IN DIESEM KAPITEL

- Cybersicherheit definieren
- Den Unterschied zwischen Cybersicherheit und Informationssicherheit verstehen
- Cybersicherheit als bewegliches Ziel begreifen
- Den Zweck von Cybersicherheit verstehen
- Risiken mit Cybersicherheit minimieren

Kapitel 1
Was ist eigentlich Cybersicherheit?

Wenn Sie sich persönlich und Ihre Familie im Cyberraum absichern möchten, müssen Sie zunächst verstehen, was Cybersicherheit bedeutet, was Ihre Ziele dabei sein sollten und wogegen Sie sich genau absichern. Die Antworten auf diese Fragen mögen einfach erscheinen, aber lassen Sie sich nicht täuschen: Sie sind es nicht. In diesem Kapitel erfahren Sie, dass die Antworten für verschiedene Menschen, Unternehmen und Abteilungen vollkommen unterschiedlich ausfallen können. Sie können sich auch im Laufe der Zeit verändern.

Cybersicherheit definieren

Sie denken sich vermutlich: Wie schwer kann es sein, den Begriff *Cybersicherheit* zu definieren? Glauben Sie mir: Wenn Sie fünf Personen fragen, werden Sie acht verschiedene Erklärungen erhalten. Der Begriff hat für verschiedene Menschen in verschiedenen Situationen verschiedene Bedeutungen. Das führt zum Einsatz ganz unterschiedlicher Prozesse und Methoden.

Wenn Sie als Privatperson beispielsweise Ihre Social-Media-Konten vor Hacker-Angriffen schützen möchten, wäre es etwas übertrieben, wenn Sie dafür die Technologien einsetzen, die das Verteidigungsministerium zum Schutz seines Netzwerks einsetzt.

Diese kleine Übersicht soll Ihnen einen Eindruck dessen vermitteln, was jeweils mit Cybersicherheit gemeint sein kann:

- ✔ **Privatanwender:** Persönliche Daten sind nur für einen selbst und für Personen zugänglich, die über eine entsprechende Berechtigung verfügen. Alle Computer und computerähnlichen Geräte funktionieren korrekt und sind frei von Malware.
- ✔ **Geschäftsinhaber:** Die Daten von Kredit- und Bankkarten sind angemessen geschützt und Sicherheitsstandards werden an der Kasse eingehalten. Sicherheitskameras funktionieren einwandfrei und ihre Daten können nicht von Unbefugten abgegriffen werden.
- ✔ **Online-Händler:** Die Server, mit denen nicht vertrauenswürdige Außenstehende laufend interagieren, sind angemessen geschützt.
- ✔ **Anbieter von Shared Services:** Mehrere Datenzentren mit einer großen Anzahl von Servern mit wiederum vielen virtuellen Servern verschiedener Unternehmen müssen gegen Angriffe verteidigt werden.
- ✔ **Staat:** Daten werden klassifiziert und jede Kategorie unterliegt bestimmten Gesetzen, Regelungen, Verfahren und Technologien.

Eine Definition von Cybersicherheit lässt sich zwar schnell aus dem Hut zaubern, doch die Erwartungen der Menschen unterscheiden sich stark, wenn sie diesen Begriff hören – abhängig davon, in welcher Situation sie sich befinden.

Technisch gesehen ist Cybersicherheit ein Teil der Informationssicherheit. Die Cybersicherheit beschäftigt sich mit Informationen und Informationssystemen, die Daten in elektronischer Form speichern und verarbeiten. *Informationssicherheit* hingegen ist die Sicherheit aller Daten, egal in welcher Form sie auftreten. Auch die Sicherung eines Aktenordners oder eines Aktenschranks gehört beispielsweise zur Informationssicherheit.

Allerdings werden diese Begriffe im täglichen Sprachgebrauch oft durcheinandergeworfen und Dinge, die eigentlich zur Informationssicherheit gehören, werden als Cybersicherheit bezeichnet. Diese begrifflichen Unschärfen kommen auch daher, weil die zwei Begriffe in vielen Situationen ineinandergreifen.

Nehmen wir einmal an, Sie schreiben ein Passwort auf einen Zettel und lassen diesen Zettel auf Ihrem Schreibtisch liegen, wo er für andere leicht zu finden ist (besser nicht), statt ihn in ein Schließfach oder einen Tresor zu legen (besser!). Wenn Sie den Zettel einfach so haben herumliegen lassen, haben Sie gegen die Grundsätze der Informationssicherheit verstoßen und nicht gegen die der Cybersicherheit.

Aber: Ihr unüberlegtes Handeln kann letztlich auch ernsthafte Auswirkungen auf die Cybersicherheit haben. Und sowieso wird die Abgrenzung zwischen Cybersicherheit und Informationssicherheit immer schwieriger, je mehr analoge Dokumente in digitale Dokumente überführt werden, zum Beispiel: wenn Sie den oben genannten Zettel mit dem Passwort nicht auf physischem Papier schreiben, sondern in Ihrer Notiz-App auf dem Smartphone.

Entwicklung von Cybersicherheit

Der Zweck von Cybersicherheit kann durchaus im Laufe der Zeit mehr oder weniger derselbe bleiben. Für die Gesetze, Verfahren und Technologien, die wir auf dem Gebiet einsetzen, gilt das allerdings nicht. Sie ändern sich mit der Zeit auf dramatische Weise. Viele der Technologien, die wir beispielsweise 1980 verwendet haben, um digitale Daten von Verbrauchern angemessen zu schützen, sind heute völlig nutzlos. Entweder weil ihr Einsatz unpraktisch wäre oder weil sie aufgrund des technologischen Fortschritts veraltet oder wirkungslos geworden sind.

