Allianz für Cyber-Sicherheit

INTERNET SECURITY ALLIANCE

Toolkit für das Management von Cyber-Risiken

Ein Handbuch für deutsche Unternehmensleitungen

Mit Unterstützung von:

SAP

Impressum

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

Telefon
+49 (0) 22899 9582-0

Fax
+49 (0) 22899 9582-5400

E-Mail
info@cyber-allianz.de

Internet
www.allianz-fuer-cybersicherheit.de

Stand
Oktober 2022

Texte und Redaktion
Allianz für Cyber-Sicherheit

Bildnachweis
Titel, Rückseite: AdobeStock © Alex; Titel: AdobeStock © Simple Line; S. 6: AdobeStock © Gondex; S. 9: AdobeStock © derplan13; S. 11: AdobeStock © ngupakarti; S. 12: AdobeStock © OneLineStock.com, AdobeStock © derplan13; S. 13: AdobeStock © liu_miu; S. 15: AdobeStock © Oleksandr; S. 16: AdobeStock © derplan13; S. 17: AdobeStock ©rina; S. 18: AdobeStock © derplan13; S. 20: AdobeStock © Simple Line; S. 23: AdobeStock © LuckyStep; S. 24: AdobeStock © Natalia; S. 25: AdobeStock © Simple Line; S. 26: AdobeStock © riz; S. 31: AdobeStock © OneLineStock.com.

Diese Publikation wird von der Allianz für Cyber-Sicherheit kostenlos zur Verfügung gestellt und ist nicht zum Verkauf bestimmt.

Inhalt

Roadmap für das Toolkit für das Management von Cyber-Risiken

Während die sechs Prinzipien einen allgemeinen Governance-Ansatz bieten, den Unternehmensleitungen zum Management der Cyber-Sicherheit nutzen können, bieten die folgenden Tools praktische Anleitungen zur Umsetzung dieser Prinzipien.

Prinzipien	Dazu passende Tools
 **PRINZIP 1** Cyber-Sicherheit nicht nur als IT-Thema, sondern als Baustein des unternehmensweiten Risiko-managements verstehen	**Tool A:** 10 Fragen, die ein Mitglied der Unternehmensleitung zur Cyber-Sicherheit stellen sollte
 **PRINZIP 2** Rechtliche Auswirkungen von Cyber-Risiken verstehen.	**Tool C:** Risiken in der Lieferkette und gegenüber Dritten **Tool D:** Reaktion auf Vorfälle **Tool G:** Verbesserung der Offenlegung von Informationen zur Cyber-Sicherheitsaufsicht – 10 Fragen für Unternehmensleitung
 **PRINZIP 3** Zugang zu Cyber-Sicherheitsexpertise sowie regelmäßigen Austausch sicherstellen	**Tool A:** 10 Fragen, die ein Mitglied der Unternehmensleitung zur Cyber-Sicherheit stellen sollte **Tool B:** Die Bedrohung durch Innentäter oder Innentäterinnen – eine reale und allgegenwärtige Gefahr **Tool F:** Im regelmäßigen Austausch mit CISO/ IT-Sicherheitsbeauftragten **Tool H:** Persönliche Cyber-Sicherheit für Mitglieder der Unternehmensleitung
 **PRINZIP 4** Umsetzung geeigneter Rahmenbedingungen sowie Ressourcen für das Cyber-Risikomanagement sicherstellen	**Tool B:** Die Bedrohung durch Innentäter oder Innentäterinnen – eine reale und allgegenwärtige Gefahr **Tool C:** Risiken in der Lieferkette und gegenüber Dritten **Tool D:** Reaktion auf Vorfälle **Tool E:** Metriken zur Cyber-Sicherheit auf Ebene der Unternehmensleitung **Tool F:** Im regelmäßigen Austausch mit CISO/ IT-Sicherheitsbeauftragten **Tool G:** Verbesserung der Offenlegung von Informationen zur Cyber-Sicherheitsaufsicht – 10 Fragen für Unternehmensleitung **Tool I:** Ressourcen der Bundesregierung Deutschland
 **PRINZIP 5** Risikoanalyse erstellen sowie Definition von Risikobereitschaft in Abhängigkeit von Geschäftszielen und -strategien formulieren	**Tool D:** Reaktion auf Vorfälle **Tool E:** Metriken zur Cyber-Sicherheit auf Ebene der Unternehmensleitung
PRINZIP 6 Unternehmensweite Zusammenarbeit und den Austausch von Best Practice fördern	**Tool F:** Im regelmäßigen Austausch mit CISO/ IT-Sicherheitsbeauftragten

TOOL A

10 Fragen, die die Unternehmensleitung zum Thema Cyber-Sicherheit stellen sollte

Nach:
Jeff Brown, Chief Information Security Officer, Raytheon

Zielsetzung:
Dieses Tool enthält Vorschläge für Fragen, die Mitglieder der Unternehmensleitung der Geschäftsführung stellen können, um ihr Cyber-Risikomanagement zu überwachen, und erklärt, wie die Antworten auf diese Fragen aussehen könnten.

Stufe 1. Politik und Governance

Dies umfasst eine Reihe von grundlegenden Kontrollfragen, mit denen sich jedes Unternehmen und jede Organisation befassen muss. Wenn diese Fragen nicht zufriedenstellend beantwortet werden, wird die Fortsetzung der Fragen der Stufen 2 und 3 kaum nützliche Erkenntnisse bringen.

1. Wie werden persönlich identifizierbare Informationen (PII) im In- und Ausland behandelt? Welche Sicherheitsvorkehrungen gibt es für gestohlene Geräte?

Warum diese Frage wichtig ist: Die gesetzlichen Sanktionen für Verstöße beim Umgang mit persönlich identifizierbaren Informationen (PII) sind streng. Die Anforderungen sind von Bundesstaat zu Bundesstaat (Anm. d. Übers. der USA) und insbesondere von Land zu Land sehr unterschiedlich. Da es sich bei den meisten Computern der Mitarbeitenden um Laptops oder Tablets handelt, ist es nicht unwahrscheinlich, dass einige davon verloren gehen oder gestohlen werden.

Hilfreiche Antwort: Wir wissen, wo alle unsere personenbezogenen Daten gespeichert sind. Sie sind sowohl während der Nichtnutzung, als auch während der Übertragung verschlüsselt. Alle unsere Mitarbeitenden, die routinemäßig mit personenbezogenen Daten umgehen, werden in Sicherheitsverfahren geschult. Wir schulen unsere Mitarbeitenden regelmäßig (in der Regel jährlich) zum Thema personenbezogener Daten. Wir sind uns der unterschiedlichen Anforderungen an personenbezogene Daten, insbesondere in Europa, bewusst und haben die notwendigen Schritte unternommen, um Diese einzuhalten.

Antworten, die weitere Nachfrage erfordern:

- Unsere Mitarbeitenden nutzen die Festplattenverschlüsselung ihrer Laptops nicht.

- Wir haben nicht so viele personenbezogene Daten.
- Unsere Mitarbeitenden, die nicht aus der Personalabteilung kommen, haben keinen Umgang mit personenbezogenen Daten. Wir müssen sie deshalb nicht schulen.

