Table of Contents

» Verstehen des Unterschieds zwischen Cybersicherheit und Informationssicherheit
» Aufzeigen, warum Cybersicherheit ein sich ständig bewegendes Ziel ist
» Verstehen der Ziele der Cybersicherheit
» Betrachten der Risiken, die durch Cybersicherheit gemindert werden

Was genau ist Cybersicherheit? [1]

Um Ihre Fähigkeit zur Sicherung Ihrer eigenen und Ihrer Lieben im Cyberspace zu verbessern, müssen Sie verstehen, was Cybersicherheit bedeutet, welche Ziele Sie in Bezug auf Cybersicherheit haben sollten und gegen welche Bedrohungen Sie genau absichern.

Während die Antworten auf diese Fragen anfangs einfach und unkompliziert erscheinen mögen, sind sie es nicht. Wie Sie in diesem Kapitel sehen werden, können diese Antworten dramatisch variieren, je nach Personen, Unternehmensbereichen, Organisationen und sogar innerhalb derselben Einheit zu verschiedenen Zeiten.

Cybersicherheit bedeutet verschiedenen Leuten verschiedene Dinge

Obwohl Cybersicherheit wie ein einfacher Begriff klingt, ist er in der Praxis für verschiedene Menschen in verschiedenen Situationen recht unterschiedlich, was zu äußerst vielfältigen relevanten Richtlinien, Verfahren und Praktiken führt. Personen, die zum Beispiel ihre Social-Media-Konten vor Hackerübernahmen schützen möchten, sind äußerst unwahrscheinlich, viele der Ansätze und Technologien zu übernehmen, die Pentagon-Mitarbeiter zur Sicherung klassifizierter Netzwerke verwenden.

1 Cybersecurity A L L - I N - O N E by Joseph Steinberg; Kevin Beaver; Ted Coombs; and Ira Winkler

Typischerweise bedeutet Cybersicherheit zum Beispiel:

» Für Einzelpersonen bedeutet Cybersicherheit, dass ihre persönlichen Daten nur für sie selbst und autorisierte Personen zugänglich sind und dass ihre Computergeräte ordnungsgemäß funktionieren und frei von Malware sind.

» Für kleine Unternehmensinhaber kann Cybersicherheit die Sicherstellung umfassen, dass Kreditkartendaten ordnungsgemäß geschützt sind und dass Standards für Datensicherheit an Kassen ordnungsgemäß umgesetzt werden.

» Für Unternehmen, die Online-Geschäfte tätigen, kann Cybersicherheit den Schutz von Servern umfassen, mit denen nicht vertrauenswürdige Außenstehende regelmäßig interagieren.

» Für Shared-Service-Anbieter kann Cybersicherheit den Schutz zahlreicher Rechenzentren umfassen, die zahlreiche Server beherbergen, die wiederum viele virtuelle Server verschiedener Organisationen hosten.

» Für die Regierung kann Cybersicherheit die Einführung verschiedener Klassifizierungen von Daten umfassen, jede mit ihrem eigenen Satz von damit verbundenen Gesetzen, Richtlinien, Verfahren und Technologien.

Letztendlich ist das Wort Cybersicherheit zwar leicht zu definieren, aber die praktischen Erwartungen, die Menschen haben, wenn sie das Wort hören, variieren recht stark.
Technisch gesehen ist Cybersicherheit der Teil der Informationssicherheit, der sich mit Informationen und Informationssystemen befasst, die Daten in elektronischer Form speichern und verarbeiten, während Informationssicherheit die Sicherheit aller Arten von Daten umfasst (zum Beispiel die Sicherung einer Papiervorlage und eines Aktenschranks).

Das gesagt, heute verwenden viele Leute umgangssprachlich die Begriffe oft austauschbar und beziehen sich oft auf Aspekte der Informationssicherheit, die technisch gesehen nicht Teil der Cybersicherheit sind, als Teil letzterer. Eine solche Verwendung resultiert auch aus der Verschmelzung der beiden in vielen Situationen. Technisch gesehen hat zum Beispiel jemand, der ein Passwort auf ein Stück Papier schreibt und das Papier auf einem Schreibtisch liegen lässt, wo andere Leute das Passwort sehen können, anstelle das Papier in einem Safe oder Bankschließfach zu platzieren, ein Prinzip der Informationssicherheit verletzt, nicht der Cybersicherheit, obwohl diese Handlungen ernsthafte Cybersicherheitsfolgen haben können.

Cybersicherheit ist ein sich ständig bewegendes Ziel

Während das ultimative Ziel der Cybersicherheit im Laufe der Zeit nicht viel ändern mag, ändern sich die Richtlinien, Verfahren und Technologien, die zur Erreichung dieses Ziels eingesetzt werden, dramatisch im Laufe der Jahre. Viele Ansätze und Technologien, die beispielsweise im Jahr 1980 mehr

als ausreichend waren, um die digitalen Daten von Verbrauchern zu schützen, sind heute effektiv wertlos, entweder weil sie nicht mehr praktikabel sind oder weil technologische Fortschritte sie veraltet oder wirkungslos gemacht haben.

Obwohl es praktisch unmöglich ist, eine vollständige Liste aller Fortschritte zusammenzustellen, die die Welt in den letzten Jahrzehnten gesehen hat, und wie sich diese Änderungen auf die Cybersicherheit auswirken, können wir mehrere Schlüsselentwicklungsbereiche und ihre Auswirkungen auf die sich ständig weiterentwickelnde Natur der Cybersicherheit untersuchen: technologische Veränderungen, Verschiebungen im wirtschaftlichen Modell und Outsourcing.

Technologische Veränderungen

Technologische Veränderungen beeinflussen die Cybersicherheit enorm. Neue Risiken kommen mit den neuen Fähigkeiten und Annehmlichkeiten, die neue Angebote bieten. Da das Tempo des technologischen Fortschritts weiter zunimmt, nimmt daher auch das Tempo neuer Cybersicherheitsrisiken zu. Obwohl die Anzahl solcher Risiken, die in den letzten Jahrzehnten als Ergebnis neuer Angebote entstanden sind, erstaunlich ist, haben die in den folgenden Abschnitten beschriebenen Bereiche eine unverhältnismäßige Auswirkung auf die Cybersicherheit.

Digitale Daten

In den letzten Jahrzehnten haben sich dramatische Veränderungen in den vorhandenen Technologien sowie in der Nutzung solcher Technologien, wie sie genutzt werden und zu welchen Zwecken, ergeben. All diese Faktoren beeinflussen die Cybersicherheit.

