Mit Unterstützung von:

AIG

Allianz für Cyber-Sicherheit

INTERNET SECURITY ALLIANCE

Management von Cyber-Risiken:

Handbuch für Unternehmensvorstände und Aufsichtsräte

„Cybersecurity ist eines der wichtigsten Themen, mit denen sich ein Unternehmensvorstand und Aufsichtsrat auseinandersetzen muss. Dieses Handbuch bietet einen kohärenten Satz von Prinzipien, die deutsche Vorstände und Aufsichtsräte bei der Betrachtung von Cyber-Risiken befolgen können, sowie eine Reihe von pragmatischen Fragen, die Vorstandsmitglieder in Verbindung mit dem Senior Management verwenden können.“

Arne Schönbohm
Präsident, BSI

VORWORTE VON

Peter Gleason
President and CEO, National Association of Corporate Directors

UND

Larry Clinton
President a CEO, Internet Security Alliance

Basierend auf dem Cyber Risk Oversight Director’s Handbook der National Association of Corporate Directors

Management von Cyber-Risiken:

Handbuch für Unternehmensvorstände und Aufsichtsräte

INTERNET SECURITY ALLIANCE

VON

Larry Clinton

President and CEO, Internet Security Alliance

UND

Stacey Barrack

Senior Director of Policy, Internet Security Alliance

Warum ein Handbuch zur Cyber-Risiko-Aufsicht für Unternehmensvorstände und Aufsichtsräte?

Cyber-Vorfälle sind die am schnellsten wachsende und vielleicht gefährlichste Bedrohung für moderne Unternehmen. Für Vorstände rückt die Bewältigung von Cyber-Risiken zunehmend in den Vordergrund. Aufgrund der jüngsten Bedrohungslage und des sich ständig verändernden Bedrohungscharakters suchen Vorstände jedoch nach einem kohärenten Ansatz, um das Thema auf Vorstandsebene zu behandeln. Als Reaktion darauf haben die Internet Security Alliance (ISA) und die National Association of Corporate Directors (NACD) 2014 das erste *Cyber-Risk Oversight Handbook for Corporate Boards* erstellt. Das Handbuch war sehr erfolgreich darin, Vorstände bei der Bekämpfung von Cyber-Risiken auf globaler Ebene zu unterstützen. Auch PricewaterhouseCoopers verwies in seinem Global Information Security Survey 2016 namentlich auf das Handbuch und bestätigt:

„Die Leitlinien der National Association for Corporate Directors (NACD) raten Vorständen, Cyber-Sicherheitsrisiken und Abwehrbereitschaft mit dem Management zu besprechen und Cyber-Bedrohungen im Kontext der Gesamtrisikotoleranz der Organisation zu betrachten."

„Vorstände und Aufsichtsräte scheinen diesen Empfehlungen zu folgen. In diesem Jahr verzeichneten wir in den meisten Bereichen der Informationssicherheit eine zweistellige Steigerung der Vorstandsbeteiligung. Die Befragten sagten, dass diese stärkere Beteiligung der Vorstände dazu beigetragen hat, die Cyber-Sicherheitspraktiken in vielerlei Hinsicht zu verbessern. Da immer mehr Vorstände an den Diskussionen über das Budget für Cyber-Sicherheit teilnehmen, ist es daher kein Zufall, dass wir einen Anstieg der Sicherheitsausgaben um 24 Prozent feststellen konnten."

„Andere bemerkenswerte Ergebnisse, die von den Befragten genannt werden, sind die Identifizierung von Schlüsselrisiken, die Förderung einer organisatorischen Sicherheitskultur und eine bessere Abstimmung der Cyber-Sicherheit auf das allgemeine Risikomanagement und die Unternehmensziele. Besonders hervorzuheben ist die Tatsache, dass das aktive Interesse der Vorstände die Kommunikation zwischen Führungskräften und Direktoren dahingehend geändert hat, Cyber-Sicherheit als wirtschaftliches Thema zu betrachten." [1]

[1] PricewaterhouseCoopers (PwC), *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016* (PwC, 2015), Web.

Inhaltsverzeichnis

Danksagungen

Wir möchten nachstehenden Experten für ihre Beiträge zur Entwicklung dieses Handbuchs durch Teilnahme an Projektmeetings, Workshops, Telefonkonferenzen und die Bereitstellung von Texten danken.

Das Handbuch der US-Version 2017 wurde auf Grundlage des kollektiven Inputs nach einem Konsensprozess überarbeitet und spiegelt nicht notwendigerweise die Ansichten der aufgeführten Unternehmen und Organisationen wider.

Anhang F wurde von der Allianz für Cyber-Sicherheit (ACS), einer Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI), im Rahmen der Mitwirkung an der Überarbeitung des Handbuchs für den deutschen Markt erstellt.

Vorstand der Internet Security Alliance

* Vorsitzender einer der Arbeitsgruppen

INTERNET SECURITY ALLIANCE **Larry Clinton**
INTERNET SECURITY ALLIANCE **Stacey Barrack**
RAYTHEON **Jeff Brown, Chairman***
USAA **Gary McAlum, First Vice Chairman**
NORTHROP GRUMMAN CORPORATION **JR Williamson, Second Vice Chairman**
AIG **Tracie Grella***
VODAFONE **Richard Spearman***
BNY MELLON **Robert Ife***
ERNST & YOUNG **Andrew Cotton***
CENTER FOR AUDIT QUALITY **Catherine Ide**
BUNGE **Bob Zandoli**
CENTENE **Lou DeSorbo**
SECURE SYSTEMS INNOVATION CORPORATION **John Frazzini**
LEIDOS **Stephen Hull**
GENERAL ELECTRIC **Nasrin Rezai**
LOCKHEED MARTIN **Corporation Jim Connelly**
RSA **Niloofar Howe**
STARBUCKS **Dave Estlick**
UTILIDATA **Ed Hammersla**
SYNCHRONY FINANCIAL **Larry Trittschuh**
DIRECT COMPUTER RESOURCES **Joe Buonomo**
CARNEGIE MELLON UNIVERSITY **Tim McNulty**
NATIONAL ASSOCIATION OF MANUFACTURERS **Brian Raymond**
THOMSON REUTERS **Tim McKnight**

Mitwirkende

AIG **Garin Pace***
AIG **Sebastian Hess**
AIG **Chloe Green**
AIG **Susanne Pauer**
AIG **Mark Camillo**
AIG **Richard Hebblethwaite**
AIG **Nepomuk Loesti**
AIG **Oliver Delvos**
RAYTHEON ANSCHÜTZ **Dirk Sann**
BUNGE **Angelo Micciche**
DLA PIPER **Christian Schoop**
DLA PIPER **Jan Pohle**
DLA PIPER **Jim Halpert**
DLA PIPER **Jan Spittka**
DLA PIPER **Dr. Andreas Meyer-Landrut**
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS **Peter Gleason**
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS **Erin Essenmacher**
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS **Robyn Bew**
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK **Arne Schönbohm**
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK **Roland Hartmann**
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK **Stefan Wunderlich**
BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK **Till Kleinert**
CYBER-SICHERHEITSRAT DEUTSCHLAND **e.V. Philipp v. Saldern**
CYBER-SICHERHEITSRAT DEUTSCHLAND **e.V. Hans-Wilhelm Dünn**
CYBER-SICHERHEITSRAT DEUTSCHLAND **e.V. Florian Till Patzer**
FORMER HEAD OF NATO C&I AGENCY **Koen Gijsbers**
CONNECTING TRUST **Tom Koehler**
CYCLESEC **Sebastian Klipper**
SWISS REINSURANCE COMPANY **Maya Bundt**
HATHAWAY GLOBAL STRATEGIES **Melissa Hathaway**
RICHARD KNOWLTON ASSOCIATES **Richard Knowlton**
GEC RISK ADVISORY **Andrea Bonime-Blanc**
AXIO **Scott Kannry**
BASF **Patrick Fiedler**
COMMERZBANK **Thoralf Reichelt**
DEUTOR CYBER SECURITY SOLUTIONS **Stefanie Frey**
DEUTOR CYBER SECURITY SOLUTIONS **Michael Bartsch**
DEUTSCHE BANK **Osama Jamaleddine**
KEYIDENTITY **Arved Graf von Stackelberg**
KÖBERICH FINANCIAL LINES **Harald Köberich**
MARSH **Göran Weinert**
MARSH **Ute Sauer**
MARSH **Michael Rieger-Goroncy**
VARD **Peter Dehnen**
FIS GLOBAL **Kara Hill**
CLEARSTREAM **Nancy Jansen**
ISABEL GROUP **Cedomir Karlicic**
DAIMLER **Sascha Kazmaier**
ANAPUR **Kruschitz Erwin**

Vielen Dank für die Unterstützung und Teilnahme aller Organisationen, die Experten für diese Initiative zur Verfügung gestellt haben. Ohne die Beiträge dieser Einzelpersonen und ihre kollektive Expertise wäre dieses Endergebnis nicht möglich gewesen. Besonderer Dank gilt in diesem Zusammenhang den Personen, die die verschiedenen Arbeitsgruppensitzungen geleitet und aktiv mitgewirkt haben.

Wir möchten an dieser Stelle ganz besonders der AIG Europe Limited als Projektinitiator und treibende Kraft in der Umsetzung des vorliegenden Handbuchs danken. Eine besondere Würdigung gilt hierbei der außerordentlichen Unterstützung der Workshop-Aktivitäten in Form der Bereitstellung von Veranstaltungsorten, Logistik sowie Marketingaktivitäten. Die Führungsqualitäten von AIG und das Engagement bei Gestaltung des Inhalts, Leitung der Verfahren und genereller Konsensbildung sowie der anschließenden Distribution waren ausschlaggebend für den Erfolg des Endergebnisses dieses Handbuchs.

Unser herzlichster Dank gilt zudem Sebastian Hess, AIG, für die Übersetzung des Handbuchs in die deutsche Sprache.

Ein besonderer Dank gilt auch DLA Piper für ihre juristische Expertise.

Vorwort zu den lokal angepassten Versionen des Handbuchs zur Cyber-Risiko-Aufsicht

PETER GLEASON, PRESIDENT AND CEO, NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Digitale Konnektivität verändert die Art und Weise, wie wir leben und arbeiten. Im Jahr 2017 waren weltweit fast 4 Milliarden Menschen an das Internet angeschlossen.[2] Die grenzüberschreitende Datenübermittlung ist zwischen 2005 und 2016 um das 45-Fache gestiegen und wird in Zukunft noch stärker zunehmen.[3] Im geschäftlichen Bereich haben Datenströme heute weltweit einen größeren Einfluss auf das BIP-Wachstum als der traditionelle Warenhandel,[3] und die neuen Technologien eröffnen großen und kleinen Unternehmen ungeahnte Möglichkeiten.

Doch während der technologische Fortschritt immer stärker spürbar wird, wächst auch die Besorgnis der weltweit führenden Unternehmen über Cyber-Bedrohungen und die damit verbundenen Kosten. In Studien äußern viele Führungskräfte, Regierungschefs und Strafverfolgungsbeamte Unsicherheit darüber, ob ihre Organisationen in der Lage sind, Cyber-Risiken zu managen und darauf zu reagieren, und stellen Fragen darüber, wie sich die digitale Revolution auf die Datensicherheit und den Datenschutz auswirken wird. In der jüngsten Umfrage der National Association of Corporate Directors (NACD) unter Vorstandsmitgliedern börsennotierter Unternehmen sind 58 Prozent der Befragten der Ansicht, dass es für ihren Vorstand etwas oder sehr schwierig ist, Cyber-Risiken effektiv zu überwachen.[4]

Cyber-Sicherheit ist zu einer festen Größe auf der Agenda von Unternehmen auf der ganzen Welt geworden und die Vorstandsmitglieder müssen darauf vorbereitet sein, eine angemessene und wirksame Überwachung von Cyber-Risiken zu gewährleisten. Cyber-Sicherheit als unternehmensweites Strategiethema in den Geschäftskontext zu stellen, ist unerlässlich.

NACD ist die älteste und größte gemeinnützige Bildungsvereinigung der USA für Aufsichtsratsmitglieder. Wir waren stolz darauf, mit der Internet Security Alliance (ISA) bei der Entwicklung des ursprünglichen *NACD Director's Handbook on Cyber-Risk Oversight* 2014 und der aktualisierten Ausgabe 2017 zusammenzuarbeiten. Die Veröffentlichung war Neuland, indem sie eine Reihe von fünf Grundprinzipien für die Überwachung von Cyber-Risiken durch Aufsichtsratsmitglieder aufzeigte, die sich seit langem bewährt haben, auch wenn sich das Umfeld für Cyber-Bedrohungen ständig weiterentwickelt hat.

Die NACD dankt ISA, AIG und dem Bundesamt für Sicherheit in der Informationstechnik dafür, dass sie zur Weiterentwicklung der in diesem Handbuch dargelegten Grundsätze beigetragen und diese in einen praktischen Kontext für Vorstände von Unternehmen in Deutschland gestellt haben.

Peter Gleason
President and CEO, NACD

[2] Steve Morgan, Top 5 cybersecurity facts, figures and statistics for 2018, CSO, 23. Jan. 2018.

[3] James Manyika et al., *Digital globalization: the new era of global flows*, McKinsey Global Institute, 2016.

[4] Ibid.

[5] *NACD 2017–2018 Public Company Governance Survey*, Seite 23.

Vorwort: Cyber-Sicherheit: Ein Thema, das uns alle angeht

LARRY CLINTON, PRESIDENT AND CEO, INTERNET SECURITY ALLIANCE

In den letzten Jahren wurde das Bewusstsein der Öffentlichkeit, darunter auch das von Vorständen und Aufsichtsräten, in Bezug auf Cyber-Risiken geschärft.

Gleichzeitig wurden die Vorstands- und Aufsichtsratsmitglieder von allen Arten von Beratern und so genannten Spezialisten mit verwirrenden, inkonsistenten und sogar widersprüchlichen Vorschlägen für den Umgang mit Cyber-Risiken bombardiert.

Die Cyber-Risiko-Handbücher der ISA sind ein Versuch, Vorstands- und Aufsichtsratsmitgliedern einen einfachen und kohärenten Rahmen für das Verständnis von Cyber-Risiken anzubieten, gekoppelt mit einer Reihe von einfachen Fragen an das Management, um sicherzustellen, dass ihre Organisation ihre individuelle Haltung gegenüber Cyber-Risiken korrekt adressiert.

Unabhängige Untersuchungen zu früheren Ausgaben des *Cyber Risk Oversight Handbook* – fokussiert auf die gleichen Grundprinzipien – haben gezeigt, dass die Anwendung dieser Prinzipien zu einer besseren Budgetierung der Cyber-Sicherheit, einem besseren Cyber-Risiko-Management, einer stärkeren Ausrichtung der Cyber-Sicherheit an den Geschäftszielen und zur Schaffung einer Sicherheitskultur führten.[6]

Dieses Handbuch wurde von fast hundert Cyber-Sicherheitsexperten aus verschiedenen Ländern und Industriezweigen zusammengestellt, die auf freiwilliger Basis zusammenarbeiteten. Niemand wurde dafür bezahlt, einen Beitrag zu leisten, und das Handbuch selbst wird kostenfrei zur Verfügung gestellt. Die Mitwirkenden dieses Handbuchs stellen ihre Beiträge nicht für einen finanziellen Gewinn zur Verfügung. Sie arbeiten zusammen, weil Cyber-Kriminelle uns alle ins Visier nehmen. Politik, Industrie und Privatpersonen stehen in diesem Kampf auf der gleichen Seite. Wir müssen alle zusammenarbeiten.

Wir erwarten, dass es weitere Auflagen dieses Handbuches geben wird. Daher freuen wir uns über Ihr Feedback, da wir alle gemeinsam daran arbeiten, unsere Daten in einem nachhaltig sicheren Cyber-System zu schützen.

Larry Clinton
President and CEO, ISA

[6] PricewaterhouseCoopers (PwC), *Turnaround and Transformation in Cybersecurity: Key Findings from the Global State of Information Security Survey 2016* (PwC, 2015), Web.

Einführung

Die Art, den Wert eines Unternehmens zu berechnen, hat sich in den letzten 25 Jahren signifikant verändert: Betrachtete man früher überwiegend physische Werte, sind heute für die Berechnung nahezu ausschließlich virtuelle Werte ausschlaggebend. Nahezu 90 Prozent des Gesamtwertes der Fortune-500-Unternehmen bestehen heute aus geistigem Eigentum (IP) und anderen immateriellen Vermögenswerten.[7] Mit der rasant wachsenden „Digitalisierung" der Unternehmenswerte ist auch eine entsprechende Digitalisierung der Unternehmensrisiken verbunden. Dementsprechend sind politische Entscheidungsträger, Regulierungsbehörden, Aktionäre und die Öffentlichkeit mehr denn je für die Risiken der Cyber-Sicherheit von Unternehmen sensibilisiert. Der Verlust von geistigem Eigentum und Handelsalgorithmen, vernichtete oder manipulierte Daten, schwindendes öffentliches Vertrauen, Ausfälle kritischer Infrastrukturen und sich entwickelnde regulatorische Sanktionen gefährden Unternehmen. Jedes dieser Risiken kann die Wettbewerbsposition, den Aktienkurs und den Unternehmenswert negativ beeinflussen.

Führende Unternehmen sehen Cyber-Risiken – ebenso wie andere kritische Risiken – im Sinne einer Abwägung von Risiko und Nutzen. Im Falle der Cyber-Risiken ist dies aus zwei Gründen eine besondere Herausforderung. Zum einen ist die Komplexität von Cyber-Risiken dramatisch gestiegen. Unternehmen sehen sich heute mit immer intelligenteren Vorfällen konfrontiert, für die traditionelle Abwehrmechanismen nicht mehr ausreichen. Mit zunehmender Komplexität dieser Angriffe steigt auch das Risiko, das diese Angriffe für Unternehmen darstellen. Die potenziellen Auswirkungen eines erfolgreichen Angriffs gehen weit über den reinen Datenverlust oder Produktivitätsausfälle hinaus. Cyber-Angriffe können schwerwiegende Auswirkungen auf die Reputation und die Marke eines Unternehmens haben, die stärker von Faktoren wie Zeitpunkt oder Publicity als vom tatsächlichen Datenverlust beeinflusst werden. Auch können sich aus Cyber-Angriffen rechtliche Implikationen für Unternehmen und Vorstände ergeben. Gleichzeitig ist die Motivation neueste Technologien einzusetzen, um Kosten zu senken, den Kundenservice zu verbessern und Innovationen voranzutreiben, stärker denn je. Diese konkurrierenden Anforderungen an die Belegschaft von Unternehmen und an Führungskräfte machen eine gewissenhafte und umfassende Kontrolle auf Vorstands- und Aufsichtsratsebene unerlässlich. Um Cyber-Risiken erfolgreich bewältigen und Schäden begrenzen zu können, bedarf es einer strategischen Weitsicht und Planung, die weit über das Know-how der IT-Abteilung hinausgeht.

Die NACD hat, in Zusammenarbeit mit AIG und der Internet Security Alliance, fünf Schritte festgelegt, die von Vorständen in Betracht gezogen werden sollten, um die Überwachung von Cyber-Risiken zu verbessern. Dieses Handbuch ist nach den folgenden fünf Grundprinzipien aufgebaut:

1. Die Unternehmensleitung (d. h. Vorstand und Aufsichtsrat) muss Cyber-Sicherheit als unternehmensweites Risiko-Management-Thema verstehen und adressieren – nicht als reines IT-Problem.
2. Die Unternehmensleitung sollte die rechtlichen Auswirkungen von Cyber-Risiken in Bezug auf die individuellen Anforderungen ihres Unternehmens verstehen.
3. Die Unternehmensleitung sollte angemessenen Zugang zu Cyber-Sicherheitsexpertise haben und Diskussionen über das Cyber-Risiko-Management sollten regelmäßig und in angemessenem Zeitumfang auf der Tagesordnung der Vorstandssitzungen platziert werden.
4. Die Unternehmensleitung sollte die Erwartung formulieren, dass das Management einen unternehmensweiten Rahmen für das Cyber-Risiko-Management mit adäquater Personalausstattung und angemessenem Budget schaffen wird.
5. In der Diskussion der Unternehmensleitung über Cyber-Risiken sollte geklärt werden, welche Risiken vermieden, welche akzeptiert und welche über Versicherungen gemindert oder verteilt werden sollen – und welche spezifischen Maßnahmen mit jeder dieser Varianten einhergehen sollten.

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-Bedrohungslandschaft verändert sich schnell

Noch vor wenigen Jahren waren Cyber-Angriffe weitgehend ein Spielfeld von Hackern und einigen hoch spezialisierten Individuen. Die Angriffe waren durchaus problematisch, wurden aber von vielen Unternehmen eher als unbedeutendes Problem abgetan.

Heutzutage sind Unternehmen Angreifern ausgesetzt, die Teil von hoch entwickelten Teams sind, welche zunehmend zielgerichtete Schadprogramme gegen Systeme und Einzelpersonen

[7] Ocean Tomo, "Annual Study of Intangible Asset Market value from Ocean Tomo, LLC", Pressemitteilung vom 5. März 2015.

in mehrstufigen, schwer zu entdeckenden Angriffen einsetzen. Diese Angriffe, die auch als APTs (Advanced Persistent Threats) bezeichnet werden, wurden anfangs vorwiegend gegen Regierungseinrichtungen und Rüstungsunternehmen eingesetzt. In letzter Zeit lässt sich jedoch beobachten, dass sie die gesamte Wirtschaft durchdrungen haben, was bedeutet, dass praktisch jede Organisation gefährdet ist.

Eines der charakteristischen Merkmale dieser Angriffe ist, dass sie praktisch alle Abwehrsysteme eines Unternehmens wie Firewalls oder Systeme zur Entdeckung von Angriffen überwinden können. Eindringlinge suchen nach mehreren Wegen, um alle Ebenen von Cyber-Sicherheitsschwachstellen auszunutzen, bis sie ihr Ziel erreichen. In der Realität sieht es so aus, dass ein professioneller Angreifer mit ziemlicher Sicherheit in eines der Systeme eines Unternehmens, auf das er abzielt, erfolgreich eindringen wird.