2. Wie viele Dritte haben Zugang zu Ihren Daten und Systemen, und wie werden sie kontrolliert?

Warum diese Frage wichtig ist: Dazu gehören ausgelagerte Cloud-Anwendungen (z. B. solche, die üblicherweise für die Verwaltung von Kundenbeziehungen oder die Gehaltsabrechnung verwendet werden), Anwendungen oder Systeme, die sich in Ihren Räumlichkeiten befinden, aber von einem Dritten von außerhalb verwaltet werden (z. B. Anlagenüberwachung), oder ausgelagerte Infrastruktur. IT-Sicherheitsmaßnahmen von Drittanbietern sind nicht immer bekannt.
Ihre Kontrollen sind eher allgemeiner Natur. Außerdem zielen fortschrittliche Angriffsmethoden zunehmend auf Zulieferer ab, so dass ein kompromittiertes Mitarbeiterkonto eines Zulieferers eine Hintertür in Ihre Systeme sein könnte. Wenn Ihre Daten und Systeme ausgelagert sind, ist es viel schwieriger herauszufinden, wann diese von einem Ausfall betroffen sind.

Hilfreiche Antwort: Wir haben ein formelles Verfahren zur Überprüfung von Verträgen mit Dienstleistern und deren Konnektivität. Die Anforderungen an die Überprüfung des Personals von Dienstleistern und an die Systemsicherheit sind in den Verträgen enthalten. Der Zugang von Einzelpersonen wird streng kontrolliert, um ihn auf die notwendigen Daten zu beschränken.

Antworten, die weitere Nachfrage erfordern:

- Wir verlassen uns darauf, dass unsere Dienstleister sicher sind.
- Jeder Geschäftszweig verwaltet den Zugang seiner Dienstleister selbst.
- Wir haben keine Auflistung der Daten, zu denen Dienstleister Zugang haben.

3. Haben Sie einen Reaktionsplan für den Fall, dass Sie Ihr eigenes geistiges Eigentum oder das eines Kunden verlieren?

Warum diese Frage wichtig ist: Die Unternehmensleitung muss eingeschaltet werden, wenn die Daten eines Kunden durch einen Angriff gestohlen werden, wenn es zu einer Kompromittierung von personenbezogenen Daten kommt, welche den Betroffenen öffentlich mitgeteilt werden muss, oder wenn ein Mitarbeiter oder eine Mitarbeiterin Informationen über eine solche Kompromittierung durchsickern lässt, die andernfalls nicht veröffentlicht worden wären. Es handelt sich nicht mehr um eine Aufgabe der IT-Sicherheit. Die Rechtsabteilung muss sich mit den rechtlichen Auswirkungen befassen. Die Kommunikationsabteilung muss sich mit der Presse auseinandersetzen. Die verantwortliche Abteilung muss mit den Kunden sprechen. Bei einem Verstoß gegen die Datenschutzbestimmungen muss die Personalabteilung die Mitarbeiter informieren. Und in einigen Branchen sind die Unternehmen für die Meldung von Verstößen bei Dienstleistern verantwortlich, so dass die Abteilungen, die verantwortlich für Lieferketten und Vertragswesen / Beschaffung sind, einbezogen werden müssen. Es muss einen Notfallplan geben, der entsprechend ausgeführt werden muss.

Hilfreiche Antwort: Unser Notfallplan auf Unternehmensebene enthält Bestimmungen für Cyber-Vorfälle, insbesondere für solche, die eine Benachrichtigung von Kunden und/oder Aufsichtsbehörden erfordern würden. Die gesamte Unternehmensleitung ist daran beteiligt. Wir üben und erproben den Plan in regelmäßigen Abständen.

Antworten, die weitere Nachfrage erfordern:

- Hierfür sind die einzelnen Geschäftsbereiche zuständig.
- Jedes potenzielle Ereignis ist so unterschiedlich, dass es sinnlos ist, für jedes davon zu planen.
- Wir sind kein Ziel, also müssen wir auch nicht so aufwendig vorgehen.

Stufe 2.
Zentrale Sicherheitsinfrastruktur und -prozesse

Dies sind einige der besten Praktiken für Unternehmen, die effektiv sein wollen, insbesondere gegen hochmotivierte Angreifende und andere Cyber-Bedrohungen. Die unten aufgeführten Punkte sind für die erfolgreiche

Bewältigung dieser Angriffe von grundlegender Bedeutung. Wenn ein Unternehmen diese drei Praktiken nicht richtig umsetzt, besteht die Gefahr, dass die meisten seiner anderen Bemühungen zum Schutz vor Cyber-Angriffen zunichtegemacht werden.

1. Erlauben Sie, dass irgendetwas in Ihrem Netzwerk direkt mit dem Internet kommuniziert?

Warum diese Frage wichtig ist: Wenn die Computer der einzelnen Mitarbeitenden direkt mit dem Internet kommunizieren können, werden alle Punkte umgangen, an denen der Datenverkehr überwacht oder kontrolliert werden kann. Damit ist das Unternehmen haftbar, wenn es nicht in der Lage ist, schadhaften Datenverkehr auszusortieren oder unangemessenes Surfen zu verhindern. Noch wichtiger ist, dass Angreifende diese Konfiguration ausnutzen können. Sie haben direkten Zugang zu ihren Zielen, ohne dass Ihre Abwehrmechanismen im Weg stehen.

Hilfreiche Antwort: Kein Nutzer oder keine Nutzerin sowie Server kann direkt mit dem Internet kommunizieren. Alles, was wir haben, läuft über eine Art Proxy, um unsere interne Struktur zu verschleiern und eine Kontroll- und Überwachungsstelle zu schaffen.

Antworten, die weitere Nachforschungen erfordern:

- Unsere Ingenieure bestehen auf einem direkten Internetzugang für ihre Recherchen.
- Web-Proxys sind zu teuer.
- Einige unserer Anwendungen benötigen direkten Zugriff. (Ja, die schlecht konzipierten Anwendungen!)

2. Erlauben Sie eine Ein-Faktor-Authentifizierung für den Fernzugriff?

Warum diese Frage wichtig ist: Wenn Angreifende in Ihr Netzwerk eindringen, werden sie als Erstes versuchen, mit einer Reihe von relativ einfachen Methoden Passwörter zu erbeuten. Das gelingt ihnen fast immer. Wenn der VPN-Zugang (Virtual Private Network) oder der E-Mail-Zugang eines Unternehmens nur mit Benutzerkennungen und Passwörtern arbeitet (single factor), müssen sie Ihr Unternehmen nicht mehr komplex angreifen. Sie melden sich schlichtweg als einer Ihrer Mitarbeitenden mit allen entsprechenden Zugängen und Berechtigungen an. Sie werden zu Insidern.

Hilfreiche Antwort: Alle Fernzugriffs-VPNs erfordern eine Zwei-Faktor-Authentifizierung. Bestimmte Webseiten mit Internetzugang können eine Ein-Faktor-Authentifizierung oder keine Authentifizierung haben, nachdem ein Governance-Prozess bestätigt hat, dass die Inhalte der Webseite für die Öffentlichkeit freigegeben werden können.

Antworten, die weitere Nachfrage erfordern:

- Wir haben ein Ein-Faktor-VPN.
- Wir verwenden Outlook Web Access mit nur einem Authentifizierungsfaktor.

3. Wie verwalten Sie Ihre Internet-Gateways?

Warum es wichtig ist: Internet-Gateways sind die erste Linie einer mehrschichtigen Verteidigung. Wenn sie schlecht verwaltet oder konzipiert werden, belastet dies alle anderen Verteidigungsmaßnahmen überproportional. Mehr als an jeder anderen Stelle des Netzes entscheidet hier die Konsistenz über Erfolg oder Misserfolg Ihrer Cyber-Sicherheit. Dies setzt in der Regel eine zentrale IT-Verwaltung voraus, da lokales IT-Personal zu anfällig für Schulungslücken und den Druck der Führungskräfte vor Ort wäre, wichtige, aber unbequeme Kontrollen zu umgehen. Zudem ist eine zentrale IT-Verwaltung auch meist günstiger.

