Präsentiert von:

ESET

Datenschutz

für dummies

- Erfahren Sie alles über aktuelle Gefahren für die IT-Security
- Lernen Sie, wie Sie kleine und mittelständische Unternehmen schützen
- Minimieren Sie die Folgen von Datenschutzvorfällen

Limitierte ESET Edition

Lawrence Miller

Über ESET

ESET begann als Pionier in der Entwicklung von Virenschutz und bietet seit mehr als 30 Jahren ausgezeichnete Sicherheitslösungen zum Schutz vor Bedrohungen aller Art. Heute bieten unsere innovativen Produkte Unternehmen und Privatkunden in mehr als 200 Ländern und Regionen besten Schutz für ihre digitale Welt. Dabei haben wir uns als europäisches Unternehmen kein geringeres Ziel gesetzt, als Technologie für alle sicher zu machen und dafür zu sorgen, dass sie die neuesten Entwicklungen entspannt genießen können.

Datenschutz

limitierte ESET Auflage

von Lawrence Miller

für dummies®

Datenschutz für Dummies®, limitierte ESET® Auflage

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Limitierte Auflage 2019

Veröffentlicht von: **John Wiley & Sons, Ltd.**,
The Atrium, Southern Gate Chichester, West Sussex,
www.wiley.com

Gedruckt bei Hobbs the Printers Ltd, Hampshire, UK

ISBN Softcover: 978-1-119-60684-0

ISBN ebook: 978-1-119-60686-4

Table of Contents

Einleitung

„Ihr Unternehmen ist so klein, da lohnt sich ein Angriff gar nicht,“

– Sie glauben nicht wirklich, dass Sie diesen Satz jemals so hören werden, oder? Hacker und Cyberkriminelle handeln opportunistisch. Natürlich sind kleine und mittelständische Unternehmen (KMU) nicht die typischen Ziele, die man beim Gedanken an Cyberkriminalität im Kopf hat. Trotzdem sind sie willkommener Beifang, mit dem sich ebenso Geld machen lässt – vor allem dann, wenn Netzwerke, Server, Anwendungen, Daten, Desktops, Laptops und Mobilgeräte nicht ausreichend geschützt sind. Klar: Datenlecks in KMU verursachen keinen großen Medienwirbel, wie wir ihn von Vorfällen bei Bupa, CEX, Clarksons, Equifax, Target, Uber, oder Yahoo! gewohnt sind. Dafür sind die Auswirkungen für kleinere Unternehmen teilweise umso gravierender und können schlimmstenfalls den Ruin Ihrer Firma nach sich ziehen. Vor allem, weil mit fortschreitender Digitalisierung aller Unternehmensbereiche IT-Sicherheit auch für kleine Unternehmen immer mehr zum zentralen Asset wird. Doch keine (unnötige) Sorge: Sie haben bereits eine erste wichtige Investition getätigt und dieses Buch gekauft. Jetzt steht der Optimierung Ihrer digitalen Prozesse (fast) nichts mehr im Weg.

Natürlich sind Cyberangriffe und Datenschutzvorfälle beileibe nichts Neues. Schon seit Jahren kommen die Medien manchmal kaum hinterher, wenn über Datenlecks in großen Unternehmen berichtet werden soll. (Kleine Firmen wird es ab und zu genauso betroffen haben. Nur hat eben kaum jemand darüber berichtet.) Allerdings haben sich mittlerweile die kriminellen Technologien und Strategien im Vergleich zu früher erheblich weiterentwickelt – und mit ihnen die „Betätigungsfelder“ der Angreifer. So werden nun auch kleine und mittelständische Unternehmen interessant und avancieren teilweise sogar zu den Hauptangriffszielen für Malware-Kampagnen.

Verständlicherweise: KMU machen mehr als 99 % aller Unternehmen weltweit aus, beschäftigen mehr als die Hälfte der Arbeitskräfte und tragen über 50 % zum Bruttoweltprodukt bei. Klingt nach einem ziemlich attraktiven Angriffsziel, oder?

Zu den aktuellen Angriffsmethoden zählen:

- Ausgeklügelte Malware-Technologien (wie Polymorphismus und Metamorphismus), Ransomware und Remote Access Trojaner (RAT),
- Directory-Harvest-Angriffe (DHA), gezielter Spam und Phishing (Spearphishing) per E-Mail,
- automatisierte Botnetze,
- DNS-Hijacking und Cache-Poisoning,
- Port-Hopping und gefälschte SSL-Zertifikate,
- (immer noch und wieder mehr) DDoS-Angriffe.

Mal ehrlich: Welche Branche kommt heute noch ohne IT aus? Gleichzeitig wird die Bedrohungslandschaft immer komplexer und weitreichender. Kleinere Unternehmen haben oft weder die finanziellen Mittel noch gut ausgebildetes Personal in genügender Menge, um sich hier ausreichend zur Wehr zu setzen.

Sie haben aber auch einen ganz entscheidenden Vorteil: KMU arbeiten mit weniger komplexen Netzwerken und sind so anpassungsfähiger und weniger behäbig, wenn es um die Erstellung und Umsetzung von Datenschutzstrategien geht. Nutzen Sie diesen Vorteil! Wenn Sie rechtzeitig die richtigen Entscheidungen treffen, wird Ihr Unternehmen für Angreifer wesentlich unattraktiver. Und das ist noch immer der beste Schutz vor Angriffen.

Dieses Buch soll Ihnen dabei helfen und informiert Sie zu Sicherheitstechnologien, Tools und Prozessen, mit denen Sie Ihre Datenschutzmaßnahmen umfassend optimieren. Natürlich werden sich Datenlecks nie komplett verhindern lassen. Mit einer vernünftigen Datenschutzstrategie halten Sie die negativen Folgen aber so gering wie möglich.

Über dieses Buch

Datenschutz für Dummies®, limitierte ESET Auflage, enthält sechs kurze Kapitel zu den folgenden Themen:

- Typische Cyberangriffe und aktuelle Trends, gesetzliche Vorgaben und die Auswirkungen von Datenpannen (Kapitel 1)
- Beurteilung verschiedener Methoden für den Schutz von Unternehmensdaten, inkl. Umsetzung (Kapitel 2)
- Risikobewertung, Identifikation von Vermögenswerten, Gefahrenanalyse und Bewertung von Schwachstellen (Kapitel 3)
- Vorstellung von Methoden (Verschlüsselung, Endpoint-Schutz, Firewalls etc.) (Kapitel 4)

- Wichtige organisatorische und prozessbezogene Kontrollmechanismen (Kapitel 5)
- Zehn Schlüsselfaktoren für effizienten Datenschutz in KMU (Kapitel 6)

Am Ende des Buchs finden Sie außerdem ein Glossar, in dem Sie schnell und unkompliziert Abkürzungen und Begriffe nachschlagen können.

Für wen ist dieses Buch gedacht?

Dieses Buch wurde genau für Sie geschrieben. Wir gehen davon aus, dass Sie in der IT-Abteilung eines KMU arbeiten, entweder als Manager eines kleinen Allround-Teams oder sogar ganz allein. Sie und gegebenenfalls Ihr Team sind verantwortlich für alles, was „irgendwie" mit IT zu tun hat: vom Austausch der Druckerpatronen und Setup von Endgeräten über das Management des Firmennetzwerks bis hin zur Behebung von Sicherheitsproblemen. Entsprechend verfügen Sie über umfassende und breit gefächerte IT-Kenntnisse und die nötige Erfahrung. Trotzdem gibt es vielleicht Bereiche – beispielsweise IT-Sicherheit und Datenschutz – über die Sie mehr erfahren wollen.

Selbst wenn keine der Aussagen zutrifft, lesen Sie trotzdem weiter. Wenn Sie mit dem Lesen fertig sind, wird Ihnen in Sachen Datenschutz so schnell niemand mehr etwas vormachen.

Symbole in diesem Buch

In diesem Buch verwenden wir gelegentlich spezielle Symbole, um auf wichtige Informationen hinzuweisen. Die Symbole sehen folgendermaßen aus:

ERINNERUNG

Dieses Symbol weist auf eine Information hin, die Sie unbedingt löschsicher in Ihrem Speicher ablegen sollten – metaphorisch gesprochen.

TIPP

Tipps sind wie Trinkgeld: nicht unbedingt verpflichtend, aber nett. Dieses Symbol weist auf nützliche Informationen und hilfreiche Ratschläge hin.

ACHTUNG

Dieses Symbol hilft Ihnen, potenziell kostspielige Fehler zu vermeiden.

Über das Buch hinaus

Wir haben dieses Büchlein bewusst knapp gehalten. Deshalb können wir natürlich nicht alle Themen bis ins kleinste Detail besprechen. Weitere Infos rund um IT-Sicherheit und Datenschutz finden Sie auf dem `http://www.welivesecurity.de`-Blog und unter `http://www.eset.de`.

Und jetzt?

Wir entschuldigen uns schon im Voraus für das dreiste (und schlechte) Plagiat bei Lewis Carroll, Alice und der Grinsekatze:

„Willst du mir wohl sagen, wenn ich bitten darf, welchen Weg ich hier nehmen muss?“

„Das hängt zum guten Teil davon ab, wohin du gehen willst“, sagte die Katze, äh … der Autor dieses Buches.

„Es kommt mir nicht darauf an, wohin –“, sagte Alice.

„Dann kommt es auch nicht darauf an, welchen Weg du nimmst,“ sagte die Katze.

„– wenn ich nur irgendwo hinkomme.“

Das gilt so oder so ähnlich auch für unser Buch *Datenschutz für Dummies* (das selbstverständlich ein ebenso zeitloser Klassiker werden wird wie *Alice im Wunderland*, keine Frage).

Falls Sie auch nicht wissen, wohin Sie der Weg führen soll, können Sie mit jedem beliebigen Kapitel anfangen. Kapitel 1 bietet sich an. Sollten Sie aber an einem bestimmen Thema interessiert sein, blättern Sie einfach direkt dorthin. Das Buch ist so konzipiert, dass jedes Kapitel unabhängig von den anderen gelesen werden kann. Sie können das Buch also so lesen, wie Sie es für richtig halten. Es hat sich aber als wenig praktikabel erwiesen, es rückwärts zu lesen oder beim Lesen auf dem Kopf zu halten. Aber wer sind wir, Ihnen Vorschriften zu machen?

INHALT DIESES KAPITELS

Kapitel 1
Datenschutz in Unternehmen – Ein notwendiges Übel?

In diesem Kapitel informieren wir Sie über die negativen Folgen von Datenpannen für Unternehmen, die Entwicklung der modernen Bedrohungslandschaft, den Einfluss jüngster Datenschutzvorfälle in KMU und über die Bedeutung von Änderungen rechtlicher und regulatorischer Anforderungen.

Kosten eines Datenlecks

Kleine und mittelständische Unternehmen machen 99 % aller Unternehmen in der EU und mehr als 95 % der Unternehmen weltweit aus. Da ist es natürlich nicht verwunderlich, dass in mehr als 70 % der Fälle KMU die Leidtragenden von Datenschutzvorfällen sind (laut International Data Corporation, IDC). Viele Unternehmen sind trotzdem nach wie vor der Meinung, dass sie nicht zum Ziel von Cyberangriffen werden können – bieten sie doch aufgrund ihrer geringen Größe vermeintlich kaum attraktive Vermögenswerte. Dummerweise ist es so einfach dann doch nicht.

ERINNERUNG

Dem 2017 von Verizon erstellten *Data Breach Investigations Report* (DBIR) zufolge geht der Fokus von Cyberattacken immer mehr in Richtung Restaurants und kleiner Unternehmen. Interessant sind vor allem Kassensysteme, da sich hier viele gut verwertbare Daten abziehen lassen.

Darüber hinaus sind drei Viertel der Opfer der sechs häufigsten Angriffsmethoden – Diebstahl von Anmeldeinformationen, Backdoors, Spyware, Phishing, Datenexfiltration und C&C-Malware (Command and-Control) – kleine, webbasierte, einzelhandelsfremde Unternehmen.

Wie das Versicherungsunternehmen Zurich berichtet, wurden in Großbritannien im letzten Jahr mehr als 875.000 kleine und mittlere Unternehmen Opfer von Cyberangriffen. Bei über einem Fünftel dieser Unternehmen betrug der Schaden mehr als 13.000 US-Dollar, bei einem Zehntel sogar mehr als 69.000 US-Dollar. Datenlecks in großen Unternehmen verursachten im Schnitt Schäden von mehr als 3,62 Millionen US-Dollar (*Cost of a Data Breach Study 2017*, Ponemon Institute).

Logisch: Die Schäden im KMU-Bereich sind nicht mit denen großer Unternehmen zu vergleichen. Gleichzeitig besitzen kleinere Unternehmen aber meist auch nicht genügend Ressourcen, um angemessen auf Datenschutzvorfälle zu reagieren und sich schnell davon zu erholen. Verordnungen wie die Europäische Datenschutz-Grundverordnung (DSGVO), so wichtig sie für den Verbraucher sein mögen, machen KMU das Leben zusätzlich schwer, indem sie von allen Unternehmen, ganz gleich welcher Größe, eine detaillierte forensische Analyse von Datenschutzvorfällen fordern.

Insgesamt haben sich die durchschnittlichen Kosten von Datenschutzvorfällen vom Jahr 2014 auf 2015 mehr als verdoppelt, so eine Studie über die Kosten von Datenlecks weltweit. Die Kosten für jeden verloren gegangenen oder gestohlenen Datensatz stiegen dabei, wenn auch nur geringfügig, auf fast 150 Euro. Die Anzahl an Datenlecks steigt also, die Kosten jedes einzelnen ebenfalls. Je mehr sensible Daten ein Unternehmen verarbeitet, desto höher sind natürlich die potenziellen Gesamtkosten eines Datenschutzvorfalls. Und seit Inkrafttreten der DSGVO sind sehr viele Daten zu sensiblen Daten geworden. Welche Folgen das hat, kann sich wohl jeder denken. Diese Kosten sollten, insbesondere bei der Strategieentwicklung in Sachen Datenschutz, unbedingt berücksichtigt werden.

Datenvorfälle verursachen unter anderem Kosten durch:

- Betriebsunterbrechungen (einschließlich Zeit- und Produktivitätsverlusten),
- direkte Kosten (wie Kundeninformation und -support, Buchhaltungsausfälle, Entschädigungszahlungen, flächendeckende Neuausstattung mit Kunden- und Kreditkarten usw.),
- Verlust von Kunden (Abwanderung), Markenschaden und Ansehensverlust,

- Gerichtskosten (Klagen durch Konsumenten, Geschäftspartner und Investoren),
- Bußgelder und Strafen,
- Wiederherstellungs- und forensische Kosten (diese machen meist den Löwenanteil der Kosten aus),
- Verlust von Vermögenswerten (z. B. geistiges Eigentum).

ACHTUNG

Der National Cyber Security Alliance zufolge müssen 60 % der kleinen Unternehmen innerhalb von sechs Monaten nach einem Cyberangriff schließen.

TIPP

Versicherungen gegen die Folgen von Cyberattacken sind für KMU sehr attraktiv – versprechen sie doch, die potenziellen Kosten von Angriffen und Datenpannen zu senken. Das ist auch (meist) richtig. Es darf aber nicht vergessen werden, dass solche Versicherungen natürlich nicht vor Angriffen oder Lecks selbst schützen. Nur weil Sie eine Brandschutzversicherung haben, stellen Sie ja keine brennende Kerze unter die Gardinen. Entsprechend sind Versicherungen definitiv keine Alternative zu Best Practices und Strategien, ihrer gewissenhaften Umsetzung im ganzen Unternehmen und regelmäßigen Kontrollen.

Die moderne Bedrohungslandschaft

Auf absehbare Zeit werden Anzahl, Umfang und Kosten von Datenpannen immer weiter steigen. Vor allem folgende Trends leisten hierzu einen wesentlichen Beitrag:

- **Umfassende, automatisierte Angriffe** werden zum Standard für Cyberkriminelle. Die Zeiten des Scriptkiddies, das einige wenige Rechner aus bloßer Zerstörungswut mit wenig professionellen Methoden lahmlegt, sind definitiv vorbei. Moderne Hacker nutzen komplexe Malware und Botnetze, um möglichst viele Unternehmen und Netzwerke gleichzeitig anzugreifen. Sobald Rechner Ihres Unternehmens mit dem Internet verbunden sind, sind Sie potenziell gefährdet. Niemand ist Ziel, aber jeder kann zum Opfer werden.
- **Ransomware** ist und bleibt eine ernstzunehmende Gefahr für Unternehmen. Laut einer Studie von Datto wurden im vergangenen Jahr rund 5 % aller KMU weltweit Opfer von Ransomware-Angriffen. 35 % der Managed Service Provider (MSP) berichten, dass 15 % der betroffenen KMU trotz Zahlung des Lösegelds ihre Daten nicht zurückerhielten.