Hinzu kommt, dass Mitarbeiter – ob unzufrieden oder nur ungenügend geschult – Unternehmen mindestens ebenso exponieren, wie dies durch Angriffe von außen geschieht. Daher benötigen Unternehmen ein starkes und anpassungsfähiges Cyber-Sicherheitsprogramm, das sowohl externe als auch interne Bedrohungen umfasst. Wenn Unternehmen nicht in der Lage sind, einfache Angriffe zu stoppen, werden sie nicht mit komplexen Attacken umgehen können.[8]

Größere Vernetzung, größeres Risiko

Aufgrund der flächendeckenden Vernetzung von Datensystemen reicht es nicht mehr aus, dass Organisationen nur noch „ihr" Netzwerk sichern. Lösungsanbieter, Lieferanten, Partner, Kunden oder andere mit dem Unternehmen elektronisch verbundene Unternehmen können zu einem potenziellen Schwachpunkt werden. So gelangte beispielsweise ein raffinierter Angreifer in die Systeme eines großen Ölkonzerns, indem er Malware in das Online-Bestellsystem eines chinesischen Restaurants einschleuste, das bei den Mitarbeitern des Ölkonzerns beliebt war, nachdem er nicht über den klassischen Weg in das Netzwerk eindringen konnte. Anschließend waren die Eindringlinge in der Lage, das eigentliche Kerngeschäft anzugreifen.[9]

Die zunehmende Verknüpfung traditioneller Informationssysteme mit nicht-traditionellen Geräten wie Sicherheitskameras, Kopierern, Videospielplattformen und Fahrzeugen – das so genannte *Internet of Things* – hat zu einem exponenziellen Anstieg

Cyber-Bedrohungen in Zahlen

- 48 Prozent der Informationsschutzverletzungen resultieren aus kriminellen oder böswilligen Angriffen.[i] 80 Prozent der Black Hat Hacker haben Verbindungen zum organisierten Verbrechen.[ii]
- Zu den wichtigsten Zugriffsmethoden für Cyber-Kriminelle gehörten die Verwendung gestohlener Zugangsdaten und von Schadsoftware.[iii] Angriffe auf mobile Geräte und Angriffe mit Cyber-Erpressung nehmen zu.[iv]
- Die durchschnittliche Anzahl der Tage, die eine Organisation unbemerkt kompromittiert ist, bevor sie eine Informationssicherheitsverletzung entdeckt, beträgt 146 Tage.[v] 53 Prozent der Cyber-Angriffe werden zuerst von Strafverfolgungsbehörden oder Dritten identifiziert, verglichen mit 47 Prozent, die intern entdeckt werden.[vi]
- 48 Prozent der IT-Sicherheitsexperten untersuchen die Cloud nicht auf Malware, obwohl 49 Prozent aller Geschäftsanwendungen inzwischen in der Cloud gespeichert sind. Von diesen cloudbasierten Anwendungen ist weniger als die Hälfte bekannt, sanktioniert oder von der IT genehmigt.[vii]
- 38 Prozent der IT-Abteilungen verfügen nicht über definierte Prozesse zur Überprüfung ihrer Pläne für die Reaktion auf Cyber-Vorfälle, und fast ein Drittel hat die Pläne nach dem Erstellen nicht überprüft oder aktualisiert.[viii]

[i] Ponemon Institute and IBM, 2016 Cost of Data Breach Study: Global Analysis, Seite 2.
[ii] Limor Kessem, 2016 Cybercrime Reloaded: Our Predictions for the Year Ahead, 15. Jan. 2016.
[iii] Verizon, 2016 Data Breach Investigations Report, Seiten 8 - 9.
[iv] Kessem, 2016 Cybercrime Reloaded.
[v] FireEye Inc, Mandiant M-Trends 2016, Seite 4.
[vi] Mandiant M-Trends, Seite 7, 2016 Data Breach Investigations Report, Seite 11.
[vii] Jeff Goldman, 48 Percent of Companies Don't Inspect the Cloud for Malware, eSecurity Planet (blog), 12. Okt. 2016.
[viii] Thor Olavsrud, Companies complacent about data breach preparedness, CIO, 28. Okt. 2016.

[8] Verizon RISK Team et al., *2013 Data Breach Investigations Report*, März 2013.
[9] Nicole Perlroth, Hackers Lurking in Vents and Soda Machines, the *New York Times*, 7. April 2014.

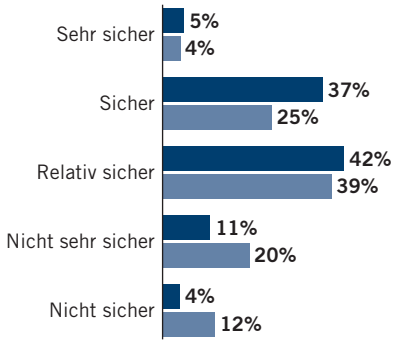
der Anzahl möglicher Einstiegspunkte für Cyber-Angreifer und damit zu der Notwendigkeit geführt, dass Organisationen ihre Überlegungen zur Cyber-Risiko-Abwehr erweitern müssen. Ein „Distributed Denial of Service"-Angriff im Jahr 2016, der den Zugriff auf über 1.000 Unternehmenswebsites, darunter Twitter, PayPal und Netflix, stark einschränkte, wurde von Hackern koordiniert, die Hunderttausende von Endgeräten, darunter digitale Heimvideorekorder und Webcams, nutzten.[10]

Regierungsbehörden konzentrieren sich in erster Linie darauf, die kritische Infrastruktur des Landes (einschließlich Energie- und Wasserversorgung, Kommunikations- und Transportnetzen und dergleichen) vor Cyber-Angriffen zu schützen. Solche Angriffe sind technisch möglich und können schwerwiegende Folgen haben, dennoch ist die überwiegende Mehrheit der Vorfälle wirtschaftlich motiviert.[11] Cyber-Angreifer versuchen routinemäßig alle Arten von Daten zu stehlen, beispielsweise persönliche Informationen von Kunden und Mitarbeitern, Finanzdaten, Geschäftspläne, Geschäftsgeheimnisse und geistiges Eigentum. Immer häufiger setzen diese Angreifer dazu Software ein, welche die Daten einer Organisation verschlüsselt und sie unter Verschluss hält, bis sie eine Zahlung erhalten – so genannte Ransomware. Die Schätzung der Schäden durch Cyber-Angriffe ist schwierig, aber einige Stellen gehen von mehr als 400 - 500 Milliarden US-Dollar pro Jahr aus, wobei ein erheblicher Teil der finanziellen Schäden unentdeckt bleibt.[12] Die Kosten für Cyber-Kriminalität haben sich zwischen 2013 und 2015 verfünffacht und könnten bis 2019 auf über 2 Billionen US-Dollar pro Jahr steigen.[13]

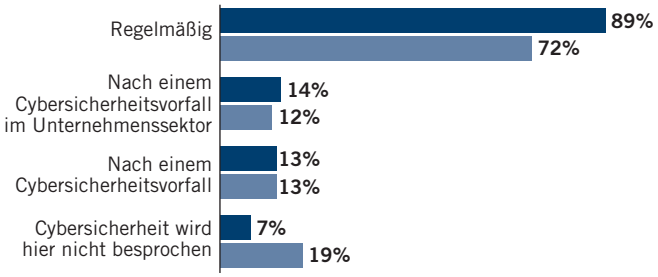
Auch wenn viele kleinere und mittelständische Unternehmen in der Vergangenheit überzeugt waren, dass sie zu unbedeutend für einen Angriff seien, hat sich diese Wahrnehmung als falsch erwiesen. Tatsächlich ist die Mehrheit der kleinen und mittelständischen Unternehmen bereits Opfer von Cyber-Angriffen geworden.[14,15] Kleinere Unternehmen sind nicht nur selbst Ziele, sondern oft Einstiegspunkte für Angriffe auf größere Organisationen über Kunden-, Lieferanten- oder Joint-Venture-Beziehungen. Damit wird das Lieferanten- und Partnermanagement zu einer kritischen Aufgabe für alle miteinander vernetzten Organisationseinheiten.

ABBILDUNG 1

Wie sicher sind Sie, dass Ihr Unternehmen gegen einen Cyber-Angriff geschützt ist?



Wie oft wird das Thema Cyber-Sicherheit in Vorstandssitzungen diskutiert?



Quelle: Diese Daten stammen aus den Erhebungen der NACD 2016 - 2017 zur Governance von öffentlichen und privaten Unternehmen.

[10] Samuel Burke, Massive cyberattack turned ordinary devices into weapons, CNNMoney.com, 22. Okt. 2016.

[11] Verizon, *2016 Data Breach Investigations Report*, Seite 7.

[12] Steve Morgan, Cyber Crime Costs Projected to Reach $2 Trillion by 2019, *Forbes*, 17. Jan. 2016.

[13] Ibid.

[14] Patricia Harmn, 50% of small businesses have been the target of a cyber attack, PropertyCasualty360.com, 7. Okt. 2015.

[15] Mark Smith, Huge rise in hack attacks as cyber-criminals target small business, *The Guardian*, 8. Feb. 2016.

Warum sollten sie uns angreifen?

Einige Organisationen halten es für unwahrscheinlich, dass sie Opfer eines Cyber-Angriffs werden, weil sie relativ klein sind, keinen bekannten Markennamen haben und nicht oder nur begrenzt über umfangreiche Mengen an sensiblen Kundendaten wie Kreditkartennummern oder medizinischen Informationen verfügen.

Tatsächlich zielen Angreifer auf Organisationen jeder Größe und aus jeder Branche ab und suchen nach allem, was von Wert sein könnte, wie zum Beispiel:

- Businesspläne, einschließlich Strategien für Fusionen oder Übernahmen, Angebote etc.
- Handelsalgorithmen
- Verträge oder vorgeschlagenen Vereinbarungen mit Kunden, Lieferanten, Distributoren, Joint-Venture-Partnern etc.
- Log-in-Berechtigungen von Mitarbeitern
- Gebäudeinformationen, einschließlich Anlagen- und Ausrüstungsentwürfe, Gebäudepläne und zukünftige Planungen
- F&E-Informationen, einschließlich neuer Produkte oder Dienstleistungen, die sich in der Entwicklung befinden
- Informationen zu wichtigen Geschäftsprozessen
- Quellcodes
- Listen von Mitarbeitern, Kunden, Auftragnehmern und Lieferanten
- Kunden-, Spender- oder Treuhänderdaten

Quelle: Internet Security Alliance

Im Bereich Cyber-Sicherheit herrscht allgemeiner Konsens darüber, dass Cyber-Angreifer den Unternehmen, die sich gegen sie verteidigen müssen, oft deutlich voraus sind. Cyber-Angriffe sind relativ preiswert, aber hochprofitabel, und die Ressourcen und Fertigkeiten, die notwendig sind, um einen Angriff zu starten, sind einfach zu erwerben. So überrascht die Einschätzung vieler Beobachter nicht, dass die Cyber-Risiko-Abwehr tendenziell eine Generation hinter den Angreifern zurückbleibt. Es ist schwierig, die Rentabilität (*Return on Investment* [ROI]) für die Prävention von Cyber-Angriffen nachzuweisen, und eine erfolgreiche Reaktion der Strafverfolgungsbehörden auf solche Angriffe ist praktisch nicht existent. Nach einigen Schätzungen werden weniger als 1 Prozent der Cyber-Angreifer erfolgreich strafrechtlich verfolgt.[16]

Dies bedeutet in der Folge nicht, dass Schutz unmöglich ist. Vielmehr heißt es, dass die Vorstandsmitglieder sicherstellen müssen, dass sich das Management mit vollem Engagement dafür einsetzt, die Systeme der Organisation im Rahmen der wirtschaftlichen Möglichkeiten so widerstandsfähig wie möglich zu machen. Dazu ist es unter anderem erforderlich, umfassende Verteidigungs- und Reaktionsstrategien zu entwickeln, die in der Lage sind, ausgefeilte Angriffsmethoden auch über Unternehmensgrenzen hinweg effektiv zu adressieren.

Balance zwischen Cyber-Sicherheit und Wirtschaftlichkeit

Wie andere kritische Risiken, mit denen Unternehmen konfrontiert sind, kann Cyber-Sicherheit nicht isoliert betrachtet werden. Die Mitglieder der Geschäftsleitung und des Aufsichtsrates müssen ein angemessenes Gleichgewicht zwischen der Sicherheit einer Organisation und der Minimierung von Verlusten finden. Gleichzeitig müssen sie Profitabilität und Wachstum in einem wettbewerbsorientierten Umfeld sicherstellen.

Viele technische Innovationen und Geschäftspraktiken, die die Wirtschaftlichkeit erhöhen, können gleichzeitig die Cyber-Sicherheit untergraben. Mobile Technologien, Cloud Computing und „smarte" Geräte sorgen zwar einerseits für erhebliche Kosteneinsparungen und höhere Effizienz, können aber andererseits auch eine große Herausforderung hinsichtlich des Themas Cyber-Sicherheit darstellen, wenn sie unbedacht implementiert werden. Richtig eingesetzt können sie die Sicherheit erhöhen, aber dies hat seinen Preis. Die Unternehmensführung benötigt eine weitgefasste Strategie, die u. a. auch die digitalen Unternehmensabläufe umfasst, um ihrer Aufsichtspflicht gerecht zu werden.

Ebenso können Trends wie BYOD (*bring your own device*), der 24/7-Zugriff auf Informationen, das Wachstum von ausgefeilten „Big Data"-Analysen und die Nutzung langer, internationaler Lieferketten so kosteneffizient sein, dass sie für die

[16] Gary Miller, "60% of small companies that suffer a cyber attack are out of business within six months," the Denver Post, Oct. 24, 2016.

Wettbewerbsfähigkeit eines Unternehmens erforderlich sind. Allerdings können auch diese Maßnahmen die Cyber-Sicherheit der Organisation signifikant schwächen.

Es ist für Unternehmen möglich, sich zu verteidigen und gleichzeitig wettbewerbsfähig zu bleiben sowie die Wirtschaftlichkeit aufrechtzuerhalten. Erfolgreiche Cyber-Sicherheitsmaßnahmen lassen sich jedoch nicht einfach am Ende von Geschäftsprozessen „anflanschen". Cyber-Sicherheit muss durchgehend in die wichtigsten Systeme und Prozesse eines Unternehmens integriert werden. Erfolgreich implementiert kann sie dazu beitragen, Wettbewerbsvorteile zu erlangen. Eine Studie ergab, dass vier grundlegende Sicherheitskontrollen ausreichten, um 85 Prozent aller Cyber-Angriffe zu verhindern:

- Einschränken der Installation von Anwendungen durch Benutzer („Whitelisting")
- Sicherstellen, dass das Betriebssystem mit aktuellen Updates „gepatcht" wird
- Sicherstellen, dass Softwareanwendungen regelmäßig aktualisiert werden
- Einschränken der Administratorrechte (d. h. der Möglichkeit, Software zu installieren oder die Konfigurationseinstellungen eines Computers zu ändern)[17]

Die Studie zeigte auch, dass diese Kernpraktiken der Cyber-Sicherheit nicht nur effektiv waren, sondern auch die Wirtschaftlichkeit von Unternehmen verbesserten und sich sofort positiv auf die Rendite auswirkten. Hinzu kommen noch die zusätzlichen positiven wirtschaftlichen Effekte durch die Reduzierung von Cyber-Vorfällen.[18]

Um effektiv zu sein, muss die Cyber-Strategie eines Unternehmens mehr als nur reaktiv sein. Führende Organisationen erneuern ihre Informationen über die Cyber-Risiko-Umgebung kontinuierlich, um damit das Vorgehen potenzieller Angreifer zu antizipieren. Darüber hinaus führen sie regelmäßige ausführliche Tests der eigenen Systeme und Prozesse durch, um Schwachstellen zu identifizieren.

Die in diesem Handbuch beschriebenen fünf Prinzipien für eine wirksame Überwachung von Cyber-Risiken werden in einer relativ verallgemeinerten Form dargestellt, um die Diskussion und Reflexion in den Aufsichtsgremien zu fördern. Natürlich wird die Unternehmensführung diese Empfehlungen auf der Grundlage der individuellen Merkmale der eigenen Organisation anpassen müssen, darunter Unternehmensgröße, Strategie, Businesspläne, Branche, Geografie und Kultur.

[17] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, Okt. 2013. Siehe auch: Internet Security Alliance, *Sophisticated Management of Cyber Risk* (Arlington, VA: Internet Security Alliance, 2013).

[18] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, Okt. 2013.

PRINZIP 1

Die Unternehmensleitung (d. h. Vorstand und Aufsichtsrat) muss Cyber-Sicherheit als unternehmensweites Risiko-Management-Thema verstehen und adressieren – nicht als reines IT-Problem.

In der Vergangenheit haben Unternehmen Informationssicherheit als ein technisches oder operatives Problem kategorisiert, das überwiegend in der Verantwortung der Abteilung für Informationstechnologie (IT) liegt. Dieses Missverständnis wird durch Silo-Strukturen in Unternehmen gefördert, die dazu führen können, dass sich Rollen und Geschäftseinheiten innerhalb der Organisation nicht für die Sicherheit der eigenen Daten verantwortlich fühlen. Stattdessen wird diese kritische Verantwortung gerne an die IT übergeben, eine Abteilung, die in den meisten Organisationen über geringe Ressourcen und Budgetverantwortlichkeit verfügt. Darüber hinaus schränkt eine Verlagerung der Verantwortung in die IT eine kritische Analyse und Kommunikation über Sicherheitsfragen ein und erschwert die Umsetzung effektiver Cyber-Sicherheitsstrategien.

Mit zunehmender Digitalisierung wächst der Wert der Daten in einem Unternehmen. Die Absicherung ebendieser Daten wird immer wichtiger für die Geschäftskontinuität der Unternehmen. Daher sollten Cyber-Risiken in erster Linie im geschäftlichen Kontext bewertet werden, analog zur Bewertung der physischen Sicherheit von Mitarbeitern und physischen Unternehmenswerten sowie der Risiken im Zusammenhang mit ihrer Schädigung. Mit anderen Worten: Cyber-Sicherheit gehört zum unternehmensweiten Risikomanagement, das aus strategischer, operationeller, abteilungsübergreifender und wirtschaftlicher Sicht angegangen werden muss.[19]

Cyber-Risiken und das Ökosystem des Unternehmens

Eine gute Cyber-Hygiene ist unerlässlich für die Abwehr vieler Angriffe. Die Ursache für einige der bekanntesten bisherigen Cyber-Vorfälle hat jedoch wenig mit traditionellem Hacking zu tun. Viele Studien deuten beispielsweise darauf hin, dass dem Unternehmen schlecht gesonnene oder schlecht geschulte Personen, die über einen autorisierten Zugang zum System verfügen, die Ursache für viele Vorfälle sind. Das zusätzliche Bereitstellen von Zugangspunkten im Rahmen von Lieferantenbeziehungen oder gar Kundenkontakten kann das Cyber-Risiko vervielfachen. Auch Produkteinführungen oder Produktionsstrategien, die komplexe Lieferketten über mehrere Länder und Regionen hinweg nutzen, können das Cyber-Risiko erhöhen. Ebenso stellen Fusionen und Übernahmen, die die Integration komplizierter Systeme erfordern und oft unter hohem Zeitdruck und ohne Due Diligence erfolgen, eine Gefahr für einen Cyber-Vorfall dar.

Abhängig von Größe und Komplexität des Unternehmens, stellt sich beim Grad der Vernetzung des Unternehmensnetzwerks mit Partnern, Lieferanten, verbundenen Tochtergesellschaften und Kunden die Frage, wie man ein sicheres System für das Unternehmen schaffen kann. Mehrere bedeutende und öffentlich bekannte Informationssicherheitsverletzungen haben nicht in den IT-Systemen des angegriffenen Unternehmens begonnen, sondern resultierten aus Schwachstellen bei einem ihrer Lösungsanbieter oder Lieferanten, wie die Beispiele im Abschnitt „Größere Vernetzung, größeres Risiko“ auf Seite 8 zeigen. Darüber hinaus verlagern immer mehr Organisationen einen Teil ihrer Daten in externe Netzwerke oder in eine öffentliche „Cloud“, die sie weder besitzen noch betreiben und auf deren Sicherheit sie wenig Einfluss haben. Diese Abhängigkeiten können die Cyber-Sicherheit eines Unternehmens untergraben. Einige Organisationen sind mit nationalen und länderübergreifenden kritischen Infrastrukturen verbunden. Daraus ergibt sich die Möglichkeit, dass unzureichende Cyber-Sicherheit bei einem Unternehmen oder einer Institution zu einer Gefahrenquelle für die öffentliche Sicherheit oder sogar die regionale bzw. nationale Sicherheit wird.

Daher sollten die Vorstände und der Aufsichtsrat sicherstellen, dass das Management die Cyber-Sicherheit nicht nur im Hinblick auf die eigenen Netzwerke bewertet, sondern auch im

Identifizierung der „Kronjuwelen“ des Unternehmens

Der Aufsichtsrat sollte mit Vorstand und Management in regelmäßigen Abständen die folgenden Fragen erörtern:

- Welches sind die kritischsten Daten für unser Unternehmen?
- Wo sind diese lokalisiert? Befinden sie sich auf einem oder mehreren Systemen?
- Wie wird auf sie zugegriffen? Wer hat die Berechtigung, auf sie zuzugreifen?
- Wie oft haben wir unsere Systeme getestet, um sicherzustellen, dass sie unsere Daten angemessen schützen?

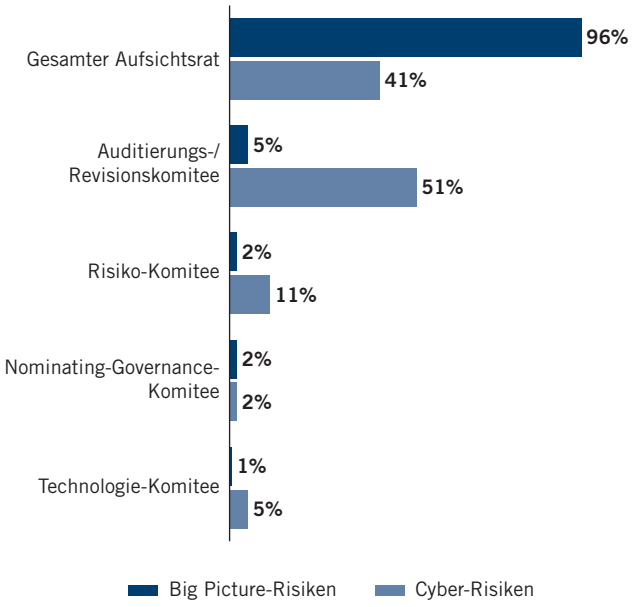
[19] Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*, 2010.

Hinblick auf das größere Ökosystem, in dem das Unternehmen tätig ist. Vorausschauende und proaktive Vorstände werden das Management in eine Diskussion über die unterschiedlichen Ebenen oder Risiken, die in der Ökosphäre des Unternehmens bestehen, einbeziehen und diese bei der Berechnung der angemessenen Cyber-Risiko-Haltung und -Toleranz für das eigene Unternehmen berücksichtigen.[20] Sie sollten auch verstehen, welche „Kronjuwelen" das Unternehmen am meisten schützen muss, und sicherstellen, dass das Management über eine abgestimmte Schutzstrategie für diese unternehmenskritischen Güter verfügt. Der Vorstand sollte das Management anweisen, nicht nur die wahrscheinlichsten Angriffe und Abwehrmaßnahmen zu berücksichtigen, sondern auch solche mit geringer Wahrscheinlichkeit und hoher Wirkung, die jedoch katastrophale Auswirkungen auf das Geschäft hätten.[21]

Anhang B enthält eine Liste von Fragen zur Cyber-Sicherheit, die Aufsichtsrats- und Vorstandsmitglieder an das Management zu Themen wie Lagebild, Strategie und Betrieb, Bedrohung durch Innentäter, Risiken in der Lieferkette/Drittparteien, Reaktion auf Zwischenfälle und Reaktion nach einem Vorfall stellen können.
Anhang C beschreibt Cyber-Sicherheitsüberlegungen im Zusammenhang mit Fusionen und Übernahmen.
Anhang E beschreibt die Unterschiede zwischen den deutschen Gremienstrukturen, z. B. Beirat, Aufsichtsrat und Vorstand.

ABBILDUNG 2

Welcher Gruppe hat der Aufsichtsrat die Mehrheit der Aufgaben zugewiesen, die mit den folgenden Bereichen der Risikokontrolle zusammenhängen? (Unvollständige Liste der Antwortmöglichkeiten; Mehrfachauswahl erlaubt)



Quelle: 2016–2017 NACD Public Company Governance Survey.

Aufsichtsverantwortung für Cyber-Risiken auf Vorstandsebene

Die Frage, wie der Aufsichtsrat zu organisieren ist, um die Überwachung von Cyber-Risiken – und, allgemeiner gesagt, die Risikokontrolle auf Unternehmensebene – zu steuern, ist Gegenstand erheblicher Diskussionen. Jedes Unternehmen ist anders organisiert, je nach seinem spezifischen geschäftlichen und regulatorischen Umfeld. In Deutschland sind bestimmte Arten/Größen von Unternehmen gesetzlich verpflichtet, Aufsichtsgremien zu bilden und zu unterhalten. Für andere ist es eine freiwillige Entscheidung, ob ein solches Gremium für die eigene Unternehmensstruktur geeignet ist. Für Unternehmen mit Aufsichtsräten (ob mandatiert oder freiwillig) sollte die Größe und Struktur des Aufsichtsrates dem Geschäftsrisiko Rechnung tragen. Die Entscheidung, ob der Vorstand eine Management- oder eine Beratungsfunktion hat, ist ausschlaggebend für die Entscheidung über die Verantwortlichkeiten der Cyber-Risiko-Aufsicht. So haben beispielsweise Aufsichtsräte klare Rollen und Kompetenzen, die sie in die Lage versetzen, das Unternehmen bzw. die Unternehmensführung zu überwachen.

