Michael Bartsch
Stefanie Frey

Cyberstrategien für Unternehmen und Behörden

Maßnahmen zur Erhöhung der Cyberresilienz

Springer Vieweg

Cyberstrategien für Unternehmen und Behörden

Michael Bartsch • Stefanie Frey

Cyberstrategien für Unternehmen und Behörden

Maßnahmen zur Erhöhung der Cyberresilienz

Springer Vieweg

Michael Bartsch
Siegburg, Deutschland

Stefanie Frey
Lovatens, Schweiz

ISBN 978-3-658-16138-5 ISBN 978-3-658-16139-2 (eBook)
DOI 10.1007/978-3-658-16139-2

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

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Strasse 46, 65189 Wiesbaden, Germany

Geleitwort

Noch immer ist vielen Unternehmen und öffentlichen Einrichtungen nicht bewusst, wie vielen Cyber-Gefahren sie inzwischen jeden Tag ausgesetzt sind und wie vielfältig und raffiniert diese Bedrohungen mittlerweile sind.

Gleichzeitig wird es für IT-Sicherheitsfachleute immer schwieriger, Arbeitsplatzrechner, mobile Endgeräte sowie das gesamte Unternehmensnetz vor Cyberangriffen zu schützen. Denn die Zahl der Attacken nimmt immer weiter zu. Allein der Volkswagen-Konzern registriert mittlerweile pro Tag unglaubliche 6000 Cyberangriffe auf seine IT-Infrastruktur. Hinzu kommt, dass die Urheber von Schadsoftware immer professioneller und kreativer vorgehen. Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI; 2016) wurden etwa 32 Prozent der deutschen Unternehmen z. B. Opfer von Angriffen mittels Erpresser-Software. Und wir können davon ausgehen, dass die Dunkelziffer noch um einiges höher liegen dürfte. In jedem fünften Fall der erfassten „Locky"-Angriffe kam es dadurch zu einem Ausfall von zentralen Teilen der IT-Infrastruktur. Etwa 11 Prozent der betroffenen Unternehmen verloren dadurch wichtige Daten. Trotzdem wird das Thema Cyber-Security teilweise immer noch stiefmütterlich behandelt. Eine fachgerechte Aufklärung über Cyberbedrohungen, Schadenspotenziale und Kostenpunkte, wie sie dieses Buch bietet, ist daher dringend vonnöten.

Denn eine Besserung der Lage ist nicht in Sicht. Im Gegenteil: Die Gefährdung deutscher Unternehmen und öffentlicher Einrichtungen durch Cyberangriffe steigt ungebremst weiter an. Durch die zunehmende Digitalisierung von Geschäftsprozessen und die nahtlose Vernetzung von Menschen, Maschinen und Dingen – vom Kühlschrank über Werkzeuge und Unterhaltungselektronik bis hin zum Auto – nimmt die Zahl der Angriffspunkte massiv zu.

Sind wir dagegen wirklich wehrlos? Nein! Mit einem risikobasierten und ganzheitlichen Lösungsansatz, der die bestehende IT-Infrastruktur Ende-zu-Ende einbezieht, können Unternehmen und Behörden funktionierende Sicherheitskonzepte etablieren und zentralen IT-Gefahren wirksam begegnen. Dabei kommt modernen Methoden zur fehlerfreien Personenidentifizierung eine immer größere Bedeutung zu: Der effektive Schutz des physischen Datenzuganges – beispielsweise durch biometrische Authentifizierungssysteme auf Venenmuster-Basis – ist dabei weit mehr als nur ein guter Anfang.

Dr. Rolf Werner, Vorsitzender der Geschäftsführung und Head of Central Europe, Fujitsu.

Vorwort

Cyberbedrohungen und der religiöse Terrorismus sind die dominierenden gesellschaftlichen Bedrohungen des 21. Jahrhunderts. Die Digitalisierung und Automatisierung von immer mehr Lebens- und Wirtschaftsbereichen ist in den letzten Jahren so weit fortgeschritten, dass nicht nur Chancen, sondern auch Risiken entstanden sind. Das Vermeiden dieser Risiken bei gleichzeitiger Nutzung der Chancen ist eine gesamtgesellschaftliche Herausforderung. Ohne eine zuverlässige Cybersicherheit werden die Chancen der Digitalisierung zum Vorteil von Straftätern, Terroristen, informationshungrigen Staaten oder totalitären Regimen ausgenutzt. Wir müssen hier wachsam und innovativ bleiben, um den kriminellen Handlungen der Täter entgegentreten zu können.

