



© anatolir – AdobeStock.com

Cybercrime

**Cybercrime hat viele Gesichter –
und es kommen immer mehr dazu.
Schützen Sie sich und Ihr Unternehmen**

Inhaltsverzeichnis



Cybercrime – die größte Gefahr des 21. Jahrhunderts

1

Fakten zum Thema IT-Sicherheit

2

Motive der Hacker – warum wird angegriffen?

3

Gute Hacker setzen ihre Fähigkeiten nicht ein, um Schaden anzurichten

5

Angreifer haben unterschiedliche Angriffsziele

6

Tipps zum Schutz vor Social Engineering

8

Prävention ist immer günstiger

10

Wie sich Unternehmen schützen können

11

Fazit: Ohne Datenschutz der Willkür ausgeliefert

12

Cybercrime – die größte Gefahr des 21. Jahrhunderts

Aufgrund der Digitalisierung sind die gesellschaftliche Entwicklung sowie deren Dynamik höchst komplex geworden. Egal ob Internet of Things oder neue Geschäftsmodelle – letztendlich basiert alles auf dem Austausch und der Auswertung von Daten. Aber neben den großen Chancen, die damit verbunden sind, ergeben sich auch viele Risiken. Leider sind die virtuellen Gefahren, die wohl am meisten unterschätzte Bedrohungen des 21. Jahrhunderts. Erpressungswellen im Internet, die mittels Bank- und E-Commerce-Betrug Privatpersonen um das Ersparte bringen oder die im Firmenumfeld mittels Ransomware Daten verschlüsseln, sind hier nur zwei Beispiele. Allein die Deutsche Telekom registriert bis zu 46 Millionen Cyberangriffe – pro Tag, die totale Vernetzung der Welt macht es möglich.



© timusi – pixabay

Hacker verursachen Schäden in Milliardenhöhe.

Gemäß dem Branchenverband Bitkom entsteht der deutschen Wirtschaft durch Datendiebstahl, Spionage und Sabotage ein jährlicher Schaden in Höhe von 55 Mrd. €. Über 70 % der Unternehmen in Deutschland sind pro Jahr nachweislich von Cyberangriffen betroffen. Die Welt dreht sich einfach zu schnell. Das kann an folgendem Beispiel deutlich gemacht werden: Um eine Nachricht im Jahre 1860 über 3.000 km zu senden, wurden im Durchschnitt zehn Tage benötigt. Im Einsatz waren 120 Pferde und 40 Reiter, die Tag und Nacht im Sattel saßen. Dazu 127 Stationen für Pferde- und Reiterwechsel, denn alle 16 km musste das Pferd gewechselt werden. Heute benötigt eine solche Nachricht gerade ein paar Millisekunden.

Versprochen wird uns eine neue, bessere und einfachere Welt. Doch die Wahrheit sieht ganz anders aus. Belohnt wird in der Computer- bzw. Software-Industrie vor allem nur eines: Innovationen, die es schaffen, den Menschen dazu zu verleiten, noch mehr Daten über sich und sein Unternehmen preiszugeben. Die Illusion ist perfekt: Freiheit durch Datenfreizügigkeit. Daher stehen gerade Datenschützer täglich vor großen Herausforderungen.

Fakten zum Thema IT-Sicherheit

Aufgrund der Komplexität steigt auch die Gefahr, dass durch Datenpannen und Hackerangriffe mit Datenverlusten, Wirtschaftsspionage oder auch das Ausspähen umfangreich verknüpfter sensibler Persönlichkeitsdaten große Schäden angerichtet werden können. An dieser Stelle möchte ich Ihnen ein paar Fakten zum Thema IT-Sicherheit aufzeigen, die Ihnen deutlich machen, wie die Situation heute und zukünftig gemäß laut einer Studie von McAfee sein wird:

Geschätzte tägliche Cyberkriminalität	
Cybervergehen	Geschätzte tägliche Aktivität
Bösartige Scans	80 Milliarden
Neue Malware	300.000
Phishing	33.000
Ransomware	4.000
Durch Hacking verlorene Datensätze	780.000

Diese Zahlen machen deutlich, dass die Lage ernst ist und die Bedrohung weiter zunehmen wird. Mithilfe der Nutzung künstlicher Intelligenz wird die Hacker-Industrie auch noch gefährlicher, denn die künstliche Intelligenz täuscht die gebräuchlichen Sicherheitsvorkehrungen ferner durch Imitation menschlichen Verhaltens.

