Praxistipps IT

Cybersecurity in der Praxis

Gefahren, Präventionsmaßnahmen, Krisenmanagement

Krüger/Simon/Trappe

IDW VERLAG GMBH

1 Einleitung

Computer, oder besser gesagt IT-Systeme dienen heutzutage nicht mehr nur der Unterstützung aufkommender „Büroarbeit“, sondern stellen viel eher den zentralen Dreh- und Angelpunkt der eigenen Geschäftsprozesse, in einem zum Teil global vernetzten Umfeld, dar. Mit dem Fortschreiten der Digitalisierung kommt „dem Computer“ inzwischen gar eine gänzlich neue Rolle zu.

Der digitalisierte Arbeitsplatz ist heutzutage ein absolut kritisches Asset, ohne den die Aufrechterhaltung der eigenen Geschäftsprozesse nicht mehr möglich ist. Im gleichen Atemzug wächst durch die stetig zunehmende Vernetzung die Komplexität informationsverarbeitender Systeme. Die Grenzen des eigenen Verantwortungsbereichs aber auch der eigenen Handlungsmöglichkeiten verschwimmen zunehmend. Die Hoheit über die eigenen Daten endet dort, wo Produkte oder Services externer Dienstleister ihre Verarbeitung übernehmen sollen. Ein prägnantes Beispiel dafür ist die Verlagerung ganzer Prozesse in die Cloud.

Allen Vorteilen moderner IT stehen mindestens ebenso viele Risiken gegenüber, wie die folgenden Abschnitte zeigen. Sich dagegen angemessen und wirtschaftlich zu wappnen stellt für viele Organisationen eine große Herausforderung dar.

„Illegaler Wissens- und Technologietransfer, Social-Engineering und auch Wirtschaftssabotage sind keine seltenen Einzelfälle, sondern ein Massenphänomen.“
– Thomas Haldenwang, Vizepräsident des Bundesamtes für Verfassungsschutz (BfV), Berlin 2018

In letzter Vergangenheit gab es gehäuft Nachrichten über Datenpannen in den Medien. Fast monatlich werden sensible Kundendaten öffentlich gemacht. Laut einer Studie von IBM[1] kosteten in Deutschland im Jahr 2019 Datenpannen Unternehmen im Durchschnitt 4,3 Millionen Euro[2]. Die Dunkelziffer liegt dabei vermutlich noch höher. Den höchsten Schaden durch Cyberangriffe erlitt die Gesundheitsindustrie gefolgt von dem Fi-

[1] https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf (abgerufen am 22.09.2019).
[2] IBM Studie, gemeldete Vorfälle zwischen Juli 2018 und April 2019.

nanzsektor. **Abb. 1.1** zeigt auf, dass mehr als die Hälfte der Data Breaches (Datenlecks / Datenpannen) durch böswillige oder kriminelle Angreifer geschieht.

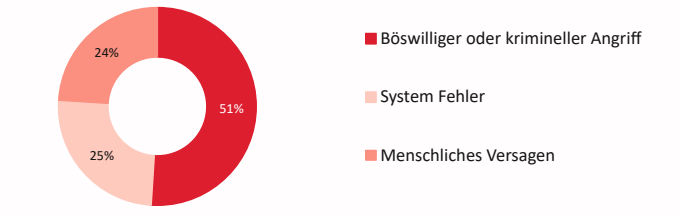

Abb. 1.1 Gründe für Data Breaches[3]

Auch deutsche KMUs (kleine und mittlere Unternehmen) bleiben vor Cyberangriffen nicht verschont. Die Auswirkungen sind dabei keineswegs gering. Der Mittelstand bildet das Rückgrat der deutschen Wirtschaft. Cyberkriminelle haben dieses Potenzial längst für sich erkannt und verursachen großen Schaden. Aus Sicht der Angreifer sind KMUs besonders attraktiv, da sie in der Regel nur über grundlegende Sicherheitsvorkehrungen verfügen und als Sprungbrett für größere Hacking-Kampagnen dienen.