In den letzten Jahren sind Qualität und Quantität der Cyberangriffe massiv angestiegen, und immer weitere Lebens- und Wirtschaftsbereiche sind betroffen. Das Geschäft mit der globalen Unsicherheit war schon immer lukrativ, und im Internet gibt es keine staatlichen Grenzen, die Schutz und Kontrolle gewährleisten. Allen Cyberangriffen liegt die Motivation der Täter zugrunde, sich anhand unsicherer Informationstechnologien einen Vorteil zu verschaffen. Die IT-Systeme sind nicht das Ziel, sie sind lediglich das Mittel zum Zweck. Die Angreifer nutzen zur Erreichung ihrer Ziele Methoden wie Cybercrime, Cyberspionage oder Cybersabotage, um einen finanziellen, politischen, wirtschaftlichen oder militärischen Vorsprung zu erlangen. Welche Methode von den Tätern angewandt wird, hängt vom übergeordneten Ziel des Cyberangriffs ab. Cyberangriffe stellen nicht nur ein technisches Problem dar, sondern beinhalten auch nichttechnische Aspekte. Daher können Cyberrisiken und Bedrohungen nicht nur mit technischen Sicherheitsmaßnahmen bekämpft werden, sondern müssen zwingend auch nichttechnische, wie physische, personelle und organisatorische Mittel beinhalten.

Vor diesem Hintergrund wird auch klar, dass Cybersicherheit hauptsächlich eine Management-Verantwortung darstellt und auf der obersten Führungsebene behandelt werden muss. Ein Abwälzen auf die IT-Abteilung hilft da nur bedingt. IT-Abteilungen denken in Funktion, Innovation und Kosten und richten ihre Sicherheitsarchitekturen dementsprechend danach aus. Das Denken im Rahmen sicherheitsrelevanter Geschäftsstrategien, globaler Sicherheitsgesetze und Regulierungen, Produktsicherheitsstrategien sowie in kriminellen, wettbewerblichen und staatlichen Täterstrukturen erfordert neue Rollen und Aufgaben im

Unternehmen, die es heutzutage, wenn überhaupt, nur auf vielen Schultern verteilt gibt. Ein umfassender strategischer Ansatz ist hier notwendig, andernfalls werden einige Unternehmen eine unsichere Zukunft erleben. Die Risiken reichen von finanziellen Schäden über Reputationsverluste bis hin zur drohenden Geschäftsaufgabe. Wie bei der Digitalisierung werden auch der Cybersicherheit etablierte Unternehmen zum Opfer fallen.

Obwohl sich langsam ein Paradigmenwechsel abzeichnet, neigt das Management immer noch dazu, die Cyberproblematik zu ignorieren oder in Form von IT-Sicherheit an die IT-Abteilung zu delegieren. Verständlicherweise sind die technischen Komponenten und die IT-Infrastrukturen der zentrale Angriffspunkt der Angreifer, aber sie sind letztlich nur Teil eines viel komplexeren Problems. Jedes Unternehmen sollte daher eine Grundhygiene etablieren, damit die einfachsten Angriffsarten nicht durchgeführt werden können, und parallel dazu alle weiteren relevanten Ebenen und Bereiche in Betracht ziehen.

Cybersicherheit sollte eines der wichtigsten strategischen Ziele des Unternehmens sein und ein integraler Bestandteil der Unternehmensstrategie. Dies bedeutet, dass alle relevanten Abteilungen bei der Entwicklung der Cyberstrategie einbezogen werden müssen. Zur Abklärung, ob ein Unternehmen potenziell Ziel eines Cyberangriffes werden wird, sollte es seine kritischen Prozesse und Infrastrukturen sowie das cyberrelevante Umfeld kennen und eruieren, wie abhängig die jeweiligen Geschäftsfelder von der Digitalisierung und Vernetzung sind. Ohne einen allumfassenden strategischen Ansatz, der die wesentlichen Leitlinien für den Umgang mit Cyberbedrohungen setzt, steigen die Eintrittswahrscheinlichkeit und das Schadensausmaß eines Cyberangriffs. Investitionen in IT Sicherheit können somit nicht zielgerichtet eingesetzt werden.