Hilfreiche Antwort: Alle Gateways (unabhängig von der Anzahl) werden von einer zentralen IT-Verwaltung verwaltet, die gemeinsame Tools und Prozesse einsetzt. Dadurch wird sichergestellt, dass unsere Konfigurationen von Routern, Firewalls, Proxys usw. alle einheitlich sind. Alle Protokolle der Gateways werden zur zentralen Überprüfung und Archivierung herangezogen.

Antworten, die weitere Nachfrage erfordern:

- Jede unserer geografischen Regionen bzw. jedes unserer Unternehmen hat seine eigene Organisation.
- Der Internetzugang liegt in der Verantwortung des Standorts.
- Wir haben Standards; wir erwarten, dass unsere Unternehmen/Standorte diese einhalten.

Stufe 3.
Fortgeschrittene Abwehr

Wenn die Antworten auf alle oben genannten Fragen zufriedenstellend sind, kann die Unternehmensleitung einige der weniger verbreiteten, aber höchst effektiven Praktiken, die von den führenden Cyber-Sicherheitsorganisationen empfohlen werden, etwas genauer untersuchen.

1. Wie verwenden und speichern Sie Netflow-Daten?

Warum diese Frage wichtig ist: Netflow-Daten sind der wichtigste Datensatz, den Sie zur Untersuchung von Vorfällen haben. Es handelt sich einfach um eine Aufzeichnung der Metadaten des Datenverkehrs in Ihrem Netz. Welche Adressen haben wann miteinander kommuniziert, welches Protokoll wurde verwendet (E-Mail, Web, Steuerung usw.) und wie viele Daten wurden übertragen. Anhand dieser Daten können Sie die Bewegungen eines oder einer Angreifenden im gesamten Netz verfolgen. Ohne diese Daten sind die Chancen, alle Computer zu finden, auf die der oder die Angreifende zugegriffen hat, gering. Wenn Sie einen kompromittierten Computer übersehen, müssen Sie die Untersuchung in sechs Monaten erneut durchführen.

Hilfreiche Antwort: Wir sammeln Netflow-Daten von fast jedem Router im Netz (nicht nur an den Internet-Gateways). Wir speichern die Daten für mindestens drei Monate (vorzugsweise viel länger) und haben Mitarbeitende, die wissen, wie man die Daten analysiert.

Antworten, die weitere Nachfrage erfordern:

- Was ist Netflow?
- Wir behalten die Daten nur X Tage, weil die Speicherkosten hoch sind.
- Das steht auf unserer To-Do-Liste (das Einschalten und Speichern ist keine technische Herausforderung).

2. Wie verwalten Sie den Lebenszyklus Ihrer IT- und OT-Systeme?

Warum diese Frage wichtig ist: Zahlreiche Cyber-Vorfälle in den letzten zehn Jahren haben gezeigt, dass Systeme, die nicht mit den neuesten Software-Updates aktualisiert werden, ein entscheidender Faktor bei erfolgreichen Kompromittierung von Unternehmen sind. Für Systeme mit nicht gepatchten Sicherheitslücken besteht ein hohes Risiko, das diese von einem Angreifenden ausgenutzt werden, insbesondere wenn die Systeme mit dem Internet verbunden sind. Eine große Anzahl von Systemen, die mit nicht gepatchter oder nicht mehr unterstützter Software betrieben werden, ist auch ein Anzeichen dafür, dass die Organisation möglicherweise nicht über

geeignete technologische Governance-Prozesse verfügt, um umfassendere systemische Risiken in ihrer digitalen Dienstleistungslandschaft zu verwalten.

Hilfreiche Antwort: Unsere Prozesse für das Management von Technologiedienstleistungen stellen sicher, dass alle Systeme auf fehlende Sicherheitsupdates überwacht und gemäß unseren Richtlinien aktualisiert werden. Im Rahmen unseres System-Lebenszyklus-Managements planen wir proaktiv Upgrades oder die Stilllegung von Systemen, die sich dem Ende des Supports durch den Anbieter nähern.

Antworten, die weitere Nachfrage erfordern:

- In unserer Organisation gibt es keine nicht unterstützten Systeme.
- Wir haben keinen vollständigen Überblick darüber, welche Systeme keine Sicherheitsupdates erhalten.
- Lieferant X / Geschäftsbereich Y hat mitgeteilt, dass wir keine Sicherheitsupdates installieren / auf eine neuere Softwareversion aktualisieren können.

3. Gibt es eine zentrale Behörde, die alle Ihre Active Directory-Domänen verwaltet?

Warum diese Frage wichtig ist: Active Directory ist der Durchsetzungsmechanismus für alle Desktop-Sicherheitsrichtlinien. Mit einer einzigen Domäne oder einer kleinen Gruppe zentral verwalteter Domänen können Sie Desktop-Richtlinien konsequent durchsetzen. Außerdem lassen sich so viele Zero-Day-Angriffe schnell entschärfen. Schließlich können Sie verschiedene Tools auf Active Directory-Datenbanken anwenden, um inaktive Objekte (Personen oder Maschinen) zu entfernen. Mehrere, unterschiedliche Datenbanken zu verwalten, mindert die Effizienz.

Hilfreiche Antwort: Wir haben im gesamten Unternehmen eine einzige Domäne (oder sehr wenige). Sie haben alle das gleiche Design und werden von einer zentralen Gruppe von Domänenadministratoren verwaltet.

Antworten, die weitere Nachfrage erfordern:

- Jedes Unternehmen bzw. jede Region betreibt seine eigene Domäne.
- Unsere Administratoren und Administratorinnen (oder Outsourcer) müssen in der Lage sein, Server problemlos aus der Ferne zu verwalten.

4. Wie erhalten Sie verwertbare, nicht klassifizierte Cyber-Informationen?

Warum es wichtig ist: Niemand kann im Bereich der IT-Sicherheit allein erfolgreich sein. Man braucht Mitstreiter. Wenn man schnell über Informationen verfügt und darauf reagiert, kostet das nur wenig, trägt aber wesentlich zum Schutz eines Unternehmens bei, das sich in einer möglichen zweiten Angriffswelle befindet.

Hilfreiche Antwort: Wir sind Mitglied im Informationsaustausch- und Analysezentrum unserer Branche (ISAC/ISAO). Wir haben auch mehrere kommerzielle Bedrohungsdaten gekauft. Wir haben Verfahren, um die Informationen in unsere Netzwerksensoren und -prozesse zu integrieren. Eine weitere gute Antwort wäre, dass: ... unser Sicherheitsdienstleister Zugang zu zahlreichen Informationsquellen hat.

Antworten, die weitere Nachfrage erfordern:

- Wir haben nicht das Fachwissen oder die Verantwortung (Dies ist bei kleineren Unternehmen häufiger der Fall.)
- Wir sind gut genug, dass wir nicht zusammenarbeiten müssen.
- Das tun wir, aber wir haben nicht viel davon. (Man bekommt raus, was man reinsteckt.)