Es gibt verschiedene Bereiche, die große Auswirkungen auf die Cybersicherheit gehabt haben. Die wichtigsten der letzten Jahrzehnte waren der technologische Wandel und die Weiterentwicklung von Geschäftsmodellen und Outsourcing, also die Auslagerung von Produktion und Dienstleistungen.

Technologischer Wandel

Der technologische Wandel hat enorme Auswirkungen auf die Cybersicherheit. Neue Entwicklungen bringen nicht nur neue Funktionen und neuen Komfort mit, sondern immer auch neue Risiken. Mit fortschreitender technologischer Entwicklung nehmen auch die Bedrohungen für die Cybersicherheit zu. Die Anzahl der neuen Gefahren, die in den letzten Jahrzehnten aufgrund neuer Entwicklungen entstanden sind, ist erstaunlich. In den folgenden Abschnitten beschreibe ich die Bereiche, die einen unverhältnismäßig großen Einfluss auf Cybersicherheit hatten.

Digitale Daten

In den letzten Jahrzehnten haben wir ganz erhebliche technologische Veränderungen erlebt: bei den Technologien selbst, bei denjenigen, die sie einsetzen, sowie bei der Art, wie sie verwendet werden und zu welchem Zweck. All diese Faktoren wirken sich auf Cybersicherheit aus.

Als viele der heute lebenden Menschen im Kindesalter waren, sah die Zugangskontrolle zu Daten in einer geschäftlichen Umgebung anders aus als heute. Wenn Sie damals Daten sichern wollten, legten Sie einen Ordner aus Papier in einen abschließbaren Aktenschrank und gaben den Schlüssel zu diesem Schrank nur den Mitarbeitern, die zum Zugriff berechtigt waren. Und das auch nur während der Geschäftszeiten. Für das extra Quäntchen an Sicherheit stand dieser Aktenschrank in einem Büro, das nach Feierabend abgeschlossen wurde, und das Büro wiederum befand sich in einem abschließbaren Gebäude, das durch eine Alarmanlage geschützt war.

Heute sieht das anders aus: Mit der digitalen Speicherung von Daten wurden diese einfachen Ablage- und Schutzmechanismen durch komplexe Technologien ersetzt, bei denen Nutzer, die von jedem Ort auf der Welt und zu jeder Zeit an die Daten herankommen wollen, automatisch authentifiziert werden. Dabei wird nicht nur festgestellt, ob der Nutzer berechtigt ist, auf bestimmte Daten zuzugreifen (woraufhin die richtigen Daten dann sicher bereitgestellt werden), sondern gleichzeitig werden alle möglichen Angriffe verhindert: auf

das System, das die Datenabfrage verarbeitet, auf die Daten, die gerade übertragen werden, und auf die Sicherheitsmechanismen, die beides schützen sollen.

Dazu kommt, dass wir immer weniger Briefe, sondern immer mehr E-Mails und Chat-Nachrichten schreiben. Das hat dazu geführt, dass enorme Mengen an sensiblen Informationen über Server übertragen werden, die mit dem Internet verbunden sind. Auch der Bereich der Fotografie ist nicht unberührt geblieben. Die Entwicklung von klassischem Film zur digitalen Fotografie und Videografie hat die Anforderungen an die Cybersicherheit weiter wachsen lassen. Heute wird fast jedes aufgenommene Foto oder Video elektronisch und nicht auf Filmen und Negativen gespeichert. Das führt dazu, dass Kriminelle auf der ganzen Welt Bilder stehlen und unerlaubt verbreiten oder sie sogar damit erpressen. Da Filme und Fernsehserien heute elektronisch gespeichert und übertragen werden, werden sie zuhauf unerlaubt kopiert und der breiten Masse angeboten – manchmal mit einem Virus oder anderer Schadsoftware als Sahnehäubchen oben drauf.

Das Internet und Kryptowährungen

Das Internet war die technologische Entwicklung mit den mit Abstand größten Auswirkungen auf die Cybersicherheit. Vor wenigen Jahrzehnten noch war es unvorstellbar, dass es Hackern weltweit gelingt, Geschäftsprozesse zu stören, Wahlen zu manipulieren oder eine Milliarde Euro zu stehlen. Heute kann das keiner mehr ausschließen. Vor dem Internet-Zeitalter war es für einen durchschnittlichen Hacker extrem schwer, Geld mit der Hackerei zu verdienen.

Die Einführung des Onlinebankings und des Internet-Handels in den 1990er Jahren war der Wendepunkt: Hacker konnten jetzt direkt Geld oder Waren und Dienstleistungen erbeuten. Die Anreize für eine Karriere als Cyberkrimineller wurden größer. Und sie werden immer noch größer, je mehr das Volumen des Online-Handels ansteigt. Das hängt auch mit unseren Smartphones zusammen: Leute bestellen Sachen im Internet nicht nur von ihrem Computer zu Hause aus, sondern auch, wenn sie fünf Minuten an der Straßenbahnhaltestelle warten müssen oder in einer langweiligen Besprechung sitzen.

Noch einmal verstärkt wurden diese Anreize durch die Einführung und Verbreitung von Kryptowährungen im Laufe des letzten zehn Jahre. Herkömmliche Gauner hatten stets das Problem, dass sie das erbeutete Geld letztlich von einem Bankkonto abheben mussten, wodurch sie Spuren hinterließen. Kryptowährungen sind eine charmante Lösung für dieses Problem.