Die *NACD Blue Ribbon Commission on Risk Governance* hat empfohlen, dass die Risikokontrolle eine Funktion des Gesamtvorstands sein sollte.[22] NACD-Untersuchungen kommen zu dem Schluss, dass dies bei den meisten Vorstände börsennotierter Unternehmen mit sogenannten big picture risks (d. h. Risiken mit weitreichenden Auswirkungen auf die strategische Ausrichtung oder Diskussionen über das Zusammenspiel verschiedener Risiken) der Fall ist. Etwas mehr als die Hälfte der Gremien überträgt jedoch die Mehrheit der mit der Cyber-Sicherheit verbundenen Risikoüberwachungsaufgaben an

[20] NACD, et al., Cybersecurity: Boardroom Implication (Washington, DC: NACD, 2014) (an NACD white paper).
[21] Ibid. Siehe auch: KPMG Audit Committee Institute, *Global Boardroom Insights: The Cyber Security Challenge*, 26. März 2014.
[22] NACD, *Report of the Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward* (Washington, DC: NACD, 2009).

das Auditierungs-/Revisionskomitee (Abbildung 2), das auch eine wesentliche Verantwortung für die Beaufsichtigung der Finanzberichterstattung und der Compliance-Risiken übernimmt.

Die neue Datenschutzgrundverordnung (DSGVO) verlangt besondere Aufmerksamkeit für den Datenschutz durch die Vorstandsebene. Der Vorstand muss sicherstellen, dass Datenschutz und Privatsphäre gewahrt und gut organisiert sind. Datenverlust kann zu erheblichen Strafen (bis zu 4 Prozent des weltweiten Jahresumsatzes) und zur persönlichen Haftung von Mitgliedern der Geschäftsführung führen.

Es gibt keinen universellen Ansatz, der auf jedes Gremium passt. Einige entscheiden sich dafür, alle Diskussionen im Zusammenhang mit Cyber-Risiken auf der Ebene des Gesamtvorstands zu führen. Andere weisen einem oder mehreren Ausschüssen (Audit, Risiko, Technologie etc.) spezifische Cyber-Sicherheitsaufsichtsaufgaben zu. Wieder andere verwenden eine Kombination dieser Methoden. Der Nominierungs- und Governanceausschuss sollte sicherstellen, dass der vom Vorstand gewählte Ansatz in den Satzungen der jeweiligen Gremien klar definiert ist, um unklare Zuständigkeiten oder Doppelarbeit zu vermeiden. Der Gesamtvorstand sollte mindestens halbjährlich über Cyber-Sicherheitsfragen informiert werden, und zwar so, wie es für bestimmte Vorkommnisse oder Situationen erforderlich ist. Ausschüsse, die für die Risikoüberwachung – und insbesondere für die Überwachung von Cyber-Risiken – zuständig sind, sollten mindestens vierteljährlich informiert werden.

Um den Wissensaustausch und den Dialog zu fördern, laden einige Aufsichtsräte alle Mitglieder der Unternehmensführung ein, an Diskussionen auf Ausschussebene über Cyber-Risiko-Themen teilzunehmen oder direkt die eigene Mitgliedschaft in anderen Ausschüssen zu nutzen. Zum Beispiel hat das Technologie-Komitee auf Vorstandsebene eines globalen Unternehmens Mitglieder der Unternehmensführung, die Experten für Datenschutz und Sicherheit aus Kundensicht sind, zu Mitgliedern des Komitees gemacht. Bei diesem Unternehmen sind die Vorsitzenden der Audit- und Technologieausschüsse ebenso Mitglieder des jeweils anderen Ausschusses. Beide Ausschüsse treffen sich einmal im Jahr zu einer Diskussion, die einen „Deep Dive" zum Thema Cyber-Sicherheit beinhaltet.[23]

Auch wenn die Einbeziehung von Cyber-Sicherheit als eigenständigem Punkt auf der Tagesordnung der Sitzungen der Unternehmensführung inzwischen weit verbreitet ist, sollte das Thema auch in die Diskussionen der Unternehmensführung selbst miteinbezogen werden, um beispielsweise neue Geschäftspläne und Produktangebote, Fusionen und Übernahmen, den Eintritt in neue Märkte, den Einsatz neuer Technologien, wichtige Investitionsentscheidungen wie Anlagenerweiterungen oder IT-System-Upgrades und dergleichen aus Cyber-Risiko-Sicht zu bewerten.

In Anhang A finden Sie Vorschläge für Fragen, die der Unternehmensführung helfen sollen, den Kenntnisstand ihres Vorstands in Bezug auf Fragen der Cyber-Sicherheit zu beurteilen.
Anhang H enthält Beispiele für Evaluierungsfragen im Zusammenhang mit der Überwachung der Cyber-Sicherheit.

[23] Adaptiert aus Robyn Bew, *Cyber-Risk Oversight: 3 Questions for Directors*, *Ethical Boardroom*, Frühjahr 2015.

PRINZIP 2

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

Die rechtliche und regulatorische Landschaft in Bezug auf die 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 Haftungsfragen ihrer Organisationen – und möglicherweise auch der Vorstände auf individueller oder kollektiver Basis – im Klaren sein. Das externe Haftungsrisiko für Organmitglieder unterliegt nach deutschem Recht aktuell nicht dem Datenschutz- oder Cyber-Sicherheitsrecht, sondern den allgemeinen Sorgfaltspflichten, die der Aufsichtsrat der Gesellschaft gegenüber Vorstandsmitgliedern durchsetzen kann. Beispielsweise können öffentlichkeitswirksame Angriffe D&O-(Directors & Officers)-Haftungsansprüche auslösen, die den Vorstand der Misswirtschaft, Verschwendung von Unternehmensvermögen oder Vernachlässigung der Treuepflicht beschuldigen, da unzureichende Schritte unternommen wurden, um die Angemessenheit des Schutzes des Unternehmens vor Cyber-Angriffen oder Datenverstößen zu überprüfen. Abhängig von der Branche und den Standorten des Unternehmens bzw. der Organisation können die Risiken erheblich variieren.

Die Business Judgement Rule (§ 93 Abs. 1 Satz 2 AktG) ist geeignet, Vorstände nach einem schwerwiegenden Cyber-Sicherheitsvorfall zu schützen, sofern der Vorstand das Cyber-Sicherheitsprogramm des Unternehmens auf der Grundlage angemessener Informationen solide überwacht hat. Es wird dringend empfohlen, Aufzeichnungen über die Diskussionen im Rahmen der Vorstandssitzungen über das Cyber-Sicherheitsprogramm, die Cyber-Risiken und die Risikomanagement-Strategie der Organisation zu erstellen, sich regelmäßig über branchen-, regions- oder sektorspezifische Anforderungen, die für die Organisation gelten, zu informieren und zu definieren, was in der Folge eines Cyber-Angriffs offenzulegen ist. Es ist auch ratsam, dass die Unternehmensleitung an einer oder mehreren Cyber-Vorfall-Simulationen oder „Table-Top-Übungen" teilnimmt, um im Falle eines schwerwiegenden Vorfalls die Reaktionsprozesse des Unternehmens zu kennen.

Obwohl viele Fälle von Cyber-Angriffen gegen Unternehmen öffentlich bekannt geworden sind (z. B. die Angriffe durch „WannaCry" und „Petya/NotPetya" im Jahr 2017 oder Fälle von CEO-Fraud), sind Gerichtsurteile, die sich in diesem Zusammenhang mit der D&O-Haftung befassen, noch nicht ergangen.

Gleichzeitig sollte die Unternehmensleitung vom Datenschutzbeauftragten (DSB) ihrer Organisation oder, wenn es keinen DSB gibt, von einem Berater darüber informiert werden, wie die Datenschutzelemente des Cyber-Sicherheitsprogramms der Organisation zu strukturieren sind. Dies beinhaltet auch die Datenschutzvorgaben zum Mitarbeiterschutz bei der Netzwerküberwachung zur Angriffserkennung und -verhinderung.

Protokolle der Vorstandssitzungen

Die Protokolle der Vorstandssitzungen sollten die Anlässe dokumentieren, bei denen die Cyber-Sicherheit auf der Tagesordnung der Sitzungen des Gesamtverwaltungsrats und/oder der wichtigsten Ausschüsse des Verwaltungsrats stand, je nach Verteilung der Aufsichtsaufgaben. Die Diskussionen auf diesen Treffen können Updates bezüglich spezifischer Risiken und Schadenbegrenzungsstrategien sowie Berichte über das gesamte Cyber-Sicherheitsprogramm des Unternehmens und die Integration der Technologie mit der Strategie, den Richtlinien und den Geschäftsaktivitäten des Unternehmens umfassen. Die Aufzeichnungen in den Protokollen sollten zeigen, wie der Vorstand die Risiken für die Organisation in seinen Entscheidungen abwägte und priorisierte.

Offenlegung und Berichtspflichten

Unternehmen und Organisationen können einer Reihe von Offenlegungs- oder Compliance-Verpflichtungen im Zusammenhang mit Cyber-Sicherheitsrisiken und Cyber-Vorfällen unterliegen:

- Meldepflichten für Cyber-Vorfälle im Rahmen der EU-Datenschutzgrundverordnung und des deutschen Bundesdatenschutzgesetzes, aber auch Vorgaben im Hinblick auf Datenschutz-, Datengeheimhaltungs- und Arbeitsgesetze, die das Cyber-Sicherheitsprogramm der Organisationen betreffen.
- der Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) und Anforderungen an die Meldung von Cyber-Sicherheitsvorfällen sowie Möglichkeiten zum Informationsaustausch, die es dem Unternehmen ermöglichen, sich über Cyber-Sicherheitsbedrohungen zu informieren.

- Betreiber kritischer Infrastrukturen[24] müssen eine erhebliche Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit oder eine außergewöhnliche IT-Störung gegenüber dem Bundesamt für Sicherheit in der Informationstechnik nach § 8b(4) des IT-Sicherheitsgesetzes melden.
- branchenspezifischen Vorschriften für die Sektoren Energie Informationstechnik und Telekommunikation (ITK), Wasser, Ernährung, Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr, die alle die Offenlegung von signifikanten Störungen aufgrund eines Cyber-Sicherheitsvorfalls oder einer anderen signifikanten IT-Störung vorschreiben. (Das Bundesamt für Sicherheit in der Informationstechnik [BSI] kann seinerseits andere Parteien von der Störung in Kenntnis setzen, wenn der Bericht nicht im Widerspruch zu den Interessen der offenlegenden Partei steht).
- anderen anwendbaren länderspezifischen Gesetzen, Vorschriften und Standards in anderen Ländern, denen die Organisation unterliegt. Dazu können weitere Sicherheitsanforderungen, unterschiedliche Datenschutzbeschränkungen, Einschränkungen beim Einsatz von Sicherheitstechnologien wie Verschlüsselung und Datenlokalisierung sowie Einschränkungen beim „Zurückhacken" gehören.
- Obwohl es keine besondere Informationspflicht gegenüber der Staatsanwaltschaft gibt, kann die Einschaltung der Staatsanwaltschaft in einigen Fällen zur Klärung des Sachverhalts und zur Erhebung von Beweismitteln für die von und gegen das Unternehmen geltend gemachten Schadenersatzforderungen beitragen.

Zu den Herausforderungen gehören sich überschneidende und widersprüchliche Vorschriften und Anforderungen, mangelnde Koordinierung zwischen Regulierungs- und Gesetzgebungsbehörden und unterschiedliche Prioritäten, die die Entwicklung neuer Vorschriften vorantreiben – einschließlich unterschiedlicher Auffassungen zu grundlegenden Fragen wie der Definition personenbezogener Daten sowie unterschiedlicher Gewichtung legitimer Interessen und Arbeitnehmerrechte. Die Unternehmensleitung muss nicht unbedingt über tiefgehende Kenntnisse in diesem immer komplexer werdenden Rechtsgebiet verfügen, aber sie sollte regelmäßig von internen oder externen Anwälten über die für das Unternehmen geltenden rechtlichen Anforderungen informiert werden. Berichte des Managements sollten es dem Vorstand ermöglichen, zu beurteilen, ob die Organisation diesen potenziellen rechtlichen Risiken angemessen begegnet.

Die Offenlegung von Cyber-Sicherheitsrisiken ist momentan noch nicht erforderlich, kann aber in der Zukunft erfolgen.

Der Vorstand sollte das Management auffordern, die Einschätzung eines externen Rechtsberaters zu Fragen der Offenlegung mit vorausschauendem Blick auf Risikofaktoren im Allgemeinen und auf den Ablaufplan für die Reaktion auf einen größeren Angriff oder einen anderen Cyber-Vorfall einzuholen.

Da sich die Offenlegungsstandards, die regulatorischen Vorgaben, die formalen Anforderungen und die Umstände des Unternehmens ständig weiterentwickeln, sollten das Management und die Unternehmensleitung erwarten, dass sie regelmäßig durch einen Berater auf dem Laufenden gehalten werden müssen. Schlussendlich sollten die Vorstände das Management auffordern, ein integriertes Cyber-Risiko-Management aufzubauen, das rechtliche Risiken, Cyber-Bedrohungen und Geschäftsauswirkungen miteinander kombiniert, um die Gesamtrisikominderungsstrategie zu verbessern.

[24] Kritische Infrastrukturen sind organisatorische und physische Strukturen und Einrichtungen, die für die Gesellschaft und Wirtschaft eines Landes von so entscheidender Bedeutung sind, dass ihr Versagen oder ihre Verschlechterung zu anhaltenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würde.

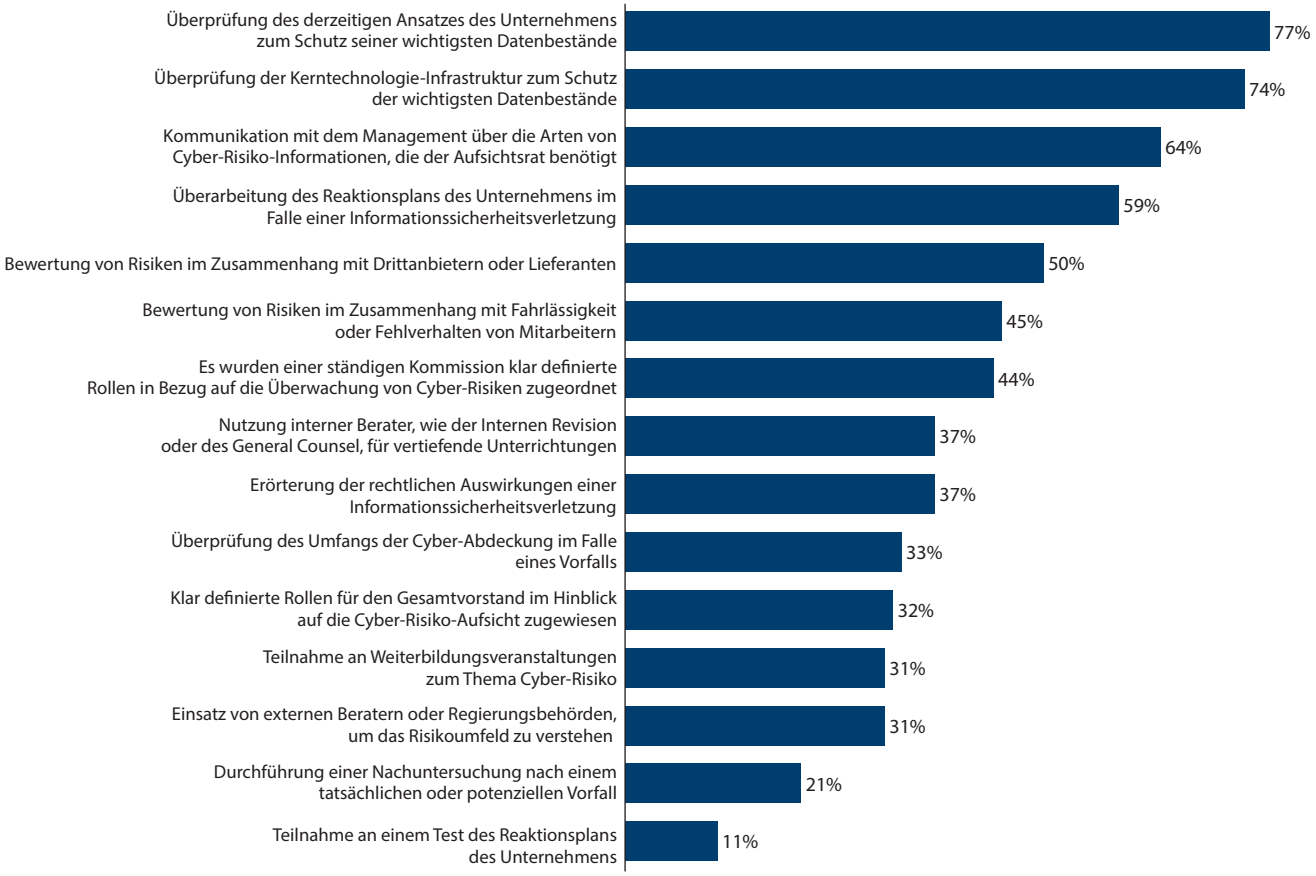
PRINZIP 3

Die Unternehmensleitung sollte angemessenen Zugang zu Cyber-Sicherheitsexpertise haben und Diskussionen über das Cyber-Risiko-Management sollten regelmäßig und in angemessenem Zeitumfang auf der Tagesordnung der Vorstandssitzungen platziert werden.

In „Die Lage der IT-Sicherheit in Deutschland 2017"[25] zieht das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Fazit, dass die Cyber-Gefährdungslage weiterhin auf hohem Niveau angespannt ist. Der Bericht macht deutlich, dass Cyber-Sicherheit eine wesentliche Voraussetzung für das Gelingen der Digitalisierung in Deutschland ist. In einer kürzlich durchgeführten Umfrage unter Vorständen börsennotierter US-amerikanischer Unternehmen gaben 89,1 Prozent der Befragten an, dass ihre Vorstände „regelmäßig" über Cyber-Sicherheit diskutieren[26] (siehe Abbildung 3 für weitere Details). Trotz dieser Aktivität glauben jedoch nur etwa 14 Prozent der Vorstände, dass ihr Vorstand über ein „hohes" Wissen über Cyber-Sicherheitsrisiken verfügt.[27] Wie ein Vorstandsmitglied bemerkte: „[Cyber Security] ist ein ‚bewegliches Ziel'. Die Bedrohungen und Schwachstellen ändern sich fast täglich und die Standards für das Management und die Überwachung von Cyber-Risiken nehmen erst allmählich Gestalt an."[28] Bei einer anderen Sitzung von Vorständen verschiedener Konzerne schlug jemand diese

ABBILDUNG 3

Welche der folgenden Kontroll-Praktiken zur Gewährleistung der Cyber-Sicherheit hat der Vorstand in den letzten 12 Monaten umgesetzt?



Quelle: 2016–2017 NACD Public Company Governance Survey.

[25] BSI, Die Lage der IT-Sicherheit in Deutschland 2017, https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

[26] NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), Seite 28.

[27] NACD, *2016-2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), Seite 26.

[28] NACD Audit Committee Chair and Risk Oversight Advisory Councils, *Emerging Trends in Cyber-Risk Oversight*, 17. Juli 2015, Seite 1.

nützliche Analogie vor: „Man kann Cyber-Basiswissen mit dem Grundwissen im Bereich Finanzen vergleichen. Nicht jeder im Vorstand ist ein Wirtschaftsprüfer, aber jeder sollte in der Lage sein, einen Geschäftsbericht zu lesen und die Geschäftssprache der Finanzwelt zu verstehen."[29]

Verbesserung des Zugangs zu Expertenwissen im Bereich der Cyber-Sicherheit

Mit der Zunahme der Cyber-Bedrohungen wächst auch die Verantwortung (und die Erwartungshaltung) der Vorstandsmitglieder. Die Vorstände müssen mehr tun, als Berichte vom Management zu erhalten und nur zu verstehen, dass es Bedrohungen gibt. Sie müssen dieselben Prinzipien der Befragung und konstruktiven Herausforderung anwenden, wie sie in den Diskussionen des Vorstands über Strategie, Anpassungen und Performance des Unternehmens üblich sind. Daher überlegen einige Unternehmen, ob sie Cyber-Sicherheits- und/oder IT-Sicherheitsexpertise über die Rekrutierung neuer Führungskräfte direkt in den Vorstand einbringen wollen. Dies mag für einige Unternehmen oder Organisationen angemessen sein, aber es gibt keinen einheitlichen Ansatz, der überall anwendbar ist (siehe „Ein Cyber-Experte für jedes Gremium?"). Bei einem runden Tisch der NACD mit Vorständen und führenden Investoren äußerten die Teilnehmer Bedenken hinsichtlich der Forderung, alle Gremien um Mitglieder mit singulären Verantwortungsbereichen zu erweitern, die entweder strikt auf Cyber-Sicherheit oder andere Bereiche spezialisiert sind.[30]

Nominierungs- und Governance-Ausschüsse müssen viele Faktoren bei der Besetzung von Vorstandspositionen ausbalancieren, einschließlich des Bedarfs an Branchenexpertise, Finanzwissen, globaler Erfahrung oder anderen gewünschten Fähigkeiten, je nach den strategischen Bedürfnissen und Umständen des Unternehmens. Unabhängig davon, ob sie sich dafür entscheiden, ein Vorstandsmitglied mit spezifischer Expertise in der Cyber-Domäne hinzuzufügen oder nicht, können Vorstände andere Möglichkeiten nutzen, um sachkundige Perspektiven zu Fragen der Cyber-Sicherheit in den Sitzungssaal zu bringen. Dies schließt u. a. folgende Strategien ein:

- Anberaumen von Vertiefungsgesprächen oder Untersuchungen unabhängiger und objektiver externer Experten, die darlegen, ob das Cyber-Sicherheitsprogramm auf die Unternehmensstrategie abgestimmt ist und es seine Ziele erreicht.
- Einbeziehen der bestehenden unabhängigen Berater des Aufsichtsrates, wie externe Wirtschaftsprüfer und externe Berater, die eine mandanten- und branchenweite Sichtweise auf Cyber-Risiko-Trends einbringen können.
- Teilnahme an einschlägigen Programmen für die Weiterbildung von Führungskräften, unabhängig davon, ob diese intern oder extern durchgeführt werden. Viele Gremien nehmen einen Tagesordnungspunkt „Report back" in ihre Agenda auf, um es den Mitgliedern zu ermöglichen, ihre Erfahrungen von externen Programmen und Schulungen mit anderen Board-Mitgliedern zu teilen.

Es gibt mehrere Möglichkeiten, wie Aufsichtsräte ihren Zugang zu Cyber-Sicherheitsexpertise erweitern können. Cyber-Sicherheit ist wie Händewaschen in Krankenhäusern – jeder muss es einfach tun. Unternehmen müssen entscheiden, welcher Ansatz für ihre strategischen Ziele und Geschäftsziele am besten geeignet ist, ob sie nun einen Cyber-Sicherheitsexperten in das Board aufnehmen oder einfach nur den Zugang zu Cyber-Sicherheitsexperten verbessern wollen. Insgesamt sollten sich die Gremien in regelmäßigen Abständen der Expertise im Bereich der Cyber-Sicherheit bedienen, und die Diskussionen über das Cyber-Risiko-Management sollten sich regelmäßig und in angemessenem Zeitumfang auf den Tagesordnungen der Vorstandssitzungen wiederfinden.