TIPP: Um die geeigneten technischen und organisatorischen Maßnahmen ergreifen zu können, sollten Sie sich als Datenschutzbeauftragter unter anderem fragen, was auf welche Weise über das Internet erreichbar ist und zu welchem Zweck.

Unternehmen befinden sich in einem laufenden Spannungsverhältnis von Flexibilität versus Datenschutz und Datensicherheit. Die meisten wissen erst gar nicht, was ihre speziellen kritischen Prozesse und was genau ihre wertvollen Daten sind. Als Datenschutzbeauftragter ist es daher hier auch Ihre Aufgabe, die Kategorisierung von Daten vorzunehmen bzw. die Kritikalität von Daten transparent zu machen.

Motive der Hacker – warum wird angegriffen?

Sicherlich wurden Sie als Datenschutzbeauftragter schon häufig von privaten Personen, Kollegen oder auch der Geschäftsleitung von Unternehmen mit der Frage konfrontiert „Warum sollten gerade meine/unsere Daten so interessant für Hacker sein?“ Jeder denkt, seine personenbezogenen Daten seien uninteressant oder irrelevant für Hacker, und somit könnte einen selbst als Person oder Unternehmen ein Hacking-Angriff nicht treffen. Weit gefehlt!

Die Anbindung von Produktionssystemen ans Internet und an Clouddienste verspricht im Zuge der Industrie 4.0 mehr Effizienz und Produktivität im Industrie- und Infrastruktursektor. Doch Vorsicht, denn diese bieten durch zusätzliche digitale Komponenten eine deutlich höhere Anzahl an Schwachstellen und Angriffsmöglichkeiten für Hacker. Als eine der größten Industrienationen steht damit natürlich die Bundesrepublik Deutschland ganz oben auf der Liste von Cyberkriminellen.

Ein falsches Verständnis in den Unternehmen führt häufig dazu, dass der Datenklau nicht ernst genommen wird. Noch immer denken kleine und mittlere Unternehmen, sie seien zu unbedeutend, um angegriffen zu wer-

den. Konzerne dagegen glauben, ausreichend geschützt zu sein. Beides ist in der Regel falsch. Gestohlene Kundendaten oder entwendete Kreditkarteninformationen sind dabei nur besonders offensichtliche Ziele. Die Monetarisierbarkeit von offenkundig nicht mit Finanzdaten verknüpften Informationen geht viel weiter! Die Motive der Hacker sind vielfältig.

Meistens verschaffen sie sich unberechtigten Zugang zu fremden Computersystemen, um die Kontrolle über das System zu übernehmen oder Daten zu stehlen. Hier werden die gestohlenen Informationen gegen Lösegeld zum Rückkauf angefordert oder an die Öffentlichkeit getragen. Auch der Diebstahl von Daten, die beispielsweise für das Internetbanking benutzt werden, ist immer wieder Thema. Eine beliebte Methode der Hacker ist der sogenannte Drive-by Download, hierbei wird, sobald ein User eine Seite besucht, für ihn unbemerkt, eine Software heruntergeladen. Dies geschieht, ohne dass der Nutzer irgendetwas bestätigen muss. Die Software hat danach dieselben Rechte, wie der in das Betriebssystem eingeloggte Nutzer. Hierbei kann also das Internetbanking durch einen Hacker ausgeführt werden – welchen Schaden dies im Unternehmen anrichten wird, kann sich wohl jeder selber ausmalen. Ein weiteres Motiv von Hackern ist das Aufdecken von Sicherheitslücken. Die Idee dahinter ist, dass Schwachstellen in der Soft- und Hardware erkannt und verbessert werden. Vor einigen Jahren hat sich ein Journalist aus den Niederlanden mithilfe der Smartcard eines ehemaligen Mitarbeiters Zugang zum Regierungsgebäude verschafft, die Smartcard hatte offensichtlich noch alle Funktionen, die damals dem Mitarbeiter eingeräumt wurden. Die Beweggründe von Hackern sind also vielfältig. Für einige sind nur wirtschaftliche Gründe entscheidend. Wirtschaftsspionage oder Konkurrenzausspähung ist dann der Fokus der Hacking-Attacke. Oder aber Hacker finanzieren sich mithilfe selbst geschriebener Software, die Sicherheitslücken aufdeckt. Was die Käufer mit diesen Informationen anstellen, interessiert die Täter nicht.