Mobiles Arbeiten und Fernzugriff

Vor dem Internetzeitalter (und das ist noch gar nicht so lange her) war es für Hacker unmöglich, aus der Ferne auf Firmensysteme zuzugreifen, da diese Netzwerke nicht mit öffentlichen Netzwerken verbunden waren. Ein Fernzugriff war einfach nicht vorgesehen. Der Manager rief damals von unterwegs im Büro an und ließ sich auf diese Weise Nachrichten übermitteln. Als diese Systeme an das Internet angeschlossen wurden, brachte das zwar einige Risiken mit sich, doch anfangs hielten Firewalls Außenstehende noch effektiv davon ab, auf Unternehmensnetzwerke zuzugreifen. Da es noch keine fehlerhaften Firewall-Konfigurationen oder Bugs gab, waren die meisten internen Systeme mehr oder weniger

isoliert. Mit dem Beginn des E-Commerce und des Onlinebankings mussten bestimmte Systeme dann natürlich für die Außenwelt erreichbar sein, doch Mitarbeiternetzwerke beispielsweise blieben in aller Regel weiterhin isoliert.

Mit den ersten Technologien für Fernzugriff, wie zum Beispiel Outlook Web Access oder pcAnywhere, die sich später zu vollständigen VPN und VPN-ähnlichen Zugriffstechnologien entwickelten, änderten sich die Spielregeln allerdings grundlegend.

Smarte Geräte

Ähnliches konnten wir im Zuge der atemberaubend schnellen Verbreitung von smarten Geräten und dem *Internet der Dinge* (Sie wissen schon: Kühlschränke und Kaffeemaschinen, die mit dem Internet verbunden sind) beobachten. Dabei werden unangreifbare, abgeschottete Geräte immer häufiger durch Geräte ersetzt, die Hacker auf der anderen Seite der Welt leicht kontrollieren können. Hinzu kommt der Trend, dass auch Privatleute ihre Häuser und Wohnungen und Gärten mit Kameras und anderen Geräten überwachen lassen – und diese Daten über das Netz an Smartphones übertragen werden.

Über die gigantischen Risiken, denen diese vielen smarten Geräte ausgesetzt sind, erfahren Sie mehr in Kapitel 10.

Big Data

Big Data, das heißt große Datenaufkommen, erleichtern die Entwicklung vieler Cybersicherheitstechnologien. Gleichzeitig locken sie aber auch Angreifer an. Wenn große Datenmengen über Menschen in einem Unternehmen miteinander in Verbindung gesetzt werden, können Kriminelle leichter als je zuvor den perfekten Weg entwickeln, sich in das Unternehmen einzuschleusen und mögliche Schwachstellen in der Firmeninfrastruktur zu entdecken und auszunutzen. Unternehmen sind daher gezwungen, verschiedene Kontrollmechanismen einzuführen, um Vorfälle zu verhindern. Bücher über Bücher wurden über die Auswirkungen des technologischen Fortschritts geschrieben. Für Sie ist wichtig, Folgendes zu verstehen: Der technologische Fortschritt hatte einen erheblichen Einfluss auf Cybersicherheit. Er macht es schwieriger, Sicherheit zu gewährleisten, und wer es versäumt, seine Daten richtig zu schützen, hat viel zu verlieren.

Die Pandemie und ihre Nachwirkungen

Für viele von uns ist die COVID-19-Pandemie eine Zeit, an die wir nicht gerne zurückdenken. Sie war nicht nur eine riesige Herausforderung für die Menschheit, sondern stellte zugleich einen Wendepunkt in der Geschichte der Cybersicherheit dar. Indem sie die Menschen dazu zwang, zu Hause zu bleiben – in Häusern und Wohnungen, die in einem beispiellosen Maß voneinander isoliert waren –, veränderte das neue Coronavirus die Art und Weise, wie Menschen in der westlichen Welt arbeiten, und zwar vermutlich dauerhaft. Dies hatte auch nachhaltige Auswirkungen auf die Cybersicherheit.

Mehr zu diesem Thema finden Sie in Kapitel 6.

Kurzfristig verursachte die Pandemie alle möglichen Cybersicherheitsprobleme. Organisationen, die keine Infrastruktur für Homeoffice (mobiles Arbeiten, Heimarbeit) besaßen, oder diese nur für einen begrenzten Teil ihrer Mitarbeitenden eingerichtet hatten, sahen sich plötzlich gezwungen, Heimarbeit zu ermöglichen, oft ohne die Möglichkeit, Benutzer, Richtlinien, Verfahren und Technologien im Voraus vorzubereiten. Viele dieser Unternehmen konnten Laptops oder Sicherheitsgeräte nicht schnell genug bereitstellen, um Arbeitsunterbrechungen zu verhindern, und waren daher darauf angewiesen, dass Mitarbeiter ihre privaten Geräte für berufliche Zwecke nutzten – ohne zusätzliche Sicherheitsebenen.

Ebenso boten nur wenige Organisationen ihren Mitarbeitenden separate Internetverbindungen oder eigene Router für ihre Heimarbeitsplätze an, sodass Remote-Arbeiter fast immer physische und logische Netzwerke mit ihren privaten Geräten teilten – und möglicherweise auch mit ihren Kindern, die spielten oder am Online-Unterricht teilnahmen.