Zugang zu adäquater Cyber-Security-Expertise gewinnen

Von den meisten Vorständen wird zunehmend erwartet, dass sie immer mehr über die wichtigsten, eng verflochten Geschäftsrisiken wissen. Auch wenn sie über bestimmte Fachkenntnisse verfügen, die sich aus ihrer früheren Laufbahn ableiten lassen, sollten Mitglieder des Vorstands eine breitere Sichtweise in Bezug auf das unternehmensweite Risikomanagement und die Reaktion darauf einbringen. Wie erhalten sie Zugang zu adäquater Cyber-Sicherheitsexpertise? Was wird als adäquates Fachwissen im Bereich der Cyber-Sicherheit angesehen? Es beginnt mit dem Grundverständnis, das in Prinzip 1 dieses Handbuchs beschrieben ist – die Gremien müssen verstehen, dass Cyber-Sicherheit

[29] NACD et al., *Cybersecurity: Boardrooms Implications* (Washington, DC: NACD, 2014) (an NACD white paper), Seite 3.

[30] Diskussion während einer gemeinsamen Sitzung des NACD Advisory Council for Audit Committee Chairs and Nominating and Governance Committee Chair, 5. Okt. 2016.

kein IT-Problem ist, sondern eine Herausforderung für das unternehmensweite Risikomanagement. Deshalb sollten die Gremien es vermeiden, es ausschließlich den IT-Abteilungen und IT-Sicherheitsbeauftragten zu überlassen, das Problem „zu lösen".

Hält eine Organisation es im Interesse des Unternehmens für angemessen, jemanden mit Cyber-Know-how in ihren Vorstand aufzunehmen, sollte gefordert werden, dass die Nominierungsausschüsse die Art und Weise überprüfen, wie jemand für den Vorstand ausgewählt wird. Sie sollten sich mit den Fähigkeiten und der Qualität der Vorstandsmitglieder befassen, um zu versuchen, das Fachwissen im Bereich der Cyber-Sicherheit zu verbessern. Cyber-Risiken sind anders als traditionelle oder wirtschaftliche Risiken – dies sollte das zukünftige Vorstandsmitglied verstehen. Bei traditionellen Risiken (Stürme, Brände, Überschwemmungen etc.) und wirtschaftlichen Risiken (Wettbewerb, Produkthaftung, Vermögensschäden etc.) lässt sich die Wahrscheinlichkeit des Eintretens eines Schadenfalls abschätzen. Wir verfügen über historische Daten, z. B. Wettertrends und die Anzahl früherer Vorfälle, die zur Vorhersage potenzieller zukünftiger Risiken verwendet werden können (traditionelle Risiken), sowie das bisherige Marktverhalten, um die Auswirkungen dieser Risiken und die Möglichkeiten, diesen entgegenzuwirken, zu ermitteln (wirtschaftliche Risiken). Bei Cyber-Risiken müssen wir jedoch davon ausgehen, dass jedes Unternehmen zu einem gegebenen Zeitpunkt erfolgreich angegriffen wird.

Darüber hinaus weisen Cyber-Risiken einige wichtige Unterschiede zu traditionellen Risiken auf. Beispielsweise können sich Organisationen in einer vernetzten Welt nicht vollständig schützen. Cyber-Gegenspieler, darunter auch fremde Staaten, haben möglicherweise größere Ressourcen als selbst die größten Konzerne, und die rechtlichen Schutzmaßnahmen in der physischen Welt gehen weit über das hinaus, was im Cyber-Raum verfügbar ist. Dies sollten die mit der Cyber-Aufsicht betrauten Mitglieder des Vorstandes verstehen.

Boards können ein *Checks-and-Balances*-System erstellen, indem sie Ratschläge aus verschiedenen Quellen einholen. Beispielsweise könnte eine Organisation unterschiedliche Berichtsstrukturen aus drei unabhängigen (nicht notwendigerweise externen) Quellen haben: der Perspektive der Person, die für das Cyber-Risiko verantwortlich ist, der Perspektive der Person, die das Cyber-Risiko bewertet, und der Perspektive des operativen Managers. Dies versetzt eine Organisation in die Lage, die Rollen und Vorgehensweisen zu hinterfragen und das Cyber-Risiko aus vielen Perspektiven zu betrachten, um die Risikoschwelle zu senken.

Ein Cyber-Experte für jedes Gremium?

Im Jahr 2008 haben NACD, das US-amerikanische Council of Institutional Investors und die ebenfalls US-amerikanische Organisation Business Roundtable gemeinsam eine Reihe von allgemeinen Schlüsselprinzipien zur Unternehmensaufsicht (Key Agreed Principles for Corporate Governance) entwickelt, die Vorständen/Aufsichtsräten und Aktionären dabei helfen sollen, einen durchdachten und systematischen Ansatz zu entwickeln. Dazu gehört unter anderem die Idee, dass (vorausgesetzt, alle geltenden gesetzlichen, regulatorischen und im Rahmen der Börsennotierung vorausgesetzten Anforderungen werden erfüllt) die einzelnen Gremien die Verantwortung für die Gestaltung der Strukturen und Praktiken tragen, die es ihnen ermöglichen, ihre treuhänderischen Verpflichtungen effektiv und effizient zu erfüllen – und dass sie dazu verpflichtet sind, diese Strukturen und Praktiken transparent an alle Stakeholder zu kommunizieren. Vorschläge, die beispielsweise auf die generelle Forderung abzielen, dass alle Vorstände/Aufsichtsräte ein Mitglied haben müssen, das ein dezidierter „Cyber-Sicherheitsexperte" ist, würden die wichtige Verantwortung für die Zusammensetzung des Aufsichtsrates und die Rekrutierung von Vorständen aus den Händen der einzigen Gruppe nehmen, die aus erster Hand über die aktuellen und zukünftigen Qualifikationsanforderungen des jeweiligen Vorstands/Aufsichtsrats informiert ist. Hinzu kommt, dass eine solche Anforderung angesichts des aktuellen Mangels an Cyber-Security-Experten mit der nötigen Erfahrung in der Praxis nicht umsetzbar wäre. In der Publikation „Key Agreed Principles" heißt es weiter, dass „die Bevorzugung von Transparenz gegenüber einer [mechanischen] Befolgung einer Reihe von [so genannten] Best Practices Gremien dazu ermutigen kann, zu experimentieren und Ansätze zu entwickeln, die den eigenen Bedürfnissen entsprechen".

Quelle: Internet Security Alliance, The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity (Washington, DC: ISA, 2016), Seite 335–338; NACD, Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly-Traded Companies (Washington, DC: NACD, 2011), Seite 5.

Die Vorstände können auch externe Berater als „Cyber-Coaches“ hinzuziehen. Dies wäre eine Ressource, die die Probleme der Cyber-Sicherheit versteht und sie abteilungsübergreifend diplomatisch angehen kann. Diese Ressource hätte sowohl Cyber-Sicherheit als auch umfassende Management-Expertise.

Verbesserung der Berichte des Managements an den Vorstand

Eine Umfrage im Jahr 2012 ergab, dass weniger als 40 Prozent der Vorstände regelmäßig Berichte über Datenschutz- und Cyber-Sicherheitsrisiken erhielten und 26 Prozent selten oder nie solche Informationen erhielten.[31] Seitdem hat sich die Praxis in den Vorstandsetagen signifikant verändert: Wie auf Seite 17 erwähnt, sagen fast 90 Prozent der Vorstände börsennotierter Unternehmen, dass ihre Aufsichtsräte regelmäßig über Cyber-Sicherheitsthemen diskutieren und Informationen von einer Reihe von Mitgliedern des Managementteams erhalten. Dennoch ist eine beträchtliche Anzahl von Vorständen der Meinung, dass bei ihren Organisationen in diesem Bereich noch Verbesserungsbedarf besteht. Auf die Frage nach der Qualität der Informationen, die der Vorstand dem oberen Management zur Verfügung stellt, wurden die Informationen über die Cyber-Sicherheit als am niedrigsten eingestuft, wobei fast ein Viertel der Vorstände börsennotierter Unternehmen angaben, dass sie mit der Qualität der Informationen, die das Management zur Cyber-Sicherheit zur Verfügung stellt, unzufrieden oder sehr unzufrieden seien. Weniger als 15 Prozent gaben an, dass sie mit der Qualität der erhaltenen Informationen sehr zufrieden waren, verglichen mit einer rund 64-prozentigen Zufriedenheitsrate bezüglich der Informationen über die finanzielle Performance.[32]

Die Befragten in der jüngsten Umfrage unter Vorstandsmitgliedern identifizierten mehrere Gründe für ihre Unzufriedenheit mit der Cyber-Sicherheitsberichterstattung des Managements:

- Schwierigkeiten bei der Verwendung der Informationen für ein Benchmarking der Performance, sowohl intern (zwischen den Geschäftseinheiten innerhalb der Organisation) als auch extern (mit Unternehmen derselben Branche);
- unzureichende Transparenz bezüglich der Leistung;
- Schwierigkeiten bei der Interpretation der Informationen.[33]

Cyber-Sicherheit und Cyber-Risiko-Analyse sind relativ neue Disziplinen – sicherlich viel weniger ausgereift als die Finanzanalyse – und es wird einige Zeit dauern, bis die Berichtspraktiken ausgereift sind. Nichtsdestotrotz sollten die Vorstandsmitglieder mit dem Management klare Erwartungen an das Format, die Häufigkeit und den Detaillierungsgrad der Cyber-Sicherheitsinformationen stellen, die sie erhalten möchten. Sie sollten darauf hinarbeiten, das Cyber-Risiko zum Bestandteil des finanziellen Risikos des Unternehmens zu machen, unabhängig davon, ob es sich dabei um Kosten für die Behebung von Schäden eines erfolgreichen Angriffs, indirekte Kosten als Folge der Nichtbetriebsfähigkeit, gestohlene Vermögenswerte, Strafen als Folge von Compliance-Verstößen oder Einbußen des Börsenwerts als Folge der beschädigten Reputation handelt. Bei der Prüfung von Berichten des Managements sollten die Vorstände auch bedenken, dass es eine inhärente Tendenz seitens des Managements geben könnte, den wahren Zustand des Risikoumfelds herunterzuspielen. Eine Studie ergab, dass 60 Prozent der IT-Mitarbeiter Cyber-Sicherheitsrisiken erst dann melden, wenn sie akut sind – und bestätigten, dass sie versuchen, negative Ergebnisse herauszufiltern.[34]

Im Anhang D und Anhang E finden Sie Beispiele für Cyber-Risiko-Reporting-Kennzahlen und Dashboards.

[31] Jody R. Westby, Carnegie Mellon University, *Governance of Enterprise Security: CyLab 2012 Report*, (Pittsburgh, PA: Carnegie Mellon University, 2012), Seite 7 und Seite 16.

[32] NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), Seite 28.

[33] Ibid.

[34] Sean Martin, *Cyber Security: 60 % of Techies Don't Tell Bosses About Breaches Unless It's Serious*, *International Business Times*, 16. Apr. 2014.

PRINZIP 4

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

Technologie integriert moderne Organisationen, unabhängig davon, ob die Mitarbeiter auf der anderen Seite des Flurs oder auf der anderen Seite der Welt arbeiten. Doch wie bereits angemerkt sind die Berichtsstrukturen und Entscheidungsprozesse in vielen Unternehmen ein Erbe des Silodenkens der Vergangenheit, als jede Abteilung und jeder Geschäftsbereich relativ eigenständig Entscheidungen treffen konnte, ohne die heutige digitale Interdependenz zu berücksichtigen. Die Vorstände sollten sich Zusicherungen vom Management einholen, dass diese digitalen Interdependenzen verstanden werden und ein unternehmensweiter Ansatz zur Cyber-Sicherheit, der ausreichende Ressourcen und Autorität zuweist, verfolgt wird.

Anhang F umreißt die Cyber-Sicherheitsressourcen deutscher staatlicher Organe/deutscher Behörden, die dem privaten Sektor zur Verfügung stehen. Die Geschäftsführung kann diese Übersicht nutzen, um in den Diskussionen mit dem Management zu überprüfen, wie die Organisation diese Ressourcen nutzt.
Anhang G enthält Überlegungen zum Aufbau einer Beziehung zum CISO/IT-Sicherheitsbeauftragten.

EU-Standards

Die EU hat Verordnungen und Richtlinien erlassen, die sich direkt auf die Risikopraktiken von Unternehmen im Bereich der Cyber-Sicherheit auswirken. Zwei davon haben einen hohen Einfluss auf die Unternehmenspraxis.

- Die Datenschutzgrundverordnung (DSGVO) der Europäischen Union, die am 25. Mai 2018 in Kraft getreten ist, ist ein bindender Leitfaden für Unternehmen, die über personenbezogene Daten verfügen, und dient als Maßnahme zum Schutz der Privatsphäre.
- Die europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (Directive on security of network and information systems, NIS Directive) setzt Cyber-Standards für Unternehmen durch, die Teil der kritischen europäischen und nationalen Infrastrukturen sind. Einige dieser Vorschriften sind oder werden in nationales Recht übersetzt, bevor sie in Kraft treten. Diese Regeln gelten nicht nur für Unternehmen, die europäischen Eignern gehören, sondern auch für ausländische Unternehmen, die in Europa tätig sind. Dies gilt auch für europäische Unternehmen, die beispielsweise in den USA oder China tätig sind. Sie müssen auch dort die örtlichen Vorschriften einhalten.

Rollen und Verantwortlichkeiten des oberen Managements

Obwohl jede Organisation über eine individuelle Managementstruktur mit unterschiedlichen Titeln, Rollen und Verantwortlichkeiten verfügt, ist es unerlässlich, dass die Unternehmen die Rollen und Verantwortlichkeiten der wichtigsten Führungskräfte klar festlegen, insbesondere wenn es um die Schaffung eines integrierten und organisationsübergreifenden Cyber-Risiko-Management-Teams geht. Eine Organisation könnte z. B. folgende Struktur- und Rollendefinitionen haben:

- Chief Risk Officer – Cyber-Risiko-Erkennung, -Prävention und -Minderung; Schulung und Kommunikation
- Chief Compliance (& Ethics) Officer – Grundsatzrichtlinienentwicklung und -durchsetzung; Schulung und Kommunikation; unternehmensinterne Ermittlungen
- Chief Legal Officer/General Counsel – Beobachtung der Gesetzes- und Regulierungslandschaft, Compliance, Richtlinien, Rechtsstreitigkeiten; unternehmensinterne Ermittlungen
- Chief Information Officer – technische Expertise
- Chief Privacy Officer – eingehende Kenntnis der Datenschutzgesetze und -regeln; Entwicklung und Durchsetzung von Richtlinien; Schulung und Kommunikation; Datenschutzaudits
- Datenschutzbeauftragter (Data Protection Officer)- juristische Person (mandatiert durch die DSGVO), betrachtet die Sicherheit aus einer juristischen und Compliance-Perspektive
- Informationssicherheitsbeauftragter (Chief Information Security Officer / IT Security Officer) – verantwortlich für die Sicherheit aller Informationen, nicht nur der digitalen Daten
- Legal Counsel – Outside Legal Counsel – externe Rechtshilfe bei Bedarf; Anwaltsgeheimnis; Ermittlungen; Vertretung gegenüber Behörden und Aufsichtsbehörden.

Ein integrierter Ansatz für Cyber-Risiko-Governance

Um im digitalen Zeitalter wettbewerbsfähig zu bleiben, kann ein Umdenken in Bezug auf traditionelle Geschäfts- und Governance-Strukturen erforderlich werden. Diese Modifikationen können zu Spannungen unter den Mitarbeitern führen, die sich mit den gewohnten, wenn auch möglicherweise überholten Mechanismen auskennen und wohlfühlen. Es muss darauf geachtet werden, dass die Mitarbeiter angemessen in solche Änderungen einbezogen werden, um möglichst alle „mitzunehmen" und ihre Unterstützung für erforderliche Änderungen und Anpassungen zu fördern.
Die Entwicklung von Geschäftsstrukturen, die moderne digitale Sicherheit berücksichtigen, kann die Privatsphäre der Mitarbeiter und die Produktivität des Unternehmens potenziell verbessern.
Ein Modell, das von vielen Unternehmen adaptiert wird, ist ein abteilungsübergreifender Ansatz, mit dessen Hilfe Informationen um den Input aus dem gesamten Spektrum der Organisation erweitert werden. Dies sollte dazu beitragen, eine Kultur der Cyber-Sicherheit sowohl für die Organisation als Ganze als auch für ihre Mitarbeiter zu schaffen. Erwägen Sie die folgenden Schritte bei der Umsetzung eines solchen unternehmensweiten Ansatzes:

1. Etablieren Sie die Verantwortung für Cyber-Risiken abteilungsübergreifend. Ein Senior Manager mit bereichsübergreifenden Befugnissen, wie der Chief Financial Officer, der Chief Risk Officer, der Chief Operating Officer oder eine ähnliche Funktion, sollte das Team leiten.
2. Ernennen Sie ein organisationsübergreifendes Cyber-Risiko-Management-Team. Alle wesentlichen betroffenen Abteilungen müssen vertreten sein, einschließlich Leiter der Geschäftsbereiche, Recht und Compliance, Finanzen, Datenschutz, Personal, IT und Risikomanagement (Siehe Auszug „Rollen und Verantwortlichkeiten des oberen Managements" Seite 21). Als wesentliches Ziel eines solchen organisationsübergreifenden Ansatzes stellen Sie sicher, dass es innerhalb der Organisation kein schwaches Glied und keine Ausnahmen im Bereich der Cyber-Sicherheit gibt. Die interne Revision sollte dabei unabhängig bleiben und nicht Teil dieses Teams sein.
3. Das Cyber-Risiko-Team muss eine vorausschauende, unternehmensweite Risikobewertung durchführen und dabei einen systematischen Rahmen verwenden, der die Komplexität des Cyber-Risikos berücksichtigt – einschließlich, aber nicht beschränkt auf die Identifizierung kritischer Daten („Kronjuwelen") und Prozesse sowie die Einhaltung gesetzlicher Vorschriften.
4. Bewerten Sie die aktuelle Bedrohungslandschaft und das Risikobild des Unternehmens. Dann legen Sie verbindlich die eigene Risikobereitschaft fest. Die Identifizierung potenzieller Risiken für die Organisation sowie des Schwellenwertes des akzeptierten Risikos wird dem Cyber-Risiko-Team helfen, zu beurteilen, welche Rahmenbedingungen oder Standards (z. B. der IT-Grundschutz des BSI) am besten zu ihrem Auftrag und ihren Zielen passen.
5. Beachten Sie , dass die Cyber-Sicherheitsvorschriften je nach anwendbarer Rechtsordnung stark variieren können (z. B. zwischen Staaten, Bundesländern, Sektoren oder Branchen). Wie in Prinzip 2 erwähnt, sollte das Management Ressourcen für die Erfüllung der Standards und Anforderungen bereitstellen, die für die Organisation gelten, zumal die Regierungen einiger Länder ihre Einflussnahme auf den Bereich der Cyber-Sicherheit massiv erweitern.
6. Entwickeln Sie einen unternehmensweiten Plan für Cyber-Risiko-Management und -Resilienz sowie eine interne Kommunikationsstrategie und führen Sie diese für alle Abteilungen und Geschäftseinheiten ein. Obwohl die Cyber-Sicherheit offensichtlich eine wesentliche IT-Komponente hat, müssen alle Beteiligten zur Entwicklung des Plans hinzugezogen werden und sich bei diesem „mitgenommen" fühlen, einschließlich der Rechts-, Prüfungs-, Risiko- und Compliance-Rollen. Die Prüfung des Plans sollte routinemäßig durchgeführt werden.
7. Entwickeln und verabschieden Sie ein Gesamtbudget für Cyber-Risiken mit ausreichenden Ressourcen, um den Bedürfnissen und der Risikobereitschaft der Organisation gerecht zu werden. Die Personalplanung sollte dem gravierenden Mangel an erfahrenen Cyber-Sicherheitsfachkräften Rechnung tragen und ermitteln, welche Anforderungen intern abgedeckt werden können und welche nicht. Da Cyber-Sicherheit mehr ist als IT-Sicherheit, sollte das Budget für Cyber-Sicherheit nicht ausschließlich an eine Abteilung gebunden sein: Zuteilungen können beispielsweise auch an Bereiche wie Mitarbeiterschulung, die Beobachtung gesetzlicher Vorschriften, Öffentlichkeitsarbeit, Produktentwicklung und Lieferantenmanagement gehen.
8. Entwickeln Sie gemeinsam Berichte für den Vorstand. Von den Führungskräften sollte erwartet werden, dass sie Kennzahlen zur Quantifizierung der geschäftlichen Auswirkungen von Cyber-Bedrohungen und der damit verbundenen Aktivitäten im Risikomanagement verfolgen und darüber Bericht erstatten. Die Bewertung der Effektivität des Cyber-Risiko-Managements und der Cyber-Resilienz des Unternehmens sollte im Rahmen von vierteljährlichen internen Audits und anderen Leistungsüberprüfungen erfolgen. Diese Berichte sollten die richtige Balance zwischen zu vielen Details und dem, was für die Berichterstattung an den Aufsichtsrat strategisch wichtig ist, finden.

Quelle: Internet Security Alliance.

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

BSI-Standards und IT-Grundschutz

Der IT-Grundschutz des BSI ist eine bewährte Methodik, um das Niveau der Informationssicherheit in Behörden und Unternehmen jeder Größenordnung zu erhöhen. Die Angebote des IT-Grundschutzes gelten in Verwaltung und Wirtschaft als Maßstab, wenn es um die Absicherung von Informationen und den Aufbau eines Managementsystems für Informationssicherheit (ISMS) geht. Der IT-Grundschutz ist kompatibel zu ISO/IEC 27001.

Die BSI-Standards enthalten Methoden und Vorgehensweisen zu den unterschiedlichsten Themen aus dem Bereich der Informationssicherheit. Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein ISMS. Mit dem BSI-Standard 200-2 zur IT-Grundschutz-Methodik kann ein solides ISMS aufgebaut werden. Der BSI-Standard 200-3 zum Risikomanagement enthält alle risikobezogenen Arbeitsschritte zur Umsetzung des IT-Grundschutzes (siehe auch Appendix F). Das begleitende IT-Grundschutz-Kompendium, die modernisierte Fassung der IT-Grundschutz-Kataloge, enthält die so genannten IT-Grundschutz-Bausteine, in denen jeweils Gefährdungen und Sicherheitsanforderungen für ein Thema der Informationssicherheit erläutert werden. Mit den Bausteinen erhalten Anwender konkrete Empfehlungen zur Umsetzung der IT-Grundschutz-Methodik.

Aufsichtsratsmitglieder sollten die Erwartung äußern, dass das Management die BSI-Standards bei der Entwicklung der Cyber-Risiko-Abwehr- und -Reaktionspläne des Unternehmens berücksichtigt. Auf diese Weise kann die Geschäftsleitung sicherstellen, dass ihre Organisation ein angemessenes Basis-Niveau für die Cyber-Sicherheit schafft. Die Verwendung der BSI-Standards bedeutet für ein Unternehmen keine absolute Cyber-Sicherheit, ebenso wenig wie die Konformität mit anderen Frameworks oder Vorschriften. Die Realisierung eines Basis-Niveaus für Informationssicherheit hilft Organisationen jedoch dabei, herauszufinden, was ihre Ausgangslage im Bezug auf Cyber-Sicherheit ist, wie Cyber-Sicherheit ihren individuellen Geschäftsanforderungen gerecht werden kann und wo Verbesserungsbedarf besteht. Aufsichtsratsmitglieder müssen sich darüber im Klaren sein, dass die Implementierung von Rahmenbedingungen keine einmalige Tätigkeit ist, sondern eine kontinuierliche Überwachung, Bewertung und Anwendung der Standards erfordert, um angemessen und schnell auf eine sich ändernde Bedrohungslage reagieren zu können.

PRINZIP 5

In der Diskussion der Unternehmensleitung über Cyber-Risiken sollte geklärt werden, welche Risiken vermieden, welche akzeptiert und welche über Versicherungen gemindert oder verteilt werden sollen – und welche spezifischen Maßnahmen mit jeder dieser Varianten einhergehen sollten.