Aktuell ist neben dem Erpressungsversuch auch Cryptojacking ein großes Geschäft, denn das Schürfen von Kryptowährungen ist sehr lukrativ. Hier werden Computer, Smartphones, Tablets oder sogar Server ohne das Wissen der Benutzer verwendet, um insgeheim Kryptowährung auf Kosten des Opfers zu schürfen. Anstatt spezielle Computer für das Cryptomining zu bauen, stehlen Hacker mittels Cryptojacking die Ressourcen von Dritten, die ihnen zum Opfer fallen. Wenn man all diese Ressourcen addiert, sind Hacker in der Lage, mit hoch entwickelten Cryptomining-Operationen mit-

zuhalten, ohne für die teuren Betriebskosten aufkommen zu müssen. Wenn Sie zum Opfer von Cryptojacking werden, merken Sie es womöglich nicht. Die meiste Cryptojacking-Software bleibt dem Benutzer von ihrem Design her verborgen, aber das heißt nicht, dass dies keinen Preis hat. Dieser Diebstahl Ihrer Rechenressourcen verlangsamt andere Prozesse, treibt Ihre Kosten für Strom in die Höhe und verkürzt das Leben Ihres Equipments. Die Motivation hinter Cryptojacking ist einfach: Geld.

Gute Hacker setzen ihre Fähigkeiten nicht ein, um Schaden anzurichten

Glücklicherweise gibt es auch Hacker, die ihr Können in einem legalen Beruf einsetzen, die sogenannten Penetrationstester. Unter einer Penetration versteht man in der IT das unautorisierte Eindringen in ein System, meistens durch eine Fremdperson. Ein Penetrationstest ist die Prüfung der Sicherheit eines Systems durch Anwenden von Mitteln und Methoden, die ein Hacker zur Durchführung eines Angriffs verwenden könnte. Im Gegensatz zu Vulnerability Scans, in denen ein Tool automatisiert nach Sicherheitslücken sucht, wird ein Penetrationstest immer von einer Person, dem Penetrationstester, und nicht von einer Maschine durchgeführt. Damit soll das Szenario eines Angriffs originalgetreu simuliert werden. Die breit gestreute Motivation der Hacker macht vorbeugende Maßnahmen so komplex. Es ist nicht immer der Täter von außen, der angreift, sondern auch der Innentäter muss bedacht werden. Aufgrund der großen Mengen werden zunehmend Daten und auch die Tools zur Auswertung in die Cloud ausgelagert.

Damit entsteht für die Unternehmen eine Abhängigkeit von Cloudanbietern. Falls hier keine geeigneten Konzepte zur Sicherung der eigenen Daten seitens der Unternehmen bestehen, könnte ein Angriff auf einen zentralen Anbieter (z. B. Amazon, hier Amazon Web Services einen enormen wirtschaftlichen Schaden anrichten. Darum muss jeder Datenschutzbeauftragte die Auftragsdatenverarbeitung auch in den absoluten Fokus seiner Tätigkeiten rücken. Die Überprüfung der technischen und organisatorischen Maßnahmen ist deshalb so wichtig geworden. Wenn das Unternehmen geeignete Maßnahmen zum Schutz ergriffen hat, bleiben durch Dienstleister noch immer Risiken bestehen.

