitdem wuchs das ARPANET kontinuierlich auf 213 Hosts bis 1981 mit einem durchschnittlichen Wachstum von einem neuen Host alle 20 Tage. Im Jahr 1971 wurde das ARPANET für den Betrieb freigegeben. Am 1. Januar 1983 wurde das bisher verwendete Kommunikationsprotokoll durch TCP ersetzt. Wer an der gesamten Geschichte des Internets interessiert ist, dem sei die aufschlussreiche Zusammenfassung der Internet Society »A Brief History of the Internet« empfohlen (`https://aware.link/00101`).

Das ARPANET nutzte viele technologische Neuerungen, die mittlerweile zum Standard geworden sind. Für das Netzwerk wurden speziell Telnet und das File Transfer Protocol (FTP) entwickelt und bis 1973 implementiert. Telnet ermöglichte Client-Server-Verbindungen basierend auf einem zeichenorientierten Datenaustausch. Heutzutage wird SSH als Alternative zum unverschlüsselten Telnet verwendet. Auch FTP, das die Dateiübertragung zwischen Clients und Servern ermöglicht, legte einen wichtigen Grundstein in Bezug auf Protokolle. FTP wird noch häufig genutzt, oft in der verschlüsselten Version als Secure File Transfer Protocol (SFTP).

Die paketorientierte Kommunikation war ebenfalls eine neuartige und heute unverzichtbare Entwicklung. Obwohl die Paketvermittlung das Risiko des Paketverlusts birgt, bietet sie immense Vorteile, wie beispielsweise die gleichzeitige Nutzung der verfügbaren Leitungen durch mehrere Nutzer.

Mit der Entwicklung des neuen Netzwerks NSFNET, das Supercomputer und Wissenschaftler verband, kam das ARPANET-Projekt Ende der 1980er-Jahre zum Abschluss. Am 28. Februar 1990 wurde das ARPANET stillgelegt, einige Hosts wurden noch bis Juli 1990

betrieben. Vinton Cerf, eine der treibenden Kräfte hinter dem Projekt, verfasste zum Anlass der Stilllegung das »Requiem of the ARPANET«:

> It was the first, and being first, was best,
>
> but now we lay it down to ever rest.
>
> Now pause with me a moment, shed some tears.
>
> For auld lang syne, for love, for years and years
>
> of faithful service, duty done, I weep.
>
> Lay down thy packet, now, O friend, and sleep.

Vinton Cerf (gesamtes Requiem abrufbar bei `https://aware.link/00102`)

Es steht außer Frage, dass die Entwicklung des ARPANETs viele Protokolle hervorgebracht hat, die heute unverzichtbare Bestandteile aktueller Verfahren sind.

Creeper – die erste Malware

Bereits im ARPANET gab es erste Computerviren, welche die Geschichte des ARPANETs und die Computergeschichte allgemein geprägt haben. Die Rede ist von *Creeper* und *Reaper*.

Creeper

Creeper, entwickelt von Bob Thomas im Jahr 1971, gilt als der erste Computerwurm. Thomas wollte herausfinden, ob es möglich ist, ein replizierendes Programm zu schreiben, und setzte es aufgrund eines Fehlers im Firmennetzwerk frei. Es war nicht bösartig und hatte lediglich die Aufgabe, von Maschine zu Maschine zu springen und dabei die folgende Nachricht zu hinterlassen:

```
I'm the creeper, catch me if you can!
```

Creeper war nicht dazu ausgelegt, Schaden zu verursachen oder Daten zu stehlen. Der harmlose Wurm erwies sich aber nach kurzer Zeit als extrem lästig, da immer wieder die oben genannte Nachricht auf dem Bildschirm erschien.

Reaper

Die Antwort auf Creeper war Reaper, ein Programm, welches als erstes Anti-Virus-Programm der Geschichte gilt. Entwickelt von Ray Tomlinson hatte Reaper nur eine einzige Aufgabe: Creeper zu finden und zu löschen. Reaper hat damit den Grundstein für zukünftige Anti-Malware- und Anti-Virus-Programme gelegt, indem es demonstriert, dass schädliche oder störende Programme automatisch gefunden und beseitigt werden können. Dabei hatte Reaper selbst auch Eigenschaften eines Netzwerkwurms.