Zu den durch COVID-19 verursachten Cybersicherheitsproblemen kam hinzu, dass zwar viele Arbeitgeber eine Form von Endpunktsicherheitssoftware bereitstellten, viele andere dies aber nicht taten – und selbst diejenigen, die es taten, berücksichtigten selten hardwarebasierte Risiken. So wissen viele Arbeitgeber bis heute beispielsweise nicht, welche Router-Modelle ihre Mitarbeitenden für den Fernzugriff verwenden, oder wann diese Geräte zuletzt aktualisiert wurden.

Ein weiteres großes Cybersicherheitsproblem, das durch die Pandemie entstand, war die Verlagerung der Kommunikation von Besprechungsräumen auf virtuelle Meetings. Dadurch öffneten sich neue Möglichkeiten für Hacker, Kommunikation zu stören oder vertrauliche Informationen zu stehlen.

Natürlich führte auch die Tatsache, dass Menschen, die normalerweise am selben Ort zusammenarbeiten würden, plötzlich nicht mehr persönlich miteinander kommunizieren konnten, zu einer Zunahme von Social-Engineering-Angriffen. So kann ein Mitarbeiter im Finanzwesen einer Firma, der eine E-Mail vom »Chef« erhält, in der eine Zahlung an ein bestimmtes Konto angeordnet wird, nicht mehr einfach ein paar Schritte gehen, um persönlich zu überprüfen, ob die Nachricht tatsächlich vom Chef stammt. In Kombination mit den durch künstliche Intelligenz ermöglichten Deepfake-Fähigkeiten hat diese gesellschaftliche Veränderung für manche Organisationen zu einem wahren Albtraum geführt.

Darüber hinaus leiden Menschen, die in Haushalten mit Kindern arbeiten – sei es im Homeschooling, in Quarantäne oder einfach zu Hause lebend – oft unter weit häufigeren Unterbrechungen als im Büro. Unterbrechungen führen häufig zu Fehlern und Fehler führen oft zu Cybersicherheitsproblemen.

Auf makroökonomischer Ebene bedeutete der plötzliche Übergang zur Heimarbeit, dass viele Cybersicherheitsexperten zunehmend überlastet sind – ein Problem, das sich dadurch verschärfte, dass Organisationen Ressourcen umverteilen mussten, indem sie Mitarbeiter und finanzielle Mittel von Sicherheitsprojekten auf die Aufrechterhaltung des Geschäftsbetriebs verlagerten.

Und natürlich bot die häusliche Isolation auch Hackern mehr Zeit, ihre Fähigkeiten zu verfeinern, was möglicherweise zu dem deutlichen Anstieg an *Zero-Day*-Angriffen und anderen neuen Formen von Cyberattacken beitrug, die in der Pandemie beobachtet wurden.

Gesellschaftlicher Wandel

Die Veränderungen im menschlichen Verhalten und Interaktion hatten ebenfalls große Auswirkungen auf die Cybersicherheit. Das Internet ermöglicht es Menschen auf der ganzen Welt, in Echtzeit miteinander zu interagieren. Selbstverständlich haben Kriminelle durch diese Echtzeit-Interaktion auch die Möglichkeit, auf der ganzen Welt und zu jeder Zeit Verbrechen zu begehen, ohne dabei überhaupt vor Ort sein zu müssen. Andererseits ermöglicht das Internet Menschen, die in repressiven Regimen leben, mit Menschen in der freien Welt zu kommunizieren. Sie haben damit die Chance, Propaganda zu überwinden und sich eine Lebensqualität zu schaffen, wie es sie in demokratischen Ländern gibt. Gleichzeitig haben Cyberkrieger gegnerischer Staaten Möglichkeiten entwickelt, über exakt dasselbe Netzwerk Angriffe gegeneinander zu starten.

Der Wandel verschiedener Informationsmanagementsysteme – von Papier zu Computer, von isoliert zu internetverbunden und von ortsgebunden zu mobil – hat die Situation dramatisch verändert. Schauen Sie sich nur einmal an, welche Informationen Hacker heute stehlen können. In vielen Fällen wurde dieser Wandel aus Sicherheitsgründen zunächst gar nicht vollzogen, doch da die Menschen mittlerweile erwarten, dass alle Daten jederzeit und überall für sie verfügbar sind, kam er schließlich doch – und hat damit auch weitere Felder für Kriminalität eröffnet. Unternehmen, die in der Vergangenheit so klug waren, sensible Informationen zu schützen, indem sie sie offline aufbewahrten, können sich diesen Luxus heute nicht mehr leisten, wenn sie weiterhin im Geschäft bleiben möchten – zur Freude der Hacker.

Mit den sozialen Medien hat sich ebenfalls die Welt der Information gewandelt. Die Menschen sind daran gewöhnt, viel mehr als je zuvor über sich persönlich preiszugeben – oft auch einem viel größeren Publikum. Aufgrund dieser Verhaltensänderungen ist es heute für Kriminelle kinderleicht, Listen mit den Freunden, Arbeitskollegen und Verwandten einer Zielperson zusammenzustellen und die Kommunikationsmechanismen mit all diesen Menschen zu identifizieren. Es ist auch so einfach wie nie zuvor, herauszufinden, welche Technologien ein bestimmtes Unternehmen einsetzt und zu welchem Zweck, wohin Menschen wann reisen und welche Meinung sie zu bestimmten Themen vertreten oder welchen Musik- oder Filmgeschmack sie haben. Der Trend zur sorglosen Freigabe von Informationen geht weiter. Die meisten sind sich nicht darüber im Klaren, wie viele Informationen über sie in Computern mit Verbindung zum Internet weiterleben und wie viele andere Informationen über sie aus all diesen Daten abgeleitet werden können.

