Thomas R. Köhler

CHEFSACHE CYBER SICHERHEIT

campus

Thomas R. Köhler

CHEFSACHE
CYBERSICHERHEIT

Der 360-Grad-Check
für Ihr Unternehmen

Campus Verlag
Frankfurt/New York

ISBN 978-3-593-51373-7 Print
ISBN 978-3-593-44742-1 E-Book (PDF)
ISBN 978-3-593-44741-4 E-Book (EPUB)

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt.
Jede Verwertung ist ohne Zustimmung des Verlags unzulässig. Das gilt
insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen
und die Einspeicherung und Verarbeitung in elektronischen Systemen.
Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung
für die Inhalte externer Links. Für den Inhalt der verlinkten Seiten sind
ausschließlich deren Betreiber verantwortlich.
Copyright © 2021. Alle deutschsprachigen Rechte bei Campus Verlag GmbH,
Frankfurt am Main.
Umschlaggestaltung: Guido Klütsch, Köln
Umschlagmotiv: © shutterstock/Varunyuuu (Hintergrund) shutterstock/senee sriyota (Schild)
Satz: Publikations Atelier, Dreieich
Gesetzt aus der Sabon Next und der URW DIN
Druck und Bindung: Beltz Grafische Betriebe GmbH, Bad Langensalza
Printed in Germany

www.campus.de

INHALT

Cybersicherheit ist Chefsache! 7
Alarmierend – Cyberattacken in Zahlen 7
Schädlich – vielfältige Kosten durch Cyberangriffe 8
Bedenklich – Sorglosigkeit in der Chefetage 9
Fatal – Kleinreden der Cybersecurity 11
Vorbildlich – Wege aus dem Cybersecurity-Dilemma 15

1 Attacken von vielen Seiten 22
Eine altbekannte Plage – Computerviren und -würmer 22
Hinterhältig – Trojaner 24
Hier lockt das große Geld – E-Mail-Scams 26
Sie haben Post! Phishing-Mails als Einfallstor 34
Social Engineering – Täuschungsmanöver auf hohem Niveau 42
Enkeltrick für Unternehmen – CEO-Fraud 47
Erpressung und Datendiebstahl in einem – dank Ransomware 50
Angriff der Bots – lahmgelegte Websites durch DDoS-Attacken 63
Ihre Abwehrkräfte – mobilisieren Sie Ihre Verteidigung! 64

2 Cybersecurity im Zeichen der Burg 82
Innerhalb der Burgmauern – Cybersecurity im Büro 83
Wildwuchs in der Ablage – Datensicherheit und Datenschutz 92
Smarte Geräte überall – intelligente Büroumgebung 99
Mobiles Arbeiten 105
Im Homeoffice 114
Dauerbrenner Cloud-Computing 120
Industrieanlagen und Logistik – lohnende Ziele 125
Fahrzeugsicherheit – mit einer neuen Dimension 131
Opfer überall – Cyberkriminelle ohne Skrupel 136

3 Ungleichgewicht zwischen Angriff und Verteidigung 141
Eine Lücke reicht – das Grundproblem der Cybersicherheit 142
Kennen Sie Ihre Feinde? Einige Typen und Motive 142

Die Gefahr von innen – Bedrohungen durch Mitarbeiter 149
Schlamperei – kaum Anreize für Sorgfalt 155
Die Sache mit der Anonymität – ohne klare Identität im Internet 162
Allein auf weiter Flur – der Chief Information Security Officer 167
Mit im Boot – Sensibilisierung der Mitarbeiter 173
Ihre Verteidigungslinien –
mehr Cybersicherheit in Ihrem Unternehmen 174

4 Künstliche Intelligenz und Cybersicherheit 185
Stand der Technik – wie intelligent ist KI? 186
Deep Fake – wem können Sie noch trauen? 190
Künstliche Helfer – mit Algorithmen gegen Cyberkriminelle 193

5 Ohne wirksames Gegenmittel 195
Attraktive Schlüsselstelle – Sicherheitsdienstleister im Visier 195
Versierte Marktschreier – mehr Schein als Sein 199
Spiel mit der Angst – und mit dem Feuer 201
Hart an der Grenze – Hilfe nach Ransomware-Attacken 202
Schwarze Schafe – auch in der Cybersicherheitsbranche 203

6 Investitionen in Cybersicherheit 205
Erste Einordnung – Marktprognosen und Investitionsvorhaben 205
Schwarz auf weiß – Kennzahlen für Cybersicherheit 208
IT-Benchmarking – Maßstab für IT-Ausgaben 214
Über den Daumen gepeilt – eine grobe Kostenschätzung 216
Undurchsichtige Vielfalt – Cybersecurity-Lösungen en masse 217

7 Die Kronjuwelen Ihres Unternehmens 221
Rundum geschützt – aber wie? 221
Schützenswert – was Cybersicherheit ausmacht 222
Das CE21-Cybersecurity-Modell 360+ 233
Sicherheit versus Komfort 236

Keine Illusionen, aber ein Hoffnungsschimmer 241

Glossar 245
Anmerkungen 259
Der Autor 272

CYBERSICHERHEIT IST CHEFSACHE!

Cybersicherheit ist Chefsache – eigentlich eine triviale Erkenntnis, möchte man meinen, angesichts von Sicherheitsvorfällen großer Tragweite, die immer wieder Schlagzeilen in den Medien machen. Im Zuge der Vernetzung unserer Lebens- und Arbeitswelt in den letzten 25 Jahren wurden wir mit neuen, teils unvorhersehbaren Risiken konfrontiert, von technischen Schwachstellen und Sicherheitslücken über Cyberkriminelle, die geschickt menschliche Schwächen ausnutzen, bis hin zu automatisierten Attacken, die potenziell unsere Infrastrukturen bedrohen.

Nicht selten wurden diese Risiken befeuert von einer Technologiebranche, die es über Jahrzehnte geschafft hat, sich aus der Verantwortung für ihre eigenen Produkte zu stehlen. Hinzu kommen schwarze Schafe in der Cybersecurity-Branche, die jede Gelegenheit nutzen, um potenzielle Kunden mit immer neuen Schreckensszenarien einzuschüchtern und ihnen möglichst viel Geld für unnütze Produkte und Dienstleistungen aus der Tasche zu ziehen. Umfassenden Schutz gibt es angeblich nur durch den Erwerb immer neuer Wunderwaffen gegen Cyberkriminalität in Gestalt von Programmen, Geräten und Diensten. Doch mitunter bringen die Sicherheitslösungen selbst neue Sicherheitsrisiken mit sich.

Alarmierend – Cyberattacken in Zahlen

Nach wie vor sind bei viel zu vielen kleinen und mittelständischen Unternehmen die Brisanz von Cyberattacken und die Relevanz des Themas Cybersicherheit für die eigene Zukunftsfähigkeit nicht bis in die Management- und Chefetagen durchgedrungen, allen dokumentierten Vorfällen zum Trotz.