Denken Sie zum Beispiel daran, dass die Kontrolle des Zugangs zu Daten in einer Geschäftsumgebung für viele der heute lebenden Menschen einfach bedeutete, dass der Dateninhaber eine physische Datei mit den Informationen in einen verschlossenen Schrank legte und den Schlüssel nur an Personen übergab, die der Inhaber als autorisiert erkannte, und dies nur, wenn sie den Schlüssel während der Geschäftszeiten anforderten. Zur zusätzlichen Sicherheit könnte der Dateninhaber den Schrank in einem Büro platziert haben, das nach Geschäftsschluss verschlossen war und sich selbst in einem Gebäude befand, das ebenfalls verschlossen und alarmiert war.

Heutzutage wurden jedoch einfache Ablage- und Schutzschemata durch komplexe Technologien ersetzt, die Benutzer automatisch authentifizieren müssen, die Daten möglicherweise von jedem Ort zu jeder Zeit anfordern, feststellen müssen, ob die Benutzer berechtigt sind, auf ein bestimmtes Element oder eine bestimmte Datenmenge zuzugreifen, und die richtigen Daten sicher übermitteln müssen - und das alles, während sie jegliche Angriffe gegen das System verhindern, das Datenanfragen bedient, jegliche Angriffe gegen die Daten im Transit und jegliche Sicherheitskontrollen, die beide schützen.

Darüber hinaus hat der Übergang von schriftlicher Kommunikation zu E-Mail und Chat enorme Mengen sensibler Informationen auf Internet-verbundene Server verschoben. Ebenso hat der Übergang der Gesellschaft von Film zu digitaler Fotografie und Videografie die Einsätze für die Cybersicherheit erhöht. Heutzutage werden fast alle Fotos und Videos elektronisch gespeichert, anstatt auf Film und Negativ - eine Situation, die es Kriminellen überall ermöglicht, entweder die Bilder von Menschen zu stehlen und sie zu veröffentlichen, wertvolle Bilder von Menschen mit Erpressungssoftware zu erpressen oder sie zu verwenden, um Unruhe im persönlichen Leben von Menschen zu stiften, indem sie beispielsweise gefälschte Profile auf Dating-Seiten erstellen. Die Tatsache, dass Filme und Fernsehsendungen jetzt elektronisch gespeichert und übertragen werden, hat auch Piraten ermöglicht, sie zu kopieren und der Masse anzubieten - manchmal über mit Malware infizierte Websites.

Das Internet

Der bedeutendste technologische Fortschritt in Bezug auf den Einfluss auf die Cybersicherheit war das Zeitalter des Internets und genauer gesagt die Transformation des Internets von einem kleinen Netzwerk, das Forscher an einigen Universitäten verband, in ein enormes weltweites Kommunikationssystem, das von einer enormen Anzahl von Menschen, Unternehmen und Organisationen genutzt wird. In den letzten Jahren ist das Internet auch zum Kommunikationskanal sowohl von Milliarden von intelligenten Geräten als auch von Personen geworden, die sich remote mit industriellen Steuersystemen verbinden. Noch vor wenigen Jahrzehnten war es unvorstellbar, dass Hacker aus aller Welt ein Unternehmen stören, eine Wahl manipulieren, einen Treibstoffmangel verursachen, Trinkwasser verschmutzen oder eine Milliarde Dollar stehlen könnten. Heute würde kein sachkundiger Mensch solche Möglichkeiten abtun.

Vor dem Internet-Zeitalter war es für den durchschnittlichen Hacker äußerst schwierig, finanziell durch Hacking zu profitieren. Die Einführung von Online-Banking und -Handel in den 1990er Jahren bedeutete jedoch, dass Hacker direkt Geld oder Waren und Dienstleistungen stehlen konnten - was bedeutete, dass Hacker ihre Bemühungen nicht nur schnell und einfach monetarisieren konnten, sondern auch unethische Personen starke Anreize hatten, in die Welt der Cyberkriminalität einzusteigen.

Kryptowährungen

Die Ankunft und Verbreitung von Kryptowährungen in den letzten zehn Jahren hat diese Anreize mehrfach verstärkt, zusammen mit Innovationen, die das potenzielle Return-on-Investment für Kriminelle, die in Cyberkriminalität verwickelt sind, dramatisch erhöht haben, wodurch ihre Fähigkeit, Geld durch Cyberkriminalität zu verdienen, gleichzeitig verbessert und ihre Fähigkeit, sich dabei zu verstecken, verbessert wurde. Kriminelle standen historisch vor der Herausforderung, Zahlungen zu

erhalten, da das Konto, von dem sie letztendlich das Geld abgehoben haben, oft mit ihnen verbunden werden konnte. Kryptowährungen haben solche Risiken effektiv beseitigt.

Darüber hinaus hat nicht nur der dramatische Anstieg des Werts von Kryptowährungen, die von Kriminellen in den letzten Jahren gehalten wurden, viele Ganoven bereichert und Kriminellen die Ressourcen zur Verfügung gestellt, um ihre Cyber-Arsenale zu verbessern, sondern auch die öffentliche Wahrnehmung von Kryptowährungen als schneller Weg, reich zu werden, hat Betrüger dazu veranlasst, alle Arten von auf Social Engineering basierenden Cyberverbrechen im Zusammenhang mit der Investition in Kryptowährungen zu begünstigen.

Darüber hinaus hat die Verfügbarkeit und weltweite Liquidität von Kryptowährungen Kriminellen geholfen, Geld zu waschen, das durch die Begehung aller Arten von Verbrechen erlangt wurde.

Mobile Arbeitskräfte und allgegenwärtiger Zugang

Noch vor nicht allzu vielen Jahren, in der Vor-Internet-Ära, war es für Hacker unmöglich, auf Unternehmenssysteme remote zuzugreifen, da Unternehmensnetzwerke nicht mit öffentlichen Netzen verbunden waren und oft keine Einwahlmöglichkeiten hatten. Führungskräfte unterwegs riefen oft ihre Assistenten an, um Nachrichten zu überprüfen und notwendige Daten abzurufen, während sie remote waren. In späteren Jahren könnten sie sich möglicherweise über spezielle Einwahlverbindungen über Telefonleitungen mit dem Unternehmensnetzwerk verbunden haben, um äußerst eingeschränkten Zugriff auf nur ein oder zwei spezifische Systeme zu erhalten.

Die Konnektivität zum Internet schuf natürlich Risiken, aber zunächst waren die meisten Firewalls so eingerichtet, dass Personen außerhalb der Organisation keine Kommunikation initiieren konnten - daher blieben die meisten internen Systeme trotz Firewall-Fehlkonfigurationen und/oder -Bugs relativ isoliert.