Alle diese Veränderungen zeigen sich in einer erschreckenden Realität: Aufgrund des gesellschaftlichen Wandels kann ein Krimineller von heute viel leichter eine ausgefeilte Social-Engineering-Attacke durchführen, als es noch vor zehn Jahren möglich gewesen wäre.

Wandel von Geschäftsmodellen

Fast die gesamte Welt ist heute miteinander verbunden. Das Internet hat Entwicklungen ermöglicht, die gigantische Konsequenzen für die Cybersicherheit hatten. Geschäftsmodelle, die einst undenkbar waren, bilden die Grundlage vieler Unternehmen. Heute ist es nicht ungewöhnlich, dass eine amerikanische Firma ein Callcenter in Indien betreibt und die Software auf den Philippinen entwickelt wird. Dieser Wandel hat allerdings zu Cybersicherheitsbedrohungen aller Art geführt.

In den letzten 20 Jahren konnten wir einen enormen Anstieg bei der Auslagerung von Dienstleistungen an Länder beobachten, in denen diese zu sehr viel geringeren Kosten angeboten werden. Vor nicht allzu langer Zeit wäre es pure Science-Fiction gewesen, dass ein Unternehmen in Deutschland oder den USA ausschließlich Software-Programmierer in Indien oder auf den Philippinen beschäftigt. Oder dass ein Berliner Start-up die Erstellung eines Logos in Auftrag gibt, jemandem auf der anderen Seite des Erdballs dafür 5,50 Euro bezahlt und die Lieferung am nächsten Morgen zum Frühstück im E-Mail-Postfach vorfindet. Heute ist das absolut vorstellbar.

Natürlich haben auch diese Geschäftsmodelle Auswirkungen auf Fragen der Cybersicherheit. Wenn Daten übertragen werden, müssen sie vor Zerstörung, Manipulation und Diebstahl geschützt werden. Außerdem muss gewährleistet werden, dass dem Code nicht absichtlich oder unabsichtlich Hintertüren hinzugefügt werden. Stärkerer Schutz ist erforderlich, um Diebstahl von geistigem Eigentum und andere Formen der Industrie- und Wirtschaftsspionage zu verhindern. Hacker müssen nicht mehr zwangsläufig die Unternehmen selbst knacken, sie müssen einfach nur einen oder mehrere ihrer Diensteanbieter entern, die womöglich einen deutlich lascheren Umgang mit Informationssicherheit pflegen als das eigentliche Ziel.

Politischer Wandel

Auch politische Veränderungen haben sich erheblich auf Cybersicherheit ausgewirkt. Einige dieser Auswirkungen scheinen ständig in den Schlagzeilen zu sein. Die Kombination aus Regierungsmacht und leistungsfähiger Technologie hat sich schon oft als negativ für die Bürger herausgestellt. Wenn sich der aktuelle Trend fortsetzt, wird sich der Einfluss verschiedener politischer Veränderungen auf die Cybersicherheit in der absehbaren Zukunft weiter verstärken.

Datensammlung

Die Verbreitung von Informationen im Internet und die Fähigkeit, Computer auf der ganzen Welt anzugreifen, bedeutet, dass Staaten ihre eigenen Bürger und die anderer Länder in einem Ausmaß ausspähen können, das zuvor undenkbar war. Da immer mehr geschäftliche, persönliche und gesellschaftliche Aktivitäten digitale Fußabdrücke hinterlassen, haben Staaten und Regierungen heute leichten Zugriff auf eine viel größere Menge an Informationen über ihre potenziellen Spähziele, als sie noch vor wenigen Jahren mit viel höherem Kostenaufwand hätten erwerben können. Einhergehend mit den relativ geringen Kosten für die digitale Speicherung, fortschrittlichen Big-Data-Technologien und der zu erwartenden Machtlosigkeit vieler aktueller Verschlüsselungstechnologien haben Staaten heute einen starken Anreiz, so viele Daten wie möglich über so viele Menschen wie möglich zu sammeln und zu speichern. Diese könnten ja später irgendwann einmal nützlich werden. Es besteht kaum Zweifel daran, dass einige Staaten genau so handeln.

Die langfristigen Konsequenzen dieses Phänomens sind zum aktuellen Zeitpunkt natürlich noch unbekannt, aber eines ist klar: Wenn Unternehmen Daten nicht angemessen schützen, werden sich wenig freundlich gesinnte Staaten diese unter den Nagel reißen und sie bis zu ihrem Einsatz – jetzt oder später, oder beides – auf Halde legen.

Wahlbeeinflussung

Vor einigen Jahrzenten noch war die Einflussnahme eines Staats auf die Wahlen eines anderen keine banale Angelegenheit. Selbstverständlich gab es auch früher schon Einmischungen – die gibt es, seit es Wahlen gibt –, doch waren derartige Kampagnen teuer, ressourcenaufwendig und riskant.

Um Falschinformationen und andere Propaganda zu verbreiten, mussten Materialien gedruckt und unter die Leute gebracht oder aufgenommen und über das Radio übertragen werden. Einzelne Kampagnen erreichten daher nur eine kleine Zielgruppe. Die Wirkung dieser Anstrengungen waren recht gering und das Risiko, entdeckt zu werden, war für den Initiator der Kampagne vergleichsweise hoch.

