COMMERZBANK
Die Bank an Ihrer Seite

Fokusbericht

Cybersecurity

Datenstand: 22.7.2019

Inhalt

04 Executive Summary

05 1. Es sollte ein normaler Tag sein

07 2. Cyberkriminalität

07 2.1 Motive der potenziellen Angreifer

08 2.2 Wie arbeiten Cyberkriminelle heute?

09 2.3 Welchen Bedrohungen sehen sich Firmen heute ausgesetzt?

16 2.4 Selbstbetroffenheit/Selbsteinordnung

19 3. Cybersicherheit – Schützen Sie Ihr Unternehmen

19 3.1 Herausforderungen für Unternehmen

20 3.2 Technologische Maßnahmen

22 3.3 Organisation

24 3.4 Mitarbeiter

24 3.5 Cyber-Versicherung

25 3.6 Gesetzliche Vorgaben

27 4. Was tun, wenn die eigene Firma Opfer geworden ist?

29 5. Nützliche Adressen/Nützliches Material

30 6. Checkliste Cybersecurity

Executive Summary

Absolute Sicherheit vor Angriffen aus dem Netz gibt es nicht. Cybersecurity kann jedoch die Risiken eines Angriffs und dessen negative Folgen minimieren. Ziel der Sicherheitsmaßnamen ist es daher, die Resilienz beziehungsweise Widerstandsfähigkeit des Unternehmens vor Cyberangriffen zu erhöhen. Dabei zeigt sich, dass der Schutz vor Cyberangriffen immer mit einer Abwägung von unterschiedlichen Unternehmenszielen verbunden ist.

Der Schutz gegen Cyberkriminalität beginnt mit dem Verständnis für die Gefahren beziehungsweise Risiken, denn es zeigt sich, dass die Schadprogramme und Methoden immer variantenreicher werden – was wiederum eine steigende Komplexität mit sich bringt.

Technische Maßnahmen wie ein Basisschutz – Passwortsicherung, Firewalls, Virenscanner, Updates und Back-ups – sind nahezu in allen Unternehmen vorhanden. Dieser Mindeststandard erweist sich aber angesichts der ständigen Weiterentwicklung auf der Seite der Angreifer als nicht ausreichend. Die IT-Technologie und -Infrastruktur sowie die Software-Anwendungen müssen daher permanent kontrolliert beziehungsweise aktualisiert werden. In regelmäßigen Abständen sollten Unternehmen darüber hinaus prüfen – auch durch bestellte Hackerangriffe – ob das Cybersecurity-Niveau noch ausreichend ist.

Hinsichtlich der organisatorischen Maßnahmen sollten bei der Cybersecurity klare personelle Verantwortlichkeiten festgelegt werden. Bei größeren Unternehmen ist die Einrichtung eines Chief Information Security Officers sinnvoll. Ebenso wichtig wie die Sensibilität der Führungskräfte für das Thema Cybersecurity ist die Aufmerksamkeit der Mitarbeiter. Es sollte ihnen vermittelt werden, dass sie durch ihr Handeln einen wichtigen Beitrag zum Schutz des Unternehmens liefern.

Für den Fall eines Angriffs sollte ein Notfallplan zur Verfügung stehen, um kritische Funktionen aufrechtzuerhalten und nach einem Angriff wieder schnell zur Normalität zurückzukehren. Der Plan sollte in analoger Form vorliegen. Für die Zeit danach gilt: Sobald ein finanzieller Schaden durch Erpressung oder Betrug entsteht, ist zur Schadensbegrenzung die Bank als erster Ansprechpartner zu nennen. Bei jedem Vorfall muss nach vorheriger interner Abstimmung die Polizei eingeschaltet werden. Schließlich gilt es, durch eine transparente interne und externe Kommunikation die beschädigte Reputation wiederherzustellen.

1. Es sollte ein normaler Tag sein

Es ist ein Montag. Herr Dr. Bottlich ist spät dran und eilt von der Tiefgarage seines Arbeitgebers hoch in sein Büro. Er ist kaufmännischer Leiter eines mittelständischen Unternehmens und steckt mit seiner Abteilung mitten im Jahresabschluss, sodass er einen anstrengenden Tag erwartet. Außerdem ist heute der Geburtstag seiner Frau. Der Tisch in ihrem Lieblingsrestaurant ist für abends schon reserviert. Daher möchte er das Büro heute nicht allzu spät verlassen.

Doch während er aus dem Aufzug in den Flur tritt, ist irgendetwas anders. Es ist ungewohnt still auf dem Gang. Wo sind seine Mitarbeiter? Die Sekretärin begrüßt ihn ganz aufgeregt und eilt ihm erklärend entgegen. „Die meisten haben wir in die Cafeteria geschickt. Ich bin ja so froh, dass Sie da sind, Herr Dr. Bottlich. Nichts geht mehr: Kein Telefon, kein Computer und die Webseite ist nicht erreichbar. Die IT ist schon informiert. In 10 Minuten soll es ein Krisenmeeting beim Chef geben.“ Die Menge an Informationen überrollt Herrn Dr. Bottlich, und er versteht die Lage sowie ihre Tragweite noch nicht. „Heißt das, die Produktion steht auch?“ – „Ja, alles – es heißt, dass wir wohl Opfer eines Verschlüsselungstrojaners wurden. Wir haben keinen Zugang mehr zu irgendwelchen Systemen oder Daten.“

Herr Dr. Bottlich legt Mantel und Tasche ab, eilt in die Etage der Geschäftsleitung. Dort ist der Ernst der Lage in den Gesichtern ablesbar; der Chef erklärt die Situation: „Fast alles ist verschlüsselt. Irgendwie haben Hacker eine Schadsoftware ins Unternehmen geschleust. Wie genau, dass steht noch nicht fest. Nur so viel ist bis jetzt klar: Der oder die Täter verlangen von uns 2 Millionen Euro, die wir in Bitcoins zahlen sollen. Erst nach dieser Zahlung bekommen wir einen Code zugeschickt, mit dem wir angeblich wieder alles entschlüsseln können.“ Es herrscht vollkommene Ratlosigkeit.

Fragen und Antworten eilen durch den Raum:
„Was ist mit den Backups?“ – „Auch verschlüsselt, das Meiste jedenfalls.“ – „Ist noch irgendetwas zur retten?“ – „Das wissen wir nicht genau. Es waren zwei verschiedene Server offline – aus Wartungsgründen. Wir überprüfen gerade, was dort gespeichert ist.“ – „Können wir die produzierten Maschinen der letzten Woche ausliefern?“ – „Nein. Wir haben keinen Zugriff auf die Verträge, Adressen und Frachtpapiere.“ – „Was machen wir mit den Logistikunternehmen, die auf dem Hof stehen?“ – Schulterzucken.

Nun denkt Herr Dr. Bottlich an seinen Jahresabschluss, der schon zu 75 Prozent fertig war. Er fragt den IT-Chef, was der jüngste Stand ist, der noch gesichert ist. Dieser schaut ihn aber nur an, als wäre er unwillig zu wiederholen, was er gerade zum Thema Back-ups gesagt hat.

Die Runde berät die nächsten Schritte: Wie informieren wir die Mitarbeiter? E-Mails und Intranet sind ja offline. Damit besteht auch kein Zugriff auf Organigramme und Telefonlisten. Ist der Angreifer noch im System? Was sagen wir Kunden und Lieferanten? Außerdem einigt man sich nach längerer Diskussion darauf, die Polizei zu informieren.

Für 12 Uhr wird das nächste Meeting ins Auge gefasst, bei dem man weiter beraten will, wie es weitergehen soll. Dann muss auch entschieden werden, ob man die Mitarbeiter für heute nach Hause schickt.

Jeder bekommt zum Schluss noch den Auftrag, bis dahin eine Liste mit allen Mitarbeitern seiner Abteilung und deren Erreichbarkeit anzufertigen. „Für die IT übernimmst Du das bitte, Jürgen. Die haben jetzt anderes zu tun. Wir brauchen Namen, Abteilung, Handynummern und private E-Mail-Adressen.“ Herr Dr. Bottlich fragt noch, ob die Bank informiert werden soll. „Nur das nichts passiert.“ – „Gute Idee. Aber bitte noch kein Wort über die Details.“

Herr Dr. Bottlich geht in sein Büro. Als Erstes sucht er die Visitenkarte seines Bankers, findet sie aber nicht. Deshalb sucht er über den Browser seines Smartphones die allgemeine Hotline der Bank. Über diese landet er im zentralen Callcenter der Bank – irgendwo in Deutschland. Er versucht sich zu seinem Berater durchstellen zu lassen, was nach mehreren Anläufen auch gelingt. Der Bankangestellte ist allerdings verwundert. „Sind Sie es wirklich, Herr Dr. Bottlich? Die Nummer, von der aus Sie anrufen, kenne ich nicht. Und wieso kommen Sie überhaupt über die Hotline rein und haben nicht direkt angerufen? Ich bin etwas verunsichert. Darf ich Sie gleich zurückrufen? Ich schaue gerade in unserem System nach Ihren Kontaktdaten.“

Es vergeht etwas Zeit und sein Berater meldet sich wieder – auf dem Handy. Denn auf dem Festnetz ist trotz Freizeichen keiner ans Telefon gegangen.

Dies ist zwar eine fiktive Geschichte, die sich aber in ähnlicher Form in der Realität in mehreren Firmen 2018 und 2019 so abgespielt hat. Ohne funktionierende Back-ups brauchen betroffene Unternehmen Wochen, ja Monate, um einen vollständigen Normalbetrieb wiederherzustellen. Und selbst dann sind Daten dabei meist für immer verloren.

Nach mehreren Tagen ohne Aussicht auf Erfolg ist in fast allen betroffenen Unternehmen der Tiefpunkt erreicht und die Aussichtslosigkeit so groß, dass sich einige der Firmen auch mit dem Gedanken abfinden, der Erpressung nachzugeben. Sie hoffen auf den „Schlüssel", der alles wieder rückgängig macht. Für einige Firmen beginnt mit solch einem Tag der Weg in die Krise und letztlich in die Insolvenz.

Grundsätzlich ist die Wahrscheinlichkeit, unabhängig von Branche und Größe des Unternehmens Ziel eines Cyberangriffs zu werden, extrem hoch. Cybersecurity ist daher ein Thema, mit dem sich jedes Unternehmen zwingend auseinandersetzen muss. Denn es betrifft keinesfalls nur große Konzerne oder Internetfirmen.

Erst mit Cybersecurity können Unternehmen das gesamte Potenzial der Digitalisierung realisieren.

Dieser Fokusbericht widmet sich der Sicherheit Ihres Unternehmens und zeigt Ihnen eine Vielzahl an Möglichkeiten, wie Sie sich und Ihre Firma in unternehmerischer Verantwortung vor solch einem Szenario schützen können.

Der Schutz gegen Cyberkriminalität beginnt dabei mit dem Verständnis für die Gefahren beziehungsweise Risiken. Dies sind neue Gefahren, auf die sich die Unternehmen im Zuge der Digitalisierung einstellen müssen. Die Vielzahl an vernetzten Geräten und digitalen Kanälen führt dazu, dass nahezu alles ein potenzielles Ziel ist und eröffnet den (Cyber-)Kriminellen nie dagewesene Einfallstore.

2. Cyberkriminalität

Um sich gegen Cyberangriffe zu wappnen, ist es für Unternehmen elementar, die (Cyber-)Gefahren und die aktuelle Risikolage zu kennen. Und diese Lage ist nach Aussage von Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), „sehr ernst". Es zeigt sich, dass die Schadprogramme immer variantenreicher werden, was wiederum eine steigende Komplexität mit sich bringt. Dies kann Unternehmen, beziehungsweise deren Sicherheitsexperten und gegebenenfalls vorhandene Schutzkonzepte schnell überfordern.

Es stellt sich eine Vielzahl von Fragen, auf die Antworten gefunden werden müssen: Sind Sie ein reines Zufallsopfer? Oder richtete sich ein Angriff gezielt gegen Ihr Unternehmen? Auf was haben es die Angreifer abgesehen, was kann man bei Ihnen „holen"? Geht es um das Vermögen Ihres Unternehmens? Um Patente oder Knowhow? Ist es nur „Schnüffelei" oder will man Daten stehlen, womöglich noch die Ihrer Kunden? Will man Ihre Produktionspreise kennenlernen oder jene, mit denen Sie bei einer Ausschreibung um einen Auftrag beworben haben? Geht es ums Kopieren oder nutzt man nur Ihre Rechnerleistung? Will man Ihr Unternehmen nur einmal finanziell schädigen, oder will man Sie gezielt dauerhaft schwächen und schlechter stellen als Ihre Konkurrenz? Wer greift Sie überhaupt an?

Mit all diesen Fragen lassen sich die meisten Attacken in wichtige Kategorien einteilen, was dem Ordnen der vielfältigen Herangehensweisen und dem Erkennen der eigenen Betroffenheit hilft.

2.1 Motive der potenziellen Angreifer

2.1.1 Cybercrime
Cybercrime ist der Oberbegriff sowohl für Attacken, bei denen Schadsoftware oder Hacks zum Einsatz kommen, als auch für Straftaten unter Anwendung marktüblicher Computer-Technologien. Zugleich spricht man ebenfalls von Cybercrime, wenn das direkte monetäre Interesse der Täter im Mittelpunkt der Tat steht, wobei finanzielle Motive für die meisten Tätergruppen in Betracht kommen. Hierbei geht es darum, durch Erpressung, Betrug oder den Verkauf gestohlener Informationen Geld zu erlangen. Eine weitere Ausprägung besteht darin, die Cyberattacke selbst als „Crime as a Service" online zum Kauf anzubieten. Cyberkriminalität entwickelt sich damit zu einem eigenen „Geschäftsmodell". Kriminalität als Serviceleistung ist zur Basis für einen florierenden ungeordneten Markt geworden. In diesem Sinne hat sich ein eigener Marktplatz, eine eigene industriegleiche Handelstätigkeit „dunkler Dienstleistungen" gebildet – nicht nur im Darknet. Bei dieser Markwirtschaft der Cyberkriminalität gibt es meistens eine arbeitsteilige Wertschöpfungskette mit verschiedenen Stufen. Ein Hacker besorgt Daten, eine zweite Person prüft die Qualität und Dritte nutzen beziehungsweise monetisieren sie. Schadsoftware, von Hackern programmiert, wird über das Darknet (zum Beispiel Tor-Netzwerk) verkauft – mit Sicherheitsgarantien für den Käufer, dass die Malware nicht von gängigen Antivirenprogrammen erkannt wird. Sollte sich das ändern, werden innerhalb einer versprochenen Frist Software-Updates in Aussicht gestellt, die das Problem beheben sollen. Auch Schadsoftware-Leasing und „Pay-per-Use"-Modelle sind verfügbar, zum Beispiel bei Botnetzen. Genauso gut ist die Infiltration einer bestimmten Stückzahl von Rechnern mit Malware bestellbar. Die Anbieter dieser Dienste wiederum sind nicht direkt in die kriminelle Handlung eingebunden. Sie stellen meist nur die Schadsoftware zum Verkauf. Oder sie bieten Hintergrundinformationen, gefälschte Dokumente oder Geldwäsche an.

2.1.2 Cybervandalismus
Interessengruppen oder Aktivisten werden von politischen Motiven und eigener Überzeugung geleitet, durch ihre Tat der Gerechtigkeit Genüge zu tun. Im Fokus der Kampagnen kann dabei schon allein das illegale Beschaffen und Veröffentlichen vertraulicher beziehungsweise sensibler Unterlagen stehen, die für das betroffene Unternehmen zu einem Imageschaden führen, egal ob die Story dahinter aus Sicht des Unternehmens nun konstruiert erscheint oder nicht. Genauso wenig wird von Aktivisten dabei berücksichtigt, ob man durch die Bekanntgabe erbeuteter streng vertraulicher Informationen eine Gefährdungslage allgemeiner Natur oder nur für Einzelne erzeugt. Durch digitale Sabotage beziehungsweise Vandalismus wird versucht, den Produktionsbetrieb respektive Abläufe im Unternehmen gezielt zu stören, um ein „höheres Ziel" zu erreichen oder ein Unternehmen „abzustrafen". So wird gemutmaßt, dass die Täter der DDoS-Attacke vom September 2018 auf RWE aus dem Umfeld der Proteste gegen die Abholzung des Hambacher Forsts stammen.

2.1.3 Spionage
Ökonomische Motive leiten konkurrierende Unternehmen bei potenziellen Attacken, wenn sie zum Beispiel mit dem Diebstahl von Daten beziehungsweise geistigem Eigentum ihre Wettbewerbsposition verbessern wollen. Dies gilt auch dann, wenn ihr Gebot und ihre Positionierung bei der Ausschreibung eines Großprojekts ausspioniert werden. Vergleichbare Beweggründe haben die zum Teil staatsnahen Gruppierungen

und ausländische Nachrichtendienste bei ihren Spionage-Angriffen auf Unternehmen. Mit den gestohlenen Informationen können sie das Wachstum staatseigener beziehungsweise staatsnaher Unternehmen unterstützen. Diese Form der Cyberkriminalität geht sehr oft von Ländern aus, in denen es eine enge Verknüpfung von Staat und Wirtschaft gibt. Opfer sind dann überwiegend forschungs- und technologieintensive Unternehmen und Branchen. In sehr vielen Fällen wird die Spionage nicht oder erst spät bemerkt. Für Roland Busch, Technikvorstand von Siemens, handelt es sich beispielsweise bei vielen Attacken auf Siemens um Industriespionage.

2.1.4 Cyberwar

Die höchste Gefahr für eine hochgradig technisierte und durch und durch vernetzte Gesellschaft stellt ein Cyberkrieg dar. Immer häufiger machen sich politische Institutionen das Internet zunutze, um Länder zu destabilisieren und die Politik im Ausland zum eigenen Vorteil zu lenken. Diese Destabilisierungspolitik ist nicht neu, nur ist sie im digitalen Zeitalter viel effektiver und den Initiatoren schwerer nachzuweisen. Bevorzugtes Mittel sind bisher Kampagnen, die mit Bots und Internettrollen Stimmungen in Ländern aufgreifen und verstärken oder sie sogar erst entstehen lassen. Die Bevölkerung wird so gezielt zum Protest und Aufbegehren angestachelt. Die Unruhe entsteht für die politische Elite scheinbar aus dem Nichts. Dass auch Wahlen mit geopolitischem Interesse beeinflusst werden, dürfte inzwischen niemandem mehr entgangen sein.

Es gibt aber auch Cyberwar-Beispiele, die über eine reine Desinformation hinausgehen. Ziel des Schadprogramms Stuxnet war eine bestimmte Siemens-Steuerungsanlage, um damit das iranische Atomprogramm zu sabotieren. Allen staatlichen Einflussnahmen gemein ist in der Regel, dass die finanziellen Möglichkeiten bei der Entwicklung und Verbreitung der Schadsoftware nahezu unbegrenzt sind; dass bis dahin unbekannte Sicherheitslücken genutzt werden und dass es sich meist um hochkomplexe Funktionsweisen handelt, die nur schwer zu entdecken sind. Stuxnet war beispielsweise bereits mehrere Jahre vor der Entdeckung aktiv. So wurde Stuxnet der Entdeckung und dem Nachweis durch Antiviren-Experten im Jahr 2010 aktiv. Die erste Infektion, die erst im Nachgang verifiziert wurde, muss aber bereits 2007 stattgefunden haben.