Das Aufkommen von Remote-Zugriffstechnologien - angefangen bei Diensten wie Outlook Web Access und pcAnywhere und weiterentwickelt zu vollständigen VPN- und VPN-ähnlichen Zugriffen - hat das Spiel völlig verändert.

Die dramatische Reduzierung der Kosten für zellularen Hochgeschwindigkeits-Internetzugang und die Verfügbarkeit von mobilen Datentarifen, die Datenlimits unterstützen, die ausreichen, um eine effektive Vollzeitanwendung zu ermöglichen, haben den Bedarf an der Nutzung von öffentlichen WLAN-Verbindungen dramatisch reduziert. Risiken, die man vor einigen Jahren als vernünftig erachten könnte, um verschiedene Geschäftsziele zu erreichen, sind unnötig geworden, und als solche müssen Richtlinien und Verfahren bezüglich des Zugangs zu öffentlichen WLAN-Verbindungen aktualisiert werden.

Intelligente Geräte

Ebenso bedeutet die Ankunft von intelligenten Geräten und dem Internet der Dinge (das Universum von Geräten, die mit dem Internet verbunden sind, aber keine herkömmlichen Computer sind) - deren

Verbreitung und Expansion derzeit in alarmierendem Tempo stattfinden - dass unhackbare Festkörpermaschinen schnell durch Geräte ersetzt werden, die potenziell von Hackern auf der ganzen Welt kontrolliert werden können.

Globalisierung hat auch bedeutet, dass günstige Internet der Dinge (IoT)-Geräte von Verbrauchern in einem Land bei einem Lieferanten in einem anderen Land bestellt werden können - was ohne jegliche Aufsicht allerlei unbekannte Hardware in persönliche und Unternehmensumgebungen einführt.

Big Data

Während Big Data dazu beiträgt, die Entwicklung vieler Cybersicherheitstechnologien zu erleichtern, schafft es auch Möglichkeiten für Angreifer. Indem sie große Mengen an Informationen über die Mitarbeiter einer Organisation korrelieren, können Kriminelle beispielsweise idealere Methoden zur sozialen Manipulation identifizieren, um in die Organisation einzudringen, oder mögliche Schwachstellen in der Infrastruktur der Organisation ausfindig machen. Als Ergebnis wurden verschiedene Organisationen effektiv gezwungen, alle möglichen Kontrollen zu implementieren, um das Auslaufen von Informationen zu verhindern, und die Praktiken vieler Organisationen haben alle möglichen Anschuldigungen bezüglich Datenmissbrauchs und unangemessenen Schutzes von sowohl Mitarbeitern als auch Außenstehenden hervorgerufen.

Die COVID-19-Pandemie

Die COVID-19-Pandemie markierte einen Wendepunkt in der Geschichte der Cybersicherheit. Indem sie die Menschen zwang, in Umgebungen zu Hause zu bleiben, die beispiellos voneinander isoliert waren, hat das neuartige Coronavirus die Art und Weise, wie Menschen in der westlichen Welt arbeiten, dramatisch - und wahrscheinlich dauerhaft - verändert, was wiederum mehrere signifikante Auswirkungen auf die Cybersicherheit hatte.

Kurzfristig hat die Pandemie alle Arten von Cybersicherheitsproblemen verursacht. Organisationen, die keine Home-Office-Infrastrukturen hatten oder eine solche Infrastruktur nur für einen begrenzten Teil ihrer Mitarbeiter hatten, sahen sich plötzlich damit konfrontiert, Menschen das Arbeiten von zu Hause aus zu ermöglichen - oft ohne die Möglichkeit, Benutzer, Richtlinien, Verfahren und Technologien im Voraus vorzubereiten. Viele solcher Unternehmen konnten Laptops oder Sicherheitsgeräte nicht schnell genug verteilen, um Arbeitsunterbrechungen zu verhindern, und verließen sich daher darauf, dass die Benutzer ihre persönlichen Geräte für Arbeitszwecke nutzen, ohne zusätzliche Sicherheitsebenen hinzuzufügen.

Ebenso boten nur wenige Organisationen ihren Mitarbeitern separate Internetverbindungen oder separate Router für ihre Remote-Arbeitsplätze an, sodass Remote-Mitarbeiter fast immer physische und logische Netzwerke mit ihren anderen persönlichen Geräten sowie möglicherweise mit ihren Kindern teilten, die vielleicht Spiele spielten und/oder virtuellen Unterricht besuchten. Die Sicherheitsrisiken einer solchen Vorgehensweise werden im Detail erörtert.

Die durch COVID-19 verursachten Cybersicherheitsprobleme wurden durch die Tatsache verschärft, dass zwar viele Arbeitgeber einige Formen von Endpunktsicherheitssoftware bereitstellten, viele jedoch nicht, und selbst diejenigen, die dies taten, selten hardwarebasierte Risiken ansprachen. Bis heute haben zum Beispiel viele Arbeitgeber keine Ahnung, welche Router-Modelle ihre Mitarbeiter für den Remote-Zugriff verwenden oder wann diese Geräte zuletzt aktualisiert wurden.

Ein weiteres bedeutendes Cybersicherheitsproblem, das durch die Pandemie entstanden ist, war, dass die Kommunikation zwischen Mitarbeitern von Konferenzräumen auf Remote-Meetings verschoben wurde, was Hackern die Möglichkeit eröffnete, die Kommunikation zu stören oder vertrauliche Informationen zu stehlen. Die Probleme waren so gravierend, dass im Jahr 2020 ein neuer Begriff "Zoom-Bombing" geprägt wurde, um sich auf die Praxis von Scherzbolden zu beziehen, die sich virtuellen Meetings anschlossen und dort Unruhe stifteten, zu denen sie nie eingeladen worden waren.

Natürlich hat auch die Tatsache, dass Menschen, die sonst an einem Ort zusammenarbeiten würden, plötzlich nicht mehr persönlich schnell kommunizieren können, die Tür für viele Social-Engineering-Angriffe geöffnet. Zum Beispiel kann ein CFO, der eine E-Mail vom Chef erhält, in der er gebeten wird, der Firma für Dienstleistungen eine bestimmte Zahlung zu leisten, die Gültigkeit des Antrags nicht überprüfen, wie er es in der Vergangenheit oft getan hat, indem er zehn Fuß zum Büro des Chefs geht, um zu bestätigen, dass der Chef die Nachricht tatsächlich gesendet hat.