Ein beliebtes Bonmot unter IT-Sicherheitsexperten lautet nicht von ungefähr: »Es gibt nur zwei Arten von Unternehmen – die, die gehackt wurden, und die,

die es noch nicht wissen.« Mehr als 1000 deutsche Unternehmen hat Bitkom Research für die Studie »Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt: Studienbericht 2020« befragt:[1] »75 Prozent der Unternehmen waren in den vergangenen zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen. Weitere 13 Prozent waren vermutlich betroffen – denn nicht immer lässt sich ein Angriff zweifelsfrei feststellen.« In Summe ist das ein deutlicher Sprung zu den Studienergebnissen aus 2015 und 2017, die jeweils knapp über 50 Prozent der Unternehmen als »Betroffene« identifiziert hatten. Und diese Identifikation kann dauern. Der US-Sicherheitsanbieter FireEye geht in seinen Sicherheitsreports für die EMEA-Region, zu der auch Deutschland gehört, durchschnittlich von 106 Tagen, also gut drei Monaten aus.[2] Der von IBM Security herausgegebene »Bericht über die Kosten einer Datenschutzverletzung 2020« nennt 279 Tage zwischen einem Sicherheitsvorfall und dessen Entdeckung, für Deutschland werden »nur« rund 170 Tage genannt.[3] Egal welchen Schätzwert man zugrunde legt: In jedem Fall ist es eine viel zu lange Zeit, in der sich die Angreifer ungestört umsehen, Daten exfiltrieren und Systeme manipulieren können.

Ein Lichtblick ist, dass die interne Risikobewertung der Unternehmen sich anscheinend langsam, aber sicher auf die Gefahr durch Cyberkriminelle einstellt. Einen Hinweis darauf liefert das Allianz-Risk-Barometer, das jährlich die wichtigsten Risiken aus Sicht der deutschen Unternehmen beleuchtet: 2013 waren nur rund 6 Prozent der Befragten der Meinung, dass Cybersicherheit ein wesentliches Businessrisiko sei. Damit landete sie auf Platz 15.[4] 2020 steht die Angst vor Cyberattacken an der Spitze der Liste[5] – meiner Meinung nach vollkommen zu Recht! Cyberattacken können heutzutage jeden treffen, und deswegen ist Cybersicherheit für alle Unternehmen, die großen, die mittelständischen und die kleinen, eine Grundvoraussetzung. Setzen Sie das Thema in Ihrem Unternehmen auch ganz oben auf die Agenda!

Schädlich – vielfältige Kosten durch Cyberangriffe

Die Schäden für die deutsche Wirtschaft durch Cyberattacken belaufen sich Bitkom Research zufolge auf rund 100 Milliarden Euro pro Jahr. Miteinbezogen wurden dabei die Kosten für Ermittlungen, Ersatzmaßnahmen, Rechtsstreitigkeiten, datenschutzrechtliche Maßnahmen, entstandene Kosten durch Erpressung mit gestohlenen oder verschlüsselten Daten sowie durch Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder

Betriebsabläufen, Umsatzeinbußen durch Plagiate oder den Verlust von Wettbewerbsvorteilen sowie entstandene Imageschäden, etwa durch negative Berichterstattung. Als weitere negative Folge identifiziert, aber nicht in Euro beziffert wurde im Rahmen der Studie eine erhöhte Mitarbeiterfluktuation beziehungsweise das Abwerben von Mitarbeitern.[6]

Ob und wieweit die von Bitkom Research ermittelte jährliche Schadenssumme stimmig ist, ist umstritten, denn bei der Bezifferung der Schäden gehen die Schätzungen weit auseinander. Einigkeit besteht eigentlich nur insoweit, als die Kosten für eine Cyberattacke mit Datenverlust dramatisch variieren und alleine aus diesem Grund simple Mittelwerte immer problematisch sind, da sie durch einzelne Großereignisse massiv verschoben werden und natürlich viele kleinere Schäden gar nicht erst bekannt werden.

Um dennoch eine Indikation zu haben, ist IBM eine erste Anlaufstelle. Der IBM Data Breach Report kalkuliert die Kosten je Cybersecurity-Vorfall weltweit auf 3,92 Millionen US-Dollar und in Deutschland auf rund 4,78 Millionen US-Dollar.[7] Weltweiter Spitzenreiter sind die USA mit 8,19 Millionen US-Dollar. Für die Schweiz geht die Melde- und Analysestelle Informationssicherung mit dem schönen Akronym »Melani« von rund 4,7 Millionen Schweizer Franken aus.[8] Woran die Unterschiede im Detail liegen, ist nicht klar. Einige Untersuchungen adressieren die angesprochenen Verzerrungen und stellen detailliertere Analysen an. Die Cyentia Information Risks Insights Study 2020 etwa gliedert nach Branchen auf und ermittelt Durchschnitts- sowie Extremwerte der bei Sicherheitsvorfällen erlittenen Verluste. Der Durchschnittswert schwankt demnach zwischen 132 000 US-Dollar (öffentlicher Sektor) und 782 000 US-Dollar (Informationstechnologie). Der Extremwert liegt bei rund 63 Millionen US-Dollar.[9]

Es ist müßig, sich über derartige Schätzungen zu streiten. Unbestritten ist jedoch, dass das Kostenrisiko für die direkten wie für die indirekten Folgen eines Cybersicherheitsvorfalls für die meisten Unternehmen enorm ist und existenzbedrohend sein kann. Um sich dagegen zu wappnen, muss die Initiative jedoch von ganz oben kommen, und dort fehlt oftmals nach wie vor das Problembewusstsein.

Bedenklich – Sorglosigkeit in der Chefetage

»Wir haben hier nur ein Sicherheitsrisiko – und das ist der Chef.« So ungewohnt deutlich teilte mir vor Kurzem der IT-Leiter eines bayerischen Automobilzulieferers seine Bedenken mit. Der Inhaber verweigere die Nutzung von

Passwörtern, weil er sie lästig finde, und bestehe darauf, seinen privaten Laptop sowie sein Smartphone mit in den Betrieb zu bringen und zu nutzen. Mehr als einmal habe der Chef seine mobilen Geräte bereits in Restaurants, in Taxis und am Flughafen vergessen. Jenseits des individuellen Risikos für sich und sein Unternehmen ist dieser Chef zweifellos kein gutes Vorbild für seine Mitarbeiter.

Doch auch in nicht inhabergeführten Unternehmen gibt es erfahrungsgemäß vermeidbare Sicherheitsrisiken, die auf diejenigen zurückgehen, die das Sagen haben und die – womöglich mangels technischer Kenntnisse – Cybersicherheit als notwendiges Übel oder gar als überflüssig sehen.

Sorglosigkeit als Lifestyle – eine Einstellung, die IT-Verantwortlichen verständlicherweise schwere Bauchschmerzen bereitet. Mir ist vollkommen bewusst: In den Führungsetagen der meisten kleinen und mittelständischen Unternehmen sitzen selten Experten für Cybersicherheit. Dort sind andere Kompetenzen gefragt, das versteht sich von selbst. Dennoch ist es heute wichtiger denn je, dass auch Sie als Inhaber oder Manager sich bis zu einem gewissen Grad mit der Materie auskennen. Cyberrisiken sind wesentlich für eine Bewertung von betrieblichen Risiken und sollten zumindest unter diesem Gesichtspunkt Aufmerksamkeit finden. Sollten Sie jemand im Betrieb haben, der für das Thema verantwortlich ist, nehmen Sie sich ein paar Stunden und lassen Sie sich briefen. Holen Sie sich im Zweifel auch vertrauenswürdigen externen Rat. Fragen Sie beispielsweise in Ihrem Branchenverband nach seriösen Anlaufstellen. Und dass Sie dieses Buch in der Hand halten und gerade darin lesen, ist natürlich ein guter Anfang.