5. Setzen Sie ein Produkt zur Verhinderung von Datenlecks als Teil eines Programms gegen Insider-Bedrohungen ein?

Warum diese Frage wichtig ist: Insider-Bedrohungen werden oft als die schwerwiegendste Cyber-Bedrohung bezeichnet, weil ein Insider bereits über einen längeren Zeitraum Zugang zu den Systemen hatte. Dies gilt umso mehr, wenn man bedenkt, dass ein raffinierter Angreifender, sobald er sich in einem Netzwerk befindet, im Grunde ein Insider ist. Daher wird es immer wichtiger, abnormale oder richtlinienwidrige Aktivitäten zu erkennen. In einigen Branchen, z. B. im Finanzwesen oder in der Pharmazie, ist dies sogar überlebenswichtig.

Hilfreiche Antwort: Als Teil eines größeren Programms setzen wir Systeme zur Verhinderung von Datenlecks auf dem Desktop oder am Perimeter ein. Wir haben eine Gruppe von Mitarbeitenden (entweder in der IT-Sicherheit oder in der industriellen Sicherheit), die die Warnmeldungen überwachen und darauf reagieren.

Antworten, die zusätzliches Nachhaken erfordern:

- Es gibt zu viele falsch positive Ergebnisse. (Dies ist oft der Fall, aber eine gute Abstimmung kann die Anzahl erträglich machen).
- Wir haben es versucht, aber wir haben zu viele private Mitarbeitendeninformationen erhalten.
- Wir wollen nicht wie Big Brother aussehen.

Die wichtigsten Fragen, die die Unternehmensleitung zur Cyber-Sicherheit ihrer Organisation stellen sollte

Zusätzlich zu den detaillierten Fragen, die die Unternehmensleitung zur Cyber-Sicherheit stellen sollte, gibt es auch einige Fragen, die sie bei der Bewertung des Cyber-Risikomanagements der Organisation berücksichtigen sollte:

- Was betrachten wir als unser wertvollstes Gut?
- Wie interagiert unser IT-System mit diesen Werten? Was wäre nötig, um sicher zu sein, dass diese Werte geschützt sind?
- Berücksichtigen wir die Cyber-Sicherheitsaspekte unserer wichtigsten Geschäftsentscheidungen, wie Fusionen und Übernahmen, Partnerschaften, die Einführung neuer Produkte usw., rechtzeitig?
- Wer hat die Verantwortung? Haben wir die richtigen Talente und klare Verantwortlichkeiten für die Cyber-Sicherheit?

TOOL **B**

Die Bedrohung durch Cyber-Insider - eine reale und allgegenwärtige Gefahr

Nach:
Gary McAlum, Chief Security Officer, USAA; Adrian Peters, Chief Technology Risk Officer, BNY Mellon; and J. R. Williamson, Chief Information Security Officer, Leidos

Zielsetzung:
Dieses Tool beschreibt die Arten von Insider-Bedrohungen, mit denen Unternehmen konfrontiert sind, und die Fragen, die sich Unternehmensleitungen stellen sollten.

Der Data Breach Report von Verizon nennt fünf Arten von Cyber-Insider-Bedrohungen[1]:

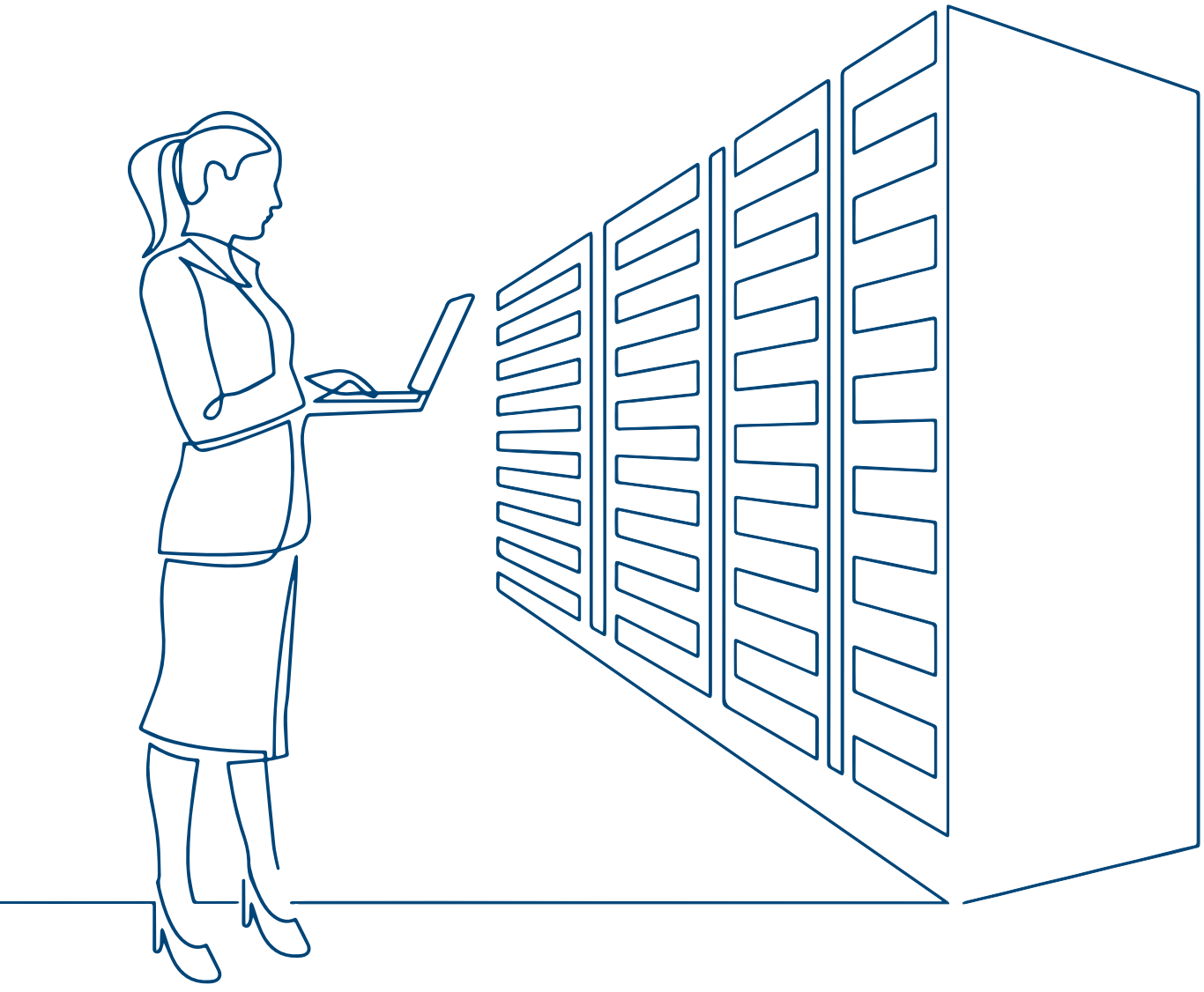
- **Unvorsichtige Mitarbeitende:** Mitarbeitende, die ohne böswillige Absicht Ressourcen missbrauchen, gegen Nutzungsrichtlinien verstoßen, Daten falsch handhaben, nicht zugelassene Anwendungen installieren, usw.
- **Insider-Agenten:** Insider, die von Dritten rekrutiert, umworben oder bestochen werden, um Daten zu exfiltrieren.
- **Verärgerte Mitarbeitende:** Insider, die versuchen, ihrem Unternehmen durch die Zerstörung von Daten oder die Störung von Geschäftsabläufen zu schaden.
- **Böswillige Insider:** Akteure, die ihre Privilegien nutzen, um zum eigenen Vorteil auf Daten zuzugreifen.
- **Rücksichtslose Dritte:** Geschäftspartner, die die Sicherheit durch Nachlässigkeit, Missbrauch oder böswilligen Zugriff auf oder die Nutzung von Anlagen gefährden.