Ebenso leiden Menschen, die in Häusern arbeiten, in denen Kinder virtuellen Unterricht haben, in Quarantäne sind oder einfach leben, oft unter viel mehr Unterbrechungen, als wenn sie in einem Büro arbeiten würden. Unterbrechungen führen oft zu Fehlern, und Fehler führen oft zu Cybersicherheitsproblemen. Die Belastung durch lang anhaltende soziale Isolation erhöht ebenfalls die Wahrscheinlichkeit, dass Menschen gefährliche Cybersicherheitsfehler machen.

Auf makroökonomischer Ebene bedeutet der plötzliche Wechsel zu Heimarbeit-Regelungen, dass viele Cybersicherheitsexperten zunehmend überlastet sind, ein Problem, das durch Organisationen weiter verschärft wird, die Ressourcen neu zuweisen müssen - manchmal sowohl Personen als auch Gelder von Sicherheitsprojekten auf Bemühungen zur Sicherstellung der Betriebskontinuität umlenken.

Und natürlich haben viele Hacker durch ihre Einschränkung auf ihre Häuser mehr Zeit, an ihren Handwerken zu arbeiten, was möglicherweise zu dem signifikanten Anstieg der Anzahl von Zero-Day-Angriffen und anderen neueren Formen von Cybersicherheitsangriffen beigetragen hat, die seit Beginn der Pandemie beobachtet werden. Wir werden viele der gängigen Cyberangriffe analysieren.

Es wurden ganze Bücher über die Auswirkungen des technologischen Fortschritts geschrieben. Der wichtigste Punkt zu verstehen ist, dass der technologische Fortschritt einen erheblichen Einfluss auf die Cybersicherheit hatte, die Sicherheit schwieriger zu gewährleisten machte und die Einsätze erhöhte, wenn Parteien es versäumen, ihre Vermögenswerte ordnungsgemäß zu schützen. Darüber hinaus können unvorhergesehene Entwicklungen, wie Pandemien, plötzliche, enorme technologische Veränderungen mit sich bringen, die immense Cybersicherheitsgefahren bergen.

Soziale Veränderungen

Verschiedene Veränderungen in den Verhaltensweisen und der Interaktion zwischen Menschen haben ebenfalls einen erheblichen Einfluss auf die Cybersicherheit gehabt. Das Internet ermöglicht es zum Beispiel Menschen aus der ganzen Welt, in Echtzeit miteinander zu interagieren. Natürlich ermöglicht diese Echtzeitinteraktion auch Kriminellen auf der ganzen Welt, Verbrechen aus der Ferne zu begehen. Aber es ermöglicht auch Bürgern repressiver Länder und freier Länder, zu kommunizieren und schafft damit Möglichkeiten, die ewige Propaganda zu zerstreuen, die als Ausrede für das Scheitern des Totalitarismus, Lebensqualität zu erzeugen, genutzt wird, die mit der demokratischen Welt vergleichbar ist. Gleichzeitig bietet es den Cyberkriegern von Regierungen, die sich gegenseitig im Streit liegen, die Möglichkeit, Angriffe über dasselbe Netzwerk zu starten.

Die Umwandlung verschiedener Informationsmanagementsysteme von Papier zu Computer, von isoliert zu Internet-vernetzt und von nur im Büro zugänglich zu von jedem Smartphone oder Computer zugänglich, hat die Gleichung dramatisch verändert, wenn es darum geht, welche Informationen Hacker stehlen können. Und die COVID-19-Pandemie hat viele dieser Probleme in den Vordergrund gerückt.

Darüber hinaus, in vielen Fällen, in denen technologische Umstellungen aus Sicherheitsgründen zunächst nicht durchgeführt wurden, hat der Druck, der aus den Erwartungen der modernen Menschen resultiert, dass jede Art von Daten zu jeder Zeit und von überall aus verfügbar sein muss, solche Umstellungen erzwungen und damit zusätzliche Möglichkeiten für Kriminelle geschaffen. Zur Freude von Hackern haben viele Organisationen, die in der Vergangenheit sensible Informationen durch Offline-Aufbewahrung geschützt haben, einfach die Möglichkeit verloren, solche Schutzmaßnahmen zu genießen, wenn sie im Geschäft bleiben wollen. Kein modernes Beispiel verdeutlicht dies besser als der plötzliche globale Übergang zu Fernarbeitsregelungen im Jahr 2020.

Soziale Medien haben auch die Welt der Information transformiert - mit Menschen, die sich daran gewöhnt haben, weit mehr über sich selbst zu teilen als je zuvor - oft auch mit viel größeren Zielgruppen als zuvor. Heute ist es aufgrund des Verhaltenswandels in dieser Hinsicht trivial für Übeltäter von überall her, Listen von Freunden, Berufskollegen und Verwandten eines Ziels zusammenzustellen und Mechanismen für die Kommunikation mit all diesen Menschen zu etablieren. Ebenso ist es einfacher als je zuvor, herauszufinden, welche Technologien ein bestimmtes Unternehmen nutzt und wofür, Reisepläne von Menschen herauszufinden und ihre Meinungen zu verschiedenen Themen oder ihre Vorlieben in Musik und Filmen zu ermitteln. Der Trend zu vermehrtem Teilen setzt sich fort. Die meisten Menschen sind sich blind dessen bewusst und machen sich keine Gedanken darüber, wie viele Informationen über sie auf Internet-vernetzten Maschinen vorhanden sind und wie viele andere Informationen über sie aus den genannten Daten extrapoliert werden können.

All diese Veränderungen haben sich in eine beängstigende Realität übersetzt: Aufgrund der gesellschaftlichen Veränderungen können Übeltäter heute viel größere und raffiniertere Social-Engineering-Angriffe starten als noch vor wenigen Jahren.

Ökonomische Modellverschiebungen

Die nahezu weltweite Vernetzung hat es dem Internet ermöglicht, andere Trends mit enormen Auswirkungen auf die Cybersicherheit zu fördern. Betriebsmodelle, die einst undenkbar waren, wie beispielsweise das einer amerikanischen Firma, die ein Callcenter in Indien und eine Softwareentwicklungsfirma auf den Philippinen nutzt, sind zum Hauptbestandteil vieler Unternehmen geworden. Diese Veränderungen bringen jedoch Cybersicherheitsrisiken vieler Arten mit sich.