- **Crime-as-a-Service (CaaS)** wird mit Verbesserung der Schadsoftware-Technologien immer beliebter. Kriminelle Gruppen erschließen neue Märkte und weiten ihre Aktivitäten weltweit aus. Angriffskampagnen werden immer umfassender – und entsprechend die Schäden. Selbst technisch unbedarfte Kriminelle sind durch „Dienstleistungen" wie Ransomware-as-a-Service oder Websites wie nulled.to in der Lage, IT-Infrastrukturen anzugreifen.
- Das **Internet der Dinge** (Internet of Things, IoT) soll das Leben seiner Nutzer komfortabler machen – birgt aber teils erhebliche Risiken, auch für Unternehmen. Schlecht produzierte oder konfigurierte IoT-Geräte sind willkommenes Fressen für Kriminelle. Sind Geräte mobil, verlassen mit ihnen zudem auch große Mengen potenziell sensibler Daten das Unternehmen.
- Dank **Cloud Computing** können auch kleinere Unternehmen bei den „großen Fischen" mitschwimmen. Über die Cloud können KMU leistungsstarke Rechner nutzen, ohne selbst große Investitionen in Hardware und Personal leisten zu müssen. Dem britischen Cloud-Anbieter BCSG zufolge nutzen bereits etwa zwei Drittel der kleinen und mittelständischen Unternehmen durchschnittlich drei cloudbasierte Software-as-a-Service (SaaS)-Anwendungen. Typische SaaS-Anwendungen für KMU sind dabei das Customer Relationship Management (CRM), webbasierte Kooperationstools für Mitarbeiter, die Speicherung größerer Datenmengen oder sensibler Daten, Online-Marketing, Vertragsmanagement- und SCM (Supply Chain Management)-Software. Grundsätzlich ist das Auslagern von Daten in die Cloud natürlich sicherer als die Ablage auf lokalen Rechnern. Nichtsdestotrotz befreit es die Unternehmen nicht von der Pflicht, ihren Cloud-Anbieter auf Herz und Nieren zu prüfen und sicherzustellen, dass dieser datenschutzkonform handelt (insbesondere in Bezug auf die DSGVO) und entsprechende Service-Level-Agreements (SLAs) zu vereinbaren. Zusätzlich muss sichergestellt sein, dass Accounts und Zugangsdaten effizient verwaltet werden, die Authentifizierung sicher ist und die Server korrekt konfiguriert und betrieben sowie regelmäßig gewartet werden (bei Infrastructure-as-a-Service bzw. IaaS).
- Jedes Unternehmen, egal wie klein, ist Teil der **Supply Chain**. Bedenken Sie, dass durch erfolgreiche Angriffe auf vor- oder nachgeschaltete Partner in der Lieferkette auch ihre Daten potenziell gefährdet sind.
- **Verordnungen** erhöhen den Ressourcenaufwand für Unternehmen erheblich. (Details dazu finden sich weiter unten in diesem Kapitel.) Während Unternehmen damit beschäftigt sind, die gesetzlichen

Vorgaben zu erfüllen, kann es passieren, dass andere, ebenso wichtige Sicherheitsinitiativen nicht die nötige Aufmerksamkeit bekommen.

Besonders für kleine und mittelständische Unternehmen sind all diese Entwicklungen natürlich schlechte Nachrichten. Kleinere Betriebe sind nicht selten leichte Beute für Cyberkriminelle, da sie über geringere finanzielle Ressourcen und generell weniger Sicherheitsmechanismen als große Unternehmen verfügen (siehe Abbildung 1-1). Doch nicht nur Cyberkriminelle richten Schaden an: Auch unbeabsichtigte Sicherheitsverstöße durch Mitarbeiter sind ein Problem.

Wie das Information Security Forum (ISF) feststellt, wird die Zunahme von Datenschutzvorfällen und die größere Menge betroffener Datensätze je Fall zukünftig die Kosten für Unternehmen jeder Größe in die Höhe treiben.

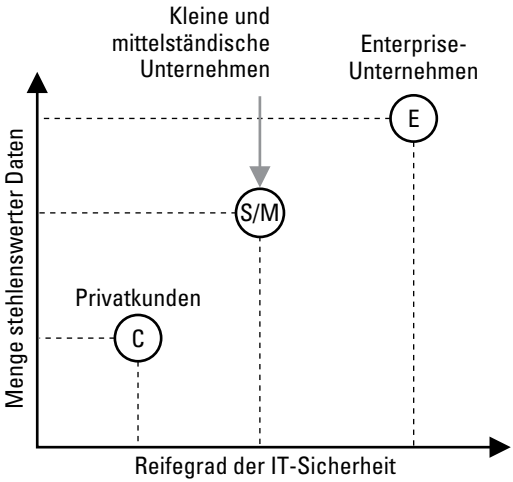

ABBILDUNG 1-1: KMU sind attraktivere Ziele als einfache Endnutzer, Angriffe haben häufig gravierendere Auswirkungen als Attacken auf große Unternehmen.

Bisherige Vorfälle

Natürlich lösen Datenlecks bei großen Unternehmen, vor allem solchen, die mit sensiblen Daten arbeiten, viel größeren Wirbel aus als Angriffe auf die Firma von Lieschen Müller mit zehn Angestellten. Dabei sind Datenschutzvorfälle in KMU keineswegs besonders selten oder weniger gravierend in ihren Auswirkungen. Bedenkt man, wie viele kleine und mittelständische Unternehmen es gibt und wie begrenzt deren Budget und andere Ressourcen sind, wird schnell klar,

dass die Auswirkungen eines Angriffs für den weiteren Unternehmensverlauf äußerst dramatisch sein können.

ERINNERUNG

Kleine Unternehmen mit weniger als 50 Mitarbeitern sowie Klein- und Heimbüros sind für die Medien nicht so spannend wie große Unternehmen. Ihr Risiko, von einem Cyberangriff oder einem Datenleck betroffen zu sein, ist deshalb aber keineswegs geringer.

Hier einige Beispiele für Datenschutzvorfälle in KMU weltweit:

- **Obike:** Im Dezember 2017 wurde bekannt, dass Obike, ein in Singapur ansässiges Unternehmen mit Bike-Sharing-Services in mehreren Städten im asiatisch-pazifischen Raum, in Europa und in Großbritannien, bereits im Juni 2017 von einem Datenleck betroffen gewesen war. Angreifer erhielten Zugriff auf sensible Kundeninformationen wie Namen, Kontakte, Profilfotos und Adressen.
- **TIO Networks USA:** TIO Networks ist ein kanadischer Anbieter von Zahlungsdiensten, der Ende 2017 von PayPal gekauft wurde. Ebenfalls im Dezember 2017 wurde bekannt, dass das Unternehmen Opfer einer Attacke geworden war. Persönliche und Finanzdaten von etwa 8.000 Kunden der Stadtwerke von Tallahassee, Florida, waren in unbefugte Hände gelangt.
- **Longs Peak Family Practice:** Im November 2017 entdeckte die Longs Peak Family Practice, eine im US-amerikanischen Colorado ansässige Privatklinik, ein Datenleck, durch das mutmaßlich Namen, Geburtsdaten, Telefonnummern, E-Mail-Adressen, Sozialversicherungsnummern, Führerscheinnummern, Versicherungsdaten und andere sensible Informationen von Patienten nach außen gelangt waren.
- **Royal National Institute of Blind People (RNIB):** Im November 2017 war das britische RNIB von einem Datenschutzvorfall betroffen, dem die Bankdaten und Kreditkarteninformationen von 817 Kunden des Online-Shops der Wohltätigkeitsorganisation zum Opfer fielen.
- **Chilton Medical Center:** Im Oktober 2017 entdeckte das Chilton Medical Center im US-Bundesstaat New Jersey, dass ein ehemaliger Mitarbeiter eine gestohlene Festplatte mit Gesundheitsdaten von über 4.600 Patienten verkauft hatte.

ACHTUNG

Dem 2017 von Verizon erstellten *Data Breach Investigations Report* (DBIR) zufolge handelt es sich bei 60 % der Datenschutzvorfälle um Datendiebstahl durch (ehemalige) Mitarbeiter und andere Insider.

- **London Bridge Plastic Surgery and Aesthetic Centre (LBPS):** Im Oktober 2017 wurde bekannt, dass das LBPS einem Cyberangriff zum Opfer gefallen war. Es ist davon auszugehen, dass Unbefugte umfangreichen Zugriff auf sensible Patientendaten und -bilder hatten.
- **Colorado Center for Reproductive Medicine (CCRM):** Ebenfalls im Oktober 2017 wurde das CCRM Minneapolis (US-Bundesstaat Minnesota) Opfer eines Ransomware-Angriffs. Die Angreifer erhielten vermutlich Zugriff auf Gesundheitsdaten von fast 3.300 Patienten.
- **Heritage Valley Health Systems:** Im Juni 2017 wurde Heritage Valley Health Systems, ein Gesundheitsnetzwerk, das zwei Krankenhäuser und zahlreiche Akut-, Ambulanz- und Zusatzpflegedienste im Westen des US-Bundesstaates Pennsylvania verwaltet, Opfer eines umfassenden Ransomware-Angriffs.

Gesetzliche Vorgaben

Weltweit sind Hunderte unterschiedliche Vorschriften zur Informationssicherheit und zum Datenschutz in Kraft. Unabhängig von der Größe wird es für Unternehmen immer schwieriger, all diesen Anforderungen gerecht zu werden. Zur Veranschaulichung hier nur einige Vorschriften und Normen:

- **EU-Datenschutz-Grundverordnung (DSGVO):** Gilt für alle Unternehmen, die mit EU-Bürgern Geschäfte machen. Hiermit soll der Datenschutz von EU-Bürgern systematisch geschützt werden. Regelt auch den Export personenbezogener Daten aus der EU.
- **Schweizer Bundesgesetz über den Datenschutz (DSG):** Erst kürzlich wurde in der Schweiz das Bundesgesetz über den Datenschutz (DSG) von 1992 aktualisiert, um die Konformität mit den Anforderungen der DSGVO sicherzustellen. Hiermit werden die bestehenden schweizerischen Datenschutzgesetze modernisiert, um den durch die Europäische Kommission erteilten Angemessenheitsbeschluss nicht in Frage zu stellen. Dieser sorgt dafür, dass – ähnlich wie andere Güter – Daten aus der EU ungehindert in die Schweiz fließen können und umgekehrt. Die Datenschutzgesetze der EU-Staaten wurden zum Inkrafttreten der DSGVO ähnlich überarbeitet.
- **South Africa Protection of Personal Information (PoPI) Act:** Stellt sicher, dass südafrikanische Unternehmen personenbezogene Daten verantwortungsbewusst erfassen, verarbeiten,

speichern und weitergeben. Einzelpersonen werden als rechtmäßige Eigentümer ihrer personenbezogenen Daten behandelt und haben entsprechende Schutz- und Kontrollrechte inne.

- **US Health Insurance Portability and Accountability Act (HIPAA):** Gesetz des US-Department of Health & Human Services für alle Unternehmen, die sensible Gesundheitsdaten verarbeiten oder speichern. Dient unter anderem dem Schutz von vertraulichen Patientendaten.
- **Canada Personal Information Protection and Electronic Documents Act (PIPEDA):** Verordnung für Unternehmen, die mit kanadischen Bürgern Geschäfte abschließen. Dient dem Schutz der personenbezogenen Daten kanadischer Bürger.
- **International Organisation of Standardisation/International Electrotechnical Commission (ISO/IEC), Normenfamilie 27000:** International anerkannte Normen für Informationssicherheit: Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001), Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002), Informationstechnik - Sicherheitsverfahren - Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste (ISO/IEC 27017) und Informationstechnik - Sicherheitsverfahren - Anwendungsregel für den Schutz von personenbezogenen Daten (PII) in Public Clouds, die derartige Daten verarbeiten (ISO/IEC 27018).
- **Payment Card Industry Data Security Standard (PCI-DSS):** Gilt für jedes Unternehmen, das Kartenzahlungen akzeptiert, verarbeitet oder speichert (z. B. Kredit- und EC-Karten).

Diese und andere Verordnungen sollen gewährleisten, dass die Unternehmen ausreichende Vorkehrungen zum Schutz sensibler Daten, z.B. Kundendaten, treffen. Leider ist die Umsetzung oft komplex und kostspielig. Gleichzeitig sind die Anforderungen wenig konkret. Unternehmen sind froh, wenn ihre Ressourcen ausreichen, um die Vorschriften möglichst genau einzuhalten. Für eigene Strategien zu Datenschutz und Informationssicherheit fehlen oftmals Zeit und Geld.

ERINNERUNG

Nur weil ein Unternehmen Gesetze und Vorschriften zum Thema Datenschutz genau einhält, heißt das nicht zwangsläufig, dass es auch wirklich sicher ist. Umgekehrt kann ein ausreichend gesichertes Unternehmen datenschutzrechtliche Regelungen (unbeabsichtigt) missachten.

IN FÜNF SCHRITTEN DSGVO-KONFORM – EIN LEITFADEN FÜR KMU –

Die DSGVO dient dem Schutz der personenbezogenen Daten von EU-Bürgern und gibt Einzelpersonen umfassendere Kontrollmöglichkeiten über ihre personenbezogenen Daten. So können Einzelpersonen Unternehmen zum Beispiel auffordern:

- eine Kopie ihrer Daten in einem strukturierten, gebräuchlichen und maschinenlesbaren Format bereitzustellen,
- ihre Daten einem anderen Verantwortlichen zu übermitteln („Recht auf Datenübertragbarkeit"),
- ihre Daten zu löschen („Recht auf Vergessenwerden").

Zusätzlich verschärft die DSGVO bestehende Bestimmungen zu Einwilligung, Meldung von Datenlecks, Folgenabschätzungen sowie zum „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen". Eine Verletzung der DSGVO kann zu Strafen in Höhe von bis zu 4 % des weltweiten Jahresumsatzes eines Unternehmens bzw. von bis zu 20 Mio. Euro führen – je nachdem, welcher Betrag höher ist.

Die DSGVO schlägt eine Reihe an technischen Maßnahmen zur Umsetzung der Datenschutzvorgaben vor. Unter anderem:

- Die Pseudonymisierung oder Verschlüsselung personenbezogener Daten,
- die Sicherstellung, dass die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten fortlaufend gewährleistet werden können,
- die Sicherstellung, dass die Verfügbarkeit personenbezogener Daten und der Zugang zu diesen Daten im Fall von physischen oder technischen Zwischenfällen schnell wiederherzustellen sind,
- Verfahren zur regelmäßigen Prüfung, Beurteilung und Bewertung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der sicheren Verarbeitung personenbezogener Daten.

(Fortsetzung auf der nächsten Seite)

(Fortsetzung von vorheriger Seite)

Die folgenden fünf Schritte sollen Ihnen helfen, die DSGVO-Konformität Ihres Unternehmens zu gewährleisten:

- **Dokumentieren und bewerten Sie, wie Sie mit Daten umgehen.** Das gründliche Verständnis dessen ist Grundlage aller weiteren Maßnahmen. Bisher waren allein die direkten Datenverantwortlichen für die Einhaltung der Datenschutzpflichten zuständig. Die DSGVO ändert das und macht nun auch Auftragsverarbeiter von Daten verantwortlich für die Einhaltung der Regelungen. Für Sie heißt das, dass Sie zunächst entscheiden müssen, in welcher Rolle Sie agieren. Sind Sie Datenverantwortlicher oder Datenverarbeiter? Oder beides? Zugleich sollten Sie in Erfahrung bringen, wo die Daten gespeichert sind. Nur so können Sie sicherstellen, dass die Speicherorte sicher sind und dass die abgelegten Daten nur kontrolliert weitergegeben werden.
- **Lernen Sie aus Fehlern anderer.** Setzen Sie sich mit vergangenen Datenlecks in anderen Unternehmen auseinander, um zu erfahren, wie Sie sich vor zukünftigen Vorfällen schützen und angemessen reagieren können. Fragen Sie sich vor allem, ob die damals unternommenen Schritte den aktuellen DSGVO-Bestimmungen entsprechen würden. So müssen jetzt beispielsweise Datenschutzvorfälle innerhalb von 72 Stunden gemeldet werden. Diese Meldung muss unter anderem Informationen zur Schwere des Angriffs enthalten. Kommt Ihr Unternehmen dieser Verpflichtung nicht nach, kann das schwerwiegende Konsequenzen in Form von finanziellen Strafen nach sich ziehen. Aktualisieren bzw. erstellen Sie einen Incident Response Plan und überprüfen Sie ihn regelmäßig auf Wirksamkeit. Nur so können Sie sicherstellen, dass Ihr Unternehmen DSGVO-konform handelt.
- **Ernennen Sie einen Datenschutzbeauftragten** bzw. eine Person mit formaler Verantwortung für den Schutz von Daten im Unternehmen. Für Unternehmen mit großem Budget kein Problem. Verfügen Unternehmen allerdings aufgrund ihrer geringeren Größe über weniger finanzielle Mittel, wirken die zusätzlichen Kosten, die eine solche Maßnahme mit sich bringt, verständlicherweise abschreckend. Stellt man diese Kosten jedoch den möglichen Strafen gegenüber, erscheinen sie schon wesentlich weniger massiv. Ein Datenschutzbeauftragter muss auch nicht zwangsläufig in Vollzeit für diese Aufgabe eingestellt sein. Der Datenschutzbeauftragte arbeitet selbstständig, untersteht der obersten Managementebene und hat die Aufgabe, die Umsetzung der DSGVO-Anforderungen zu

unterstützen. Die Einrichtung eines verantwortlichen Postens sorgt so dafür, dass Ihr Unternehmen nicht nur DSGVO-konform, sondern zugleich in der Lage ist, Datenschutzvorfälle effizient zu bearbeiten.