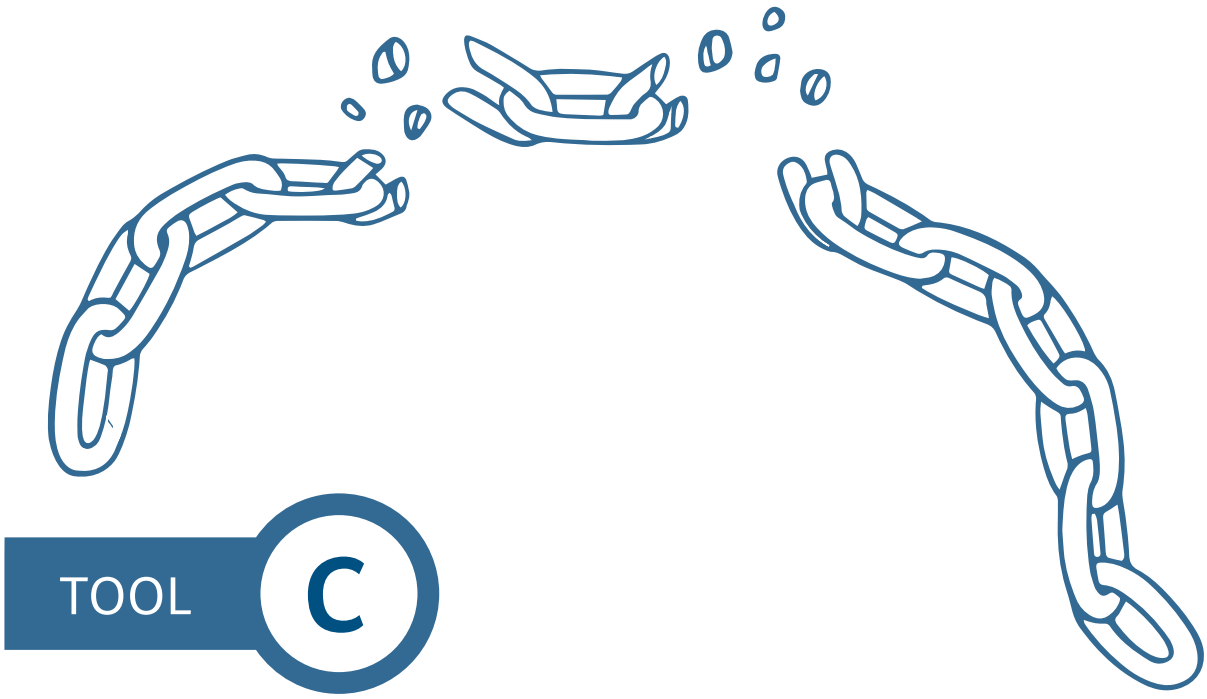
Fragen, die die Unternehmensleitung zu Insider-Bedrohungen stellen sollte:

- Welche Systeme gibt es (Hintergrundüberprüfungen, Kanäle für Mitarbeitende zur Meldung von Bedenken usw.), um Mitarbeitende zu überprüfen und bösartiges Verhalten zu erkennen? Besteht eine enge Zusammenarbeit zwischen der Informationssicherheit, der physischen Sicherheit, der Rechtsabteilung, der Personalabteilung, den Unternehmensermittlungen und anderen wichtigen Partnern bei der Verwaltung dieser Systeme?
- Erhalten die Mitarbeitenden nur Zugang zu Daten und Systemen, die sie für ihre Arbeit benötigen (nicht mehr und nicht weniger)? Wie wird der Zugang verwaltet, wenn ein Mitarbeitende das Unternehmen verlässt oder eine neue Stelle im Unternehmen annimmt?

[1] Verizon (2019). Verizon Insider Threat Report: Aus den Augen aus dem Sinn sollte man nie sein. Online: Verizon, S. 5.

- Weiß das Sicherheitsteam genau, welche Mitarbeitenden über erhöhte Privilegien verfügen, und werden diese überwacht, um sicherzustellen, dass sie ihren Zugang nicht missbrauchen?
- Gibt es Verfahren und Technologien, um zu erkennen und zu verhindern, dass Informationen das Netz verlassen? Wird die Verwendung von Wechseldatenträgern (wie externe Speichermedien) kontrolliert?
- Gibt es eine Richtlinie zur Datenklassifizierung, die eine ordnungsgemäße Kennzeichnung und Handhabung gewährleistet?
- Woher wissen wir, dass unsere Erkennungsversuche funktionieren und wie wirksam sie sind? Testen wir sie regelmäßig mit internen Mitteln und externen Parteien, um sie zu validieren?
- Gibt es einen umfassenden Plan für die Reaktion auf Vorfälle, der alle Beteiligten einbezieht (Personalabteilung, Rechtsabteilung, Compliance, Sicherheit und andere)? Besteht eine enge Beziehung zu Partnern der Strafverfolgungsbehörden für die Reaktion auf Vorfälle? Gibt es interne forensische Fähigkeiten oder wird ein externes Unternehmen beauftragt?
- Verfügen wir über ein Sicherungs- und Wiederherstellungsprogramm? Können wir unsere Systeme und kritischen Daten wiederherstellen, wenn der Zugriff auf das Hauptsystem verhindert wird oder die Daten beschädigt werden? Verfügen wir über strenge Kontrollen in Bezug auf unsere kritischen Lieferantenbeziehungen?





TOOL C

Risiken in der Lieferkette und gegenüber Dritten

Nach:
Lisa Humbert, Operational Risk Officer of the Americas, Bank of Tokyo Mitsubishi, MUFG; and Tim McKnight, Chief Security Officer, SAP

Zielsetzung:
Viele Datenschutzverletzungen werden durch Schwachstellen bei Dritten verursacht. Daher hängt die Stärke der Cyber-Sicherheit eines Unternehmens oft vom schwächsten Glied seiner Lieferkette ab, was sich direkt auf die Rentabilität und den Ruf des Unternehmens auswirken kann. Dieses Tool enthält detaillierte Fragen, die die Unternehmensleitung stellen sollte, um sicherzustellen, dass angemessene Sicherheitsmaßnahmen zur Bewältigung von Risiken in der Lieferkette und anderen Risiken Dritter vorhanden sind.

Das National Institute of Standards and Technology (NIST) definiert **Cyber Supply Chain Risk** Management (C-SCRM) als „den Prozess der Identifizierung, Bewertung und Abschwächung der Risiken, die mit der verteilten und vernetzten Natur von [IT-] Produkt- und Dienstleistungslieferketten verbunden sind."[2]

Third-Party Risk Management (TPRM) ist der standardisierte Prozess, den Unternehmen zur Überwachung und Verwaltung von Risiken im Zusammenhang mit wichtigen Partnern und Anbietern einsetzen.

Cyber-Sicherheitsrisiko in der Lieferkette zu berücksichtigen:

Zusätzlich zu den detaillierten Fragen die Unternehmensleitungen zur Cyber-Sicherheit stellen sollten, gibt - wenn man das große Ganze im Blick hat - Fragen, die Unternehmensleitungen ebenfalls zur Evaluierung des Cyber-Risikomanagements betrachten sollten:

- Jeder neue Anbieter bringt zusätzliche Sicherheitslücken mit sich
- Cyber-Angreifende haben es oft auf Dritte abgesehen, die privilegierten Zugang zum eigentlichen Zielunternehmen haben.
- Verstehen, welche Lieferanten über Daten verfügen, wo sie gespeichert sind und wer Zugang zu ihnen hat
- Überprüfung der Datenqualität und Abbildung des Datenflusses
- Vertragsverhandlungen und Kündigungen
- Qualifikationsniveau der Mitarbeitenden
- Unterauftragnehmende
- Alter der Verträge
- Interner Reifegrad der Cyber-Sicherheit
- End-to-End-Prozessmanagement und -Überwachung

[2] National Institute of Standards and Technology (2022). Cybersecurity Supply Chain Risk Management. Online: NIST.