In den letzten 20 Jahren hat die Auslagerung verschiedener Aufgaben aus teureren Regionen in Regionen, in denen sie zu viel geringeren Kosten durchgeführt werden können, ein enormes Wachstum erlebt. Die Vorstellung, dass sich ein Unternehmen in den Vereinigten Staaten hauptsächlich auf Programmierer in Indien oder den Philippinen verlassen könnte, oder dass Unternehmer in New York kurz bevor sie schlafen gehen, jemandem auf der anderen Seite des Globus 5,50 US-Dollar zahlen könnten, um ein Logo für ihr Unternehmen zu erstellen, und das Logo dann sofort am nächsten Morgen in ihrem E-Mail-Postfach haben könnten, klang vor einer Generation wie ökonomische Science-Fiction. Heute ist es nicht nur üblich, sondern in vielen Fällen ist es häufiger als jede andere Methode, ähnliche Ergebnisse zu erzielen.

Natürlich ergeben sich aus solchen Transformationsprozessen in der Art und Weise, wie Geschäfte getätigt werden, viele Cybersicherheitsfragen.

Daten, die übertragen werden, müssen vor Zerstörung, Modifikation und Diebstahl geschützt werden, und die Globalisierung bedeutet, dass eine größere Sicherheit erforderlich ist, um sicherzustellen, dass keine Hintertüren absichtlich oder unbeabsichtigt in den Code eingefügt werden. Größere Schutzmaßnahmen sind erforderlich, um den Diebstahl von geistigem Eigentum und andere Formen von Wirtschaftsspionage zu verhindern. Code, der in ausländischen Ländern entwickelt wurde, könnte beispielsweise Gefahr laufen, von Agenten ihrer jeweiligen Regierungen mit Hintertüren versehen zu werden. Ebenso könnten in Computergeräte Hintertüren in Hardwarekomponenten eingefügt werden - ein Problem, mit dem die Regierung zu kämpfen hat, während wir diskutieren.

Hackern ist es nicht mehr unbedingt erforderlich, direkt in die Organisationen einzudringen, die sie hacken möchten; sie müssen lediglich einen oder mehrere der Anbieter der Organisationen kompromittieren. Und solche Anbieter sind möglicherweise bei der Informationssicherheit und den Personalpraktiken weit weniger sorgfältig als das endgültige Ziel oder unterliegen möglicherweise der Manipulation durch Regierungen, die bei weitem weniger respektvoll gegenüber den Rechten der Menschen sind als die Machthaber am endgültigen Standort des Ziels.

Politische Verschiebungen

Wie bei technologischen Fortschritten haben politische Verschiebungen enorme Auswirkungen auf die Cybersicherheit, von denen einige dauerhafte Fixpunkte in den Nachrichten zu sein scheinen. Die Kombination aus Regierungsmacht und mächtiger Technologie hat sich oft als teuer für gewöhnliche

Menschen erwiesen. Wenn die aktuellen Trends anhalten, wird der Einfluss verschiedener politischer Verschiebungen auf die Cybersicherheit in absehbarer Zukunft erheblich zunehmen.

Datensammlung

Die Verbreitung von Informationen online und die Möglichkeit, weltweit Maschinen anzugreifen, bedeuten, dass Regierungen die Bürger ihres eigenen Landes und die Bewohner anderer Nationen in einem bisher nie dagewesenen Umfang ausspionieren können.

Darüber hinaus haben Regierungen dank immer mehr digitaler Spuren von Geschäfts-, persönlichen und gesellschaftlichen Aktivitäten einen viel einfacheren Zugang zu einer viel größeren Menge an Informationen über ihre potenziellen Geheimdienstziele als noch vor wenigen Jahren zu deutlich höheren Kosten möglich war. In Verbindung mit den relativ geringen Kosten für digitale Speicherung, fortschreitenden Big-Data-Technologien und der erwarteten letztendlichen Unwirksamkeit vieler heutiger Verschlüsselungstechnologien aufgrund des Aufkommens von Quantencomputing und anderen hochmodernen Entwicklungen haben Regierungen einen starken Anreiz, so viele Informationen wie möglich über so viele Menschen wie möglich zu sammeln, für den Fall, dass sie später einmal nützlich sein könnten. Es ist wahrscheinlicher als nicht, dass feindselige Regierungen bereits damit begonnen haben, Dossiers über die Personen zusammenzustellen, die in 25 Jahren als Präsident und Vizepräsident der Vereinigten Staaten fungieren werden.

Die langfristigen Folgen dieses Phänomens sind offensichtlich noch nicht bekannt, aber eines ist klar: Wenn Unternehmen Daten nicht ordnungsgemäß schützen, werden weniger freundliche Nationen sie höchstwahrscheinlich beschaffen und für den Einsatz entweder kurzfristig, langfristig oder beides speichern.

Wahlbeeinflussung

Vor einer Generation war es keine triviale Angelegenheit, wenn eine Nation in die Wahlen einer anderen eingriff. Natürlich gab es solche Einmischungen - sie haben stattgefunden, solange es Wahlen gibt -, aber bedeutende Einmischungskampagnen durchzuführen war teuer, ressourcenintensiv und äußerst riskant.

Um Desinformationen und andere Propaganda zu verbreiten, mussten Materialien gedruckt und physisch verteilt oder aufgezeichnet und über das Radio übertragen werden, was bedeutete, dass individuelle Kampagnen wahrscheinlich nur kleine Zielgruppen erreichen würden. Infolgedessen waren die Wirksamkeit solcher Bemühungen oft recht gering, und das Risiko, dass die Partei, die die Kampagne betrieb, entdeckt wurde, relativ hoch und trug oft das Potenzial für schwerwiegende Folgen.

Die Manipulation von Wählerregistrierungsdatenbanken, um legitime Wähler am Wählen zu hindern und/oder falschen Wählern das Wählen zu ermöglichen, war äußerst schwierig und mit enormen Risiken verbunden; jemand "aus dem Inneren", der tatsächlich Einfluss auf Wahlergebnisse haben wollte, müsste wahrscheinlich nichts weniger als ein Verräter sein. In einem Land wie den Vereinigten Staaten, in dem Wählerregistrierungsdatenbanken dezentralisiert und auf Landkreisebene verwaltet werden, wäre es wahrscheinlich unmöglich gewesen, ausreichend Saboteure zu rekrutieren, um eine bedeutende Wahl wirklich zu beeinflussen, und die Wahrscheinlichkeit, beim Versuch, dies zu tun, erwischt zu werden, wäre wahrscheinlich extrem hoch gewesen.

Ebenso war es im Zeitalter von Papierwahlzetteln, die persönlich abgegeben und manuell ausgezählt wurden, für eine ausländische Macht praktisch unmöglich, tatsächliche Stimmenzählungen in großem Umfang zu manipulieren.

