Allianz für Cyber-Sicherheit

INTERNET SECURITY ALLIANCE

Management von Cyber-Risiken

Ein Handbuch für die Unternehmensleitung

Mit Unterstützung von:

SAP

Inhalt

Danksagung

Wir möchten den folgenden Personen für ihre Beiträge zu diesem Handbuch danken (in alphabetischer Reihenfolge).

Insbesondere bedanken wir uns bei AIG und SAP für die Unterstützung bei der Erstellung des Handbuchs.

Internet Security Alliance Board of Directors

Justin Acquaro
Interim Global Chief Information and Product Cyber Security Officer
GE

Wil Bennett
Vice President, Chief Information Security Officer
USAA

Robyn M. Boerstling
Vice President of Infrastructure, Innovation and Human Resources Policy
National Association of Manufacturers

Ryan Boulais
Chief Information Security Officer
AES

Andrew Cotton
Partner and Americas Cybersecurity Leader
Ernst & Young, LLP

Deneen DeFiore
Vice President and Chief Information Security Officer
United Airlines

Jason Escaravage
Chief Information Security Officer
Thomson Reuters

John Frazzini
President and CEO
X-Analytics

Mike Gordon
Chief Information Security Officer
Lockheed Martin Corporation

Ron Green
Executive Vice President and Chief Security Officer
Mastercard

Tracie Grella
Global Head of Cyber
AIG

Michael Higgins
Vice President, Information Security and Chief Information Security Officer
L3 Harris

Lisa Humbert
Operational Risk Management Officer for the Americas
MUFG Americas

Andy Kirkland
Chief Information Security Officer, Global Cyber Security
Starbucks

Shaun McAdams
Executive Director, Cyber Operations
Raytheon Technologies

Tim McKnight
Chief Security Officer
SAP

Tim McNulty
Associate Vice President of Government Relations
Carnegie Mellon University

Greg Montana
Corporate Executive Vice President, Chief Risk Officer
FIS

Richard Rocca
Chief Information Security Officer
Bunge Ldt.

Carolann Shields
Chief Information Security Officer, Digital Technology
Baker Hughes

Richard Spearman
Group Corporate Security Director
Vodafone

Dimitrios Stratakis
Chief Technology Risk Officer
Bank of New York Mellon

Ted Webster
Senior Vice President, Security Governance, Risk and Compliance
Centene Corporation

J.R. Williamson
Senior Vice President and Chief Information Security Officer
Leidos

Larry Clinton
President and Chief Executive Officer
Internet Security Alliance

Josh Higgins
Senior Director of Policy and Communications
Internet Security Alliance

Anton Marx
Senior Executive Assistant to the President and CEO
Internet Security Alliance

National Association of Corporate Directors (NACD)

Peter R. Gleason
Chief Executive Officer

Erin Essenmacher
President and Chief Strategy Officer

Friso van der Oord
Director of Research and Editorial

Leah Rozin
Senior Research Manager

Barton Edgerton
Senior Manager Governance Analytics

Ted Sikora
Manager of Benchmarking and Data Insights

Reaa Chadha
Senior Research Analyst

Andrew Lepczyk
Research Analyst

Margaret Suslick
Senior Copy Editor

Patricia W. Smith
Art Director

Alex Nguyen
Graphic Designer

Mitwirkende der deutschen Version

Sebastian Hess
AIG

Torben Schwierzke
AIG

Erwin Kruschitz
Anapur

Matteo Große-Kampmann
AWARE7

Gregor Buerner
BASF Digital Solutions

Dietrich Kästner
BMW

Stefan Becker
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Simona Autolitano
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Benedikt Scherer
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Agnieszka Pawlowska
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Fabian Nißing
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Adrian Schneider
Commerzbank

Jens.Berwanger
Commerzbank

Sebastian Klipper
CycleSEC

Axel Petri
Deutsche Telekom

Christian Schoop
DLA Piper UK

Jan Pohle
DLA Piper UK

Niels Hoffmann
DLA Piper UK

Michael Ebner
Energie Baden-Württemberg

Gerhard Oppenhorst
ESC – Enterprise Security Center

Koen Gijsbers
Former Head of NATO NCI Agency

Larry Clinton
Internet Security Alliance

Josh Higgins
Internet Security Alliance

Anton Marx
Internet Security Alliance

Daniel Schatz
QIAGEN

Milen Volkmar
Q-SOFT

Tim McKnight
SAP

Niall Brennan
SAP

Florestan Peters
SoSafe

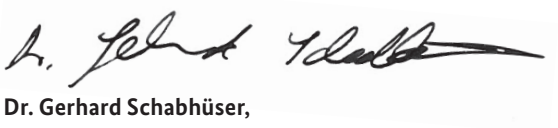
Vorwort

Seit Veröffentlichung des ersten Handbuches „Management von Cyber-Risiken“ im Jahr 2018 haben sich die Rahmenbedingungen unserer Arbeitswelt erheblich verändert. Die Corona-Pandemie hat nicht nur für die rasante Ausweitung des Homeoffice gesorgt, sondern auch die globalen Lieferketten beeinflusst. Die Digitalisierung in Staat, Wirtschaft und Gesellschaft ist in den letzten Jahren rasant vorangeschritten. Gleichzeitig hat sich die Bedrohungslage für die Informationssicherheit weiter verschärft. 2021 musste das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die Cyber-Sicherheitsbehörde des Bundes gleich zweimal die höchste Warnstufe für akute Schwachstellen bekanntgeben – ein bisher in der BSI-Geschichte einmaliger Vorgang. Auf der Bundespressekonferenz im Oktober 2021 haben wir bei der Vorstellung des BSI-Lageberichts in Teilbereichen Alarmstufe Rot ausgerufen.

Die fortschreitende Digitalisierung bei gleichzeitig steigender Bedrohungslage verdeutlicht vor allem eines: Informationssicherheit muss bei der Prozess- und Produktplanung von Anfang an mitgedacht werden. Sie darf nicht länger als Bremsklotz missverstanden, sondern muss als Investition in die Zukunft gesehen werden. Nur wenn wir das konsequent berücksichtigen, werden wir das volle Potenzial der Digitalisierung nutzen können. Mehr als je zuvor gilt: Informationssicherheit ist die Voraussetzung für eine nachhaltig sichere Digitalisierung. Das ist eine einfache Formel, die nicht immer einfach zu vermitteln ist. Denn erfolgreiche Cyber-Sicherheit ist unsichtbar. Nur wenn etwas passiert, werden Mängel bei der Absicherung sichtbar. Ransomware-Vorfälle verursachen Produktionsausfälle und legen Unternehmen und Lieferketten lahm. Zusammen mit dem oftmals nötigen Neuaufbau der IT-Systeme erleiden Unternehmen so oftmals hohe finanzielle Schäden.

Ich bin zutiefst davon überzeugt: Entscheiderinnen und Entscheider in Unternehmen müssen dieses Mindset annehmen, wenn sie ihr Unternehmens-Risiko analysieren. Cyber-Sicherheit ist Chefinnen- und Chefsache. Aus diesem Grund hat das BSI als Veranstalter des größten deutschen IT-Sicherheitskongresses dieses Motto für seinen Kongress im Jahr 2022 gewählt. Um die richtigen Entscheidungen treffen zu können, müssen Mitglieder der Unternehmensleitung einen angemessenen Zugang zu Cyber-Fachwissen haben. Darum freue ich mich besonders über die aktualisierte Version dieses Handbuchs und empfehle die Lektüre. Denn genauso, wie die Bedrohungslandschaft wächst, müssen wir unsere Fähigkeiten entwickeln, vorausschauend Cyber-Risiken zu managen.

Internationale Expertinnen und Experten haben mit ihrem Wissen und Best Practice-Erfahrungen zum Gelingen dieses Projektes beigetragen. Mein Dank gilt ihnen und insbesondere der Internet Security Alliance für diesen wichtigen Beitrag zu mehr Cyber-Sicherheit in Unternehmen.



Dr. Gerhard Schabhüser,
Vizepräsident des Bundesamtes für Sicherheit in der Informationstechnik

Vorwort

Die Internet Security Alliance (ISA) gratuliert dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zur zweiten Auflage des Handbuchs „Management von Cyber-Risiken“. Es war für die ISA eine Ehre, mit dem BSI an beiden Ausgaben zusammenzuarbeiten.

Dieses Handbuch befasst sich mit einem kritischen und oft übersehenen Aspekt der Cyber-Sicherheit - der einzigartigen Rolle der Aufsichtsräte und des Vorstands. Obwohl die leitenden Mitarbeiter des Unternehmens die Verantwortung für das Management von Cyber-Risiken tragen, ist es die Aufgabe des Vorstands, das Managementteam angemessen zu beaufsichtigen und sicherzustellen, dass die Überlegungen zu Cyber-Risiken in alle wichtigen Geschäftsentscheidungen einfließen.

Dieses Handbuch bietet dem Vorstand klare und präzise Grundsätze und Instrumente für die Zusammenarbeit zwischen Vorstand und Managementteam im Bereich der Cyber-Sicherheit.

Die aktuelle Ausgabe baut auf der Vorgängerausgabe auf und berücksichtigt die Erkenntnisse aus der Entwicklung ähnlicher Handbücher, die inzwischen auf vier Kontinenten und in fünf Sprachen im Umlauf sind. Frühere Ausgaben wurden von der ISA gemeinsam mit Partnerorganisationen wie dem BSI erstellt, darunter das US Department of Homeland Security, das US Department of Justice und die Organization of American States (OAS).

Ebenso wie das BSI zusammen mit der Allianz für Cyber-Sicherheit an dieser Ausgabe gearbeitet hat, wurden frühere Ausgaben in Kooperation mit der Europäischen Konferenz der Direktorenvereinigungen, der US National Association of Corporate Directors und der Japanese Business Federation veröffentlicht.

Die in diesem Buch dargelegten Grundsätze und Praktiken sind die einzigen Best Practices für die Überwachung von Cyber-Risiken, die jemals von unabhängiger Seite bewertet wurden und die nachweislich die Cyber-Sicherheit von Unternehmen erheblich verbessern. PWC hat in seiner globalen Studie zur Informationssicherheit festgestellt, dass Unternehmen, die diese Grundsätze und Praktiken anwenden, eine bessere Budgetierung, ein besseres Cyber-Risikomanagement, eine engere Abstimmung zwischen Geschäftszielen und Cyber-Sicherheit und die Schaffung einer Sicherheitskultur erreicht haben.

Darüber hinaus ist dies die erste Ausgabe des Handbuchs „Management von Cyber-Risiken“, das auch die Grundsätze enthält, die im Jahr 2021 vom Weltwirtschaftsforum in Zusammenarbeit mit ISA und NACD entwickelt wurden. Diese berücksichtigen den Gedanken, dass Unternehmensvorstände bei der Betrachtung von Cyber-Risiken über die Grenzen ihres Unternehmens hinausgehen und sich auf die Bedürfnisse des gesamten Cyber-Ökosystems konzentrieren müssen.

Dieser Gedanke deckt sich mit der Bewegung hin zu mehr Wertschätzung der ökologischen und sozialen Governance (ESG). Das bestimmende Merkmal des Internets ist die weitreichende Verflechtung unterschiedlicher Systeme. Kein einziges System - weder die Regierung noch die Industrie - kann sich allein absichern. Es liegt in der Verantwortung der Unternehmensvorstände, ihre umfassendere Verantwortung nicht nur zu erkennen, sondern sie auch wahrzunehmen.

Dieses Handbuch fordert Unternehmensvorstände nicht nur auf, solide Prinzipien und Praktiken anzuwenden, um ihre eigene Cyber-Sicherheit zu gewährleisten, sondern bekräftigt auch die Verantwortung des Vorstands und des Managements, über die eigene Organisation hinauszugehen und mit Regierungs- und Industriepartnern in einem gemeinsamen Verteidigungsmodell zusammenzuarbeiten.

Durch die Befolgung der Richtlinien und Empfehlungen in diesem Handbuch können Unternehmen nicht nur sich selbst besser schützen, sondern auch die Entwicklung eines nachhaltigen Cyber-Sicherheits-Systems für alle vorantreiben.

Larry Clinton,
Präsident der Internet Security Alliance

Einführung

Die Unternehmensleitung[1] ist dafür verantwortlich, die Strategie des Managements zu überwachen und Risiken, die sich auf das gesamte Unternehmen und seinen Wert für die Stakeholder und Aktionäre auswirken, zu erkennen und wohl überlegt darauf zu reagieren. In den letzten 25 Jahren hat sich jedoch die Art des Unternehmenswertes erheblich verändert, weg vom physischen und hin zum virtuellen.

Diese rasante „Digitalisierung" von Unternehmenswerten hat eine entsprechende Transformation von Strategien und Geschäftsmodellen zur Folge – und auch zu einer Digitalisierung von Unternehmensrisiken geführt. Tatsächlich bringt die digitale Transformation Vorteile für Unternehmen mit sich, aber auch potenzielle neue Risiken.

Wie im „Global Risks Report 2019" und im kürzlich erschienenen „Global Risks Report 2022" erwähnt, zählen Führungskräfte in fortgeschrittenen Volkswirtschaften Cyber-Angriffe zu ihren größten Sorgen.[2] Ein schwerwiegender Angriff kann nicht nur die finanzielle Gesundheit eines Unternehmens zerstören, sondern auch systemische Auswirkungen haben, die der Wirtschaft als Ganzes und sogar der nationalen Sicherheit schaden.

Im Jahr 2014 erstellte die National Association of Corporate Directors (NACD) in Zusammenarbeit mit AIG und der Internet Security Alliance (ISA) diese Handbuchreihe. In dieser wurden fünf Prinzipien festgelegt, die Unternehmensleitungen bei der Verbesserung ihrer Aufsicht über Cyber-Risiken berücksichtigen sollten.