Heute haben sich die Spielregeln in weiten Teilen geändert. Für einen Staat ist es eine leichte Übung, Falschinformationen über die sozialen Medien zu verbreiten – und das Ganze kostet auch kaum noch etwas. Wenn es sich um eine wohlüberlegte Kampagne handelt, ist davon auszugehen, dass die Bevölkerung den Rest erledigt und die Falschinformationen weiterverbreitet. In Zeiten von Radioaufzeichnungen und Flugblättern war das ein Ding der Unmöglichkeit. Die Tatsache, dass immer mehr Menschen zu immer niedrigeren Kosten erreicht werden können, bedeutet auch, dass sich immer mehr Akteure wirkungsvoller in politische Wahlkämpfe einmischen können als zuvor. Andererseits können Staaten Falschinformationen über gegnerische Nationen verbreiten, um damit Unzufriedenheit bei deren Bürgern auszulösen und um Feindseligkeiten zwischen ethnischen und religiösen Gruppen in anderen Ländern zu befeuern.

Gerade in den USA ist Wahlbeeinflussung ein großes Thema, denn durch elektronisch gespeicherte Wählerregistrierungsdatenbanken, Wahlmaschinen und elektronische Stimmenauszählungen erscheint Hacking vielen immerhin machbar. Auch wenn es in der Realität vielleicht unmöglich ist, verlieren immer mehr Amerikaner heute den Glauben an Wahlen – ein Phänomen, das sich in den letzten Jahren verstärkt und auf allen Ebenen der Gesellschaft eingenistet hat. So hält sich in manchen Kreisen weiterhin hartnäckig das Gerücht, dass Donald Trump die Präsidentschaftswahl im Jahr 2016 eigentlich verloren hat, auch wenn es dafür – selbst nach gründlichen Untersuchungen der US-Ermittlungsbehörden – keinen Beweis gibt.

Sollte es also je dazu kommen, dass Wahlen online im Internet abgehalten werden, gäbe es wohl einen gigantischen Anstieg potenzieller Wahlmanipulationen durch ausländische Staaten, Kriminelle und sogar politische Rivalen. Jegliche Nachvollziehbarkeit und Nachprüfbarkeit der abgegebenen Wählerstimmen wäre dahin.

Hacktivismus und mehr Freiheiten

Darüber hinaus hat die Ausbreitung der Demokratie seit dem Zusammenbruch der Sowjetunion vor dreißig Jahren, kombiniert mit der internetbasierten Interaktion von Menschen auf der ganzen Welt, das Zeitalter des *Hacktivismus'* eingeleitet. Die Menschen wissen heute immer besser darüber Bescheid, was an anderen Orten der Welt vor sich geht. Hacker, die wütend über Politik oder Maßnahmen einer Regierung sind, können sie aus weiter Ferne ins Visier nehmen. Oft sind auch die Bürger des Landes ein Ziel.

Gleichzeitig können unterdrückte Menschen heute immer mehr über die Lebensweise von Menschen in freieren und wohlhabenderen Ländern erfahren. In einigen Staaten hat das erfreulicherweise dazu geführt, dass Menschen mehr Freiheiten gewährt werden, andere wiederum fühlten sich dazu genötigt, die Bevölkerung noch weiter in der Nutzung verschiedener Online-Dienste zu beschränken.

Sanktionen

Eine politische Dimension von Cybersicherheit sind internationale Sanktionen. Staaten, gegen die Sanktionen verhängt werden, nutzen die Möglichkeiten, die ihnen die Cyberkriminalität bietet, um diesen Sanktionen zu entgehen. Zum Beispiel wird gemeinhin angenommen, dass Nordkorea weltweit Computer mit einer Schadsoftware infizierte, die eine Kryptowährung für den totalitären Staat schürfte. Auf diese Weise entstanden dem Land keine finanziellen Einbußen durch die Sanktionen und es verdiente gleichzeitig noch Geld. Damit will ich Ihnen verdeutlichen, dass ein nicht ausreichend geschützter privater Computer direkte Auswirkungen auf internationale Politik haben kann.

Neue Machtverhältnisse

Während die militärische Macht bestimmter Nationen schon lange größer ist als die ihrer Gegner – sowohl die Qualität als auch die Quantität der Waffen variiert stark von Staat zu Staat –, sind die Machtverhältnisse in Sachen Cybersicherheit völlig andere. Zwar gibt es auch hier Unterschiede in der Qualität der verfügbaren Cyberwaffen, doch da Cyberattacken wenig kosten, hat im Grunde jedes Militär einen unbegrenzten Zugang zu allen möglichen Cyberwaffen. Meist kosten Millionen von Cyberangriffen nicht viel mehr als ein einziger.

Anders als in der realen Welt, in der ein Bombenangriff auf Zivilisten einen harten Vergeltungsschlag nach sich ziehen kann, hacken sich Schurkenstaaten in andere Länder, ohne fürchten zu müssen, dass sie je dafür zur Rechenschaft gezogen werden. Die Opfer wissen häufig gar nicht, dass sie angegriffen wurden, oder melden diese Vorfälle selten den Ermittlungsbehörden. Und wenn Angriffe gemeldet werden, lässt sich der Schuldige häufig nicht ermitteln.