Schadprogramme können aber auch für einen gezielten Angriff auf wichtige Infrastrukturen geschrieben werden. Im Zeitalter der Digitalisierung dürfte die Stromversorgung eines der Hauptziele sein. Denn in der Folge eines Stromausfalls kommen weitaus mehr Abläufe und Prozesse zum Stillstand, als es noch vor einigen Jahrzehnten vorstellbar war. Daraus resultierend müssen sich Unternehmen heute zwei Fragen stellen. Bin ich strategisch wichtig und damit ein potenzielles Angriffsziel? Und: Wie könnte ich sekundär betroffen sein, auch wenn mein Unternehmen selbst nicht Ziel eines solchen Angriffs ist?

2.2 Wie arbeiten Cyber-Kriminelle heute?

Durch die Digitalisierung haben sich die Möglichkeiten für Cyberkriminelle erweitert. So liegen immer mehr Informationen in digitaler Form vor. Es werden immer mehr Dienste online angeboten und Menschen organisieren ihr Leben zunehmend über das Netz. Nahmen Angreifer noch vor einigen Jahren bevorzugt den Weg über den Browser in lokale Betriebssysteme, bieten sich heute zusätzliche Ziele und Möglichkeiten. So ist jedes Unternehmen schon durch die permanente Präsenz im Internet erreichbar. Die Möglichkeit der Online-Steuerung ganzer Industrieanlagen von der heimischen Couch aus ermöglicht es Fremden, Angriffsvektoren durch Sicherheitslücken zu nutzen. Die potenzielle Beute ist noch verlockender, wenn sich Daten, Wissen oder Finanzen im Netz konzentriert auffinden lassen (zum Beispiel in Cloud-Services entsprechender Anbieter). Diese Daten unterliegen dort zwar meist einem höheren Schutz, aber damit auch einer fremden Kontrolle. Die Vergangenheit hat gezeigt, dass das Interesse dieser Anbieter, über Datendiebstähle zu informieren, auf natürliche Weise begrenzt schien und nicht selten erst dann erfolgte, wenn es auf andere Weise ohnehin an die Öffentlichkeit gelangt wäre.

Wie arbeiten Täter heute? Der 16-jährige Teenager, der aus einem Spielinstinkt oder einem Selbstbestätigungsdrang heraus sein IT-Wissen unter Beweis stellen will, ist eher die Ausnahme. Die Szene ist arbeitsteilig geworden und organisiert sich über ein Netz, das Darknet. Dabei agieren die Cyberkriminellen wie globale Unternehmen. Risiken werden ausgelagert, professionelles Knowhow und notwendige Informationen (Daten) eingekauft, Dienstleistungen unter Abwägung von Quantität und Qualität beauftragt. Es wird in Business Cases gedacht. Handelsbeschränkungen, Datenschutzbestimmungen, so etwas wie Zölle, fehlende Länderzuständigkeiten oder etwas mit einem Amtshilfeersuchen Vergleichbares sind hingegen aus dem Darknet bisher eher nicht bekannt.

Täter setzen aber nicht mehr allein auf die IT-technischen Lücken. Sehr oft bedienen sie sich inzwischen des schwächsten Glieds in der Kette, des Faktors Mensch. Codes kann man ändern, den sozialen Umgang und das Gefüge aller Charaktereigenschaften, die jeden von uns ausmachen, wohl eher nicht. So sammeln Täter heute unter vermeintlich typischen menschlichen oder ökonomischen Beweggründen erst Informationen über ausgesuchte Unternehmen. Ansprechpartner, Unternehmensstrukturen, Prozesse und Verbindungen werden erkundet. Das passiert oft über Monate hinweg, mit teils harmlos anmutenden E-Mails, Anrufen und Fragen. Täter bauen sich dabei das Puzzle des späteren Opfers so zusammen, dass sie mit ihrem erlangten Wissen durchaus als interner Mitarbeiter akzeptiert werden könnten. Es wird genutzt, um an weitere Interna zu gelangen und letztlich technische und prozessuale Sicherheitsmechanismen in der Firma auszuhebeln und zu überwinden **(siehe Kapitel 2.3.5)**.

Fälscherwerkstätten stehen dafür ergänzend genauso mit ihrem Service zur Verfügung, wie Anbieter von Datenbanken, die erlangtes Firmenwissen verkaufen. Erfolgt der Angriff aus monetären Beweggründen, so steht selbst für die Geldwäsche ein Dienstleister zur Verfügung. Es ist schwierig, dem einzelnen Verkäufer die kriminellen Absichten nachzuweisen. Der Verkauf von Firmenwissen ist nicht strafbar. Der Verkauf von Sicherheitslücken auch nicht. Selbst der Verkäufer von Schadsoftware ist nicht gleichzusetzen mit der Person, die diese einsetzt. Die Marktplätze auf beiden Seiten funktionieren also nach den gleichen Prinzipien und Mechanismen und ähnlich effektiv.

2.3 Welchen Bedrohungen sehen sich Firmen heute ausgesetzt?

2.3.1 Technische Angriffe

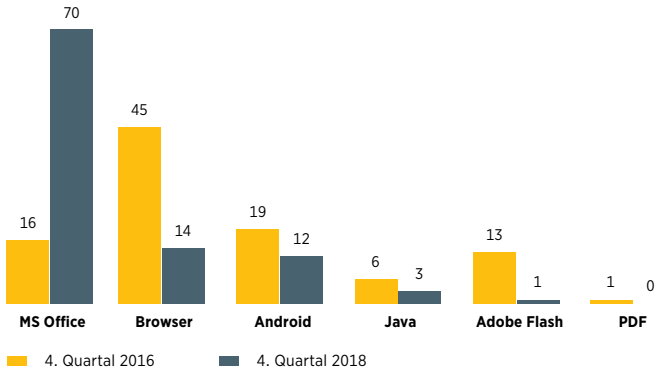
Datendiebstahl

Daten werden gern als der Rohstoff des 21. Jahrhunderts bezeichnet. Somit gibt es neben dem berechtigten auch das unberechtigte Interesse, Daten zu erlangen und diese zu verwerten. Gestohlene Daten kann der Täter entweder an Dritte weiterverkaufen, selbst nutzen oder sie dem geschädigten Unternehmen zum Rückkauf anbieten. So sah sich der Fahrdienstanbieter Uber einer solchen Geldforderung in Höhe von 100.000 Euro ausgesetzt. Dem Unternehmen waren zuvor im Oktober 2016 weltweit über 50 Millionen Kunden- und 7 Millionen Fahrerdaten gestohlen worden.

Viel wahrscheinlicher ist es, dass der Diebstahl von Kundendaten (zum Beispiel Anmeldedaten oder persönliche Informationen) erfolgt, um diese für weitere Missbräuche zu verkaufen oder selbst zu verwenden. Der Datendiebstahl kann auch sensibles Firmenwissen betreffen, zum Beispiel Informationen über Produktentwicklungen, das Design einer geplanten neuen Modelinie, ein neues Fahrzeugmodell oder aber Patente, die kurz vor der Eintragung stehen. Genauso ist das Wissen über strategische Neuausrichtungen ein potenzielles Ziel, das den Durchbruch am Markt gegenüber den Mitbewerbern bringen soll. Oder aber es ist sicherheitsrelevantes Wissen, welches zum Beispiel den physischen Schutz der Firma umfasst und Zutrittsrechte regelt. Des Weiteren können Informationen zum Unternehmen, wie Organigramme oder Berechtigungen zur Vorbereitung eines CEO-Frauds oder Social Engineering genutzt werden. Die Liste kann sehr lang sein und mancher Betroffene ist verwundert, wie knapp sein eigenes Angebot bei einer Ausschreibung vom Mitbewerber unterboten werden konnte **(siehe Grafik 1)**.

Dabei kann der Schutz vor Spionage genauso kreativ, wie inspirierend sein. Es soll Firmen geben, die auf eigenen Laufwerken bewusst falsche Informationen speichern oder Maßangaben technischer Zeichnungen nur offline im Unternehmen vorhalten.

Grafik 1: Verteilung von Cyberattacken nach betroffenen Plattformen, in %



Quelle: Kaspersky

Advanced Persistent Threats (APTs)

Neben dem gezielten Hack, dem Einsatz von Schadsoftware und der physischen Industriespionage kommt den sogenannten APTs eine besondere Bedeutung zu. Die Grenzen für die Begriffsdefinitionen sind dabei fließend. Frei übersetzt würde man fortgeschrittene, hartnäckige oder ausdauernde Bedrohung zu dieser Art des gezielten Angriffs auf eine Firma zählen. Ziel der Täter ist es, möglichst unbemerkt in das Netz des Opfers zu gelangen und dort so lange wie möglich unentdeckt zu bleiben, während man sich Zugang zu digitalisierten Informationen und Abläufen verschafft.

Aktivitäten laufen daher eher unterschwellig im Grundrauschen des normalen Datenverkehrs ab. Täter schaffen es aber, aufgrund der Dauer eines solchen Angriffs, wesentlich mehr Informationen als in einer einzelnen Attacke zu erbeuten oder einen umfassenderen Schaden im Firmennetzwerk zu verursachen, wenn zum Beispiel mit einem APT eine Verschlüsselungssoftware zur Anwendung kommt. Die angewandten Codes und Schadprogramme werden dabei maßgeschneidert für den Angriff auf das einzelne Opfer erstellt und angepasst. Die Täter eines APTs sind daher in der Regel keine Einzeltäter, sondern ähnlich einem IT-Dienstleister organisiert. Im Fall der Industriespionage wird der Täter das erlangte Wissen nur sehr sorgfältig einsetzen, um das Informationsleck auf der Opferseite nicht auffliegen zu lassen. Ein APT kann auch mit einem Schwarmangriff beginnen, so dass das Opfer mit der schieren Masse an Threats überfordert ist.

Cryptojacking

Eine andere Nutzung von APTs stellen Tools dar, welche nur die fremden Systemressourcen nutzen, zum Beispiel zum „Schürfen“ von Kryptowährungen wie Bitcoin. Bei diesem Cryptojacking werden Computersysteme mit dem Ziel des Kryptogeld-Schürfens gekapert. Opfer eines solchen Angriffs wurde beispielsweise im Januar 2018 das Landesamt für Besoldung in Baden-Württemberg. Cryptojacking ist besonders dann virulent, wenn der Wechselkurs der virtuellen Währung

sehr hoch ist. Oft merken die Opfer nicht, dass ihr System gekapert wurde, da es nicht vollständig ausfällt, sondern nur langsamer arbeitet. Die geringere Systemperformance sowie der höhere Energieverbrauch sind schwer quantifizierbar und werden oft in Schwächen der Software vermutet. Insofern ist der monetäre Schaden nur gering, das System ist aber kompromittiert und der Angreifer kann den Zugang jederzeit auch für andere Zwecke nutzen.

Hardware-Manipulation

Eine Angriffsmethode, die insbesondere im Jahr 2018 großes mediales Interesse auf sich gezogen hat, findet ihren Ursprung in der Hardware – genauer in den Computerchips. Einerseits gab es die Vermutung, dass Chips einiger Hersteller direkt ab Werk mit absichtlichen Manipulationen für künftige Angriffe ausgeliefert wurden, wobei es laut BSI keine harten Beweise dafür gibt. Andererseits gibt es eine ganze Generation von Computerchips des Herstellers Intel, bei denen Fehler in der Chiparchitektur Cyberangriffe („Meltdown"/„Spectre") ermöglichen.

Angriff auf die Chiparchitektur: „Meltdown"/„Spectre"

Anfang 2018 wurde öffentlich, dass Computerchips des Herstellers Intel eine gravierende Sicherheitslücke aufweisen. Ein Fehler in der Chiparchitektur erlaubt es Hackern, Passwörter vom Betriebssystem oder anderen Programmen auszulesen und zu stehlen. Alle Computer und mobilen Endgeräte, die diese Chips enthalten, sind anfällig für Attacken. Zwei Angriffsmuster, die diese Sicherheitslücke ausnutzen, wurden von Experten „Meltdown" und „Spectre" genannt. Um Schaden anrichten zu können, müssen die Angreifer allerdings erst Zugang zum Computersystem bekommen. Deshalb beginnen auch „Meltdown" und „Spectre" unter anderem mit einer Spam-E-Mail. Das Problem betrifft nahezu alle Intel-Computerchips der vergangenen 20 Jahre. Zwar gibt es die Möglichkeit, mittels Updates die Sicherheitslücke zu schließen, aber gerade bei „Spectre" ist dies sehr aufwändig. Zudem werden sie nicht von allen Herstellern bereitgestellt, in deren Geräte die Computerchips verbaut sind. Am Ende hilft nur ein Austausch der betroffenen Geräte.

2.3.2 Botnetze – Bedrohung durch Masse

Eine andere Form der Kaperung von Systemen und der Ausnutzung von Ressourcen sind die sogenannten Botnetze. Hierbei werden zahlreiche vernetzte Geräte (unter anderem Computer, Maschinen, Router und Geräte des IoT (Internet of Things)) infiziert und für die Zwecke der Täter mitgenutzt. Sie sind zu einem Netz zusammengefügt und werden durch Befehle aus dem Netz gesteuert. Manches Botnetz besteht aus mehreren Millionen Geräten, die nur mühsam zu bekämpfen sind, da wie bei dem Ungeheuer Hydra aus der griechischen Mythologie für einen aus einem Botnetz entfernten Bot (Robot) automatisch viele neue im gleichen Botnetz entstehen. Botnetze werden von den Angreifern für jede Art von Cyberkriminalität eingesetzt, bei der kriminelle Ziele durch Masse (Rechenleistung oder Klickrates) verfolgt werden. So infiltrierte Ende 2016 die Hacker-Gruppe „Avalanche" allein in Deutschland mehr als 50.000 Computer und erstellte aus ihnen ein Botnetz, um Konten zu plündern. Zum Einsatz kommen Botnetze aber auch beim Phishing, beim Proxy-Missbrauch oder beim Klickbetrug, wenn Werbepartner für die Anzahl Klicks auf Werbebanner bezahlt werden. Die größte Bekanntheit haben Botnetze aus ihrem Einsatz bei einer Distributed-Denial-of-Service-Attacke (DDoS). Hierfür nutzt der Angreifer die einzelnen Bots, um möglichst viel künstlichen Datenverkehr auf eine IP-Adresse zu leiten, sodass der hinter der IP-Adresse liegende Server überlastet wird und (temporär) ausfällt. Damit können der E-Mail-Verkehr, die IP-Telefonanlage, das komplette Netzwerk eines Unternehmens und auch die Webseiten ausfallen. Der Ausfall von Webseiten ist insbesondere für Unternehmen gravierend, bei denen der Online-Auftritt essenzieller Bestandteil des Geschäftsmodells ist, beispielsweise bei Medien- und E-Commerce-Unternehmen. DDoS-Angriffe können des Weiteren auch mit einer Erpressung verknüpft werden, bei der eine Wiederholung der Attacke angedroht wird.

DDoS-Attacke auf Mirai-Botnetz und RWE

Im August 2016 wurde eine massive DDoS-Attacke durch das Mirai-Botnetz durchgeführt. Basis war ein Zusammenschluss von rund 600.000 Computern und vernetzten Geräten wie Routern und Webcams. Ziel des Angriffs war der Internet-Dienstleister Dyn, der den Zugriff auf Webserver von Unternehmen regelt. Im Zuge dieser Attacke waren die Webseiten von Unternehmen wie Amazon, CNN, The Guardian, Netflix, Spotify, Twitter über Stunden nicht mehr erreichbar. Ein indirektes Opfer war auch die Deutsche Telekom, deren Router für das Botnetz genutzt werden sollte. Die Angreifer versuchten, sich Zugang über eine Fernwartungsschnittstelle der Router zu verschaffen. Zwar misslang die Einbindung der Router in das Botnetz, jedoch fielen circa 900.000 Router durch die Attacke aus, wodurch nach Unternehmensangaben ein finanzieller Schaden von 2 Millionen Euro entstand.

Am 24. September 2018 wurde RWE Opfer einer DDoS-Attacke, die die Webseite des Unternehmens störte. Sicherheitsrelevante Technik wie Kraftwerkssteuerungen waren vom Angriff nicht betroffen. Drohungen im Internet lassen die Vermutung zu, dass die Angreifer aus dem Umfeld der Proteste rund um die geplante Rodung des Hambacher Forsts im rheinischen Braunkohletagebau stammen.

2.3.3 Erpressungs- alias Kryptotrojaner

Bei Erpressungstrojaner, die sogenannte Ransomware (auf Englisch „ransom", das heißt Lösegeld), handelt es sich um Schadprogramme, die den Zugriff zu einem Rechner verwehren oder beschränken (beziehungsweise vorgeben, dies zu tun). Diese Beschränkung besteht solange, bis eine übermit-

telte Lösegeldforderung erfüllt wurde. Diese Lösegeldforderung ist oftmals auf die finanziellen Möglichkeiten der Unternehmen abgestimmt.

Bei Ransomware gibt es zwei Arten: Die Zugangssperre zu einem System oder bestimmten Systemfunktionen oder die Verschlüsselung von Dateien beziehungsweise Daten. Wenn beispielsweise in einer Produktionsanlage die Steuerungssoftware gesperrt wird, können Angreifer so die gesamte Anlage blockieren, bis das Lösegeld gezahlt wird.

Bei Ransomware gibt es eine Vielzahl von Maßnahmen, die ausreichen, um das Schutzniveau deutlich zu verbessern. Dazu zählen zum Beispiel regelmäßige Software-Updates. So gibt es für die Ransomware „Emotet", bereits seit eineinhalb Jahren das passende Update, um Sicherheitslücken zu schließen. Aber es gibt genauso viele gute Gründe, Updates erst auf Stabilität sowie Kompatibilität mit Hardware und anderer Software zu prüfen. Auch kann ein Update einen Verlust vorhandener Zertifizierungen bedeuten. Es gilt also jeweils, Pro und Contra abzuwägen. Oft sind die Hersteller ein Teil des Problems, wenn schlechte Qualitätsstandards und Preistreiberei ein generelles Mistrauen gegenüber Softwareaktualisierungen erst wecken.

Eine weitere Lösung ist die Segmentierung von Laufwerken, sodass der Schaden möglichst nicht alle Einheiten gleichzeitig betrifft. Hier sieht eine sinnvolle Lösung für jedes Unternehmen anders aus. Ein gravierender Fehler ist auch in der Back-up-Politik mancher Firmen zu finden. Back-ups, die permanent mit den zu sichernden Laufwerken verbunden sind, haben eine hohe Wahrscheinlichkeit, mit verschlüsselt zu werden. Ebenso sind Formulierungen, wie „Wir haben zwar ein Back-up, doch wir haben noch nie versucht, es wieder einzuspielen", oder „Oh, die Festplatte des Back-ups ist seit Januar voll!" im Moment der Vollverschlüsselung für ein Unternehmen totbringend. Es ist also nicht nur zielführend, sich mit den neuesten Bedrohungen zu befassen, sondern auch entsprechende Standards mit der IT klar zu regeln und in Übungen zu testen.