TIPP: Sinnvoll ist die Überprüfung der technischen und organisatorischen Maßnahmen vor Beginn bzw. Durchführung der Verarbeitung von Daten im

Auftrag. Leider ist dies in der Praxis oft schwierig. Nur so kann aber im Vorfeld verhindert werden, dass Daten nur auf dem Papier sicher übermittelt und ausgetauscht werden. Die Datenschutz-Grundverordnung (DSGVO) verlangt in Art. 28 Abs. 3, dass die Auftragsverarbeitung in einem Vertrag niedergelegt wird. Dieser Vertrag bindet den Auftragsverarbeiter in Bezug auf den Verantwortlichen. Des Weiteren sind Gegenstand und Dauer der Verarbeitung, deren Art und Zweck, die Art der personenbezogenen Daten, die Kategorien betroffener Personen sowie die Pflichten und Rechte des Verantwortlichen als Mindestinhalte festzulegen.

Aber Vorsicht: Verantwortlicher und Auftragsverarbeiter haften gemäß Art. 82 DSGVO als Gesamtschuldner für einen durch die Datenverarbeitung entstandenen Schaden, Durch die DSGVO kann die Nichteinhaltung von Auflagen zur Auftragsdatenverarbeitung mit Geldbußen von bis zu 10 Mio. € bzw. von 2 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden. Die Bußgeldtatbestände gelten für Auftraggeber wie Auftragnehmer gleichermaßen. Nur gehen die Rechtsfolgen eines Datenschutzverstoßes in den meisten Fällen voll zulasten der verantwortlichen Stelle, also des Auftraggebers. Dieser kann den Auftragnehmer dann allenfalls in Regress nehmen. Allerdings ist in den meisten Verträgen die Haftung faktisch in Bezug auf die Vertragssumme beschränkt und deckt damit meistens nicht das Schadensrisiko beim Auftraggeber ab.

Angriffe haben unterschiedliche Angriffsziele

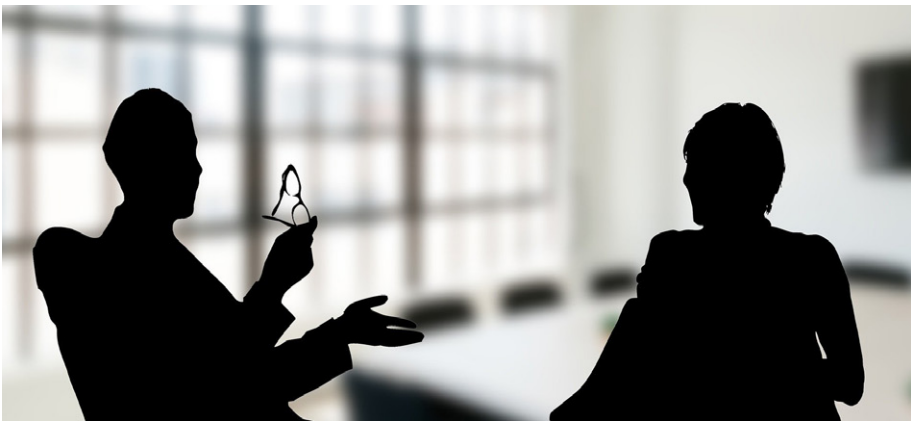
Um die Daten im Unternehmen effizient zu schützen, sollten Sie auch als Datenschutzbeauftragter wissen, wie jemand denkt, der personenbezogene Daten stehlen möchte. Angriffe werden oft über das Social Engineering erfolgreich durchgeführt. Allerdings haben Angreifer immer unterschiedliche Angriffsziele. Dabei ist zu berücksichtigen, dass es verschiedene Typen von Hackern gibt: z. B. die Scriptkiddies, denen es nur um die reine Action geht, oder die Hacktivist*innen, bei denen soziale oder politische Motive im Vordergrund stehen. Beschäftigen sollten Sie sich als Verantwortlicher insbesondere mit der Gruppe der organisierten Cyberkriminellen, die gezielte, gut getarnte Angriffe durchführen. Spionage und Sabotage stehen bei ihnen im Vordergrund und können so den Unternehmen erheblichen Schaden zufügen.