Diese Handbuchreihe wurde von unabhängiger Seite bewertet. Dabei wurde festgestellt, dass es das Management von Cyber-Risiken sowie die Budgetierung verbessert und eine engere Abstimmung zwischen den Geschäftszielen und der Cyber-Sicherheit ermöglicht. So wird die Sicherheitskultur in den Unternehmen verbessert[3].

Mit dem Ziel, Cyber-Sicherheit zur Chefinnen- und Chefsache zu machen, hat die Allianz für Cyber-Sicherheit (ACS)[4] in enger Zusammenarbeit mit der Internet Security Alliance, dem NACD und der AIG bereits 2018 ein für den deutschen Markt überarbeitetes Handbuch[5] veröffentlicht.

Darin sind die fünf wichtigsten Prinzipien formuliert, welche die Unternehmensleitung befolgen sollte, um ihrer Verantwortung für Cyber-Sicherheit gerecht zu werden:

1. **Cyber-Sicherheit nicht nur als IT-Thema, sondern als Baustein des unternehmensweiten Risikomanagements verstehen:** Die Unternehmensleitung muss Cyber-Sicherheit nicht nur als IT-Risiko, sondern als strategisches Unternehmensrisiko verstehen und angehen.

2. **Rechtliche Auswirkungen von Cyber-Risiken verstehen:** Die Unternehmensleitung sollte die rechtlichen Auswirkungen von Cyber-Risiken in Bezug auf die individuellen Anforderungen ihres Unternehmens verstehen.

3. **Zugang zu Cyber-Sicherheitsexpertise sowie regelmäßigen Austausch sicherstellen:** Die Unternehmensleitung sollte einen angemessenen Zugang zu Cyber-Sicherheits-Expertise fordern. Diskussionen über Cyber-Risikomanagement sollten regelmäßig und in angemessenem Umfang auf die Tagesordnung gesetzt werden.

4. **Umsetzung geeigneter Rahmenbedingungen sowie Ressourcen für das Cyber-Risikomanagement sicherstellen:** Die Unternehmensleitung sollte die Erwartung formulieren, dass das Management einen unternehmensweiten Rahmen für das Cyber-Risikomanagement mit adäquater Personalausstattung und angemessenem Budget schafft.

5. **Risikoanalyse erstellen sowie Definition von Risikobereitschaft in Abhängigkeit von Geschäftszielen und -strategien formulieren:** Im Austausch zwischen Unternehmensleitung und Management über Cyber-Sicherheit sollte die Identifizierung und

[1] Während sich Unternehmen in den Vereinigten Staaten von Amerika durch ein monistisches System, das sich aus dem „Board of Directors" zusammensetzt, der Unternehmensorganisation auszeichnen, wird in Deutschland üblicherweise das dualistische System genutzt, das sich aus Vorstand / Geschäftsführung und Aufsichtsrat zusammensetzt. Mit dem Begriff „Unternehmensleitung" werden in diesem Handbuch alle entsprechenden Unternehmensorgane zusammengefasst, wo im englischen Original des Handbuchs ebenfalls das „Board of Directors" benutzt wird.

[2] World Economic Forum (2019). Global Risks Report 2019. Genf, Schweiz: World Economic Forum, S. 6.

[3] PwC (2016). Global State of Information Security Survey 2016. Online: PwC.

[4] Die Allianz für Cyber-Sicherheit (ACS) ist eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit dem Bitkom. Die ACS ist ein Privat-Public-Partnership und bietet seit 2012 eine Plattform für Informationsaustausch. Die Teilnehmenden profitieren von Best Practices und der Expertise eines starken Netzwerks. Weitere Informationen finden Sie auf der Webseite der Allianz für Cyber-Sicherheit.

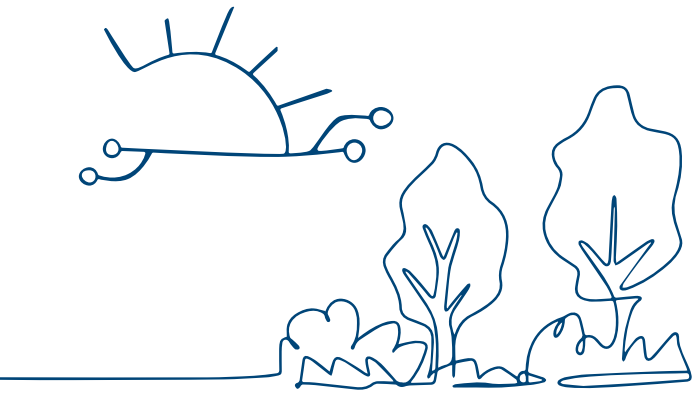
[5] Die erste Ausgabe des deutschen Handbuchs finden Sie auf der Webseite der Allianz für Cyber Sicherheit.

Quantifizierung der finanziellen Kosten in Bezug auf Cyber-Risiken diskutiert werden. Insbesondere sollte die Frage besprochen werden, welche Risiken akzeptiert, gemindert oder übertragen werden sollen, z. B. durch eine Versicherung, sowie spezifische Pläne, die mit jedem Ansatz verbunden sind.

Diese aktualisierte Ausgabe des Handbuchs baut auf diesen fünf Schlüsselprinzipien auf und enthält ein zusätzliches sechstes Prinzip:

6. **Unternehmensweite Zusammenarbeit und den Austausch von Best Practice fördern:** Die Unternehmensleitung sollte die Zusammenarbeit innerhalb ihrer Branche und mit öffentlichen und privaten Akteuren fördern, um sicherzustellen, dass jede Institution die Resilienz Aller unterstützt.

Des Weiteren erscheint neben diesem Handbuch ein umfassendes Toolkit, das die Unternehmensleitung bei der Umsetzung dieser sechs Prinzipien unterstützt. Während sich einige Formulierungen im Handbuch auf Aktiengesellschaften beziehen, gelten diese Grundsätze für alle Vorstände und Unternehmensleitungen, einschließlich der Mitglieder der Führung von privatwirtschaftlichen Unternehmen und gemeinnützigen Organisationen. Jede Organisation verfügt über wertvolle Daten und damit verbundene Ressourcen, die kontinuierlich von Cyber-Kriminellen oder anderen Widersachern bedroht sind.



Die Cyber-Bedrohungslage wächst

Der CSIS/McAfee-Bericht über Cyberkriminalität aus dem Jahr 2018 kommt zu dem Schluss: „Cyberkriminalität ist unerbittlich, unvermindert und wird wahrscheinlich nicht aufhören. Es ist einfach zu simpel und zu lohnend und die Chancen, erwischt und bestraft zu werden, werden als zu gering wahrgenommen. Cyber-Kriminelle sind technologisch genauso fortschrittlich wie die fortschrittlichsten IT-Unternehmen und haben sich wie diese schnell auf Cloud Computing, künstliche Intelligenz, [...] und Verschlüsselung eingestellt."[6]

Diesen Beobachtungen entsprechend hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Fortsetzung dieses Trends beobachtet. Zwischen Juni 2020 und Mai 2021 ist die Zahl der Angreifenden, die Schadsoftware für cyber-kriminelle Massenangriffe auf Privatpersonen, Wirtschaftsunternehmen und andere Institutionen einsetzen, exponentiell gestiegen.[7] Im Vergleich zum vorherigen Berichtszeitraum haben die Angreifenden die Produktion neuer Malware-Varianten deutlich beschleunigt. Während im vorangegangenen Berichtszeitraum durchschnittlich 322.000 neue Varianten pro Tag identifiziert wurden, erreichte dieser Tagesindikator im aktuellen Berichtszeitraum einen Durchschnitt von 394.000 Varianten - ein Anstieg von über 22 Prozent. Insgesamt produzierten Angreifende im aktuellen Berichtszeitraum also rund 144 Millionen neue Malware-Varianten.

Wer sind die Angreifer und wie greifen sie an?

Eines der charakteristischen Merkmale dieser Angriffe ist, dass sie praktisch alle Verteidigungssysteme eines Unternehmens wie Firewalls oder Intrusion-Detection-Systeme durchdringen und sogar auf cloudbasierte Daten, für die das Unternehmen nicht direkt die Sicherheit administriert, zugreifen können. Angreifende suchen nach zahlreichen Wegen, um alle Ebenen von Sicherheitsschwachstellen auszunutzen, bis sie ihr Ziel erreicht haben. Wenn Angreifende es auf die Systeme eines Unternehmens abgesehen haben, werden sie auch mit Sicherheit grenzender Wahrscheinlichkeit in diese eindringen können.

Neben Angreifenden, die sich in ein System hacken, stellen auch Insider-Bedrohungen wie Leiharbeitende und Angestellte - ob mit schädlicher Absicht oder einfach nur schlecht ausgebildet - für Unternehmen ein mindestens ebenso großes Risiko dar, wie Angriffe von außen.

[6] Lewis, J. A. (2018). Economic Impact of Cybercrime. At $600 Billion and Counting - No Slowing Down. Online: Center for Strategic and International Studies (CSIS) and McAfee, p. 4.

[7] Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland, S. 9.

[8] Bailey T., Kolo B., Rajagopalan K., Ware D. (September 2018). Insider Threat: The Human Element of Cyber Risk. Online: McKinsey & Company.

[9] Columbus L. (15. Mai, 2018). 76% Of IT Security Breaches Are Motivated By Money First. Online: Forbes.

„Wir sind zu klein, um für Angreifende interessant zu sein“ – Falsch!

Einige Unternehmen halten es für unwahrscheinlich, dass sie Opfer eines Cyber-Angriffs werden, weil sie relativ klein sind oder keinen bekannten Markennamen innehaben und eventuell über keine großen Mengen an sensiblen Kundendaten wie Kreditkartennummern, medizinischen Informationen etc. verfügen. Tatsächlich haben es Angreifende auf Unternehmen aller Größen und Branchen abgesehen und suchen nach allem, was von Wert sein könnte, einschließlich der folgenden Vermögenswerte:

- Geschäftspläne, einschließlich Fusions- oder Akquisitionsstrategien, Angebote usw.
- Handelsalgorithmen
- Verträge oder geplante Vereinbarungen mit Kunden, Lieferanten, Vertriebshändlern, Joint-Venture-Partnern usw.
- Anmeldeinformationen für Mitarbeitende
- Anlageninformationen, einschließlich Anlagen- und Ausrüstungsplänen, Gebäudeplänen und Zukunftsplänen
- F&E-Informationen, einschließlich neuer Produkte oder Dienstleistungen in der Entwicklung
- Informationen über wichtige Geschäftsprozesse
- Quellcode
- Listen von Mitarbeitenden, Kunden, Auftragnehmern und Lieferanten
- Kunden-, Spender- oder Treuhänderdaten

Quelle: Internet Security Alliance

Nach Angaben von McKinsey sind Insider-Bedrohungen bei der Hälfte aller Cyber-Vorfälle vorhanden.[8] Dies unterstreicht die Notwendigkeit eines starken und anpassungsfähigen Sicherheitskonzepts, das gleichermaßen auf externe und interne Cyber-Bedrohungen abgestimmt ist. Unternehmen können fortgeschrittene Bedrohungen nicht bewältigen, wenn sie nicht in der Lage sind, einfache Angriffe zu stoppen. In jüngster Zeit hat die Cyber-Erpressung durch Ransomware-Angriffe als Hauptrisiko für Organisationen aller Größenordnungen erheblich zugenommen. (Siehe Tool D – Reaktion auf Vorfälle.)

Die überwiegende Mehrheit der Cyber-Vorfälle ist wirtschaftlich motiviert.[9] Cyber-Kriminelle versuchen routinemäßig alle Arten von Daten zu stehlen, zu beschädigen oder zu verschlüsseln. Es gibt, wie oben beschrieben, zahlreiche typische Angriffsziele.

Viele kleinere und mittlere Unternehmen (KMU) haben in der Vergangenheit geglaubt, sie seien zu unbedeutend, um Ziel von Angriffen zu sein. Tatsächlich ist jedoch bereits die Mehrheit der KMU Opfer von Cyber-Angriffen geworden. Kleinere Firmen sind nicht nur selbst Ziel von Angriffen, sondern stellen über Kunden-, Lieferanten- oder Joint-Venture-Beziehungen häufig auch einen Angriffsvektor zu größeren Organisationen dar. Daher ist das Lieferanten- und Partnermanagement eine wichtige Funktion für alle miteinander vernetzten Unternehmen.

Die Zukunft ist die Balance zwischen Cyber-Sicherheit, Wachstum und Rentabilität

Wie andere kritische Risiken, mit denen Unternehmen konfrontiert sind, kann auch Cyber-Sicherheit nicht isoliert betrachtet werden. Die Mitglieder der Unternehmensleitung und des Managements müssen ein angemessenes Gleichgewicht zwischen dem Schutz der Sicherheit einer Organisation und der Minimierung von Verlusten finden. Gleichzeitig müssen sie die Rentabilität und das Wachstum in einem wettbewerbsorientierten Umfeld sicherstellen.

Um effektiv zu sein, darf die Cyber-Strategie nicht ausschließlich reaktiv sein. Führende Unternehmen müssen auch eine klare, vorausschauende Haltung einnehmen, indem sie Informationen über das Cyber-Risiko-Umfeld sammeln und potentielle Angriffsvektoren identifizieren. In diesem Sinne sollten sie zudem ihre eigenen Systeme und Prozesse regelmäßigen, strengen Tests unterziehen, um Schwachstellen zu ermitteln.

Die in diesem Handbuch beschriebenen sechs Prinzipien für ein effektives Management von Cyber-Risiken, werden in relativ allgemeiner Form dargestellt, um die Diskussion und Reflexion in der Unternehmensleitung anzuregen. Natürlich wird die Unternehmensleitung diese Empfehlungen je nach Größe, Lebenszyklus, Strategie, Geschäftsplänen, Branchenzugehörigkeit, geografischer Ausdehnung, Kultur usw. an die Besonderheiten ihrer Organisation anpassen müssen.

PRINZIP 1

Cyber-Sicherheit nicht nur als IT-Thema, sondern als Baustein des unternehmensweiten Risikomanagements verstehen

Die Unternehmensleitung muss die Cyber-Sicherheit nicht nur als IT-Risiko, sondern als strategisches Unternehmensrisiko verstehen und angehen.