Ransomsoftware: Krauss-Maffei Gruppe
Am 21. November 2018 wurde das Münchner Maschinenbauunternehmen Krauss-Maffei mit der Ransomware „Emotet" angegriffen. Diese Software verschlüsselte Computerdateien, sodass zu Beginn der Attacke einzelne Steuerungen in der Fertigung und Montage nicht mehr gestartet werden konnten. Auch zwei Wochen nach dem Angriff gab es noch an mehreren Standorten eine gedrosselte Leistung in der Produktion. Insgesamt kam es zu Produktionsausfällen. Aus Sicherheitsgründen wurden einige Server abgeschaltet, im Zuge dessen war auch die Verbindung zu Kunden unterbrochen. Auf elektronischem Wege war das Unternehmen nur eingeschränkt erreichbar. Die Angreifer stellten eine Lösegeldforderung in unbekannter Höhe. Ebenfalls nicht bekannt ist die Größenordnung des finanziellen Gesamtschadens.

2.3.4 Business-E-Mail-Crime
Eine neue Form der Kriminalität gegen Firmen kommt in Deutschland verstärkt seit 2015 vor. Die Rede ist vom sogenannten Business-E-Mail Scam, dem Betrug mit vermeintlich geschäftlichen E-Mails. Bei diesen Angriffen steht nicht die Technik im Mittelpunkt, sondern die Täuschung des Mitarbeiters im Unternehmen. Durch eine fingierte, glaubhafte Story soll ein Mitarbeiter dazu veranlasst werden, scheinbar korrekte Zahlungen zu autorisieren oder Fremden Zugang zum Arbeitsplatz zu gewähren – etwa durch den Einsatz von Fernwartungssoftware, mit dem Ziel, das Onlinebanking der Firma zu kompromittieren (siehe Kapitel 2.3.4.2 bis 2.3.4.6). Damit entsteht ein Schadenspotenzial, welches mit einem Angriff von Innen vergleichbar ist. Eine technische Abschirmung hilft nicht gegen diesen Betrug, denn die Ausführenden sind instrumentalisierte, grundsätzlich vertrauenswürdige Mitarbeiter. Schutz gegen diese Form des Betrugs bieten sichere Prozesse und eine ständige Aufklärung potenziell betroffener Mitarbeiter. Schließlich bereiten sich die Täter je nach Angriffsmethode sehr gezielt und zeitintensiv auf potenzielle Opfer vor. Aus Einzelfällen sind Vorbereitungszeiten von bis zu 16 Monaten bekannt, in denen das Unternehmen trickreich ausspioniert wird. Dabei kommt Social Engineering **(siehe Kapitel 2.3.6)** als eine Methode zum Einsatz. Die Tätergruppen verfügen meist über psychologisches Wissen, dem Fachwissen zum Ablauf von Zahlungen sowie technisches Knowhow. Durch falsche Identitäten werden Informationen erlangt und wie ein Puzzle zusammengesetzt, bis das erlangte Wissen für die eigentliche Täuschung ausreicht.

2.3.4.1 Tücken im Umgang mit E-Mails
Wenn wir uns bewusst machen, wie wir E-Mails lesen und bewerten, wird damit gleichzeitig auch die Grundlage aller Betrugsarten des Business-E-Mail-Crime verständlich. Geschätzt wird, dass in über 70 Prozent der deutschen mittelständischen Unternehmen noch heute eine E-Mail des Chefs tatsächlich genügt, um einen Zahlungsauftrag in der Buchhaltung auszulösen. Doch warum wird dem Medium E-Mail so vertraut? Weil es über Jahre so gut funktioniert hat und nichts passiert ist? Weil es keine anderen Möglichkeiten gibt? Oft ist es fehlendes Risikobewusstsein, gepaart mit der Bequemlichkeit, sich nicht anpassen zu müssen sowie einer falschen Anwendung des Mediums E-Mail.

Das Experiment
Bitten Sie als Chef eine Gruppe Anwender in Ihrem Unternehmen, mit Ihnen gedanklich die Schritte der E-Mail-Bearbeitung durchzugehen. Alle werden zuerst das E-Mail-Programm öffnen. Dann wird auf den Ordner Posteingang geschaut, der als Liste alle neuen und bisherigen E-Mails anzeigt. An dieser Stelle wird den meisten Anwendern zufolge der Absender und der Betreff der Nachricht gelesen und die Relevanz bewertet. Doch was kommt dann? Der Anwender öffnet die E-Mail. Wo schaut er als nächstes hin? Er schaut auf den Inhalt der E-Mail. Nur sehr selten gibt es Mitarbeiter, die hier noch einmal ganz nach oben am Beginn der E-Mail auf den Absender schauen.

Genau darin besteht eine der vielen Tücken im Umgang mit E-Mails. Im Posteingang sehen Sie eigentlich nur den Alias des Absenders! Nicht die absendende E-Mail-Adresse. Es kann dort also durchaus der richtige Name des Chefs stehen, auch wenn die Absenderadresse nichts mit Ihnen oder Ihrer Firma zu tun hat. Der Alias kann vom Absender frei festgelegt werden. Erst mit dem Öffnen der E-Mail wird die E-Mail-Adresse des Absenders wirklich ersichtlich – in eckige Klammern gesetzt, vom rechten Ende aus zu lesen. Sie ist am besten Zeichen für Zeichen zu prüfen.

Allein dieses Bewusstsein würde die überwiegende Zahl solcher Betrugsfälle verhindern. Darüber hinaus gilt: Wichtige Prozesse dürfen nicht allein auf der Basis von E-Mails ablaufen, denn in einer E-Mail kann fast alles gefälscht werden. Gute Spamfilter verhindern in der Regel aber zumindest, dass E-Mails überhaupt zugestellt werden, wenn die absendende IP-Adresse und die E-Mail-Adresse des Absenders nicht zusammenpassen.

2.3.4.2 Fernwartungssoftware

Beim Einsatz mit Fernwartungssoftware gibt sich der Betrüger zum Beispiel als IT-Mitarbeiter oder als Mitarbeiter des Softwareherstellers aus oder meldet sich als technischer Support der eigenen Hausbank. Diesen Angriffen gemein ist, dass die Hilfestellung aufgedrängt wird, ohne dass der Angerufene ein Problem wahrnehmen kann oder dieses beim IT-Support gemeldet hätte. Der Täter bittet um den Aufruf einer Fernwartungssoftware aus dem Internet. Administratorenrechte sind dafür nicht erforderlich. Geht der Mitarbeiter darauf ein, ist dies in etwa so, als würde er den eigenen Rechner ohne Passwortschutz an einer für jedermann zugänglichen Stellen positionieren.

Opfer werden während des Einsatzes der Fernwartungssoftware gebeten, das Onlinebanking zu öffnen. Passwörter sollen in Felder eingegeben werden, wo sie dann in Klartext erscheinen und nicht durch Punkte verdeckt dargestellt sind. Damit kann sie auch der Täter mitlesen. Je nach Verfahren findet der Täter auch für die Autorisierung von Zahlungen Lösungen. Die Nachvollziehbarkeit wird dadurch verschleiert, dass angebliche Reparaturen die Nutzung des Onlinebankings für einen Tag unmöglich machen. In Wirklichkeit ändert der Täter aber nur die Zugangsdaten, um Zeit zu gewinnen.

2.3.4.3 Gefälschte Zahlungsbestätigungen

Dieser Betrug ist eigentlich nicht wirklich neu, doch die Dreistigkeit der Täter hat eine neue Dimension erreicht. Dazu werden recht professionell wirkende eigene Firmenauftritte im Netz fingiert und eine seriöse Geschäftsadresse gefälscht. Seltener sind die Fälle, in denen eine echte Adresse eines Kleinunternehmens gekauft und dann mit all den positiven Bewertungen in Auskunfteien missbraucht wird. Ziel bei diesem Betrug ist es, bestellte Ware zur Auslieferung zu bringen, noch bevor der Verkäufer sein Geld erhalten hat. Dabei wird die Überweisung mittels vermeintlicher Zahlungsbestätigungen vorgetäuscht und mit gespieltem Unverständnis auf den ausstehenden Zahlungseingang reagiert. Im Vertrag festgehaltene Verzugsstrafen werden zitiert, um den Druck zu erhöhen. So entstandene Schäden gehen in Einzelfällen bis in den sechsstelligen Bereich. Dabei ist der Charakter einer Überweisung recht klar geregelt. Ähnlich wie bei einem Paket trägt der Überweisende die Verantwortung, bis das Geld auf dem Konto des Empfängers angekommen ist. Angesichts immer schnellerer Zahlungsabwicklungen erscheint die Zahlungsbestätigung und das verfrühte Freigeben von Ware eigentlich aus heutiger Sicht ein überflüssiges Überbleibsel aus vergangenen Zeiten.

2.3.4.4 Rechnungsbetrug

Rechnungsbetrug mag aus der Vergangenheit schon bekannt sein. Aber auch hier hat sich die Methodik noch einmal verändert. Taucht eine Rechnung für nicht bestellte Ware auf, wird man in der Buchhaltung möglicherweise stutzig. Anders sieht es aus, wenn der Chef die Leistung vermeintlich selbst geordert hat. Welche Buchhalterin will ihrem Chef schon den neuen Chefsessel in Abrede stellen oder mag über eine Dienstleistung oder Rechnung diskutieren, wenn doch der Chef sie persönlich an die Buchhaltung adressiert hat: „Mit der Bitte um Erledigung. Brauche hierzu keine Rückmeldung."

Täter haben gemerkt, dass es nicht immer eines großen CEO-Frauds bedarfs **(siehe Kapitel 2.3.4.6)** und Kleinvieh auch Mist machen kann. So liegen die Summen des kleinen „Chefbetrugs" bei circa 20.000 bis 150.000 Euro nur selten darüber. Der Chef hat scheinbar vergessen, eine wichtige Überweisung auszulösen und ist unterwegs. Er fragt nach dem Kontostand und ob heute noch 39.899 Euro überwiesen werden können. Fällt der Text nicht durch schlechte Übersetzungen auf, in denen aus einem Kontostand (auf Englisch: balance) auf einmal die Frage nach dem Gleichgewicht wird, kann es sein, dass die Buchhalterin den fremden Absender (in eckigen Klammern hinter dem Alias) nicht erkennt und antwortet. Danach folgt sofort die detaillierte Aufforderung zur Überweisung mit allen notwendigen Daten. Erstaunlich oft wird zuerst überwiesen, bevor die Buchhalterin stutzig wird, weil der Chef sie heute anders anspricht. Dabei ist der Prozess das Problem, denn eine E-Mail des Chefs darf nicht alles sein, was für die Auslösung einer Zahlung in einem Unternehmen nötig ist. Ändert sich hier das Verhalten nicht, wird es für die Hausbank unmöglich, in Zeiten von Instant Payments – in denen Zahlungen in zehn Sekunden von einem europäischen Konto zum anderen transferiert werden können, noch Gelder zu retten.

2.3.4.5 Betrug mit der geänderten Bankverbindung

Dieser Betrug basiert im Wesentlichen auf einem Anwenderfehler, er hat in einigen Fällen aber auch eine technische Komponente. Ziel des Betrugs ist die Änderung der Bankverbindung. Die Liste umgeleiteter Zahlungen ist so groß, wie es Zahlungsgründe gibt. Am gebräuchlichsten ist es, den E-Mail-Verkehr zwischen zwei Geschäftspartnern zu beobachten. Wo genau das passiert, ist später oft nur schwer nachzuvollziehen. Im Rahmen von Bestellung und Auftragsbestätigung bemerkt der Täter, dass hier auch Rechnungen übermittelt werden. Danach gibt es viele Optionen, an das fremde Geld zu gelangen. Eine Variante ist es, der echten Rechnungs-E-Mail gleich eine vermeintliche Korrektur-E-Mail nachzusenden – mit der Begründung, man habe vergessen, die neue Bankverbindung einzutragen. Eine weitere Variante ist es, sich in die Mailkommunikation als „Mann in der Mitte" (Man-in-the-middle) hinein zu manipulieren. Dann erhält man zwar eine erwartete E-Mail des Geschäftspartners – es ist aber nur noch die Kopie einer zuvor gelöschten Mail, die nie ihr Ziel erreicht hat.

Die Absender-E-Mail weicht nur geringfügig von der des Geschäftspartners ab. Allerdings kann der falsche Absender nicht an dem im Posteingang angezeigten Aliasnamen erkannt werden. Der ist korrekt – auch dann, wenn man die E-Mail geöffnet hat. Erst die in eckige Klammern gesetzte E-Mail-Adresse des Absenders hinter dem Alias verrät in aller Regel die Fälschung, wenn man sie Buchstabe für Buchstabe vergleicht. Wird dies nicht bemerkt, antwortet man nicht dem Geschäftspartner, sondern nur einer zum Verwechseln ähnlichen E-Mail-Adresse des Täters. Der spielt das gleiche Spiel nun auch in die Gegenrichtung. Wird auch diese Abweichung nicht bemerkt, kommunizieren nun beide nicht mehr miteinander, sondern mit dem Täter, der die Nachrichten jeweils mit der eigenen Mailadresse an die Geschäftspartner weiterreicht. Bis eines Tages eine Rechnung anhängt, in der die Bankverbindung geändert wird. Bemerkt das Opfer diese Änderung nicht – zum Beispiel durch einen Abgleich mit vorhandenen Stammdaten des Geschäftspartners - und gibt es keine Sicherheitsprozesse, wird der Betrag auf das Konto des Täters überwiesen. Selbst mit einer Mahnung wird der Betrug oft noch nicht entdeckt – und durch Nachforschungsaufträge zur Überweisung vergeht kostbare Zeit. Die Änderung von Bankkonten kann aber auch bei Gehaltskonten mit fingierten Anschreiben an die Personalabteilung erfolgen. Selbst Mietzahlungen hat man schon umzuleiten versucht. Dazu werden in den Hauseingängen Schreiben angebracht, die eine vermeintliche Änderung der Eigentumsverhältnisse anzeigen – verbunden mit der Aufforderung, die Miete ab dem nächsten Monat auf das neue Konto einzuzahlen.

Trotz der Mahnung des Geschäftspartners tun sich einige Firmen immer noch schwer damit, diesen Betrug zu erkennen und die richtigen Schritte einzuleiten. So mündet die Mahnung erst in einen Nachforschungsauftrag bei der Bank, der unnötig Zeit kostet. Denn die Antwort wird lauten, dass der Betrag dem entsprechenden Konto gutgeschrieben wurde. Auch ein Zahlungsrückruf auf Kundenwunsch ist bei einem Betrug nicht das korrekte Mittel. Denn in diesem Fall fragt die Empfängerbank den Täter nach seinem Einverständnis zur Rücküberweisung. Wie hier die Antwort lauten wird, ist absehbar. Ein Rückruf wegen Betrugs hingegen eröffnet der Empfängerbank weitreichendere Möglichkeiten. Zudem steigt die Wahrscheinlichkeit, das Geld noch zu retten, je weniger Zeit verstrichen ist – und je klarer der Rückforderung auch mit Anwälten nachgegangen wird.

2.3.4.6 CEO-Fraud

Es soll schon Unternehmen gegeben haben, die meinten, der Betrug kann sie nicht treffen, da sie ja keinen CEO haben. Einer der vielen Trugschlüsse zum CEO-Fraud, denn die Einschläge verteilen sich gleichmäßig auf Dax-Konzerne sowie kleine und mittelständische Unternehmen. Von rund 600 Versuchen waren Täter in Deutschland immerhin in etwa 100 Fällen erfolgreich. Ursachen sind oft fehlende Schulungsmaßnahmen und unzureichende Schutzmechanismen in den Unternehmen selbst. Kommt es zum CEO-Fraud und die Firma muss einen schwerwiegenden Verlust mittels Ad-hoc-Nachricht veröffentlichen, wird sie an der Börse in aller Regel wesentlich härter

abgestraft, als es der eigentliche finanzielle Schaden rechtfertigen würde. So brach der Aktienkurs der FACC AG nach einem der ersten CEO-Frauds im Januar 2016 um rund 40 Prozent ein. Durch den Betrug verlor das Unternehmen etwa ein Sechstel der Marktkapitalisierung.

Wie funktioniert der Betrug? Auch hier kann es sein, dass dem Betrug selbst eine Vorbereitungszeit von mehreren Monaten vorausging. Durch teils harmlos wirkende Anrufe wurden Informationen erfragt und Verantwortliche im Unternehmen ausfindig gemacht. Man studierte deren Xing-Profile, Verknüpfungen zu Kollegen und Geschäftspartnern, zu Key Playern in Tochter- und Mutterunternehmen. Internetauftritte, die das eigene Management darstellen und informativ Strukturen der Firma präsentieren, reichern die Informationen an. Jetzt bedarf es nur noch eines Gerüchts in den Medien. Motive für eine anstehende vertrauliche Finanztransaktion können vielseitig sein. Film- oder Marketingrechte, die erworben werden sollen, eine anstehende Fusion oder äußerst lukrative Werbeverträge im Motorsport, die es zu bezahlen gilt – ohne viel Federlesen und sehr vertraulich.

Einem nichtsahnenden Mitarbeiter kommt dabei eine besondere Bedeutung zu. Er wird zum ersten Mal so deutlich wie nie von seinem vermeintlichen Chef gelobt und quasi als Belohnung mit der Durchführung des Projekts betraut – allerdings nicht allein. Ein vorgeblich externer Profi – meist mit Doktortitel versehen und von einer Unternehmensberatung, einer namhaften Anwaltskanzlei, einer Wirtschafts- oder Steuerprüfungsgesellschaft – steht dem Mitarbeiter zur Seite und soll von diesem als erstes per E-Mail kontaktiert werden. Generell gilt ein Verbot mündlicher Absprachen – auch der Finanzaufsicht wegen. Alles muss per E-Mail kommuniziert werden, damit es dokumentiert und nachvollziehbar ist. Also bitte keine Anrufe oder Ansprachen im öffentlichen Raum.

Dabei wird der Mitarbeiter vom gefälschten Chef und dem angeblichen Berater so gekonnt und glaubwürdig umworben, dass er keinen Verdacht schöpft. Sensible Interna werden dem externen Berater bereitwillig mitgeteilt. Auf diesem Weg gelangen Kontostände, Vertretungsberechtigungen und weitere für den perfekten Betrug notwendige Informationen auf die Täterseite.