TIPP: Welche Aktivitäten Ihres Unternehmens sind für die Gruppe der Hacker von besonderer Bedeutung? Achten Sie immer darauf, mit welchen

Informationen über die Mitarbeiter des Unternehmens Verknüpfungen hergestellt werden können, um damit ein umfassendes Profil zu ermöglichen.

Die Optionen der Täter nehmen mit der immer stärkeren Vernetzung unserer Welt weiter zu. Es gibt Suchmaschinen, die es, anders als Google, nicht auf Ergebnisse über Personen absehen, sondern ganz andere erstaunliche Informationen bieten.

John Matherly ist der Mann, der diesen Service betreibt. Shodan wird als die gefährlichste Suchmaschine der Welt bezeichnet. Die Suchmaschine ist insofern einzigartig, als dass sie sich Sicherheitslücken zunutze macht. Mit ihr kann man nach Servern, Routern, spezieller Software und vielem mehr suchen. Auch die Suche nach ungesicherten Webcams ist möglich. Unheimlich, oder? Genau das ist aber für einen Angreifer ideal. Mittels der Eingabe einer URL, also ohne großen Aufwand, bekommt er Informationen darüber, welche Geräte ohne ausreichenden Schutz mit dem Internet verbunden sind. Daher lohnt sich auch hier für den Datenschutzbeauftragten einmal ein Blick in diese Suchmaschine. Vielleicht sind ja Geräte aus Ihrem Unternehmen nicht mit den entsprechenden technischen Maßnahmen zum Schutz personenbezogener Daten versehen. In Zusammenarbeit mit den entsprechenden Abteilungen und Verantwortlichen in Ihrem Unternehmen können Sie dann die richtigen Maßnahmen in Zusammenarbeit gemeinsam festlegen und den angemessenen Schutz wiederherstellen.



© Gerd Altmann – pixabay

Social Engineering ist äußerst erfolgreich.

Tipps zum Schutz vor Social Engineering

Datenschutz und IT-Security erfordern sowohl die Aufmerksamkeit der Unternehmensführung als auch die der Mitarbeiter. Besonders die Mitarbeiter-Awareness ist einer der grundlegenden Erfolgsfaktoren. Die Einschätzung von Mitarbeiterinnen und Mitarbeitern zu den Folgen von verlorengegangenen oder gestohlenen Daten ist leider aus Unwissenheit manchmal eher naiv und verharmlosend. Aus ihrer Perspektive sind die Folgen nicht immer absehbar, manche Handlung erfolgt unbewusst und ohne die Konsequenzen zu bedenken. Ein Angreifer will, dass sein Opfer aktiv wird. Dabei kann die Handlung so einfach wie die Beantwortung einer Frage oder aber so folgens schwer wie die Erlaubnis sein, in einen bestimmten gesicherten Bereich eines Unternehmens eintreten zu dürfen.

Um sein Opfer zur Mitarbeit zu bewegen, wird der Angreifer versuchen, den Mitarbeiter in ein Gespräch zu verwickeln, das die gewollte Aktion auslöst. Für den Angreifer ist es entscheidend, ob es ihm möglich ist, Informationen zu entlocken. Dafür wird er alles tun, damit sein Opfer sich wohl fühlt und widerspruchlos Informationen preisgibt. Durch Suchmaschinen und damit verbundene webbasierte Abfragen kann er sich ideal auf das Gespräch vorbereiten. Je mehr Daten er findet, desto einfacher wird es, das Verhalten seiner Opfer zu manipulieren. Deshalb muss die Unternehmensführung im Rahmen der internen Kommunikation ihre Mitarbeiterinnen und Mitarbeiter sensibilisieren. Praktische Beispiele können auch Sie als Datenschutzbeauftragter geben, die helfen, konkrete Auswirkungen zu prognostizieren und mögliche Konsequenzen anhand folgender Fragestellungen visuell deutlich zu machen: Was würde passieren, wenn ein unternehmenseigenes Laptop oder Smartphone mit Detailinformationen zu Produkten aus einem Firmenkoffer gestohlen wird? Angenommen, ein Vertriebsmitarbeiter kündigt und wechselt zu einem Marktbegleiter. Er nimmt Kundendaten auf einem USB Stick mit. Was kann er damit anfangen und kann er dem Unternehmen Schaden zufügen? Zu berücksichtigen sind die folgenden 12 goldene Regeln zum Schutz von Daten:

I. Technische Aspekte

1. Benutzung von sicheren Passwörtern
2. Bildschirme sperren
3. geeignete Informationswege wählen, kein ungeschützter Datenverkehr
4. Funktionsstellen deaktivieren (Bluetooth, WLAN, ...)

II. Verhaltensaspekte

5. sensible Informationen jeglicher Art schützen
6. offene Augen und Ohren, Unregelmäßigkeiten melden
7. elektronischen Hinweisen nicht folgen
8. Verantwortung für Informationen selbst übernehmen
9. Sicherheit vor Flexibilität
10. Sicherheitsvorfälle melden
11. Warnmeldungen ernst nehmen
12. Sicherheitspolicies ernst nehmen und hinterfragen

Als Datenschutzbeauftragter sollten Sie die Mitarbeiter vor allem für die folgenden Situationen sensibilisieren:

1. Schweigen kann Gold wert sein!

Angreifer täuschen eine falsche Identität vor. Mitarbeiter sollten daher keine Auskünfte geben, zu denen sie nicht ausdrücklich ermächtigt worden sind. Das gilt für die Arbeits- und Betriebsorganisation, Verantwortlichkeiten oder persönlichen Informationen von Kollegen. Als Datenschutzbeauftragter sollten Sie die Mitarbeiter dahingehend sensibilisieren, dass sie nur so viele Informationen preisgeben wie nötig und ungewöhnliche Anliegen eines Anrufers hinterfragen. Wenn Mitarbeiter Informationen als wertlos oder nur von geringem Wert ansehen, werden sie sich auch keine Mühe beim Schutz der Daten geben. Menschen haben eine innewohnende Hilfsbereitschaft und wollen jemandem helfen, der hilflos wirkt. Dieses Verhalten ist aber ein wesentlicher Bestandteil der Manipulation durch den Angreifer.

2. Achtung bei fremden Personen

Möchte ein scheinbar neuer Mitarbeiter aus der IT oder eines Dienstleisters dringend neue Sicherheitsupdates einspielen, sollten Mitarbeiter Rücksprache mit ihrem Vorgesetzten halten. Der vermeintlich bedeutungslose Computer dient dem Angreifer oftmals als Türöffner ins Unternehmensnetzwerk und ermöglicht es so, an sensible Informationen zu gelangen. Unbekannte Personen auf den Fluren oder gar in den Unternehmensräumen, offen stehende Türen, die in der Regel geschlossen sind, noch nicht da gewesene technische Vorrichtungen – Mitarbeiter sollten dies Vorgesetzten, wenn sie etwas Merkwürdiges beobachten, mitteilen und vor allem sich nicht davor scheuen unbekannte Personen auf dem Firmengelände anzusprechen.

3. Sicherheit im Büro und bei der Kommunikation

Das Büro, wenn dort niemand anwesend ist, sollte immer verschlossen sein. Vertrauliche Dokumente sollten niemals direkt in den Papierkorb, sondern immer geschreddert werden. Der Rechner sollte immer gesperrt werden, wenn der Mitarbeiter diesen verlässt. Andernfalls besteht die Gefahr, dass jemand an Informationen gelangt, die nicht für ihn bestimmt sind, und sich beispielsweise unter falschem Vorwand weitere Informationen erschleichen kann. Findet ein Mitarbeiter ein Wechselmedium, wie z. B. einen USB-Stick, sollte dieser an den Vorgesetzten übergeben werden. Gefundene Wechselmedien dürfen niemals an einen Firmenrechner angeschlossen werden. Machen Sie den Mitarbeitern in Zusammenarbeit mit der Geschäftsleitung klar, über welche Kommunikationskanäle (Telefon, Fax, E-Mail oder Brief) mit Geschäftspartnern, Kunden und neuen unbekannten Kontakten in welcher Weise kommuniziert werden darf.