Sollten Sie sich schon mal gefragt haben, warum Ihre IT-Abteilung Sie mit so vielen Vorschriften und Einschränkungen nervt, werden Sie nach der Lektüre hoffentlich anders darüber urteilen. Ich möchte Ihren Blick für Sicherheitsrisiken öffnen und weiten, sodass Sie in Zukunft zusammen mit Ihrer IT-Abteilung fundierte Entscheidungen über notwendige und angemessene Investitionen in puncto Cybersicherheit treffen können.

Und ich versichere Ihnen: Ihre IT-Abteilung will Sie nicht ärgern oder gar schikanieren, sondern handelt im besten Sinne Ihres Unternehmens. Nur wenn jeder im Unternehmen für Cybersecurity sensibilisiert ist und sich an bestimmte Regeln hält, kann gewährleistet werden, dass Ihre Firma gegen Angriffe – egal ob von außen oder von innen – bestmöglich geschützt ist und bleibt.

Tun Sie bereits Ihr Bestes in puncto Cybersicherheit und unterstützen Ihre IT-Verantwortlichen nach Kräften? Geben Sie ihr oder ihm den nötigen Raum und gestatten oder fördern Sie entsprechende Fortbildungen? Viel zu oft wird die IT als mehr oder weniger lästiger Bittsteller gesehen. Sollte das bei Ihnen so sein, dann ändern Sie das. Hören Sie zu und fragen Sie gezielt nach. Sie werden

sich wundern, was in Ihrem Unternehmen an Wissen über mögliche Gefahren bereits vorhanden ist, und nutzen Sie das, um einen Eindruck zu erhalten, den Sie am besten mit einem neutralen externen Experten noch mal durchsprechen. So oder so, Sie werden dazulernen.

Wie gut sind Sie Ihrer Meinung nach für die Risiken des Digitalzeitalters aufgestellt? Sind Sie eher Anfänger, Fortgeschrittener oder gar ein ausgebuffter Profi? Hiscox, ein internationaler Anbieter von Versicherungen gegen Cyberkriminalität, hat 2019 im Rahmen einer Studie Unternehmen befragt, wie gut sie sich auf Sicherheitsvorfälle vorbereitet fühlen, und um eine Selbsteinschätzung gebeten. Selbsteinschätzungen sind naturgemäß kritisch, denn Menschen neigen im Allgemeinen zu dem, was man in der Psychologie »Overconfidence Bias« nennt, das heißt, sie schätzen ihre eigenen Fähigkeiten besser ein, als diese tatsächlich sind. So hält sich ein Großteil der Autofahrer für besonders gute Autofahrer, was rein statistisch gar nicht möglich ist. Insofern sind alle Umfragen, die auf Selbsteinschätzung beruhen, mit Vorsicht zu genießen. Dennoch sei diese Studie hier genannt, schlicht weil es wenige Maßstäbe gibt, die eine Bewertung überhaupt möglich machen. So zeigt sich in der Untersuchung dieses Versicherers denn auch eine durchweg selbstkritische Einschätzung. In Deutschland sind demnach 70 Prozent der Unternehmen Cyberanfänger, 19 Prozent Cyberfortgeschrittene und 11 Prozent Cyberexperten.[10] Die Ergebnisse fallen übrigens europaweit sehr ähnlich aus. Der Unterschied bewegt sich bei wenigen Prozentpunkten. Als Fazit kann man durchaus festhalten, dass die meisten Befragten sich durchaus bewusst sind, dass sie im Bereich Cybersicherheitskenntnisse und -fähigkeiten Defizite haben. Fragt sich, warum die wenigsten Befragten tatsächlich aktiv etwas dagegen unternehmen. Die Vermutung ist, dass es erst eines hinreichenden »Schmerzlevels« braucht, um ins Handeln zu kommen.

Fatal – Kleinreden der Cybersecurity

Wenn ich in Gesprächen mit Inhabern, CEOs und Topmanagern auf deren Einstellung zum Thema Cybersicherheit zu sprechen komme, höre ich nicht selten bedenkliche bis gefährliche Aussagen. Dass es Cyberattacken gibt, ist meinen Gesprächspartnern bekannt, etwa weil es einen Konkurrenten bereits »erwischt« hat. Im Grunde genommen ist es also nur noch eine Frage der Zeit, bis ihr Unternehmen ebenfalls attackiert wird. Nichtsdestotrotz haben viele Gesprächspartner bisher wenig bis nichts für mehr Schutz unternommen und rechtfertigen das auf unterschiedliche Weise. Die nachfolgende Aufzählung im-

pliziert dabei keine Wertung. Jede genannte Ausrede ist auf ihre eigene Art gefährlich, weil sie indirekt mitursächlich sein kann für massive Sicherheitsprobleme bis hin zu existenzbedrohenden Vorfällen.

Die zehn häufigsten Rechtfertigungen von Entscheidern

- Wir sind doch versichert!
- Ach, wir schließen die Lücken später.
- Sicherheit ist doch eigentlich ganz einfach …
- Wieso, wir sind doch compliant?!
- Wir haben die Lösung gefunden!
- Das macht bei uns die IT.
- Wir sind schon vollständig geschützt.
- Sicherheit ist da eingebaut.
- Wir sind noch nie angegriffen worden.
- Wir sind zu klein dafür. Wer interessiert sich schon für uns?

»Wir sind doch versichert!« Dieser Aussage liegt die Idee zugrunde, dass man sich um Cybersicherheit nicht kümmern muss, solange eine Versicherung im Schadensfall einspringt. Das bedeutet, Führungskräfte mit diesem Mindset übertragen die Verantwortung und die Risiken lieber auf Dritte, als sich selbst um die Cybersicherheit zu kümmern und einen Versicherungsfall zu verhindern.

Diese Einstellung greift in meinen Augen aus mehreren Gründen zu kurz. Als Geschäftsführer oder Manager sind Sie dafür verantwortlich, existenzbedrohende Risiken von Ihrem Unternehmen fernzuhalten. Selbst wenn Sie eine Versicherung gegen die Folgen von Cybersicherheitsvorfällen besitzen, können Sie sich nicht blind darauf verlassen, dass eine Versicherung in jedem Fall für die entstandenen Schäden aufkommt. Vielfach sind diese Versicherungen an bestimmte technische Maßnahmen und die laufende Einhaltung gewisser Sicherheitsstandards gebunden. Sie können im Schadensfall davon ausgehen, dass der Versicherer sich sehr genau ansehen wird, was Sie zur Verhinderung des Schadenseintritts getan haben. Unter Umständen schaut der Versicherer auch sehr genau in seine Vertragsbedingungen, um von der Leistungspflicht entbunden zu werden. So machte der Fall Zurich Versicherung gegen Mondelez vor einigen Jahren Schlagzeilen, denn die Versicherungsgesellschaft sah in dem Cyberangriff auf den Lebensmittelproduzenten eine kriegerische Handlung einer fremden Macht, was als solches typischerweise nicht versichert ist.