Heutzutage hat sich jedoch das Spiel geändert. Eine Regierung kann leicht Desinformationen über soziale Medien zu extrem niedrigen Kosten verbreiten. Wenn sie eine gut durchdachte Kampagne entwirft, kann sie darauf vertrauen, dass andere Personen die Desinformationen verbreiten - etwas, das Menschen im Zeitalter von Radioaufnahmen und gedruckten Broschüren nicht in Massen tun konnten. Die Fähigkeit, viele mehr Menschen zu erreichen, zu einem viel geringeren Preis als je zuvor, hat dazu geführt, dass mehr Parteien in politische Kampagnen eingreifen können und dies mit mehr Wirksamkeit tun können als in der Vergangenheit. Ebenso können Regierungen Desinformationen verbreiten, um zivilen Unmut in den Nationen ihrer Gegner zu schüren und Feindseligkeiten zwischen ethnischen und religiösen Gruppen in fremden Ländern zu verbreiten.

Unsichere Briefwahlunterlagen, wie sie während der Präsidentschaftswahl 2020 in den Vereinigten Staaten verwendet wurden, haben das Misstrauen verstärkt. Und mit elektronisch gespeicherten Wählerregistrierungsdatenbanken, die manchmal auf Servern gespeichert sind, die zumindest indirekt mit dem Internet verbunden sind, könnten Datensätze möglicherweise von weit entfernten Orten aus hinzugefügt, geändert oder gelöscht werden, ohne entdeckt zu werden. Selbst wenn ein solches Hacking in Wirklichkeit unmöglich ist, hat die Tatsache, dass viele Bürger heute glauben, dass dies möglich sein könnte, zu einem Untergraben des Vertrauens in Wahlen geführt, ein Phänomen, das wir in den letzten Jahren beobachtet haben und das sich auf allen Ebenen der Gesellschaft ausgebreitet hat. Selbst Jimmy Carter, ein ehemaliger Präsident der Vereinigten Staaten, äußerte zu einem Zeitpunkt, dass er glaubte, dass eine vollständige Untersuchung der Präsidentschaftswahl 2016 zeigen würde, dass Donald Trump die Wahl verloren hat - obwohl es absolut keine Beweise dafür gibt, selbst nach einer gründlichen FBI-Untersuchung des Falls. Aussagen und Handlungen von der anderen Seite des politischen Spektrums - einschließlich des schrecklichen Chaos im Kapitol der Vereinigten Staaten nach der Präsidentschaftswahl 2020 - zeigten deutlich, dass Bedenken hinsichtlich der Integrität von Wahlen und der Wahrnehmung, dass Wahlen durch Cyberangriffe und andere technologiebasierte Techniken manipulierbar sein könnten, parteiübergreifend sind. Es ist auch nicht schwer sich vorzustellen, dass, wenn Online-Abstimmungen jemals eingeführt würden, das Potenzial für Manipulationen durch ausländische Regierungen, Kriminelle und sogar politische Parteien innerhalb der wählenden Nation - und für die Beseitigung der heute vorhandenen Überprüfbarkeit von Wahlzetteln - astronomisch ansteigen würde.

Als Anzeichen dafür, wie stark die Besorgnis um mögliche Wahlmanipulationen wächst, ist zu beachten, dass die Vereinigten Staaten vor einem Jahrzehnt die Computersysteme im Zusammenhang

mit Wahlen nicht als kritische Infrastruktur betrachteten und keine direkten Bundesmittel bereitstellten, um solche Systeme zu sichern. Heute ist den meisten Menschen klar, dass der Bedarf an Cybersicherheit in solchen Bereichen von höchster Bedeutung ist, und die Politik und das Verhalten von vor nur wenigen Jahren scheinen nichts weniger als verrückt zu sein.

Hacktivismus

Ebenso hat die Ausbreitung der Demokratie seit dem Zusammenbruch der Sowjetunion vor einer Generation, zusammen mit internetbasierten Interaktionen zwischen Menschen auf der ganzen Welt, das Zeitalter des Hacktivismus eingeläutet. Menschen sind sich über Ereignisse in mehr Orten bewusst als in der Vergangenheit. Hacker, die wütend über eine Regierungspolitik oder -aktivität in einem bestimmten Ort sind, können diese Regierung oder die Bürger des Landes, über das sie herrscht, aus weit entfernten Orten heraus ins Visier nehmen. Ebenso können Bürger eines Landes Entitäten in einem anderen Land angreifen, deren Politik sie ablehnen oder deren Regierung sie als nationalen Gegner betrachten.

Größere Freiheit

Gleichzeitig sind unterdrückte Menschen heute besser über die Lebensweisen in freieren und wohlhabenderen Ländern informiert, ein Phänomen, das einige Regierungen dazu gezwungen hat, sich zu liberalisieren, und andere dazu motiviert hat, Cybersicherheitskontrollen einzuführen, um die Nutzung verschiedener internetbasierter Dienste zu verhindern.

Sanktionen

Eine weitere politische Auswirkung der Cybersicherheit betrifft internationale Sanktionen: Schurkenstaaten, die solchen Sanktionen unterliegen, konnten Cyberkriminalität in verschiedenen Formen nutzen, um solche Sanktionen zu umgehen.

Beispielsweise wird vermutet, dass Nordkorea Malware verbreitet hat, die Kryptowährungen für den totalitären Staat abbaut und damit ermöglicht, dass das Land Sanktionen umgeht, indem es flüssiges Geld erhält, das überall leicht ausgegeben werden kann.

Daher kann das Versäumnis von Einzelpersonen, ihre persönlichen Computer angemessen zu sichern, sich direkt auf politische Verhandlungen auswirken.

Neue Machtverhältnisse

Während die Militärs bestimmter Nationen längst mächtiger geworden sind als die ihrer Gegner - sowohl die Qualität als auch die Quantität der Waffen variieren stark zwischen den Nationen - ist das Gleichgewicht der Kräfte in der Cybersicherheit völlig anders.

Während sich die Qualität der Cyberwaffen zwischen Ländern unterscheiden kann, bedeutet die Tatsache, dass das Starten von Cyberangriffen wenig kostet, dass alle Militärs über einen effektiv unbegrenzten Vorrat an den von ihnen verwendeten Waffen verfügen. In den meisten Fällen kosten das Starten von Millionen von Cyberangriffen nicht viel mehr als das Starten von nur einem.

Auch anders als in der physischen Welt, in der jede Nation, die zivile Häuser im Gebiet ihres Gegners bombardiert, vernichtende Vergeltung erwarten kann, hacken rogue Regierungen regelmäßig mit Straflosigkeit Menschen in anderen Ländern. Opfer sind sich oft nicht bewusst, dass sie kompromittiert wurden, melden solche Vorfälle selten an die Strafverfolgungsbehörden und wissen sicherlich nicht, wen sie beschuldigen sollen.