Fragen, die die Unternehmensleitung stellen kann, um den Ansatz des Unternehmens zum Cyber Supply-Chain-Risikomanagement zu bewerten

1. Wie können wir die finanziellen Möglichkeiten (niedrigere Kosten, höhere Effizienz usw.), die sich aus einer größeren Flexibilität der Lieferkette ergeben, mit potenziell höheren Cyber-Risiken in Einklang bringen? Hier sind einige Punkte zu bedenken:
   - **a.** Risiko- und Ertragsanalyse und Berücksichtigung von Cyber-Sicherheitsmanagement und Informationstechnologie-Governance bei der Berechnung der Gesamtbetriebskosten
   - **b.** Verhandlungsstrategien einschließlich der Bestimmungen zur Cyber-Sicherheitsversicherung
   - **c.** Umsetzung von Service-Level-Vereinbarungen einschließlich der Anforderungen an Berichterstattung, Messgrößen und laufende Überwachung

2. Was müssen wir tun, um die Cyber-Sicherheit vollständig in das aktuelle Risikomanagement der Lieferkette einzubeziehen? Hier sind einige Punkte zu berücksichtigen:
   - **a.** Schulung des Personals in der Lieferkette zur Erkennung von Cyber-Sicherheitsrisiken und zur Ermöglichung von Abhilfemaßnahmen
   - **b.** Due-Diligence-Prüfung durch Dritte während des gesamten Angebots-, Auswahl- und Onboarding-Prozesses
   - **c.** Fachwissen im Bereich Cyber-Sicherheit wird während des Verhandlungs- und Vertragsprozesses genutzt

3. Wie werden Cyber-Sicherheitsanforderungen in Verträgen und Service-Level-Agreements verankert? Wie werden sie durchgesetzt? In Verträgen und Service-Level-Vereinbarungen können Anforderungen für Folgendes festgelegt werden:
   - **a.** Bestimmungen zur Cyber-Sicherheitsversicherung
   - **b.** Personalpolitik, z. B. Hintergrundüberprüfungen, Schulungen usw.
   - **c.** Zugangskontrollen
   - **d.** Verschlüsselungs-, Sicherungs- und Wiederherstellungsrichtlinien
   - **e.** Sekundärer Zugang zu Daten
   - **f.** Einsatz von Subunternehmen und Anforderungen
   - **g.** Länder, in denen die Daten gespeichert werden
   - **h.** Datensicherheitsstandards und Meldepflichten bei Datenschutzverletzungen oder anderen Cyber-Vorfällen
   - **i.** Pläne für die Reaktion auf Unfälle
   - **j.** Audits der Cyber-Sicherheitspraktiken und/oder regelmäßige Zertifizierungen der Einhaltung der Vorschriften
   - **k.** Teilnahme an Tests und Kontingenzaktivitäten
   - **i.** Anforderungen an die rechtzeitige Rückgabe/Vernichtung von Daten bei Kündigung

4. Bieten unsere Lieferantenvereinbarungen angemessene Kontrollen für rechtliche Risiken und Compliance-Anforderungen? Welches sind die nationalen rechtlichen Anforderungen, die die Lieferkette betreffen? Hier sind einige Punkte zu berücksichtigen:
   - **a.** Zugang zu vertraulichen oder geschützten Daten, persönlich identifizierbaren Informationen (PII), sensiblen persönlichen Informationen (SPI) oder Umgang mit persönlichen Gesundheitsinformationen
   - **b.** Daten, die für regulatorische, finanzielle oder andere interne Berichte verwendet werden und von einem Dritten bereitgestellt werden
   - **c.** Einhaltung von Gesetzen, Vorschriften, Richtlinien und behördlichen Anleitungen durch Dritte

Beispiel: Europäische Bankenaufsichtsbehörde von Microsoft Exchange-Hack betroffen

Die E-Mail-Server der Europäischen Bankaufsichtsbehörde wurden durch einen weltweiten Cyber-Angriff auf Microsoft Exchange kompromittiert. Die EU-Behörde teilte mit, dass möglicherweise personenbezogene Daten von ihren Servern abgegriffen worden sind. Sie hat ihr gesamtes E-Mail-System vom Netz genommen, um den Schaden zu bewerten.

Quelle: Spiegel.

Quelle: bbc, https://www.bbc.com/news/technology-56321567

5. Sind wir gegen Sicherheitsvorfälle bei unseren Lieferanten/Anbietern abgesichert? Hier sind einige Punkte zu beachten:
   a. Sicherheitslücken, Vorfälle und Schwachstellen
   b. Begrenzung der Haftung
   c. Verstöße gegen das geistige Eigentum

Fragen, die die Unternehmensleitung stellen muss, um den Ansatz des Unternehmens für das Risikomanagement gegenüber Dritten zu bewerten

1. Was muss getan werden, um die Cyber-Sicherheit vollständig in das aktuelle Risikomanagement für Dritte einzubeziehen? Hier sind einige Punkte zu berücksichtigen:
   a. Erstmalige und laufende Überwachung der Einhaltung der Vorschriften durch Dritte und des Kontrollumfelds
   b. Bewertungsprozess und -rhythmus, um Schwachstellen und Bedrohungen zu ermitteln und zu beheben
   c. Qualifiziertes Personal, das mit der Überwachung und Beaufsichtigung der Drittpartei betraut ist

Beispiel: Mehr als 80.000 ISOC-Mitglieder von Datenschutzverletzungen Dritter betroffen

Bei der Internet Society, einer gemeinnützigen Organisation, die sich für ein offenes und sicheres Internet einsetzt, kam es zu einem weitreichenden Datenschutzvorfall durch Dritte, bei dem über 80.000 personenbezogene Daten von Mitgliedern betroffen waren.

Quelle: Security Boulevard.

2. Wie überwachen wir die Einhaltung der betrieblichen und rechtlichen Anforderungen? Hier sind einige Punkte zu beachten:
   a. Berichterstattung und Prüfung
   b. Vor-Ort- und Fernbewertungen
   c. Regelmäßige Geschäftsüberprüfungen mit der Drittpartei

3. Verfügen wir über die richtigen Fähigkeiten, um Bewertungen, Tests und die laufende Überwachung unserer Drittparteien durchzuführen? Hier sind einige Punkte zu beachten:
   a. Schaffung eines Rahmens für das Risikomanagement, einschließlich definierter Rollen und Verantwortlichkeiten
   b. Angemessenes Verständnis der von der dritten Partei angebotenen Produkte und Dienstleistungen
   c. Verständnis der externen regulatorischen Vorgaben und der Auswirkungen auf die Produkte und Dienstleistungen Dritter

4. Wie schwierig/kostenintensiv wird es sein, die Überwachung der Zugangspunkte im Lieferantennetz zu verbessern? Hier sind einige Punkte zu berücksichtigen:
   a. Schutzbedarf und Verfügbarkeit von Daten
   b. Mehrschichtige Bewertung der Datenqualität und des Datenzuflusses/-abflusses
   c. Zugang zum Lieferantennetz

5. Wie schwierig/kostspielig wird es sein, ein praktikables Cyber-Sicherheitsprogramm für unsere Risiken gegenüber Dritten einzurichten und aufrechtzuerhalten? Hier sind einige Punkte zu berücksichtigen:
   a. Technologie und Infrastruktur
   b. Organisatorische Personalausstattung
   c. Regelmäßige funktionsübergreifende Zusammenarbeit mit den Beteiligten, um wirksame Zugangskontrollen zu gewährleisten.