»Ach, wir schließen die Lücken später.« Das ist eine ähnlich gefährliche und lapidare Aussage wie der Verweis auf das Vorhandensein einer Versicherung. Nicht selten ist den Verantwortlichen dabei die Lage bewusst, vielfach gab es bereits ein IT-Sicherheits-Audit, das zu dem Ergebnis kam, dass Sicherheitslücken vorhanden sind. Die Ergebnisse des Audits zu ignorieren, ist eine gefährliche Strategie, ebenso wie wissentlich bereits bekannte Sicherheitslücken nicht zu schließen. Nicht selten verweist man auf anstehende grundlegende Upgrades, mit denen dann eben auch diese Lücken obsolet werden. Was vielfach vergessen wird: Jeder Tag mit einer nicht beseitigten Lücke kann ein Tag zu viel sein, wenn diese von einem Angreifer erfolgreich ausgenutzt wird. Und das ist – im Zeitalter automatisierter Angriffswerkzeuge – gar nicht mal so unwahrscheinlich.

»Sicherheit ist doch eigentlich ganz einfach« ist vielfach eine Metapher für Mängel bei der Konfiguration und laufenden Überwachung dieser Werkzeuge, obwohl bei den Unternehmen alles vorhanden ist – zumindest, was die Hardware und Software für Cybersicherheit angeht.

»Wieso, wir sind doch compliant?!« Das ist vielleicht die gefährlichste Aussage. Gemeint ist damit, dass man sich als Unternehmen an definierten Vorgaben orientiert, aber dabei nicht nach rechts oder links schaut. Eine sogenannte Compliance-based Security ist ein Anfang, aber dennoch vielfach das Papier nicht wert, auf dem die Anforderungen definiert wurden. Sicherheit, die nicht gelebt wird, ist – spätestens mit der nächsten großen Welle neuer Angriffe – ein Störfall mit Ansage. Das Problem: Angreifer orientieren sich nicht an Compliance-Vorgaben, sondern sie attackieren dort, wo es Erfolg versprechend scheint.

»**Wir haben die Lösung für alle Sicherheitsprobleme gefunden.«** Man mag es kaum glauben, aber selbst derartige hanebüchenen Aussagen bekommt man ab und an zu hören. Sie kommt meist von Unternehmen, die gerade frisch in eine mehr oder weniger universelle Cybersicherheitslösung investiert haben und den wolkigen Versprechungen der Anbieter eines »Rundum-Schutzes« oder einer »total security« Glauben schenken. Diese Aussage zeugt von falschem Vertrauen in eine Universallösung, die alle Anforderungen an Cybersicherheit im Unternehmen abzudecken vermag. Außerhalb von Marketingbroschüren hat dieses Wunderwerkzeug aber noch niemals jemand gefunden.

»Das macht bei uns die IT.« Diesen Satz höre ich häufig und manchmal stimmt er sogar, aber vielfach hängt damit die Verantwortung im Niemandsland und der Weg ins Desaster ist nicht weit. Festzuhalten ist: Die schlussendliche Verantwortung, wenn was schiefgeht, liegt immer bei der Geschäftsleitung. Wegdelegieren lässt sich das nicht. Auch wenn von Cybersicherheit im Aktiengesetz und

GmbH-Gesetz direkt nichts steht, gelten Grundpflichten in diesen Regelwerken auch dafür. Experten der Wirtschaftsprüfungs- und Steuerberatungsgesellschaft Rödl sehen sogar drei wesentliche Pflichten, die den Bereich der Cybersicherheit tangieren, und beschreiben diese wie folgt:[11]

- »Sorgfaltspflicht: So haben etwa Vorstandsmitglieder die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters gem. § 93 Abs. 1 (1) und (2) AktG anzuwenden. Für einen Geschäftsführer einer GmbH wird nach § 43 Abs. 1 GmbHG der gleiche Maßstab zur Sorgfalt gefordert.
- Legalitätspflicht: Diese Pflicht der Geschäftsleitung verlangt, dafür Sorge zu tragen, dass sich die Gesellschaft in ihren Außenbeziehungen rechtmäßig verhält. Dabei hat die Geschäftsleitung auch die Handlungen ihrer Mitarbeiter zu überprüfen.
- Pflicht zur Einrichtung von Überwachungssystemen: In § 91 Abs. 2 AktG wird die Einrichtung explizit gefordert. Es ist aufgrund dieser Regelung davon auszugehen, dass im Fall einer juristischen Überprüfung auch die Geschäftsführung einer GmbH oder anderer Gesellschaftsformen betroffen sind.«

Und sehen bei einer Pflichtverletzung einen Schadensersatzanspruch der Gesellschaft gegen die Geschäftsleitung.

»Wir sind schon vollständig geschützt.« Bei solchen Aussagen handelt es sich um einen klaren Fall von »Security by Marketing« und derjenige ist schlicht auf die mehr oder weniger hohlen Versprechungen der Vertriebsleute oder bunter Illustrationen auf einer Website hereingefallen. Nur zu gerne vertraut man darauf, dass Dienstleistungen und Produkte aus der IT-Sicherheit einen vollständigen Schutz bieten können. Ein gefährlicher Irrglaube, denn absolute Sicherheit gibt es nicht. Es ist daher ein bisschen wie zu glauben, dass Diätkekse wirklich schlank machen. Man wünscht sich einfach, dass das wahr wäre, und blendet Unplausibilitäten aus. Die Täuscher sterben nicht aus, solange es Kunden gibt, die sich so leicht hinters Licht führen lassen.

»Sicherheit ist da eingebaut« ist ein gern gebrauchtes Argument dafür, sich mit potenziellen oder tatsächlichen Sicherheitsproblemen von einzelnen Systemen und Anlagen, etwa Maschinen in Industriebetrieben oder medizinischen Geräten in Krankenhäusern und Arztpraxen, gar nicht erst auseinanderzusetzen. Es ist eine Mischung aus Marketinggläubigkeit und fehlendem Sicherheitsbewusstsein, die hier durchscheint und in den meisten Konstellationen zu einem schleichenden Problem wird, denn Fakt ist: Neue technische Systeme bringen – ge-

gen die Versprechungen der Hersteller – häufig neue Risiken für das System selbst, aber manchmal auch für das Unternehmen. So gut wie nie sind diese Risiken bei der Einführung und Implementierung bekannt. Praktisch immer kommen diese erst später zum Vorschein. Entscheidend ist dann, wie der Hersteller, aber auch wie der Abnehmer damit umgeht. Anders gesagt: Gibt es zeitnah Sicherheits-Updates, wenn ein Problem auftritt, und werden diese dann auch tatsächlich vom Anwenderunternehmen eingespielt? Selbst Sicherheitssoftware wie Antivirenprogramme, Firewallsysteme und andere Programme, die eigentlich die Sicherheit erhöhen, bringen manchmal Sicherheitslücken mit und verschlechtern so die Lage. »Sicherheit ist da eingebaut« ist daher stets mit Vorsicht zu genießen.