Wirtschaftsprüfer sind von dieser Herausforderung gleich in doppelter Weise betroffen. Zum einen sind sie selbst Organisationen, die im Fokus potentieller Angreifer liegen, zum anderen bewerten sie die Implementierung organisatorischer und technischer Maßnahmen hinsichtlich der Wirtschaftlichkeit in den in Prüfung befindlichen Unternehmen.

Ein interessanter Aspekt dabei ist, dass laut einer Studie von Bitkom[4], stärker digitalisierte Unternehmen in Deutschland weniger von Cyberangriffen betroffen sind, als nicht so stark digitalisierte Unternehmen. Die oft gepredigte Devise „uns kann nichts passieren, wir stützen uns nur zu einem geringen Teil auf digitalisierte Prozesse“ führt also nicht zu einer Auflösung des Dilemmas.

Imageschäden bei Kunden und Lieferanten stellen in aller Regel den größten Schaden eines Cyberangriffs dar. **Abb. 1.2** zeigt die größten Kostenverursa-

[3] IBM Studie, gemeldete Vorfälle zwischen Juli 2018 und April 2019.
[4] https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf (abgerufen 22.09.2019).

cher bei Unternehmen, welche in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren.

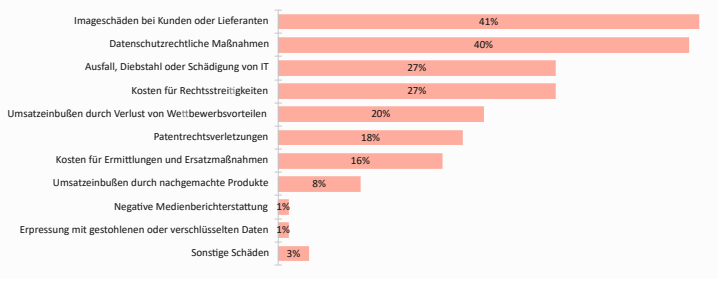

Abb. 1.2 Aufgetretene Schadensvorfälle 2018 – Mehrfachnennungen in Prozent (Quelle: Bitkom Research)

Der Täterkreis ist oftmals bekannt, doch die Aufklärung dauert nicht selten Jahre und ist oftmals nicht erfolgsversprechend. Deshalb ist es umso wichtiger, dass das Risiko eines IT-Sicherheitsvorfalls minimiert wird. Und sollte es trotz aller Präventivmaßnahmen zum Ernstfall kommen, sollten Sie wissen, welche Maßnahmen ergriffen werden müssen, um den Schaden einzuschränken.

Das vorliegende Buch wird Ihnen einen Leitfaden zur Aktion und Reaktion mit an die Hand geben, um Situationen besser einschätzen zu können und entsprechend handeln zu können. Es soll dabei einen Überblick über aktuelle Cybersecurity-Herausforderungen geben und Ihnen Maßnahmen zur Bewältigung dieser darstellen.

In den folgenden Kapiteln werden wir Ihnen zuerst die Gefahren, welche von verschiedenen Akteuren im Cyberspace ausgehen, darstellen und später Verteidigungsmaßnahmen präsentieren. Des Weiteren gehen wir, unter Berücksichtigung der unterschiedlichen Unternehmensgrößen, auf Bausteine der Cybersecurity-Basisabsicherung ein.

Wir werden Ihnen einen Überblick über alle heutzutage relevanten Themenfelder wie Cloud-Dienste, Mobile Device Security, Internet der Dinge und Open Source Security Software geben. Anschließend behandeln wir das Thema Business Continuity Management, das im Ausnahmefall dafür sorgt, dass alle relevanten Geschäftsaktivitäten aufrecht erhalten bleiben. Am Ende des Buches geben wir Ihnen in dem Kapitel 12 „Thinking outside

the Box“ einige unkonventionelle Ideen zur Auseinandersetzung mit dem Thema Cybersecurity mit auf den Weg. Diese können unter anderem dabei helfen, sich in die Rolle eines potentiellen Angreifers hineinzuversetzen oder ermöglichen einen lockeren Einstieg in dieses komplexe Themenfeld.