- **Schulen Sie sich selbst und Ihre Mitarbeiter zu den Vorgaben.** Besonderes Augenmerk sollte dem Hauptziel der Stärkung des „Rechts auf Vergessenwerden" gelten. Unternehmen benötigen von Einzelpersonen vor der Verarbeitung ihrer Daten eine „eindeutige bestätigende Handlung". Nur durch umfassendes Verständnis der geltenden Regelungen können Sie sie in Ihrem Unternehmen möglichst reibungslos umsetzen.
- **Machen Sie sich mit der für Ihr Unternehmen zuständigen Aufsichtsbehörde vertraut.** Wer für Sie zuständig ist und beispielsweise Beschwerden gegen Ihr Unternehmen bearbeitet, hängt vom Sitz Ihres Unternehmens ab und nicht davon, wo sich die Beschwerde führende Person befindet. Das kann für international agierende Unternehmen oder für Unternehmen mit Niederlassungen in verschiedenen Ländern der Erde unerwarteten Aufwand mit sich bringen. Zusätzlich können Verordnungen einzelner Länder sogar über die DSGVO hinausgehen. Diese müssen natürlich ebenso befolgt werden.

Weitere Informationen zur DSGVO und zu Maßnahmen für die Einhaltung der DSGVO in Ihrem Unternehmen finden Sie auf `https://www.eset.com/de/dsgvo/`.

INHALT DIESES KAPITELS

Kapitel 2
Erste Schritte in Richtung sichere Daten

In diesem Kapitel erfahren Sie alles über grundlegende Datenschutztechnologien, Möglichkeiten zur Umsetzung vor Ort im Unternehmen und in der Cloud sowie zu Anbietern von Managed Security Services und Outsourcing-Optionen.

Grundlagen des Datenschutzes in Unternehmen

Die Absicherung sensibler Kundendaten ist eine zentrale Verpflichtung für alle Unternehmen – egal wie klein.

Der Begriff Daten- und Informationsschutz beschreibt die Gesamtheit aller administrativen, logistischen und technischen Kontrollen zum Schutz sensibler Daten und Informationen. Das „CIA"-Prinzip (Confidentiality, Integrity, Availability) wird dabei gern verwendet, um die Entwicklung und Umsetzung eines Rahmenwerks für die Informationssicherheit in einem Unternehmen grundlegend zu regeln (siehe Abbildung 2-1):

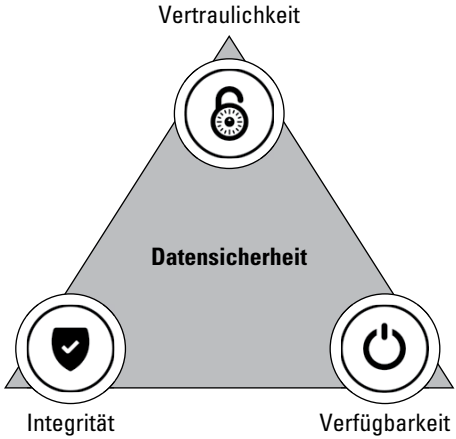

ABBILDUNG 2-1: Das CIA-Prinzip

- **Confidentiality (Vertraulichkeit)** verhindert den unautorisierten Zugriff auf und die unerlaubte Nutzung, Offenlegung, Ansicht oder Erfassung von Daten.
- **Integrität** verhindert die unautorisierte und/oder missbräuchliche Modifikation von Daten.
- **Verfügbarkeit** gewährleistet den zuverlässigen und zeitnahen Zugang zu Daten für autorisierte Benutzer und verhindert eine unerlaubte Beeinträchtigung oder Löschung von Daten.

Um zum Beispiel die **Vertraulichkeit** sensibler Daten zu gewährleisten, definieren verschiedene Richtlinien, wer innerhalb eines Unternehmens Zugang zu bestimmten Daten hat, zu welchem Zweck dieser Zugang erfolgt und was die betreffenden Personen mit diesen Daten tun dürfen. Methoden zur Gewährleistung der Vertraulichkeit umfassen das Identitäts- und Zugriffsmanagement, Verschlüsselungslösungen sowie Lösungen zur Vermeidung von Datenlecks.

Zur Sicherstellung der **Datenintegrität** lassen sich technische Lösungen wie Prüfsummen und Dateneingaben in Formularen und Datenbanken einsetzen. Digitale Signaturen und Hashing stellen die Authentizität von Daten mithilfe von Verschlüsselung sicher. Hiermit kann auch dafür gesorgt werden, dass die Daten nicht verändert werden können. Schließlich schützen Anti-Malware-Programme die Integrität der Daten (und teilweise ihre Vertraulichkeit und Verfügbarkeit).

Um die **Verfügbarkeit** von Daten vor versehentlicher (z. B. Löschung) oder vorsätzlicher (z. B. Ransomware-Angriff) Zerstörung zu schützen,

werden Backup- und Wiederherstellungssysteme sowie Richtlinien für Backups und Speicherung implementiert. Weitere Informationen zu Technologien zum Datenschutz finden Sie in Kapitel 4.

Dabei sind Unternehmen nicht nur in der Pflicht, die Vertraulichkeit, Integrität und Verfügbarkeit der von ihnen verarbeiteten Daten sicherzustellen. Sie haben auch dafür zu sorgen, dass die Systeme und Anwendungen, die diese Daten verarbeiten und speichern, den CIA-Anforderungen entsprechen.

Ein sogenannter risikobasierter Ansatz ermöglicht Unternehmen dabei, geeignete Kontrollen zur Behebung von Schwachstellen und zum Erreichen eines akzeptablen Risikoniveaus in Bezug auf spezifische Bedrohungen zu implementieren. Je höher das Risiko für bestimmte Daten ist, desto mehr und effizientere Schutzmaßnahmen sind nötig.

Das Management von Sicherheitsrisiken sollte in vier zentralen Phasen erfolgen (siehe auch Abbildung 2-2):

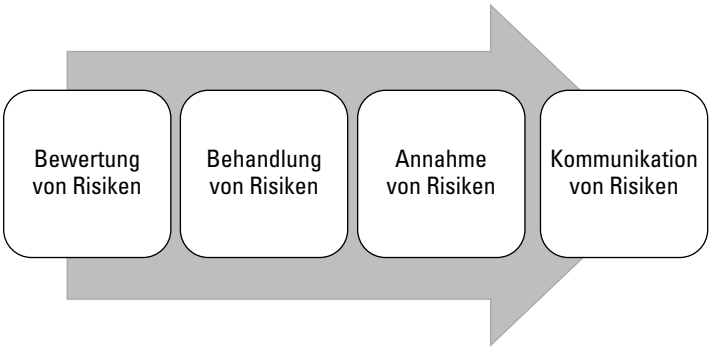

ABBILDUNG 2-2: Ein einfacher Risikomanagementprozess

- **Risikobewertung:** Es stehen viele verschiedene Methoden zur Risikobewertung zur Verfügung, die jeweils unterschiedlich umfassend sind und entsprechend unterschiedlichen Aufwand verursachen. Die grundlegenden Prozesse sind:
  - *Identifikation von Vermögenswerten:* Identifizieren Sie alle Vermögenswerte im Unternehmen (sowohl materielle als auch immaterielle), die geschützt werden müssen. Zur Bewertung gehört auch die Bestimmung der quantitativen (Kosten oder Umsatzbeiträge) und/oder qualitativen Werte (relative Bedeutung).
  - *Gefahrenanalyse:* Definieren Sie mögliche nachteilige natürliche und/oder vom Menschen verursachte Umstände oder

Ereignisse. Dazu gehören auch mögliche Folgen sowie die Wahrscheinlichkeit und Häufigkeit ihres Eintretens.

- *Bewertung von Schwachstellen:* Ermitteln Sie fehlende oder schwache Sicherheitsmaßnahmen und/oder Kontrollmechanismen, die einzelne Gefahren erhöhen und die damit verbundenen Kosten, Eintrittswahrscheinlichkeiten oder Häufigkeiten steigern.

- **Behandlung von Risiken:** Die Risikobewertung liefert die Ausgangsbasis von Managemententscheidungen für Reaktionspläne. Dazu zählen:
  - *Eindämmen von Risiken:* Umsetzung von Richtlinien, Kontrollmechanismen und/oder anderen Maßnahmen, die die Auswirkungen oder die Wahrscheinlichkeit einer Gefahr für einen Vermögenswert verringern sollen.
  - *Übertragung von Risiken:* Übertragen Sie das potenzielle Risiko auf Dritte, z. B. eine Versicherung, einen Dienstleister oder sonstige Externe, die explizit einwilligen, das Risiko zu übernehmen.
  - *Vermeidung von Risiken:* Beseitigen Sie das Risiko komplett. Das kann zum Beispiel bewerkstelligt werden, indem der Vermögenswert verkauft oder modernisiert wird oder indem man die Tätigkeit einstellt, die das Risiko verursacht.
- **Annahme von Risiken:** Hierbei handelt es sich um die formelle Genehmigung der Maßnahmen zur Risikobehandlung durch das Management und die Annahme eines Restrisikos, das nicht weiter gemildert, übertragen oder vermieden werden kann.
- **Kommunikation von Risiken:** Interessengruppen müssen über alle getroffenen Entscheidungen zur Risikobehandlung und/oder Annahme von Risiken informiert werden. Dazu gehört auch die Kommunikation der individuellen Rollen und Verantwortlichkeiten in Bezug auf spezifische Risiken.

Umsetzung vor Ort und in der Cloud

Unternehmen können heute aus einer Vielzahl von technischen Lösungen für den Schutz von Daten wählen. Sei es direkt vor Ort im Unternehmen, in der Cloud oder als Mischform, bei der sich einige Ressourcen lokal vor Ort und andere in einer Cloud befinden.

Bis vor nicht allzu langer Zeit sah das noch anders aus: Unternehmen konnten Datenschutz-Lösungen nur bei sich vor Ort umsetzen. Selbst für kleinste Unternehmen bedeutete das, kostspielige Server

anschaffen zu müssen, die dann irgendwo in der letzten Ecke einer überfüllten Abstellkammer landeten. Für den Fall der Fälle war „natürlich“ eine Sprinkleranlage an der Decke angebracht.

Für die eigentlich notwendige dauerhafte Administration und Wartung musste zusätzliches oder externes Personal organisiert werden. Doch nicht nur die Server bedurften jeder Menge Arbeit. Irgendjemand musste ja die unzähligen Router, Switches und Kabel organisieren und an der richtigen Stelle anbringen. Dabei galt das interne Netzwerk per se als vertrauenswürdig und wurde durch mindestens eine Firewall vor dem Internet „da draußen“ geschützt.

Keine Frage: Für viele Unternehmen ist die lokale Verwaltung von Servern oder Rechenzentren noch immer eine äußerst praktikable Lösung. Mit steigender Zuverlässigkeit und Stabilität von Technologien für Virtualisierung, Netzwerkanbindung und Cloud Computing während der letzten Jahre ist es jedoch für Unternehmen ebenso attraktiv geworden, IT-Ressourcen ganz oder teilweise in die Cloud zu verlagern.

Mittlerweile bietet fast jeder Technologie-Anbieter auf dem Markt Cloud-Lösungen an. Doch was genau ist das eigentlich, „diese Cloud“? Die Erläuterungen der Anbieter zum Thema sind leider oft, bewusst oder unbewusst, schwammig gehalten. Um Ihnen hier besseren Einblick zu geben, wollen wir einige wichtige Elemente der Cloud gemäß der herstellerunabhängigen Definition des US-amerikanischen National Institute of Standards and Technology (NIST) genauer erklären:

Das NIST nennt drei Servicemodelle für Cloud Computing:

- **Software-as-a-Service (SaaS):** Dem Kunden wird eine Anwendung zur Verfügung gestellt, die in der Cloud läuft. Die Anwendung kann dabei über mehrere Client-Geräte und Schnittstellen erreicht werden. Dabei weiß der Kunde nichts von der zugrundeliegenden Cloud-Infrastruktur. Das muss er aber auch nicht, da er die Systeme weder verwaltet noch steuert. Er kann aber Zugriff auf eingeschränkte und benutzerspezifische Anwendungseinstellungen erhalten. Für die verarbeiteten Daten und deren Schutz bleibt der Cloud-Anbieter verantwortlich.
- **Platform-as-a-Service (PaaS):** Kunden können selbstständig Anwendungen in der Cloud-Infrastruktur einrichten und nutzen. Dabei hat der Kunde weder Kenntnis von der zugrundeliegenden Cloud-Infrastruktur noch ist er mit deren Verwaltung oder Steuerung betraut. Der Kunde erhält Kontrolle über die eingerichteten Anwendungen und eingeschränkte Möglichkeiten zur Konfiguration der Host-Umgebung. Der Cloud-Anbieter ist im Besitz der

eingerichteten Anwendungen und der darin verarbeiteten Daten. Sowohl Cloud-Anbieter als auch Kunde sind für die Sicherheit der Daten verantwortlich.

- **Infrastructure-as-a-Service (IaaS):** Kunden haben die Möglichkeit, bereitgestellte Verarbeitungs-, Speicher-, Netzwerk- und andere Rechenressourcen zu nutzen sowie Betriebssysteme und Anwendungen einzurichten und zu nutzen. Der Kunde hat dabei weder Kenntnis von der zugrundeliegenden Cloud-Infrastruktur noch ist er mit deren Verwaltung oder Steuerung betraut. Der Kunde erhält Kontrolle über Betriebssysteme, Speicher, Anwendungen und einige Netzwerkkomponenten und ist für die Sicherheit der darin verarbeiteten Daten verantwortlich.

TIPP

Die verschiedenen Cloud-Modelle bringen unterschiedliche Implikationen für Kunden mit sich. Beispielsweise umfasst das SaaS-Angebot von Cloud-Providern wie Microsoft 365 und SalesForce Angebote zur Bereitstellung einer sicheren Infrastruktur, die Datensicherheit und Authentifizierung unterliegen allerdings weiterhin der Verantwortung des Kunden. Vor allem bei IaaS- und PaaS-Modellen teilen sich Provider und Nutzer des Cloud-Dienstes die Verantwortlichkeiten – auch in Bezug auf den Schutz von Daten. Zusätzlich gibt es gemeinsame Maßnahmen, deren Umsetzung von beiden Seiten sichergestellt werden muss. Sowohl Anbieter als auch Nutzer müssen die betriebenen Ressourcen z. B. fortwährend nach Malware durchsuchen und mithilfe von Firewalls schützen. Oftmals wird von der Absicherung einzelner Anwendungen und Infrastrukturen abgesehen und stattdessen der Fokus auf sichere Authentifizierung und Datenintegrität gelegt.

Laut NIST gibt es vier grundlegende Cloud Computing-Modelle:

- **Öffentlich:** Infrastruktur zur Nutzung von Cloud-Diensten für jedermann. Sie befindet sich im Besitz von Dritten und wird auch von diesen verwaltet und betrieben; ihr Standort ist der des Cloud-Providers.
- **Privat:** eine von einem einzelnen Unternehmen exklusiv genutzte Cloud-Infrastruktur. Sie kann sich im Besitz des Unternehmens oder von Dritten (bzw. einer Kombination aus beidem) befinden und von diesen verwaltet und betrieben werden und befindet sich entweder am Standort des Unternehmens oder an einem externen Standort.
- **Hybrid:** eine Cloud-Infrastruktur aus zwei oder mehr Deployment-Modellen, die durch standardisierte Schnittstellen verbunden sind und so die Übertragbarkeit von Daten und Anwendungen ermöglichen.

- **Gruppe (selten):** eine von einer Gruppe von Unternehmen exklusiv genutzte Cloud-Infrastruktur.

Wie viele Änderungen an der Infrastruktur beginnt auch der Weg in die Cloud mit nicht produktionsbezogenen, unkritischen Anwendungen und Systemen, z. B. einer Entwicklungsumgebung oder Backup-Systemen. Viele Unternehmen verlagern schrittweise auch bestehende Anwendungen in die Cloud oder richten ganz und gar neue Anwendungen in der Cloud ein. Zusätzlich gibt es Unternehmen, die – getreu dem Motto „Cloud first" – so viele Komponenten ihrer IT-Umgebung in die Cloud schieben wie möglich und allein für die Cloud gedachte Anwendungen für ihre Kunden entwickeln.

Die Nutzung der Cloud bietet Unternehmen dabei zentrale Vorteile:

- **Höhere Agilität und Reaktionsfähigkeit:** Der Zugriff auf Anwendungen und Daten ist von überall, jederzeit und von jedem Gerät aus möglich.
- **Schnellere Markteinführung:** Die Entwicklung und Bereitstellung von Produkten und Dienstleistungen ist in der Cloud mit PaaS oder IaaS-Ressourcen noch schneller und unkomplizierter möglich.
- **Skalierbarkeit nach Bedarf:** Zusätzliche Softwarelizenzen und/oder Infrastrukturen können bei Bedarf bereitgestellt und zurückgezogen werden. So werden vor allem schnell wachsende und zyklisch agierende Unternehmen unterstützt, die Marktveränderungen oder das Wachstum des Unternehmens nur begrenzt vorhersagen können.
- **Mehr Stabilität:** Die Cloud-Infrastruktur läuft im Allgemeinen in robusten Rechenzentren, die auf Leistung, Stabilität und Zuverlässigkeit ausgelegt sind und von entsprechenden IT-Teams verwaltet werden.
- **Geringere Investitionskosten:** Sie können Ihre gesamte IT-Infrastruktur in der Cloud bereitstellen und auf teure Investitionen verzichten. Die Cloud bietet kalkulierbare, „bedarfsgerechte" Services auf Basis eines Abonnements. Der IT-Bedarf kann so als Teil der laufenden Betriebskosten budgetiert werden.