»Wir sind noch nie angegriffen worden!« Das bedeutet leider fast immer: Die Unternehmen wurden bereits gehackt, haben es aber noch nicht bemerkt. In die gleiche Richtung geht der Spruch: »Ich hoffe, wir werden nicht attackiert.« Der Kabarettist Nico Semsrott beschrieb das Prinzip Hoffnung wider besseres Wissen einmal mit den schönen Worten: »Die Hoffnung stirbt zuletzt, aber sie stirbt!«[12]

»Wir sind zu klein. Wer interessiert sich schon für uns?« Das ist der Klassiker bei kleinen und mittelständischen Unternehmen. Wenn es Ihnen bisher noch nicht bewusst war, werden Sie spätestens bei der Lektüre anhand von zahlreichen Fallbeispielen erfahren, wie sehr gerade der Mittelstand im Fokus der Cyberkriminellen steht.

Vorbildlich – Wege aus dem Cybersecurity-Dilemma

- Wer weiß, womöglich sind Ihnen solche oder ähnliche Aussagen früher selbst einmal über die Lippen gekommen. Da Sie dieses Buch in den Händen halten, ist ein entscheidender Schritt auf dem Weg zu mehr Cybersicherheit für Ihr Unternehmen bereits getan: Sie haben erkannt, dass Sie Ihre Firma besser absichern müssen. Die Motive können dabei unterschiedlich sein, etwa wie in folgenden Beispielen:
- Sie sind Inhaber oder Mitinhaber und sehen in den Folgen von Cyberangriffen ein Risiko für Ihren Unternehmenserfolg. Sie sehen sich in der Verantwortung für sich, die Mitarbeiter und das Unternehmen.
- Sie sind angestellte Führungskraft und scheuen die persönliche Haftung oder wollen Ihren Bonus, der sich etwa auf den Aktienkurs bezieht, nicht gefährden.

- Ihr Unternehmen ist von besonderen Regelungen getroffen – etwa die BSI KRITIS-Verordnung zu sicheren Infrastrukturen – und Sie müssen investieren.
- Ihre Kunden verlangen klare vertragliche Garantien für die Verfügbarkeit von Systemen und Diensten.
- In Ihrer Branche kam es bereits zu Cyberangriffen mit enormen Schäden und Sie fragen sich, ob Ihr Unternehmen das nächste Opfer ist.
- Sie haben Ihre Aufgabe als Führungskraft neu begonnen und wollen nun überall nach dem Rechten sehen.
- Sie oder Ihr Unternehmen sehen sich persönlich im Rampenlicht, weil Sie etwa einen bedeutenden Branchenpreis gewonnen haben oder die Medien über Sie berichtet haben.
- Sie sind – aufgerüttelt von zahlreichen Medienberichten – der Meinung, man müsse mehr für Cybersicherheit tun.
- Es gab bereits einen Sicherheitsvorfall in Ihrer Organisation. Sie wollen nun ausschließen, dass es zu weiteren Problemen kommt.

Diese Aufstellung ist natürlich alles andere als vollständig. Und nicht immer sind es einzelne Motive, sondern vielfach Kombinationen daraus, die den Ausschlag geben, endlich ins Handeln zu kommen. Egal, was Ihre Motive sind. Entscheidend ist, dass Sie ins Handeln kommen. Das ist im Business nicht anders als im Privatleben: Die Feststellung, man sollte mehr Sport machen oder weniger Alkohol konsumieren, ist schnell getroffen. Tatsächlich ins Handeln zu kommen und das eigene Verhalten zu ändern, scheitert vielfach an der Bequemlichkeit. Und selbst wenn der Start gelingt, besteht immer latent die Gefahr, in alte Verhaltensmuster zurückzufallen. Man hat ja keine Zeit, der Alltag ist wichtiger.

Ich kann Ihnen aufgrund meiner langjährigen Erfahrung als Cybersicherheitsexperte versichern, dass es wesentlich ist, dass Sie das Thema Cybersicherheit systematisch in Angriff in Angriff nehmen. Definieren Sie ein Projekt, widmen Sie diesem Ressourcen und stellen Sie sich darauf ein, unterwegs das Ganze mehrfach umzuplanen, denn ganz egal wie elaboriert Sie dabei vorgehen, Sie werden auf unbequeme Wahrheiten stoßen, denen Sie sich stellen müssen. Es liegt auf der Hand, dass es besser ist, wenn Sie diese selbst finden, bevor ein Angreifer es tut.

Die Verantwortung für den richtigen Umgang mit Cyberrisiken kann Ihnen niemand abnehmen, denn als Führungskraft oder als Inhaber ist es Ihre ureigenste Aufgabe, mit Risiken umzugehen. Eine Aufgabe, die im Allgemeinen mit Risikomanagement beschrieben wird und die um »typische« Unter-

nehmensrisiken kreist. Und eine Aufgabe, die mit den oben beschriebenen Pflichten der Unternehmensleitung, »Sorgfaltspflicht«, »Legalitätspflicht« und »Pflicht zur Einrichtung von Überwachungssystemen« auch einen rechtlichen Hintergrund hat. Nach einer Auflistung auf der Industrie- und Handelskammer auf IHK24[13] sind dies insbesondere folgende Risiken:

Externe Risiken

- Wirtschaftliche Rahmenbedingungen (zum Beispiel Wachstum, Kaufkraft)
- Gesetzliche Verordnungen, regulatorischer Rahmen zur Ausübung des Geschäftes (zum Beispiel Umweltauflagen, Dosenpfand, Arbeitsschutz, Datenschutz, zusätzliche Auflagen et cetera)
- Geänderte Vergaberichtlinien für Fremdkapital
- Änderungen im Kaufverhalten (Produktsubstitutionen, veränderte Einstellungen und Vorlieben)
- Änderungen bei Kundenbedürfnissen
- Allgemeiner Preisverfall
- Konkurrenz aus Niedriglohnländern
- Energie- und Treibstoffkosten

Technologische Risiken

- Veränderungen auf der Lieferantenseite
- Fehlende Entwicklungsressourcen
- Ausfall eines Entwicklungspartners
- Ähnliche Produkte vom Wettbewerb schneller auf dem Markt als die eigenen
- Technologische Entwicklungen, die bestehende Produkte ersetzen (Produktlebenszyklus)
- Verzögerungen bei der Fertigstellung neuer Produkte
- Neue Wettbewerber mit moderner Fertigungstechnologie

Leistungswirtschaftliche Risiken

- Abhängigkeit von wenigen Lieferanten
- Engpässe bei notwendigem Material
- Abhängigkeit von wenigen Großkunden, Wegfall wichtiger Großkunden
- Vermarktungsintensität
- Steigende Vertriebskosten
- Umsatzausfälle

- Verlust von Vertriebskanälen
- Fehler im Management von Geschäftspartnern
- Fehlende Internationalisierung in Produktion und Vermarktung
- Fehler in Kundenrechnungen, Forderungsausfälle

Finanzwirtschaftliche Risiken

- Liquiditätsbedarf aufgrund neuer Angebote (zum Beispiel Leasing / Mietkauf)
- Margenreduktion durch Wettbewerbsdruck auf Preise
- Strittige Forderungen
- Verlängerung bei Debitorenzielen
- Verspätete Kapitalmaßnahmen
- Zu niedrige Eigenkapitalquote

Risiken aus der Organisation

- Fehlende Motivation
- Unzureichende Unternehmenskultur
- Schleppender Informationsfluss
- Fehlende Entscheidungsbereitschaft
- Störungen im technischen Ablauf
- Brand, Wasserschaden et cetera
- Ausfall von Führungskräften, Kündigung von Leistungsträgern
- Qualifikation von Mitarbeitern
- Fehlende Nachfolgeregelung

Die Bewertung all dieser Risiken und die adäquate Reaktion darauf sind – ohne Zweifel – ureigenste Aufgabe der Unternehmensleitung.