Die Entwicklung einer Cyberstrategie ist der erste Schritt in eine sichere und planbare Unternehmenszukunft. Egal in welcher Branche, ob Start-up, Mittelstand, Konzern oder Behörde, jeder sollte die Rahmenbedingungen setzen, die er braucht um den Cyberherausforderungen zu begegnen.

Fangen Sie an, bevor es zu spät ist.

Danksagung

Wir beschäftigen uns seit vielen Jahren mit den Problemstellungen bei der Entwicklung von Sicherheitsstrategien und technischen Lösungsszenarien für Staaten, Behörden und der Industrie. Viele Staaten haben Cyberstrategien entwickelt, aber auf der Seite der Unternehmen wurden kaum nennenswerte Fortschritte bei der Entwicklung von Cybersicherheitsstrategien gemacht. Das Thema Cybersicherheit ist unerschöpflich, daher entstand die Idee, ein Buch über Cybersicherheit und die Entwicklung von Cyberstrategien zu schreiben. Das Schreiben des Buchs hat sehr viel länger gedauert als erwartet, brachte einen erheblichen Aufwand an Recherche und Interviews mit sich und erfolgte meist an Wochenenden in Hotels in Deutschland, der Schweiz, Griechenland, Belgien, Irland, Südafrika und Tansania.

Wir bedanken uns bei den folgenden Personen für die wertvollen Beiträge, die diesem Buch die notwendige Aktualität sowie den Bezug zur Praxis geben:

Dr. Rolf Markus Werner, Vorsitzender der Geschäftsführung und Head of Central Europe, Fujitsu.
Dirk Kunze, Kriminalrat beim Landeskriminalamt Nordrhein-Westfalen.
Tobias Glemser, Geschäftsführer Secuvera GmbH, Gäufelden.
Dr. Georg Bräuchle, Marsh GmbH, Stuttgart.
Stephan Walder, Staatsanwalt lic.iur. stawa, Leiter des Kompetenzzentrums Cybercrime, Zürich.

Unser Dank gilt auch den Cybersicherheitsexperten und Fachleuten aus den deutschen Polizeien, insbesondere Stefan Becker vom Landeskriminalamt Nordrhein-Westfalen, der immer mit polizeifachlichem Rat zu Seite stand. Wir danken auch dem Deutschen Digitalverband Bitkom für seine fachliche und inhaltliche Unterstützung bei der Auswertung der Studien zum Wirtschaftsschutz und den Kosten eines Cybervorfalls. Hinter dem Bitkom stehen viele Menschen, die in den Arbeitskreisen Öffentliche Sicherheit und Wirtschaftsschutz unermüdlich an der Verbesserung der Cybersicherheit arbeiten. Wir möchten uns auch ganz herzlich bei Laura Crespo für Ihren wertvollen Beitrag zum Kapitel Staatliche Lösungen und internationale Cyberstrategien bedanken. Sie hat in den letzten Jahren die Schweizer Cyber-Außenpolitik maßgeblich mitgestaltet.

Auch ein großes Dankeschön an unseren Lektor Herr Matthias Zabel vom Lektorat Freiburg für seine Korrekturen und Anregungen unseres Manuskripts.

Unser besonderer Dank geht an Herrn Dr. Axel Garbers, Frau Ann-Kristin Wiegmann und Frau Sybille Thelen vom Springer Verlag für das Vertrauen und die Geduld in und mit unserem Buchprojekt.

Leider konnte weder eine Best Practice noch ein Unternehmen gefunden werden, welches bereit gewesen wäre über seine Cyberstrategie zu berichten. Am Ende wollten die befragten Unternehmen anonym bleiben, da sie keine Cyberstrategie haben oder weil sie an eine Geheimhaltung gebunden sind. Das liegt in der Natur der Cybersicherheit und erschwert natürlich die Erforschung des Themas. Die IT-Sicherheitsunternehmen, die wir angefragt – ob groß oder klein, ob Inland oder Ausland – haben viel versprochen, Informationen zugesagt und leider nichts zum Buch beigetragen, außer die referenzierten Berichte, die wir im Internet gefunden haben.

Dr. Stefanie Frey und Michael Bartsch
Deutschland und Schweiz, 2017

Sie erreichen uns unter: cyberstrategien@deutor.de
Webseite zu Cyberstrategien für Unternehmen: www.cyberstrategien-fuer-unternehmen.de

Inhaltsverzeichnis

Abbildungsverzeichnis