ACHTUNG

Nur weil Sie Ihre Daten und Anwendungen in die Cloud verlagern, löst sich Ihre Verantwortung für deren Sicherheit nicht in Wohlgefallen auf oder geht auf jemand anderen über. Obwohl der Provider des Cloud-Services für bestimmte Aspekte der Umgebung verantwortlich ist, bleibt die Verantwortlichkeit für die Datensicherheit allein bei Ihnen. Provider von Cloud-Services bezeichnen das meist als „Modell mit

geteilter Verantwortung“, wobei klar zwischen Ihren Verantwortlichkeiten und den Aufgaben des Providers unterschieden wird. Eins ist jedoch immer sicher: Der Provider trägt niemals die Verantwortung für die Sicherheit Ihrer Daten!

Auswahl von Managed Services und Outsourcing

Die IT-Bedrohungslandschaft wird zunehmend komplexer, die Risiken werden immer mehr. Entsprechend ist es für Unternehmen schwierig geworden, den Herausforderungen bezüglich Sicherheit, Aktualität und Konformität zu begegnen. Vor allem kleine und mittelständische Unternehmen mit begrenzten Ressourcen und kleinen IT-Teams haben hier oft schwer zu kämpfen. Viele wenden sich deshalb an Managed Service Provider (MSP). Diese bieten folgende Vorteile:

- **Bessere Kontrolle über das IT-Budget:** Managed Service Provider bieten oft wesentlich umfangreichere Produkte und Services als KMU sie intern bereitstellen könnten. Zudem ermöglichen flexible Abrechnungsmodelle den Unternehmen finanzielle Flexibilität und die transparentere Planung von Kosten. KMU können so auch ihr IT- und Sicherheitsbudget wesentlich besser überwachen.
- **Beratung mit Kompetenz und Erfahrung:** Kleine und mittelständische Unternehmen nutzen die Kompetenz und Erfahrung des vom Managed Service Provider beschäftigten IT- und Sicherheitspersonals.
- **Marktkenntnis und Marktfokus:** Managed Service Provider sind Experten, wenn es um IT-Sicherheit geht. Entsprechend gut sind ihre Marktkenntnis und ihr Wissen um aktuelle Sicherheitslösungen und ihre Fähigkeit, perfekt zugeschnittene Lösungen zu erstellen.
- **Innovation:** Spezialisierte MSP-Sicherheitsteams können die Einführung und Implementierung innovativer Lösungen erleichtern und den Kunden helfen, mit Marktentwicklungen Schritt zu halten.
- **Keine Angst vor Veränderungen:** Managed Service Provider ermöglichen ihren Kunden, Soft- oder Hardware bedarfsgerecht hinzuzufügen oder zu entfernen; ganz ohne den aufwendigen Prozess aus Akquise, Implementierung und Wartung neuer Hardware- und Softwareressourcen.

EINE ALLIANZ FÜR DIE IT: ESET LEISTET DIGITALE RISIKOVORSORGE

Mehr als einer Million Privatkunden und 100.000 Unternehmen steht die Allianz Suisse in allen Fragen rund um Vorsorge, Vermögen und Versicherungen zur Seite. Mit einem Prämienvolumen von rund 3,6 Mrd. Franken gehört sie zu den führenden Versicherungsgesellschaften in der Schweiz. Um rund um die Uhr erreichbar zu sein, setzt die Allianz dabei auf eine Multichannel-Strategie, in der vor allem Online-Angebote eine wichtige Rolle spielen. Hierbei die sensiblen Daten ihrer Kunden umfassend zu schützen – schlussendlich das Geschäftsmodell des Versicherers – stellt hohe Anforderungen an die IT-Sicherheit des Unternehmens.

Die Aufgabe

„Der moderne, ‚hybride' Kunde nutzt in der Regel sowohl das Internetangebot wie auch die persönliche Beratung", erklärt Bruno Brundia, GroupWare – System Services Allianz Suisse. Der IT-basierte Anteil des Gesamtgeschäfts legt dabei jährlich zu. Dies setzt ein ausgefeiltes IT-Management mit sehr hoher Informationsdichte sowie Verfügbarkeit voraus. „Bei 4.500 Mailboxen und 3.800 Benutzern war eine neue Größenordnung unter der laufenden IBM Lotus Domino Umgebung erreicht. Wir brauchten mehr als eine isolierte Securitylösung mit Spartenfunktionalität", erläutert Brundia.

Das Ergebnis

Seit der Installation laufen nun die mehr als 4.000 Lizenzen der ESET Mail Security für IBM Domino auf Hochtouren. „Nach der ersten Systemprüfung hatten wir etwa 850 infizierte Objekte identifiziert", erinnert sich Christian Klein, Strategischer Einkäufer bei der Allianz Suisse. Als die Allianz Suisse die Lösung zum ersten Mal in Betrieb nahm, waren alle Datenbanken innerhalb von sieben Stunden auf Herz und Nieren geprüft. Der Kunde war begeistert: „Das war sehr schnell!" Seitdem steht die umfassende Security-Lösung der Versicherungsgesellschaft rund um die Uhr als verlässlicher Partner zur Seite.

Die vollständige Case Study finden Sie unter `https://www.eset.com/de/business/casestudies/`.

INHALT DIESES KAPITELS

- Der Risikobewertungsprozess
- Identifikation von Prozessen zur Datenverarbeitung
- Auswirkungen von Datenlecks
- Identifikation relevanter Gefahren für die Datensicherheit
- Implementierung geeigneter Kontrollen

Kapitel 3
Risikobewertung in der Data Security

Dieses Kapitel zeigt Ihnen, wie Sie Risikomanagement-Prozesse (wie in Kapitel 2 beschrieben) auf die Datensicherheit anwenden.

Der Risikobewertungsprozess

Jedes Risikomanagement beginnt mit der sogenannten Risikobewertung. Diese umfasst:

- Identifikation der Vermögenswerte (materielle und immaterielle),
- Gefahrenanalyse (einschließlich Folgen und Wahrscheinlichkeiten),
- Bewertung von Schwachstellen (fehlende oder schwache Sicherheitsmaßnahmen oder Fehlen von Kontrollmechanismen).

Eine Bewertung von Risiken für die Datensicherheit umfasst:

- Identifikation von Abläufen zur Datenverarbeitung (um zu ermitteln, wie und wo Ihre Datenbestände unternehmensintern genutzt werden),
- Ermittlung potenzieller Folgen von Datenschutzvorfällen für das Unternehmen,

- Identifikation potenzieller Gefahren und Bewertung ihrer Wahrscheinlichkeit (einschließlich Häufigkeit des Auftretens),
- Beurteilung von Risiken (um entscheiden zu können, welche Sicherheitsmaßnahmen oder Kontrollen zum Schutz der Daten umgesetzt werden).

Schritt 1: Identifikation von Prozessen zur Datenverarbeitung

Auf die im Unternehmen verwendeten Daten lassen sich verschiedene Risikoprofile anwenden. Diese beziehen sich nicht nur auf deren Inhalt, sondern auch auf die Art ihrer Nutzung im Unternehmen. Am Anfang jedes Risikobewertungsprozesses steht deshalb ein tiefgreifendes Verständnis aller Datenverarbeitungsprozesse in Ihrem Unternehmen. In kleinen und mittelständischen Unternehmen werden typischerweise folgende Datenverarbeitungsprozesse durchgeführt:

- **Personalmanagement:** Gehaltsabrechnungen, Rekrutierung und Bindung von Mitarbeitern, Aufzeichnungen von Schulungen, Disziplinarmaßnahmen und Leistungsbewertungen.
- **Kundenmanagement, Marketing und Lieferanten:** Kundendaten, Einkauf und Verkauf, Rechnungen, Adressbücher, Marketingdaten und Händlerverträge.
- **Sicherheit von Personal und physische Sicherheit:** Zugriffsprotokolle, Besucherlisten und Videoüberwachung.

Dabei sind für jeden Prozess folgende Fragen zu stellen:

- Welche personenbezogenen Daten werden verarbeitet?
- Was ist der Zweck der Verarbeitung?
- Wo findet die Verarbeitung statt?
- Wer trägt die Verantwortung für den Prozess?
- Wer hat Zugang zu den Daten?

MERKEN

Das sogenannte „Prinzip der minimalen Rechte“ stellt sicher, dass Endnutzer nur minimale Zugangsrechte erhalten, und zwar genau so viele, dass sie ihre Aufgabe bzw. Funktion erfüllen können.

Schritt 2: Ermittlung potenzieller Folgen

Im nächsten Schritt muss ermittelt werden, welche Auswirkungen ein Datenschutzvorfall haben könnte. So kann ein solcher Vorfall die Vertraulichkeit von Daten (beispielsweise durch unautorisierten Zugriff), die Integrität von Daten (beispielsweise durch unautorisierte Modifikation) oder die Verfügbarkeit von Daten (beispielsweise durch einen Ransomware-Angriff) betreffen.

MERKEN

Unternehmen sind verpflichtet, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu schützen. Im Bereich der Informationssicherheit wird dies als das CIA-Prinzip bezeichnet.

In einem typischen Risikobewertungsprozess werden die potenziellen Folgen eines bestimmten Risikos als Schaden für das Unternehmen beschrieben, z. B. die Kosten, die der Verlust oder die Zerstörung von physikalischen Vermögenswerten (Server, Kopiergeräte, Fahrzeuge usw.) mit sich bringt.

Datenschutzrisiken haben ähnliche Auswirkungen wie andere Risiken auch – teilweise sind diese aber indirekt und erhalten dadurch weniger Aufmerksamkeit. Nehmen wir z. B. Datenlecks, bei denen sensible, personenbezogene Daten in falsche Hände geraten. Direkt geschädigt ist natürlich die Einzelperson, deren Daten gefährdet oder verletzt wurden. So kann es beispielsweise passieren, dass die Identität oder Vermögenswerte der Person entwendet werden oder dass ihre Privatsphäre verletzt wird. Das Unternehmen trägt hier allerdings auch indirekte, aber nichtsdestotrotz teilweise sehr kostspielige Schäden davon, unter anderem:

- Verlust von Kunden und Umsatz,
- Markenschäden und Ansehensverlust, Bußgelder und Gerichtskosten,
- Kosten für forensische Analysen und Wiederherstellung.

TIPP

Geschäftliche Auswirkungen können als gering, mittel oder hoch eingestuft werden. Die tatsächliche Definition jeder dieser Auswirkungsstufen unterscheidet sich von Unternehmen zu Unternehmen und sollte sowohl objektive (quantitative) als auch subjektive (qualitative) Faktoren einschließen.

Schritt 3: Identifikation potenzieller Gefahren und deren Wahrscheinlichkeit

Eine Gefahr kann jedes natürliche oder von Menschen verursachte Ereignis bzw. jeder Umstand sein, der das Potenzial hat, die Vertraulichkeit, Integrität oder Verfügbarkeit von personenbezogenen oder sensiblen Daten negativ zu beeinflussen. Dies schließt Angriffe auf die IT-Sicherheit, unbeabsichtigte Verluste oder Veröffentlichungen, interne Gefahren, Schäden durch Feuer und Wasser, Erdbeben und Tsunamis, extreme Wetterbedingungen (wie Orkane oder Wirbelstürme) oder Unruhen, Arbeitskämpfe etc. mit ein. Unternehmen müssen potenzielle Gefahren für ihre datenverarbeitenden Prozesse identifizieren und die Eintrittswahrscheinlichkeit (inklusive der potenziellen Häufigkeit) jeder möglichen Gefahr in der Bewertung berücksichtigen. Kümmern Sie sich insbesondere um Gefahren für Netzwerke und technische Ressourcen (Software/Hardware) zur Datenverarbeitung, Gefahren durch entsprechende Prozesse und Vorgänge, Gefahren in Verbindung mit beteiligtem Personal und Gefahren, die sich aus der Skalierung von Prozessen ergeben.

TIPP

Jede identifizierte Gefahr lässt sich entsprechend ihrer Wahrscheinlichkeit kategorisieren: gering, mittel oder hoch. Bei der Bewertung der Eintrittswahrscheinlichkeit müssen sowohl die Wahrscheinlichkeit des Eintretens der Gefahr als auch die mögliche Häufigkeit des Eintretens über einen spezifischen Zeitraum (beispielsweise ein Jahr) berücksichtigt werden.

Schritt 4: Beurteilung des Risikos

Nach der Identifikation aller datenverarbeitenden Prozesse (und der verarbeiteten Daten), der Ermittlung der potenziellen Folgen eines Vorfalls und der Identifikation der potenziellen Gefahren sowie ihrer Eintrittswahrscheinlichkeit und ihrer potenziellen Häufigkeit folgt die Bewertung der Risiken in Verbindung mit jedem Prozess. Zugleich sollten angemessene technische Maßnahmen (siehe Kapitel 4) und organisatorische/prozessbezogene Kontrollmechanismen aufgesetzt werden. Je nach Schwere des Risikos sollten letztere (siehe Kapitel 5) über einen risikobasierten Ansatz umgesetzt werden.

Abbildung 3-1 zeigt den grundsätzlichen Ablauf und ein Beispiel zur Bewertung von Datenverarbeitungsprozessen.

Matrix zur Risikobewertung für Datenverarbeitungsprozesse				Grad des Impacts			
				Bei bestimmten Datenverarbeitungsprozessen ist eine Bewertung der möglichen Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten erforderlich (CIA-Triade). Der höchste Impact der drei bestimmt den letztendlichen Impact.			
				Gering	**Mittel**	**Hoch**	**Sehr hoch**
				Kleinere Schwierigkeiten, die problemlos überwunden werden können.	Größere Schwierigkeiten, die trotz einiger Hindernisse überwunden werden können	Größere negative Konsequenzen, die unter großen Schwierigkeiten überwunden werden können	Größere und teilweise irreversible negative Konsequenzen, die nicht überwunden werden können
Eintrittswahrscheinlichkeit	Arbeiten Sie für einzelne Datenverarbeitungsprozesse eine Liste aller potenziellen Gefahren ab und bewerten Sie deren Wahrscheinlichkeiten. Die Gesamtwahrscheinlichkeit entspricht der Summe der Werte für alle Gefahren in der Liste.	**Gering**	Die Gefahr ist sehr unwahrscheinlich	Risiko bei Datenverarbeitung: **Geringes Risiko**	Risiko bei Datenverarbeitung: **Geringes Risiko**	Risiko bei Datenverarbeitung: **Hohes Risiko**	
		Mittel	Die Gefahr ist mäßig wahrscheinlich				
		Hoch	Das Auftreten der Gefahr ist wahrscheinlich	**Geringes Risiko**			

ABBILDUNG 3-1: Matrix zur Risikobewertung

Beispiel **Datenverarbeitungsprozess: Marketing** **Verarbeitete Daten:** Kontaktinformationen (z. B. Name, Adresse, Telefonnummer, E-Mail) **Datenklassifizierung:** Personenbezogene Daten **Verarbeitungszweck:** Werbung für Güter und besondere Angebote für potenzielle Kunden **Zielgruppe**: Kunden und Leads				**Grad des Impacts** Ermittlung des Impacts: Vertraulichkeit: niedrig, Integrität: niedrig, Verfügbarkeit: niedrig. **Finaler Grad des Impacts: niedrig**			
				Gering	**Mittel**	**Hoch**	**Sehr hoch**
				Kleinere Schwierigkeiten, die problemlos überwunden werden können	Größere Schwierigkeiten, die trotz einiger Hindernisse überwunden werden können	Größere negative Konsequenzen, die unter großen Schwierigkeiten überwunden werden können	Größere und teilweise irreversible negative Konsequenzen, die nicht überwunden werden können
Eintrittswahrscheinlichkeit	Gefahren für Netzwerke und technische Ressourcen (HW, SW): mittel Gefahren für Prozesse: gering Gefahren für Personal: mittel Gefahren für Unternehmensbereich: mittel **Finale Eintrittswahrscheinlichkeit: mittel**	**Gering**	Die Gefahr ist sehr unwahrscheinlich				
		Mittel	Die Gefahr ist mäßig wahrscheinlich	**X – geringes Risiko** Verarbeitung von Marketingdaten: geringes Risiko – dem Risiko entsprechende technische und organisatorische Maßnahmen treffen			
		Hoch	Das Auftreten der Gefahr ist wahrscheinlich				

ABBILDUNG 3-1: *(Fortsetzung von vorheriger Seite).*

INHALT DIESES KAPITELS

Kapitel 4
Grundlegendes zur Datenschutztechnologie

In diesem Kapitel erklären wir Ihnen, welche Sicherheits- und Datenschutztechnologien Sie in Ihrem Unternehmen verwenden können – vom Endgerät zum Netzwerk und darüber hinaus.

Ortsunabhängiger Datenschutz

Daten sind ein zentraler Vermögenswert, müssen aber unbedingt geschützt werden, um sich nicht in ein unkalkulierbares Risiko zu verwandeln. Glücklicherweise gibt es eine Vielzahl an Technologien für den Schutz von Daten an Arbeitsplätzen (also z. B. an PCs und mobilen Geräten), im Netzwerk und am Backend (z. B. für Serverräume vor Ort oder cloudbasierte Rechenzentren). In Abbildung 4-1 sehen Sie verschiedene Sicherheitstechnologien übersichtlich dargestellt, im Verlauf werden die einzelnen Komponenten im Detail besprochen. Je nach Risikoniveau und verfügbaren Ressourcen sind unterschiedliche Varianten und Kombinationen zu wählen.