TOOL D

Reaktion auf Vorfälle

Nach:
Nasrin Rezai, Global Chief Information and Product Cybersecurity Officer, General Electric; and Greg Montana, Chief Risk Officer, FIS

Zielsetzung:
Die Fähigkeit, auf Vorfälle zu reagieren, ist notwendig, um Ereignisse und Zwischenfälle schnell zu erkennen, Verluste und Zerstörungen zu minimieren, die ausgenutzten Schwachstellen zu entschärfen und die Geschäftsdienste wiederherzustellen. Dieses Toolkit beschreibt die Schritte, die Unternehmensleitung durchführen sollte, um sicherzustellen, dass ihre Organisationen über ein effektives Programm zur Reaktion auf Vorfälle verfügen.

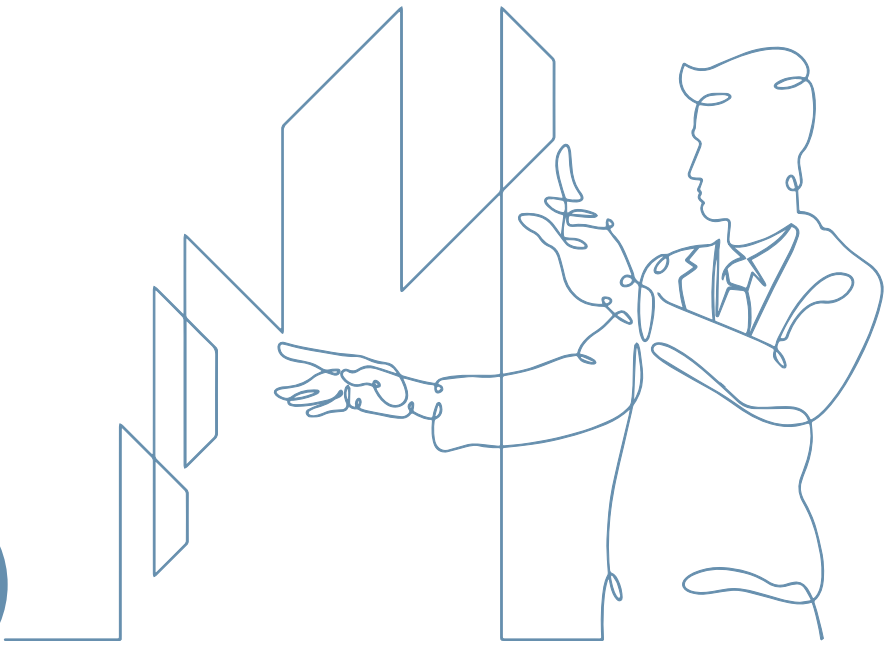
Die zur Unterstützung der Reaktion auf Vorfälle erforderlichen Fähigkeiten und Funktionen sind:

- **Verwaltung:** Kenntnis der Vermögenswerte und ihres Verbleibs mit entsprechenden Kontrollen, Datenschutz und regelmäßiger Risikobewertung und -verwaltung
- **Schutzfähigkeiten:** Richtlinien, Sensibilisierung und Schulung der Mitarbeitenden, Kontrollverfahren zur Überprüfung des Zugangs, Verfahren zum Schutz von Informationen und kontinuierliche Überprüfung:
- **Erkennung:** Fähigkeiten zur Erkennung von Anomalien und Ereignissen sowie zur kontinuierlichen Überwachung der Wirksamkeit
- **Reaktion:** Reaktionsplan, regelmäßige Cyber-Übungen, koordinierte Bemühungen zwischen Technologie-Teams, Unternehmen, Rechtsabteilung, Kommunikation und Strafverfolgungsbehörden
- **Wiederherstellen:** Rasche Abhilfe und Nachbesserung

Fragen, die die Unternehmensleitung zur Reaktion auf Zwischenfälle stellen sollte:

1. Gibt es einen Plan mit einer klaren Definition von Ereignissen, Rollen und Verantwortlichkeiten sowie Eskalationsprozessen? Sind zentrale Unternehmensfunktionen wie IT, Wirtschaft, Recht und Kommunikation in den Reaktionsplan integriert? Wie fügt er sich in den Krisen- und Geschäftswiederherstellungsplan des Unternehmens ein?
2. Welches sind die Eskalationskriterien für die Benachrichtigung der obersten Führungsebene und des Vorstands, falls erforderlich? Wer hat die endgültige Entscheidungsbefugnis?
3. Wird die Widerstandsfähigkeit Unternehmens und der Organisationen anhand großer Risikoszenarien getestet, die durch Übungen und gemeinsame Bedrohungssimulationen geübt werden?

4. Gibt es etablierte Beziehungen zu Sicherheitsbehörden, Strafverfolgungsbehörden und wichtigen Regulierungsbehörden? Gibt es Beziehungen zum Informationsaustausch durch Informationsaustausch- und Analysezentren und Konsortien und andere Unternehmen?
5. Kennt die Organisation die Melde- und Berichtspflichten (z. B. US Securities and Exchange Commission, General Data Protection Regulation, BSI-Gesetz, Verteidigungsministerium und Defense Security Service für geprüfte Auftragnehmer und die Bundesregierung) und behält sie im Auge? Wie lauten sie?
6. Welches sind die Kriterien und wie sieht das Verfahren zur Offenlegung von Vorfällen gegenüber Investoren aus?
7. Was können wir tun, um die Verluste durch einen Vorfall zu verringern?
8. Welches sind die wichtigsten Leistungsindikatoren, um die Wirksamkeit der Reaktion auf Vorfälle zu messen (z. B. Zeit bis zur Entdeckung und Zeit bis zur Reaktion)?
9. Welche wichtigen Schritte unternehmen wir nach einem kritischen Zwischenfall? Welche Schritte unternehmen wir, um sicherzustellen, dass sich ein solcher Vorfall nicht wiederholt? Was hat die Organisation aus dem Vorfall gelernt?



TOOL E

Metriken zur Cyber-Sicherheit auf Ebene der Unternehmensleitung"

Nach:
John Frazzini, President and CEO, Secure Systems Innovation Corp.; Robert Gardner, Direct Computer Resources; Lou DeSorbo, Chief Security and Risk Officer, Centene Corp.; Geoji Paul, Director Security Risk Management, Centene Corp.; and Nick Corzine, Manager Cyber Risk Computation, Centene Corp.

Zielsetzung:
Dieses Tool beschreibt, wie Metriken verwendet werden können, um die Effektivität von Cyber-Sicherheitsprogrammen zu messen und gibt Ratschläge, wie Unternehmensleitungen diese Metriken nutzen können, um die Cyber-Sicherheitsprogramme ihrer Organisation zu überwachen.

Moderne Unternehmen sind zunehmend datengesteuert. Metriken können auch für die Cyber-Sicherheit verwendet werden. Angesichts der Komplexität von Cyber-Sicherheitsproblemen können verschiedene Arten von Metriken für spezifische Geschäftsthemen besser geeignet sein als allgemeinere Cyber-Sicherheitsmetriken.