Vor dem Einstieg in das eigentliche Thema seien an dieser Stelle noch ein paar Hinweise gegeben:

Die Produktlandschaft entwickelt sich ständig weiter. Durch die Cloud-Technologie entstehen zudem kontinuierlich gänzlich neue Service-Angebote diverser Hersteller. Es darf davon ausgegangen werden, dass sich dadurch das Innovationstempo noch einmal deutlich erhöhen wird. Um diesem Leitfaden nun nicht schon zum Zeitpunkt der Erstellung ein inhaltliches Verfallsdatum mitzugeben, wurde auf die Benennung konkreter Produkte verzichtet. Wir erläutern stattdessen, wo immer dies sinnvoll ist, Fähigkeiten oder Produktkategorien, anhand derer Sie später den Markt durchsuchen und geeignete Produkte identifizieren können.

Wir werden des besseren Leseflusses wegen, von nun an für alle Berufsbezeichnungen die männliche Form nutzen, was selbstverständlich immer auch die weibliche und alle anderen Formen einschließt.

Weiterhin möchten wir Sie auf unsere online bereitgestellten Inhalte aufmerksam machen. Unter anderem finden sie dort das zu diesem Buch gehörende Glossar, sowie Checklisten für die Umsetzung von Cybersecurity-Maßnahmen in Ihrer Kanzlei bzw. zur Beurteilung bereits umgesetzter Maßnahmen bei Ihrem Kunden.

Sollten Sie in diesem Leitfaden auf *kursiv* geschriebene Wörter stoßen, werden sie diese in unserem Glossar wiederfinden.

Hinweis:
Sollten Sie Fragen oder Anmerkungen zum Buch oder den online bereitgestellten Inhalten haben, so zögern Sie nicht, uns eine E-Mail zukommen zu lassen. Sie erreichen uns unter:
Praxistipps-IT@Laokoon-Security.com

2 Akteure, Gefahren und Grundlagen

Bevor adäquate Schutzmaßnahmen ausgeplant werden können, ist zu prüfen, vor welchen Gefahren es sich überhaupt zu schützen gilt. Aus diesem Grund werden auf den folgenden Seiten die verschiedenen Entitäten des Cyberraums und deren jeweilige Interessen (Motivationen) sowie mögliche Schadensarten und Angriffsszenarien dargestellt.

Darüber hinaus wird in diesem Kapitel kurz das Thema Cloud angerissen, welches jedoch insbesondere im Kapitel 6 genauer beleuchtet wird.

2.1 Der Cyberraum (Cyberspace)

Eine klare und unumstößliche Definition für den Begriff *Cyberraum* oder Cyberspace in allen Facetten und mit allen Perspektiven herbeizuführen wäre zu akademisch und gewiss auch deutlich zu umfangreich für diesen Leitfaden.

Das Bundesamt für Sicherheit in der Informationstechnik reduziert den Begriff Cyberraum gewissermaßen auf den rein technischen Aspekt:

> *Der Cyber-Raum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyber-Raum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.*

(Quelle: Cyber-Glossar des BSI[5])

Wobei als informationstechnisches System laut BSI Folgendes verstanden wird:

> *Ein informationstechnisches System (IT-System) ist eine technische Anlage, die der Informationsverarbeitung dient und eine abgeschlossene Funktionseinheit bildet. Typische IT-Systeme sind Server, Clients, Einzelplatzcomputer, Mobiltelefone, Router, Switches und Sicherheitsgateways.*

(Quelle: Cyber-Glossar des BSI)

[5] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html (abgerufen am 12.09.2019)

Bei der Betrachtung des Themas Cybersecurity spielen jedoch, wie spätestens in Kapitel 5 zu sehen sein wird, deutlich mehr Faktoren eine Rolle. Von daher differenzieren wir an dieser Stelle zwischen dem Cyberraum im engeren Sinne, was der Definition des BSI entspricht, sowie dem Cyberraum im weiteren Sinne, wobei wir die Darstellung des BSI um Menschen und die physische Umgebung erweitern.