Fehlen nur noch die bei der Bank hinterlegten Unterschriften. Aber auch dafür gibt es eine Geschichte. Eine solche Fusion muss bei der Finanzaufsicht angemeldet werden. Der Mitarbeiter erhält einen fertig ausgearbeiteten Fusionsvertrag und soll diesen mit den für die Firma hinterlegten Unterschriften bei der BaFin einreichen. Die hierzu genannte E-Mail-Adresse gehört aber auch zum Täter, der diese Fusion bewilligen wird. Er fordert den Mitarbeiter im Unternehmen nun zur Transaktion auf. Kann dieser nicht allein und mit ausreichendem Limit elektronisch unterschreiben, erhält er einen vorunterschriebenen Zahlungsauftrag, den er bitte bei der Bank beauftragen soll. Gelingt die Überweisung, wird der Berater den Mitarbeiter loben und die nächsten Schritte absprechen, denn es stehen weitere Überweisungen an. Wird dies von der betroffenen Firma nicht entdeckt, geht der Schaden schnell in die Millionen und bedroht im schlimmsten Fall die Existenz der Firma.

Vor diesem Hintergrund ist es verständlich, dass von gut geschulten Mitarbeitern bemerkte und gemeldete CEO-Fraud-Versuche beim Chef eine Mischung aus Panik und Euphorie aufkommen lassen. Schutz gegen einen CEO-Fraud bietet vor allem eine funktionierende Unternehmenskommunikation, die alle Mitarbeiter zur Wachsamkeit anhält. Denn die Täter haben sich über Monate vorbereitet, vermutlich werden sie es gleichzeitig an mehreren Stellen im Unternehmen versucht haben. Noch unklar ist, ob die zu beobachtende hohe Trefferquote bei Abwesenheit der Chefs Zufall ist, dem Durchschnitt von Anwesenheiten entspricht oder ob hier Informationen aus Datenlecks eine Rolle spielen.

CEO-Fraud: Leoni AG
Im August 2016 wurde die Leoni AG Opfer eines CEO-Frauds. Die Täter nutzen dafür gefälschte Dokumente und Identitäten sowie elektronische Kommunikationskanäle. Der Betrüger hatte sich gegenüber den Mitarbeitern des Unternehmens als Kollege mit besonderen Befugnissen ausgegeben und so bestimmte Geschäftsvorgänge vorbereiten lassen. Das Geld, ein Betrag von 40 Millionen Euro, wurde auf Konten im Ausland transferiert und so von den Tätern erbeutet.

2.3.5 Die Werkzeuge

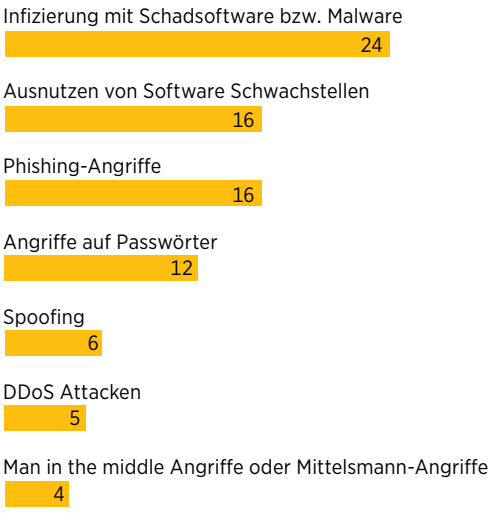
Für den illegalen Zugang zum IT-System, der Verbreitung der Ransomware und anderen Schadprogrammen stehen den Angreifern unterschiedliche Wege zur Verfügung.

Hacking

Angreifer können Schwachstellen in einem Fernwartungstool nutzen, Updatekanäle infiltrieren („Install-/Update-Hijacking"), den Zugang über ungesicherte externe Dienstleister nutzen oder auf die achtlose Verwendung von infizierten USB-Sticks setzen. So haben Forscher im April 2015 auf dem Campus einer Universität in den USA 300 USB-Sticks verteilt. Davon wurden 144 Stück aufgehoben und darin enthaltene Dateien geöffnet. Ein Hacker wird diese USB-Sticks aber noch mit schlüssigen Anreizen versehen, um mit besseren Quoten dazustehen – zum Beispiel mit einem Aufkleber „Gehaltsabrechnung 2018" oder „Personalplanungen 2019".

NetCom
Hacker drangen im Jahr 2017 in das Telefonnetz des Unternehmens NetCom ein, einer Tochter der EnBW. Der Zugang gelang ihnen über einen externen Dienstleister. Allerdings wurden Gegenmaßnahmen ergriffen und der Angriff erfolgreich abgewehrt. Außerdem wurde von EnBW versichert, dass es keine Verbindung zum Datennetz von EnBW gab und somit auch keinen etwaigen Zugriff auf die Steuerung von Kraftwerken.

Grafik 2: Digitale IT-Angriffe, die innerhalb der letzten 2 Jahre einen Schaden verursacht haben, Anteil der befragten Industrieunternehmen in %, Mehrfachnennung möglich



Quelle: Bitkom Research

Spam-E-Mails

Für den Zugang kommen auch die immer noch existenten, ganz normalen Spam-E-Mails an Mitarbeiter des Unternehmens in Betracht, die infizierten Anhänge oder Links enthalten. Sie ganz zu filtern, würde wahrscheinlich auch einzelne wichtige Geschäfts-E-Mails unbeabsichtigt aus dem Verkehr ziehen. Daher ist die Schulung von Mitarbeitern im richtigen Umgang mit E-Mails unabdingbar. Zwar ist es je nach E-Mail-Programm rein theoretisch möglich, schon aus dem Vorschaufenster einer HTML-E-Mail heraus eine Infektion zu bekommen, doch ist dies eher unwahrscheinlich. Fast alle Infektionen entstehen nach einem Klick. Daher hilft es, die Echtheit der E-Mail und des Absenders sowie den Umstand erst zu verifizieren, bevor man der E-Mail vertraut. Die Mitarbeiter sollten nach anderen Wegen suchen, die Plausibilität zu prüfen. So kann man die Internetseiten der vorgegebenen Absender direkt in einem neuen Browserfenster öffnen, ohne die Links und Anhänge der E-Mail zu benutzten. Schnell wird sich herausstellen, ob sie wirklich ein Paket bekommen, eine Rechnung aussteht oder die unberechtigte Paypal-Transaktion wirklich stattgefunden hat. Das Risiko lässt sich für eine Firma aber auch minimieren, in dem es unmissverständliche Handlungsanweisung für die Trennung von beruflicher und privater Nutzung auch im Hinblick auf beruflich genutzte Soziale Medien gibt. Denn wenn ich erst gar keine Posts unter meiner Firmen-E-Mailadresse erwarte, ist die Unterscheidung zwischen Spam und wichtiger geschäftlicher E-Mail noch einfacher.

Phishing

Spam-E-Mails werden gern zum Phishing (einer Wortschöpfung aus PIN und Fishing) eingesetzt. Mittels einer E-Mail soll der Empfänger dazu bewegt werden, vertrauliche (persönliche) Informationen preiszugeben. Das können beispielsweise Zugangsdaten zu Online-Anwendungen, Banking oder Kreditkartendaten sein. Während das simple Phishing nur eine geringe Öffnungsrate verspricht, haben sich Täter im Firmenumfeld auf zwei besondere Formen des Phishings konzentriert: dem Spear-Phishing und dem Whaling.

Spear-Phishing und Whaling

Liegen Öffnungsraten beim Phishing im unteren einstelligen Bereich, so sind Spear-Phishing-E-Mails mit einer über 70-prozentigen Leserate schon wesentlich gefährlicher für ein Unternehmen. Immer wieder ist man erschrocken, wenn man bemerkt, dass eine E-Mail trotz der genauen Ansprache, der enthaltenen persönlichen Daten bis hin zu Telefonnummer und Adresse auf einmal doch noch als Phishing-Mail erkannt wird. Womöglich hat auch der Inhalt noch Sinn, kommt die E-Mail vorgeblich von einem befreundeten Kollegen aus dem Nachbarbüro – mit der Aufforderung, sich den Inhalt anzuschauen. Einer der bekanntesten Angriffe mit dem Einsatz von Spear-Phishing richtete sich im Jahr 2015 gegen den Bundestag. Unter Vorgabe einer Betreffzeile „Ukraine conflict with Russia leaves economy in ruins“ kam die E-Mail von @un.org, was auch nach Öffnen des Links auf der Seite nichts anderes erwarten lies als eine Abhandlung der UNO über besagten Betreff. In Wirklichkeit wurden die Rechner durch den Besuch der Seite mit einem Trojaner infiziert. Von Whaling spricht man, wenn sich das Spear-Phishing gezielt gegen die Führungsebene von Unternehmen richtet.

Vishing

Vishing wird im Deutschen oft analog zum Phishing gern als Voice-Fishing erklärt. Doch ist diese Herleitung eher verwirrend, denn es geht nicht um den Fang Ihrer Stimme. Vishing funktioniert eher wie Voice Solicitation, also die stimmliche Aufforderung, Dinge zu tun und Auskünfte zu geben. Dem Täter gelingt es dadurch, einen Angriff besser vorzubereiten. Social Hacker – so werden die Angreifer eines Vishing-Calls genannt – haben meist ein hohes psychologisches Know-how und Einfühlungsvermögen, gepaart mit schauspielerischer Grundveranlagung. Sie gehen höchst planvoll vor und verwenden bei ihrem Angriff verschiedene Techniken des „Social Engineerings“. So wird vor einem Anruf jeder mögliche Gesprächsverlauf vorbereitet, potemkinsche Dörfer werden errichtet, die den Angerufenen psychologisch überrumpeln und geschickt zum eigentlichen Ziel des Angreifers führen.

Das Telefonat mag für den Angerufenen äußerst unwichtig erscheinen – ist es aber nicht. Nehmen wir das Beispiel des Praktikanten, der sich plötzlich am Telefon meldet, da er von der Personalabteilung gebeten wurde, sich vor seinem Arbeitsbeginn in 14 Tagen telefonisch vorzustellen. Er behauptet, gerade eben schon einmal verbunden worden zu sein. Als er mit einem Ihrer Kollegen sprach, wurde die Handyverbindung unterbrochen. Nun habe er sich den Namen nicht gemerkt, würde sich aber bei Nennung möglicher Namen doch erinnern. Soweit der erste Teil, der zu keinem Ergebnis führt,

da keiner der Namen passt und der Praktikant vermutet, nur falsch verbunden worden zu sein. Zwei Tage später meldet sich ein anderer Anrufer, der sich über die Telefonzentrale gezielt mit einem der genannten Mitarbeiter verbinden lässt. „Mein Name ist Herr ... Bin ich jetzt mit Frau XYZ verbunden?" – „Ja" – „Sie arbeiten in der Abteilung 123?" – „Ja" – „Im Team mit Frau ..., Herr ... und Herr ...?" – „Ja" – „Mir wurde gesagt, dass Sie mir helfen können, wenn ich den bisherigen Prozess zur Freigabe von Großbetragszahlungen benötige. Ich rufe aus dem Projekt XYZ an. Wir begleiten Ihr Unternehmen gerade in der Optimierung von Zahlungsläufen."

Man erkennt: Cyberangriffe sind nicht nur eine Frage der Technologie, vielmehr spielt der Faktor Mensch oftmals eine entscheidende Rolle, wie das Social Engineering zeigt.

2.3.6 Social Engineering
Beim Social Engineering, das ebenfalls zur Vorbereitung einer Cyberkriminalität gezählt werden kann, kommt primär keine Technologie beziehungsweise Software zum Einsatz. Im Fokus steht der Versuch, durch „Aushorchen" den Aufbau von Vertrauen oder Manipulation eines Menschen an unberechtigte Informationen beziehungsweise Zugänge zu IT-Systemen zu gelangen.

Social Engineering basiert auf psychologischen Tricks, Charisma, der Ausnutzung menschlicher Eigenschaften wie Vertrauen, Respekt vor Autorität, Hilfsbereitschaft sowie der Unbedarftheit und Leichtgläubigkeit.

Die Angreifer versuchen, so viele Informationen wie möglich zu sammeln, um das Vertrauen des Opfers zu gewinnen oder Schwachpunkte zu finden. Menschen hinterlassen allein im Netz viele kleine Informationsstücke (Facebook-Posts, Standort, Bilder), die zusammengefügt ein facettenreiches Bild über die Person und ihr Verhalten abgeben. Soziale Netzwerke sind eine gute Ausgangsbasis für Social Engineering, da dort viele Hintergrundinformationen vorhanden sind, die zur weiteren Informationsbeschaffung genutzt werden können. Oftmals vernetzen sich die Angreifer geradezu mit ihren Opfern.

Die Erfolgschancen der Manipulation sind dabei umso größer, je mehr vertrauensbildende Informationen über das Opfer gesammelt und genutzt werden. So zeigt eine Untersuchung von Forschern der Universität Erlangen-Nürnberg, dass ein Link in einer E-Mail wahrscheinlicher geklickt wird, wenn die E-Mail personalisiert ist (zum Beispiel durch die Anrede). Am Ende hat jeder Mensch einen Trigger, der ihn aus Sicht des Täters zur gewünschten Handlung veranlasst. Ziel des Angreifers ist es, diesen Trigger zu finden. Manche Menschen im Unternehmen öffnen eventuell einen Anhang oder einen USB-Stick genau dann, wenn „Gehaltstabelle Geschäftsführung" darauf steht.

Bei ihrem Angriff unterstreichen Social Engineers dann ihre vorgetäuschte Legitimation mit Selbstsicherheit und Glaubwürdigkeit. Die Täter fragen nicht einfach nach dem Passwort, was das Opfer eventuell misstrauisch machen könnte, sondern geben sich als IT-Mitarbeiter des Unternehmens aus und lassen den Mitarbeiter unbekannte Befehle ausführen, womit versteckte Zugriffsrechte geändert werden. Oder sie bieten nützliche Internetdienste an, bei denen sich die Opfer anmelden sollen, häufig mit ihrem üblichen und einheitlichen Passwort.

Weitere Beispiele für Social Engineering sind:

- Ein angeblicher IT-Mitarbeiter ruft wegen eines aktuellen Cyberangriffs oder eines Systemfehlers an und braucht dringend das Passwort des Nutzers.

- Ein Angreifer findet heraus, dass ein Mitarbeiter Mitglied der Freiwilligen Feuerwehr ist und findet dazu auch den Namen eines Feuerwehrkameraden von ihm heraus. Anschließend schickt er eine Nachricht an die geschäftliche E-Mail-Adresse des Mitarbeiters mit gefälschtem Absender, die vermeintlich vom Kameraden stammt – mit dem Betreff „Bilder vom letzten Einsatz". Der Mitarbeiter öffnet den Anhang und lädt damit eine Malware herunter.

- Ein Angreifer steht an der Eingangstür, mit beiden Händen voll beladen, und wartet auf Einlass (Tailgaiting).

- Ein Angreifer ruft im Unternehmen an und möchte einen Mitarbeiter sprechen. Dabei bekommt er die Auskunft, dass der Mitarbeiter noch fünf Tage im Urlaub und dessen Account damit fünf Tage unbeobachtet ist.

Die größere öffentliche Verfügbarkeit von Informationen im digitalen Zeitalter ist ein Aspekt, der Social Engineering erleichtert. Ein weiterer ist künstliche Intelligenz, wodurch Social Engineering effektiver wird. So können Informationen über die Opfer zielgenauer und automatisiert gesammelt werden. Ferner gelingt so eine bessere Anpassung von Phishing-E-Mails an den Stil des vermeintlichen Absenders. Schließlich gibt es automatische Systeme, die aus einzelnen Infostücken ein Gesamtbild der Zielpersonen zeichnen.

2.4 Selbstbetroffenheit/Selbsteinordnung

Für die Selbsteinordnung Ihres Unternehmens spielen verschiedene Faktoren eine Rolle. Natürlich ist hier der Technisierungsgrad maßgeblich, der gerade durch die Bestrebungen zur Digitalisierung immer größer wird. Es ist aber auch die Bekanntheit und Größe des Unternehmens, die zu einem gezielten Angriff führen können. Neben Größe und Technisierungsgrad gibt es weitere Eckpunkte, die auf ein niedriges oder hohes Risiko einer Attacke hinweisen. Werden täglich große Mengen an Transaktionen über hohe Beträge in verschiedene Länder ausgeführt, oder kommt der Kunde und bezahlt meist vor Ort Zug um Zug? Betreiben Sie einen landwirtschaftlichen

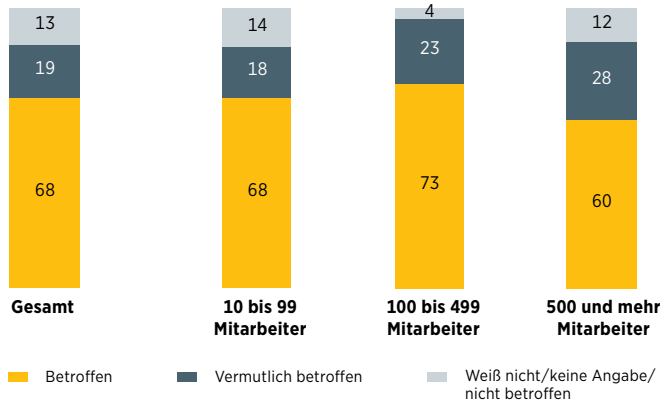
Betrieb oder sind Sie eher für die Softwareverteilung auf mehrere Unternehmen über Fernwartung zuständig? Aus der Summe dieser Faktoren ergibt sich für jedes Unternehmen eine eigene Kenngröße, ein eigenes Risiko, eigene Angriffsvektoren und ein ganz eigener Masterplan, wie mit diesem Risiko umzugehen ist und wie man sich vorbereiten sollte. Einzig eine Annahme ist falsch, sobald Sie auch nur einen Rechner in Ihrem Unternehmen haben: Dass es Sie nicht treffen kann.

2.4.1 Verbreitung von Cyberkriminalität

Cyberkriminalität ist kein Randphänomen, sondern ein Risiko, dem sich jedes Unternehmen – unabhängig von Branche und Größe – bewusst sein muss. Laut einer Bitkom-Studie waren im Jahr 2017 ungefähr zwei Drittel (67 Prozent) der Unternehmen in Deutschland von einem Cyberangriff betroffen. Im Jahr zuvor hatte der Anteilswert erst bei 53 Prozent gelegen. Zu einem ähnlichen Wert für 2017 kommt auch das BSI. Laut der Cyber-Sicherheits-Umfrage waren rund 70 Prozent der Unternehmen in Deutschland Opfer eines Cyberangriffs. Ungefähr die Hälfte dieser Angriffe war erfolgreich, wobei jeder zweite erfolgreiche Angriff mit Produktions- beziehungsweise Betriebsausfällen verbunden war. Es ist davon auszugehen, dass diese Zahlen nur den unteren Rand darstellen. Bei Cyberkriminalität gibt es eine signifikante Dunkelziffer, da Unternehmen Angriffe eventuell gar nicht erkennen. Manche Unternehmen melden die Angriffe nicht, aus Sorge um ihre Reputation oder weil sie davon ausgehen, dass die Täter sowieso nicht gefasst werden.