Zur Umsetzung dieses Prinzips siehe:

- **Tool A:** „10 Fragen, die die Unternehmensleitung zur Cyber-Sicherheit stellen sollte"

Hintergrund

In der Vergangenheit stuften viele Unternehmen und Organisationen die Informationssicherheit als technisches oder betriebliches Problem ein, das überwiegend in der Verantwortung der IT-Abteilung liegt. Cyber-Sicherheit ist jedoch mehr als nur ein IT-Thema. Dieses Missverständnis wurde durch Silostrukturen genährt, die dazu führten, dass sich Funktionen und Geschäftsbereiche innerhalb des Unternehmens nicht für die Sicherheit der eigenen Daten verantwortlich fühlten. Stattdessen wurde diese essentielle Verantwortung an die IT-Abteilung abgegeben - eine Abteilung, die in den meisten Unternehmen über zu wenig Ressourcen und Budget verfügt. Die Verlagerung der Verantwortung auf die IT-Abteilung verhinderte zudem eine kritische Analyse von und Kommunikation über Sicherheitsfragen und erschwerte die Einführung effektiver, unternehmensweiter Sicherheitsstrategien.

In den letzten Jahren sind Technologie und Daten aus ihrer Nebenrolle herausgetreten und in den Mittelpunkt der Strategie gerückt. Beispielsweise nutzen zunehmend Unternehmen neue Wege der Datenverwaltung (z. B. die Speicherung einiger Daten in externen Netzwerken oder in öffentlichen Clouds), die die Kostenwirksamkeit und Effizienz verbessern können, aber auch neue Risiken mit sich bringen. Dies bedeutet, dass Cyber-Sicherheit mehr als ein IT-Problem ist. Die IT-Komponente ist zu einem Teil der allgemeinen Risikomanagementstrategie geworden und sollte gleichranging zu anderen Sicherheitsbereichen bewertet werden. Unternehmensleitungen müssen jetzt erkennen, dass Cyber-Sicherheit ein wesentlicher Bestandteil der herausfordernden und oft sehr anspruchsvollen Veränderungen in ihrem Unternehmen ist, um im digitalen Zeitalter zu wachsen und wettbewerbsfähig zu sein.

Während die Digitalisierung voranschreitet, haben viele Unternehmensleitungen und Management-Teams immer noch veraltete Ansichten über Cyber-Sicherheit. In der NACD-Umfrage zur Unternehmensführung aus den Jahren 2019-2020 wurde festgestellt, dass die Mehrheit der Unternehmensleitungen Cyber-Sicherheit nach wie vor als verbesserungsbedürftig ansieht[10] und erwartet, dass die sich verändernden Cyber-Sicherheitsbedrohungen innerhalb der nächsten zwölf Monate erhebliche Auswirkungen auf ihr Unternehmen haben werden.[11] Eine von EY durchgeführte globale Umfrage zur Informationssicherheit kam zu ähnlichen Ergebnissen: „77 % der Unternehmen arbeiten immer noch mit nur begrenzter Cyber-Sicherheit und Resilienz [gegen Cyberbedrohungen], während 87 % der Unternehmen darauf hinweisen, dass sie noch nicht über ausreichende Budgets verfügen, um das gewünschte Maß an Cyber-Sicherheit und Resilienz zu gewährleisten."[12] In einer Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gab ebenfalls nur etwa die Hälfte aller Befragten - unabhängig von der Unternehmensgröße - an, dass in ihrem Unternehmen das Prinzip „Cyber-Sicherheit ist Chefinnen- und Chefsache" gilt.[13]

Handlungsempfehlung

Vor diesem Hintergrund beschränken sich die Schlüsselfragen für die Unternehmensleitung nicht mehr darauf, wie technologische Innovationen Geschäftsprozesse ermöglichen können. Es geht vielmehr darum, wie die digitalen Transformationsprozesse mit einem effektiven Management der damit einhergehenden Cyber-Risiken in Einklang gebracht werden können.

Die Unternehmensleitung sollte sich auch darüber im Klaren sein, welche „Kronjuwelen" das Unternehmen am dringendsten schützen muss. So kann sie sicherstellen, dass das Unternehmen über eine Präventions-, Detektions- und Reaktionsstrategie verfügt.

Darüber hinaus kann die Unternehmensleitung das Management nach dem Verfahren zur Inventarisierung von Cyber-Risiken innerhalb des Unternehmens fragen, einschließlich der Art und Weise, wie sie in verschiedenen Geschäftsbereichen arbeiten, um potenzielle Schwachstellen zu ermitteln. Die Unternehmensleitung sollte das Management anweisen, nicht nur die wahrscheinlichsten Angriffe und Abwehrmaßnahmen zu berücksichtigen, sondern auch Angriffe mit geringer Wahrscheinlichkeit jedoch mit großen Auswirkungen, die katastrophale Folgen haben könnten. Angesichts der sich abzeichnenden disruptiven Technologien ist es für Unternehmensleitungen und das Management von essenzieller Bedeutung zu prüfen, ob ihre derzeitige Definition von „Kronjuwelen" noch gültig ist.

Unternehmensleitungen und Management beginnen, den Einsatz neuer digitaler Technologien sowie neue Möglichkeiten der Datennutzung in die Besprechungen über unternehmensweite Schlüsselstrategien und Pläne zu integrieren. Idealerweise sollte Cyber-Sicherheit Teil des gleichen Dialogs sein.

Zusammenfassend: Cyber-Sicherheit sollte als unternehmensweites Strategie- und Risikomanagementthema betrachtet werden, das ganzheitlich angegangen und bei wichtigen strategischen Entscheidungen proaktiv berücksichtigt werden sollte. Konkrete Vorschläge, wie dies erreicht werden kann, sind in den Prinzipien 4 und 5 sowie im gesamten Toolkit beschrieben.

Identifizierung der „Kronjuwelen" des Unternehmens

Die Unternehmensleitung sollte mit dem Management regelmäßig eine Diskussion über die folgenden Fragen führen:

- Was sind die wichtigsten Daten unseres Unternehmens?
- Wo befinden sie sich? Befinden sie sich auf einem oder mehreren Systemen?
- Wie wird auf sie zugegriffen? Wer hat die Erlaubnis, auf sie zuzugreifen?
- Wie oft haben wir unsere Systeme getestet, um sicherzustellen, dass sie unsere Daten angemessen schützen?

[10] National Association of Corporate Directors. (2019). 2019–2020 NACD Public Company Governance Survey. Arlington, VA: NACD, p. 13.
[11] Ebd. S. 12
[12] Ernest & Young (2021). Globale Umfrage zur Informationssicherheit. Online: EY.
[13] Bundesamt für Sicherheit in der Informationstechnik (2021). Umfrage zur IT-Sicherheit im Home-Office. Online: BSI.

PRINZIP 2

Rechtliche Auswirkungen von Cyber-Risiken verstehen

Die Unternehmensleitung sollte die rechtlichen Auswirkungen von Cyber-Risiken in Bezug auf die individuellen Anforderungen ihres Unternehmens verstehen.

Zur Umsetzung dieses Prinzips siehe:

- **Tool C:** „Risiken in der Lieferkette und gegenüber Dritten“
- **Tool D:** „Reaktion auf Vorfälle“
- **Tool G:** „Verbesserung der Offenlegung von Informationen zur Cyber-Sicherheit – 10 Fragen für die Unternehmensleitung“

Hintergrund

Das rechtliche und regulatorische Umfeld in Bezug auf Cyber-Sicherheit, darunter die Meldepflicht von Vorfällen, der Schutz der Privatsphäre und persönlicher Daten, der Informationsaustausch und der Schutz von Infrastrukturen, ist komplex und entwickelt sich ständig weiter. Die Unternehmensleitung sollte sich über die aktuellen Compliance- und Haftungsfragen, mit denen ihre Organisationen - und möglicherweise auch die Mitglieder der Unternehmensleitung auf individueller oder kollektiver Basis - konfrontiert sind, informieren.

Auf der Ebene der Europäischen Union ist die Regulierungslandschaft sehr komplex. In den letzten Jahren haben die europäischen Institutionen eine Reihe von Verordnungen erlassen, die unmittelbar für Unternehmen gelten, die in der EU tätig werden wollen. Mit der Verabschiedung der Datenschutz-Grundverordnung (DSGVO) im Jahr 2016 mussten Unternehmen beispielsweise eine Reihe von Mechanismen einrichten, um eine rasche Meldung von Verletzungen des Schutzes von personenbezogener Daten zu gewährleisten.

Neben der DSGVO enthält auch die Richtlinie über die Netz- und Informationssicherheit (NIS) der Europäischen Union aus dem Jahr 2016 wichtige Anforderungen, die sich sowohl an die Mitgliedstaaten als auch an Unternehmen richten, die unter die Kategorie „Betreiber wesentlicher Dienste“ und „Anbieter digitaler Dienste“ fallen. (Anm. d. Übers.: Die Richtlinie wird derzeit überarbeitet. Zum Zeitpunkt der Erstellung dieses Handbuchs wurde eine politische Einigung zwischen dem Europäischen Parlament und dem Europäischen Rat erzielt. Die überarbeitete Richtlinie aktualisiert unter anderem die Liste der Sektoren und Tätigkeiten, die den Cyber-Sicherheitsverpflichtungen unterliegen, und verbessert ihre Durchsetzung.)

Weitere relevante Initiativen der Europäischen Union im Bereich der Cyber-Sicherheit sind im Bereich der Zertifizierung und Normung zu finden, wie etwa die Verabschiedung des „Europäischen Rechtakts zur Cyber-Sicherheit“ (Cybersecurity Act) im Jahr 2019. In jüngster Zeit sind zusätzliche Harmonisierungsbemühungen in den Richtlinien zu bestimmten Aspekten von Verträgen über die Bereitstellung digitaler Inhalte, Dienstleistungen und Waren sowie im Vorschlag für eine Verordnung über harmonisierte Vorschriften für KI zu finden.

Unternehmen sollten bedenken, dass EU-Mitgliedsstaaten aufgrund der Natur der Richtlinien der Europäischen Union die europäische Gesetzgebung umsetzen müssen, aber oft einen gewissen Spielraum behalten. Damit soll eine Mindestharmonisierung im EU-Binnenmarkt erreicht und gleichzeitig der Vielfalt der EU-Mitgliedstaaten Rechnung getragen werden. Über diese Mindestharmonisierung hinaus, können Mitgliedstaaten also zusätzliche Regelungen treffen, sofern diese nicht mit dem EU-Recht kollidieren. Aus diesem Grund sind die oben erwähnten Rechtsakte nicht die einzigen Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cyber-Sicherheitsniveaus. Infolgedessen könnten Industriezweige und Branchen innerhalb der EU immer noch unterschiedlichen Verpflichtungen unterliegen.

Wie dieser kurze, bei weitem nicht allumfassende, Überblick über legislative Maßnahmen auf europäischer Ebene zeigt, ist die europäische Rechtslandschaft sehr komplex. Aufgrund der Komplexität der rechtlichen Situation wird empfohlen, bei Bedarf interne oder externe Rechtsberatung einzuholen.

Die gleiche Komplexität gilt für die USA, wo jede Branche mit zunehmenden Anforderungen auf Landes- und Bundesebene konfrontiert ist. Einige dieser Anforderungen umfassen nun auch Governance-Strukturen, die zeitnahe Vorfallmeldung sowie die Überwachung von Drittparteien und Anbietern. Daher sollte sich die Unternehmensleitung darüber informieren, ob das Management über ein wirksames Compliance-Programm verfügt, um den sich ändernden Anforderungen und Meldepflichten und den damit verbundenen Verpflichtungen gerecht zu werden.[14]

Aufsehenerregende Angriffe können Klagen nach sich ziehen, darunter (bei börsennotierten Unternehmen) Aktionärsklagen, in denen das Unternehmen der Misswirtschaft, der Verschwendung von Unternehmensvermögen und des Kontrollmissbrauchs beschuldigt wird. Die klagenden Parteien können auch behaupten, dass die Unternehmensleitung ihre treuhänderische Pflicht vernachlässigt hat, da sie nicht hinreichend geprüft hat, ob ausreichende Maßnahmen zum Schutz der Unternehmensdaten getroffen worden sind. Die Risiken können je nach Abhängigkeit des Unternehmens von Technologie und Daten, der Branche und den Standorten sehr unterschiedlich sein.

Mitglieder der Unternehmensleitung können vor solchen Risiken geschützt werden, solange sie angemessene Aufsichtsmaßnahmen im Vorfeld eines Cyber-Sicherheitsvorfalls und Untersuchungsmaßnahmen nach einem Vorfall ergreifen. Zu den Überlegungen gehören das Führen von Aufzeichnungen über Diskussionen in der Unternehmensleitung über Cyber-Sicherheit und Cyber-Risiken, das Informieren über branchen-, regions- oder sektorspezifische Anforderungen, die für das Unternehmen gelten und die Festlegung, was nach einem Cyber-Angriff offengelegt werden soll. Es ist außerdem ratsam, dass Mitglieder der Unternehmensleitung gemeinsam an einer oder mehreren Cyber-Angriffssimulationen oder „Table-Top-Übungen“ teilnehmen, um ihre Rolle und den Reaktionsprozess des Unternehmens im Falle eines schwerwiegenden Vorfalls besser zu verstehen.

Handlungsempfehlung

In den Protokollen der Unternehmensleitung sollte festgehalten werden, bei welchen Gelegenheiten das Thema Cyber-Sicherheit auf der Tagesordnung der Sitzungen der gesamten Unternehmensleitung und/oder (je nach Verteilung der Aufsichtsaufgaben) der wichtigsten Gremien stand. Die Diskussionen bei diesen Sitzungen können Updates über spezifische Risiken und Strategien zur Risikominderung sowie Berichte über den Cyber-Sicherheitsplan des Unternehmens und die Integration von Technologie in die Strategie, die Richtlinien und die Geschäftsaktivitäten des Unternehmens umfassen. Sich der Risiken einfach nur bewusst zu sein, reicht nicht aus. Die Dokumentation der Cyber-Sicherheits-Awareness und die Konsultation eines externen Rechtsbeistands können hilfreich sein, um Risiko und Haftung zu verringern.