Selbst wenn ein Opfer feststellt, dass ein Sicherheitsvorfall aufgetreten ist und selbst wenn technische Experten die Angreifer als Täter bezeichnen, genießen die Staaten hinter solchen Angriffen oft eine glaubwürdige Abstreitbarkeit (sie behaupten zum Beispiel: "Wir haben es nicht getan, vielleicht hat es jemand anders in unserem Land getan" oder ähnliches), was verhindert, dass irgendeine Regierung öffentlich zurückschlägt. Tatsächlich ist die Schwierigkeit, die Quelle von Cyberangriffen festzustellen, gepaart mit dem Element der glaubwürdigen Abstreitbarkeit ein starkes Anreiz für Regierungen, Cyberangriffe als Mechanismus zum proaktiven Angriff auf einen Gegner zu nutzen, verschiedene Formen von Havok anzurichten, ohne befürchten zu müssen, dass es zu bedeutenden Vergeltungsmaßnahmen kommt.

Darüber hinaus hat die Welt der Cybersicherheit ein gewaltiges Ungleichgewicht zwischen Angreifern und Verteidigern geschaffen, das zu Gunsten weniger mächtiger Nationen wirkt.

Regierungen, die sich niemals leisten könnten, riesige Angriffsbombardements gegen einen Gegner in der physischen Welt zu starten, können dies problemlos in der Cyberwelt tun, wo das Starten jedes Angriffs praktisch nichts kostet. Als Ergebnis können Angreifer weiterhin angreifen, bis sie erfolgreich sind - und sie müssen Systeme nur einmal kompromittieren, um "Erfolg" zu haben - was für Verteidiger, die ihre Vermögenswerte gegen jeden einzelnen Angriff abschirmen müssen, ein enormes Problem darstellt. Dieses Ungleichgewicht hat sich zu einem erheblichen Vorteil für Angreifer gegenüber Verteidigern entwickelt und bedeutet, dass selbst kleinere Mächte erfolgreich in Systeme von Supermächten eindringen können.

Tatsächlich trägt dieses Ungleichgewicht dazu bei, warum Cybersicherheitsverletzungen scheinbar so oft auftreten, da viele Hacker einfach weiter angreifen, bis sie erfolgreich sind. Wenn eine Organisation sich erfolgreich gegen 10 Millionen Angriffe verteidigt, aber den 10.000.001 nicht stoppt, kann sie eine schwere Verletzung erleiden und in den Nachrichten erscheinen. Berichte über die Verletzung werden wahrscheinlich nicht einmal erwähnen, dass sie eine Erfolgsquote von 99,999999 Prozent beim Schutz ihrer Daten hat und dass sie Angreifer erfolgreich eine Million Mal in Folge gestoppt hat. Ebenso wird, wenn ein Unternehmen 99,999 Prozent der Patches installiert hat, die es hätte installieren sollen, aber

versäumt hat, eine einzige bekannte Schwachstelle zu beheben, wahrscheinlich eine Verletzung erleiden, aufgrund der Vielzahl von Exploits, die für Kriminelle verfügbar sind. Medienberichte werden das Versäumnis der Organisation, ordnungsgemäß zu patchen, anprangern und ihre nahezu perfekte Bilanz in diesem Bereich übersehen.

Infolgedessen hat das Zeitalter des Cyberverbrechens auch das Machtgleichgewicht zwischen Kriminellen und Strafverfolgungsbehörden verändert.

Kriminelle wissen, dass die Wahrscheinlichkeit, für ein Cyberverbrechen erwischt und erfolgreich strafrechtlich verfolgt zu werden, dramatisch geringer ist als bei den meisten anderen Verbrechen, und dass wiederholte fehlgeschlagene Versuche, ein Cyberverbrechen durchzuführen, nicht das gleiche Maß an Sicherheit vor einer Verhaftung bieten wie bei den meisten anderen Verbrechen. Sie sind sich auch bewusst, dass Strafverfolgungsbehörden nicht über die Ressourcen verfügen, um die große Mehrheit der Cyberkriminellen zu verfolgen. Die Verfolgung, Festnahme und erfolgreiche Strafverfolgung einer Person, die Daten von halb über die Welt gestohlen hat und dabei viele Länder durchläuft und ein Netzwerk von Computern nutzt, die von rechtschaffenen Menschen übernommen wurden, erfordert beispielsweise die Bereitstellung und Bindung erheblich mehr Ressourcen als das Ergreifen eines Diebes, der auf Kamera aufgenommen wurde, während er in einem Laden in einem örtlichen Polizeirevier einbrach. Es ist auch viel einfacher und lukrativer, Cyberangriffe gegen reiche Ziele aus einem Ort zu starten, an dem die Strafverfolgung "bestochen" werden kann, um wegzuschauen, als es ist, die gleiche Belohnung über einen physischen Raub zu erzielen.

Mit den geringen Kosten für das Starten wiederholter Angriffe, den zugunsten der Täter wirkenden Erfolgsaussichten, den minimalen Chancen, erwischt und bestraft zu werden, und den potenziell wachsenden Belohnungen mit zunehmender Digitalisierung wissen Kriminelle, dass sich Cyberkriminalität auszahlt, was die Notwendigkeit unterstreicht, sich selbst zu schützen.

Betrachtet man die Risiken, denen die Cybersicherheit begegnet

Die Leute erklären manchmal, warum Cybersicherheit wichtig ist, indem sie sagen, "weil sie verhindert, dass Hacker in Systeme eindringen und Daten und Geld stehlen." Aber eine solche Beschreibung unterschätzt dramatisch die Rolle, die Cybersicherheit dabei spielt, das moderne Zuhause, Unternehmen oder sogar die Welt am Laufen zu halten und die Menschen vor physischem Schaden zu schützen.

Tatsächlich kann die Rolle der Cybersicherheit aus verschiedenen Blickwinkeln betrachtet werden, wobei jeder einen anderen Satz von Zielen darstellt. Natürlich sind die folgenden Listen nicht vollständig, aber sie sollten zum Nachdenken anregen und die Bedeutung unterstreichen, zu verstehen, wie man sich selbst und seine Lieben cybersicher macht.

Das Ziel der Cybersicherheit: Die CIA-Trias

Cybersicherheitsfachleute erklären oft, dass das Ziel der Cybersicherheit darin besteht, die Vertraulichkeit, Integrität und Verfügbarkeit (Confidentiality, Integrity, and Availability oder CIA) von Daten zu gewährleisten, manchmal auch als CIA-Trias bezeichnet, mit dem Wortspiel liebevoll beabsichtigt:

» Vertraulichkeit bezieht sich darauf, sicherzustellen, dass Informationen nicht offengelegt oder auf andere Weise unbefugten Entitäten (einschließlich Personen, Organisationen oder Computerprozessen) zur Verfügung gestellt werden.