Wenn auch Unternehmen jeglicher Branche und Größe von Cyberkriminalität betroffen sind, so jedoch nicht alle im gleichen Ausmaß. Unter den Industrieunternehmen in Deutschland sind die Branchen Chemie und Pharma sowie der Automobilbau (vermutlich) überproportional von Cyberangriffen betroffen, wie der Branchenverband Bitkom berichtet. Des Weiteren zeigen die Ergebnisse der Umfrage, dass Mittelständler mit 100 bis 500 Beschäftigten am häufigsten Opfer von Cyberkriminalität sind **(siehe Grafik 3)**.

Grafik 3: Betroffenheit von Cyberangriffen in den letzten 2 Jahren, Anteil der befragten Industrieunternehmen in %



Quelle: Bitkom Research

2.4.2 Kosten von Schäden durch Cyberkriminalität

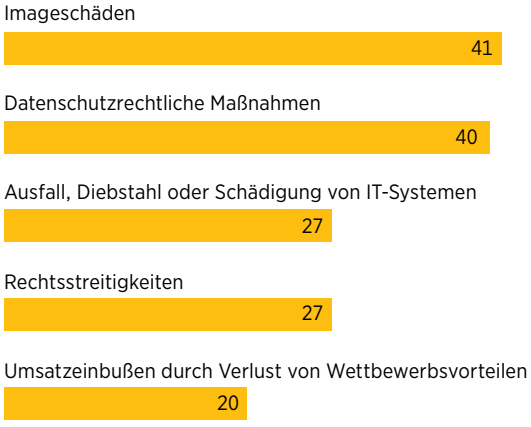
Cyberkriminalität ist ökonomisch beziehungsweise finanziell relevant, wie eine Betrachtung der dadurch verursachten Schäden und Kosten zeigt. Grundsätzlich setzen sich die gesamten Kosten aus verschiedenen einzelnen Blöcken zusammen. Dazu zählen:

- Ausfall, Diebstahl oder Schädigung von IT-Systemen
- Produktionsausfälle
- Imageschäden bei Kunden und Lieferanten
- Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen
- Kosten für die Wiederherstellung nach einem Angriff
- Verlust von geistigem Eigentum und vertraulichen Unternehmensinformationen
- Patentrechtsverletzungen
- Verlust persönlicher Daten, die für Betrug und Finanzdelikte genutzt werden
- Manipulation beziehungsweise Einflussnahme auf den Marktwert von Unternehmen

Des Weiteren kann es in Folge von Cyberangriffen auch zu Rechtsstreitigkeiten kommen. So haben insbesondere ein Diebstahl oder ein anderweitiger Verlust des Zugriffs auf persönliche Daten datenschutzrechtliche Maßnahmen zur Folge. Mit Blick auf die Datenschutzgrundverordnung (DSGVO) müssen die Unternehmen mitunter sogar mit Bußgeldern rechnen **(siehe Kapitel 3.6)**.

Diese datenschutzrechtlichen Maßnahmen sind zusammen mit den Imageschäden auch die Kosten, die am häufigsten bei Cyberangriffen auftreten. Darauf deuten die Aussagen der Industrieunternehmen in der Bitkom-Umfrage hin **(siehe Grafik 4)**. Jeweils rund 40 Prozent der Unternehmen werden im Fall eines Cyberangriffs mit diesen Kosten konfrontiert.

Grafik 4: Häufigste Kostenverursacher, Anteil der befragten Industrieunternehmen, die in den letzten zwei Jahren von Cyberangriffen betroffen waren in %, Mehrfachnennung möglich



Quelle: Bitkom Research

Weiter gefasst fallen auch die Ausgaben für Cybersecurity im Unternehmen darunter. Es gibt unterschiedliche Schätzungen zur Höhe der Kosten von Cyberkriminalität. Aggregierte Schätzungen weisen dabei eine große Bandbreite auf, was auf eine schwache Datenlage, die große Dunkelziffer sowie eine fehlende einheitliche Systematik zur Bestimmung der Kosten zurückzuführen ist. Außerdem sind nicht alle Bestandteile eindeutig zu quantifizieren. Die Kosten eines einstündigen IT-Ausfalls verursachen laut einer Umfrage des Marktforschungsunternehmens Techconsult unter deutschen Mittelständlern Kosten von durchschnittlich 41.000 Euro. Schwieriger ist allerdings die Quantifizierung von Imageschäden nach einem Cyberangriff. Vor diesem Hintergrund sind die folgenden Schätzungen zu sehen.

Für den Industriebereich kommt Bitkom zu dem Schluss, dass die Kosten in den letzten zwei Jahren eine Größenordnung von insgesamt rund 43,4 Milliarden Euro in Deutschland aufweisen. Basis dieser Zahl ist die Befragung von Industrieunternehmen im Jahr 2018, bei der von Angriffen betroffene Unternehmen ihre Schäden schätzen sollten. Anschließend wurden diese Angaben für die gesamte Industrie hochgerechnet.

Als Schadenshöhe für die Gesamtwirtschaft in Deutschland geht das Bundesamt für Verfassungsschutz von jährlich ungefähr 50 Milliarden Euro aus. Eine ähnliche Größenordnung schätzt Jörg Wälder, Experte der Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG: Demnach liegt der Schaden in Deutschland bei rund 50 Milliarden US-Dollar.

Der internationale Spezialversicherer Hiscox hat auf Basis einer Umfrage im Jahr 2017 die Kosten von Cyberangriffen für die einzelnen Unternehmen geschätzt. So liegen die durchschnittlichen Kosten aller Cyberangriffe in den letzten zwölf Monaten bei Unternehmen mit weniger als 250 Beschäftigten bei rund 55.000 US-Dollar je Unternehmen. Bei Unternehmen mit 250 und mehr Beschäftigten betragen die Kosten aller Cyberangriffe in den letzten zwölf Monaten im Schnitt pro Unternehmen knapp 407.000 US-Dollar. In diesen Werten sind allerdings nicht die Verluste an Kunden und Reputation enthalten. Außerdem ist zu berücksichtigen, dass diese Durchschnitte eine Zusammenfassung von Einzelwerten, die zum Teil eine große Bandbreite aufweisen – wie das Beispiel Leoni AG mit einem Schaden von 40 Millionen Euro bei dem CEO-Fraud im Jahr 2016 verdeutlicht.

Der Gesamtschaden durch CEO-Fraud lag für die heimische Wirtschaft laut Deutscher Telekom im Jahr 2016 bei rund 75 Millionen Euro.

Eine andere Größenordnung weisen die Schäden der Attacken durch die Schadprogramme WannaCry und NotPetya auf. So beträgt der globale Schaden durch WannaCry laut BSI einige hundert Millionen bis zu vier Milliarden US-Dollar – es wurden mehr als 200.000 Computer in 150 Ländern infiziert. Constanze Kurz, Sprecherin des Chaos Computer Clubs, beziffert den Schaden sogar auf 4,5 Milliarden US-Dollar.

Noch größer waren die Auswirkungen durch NotPetya. Hier beliefen sich die weltweiten Schäden laut Peter Hacker, ein Experte und Berater für Cybersecurity, im Jahr 2017 auf rund 10 Milliarden US-Dollar. Allein bei den Logistikunternehmen Fedex und Maersk verursachte der Angriff laut Unternehmensangaben jeweils Kosten in Höhe von ungefähr 300 Millionen US-Dollar. So mussten bei Maersk 4.000 Server, 45.000 Computer und 2.500 Applikationen reinstalliert werden.

Beim US-amerikanischen Pharmahersteller Merck & Co. versursachte NotPetya im dritten Quartal Kosten von 310 Millionen US-Dollar, die sich aus 175 Millionen US-Dollar direkte Kosten und 135 Millionen US-Dollar entgangenen Umsatz zusammensetzen.

Welche Auswirkungen Cyberangriffe auf den Marktwert eines Unternehmens haben können, zeigt das Beispiel Yahoo: Nach den Datendiebstählen verringerte sich der Wert des Unternehmens, den Verizon bei der Übernahme von Yahoo zahlte um ungefähr 350 Millionen auf 4,48 Milliarden US-Dollar.

3. Cybersicherheit – Schützen Sie Ihr Unternehmen

Den Unternehmen, die sich mit dem Thema Cybersecurity beschäftigen, sollte von vornherein klar sein, dass es eine absolute Sicherheit vor Angriffen nicht gibt. Cybersecurity kann jedoch die Risiken eines Angriffs und dessen negative Folgen minimieren. Ziel der Sicherheitsmaßnamen ist es daher, die Resilienz beziehungsweise Widerstandsfähigkeit des Unternehmens vor Cyberangriffen zu erhöhen.

Dass Cybersecurity dabei nur zu einem Teil ein technologisches Thema ist, liegt auf der Hand. Mitentscheidend für die Sicherheit des Unternehmens sind aber auch die Organisation und ihre Prozesse (Notfallplan, gleiche Verantwortlichkeiten, Verhalten) sowie der Faktor Mensch. Hier lassen sich ohne großen Aufwand Verbesserungen erreichen.

Beim Schutz vor Cyberangriffen geht es auch um ein Risikomanagement, das auf einem ganzheitlichen Ansatz basiert: Die Verantwortung sollte hierbei nicht bei der IT-Abteilung liegen, sondern bei der Unternehmensführung beziehungsweise Business-Unit-Leitern, da nur diese entscheiden können, welche Prozesse und Daten überlebensnotwendig für das Unternehmen und daher besonders schützenswert sind. Cybersecurity umfasst die IT-Technologie und -Infrastruktur, die Software-Anwendungen, das Knowhow des IT-Personals und nicht zuletzt allgemein den Faktor Mensch. Und das schwächste Glied in dieser Kette bestimmt das allgemeine Sicherheitsniveau.

Die Effektivität der Cybersecurity-Maßnahmen lässt sich steigern, wenn sie mit einer kohärenten Strategie verknüpft wird. Teil dieser Strategie sollte nicht nur die Prävention sein. Die Unternehmen sollten vielmehr immer davon ausgehen, dass der Angreifer schon mitten im System sein könnte. Cybersecurity bedeutet damit auch „Detect“, sprich die aktive Suche nach Angriffen und ungewöhnlichen Entwicklungen beziehungsweise Zugriffen, sowie „Response“, also eine durchgeplante Krisenreaktion. Am Ende ist es bei einem Angriff die Krisenreaktion, die die Schadenshöhe bestimmt.

Cybersecurity ist unbestritten ein Kostenfaktor, der allerdings angesichts potenziell existenzgefährdender Risiken essenziell ist. Investitionen in Cybersecurity sollten von den Unternehmen daher nicht nachrangig behandelt werden. Laut Dirk Backofen, Leiter Security der Deutschen Telekom, sollten 5 bis 6 Prozent des IT-Budgets für Cybersecurity ausgegeben werden, damit ein ausreichendes Schutzniveau erreicht wird. Unternehmen aus dem Bereich der kritischen Infrastruktur sollten 10 Prozent einplanen. Allerdings betonte Gundbert Scherf, Partner bei McKinsey & Company und Experte für Cybersecurity, bei der Handelsblatt Jahrestagung Cybersecurity 2018 in Berlin, dass mehr Investitionen nicht zwangsläufig zu einem höheren Schutzniveau führen. Entscheidend sei der richtige Einsatz der Mittel.

3.1 Herausforderungen für Unternehmen

Beim Thema Cybersecurity werden die Unternehmen mit unterschiedlichen Herausforderungen konfrontiert. Die größte Herausforderung besteht aktuell darin, geschultes Personal zu finden; es herrscht ein eklatanter Fachkräftemangel.

Außerdem erfordert ein effektiver Schutz vor Cyberangriffen die Kenntnis der allgemeinen Gefährdungslage und der aktuellen Bedrohungen. Die Angriffsmethoden unterliegen einer dynamischen Entwicklung, wodurch der Aufwand für Cybersecurity bei Unternehmen permanent ansteigt – nicht zuletzt durch die häufigen Software-Veränderungen.

So werden beispielsweise Plattformen wie WhatsApp und Slack, die verstärkt in Unternehmen Anwendung finden, ständig verändert beziehungsweise weiterentwickelt (zum Beispiel neue Funktionen). Dies erschwert die Anpassung der Cybersecurity-Maßnahmen. Dazu kommt, wie bereits im Kapitel 2 betont wurde, dass Hacker nicht nur immer neue Malware-Varianten haben, sondern durch die zunehmende Vernetzung von Geräten auch immer mehr potenzielle Angriffspunkte finden.

Um diese vernetzten Geräte vor Angriffen zu schützen, müssen die Unternehmen mit drei wesentlichen externen Herausforderungen umgehen:

- Die ganzheitliche Betrachtung aller Systeme ist zwingend erforderlich, denn oft werden Maschinen und Produktionsanlagen länger genutzt als die Hersteller Softwareupdates anbieten. So gibt es immer noch Computer in der Anlagensteuerung, die mit WindowsXP als Betriebssystem laufen, aufgrund der Vernetzung mit den sonstigen Systemen dann jedoch das schwächste Glied in der Sicherheitskette darstellen und Einfallstor für Angriffe sind. Bei IoT-Geräten aus dem B2C-Bereich, beispielsweise mobilen Endgeräten, ist die Verfügbarkeit von Updates – angesichts einer kürzeren Lebensdauer, verglichen mit Maschinen – das kleinere Problem.

- Außerdem fällt künftig stärker ins Gewicht, dass die Hersteller aufgrund kurzer Produktzyklen und einem Fokus auf den Kostenaspekten das Thema Sicherheit in der Entwicklung nur zweitrangig behandeln. Vielfach gilt: „Functionality first, Cybersecurity later“. Angesichts eines hohen Innovationsdrucks – jeder Hersteller möchte mit einem neuen Produkt der Erste am Markt sein – wird Sicherheit nicht von Anfang mitgedacht oder gänzlich vernachlässigt. Bei den Kunden geht dies dann zulasten von Datensicherheit, Resilienz gegen Cyberangriffe und der strategischen Wartungsmöglichkeiten der Produkte. Schlecht geschützte beziehungsweise gepfleg-

te Geräte können allerdings erfolgreich angegriffen und zum Beispiel zu Botnetzen zusammengeschaltet werden. Angreifer können über eine gehackte Webcam in die Maschinensteuerung eindringen und enorme Schäden anrichten.

- Der Schutz vor Cyberangriffen muss entlang der gesamten Liefer- beziehungsweise Wertschöpfungskette gedacht werden. Mit zunehmender Vernetzung zwischen den Lieferanten und Herstellern reicht ein hohes Schutzniveau bei einem Unternehmen nicht aus, wenn ein Zugang ins System über die schlechter gesicherte IT eines Lieferanten möglich ist. Daher erfordert Cybersecurity auch eine Zusammenarbeit und Abstimmung mit anderen Unternehmen.

Die Aufgabe Cybersecurity stellt die Unternehmen zudem vor fünf interne Herausforderungen:

- Einem Teil der Unternehmen ist nicht klar, auf welchem Weg ein effektiver Schutz sowie eine Resilienz gegen Cyberangriffe erreicht werden kann – auch, weil es kein Patentrezept gibt.

- IT-seitig benannte Risiken werden nicht von allen Beteiligten im Unternehmen verstanden. Selbst wenn einzelne Maßnahmen umgesetzt werden, fehlt es in manchen Fällen an der verbindenden Struktur beziehungsweise Strategie.

- In manchen Unternehmen wird Cybersecurity durch Organisations- und Datensilos gehemmt. Einzelne Bereichsverantwortliche haben jeweils nur ihre Abteilungen im Blick und dafür die richtigen Maßnahmen ergriffen. Für das Unternehmen stellen diese Einzelmaßnahmen aber unter Umständen keine optimale Gesamtlösung dar.

- Eine weitere Herausforderung betrifft die unternehmensinternen Kapazitäten. Häufig fehlt ein spezielles Team für Cybersecurity, vielmehr muss sich die allgemeine IT auch um den Datenschutz kümmern. Dies führte insbesondere im Frühjahr 2018 zu einigen Engpässen, als diese Mitarbeiter für die Einführung der Datenschutzgrundverordnung (DSGVO) eigespannt waren.

- Bei den Mitarbeitern außerhalb die IT-Bereichs besteht die Gefahr, dass sich ein Widerstand gegen (zu viel) Cybersecurity bildet. Viele Mitarbeiter empfinden Cybersecurity als überflüssige Bürokratie (zum Beispiel deaktivierte USB-Ports, fehlende Administratorrechte, Zwei-Faktor-Autorisierung, Verbot eigener mobiler Endgeräte). Insofern müssen Unternehmen abwägen zwischen dem Schutzbedürfnis des Unternehmens und der Nutzbarkeit der IT beziehungsweise dem Komfort der Mitarbeiter.

- Eine weitere Abwägung betrifft die Frage von Schutzniveau versus Geschwindigkeit und Agilität bei den Prozessen. Die Anforderungen der Cybersecurity können unter Umständen die Innovationsfähigkeit und die Entwicklungsgeschwindigkeit im Unternehmen blockieren beziehungsweise verlangsamen. Hier gilt es, eine akzeptable Balance der Maßnahmen zu finden.

3.2 Technologische Maßnahmen

Ähnlich vielfältig wie die Möglichkeiten für Angreifer sind die technologischen Instrumente für Cybersecurity in den Unternehmen. Ein Basisschutz wie Passwortsicherung, Firewalls, Virenscanner, Updates und Back-ups ist nahezu in allen Unternehmen vorhanden. Dieser Mindeststandard erweist sich aber angesichts der ständigen Weiterentwicklung auf der Angreiferseite als nicht ausreichend.

In jedem Fall sollte die Cybersecurity im Unternehmen neben der IT auch die Organisation Technology (OT) umfassen. Das sind die Programme, die unmittelbar für die Steuerung der Maschinen zuständig sind. Die Maschinen und Produktionsanlagen sowie deren vernetzte Steuerungssysteme sind bei den Schutzmaßnahmen mitzudenken beziehungsweise einzuplanen.

Dabei sollten IT und OT getrennt bleiben, denn eine Trennung beispielsweise von Verwaltungs- und Produktionssystem oder eine Segmentierung des gesamten Unternehmensnetzwerkes begrenzt die Folgen einer Infektion mit Malware. Allerdings steht dieses Vorgehen im Widerspruch zu den Bestrebungen, im Zuge der Digitalisierung die verschiedenen Systeme im Unternehmen stärker zu vernetzten. Hier zeigt sich erneut, dass der Schutz vor Cyberangriffen immer mit einer Abwägung von unterschiedlichen Unternehmenszielen verbunden ist.

Software
Grundsätzlich kommen für technologische Cybersecurity-Maßnahmen auf der Softwareebene zahlreiche Maßnahmen in Betracht. Eine genaue Auflistung ist den Materialien des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu entnehmen. Unternehmen sollten für die Auswahl der notwendigen Maßnahmen im Zweifel externe Beratung oder Unterstützung nutzen. Auch sollte überlegt werden, Teil der Cybersecurity outzusourcen, wenn im Unternehmen nicht die notwendigen Kompetenzen oder Kapazitäten vorhanden sind.