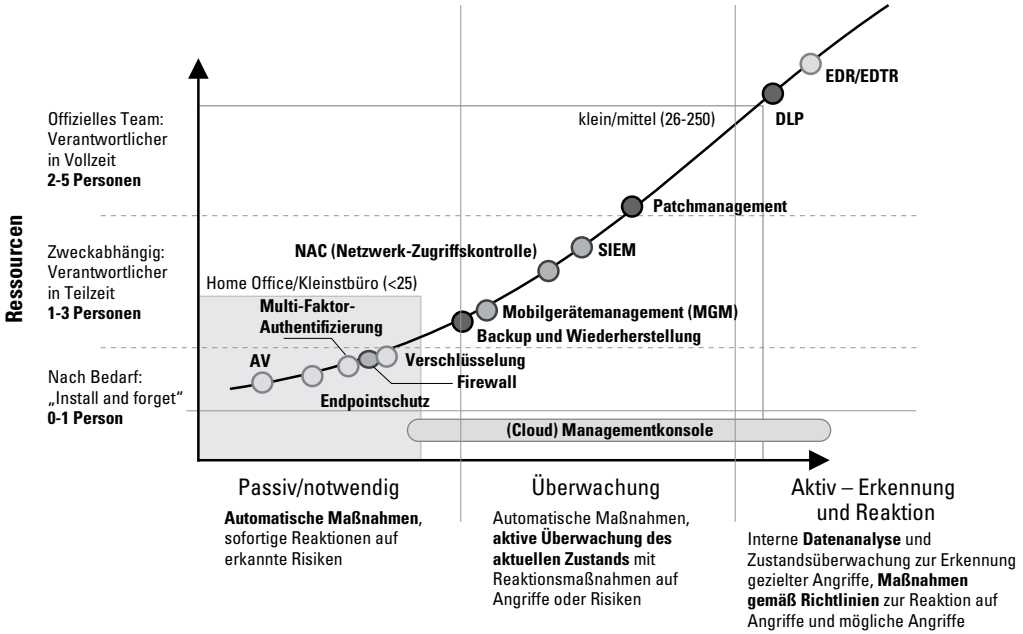

ABBILDUNG 4-1: Sicherheitstechnologien

Zusätzlich zu einer grundlegenden Virenschutz-Software sollten KMU folgende Komponenten verwenden:

- **Endgeräteschutz:** Ein Endgeräteschutz/Endpointschutz ist mehr als ein bloßer Schutz vor Viren. Eine mehrschichtige Technologie schützt vor Malware (einschließlich Viren, Würmern, Ransomware, Spyware, Trojaner, Remote Access Trojaner und Rootkits/Bootkits), Infektionen, Exploits von Schwachstellen, Netzwerkangriffen, Missbrauch durch Botnetze u.v.m. (siehe „Auswahl des Endgeräteschutzes").
- **Multi-Faktor-Authentifizierung (MFA):** Eine MFA fordert vom Nutzer zur Anmeldung am System oder in einer Anwendung zusätzlich zur Standardauthentifizierung (z. B. Benutzername und Passwort) die Angabe eines weiteren Faktors. Üblich ist hier die Verwendung eines einmaligen Codes, der an eine zuvor konfigurierte und unabhängige E-Mail-Adresse oder als Textnachricht an ein Handy oder Smartphone gesendet wird. Benutzer werden bei der Anmeldung zunächst nach ihrem Benutzernamen und Passwort gefragt. Dann werden sie aufgefordert, das Einmalpasswort einzugeben. Dieses dient der Authentifizierung einer einzelnen Sitzung und kann nur innerhalb eines eingeschränkten Zeitrahmens (beispielsweise 60 Sekunden) genutzt werden. Replay-Angriffe, bei denen der Code abgefangen und zur Authentifizierung einer weiteren Sitzung genutzt wird, werden wirkungslos. Mit der modernsten Form der Challenge-Response-MFA (z. B. in ESET Secure Authentication) können Nutzer den zweiten Faktor einfach auf dem verbundenen Smartphone bestätigen und müssen das Einmalpasswort nicht abtippen.
- **Firewalls:** Siehe weiter hinten in diesem Kapitel.
- **Verschlüsselung:** Durch Verschlüsselung werden Daten für denjenigen, der nicht den passenden Schlüssel besitzt, unbrauchbar. Dabei können sowohl Ver- als auch Entschlüsselung per Hardware (schneller) oder Software (günstiger) erfolgen. Daten auf Servern, Desktop-PCs, Laptops und mobilen Geräten lassen sich durch eine zeitweise vollständige Verschlüsselung schützen, falls das Endgerät verloren geht oder gestohlen wird. Die Verschlüsselung von Dateien, Ordnern und E-Mails ermöglicht außerdem, Daten über Arbeitsgruppen und Teams hinweg gemeinsam zu bearbeiten. Die Sicherheitsrichtlinien für jedes einzelne Endgerät können dabei zentral per Fernzugriff verwaltet werden.
- **Backup und Wiederherstellung:** Backups dienen dem Schutz von Unternehmen vor unbeabsichtigter oder böswilliger Zerstörung, Löschung oder Änderung von Daten (auch durch Ransomware-Angriffe) und sorgen dafür, dass Unternehmensprozesse auch im Katastrophenfall weiterlaufen. Systeme für Backups und zur

Datenwiederherstellung umfassen entsprechende Software und Medien, entweder vor Ort (und extern gelagert), per Fernzugriff oder in der Cloud. Sicherungskopien sollten regelmäßig geprüft werden, um zu gewährleisten, dass die Daten daraus auch wirklich wiederhergestellt werden können und dass Backups von allen notwendigen Systemen und Daten vorhanden sind.

- **Mobilgerätemanagement (Mobile Device Management, MDM):** Viele – und besonders kleinere – Unternehmen erlauben Mitarbeitern die Nutzung ihrer persönlichen Mobilgeräte für arbeitsbezogene Aufgaben. Dieser Trend wird als „Bring Your Own Device" (BYOD) bezeichnet. Unternehmen müssen allerdings gewährleisten, dass diese Geräte sicher sind und empfindliche Informationen oder Kundendaten bei Verlust oder Diebstahl oder bei anderen Datenschutzvorfällen nicht in falsche Hände geraten können. MDM-Software beinhaltet meist Funktionen für die Durchsetzung interner Vorgaben, für die Verschlüsselung, Isolation (zur Trennung von geschäftlichen Apps/Daten von persönlichen Apps/Daten) und Löschung/Verschlüsselung per Fernzugriff.
- **Vermeidung von Datenverlusten (Data Loss Prevention, DLP):** DLP-Software verhindert die versehentliche (oder mutwillige) Offenlegung bestimmter Daten wie Gesundheits- und Finanzdaten, indem sie E-Mails und Dokumente nach bestimmten Schlüsselwörtern und Datenmustern durchsucht.

ACHTUNG

Für ein effektives DLP braucht es mehr als nur Software. Es muss möglich sein, im Bedarfsfall Richtlinien zu verändern, interne und externe Vorfälle zu bewerten sowie Gegenmaßnahmen ohne größere Schwierigkeiten umzusetzen. Das bringt einen signifikanten Mehraufwand mit sich. Ein DLP ohne diese Maßnahmen ist jedoch so gut wie unwirksam.

AUSWAHL VON ENDGERÄTESCHUTZ

Wie Angreifer in der physischen Welt auch nutzen Kriminelle beim Angriff auf Ihr Netzwerk typischerweise das schwächste Glied. Entsprechend gut muss der Schutz von Geräten sein, die durch viele und potenziell unbedarfte Nutzer verwendet werden: Desktop-PCs, Mobilgeräte und Server. Für den Endpointschutz auf kostenfreie Angebote zu vertrauen, endet deshalb nicht selten in Infektionen oder Datenlecks.

Viele Anbieter von Produkten zum Schutz von Endgeräten bezeichnen sich selbst als „nächste Generation" (NextGen) der Sicherheitsanbieter und geben vor, „the next big thing" im Kampf gegen Malware zu sein. Dabei sind die Produkte nur deshalb „NextGen", weil sie eine einzige, vorgeblich neuartige Technologie nutzen. Vom Umstand abgesehen, dass Technologien wie Machine Learning keineswegs neu sind, reicht ein einziger Verteidigungsmechanismus – und mag er noch so gut sein – keineswegs aus. Ein vernünftiger Endpointschutz kombiniert daher meist mehrere, hochentwickelte Technologien wie Machine Learning, Pre-Execution Detection, Sandboxing und andere in einer Mehrschichtlösung. Sie sollten also nach einer Lösung Ausschau halten, die möglichst viele, wenn nicht alle der folgenden Mechanismen beinhaltet: Machine Learning, Pre-Execution Detection, Sandboxing ebenso wie „althergebrachte" signaturbasierte Erkennung. Diese sollte mithilfe von Echtzeitinformationen aus der Cloud möglichst aktuell gehalten werden.

Zusätzlich sollte ein Endgeräteschutz folgende Anforderungen erfüllen:

- **Geringe Installationsanforderungen.** Anti-Malware, die viel Speicherplatz auf der Festplatte oder dem Arbeitsspeicher und viel Rechenleistung erfordert, kann die Gesamtperformance von Systemen beeinträchtigen. Das führt nicht selten dazu, dass Nutzer sie genervt deaktivieren oder anderweitig umgehen.
- **Robuste Updatefunktionen.** Die Software muss den Abruf von Echtzeitinformationen ermöglichen. Einzelne Schwachstellen oder Bottlenecks (wie ein Updateserver im Netzwerk) dürfen kein Problem sein. Zur Bereitstellung von Updates und Informationen an Endgeräte wird zunehmend auf die Cloud zurückgegriffen.
- **Widerstandsfähigkeit.** Die Software muss auch dann funktionieren, wenn die Verbindung zum Netzwerk unterbrochen wird. Weiterhin muss sie selbst ausreichend gut vor Malware geschützt sein, die sie zu deaktivieren versucht.
- **Produktstabilität.** Die Software und ihr Anbieter sollten belegbare Erfolge vorweisen können in Bezug auf Sicherheit, Stabilität und Fehlerfreiheit.
- **Zentrales Management.** Zusätzlich zu einem Endpunktschutz müssen Unternehmen in der Lage sein, die korrekte Installation, Funktion und regelmäßige Aktualisierung von Software zu gewährleisten. Es muss möglich sein, Probleme per Fernzugriff zu lösen und die korrekte Funktion des Schutzes jederzeit zu bestätigen (beispielsweise durch Logs und regelmäßige Audits).

Netzwerksicherheit

Mit der Verbreitung von mobilen Geräten und Cloud Computing im Unternehmenskontext wird es zunehmend anspruchsvoller, Unternehmensnetzwerke ausreichend abzusichern. Doch gerade hier sind umfassende Sicherheitsmechanismen essenziell, sollen Daten und Informationen vor Fremdzugriff und Missbrauch geschützt werden. Zu solchen Mechanismen gehören zum Beispiel:

- **Firewalls:** Firewalls sind Grundpfeiler der Netzwerkabsicherung und stellen die wichtigste Investition dar, die ein Unternehmen hierfür tätigen kann. Einfache Firewalls enthalten dabei meist mindestens Paketfilter und überprüfen den Netzwerk-Traffic. Eine Next Generation Firewall (NGFW) bietet zusätzliche Funktionalitäten wie Malwareschutz, Inhaltsfilter, Intrusion Detection and Prevention Systeme (IDS/IPS) sowie Threat Intelligence-Komponenten. Bei einer Web Application Firewall (WAF) handelt es sich um eine Firewall, die gezielt Unternehmenswebseiten und mit dem Internet verbundene Anwendungen schützt.
- **IDS/IPS zur Abwehr von Eindringlingen:** IDS und IPS erkennen schädlichen Netzwerk-Traffic anhand vorkonfigurierter Signaturen und Regeln. Ein IDS ist dabei ein rein passives System, welches Sicherheitsteams über mögliche bereits erfolgte Angriffe informiert. Ein IPS hingegen ist ein aktives System, das gezielt Maßnahmen, wie z. B. das Blocken von als schädlich identifiziertem Traffic, durchführt.
- **Software-as-a-Service (SaaS):** Vor allem im Unternehmenskontext sind SaaS-Anwendungen mittlerweile zum Standard geworden. Hiermit haben Nutzer schnell und unkompliziert Zugriff auf Software, die sie bei ihrer täglichen Arbeit unterstützt. Beispiele für SaaS sind bekannte Anwendungen wie Dropbox, Google Docs und OneDrive. So komfortabel die Anwendungen auch sind: Im Unternehmenskontext muss ihre Verwendung umfassend überwacht und gegebenenfalls – insbesondere bei der Herausgabe sensibler Daten – reglementiert oder gesperrt werden.
- **VLAN-Segmentierung:** Bei einer VLAN-Segmentierung (Virtual Local Area Network) handelt es sich um die logische Segmentierung eines Netzwerks, beispielsweise entsprechend Abteilungen (Finanzen, HR, Operations). So lässt sich das Risiko eines unautorisierten Zugriffs auf bestimmte Daten verringern und ein übermäßig hoher Netzwerk-Traffic (z.B. durch einen Broadcast-Sturm) vermeiden, der die Antwortzeit des Netzwerks teilweise dramatisch erhöhen kann.

- **Virtual Private Network (VPN):** Eine VPN-Anwendung oder -Software ermöglicht externen Nutzern den Zugriff auf ein Firmennetzwerk via verschlüsseltem Zugang über das Internet. Ein VPN kann auch für die Verbindung zu Partner- und/oder Provider-Netzwerken, beispielsweise einem Zulieferer, Händler oder einem Cloud-Dienstleister, genutzt werden.
- **Network Access Control (NAC):** Die Netzwerkzugriffskontrolle ist dazu da, Sicherheitsrichtlinien durchzusetzen. Dies geschieht, indem der Zugriff auf bestimmte Teile des Netzwerks nur dann zugelassen wird, wenn Nutzer oder Systeme den Vorgaben entsprechen (z. B. Aktualität von Sicherheitspatches und Antivirus-Signaturen, Verschlüsselung der Netzwerkverbindung über VPN etc.).
- **Security Information and Event Management (SIEM):** SIEM-Lösungen ermöglichen die Erfassung und Analyse von Berichten verschiedener Datenquellen wie Firewalls, IDS/IPS, WAFs, Server und Endgeräte.
- **Patchmanagement:** Schwachstellen auf Servern und Endgeräten durch Patches zu beheben, ist elementar wichtig für die Absicherung von Unternehmensnetzwerken. Allerdings kann die Installation solcher Patches bei mehreren Hundert Servern und Endgeräten im Netzwerk – und das ist selbst bei kleineren Unternehmen mittlerweile gar nicht mehr so selten – eine äußerst arbeits- und zeitaufwendige Aufgabe sein. Lösungen für das Patchmanagement helfen hier durch Funktionalitäten für Automatisierung und Verwaltung.
- **Passwortmanager:** Passwörter sind oftmals eine große Schwachstelle in Unternehmen – machen sie sich doch den profitabelsten Angriffsvektor, die Mitarbeiter, zunutze. Mehrfach verwendete, schlecht gewählte oder gedankenlos verbreitete Passwörter machen es Angreifern unnötig leicht. Die Nutzung von Passwortmanagern im Unternehmen ist extrem einfach und macht doch oftmals den entscheidenden Unterschied.
- **Domain Name System (DNS):** Nachdem es einige Zeit von Kriminellen eher stiefmütterlich behandelt worden war, ist das DNS mittlerweile wieder ein äußerst beliebter Angriffsvektor, vor allem für DoS-Attacken. Für Unternehmen ist es unabdingbar, Sicherheitsverbesserungen am DNS-Protokoll wie z. B. DNS Security Extensions (DNSSEC) oder Best Practices für die Konfiguration von DNS-Servern (wie die Deaktivierung rekursiver Anfragen) genau umzusetzen. Weitere Optionen sind die Verwendung sicherer DNS-Geräte oder der Rückgriff auf Managed DNS.

- **Filterung von Web-Inhalten.** Die Filterung von Inhalten hält Benutzer davon ab, auf unautorisierte und potenziell schädliche Websites, Webadressen (IP-Adressen oder URL) oder Inhalte zuzugreifen.

Wachstum und Technologiewahl

Ihr Unternehmen wächst – Glückwunsch! Gleichzeitig steigt hiermit aber auch der Bedarf an Endgeräten wie Desktop-PCs, mobilen Geräte und Servern. Da wir davon ausgehen, dass Sie weder Interesse daran haben, Ihr IT-Team ins Unermessliche wachsen zu lassen, noch Ihre bestehende IT über Gebühr zu belasten, bleibt Ihnen nur, möglichst viele IT-Prozesse möglichst umfassend zu automatisieren. Eine manuelle Installation und Konfiguration von Endgeräten ist nicht länger praktikabel, vor allem dann nicht, wenn sich das Unternehmen über mehrere Standorte verteilt.

Gleichzeitig ist die manuelle Pflege jedes einzelnen Endgerätes natürlich immer auch eine Gefahr für die Datensicherheit, bringt sie doch das Risiko von Inkonsistenzen oder Konfigurationsfehlern mit sich.

Managementplattformen unterstützen die Automatisierung manueller Prozesse und sorgen sicher dafür, dass gesetzte Richtlinien eingehalten werden.


TIPP

Für kleine und mittelständische Unternehmen mit begrenzten Ressourcen können eine cloudbasierte Lösung oder ein Managed Service Provider (MSP) für Automatisierungsdienste sinnvolle Alternativen zu einer eigenen Management-Plattform sein.


TIPP

Für die zentrale Administration ihrer Sicherheitslösung nutzen viele KMU bereits das ESET Security Management Center oder den ESET Cloud Administrator (ECA). Hiermit lassen sich dezentrale und cloudbasierte Ressourcen einfach und sicher verwalten, ohne dass kostspielige Hardware vor Ort nötig wäre.