Absolute Cyber-Sicherheit ist ein unrealistisches Ziel. Cyber-Sicherheit – wie die Sicherheit im Allgemeinen – ist ein Prozess, kein Endzustand, und Sicherheit ist nicht gleichbedeutend mit Compliance. Managementteams müssen herausfinden, wo nach ihrer Ansicht die Abläufe und Kontrollen des Unternehmens in Bezug auf ein Risikospektrum optimiert werden sollten. Wie in anderen Risikobereichen auch muss die Cyber-Risikotoleranz einer Organisation mit der Geschäftsstrategie und den Geschäftszielen übereinstimmen. Die Ressourcenallokation im Bereich Cyber-Sicherheit ist eine Funktion des Ausgleichs von Geschäftszielen mit den inhärenten Risiken digitaler Systeme (siehe „Risikobereitschaft definieren", Seite 25). Es gibt vielfältige Cyber-Risiken und verschiedene Methoden, sie zu bekämpfen. Das Management muss dem Vorstand ein klares Bild der Risikolandschaft in Bezug auf die Unternehmenswertschöpfung und einen Plan zur Adressierung dieser Risiken vorlegen. Vorstände und Managementteams werden sich mit folgenden Fragen auseinandersetzen müssen:

- **Bei welchen Daten und Informationen, Systemen und Geschäftsabläufen sind wir bereit, ihren Verlust oder ihre Beschädigung zu akzeptieren?** Diskussionen über Risikotoleranz werden dazu beitragen, das Ausmaß des Cyber-Risikos zu ermitteln, das die Organisation bereit ist, im Rahmen pragmatischer geschäftlicher Überlegungen zu akzeptieren. In diesem Zusammenhang ist die Unterscheidung zwischen unternehmenskritischen Assets (siehe „Identifizierung der Kronjuwelen des Unternehmens", Seite 12) und anderen Daten oder Systemen, die zwar ähnlich wichtig, aber weniger essenziell sind, ein wichtiger erster Schritt. Das Kompromittieren von Daten und Informationen ist jedoch nicht die einzige Herausforderung bei der Betrachtung des Cyber-Risikos. Es können rechtliche Risiken bestehen, die höhere Schäden als den reinen Datenverlust erzeugen; Imageschädigungen durch negative Berichterstattung in den Medien beispielsweise kann als weiterer kostenerhöhender Faktor hinzukommen.
- **Wie sollten unsere Investitionen zur Cyber-Risikominderung auf grundlegende und fortgeschrittene Schutzmaßnahmen aufgeteilt werden?** Bei der Überlegung, wie man komplexeren Bedrohungen begegnen kann, sollte das Management sowohl technisch als auch organisatorisch den größten Wert auf ausgefeilte Abwehrmechanismen legen, die so konzipiert sind, dass sie die wichtigsten Daten und Systeme des Unternehmens schützen. Während die meisten Unternehmen dem prinzipiell zustimmen würden, wenden viele Unternehmen in der Realität die gleichen Sicherheitsmaßnahmen auf alle Daten und Systemfunktionen gleichermaßen an. Die Erfahrung zeigt jedoch, dass der Schutz von Systemen und Daten von geringer Bedeutung vor komplexen Bedrohungen größere Investitionen erfordern könnte, als es der Nutzen rechtfertigt. Für Informationen mit geringerer Priorität sollten Unternehmen in Erwägung ziehen, ein höheres Cyber-Sicherheitsrisiko als für Informationen mit höherer Priorität zu akzeptieren oder stattdessen die Auswirkungen solcher Risiken auf Versicherungen zu übertragen.[35] Die Vorstände sollten das Management dazu ermutigen, die Cyber-Sicherheitsrisiken und Investitionen des Unternehmens in Bezug auf ihre Wirtschaftlichkeit zu bewerten und regelmäßig zu überprüfen. Aktuell sind neue Analyseinstrumente auf den Markt gekommen, die das Management dabei unterstützen können, das Cyber-Risiko in wirtschaftlicher Hinsicht besser zu definieren. Das Management sollte gleichzeitig prüfen, ob diese Instrumente für die Berechnung des Cyber-Risikos geeignet sind.[36]
- **Welche Optionen stehen zur Verfügung, um uns bei der Minderung bestimmter Cyber-Risiken zu unterstützen?** Unternehmen aller Branchen und Größen haben Zugang zu Komplettlösungen, die helfen können, einen Teil des Cyber-Risikos zu reduzieren. Dazu gehört eine Reihe von Präventivmaßnahmen wie die Anlehnung an Cyber-Sicherheits-Frameworks und Governance-Praktiken, Mitarbeiterschulungen sowie Responsedienstleistungen und Beratung. Über die Deckung von finanziellen Verlusten hinaus können diese Werkzeuge dazu beitragen, das Risiko einer Organisation zu reduzieren, Sach- und Personenschäden zum Opfer zu fallen, die durch einen Cyber-Vorfall verursacht werden. Einige Lösungen beinhalten auch den Zugriff auf proaktive Methoden. Die Einbeziehung dieser Mehrwertdienste beweist einmal mehr, wie wichtig es ist, die Cyber-Sicherheitsgovernance außerhalb der IT-Abteilung in unternehmensweite Risiko- und Strategiediskussionen auf Management- und Vorstandsebene zu verlagern. Allerdings muss das Management den Vorstand über die sich rasch verändernde Cyber-Risikolandschaft auf

[35] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, Oktober 2013, Seite 8.

[36] Beispiele für Analysetools kommen u.a. von Secure System Innovations Corp und X-Analytics sowie vom FAIR Institute, um nur einige zu nennen. Außerdem verweist AIG im Executive Summary Report vom 12. Dezember 2017 auf ihre patentierte Methode zur Messung und Modellierung von Cyber-Risiken in wirtschaftlicher Hinsicht, die sie im Underwriting-Prozess verwenden.

dem Laufenden halten und agil genug sein, um sich auf schnell wechselnde Technologien und Cyber-Angriffsszenarien wie Datendiebstahl, Datenkorruption und sogar den Einsatz von Sicherheitsmechanismen (Verschlüsselung) als Angriffsmethoden (Ransomware) einzustellen.

- **Welche Optionen stehen zur Verfügung, um uns bei der Übertragung bestimmter Cyber-Risiken zu unterstützen?** Eine Cyber-Versicherung ermöglicht die finanzielle Erstattung von unerwarteten Verlusten im Zusammenhang mit Cyber-Vorfällen. Dazu kann die versehentliche Offenlegung von Daten gehören, wie der Verlust eines unverschlüsselten Laptops, oder böswillige externe Angriffe, wie Phishing, Malware-Infektionen oder Denial-of-Service-Angriffe. Bei der Wahl eines Cyber-Versicherungspartners ist es für eine Organisation wichtig, einen Versicherer zu wählen, der am besten zu den Bedürfnissen der Organisation passt, sei es ein erfahrener, breit aufgestellter internationaler Anbieter oder ein kleines Versicherungsunternehmen aus der jeweiligen Region. Versicherer führen während des Underwriting-Prozesses häufig eingehende Überprüfungen der eingesetzten Cyber-Sicherheitsrahmenwerke von Unternehmen durch. Die Preisgestaltung von Verträgen kann ein starkes Signal sein, das Unternehmen dabei unterstützt, ihre Stärken und Schwächen im Bereich der Cyber-Sicherheit zu verstehen. Wenn ein Unternehmen Informationen mit seinem Versicherer teilt, kann es gemeinsam ein kosteneffizientes Programm zur Bewältigung des Cyber-Risikos entwickeln. Viele Versicherer bieten über Partnerschaften mit Technologieunternehmen, Anwaltskanzleien, Public-Relations-Firmen und anderen Unternehmen auch Zugang zu den oben beschriebenen Präventiv- und Notfallmaßnahmen an. Cyber-Risiken können auch durch Outsourcing-Optionen übertragen werden; Beschaffungsverträge sollten eine klare Sprache über die Risikominimierung und Akzeptanz durch den Technologiepartner sowie Vertragsstrafen für Verstöße enthalten, die bereits weiter oben besprochen wurden.
- **Wie sollten wir die Auswirkungen von Cyber-Sicherheitsvorfällen bewerten?** Die Durchführung einer ordnungsgemäßen Folgenabschätzung kann angesichts der Vielzahl von Faktoren, inklusive der unvorhergesehenen Risiken, die das Management nicht abgeschätzt hat, eine Herausforderung darstellen. In einer vernetzten Welt gibt es Cyber-Risiken für die Organisation, die außerhalb der internen Absicherungsfähigkeiten ebendieser liegen – diese gilt es, direkt und effektiv zu mindern. So kann beispielsweise die öffentliche Berichterstattung über einen Datenvorfall den Prozess der Risikobewertung erheblich erschweren. Stakeholder – darunter Mitarbeiter, Kunden, Lieferanten, Investoren, die Presse, die Öffentlichkeit und Regierungsstellen – vermögen es kaum, einen Unterschied zwischen einem vergleichsweise kleinen und einem großen und gefährlichen Verstoß festzustellen. In der Folge entstehende Reputationsschäden und die damit verbundenen Auswirkungen (z. B. die Reaktionen von Medien, Investoren und anderen wichtigen Stakeholdern) können schwerwiegender sein, als es die tatsächliche Schwere des Angriffs rechtfertigt. Der Vorstand sollte sich die Zusicherung einholen, dass das Management diese Implikationen sorgfältig durchdacht hat, indem es organisatorische Strategien für das Cyber-Risiko-Management entwickelt hat. Dazu gehört beispielsweise ein operatives IT-Management, das Strategien für rechtliche Vereinbarungen mit Partnern und Anbietern gewährleistet, die eine angemessene Cyber-Sicherheit sicherstellen und die Kommunikationspläne zur Bewältigung des Image-Risikos bei Eintreten eines Ereignisses umfassen.

Risikobereitschaft definieren

Risikobereitschaft ist die Höhe des Risikos, das eine Organisation bereit ist, bei der Verfolgung seiner strategischen Ziele einzugehen. Daher sollte sie einen Risiko-Schwellenwert festlegen, ab welchem geeignete Maßnahmen ergriffen werden müssen, um das Risiko auf ein akzeptables Maß zu reduzieren. Wenn die Risikobereitschaft richtig definiert und kommuniziert ist, bestimmt sie das Verhalten, indem klare Grenzen für Geschäftspraktiken und die Nutzung von Marktchancen gesetzt werden.
Eine Diskussion über die Risikobereitschaft sollte sich mit folgenden Fragen befassen:

- Unternehmenswerte – Welche Risiken gehen wir nicht ein?
- Strategie – Welche Risiken müssen wir eingehen?
- Stakeholder – Welche Risiken sind wir bereit, zu tragen, und auf welcher Ebene?
- Kapazität – Welche Ressourcen werden benötigt, um diese Risiken zu managen?

„Die Risikobereitschaft ist eine Frage der Beurteilung, die auf den spezifischen Gegebenheiten und Zielen des jeweiligen Unternehmens basiert. Es gibt keine Einheitslösung."

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

Fazit

Cyber-Sicherheit ist ein ernstzunehmendes Risiko-Management-Thema, das praktisch alle Ebenen der betrieblichen Aktivitäten eines Unternehmens betrifft. Mehrere Merkmale machen dieses Risiko besonders schwerwiegend: die Komplexität und die Geschwindigkeit der Weiterentwicklung, das Potenzial für erheblichen finanziellen Schaden, Wettbewerbs- und Reputationsschäden und die Tatsache, dass vollständiger Schutz nicht zu erreichen bzw. ein unrealistisches Ziel ist. Angesichts dieser Bedrohungen und trotz der dramatischen Zunahme der Ausgaben für Cyber-Sicherheit im privaten Sektor [37] sind Angreifer nach wie vor begünstigt. Darüber hinaus sind viele Geschäftsinnovationen mit vermehrten Sicherheitsbedrohungen verbunden, und Risikomanagement im Allgemeinen – insbesondere IT- und cyberbezogene Sicherheitsmaßnahmen – werden traditionell als Kostenstelle in den meisten gewinnorientierten Unternehmen angesehen.

Aufsichtsräte müssen ihre Fähigkeit, das Thema Cyber-Sicherheit zu adressieren, kontinuierlich überprüfen, sowohl im Hinblick auf ihre eigene treuhänderische Verantwortung als auch auf ihre Aufsicht über die Aktivitäten des Managements, und viele werden Lücken und Verbesserungsmöglichkeiten erkennen. Während die Ansätze der einzelnen Gremien unterschiedlich sein werden, bieten die Prinzipien in diesem Handbuch Vergleichswerte und Anhaltspunkte. Die Gremien sollten versuchen, das Cyber-Risiko aus unternehmensweiter Sicht zu betrachten:

- Verstehen Sie selbst die rechtlichen Konsequenzen für das Unternehmen und den Vorstand.
- Stellen Sie sicher, dass die Vorstände über genügend Zeit auf der Tagesordnung und Zugang zu Experteninformationen verfügen, um gut informierte Gespräche mit dem Management führen zu können.
- Integrieren Sie Cyber-Risiko-Diskussionen in die Diskussionen zur Gesamtrisikotoleranz des Unternehmens.

„Cyber-Sicherheit ist ein Problem von Menschen“, [38] wie es ein Vorstand formulierte. Die Aufgabe des Aufsichtsrates besteht darin, dem Management wirksame Leitlinien an die Hand zu geben und sicherzustellen, dass die Cyber-Sicherheitsstrategie des Unternehmens angemessen konzipiert und ausreichend belastbar ist. Dabei gilt es, die strategischen Voraussetzungen und die Realitäten des Geschäftsökosystems, in dem das Unternehmen tätig ist, zu berücksichtigen.

[37] Steve Morgan, “Worldwide Cybersecurity Spending Increasing to $170 Billion by 2020,” Forbes, Mar. 9, 2016. See also Piers Wilson, Security market trends and predictions from the 2015 member survey, Institute of Information Security Professionals.
[38] NACD, et al., Cybersecurity: Boardroom Implications (Washington, DC: NACD, 2014) (an NACD white paper), p.7.

ANHANG A

Fragen, die sich Vorstände stellen können, um die eigene „Cyber-Expertise“ einzuschätzen

Schon vor einer Vorstandssitzung ist es ratsam, zur eigenen Selbsteinschätzung verschiedene Aspekte der Cyber-Sicherheit betrachtet zu haben, die über die technischen und betrieblichen Aspekte hinausgehen. Insbesondere sollten die Vorstände über Cyber-Sicherheit in geschäftlicher Hinsicht nachdenken und auch darüber, wie sie ihre Organisation auf strategischer Ebene angemessen vorbereiten.

1. Fördert der Geschäftsführer den offenen Zugang des Vorstands zu Informationen über neue Cyber-Bedrohungen, u. a. durch externe Berichte und Informationen aus dem Management?
2. Diskutieren wir das Cyber-Risiko in den Vorstandssitzungen regelmäßig? Erhalten wir Kennzahlen, die zeigen, wo wir in Bezug auf Cyber-Resilienz und Bedrohung stehen?
3. Was halten wir für unsere wertvollsten Betriebsgeheimnisse? Wie interagieren unsere IT-Systeme mit diesen Assets?
4. Glauben wir, dass es einen ausreichenden Schutz gibt, wenn jemand an unsere „Kronjuwelen“ herankommen oder sie kompromittieren will? Was braucht es, um sicher zu sein, dass diese Vermögenswerte geschützt sind?
5. Berücksichtigen wir die Cyber-Sicherheitsaspekte bei unseren wichtigsten Geschäftsentscheidungen wie Fusionen und Übernahmen, Partnerschaften und Produktneueinführungen?
6. Geben wir an den richtigen Stellen Geld für Cyber-Sicherheitslösungen und Schulungen aus? Wissen wir, ob unsere Ausgaben kosteneffektiv sind?
7. Wer ist für unsere Cyber-Sicherheit verantwortlich? An wen richtet sich die Berichterstattung über die Cyber-Sicherheit? Gibt es genügend gegenseitige Kontrollen? Haben wir die richtigen Personen und klare Kommunikationswege/Verantwortlichkeiten für die Cyber-Sicherheit? Kenne ich die Person in meinem Unternehmen, die für Cyber-Sicherheit (IT-Sicherheitsbeauftragter, CISO) zuständig ist?
8. Sind Cyber-Risiken in unserem Risikoregister enthalten?[39]
9. Haben wir uns Gedanken darüber gemacht, wie wir unsere Unternehmenskommunikation im Falle eines Ereignisses handhaben würden, einschließlich der Kommunikation mit der Öffentlichkeit, unseren Kunden, unseren Aktionären, unseren Aufsichtsbehörden, unseren Rating-Agenturen? Haben wir Kommunikationsstrategien für jede dieser Zielgruppen? Und was ist mit einer Cyber-Krise? Haben wir den Ernstfall geprobt und sind ausreichend dafür vorbereitet?
10. Sind wir in einer der Organisationen für Cyber-Sicherheit und den Austausch von Sicherheitsinformationen für den öffentlichen oder privaten Sektor aktiv? Sollten wir es sein?
11. Überwacht die Organisation adäquat die aktuelle und zukünftige Gesetzgebung und Regulierung im Bereich der Cyber-Sicherheit?[40]
12. Verfügt das Unternehmen über eine ausreichende Versicherung, eine Cyber-Versicherung, Directors-and-Officers-Versicherung (Organhaftpflicht), die Cyber-Events abdeckt? Was genau ist versichert und bis zu welchem Höchstbetrag?[41] Gibt es Vorteile, die eine Versicherungslösung bringt, die über den reinen Risikotransfer hinausgehen?[42]
13. Haben wir genügend Cyber-Experten in unserem Team? Tun wir genug, um die Entwicklung von Arbeitskräften im Bereich der Cyber-Sicherheit zu fördern?

[39] Lexology.com, Ed Batts, DLA Piper LLP, Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members, 23. Jan. 2014.

[40] Ibid.

[41] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, Board Oversight.

[42] Ibid.

ANHANG B

Fragen des Vorstandes zum Thema Cyber-Sicherheit an das Management

Beobachtung der IT-Sicherheitslage

1. Wissen wir als Vorstand, wo wir in Bezug auf die Cyber-Sicherheitslage stehen? Wurden wir über bereits aufgetretene Cyber-Angriffe informiert und darüber, wie schwerwiegend sie waren? Hat das Unternehmen diese Vorfälle selbst festgestellt?
2. Was sind die Cyber-Sicherheitsrisiken des Unternehmens und wie geht das Unternehmen mit diesen Risiken um?[43] Was sind unsere Strategien zur Schadenbegrenzung?
3. Haben wir unsere kritischsten digitalen Assets identifiziert – unsere digitalen „Kronjuwelen"? Verfügen wir über ein angemessenes Situationsbewusstsein für die Bedrohungen dieser Vermögenswerte?
4. Wie werden wir wissen, ob wir gehackt wurden, und wie können wir sicherstellen, dass wir dies herausfinden werden?
5. Wer sind unsere wahrscheinlichen Angreifer?[44] Welche dieser Angreifer haben die nötigen Fähigkeiten, uns zu schaden?
6. Was ist nach Ansicht des Managements die schwerwiegendste Schwachstelle im Zusammenhang mit der Cyber-Sicherheit (innerhalb unserer IT-Systeme, unseres Personals oder unserer Prozesse)? Welche zusätzlichen Schwachstellen gibt es?
7. Wenn ein Angreifer unserem Unternehmen den größtmöglichen Schaden zufügen wollte, wie würde er das tun? Haben wir verschiedene Szenarien durchgespielt, einen Minimum-/Maximum-Schadenangriff oder einen Komplettausfall des Systems? Wo würde es uns am meisten treffen?
   a. Fragen Sie das Management nach spezifischen Geschäftsszenarien. Dies sollte mehrere Teile umfassen:
      i. Vorgehen der IT-Abteilung.
      ii. Geschäftsstrategien zur Bewältigung des Vorfalls, nachdem die IT-Abteilung auf den Vorfall reagiert hat.
8. Hat das Unternehmen die potenziellen Risiken für menschliches Versagen bewertet?[45]
9. Wie lassen wir unser Sicherheitssystem auf Schwachstellen testen? Wann haben wir das letzte Mal diese unabhängigen und externen Bewertungen durchgeführt? Was waren die wichtigsten Ergebnisse und wie gehen wir damit um? Wie hoch ist unser Reifegrad?
10. Weist unser Revisor darauf hin, dass wir bei den internen Kontrollen des Unternehmens für die Finanzberichterstattung Mängel im Zusammenhang mit der Cyber-Sicherheit haben? Wenn ja, welches sind sie, und was tun wir, um diese Mängel zu beheben?
11. Haben wir erwogen, eine unabhängige, externe Bewertung unseres Cyber-Sicherheitsrisikomanagementprogramms zu beauftragen?

Strategie und Betrieb

1. Was sind die bewährten Herangehensweisen für Cyber-Sicherheit, und inwiefern unterscheiden diese sich von unserem Vorgehen?
2. Haben wir entsprechend differenzierte Strategien für die allgemeine Cyber-Sicherheit und den Schutz unserer unternehmenskritischen Assets?
3. Verfügen wir über ein unternehmensweites, unabhängig budgetiertes Cyber-Risiko-Management-Team? Ist das Budget ausreichend? Wie ist es in den gesamten Risiko-Management-Prozess des Unternehmens integriert?
4. Nutzen wir eine systematische Vorgehensweise, auf Basis von ISO 27000 oder des IT-Grundschutzes des BSI, um die Cyber-Sicherheit anzugehen und eine angemessene Cyber-Sicherheitshygiene zu gewährleisten?
5. Wenn Sie zusätzliche XXX Euro hätten, wo würden Sie diese zusätzlichen finanziellen Mittel ausgeben?
6. Verfügen die ausgelagerten Anbieter und Auftragnehmer des Unternehmens über Cyber-Sicherheitskontrollen und -richtlinien? Werden diese Kontrollen überwacht? Stimmen diese Richtlinien mit den Erwartungen unseres Unternehmens überein?
7. Hat die Firma eine Cyber-Versicherung? Wenn ja, ist sie angemessen?
8. Gibt es ein laufendes, unternehmensweites Schulungsprogramm zum Thema Cyber-Sicherheit?
9. Ist unser Sicherheitsteam an den strategischen Entscheidungen zur Einführung neuer Technologien beteiligt? Wie wird Sicherheit in Geschäftsprozesse und Produkte sowie in das Design und den Lebenszyklus integriert? Sind wir uns der potenziellen Risiken und Chancen für unser Unternehmen im Bereich der neuen Technologien bewusst?
10. Wie gehen wir mit den Sicherheitslücken um, die eine zunehmend „mobile" Belegschaft aufweist?

[43] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, Board Oversight.

[44] Lexology.com, Ed Batts, DLA Piper LLP, "Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members," Jan. 23, 2014.

[45] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, Board Oversight.

Faktor „Mensch“

1. Wie können Mitarbeiter durch unbeabsichtigtes menschliches Versagen zu Bedrohungen werden, auch wenn sie mit den besten Absichten handeln?
2. Was sind die erfolgreichsten Methoden zur Bekämpfung menschlichen Versagens, und wie unterscheiden sich unsere Methoden davon?
3. Wie arbeiten die Schlüsselfunktionen (IT, HR, Datenschutzbeauftragter, Recht, Compliance und Geschäftsleitung) mit den Geschäftseinheiten zusammen, um eine Kultur des Cyber-Risikobewusstseins und der Eigenverantwortung für die Cyber-Sicherheit zu etablieren? Zu den Überlegungen gehören unter anderem:
   a. Schriftliche Richtlinien, die Daten, Systeme und mobile Geräte abdecken und für alle Mitarbeiter gelten.
   b. Schaffung eines Vertrauensumfelds für die Meldung von Cyber-Ereignissen (z. B. Meldung versehentlich verursachter Probleme durch Mitarbeiter).
   c. Regelmäßige Schulungen zur Umsetzung der Cyber-Sicherheitsrichtlinien des Unternehmens und zur Erkennung von Bedrohungen.
   d. Konsultation mit den Betriebsräten darüber, wie man die Sicherheitsmaßnahmen am besten anwendet.
4. Wie haben wir unsere Personalpolitik an die Cyber-Sicherheit angepasst, Eingangsschulung für neue Mitarbeiter, Schulungen im Zusammenhang mit Abteilungs-/Rollenwechseln, Mitarbeiteraustritte u. Ä.? Gibt es Einschränkungen bei den Zugangsrechten, die auf Rollen und Verantwortlichkeiten beruhen?
5. Wie können unsere operativen Kontrollen, einschließlich Zugriffsbeschränkungen, Verschlüsselung, Datensicherung, Überwachung des Netzwerkverkehrs usw. zum Schutz vor unbeabsichtigten menschlichen Fehlern beitragen?