Auch wenn die Mitglieder der Unternehmensleitung nicht über umfassende Kenntnisse in diesem zunehmend komplexen Rechtsgebiet verfügen müssen, sollten sie regelmäßig von internen oder externen Rechtsberatenden über die für das Unternehmen geltenden Anfor-

[14] Obwohl einige dieser Vorschriften in diesem Prinzip und im gesamten Handbuch hervorgehoben werden, handelt es sich um Beispiele, die bei weitem nicht allumfassend sind.

derungen informiert werden. Anhand von Management Reports sollte die Unternehmensleitung beurteilen können, ob das Unternehmen diesen potenziellen rechtlichen Risiken angemessen begegnet oder nicht.

Unternehmen und Organisationen können einer Reihe von Offenlegungs- oder Compliance-Verpflichtungen im Zusammenhang mit Cyber-Sicherheitsrisiken und Cybervorfällen unterliegen, darunter die folgenden:

1. DSGVO und BDSG (Bundesdatenschutzgesetz), Meldepflichten bei Datenschutzverletzungen sowie datenschutzrechtliche, aus dem Datengeheimnis resultierende sowie arbeitsrechtliche Einschränkungen, die sich auf den Cyber-Sicherheitsplan des Unternehmens auswirken.

2. NIS-Richtlinie und Anforderungen für die Meldung von Cyber-Sicherheitsvorfällen sowie Möglichkeiten des Informationsaustausches, die die Organisation in die Lage versetzen, sich über Cyber-Sicherheitsbedrohungen zu informieren.

3. Anbieter Kritischer Infrastrukturen[15] müssen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nach § 8b Abs. 4 des BSI-Gesetz (BSIG) eine erhebliche Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit oder eine außergewöhnliche Störung der IT melden. Die branchenspezifischen Vorschriften für die Sektoren Kommunikation, Finanzdienstleistungen, Energie und Kernenergie schreiben alle die Offenlegung erheblicher Unterbrechungen aufgrund eines Cyber-Sicherheit-Ereignisses oder einer anderen erheblichen IT-Störung vor (das BSI kann seinerseits andere Parteien über die Störung informieren, wenn es die Meldung erhält und dies nicht den Interessen der offenlegenden Partei zuwiderläuft).

4. Unternehmen im besonderen öffentlichen Interesse müssen gemäß § 8f Abs. 7 und Abs. 8 des BSI-Gesetzes (BSIG) die folgenden Störungen unverzüglich an das BSI melden[16]:
   a. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit der IT-Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung bzw. zu einem Störfall nach der Störfall-Verordnung geführt haben.
   b. Erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit der IT-Systeme, Komponenten oder Prozesse, die zu einer Beeinträchtigung der Erbringung der Wertschöpfung bzw. zu einem Störfall nach der Störfallverordnung führen können.

5. Sonstige geltende länderspezifische Gesetze, Vorschriften und Normen denen die Organisation unterliegt. Dazu können klare Sicherheitsanforderungen, verschiedene Datenschutzbeschränkungen, Beschränkungen beim Einsatz von Sicherheitstechnologien wie Verschlüsselung und Datenlokalisierungsanforderungen sowie Beschränkungen beim Hackback gegen Cyber-Kriminelle gehören.

6. Obwohl es keine spezielle Pflicht zur Information der Staatsanwaltschaft gibt, kann die Einschaltung der Staatsanwaltschaft in einigen Fällen zur Klärung des Sachverhalts und zur Sammlung von Beweisen beitragen, die für Schadensersatzansprüche von und gegen das Unternehmen relevant sind.

Die Offenlegung von Cyber-Sicherheitsrisiken in öffentlichen Berichten und Veröffentlichungen ist noch nicht vorgeschrieben, könnte aber in Zukunft erforderlich werden. Daher sollten die Mitglieder der Unternehmensleitung das Management bitten, Rechtsberatung zu potenziellen Offenlegungserwägungen in Bezug auf mögliche zukünftige Risikofaktoren im Allgemeinen und auch in Bezug auf das Notfall- und Krisenkonzept des Unternehmens für die Reaktion auf eine größere Sicherheitsverletzung oder einen anderen Cyber-Vorfall einzuholen. Da sich die Offenlegungsstandards, die behördlichen Richtlinien, die formalen Anforderungen und die Gegebenheiten des Unternehmens ständig weiterentwickeln, sollte die Unternehmensleitung und das Management damit rechnen, dass sie von den Rechtsbeiständen regelmäßig auf den neuesten Stand gebracht werden. Schlussendlich sollten die Mitglieder der Unternehmensleitung das Management auffordern, ein integriertes Cyber-Risikomanagement aufzubauen, das rechtliche Risiken, Cyber-Bedrohungen und Auswirkungen auf die Geschäftserwartungen kombiniert, um ihre Gesamtstrategie zur Risikominderung zu verbessern.

[15] Kritische Infrastrukturen (KRITIS) sind organisatorische und physische Strukturen und Einrichtungen, die für die Gesellschaft und Wirtschaft eines Landes so wichtig sind, dass ihr Ausfall oder ihre Beeinträchtigung zu anhaltenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würde. Am häufigsten werden mit diesem Begriff beispielsweise Einrichtungen für Unterkünfte, Heizung, Landwirtschaft, Lebensmittelproduktion und -verteilung, Wasserversorgung, Verkehrssysteme oder öffentliche Gesundheit in Verbindung gebracht.

[16] Unternehmen im besonderen öffentlichen Interesse werden im § 2 Abs. 14 BSIG definiert. Weitere Informationen zu den Pflichten und, ab wann diese für die in § 2 Absatz 14 definierten Unternehmen gelten, finden sich in § 8f BSIG und auf der BSI-Webseite.

PRINZIP 3

Zugang zu Cyber-Sicherheitsexpertise sowie regelmäßigen Austausch sicherstellen

Die Unternehmensleitung sollte einen angemessenen Zugang zu Cyber-Sicherheits-Expertise fordern. Diskussionen über Cyber-Risikomanagement sollten regelmäßig und in angemessenem Umfang auf die Tagesordnung gesetzt werden.

Zur Umsetzung dieses Prinzips siehe:

- **Tool A:** „10 Fragen, die ein Mitglied der Unternehmensleitung zur Cyber-Sicherheit stellen sollte“
- **Tool B:** „Die Bedrohung durch Innentäter oder Innentäterinnen – eine reale und allgegenwärtige Gefahr“
- **Tool F:** „Im regelmäßigen Austausch mit CISO/IT-Sicherheitsbeauftragten“
- **Tool H:** „Persönliche Cyber-Sicherheit für Mitglieder der Unternehmensleitung“

Hintergrund

Mit der zunehmenden Cyber-Bedrohung sind auch die Verantwortlichkeiten (und die Erwartungen) der Mitglieder der Unternehmensleitung gewachsen. Die Mitglieder der Unternehmensleitung müssen mehr tun, als nur zu verstehen, dass es Bedrohungen gibt, und Berichte entgegenzunehmen. Sie müssen dieselben Prinzipien des kritischen sowie konstruktiven Hinterfragens anwenden, die bei Diskussionen zwischen Unternehmensleitung und Management über Strategie und Unternehmensleistung zum Standard gehören. Wie ein Unternehmensleitender auf einem NACD-Forum feststellte „kann man Cyber-Kenntnisse ähnlich wie Finanzkenntnisse betrachten. Nicht jeder in der Unternehmensleitung ist ein Wirtschaftsprüfer, aber jeder sollte in der Lage sein, einen Finanzbericht zu lesen und die Finanzsprache der Wirtschaft zu verstehen.“[17]

Wie in Prinzip 1 erläutert, haben Unternehmensleitungen inzwischen verstanden, dass Cyber-Sicherheit nicht einfach ein separater Tagesordnungspunkt ist, der am Ende einer Sitzung ein paar Minuten lang behandelt wird. Vielmehr ist die Cyber-Sicherheit ein wesentliches Element vieler Geschäftsentscheidungen auf Unternehmensleitungsebene und muss frühzeitig im Austausch über Themen wie Fusionen, Übernahmen, Entwicklung neuer Produkte, strategische Partnerschaften usw. einbezogen werden.

Infolgedessen müssen Unternehmensleitungen nicht nur auf Informationen aus der IT und dem technischen Betrieb zugreifen, sondern auch auf Informationen aus einer Viel-

[17] National Association of Corporate Directors, et al. (2014). Cybersecurity: Boardroom Implications. Washington DC: NACD, S. 3.

zahl von Quellen wie Personalwesen, Finanzen, Öffentlichkeitsarbeit, Recht und Compliance und anderen.

Ausführlichere Informationen darüber, wie das Management dieses moderne Konzept des Cyber-Risiko-Managements besser umsetzen kann, finden Sie in „Cybersecurity for Business“[18], dem Begleitband zum „Cyber Risk Oversight Handbook“.

In den letzten zehn Jahren sind die Unternehmensleitungen bei der Überwachung der Cyber-Sicherheit aktiver geworden und fordern mehr Informationen vom Management.

Eine Umfrage aus dem Jahr 2012 ergab, dass weniger als 40 Prozent der Unternehmensleitungen regelmäßig Berichte über Datenschutz- und Sicherheitsrisiken erhielten, und 26 Prozent erhielten solche Informationen selten oder nie.[19]

Seitdem haben sich die Praktiken in den Unternehmensleitungen drastisch verändert. In einer NACD-Umfrage unter Mitgliedern von Unternehmensleitungen öffentlicher Unternehmen sind 79 Prozent der Meinung, dass sich das Verständnis der Unternehmensleitung für Cyber-Risiken im Vergleich zu vor zwei Jahren deutlich verbessert hat.[20] Tatsächlich geben die meisten Unternehmensleitungen an, dass sie regelmäßig Fragen der Cyber-Sicherheit besprechen und Informationen von unterschiedlichen Mitgliedern des Management-Teams erhalten. Die Mehrheit der Unternehmensleitungen hat im vergangenen Jahr die Reaktionspläne und den Datenschutz ihres Unternehmens geprüft, Informationen von internen Beratern erhalten, und sich mit dem Management-Team über den Umgang mit Cyber-Risiken ausgetauscht. Mehr als 75 Prozent der Unternehmensleitungen haben im vergangenen Jahr den aktuellen Ansatz ihres Unternehmens zur Sicherung seiner wichtigsten Vermögenswerte gegen Cyber-Angriffe überprüft.[21]

Nebst dieser Anzeichen von Fortschritt, will die Mehrheit der Mitglieder von Unternehmensleitungen ihre „Aufsichtsaufgaben in Bezug auf Cyber-Sicherheit im kommenden Jahr verstärkt wahrnehmen.“[22] Sie verfügen häufig über juristisches und finanzielles Fachwissen, aber nicht über Cyber-Sicherheitskenntnisse. Tatsächlich glaubt nur ein kleiner Prozentsatz der Unternehmensleitenden, dass ihre Unternehmensleitung über ein „hohes“ Maß an Wissen über Cyber-Sicherheitsrisiken verfügt, und nur wenige Unternehmen geben an, dass ihre Informationssicherheitsberichterstattung derzeit ihre Erwartungen vollständig erfüllt.[23]

Zusammenfassend lässt sich sagen, dass mit der zunehmenden Verantwortung der Unternehmensleitung für die Überwachung von Cyber-Risiken auch der Bedarf an Informationen und Fachwissen im Bereich der Cyber-Sicherheit steigt.

Handlungsempfehlung

Es gibt keinen einheitlichen Ansatz, der für jede Unternehmensleitung geeignet ist: Einige entscheiden sich dafür, alle Diskussionen über Cyber-Risiken auf der Ebene der gesamten Unternehmensleitung zu führen; andere weisen einem oder mehreren Ausschüssen (Prüfungs-, Risiko-, Technologieausschuss usw.) spezifische Aufsichtsaufgaben im Zusammenhang mit der Cyber-Sicherheit zu; und wieder andere verwenden eine Kombination dieser Methoden.

Die Mitglieder der Unternehmensleitung sollten klare Erwartungen an das Management hinsichtlich des Formats, der Häufigkeit und der Detailtiefe der cyber-sicherheitsbezogenen Informationen, die sie erhalten möchten, formulieren. Dem sollte vorausgehen, dass das Fachwissen über Cyber-Sicherheit innerhalb des Unternehmens genutzt wird, um die Kenntnisse zu erweitern. Unternehmensleitungen sollten hierzu in direktem Kontakt mit dem Chief Information Security Officer (CISO) stehen. Die Unternehmensleitung kann gemeinsam mit dem CISO und dem Sicherheitsteam „Deep Dives“ und Schulungsprogramme planen, um die Unternehmensleitung in Cyber-Fragen fortzubilden.

Um aktuelle Informationen über den Stand der Cyber-Sicherheit im Unternehmen zu gewährleisten, sollte die Unternehmensleitung das Management auffordern einen umfassenderen, unternehmensweiten Risikorahmen und eine Berichtsstruktur einzuführen, wie sie in Prinzip 4 erörtert werden.

[18] Clinton, L. ed. (2022). Cybersecurity for Business: *Organization-wide Strategies To Ensure Cyber Risk is NOT Just an “IT” Issue*. London, New York, New Delhi: Kogan Page.

[19] Westby J. R. (2012). *Governance of Enterprise Security: CyLab 2012 Report*. Pittsburgh, PA: Carnegie Mellon University, p. 7 and p. 16.

[20] National Association of Corporate Directors (2019). 2019–2020 NACD Public Company Governance Survey. Arlington, VA: NACD, p. 20.

[21] Ebd. S. 10.

[22] National Association of Corporate Directors (2019). Current and Emerging Practices in Cyber Risk Oversight. Arlington, VA: NACD, p.1.