Eine kurze Geschichte der Schadsoftware

In den frühen Tagen des Internets waren Computer und Netzwerke nicht so verbreitet wie heute, und es gab nur wenige Bedrohungen, die auf Computer abzielten. Lange Zeit ging es bei Angriffen auf Computersysteme auch ausschließlich um technische Angriffe und es wurde vor allem Schadsoftware geschrieben. Wenn Schadsoftware geschrieben wurde, dann wurde sie häufig nur verbreitet um der Verbreitung willen. Das erste Computervirus auf der Welt verbreitete sich über »Disketten«, wurde im Jahr 1981 entdeckt und hieß »Elk Cloner«. Elk Cloner hatte es nur auf Apple-Computer abgesehen. Das Programm verbreitete sich selbstständig und richtete keinen direkten Schaden an den Geräten an. Für die Nutzenden war das Virus dennoch störend, da sich der Bildschirminhalt löschte und der folgende Text erschien, der erst nach einem Neustart des Computers entfernt wurde:

```
ELK CLONER:
   THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES IT'S CLONER!

IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM TOO
SEND IN THE CLONER!
```

Das erste Schadprogramm, das als digitale Pandemie bezeichnet werden kann, war »ILOVEYOU«. Es wurde von einem philippinischen Informatikstudenten entwickelt und verbreitete sich im Mai 2000 extrem schnell über das gesamte Internet. Dieses Schadprogramm wird als E-Mail-Wurm bezeichnet. Nutzende, die auf den Anhang einer infizierten Mail klickten, schickten diese Nachricht an ihr gesamtes Adressbuch weiter. Das dadurch deutlich erhöhte Aufkommen an E-Mails konnten die damaligen E-Mail-Server nicht bewältigen, und sie stürzten ab.

Der Fokus lag also gerade zu Beginn des Internets hauptsächlich auf Viren und Würmern, die darauf abzielten, Computer zu infizieren, zu verlangsamen oder zu zerstören. Diese Bedrohungen wurden hauptsächlich von Hackern entwickelt, die entweder die Grenzen der digitalen Welt ausloten oder Chaos stiften wollten.

Schadsoftware heutzutage

Mit der zunehmenden Verbreitung des Internets und der damit verbundenen Technologien wie Smartphones und anderen vernetzten Geräten hat sich das Bedrohungsszenario jedoch dramatisch verändert.

Mit vernetzten Geräten sind an dieser Stelle Geräte aus dem »Internet der Dinge« gemeint. Dies können verschiedene Geräte sein, die eine Netzwerkverbindung haben, zum Beispiel Kühlschränke, Kaffeemaschinen oder Kinderspielzeug.

Heute gibt es eine Vielzahl von Bedrohungen, die darauf abzielen, persönliche Daten zu stehlen, Finanzbetrug zu begehen oder Unternehmen zu erpressen. Phishing und andere Angriffe, die nicht die Technologie, sondern den Menschen, der die Technologie bedient, angreifen, sind zu einer der größten Bedrohungen geworden. Betrüger verwenden gefälschte E-Mails, SMS oder Social-Media-Beiträge, um ihre Opfer dazu zu bringen, persönliche Daten oder Passwörter preiszugeben. Besonders perfide sind E-Mails mit einem Dateianhang, welche im Rahmen von Ransomware-Kampagnen versendet werden. Diese Ransomware geht häufig so vor, dass sie versucht, weitere Systeme im Netzwerk zu übernehmen, Daten von diesen Systemen stiehlt und im Anschluss alles verschlüsselt und dann ein Lösegeld einfordert. Näheres zu dieser Art von Angriffen erfahren Sie in Kapitel 12.

Wenn Sie in einer Organisation oder einem Unternehmen arbeiten, ist es die Aufgabe der dortigen IT-Abteilung, die Auswirkungen von Phishing oder von schadhaften Dateianhängen zu minimieren und beispielsweise Back-up-Konzepte oder Notfallpläne vorzuhalten. Für Sie als Privatperson sind jedoch nur Sie selbst verantwortlich und wir werden Ihnen im Laufe dieses Buches das nötige Handwerkszeug an die Hand geben, um sich selbst zu schützen und die Auswirkungen eines Cyberangriffs zu minimieren.