Hardware
Cybersecurity kann vielfach auch Hardware-Maßnahmen erforderlich machen, zum Beispiel in Unternehmen, die Cloud Computing nutzen, wodurch neue Angriffsrisiken entstehen. Ein vermehrter Einsatz von Edge Computing, bei dem Anwendungen, Daten und Dienste weg von zentralen Rechenzentren beziehungsweise der Cloud hin zu den äußeren Rändern des Netzwerks verlagert werden, könnte diese Angriffsrisiken verringern. Hierbei würden beispielsweise leistungsfähige Kleincomputer die Daten direkt an den Maschinen verarbeiten, ohne dass sie in die Cloud transferiert werden müssen. Auch sollten die Back-up-Systeme nicht dauerhaft mit dem Hauptsystem beziehungsweise dem Internet verbunden sein, um nicht von sich selbst verbreitender Malware infiziert zu werden.

Künstliche Intelligenz (KI)
Der Einsatz von künstlicher Intelligenz in der Cybersecurity wird häufig als eine Möglichkeit für Unternehmen mit nur geringen personellen Kapazitäten in der IT genannt. Unter Umständen können KI-Systeme unter anderem beim Aufspüren von Anomalien eingesetzt werden und dadurch die Sicherheit erhöhen. Denn KI hat die Fähigkeit, Muster und Unregelmäßigkeiten in Daten zu erkennen, die Menschen übersehen. Allerdings sollten Unternehmen sich mitunter von dem Hype um KI nicht täuschen lassen. KI kann sehr personalintensiv sein. Möglicherweise meldet das System konstruktionsbedingt Unmengen von Fehlalarmen, die dann die Mitarbeiter bearbeiten müssen. Auch muss man die KI anpassen, damit sie nicht bei jeder kleinen Veränderung in der Umgebung wieder Fehlalarme generiert. Des Weiteren ist die KI keine universelle Lösung. Vielmehr ist es angebracht, KI nur für Tätigkeiten zu nutzen, die bisher von Menschen ineffizient ausgeführt wurden. Bei manchen Cybersecurity-Maßnahmen werden weiterhin menschliche Fähigkeiten wie die Kreativität benötigt. Dennoch können Unternehmen KI in der Cybersecurity mit Gewinn einsetzen, zum Beispiel für einen maßgeschneiderten Schutz sowie Effizienzsteigerungen.

Relevant ist dies zum Beispiel beim Schutz des Zahlungsverkehrs, der mithilfe von KI und Big Data überwacht werden kann, sodass verdächtige und unautorisierte Überweisungen identifiziert und frühzeitig gestoppt werden können.

KI kann jedoch auch von Angreifern eingesetzt werden, in diesem Sinne ist KI eine Dual-Use-Technologie. Außerdem kann die KI selbst Ziel von Cyberangriffen sein. Und weil die Prozesse und Entscheidungen der Algorithmen nicht transparent sind, ist es sehr schwierig zu erkennen, wann die Systeme gehackt und manipuliert werden. Dies ist ein (dramatisches) Problem, für das es derzeit noch keine vernünftige Lösung gibt.

Security by Design
Wenn sich Unternehmen mit dem Thema Cybersecurity auseinandersetzen, liegt der Fokus häufig auf dem Schutz des eigenen Unternehmens. Doch insbesondere für Hersteller von Gütern und Software sollte der Schutz vor Cyberangriffen auch bei den eigenen Produkten für die Nutzer mitgedacht werden. Und zwar im Sinne von Security by Design schon in der Entwicklungsphase. Damit können frühzeitig die Anzahl an Fehlern und Sicherheitslücken minimiert werden. Dies ist auch unter dem Blickwinkel verringerter Haftungsrisiken zu sehen. Künftig könnten Hersteller haftbar gemacht werden, wenn das Thema Sicherheit bei der Entwicklung der Produkte ausreichend berücksichtigt wurde. Natürlich können etwaige Lücken im Nachhinein immer noch mit Software-Updates geschlossen werden. Aber insbesondere bei langlebigen Maschinen müssen sich Hersteller die Frage stellen, wie lange solche Updates dann angeboten werden müssen oder unter wirtschaftlichen Aspekten angeboten werden können.

Weitere Maßnahmen
Weitere Cybersecurity-Maßnahmen bestehen in der Protokollierung von Zugriffen, Penetrationstests und Detection Systemen. Außerdem können Services des Internetproviders genutzt werden, die Verbindungen kappen, wenn der Datenverkehr zum Beispiel bei der DDoS-Attacke hochschnellt und zu Überlastungen führt. Wie in vielen Bereichen gilt auch bei Cybersecurity, dass Unternehmen – insbesondere kleine und mittelständische – nicht alles selbst machen müssen, sondern externe Dienstleister und Anbieter nutzen können. Am Ende sollten alle durchgeführten Maßnahmen zusammenpassen. Eine wenig durchdachte Zusammenstellung von Angeboten unterschiedlicher Hersteller kann dazu führen, dass die Produkte nicht harmonieren und schlecht zu warten sind, wodurch sich die Schutzwirkung verringert.

3.3 Organisation

Cybersecurity ist mehr als eine technologische Aufgabe. Auch Veränderungen und Maßnahmen in der Unternehmensorganisation helfen dabei, den Schutz vor Cyberangriffen zu erhöhen. Zu Beginn steht die Risikoanalyse. Folgende Fragen sind zu beantworten:

- Was gilt es zu schützen, um den Geschäftsbetrieb mindestens aufrecht erhalten zu können? Was sind die Kronjuwelen, die unter allen Umständen zu schützen sind, um die Existenz des Unternehmens zu sichern?
- Welche Daten existieren, wo werden diese vorgehalten und wofür sind sie erforderlich?
- Wer hat auf die Daten Zugriff? Welche Gruppen von internen und externen Personen?
- Wo sind die Daten gespeichert?
- Welche Cybersecurity-Fähigkeiten und -Ressourcen sind vorhanden?

Unternehmen können ein Risikoprofil erstellen mit Angriffswahrscheinlichkeit und potenziellen Schäden (Risiko-Verlust-Matrix). Aus einem Soll-Ist-Vergleich bei den Fähigkeiten können Unternehmen dann eine spezifische Cybersecurity To-do-Liste erstellen. Hier ist auch die Festlegung des maximal akzeptablen Risikos wichtig. Zudem sind die bereits erwähnten Abwägungen der Unternehmensziele zu berücksichtigen sowie die Wirtschaftlichkeit der Maßnahmen.

Bei diesen ersten Überlegungen ist insbesondere die Frage nach den Kronjuwelen nicht trivial. So könnten beispielsweise die IT-Abteilungen andere Bereiche als der Vertrieb für wichtig erachten. Sichert die Kundenliste die Existenz des Unternehmens? Oder ist es möglicherweise in einem Produktions- oder Logistikunternehmen die Nutzbarkeit des Hand-Scanners? Fallen die Scanner im Zuge eines Cyberangriffes aus, sind Just-in-Time-Abläufe essenziell gestört. Dies zeigt, dass eine Risiko-Abwägung sehr wichtig ist, gerade wenn ein umfassender Schutz vor Cyberangriffen Unternehmen finanziell überfordert.

Nach der Risikoanalyse kommen dann verschiedene organisatorische Maßnahmen in Betracht:

- durchdachtes IT-Rechte-Management
- nur zeitlimitierte Zugänge
- nur temporäre Administratorrechte
- festgelegte Zugriffsrechte für bestimmte Informationen
- Löschung der Rechte beim Ausscheiden eines Mitarbeiters
- Klassifizierung von Betriebsgeheimnissen
- klare Regeln für den Umgang mit schützenswerten Informationen – auch bei Auffinden von unbekannten USB-Sticks in einer Firma
- Regeln für den Umgang mit Social Media
- Melde-Mechanismen für Social Engineering
- Zwei-Faktor-Authentifikation
- regelmäßige Sicherheits-Audits
- Ausführung sensibler Prozesse (Überweisung, Änderung Bankverbindung) über mehrere Kanäle prüfen
- Ernstfall proben (analog zu Räumungsübung)
- Simulation und Stresstest, um Schwachstellen zu identifizieren: Was passiert beziehungsweise wird gemacht, wenn Anlage XY attackiert wird und ausfällt?

In regelmäßigen Abständen sollten Unternehmen außerdem prüfen, ob das Cybersecurity-Niveau noch ausreichend ist. Bei dieser Prüfung können auch Penetrationstest zum Einsatz kommen. Im Rahmen eines „White Hack“ beauftragt das Unternehmen beispielsweise echte Hacker, um das Unternehmen anzugreifen und so Schwachstellen zu identifizieren. Ähnlich funktionieren „Bug Bounds“. Hier loben Unternehmen eine Belohnung dafür aus, dass Hacker Schwachstellen bei Unternehmen melden. Die Deutsche Lufthansa AG belohnt für eine gemeldete Sicherheitslücke zum Beispiel mit 10.000 bis 1 Millionen Meilen ihres Bonusprogramms.

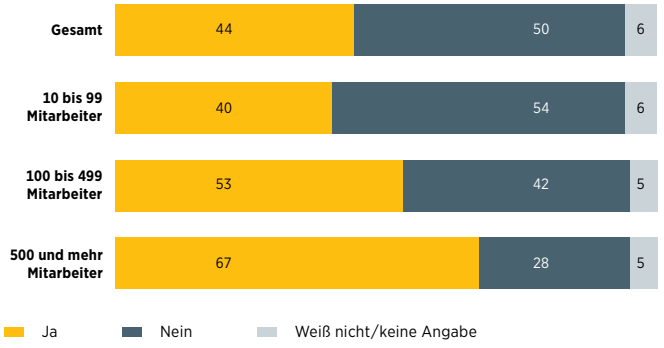
Notfallplan

Trotz der besten Vorkehrungen ist ein Cyberangriff immer möglich. Auch dafür müssen die Unternehmen vorbereitet sein und einen Notfallplan zur Verfügung haben. Laut BSI ist dies allerdings nur bei ungefähr jedem zweiten Unternehmen der Fall (58 Prozent). Dies ist das Ergebnis der Cybersicherheits-Umfrage 2017. Im Bereich der Industrie ist dieser Anteil etwas geringer, wie die Umfrage von Bitkom unter Industrieunternehmen zeigt **(siehe Grafik 5)**. Hier zeigt sich außerdem ganz klar, dass die Wahrscheinlichkeit für das Vorliegen eines Notfallplans mit der Unternehmensgröße ansteigt.

Grundsätzlich geht es bei einem Notfallplan darum,

- kritische Funktionen aufrecht zu erhalten und
- nach einem Angriff wieder schnell zur Normalität zurückzukehren.

Grafik 5: Existiert ein Notfallplan für Cyberangriffe?
Anteil der befragten Industrieunternehmen in %



Quelle: Bitkom Research

Der Plan umfasst eine Liste, wer im Ernstfall zu kontaktieren ist. Außerdem sollte in einem Kommunikationsplan geregelt werden, wer im Angriffsfall welche Informationen veröffentlichen darf. Bei der Kommunikation sollten die Unternehmen auch an Kunden, Investoren und Kreditgeber denken. In einem Notfallplan sind auch spezielle Handlungsvollmachten für kurzfristige Anschaffungen im Krisenfall zu regeln. Ferner sollten Anweisungen enthalten sein, wie die IT-Systeme bei einer Attacke heruntergefahren werden und anschließend wieder hochzufahren sind. Dabei ist allerdings zu bedenken, dass ein Herunterfahren nicht immer sinnvoll ist, denn dabei werden bestimmt Schadprogramme und Spuren, die nur im Speicher liegen, gelöscht. Möchte das Unternehmen anschließend Ermittlungen durchführen, ist dies kontraproduktiv. Insofern ist es besser das System bei einem Angriff nur vom Netz zu trennen, aber nicht abzuschalten. Unternehmen können in diesem Fall auch sofort Berater und Experten zur Unterstützung holen.

Der Plan sollte in analoger Form vorliegen. Im Angriffsfall gibt es unter Umständen kein Zugriff auf die Computer und die Telefonanlage. Auch sind eventuell nicht alle Programme (z. B. Buchhaltung, Personal) über Smartphone nutzbar, wenn der Server ausgefallen ist. Hier sollten sich Unternehmen über eine Alternative Gedanken machen. Messenger wie WhatsApp können zwar für die Kommunikation genutzt werden, sind aber ungeeignet für die Übermittlung kritischer beziehungsweise vertraulicher Daten.

Vor dem Angriff muss außerdem jeder Mitarbeiter seine Rolle im Notfall kennen, notwendige externe Partner müssen identifiziert sein, eventuell besteht bereits ein Rahmenvertrag für Unterstützung im Krisenfall, und es sollte gerade bei kritischer Infrastruktur ein internes „Krisenteam“ rund um die Uhr in Bereitschaft sein. Denn Geschwindigkeit ist essenziell im Ernstfall.

Neben einem Plan für den Fall des Cyberangriffs benötigen Unternehmen auch einen Plan für die Zeit danach, um beispielsweise die beschädigte Reputation wiederherzustellen. Dazu gehört es auch zu prüfen, ob die Angreifer wirklich keinen Zugriff mehr auf die Systeme haben. Dies sollte dann kommuniziert werden. Für künftige Angriffe sollten auch die Fehler und Schwächen identifiziert werden, um daraus zu lernen.

Kurz gefasst:

- Aktuelle Telefon- und Kontaktlisten sowie Organigramme sollten offline auf einem USB-Stick und in Papierform verfügbar sein.

- Es sollte einen Online Banking Zugang für Notfälle geben, der auch außerhalb der Firma an einem normalen Rechner funktioniert.

- Haben Sie einen Bitcoin-Account für Ihre Firma?
  Das erspart Zeit, sollten Sie doch zahlen müssen, denn Sie durchlaufen auch hier Kontoeröffnungsprozesse (KYC).

- Regelung der Notfallkommunikation – wie sieht diese ohne Firmentelefone und E-Mail aus?
  (Achtung: Der Angreifer befindet sich ggf. noch im System und verfolgt die Kommunikation mit!)

- Back-up- und Recovery-Pläne
  (Online-Back-ups und Offside-Back-ups).

- Regelung, wer wird wann eingeschaltet und wer hat die Berechtigung dazu: Polizei, Anwälte, Banken, Versicherung.

- Festlegung eines Datenschutzbeauftragten im Unternehmen.

- Identifikation der notwendigen Meldungen und Meldefristen beim Abhandenkommen von Daten (DSGVO), sodass Strafzahlungen vermieden werden.

Chief Information Security Officer

Wie bei der Digitalisierung sollten auch bei der Cybersecurity klare personelle Verantwortlichkeiten festgelegt werden. In einigen Unternehmen ist dafür ein Chief Information Security Officer (CISO) zuständig. Er ist der Key Enabler für die Digitalisierung des Unternehmens, da Cybersecurity die Grundlage der digitalen Transformation ist. Der CISO sollte neben technologischem auch über betriebswirtschaftliches Knowhow verfügen, um beispielsweise die wirtschaftlich relevantesten Bereiche für den Schutz zu identifizieren. Da außerdem das Thema Cybersecurity in allen Geschäftsbereichen und -prozessen mitgedacht werden sollte, erfordert dies vom CISO einen Kontakt und Austausch mit allen Unternehmensbereichen.

Die Position eines CISO ist für größere Mittelständler eine bedenkenswerte Option, entbindet aber die Unternehmensführung nicht von ihrer Verantwortung. Zum einen ist Cybersecurity immer ein Haftungsthema, sodass grob fahrlässige Versäumnisse beim Schutz vor Cyberangriffen unter Umständen ein Fall für die Managerhaftung (D&O) sind. Zum Zweiten ist die erste Führungsebene Vorbild für die Belegschaft. Schließlich hat häufig nur die Geschäftsführung die nötige Budgetverantwortung, um die notwendigen Finanzmittel für Cybersecurity freizugeben.

3.4 Mitarbeiter

Ebenso wichtig wie die Sensibilität der Führungskräfte für das Thema Cybersecurity ist die Aufmerksamkeit der Belegschaft. Viele Angriffe haben ihren Ursprung in fahrlässigem oder falschem Handeln aus Unwissenheit. Der theoretisch beste technologische Schutz ist lückenhaft, wenn die Mitarbeiter nicht geschult (Knowhow), beziehungsweise dafür sensibilisiert (Awareness) sind – wenn sie zum Beispiel einen verdächtigen Anhang oder Link öffnen oder ihren Computer beim Verlassen des Büros nicht sperren. Es ist sinnlos, wenn die Technologie nur als ein Punkt auf einer To-do-Liste abgehackt wird, sie aber eigentlich nicht vorhanden ist, da sie kein Mitarbeiter bedienen kann oder will.

Insofern ist es wichtig Cybersecurity-Awareness und Cybersecurity-Knowhow zu schaffen, um mit den Mitarbeitern eine Human Firewall zu errichten. Um bei ihren Mitarbeitern Cybersecurity-Fähigkeiten, -Wissen und -Awareness aufzubauen, können Unternehmen unter anderem (Web-)Schulungen, Live-Hacking-Demonstrationen oder (Gruppen-)Workshops nutzen. Diese sollten für unterschiedliche Gruppen in einem gesonderten Unternehmen angeboten werden. Für Vertrieb, Technik, Geschäftsführung oder auch Assistenz der Geschäftsführung sind mitunter verschiedene Bereiche der Cybersecurity relevant. So müssen auch die Fach- und Führungskräfte dazu befähigt werden, Cybersecurity in ihren Bereichen zu etablieren.

Schulungen können aber nur ein erster Schritt sein. Um die Mitarbeiter auf die Cyberrisiken vorzubereiten, sollten sie aktiv und kontinuierlich in die Cybersecurity-Strategie einbezogen werden. Dabei sollte ihnen vermittelt werden, dass sie durch ihr Handeln einen wichtigen Beitrag zum Schutz des Unternehmens liefern. Mitarbeiter sollten daher ermutigt werden, verdächtige Ereignisse zu melden – auch auf die Gefahr hin, einen Fehlalarm auszulösen. Denn oftmals dauert es zu lange, einen Angriff zu erkennen. Laut McKinsey benötigen Unternehmen im Schnitt 99 Tage, bis ein Angriff identifiziert wird. Das BSI setzt für diesen Zeitraum sogar 200 bis 400 Tage an. Das Unternehmen Bosch hat daher eine „Helden-Kampagne“ mit Imagevideo initiiert, wonach jeder Mitarbeiter ein „Alltagsheld“ sein kann, der das Unternehmen schützen kann. Die Unternehmensleitung unterstreicht damit die wichtige Bedeutung des Themas Cybersecurity.

Richtiges Handeln der Mitarbeiter bedeutet auch einen bewussten Umgang mit sozialen Netzwerken, Vorsicht bei Kontaktanfragen von unbekannten Personen sowie E-Mail-Anhängen und -Links. Gleiches gilt für den Umgang mit mobilen Endgeräten. Unternehmen können hier vorgeben, dass Apps – wenn überhaupt – nur aus offiziellen Stores heruntergeladen werden. Ferner sind Vorgaben oder Verbote für die dienstliche Nutzung privater Geräte vorstellbar.