Lieferketten-/Drittanbieter-Risiken

1. Haben wir derzeit eine Bestandsaufnahme unserer Lieferanten und Drittanbieter und einen Prozess, um die Liste auf dem neuesten Stand zu halten? Wie organisieren wir die Übersicht derjenigen, die uns beliefern? Priorisieren wir unsere Sicherheit auf der Grundlage der potenziellen Risiko-Exponierung des Lieferanten, der Größe und des Verhältnisses zu unseren wertvollsten Daten?
2. Verfügen wir über ein Managementsystem, das Cyber-Sicherheit vollständig in unser Lieferketten-Risikomanagement einbezieht?
3. Wie viel Transparenz haben wir derzeit in unserer gesamten Lieferkette in Bezug auf Cyber-Risiko-Exponierung und -Kontrollen? Welche Abteilungen/Geschäftsbereiche sind involviert?
4. Wie können wir die finanziellen Vorteile (niedrigere Kosten, höhere Effizienz usw.), die sich aus einer größeren Flexibilität der Lieferkette ergeben, gegen potenziell höhere Cyber-Risiken abwägen?

Nach einem Cyber-Sicherheitsvorfall

1. Wie haben wir von dem Vorfall erfahren? Wurden wir von einer externen Partei benachrichtigt oder wurde der Vorfall intern entdeckt?
2. Hätte der Informationsaustausch mit unseren Partnern den Vorfall verhindern können? Warum haben unsere Partner uns nicht dabei unterstützt, unsere Abwehr besser vorzubereiten?
3. Was, glauben wir, wurde gestohlen, kopiert, modifiziert oder verändert?
4. Wie ist unsere Organisation und/oder wie sind andere von dem Vorfall betroffen?
5. Was können wir tun, um die durch den Vorfall verursachten Schäden zu mindern?
6. Haben wir eine Versicherung zur Erstattung von Benachrichtigungskosten?
7. Wurden unsere Geschäftsaktivitäten beeinträchtigt sind Partner oder weitere Geschäftsbeziehungen betroffen?
8. Ist unser Cyber-Vorfall-Reaktionsplan aktiv und funktioniert er wie geplant?
9. Was unternimmt das Vorfall-Team, um sicherzustellen, dass der Vorfall unter Kontrolle ist und der Hacker keinen Zugriff mehr auf unser internes Netzwerk hat?
10. Glauben wir, dass der Hacker ein interner oder externer Akteur war? Wurde dem Hacker von innen heraus geholfen?
11. Welche Schwachstellen in unserem System haben es ermöglicht, dass der Cyber-Sicherheitsvorfall eintrat (und warum)?
12. Welche Schritte können wir unternehmen, um sicherzustellen, dass sich solche Vorfälle nicht wiederholen? Was sind die Lehren aus diesem Vorfall? Was ist unsere Richtlinie für den Austausch von Informationen über Vorfälle, sowohl intern als auch extern?

Quelle: NACD, löschen et al., Cybersecurity: Boardroom Implications (Washington, DC: NACD, 2014) (ein NACD Whitepaper).

   a. Werden wir angemessen gegen Sicherheitsvorfälle unserer Lieferanten abgesichert?
   b. Können wir eine Cyber-Versicherung für einen Lieferanten zwingend vorschreiben?
5. Wie werden Cyber-Sicherheitsanforderungen in Verträgen und Service-Level-Agreements integriert? Wie werden sie überwacht, und führen wir unsere Due Diligence zur Durchsetzung von Verträgen durch? Verträge und Service-Level-Agreements können so geschrieben werden, dass sie Anforderungen für die folgenden Bereiche enthalten:
   a. Schriftliche Richtlinien zur Cyber-Sicherheit; Einhaltung gesetzlicher Vorschriften (DSGVO, NIS)
   b. Personalanforderungen, wie Personenüberprüfungen und Schulungen
   c. Zugangskontrollen
   d. Verschlüsselungs-, Backup- und Wiederherstellungsrichtlinien
   e. Sekundärzugriff auf Daten
   f. Länder, in denen Daten gespeichert werden müssen
   g. Benachrichtigung über Datenverstöße oder andere Cyber-Ereignisse
   h. Cyber-Vorfall-Planungen/Notfallpläne
   i. Audits von Cyber-Sicherheitspraktiken und/oder regelmäßige Konformitätsbescheinigungen
6. Wie schwierig und kostenintensiv wird es sein, eine funktionierende Schwachstellen- und Verwundbarkeitsanalyse bzw. relevante Testsysteme für unsere Lieferkette einzurichten und aufrechtzuerhalten?
7. Bringen unsere Lieferantenvereinbarungen neue rechtliche Risiken mit sich oder generieren sie zusätzliche Compliance-Anforderungen? Haben wir alle anwendbaren Gesetze, wie sektor- oder branchenspezifische Gesetze und Verordnungen, berücksichtigt?
8. Wie gehen wir mit den Datenschutzbestimmungen um, wenn wir Daten aus Europa in ein anderes Land übertragen?

Reaktion auf Vorfälle (Incident Response)

1. Wie sind wir in der Lage, Vorfälle zu erkennen?
2. Wie schnell können wir auf einen Vorfall reagieren?
3. Wen müssen wir benachrichtigen und wann? Wie sieht der Zeitplan für die Meldung von Vorfällen an die Verbraucher aus? Aufsichtsbehörden? Lieferanten/Partner? Intern? Mitbewerber? Wie kontaktieren wir diejenigen, die wir benachrichtigen müssen?
4. Wie werden Investoren Cyber-Sicherheitsvorfälle mitgeteilt und welche Kriterien werden für diese Offenlegungen herangezogen?
5. Wie sieht unsere Richtlinie für die Meldung von Vorfällen an den Vorstand aus und zu welchem Zeitpunkt sollte der Vorstand über einen Vorfall informiert werden?
6. Unter welchen Umständen werden Strafverfolgungsbehörden und andere relevante Regierungsstellen benachrichtigt?[46]
7. Wie wird das Management auf einen Cyber-Angriff reagieren?[47] Testen wir unsere Pläne zur Cyber-Abwehrbereitschaft und -reaktion adäquat?
8. Haben wir den Krisenmanagementplan geübt und getestet?
9. Wie sieht unsere Kommunikations- und PR-Strategie für eine Cyber-Krise aus?
10. Was tun wir, um zu vermeiden, dass das Problem für unsere Organisation noch schlimmer wird? Ziehen wir rechtlichen Beistand hinzu? Ist unser Rechtsbeistand auf den Empfang solcher Mitteilungen vorbereitet?

Benachrichtigen von externen Parteien

Zusätzlich zu den externen Beratern sollten Vorstände und Managementteams darüber nachdenken, ob sie folgende Parteien unterrichten sollten:

- unabhängige forensische Ermittler.
- den Versicherer des Unternehmens.
- die externe Wirtschaftsprüfungsgesellschaft des Unternehmens.
- Krisenkommunikationsberater.
- Strafverfolgungsbehörden.
- öffentliche Stellen (z. B. BSI).
- Computer Emergency Response Team (CERT).

Adaptiert aus Jody Westby's post in Forbes.com, Don't Be a Cyber Target: A Primer for Boards and Senior Management, 20. Jan. 2014.

[46] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, *Board Oversight.*
[47] Ibid.

ANHANG C

Überlegungen zur Cyber-Sicherheit bei Fusionen und Übernahmen

Unternehmen, die andere Unternehmen übernehmen oder mit ihnen fusionieren, übernehmen gleichzeitig mit diesem Schritt auch die Cyber-Risikolage der Zielgesellschaft. Aus diesem Grund muss die übernehmende Gesellschaft noch vor Abschluss der Transaktion eine sorgfältige Prüfung durchführen und zudem bereit sein, diese Risiken nach Abschluss der Transaktion zu mindern. Ebenso besteht die Wahrscheinlichkeit, dass das erworbene Unternehmen neuen Cyber-Risiken ausgesetzt wird, da potenzielle Angreifer, zu Recht oder zu Unrecht, davon ausgehen, durch dieses einen einfachen Zugang zu dem übernehmenden Unternehmen zu erhalten. Unabhängig davon, auf welcher Seite der Transaktion Sie sich befinden: Als Vorstand sind Sie dafür verantwortlich, dass das Management solche Risiken erkennt und entsprechend handelt. Denn: Werden Cyber-Risiken während des Akquisitionsprozesses nicht berücksichtigt, besteht ein reales Risiko sowohl für den Wert der Transaktion als auch den Return on Investment.

Kurzfristige Risiken

- Cyber-Sicherheitsvorfälle bei Anwaltskanzleien oder Finanzinstituten, die an der Transaktion beteiligt sind, könnten Informationen wie Bewertungen oder Verhandlungspositionen offenlegen, die die Transaktion zum Scheitern bringen würden.
- Eine verfrühte öffentliche Diskussion über den Transaktionszeitraum könnte dazu führen, dass potenzielle Angreifer versuchen, sich Zugang zum Netzwerk des Zielunternehmens zu verschaffen, um in das Netzwerk des Käufers zu gelangen.
- Die Unterlassung der Offenlegung von Gewährleistungsansprüchen, laufenden Verstößen oder Verlusten an geistigem Eigentum durch Sicherheitsvorfälle in der Vergangenheit könnte die Bewertung des Geschäfts verzerren.
- Potenzieller Schaden durch Mitarbeiterhandlungen im Hinblick auf bevorstehende M&A-Aktivitäten.

Langfristige Risiken

- Regulatorische oder rechtliche Schritte, die sich aus Umständen ergeben, die während der Due-Diligence-Untersuchung nicht entdeckt wurden, könnten den Return on Investment des Geschäfts gefährden. Der Verlust von Kunden, Reputations- und damit verbundene Umsatz- und Gewinnschäden, die sich aus nicht erkannten Umständen im Rahmen der Due-Diligence-Prüfung ergeben, könnten ebenfalls den Return on Investment reduzieren.
- Eine unzureichende Integration der Systeme der fusionierten Unternehmen in eine nachhaltig sichere Struktur kann zu einem Vorfall führen. Dies würde sich nachteilig auf beide Unternehmen auswirken, sofern es zu einem Verlust von Marktanteilen gegenüber Wettbewerbern ohne öffentlich bekannte Sicherheitsvorfälle führen könnte.

Vorstände sollten daher sicherstellen, dass das Management seine Führungsverantwortung im Bereich der Cyber-Sicherheit übernimmt. So sollte für jede Phase des Lebenszyklus der Transaktion eine Cyber-Risikobewertung durchgeführt werden, um die Sicherheit von Systemen und Prozessen zu bestätigen und die Risiken zu beziffern, die sich auf das Unternehmen nach Abschluss der Transaktion auswirken könnten – einschließlich Umsatz, Gewinn, Marktwert, Marktanteil und Markenimage.

Strategie- und Zielfindungsphase

Das Risiko eines Angriffs beginnt bereits vor dem offiziellen Angebot oder der Ankündigung einer Fusion. Anwaltskanzleien, Finanzberater und andere assoziierte Firmen sind für Hacker attraktiv, weil sie Geschäftsgeheimnisse und andere sensible Informationen über Firmenkunden besitzen. Diese umfassen besonders Details über die Anbahnung von Geschäften im Frühstadium, die für Insidergeschäfte oder für einen Wettbewerbsvorteil bei Geschäftsverhandlungen missbraucht werden können.

Angreifer suchen sehr gezielt nach Hinweisen, dass ein Unternehmen eine Fusion, Übernahme oder Veräußerung in Betracht zieht. Branchenklatsch, eine Verlangsamung des Release-Zyklus eines Unternehmens, Personalabbau oder aber Datenverlust über Social-Media-Kanäle können für diese Personen mögliche Indizien sein.

Dazu gehört auch die Modellierung der finanziellen Auswirkungen der identifizierten Cyber-Risiken eines Zielunternehmens. Diese Risiken können sich nicht nur auf die Rendite des investierten Kapitals auswirken, sondern auch zum Verlust von Wettbewerbsvorteilen, kostspieligen Sanierungsmaßnahmen, Geldbußen und möglicherweise jahrelangen Rechtsstreitigkeiten führen, je nachdem, was gestohlen wurde. Eine erste Abschätzung der Auswirkungen kann schwerwiegend genug sein, um die Strategieteams zu ermutigen, die Übernahmestrategie neu zu bewerten. Entscheidet sich das Team trotz der in dieser Phase identifizierten Risiken für eine Fortführung, sollten diese Risiken im Rahmen von Due-Diligence-Gesprächen mit dem Zielunternehmen viel

gründlicher bewertet werden. Das Management kann bereits vor Beginn der direkten Zusammenarbeit mit dem Zielunternehmen folgende Analysen durchführen:

- Das Management muss ein dezidiertes Verständnis für die mit dem Zielunternehmen verbundenen Cyber-Risiken entwickeln und die Auswirkungen dieser Risiken auf den Compliance-Status, die Finanzplanung und die potenziellen Bewertungen einschätzen können.
- Durchführung öffentlicher Recherchen über das Unternehmen, seine Systeme und Daten sowie sein geistiges Eigentum. Auf diese Weise kann festgestellt werden, ob das Unternehmen bereits auf dem Radar von Hackern ist, ob Systeme oder Zugangsdaten bereits kompromittiert sind oder ob sensible Daten zum Verkauf stehen oder angeboten werden.
- Untersuchung von Schadsoftware-Infektionen im Zielunternehmen und von Schwachpunkten in den Schutzmaßnahmen gegenüber Gefahren aus dem Internet. Solche Informationen sind öffentlich zugänglich oder können über Lösungsanbieter erworben werden. Sie ermöglichen einen effizienten Vergleich von Unternehmen miteinander, was dazu führt, dass Unternehmen mit einem sehr hohen Risikoprofil bereits ab diesem Punkt nicht in weitere Planungen mit einbezogen werden.

Due-Diligence- und Durchführungsphasen

Diese beiden Phasen dienen dem erwerbenden Unternehmen zur Evaluation des Cyber-Risiko-Status des Zielunternehmens. Dabei sollte der Vorstand sich im Klaren sein, dass gegebenenfalls gerade die Personen, die am besten über die Cyber-Status des Zielunternehmens Bescheid wissen, nicht im Kreise derer sind, die über den geplanten Kauf informiert sind – sodass eine Offenlegung von Cyber-Problemen erst *nach* dem Abschluss des Geschäfts erfolgen könnte. In dieser Phase identifizierte signifikante Probleme können nichtdestotrotz die Aushandlung einer Kaufpreisreduktion zur Deckung der Kosten notwendiger Sanierungen oder die Bereitstellung von Mitteln zur Behebung von Mängeln nach Abschluss der Transaktion rechtfertigen. Abhängig von den identifizierten Risiken kann der Vorstand die Genehmigung der Transaktion bis zum Abschluss der Sanierung aufschieben oder den Rückzug aus einer Transaktion beschließen, wenn die identifizierten Risiken eine solche Entscheidung nahelegen. Die Identifizierung von Cyber-Sicherheitsrisiken während der Prüfungsphase kann durch die Durchführung einer Cyber-Sicherheitsdiligence erfolgen, die darauf ausgelegt ist, die folgenden Risiken aufzudecken:

- Unzureichende Investitionen in Cyber-Sicherheits-Infrastrukturen und Datenschutzmaßnahmen sowie Mängel bei Personalressourcen, Richtlinien usw.
- Unternehmenskultur weist Nachlässigkeit gegenüber Cyber-Risiken oder gegenüber dem Schutz der Privatsphäre auf.
- Regelung konkreter Cyber-Sicherheitsbedingungen in Kunden- und Lieferantenverträgen, die zu potenziellen finanziellen Auswirkungen oder zu Rechtsstreitigkeiten wegen Nichteinhaltung führen können.
- Aufdeckung von Verstößen gegen Informationssicherheitsaspekte von Datenschutzgesetzen oder gegen andere geltende Vorschriften und Anforderungen.
- Identifikation aktueller Datenpannen oder anderer Vorfälle im Bereich der Cyber-Sicherheit.
- Eine effektive Due Diligence zu Fragen der Cyber-Sicherheit zeigt Investoren, Aufsichtsbehörden und anderen Interessengruppen, dass das Management aktiv daran arbeitet, den Wert und die strategischen Überlegungen hinter der potenziellen Transaktion zu schützen. Zudem macht ein solches Verhalten deutlich, dass das Ziel einer Senkung des Risikos eines potenziellen Cyber-Angriffs noch vor der Integration aktiv verfolgt wird.

Die identifizierten Risiken und Stärken können anschließend in den initialen Kaufpreis sowie in Investitionen zur Steigerung der Performance eingerechnet werden, welche wiederum den Wert der Transaktion erhöhen. Auf diese Weise kann schlussendlich den Aktionären ein solider Transaktionsvorschlag zur Genehmigung vorgelegt werden.

Integrationsphase

Die sogenannte Post-Deal-Integrationsphase stellt für beide Parteien ein hohes Risiko dar. Im Allgemeinen ist jede Akquisition von einer Reihe von Herausforderungen begleitet, welche mit der Zusammenführung von Mitarbeitern, Prozessen, Systemen und Unternehmenskulturen verbunden sind. Cyber-Risiken erweitern diese Phase der Transaktion um eine weitere Dimension der Komplexität und des Risikos. Nachdem die Transaktion öffentlich bekannt ist, werden Hacker versuchen, die Inkonsistenzen zwischen den Plattformen und technischen Strategien der Muttergesellschaft und der neu fusionierten oder erworbenen Einheit auszunutzen. Dies ist auch der Zeitraum, in

dem neue Cyber-Risiken erkannt werden können, da die Cyber-Sicherheitsverantwortlichen des Mutterkonzerns ab sofort in der Lage sind, mit allen Mitarbeitern des Zielunternehmens zusammenzuarbeiten, um ein tieferes Verständnis des dortigen Cyber-Sicherheitsniveaus zu erlangen. Mögliche Inkonsistenzen in den Datenschutzrichtlinien und -vereinbarungen der beiden Unternehmen müssen in der Folge erkannt und anschließend entsprechend vereinheitlicht werden.

In diesem Zeitraum des erhöhten Risikos ist es Aufgabe des Vorstands sicherzustellen, dass das Management eine strategische Entscheidung hinsichtlich des Umgangs mit der IT-Infrastruktur des Zielunternehmens getroffen hat. Das heißt, entweder wird die IT des erworbenen Unternehmens vollständig in die Infrastruktur des Mutterunternehmens integriert oder aber weiterhin als eigenständige Einheit belassen.

Diese Grundsatzentscheidung bestimmt die Cyber-Strategie maßgeblich. Fällt diese dahingehend aus, dass eine Integration umgesetzt wird, sollte der Vorstand den vorgeschlagenen Zeitplan für die Integration bewerten und sicherstellen, dass das Budget für die Cyber-Sanierung nicht anderweitig verwendet wird. Wenn die IT-Infrastruktur des Zielunternehmens als eigenständige Einheit belassen werden soll, muss der Vorstand dafür sorgen, dass das Management ausreichend in das Ziel investiert, es mit den technischen Möglichkeiten und der Risikobereitschaft der Muttergesellschaft in Einklang zu bringen. Gleichermaßen ist entscheidend, dass der Cyber-Sicherheitsbeauftragte des Mutterunternehmens die Governance-Aufsicht über das erworbene Unternehmen übernimmt. Bei beiden Varianten bedarf es einer entsprechend schnellen Reaktion, um den Zeitraum des erhöhten Cyber-Risikos zu reduzieren.

Weiterhin muss die Geschäftsleitung der Zielgesellschaft das Management dahingehend sensibilisieren, dass in dieser Phase eine erhöhte Wahrscheinlichkeit besteht, dass Hacker die Mitarbeiter selbst ins Visier nehmen.

Das Endergebnis der Integrationsphase muss ein Cyber-Risiko-Niveau sein, bei dem das erworbene Unternehmen das Risiko für das Mutterunternehmen nicht erhöht und die Datenschutzkontrollen konsistent sind.

Wertschöpfungsphase nach der Transaktion

Nach Abschluss einer Transaktion kann die kontinuierliche Überwachung der Cyber-Risiken durch das Management zahlreiche Möglichkeiten zur Portfolioverbesserung und zum Wachstum eröffnen.

Das Management sollte weiterhin den Cyber-Reifegrad der fusionierten oder erworbenen Einheit bewerten, insbesondere wenn diese Einheit eine eigenständige Organisation bleibt. Dies kann durch Benchmarking gegenüber Industriestandards und Mitbewerbern geschehen, genau wie beim Kerngeschäft. Ein niedriger Reifegrad könnte die Wachstumsprognosen und die Reputation der Marke aufgrund von Cyber-Unfällen und möglichen Bußgeldern beeinträchtigen. Ein Vorfall oder ein Compliance-Problem könnte die Aufsichtsbehörden veranlassen, Nachforschungen anzustellen, was zu einem finanziellen Verlust oder zum Stillstand von Ausstiegsplänen nach der Transaktion führen könnte. Cyber-Vorfälle können weiterhin dazu führen, dass Kunden und Lieferanten rechtliche Schritte einleiten, die wiederum zu Wertverlusten und geringeren Erträgen führen.

Schlussfolgerung

Cyber-Security-Diligence bei M&A erfordert einen zweigleisigen Ansatz. Unternehmen müssen die Cyber-Risiken des Zielunternehmens einer strengen Due Diligence unterziehen und damit verbundene Geschäftsauswirkungen während des gesamten Transaktionszyklus bewerten. Nur so können ein Return on Investment der Transaktion und der Wert des Unternehmens nach der Transaktion geschützt werden. Darüber hinaus müssen sich alle an der Fusion oder Übernahme beteiligten Parteien der erhöhten Wahrscheinlichkeit eines Cyber-Angriffs während des Transaktionsprozesses selbst bewusst sein und die Maßnahmen in Bezug auf die Cyber-Sicherheit beider Unternehmen intensiv fortsetzen. Die Umsetzung eines solchen zweigleisigen Ansatzes bei Fusionen und Übernahmen dient schlussendlich dem Schutz des Stakeholder Value.

ANHANG D

Kennzahlen zur Cyber-Sicherheit auf Vorstandsebene

Welche Kennzahlen zur Cyber-Sicherheit sollten Teil eines Briefings für die Geschäftsleitung sein? Diese Frage ist nur scheinbar einfach. Ähnlich wie jede andere Abteilung innerhalb einer Organisation sammelt und analysiert das Cyber-Sicherheitsteam eine enorme Menge an Daten. Es herrscht jedoch kein Konsens, welche kritischen Informationen genau an die Geschäftsleitung berichtet werden sollten. Erschwerend kommt hinzu, dass Cyber-Sicherheit ein relativ neuer Bereich ist, mit Standards und Benchmarks, die sich noch in der Entwicklung bzw. im Fluss befinden.

Fest steht: Die Vorstände müssen mit der Unternehmensführung zusammenarbeiten, um die Cyber-Sicherheitsinformationen, -kennzahlen und andere Daten zu definieren, die für sie im Blick auf die operativen Abläufe der Organisation am relevantesten sind. Eine solche Betrachtung sollte dabei Parameter wie Branche oder Sektor, regulatorische Anforderungen und Geografie mit einschließen. In den meisten Fällen sehen die Gremien eine Flut an operativen Kennzahlen, die jedoch nur sehr wenig strategische Erkenntnisse bezüglich des Status des Cyber-Sicherheitsprogramms der Organisation bieten. Typische Kennzahlen sind Statistiken wie „Anzahl blockierter Angriffe", „Anzahl nicht gepatchter Schwachstellen" und andere isolierte, complianceorientierte Maßnahmen, die wenig strategischen Kontext zu Performance und Risikoniveau des Unternehmens liefern.