Selbst wenn ein Opfer den Hack bemerkt und selbst wenn Technikexperten den Angreifer ausmachen können, streiten die verantwortlichen Nationen dies meist ab, wodurch öffentliche Gegenschläge wirksam verhindert werden. Da sich die Verantwortlichen von Cyberattacken schwer ermitteln und sich die Vorwürfe leicht abstreiten lassen, nutzen einige Staaten Cyberangriffe gerne für Präventivschläge. Sie richten Verwüstung an, müssen aber keine Vergeltung fürchten. Die Welt der Cybersicherheit hat ein erhebliches Ungleichgewicht geschaffen zwischen denen, die angreifen, und denen, die sich verteidigen.

Staaten, die sich reale Militärschläge niemals leisten könnten, steht die Welt der Cyberattacken offen. Angriffe sind dort zum Spottpreis zu haben. Die Angreifer probieren es einfach so lange, bis sie mit ihren Attacken Erfolg haben. Für einen Erfolg muss ein System nur ein einziges Mal geknackt werden. Für die Verteidigung stellt dies ein enormes Problem dar, denn sie müssen sich gegen einen einzigen Angriff schützen. Aufgrund dieser verschobenen

Machtverhältnisse gelingt es weniger mächtigen Staaten mittlerweile mit Leichtigkeit, die Systeme von Supermächten zu beeinträchtigen.

Dieses Ungleichgewicht ist übrigens auch einer der Gründe, warum Cybersicherheitsvorfälle gefühlt so oft vorkommen: Viele Hacker greifen schlichtweg so lange an, bis sie Erfolg haben. Wenn ein Unternehmen erfolgreich 10 Millionen Angriffe abwehrt, doch Angriff Nummer 10.000.001 nicht verhindern kann, kann dies ein erheblicher Vorfall sein und – Schwupps! – das Unternehmen landet in den Schlagzeilen. Sie erfahren höchstwahrscheinlich nichts davon, dass 99,999999 Prozent aller Angriffe abgewehrt wurden. Gleiches geschieht einem Unternehmen, das 99,999 Prozent aller Sicherheitspatches installiert und nur eine einzige Schwachstelle übersehen hat. Diese wird dann aber höchstwahrscheinlich sehr schnell ausgenutzt. Die Medien werden sich darauf stürzen, dabei aber vermutlich nicht berichten, dass das Unternehmen seine Systeme bis dahin fast perfekt geschützt hatte. Knapp daneben ist eben oft leider auch vorbei!

Das Cyber-Zeitalter hat auch die Machtverhältnisse zwischen Kriminellen und Strafverfolgungsbehörden verändert. Die Schurken wissen, dass die Risiken der Entdeckung und erfolgreichen Verurteilung für ein Cyberverbrechen erheblich geringer sind als bei herkömmlichen Verbrechen. Wiederholte fehlgeschlagene Versuche bei der Verbrechensbegehung sind für Cyberkriminelle auch kein Garant dafür, verhaftet zu werden, wie es sonst der Fall ist. Die Kriminellen sind sich auch darüber im Klaren, dass den Strafverfolgungsbehörden die Ressourcen fehlen, um den Großteil der Cyberverbrechen zu verfolgen. Es sind deutlich mehr Mittel und Personal erforderlich, um eine Person aufzuspüren, zu verhaften und erfolgreich anzuklagen, wenn diese von der anderen Seite der Welt aus Daten stiehlt und dabei ein Netzwerk von Computern Unbescholtener hackt. Der Dieb im Supermarkt um die Ecke, der direkt in die Überwachungskamera blickt, ist deutlich leichter zu fassen.

Da die Kosten für wiederholte Angriffe so gering sind, ist die Wahrscheinlichkeit groß, dass die Angreifer irgendwann damit erfolgreich sind. Die Wahrscheinlichkeit, geschnappt und bestraft zu werden, ist hingegen minimal. Außerdem steigt der mögliche Verdienst mit wachsender Digitalisierung. Kriminelle wissen, dass sich Straftaten im Cyberraum auszahlen, weshalb es auch so wichtig ist, dass Sie sich davor schützen.

Risiken mit Cybersicherheit minimieren

Häufig wird die Bedeutung von Cybersicherheit damit erklärt, dass sie »Hacker davon abhält, in Systeme einzubrechen und Daten und Geld zu stehlen.« Diese Beschreibung geht nicht weit genug und redet die Rolle von Cybersicherheit im modernen Heim und in der Unternehmenswelt viel zu klein. Die Bedeutung und die Ziele von Cybersicherheit sind je nach Blickwinkel unterschiedlich. Die folgenden Listen erheben keinen Anspruch auf Vollständigkeit, doch regen sie zum Denken an und zeigen, wie wichtig Cybersicherheit für Sie selbst und Ihre Familie ist.

Die Ziele von Cybersicherheit: Die CIA-Triade

Cybersicherheitsexperten erläutern die Ziele von Cybersicherheit gerne anhand der CIA-Triade. (Und bevor Sie auf falsche Gedanken kommen: Nein, der US-Geheimdienst hat

nichts damit zu tun.) Die Buchstaben CIA stehen für die *Confidentiality* (Vertraulichkeit), *Integrity* (Integrität) und *Availability* (Verfügbarkeit) von Daten:

- ✔ **Vertraulichkeit:** Informationen werden nicht offengelegt oder auf irgendeine andere Art und Weise Personen, Unternehmen oder Computerprozessen ohne Berechtigung zugänglich gemacht.