JEWO – VOLLE LADUNG SECURITY

Bei JEWO, einem Anbieter für Batterietechnik aus dem Herzen des Ruhrgebiets, stand am Anfang die Optimierung der Unternehmenssicherheit mit Blick auf die DSGVO auf dem Programm. Doch in Zusammenarbeit mit ESET und dem betreuenden Systemhaus Otten + Freckmann wurde daraus ein übergreifendes Sicherheitskonzept, das auch die künftigen Entwicklungen berücksichtigt.

Bei der stark auf den Service am Kunden orientierten JEWO werden Auftragsentwicklung und Kundenmanagement über ein modernes CRM abgewickelt, sowohl im Office als auch über mobile Geräte beim Kunden vor Ort. Die ortsunabhängige Verfügbarkeit von Daten setzt aber natürlich voraus, dass diese umfassend geschützt sind. Hierfür beauftragte die JEWO ihren langjährigen Systempartner Otten + Freckmann mit der Überarbeitung des bestehenden Sicherheitskonzepts. Dieses beinhaltete nicht nur die Verschlüsselung der Systeme, sondern auch die sichere Anmeldung via Zwei-Faktor-Authentifizierung (2FA). Zudem sollte der eingesetzte Virenscanner durch eine aktuelle Lösung ausgetauscht werden, um auch in Zukunft geschützt zu sein.

Die Aufgabe

Eine eingehende Analyse der Datenwege im Unternehmen ergab, dass sowohl interne Mitarbeiter über die Clients an ihrem Arbeitsplatz Zugriff auf Kundendaten haben als auch Mitarbeiter im Außendienst über unterschiedlichste Endgeräte. Die gesuchte Lösung sollte entsprechend sowohl Server als auch stationäre Clients und Mobilgeräte abdecken und gleichzeitig möglichst einfach zu handhaben und zu verwalten sein.

Das Ergebnis

„Mit ESET Endpoint Protection Advanced und ESET Endpoint Encryption haben wir ein Security-Paket für unseren Kunden JEWO gefunden, das alle Anforderungen der DSGVO erfüllt und darüber hinaus auch ideal in heterogenen Netzstrukturen implementierbar ist", erklärt Benjamin Engelke, Leiter IT-Systeme bei Otten + Freckmann. ESET Endpoint Protection Advanced umfasst die Module ESET Endpoint Security und ESET Mobile Security sowie ESET Virtualization Security und schützt eingesetzte Clients und Server vor Malware. Verwaltet wird alles über eine zentrale Konsole, ohne dass offene Ports an systemkritischen Komponenten notwendig wären. Für die Datenverschlüsselung kam

(Fortsetzung auf der nächsten Seite)

(Fortsetzung von vorheriger Seite)

zusätzlich ESET Endpoint Encryption zum Einsatz, welches ebenfalls zentral durch den Admin gesteuert wird und so von der Mitwirkung der einzelnen Kollegen unabhängig ist. Abgerundet wird die Security Suite durch die ESET Secure Authentication, welche die Zugriffe insbesondere auf sensible Daten durch Policys zuverlässig regelt.

„Unser Systempartner Otten + Freckmann hat nach einer eingehenden Analyse unserer IT-Infrastruktur die Security Lösung von ESET empfohlen. Neben der Sicherheit und natürlich der DSGVO-Compliance war für uns ausschlaggebend, dass der administrative Aufwand sehr gering gehalten wird und sich das Lösungspaket auch sehr leicht skalieren lässt. So sind wir auch für kommende Herausforderungen optimal aufgestellt", betont Michael Teupen, Geschäftsführer bei JEWO.

Die vollständige Case Study finden Sie unter `https://www.eset.com/de/business/casestudies/`.

INHALT DIESES KAPITELS

Kapitel 5

Organisatorische und prozessbezogene Kontrollmechanismen

In diesem Kapitel erfahren Sie, wie organisatorische und prozessbezogene Kontrollmechanismen mit technischen Kontrollen zusammenspielen und so Daten in Ihrem Unternehmen umfassend schützen.

Technische Kontrollen und organisatorische Unterstützung

Wirksamer Datenschutz erfordert mehr als nur technische Lösungen. Ausschließlich in Kombination mit organisatorischen Kontrollen kann sichergestellt werden, dass technische Kontrollmechanismen ordnungsgemäß eingesetzt, konfiguriert und betrieben werden. Nur so lässt sich eine zielgerichtete Strategie für das Sicherheitsmanagement eines Unternehmens umsetzen.

Beispiele für organisatorische Kontrollmechanismen:

» **Schutz privater und sensibler personenbezogener Daten:** Technische Kontrollmechanismen wie Verschlüsselung und DLP-Software stellen teilweise hohe Ansprüche an Rechenressourcen und sind zudem kostspielig. So erfordert die Verschlüsselung von Daten

zusätzliche Verarbeitungsschritte zum Ver- und Entschlüsseln. DLP-Lösungen wiederum müssen in Dokumenten nach Schlüsselwörtern und Mustern suchen, um private oder sensible Daten wie Kreditkartennummern, Gesundheitsinformationen und Sozialversicherungsnummern zu identifizieren. Beides kann dauern und/oder manuellen Eingriff erfordern. Hier hilft es, Daten von vornherein entsprechend eines Schemas zu klassifizieren. Nutzer erfahren so auf einfache Art und Weise, welche Daten geschützt werden müssen, warum und wie.

- **Dokumentation und Auditing:** Unternehmen, die sensible Daten erfassen, verarbeiten und/oder speichern, müssen dokumentieren, warum sie genau diese Daten erfassen, wie sie erfasst werden (aus welchen Quellen), wie sie verwendet werden und wie die Daten geschützt werden. Die Dokumentation unternehmensinterner Datenschutzrichtlinien kann Ihnen helfen, diese Fragen ohne großen Mehraufwand zu beantworten und Auditanforderungen zu erfüllen, vor allem auch im Hinblick auf Regelwerke wie die EU-DSGVO.
- **Sicherheitsrichtlinien:** Richtlinien müssen keine dicken Bücher sein. Tatsächlich ist es oft sogar besser, Mitarbeitern keine Wälzer vor die Nase zu legen. Die liest ja doch niemand wirklich durch (außer vielleicht der übermotivierte Praktikant) und sonderlich motivierend, sich an die Vorgaben zu halten, ist ein solcher Batzen sicher auch nicht. Oft reichen einige, auf Rollen und Verantwortlichkeiten zugeschnittene Absätze, die den Umgang mit personenbezogenen Daten klar definieren. Beispiele für wichtige Sicherheitsrichtlinien, die von jedem Unternehmen erstellt werden sollten, umfassen:
  - Richtlinie für den Zugriff auf das Internet und auf E-Mails,
  - BYOD-Richtlinie zur Nutzung eigener Geräte,
  - Richtlinie für den Fernzugriff,
  - Richtlinie zu autorisierter Software.
- **Personalmanagement:** Richtlinien und Prozesse zum Schutz von personenbezogenen Daten (z. B. Bewerbungsunterlagen, Gehaltsabrechnungen, Schulungsmaterial und Dokumentation disziplinarischer Maßnahmen), die durch das Personalmanagement gesammelt, verwaltet und verarbeitet werden. Außerdem abgedeckt sind Prozesse wie Bewerberauswahlverfahren, Drogentests und Arbeitsplatzwechsel.
- **Nutzung eines Security Maturity Modells:** Ein Security Maturity Modell kann Sie dabei unterstützen, den Schutz einzelner Bereiche genau zu analysieren und ggf. Lücken zu identifizieren. Dabei sind verschiedene Faktoren relevant:

- Was Sie schützen – z. B. sensible Daten, Finanzinformationen, geistiges Eigentum, medizinische Geräte oder kritische Infrastrukturen,
- Ihre Branche – z. B. Medizin, Finanzen, Einzelhandel, Verteidigung oder öffentliche Versorgung,
- Von Ihnen zu erfüllende regulatorische Bestimmungen – z. B. Datenschutz-Grundverordnung (DSGVO), Bundesdatenschutzgesetz (BDSG), Landesdatenschutzgesetze, weitere Spezialgesetze (z. B. zum Gesundheitsdatenschutz),
- Ihr Gefahrenprofil – befinden Sie sich in einem Krisengebiet bzw. einer instabilen Region, einer Stadt mit hoher Kriminalitätsrate oder einem anderweitig gefährlichen Gebiet?

» **Mitarbeiterschulung:** Regelmäßige Schulungen für alle Ihre Mitarbeiter sorgen dafür, dass diese nicht das schwächste Glied in Ihrem Unternehmen bleiben. Insbesondere sind Themen wie Passwortsicherheit, Spam und Phishing, Malware-Schutz, Konformitätsanforderungen und Datenschutz (wie Datenklassifizierung, Arten sensibler Daten und Datenschutztechnologien) zu behandeln. Wichtig ist auch, das Erlernte regelmäßig aufzufrischen und zu überprüfen. Nur so ist gewährleistet, dass die Schulungen ihren Zweck erfüllen.

» **Datenschutzfolgenabschätzungen:** Datenschutzfolgenabschätzungen werden von der DSGVO gefordert, wenn die Datenverarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" zur Folge haben könnte. Eine Datenschutzfolgenabschätzung ähnelt dem grundlegenden Risikomanagementprozess (beschrieben in Kapitel 2), legt allerdings weitere Parameter im Zusammenhang mit der Verarbeitung personenbezogener Daten fest.

» **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:** Die DSGVO fordert „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen". Das heißt, Unternehmen sind verpflichtet, technische und organisatorische Maßnahmen zu treffen, um die Erfassung, Verarbeitung und Speicherung personenbezogener Daten so gering wie möglich zu halten.

DATENSCHUTZ VON A BIS Z (ODER ZUMINDEST BIS F)

Das folgende Schema soll Sie bei der Absicherung wertvoller und sensibler Daten in Ihrem Unternehmen unterstützen. Folgen Sie einfach den Schritten von A bis F:

A) ASSESS – Bewerten Sie Ihre Vermögenswerte, Risiken und Ressourcen

Erstellen Sie eine Liste aller IT-Systeme und -Services, die in Ihrem Unternehmen genutzt werden. Schließlich müssen Sie erst einmal wissen, was Sie haben, damit Sie es schützen können. Vergessen Sie dabei auch mobile Geräte wie Smartphones und Tablets nicht, die zum Zugriff auf unternehmensinterne oder Kundeninformationen genutzt werden können. Das Ponemon Institute hat nämlich ermittelt, dass 60 % aller Mitarbeiter Sicherheitsfunktionen auf ihren mobilen Geräten umgehen und 48 % die von ihrem Arbeitgeber geforderten Sicherheitseinstellungen deaktivieren. Nicht vergessen sollten Sie auch Cloud-Services wie Dropbox, iCloud, Google Docs, Office 365, OneDrive und SalesForce.

Gehen Sie die Liste im Anschluss nochmal durch und überlegen Sie, welche Risiken mit jedem einzelnen Punkt einhergehen. Wird das System, die Software oder der Service wirklich noch benötigt? Wer oder was stellt eine Gefahr dar? Eine weitere gute Frage, die Sie sich stellen sollten, ist: „Was kann alles schieflaufen?" Die Eintrittswahrscheinlichkeit einiger Risiken ist höher als die anderer. Nichtsdestotrotz müssen alle Risiken aufgeführt und dann ihrem potenziellen Schaden und ihrer Eintrittswahrscheinlichkeit nach sortiert werden.

Es kann sinnvoll sein, sich für diesen Prozess externe Hilfe zu holen. Das kann ein kompetenter und sicherheitsbewusster Mitarbeiter sein, aber auch ein Partner oder Händler. Sie brauchen also eine weitere Liste, nämlich die, die Ihre verfügbaren Ressourcen für Sicherheitsfragen im IT-Bereich beinhaltet. Handelsgruppen und Wirtschaftsverbände können hier ebenfalls mit Ratschlägen oder Ressourcen weiterhelfen. Die in Deutschland durch das BSI gegründete „Allianz für Cybersicherheit" z. B. bietet kostenloses Infomaterial, Leitfäden und Schulungsmaterial für Mitarbeiter.

B) BUILD – Stellen Sie Richtlinien auf

Ein zuverlässiges Security-Programm beginnt mit den entsprechenden Richtlinien. Wie immer stinkt auch hier der Fisch am Kopf zuerst: Sind Sie der Chef des Unternehmens, müssen Sie für alle deutlich machen, wie wichtig Ihnen das Thema Sicherheit ist und dass sich Ihr Unternehmen verpflichtet hat, alle persönlichen und sensiblen Daten, mit denen gearbei-

tet wird, umfassend zu schützen. Anschließend müssen Sie entsprechende Richtlinien formulieren. Solche Richtlinien können beispielsweise den unbefugten Zugriff auf Unternehmenssysteme und -daten verhindern oder sicherstellen, dass Mitarbeiter die Sicherheitseinstellungen ihrer Mobilgeräte verändern oder deaktivieren.

C) CHOOSE – Wählen Sie Kontrollmechanismen aus

Ohne Kontrollmechanismen bringen die besten Richtlinien nichts. Soll beispielsweise die Richtlinie durchgesetzt werden, dass niemand unbefugt auf Unternehmenssysteme und -daten zugreifen darf, lässt sich das kontrollieren, indem der Zugriff nur mit eindeutigem Benutzernamen, Passwort und Token möglich ist.

Um zu verhindern, dass unerwünschte Programme auf Unternehmensrechnern ausgeführt werden, lässt sich die Vergabe von Administratorrechten an Mitarbeiter einschränken. Um Datenlecks durch verlorene oder gestohlene Mobilgeräte zu verhindern, können Sie Mitarbeiter verpflichten, entsprechende Vorfälle noch am selben Tag zu melden. Betroffene Geräte können so per Fernzugriff gesperrt oder Daten gelöscht werden.

Die folgenden drei Technologien sollten zur Umsetzung von Richtlinien mindestens zum Einsatz kommen:

- **Anti-Malware**, die den Download von schädlichem Code (Viren, Ransomware etc.) auf Unternehmensgeräte verhindert,
- **Verschlüsselungssoftware**, die den Zugriff auf Daten auf verlorenen oder gestohlenen Geräten unterbindet,
- **Multi-Faktor-Authentifizierung**, die neben Benutzernamen und Passwort zusätzliche Informationen abfragt (z. B. ein Einmalpasswort, das an ein registriertes Mobiltelefon gesendet wird).

D) DEPLOY – Wenden Sie die Kontrollen an

Achten Sie bei der Umsetzung von Kontrollen darauf, dass diese auch funktionieren. Nehmen wir an, Sie setzen eine Richtlinie zum Verbot von unautorisierter Software auf Unternehmenssystemen fest. Dazu implementieren Sie eine Anti-Malware-Software, die nach schädlichem Code sucht. Diese muss aber auch umfassend getestet werden, vor allem um sicherzustellen, dass sie betriebliche Abläufe nicht beeinträchtigt. Außerdem müssen Maßnahmen festgelegt werden, die im Fall eines Malware-Alarms zu treffen sind.

E) EDUCATE – Schulen Sie Mitarbeiter, Partner und Händler

Mitarbeiter müssen nicht nur die unternehmensinternen Sicherheitsrichtlinien und Prozesse kennen, sondern vor allem auch verstehen, *warum*

(Fortsetzung auf der nächsten Seite)

(Fortsetzung von vorheriger Seite)

diese Maßnahmen erforderlich sind. Die Investition in das Sicherheitsbewusstsein aller Mitarbeiter ist eine der wirksamsten Sicherheitsmaßnahmen überhaupt.

Durch die Zusammenarbeit mit Ihren Mitarbeitern können Sie ein Bewusstsein für Probleme schaffen. Denken Sie zum Beispiel an Phishing-E-Mails. Der kürzlich von Verizon veröffentlichte Data *Breach Investigations Report* (DBIR) ergab, dass 23 % der Phishing-Mails von Mitarbeitern gelesen und immerhin 11 % aller Anhänge geöffnet werden. Die Gefahr für Datenlecks oder Datendiebstahl steigt erheblich.

Schulen Sie jeden, der Ihr System nutzt – einschließlich Vorgesetzte, Händler und Partner. Und vergessen Sie nicht, dass eine Verletzung von Sicherheitsrichtlinien Konsequenzen nach sich ziehen muss. Ohne diese sind alle vorher getroffenen Maßnahmen und Richtlinien umsonst.

F) FURTHER – Führen Sie zusätzliche Bewertungen, Audits und Prüfungen durch

IT-Security ist für jedes Unternehmen, egal wie klein, kein einmaliges Projekt. Es handelt sich vielmehr um einen Prozess, der dauerhaft bei allen betrieblichen Abläufen mitlaufen muss. Planen Sie eine regelmäßige Neubewertung Ihrer Sicherheitsvorkehrungen – mindestens jedoch einmal pro Jahr. Bleiben Sie auf dem Laufenden über neue Bedrohungen, indem Sie regelmäßig Sicherheitsnews lesen. Nützliche Websites sind zum Beispiel `WeLiveSecurity.de`, `KrebsOnSecurity.com` und `DarkReading.com`.

Möglicherweise müssen Sie Ihre Sicherheitsrichtlinien und -kontrollen mehr als einmal im Jahr überarbeiten, je nach Änderungen im Unternehmen (neue Lieferanten, neue Projekte, neue Mitarbeiter oder ausscheidende Mitarbeiter) oder der Umwelt.

Eventuell kann ein externer Berater sinnvoll sein, der Penetrationstests und Sicherheitsaudits durchführt. So lassen sich Schwachstellen in Ihren Systemen am besten aufdecken und bei Bedarf beheben.