Als Ausgangspunkt können die Vorstände dieselben allgemeinen Prinzipien anwenden, die auch für andere Arten von Kennzahlen auf Vorstandsebene verwendet werden (siehe „Kennzahlen zur Cyber-Sicherheit auf Vorstandsebene").

Die folgenden Empfehlungen bieten einen Ausgangspunkt für die Arten von Cyber-Sicherheitskennzahlen, die Vorstandsmitglieder potentiell vom Management anfordern sollten.

1. Was ist unser Cyber-Risiko-Appetit? Dies ist eine grundlegende Frage, der der Chief Information Security Officer (CISO) gemeinsam mit dem Chief Risk Officer (CRO) nachgehen sollte. Diese Art der Zusammenarbeit kann qualitative und quantitative Daten liefern, die dem Vorstand als Kontext für die Bestimmung des Cyber-Risiko-Appetits präsentiert werden können.

2. Welche Kennzahlen zur Cyber-Sicherheit auf Vorstandsebene haben wir, die auf ein Risiko für das Unternehmen hinweisen? Ein Unternehmen hat beispielsweise einen Cyber-Sicherheitsrisiko-„Index" eingeführt, der mehrere individuelle Kennzahlen umfasst, die Unternehmens-, Lieferketten- und Kundenrisiken abdecken.

3. Wie hoch ist der Anteil des IT-Budgets, welchen wir für Cyber-Sicherheitsaktivitäten ausgeben? Wie verhält sich dieser im Vergleich zu unseren Mitbewerbern/Unternehmen derselben Branche und/oder zu anderen externen Benchmarks? Diese Kennzahlen bieten eine valide Grundlage für Gespräche mit dem Management hinsichtlich Aussagen darüber, „wie viel Geld ausreicht" und/oder ob steigende Investitionen das Restrisiko der Organisation reduzieren können. Weitere Folgefragen sind u. a.:
   - Welche Initiativen wurden nicht aus dem diesjährigen Haushalt finanziert? Warum?
   - Welche Zugeständnisse wurden gemacht?
   - Verfügen wir über die richtigen Ressourcen, einschließlich Personal und Systeme, und werden diese effektiv eingesetzt?

4. Wie messen wir die Effektivität des Cyber-Sicherheitsprogramms unserer Organisation und wie lässt es sich im Vergleich zu den Programmen anderer Unternehmen bewerten? Die Kennzahlen für die Geschäftsführung sollten Veränderungen, Trends und Muster über einen gewissen Zeitraum hinweg hervorheben, die relative Leistung und die Effektivität aufzeigen. Externe Anbieter von Penetrationstests

Leitsätze für Vorstandskennzahlen

- Sicherstellung der Relevanz für das Publikum (Gesamtvorstand; Schlüsselkomitees).
- Leserfreundlichkeit: Verwenden Sie Zusammenfassungen, Beschreibungen, Grafiken und andere visuelle Elemente; vermeiden Sie Fachjargon.
- Aussagekraft: konkrete Einsichten vermitteln; keine Beschränkung auf eine bloße Informationsweitergabe.
  - Hervorheben von Veränderungen, Trends und Mustern im Laufe der Zeit.
  - Aufzeigen der relativen Performance im Vergleich zu Wettbewerbern, Branchendurchschnittswerten, anderen relevanten externen Indikatoren usw. (z. B. Reifegradbewertungen).
  - Geben Sie die Auswirkungen auf den Geschäftsbetrieb, die Kosten, den Marktanteil usw. an.
- Kurz und bündig: Vermeiden Sie Informationsüberflutung.
- Und vor allem: Ermöglichen Sie Diskussion und Dialog.

Quelle: NACD.

Entwicklung von Cyber-Geschäftskennzahlen

Das Cyber-Risiko wird nun als Thema auf Vorstandsebene akzeptiert. Die Herausforderung besteht jedoch darin, die finanziellen Auswirkungen von Cyber-Vorfällen effektiv und präzise an den Vorstand zu kommunizieren. Bevor Vorstände fundierte Entscheidungen über das Management von Cyber-Risiken treffen können, müssen sie in der Lage sein, Cyber-Sicherheitsdaten in Finanzkennzahlen zu übersetzen. Eine Zusammenarbeit mit dem Management ist hierbei das A und O, um die relevantesten Cyber-Sicherheitsinformationen zu skizzieren, die das gesamte Betriebsumfeld der Organisation betreffen. Die folgenden Empfehlungen zum Cyber-Risiko auf Vorstandsebene bieten einen Ausgangspunkt für mögliche Forderungen, die die Geschäftsführung an das Management richten sollte:

- Welches sind unsere vierteljährlichen Kennzahlen für die erwartete Verlustquote in Bezug auf unsere Cyber-Risikosituation in den verschiedenen Geschäftsbereichen und Betriebsumgebungen?
- Welche finanziellen Auswirkungen ergeben sich aus unserem Cyber-Risiko-Worst-Case-Szenario?
- Welche Prozesse haben wir etabliert, um Entscheidungen über die Akzeptanz von Cyber-Risiken, die Behebung von Cyber-Risiken und die Übertragung von Cyber-Risiken zu treffen? Wie messen wir, wie diese Entscheidungen unsere finanzielle Gefährdung durch Cyber-Risiken verringern?
- Wie messen und priorisieren wir unsere Kontroll- und Implementierungsaktivitäten und Cyber-Sicherheitsbudgets in Bezug auf unsere finanzielle Exposition gegenüber Cyber-Risiken? Haben wir unsere Strategie zur Implementierung von Kontrollmaßnahmen und Cyber-Sicherheitsprogrammen, einschließlich Budgets, mit unserer Strategie zur Übertragung von Cyber-Risiken verknüpft?
- Wie kann sich das Cyber-Risiko auf unsere finanzielle Performance auswirken, basierend auf unseren finanziellen Leistungszielen? Wie hoch ist unser jährlicher Cyber Risk Expected Loss Value?
- Wie sieht unser Cyber-Risiko-Sanierungsplan aus, um die angestrebte Toleranzgrenze für erwartete Verluste zu erreichen? Führt unser Plan zu einem positiven Nettofinanzertrag?
- Wie passt unser Cyber-Sicherheitsprogramm die cyberrisikobasierte Analyse der erwarteten Verlustquote und die Ziele für die erwartete Verlusttoleranz an? Wie messen, verfolgen und demonstrieren wir, wie unsere Investitionen in die Cyber-Sicherheit die finanzielle Gefährdung durch Cyber-Unfälle verringern und einen Return on Investment für die Cyber-Sicherheit liefern?
- Wie messen und koordinieren wir unsere auf Cyber-Risiken basierende Expected-Loss-Ratio-Analyse und Cyber-Sicherheitsplanung mit unserem Cyber-Versicherungsrisiko-Transferplan?
- Wie messen wir die Effektivität des Cyber-Sicherheits-programms unserer Organisation und wie wird es mit denen anderer Unternehmen verglichen?

Quelle: Secure Systems Innovation Corporation (SSIC) and X-Analytics.

und externe Experten können unter Umständen einen Vergleich zwischen „Äpfeln und Äpfeln“ innerhalb einer Branche ermöglichen.

5. Wie viele Datenvorfälle (exponierte sensible Daten) hat die Organisation in der letzten Berichtsperiode erlebt? Diese Kennzahlen liefern einen Hintergrund für Erörterungen von Trends, Mustern und Ursachen.

6. Beziehungen innerhalb der Wertschöpfungskette stellen typischerweise ein erhöhtes Risiko für Unternehmen dar, da der Grad der Systemvernetzung und des Datenaustausches, der mittlerweile zum täglichen Geschäftsbetrieb gehört, sehr hoch ist. Wie beurteilen wir die Cyber-Risikoposition unserer Lösungsanbieter, Lieferanten, Joint-Venture-Partner und Kunden? Wie erfolgt die laufende Überwachung der Risikohaltung? Wie viele externe Anbieter verbinden sich mit unserem Netzwerk oder erhalten sensible Daten von uns?
Dies ist keine eigentliche operative Kennzahl, sie kann aber dazu beitragen, Diskussionen mit dem Management über Restrisiken durch Dritte zu unterstützen. Auf dem Anbietermarkt für Cyber-Sicherheit gibt es Dienstleister, die eine passive und kontinuierliche Überwachung des

Cyber-Sicherheitsniveaus von Unternehmen anbieten. Immer mehr Unternehmen nutzen diese Dienste, um ihre mit hohem Risiko verbundenen Beziehungen zu Drittanbietern sowie ihren eigenen Status der Cyber-Sicherheit zu bewerten.

7. Welche operativen Kennzahlen werden routinemäßig von unserem Security-Team verfolgt und überwacht? Auch wenn operative Kennzahlen primär die Domäne des IT-Sicherheits-Teams sind, wäre es für die Vorstände von Vorteil, die Breite und Tiefe der Überwachungsaktivitäten der Cyber-Sicherheit des Unternehmens zu verstehen, um das eigene Bewusstsein für die Cyber-Sicherheitslage zu erhöhen.

8. Welche Kennzahlen verwenden wir, um das Bewusstsein für Cyber-Sicherheit im gesamten Unternehmen zu evaluieren? Daten über die Einhaltung von Richtlinien, die Durchführung und den erfolgreichen Abschluss von Schulungsprogrammen und dergleichen dienen dazu, Gespräche über Insiderrisiken auf verschiedenen Unternehmensebenen, in verschiedenen Regionen und Unternehmensbereichen zu führen.

9. Wie verfolgen wir die Aktivitäten der Personen oder Gruppen, die von wichtigen Sicherheitsrichtlinien, Aktivitätsüberwachung usw. ausgenommen sind? Diese Frage wird das Bewusstsein für Bereiche schärfen, in denen das Unternehmen zusätzlichen Risiken ausgesetzt ist, und auf diese Weise Diskussionen über Risiko-Rendite-Kompromisse forcieren.

ANHANG E

Verständnis der deutschen Gremienstrukturen

Wie eingangs angedeutet, basiert dieses Handbuch auf Ergebnissen, die in den USA von der *National Association of Corporate Directors* veröffentlicht wurden, sich jedoch auch auf internationaler Ebene als effektiv erwiesen haben. Allerdings haben deutsche Gremien eine etwas andere Struktur als im angloamerikanischen Raum. Diese Strukturen werden deutschen Unternehmen bekannt sein, viele Organisationen operieren jedoch in unterschiedlichen Jurisdiktionen, sodass es sinnvoll ist, in diesem Dokument einige der spezifischen Merkmale deutscher Gremien kurz zu skizzieren. Obwohl die Strukturen der Gremien unterschiedlich sind, sollten die Kernprinzipien des Cyber-Risiko-Managements und die Best Practices zur Umsetzung dieser Prinzipien unabhängig von den strukturellen Unterschieden im Unternehmen wirksam bleiben.

Die beiden Hauptkonzepte, die weiterer Aufmerksamkeit bedürfen, sind der Aufsichtsrat und der Vorstand. Je nach Größe, Struktur und Art des Unternehmens ist es erforderlich, dass ein Unternehmen einen Aufsichtsrat und/oder Vorstand hat.

Aufsichtsrat

Die Rolle des Aufsichtsrats besteht darin, den Vorstand zu beraten und zu überprüfen, indem er eine Aufsicht ausübt. Der Aufsichtsrat hat keinerlei Exekutivgewalt. Die Einrichtung eines Aufsichtsrats ist für Kapitalgesellschaften und einige andere Organisationen (Genossenschaften) zwingend vorgeschrieben. Die gesetzliche Grundlage ist im deutschen Aktiengesetz verankert. Die Größe und Struktur (z. B. das Erfordernis der Integration von Arbeitnehmervertretern) eines bestimmten Aufsichtsrats variiert stark zwischen den verschiedenen Arten von Unternehmen und Organisationen. Eine detaillierte Analyse der Anforderungen an einen Aufsichtsrat ist nicht Gegenstand dieses Handbuchs.

Die Hauptaufgabe des Aufsichtsrats ist es, als Kontrollorgan gegenüber dem Vorstand zu fungieren. Dies beinhaltet, die Tätigkeit des Vorstands zu überprüfen, was unter anderem die Validierung des jährlichen Geschäftsberichts erfordert. Dazu gehört auch, dass der Vorstand unter Umständen verpflichtet ist, bestimmte Aktivitäten oder Entscheidungen durch den Aufsichtsrat genehmigen zu lassen. Mit anderen Worten, der Aufsichtsrat vertritt die gesamte Gesellschaft gegenüber dem Vorstand, was auch die Auswahl und Bestellung der Vorstandsmitglieder einschließt.

Die genauen Aufgaben und Zuständigkeiten eines Aufsichtsratsmitglieds sind in seiner Satzung festgelegt.

Vorstand

Der Vorstand ist das Leitorgan eines Unternehmens, welches das Unternehmen nach außen hin rechtsfähig vertritt, die gleiche Funktion jedoch auch nach innen wahrnimmt, indem er das Handeln des Unternehmens lenkt. Die Satzung der Gesellschaft definiert die Aufgaben und Verantwortlichkeiten des Vorstands als Gremium, aber auch die Rollen und Verantwortungsbereiche der einzelnen Mitglieder. Ein Vorstandsmitglied kann Aktionär der Gesellschaft sein, darf aber nicht dem Aufsichtsrat angehören. Der Vorstand ist befugt, unabhängig zu handeln. Während die Verantwortung für das Geschäft immer beim Vorstand liegt, können bestimmte Verantwortlichkeiten im gesamten Unternehmen delegiert werden. Die Mitglieder des Vorstandes haften persönlich für schuldhaftes Handeln des Vorstands.

Diese Aufstellung ermöglicht eine klar definierte Handhabung aller Aspekte der Cyber-Sicherheit innerhalb eines Unternehmens. Innerhalb des Aufsichtsrats ist es entscheidend, die Risikobereitschaft gegenüber Cyber-Sicherheitsrisiken zu verstehen und zu bewerten. Darüber hinaus muss der Aufsichtsrat in der Lage sein, den Inhalt und die Priorisierung interner und externer Cyber-Security-Audits zu verstehen, um zu beurteilen, ob die Risiken für das Unternehmen angemessen gemildert werden. Da es unwahrscheinlich ist, dass der gesamte Aufsichtsrat in der Lage sein wird, sich mit dem Thema vertraut zu machen, ist es ausreichend, ein Mitglied oder eine Gruppe von Mitgliedern als Experten für Cyber-Risiken auszuwählen (oder zu ernennen). Während in der Vergangenheit eine solche allgemeine Empfehlung fragwürdig gewesen wäre, sollte in der heutigen Geschäftswelt, insbesondere unter der Prämisse, dass Unternehmen in ihrer Arbeit immer mehr von Informationstechnologien und Wertschöpfung durch Digitalisierung abhängig sind (Industrie 4.0), eine solche allgemeine Empfehlung in Betracht gezogen werden.

Innerhalb des Vorstands muss Cyber-Sicherheit etwas anders angegangen werden. Zunächst ist es wichtig, zu verstehen, dass die Verantwortung für alle Fragen der Cyber-Sicherheit, des Datenschutzes und der Compliance beim Vorstand liegt. Ausgehend von der gleichen Logik, wie sie für den Aufsichtsrat gilt, ist es von entscheidender Bedeutung, (mindestens) einen Fachexperten für alle Cyber-Themenbereiche als verantwortliche Person / Cyber-Sponsor innerhalb des Vorstands zu identifizieren. Die am besten geeignete Person im Vorstand ist stark abhängig von der Art des Geschäfts – doch sollten Unternehmen anstelle der Wahl eines Vorstandsmitglieds, welches ausreichende Fähigkeiten innehat, vielmehr in Betracht ziehen, die Position eines Chief (Information) Security Officer zu schaffen und diese in den Vorstand mit aufzunehmen.

ANHANG F

Ressourcen der Bundesregierung Deutschland

Die Internet Security Alliance empfiehlt Unternehmen, nicht erst nach dem ersten erfolgreichen Cyber-Angriff oder Sicherheitsvorfall mit den zuständigen Behörden in Kontakt zu treten. Organisationen sollten vielmehr proaktiv Beziehungen zu den betreffenden Behörden auf Bundes- oder Länderebene aufbauen und sich über verfügbare Beratungsangebote und Handlungsempfehlungen für den Krisenfall informieren. In diesem Appendix stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die zentrale nationale Behörde für Fragen der Cyber-Sicherheit in Deutschland relevante Ressourcen für Unternehmen vor.

Das BSI als zentrale Anlaufstelle für Cyber-Sicherheit

Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Das BSI untersucht und bewertet bestehende Sicherheitsrisiken und schätzt vorausschauend die Auswirkungen neuer Entwicklungen ab. Auf Grundlage dieses Wissens bietet es umfassende Dienstleistungen in den vier Kernbereichen Information, Beratung, Entwicklung und Zertifizierung an.

Die Aufgaben und Befugnisse des BSI sind durch das IT-Sicherheitsgesetz geregelt und umfassen unter anderem folgende Aktivitäten:

- Als zentrale Meldestelle für IT-Sicherheit sammelt das BSI Informationen über Sicherheitslücken und neue Angriffsmuster und wertet diese aus. Hierdurch können ein verlässliches Lagebild erstellt, Angriffe frühzeitig erkannt und Gegenmaßnahmen ergriffen werden.
- Das BSI darf Informationen und Warnungen vor Sicherheitslücken in IT-Produkten und -Diensten sowie vor Schadprogrammen – nach erfolgter Information der Hersteller – an die betroffenen Stellen oder die Öffentlichkeit weitergeben.
- Das BSI ist die zentrale Meldestelle für die IT-Sicherheit Kritischer Infrastrukturen.

Frameworks/Standards

- Mit dem **IT-Grundschutz** stellt das BSI eine bewährte Methodik zur Verfügung, um das Niveau der Informationssicherheit in Behörden und Unternehmen jeder Größenordnung zu erhöhen. Dabei ist der IT-Grundschutz durch seine Kompatibilität zu ISO 27001 auch international angesehen. Er umfasst die BSI-Standards 200-x und das IT-Grundschutz-Kompendium:
  - 200-1: Managementsysteme für Informationssicherheit (ISMS)
  - 200-2: IT-Grundschutz-Methodik
  - 200-3: Risikomanagement
  - 100-4: Notfallmanagement
  - IT-Grundschutz-Kompendium: Bausteine mit konkreten Sicherheitsanforderungen für zahlreiche Themen der Informationssicherheit als Grundlage zur Umsetzung der IT-Grundschutz-Methodik

  https://www.bsi.bund.de/grundschutz
- Die **IT-Grundschutzprofile** stellen Schablonen dar, mit denen Anwendergruppen einen Sicherheitsprozess nach IT-Grundschutz anhand von Musterszenarien zielgenau auf die Sicherheitsanforderungen ihrer Institutionen anpassen können.
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/itgrundschutzProfile_node.html
- Der **Cloud Computing Compliance Controls Catalogue (C5)** richtet sich in erster Linie an professionelle Cloud-Diensteanbieter, deren Prüfer und Kunden. Es wird festgelegt, welche Anforderungen die Cloud-Anbieter erfüllen müssen bzw. auf welche Anforderungen der Cloud-Anbieter mindestens verpflichtet werden sollte.
  https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

Netzwerke

- Im Rahmen der Allianz für Cyber-Sicherheit (ACS) bietet das BSI Unternehmen umfangreiche Hilfestellungen bei der Planung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen zur Erhöhung der Cyber-Sicherheit.
  https://www.allianz-fuer-Cybersicherheit.de

- Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen. Alle Organisationen mit Sitz in Deutschland, die Kritische Infrastrukturen in Deutschland betreiben, nationale Fach- und Branchenverbände, vom UP KRITIS anerkannte SPOCs aus den KRITIS-Sektoren sowie die zuständigen Behörden können Teilnehmer des UP KRITIS werden.
  https://www.kritis.bund.de

Informationsaustausch

- Das **CERT-Bund,** das nationale Computer Emergency Response Team für Bundesbehörden, ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computersystemen. Das CERT-Bund kooperiert eng mit den über 40 im CERT-Verbund zusammengeschlossenen CERTs auf Bundes- oder Länderebene sowie mit dem EU-CSIRTs-Netzwerk, das im Rahmen der NIS-Richtlinie geschaffen wurde.
  https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/CERT-Bund/certbund_node.html
- Das **Nationale IT-Lagezentrum** des BSI erfasst und bewertet IT-Sicherheitsvorfälle, um jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland zu verfügen. Es analysiert den Handlungsbedarf und die Handlungsoptionen bei Vorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft und veröffentlicht entsprechende Informationen und Warnungen.
  https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Lagezentrum/itlagezentrum_node.html
- Das nationale **Cyber-Abwehrzentrum** (Cyber-AZ) ist die zentrale Kooperationsplattform der deutschen IT-Sicherheitsbehörden. Dort werden alle Informationen zu Cyber-Angriffen auf Informationsinfrastrukturen zusammengeführt, von denen die sicherheitsrelevanten Behörden erfahren: Cyber-Spionage, Cyber-Ausspähung, Cyber-Terrorismus und Cyber-Crime. Das Ziel: schneller Informationsaustausch, schnelle Bewertungen und daraus abgeleitete konkrete Handlungsempfehlungen.

Informationssicherheitsberatung

- Das BSI berät umfassend bei der Findung ausgewogener Lösungsansätze in Fragen der Informationssicherheit. Die Unterstützung orientiert sich dabei immer am konkreten Bedarf unter wirtschaftlich angemessenen Gesichtspunkten. Das Dienstleistungsangebot des BSI richtet sich an Dienststellen der öffentlichen Verwaltung und die Wirtschaft.
- Kontakt:
  Telefon: 0049 (0)228 99 9582-333
  E-Mail: Sicherheitsberatung@bsi.bund.de

Melden von IT-Sicherheitsvorfällen

Meldepflicht für Betreiber Kritischer Infrastrukturen

- Seit dem Inkrafttreten der BSI-Kritisverordnung am 03.05.2016 gilt eine Meldepflicht für außergewöhnliche IT-Störungen für die vier Sektoren Energie, Informationstechnik und Telekommunikation (IKT), Wasser und Ernährung. Im Juni 2017 wurden die Sektoren Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr ergänzt.
- Betroffene Unternehmen erhalten über ihre Kontaktstelle Informationen zu Meldewegen und Erreichbarkeit.
- Betreiber Kritischer Infrastrukturen, die nicht unter die BSI-Kritisverordnung fallen, können freiwillige Meldungen über außergewöhnliche IT-Störungen über die Meldestelle der Allianz für Cyber-Sicherheit abgeben.
  https://www.allianz-fuer-Cyber-Sicherheit.de/ACS/DE/Meldestelle/meldestelle.html
- Weitere Informationen: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht_node.html

Meldestelle der Allianz für Cyber-Sicherheit

- Unternehmen, die einen Beitrag zum vom BSI zu erstellenden Lagebild leisten möchten, können IT-Sicherheitsvorfälle und Cyber-Angriffe über die Meldestelle der Allianz für Cyber-Sicherheit melden – auch anonym. Die übermittelten Informationen werden vertraulich behandelt. Erkenntnisse aus den Sicherheitsvorfällen werden anonymisiert zur Erstellung von IT-Lagebildern und ggf. Warnungen für die verschiedenen Zielgruppen des BSI genutzt. Gemeldete Sicherheitslücken in IT-Produkten werden im „Responsible Disclosure"-Verfahren an den Hersteller des Produktes weitergeleitet.
- Online-Formular: https://www.allianz-fuer-Cyber-Sicherheit.de/ACS/DE/Meldestelle/meldestelle.html
- Meldung per E-Mail: Meldestelle@bsi.bund.de

Was sollten Unternehmen melden?