Social Engineering
Im Mittelpunkt steht der Mitarbeiter auch beim Social Engineering **(siehe Kapitel 2.3.6)**. Um das Schutzniveau zu steigern, sollten die Mitarbeiter folgende Regeln beachten:

- Keine/möglichst wenige (persönliche) Informationen über das eigene Leben an Fremde oder über digitale Kanäle weitergeben.
- Informationen nie fahrlässig preisgeben (zum Beispiel Teilnahme an Gewinnspielen).
- Für Passwörter (oder Sicherheitsfragen) keine persönlichen Informationen, Hobbies, Freunde ... verwenden.
- Für Sicherheitsfragen, bei denen es häufig nur eine begrenzte Anzahl an Kategorien (zum Beispiel Geburtsname der Mutter) gibt – Informationen, die zumeist leicht zu finden sind – Zufallsantworten bilden.
- Keine Passwörter mehrfach verwenden, da mit einem erfolgreichen Hack die Angreifer Zugriff auf alle Konten haben.
- Immer skeptisch sein. So würden seriöse Institutionen nie nach vertraulichen Informationen fragen. Bei Zweifel einfach zurückrufen.
- Bei einem Verdacht auf einen CEO-Fraud, sollten Mitarbeiter versuchen, die Identität des Absenders mit den ihnen zur Verfügung stehenden Mittel zu überprüfen (zum Beispiel Passt die E-Mail-Adresse (mit Endung)?).

Inwieweit die Mitarbeiter schon ausreichend für das Thema sensibilisiert sind, sollten Unternehmen anschließend in regelmäßigen Abständen mittels (Social-)Penetrations-Tests, Übungen und Simulationen überprüfen. Dies ist auch ein Bestandteil im „Human-Firewall-Projekt“ von Innogy. Hier werden Phishing-E-Mails zu Testzwecken an die Mitarbeiter geschickt. Ferner gehören zum Projekt Lernvideos, Schulungen, Live-Hacks, eine Roadshow im Ausland sowie „War-Gaming-Szenarios“ in Kleingruppen im unternehmenseigenen Cybersecurity-Trainingszentrum.

3.5 Cyber-Versicherung

Eine Möglichkeit für die Unternehmensführung, mit dem Thema Haftung bei Cyberangriffen umzugehen und einen Teil des Risikos abzudecken, stellen spezielle Cyber-Versicherungen dar. Diese Versicherungsprodukte, die Schäden in Folge von Cyberangriffen abdecken, gewinnen an Bedeutung; der Markt in Deutschland wächst langsam und zögerlich, aber stetig.

Bevor Unternehmen sich allerdings für eine Cyber-Versicherung entscheiden, sollten sie die Wirtschaftlichkeit genau prüfen. So sind zum Teil umfangreiche Vorgaben und Vorprüfungen nötig, um die Höhe der Prämie zu beschränken. Vor diesem Hintergrund sollten Unternehmen auch überlegen, ob es nicht sinnvoller ist, die Finanzmittel direkt in Cybersecurity-Maßnahmen zu investieren. Denn eine Versicherung entbindet nicht von den Bemühungen, das Unternehmen vor Cyberangriffen zu schützen, da sie angesichts einer Deckungsobergrenze unter Umständen nur einen Teil des Schadens abdeckt. Ein Angriff mit Ransomware im Sommer 2017 verursachte beispielsweise bei Merck & Co. in den USA laut Schätzungen von Experten einen Schaden im Milliardenbereich, die Versicherungen mussten aber nur für rund 275 Millionen US-Dollar aufkommen.

Bei Munich Re, einem Anbieter von Cyber-Versicherungen in Kooperation mit dem Spezialversicherer Beazley, beträgt die Schadensdeckung beispielsweise maximal 100 Millionen US-Dollar. Der Versicherer schließt allerdings nicht aus, dass die Obergrenze in Zukunft noch angehoben wird, wenn man mehr über die Risiken gelernt hat.

Ein weiterer Anbieter ist Euler Hermes. Deren Vertrauensschadensversicherung hat eine Deckungsobergrenze von 100 Millionen Euro, die aber für einzelne Vorfälle auch geringer sein kann (zum Beispiel bei CEO-Fraud: maximal 5 Millionen Euro). Die Versicherung von Euler Hermes deckt (Vermögens-)Schäden bei gehackten Cloud-Speichern, Datendiebstahl, Identitätsdiebstahl (CEO-Fraud), Ersatzinvestitionen in Hard- und Software für die Fortführung des Geschäftsbetriebs, Geheimnisverrat sowie Betrug, Veruntreuung und Diebstahl durch Mitarbeiter oder Dritte.

Neben dem eigentlichen Versicherungsprodukt bieten Versicherer – so auch Munich Re – noch weitere Dienstleistungen im Bereich Cybersecurity an. Dazu zählen Unterstützung bei Prävention und Umgang mit Cyberangriffen, bei der Schulung und Sensibilisierung der Mitarbeiter, bei der Wiederherstellung der Daten und des Systems nach einem Angriff sowie bei der Krisenkommunikation.

3.6 Gesetzliche Vorgaben

Die Ausgestaltung der Cybersecurity unterliegt nicht allein der Entscheidung des Unternehmens, es gibt dazu vielmehr gesetzliche Vorgaben. Allerdings sind die Unternehmen bei der Bewältigung der Herausforderung Cybersecurity nicht auf sich allein gestellt sind. So gibt es diverse Unterstützungsmöglichkeiten, von denen im Folgenden nur einige wenige skizziert werden.

IT-Sicherheitsgesetz
Gemäß dem IT-Sicherheitsgesetz müssen bestimmte Unternehmen Mindeststandards bei Cybersecurity einhalten und relevante Angriffe melden. Dies gilt für Unternehmen aus Bereichen der kritischen Infrastruktur wie Energieversorgung, Telekommunikation, Internetversorgung (KRITIS) sowie für größere Unternehmen aus Gesundheit und Transport. Für diese Unternehmen bedeutet das Gesetz, dass Cybersecurity für sie aufgrund von Berichten, Nachweisen, Abstimmungen und Meldungen mit einem größeren Aufwand verbunden ist. Gesetzesverstöße sind mit Strafen verbunden.

Aktuell arbeitet die Bundesregierung an einer Weiterentwicklung des Gesetzes (IT-Sicherheitsgesetz 2.0). So ist geplant, den Anwendungsbereich des Gesetzes auf den Mittelstand auszuweiten.

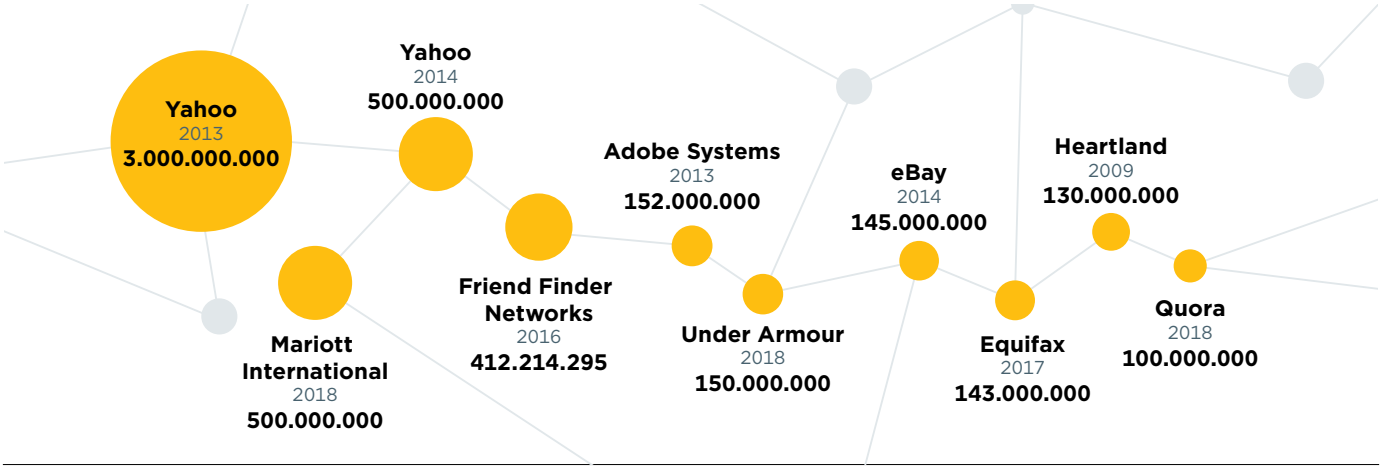
Datenschutzgrundverordnung (DSGVO)
Auch die DSGVO stellt Anforderungen an den Schutz vor Cyberangriffen, insbesondere hinsichtlich des Problems Datendiebstahl. Gemäß der DSVGO müssen Unternehmen den Eigentümern der persönlichen Daten immer transparent aufzeigen können, was mit den personenbezogenen Daten passiert. Bei einer Datenpanne (zum Beispiel Datendiebstahl, unbefugter Zugriff auf persönlich Daten, Verlust eines USB-Device mit Daten) müssen Unternehmen die Aufsichtsbehörden sowie die Nutzer innerhalb von 72 Stunden informieren. Außerdem haben die Nutzer auch Anspruch auf eine Unterstützung der Unternehmen bei der Wiederherstellung des Schutzes ihrer Daten.

Die Informationspflicht umfasst auch Sicherheitsverstöße wie Ransomware oder eine (versehentliche) Löschung der Daten, sprich die (temporäre) Nichtverfügbarkeit der persönlichen Daten.

Für diese Fälle sollten die Unternehmen neben dem allgemeinen Notfallplan auch immer einen „Data Breach Response Plan“ parat haben. Verstöße gegen die DSGVO werden mit Bußgeldern von bis zu 20 Millionen Euro beziehungsweise 4 Prozent des weltweiten Umsatzes geahndet. Wenn Unternehmen beweisen können, dass personenbezogene Daten von Unbefugten nicht gelesen werden konnten (zum Beispiel wegen einer Verschlüsselung) können die Bußgelder reduziert werden.

Zu den Bußgeldern kommt für die Unternehmen dann noch der Imageschaden.

Grafik 6: Bedeutende Datendiebstähle, Anzahl gestohlener Datensätze bei einem Vorfall im jeweiligen Jahr



Quellen: BBC, cNet, Guardian, New York Times, Reuters, Washington Post, ZDNet

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Eine erste Anlaufstelle für Unternehmen, um Unterstützung in Sachen Cybersecurity zu erhalten, ist das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das BSI bietet Unternehmen Informations- und Beratungsangebote und vermittelt bei Bedarf weitere Unterstützung.

2012 hat das BSI außerdem die Allianz für Cybersicherheit ins Leben gerufen – mit dem Ziel, die Widerstandsfähigkeit des Standorts Deutschland gegenüber Cyberangriffen zu stärken. Den teilnehmenden Unternehmen und Institutionen stehen verschiedene Angebote sowie ein Informationspool zur Verfügung. Sie erhalten außerdem automatisierte Meldungen über Cyberangriffe.

Ferner steigert das BSI die Widerstandsfähigkeit des Standorts Deutschland gegenüber Cyberangriffen auch mittels der Festlegung von Sicherheitsstandards. Dazu zählt der BSI Cloud-Standard „C5“, der von den meisten globalen Cloud-Anbietern (zum Beispiel Microsoft, IBM, Amazon, Alibaba, Google) anerkannt und erfüllt wird. Unternehmen erhalten dadurch Gewissheit, dass die Anbieter bestimmte Sicherheitsstandards einhalten.

Ein weiteres Unterstützungsangebot ist die MISP-Datenbank (Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing). Es ist eine der größten Datenbank für die Malware-Analyse.

Des Weiteren gibt es das German Competence Centre against Cyber Crime. Dies ist ein Verein mit Mitgliedern aus dem Bereich der Finanzwirtschaft (zum Beispiel Commerzbank, HypoVereinsbank, Schufa Holding, Diebold Nixdorf, KfW), der auch mit dem BSI und dem Bundeskriminalamt kooperiert. Der Verein sieht sich als praktischer Unterstützer, Vorreiter- und Vordenker, der aus dem Austausch über Phänomene der Cyberkriminalität heraus Hilfestellungen, Methoden und Empfehlungen zur Prävention gegen Cyberkriminalität entwickelt und so seine Mitglieder unterstützt.

Daneben gibt es auch die Charta Cybersicherheit, die Anfang 2018 auf Initiative von Siemens erstellt wurde. Mitunterzeichner sind unter anderem Airbus, Allianz, IBM, Daimler und die Deutsche Telekom. In dieser Charta werden Prinzipien beziehungsweise Handlungsfelder für Politik und Wirtschaft aufgelistet, unter anderem:

- Eine Verantwortung für Cybersecurity muss festgelegt und in der Unternehmensführung angesiedelt werden.
- In der digitalen Lieferkette muss für Verschlüsselung, Identitätsmanagement und kontinuierlichen Schutz gesorgt werden.
- Cybersecurity als Werkseinstellung: Unternehmen sollten Cybersecurity von Beginn an bei der Entwicklung mitdenken.
- Bedürfnisse der Nutzer in den Mittelpunkt stellen: Produkte und Services passend zu den Sicherheitsanforderungen der Kunden entwickeln.
- Innovation und Co-Creation: Zusammenarbeit innerhalb der Branchen als auch zwischen Wirtschaft und Staat beim Thema Cybersecurity.
- Cybersecurity als fester Teil in der Ausbildung: (Künftige) MA von Anfang an schulen und sensibilisieren.
- Kritische Infrastruktur und IoT-Lösungen zertifizieren.
- Transparenz und Reaktionskraft steigern, beispielsweise durch eine Zusammenarbeit der Unternehmen in einem Cybersecurity-Netzwerk zum Austausch von Informationen.
- Regulatorischer Rahmen: Standards bei Cybersecurity schaffen und Cybersecurity in internationale Verträge aufnehmen.
- Gemeinsame Initiativen von Unternehmen als auch Wirtschaft und Politik vorantreiben.

4. Was tun, wenn die eigene Firma Opfer geworden ist?

Grundsätzlich sollten Sie sich über diese Frage im Vorfeld Gedanken machen und eine Notfallplanung und Krisenkommunikation erarbeiten. Denn in jeder Firma bedarf es anderer Abstimmungswege und Genehmigungen, was ohne Vorbereitung sehr viel wertvolle Zeit kosten kann. So hat Ihre Geschäftsleitung als auch Ihr Datenschutzbeauftragter naturgemäß eine genaue Vorstellung davon, was wann in welcher Reihenfolge passieren soll. Nur sollten Sie es vorher niederschreiben, denn es nimmt der Situation sehr viel Chaos-Potenzial und Hysterie, wenn jeder weiß, was von ihm in der Stunde der Wahrheit erwartet wird. Die Notfallpläne sollten in jedem Fall offline verfügbar sein – auf USB-Sticks und auf jeden Fall auch in Papierform! Beachten Sie bei der Überlegung zu Kommunikationswegen, dass der Angreifer sich noch im System befinden kann und daher gegebenenfalls Zugriff auf die gesamte Kommunikation hat.

Informieren Sie Ihre Bank
Je nachdem um welche Art des Angriffs es geht, ist bei einer möglicherweise in Betracht zu ziehenden Überweisung zur Schadensbegrenzung die Bank der erste Ansprechpartner. Von ihr können noch Rückrufe veranlasst werden und es kann vielleicht noch eine Betragssicherung oder Kontosperre des Zielkontos erzielt werden. Auch bei einem Krypto-Trojaner sollte die Bank mit als Erstes informiert werden, denn es gibt auch die Kombination verschiedener Angriffsszenarien. Dabei kann es zum Beispiel noch vor der Verschlüsselung zur Autorisierung von Zahlungen gekommen sein, die sie durch das gestiftete Chaos nicht entdecken sollen.

Anzeige bei der Zentralen Ansprechstelle Cybercrime des zuständigen Landeskriminalamts
Bei einem Vorfall sollte immer nach vorheriger interner Abstimmung die Polizei eingeschaltet werden. Hier gibt es in jedem Bundesland Spezialeinheiten ausschließlich für Firmen (Zentrale Ansprechstelle Cybercrime), die einen wertvollen Dienst liefern können und ihrerseits wiederum über beste Kontakte verfügen, um die Situation zu meistern. Die Rufnummer des ZAC beim für Sie zuständigen Landeskriminalamt sollten Sie also auch in Ihren Offline-Kontakten führen.

Kommunikation mit weiteren wichtigen Kontakten
Im nächsten Schritt werden Sie an Ihre Anwälte denken, an Versicherungen, an Ihre Geschäftspartner und an Ihre Außenkommunikation. Auch hier muss es einen Plan für eine Krisenkommunikation geben, denn je nach Art des Angriffs kann es sein, dass Sie der Öffentlichkeit das Problem gar nicht kontrolliert bis zu einer Kommunikation vorenthalten können. Sollte es zu einer betrügerischen Überweisung in ein anderes Land gekommen sein, ist es in der Regel unabdingbar, dass Sie einen Anwalt mit einer Lizenz zur Vertretung im Zielland engagieren. Hier können Sie neben Ihrer Bank auch die Außenhandelskammer der DIHK unterstützen. Denken Sie an Meldepflichten und gesetzliche Vorgaben, wie mit Datenverlust umzugehen ist.

Unternehmenskommunikation
In der Unternehmenskommunikation ist es wichtig, dass jeder die Information bekommt, die er für die Bewältigung des Problems entsprechend seiner Aufgaben und Kompetenzen benötigt. Meist entsteht in Unternehmen ein noch höherer Schaden durch falsche oder unterlassene Kommunikation. Dies gilt nicht nur für unternehmensinterne, sondern auch für die externe Kommunikation. Einige Firmen haben eine Präsenz in den Sozialen Medien, sind sich aber nicht bewusst, wie sich das in einer kommunikativ schlecht gelösten Krisensituation gegen ihre Firma und ihre Marke richten kann. Bis hin dazu, dass hier bekanntgegebene Einzelheiten, Reaktionen oder fehlende Stellungnahmen wie eine Veröffentlichung oder ein Statement gewertet werden können – und damit auch einen Regulator auf den Plan rufen können. Es ist also genau abzuwägen, welche Information man wem weitergibt – auch um einen ungewollten Impact auf die Bewertung und Reputation des eigenen Unternehmens nicht noch zusätzlich zu forcieren.

Soziale Verantwortung für das Opfer

Im Rahmen der Aufklärung des Betrugs- oder Cybercrimevorfalls, werden Sie den Zeitpunkt der Infektion feststellen. Sie werden die erste Mail finden, den Anruf und auch, wie Informationen an den Täter gelangt sind. Sie werden Betrugs-E-Mails finden, auf die Ihre Mitarbeiter hereingefallen sind und es wird – das ist nur allzu menschlich – im Nachgang alles ganz einleuchtend Betrug sein. Zuweilen kommen auch Äußerungen von Unverständnis über die Reaktionen und das Eingehen auf eine vom Ende aus gesehen ganz offensichtlich gefälschte Kommunikation. Dabei verrutscht das Bild etwas und der Mitarbeiter, der bei sachlicher Betrachtung Opfer ist, wird in der Firma zuweilen zum Täter stilisiert. Diese Art von schlechtem Krisenmanagement, die auch schon von Anwaltskanzleien in Artikeln forciert wurde, kann sehr gefährliche Auswirkungen haben, die in der Vergangenheit auch schon einmal bis zum Suizid des betroffenen Mitarbeiters reichten. Opfer brauchen auch eine Betreuung als Opfer. Sie müssen psychologisch abgesichert werden. Dafür gibt es Organisationen, die dies leisten können. Es empfiehlt sich, von der betroffenen Person ein genaues Gedächtnisprotokoll anfertigen zu lassen, um spätere Bewusstseinsverfälschungen auszuschließen. Aus Unternehmersicht ist die zielführendere Frage, ob die Firma als Arbeitgeber alles geleistet hat, um solch einen Betrug zu verhindern. Es sollten Schwachstellen analysiert und Schritte unternommen werden, die dies in der Zukunft verhindern.