Dazu dient das Risikomanagement. Haufe Office definiert dies wie folgt: »Risikomanagement umfasst alle Aktivitäten eines Unternehmens, die sich auf die Analyse und den Umgang mit Chancen und Gefahren beziehen. Die wichtigsten Teilaufgaben des Risikomanagements sind die Identifikation, Quantifizierung, Aggregation, Überwachung und Bewältigung von Risiken (...)«.[14] Über Risikomanagement sind ganze Regalmeter in Bibliotheken geschrieben worden, es gibt Normen (ISO 31000) und Modelle und natürlich jede Menge Konzepte von Unternehmensberatern, die Mindestanforderungen sind jedoch recht einfach zu beschreiben und ergeben sich für Aktiengesellschaften aus § 91 Abs. 2 AktG:

»Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand gefährdende Entwicklungen früh erkannt werden.«

Aber nicht nur der deutsche Rechtsrahmen deutet auf ein Mehr an Verantwortung hin. Die Analystenfirma Gartner sieht weltweit CEOs und Führungskräfte in der Pflicht und Verantwortung und verweist dazu auf verschiedentlichen regulatorischen Wandel, der in Folge zunehmender Sicherheitsvorfälle weltweit zu einer Verschärfung der Haftungsregeln in der Praxis führt.[15]

Dass Cyberattacken den Fortbestand eines Unternehmens gefährden können, steht spätestens nach einem Fall Anfang 2020 in der Schweiz fest. Ein Fensterbau-Unternehmen mit 170 Mitarbeitern musste nach einem Ransomware-Vorfall Konkurs anmelden. In einer Nachricht des Verwaltungsrates wird die Cyberattacke als ursächlich für die Pleite angegeben: »Eine massive Cyberattacke auf unsere Systeme führte jedoch im Mai 2019 zu einem herben Rückschlag für unser Unternehmen. Die Folge war ein Produktionsausfall von über einem Monat, begleitet von massiven Folgekosten (...)«, hieß es darin unter anderem.[16]

Aber zurück zu den Unternehmensrisiken. Auffällig bei obiger Auflistung ist, dass Cyberrisiken nicht oder – wohlwollend interpretiert – nur indirekt etwa bei den »Störungen im technischen Ablauf« auftauchen. Es wird Zeit, Cyberrisiken in der Debatte den Platz einzuräumen, der ihnen aus den Erfahrungen der Praxis gegeben werden sollte. Bei »Störungen im technischen Ablauf« denkt man an den Ausfall einer Maschine, aber wohl kaum an tage- oder monatelange weitreichende Beeinträchtigungen oder – im Extremfall – gar Komplettausfälle aller technischer Anlagen. Dies offenbart ein weiteres Problem, selbst wenn wir nun Cyberrisiken als eigene Risikoklasse sehen oder zumindest als Verursacher potenziell substanzgefährdender Probleme wahrnehmen: Was ist mit der Identifikation, Bewertung und Analyse der Risiken? Bei gewöhnlichen Risiken – also den Risiken aus obiger Auflistung – gibt es meist eine vernünftige Datenbasis. Ein Logistiker mit einem Fuhrpark an Lieferfahrzeugen hat meist ein relativ klares Bild von der Lebensdauer und Ausfallwahrscheinlichkeit der Fahrzeuge und weiß auch, wie oft sich typischerweise Unfälle ereignen, mithin kann er dafür geeignete Vorsorge treffen, etwa bei der Wartung der Fahrzeuge, der Ausgestaltung der Versicherungsverträge oder auch der Verhandlung der Konditionen mit Autovermietungen für Ersatzfahrzeuge. Bereits mittelständische Unternehmen verfügen hier in aller Regel über vernünftige Bemessungsgrundlagen und selbst als Einzelunternehmer mit nur einem LKW sind Sie nicht ganz aufgeschmissen, da es Erwartungswerte für Lebensdauer wie Unfallhäufigkeiten gibt, die sich natürlich in die eigene Planung integrieren lassen.

Wie steht es jedoch Cyberrisiken insbesondere um die Eintrittswahrscheinlichkeiten und möglichen Auswirkungen? Hier gibt es wenig belastbare Informationen, wenn es um das große Ganze geht. Einfache technische Risiken der Informationstechnologie lassen sich – analog zum LKW-Beispiel – jedoch recht gut bewerten. Die Ausfallquote von Rechnern oder Maschinen eines bestimmten Bautyps ist für viele mittelständische Unternehmen alles andere als Rocket Science. Wie oft und mit welchen erwarteten Auswirkungen jedoch ein Cybersicherheitsvorfall eintreten wird, ist nicht ohne Modellrechnungen mit vielen unbekannten Variablen zu bewältigen. In der Praxis sind diese meist nutzlos. Das ist die bittere Lektion des Autors aus gut zwei Jahrzehnten Beschäftigung mit dem Thema. Es geht nie um das Ob, sondern nur um das Wann und in welcher Form. Viele Unternehmen, die sich mit dem Gedanken tragen, den Umgang mit Cybersicherheit im eigenen Haus zu professionalisieren, stellen zudem im Laufe der Untersuchungen fest, dass sie längst gehackt worden sind, aber die Auswirkungen noch nicht oder noch nicht in Gänze erfassen können.

Wo auch immer Sie mit Ihren Überlegungen stehen: Den ersten Schritt für Ihr Unternehmen haben Sie spätestens mit Lektüre dieses Buchs bereits vorgenommen. Sie nehmen Cyberrisiken als Unternehmensrisiko an und sehen dieses – wie andere Risiken – im Verantwortungsbereich der Geschäftsleitung. Entscheidend ist nun der richtige – praxistaugliche – Umgang mit diesen schwer fassbaren Risiken neuer Art. Die alles entscheidende Frage lautet: Was können oder müssen Sie tun, um Ihr Unternehmen weitgehend vor Cyberattacken zu schützen? Um eine Antwort zu finden, müssen Sie zunächst wissen, welche Angriffe überhaupt denkbar sind und welche Einfallstore es für Cyberkriminelle generell gibt. Danach geht es darum zu bewerten, welche davon für Ihr Unternehmen relevant sind und was im Ernstfall auf dem Spiel steht. Im Anschluss kümmern Sie sich um entsprechende Vorsichtsmaßnahmen – in enger Zusammenarbeit mit Ihren IT-Verantwortlichen oder externen Dienstleistern. Dabei kommen natürlich auch die Kosten dieser Investitionen zur Sprache. Zudem sollten Sie wissen, was konkret zu tun ist, wenn es Sie persönlich, Ihre Mitarbeiter oder Ihr ganzes Unternehmen trotz aller Vorsicht erwischt hat, und brauchen einen Notfallplan, damit Sie in der Hektik nichts vergessen.