Verwechseln Sie nicht Vertraulichkeit mit Schutz der Privatsphäre: Die Vertraulichkeit von Daten ist ein Bestandteil des Schutzes der Privatsphäre. Bei Vertraulichkeit geht es insbesondere darum, dass Daten vor dem Zugriff Unbefugter geschützt werden, während es beim Schutz der Privatsphäre um viel mehr geht. Hacker, die Daten stehlen, untergraben die Vertraulichkeit.

- ✔ **Integrität:** Die Daten sind sowohl richtig als auch vollständig. *Richtig* meint hier zum Beispiel, dass die Daten nicht von einer unberechtigten Partei oder durch einen technischen Fehler verändert wurden. *Vollständig* bedeutet, dass keine Datenbestandteile durch Unberechtigte oder durch technische Fehler entfernt wurden. Zur Integrität gehört auch die Nachweisbarkeit, das heißt, die Daten müssen so erstellt und verarbeitet werden, dass niemand den Vorwurf erheben kann, sie seien falsch oder unvollständig. Cyberangriffe, bei denen Daten abgefangen und vor der Weiterleitung an ihr Ziel manipuliert werden – bekannt als *Man-in-the-Middle-Angriffe* –, beeinträchtigen die Integrität.

- ✔ **Verfügbarkeit:** Systeme zur Speicherung und Verarbeitung von Informationen, die Kommunikationsmechanismen für den Zugriff auf Informationen und deren Weiterleitung sowie die dazugehörigen Sicherheitskontrollfunktionen laufen einwandfrei und erreichen eine bestimmte Zielmarke, beispielsweise eine Verfügbarkeit von 99,99 Prozent. Wer sich nicht so intensiv mit Cybersicherheit beschäftigt, betrachtet Verfügbarkeit bei Informationssicherheit häufig als zweitrangig im Vergleich zu Vertraulichkeit und Integrität. Das ist jedoch ein Trugschluss. Verfügbarkeit ist ein wesentlicher Bestandteil von Cybersicherheit. Es ist nur nicht immer leicht, sie zu gewährleisten. Ein Grund dafür ist, dass in die Aufrechterhaltung der Verfügbarkeit oft viele Laien auf dem Gebiet der Cybersicherheit einbezogen werden. Hier haben wir dann das Problem, dass viele Köche eben den Brei verderben, insbesondere in größeren Unternehmen. *Distributed-Denial-of-Service-Angriffe* beeinträchtigen die Verfügbarkeit (siehe Kapitel 2). Bedenken Sie dabei auch, dass für DDoS-Angriffe große Mengen an gestohlener Rechenkraft und Bandbreite genutzt werden, doch die für die Verfügbarkeit Verantwortlichen oft nur begrenzte Ressourcen zur Verfügung haben.

Risiken für den Menschen

Die Bedrohungen, denen wir im Cyberraum begegnen, haben in ganz unterschiedlichen Bereichen unseres Lebens Auswirkungen auf uns:

- ✔ **Privatsphäre:** Wenn Sie die Kontrolle über Ihre persönlichen oder anderen vertraulichen Daten verlieren oder diese missbraucht werden, entstehen daraus Risiken für Sie.

- ✔ **Finanziell:** Durch Hacking können Sie finanziellen Schaden erleiden. Finanzielle Verluste können unmittelbar erfolgen, beispielsweise weil ein Hacker Ihr Onlinebanking geknackt und Ihr Konto leergeräumt hat, oder mittelbar, weil zum Beispiel Kunden eines kleinen Unternehmens diesem nach einem Sicherheitsleck nicht mehr vertrauen.
- ✔ **Beruflich:** In erster Linie erleiden natürlich Cybersicherheitsexperten einen Karriereknick, wenn ein Vorfall direkt vor ihrer Nase geschieht, ohne dass sie ihn bemerken. Doch auch die beruflichen Laufbahnen anderer können dadurch beschädigt werden. Leitende Angestellte können entlassen und Vorstandsmitglieder verklagt werden. Es kann Ihrer Karriere schaden, wenn Hacker Ihre private Kommunikation oder Daten veröffentlichen, die Sie in einem schlechten Licht dastehen lassen.
- ✔ **Geschäftlich:** Unternehmen und Geschäfte sind denselben Risiken ausgesetzt wie Privatanwender. Als bei Sony Pictures nach einem Sicherheitsleck interne Dokumente veröffentlicht wurden, warfen diese ein schlechtes Licht auf die Firma hinsichtlich ihrer Lohn- und Gehaltspraxis.
- ✔ **Persönlich:** Viele speichern private Informationen auf ihren elektronischen Geräten. Da finden sich intime Fotos oder Aufzeichnungen über die Teilnahme an Aktivitäten, die im sozialen Umfeld der Betroffenen nicht unbedingt als angemessen gelten. Diese Daten können bei Verbreitung den zwischenmenschlichen Beziehungen erheblich schaden. Auch können Kriminelle anhand erbeuteter persönlicher Daten ganze Identitäten stehlen, was viele weitere Probleme nach sich ziehen kann.
- ✔ **Leben und Gesundheit:** Immer mehr hat die Cybersicherheit auch Auswirkungen auf unsere physische Umgebung: Stromausfälle, Ausfälle von öffentlichen Dienstleistungen und sogar Störungen der Gesundheitsversorgung durch Angriffe auf Krankenhäuser. So wurde im Jahr 2020 ein Fall bekannt, in dem ein Krankenhaus durch Ransomware lahmgelegt wurde und eine Patientin verstarb, die wegen dieses Vorfalls in ein weiter entferntes Krankenhaus transportiert werden musste.