Das zentrale Element des Cyberraums im engeren wie auch im weiteren Sinne ist das Internet. In der heutigen Zeit handelt es sich dabei in erster Linie um einen Marktplatz für Services aller Art. Ferner handelt es sich auch um ein etabliertes Kommunikationsmittel (oder zumindest die technische Grundlage für zeitgemäße Kommunikation) oder gar sozialen Lebensraum für Millionen Menschen weltweit. Letzten Endes hat uns bspw. Facebook in den vergangenen Jahren gelehrt, dass am Ende auch diese vermeintliche soziale Geborgenheit als Service zu verstehen ist.

Der Mensch tritt also als Servicebereitsteller (vgl. Webseiten, Online-Spiele, Social-Media-Plattformen) und Servicekonsument in Erscheinung.

Darüber hinaus ist der Mensch ein manipulierbarer Entscheidungsträger, der durch sein unvorsichtiges Handeln, z.B. im Cyberraum, den Fortbestand eines Unternehmens gefährden kann. Er ist häufig schlecht abzusichern und sein Fehlverhalten führt nicht selten zu ernsten Konsequenzen (vgl. *Ransomware/*verschlüsselte Datenträger). Dem Menschen kommt daher im Cyberraum eine ganz besondere Rolle zu.

Hinweis:
Die Darstellung des im Cyberraum aktiven Individuums als einfacher Konsument der im Cyberraum angebotenen Services ist natürlich stark abstrahiert. So handelt es sich in der Praxis nicht ausschließlich um den passiven Konsum, sondern viel eher um aktive Interaktion. Der Einfachheit halber fassen wir dennoch all jene, die keinen eigenen Service im Cyberraum bereitstellen, als Servicekonsumenten zusammen.

In diesem Guide werden die Begriffe Unternehmen, Gesellschaft, Organisation und Kanzlei synonym verwendet.

Die physische Umgebung ist zumindest mittelbar mit dem Cyberraum verknüpft. Wie in Kapitel 5 gezeigt wird, sind Maßnahmen in diesem Spektrum

wesentlich für die Gewährleistung einer störungsfreien Serviceerbringung und leisten somit einen wichtigen Beitrag für den Erhalt des Cyberraums.

2.2 Cybersecurity

Cybersecurity ist, wie oben bereits angeklungen, die Gesamtheit aller Maßnahmen, die vor den Gefahren des *Cyberraums* (im weiteren Sinne) schützen. Dabei beschränkt sich dieses Themenfeld nicht auf etwaige technische Maßnahmen oder den virtuellen Raum, sondern umfasst auch jene Aspekte, die der Absicherung des IT-Anwenders und seines Umfelds dienen.

Hinweis:

In der englischen Sprache existieren für das Wort Sicherheit zwei Begriffe, *Security* und *Safety*. Sie ermöglichen unterschiedliche Blickwinkel auf den Begriff Sicherheit. Security bedeutet dabei sinngemäß, dass ein Objekt in Sicherheit ist. Safety hingegen beschreibt, inwiefern die Umgebung des Objekts in Sicherheit, also sicher vor dem Objekt selbst, ist.

So ist eine Schließanlage, die das Betreten einer Kanzlei (das Objekt) verhindert, eine Security-Maßnahme. Dass dieselbe Schließanlage im Falle eines Stromausfalls innerhalb der Kanzlei jedoch öffnet und den Menschen die Möglichkeit bietet, die Kanzlei zu verlassen, ist eine Safety-Maßnahme.