Ich gebe Ihnen in diesem Buch auf viele Fragen rund um Cybersicherheit fundierte Antworten. Übrigens: Wenn hier von einem »Experten« die Rede ist, sind selbstverständlich Personen jeglichen Geschlechts gemeint. Wo es möglich ist, verzichte ich auf überflüssigen Technikballast und Expertenkauderwelsch. Neue Cyber-Security-Vokabeln übersetze ich für Sie an Ort und Stelle und zum Nachschlagen finden Sie am Ende des Buchs ein Glossar.

Ich möchte Ihren Blick schärfen: nicht nur für Technologien und deren Schwächen, sondern vor allem für den Faktor Mensch, denn dieser spielt im Bereich Cybersicherheit eine wesentliche Rolle. Eins verrate ich Ihnen gleich vorweg: Es gibt weder ein Universalwerkzeug noch ein Patentrezept für die perfekte Cybersecurity-Strategie. Aber es gibt praxiserprobte Maßnahmen und bewährte Vorgehensweisen, an denen Sie sich orientieren können, um Ihre maßgeschneiderte Lösung zu finden. Mithilfe des CE21-Cybersecurity-Modells, das ich mitentwickelt habe, können Sie eine Risikobewertung für Ihr Unternehmen durchführen, erhalten einen schnellen Überblick über Ihren Cybersicherheitsstatus und identifizieren die Handlungsfelder für Investitionen in Sicherheit.

Laufende Updates zum Thema Cybersicherheit finden Sie in meinem LinkedIn-Feed unter https://www.linkedin.com/in/thomasrkoehler. Schauen Sie auch gerne auf meiner Website www.thomaskoehler.de vorbei! Dort finden Sie weitere Beispiele meiner Arbeit rund um den Schutz vor Cyberrisiken für Unternehmen wie Privatleute.

1 ATTACKEN VON VIELEN SEITEN

Ein durch Schadsoftware lahmgelegter Rechner, eine gehackte Website oder ein über ausgespähte Zugangs- oder Kreditkartendaten geplündertes Konto – von solchen Ereignissen betroffene Personen oder Firmen kennt inzwischen jeder. Direkt aus dem eigenen Bekanntenkreis oder indirekt aus den Medien. In der Businesswelt ist schnell von Millionenschäden die Rede, ja sogar von Unternehmen, die aufgrund einer Cyberattacke Insolvenz anmelden mussten. Sie kennen vielleicht solche Fälle aus Ihrer Branche, womöglich zählen Sie bedauerlicherweise sogar selbst zu den Opfern.

Einige Begriffe rund um Cyberangriffe haben Sie bestimmt schon einmal gehört oder gelesen, bei anderen wissen Sie aber nicht ganz genau, was Sie sich darunter vorstellen sollen und warum das Ganze so gefährlich ist. Geschweige denn, wie Sie mit solchen Attacken umgehen oder Angriffe verhindern könnten.

Es gibt eine ganze Reihe von Cyberattacken, die Ihr Unternehmen bedrohen. Doch wie gelingt es Cyberkriminellen, Ihr Unternehmen zu attackieren oder zu infiltrieren? Mit welchen Angriffen müssen Sie rechnen und wie können Sie sich dagegen wappnen?

Eine altbekannte Plage – Computerviren und -würmer

Der Computervirus – ein selbstreproduzierendes Programm, das Schaden stiften kann – als Urform und Vorläufer aller heute existierenden Bedrohungen der Cybersicherheit ist schon relativ alt. Anno 1949 veröffentlichte der Mathematiker John von Neumann seine These, dass sich Computerprogramme selbst replizieren können.[1] Es dauerte aber noch bis zum Beginn der 1960er-Jahre, bis in den Bell Labs, einem berühmten Forschungszentrum im Silicon Valley, ein Computerspiel namens »Darwin« entwickelt wurde (später unter »Core Wars« bekannt), in dem zwei Algorithmen gegeneinander kämpften: Sie versuchen, sich

gegenseitig zu überschreiben und so die Vorherrschaft über das Rechnersystem zu gewinnen.[2] Unter dem etwas sperrigen Titel »Selbstreproduzierende Automaten mit minimaler Informationsübertragung« beschrieb der österreichische Ingenieur Veith Risak 1972 dann einen zu Forschungszwecken geschriebenen Virus in einem Fachartikel. Das Programm selbst lief einwandfrei auf einem damals gängigen Siemens-Großrechner Typ 4004/35 und brachte alle grundlegenden Funktionen mit, die man heute mit einem Computervirus assoziiert.[3] Es konnte sich selbst reproduzieren und so weiter ausbreiten und war in der Lage, Veränderungen an den befallenen Systemen vorzunehmen.

Im selben Jahr tauchte auch der Begriff »Computervirus« erstmals auf – in einer Science-Fiction-Geschichte des (Drehbuch-)Autors David Gerrold mit dem Titel »When Harlie Was One«. Sowohl der Begriff als auch der Gedanke dahinter wurden in der Folge vielfach aufgegriffen, 1975 etwa in dem Roman *Der Schockwellenreiter*. Darin beschreibt der Autor John Brunner viele heute gängige Konzepte bis hin zur Grundidee der Schwarmintelligenz, aber eben auch die Gefahren von Computerviren und anderen selbstreproduzierenden Algorithmen. Die Büchse der Pandora war geöffnet und Wissenschaftler wie Praktiker stürzten sich auf dieses neue Konzept.

Im Jahr 1980 entstand am Informatik-Lehrstuhl der Universität Dortmund eine Diplomarbeit, in welcher der Vergleich angestellt wurde, dass sich bestimmte Programme ähnlich wie biologische Viren verhalten können. Zwei Jahre später schrieb ein damals 15-jähriger US-amerikanischer Schüler ein Computerprogramm namens »Elk Cloner«, das sich auf Apple-II-Systemen via Diskettenaustausch verbreitete. Die eigentliche Schadfunktion von Elk Cloner war überschaubar, so ist überliefert, dass das Programm bei jeder fünfzigsten eingeschobenen Diskette die Meldung ausgab:

> Elk Cloner: The program with a personality
> It will get on all your disks
> It will infiltrate your chips
> Yes it's Cloner!
> It will stick to you like glue
> It will modify ram too
> Send in the Cloner![4]

Wann genau der erste Computervirus, der diesen Namen wirklich verdient, weil er wirkliche Schäden anrichtete, in freier Wildbahn entdeckt wurde, ist unklar.

1986 jedenfalls wurde die erste Vireninfektion auf Rechnern der Freien Universität Berlin entdeckt.[5]

Seither haben wir eine beinahe lawinenartige Zunahme verschiedenster Schadprogramme erlebt, die sich von System zu System, das heißt meist von Computer zu Computer, aber auch von Mobiltelefon zu Mobiltelefon verbreiten. Während früher die Datenübertragung von Schadsoftware zumeist per Diskette erfolgte, stehen nun schnellere und weitreichendere Übertragungswege offen, sodass sich Schadprogramme binnen weniger Stunden rund um den Globus verbreiten können.