Prozesskontrollen

Prozesskontrollen unterstützen Unternehmen dabei, die Auswirkungen eines Datenschutzvorfalls so gering wie möglich zu halten. Dazu muss ein Reaktionsprozess implementiert sein, der die Zeit zwischen Identifikation und Eindämmung effektiv reduziert. Verantwortlich für die Reaktionsmaßnahmen können ein internes Team, ein externer Dienstleister oder beide in Zusammenarbeit sein. Einer vom Ponemon Institute durchgeführten Studie zufolge können Unternehmen bei einem

Vorfall die Durchschnittskosten pro Datensatz von 141 US-Dollar auf etwa 122 US-Dollar senken. Bei einem Verlust von 10.000 Datensätzen können also im Schnitt 190.000 US-Dollar eingespart werden. Sie sehen: Die Investition in vernünftige Prozesskontrollen lohnt sich!

Bei der Einführung von Prozesskontrollen müssen Unternehmen:

- Mitarbeiter einbinden: Wie viele Initiativen darf auch diese nicht allein vom Management getragen werden. Vielmehr sind alle Personen einzubinden, die tatsächlich mit den verschiedenen Prozessen und Technologien arbeiten. Nur so wird gewährleistet, dass die Kontrollen Sinn ergeben und eine wirksame Umsetzung in der Praxis möglich ist.
- Verantwortlichkeiten definieren: Einzelne Verantwortlichkeiten müssen klar definiert und verständlich sein. Jeder muss über seine Rolle Bescheid wissen, um die Aufgaben entsprechend umsetzen zu können.
- Gründe für Prozesskontrollen erläutern: Sicherheitsmaßnahmen erscheinen Mitarbeitern oft als Last oder Hindernis. Ohne ausreichende Information aller Mitarbeiter können diese kaum nachvollziehen, warum die Kontrollen wichtig und in genau dieser Form notwendig sind. Das führt nicht selten dazu, dass sie ignoriert oder (manchmal auffallend kreativ) umgangen werden.

ERINNERUNG

Dem Ponemon Institute zufolge werden Datenschutzvorfälle im Schnitt erst nach 191 Tagen erkannt. Die durchschnittliche Zeit zur Eindämmung beträgt noch einmal 66 Tage. Dabei werden das Ausmaß und die Kosten, die mit einem solchen Vorfall einhergehen, mit zunehmendem Zeithorizont immer gravierender.

Wenn Unternehmen Prozesse für den sicheren Datentransfer implementieren, sorgen sie zugleich dafür, dass die Kosten eventueller Datenpannen wesentlich geringer ausfallen. Dem Ponemon Institute zufolge reduzieren sich die Kosten pro verlorenem Datensatz im Schnitt um 16 US-Dollar, wenn die Daten vorher verschlüsselt worden waren. Im Fall eines Vorfalls, der 10.000 Datensätze betrifft, verringern sich die Kosten damit um 160.000 US Dollar. Dabei reduziert allein der Nachweis, dass Daten ordnungsgemäß verschlüsselt worden sind, die Kosten dramatisch. Hiermit erfüllen Unternehmen nämlich die sogenannte „Safe Harbor"-Vorgabe und sind nicht verpflichtet, Datenschutzvorfälle an die Behörden zu melden. So verringern sich sowohl direkte Kosten (z. B. Kosten für die Meldung und eventuelle Gerichtskosten) als auch indirekte Kosten (z. B. Markenschäden und Kundenabwanderung).

Die wichtigsten Prozesskontrollen sind:

- **Richtlinien zu Zugriffskontrollen:** Sie definieren, wer Zugang zu verschiedenen Systemen, Anwendungen und Daten hat und zu welchem Zweck.
- **Management von Ressourcen/Vermögenswerten:** Es ist wichtig zu wissen, was genau Sie schützen und warum (Wert/Risiko für das Unternehmen). Unternehmen müssen nicht nur genau dokumentieren, welche Rechner und Datenbestände/Ressourcen sie besitzen. Sie müssen auch für ein angemessenes Sicherheitsumfeld sorgen, indem Systeme und Anwendungen auf dem neuesten Stand gehalten werden (Stichwort Sicherheitspatches) und sensible Daten, die nicht mehr benötigt werden, gemäß den festgelegten Richtlinien zur Datenspeicherung, Archivierung und Löschung unverzüglich gelöscht bzw. vernichtet werden.
- **Änderungsmanagement:** Hiermit wird sichergestellt, dass alle Änderungen an Systemen und Anwendungen dokumentiert, geprüft und genehmigt werden. So wird sichergestellt, dass alle Auswirkungen einer Änderung auf die Sicherheit des Unternehmens nachvollzogen werden können.
- **Incident-Response:** Bei einem Vorfall (z. B. Datenleck oder Hackerangriff) benötigen Unternehmen einen klar definierten und einfach nachvollziehbaren Reaktionsplan. Dadurch wird gewährleistet, dass schnell und effizient reagiert und der Schaden eingedämmt wird. Zu möglichen Reaktionen gehören Datenwiederherstellung, Beweissicherung, interne und externe Kommunikation sowie Ursachenanalyse.
- **Geschäftskontinuität:** Durch Planung der Geschäftskontinuität werden die Auswirkungen von Ausfällen oder Katastrophen minimiert. Außerdem wird die Aufrechterhaltung des Geschäftsbetriebs ermöglicht, bis der Status quo wiederhergestellt ist.

Zusätzlich besteht natürlich auch immer die Möglichkeit, professionelle Sicherheitsanbieter ins Boot zu holen, um interne Prozesse zu unterstützen. Diese können zum Beispiel laufend aktuelle Informationen zu extern bestehenden Gefahren liefern sowie helfen, interne Prozesse zu evaluieren und zu überwachen. Im Bedarfsfall können sie helfen, Angriffe zu erkennen und darauf zu reagieren. Damit unterstützen sie forensische Analysen, Bewertungs- und Auditaktivitäten, Krisenmanagement sowie interne und externe Kommunikation.

ERINNERUNG

Noch ein Hinweis zum Schluss: Alle organisatorischen und prozessbezogenen Kontrollen sollten dem Risikoniveau angemessen sein, um zwar stets passend reagieren zu können, aber nicht mit Kanonen auf Spatzen zu schießen.

INHALT DIESES KAPITELS

- Einführung administrativer Kontrollmechanismen
- Was Sie schützen und wie Sie es schützen
- Umsetzung technischer Kontrollen
- Backup und Wiederherstellung, Incident Response und Disaster Recovery
- Zusammenarbeit mit Nutzern und Sicherheitsexperten

Kapitel 6
Zehn Tipps für effektiven Datenschutz

In diesem Kapitel lernen Sie zehn Best Practices kennen, mit denen Sie sicherstellen, dass Daten in Ihrem Unternehmen umfassend geschützt sind.

- **Sicherheitsrichtlinien aufstellen:** Viele Unternehmen vergessen die Wichtigkeit schriftlich dokumentierter Sicherheitsrichtlinien und gehen gleich zu technischen Kontrollen über. Technische Kontrollmechanismen wie Firewalls, Endgeräteschutz etc. können ohne administrative Maßnahmen wie Richtlinien und dokumentierte Prozesse jedoch fast immer nur auf bestimmte, schon eingetretene Situationen reagieren. Werden sie nicht im Rahmen einer fundierten und durchdachten Sicherheitsstrategie eingesetzt, sind technische Lösungen daher nur begrenzt effektiv. Entsprechend geben Sie meist viel zu viel Geld für teilweise unzureichenden Schutz aus.
- **Identifizieren Sie Ihre Vermögenswerte:** Sie müssen genau wissen, was Sie schützen. Führen Sie daher genau Buch über die in Ihrem Unternehmen installierte Hard- und Software, damit Sie keine Komponenten übersehen. Sind diese nämlich schwach abgesichert oder arbeiten sie mit sensiblen Daten, erhöhen sie das Risiko für Datenpannen enorm. Beim Angriff auf die Einzelhandelskette Target im Jahr 2013 beispielsweise nutzten die Angreifer das Wartungssystem für die Klimaanlagen, um Zugriff auf Bank- und personen-

bezogene Daten von 110 Millionen Kunden zu erhalten. Kostenlose Tools zum Scannen von Netzwerken und Endgeräten gibt es wie Sand am Meer. Diese haben auch durchaus ihre Berechtigung. Kostenpflichtige Lösungen haben allerdings den Vorteil, dass Sie sie meist zusätzlich bei der Pflege und Wartung Ihrer IT-Infrastruktur unterstützen, beispielsweise mit Funktionen zur Installation, Löschung und Aktualisierung von Software per Fernzugriff. Grundsätzlich gilt: Machen Sie es Angreifern so schwer wie möglich, indem Sie Ihr Netzwerk genau kennen und angemessene Sicherheitssysteme implementieren. Achten Sie auch darauf, nur diejenigen Geräte mit dem Internet zu verbinden, die tatsächlich nach außen kommunizieren müssen.

- **Finden Sie heraus, wo Sie stehen:** Wie gut ist die Sicherheit Ihrer IT-Infrastruktur und der verarbeiteten Daten aktuell? Erstellen Sie beispielsweise eine Roadmap oder ein Maturity Modell, um den Ist-Zustand zu verdeutlichen. Nutzen Sie einen risikobasierten Ansatz, um relevante Bedrohungen für Ihre Assets zu bestimmen (siehe vorheriger Tipp) und angemessene Sicherheits- und Datenschutzmaßnahmen zu entwickeln. Führen Sie anschließend eine Gap-Analyse durch und ermitteln Sie, wo ggf. Investitionen nötig sind. In Kapitel 3 finden Sie weitere Informationen zur Risikobewertung im Bereich Datensicherheit.
- **Klassifizieren Sie alle Ihre Daten:** Für viele Unternehmen sind Personendaten von Kunden und andere sensible Daten die „Kronjuwelen" des Unternehmens. Die Sicherheits- und Kontrollmechanismen, die Sie solchen Daten angedeihen lassen, sind natürlich nicht für alle Daten über deren gesamten Lebenszyklus hinweg sinnvoll oder praktisch umsetzbar. Überlegen Sie stattdessen, welche Daten auf keinen Fall verloren gehen oder gestohlen werden dürfen. Welche Auswirkungen hätte ein Leck an dieser Stelle auf das Ansehen Ihres Unternehmens, die Loyalität Ihrer Kunden oder vielleicht sogar den Fortbestand Ihrer Firma? Erstellen (und dokumentieren) Sie eine möglichst intuitiv nachvollziehbare Richtlinie zur Klassifizierung von Daten. Verwenden Sie hierfür zum Beispiel Labels wie „Nur interne Verwendung", „Sensible Daten" und „Zur Veröffentlichung freigegeben" und ordnen Sie den einzelnen Kategorien Datenschutzanforderungen (z. B. Verschlüsselung, Backups, Freigabe und Löschung) zu.

TIPP

Die Datenschutz-Grundverordnung (DSGVO) fordert von Unternehmen die Löschung personenbezogener Daten, wenn dies gewünscht wird (z. B. von einer Einzelperson). Um der DSGVO hier zu entsprechen, kann es sinnvoll sein, personenbezogene Daten (einschließlich ihrer

Backups) zusätzlich als solche zu kennzeichnen, die in Zukunft gelöscht oder anderweitig bearbeitet werden müssen.

- **Verschlüsseln Sie Ihre sensiblen Daten:** Bei der Verschlüsselung von Daten wird Text in eine nicht lesbare Form (Ciphertext/Chiffretext) gebracht, sodass er ohne entsprechenden Schlüssel nicht mehr lesbar ist und für Unautorisierte wertlos wird. Das gilt natürlich nur dann, wenn der Schlüssel selbst entsprechend gut vor Diebstahl oder Verlust geschützt ist. Verschlüsselung sollte zumindest für inaktive Daten (Data at Rest) Standard sein. Sie kann zusätzlich sinnvoll sein für Daten, die übertragen werden (Data in Motion/Data in Transit) – z. B. in Form einer SSL-Verschlüsselung. Aber auch Daten, die laufend in Verwendung sind (Data in Use), sollten durch eine auf die Verwendung angepasste Verschlüsselung geschützt werden. Die Verschlüsselung kann in allen Fällen entweder per Hard- (schneller) oder Software (günstiger) erfolgen.

TIPP

Die meisten aktuell gültigen Datenschutzverordnungen enthalten sogenannte „Safe Harbor"-Bedingungen, darunter die Verschlüsselung von Daten. Dadurch reduzieren sich die Kosten von Datenschutzvorfällen teilweise erheblich.

- **Erstellen Sie Backups wertvoller Daten** (und überprüfen Sie, ob sie sich daraus wirklich wiederherstellen lassen): Regelmäßige und zuverlässige Backups von Systemen und Daten stellen eine essenzielle Best Practice für die Absicherung von Daten dar. Aus guten und regelmäßigen Backups lassen sich versehentlich gelöschte Dateien und Inhalte beschädigter Festplatten wiederherstellen. Die finanziellen und personellen Kosten für Backup-Lösungen sind mittlerweile so gering, dass es keine sinnvolle Entschuldigung mehr gibt, im Unternehmenskontext auf Backups zu verzichten. Vor allem die rasante Verbreitung von Ransomware innerhalb der letzten Jahre macht deutlich, dass Sicherungskopien unverzichtbar sind. Nur so können Sie Ihre Daten garantiert zurückbekommen, sollten Sie Opfer eines Ransomware-Angriffs werden. Auch ohne das Lösegeld zu zahlen.

ERINNERUNG

Es muss regelmäßig überprüft werden, ob sich kritische Systeme und Daten auch wirklich aus den generierten Backups wiederherstellen lassen. Nur so ist gewährleistet, dass die Backups nicht beschädigt sind, aber auch, dass der Prozess zur Wiederherstellung den Verantwortlichen bekannt und praktikabel ist.

- **Investieren Sie in Endpointschutz:** „Investieren" bedeutet dabei nicht, kostenlose Anti-Viren-Software herunterzuladen. Vielmehr ist eine leistungsstarke kommerzielle Lösung nötig, um Desktop-PCs, Mobilgeräte und Server verlässlich abzusichern. Endpoints sind die Stellen, an denen alles zusammenkommt. Entsprechend viel Wert sollte auf ihren Schutz gelegt werden.
- **Denken und agieren Sie vorausschauend:** Nur mit einer durchdachten Strategie zur Reaktion auf Vorfälle, zur Sicherstellung der Geschäftskontinuität und zur Wiederherstellung des Status quo ist ein Unternehmen auf den Ernstfall vorbereitet. Krisenteams benötigen Kompetenzen bezüglich grundlegender forensischer Analysen, denn jeder Datenschutzvorfall ist ein potenzieller Fall für das Gericht. Entsprechend lückenlos sollte die Beweiskette gehalten werden. Business Continuity-Pläne und Wiederherstellungsstrategien helfen, auch bei besonders schweren Vorfällen, schnell zum normalen Geschäftsbetrieb zurückzukehren. Zentraler Bestandteil ist die widerspruchsfreie und zeitnahe Kommunikation nach innen und außen während der Planung und bei Vorfällen.
- **Schulen Sie Nutzer eingehend:** Endnutzer waren schon immer das schwächste Glied in der Kette, wenn es um die Absicherung von Unternehmensnetzwerken ging und werden es wohl auch noch lange bleiben. Das ist nicht notwendigerweise die Schuld der Nutzer: Wir gehen davon aus, dass Sie nicht jeden Ihrer Mitarbeiter aufgrund seiner Fachkenntnisse in der IT-Security eingestellt haben. Das wissen auch Angreifer und nutzen sogenannte Social-Engineering-Techniken, um Mitarbeiter dazu zu bringen, schädliche Links in Spam- oder Phishing-Mails anzuklicken, ihre Passwörter preiszugeben (siehe „Erstellung starker Passwörter") oder schädliche Websites zu besuchen. Führen Sie regelmäßige, verpflichtende, relevante und *kurze* Sicherheitsschulungen durch, um Ihre Mitarbeiter dabei zu unterstützen, sich selbst und – über kurz oder lang – Ihrem Unternehmen zu helfen.
- **Holen Sie Verstärkung:** Angreifer auf Ihr Unternehmensnetzwerk arbeiten nicht allein. Sie kollaborieren mit anderen zwielichtigen Gestalten, um ihre kriminellen Ziele zu erreichen, verwenden vorgefertigten Schadcode aus dem Dark Web oder besorgen sich Zugangsdaten ahnungsloser Opfer und machen deren Endgeräte zu Bots, um wiederum weitere Opfer zu finden. Doch auch die Guten sind nicht allein. Ihnen steht eine breite Front aus Sicherheitsexperten, Polizei, Berufsverbänden, externen Sicherheitsdienstleistern, Managed Security Services, cloudbasierter Threat Intelligence und vielem mehr zur Verfügung. Nutzen Sie sie!

WIE ERSTELLT MAN EIN STARKES PASSWORT?