Die digitale Bedrohungslandschaft ist also ständig im Wandel, und es ist wichtig, dass Unternehmen und Einzelpersonen sich auf dem neuesten Stand halten, um sich vor Bedrohungen zu schützen. Dazu gehören regelmäßige Software-Updates, starke Passwörter und der Einsatz von Sicherheitssoftware wie Antivirus-Programmen und Firewalls. Eine frühzeitige Erkennung von Bedrohungen und eine schnelle Reaktion sind der beste Weg, um digitale Bedrohungen zu minimieren und zu verhindern, dass sie sich zu ernsthaften Problemen entwickeln. Darüber hinaus kann es helfen, wenn Sie Informationen über aktuelle Betrugsmaschen kennen und auf dem Schirm haben. An dieser Stelle haben Sie mit dem Kauf dieses Buches schon einen Schritt in die richtige Richtung gemacht.

Wann man sicher ist

Der IT-Sicherheitsexperte Eugene Spafford sagt, dass das einzig sichere System eines ist, welches »nicht am Strom hängt, in Beton gegossen wurde und in einem mit Blei verkleideten Raum aufgestellt ist«. Ein solches System ist natürlich sicher, allerdings hat es auch eine sehr eingeschränkte Funktionalität und Nutzbarkeit. Dies ist das Dilemma, in dem sich die digitale Sicherheit heutzutage befindet. Mit jedem Schritt an zusätzlicher Sicherheit werden Systeme meist unkomfortabler in Bezug auf ihre Nutzbarkeit und die Produktivität. Darüber hinaus muss auch immer in Betracht gezogen werden, dass eine Sicherheitsmaßnahme »angemessen« sein muss.

Das geheime Lieblingsrezept für einen sehr fluffigen Pizzateig kann in einem bewachten, hermetisch abgeriegelten Gebäude in einem extra bewachten Safe lagern. Allerdings ist dies vermutlich nicht angemessen. Für das Rezept reicht es in den meisten Fällen aus, dieses in einer Küchenschublade zu lagern, ohne weitere Sicherheitsmaßnahmen zu treffen.

Auch hier ist jedoch Vorsicht die Mutter der Porzellankiste. Wenn Sie Pizzeria-Besitzer sind, lässt sich die Aufbewahrung des Rezepts im Safe schon eher rechtfertigen.

So wie mit der Pizza ist es auch mit der digitalen Sicherheit. Wir müssen für unser persönliches Risikoempfinden ein akzeptables Schutzniveau finden. Dieses kann je nach individuellen Umständen verschieden sein und muss dementsprechend immer im Einzelfall definiert werden.

Wenn wir über Risiken sprechen, müssen wir zunächst über digitale Bedrohungen sprechen. Diese sind in drei essenzielle Konzepte der digitalen Sicherheit aufgeteilt:

- ✔ Vertraulichkeit (Confidentiality)
- ✔ Integrität (Integrity)
- ✔ Verfügbarkeit (Availability)

Diese drei Konzepte werden auch als CIA-Triade bezeichnet.

Vertraulichkeit

Vertraulichkeit ist die Eigenschaft eines Systems, Ihre persönlichen Daten vor fremden Blicken zu schützen. Arbeitet man beispielsweise an einem öffentlichen Ort an einem Laptop und hat keine weiteren Schutzmaßnahmen getroffen, können Menschen, die hinter einem stehen oder sitzen, einfach auf den Rechner schauen und Daten einsehen. Eine nichttechnische Gegenmaßnahme wäre hier eine Sichtschutzfolie (s. Abbildung 1.1). Preislich bewegen sich die Folien im Bereich von 10–50 EUR.

Abbildung 1.1: Die Einsicht auf den Bildschirm ist von der Seite dank der Sichtschutzfolie erheblich schwieriger.

Technisch wird Vertraulichkeit meist über die sogenannte Kryptografie hergestellt. Es wird mithilfe der Kryptografie mathematisch sichergestellt, dass Dritte nicht unberechtigt Einsicht in die Daten erhalten.