- Neuartige Angriffsmethoden
- Angriffe auf Unternehmen zum Zweck der Spionage
- Angriffe auf Prozesssteuerungssysteme
- Angriffe auf Sicherheitsinfrastrukturen
- Neue Schwachstellen
- Abfluss von Daten und Informationen, die großflächige oder gezielte Angriffe ermöglichen (wie Code-Signing-Zertifikate, Passwörter für wichtige Infrastrukturen)

Kontakt zu Polizeibehörden (Zentrale Ansprechstellen Cybercrime, ZAC)

- Die Sichtbarkeit von Angriffen, wie sie durch diese Meldestelle verfolgt wird, sollte sich auch in Strafverfolgung und Kriminalstatistik wiederfinden. Bitte prüfen Sie bei Angriffen und Schäden in Ihrem Unternehmen daher aktiv, ob die Erstattung einer Anzeige möglich ist.
- Kontaktdaten der Zentralen Ansprechstellen Cybercrime der Länder und des Bundes: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/ZAC/polizeikontakt.html

ANHANG G

Aufbau einer Beziehung zum CISO/IT-Sicherheitsbeauftragten

Vor nicht allzu langer Zeit war das Konzept einer Führungskraft, die sich dezidiert der Gewährleistung der Cyber-Sicherheit des Unternehmens widmet, für viele Unternehmen außerhalb der Technologiebranche fremd.

Doch die Zeiten haben sich geändert: Engagierte Führungskräfte auf C-Level, die für die Kontrolle digitaler Risiken verantwortlich sind, sind in mittleren und großen Unternehmen verschiedener Branchen auf dem Vormarsch; eine Folge des Geschäftsalltags in der heutigen, ständig vernetzten Welt.

Einer Studie zufolge beschäftigen 54 Prozent der Unternehmen weltweit eine spezielle Person, die für die Cyber-Sicherheit verantwortlich ist. Diese Person wird zunehmend als Chief Information Security Officer (CISO) bezeichnet, womit die Wichtigkeit dieser Rolle unterstrichen wird.[48] Eine weitere Umfrage ergab, dass Unternehmen, die eine entsprechende Person eingesetzt haben, vermehrt über dedizierte Teams und Pläne für den Umgang mit Cyber-Vorfällen verfügen und zugleich mehr Vertrauen in die Stärke der Abwehrmaßnahmen ihres Unternehmens gegen Bedrohungen wie z. B. Schadsoftware haben.[49]

Mit zunehmender Reife der Rollen im Bereich Informationssicherheit im Unternehmen stellt sich eine neue Frage: Wie kann der Vorstand effektiv mit dem Sicherheitsverantwortlichen kommunizieren? Die Person, die diese Position innehat, ist für die Bewältigung großer Mengen von operativen, Reputations- und finanziellen Risiken verantwortlich, weshalb ein Vertrauensverhältnis zum Vorstand unerlässlich ist.

Auf dem ersten globalen Cyber Summit der NACD im Jahr 2015 diskutierten mehr als 200 Vorstände von Fortune-Global-500-Unternehmen und Cyber-Sicherheitsexperten über die sich immer weiter entwickelnde Rolle des Sicherheitsverantwortlichen, beispielsweise sein Potenzial, als maßgebliche Quelle für Informationen und wichtige Erkenntnisse für das Board zu agieren. Wie ein Vorstand bemerkte: „Ein starkes Cyber-Sicherheitsprogramm ermöglicht es unserem Unternehmen, konkurrenzfähig zu bleiben und zu florieren. Eine Führungskraft im Bereich der Cyber-Sicherheit mit den richtigen Fähigkeiten kann ein enormer Gewinn sein und auch als Augen und Ohren für Vorstände dienen. Dennoch werden sie bei zu vielen Unternehmen immer noch als taktische Unterstützung für den CIO angesehen."[50]

Viele Vorstandsmitglieder versuchen nun, eine kontinuierliche Beziehung zum Sicherheitsverantwortlichen aufzubauen, und beziehen ihn oder sie mehr und mehr in die Diskussionen über Cyber-Sicherheitsangelegenheiten auf Aufsichtsrats- und/oder Schlüsselkomitee-Ebene mit ein.

Die folgenden Fragen und Richtlinien können Vorstände dabei unterstützen, eine solche engere Beziehung mit dem Cyber-Sicherheitsverantwortlichen aufzubauen oder diese zu vertiefen. Darüber hinaus können sie den Vorstandsmitgliedern helfen, ihre Kommunikation mit der Geschäftsleitung zu verbessern und die Vorstände dabei zu unterstützen, ein besseres Verständnis für die Gesamtstrategie des Unternehmens im Bereich der Cyber-Sicherheit zu erlangen. Da nicht jede Frage für jedes Unternehmen relevant ist, sollten die Vorstände diejenigen auswählen, die am besten zu den jeweiligen Themen und Umständen passen.

1. Verstehen der Rolle und des Mandat des IT-Sicherheitsbeauftragten

- Was ist der Verantwortungs- und Zuständigkeitsbereich des Beauftragten für IT-Sicherheit in Bezug auf Ressourcen, Entscheidungsbefugnis, Budget, Personalausstattung und Zugang zu Informationen und Personal des Unternehmens, einschließlich des Vorstands (siehe Anhang E zu den deutschen Gremienstrukturen)? Entspricht dies den bewährten Praktiken in unserer Branche und allgemein?[51] Eine Schlüsselfrage, die Sie sich stellen sollten: Verstehen Sie die gesamte Cyber-Sicherheitslage des Unternehmens, indem Sie mit einer einzelnen Person sprechen? Wenn nein, dann ist der Verantwortungsbereich Ihres Sicherheitsbeauftragten zu eng gefasst.

[48] PwC, Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016 (New York, NY: PwC, 2015), Seite 26, siehe auch Paul Solman, Chief information security officers come out from the basement, *Financial Times*, 29. Apr. 2014.

[49] Kris Monroe, Why are CISOs in such high demand?, *Cyber Experts Blog*, 8. Febr. 2016.

[50] Zitat eines Teilnehmers des Global Cyber Summit am 15. Apr. 2016 in Washington, DC. Die Diskussion wurde nach den Regeln des Chatham House durchgeführt.

[51] Siehe z. B. Marc van Zadelhoff, Kristin Lovejoy und David Jarvis, *Fortifying for the Future: Insights from the 2014 IBM Chief Information Security Officer Assessment* (Armonk, NY: IBM Center for Applied Insights, 2014).

- In welcher organisatorischen Beziehung steht der Sicherheitsbeauftragte zum Datenschutzbeauftragten und zu anderen für den Datenschutz zuständigen Führungskräften?
- Ist das Unternehmen so strukturiert, dass ein Überblick über den gesamten Cyber-Sicherheitsstatus, einschließlich des Budgets, möglich ist? Die Antwort auf diese Frage sollte zu einer Diskussion darüber führen, wie das Cyber-Sicherheitsbudget des Unternehmens festgelegt wird. Der Vergleich dieser Zahl mit der Entwicklung der Ausgaben in der Branche ist wahrscheinlich der beste Weg, die Angemessenheit der Finanzierung zu beurteilen. Wie hoch ist das Budget (z. B. Anteil an den gesamten IT-Ausgaben), und wie verhält sich diese Zahl im Vergleich zur üblichen Praxis in unserer Branche und allgemein? Welche Rolle spielt der Sicherheitsbeauftragte bei der Budgetvergabe und bei Investitionsentscheidungen im Bereich der Cyber-Sicherheit? Eine der möglicherweise aufschlussreichsten Fragen ist schließlich, welche Sicherheitstools oder anderen Investitionen Budgetkürzungen zum Opfer fielen.
- An wen berichtet der IT-Sicherheitsbeauftragte (z. B. CIO, CTO, COO, CRO, Leiter Corporate Security, Board, Sonstige)? Bestehen Unterschiede zur funktionalen Berichtskette? Wenn nein: Welche Protokolle gibt es, um sicherzustellen, dass der IT-Sicherheitsbeauftragte über einen unabhängigen Kanal verfügt, um Probleme zu eskalieren und um eine sofortige und vollständige Offenlegung von Cyber-Sicherheitsdefiziten zu gewährleisten?[47]
- Welche Rolle spielt der IT-Sicherheitsbeauftragte in der Unternehmensstruktur des Risikomanagements und den damit verbundenen Prozessen?
- Welche Rolle, wenn überhaupt, spielt der IT-Sicherheitsbeauftragte über die Festlegung und Durchsetzung von Cyber-Sicherheitsrichtlinien und verwandten Kontrollsystemen hinaus?
  - Gibt der IT-Sicherheitsbeauftragte z. B. Anregungen für den Entwicklungsprozess neuer Produkte, Dienstleistungen und Systeme oder liefert er Input für die Gestaltung von Partnerschafts- und Allianzvereinbarungen usw. mit dem Ziel, dass die Cyber-Sicherheit von vornherein integriert und nicht nachträglich als „Add-on" hinzugefügt wird?

2. Machen Sie sich mit dem Sicherheitsteam vertraut, bevor ein Zwischenfall eintritt

- Ist der Krisenfall eingetreten, ist dies der wohl schlechteste Zeitpunkt für Vorstände, sich mit dem Sicherheitsverantwortlichen und dem Schlüsselpersonal erstmals vertraut zu machen. Wichtig ist, dass Vorstandsmitglieder bereits vor Eintritt eines Cyber-Vorfalls mit dem Sicherheitsteam in Kontakt treten. So ist zu empfehlen, sich von Mitarbeitern, die an vorderster Front der Cyber-Sicherheit agieren, aus erster Hand informieren zu lassen – sei es in Verbindung mit einer regulären Vorstandssitzung oder einem Besuch vor Ort. Diese Sitzungen werden den Vorstandsmitgliedern wertvolle Einblicke und Erkenntnisse bieten. Weiterhin wird es auch das Sicherheitsteam zu schätzen wissen, erhöhen Besuche wie diese doch die eigene Sichtbarkeit im Unternehmen, stärken die Motivation und verdeutlichen, dass dieser Bereich im Fokus steht.
- Mitglieder der Geschäftsleitung können den Sicherheitsbeauftragten auch um eine Einschätzung ihrer persönlichen Cyber-Sicherheitssituation bitten, etwa bezüglich der Sicherheit ihrer Geräte, Heimnetzwerke usw. Diese Gespräche sind nicht nur informativ für die einzelnen Führungskräfte, sondern tragen auch dazu bei, die große Menge an vertraulichen Informationen, die diese im Rahmen ihrer Tätigkeit erhalten, besser abzusichern.
- Viele Sicherheitsteams erstellen routinemäßig interne Berichte für das Management und die Führungskräfte über Trends und Vorfälle im Zusammenhang mit Cyber-Angriffen. Der Aufsichtsrat kann mit dem CISO und dem Vorstand besprechen, ob diese Informationen relevant und nützlich sein könnten, um sie in die Aufsichtsratsmaterialien aufzunehmen.

[52] Eine 2014 durchgeführte Studie zur globalen Informationssicherheit ergab, dass Unternehmen, in denen CISOs an eine andere Stelle als das CIO-Büro berichten, weniger Ausfallzeiten und geringere finanzielle Verluste in Bezug auf Cyber-Sicherheitsvorfälle aufweisen, als Unternehmen, bei denen direkt an den CIO berichtet wird. Sehen Sie Bob Bragdon, vielleicht ist es wirklich wichtig, von wem der CISO berichtet, *The Business Side of Security* (Blog), 20. Juni 2014.

3. Gewinnen Sie Einblicke in das Netzwerk des IT-Sicherheitsbeauftragten

Innerhalb der Organisation

- Wie arbeitet der Sicherheitsbeauftragte oder das Informationssicherheitsteam mit anderen Abteilungen und Unternehmensfunktionen bei Cyber-Sicherheitsfragen zusammen? Koordiniert er sich z. B. mit:
  - dem Datenschutzbeauftragten bezüglich der Ausgewogenheit von Datenschutz und Sicherheitsüberwachung;
  - dem Senior Risk Officer, um das technische/digitale Risiko als Teil des Gesamtrisikos des Unternehmens zu betrachten;
  - dem Bereich Business Development hinsichtlich der Umsetzung von Due Diligence von Akquisitionszielen und Partnerschaftsverträgen;
  - der internen Revision zur Bewertung und Erprobung von Kontrollsystemen und -vorgaben;
  - HR mit Blick auf Mitarbeiterschulungen und Zugangsprotokollen;
  - den Bereichen Einkauf und Lieferkettenmanagement in Bezug auf Cyber-Sicherheitsprotokolle mit Lösungsanbietern, Kunden und Lieferanten und/oder
  - der Rechtsabteilung, um Hinweise zur Einhaltung gesetzlicher Vorschriften und Berichterstattungsstandards im Bereich der Cyber-Sicherheit und des Datenschutzes zu erhalten?

Der Sicherheitsbeauftragte sollte generell in der Lage sein, verständlich und klar zu kommunizieren, dass Cyber-Sicherheit nicht nur ein technisches Problem ist, sondern dass es vielmehr darum geht, die Unternehmensstrategie so sicher wie möglich umzusetzen.

- Welche Unterstützung erhält der CISO vom CEO, CIO und Senior Management Team? Dies spiegelt sich oft im Budget wider, aber auch in der Anzahl der Community oder Rollen im Unternehmen, die für wichtige Sicherheitsrichtlinien oder -kontrollen freigestellt sind.

Außerhalb der Organisation

- Beteiligt sich der Sicherheitsbeauftragte oder das Informationssicherheitsteam an Initiativen zum Informationsaustausch im Bereich der Cyber-Sicherheit (z. B. branchen-orientierte, auf die IT-Community ausgerichtete oder öffentlich-private Partnerschaften)? Wie werden die Informationen, die aus der Teilnahme an solchen Initiativen gewonnen werden, innerhalb der Organisation genutzt und weitergegeben?
- Hat der CISO (oder das Informationssicherheitsteam) Beziehungen zu öffentlichen Akteuren wie Strafverfolgungsbehörden (z. B. Landeskriminalämter [LKA] oder Bundeskriminalamt [BKA]), dem Bundesamt für Sicherheit in der Informationstechnik [BSI] oder nationalen oder internationalen Computer-Emergency-Response-Teams?

Innerhalb und außerhalb der Organisation

- Wie entwickelt und pflegt der Sicherheitsbeauftragte oder das Informationssicherheitsteam das Wissen über die strategischen Ziele, das Geschäftsmodell und die operativen Aktivitäten der Organisation?
  - Unternehmen, die z. B. aktiv eine Cloud-Strategie verfolgen: Inwiefern versteht der Sicherheitsbeauftragte die Strategie und in welcher Art und Weise trägt er zu deren sicherer Umsetzung bei?
- Welche Weiterbildungsmaßnahmen werden vom Sicherheitsverantwortlichen und vom Informationssicherheitsteam durchgeführt, um in Sachen Cyber-Sicherheit auf dem Laufenden zu bleiben?

4. Beurteilung der Performance

- Wie wird die Leistung des Sicherheitsbeauftragten bewertet? Wie wird die Leistung des Informationssicherheitsteams bewertet? Wer führt diese Auswertungen durch und welche Kennzahlen werden verwendet?
- Welche Cyber-Sicherheitskennzahlen und Meilensteine wurden für die gesamte Organisation festgelegt? Verwenden Sie einen risikobasierten Ansatz, der ein höheres Schutzniveau für die wertvollsten und kritischsten Vermögenswerte des Unternehmens bietet?

- Inwieweit sind Cyber-Risikobewertungs- und -management-Aktivitäten in die unternehmensweiten Risikomanagement-Prozesse der Organisation integriert? Verwenden wir einen anerkannten Rahmen, um die Cyber-Sicherheitshygiene aus einer organisationsweiten Perspektive zu beurteilen?

5. Holen Sie den CISO bei Gesprächen über die „Lage der Organisation" mit an den Tisch

- Welches war der bedeutendste Cyber-Sicherheitsvorfall der Organisation im vergangenen Quartal? Wie wurde dieser entdeckt? Wie haben Sie darauf reagiert? Wie war die Erkennungs- und Wiederherstellungsgeschwindigkeit im Vergleich zu früheren Vorfällen? Welche Lehren haben Sie daraus gezogen und wie werden diese in die kontinuierlichen Verbesserungsbemühungen der Organisation einfließen?
- Wo haben Sie im Bereich der Cyber-Sicherheit in den letzten sechs Monaten die größten Fortschritte erzielt, und auf welchen Faktor bzw. welche Faktoren sind diese Fortschritte zurückzuführen? Wo bestehen die größten Lücken, und wie sieht Ihr Plan aus, diese Lücken zu schließen?

ANHANG H

Bewertung der Cyber-Sicherheitskultur des Vorstands und Aufsichtsrats

Im Jahr 2010 definierte der Bericht der NACD Blue Ribbon Commission on Board Evaluation die Vorstandskultur als „die gemeinsamen Werte, die der Kommunikation, den Interaktionen und der Entscheidungsfindung im Vorstand zugrunde liegen und diese vorantreiben. Es ist die Essenz dessen, wie die Dinge wirklich gemacht werden."[53] Fünf Jahre später, auf dem ersten Global Cyber Summit der National Association of Corporate Directors (NACD), diskutierten mehr als 200 Vorstände von Fortune-Global-500-Unternehmen und Cyber-Sicherheitsexperten über verschiedene Möglichkeiten, wie die Vorstandskultur die Cyber-Sicherheitsbemühungen des Managements unterstützen oder behindern kann.

Mit den Worten eines Teilnehmers:

> *„Boards müssen ihre Einstellung ändern. Wir müssen uns von der Frage verabschieden: „Wie hoch ist die Wahrscheinlichkeit, dass wir angegriffen werden?" Stattdessen müssen wir sagen: „Es ist wahrscheinlich, dass wir angegriffen wurden. Weg von der Betrachtung der Cyber-Sicherheit als Kostenfaktor hin zur Betrachtung als Investition, die uns dabei hilft, wettbewerbsfähig zu bleiben. Weg von der Erwartung, dass das Management Cyber-Bedrohungen vorbeugen oder sich dagegen wehren kann, hin zur Frage, wie schnell es diese erkennen und darauf reagieren kann."*[54]

Vorstände, die eine Cyber-Sicherheitskomponente in die Selbsteinschätzung ihrer Gremien einbeziehen möchten, können die Fragen in der untenstehenden Tabelle als Ausgangspunkt verwenden. Die Bewertung 1 ist niedrig, das Rating 5 ist exzellent.

Benutzen Sie die numerische Skala, um anzugeben, wo die Kultur des Vorstandes/ Aufsichtsrates im Allgemeinen auf das unten gezeigte Spektrum fällt. ◄——►							Aktion
Wir betrachten Cyber-Sicherheit in erster Linie als IT-Thema.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Wir verstehen Cyber-Sicherheit als unternehmensweites Risiko-Management-Problem.	
Wir stützen uns auf die rechtlichen Rahmenbedingungen für Cyber-Sicherheit, die weitgehend stabil und allgemeingültig für die meisten Unternehmen sind und gleichermaßen anwendbar.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Wir sind uns bewusst, dass es notwendig ist, regelmäßig Rechtsbeistand zu suchen, um eine neue Cyber-Rechtslandschaft zu verstehen, die auf unsere sich entwickelnden Geschäftspläne und -umgebungen zugeschnitten ist.	
Wir benötigen keine regelmäßige Aktualisierung der Cyber-Sicherheit durch Branchenexperten.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Wir suchen regelmäßig nach Cyber-Expertise in Bezug auf unsere neu entstehenden Cyber-Bedürfnisse und Bedrohungsbilder.	
Wir sind nicht der Meinung, dass das Management einen spezifischen Plan für das Managen von Cyber-Risiken erstellen muss.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Wir erwarten vom Management, dass es uns einen operativen Rahmen zur Verfügung stellt, der die modernen Auswirkungen der digitalen Technologie widerspiegelt und zeigt, wie wir diese digitalen Risiken im Einklang mit unseren Geschäftsanforderungen und -risiken managen.	
Wir erwarten nicht, dass das Management die Cyber-Risiken eindeutig bewertet und managt.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Wir erwarten von der Geschäftsführung eine klare Analyse der Cyber-Risiken hinsichtlich eines Ergebnisses, welches aufzeigt, welche Risiken wir akzeptieren, welche wir abschwächen können und welche wir, im Einklang mit unseren Geschäftszielen, übertragen können.	

[53] *Report of the NACD Blue Ribbon Commission on Board Evaluation: Improving Director Effectiveness* (Washington, DC: NACD, 2010), Seite 7.

[54] Kursiv zitierte Zitate stammen von Teilnehmern des Global Cyber Summit vom 15.-16. April 2015, in Washington, DC. Diskussionen wurden unter der Chatham House Rule geführt.

Die Mitwirkenden

Die **Allianz für Cyber-Sicherheit** (ACS), eine Initiative des Bundesamts für Sicherheit in der Informationstechnik (BSI), unterstützt Unternehmen mit Sitz oder Niederlassung in Deutschland dabei, das Niveau der Informationssicherheit im Unternehmen zu erhöhen und sich wirksam gegen Cyber-Bedrohungen und IT-bedingte Produktivitätsausfälle zu schützen. Im Rahmen der ACS arbeitet das BSI intensiv mit Partnern und Multiplikatoren zusammen, um strategische und praktische Hilfestellungen für Unternehmen jeder Größe und Branche zu leisten. Teilnehmer erhalten über die Website der ACS einen Überblick über die aktuelle Bedrohungslage und über erprobte Ansätze zum Schutz von Unternehmenswerten. Mit Veranstaltungen und Arbeitskreisen fördert die ACS den vertraulichen Austausch von Wissen und Erfahrungen zwischen Teilnehmern aus Wirtschaft und Forschung.

Als Zusammenschluss aller wichtigen Akteure im Bereich Cyber-Sicherheit in Deutschland umfasst die Allianz für Cyber-Sicherheit rund 2.600 Mitglieder, 100 Partner und 45 Multiplikatoren (Stand Februar 2018).

Die **Internet Security Alliance** (ISA) ist eine im Jahr 2000 gegründete internationale Handelsvereinigung, die sich ausschließlich auf Cyber-Sicherheit konzentriert. Der ISA-Vorstand besteht aus dem primären Cyber-Sicherheitspersonal internationaler Unternehmen, das praktisch alle Wirtschaftssektoren repräsentiert. Die Mission der ISA ist es, Wirtschaft mit fortschrittlicher Technologie und Regierungspolitik zu verbinden, um nachhaltig sichere Cyber-Systeme zu schaffen. Im Jahr 2014 hat ISA das erste Cyber Risk Oversight Handbook herausgegeben, das speziell auf die einzigartige Rolle von Corporate Boards beim Management von Cyber-Risiken eingeht. In ihrem jährlichen Global Information Security Survey berichtete PricewaterhouseCoopers (PwC), dass das Handbuch von den Unternehmensvorständen in großem Umfang angenommen wurde und dass die Verwendung zu einer besseren Budgetierung der Cyber-Sicherheit, einem besseren Cyber-Risiko-Management, einer engeren Abstimmung der Cyber-Sicherheit mit den allgemeinen Geschäftszielen und zur Schaffung einer Sicherheitskultur in Organisationen führte. Weitere Informationen über ISA finden Sie unter www.isalliance.org.

American International Group, Inc. (AIG) ist ein internationales Versicherungsunternehmen. Es wurde 1919 gegründet und bietet heute eine große Bandbreite an Sach- und Unfallversicherungen, Lebensversicherungen, Altersvorsorgeprodukten und anderen Finanzdienstleistungen für Kunden in mehr als 80 Ländern und Jurisdiktionen. Zu unseren unterschiedlichen Angeboten gehören Produkte und Dienstleistungen, die Geschäfts- und Privatkunden dabei unterstützen, ihre Vermögenswerte zu schützen, sich gegen Risiken abzusichern und für das Alter vorzusorgen. Stammaktien von AIG sind an den Börsen in New York und Tokio notiert.

Weitere Informationen über AIG finden Sie unter www.aig.com | YouTube | Twitter: @AIGinsurance | LinkedIn.

2500 Wilson Blvd. #245
Arlington, VA 22201, USA
+1 (703) 907-7090
isalliance.org