Fast alles, was wir online tun, erfordert einen Login und jeder Login erfordert eine Form der Authentifizierung. Nur so können wir bestätigen, dass wir auch der sind, der wir vorgeben zu sein. Dementsprechend sollte Ihr Passwort so einzigartig (und komplex) sein, wie auch Sie es sind. Hier einige Tipps:

- **Verwenden Sie lange Passwörter und Passphrasen.** Passwörter sollten mindestens acht Zeichen lang sein, aber nicht so lang, dass Sie sie sich nicht merken können (siehe Tipp unten). Auf der folgenden Website können Sie prüfen, ob Ihr Passwort in einem Datenleck öffentlich geworden ist: `https://haveibeenpwned.com/Passwords`.
- **Verwenden Sie einzigartige Phrasen und Sonderzeichen.** Eine kurze Phrase aus 30 oder mehr Zeichen (vielleicht mit einigen Zahlen, Groß-/Kleinschreibung und Satzzeichen), die Sie sich merken können, ist viel besser als ein Wort mit acht Zeichen und üblicher Ersetzung von Buchstaben (beispielsweise „3" für „E").
- **Verwenden Sie einen Passwortmanager (kostenlos oder kostenpflichtig).** Ein Passwortmanager kann Ihnen dabei helfen, einzigartige und starke Passwörter für alle von Ihnen verwendeten Geräte, Systeme und Anwendungen zu erstellen, zu speichern und zu verwalten. Kommen Sie bitte nicht auf die Idee, Ihre Passwörter auf Klebezetteln zu notieren!
- **Verwenden Sie Passwörter, die Sie sich merken können.** Zu komplexe und zufällige Passwörter, die man sich kaum merken kann, können tatsächlich sogar kontraproduktiv sein. Nicht selten kommt man nämlich dadurch in Versuchung, sie doch irgendwo „ganz versteckt" aufzuschreiben oder einfach dasselbe Passwort für verschiedene Benutzerkonten zu verwenden – am Arbeitsplatz *und* Zuhause.
- **Nutzen Sie eine Multi-Faktor-Authentifizierung (MFA).** Wenn möglich, sollten Sie Ihre Benutzerkonten per MFA anstelle von oder zusätzlich zu Passwörtern schützen. MFA erfordert die Authentifizierung über zwei oder mehr Faktoren (im Allgemeinen „etwas, das Sie kennen", d.h. Benutzername und/oder Passwort, und „etwas, das Sie haben", also Hard- oder Software-Token oder Smartphone). Meldet sich ein Nutzer auf einem MFA-Benutzerkonto an, wird ein

(Fortsetzung auf nächster Seite)

(Fortsetzung von vorheriger Seite)

einzigartiger Code generiert, der nur einmal und nur für einen bestimmten Zeitraum verwendet werden kann (typischerweise eine bis fünf Minuten). Angreifern wird es so erschwert, den Code abzufangen und vor Ablauf seiner Gültigkeit unbemerkt für den Login in Ihr System zu nutzen.

- **Auch wenn Sie das beste Passwort der Welt haben:** Verwenden Sie es niemals mehrfach. Gelangt es doch in die Hände von Kriminellen, werden Cyberkriminelle versuchen, es auch an anderen Stellen zu verwenden.
- **Geben Sie Ihr Passwort niemals weiter – an niemanden!** Schützen Sie Ihr Passwort besser als Ihre Zahnbürste (die Sie vielleicht auch mal mit Ihrer besseren Hälfte teilen – oder Ihrem Hund).
- **Verwenden Sie keine „normalen" Wörter.** Vielleicht kennen Sie noch den Hacker aus Filmen der 80er Jahre, der vor einem Rechner sitzt und durch mehrfaches Probieren Passwörter knackt. Heute übernehmen das Programme – in wesentlich höherer Geschwindigkeit. Wörter, die im Wörterbuch stehen (auch fremdsprachliche oder medizinische, juristische oder technische Fachbegriffe) sind so schnell erraten. Vermeiden Sie auch die Wiederholung gleicher Buchstaben (z. B. „aaaa"), Zeichenfolgen (z. B. „1234") und geläufige Muster (z. B. „qwertz").
- **Verwenden Sie keine persönlichen Informationen in Ihrem Passwort.** Soziale Medien machen es Cyberkriminellen heute einfacher als je zuvor, persönliche Informationen über Sie zu sammeln – einschließlich Ihres zweiten Vornamens, Geburtsdatums, Ihrer Adresse, Schule, des Namens Ihres Ehegatten oder Kindes oder was Sie letzten Sommer getan haben.

Glossar

Adware: Programme, die meist bei der Installation von Freeware oder Shareware mitinstalliert werden und (unerwünschte) Werbung einblenden. Werden teilweise als →Malware klassifiziert.

Backdoor: Malware, mit der die Authentifizierung, die für den Zugriff auf Systeme notwendig ist, umgangen werden kann. *Siehe auch* →Malware.

Bootkit: Rootkit, das bereits im Betriebssystemkern aktiv wird und so selbst verschlüsselte Festplatten kompromittiert. *Siehe auch* →Malware *und* →Rootkit.

Bot: Mit Malware infiziertes System, das als Teil eines Botnets missbraucht wird. *Siehe auch* →Botnet *und* →Malware.

Botnet: Netzwerk aus infizierten Systemen, die über einen Command-and-Control (C&C)-Server gesteuert und für Angriffe missbraucht werden. *Siehe auch* →Bot *und* →Malware.

Bring Your Own Device (BYOD): Unternehmenspolicy zum Umgang mit privaten Mobilgeräten, z. B. Smartphones und Tablets, die dann sowohl am Arbeitsplatz als auch privat genutzt werden können.

Chiffretext/Ciphertext: (Plain-)Text, welcher durch Verschlüsselung so verändert wurde, dass er ohne den Entschlüsselungs-Key unlesbar ist. *Siehe auch* →Entschlüsselung, →Verschlüsselung *und* →Plaintext.

Directory Harvest Attack (DHA): Hiermit identifizieren Spammer echte E-Mail-Adressen innerhalb einer Domain.

Distributed Denial-of-Service (DDoS)-Attacke: Großangelegter Angriff, bei dem die Bots in einem Botnet verwendet werden, um Netzwerke oder Server lahmzulegen. *Siehe auch* →Bot *und* →Botnet.

DNS-Cache Poisoning: Auch bekannt als DNS-Spoofing. Nutzt Schwachstellen im DNS, um Traffic von legitimen Zielservern auf Fake-Server umzuleiten. *Siehe auch* →Domain Name System (DNS).

DNS-Hijacking: Angriff, bei dem Anfragen an legitime DNS-Server auf Fake-Server umgeleitet werden. *Siehe auch* →Domain Name System (DNS).

Domain Name System (DNS): Dezentrale, hierarchische Datenbank für Rechner, Dienste und andere Ressourcen, welche mit einem Netzwerk oder dem Internet verbunden sind. Stellt numerische (→IP-)Adressen zur eindeutigen Bezeichnung von Domains sowie weitere Informationen zur Verfügung.

Drive-by-Download: Software (meist Malware), welche vom Nutzer unbemerkt und unautorisiert aus dem Internet (z. B. beim Besuch einer Webseite) heruntergeladen wird.

DSGVO (Datenschutz-Grundverordnung): Gilt für jedes Unternehmen, welches Geschäfte mit EU-Bürgern abschließt. Stärkt den Schutz persönlicher Daten von EU-Bürgern auch bei Geschäftsbeziehungen mit Nicht-EU-Unternehmen.

Dumpster Diving: Die Angreifer verschaffen sich Zugriff auf sensible Informationen (Passwörter, Kundendaten usw.), indem sie den Müll des Opfers durchsuchen.

Endpoint: Vom Endnutzer verwendetes Gerät, z.B. Desktop-PC, Laptop, Tablet oder Smartphone.

Entschlüsselung: Umwandlung von →Chiffretext in →Plaintext.

Exploit: Software oder Teile davon, welche Schwachstellen in Betriebssystemen oder Anwendungen ausnutzen und unerwünschtes Verhalten auslösen, beispielsweise Rechteausweitung, Remote-Zugriff oder Denial-of-Service.

Internationale Organisation für Normung (ISO): Vereinigung von Normungsorganisationen zur Erstellung international einheitlicher Standards. „Isos" ist griechisch und bedeutet „gleich".

Internet Protocol (IP): Zentrales Protokoll des TCP/IP-Standards für die Kommunikation zwischen Routern und dem Internet. *Siehe auch* → Transmission Control Protocol (TCP).

Intrusion Detection System (IDS): Hard- oder Software-Anwendung, die Eindringversuche in Netzwerke und Rechner identifiziert.

Intrusion Prevention System (IPS): Hard- oder Software-Anwendung, die Eindringversuche in Netzwerke oder Rechner erkennt und blockiert.

Kryptowährung: Digitale Währung auf Kryptographie-Basis, mit der sich sichere Transaktionen durchführen lassen, die Übertragung von Vermögenswerten verifiziert werden kann und die die Generierung neuer Währungseinheiten nachvollziehbar macht. Die wohl bekannteste Kryptowährung ist Bitcoin.

Logic Bomb: Schadsoftware oder -code, der aktiv wird, sobald eine bestimmte (logische) Bedingung eintritt. *Siehe auch* →Malware.

Malware: Schadsoftware oder -code zur Schädigung, Zerstörung oder Fremdsteuerung von Rechnern oder zum Diebstahl von Informationen. Malware ist Oberbegriff für →Viren, →Würmer, →Trojaner, →Logic Bombs, →Ransomware, →Rootkits, →Bootkits, →Backdoors, →Spyware und →Adware.

Metamorphismus: Metamorphe Malware ändert ihren eigenen Code bei jeder Iteration, sodass die neue Version sich komplett von der vorherigen unterscheidet. *Siehe auch* →Malware und →Polymorphismus.

Next-Generation Firewall (NGFW): Sicherheitslösungen für Netzwerke, die zusätzlich zur traditionellen Firewall *und* →IDS/→IPS weitere Sicherheitsfunktionen bieten. Der Datenstrom lässt sich so genauestens analysieren und Pakete klassifizieren (Deep Packet Inspection, DPI). Ebenso lassen sich Nutzer und Nutzergruppen identifizieren und exakt zugeschnittene Policies festlegen. →*Siehe auch* Intrusion Prevention System (IPS).

Phishing: Eine Form des sogenannten →Social Engineering, bei dem das Opfer eine E-Mail von einem vermeintlich vertrauenswürdigen Absender (z. B. einer Bank) erhält. Ziel ist, dass das Opfer den (mit Malware oder Exploit infizierten) Anhang der Mail öffnet oder einem Link in der Mail folgt. Dieser Link wiederum führt zu einer bösartigen Webseite, auf der das Opfer aufgefordert wird, sensible Daten (z.B. Anmeldedaten) einzugeben oder von der unbemerkt Malware heruntergeladen wird. *Siehe auch* →Drive-by-Download, →Endpoint, →Exploit *und* →Malware.

Plaintext: Text in seinem ursprünglichen, menschen- oder maschinenlesbaren Format oder Chiffretext, der vollständig und richtig entschlüsselt wurde. *Siehe auch* →Chiffretext *und* →Entschlüsselung.

Polymorphismus: Polymorphe Malware ändert ihren eigenen Code bei jeder Iteration, sodass die neue Version sich leicht von der vorherigen unterscheidet. *Siehe auch* →Malware *und* →Metamorphismus.

Port Hopping: Ursprünglich genutzt, um die Erreichbarkeit von Rechnern zu verbessern, wird Port Hopping heute von Kriminellen dazu verwendet, die Ports der TCP-Verbindung laufend zu wechseln, um einer Erkennung zu entgehen. *Siehe auch* →Transmission Control Protocol (TCP).

Ransomware: Malware, die die Daten eines Opfers verschlüsselt und erst gegen Zahlung eines Lösegeldes (meist in Kryptowährung) wieder entschlüsselt. (Die Zahlung des Lösegeldes garantiert allerdings nicht, dass die Daten auch tatsächlich wieder entschlüsselt werden.) *Siehe auch* →Kryptowährung *und* →Malware.

Remote Access Trojaner (RAT): Malware mit einer Backdoor, mit deren Hilfe Angreifer Admin-Zugriff auf den Zielrechner bekommen.

Rootkit: Malware, die Angreifern Zugriff auf Root-Ebene gibt. *Siehe* → Malware.

Schwachstelle: Fehler in einer Software, der durch Angreifer ausgenutzt werden kann. *Siehe auch* →Exploit.

Secure Sockets Layer (SSL): Transportschicht (Transport Layer)-Protokoll, mit welchem sich Einzelsitzungen durch Verschlüsselung und Authentifizierung absichern lassen, um die Kommunikation zwischen Clients und Servern zu schützen.

Shoulder Surfing: Der Angreifer erhält Einblick in sensible Daten des Opfers, indem er ihm entweder tatsächlich oder sprichwörtlich (z. B. mithilfe von optischen Hilfsmitteln) über die Schulter schaut.

Social Engineering: Angriff, bei dem Techniken wie →Shoulder Surfing *und* →Dumpster Diving zum Einsatz kommen. Die Angreifer gelangen so mit geringem technischen Aufwand an sensible Daten wie Passwörter.

Spam: Unerwünschte Massenmails, die nicht selten auch Malware via infizierter Mailanhänge oder Links zu bösartigen Webseiten verbreiten. *Siehe auch* →Malware.

Spearphishing: Gezielt auf ein Opfer zugeschnittener Phishing-Versuch, der dadurch besonders glaubwürdig wirkt und mit entsprechend größerer Wahrscheinlichkeit erfolgreich ist. So kann als (vermeintlicher) Absender die Mailadresse eines Unternehmen oder einer Person verwendet werden, die das Opfer kennt. *Siehe auch* →Phishing.

Spyware: Schadsoftware, die ohne Wissen und Einwilligung des oder der Betroffenen Informationen über Einzelpersonen oder Unternehmen sammelt. *Siehe auch* →Malware.

SSL Hiding: Technik, bei der Angreifer die SSL-Verschlüsselung nutzen, um die Inhalte des Netzwerktraffics zu verschleiern und so Schutzmechanismen des Netzwerks für eine gewisse Zeit zu umgehen. In dieser Zeit können sie unbehelligt sensible Daten stehlen (Data Exfiltration).

Transmission Control Protocol (TCP): Eines der zentralen Internetprotokolle. TCP ergänzt das →Internet Protocol (IP), weshalb man auch meist von TCP/IP spricht. TCP sorgt für die sichere und strukturierte Übertragung von einem Programm auf einem Computer zu einem Programm auf einem anderen Computer. Die meisten Anwendungen im Internet, darunter das World Wide Web, E-Mail, Remote-Administration und Datei-Transfer nutzen TCP.

Trojaner: Schadsoftware, die vorgibt, eine bestimmte Funktion auszuführen, tatsächlich aber eine andere (im Allgemeinen schädliche) Aktivität durchführt.

Unified Threat Management (UTM): Security-Appliance, die verschiedene Funktionalitäten in sich vereint, z. B. Firewall, Malwareschutz und Schutz vor unerwünschten Eindringlingen (→IDS/→IPS).

Uniform Resource Locator (URL): Eine eindeutige Adresse im World Wide Web.

Verschlüsselung: Umwandlung von →Plaintext in →Chiffretext.

Virtual Local Area Network (VLAN): Lokales Teilnetz, welches vom Gesamtnetzwerk abgetrennt ist und unabhängig von diesem läuft.

Virtual Private Network (VPN): Ein privates Netzwerk, mit welchem dank Verschlüsselung und Kapselung nicht-öffentlich über ein öffentliches Netzwerk kommuniziert werden kann.

Virus: Programmcode, der sich in einem anderen Computerprogramm einnistet mit dem Ziel, sich zu reproduzieren und zu verbreiten. *Siehe auch* →Malware.

Web Application Firewall (WAF): Spezielle Firewall zum Schutz webbasierter Anwendungen und von Webservern.

Wurm: Schadsoftware, die sich nach der ersten Ausführung von allein von Rechner zu Rechner verbreitet. Im Gegensatz zum →Virus verbreitet sie sich, ohne fremde Dateien mit ihrem Code zu infizieren. *Siehe auch* →Malware.

IHRE DATEN – IHR KAPITAL

Schützen Sie Ihr Unternehmen vor Datenpannen und Sicherheitslecks

ESET Endpoint Encryption – Umfassender und komfortabler Schutz für sensible Daten:

- Sichere Verschlüsselung von Festplatten, Wechselmedien, Dateien und Postfächern.
- Höchste Sicherheit für Daten entsprechend der gesetzlichen Vorgaben.
- Die perfekte Ergänzung für noch besseren Schutz: ESET Secure Authentication.

Entdecken Sie die ganze Vielfalt der ESET Produkte.

eset ENJOY SAFER TECHNOLOGY™

ESET.DE | ESET.AT | ESET.CH

Schützen Sie die Daten in Ihrem Unternehmen!

Beinahe täglich werden Meldungen zu Datenlecks und Angriffen auf Unternehmen veröffentlicht. Es zeigt sich, dass auch kleine und mittelständische Unternehmen den Schutz von Daten auf keinen Fall vernachlässigen dürfen. *Datenschutz für Dummies* soll Ihnen helfen, für Ihr Unternehmen passende Technologien und organisatorische Maßnahmen zu finden – egal ob Sie Einzelunternehmer sind oder 250 Mitarbeiter beschäftigen. Erfahren Sie alles Wichtige zu den neuesten Sicherheitstechnologien, Tools und Prozessen, um die negativen Folgen möglicher Datenschutzvorfälle so gering wie möglich zu halten.

Erfahren Sie...

- ... welche Folgen Cyberangriffe für Unternehmen haben können.
- ... welche Möglichkeiten es gibt, die Datensicherheit in Ihrem KMU zu stärken (inklusive Technologien, Deployment-Optionen und Service-Modelle).
- ... welche Vorteile effektiver Datenschutz für Ihr Unternehmen bietet.
- ... welchen unternehmerischen Wert wirksamer Datenschutz hat.

ISBN: 978-1-119-60684-0
Nicht für den Wiederverkauf bestimmt.

für dummies®

Auch als E-Book erhältlich

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.