[23] Ernest & Young (August 16, 2019). EY Global information Security Survey. Online: EY.

Darüber hinaus muss der von der Unternehmensleitung gewählte Ansatz in den Satzungen der Ausschüsse klar definiert sein, um Verwirrung oder Doppelarbeit zu vermeiden. Die gesamte Unternehmensleitung sollte regelmäßig und bei bestimmten Vorfällen oder Situationen über Cyber-Sicherheitsfragen informiert werden. Ausschüsse, die für das Risiko- und insbesondere Cyber-Risikomanagement zuständig sind, sollten mindestens vierteljährlich unterrichtet werden.

Um den Wissensaustausch und den Dialog zu fördern, kann die Unternehmensleitung auch Mitglieder zum Austausch über Cyber-Risikothemen auf Ausschussebene einladen. Es sollte auch die die Möglichkeit des ausschussübergreifenden Austauschs genutzt werden.

Die Berichterstattung des Managements über relevante Cyber-Sicherheitsangelegenheiten an die Unternehmensleitung sollte in ihrer Struktur flexibel genug sein, um das sich verändernde Bedrohungsumfeld zu berücksichtigen. Darin sollten sich auch die sich verändernden Unternehmensumstände, sowie die Bedarfe der Unternehmensleitung wiederspiegeln.

Die Aufnahme des Themas Cyber-Sicherheit als eigenständigen Punkt in die Tagesordnungen von Sitzungen der Unternehmensleitung und/oder Ausschüssen ist mittlerweile weit verbreitet. Cyber-Sicherheitt sollte jedoch auch in eine Vielzahl von weiteren Themen integriert werden, die der Unternehmensleitung vorgelegt werden, wie z. B. Diskussionen über neue Geschäftspläne und Produktangebote.

Da, wie in Prinzip 1 bereits dargestellt, die Vermögenswerte eines Unternehmens immer mehr zu digitalen Vermögenswerten werden, sind praktisch alle wichtigen Geschäftsentscheidungen, die der Unternehmensleitung vorgelegt werden, mit Cyber-Sicherheits-Aspekten verbunden. In vielerlei Hinsicht ist die Cyber-Sicherheit heute ein Querschnittsthema, ähnlich wie die Bereiche Recht und Finanzen. Effektive Unternehmensleitungen betrachten Cyber-Sicherheit als ein unternehmensweites Risikomanagement-Thema.

Andere Methoden zur Erweiterung des eigenen Fachwissens:

- Planen von vertiefenden Briefings oder Prüfungen durch unabhängige und objektive externe Expertinnen und Experten, die bestätigen, ob die Cyber-Sicherheitsstrategie des Unternehmens seine Ziele erreicht.

- Nutzung der bestehenden unabhängigen Beraterinnen und Berater der Unternehmensleitung, wie externe Wirtschaftsprüfer und externe Anwälte, die eine kunden- und branchenübergreifende Perspektive auf Cyber-Risikotrends haben.

- Teilnahme an einschlägigen internen und externen Fortbildungsprogrammen für Führungskräfte sowie an Veranstaltungen wie dem Deutschen IT-Sicherheitskongress.[24] Solche Veranstaltungen bieten eine gute Gelegenheit zum Austausch und Lernen. Hier können Unternehmensleitungen voneinander lernen und relevante Informationen teilen, um das systemische und individuelle Risiko zu minimieren. Wichtig ist auch, dass die Unternehmensleitungen einen Punkt „Rückmeldung“ in ihre Tagesordnungen aufnehmen, um ihre Erkenntnisse aus den externen Veranstaltungen mit anderen Führungskräften teilen zu können.

- Einen regelmäßigen Austausch mit den Strafverfolgungsbehörden und Regierungsvertretenden, mit denen das Unternehmen im Falle eines Cyber-Vorfalls oder einer Sicherheitsverletzung zusammenarbeiten wird, etablieren, um Angriffe zu untersuchen und darauf zu reagieren. So können Unternehmen beispielsweise Beziehungen zum Bundesamt für Sicherheit in der Informationstechnik und zu lokalen Strafverfolgungsbehörden aufbauen. Im Hinblick auf eine mögliche Sicherheitsverletzung wird damit die Koordination zwischen Wirtschaft und Staat besser gewährleistet. Ein erfolgreiches Beispiel für die Zusammenarbeit zwischen Wirtschaft und dem BSI ist die Allianz für Cyber-Sicherheit. Die ACS ist eine öffentlich-private Partnerschaft, die seit 2012 eine Plattform für den Informationsaustausch, die gemeinsame Nutzung bewährter Verfahren und die Zusammenarbeit zwischen den Mitgliedern des Netzwerks bietet.

[24] Mehr Informationen zum IT-Sicherheitskongress erfahren Sie auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik.

Snapshot: Derzeitige Debatte

Die Frage, wie die Unternehmensleitung die Überwachung von Risiken, insbesondere im Sinne eines Cyber-Risikomanagements, organisieren soll, ist Gegenstand der derzeitigen Debatte. Ein Ansatz, der aktuell diskutiert wird, könnte darin liegen, die Unternehmensleitenden direkt mit Fachwissen im Bereich Cyber-Security und/oder IT-Sicherheit auszustatten indem neue Mitglieder der Unternehmensleitung eingestellt würden. Auch wenn dies für einige Unternehmen oder Organisationen angemessen sein mag, gibt es keine allgemeingültige Lösung. Es gibt mehrere Fragen, die die Unternehmensleitung berücksichtigen sollte, bevor sie sich für diese Strategie entscheidet:

- Wie definieren wir den Begriff „Cyber-Experte“ bzw. „Cyber-Expertin”? Das erste Prinzip dieses Handbuchs lautet, dass Cyber-Sicherheit nicht nur ein „IT“-Thema, sondern Bestandteil des unternehmensweiten Risikomanagements ist. Sucht die Unternehmensleitung also nach einem Experten oder einer Expertin für unternehmensweite Sicherheitsfragen?
- Wird mit dieser Strategie wirklich die Übernahme der Verantwortung für Cyber-Sicherheit an eine einzelne Person delegiert, die eigentlich die gesamte Unternehmensleitung innehaben sollte? Wäre es nicht sinnvoller, wenn die gesamte Unternehmensleitung ihr Verständnis von Cyber-Sicherheitssystemen auf eine Art und Weise verbessern würde, die dem Verständnis entspricht, das Nicht-Juristen und Nicht-Juristinnen sowie Nicht-Finanzexperten und Nicht-Finanzexpertinnen von diesen jeweiligen Themen haben?
- Wie verträgt sich ein einzelner Cyber-Experte oder eine einzelne Cyber-Expertin in der Unternehmensleitung mit den funktionsübergreifenden Cyber-Management-Strukturen, die immer häufiger anzutreffen sind (z. B. das auf Seite 34 beschriebene Modell der „Three Lines of Defense“)?
- Ist die Aufnahme eines Cyber-Experten oder einer Cyber-Expertin in die Unternehmensleitung ein Präzedenzfall für die Zuweisung von Sitzen für andere Fachbereiche wie Diversität oder Umwelt-, Sozial- und Governance-Angelegenheiten?

PRINZIP 4

Umsetzung geeigneter Rahmenbedingungen sowie Ressourcen für das Cyber-Risikomanagement sicherstellen

Die Unternehmensleitung sollte die Erwartung formulieren, dass das Management einen unternehmensweiten Rahmen für das Cyber-Risikomanagement mit adäquater Personalausstattung und angemessenem Budget schafft.

Zur Umsetzung dieses Prinzips siehe:

- **Tool B:** „Die Bedrohung durch Innentäter oder Innentäterinnen – eine reale und allgegenwärtige Gefahr“
- **Tool C:** „Risiken in der Lieferkette und gegenüber Dritten“
- **Tool D:** „Reaktion auf Vorfälle“
- **Tool E:** „Metriken zur Cyber-Sicherheit auf Ebene der Unternehmensleitung“
- **Tool F:** „Im regelmäßigen Austausch mit CISO/IT-Sicherheitsbeauftragten“
- **Tool G:** „Verbesserung der Offenlegung von Informationen zur Cyber-Sicherheitsaufsicht - 10 Fragen für Unternehmensleitungen“
- **Tool I:** „Ressourcen der Bundesregierung Deutschland“

Hintergrund

Während sich Prinzipien 1, 2 und 3 dieses Handbuchs darauf konzentrierten, was die Unternehmensleitung selbst tun sollte, fokussieren sich die Prinzipien 4 und 5 eher darauf, was die Unternehmensleitung vom Management erwarten sollte. Damit die Unternehmensleitung wirksam ihre Aufsichtspflicht ausüben kann, ist es wichtig, dass sie die Verantwortlichkeiten des Managements im Hinblick auf die Cyber-Sicherheit der Organisation vollständig versteht.

Wie in Prinzip 1 dargelegt, sollte sich die Unternehmensleitung vergewissern, dass das Management einen angemessenen unternehmensweiten Ansatz für die Cyber-Sicherheit verfolgt. Gleichzeitig sollte klar kommuniziert werden, dass die Erfüllung der regulatorischen Anforderungen nicht zwangsläufig bedeutet, dass das Unternehmen sicher ist. Daher sollte ein geeigneter Rahmen für die dynamische Struktur des Unternehmens gewählt werden, um die von der Unternehmensleitung und dem Management festgelegte Risikobereitschaft zu erfüllen.

Handlungsempfehlung

Die Unternehmensleitung sollte insbesondere prüfen, ob das Management sowohl einen unternehmensweiten technischen Rahmen als auch einen Managementrahmen geschaffen hat, der eine wirksame Steuerung von Cyber-Risiken ermöglicht:

1. Erstellung eines technischen Rahmens

Moderne digitale Technologiesysteme sind äußerst komplex. Man kann natürlich nicht erwarten, dass Unternehmensleitende alle aktuellen Entwicklungen– z. B. künstliche Intelligenz (KI), Cloud-Konfigurationen, Blockchain – und ihre Auswirkungen auf die Cyber-Sicherheit vollständig verfolgen und verstehen. Das Management sollte die Unternehmensleitung in Kenntnis setzen, dass der passende Cyber-Sicherheitsrahmen verwendet wird, um die für das Unternehmen und seine Abläufe unerlässlichen digitalen Systeme zu schützen.

Obwohl sich einige Unternehmen für ein einziges Cyber-Sicherheits-Framework entscheiden, ist es wahrscheinlicher, dass Unternehmen und Organisationen spezifische Aspekte verschiedener Frameworks auswählen und diese an ihre individuellen Geschäftsanforderungen anpassen.

Bislang konnte noch keinem Rahmenwerk empirisch nachgewiesen werden, dass es aus der Sicherheitsperspektive überlegen ist (was möglicherweise auf die enorme Varianz der Cyber-Angriffsmethoden zurückzuführen ist). Es werden jedoch zunehmend Tools entwickelt, die sich an verschiedenen Rahmenwerken orientieren und es dem Management ermöglichen, das Sicherheitsmanagement der ausgewählten Systeme zu bestimmen und in einigen Fällen zu quantifizieren.

1.1. EU-Normen

Die EU hat Verordnungen und Richtlinien erlassen, die sich direkt auf die Cyber-Sicherheitspraktiken von Unternehmen auswirken. Zwei der Verordnungen haben besonders große Auswirkungen auf die Geschäftstätigkeit und die Praxis von Unternehmen.

1. Die Datenschutz-Grundverordnung (DSGVO), die am 25. Mai 2018 in Kraft getreten ist, sieht eine Harmonisierung der Datenschutzbestimmungen in der gesamten EU vor. Sie erweitert den Geltungsbereich des EU-Datenschutzrechts auf alle ausländischen Unternehmen, die Daten von in der EU ansässigen Personen verarbeiten.

2. Die Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) setzt Cyber-Standards für Unternehmen durch, die Teil der europäischen und nationalen kritischen Infrastrukturen sind. Einige dieser Vorschriften sind oder werden in deutsches Recht übersetzt, bevor sie in Kraft treten. Diese Vorschriften gelten nicht nur für Unternehmen, die in europäischem Besitz sind, sondern auch für ausländische Unternehmen, die in Europa tätig sind. Dies gilt auch für europäische Unternehmen, die zum Beispiel in den USA oder China tätig sind.

1.2. IT- Grundschutz

Mit dem IT-Grundschutz[25] stellt das BSI ein umfassendes Rahmenwerk zur Verfügung, das es Behörden und Unternehmen ermöglicht, ein angemessenes Sicherheitsniveau für alle Arten von Informationen einer Organisation zu erreichen. Der IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz.

Durch die ordnungsgemäße Anwendung bewährter technischer, organisatorischer, personeller und infrastruktureller Schutzmaßnahmen können Organisationen ein Sicherheitsniveau erreichen, das geeignet und ausreichend ist, um geschäftsbezogene Informationen mit normalen Schutzanforderungen zu schützen.

Auch bei IT-Systemen und -Anwendungen, die ein hohes Schutzniveau erfordern, stellt der IT-Grundschutz Maßnahmen zur Verfügung. Der IT-Grundschutz ist kompatibel zur ISO/IEC 27001.

Die entsprechenden BSI-Standards enthalten Empfehlungen zu Methoden, Prozessen, Verfahren, Ansätzen sowie Maßnahmen zu den verschiedenen Aspekten der Informationssicherheit. Die aktuellen Versionen der BSI-Standards (200-1, 200-2 und 200-3) wurden im Oktober 2017 veröffentlicht.

Als Ergänzung zu den BSI-Standards beschreibt das IT-Grundschutz-Kompendium spezifische Anforderungen in Form von Modulen (IT-Grundschutz-Bausteinen) zu verschiedenen Aspekten der Informationssicherheit wie Anwendungen, industrielle Sicherheit oder

[25] Ausführliche Informationen zum IT-Grundschutz finden Sie auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik.

Informationssicherheits-Managementsysteme. Das IT-Grundschutz-Kompendium wird jedes Jahr zum 01.02. aktualisiert.