Prävention ist immer günstiger

Neben dem Reputationsverlust für das Unternehmen durch die Berichterstattung in der Presse, sozialen Netzwerken und in Blogs ist der Datenverlust der höchste Kostenpunkt. Die Risiken IT-basierter Geschäftsprozesse werden heute leider in vielen Unternehmen unterschätzt. Am sinnvollsten ist hier eine Analogie aus der Medizin: Um Karies zu verhindern, muss sich jeder täglich die Zähne putzen und regelmäßig zur Vorsorgeuntersuchung zum Zahnarzt gehen. Das ist zwar manchmal lästig, aber ein gesundes Lächeln ist durch nichts zu ersetzen und jeder freut sich, wenn er den Zahnarzt, ohne dass gebohrt werden musste, wieder verlassen kann. Zudem ist es wirtschaftlich sinnvoll, denn tägliche Zahnpflege kostet nicht annähernd den Betrag, den eine Krone oder gar ein Gebiss kostet. In der vierten Ausgabe des jährlichen globalen Ransomware Report von Datto werden die Kosten für die Ausfallzeit der IT-Systeme auf durchschnittlich 121.500 Euro beziffert. Der Report zeigt ebenfalls, dass die Kosten für Ausfallzeiten über 23-mal höher sind als die Lösegeld-Forderung der Cyber-Kriminellen, die durchschnittlich bei ca. 5.070 EUR liegt. Wenn nur ein Teil dieser Zeit und dieses Betrags in den Datenschutz mit seinen technischen und organisatorischen Maßnahmen stecken würde, wird schon deutlich, wie viel mehr an Sicherheit erreicht werden könnte. Nur wer die IT-Umgebung und auch deren Schachstellen kennt, kann sie wirksam absichern. Das schafft die Voraussetzung für effizientes Konfigurations- und Patchmanagement. Damit gelingt es laut dem Bundesamt für Sicherheit in der Informations-

technik Unternehmen, bis zu 95 % aller potenziellen Hacker-Angriffe bereits im Vorfeld zu verhindern.

Wie sich Unternehmen schützen können

Neben allen technischen und organisatorischen Aspekten, kann es sinnvoll sein, für das Unternehmen eine Versicherung gegenüber Hacking-Risiken abzuschließen. Diese sogenannten Cyberversicherungen müssen in der digitalen Wirtschaft zur Selbstverständlichkeit werden. Das Risiko durch Cyberangriffe ist für viele Unternehmen wesentlich höher als bei den bekannten „klassischen“ Gefahren, wie etwa Feuer und Wasserschaden.

In Bezug auf einen Hacking-Angriff stellt sich nicht die Frage, ob er passieren wird, sondern nur wann! Cyberversicherungen decken verschiedenste finanzielle Schäden ab und unterstützen im Schadensfall. Bevor Unternehmen versichert werden, prüfen allerdings die Versicherungen die technischen und organisatorischen Maßnahmen und geben Empfehlungen, wie sich die Risiken minimieren lassen. In diesem Moment kommt dann auch wieder die Auftragsverarbeitung in Spiel: Ist alles vollständig dokumentiert? Ist die Liste der Dienstleister vollständig und ist mit allen Geschäftspartnern, die personenbezogene Daten verarbeiten, ein Vertrag gemäß Art. 28 DSGVO geschlossen? Als Datenschutzbeauftragter sollten Sie auch die Hersteller und Lieferanten von Komponenten und Software in die Mitverantwortung für Sicherheitslücken in ihren Produkten nehmen. Fragen Sie hier nach, welche technischen und organisatorischen Maßnahmen schon „ab Werk“ ergriffen worden sind oder was im Vorfeld schon geleistet werden kann. Datenschutz ist ohne Datensicherheit nur eine leere Hülle.