Integrität

Integrität beschreibt die Eigenschaft eines Systems, dass die Daten nicht durch Dritte geändert werden können. Dies wird einerseits erreicht, indem technische Maßnahmen eingesetzt werden, welche nicht erlauben, Daten zu ändern, und Maßnahmen, die eine nicht erlaubte Änderung wieder rückgängig machen. Beispielsweise möchte man einer Freundin 100 Euro überweisen. Mechanismen der Integrität stellen sicher, dass man an die ausgewählte Freundin auch tatsächlich 100 Euro überweist und nicht 150 an eine andere Person. Integrität ist vor allem dann wichtig, wenn die zu schützenden Daten eine Grundlage für andere Entscheidungen darstellen. Beispielhaft zu nennen wären hier zum Beispiel Behandlungen oder Medikamente, die einem Patienten durch einen Arzt verschrieben werden.

Verfügbarkeit

Das letzte Schutzziel ist die Verfügbarkeit . Dies beschreibt die Eigenschaft eines Systems, auf Daten zuzugreifen, wenn der Zugriff benötigt wird. Verfügbarkeit kann auch durch analoge Ereignisse, wie zum Beispiel einen Stromausfall, ausgelöst werden. Auch kann eine Verschlüsselung, welche nicht mehr rückgängig zu machen ist, da beispielsweise das Passwort verloren wurde, dazu führen, dass die Verfügbarkeit eingeschränkt ist.

Diese Schutzziele erlauben es uns nun, detaillierter und genauer über Sicherheit sowie die Beeinträchtigung von Sicherheit zu sprechen.

Eine Behörde unserer Stadt fragt Informationen über uns ab. Wir versenden die Informationen über ein Portal, welches über ein nicht gültiges TLS-Zertifikat verfügt (vgl. Kapitel 4). Die Vertraulichkeit ist nun beeinträchtigt, da die Dateien während des Hochladens beim Portal nicht verschlüsselt wurden. Dies kann ebenfalls zu einer Manipulation der Integrität führen, wenn ein unberechtigter Dritter die Dateien abfängt, wenn das Dokument nicht zusätzlich qualifiziert signiert wurde. Die Verfügbarkeit der Datei ist nicht beeinträchtigt, da die Originaldatei noch auf dem Rechner liegt und weiterhin nutzbar ist.

Risikomanagement

Nachdem wir im vorherigen Abschnitt definiert haben, wie wir über die Beeinträchtigung von IT-Sicherheit sprechen wollen und in welchen Dimensionen, wollen wir nun über das Thema Risiko sprechen. Risikomanagement ist grundsätzlich der Prozess, bei dem potenzielle Gefahren und Schwachstellen identifiziert, analysiert und bewertet werden. Aus dieser

Analyse werden dann Maßnahmen zum Schutz von Informationen und Systemen abgeleitet. Im ersten Schritt muss alles, was für einen selbst »von Wert« ist, identifiziert werden. Typische Fragen, um Werte und Wertvolles im privaten Bereich zu identifizieren, sind:

- ✔ Nutze ich digitales Banking?
- ✔ Habe ich eine E-Mail-Adresse?
- ✔ Welche Plattformen, Netzwerke und Services sind mit meiner E-Mail-Adresse verknüpft?
- ✔ Habe ich viele sensible oder wichtige Daten auf meinem Computer gespeichert?
- ✔ Ist mein Smartphone ein Dreh- und Angelpunkt meiner digitalen Identität?

Nachdem wir die für uns relevanten Werte identifiziert haben, beginnen wir, uns Gedanken über mögliche Bedrohungen zu machen. Diese Bedrohungen können wir mithilfe der CIA-Triade aus dem vorherigen Abschnitt modellieren. Beispielsweise haben wir unser Smartphone als werthaltig identifiziert. Dann können wir folgende Bedrohungen identifizieren:

- ✔ **Vertraulichkeit:** Wenn das Smartphone ungesperrt an einem Ort liegt, sind Daten einsehbar.
- ✔ **Integrität:** Wenn ich in den Systemeinstellungen die »Installation aus Drittquellen« zulasse, kann dies dazu führen, dass ich schadhafte Applikationen auf mein Smartphone lade. Diese könnten andere Apps und in Verbindung stehenden Daten manipulieren.
- ✔ **Verfügbarkeit:** Vergesse ich mein Smartphone, dann bin ich nicht erreichbar und habe keinen unverzüglichen Zugriff auf die Daten auf dem Smartphone.