Aufsichtsratsmitglieder sollten die Erwartung äußern, dass das Management die BSI-Standards bei der Entwicklung der Cyber-Risikoabwehr- und Reaktionspläne des Unternehmens berücksichtigt hat. Auf diese Weise stellen sie sicher, dass ihr Unternehmen ein Fundament für die Cyber-Sicherheit schafft. Die Verwendung der BSI-Standards bedeutet für ein Unternehmen keine absolute Cyber-Sicherheit, ebenso wie die Einhaltung von Rahmenbedingungen oder Vorschriften nicht gleichbedeutend mit absoluter Cyber-Sicherheit ist.

Die Erstellung einer Cyber-Sicherheits-Risikoanalyse hilft Unternehmen jedoch dabei, herauszufinden, wo ihr Ausgangspunkt für Cyber-Sicherheit liegen sollte, wie Cyber-Sicherheit ihren speziellen Geschäftsanforderungen zugutekommen kann und in welchen Bereichen Verbesserungen erforderlich sind.

Die Unternehmensleitung muss verstehen, dass die Umsetzung eines Rahmens keine einmalige Angelegenheit ist - sie erfordert eine kontinuierliche Überwachung, Bewertung und Anwendung der Standards, um auf ein sich veränderndes Bedrohungsumfeld reagieren zu können.

1.3. Zusätzliche Rahmenwerke

Verschiedene technische Frameworks können kombiniert werden, um die von der Unternehmensleitung festgelegten Anforderungen zu erfüllen. Es gibt eine Vielzahl verschiedener Frameworks, aus denen Unternehmen auswählen können. Im Folgenden werden die am häufigsten verwendeten technischen Frameworks für das Management beschrieben. Diese Rahmenwerke dienen als Beispiele und sind nicht verbindlich:

- Das Rahmenwerk für Cyber-Sicherheit des National Institute of Standards and Technology (NIST), das aus „Standards, Richtlinien und bewährten Verfahren zur Verwaltung von Risiken im Zusammenhang mit der Cyber-Sicherheit“ besteht.[26] Der „Kern“ des NIST-Rahmenwerks für Cyber-Sicherheit umfasst fünf Schlüsselfunktionen: identifizieren, schützen, erkennen, reagieren und wiederherstellen.[27] Das Rahmenwerk wird sowohl in einem 55-seitigen PDF-Dokument[28] als auch in einer Excel-Tabelle, die mehr als hundert Sicherheitsempfehlungen auflistet, präsentiert.[29]

- Die Internationale Organisation für Normung (ISO) hat die ISO/IEC 27000-Normen für Informationssicherheit entwickelt. Die ISO erklärt, dass „die Verwendung dieser Normenfamilie Ihrer Organisation helfen wird, die Sicherheit von Vermögenswerten wie Finanzdaten, geistiges Eigentum, Daten oder Informationen, die Ihnen von Dritten anvertraut wurden, zu verwalten“.[30]

- Die „CIS-Kontrollen“ des Center for Internet Security enthalten eine Liste von 20 verschiedenen Sicherheitskontrollen für Unternehmen, die als „basal“, „grundlegend“ oder „organisatorisch“ eingestuft werden.[31] Diese Kontrollen reichen von der Erstellung eines Inventars von Hardware- und Softwarebeständen bis hin zu Penetrationstests und Red-Team-Übungen.[32]

- Die Payment Card Industry (PCI)-Datensicherheitsstandards legen „betriebliche und technische Anforderungen für Organisationen fest, die Zahlungstransaktionen akzeptieren oder verarbeiten, sowie für Softwareentwickler und Hersteller von Anwendungen und Geräten, die bei diesen Transaktionen verwendet werden.“[33]

2. Erstellung eines Managementrahmens

Im Einklang mit dem in Prinzip 1 dargelegten Verständnis, muss Cyber-Sicherheit unternehmensweit organisiert werden. Die Verantwortung für die Ausgestaltung müssen die entsprechenden unterschiedlichen Bereiche der Organisation übernehmen. Sie werden für ihren

[26] Weitere Informationen zum Cybersecurity Framework finden Sie auf der Webseite des „National Institute of Standards and Technology“.
[27] National Institute of Standards and Technology. (16. April 2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Online: NIST.
[28] Ebd.
[29] National Institute of Standards and Technology. (16. April 2022). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (Excel). Online: NIST.
[30] Weitere Informationen zum ISO/IEC 27001 Information Security Management finden Sie auf der Website der Internationalen Organisation für Normung.
[31] Weitere Informationen über „Die 20 CIS-Kontrollen und Ressourcen“ finden Sie auf der Webseite des “Center for Internet Security”.
[32] Ebd.
[33] Weitere Informationen zum „Aufrechterhaltung der Zahlungssicherheit“ finden Sie auf der Webseite des „PCI Security Standards Council“.

Beitrag zu einem effektiven unternehmensweiten Programm zur Rechenschaft gezogen.

Ein unternehmensweiter Ansatz bedeutet, dass alle Beteiligten an einem Strang ziehen müssen, um die Cyber-Sicherheit unternehmensweit zu verwalten - im Gegensatz zu verschiedenen Systemen in verschiedenen Teilen des Unternehmens.

Daraus ergibt sich, dass die besten Erfolgschancen eines Unternehmens darin bestehen, so viel wie möglich zu zentralisieren. Dies hat organisatorische, finanzielle und betriebliche Auswirkungen. Organisatorisch gesehen sind die Chancen, dass alle Geschäftsbereiche gleichermaßen gut funktionieren, gering, wenn die Sicherheit von den einzelnen Geschäftsbereichen oder geografischen Regionen in einem losen Verbund betrieben wird. Aus finanzieller Sicht ist eine zentral geführte Sicherheitsfunktion weniger kostspielig. Doppelarbeit wird reduziert, und Sie haben mehr Einfluss auf die Anbieter. Aus betrieblicher Sicht bedeutet die Überwachung von einem einzigen Standort aus, dass alle potenzielle Vorfälle nach Prioritäten geordnet werden können und darauf reagiert werden kann.

Es gibt kein Modell, das perfekt auf alle Organisationen anwendbar ist. Ein funktionsübergreifender Ansatz mit mehreren Interessengruppen ist aber mit Sicherheit etwas, das die Unternehmensleitung in Betracht ziehen sollte. Wir sind uns bewusst, dass Organisationen ihren Ansatz auf ihre Bedürfnisse zuschneiden wollen, und bieten zwei verschiedene Modelle an, die als Ausgangspunkt dienen können.

2.1. Das ISA-ANSI Rahmenwerk

Eines der ersten Multistakeholder-Modelle wurde von der Internet Security Alliance (ISA) und dem American National Standards Institute (ANSI) in ihrer gemeinsamen Veröffentlichung von 2008, *The Financial Management of Cyber Risk: 50 Questions Every CFO Should Ask*, entwickelt.

Dieses grundlegende Modell betont nicht nur, dass mehrere Interessengruppen beteiligt sein sollten, sondern plädiert auch für eine bestimmte Führungsperson - nicht aus der IT-Abteilung -, die über organisationsübergreifende Befugnisse verfügt. Im Gegensatz zum traditionellen Modell, bei dem Cyber-Sicherheit in das IT-Budget integriert wird, wird außerdem ein separates Budget für Cyber-Sicherheit befürwortet.

Das ISA-ANSI-Rahmenwerk sieht die folgenden sieben Schritte vor[34]:

1. Legen Sie abteilungsübergreifend die Verantwortung für Cyber-Risiken fest. Leitende Angestellte mit abteilungsübergreifenden Befugnissen, z. B. der Chief Financial Officer, Chief Risk Officer oder Chief Operating Officer (nicht der Chief Information Officer), sollten das Team leiten.

2. Ernennen Sie ein organisationsübergreifendes Cyber-Risikomanagement-Team. Alle wichtigen Abteilungen müssen vertreten sein, einschließlich der Leitenden der Geschäftsbereiche, der Rechtsabteilung, der Innenrevision und der Compliance, der Finanzabteilung, der Personalabteilung, der IT-Abteilung (einschließlich der Informationssicherheit) und des Risikomanagements.

3. Das Cyber-Risiko-Team muss eine vorausschauende, unternehmensweite Risikobewertung durchführen und dabei einen systematischen Rahmen verwenden, der die Komplexität von Cyber-Risiken berücksichtigt - einschließlich, aber nicht beschränkt auf die Einhaltung gesetzlicher Vorschriften.

4. Seien Sie sich bewusst, dass die Vorschriften zur Cyber-Sicherheit von Staat zu Staat sehr unterschiedlich sind. Wie in Prinzip 2 erwähnt, sollte das Management genug Ressourcen bereitstellen, um die für das Unternehmen geltenden aktuellen Standards und Anforderungen zu identifizieren und zu berücksichtigen. Dies ist auch vor dem Hintergrund wichtig, dass einige Staaten den Umfang der staatlichen Regulierung im Bereich der Cyber-Sicherheit ausweiten.

5. Verfolgen Sie bei der Erstellung von Berichten an die Unternehmensleitung einen kooperativen Ansatz. Von Führungskräften sollte erwartet werden, dass sie die Auswirkungen von Cyber-Bedrohungen auf das Geschäft und die damit verbundenen Risikomanagement-Bemühungen überwachen und darüber berichten. Die Bewertung der Effektivität des Cyber-Risiko-Managements und der Cyber-Resilienz des

[34] Angepasst von Internet Security Alliance und American National Standards Institute (2010). *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*. Washington, DC: ANSI. Siehe auch: Internet Security Alliance (2013). *Sophisticated Management of Cyber Risk*. Arlington, VA: ISA.

Unternehmens sollte im Rahmen vierteljährlicher interner Audits und anderer Leistungsüberprüfungen durchgeführt werden.

6. Entwickeln und verabschieden Sie einen unternehmensweite Strategie für das Management von Cyber-Risiken und eine interne Kommunikationsstrategie für alle Abteilungen und Geschäftsbereiche. Auch wenn die Cyber-Sicherheit natürlich eine wesentliche IT-Komponente hat, müssen alle Beteiligten in die Entwicklung des Unternehmensplans einbezogen werden und sollten das Gefühl haben, dass sie ihn mittragen. Die Überprüfung des Plans sollte routinemäßig erfolgen.

7. Entwickeln und verabschieden Sie ein umfassendes Cyber-Risiko-Budget mit ausreichenden Ressourcen, um den Bedürfnissen und der Risikobereitschaft des Unternehmens gerecht zu werden. Bei der Entscheidung über die Ressourcen sollte der gravierende Mangel an erfahrenen Cyber-Sicherheitsfachkräften berücksichtigt werden, und es sollte ermittelt werden, welche Anforderungen intern erfüllt werden können und welche an Dritte ausgelagert werden können oder sollten. Da Cyber-Sicherheit mehr ist als IT-Sicherheit, sollte das Budget für Cyber-Sicherheit nicht ausschließlich an eine Abteilung gebunden sein: Beispiele sind Zuweisungen in Bereichen wie Mitarbeitendenschulung, Nachverfolgung rechtlicher Vorschriften, Öffentlichkeitsarbeit, Produktentwicklung und Lieferantenmanagement.

2.2. Das „Three Lines of Defense"-Modell

In den letzten Jahren hat sich ein zweites konzeptionelles Modell herausgebildet, das ursprünglich aus dem Finanzdienstleistungssektor stammt, aber zunehmend von führenden Organisationen in verschiedenen Sektoren übernommen wird. Dieses „Three Lines of Defense"-Modell legt den Schwerpunkt auf mehrere unabhängige Vorgänge innerhalb der Organisation, die unterschiedliche und zunehmende Rollen bei der Bewertung und Kontrolle des Cyber-Risiko-Managements spielen.

Das Modell lässt sich folgendermaßen zusammenfassen:

- **Linie 1:** Wird durch das Unternehmen betrieben, hier ist das Risikokonzept verortet und werden die wichtigen Schritte implementiert.
- **Linie 2:** Hier werden die Richtlinien festgelegt und der Rahmen für das Risikomanagement definiert. Diese Linie prüft und überwacht die erste Linie und ist für die Bewertung der Risikoexposition verantwortlich, damit die Unternehmensleitung die Risikobereitschaft festlegen kann.
- **Linie 3:** In der Regel ist die Innenrevision für die unabhängige Bewertung der ersten und zweiten Linie zuständig.

Die Rollen für die einzelnen Verteidigungsebenen können auf diese Weise weiter detailliert werden:

Linie 1:

- Gründliche Prüfung der Arbeit von Linie 1 - tut das Unternehmen genug? Jeder Geschäftszweig definiert das Cyber-Risiko, dem er ausgesetzt ist, und bindet Cyber-Risiken und deren Bewertung in die Prozesse für Risiko, Betrug, Krisenmanagement und Widerstandsfähigkeit ein.
- Die Geschäftsbereiche müssen bestehende und künftige Risiken und Schwachstellen aktiv überwachen. Sie müssen beurteilen, welche Auswirkungen Cyber-Risiken auf die Einführung neuer Technologien, Kundenbeziehungen und Geschäftsstrategien haben.

Linie 2:

- Linie 2 sollte als separate, unabhängige Funktion eingerichtet werden. Linie 2 verwaltet die Cyber-Risikobereitschaft des Unternehmens und den Rahmen für das Risikomanagement innerhalb des Gesamtunternehmensrisikos. Linie 2 prüft und überwacht die erste Linie, legt fest, wie Cyber-Risiken angemessen zu messen sind, und integriert die Ergebnisse in eine Risikotoleranzerklärung für das Unternehmen.
- Der Schwerpunkt der ersten und zweiten Linie muss auf einem effektiven Risikomanagement liegen, nicht auf der Einhaltung von Vorschriften, obwohl die Einhaltung von Vorschriften in diese Linien integriert werden kann.