2.3 Akteure des Cyberraums

Wir betrachten Menschen im *Cyberraum* in erster Linie als Servicekonsumenten oder ggf. Servicebereitsteller. Da diese beiden Facetten jedoch von ihren Interessen her verhältnismäßig dicht beieinander liegen und quasi in einer Symbiose existieren, fassen wir diese beiden Seiten unter dem Begriff Anwender, im Sinne eines regulären IT-Anwenders, zusammen. Darüber hinaus verallgemeinern wir weiter, indem wir nun festlegen, dass diese Anwender keine zwangsläufig natürlichen Personen sein müssen. Wir zählen Ihre Kanzlei demnach auch als eigenständige Entität mit der Absicht, Services zu konsumieren, zu dieser Gruppe hinzu.

Dem gegenüber stehen jene Entitäten, die sich vermeintlich schädlich diesen Anwendern gegenüber verhalten.

2.3.1 Anwender

Als Anwender verstehen wir also alle Entitäten innerhalb des Cyberraums, die keine potenziell kriminellen Absichten verfolgen.

Ein Anwender konsumiert Services bspw. zu Gunsten der Aufrechterhaltung seiner Geschäftsprozesse (Office-, Buchhaltungsapplikationen oder sonstige Cloud-Dienste) oder seiner eigenen Bedürfnisse, oder stellt Services bereit.

Durch die Aktivitäten der Anwender innerhalb des Cyberraums werden sie darüber hinaus jedoch auch zur Zielscheibe. Es war lange Zeit üblich, diese Gruppe der potenziellen Ziele für Cyberangriffe ihrer Größe, Ausprägung oder Sichtbarkeit nach zu unterscheiden. Tatsächlich zeigt die jüngere Vergangenheit, dass eine solche Unterscheidung nicht mehr zutrifft und häufig nur noch in der Art und Intensität der Angriffe variiert.

Natürlich kommen bestimmte Angriffe häufiger gegen bestimmte Ziele vor als andere. So werden Privatpersonen und Kanzleien seltener Opfer langfristig angelegter Sabotagekampagnen, als das bspw. bei zwischenstaatlichen Konflikten beobachtet werden kann.

Was in diesem Zusammenhang durchaus von Interesse ist, ist die Frage nach möglichen Schäden, die durch einen Cyberangriff entstehen können. Tabelle **Tab. 2.1** gibt daher einen kleinen Überblick über mögliche Schadensarten, wobei die Reihenfolge als Annahme hinsichtlich der Eintrittswahrscheinlichkeit verstanden werden kann.

Bezeichnung	Beschreibung
Datenverlust/ -manipulation	Hierunter zählt Datendiebstahl auf der einen und die Unbrauchbarmachung von Informationen (*Ransomware*) auf der anderen Seite. Mit Einführung der DSGVO im Mai 2018 hat insbesondere der erste Punkt an Bedeutung gewonnen. Die Erfahrung zeigt jedoch, dass erhebliche Schäden gerade durch defekte Daten (inkl. Backups) entstanden sind. Ein Aspekt, der hierbei häufig vergessen wird, ist die gezielte Datenmanipulation. Insbesondere für Services, die auf die Integrität der Daten angewiesen sind, kann dies deutlich schlimmer sein als der bloße Datenverlust. Für Privatpersonen ist dies zudem der wohl am häufigsten auftretende und zugleich gefürchtetste Schadensfall, da dies nicht selten mit der Offenlegung sensibler/intimer Informationen einhergeht.
Reputationsschäden	Je nach Ausmaß des Angriffs ist grundsätzlich mit einem Reputationsschaden zu rechnen.

Bezeichnung	Beschreibung
Technische Schäden	Hierunter zählen bspw. Systemausfälle. Selten, jedoch nicht auszuschließen, sind neben dem temporären Ausfall einzelner Systeme durch Unregelmäßigkeiten auf Ebene der Software echte Schäden an der Hardware.
Wirtschaftliche Schäden	Abstrakt, aber dennoch unmittelbar auf Cyberangriffe zurückzuführen, sind unter Umständen Ausfälle der Produktion, des Vertriebs oder allgemein der Servicebereitstellung mit dem Ergebnis finanzieller Einbußen. Wenngleich hier wohl der Interessensschwerpunkt für das Management liegen dürfte, so sollte bedacht werden, dass es sich hierbei um kein exklusives Cyber-Thema handelt.
Organisatorische Schäden	Ein gezielter Angriff auf existenzielle Fähigkeiten eines Unternehmens kann zum Zusammenbrechen der Organisation an sich führen. Gemeint ist hierbei der Zusammenbruch bestehender Prozesse/Prozessketten. Hiervon kann sowohl die Fertigung wie auch die Unternehmensführung betroffen sein.
Personenschäden	Der wohl schlimmste anzunehmende Schaden ist Personenschaden. Heutzutage kann dies durch die starke Vernetzung von bspw. Steuer- und Regelanlagen leider nicht mehr ausgeschlossen werden. Man denke insbesondere an den gesamten Bereich KRITIS.