Ziehen Sie einen IT-Forensiker hinzu

Bei einem Verschlüsselungstrojaner kann es der bessere Weg sein, externen Rat hinzuziehen – auch wenn Sie selbst über eine gute IT-Abteilung verfügen. Hierfür ist es wichtig, dass diese Firma auf dem Gebiet der IT-Forensik Profi ist. Denn bei einem halbherzigen Versuch einer Wiederherstellung kann es auch passieren, dass noch größerer Schaden angerichtet wird. Ein Recovery muss geplant sein und es muss im Vorfeld klar sein, dass eine Rücksicherung auch gelingen wird. Ist dies nicht klar, oder haben Sie die Vermutung, dass Ihnen danach noch immer existenziell notwendige Daten fehlen könnten, sollten Sie die Finger von der Technik lassen, bis das geklärt ist. Nach einer versuchten Wiederherstellung kann es sein, dass auch der korrekte Key für die Entschlüsselung nicht mehr funktioniert, sollten Sie sich später doch für die Zahlung einer Lösegeldforderung entscheiden.

5. Nützliche Adressen/ Nützliches Material

Informationen des Bundesamts für Sicherheit in der Informationstechnik (BSI)
Postfach 200363
53133 Bonn

Telefon: +49 228 99 9582-0
Telefax: 0228 99 9582-5400

E-Mail: bsi@bsi.bund.de
De-Mail: poststelle@bsi-bund.de-mail.de
https://www.bsi.bund.de/DE/Home/home_node.html

Polizei – Zentrale Ansprechstelle Cybercrime des Landeskriminalamtes (ZAC)
https://www.polizei.de/Polizei/DE/Einrichtungen/
ZAC/zac_node.html

Commerzbank AG, Fraud Prevention Team
Bitte informieren Sie uns immer mit Ihrem
Kundenberater in CC.

Telefon: +49 69 136 82777
E-Mail: msb.sicherheit@commerzbank.com

Zwei Beispiele für IT-Spezialisten in der Prävention und Forensik:

G Data Advanced Analytics GmbH
G Data Campus
Königsallee 178b
44799 Bochum

http://www.gdata-advancedanalytics.de

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

http://www.to.com

Nützliche Links zum Thema E-Mail-Sicherheit und Social-Engineering:
Clip von Secuso.org: https://youtu.be/4xlU1lPJs_4

Clip von Fusion.net: https://youtu.be/lc7scxvKQOo

6. Checkliste Cybersecurity

Zum Schluss sollten Sie diese Fragen für Ihr Unternehmen beantworten:

- Sind wir uns der Bedrohung bewusst?
- Haben wir alle wichtigen Unternehmensdaten, -prozesse und -systeme, die existenzsichernden Kronjuwelen des Unternehmens identifiziert?
- Sind die Schwachstellen des Unternehmens bekannt?
- Kennen wir die potenziellen Ziele von Angreifern im Unternehmen?
- Kennen wir die potenziellen Auswirkungen von Angriffen auf unser Unternehmen?
- Ist das Unternehmen ausreichend vor Angriffen geschützt?
- Sind im Unternehmen die Instrumente und Konzepte für Cybersecurity bekannt?
- Haben wir die richtige Strategie, Pläne, Teams für eine wirkungsvolle Cybersecurity?
- Haben wir einen Notfallplan für den Ernstfall eines Cyberangriffs und steht dieser in aktuellster Fassung, jederzeit verfügbar – auch offline – allen relevanten Personen zur Verfügung?
- Stehen alternative Kommunikationskanäle zur Verfügung, sofern der Angreifer in den Systemen mitlesen kann?
- Proben wir den Ernstfall eines Cyberangriffs regelmäßig?
- Gibt es klare Verantwortlichkeiten für die Cybersecurity im Unternehmen?
- Sind die Mitarbeiter sensibilisiert für die verschiedenen Bedrohungen der Cyberkriminalität?
- Werden regelmäßig Software-Updates durchgeführt?
- Werden regelmäßig Back-ups erstellt?
- Wird bei der Entwicklung neuer Produkte und Dienstleistungen das Thema Sicherheit von Anfang an mitgedacht und gegebenenfalls extern begleitet?
- Verstehen wir Cybersecurity als fortwährenden Prozess, der nie abgeschlossen ist und kontinuierlich weiterentwickelt werden muss?

Commerzbank Research Für die Erstellung dieser Ausarbeitung ist das Segment Firmenkunden der Commerzbank AG, Frankfurt am Main, verantwortlich.

Die Verfasser bestätigen, dass die in diesem Dokument geäußerten Einschätzungen ihre eigenen Einschätzungen genau wiedergeben und kein Zusammenhang zwischen ihrer Dotierung – weder direkt noch indirekt noch teilweise – und den jeweiligen, in diesem Dokument enthaltenen Empfehlungen oder Einschätzungen bestand, besteht oder bestehen wird. Der (bzw. die) in dieser Ausarbeitung genannte(n) Analyst(en) ist (sind) nicht bei der FINRA als Research-Analysten registriert/qualifiziert. Solche Research-Analysten sind möglicherweise keine assoziierten Personen der Commerz Markets LLC und unterliegen daher möglicherweise nicht den Einschränkungen der FINRA Rule 2241 in Bezug auf die Kommunikation mit einem betroffenen Unternehmen, öffentliche Auftritte und den Handel mit Wertpapieren im Bestand eines Analysten.

Disclaimer Dieses Dokument dient ausschließlich zu Informationszwecken und berücksichtigt nicht die besonderen Umstände des Empfängers. Es stellt keine Anlageberatung dar. Die Inhalte dieses Dokuments sind nicht als Angebot oder Aufforderung zum Kauf oder Verkauf von Wertpapieren oder irgendeiner anderen Handlung beabsichtigt und dienen nicht als Grundlage oder Teil eines Vertrages. Anleger sollten sich unabhängig und professionell beraten lassen und ihre eigenen Schlüsse im Hinblick auf die Eignung der Transaktion einschließlich ihrer wirtschaftlichen Vorteilhaftigkeit und Risiken sowie ihrer Auswirkungen auf rechtliche und regulatorische Aspekte sowie Bonität, Rechnungslegung und steuerliche Aspekte ziehen.

Die in diesem Dokument enthaltenen Informationen sind öffentliche Daten und stammen aus Quellen, die von der Commerzbank als zuverlässig und korrekt erachtet werden. Die Commerzbank übernimmt keine Garantie oder Gewährleistung im Hinblick auf Richtigkeit, Genauigkeit, Vollständigkeit oder Eignung für einen bestimmten Zweck. Die Commerzbank hat keine unabhängige Überprüfung oder Due Diligence öffentlich verfügbarer Informationen im Hinblick auf einen unverbundenen Referenzwert oder -index durchgeführt. Alle Meinungsaussagen oder Einschätzungen geben die aktuelle Einschätzung des Verfassers bzw. der Verfasser zum Zeitpunkt der Veröffentlichung wieder und können sich ohne vorherige Ankündigung ändern. Die hierin zum Ausdruck gebrachten Meinungen spiegeln nicht zwangsläufig die Meinungen der Commerzbank wider. Die Commerzbank ist nicht dazu verpflichtet, dieses Dokument zu aktualisieren, abzuändern oder zu ergänzen oder deren Empfänger auf andere Weise zu informieren, wenn sich ein in diesem Dokument genannter Umstand oder eine darin enthaltene Stellungnahme, Schätzung oder Prognose ändert oder unzutreffend wird.

Diese Ausarbeitung kann Handelsideen enthalten, im Rahmen derer die Commerzbank mit Kunden oder anderen Geschäftspartnern in solchen Finanzinstrumenten handeln darf. Die hier genannten Kurse (mit Ausnahme der als historisch gekennzeichneten) sind nur Indikationen und stellen keine festen Notierungen in Bezug auf Volumen oder Kurs dar. Die in der Vergangenheit gezeigte Kursentwicklung von Finanzinstrumenten erlaubt keine verlässliche Aussage über deren zukünftigen Verlauf. Eine Gewähr für den zukünftigen Kurs, Wert oder Ertrag eines in diesem Dokument genannten Finanzinstruments oder dessen Emittenten kann daher nicht übernommen werden. Es besteht die Möglichkeit, dass Prognosen oder Kursziele für die in diesem Dokument genannten Unternehmen bzw. Wertpapiere aufgrund verschiedener Risikofaktoren nicht erreicht werden. Hierzu zählen in unbegrenztem Maße Marktvolatilität, Branchenvolatilität, Unternehmensentscheidungen, Nichtverfügbarkeit vollständiger und akkurater Informationen und/oder die Tatsache, dass sich die von der Commerzbank oder anderen Quellen getroffenen und diesem Dokument zugrunde liegenden Annahmen als nicht zutreffend erweisen.

Die Commerzbank und/oder ihre verbundenen Unternehmen dürfen als Market Maker in den(m) Instrument(en) oder den entsprechenden Derivaten handeln, die in unseren Research-Studien genannt sind. Mitarbeiter der Commerzbank oder ihrer verbundenen Unternehmen dürfen unseren Kunden und Geschäftseinheiten gegenüber mündlich oder schriftlich Kommentare abgeben, die von den in dieser Studie geäußerten Meinungen abweichen. Die Commerzbank darf Investmentbanking-Dienstleistungen für in dieser Studie genannte Emittenten ausführen oder anbieten.

Weder die Commerzbank noch ihre Geschäftsleitungsorgane, leitenden Angestellten oder Mitarbeiter übernehmen die Haftung für Schäden, die ggf. aus der Verwendung dieses Dokuments, seines Inhalts oder in sonstiger Weise entstehen.

Die Aufnahme von Hyperlinks zu den Websites von Organisationen, die in diesem Dokument erwähnt werden, impliziert keineswegs eine Zustimmung, Empfehlung oder Billigung der Informationen der Websites bzw. der von dort aus zugänglichen Informationen durch die Commerzbank. Die Commerzbank übernimmt keine Verantwortung für den Inhalt dieser Websites oder von dort aus zugänglichen Informationen oder für eventuelle Folgen aus der Verwendung dieser Inhalte oder Informationen.

Dieses Dokument ist nur zur Verwendung durch den Empfänger bestimmt. Es darf weder in Auszügen noch als Ganzes ohne vorherige schriftliche Genehmigung der Commerzbank auf irgendeine Weise verändert, vervielfältigt, verbreitet, veröffentlicht oder an andere Personen weitergegeben werden. Die Art und Weise, wie dieses Produkt vertrieben wird, kann in bestimmten Ländern, einschließlich der USA, weiteren gesetzlichen Beschränkungen unterliegen. Personen, in deren Besitz dieses Dokument gelangt, sind verpflichtet, sich diesbezüglich zu informieren und solche Einschränkungen zu beachten. Mit Annahme dieses Dokuments stimmt der Empfänger der Verbindlichkeit der vorstehenden Bestimmungen zu.

Zusätzliche Informationen für Kunden in folgenden Ländern:
Deutschland: Die Commerzbank AG ist im Handelsregister beim Amtsgericht Frankfurt unter der Nummer HRB 32000 eingetragen. Die Commerzbank AG unterliegt der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Straße 108, 53117 Bonn, Marie-Curie-Straße 24-28, 60439 Frankfurt am Main und der Europäischen Zentralbank, Sonnemannstraße 20, 60314 Frankfurt am Main, Deutschland.

Großbritannien: Dieses Dokument wurde von der Commerzbank AG, Filiale London, herausgegeben oder für eine Herausgabe in Großbritannien genehmigt. Die Commerzbank AG, Filiale London, ist von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und von der Europäischen Zentralbank amtlich zugelassen und unterliegt nur in beschränktem Umfang der Regulierung durch die Financial Conduct Authority und Prudential Regulation Authority. Einzelheiten über den Umfang der Genehmigung und der Regulierung durch die Financial Conduct Authority und Prudential Regulation Authority erhalten Sie auf Anfrage. Diese Ausarbeitung richtet sich ausschließlich an „Eligible Counterparties" und „Professional Clients". Sie richtet sich nicht an „Retail Clients". Ausschließlich „Eligible Counterparties" und „Professional Clients" ist es gestattet, die Informationen in dieser Ausarbeitung zu lesen oder sich auf diese zu beziehen. Commerzbank AG, Filiale London bietet nicht Handel, Beratung oder andere Anlagedienstleistungen für „Retail Clients" an.

USA: Die Commerz Markets LLC („Commerz Markets") hat die Verantwortung für die Verteilung dieses Dokuments in den USA unter Einhaltung der gültigen Bestimmungen übernommen. Wertpapiertransaktionen durch US-Bürger müssen über die Commerz Markets, Swaptransaktionen über die Commerzbank AG abgewickelt werden. Nach geltendem US-amerikanischen Recht können Informationen, die Commerz Markets-Kunden betreffen, an andere Unternehmen innerhalb des Commerzbank-Konzerns weitergegeben werden. Sofern dieses Dokument zur Verteilung in den USA freigegeben wurde, ist es ausschließlich nur an „US Institutional Investors" und „Major Institutional Investors" gerichtet, wie in Rule 15a-6 unter dem Securities Exchange Act von 1934 beschrieben. Commerz Markets ist Mitglied der FINRA und SIPC. Die Commerzbank AG ist bei der CFTC vorläufig als Swaphändler registriert.

Kanada: Die Inhalte dieses Dokuments sind nicht als Prospekt, Anzeige, öffentliche Emission oder Angebot bzw. Aufforderung zum Kauf oder Verkauf der beschriebenen Wertpapiere in Kanada oder einer kanadischen Provinz bzw. einem kanadischen Territorium beabsichtigt. Angebote oder Verkäufe der beschriebenen Wertpapiere erfolgen in Kanada ausschließlich im Rahmen einer Ausnahme von der Prospektpflicht und nur über einen nach den geltenden Wertpapiergesetzen ordnungsgemäß registrierten Händler oder alternativ im Rahmen einer Ausnahme von der Registrierungspflicht für Händler in der kanadischen Provinz bzw. dem kanadischen Territorium, in dem das Angebot abgegeben bzw. der Verkauf durchgeführt wird. Die Inhalte dieses Dokuments sind keinesfalls als Anlageberatung in einer kanadischen Provinz bzw. einem kanadischen Territorium zu betrachten und nicht auf die Bedürfnisse des Empfängers zugeschnitten. In Kanada sind die Inhalte dieses Dokuments ausschließlich für Permitted Clients (gemäß National Instrument 31-103) bestimmt, mit denen Commerz Markets LLC im Rahmen der Ausnahmen für internationale Händler Geschäfte treibt. Soweit die Inhalte dieses Dokuments sich auf Wertpapiere eines Emittenten beziehen, der nach den Gesetzen Kanadas oder einer kanadischen Provinz bzw. eines kanadischen Territoriums gegründet wurde, dürfen Geschäfte in solchen Wertpapieren nicht durch Commerz Markets LLC getätigt werden. Keine Wertpapieraufsicht oder ähnliche Aufsichtsbehörde in Kanada hat dieses Material, die Inhalte dieses Dokuments oder die beschriebenen Wertpapiere geprüft oder genehmigt; gegenteilige Behauptungen zu erheben, ist strafbar.

Europäischer Wirtschaftsraum: Soweit das vorliegende Dokument durch eine außerhalb des Europäischen Wirtschaftsraumes ansässige Rechtsperson erstellt wurde, erfolgte eine Neuausgabe für die Verbreitung im Europäischen Wirtschaftsraum durch die Commerzbank AG, Filiale London.

Singapur: Dieses Dokument wird in Singapur von der Commerzbank AG, Filiale Singapur, zur Verfügung gestellt. Es darf dort nur von institutionellen Investoren laut Definition in Section 4A des Securities and Futures Act, Chapter 289, von Singapur („SFA") gemäß Section 274 des SFA entgegengenommen werden.

Hongkong: Dieses Dokument wird in Hongkong von der Commerzbank AG, Filiale Hongkong, zur Verfügung gestellt und darf dort nur von „professionellen Anlegern" im Sinne von Schedule 1 der Securities and Futures Ordinance (Cap. 571) von Hongkong und etwaigen hierin getroffenen Regelungen entgegengenommen werden.

Japan: Dieses Dokument und seine Verteilung stellen keine „Aufforderung" gemäß dem Financial Instrument Exchange Act (FIEA) dar und sind nicht als solche auszulegen. Dieses Dokument darf in Japan ausschließlich an „professionelle Anleger" gemäß Section 2(31) des FIEA und Section 23 der Cabinet Ordinance Regarding Definition of Section 2 of the FIEA durch die Commerzbank AG, Tokyo Branch, verteilt werden. Die Commerzbank AG, Tokyo Branch, war jedoch nicht an der Erstellung dieses Dokuments beteiligt. Nicht alle Finanz- oder anderen Instrumente, auf die in diesem Dokument Bezug genommen wird, sind in Japan verfügbar. Anfragen bezüglich der Verfügbarkeit dieser Instrumente richten Sie bitte an die Abteilung Corporates & Markets der Commerzbank AG oder an die Commerzbank AG, Tokyo Branch. [Commerzbank AG, Tokyo Branch] Eingetragenes Finanzinstitut: Director of Kanto Local Finance Bureau (Tokin) Nr. 641 / Mitgliedsverband: Japanese Bankers Association.

Australien: Die Commerzbank AG hat keine australische Lizenz für Finanzdienstleistungen. Dieses Dokument wird in Australien an Großkunden unter einer Ausnahmeregelung zur australischen Finanzdienstleistungslizenz von der Commerzbank gemäß Class Order 04/1313 verteilt. Die Commerzbank AG wird durch die BaFin nach deutschem Recht geregelt, das vom australischen Recht abweicht.

Beratung
und Terminvereinbarung für Firmenkunden

Filialen

Die Commerzbank ist an mehr als 100 Standorten für Firmenkunden in Deutschland und weltweit in knapp 50 Ländern vor Ort vertreten.

Online

www.commerzbank.de/firmenkunden

Commerzbank AG
Zentrale
Kaiserplatz
Frankfurt am Main

Postanschrift
60261 Frankfurt am Main
SectorDesk@commerzbank.com

Der Bericht beruht auf Analysen und Einschätzungen durch die Commerzbank AG.

Die redaktionelle und grafische Aufbereitung des Berichts erfolgt in Kooperation mit dem Handelsblatt Research Institute.

Dieser Bericht wurde im Juli 2019 erstellt.