Linie 3:

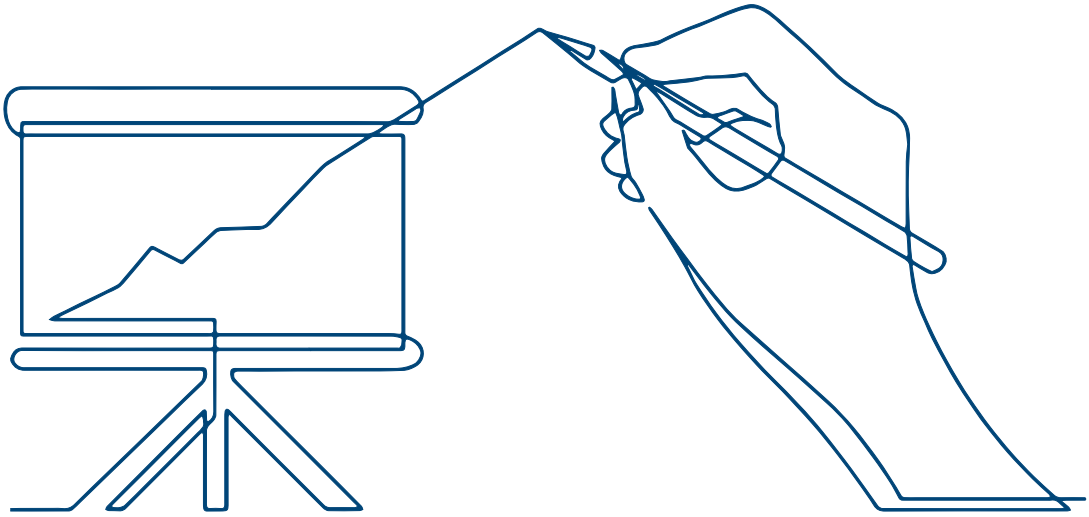
- Linie 3 bietet eine unabhängige, objektive Bewertung der Unternehmensprozesse und -kontrollen in den Linien 1 und 2 mit Schwerpunkt auf betrieblicher Wirksamkeit und Effizienz. Traditionell hat sich die Innenrevision bei ihren Prüfungen auf technische IT-Kontrollen konzentriert, doch wird sie ihren Aufgabenbereich erweitern müssen, um zu beurteilen, ob die Cyber-Sicherheit als Unternehmensrisiko wirksam gehandhabt wird.

- Die Innenrevision führt Prozess- und Kontrollbewertungen durch, validiert die technologische Infrastruktur, überprüft die Kontrollen zur Minderung von Risiken Dritter, führt unabhängige Penetrationstests durch und hält sich über neue Bedrohungen auf dem Laufenden.

2.3. „Best Practice“ im Einklang mit dem unternehmensweiten Modell für Cyber-Sicherheit

Eine detailliertere Erläuterung der Rollen und Verantwortlichkeiten für zahlreiche Unternehmensbereiche, die mit dem unternehmensweiten Cyber-Risiko-Organisationsmodell übereinstimmen, findet sich im Begleitdokument „Cyber Risk Oversight Handbook Cybersecurity for Business“ (Kogan Page 2022). Dieses Buch basiert auf den in diesem Handbuch dargelegten Grundsätzen für das Management von Cyber-Risiken durch die Unternehmensleitung und definiert bewährte Verfahren, die mit diesem aktualisierten Ansatz vereinbar sind. Das Handbuch behandelt “Best Practices” für die Personalverwaltung, Lieferketten, Rechtliches, Vorfallbehandlung, Audit und technischer Betrieb im Einklang mit einer unternehmensweiten Cyber-Risikobewertungsmethode.[35]

[35] Clinton, L. (2022). *Cybersecurity for Business: Organization-wide Strategies To Ensure Cyber Risk is NOT Just an “IT” Issue*. London, New York, New Delhi: Kogan Page.



PRINZIP 5

Risikoanalyse erstellen sowie Definition von Risikobereitschaft in Abhängigkeit von Geschäftszielen und -strategien formulieren

Im Austausch zwischen Unternehmensleitung und Management über Cyber-Sicherheit sollte die Identifizierung und Quantifizierung der finanziellen Kosten in Bezug auf Cyber-Risiken diskutiert werden. Insbesondere sollte die Frage besprochen werden, welche Risiken akzeptiert, gemindert oder übertragen werden sollen, z. B. durch eine Versicherung, sowie spezifische Pläne, die mit jedem Ansatz verbunden sind.

Zur Umsetzung dieses Prinzips siehe:

- **Tool D:** „Reaktion auf Vorfälle“
- **Tool E:** “Metriken zur Cyber-Sicherheit für die Unternehmensleitung“

Hintergrund

Hundertprozentige Cyber-Sicherheit ist ein unrealistisches Ziel. Das Verständnis und das Management der finanziellen Gefährdung durch Cyber-Risiken ist jedoch eine wichtige Komponente der Risikoüberwachung durch die Unternehmensleitung. Das Management von Cyber-Risiken ist - wie bei allen Risiken im Allgemeinen - ein Kontinuum und kein Endzustand. Über die bestehenden Sicherheitsinitiativen und Compliance-Diskussionen hinaus wird es immer wichtiger, Cyber-Risiken in wirtschaftlicher Hinsicht zu verstehen, wenn es um die Überwachung von Cyber-Risiken in Unternehmen geht.

Die Unternehmensleitung muss verstehen, wie das Management die Wirksamkeit der Kontrollen und Verfahren des Unternehmens ermittelt hat, um das Cyber-Risiko auf ein akzeptables Niveau zu verringern. Das Management muss in der Lage sein, das Cyber-Risiko aus einer wirtschaftlichen Perspektive zu kommunizieren, da die Unternehmensleitung seine Entscheidungen auf dieser Grundlage trifft. Eine solche Quantifizierung eines effektiven Cyber-Risiko-Managements ermöglicht es dem Unternehmen, risikobasierte Entscheidungen über seine Strategie und damit über die Zuteilung von Ressourcen zu treffen (siehe untenstehenden Infokasten „Definition der Risikobereitschaft“).

Herkömmliche Risikobewertungsansätze hatten Schwierigkeiten, diese Anforderungen zu erfüllen. In der Vergangenheit wurden bei Cyber-Risikobewertungen meist lange Checklisten mit hochtechnischen Informationen oder Kontrollanforderungen, mit oft über 500 Punkten, erstellt.

Bei diesen Methoden handelte es sich in der Vergangenheit um qualitative Bewertungen, bei denen Cyber-Risiken nicht nach wirtschaftlichen Gesichtspunkten beurteilt wurden.[36] Die quantitativen wirtschaftlichen Bewertungen von Cyber-Risiken sind jedoch so weit ausgereift, dass Cyber-Risiken jetzt quantitativ bewertet werden können. So wie andere Disziplinen gravierende Risiken, wie Markt-, Kredit-, Versicherungs- und strategische Risiken finanziell modellieren, können Cyber-Risiken nun quantitativ modelliert werden, um die Leistung des Risikomanagements zu verbessern.

Häufig werden die Ergebnisse der Bewertung von Cyber-Risiken als „kritisch", „hoch", „mittel" usw. angegeben. Diese Art der Einstufung liefert zwar ein Maß für die Größenordnung (ordinale Messung), hilft den Entscheidungsträgern aber nicht dabei, verschiedene Cyber-Risiken zu vergleichen oder Cyber-Risiken mit anderen Arten von Risiken zu vergleichen, denen das Unternehmen ausgesetzt ist.

Definition der Risikobereitschaft

Die Risikobereitschaft ist die Höhe des quantifizierbaren Risikos, das eine Organisation bei der Verfolgung ihrer strategischen Ziele zu akzeptieren bereit ist. Sie sollte also durch Messung das Risikoniveau festlegen, ab dem geeignete Maßnahmen erforderlich sind, um das Risiko auf ein akzeptables Niveau zu reduzieren. Wenn diese richtig definiert und kommuniziert wird, steuert sie das Verhalten, indem es die Grenzen für die Führung des Unternehmens und die Nutzung von Chancen festlegt.

Bei der Erörterung der Risikobereitschaft sollten die folgenden Fragen angesprochen werden:

- Unternehmenswerte - Welche Risiken werden wir nicht akzeptieren?
- Strategie - Welches sind die Risiken, die wir eingehen müssen?
- Stakeholder - Welche Risiken sind die Stakeholder bereit zu tragen, und in welchem Umfang?
- Kapazität - Welche Ressourcen sind für die Bewältigung dieser Risiken erforderlich?
- Finanzen - Sind wir in der Lage, die Wirksamkeit unseres Risikomanagements angemessen zu quantifizieren und unsere Ausgaben für Risikokontrollen zu harmonisieren?
- Messbarkeit - Können wir messen und Berichte erstellen, um sicherzustellen, dass eine ordnungsgemäße Überwachung, Trendbestimmung und Kommunikation erfolgt?

Quelle: PwC (2014)., Board oversight of risk: Defining risk appetite in plain English. *(New York, PwC, S. 3.)*

Handlungsempfehlung

Da die Unternehmen den Wert der Quantifizierung von Cyber-Risiken erkannt haben, wird viel daran gearbeitet, die quantitative Analyse weiterzuentwickeln.

Im Rahmen dieses Ansatzes können Unternehmen ihre Werte und Risiken ermitteln und auf dieser Basis eine Lösung anstreben. Dies sollte ein zirkulärer und fortlaufender Prozess sein, der auf kontinuierliche Verbesserung abzielt. Bei diesem Ansatz sollte neben der Haftung auch die Wirtschaftlichkeit des Risikos in den Vordergrund gestellt werden.

1. Sicherstellung des Übergangs von der Cyber-Sicherheitsverteidigung zum umfassenden Cyber-Risikomanagement

Die Unternehmensleitung sollte dem Management die richtigen Fragen stellen, um zu beurteilen, ob es eine klare und umfassende Bewertung der Cyber-Risiken durchführt. Auf einer konzeptionellen Ebene sollte die Unternehmensleitung erwägen, u.a. folgende Fragen zu stellen:

[36] Jones J. (2019). Understanding Cyber Risk Quantification: A Buyer's Guide. Online: Fair Institute.

- **Welche und wie viele Daten sind wir bereit zu speichern, zu verlieren, weiterzugeben oder deren Kompromittierung zuzulassen.** In diesem Zusammenhang ist der entscheidende Faktor eine zuvor definierte Unterscheidung zwischen unternehmenskritischen Daten und anderen wichtigen Daten.

- **Wie lange können wir uns den Ausfall der Geschäftsprozesse leisten?** Neben dem Datenverlust muss auch die Unterbrechung des Geschäftsbetriebs berücksichtigt werden.

- **Wie sollten die Investitionen zur Minderung von Cyber-Risiken auf grundlegende und erweiterte Schutzmaßnahmen verteilt werden?** Für Anlagen mit geringerer Priorität sollten Unternehmen in Betracht ziehen, ein höheres Sicherheitsrisiko in Kauf zu nehmen, als für Anlagen mit höherer Priorität, da die Kosten für die Verteidigung wahrscheinlich den Nutzen übersteigen. Die Unternehmensleitung sollte das Management dazu ermutigen, die Ausgaben des Unternehmens für Cyber-Sicherheit unter dem Gesichtspunkt der Investitionsrendite (ROI) und der Wahrscheinlichkeit eines Angriffs zu betrachten. Außerdem sollten sie die Eintrittswahrscheinlichkeit und den ROI regelmäßig neu bewerten, da sich die Kosten für den Schutz, die Prioritäten des Unternehmens und das Ausmaß der Bedrohung im Laufe der Zeit ändern werden.

- **Welche Möglichkeiten gibt es, um bestimmte Cyber-Risiken zu mindern?** Unternehmen aller Branchen und Größen haben Zugang zu umfassenden Lösungen, die dabei helfen können, einen Teil des Cyber-Risikos zu mindern, indem sie die Wahrscheinlichkeit eines Angriffs direkt reduzieren. Darüber hinaus sollten Unternehmen die Einbeziehung von Präventivmaßnahmen, wie z. B. die Überprüfung von Cyber-Sicherheitsrahmen und Governance-Praktiken, Mitarbeiterschulungen, IT-Sicherheit, Vorfalldienstleister und beratende Sicherheitsdienste prüfen.

- **Welche Möglichkeiten gibt es, um uns bei der Übertragung bestimmter Cyber-Risiken zu unterstützen?** Eine Cyber-Versicherung kann eine praktische Option sein, wenn die Risikominderung, die sie im Vergleich zu den Kosten erzielt, günstiger ist, als die Risikominderung, die andere Maßnahmen bieten würden. Bei der Auswahl eines Cyber-Versicherungspartners sollte ein Unternehmen unbedingt die Bedürfnisse des Unternehmens berücksichtigen. Versicherungen führen häufig eingehende Überprüfungen der Cyber-Sicherheitsstrukturen von Unternehmen durch. Dies kann Unternehmen dabei helfen, ihre Stärken und Schwächen im Bereich der Cyber-Sicherheit zu verstehen und einen möglichen Weg zur Verbesserung ihrer Cyber-Sicherheitsreife aufzuzeigen. Viele Versicherer bieten in Zusammenarbeit mit Technologieunternehmen, Anwaltskanzleien, PR-Firmen und anderen auch Zugang zu den oben genannten Präventivmaßnahmen.

- **Wie sollten die Auswirkungen von Cyber-Sicherheitsvorfällen bewertet werden?** Die Durchführung einer angemessenen Folgenabschätzung kann angesichts der Vielzahl der beteiligten Faktoren eine Herausforderung sein. Um ein Beispiel zu nennen: Die Veröffentlichung von Cyber-Sicherheitsvorfällen kann den Risikobewertungsprozess erheblich erschweren. Die Beteiligten - Mitarbeitende, Kunden, Lieferanten, Investoren und Investorinnen, die Presse, die Öffentlichkeit und Regierungsbehörden - sehen möglicherweise kaum einen Unterschied zwischen einer vergleichsweise kleinen und einer großen und gefährlichen Sicherheitsverletzung. Infolgedessen korrelieren der Reputationsschaden und die damit verbundenen Auswirkungen (einschließlich der Reaktionen von Medien, Investoren und anderen wichtigen Interessengruppen) möglicherweise nicht mit der Größe oder Schwere des Ereignisses. Die Unternehmensleitung sollte sich vergewissern, dass das Management diese Auswirkungen bei der Festlegung der Prioritäten für das Cyber-Risiko-Management sorgfältig durchdacht hat.