Verwechseln Sie Vertraulichkeit nicht mit Datenschutz: Vertraulichkeit ist ein Teilbereich des Datenschutzes. Es geht speziell darum, Daten vor unbefugten Betrachtern zu schützen, während Datenschutz im Allgemeinen viel mehr umfasst.

Hacker, die Daten stehlen, untergraben die Vertraulichkeit.

» Integrität bezieht sich darauf, sicherzustellen, dass Daten sowohl genau als auch vollständig sind.

Genau bedeutet beispielsweise, dass die Daten niemals von einer unbefugten Partei oder durch einen technischen Fehler in irgendeiner Weise geändert werden. Vollständig bezieht sich beispielsweise auf Daten, die von keiner unbefugten Partei oder durch technische Fehler entfernt wurden.

Integrität umfasst auch die Sicherstellung der Nichtabstreitbarkeit, was bedeutet, dass Daten so erstellt und behandelt werden, dass niemand vernünftigerweise behaupten kann, die Daten seien nicht authentisch oder ungenau.

Cyberangriffe, die Daten abfangen und ändern, bevor sie an ihr Ziel übermittelt werden — manchmal als Man-in-the-Middle-Angriffe bekannt — untergraben die Integrität.

» Verfügbarkeit bezieht sich darauf, sicherzustellen, dass Informationen, die Systeme, die zur Speicherung und Verarbeitung verwendet werden, die Kommunikationsmechanismen, die zur Zugriffs- und Weitergabe verwendet werden, und alle damit verbundenen Sicherheitskontrollen korrekt funktionieren, um einen bestimmten Benchmark zu erfüllen (z. B. eine Betriebszeit von 99,99 Prozent). Menschen außerhalb des Cybersicherheitsbereichs betrachten die Verfügbarkeit manchmal als sekundären Aspekt der Informationssicherheit nach Vertraulichkeit und Integrität. Tatsächlich ist die Gewährleistung der Verfügbarkeit ein integraler Bestandteil der Cybersicherheit. Dies zu tun ist jedoch manchmal schwieriger als die Gewährleistung von Vertraulichkeit oder Integrität. Ein Grund dafür ist, dass die Aufrechterhaltung der Verfügbarkeit oft die Beteiligung vieler mehr Nicht-Cybersicherheitsfachleute erfordert, was zu einer "zu viele Köche verderben den Brei" -Art von Herausforderung führt, insbesondere in größeren Organisationen. Verteilte Denial-of-Service-Angriffe versuchen, die Verfügbarkeit zu untergraben. Bedenken Sie auch, dass Angriffe häufig eine große Anzahl von gestohlenen Rechnerressourcen und Bandbreite nutzen, um DDoS-Angriffe zu starten, während diejenigen, die darauf abzielen, die Verfügbarkeit zu gewährleisten, nur die relativ geringe Menge an Ressourcen nutzen können, die sie sich leisten können.

Aus menschlicher Sicht

Die Risiken, denen die Cybersicherheit begegnet, können auch in Begriffen betrachtet werden, die die menschliche Erfahrung besser widerspiegeln:

» Datenschutzrisiken: Risiken, die sich aus dem potenziellen Verlust angemessener Kontrolle über oder Missbrauch persönlicher oder anderer vertraulicher Informationen ergeben.

» Finanzielle Risiken: Risiken finanzieller Verluste aufgrund von Hacking. Finanzielle Verluste können sowohl direkte — zum Beispiel der Diebstahl von Geld von jemandem Bankkonto durch einen Hacker, der in das Konto gehackt hat — als auch indirekte umfassen, wie den Verlust von Kunden, die einem kleinen Unternehmen nach einem Sicherheitsvorfall nicht mehr vertrauen.

» Berufsrisiken: Risiken für die berufliche Laufbahn, die aus Verletzungen resultieren. Offensichtlich sind Cybersicherheitsfachleute einem Karriereschaden ausgesetzt, wenn unter ihrer Aufsicht eine Verletzung auftritt und festgestellt wird, dass sie auf Fahrlässigkeit zurückzuführen ist, aber auch andere Arten von Fachleuten können aufgrund einer Verletzung Schaden erleiden. C-Level-Executives können entlassen, Vorstandsmitglieder verklagt werden, und so weiter. Beruflicher Schaden kann auch auftreten, wenn Hacker private Kommunikationen oder Daten veröffentlichen, die jemanden in ein schlechtes Licht rücken — zum Beispiel Aufzeichnungen, dass eine Person wegen eines unangemessenen Verhaltens diszipliniert wurde, eine E-Mail mit anstößigem Material gesendet hat usw.

» Geschäftsrisiken: Risiken für ein Unternehmen ähnlich den beruflichen Risiken für eine Einzelperson. Nach einer Verletzung von Sony Pictures veröffentlichte interne Dokumente malten das Unternehmen in Bezug auf einige seiner Vergütungspraktiken in einem negativen Licht.

» Persönliche Risiken: Viele Menschen speichern private Informationen auf ihren elektronischen Geräten, von expliziten Fotos bis hin zu Aufzeichnungen über die Teilnahme an Aktivitäten, die von Mitgliedern ihrer jeweiligen sozialen Kreise möglicherweise nicht als respektabel angesehen werden. Solche Daten können manchmal erheblichen Schaden für persönliche Beziehungen verursachen, wenn sie durchsickern. Ebenso können gestohlene persönliche Daten Kriminellen helfen, die Identität von Personen zu stehlen, was zu einer Vielzahl persönlicher Probleme führen kann.

» Risiken physischer Gefahr: Cyberangriffe auf Kläranlagen, Versorgungsunternehmen und Krankenhäuser in den letzten Jahren haben deutlich gezeigt, dass das Versäumnis, die Cybersicherheit aufrechtzuerhalten, zur Gefährdung menschlichen Lebens führen kann. Zum Beispiel starb 2020 eine Frau in Deutschland, während sie zwischen Krankenhäusern transportiert wurde, nachdem das Krankenhaus, in dem sie Patientin war, von Ransomware getroffen worden war. Und 2021 wurde eine Klage eingereicht, in der behauptet wurde, dass ein Baby als Folge von medizinischen Fehlern starb, als es in einem Krankenhaus in Alabama während Systemausfällen aufgrund eines Ransomware-Angriffs geboren wurde.