Oft als „Showstopper“ empfunden, sind es aber gerade solche Fragen, die ein Qualitätsverbesserungsmerkmal darstellen. Leider ist bei der Entwicklung ein Ansatz nach dem Prinzip Privacy by Design aktuell noch eher selten. Damit der Datenschutz aber gewissen Sicherheits- und Qualitätsstandards folgen kann und Angreifer bei der Datenkommunikation nicht diverse Sicherheitslücken vorfinden, ist es fundamental, die Angriffsszenarien bei der Entwicklung zu bedenken. Da Hacking-Angriffe und andere Cyberattacken immer häufiger speziell auf Firmen und Branchen zugeschnitten und damit nur sehr schwer abzuwehren sind, empfiehlt es sich, im Unternehmen über den Aufbau eines Computer Emergency Repsonse Teams (kurz: CERT) nachzudenken. Dies ist eine Gruppe von IT-Sicherheitsfachleuten,

die bei der Lösung von konkreten IT-Sicherheitsvorfällen (z. B. gezielten Angriffen) als Koordinator mitwirkt bzw. sich ganz allgemein mit Computersicherheit befasst, indem sie Warnungen vor Sicherheitslücken herausgibt, aber auch direkt Lösungsansätze mit anbietet. Was aber vor allem entscheidend ist: Wenn Sie sich mit der Zusammensetzung eines solchen CERT auseinandersetzen, werden von selbst die wichtigen Fragen im Rahmen der Prävention für solche Krisenszenarien gestellt: Wer kümmert sich bei einem Angriff um die IT-Infrastruktur? Gibt es einen Spezialisten, den wir zu Hilfe holen müssen? Wer macht die Pressearbeit und fungiert hier als Ansprechpartner? Gibt es für ein solches Szenario Notfallkonzepte und Wiederanlaufpläne, gerade auch in Bezug auf das Einspielen eines Back-ups?

Fazit: Ohne Datenschutz der Willkür ausgeliefert

Das Feld der IT-Sicherheit ist ein interdisziplinäres Arbeitsgebiet, denn die Datenverarbeitung durchzieht das gesamte Unternehmen und schafft eine starke Abhängigkeit im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der technischen Systeme. Alles unterliegt einer dynamischen Entwicklung für die neu geschaffenen technischen Möglichkeiten. Es geht beim Datenschutz nicht darum, die Daten um ihrer selbst willen zu schützen. Es geht vielmehr um den Schutz der Personen, denen die Daten zugeordnet werden. Dieses Verfahren sowie deren Implikationen sind jedem theoretisch wohl bekannt: Wenn jemand einen Arzt besucht, soll auch sichergestellt sein, dass die Daten nicht in falsche Hände geraten. Nur faktisch besteht dieser Anspruch im Zusammenhang mit den Profilen, die durch das Surfen im Web entstehen, eben nicht. Das hängt keinesfalls nur mit der – für viele unklaren – Definition des Begriffs „Datenschutz“ zusammen, sondern auch mit den absichtlich kaum vorhandenen Möglichkeiten, sich zur Wehr setzen zu können, und damit wird dem Fatalismus das Spielfeld überlassen! Hier muss der Staat eingreifen und die Spielregeln festlegen.



ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28/9 55 01 50, Fax: 02 28/3 69 64 80
Internet: www.privacyxperts.de
E-Mail: kundendienst@privacyxperts.de

Vorstand: Richard Rentrop

Verantwortlicher i.S.d.P: Michael Jodda, Theodor-Heuss-Str. 2-4, 53095 Bonn

Autor: Andreas Würtz

Satz: Holger Hellendahl, Neuss

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

© 2020 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Bukarest, Manchester, Warschau