Tab. 2.1 Schadensarten

2.3.2 Angreifer

Angreifer lassen sich nach zwei Merkmalen unterscheiden, Größe und Motivation.

Orientierte sich die Motivation bis in die 80er/90er Jahre noch recht deutlich am Ruhm, wandert sie seitdem zunehmend in den Bereich solider Geschäftsmodelle. Wenngleich es natürlich illegal ist, ein solches zu betreiben. Und damit sind wir auch schon bei dem wohl inzwischen wesentlichen Antrieb moderner krimineller Hacker angekommen, dem Geld.

Eingriffe im Sinne der Manipulation von Informationen und/oder Lähmung bspw. ganzer Wirtschaftszweige oder Regierungen sind eher große, auf Dauer angelegte verdeckte Operationen, die zwar ganzheitlich von herausragender Bedeutung, für den Einzelnen oder für KMUs jedoch nur bedingt von Bedeutung sind. Tabelle **Tab. 2.2** fasst eine Auswahl geeigneter Unterscheidungsmerkmale oder, besser gesagt, Charakteristika von im *Cyberraum* offensiv agierenden Entitäten zusammen.

Bezeichnung	Motivation	Größenordnung	Ziel
Hacktivism[6]	Ruhm, politisch motiviert; Ideale; Aufklärung; vermeintlich Missstände beseitigen	Zum Teil größere Gruppen	Erpressung; Informationsgewinnung; Kompromittierung
Cyber-Kriminelle	Geld	Einzeltäter; Kleingruppen	Erpressung; Betrug; Proliferation
Organisierte Kriminalität		Nehmen Unternehmensstrukturen an; Größe variiert stark; häufig lose Verbindungen aus Einzeltätern	
Staatlich subventionierte Hackergruppen	Geld; Ideale	Gut organisierte Kleingruppen; Größe variiert	Informationsgewinnung; Spionage; Kompromittierung; Sabotage
Staatliche Hackergruppen	Informationen; politisches und militärisches Wirkmittel; Krisenbewältigung	Angaben sind nicht öffentlich verfügbar	
Script-Kiddie[7]	Neugier; Rache; Geld	Einzeltäter	Erpressung; Kompromittierung

Tab. 2.2 Angreiferarten

Hinweis:

Die Bezeichnung „Hacker" ist ungerechtfertigterweise negativ besetzt, weil darunter oft jemand verstanden wird, der in fremde Computer einbricht. Tatsächlich bezeichnet dieses Wort allerdings lediglich Individuen, die sich durchaus intensiv mit technischen, organisatorischen oder sonstigen Grundlagen des *Cyberraums* (im weiteren Sinne) befassen und diese kritisch hinterfragen.

Ohne Hacker stünde auch der gesamte Bereich der *Cybersecurity* nicht dort, wo er heute steht.

[6] Hacktivist: Wortneuschöpfung aus „Hacking" und „Aktivist".

[7] Script-Kiddies sind unerfahrene, zum Teil unbeabsichtigt offensiv agierende Einzeltäter. Sie verfügen über keine speziellen Fähigkeiten und verfolgen nicht zwingend ein echtes Ziel, sondern sind eher von Neugier getrieben. Für Kanzleien und andere Unternehmen mit einer rudimentären Absicherung sollten Script-Kiddies keine Gefahr darstellen.