Virus oder Wurm – das ist hier die Frage

Bestimmt haben Sie den Begriff **Computerwurm** schon einmal gehört. Der wichtigste Unterschied zum Computervirus: Er verbreitet sich anders. Bei einem Computerwurm handelt es sich ebenfalls um eine Schadsoftware, die sich selbst vervielfältigt. Doch sie breitet sich autark aus, typischerweise über Netzwerke oder Wechseldatenträger, während ein Computervirus eine Wirtsdatei benötigt. Die Schadfunktionen des Computerwurms können sehr vielfältig sein.

Hinterhältig – Trojaner

Um die Begriffsverwirrung komplett zu machen, ist vielfach auch die Rede von einem weiteren Schädling: der Trojaner. Der Begriff ist entstanden in Anlehnung an das hölzerne Trojanische Pferd aus der griechischen Mythologie, das zur Eroberung des als uneinnehmbar geltenden Troja diente, indem sich griechische Soldaten in seinem Bauch versteckt hielten, die nachts – nachdem das als Geschenk präsentierte Pferd von den Trojanern in die Stadt gebracht worden war – die Tore der Stadt von innen öffneten und ihr Heer hineinließen. Als »Trojanisches Pferd« oder »Trojan Horse« oder eben meist kurz als »Trojaner« bezeichnet man in der IT entsprechend Programme, die unerwünschte Funktionen mitbringen und dazu auf fremde Rechner geschleust werden, bei denen der Betroffene vielfach unbewusst bei der Verbreitung mithilft, indem er Programme aus zweifelhaften Quellen herunterlädt und installiert. Aber auch wenn der Nutzer sich nur auf offizielle Quellen verlässt, ist er nicht vor der Gefahr, an Schadsoftware zu geraten, gefeit, denn immer wieder tauchen etwa im offiziel-

len Google Play Store trojanerverseuchte Apps auf.[6] Teilweise treiben Kriminelle erheblichen Aufwand, um die Sicherheitsmechanismen der Appstores zu umgehen. Vielfach mit Erfolg. Im Ergebnis hat der Nutzer zumeist eine App oder eine Software, die neben den gewünschten Funktionen auch unerwünschte mitbringen oder unerwünschte Programmteile nach Bedarf nachladen.

In der Praxis ist die Unterscheidung zwischen Virus, Wurm und Trojaner nicht mehr wirklich relevant. Fortgeschrittene Schadsoftware integriert Verbreitungs- wie Schadfunktionen aus unterschiedlichen Konzepten, deswegen spricht man heute besser insgesamt von Malware als wichtigstem Oberbegriff und unterscheidet lediglich, ob die Verbreitung mit oder ohne Nutzerinteraktion geschieht. Der erstere Fall ist der Regelfall. Typischerweise etwa klickt der Anwender auf einen verseuchten E-Mail-Anhang, bei Variante zwei spricht man von »Zero click Malware«.

Egal welche Malware sich eingenistet hat, im Ergebnis ist der Rechner und manchmal in Folge das ganze Netzwerk kompromittiert und ein geschickter Angreifer kann entweder auf lange Zeit unbemerkt Daten entwenden oder manipulieren oder ganz simpel Sabotage betreiben. Das in der Praxis häufigste Problem ist dabei die später noch näher beschriebene Ransomware, bei der die auf dem Rechner gespeicherten Daten dem Anwender durch Verschlüsselung entzogen und nur gegen Lösegeld freigegeben werden.

Aber egal wie man die über Jahrzehnte entwickelte Nomenklatur rund um Schadsoftware sieht: Wichtig für das Verständnis ist das damit einhergehende Risiko und Schadenspotenzial. Und das kann – weltweit gesehen – in die Milliarden gehen. Auch wenn die meisten Schadensereignisse nur lokale Folgen haben, machen doch immer wieder einzelne Cybersicherheitsvorfälle weltweit Schlagzeilen. An einen solchen besonderen Fall sei hier kurz erinnert.

Liebesbotschaft der anderen Art

»I love you« stand in der Betreffzeile einer E-Mail, die in meinem Postfach landete. Die Absenderin war eine Kollegin aus der Beratungsfirma, in der ich nach meinem Uniabschluss arbeitete. Mein erster Gedanke damals als selbstbewusst-überheblicher Nachwuchsunternehmensberater war: »Jetzt hat sie endlich gemerkt, was für ein toller Typ ich bin!« Dieser Gedanke hielt jedoch nicht sehr lange vor, denn beinahe im Minutentakt kamen von weiteren Kolleginnen – es waren natürlich nur zufällig zuerst durchweg Kolleginnen – E-Mails mit dem gleichen Betreff, noch bevor ich die erste E-Mail überhaupt geöffnet hatte. So viel Zuspruch in so kurzer Zeit? Da dämmert auch dem aufgeblasensten Ego, dass etwas nicht stimmen kann. Spätestens als der gleichlautende Be-

treff bei Nachrichten verschiedener männlicher Kollegen in meinem Postfach auftauchte, war endgültig klar: Hier läuft etwas gehörig schief!

Ich war live dabei, als der aufgrund seiner Betreffzeile »Loveletter« getaufte Computerwurm sich Anfang Mai 2000 durch die Outlook-Postfächer der Welt fraß, indem er sich rotzfrech selbst an alle E-Mail-Adressen im gespeicherten Adressbuch versendete. Das Ganze geschah ohne menschliches Zutun, das Vorhandensein einer bestimmten Programmkonstellation reichte. Neben der Funktion, die zu seiner unkontrollierten Verbreitung führte, brachte Loveletter weitere Überraschungen mit. So versuchte das Programm, Dateien mit bestimmten Endungen wie ».jpg« vom Rechner zu löschen. Mithin gab es für viele Empfänger ein böses Erwachen. Meinem damaligen Arbeitgeber passierte zum Glück nichts Nennenswertes, es blieb bei der E-Mail-Flut.

Als Urheber wurde Onel Guzman, ein Student an einem Computercollege in der philippinischen Hauptstadt Manila, identifiziert. Das war aber auch nicht weiter schwer, denn er hatte im Programmcode des Computerwurms ein Kommentarfeld mit eindeutigen Hinweisen hinterlassen[7]:

```
rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder/ispyder@mail.com/@GRAMMERSoft Group/Manila, Philippines
```

Onel Guzman wurde nicht verurteilt, denn zu diesem Zeitpunkt gab es auf den Philippinen keine Gesetze, die sein Verhalten unter Strafe gestellt hätten.[8]

Was Abhilfe schafft

Vordergründig sind das aktuelle Antivirus-Programme. In der Praxis hilft das genaue Hinsehen bei – wie im Beispiel – neuartigen Bedrohungen. Aufmerksamkeit, die nicht nur Sie, sondern auch Ihre Mitarbeiter haben sollten, ist die beste Waffe gegen derartige Bedrohungen.

Hier lockt das große Geld – E-Mail-Scams

Betrüger nutzen unterschiedliche Maschen, um an potenzielle Opfer heranzukommen und ihnen Geld – am besten jede Menge davon! – aus der Tasche zu