Im nächsten Schritt bewerten wir die Schwachstellen und die bereits durch uns eingesetzten Gegenmaßnahmen, um herauszufinden, ob diese Bedrohungen tatsächlich relevant sind:

- ✔ **Vertraulichkeit:** Wenn das Smartphone ungesperrt an einem öffentlichen Ort liegt, sind Daten einsehbar. *Die automatische Bildschirmsperre ist aktiviert. Dies ist kein Risiko.*
- ✔ **Integrität:** Wenn ich in den Systemeinstellungen die »Installation aus Drittquellen« zulasse, kann dies dazu führen, dass ich schadhafte Applikationen auf mein Smartphone lade. Diese könnten andere Apps und in Verbindung stehenden Daten manipulieren. *Diese Systemeinstellung ist nicht aktiv. Dies ist kein Risiko.*
- ✔ **Verfügbarkeit:** Vergesse ich mein Smartphone, dann bin ich nicht erreichbar und habe keinen unverzüglichen Zugriff auf die Daten auf dem Smartphone. *Es gibt keine technische Gegenmaßnahme gegen das Vergessen. Dies ist ein Risiko.*

Nun müssen wir das Risiko bestimmen. Es verbleibt ein Risiko im Bereich **Verfügbarkeit**, da wir das Smartphone immer vergessen können. Nun ist eine Argumentation zu sagen, dass kaum noch Menschen ihr Smartphone vergessen und die Wahrscheinlichkeit gering ist und wir das Risiko daher akzeptieren können. Wenn Sie diese Argumentation nicht mittragen können, da Sie immer Zugriff auf bestimmte Daten benötigen, ist eine weitere

Alternative mithilfe eines Kontrollmechanismus, das Risiko zu verlagern. Dieser könnte zum Beispiel sein, dass relevante Daten auf einem Cloud-Speicher abgelegt werden, damit die Daten nicht nur auf dem Smartphone verfügbar sind, sondern theoretisch auf jedem System mit Internetzugang.

Digitales Risikomanagement, die Bedrohungen und auch die Gegenmaßnahmen sind immer im Wandel. Das heißt, es sollten regelmäßig Risikobewertungen und -behandlungsstrategien überprüft und aktualisiert werden, um auf neue Bedrohungen und Veränderungen reagieren zu können.

Nutzen Sie Tage wie den »Ändere dein Passwort-Tag«, um sich zumindest kurz Gedanken über Ihr digitales Risiko zu machen und eventuell Gegenmaßnahmen einzuführen. Dieser Tag ist jährlich am 1. Februar.

Niemand ist perfekt und man wird immer wieder auf Bedrohungen treffen, die nicht mitbedacht wurden. Lassen Sie sich von anderen an der Stelle nicht entmutigen oder mangelnde Kompetenz unterstellen. Sehen Sie das Ganze als Erfahrungsaustausch und evaluieren Sie in Ruhe, ob der Hinweis für Sie anwendbar ist.

Der Prozess der Risikoerkennung

Das Erkennen eines Risikos ist in der Rückschau oft einfach. Die wahre Schwierigkeit im Risikomanagement besteht jedoch darin, Bedrohungen und Risiken im Voraus zu erkennen und angemessene Maßnahmen zu ergreifen, um das Risiko zu minimieren.

Risikomanagement ist dabei ein kontinuierlicher Prozess, der Risiken aktiv steuern und kontrollieren soll. Daher sollten Sie den Zyklus in regelmäßigen Abständen wiederholen, um auf neue Risiken oder Bedrohungen zu reagieren. Wenn Sie beispielsweise ein Backup an einem anderen Ort lagern, müsste dieser neue Standort eine Risikoanalyse durchlaufen. Auf diese Weise wird das Rad des Risikomanagements stetig weitergedreht.

Im weiteren Verlauf dieses Buches werden Sie verschiedene Risiken und Gegenmaßnahmen kennenlernen. Beachten Sie bitte: Sie haben vielleicht eine viel besser passende Option für sich persönlich gefunden.