2. Grundlegende Methode zur wirtschaftlichen Bewertung von Cyber-Risiken

Das Management kann systematische Methoden anwenden, um die Gefährdung durch Cyber-Risiken zu ermitteln. Wirksame Bewertungen umfassen technische Analysen, gehen aber darüber hinaus und beziehen auch andere Aspekte des Unternehmens mit ein. Zu den wichtigsten Schritten auf dem Weg zu einer fortschrittlicheren Bewertung und Management von Cyber-Risiken können die folgenden gehören:

- Das Management sollte sich um die am besten verfügbaren Daten bemühen, um mögliche Angriffsszenarien einschätzen zu können.
- Das Management sollte sich auf Szenarien konzentrieren, die wahrscheinlich sind und zu einem erwarteten Verlust führen würden, der bedeutend genug ist, um für das Unternehmen von Relevanz zu sein.
- Das Management sollte den besten, den schlimmsten und den wahrscheinlichsten Fall eines Angriffs berechnen und ermitteln, welches Maß an Verlust akzeptabel ist (Risikobereitschaft).
- Das Management sollte die Investitionen bestimmen, die erforderlich sind, um das Risiko auf ein akzeptables Niveau zu reduzieren oder zu übertragen.
- Optional: Durchführung mehrerer Szenarien mit Hilfe von Methoden wie Monte-Carlo-Simulationen zur genaueren Bestimmung des Risikos und der Kosten für die Schadensbegrenzung in verschiedenen Szenarien.

PRINZIP 6

Unternehmensweite Zusammenarbeit und den Austausch von Best-Practice fördern

Die Unternehmensleitung sollte die Zusammenarbeit innerhalb ihrer Branche und mit öffentlichen und privaten Akteuren fördern, um sicherzustellen, dass jede Institution die Resilienz Aller unterstützt.

Zur Umsetzung dieses Prinzips siehe:

- **Tool F:** „Im regelmäßigen Austausch mit CISO/ IT-Sicherheitsbeauftragten“

Hintergrund

Zu einer wirksamen Cyber-Risikostrategie gehört die Verbesserung der Cyber-Resilienz von Branchen und Sektoren. Die starke Vernetzung moderner Organisationen birgt das Risiko, dass sich Ausfälle über ein einzelnes Unternehmen hinaus auf ganze Branchen, Sektoren und Volkswirtschaften auswirken.

Im Jahr 2020 wurde weltweit Malware über ein von SolarWinds, einem US-amerikanischen Anbieter von Technologie-Infrastrukturen, installiertes Update in weite Teile der US-Bundesregierung, einschließlich des US-Verteidigungsministeriums, sowie in 425 Unternehmen der Fortune-500-Liste der USA und in Systeme anderer, noch nicht genannter Kunden, eingeschleust.

Im März 2021 veröffentlichte Microsoft ein außerplanmäßiges Sicherheitsupdate für seinen weit verbreiteten Groupware- und E-Mail-Server Exchange. Zum Zeitpunkt des Bekanntwerdens der Schwachstellen waren rund 98 Prozent der untersuchten Systeme in Deutschland gefährdet. Als Reaktion auf diese Bedrohung hob das BSI die Bedrohungsstufe auf „geschäftskritisch“ – die zweithöchste Stufe - an, um sowohl die schiere Anzahl der angreifbaren Server als auch die leichte Verfügbarkeit von Exploit-Kits zu berücksichtigen.[37]

Und die Liste geht weiter.

Wie diese Beispiele deutlich zeigen, können Cyber-Risiken überall entlang der Supply Chain – aus dem Netzwerk von Partnern, Lieferanten und Anbietern eines Unternehmens – entstehen. Die Anfälligkeit eines Unternehmens, eines Produkts oder einer Dienstleistung kann sich auch auf Ihr Unternehmen auswirken. Daher reicht es nicht mehr aus, nur die Cyber-Sicherheit des eigenen Unternehmens zu gewährleisten. Erst wenn Unternehmen und Organisationen in Bezug auf Cyber-Sicherheit zusammenarbeiten, kann branchen- und sektorweite Cyber-Resilienz entstehen.

[37] Mehr zu den Exchange-Schwachstellen können Sie u.a. im Podcast der Allianz für Cyber-Sicherheit, „CYBERSNACS“ nachhören.

Handlungsempfehlung

Mit der Erkenntnis, dass nur kollektives Handeln und Partnerschaften die Herausforderung der Cyber-Risiken wirksam bewältigen können, müssen hochrangige strategische Führungskräfte die Zusammenarbeit innerhalb ihrer Branche und mit öffentlichen und privaten Interessengruppen fördern. So kann sichergestellt werden, dass jede Institution die allgemeine Resilienz Aller unterstützt.

Unternehmen zögern vielleicht, Informationen untereinander auszutauschen. Unbestritten können Informationen und Daten oft unklar sein, was die Zusammenführung von Risikobewertungen zu einer großen Herausforderung macht. Ein kollektiver Risiko- und Informationsaustausch ist jedoch unerlässlich, um das Risiko für das gesamte Ökosystem zu verringern. Auch wenn die Rolle der Unternehmensleitung in diesem Bereich begrenzt sein mag, sollten sich die Unternehmensleitenden der kollaborativen Praktiken bewusst sein und sich damit auseinandersetzen. Im Folgenden werden einige wichtige Überlegungen dazu angestellt, wie die Unternehmensleitung bei ihren Entscheidungen im Rahmen der allgemeinen Risikoüberwachung systemische Cyber-Risiken im Auge behalten kann.

Wichtige Überlegungen für die Unternehmensleitung:

- Entwicklung einer 360-Grad-Sicht auf die Risiken und die Widerstandsfähigkeit des Unternehmens, um als sozial verantwortliche Partei in dem breiteren Umfeld, in dem das Unternehmen tätig ist, zu agieren.

- Aufbau von Peer-Netzwerken (beispielsweise in den Erfahrungs- und Expertenkreisen der Allianz für Cyber-Sicherheit), einschließlich anderer Mitglieder von Unternehmensleitungen, zum Austausch bewährter Governance-Praktiken über institutionelle Grenzen hinweg.

- Sicherstellen, dass das Management Pläne für eine effektive Zusammenarbeit, insbesondere mit dem öffentlichen Sektor, zur Verbesserung der Cyber-Resilienz hat.

- Sicherstellen, dass das Management die Risiken berücksichtigt, die sich aus den breiteren Verbindungen der Branche ergeben (z. B. Dritte, Anbieter und Partner).

Förderung der Teilnahme von Führungskräften an Branchengruppen und Plattformen zum Wissens- und Informationsaustausch.

Fazit

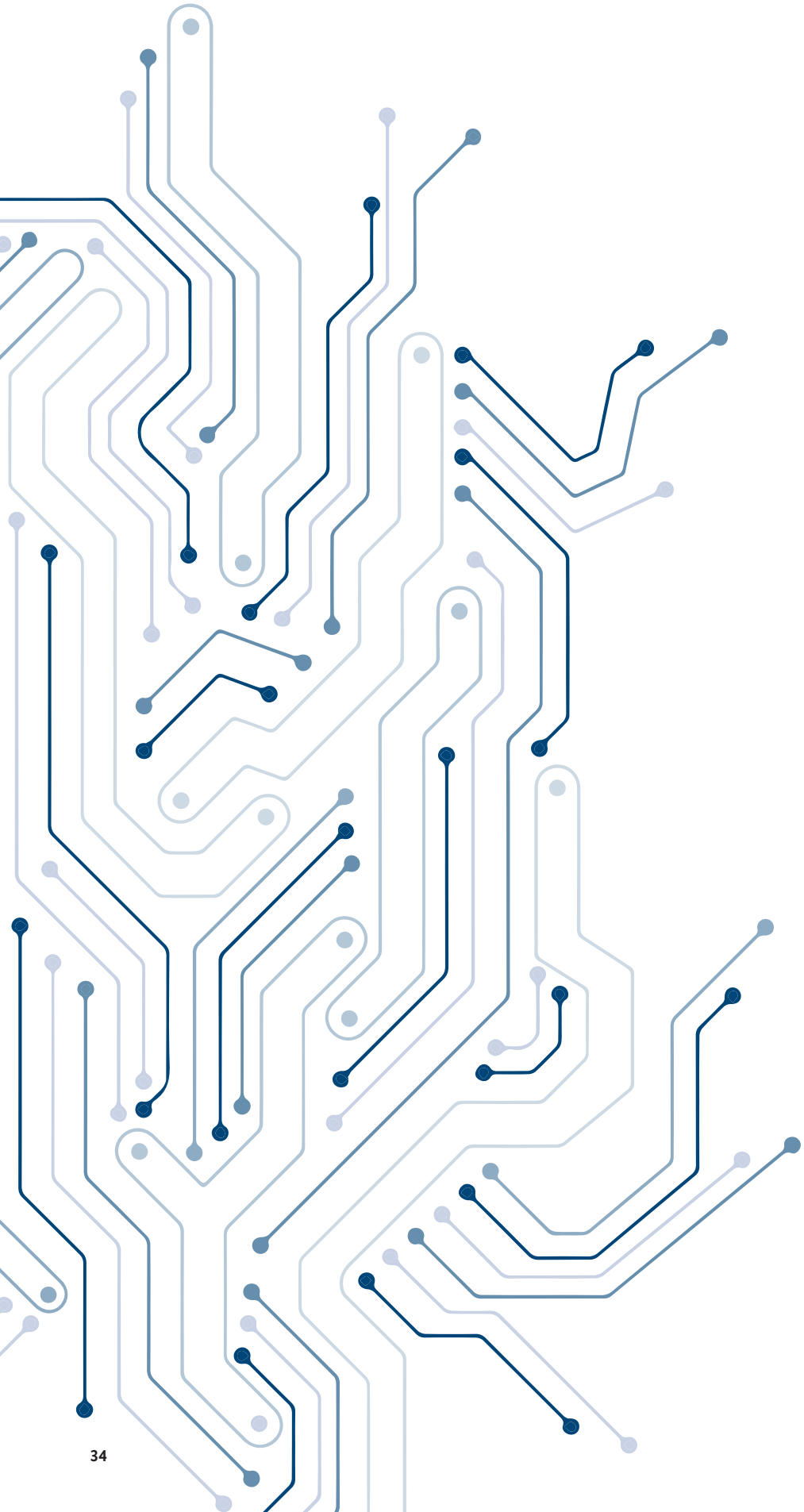
Cyber-Sicherheit ist heutzutage eine ernsthafte Herausforderung für die unternehmensweite Risiko- und Strategieplanung. Aufgrund mehrerer Faktoren ist diese Art von Bedrohung besonders gefährlich: die Komplexität und die Entwicklungsgeschwindigkeit, das Potenzial für erhebliche finanzielle Schäden bzw. Reputationsverlust und die Tatsache, dass ein vollständiger Schutz nicht möglich ist. Angesichts dieser Bedrohungen und trotz drastischer Steigerungen der Ausgaben des privaten Sektors für Cyber-Sicherheit liegt die Wirtschaftlichkeit der Cyber-Sicherheit immer noch zugunsten der Angreifenden. Zusätzlich können viele technologische Innovationen die Anfälligkeit für Cyber-Bedrohungen erhöhen.

Die Unternehmensleitung muss ihre Effektivität im Umgang mit der Cyber-Sicherheit laufend überprüfen, sowohl im Hinblick auf ihre eigene treuhänderische Verantwortung, als auch auf ihre Aufsicht über die Aktivitäten des Managements. Auch wenn die Ansätze der einzelnen Unternehmensleitungen unterschiedlich sein werden, bieten die Prinzipien in diesem Handbuch einen hilfreichen Entwurf und eine zeitgemäße Anleitung.

Unser Ziel: Die Verantwortlichen bei dieser Aufgabe zu unterstützen und Cyber-Sicherheit zur Chefinnen- und Chefsache zu machen. Um dies zu erreichen, ist jedoch ein grundlegendes Verständnis der Risiken im Bereich der Informationssicherheit entscheidend. Nur so können Unternehmensleitungen und Aufsichtsgremien das wirtschaftliche Risiko von Cyber-Sicherheitsvorfällen fundiert einschätzen und über IT-Sicherheitsstrategien entscheiden.

Letztendlich ist „Cyber-Sicherheit ein menschliches Problem“[38]. Die Rolle der Unternehmensleitung besteht darin, ihr Urteilsvermögen einzubringen und dem Management wirksame Leitlinien an die Hand zu geben, um sicherzustellen, dass die Cyber-Sicherheitsstrategie in Anbetracht der strategischen Ziele des Unternehmens und der Realitäten des Geschäftsumfelds, in dem es tätig ist, angemessen konzipiert und ausreichend widerstandsfähig ist.

[38] National Association of Corporate Directors et al. (2021). *Cybersecurity: Boardroom Implications. Washington*, DC: NACD, S. 7.



Impressum

Herausgeber
Allianz für Cyber-Sicherheit
Godesberger Allee 185-189
53175 Bonn

Telefon
+49 (0) 22899 9582-0

Fax
+49 (0) 22899 9582-5400

E-Mail
info@cyber-allianz.de

Internet
www.allianz-fuer-cybersicherheit.de

Stand
Oktober 2022

Texte und Redaktion
Allianz für Cyber-Sicherheit

Bildnachweis
Titel, Rückseite: AdobeStock © Alex; Titel: AdobeStock © Gondex, AdobeStock © derplan13; S. 06, S. 07: BSI; S. 10, S. 12, S. 14, S. 17, S.28, S. 29: AdobeStock © Simple Line; S. 20: AdobeStock © samuii; S. 30: AdobeStock © riz; S. 31: AdobeStock © the8monkey

www.allianz-fuer-cybersicherheit.de
https://isalliance.org/