Kennzahlen auf Ebene der Unternehmensleitung sollten Veränderungen, Trends und Muster im Laufe der Zeit aufzeigen, die relative Leistung darstellen und die Auswirkungen aufzeigen. All dies muss im Zusammenhang mit den Geschäftszielen des Unternehmens dargestellt werden. Externe Penetrationstestunternehmen und Drittparteiexperten können möglicherweise effektive Benchmarks innerhalb der Branche liefern.

Leitprinzipien für Metriken auf Vorstandsebene

- Relevant für die Zielgruppe (Unternehmensleitung)
- Leserfreundlich: Zusammenfassungen, Aufzählungen, Grafiken und andere visuelle Elemente verwenden; Fachjargon vermeiden
- Bedeutung vermitteln: Erkenntnisse vermitteln, nicht nur Informationen
- Aufzeigen von Veränderungen, Trends und Mustern im Laufe der Zeit
- Darstellung der relativen Leistung im Vergleich zu Gleichaltrigen, zum Branchendurchschnitt, zu anderen relevanten externen Indikatoren usw. (wie z. B. Reifegradbewertung)
- Geben Sie die Auswirkungen auf Geschäftsbetrieb, Kosten, Marktanteil usw. an.
- Kurz und bündig: Vermeidung von Informationsüberflutung
- Vor allem: Diskussion und Dialog ermöglichen

Quelle: NACD

In diesem Tool werden Fragen erläutert, die Unternehmensleitende dem Management stellen sollten, um sicherzustellen, dass die richtigen Kennzahlen zum Cyber-Risiko des Unternehmens erfasst werden.

Organisationen können nun den Beitrag des Unternehmens zum Cyber-Risiko (positiv und negativ) auf der Grundlage des Reifegrads ihres gesamten Cyber-Sicherheitsprogramms messen.

Fragen zu operativen Metriken:

Herkömmliche operative Kennzahlen bieten wenig strategischen Kontext oder Informationen über Leistung und Risikoposition. Sie können jedoch hilfreich sein, um der Unternehmensleitung zu helfen, kritische Compliance-Probleme zu verstehen und nützliche Diskussionen über Trends, Muster und Grundursachen anzuregen sowie ein Benchmarking mit anderen Unternehmen der Branche durchzuführen. Im Folgenden finden sich Beispiele für Fragen, die die Unternehmensleitung dem Management zu operativen Kennzahlen stellen kann:

- Welche operativen Messgrößen verfolgen wir und warum?
- Wie viele nicht gepatchte Sicherheitslücken haben wir in kritischen Systemen und warum?
- Wie viele blockierte Angriffe haben wir im letzten Quartal abgewehrt?
- Wie viele Datenvorfälle (z. B. Offenlegung sensibler Daten) hat die Organisation im letzten Berichtszeitraum erlebt?
- Wie sieht unser Budget für Cyber-Sicherheit im Vergleich zu anderen in unserer Branche aus?
- Welche Sicherheitsmaßnahmen wurden vorgeschlagen und nicht finanziert? Was waren die Kompromisse?
- Welche Messgrößen verwendet das Management zur Berechnung des Cyber-Risikos?
- Wie lange dauert es, bis wir ein erhebliches Cyber-Sicherheitsrisiko entdecken und beseitigen?
- Wie viel Prozent unserer Lieferkette sind bei der Cyber-Sicherheitsbewertung durchgefallen?

Fragen zu Metriken, die für bestimmte Unternehmensprogramme relevant sind:

- Wie wahrscheinlich ist es auf der Grundlage der bestmöglich verfügbaren Daten, dass es bei diesem Projekt zu einem Vorfall im Bereich der Cyber-Sicherheit kommt, der so schwerwiegend wäre, dass die Unternehmensleitung eingeschaltet werden muss?
- Wie hoch wären die zu erwartenden Kosten, wenn man die wahrscheinlichste, die unwahrscheinlichste und die durchschnittliche Wahrscheinlichkeit eines Cyber-Sicherheitsvorfalls bei diesem Projekt annimmt? (Monte-Carlo-Simulationen können bei dieser Ermittlung hilfreich sein).
- Wie hoch wären die Kosten für die Abschwächung oder Verlagerung dieses Cyber-Sicherheitsrisikos auf ein Niveau, das mit unserer Risikobereitschaft vereinbar ist?
- Welche Schlüsselfaktoren tragen am meisten zur Eintrittswahrscheinlichkeit des Risikos und zu den Auswirkungen der Verwirklichung des Cyber-Sicherheitsrisikos bei, und wie sehen unsere Strategien zur Minderung dieser Faktoren aus?

Fragen zu strategischen Metriken:

Die Unternehmensleitung sollte das Management auch nach strategischen Kennzahlen fragen, die sich auf den Sicherheits- und Risikoansatz des Unternehmens beziehen. Im Folgenden finden sich Beispiele für Fragen, die Sie berücksichtigen sollten:

- Wie hoch ist unsere Risikobereitschaft, und wie wird sie gemessen? (Siehe Prinzip 5.)
- Wie können wir die Wirksamkeit unseres Cyber-Sicherheitsprogramms messen?
- Wie messen wir den Reifegrad unserer Cyber-Sicherheit?
- Wie messen wir den Beitrag des Cyber-Sicherheitsrisikos zu den damit verbundenen Unternehmensrisiken?
- Welche Messgrößen verwenden wir, um die Sicherheit unserer Drittanbieter und Dienstleister (Lieferanten, Partner, Kunden usw.) zu messen?
- Welche Messgrößen verwenden wir, um das Bewusstsein der Mitarbeitenden und die Einhaltung der Cyber-Sicherheitsrichtlinien zu überwachen?
- Wie sieht der Prüfungsplan der Innenrevision im Bereich der Cyber-Sicherheit aus?
- Was sind die Ergebnisse der letzten Überprüfungen?
- Welche Fortschritte wurden bei der Umsetzung der Ergebnisse erzielt?
- Ist geplant, einen externen Prüfer zu beauftragen, der eine unabhängige Bewertung des Cyber-Sicherheits-Risikomanagementprogramms des Unternehmens vornimmt?
- Wie verfolgen wir Management- oder andere Ausnahmen von den organisatorischen Cyber-Sicherheitsanforderungen?

TOOL F

Im regelmäßigen Austausch mit CISO/ IT-Sicherheitsbeauftragten

Nach:
Jeff Brown, Chief Information Security Officer, Raytheon

Zielsetzung:
In dem Maße, in dem die Funktionen der Informationssicherheit in Unternehmen reifen, müssen sich die Mitglieder der Unternehmensleitung fragen, wie sie effektiv mit dem Sicherheitsbeauftragten kommunizieren können. Der Aufbau von Vertrauen und Vertrautheit zwischen dem Vorstand und dem CISO ist von entscheidender Bedeutung. Dieses Tool bietet eine Anleitung, wie Vorstände eine effektivere Arbeitsbeziehung zum CISO und dem Sicherheitsteam ihres Unternehmens aufbauen können.

Dieses Tool ist ein Leitfaden für Unternehmensleitungen, um einen regelmäßigen, vertrauensvollen Austausch mit dem CISO und dem Sicherheitsteam aufzubauen oder zu verbessern. Die nachstehenden Fragen und Leitlinien können der Unternehmensleitung dabei helfen, eine Arbeitsbeziehung zum CISO aufzubauen oder zu verbessern und so ein besseres Verständnis für den Gesamtansatz des Unternehmens im Bereich der Cyber-Sicherheit zu erlangen.

Die Rolle und das Mandat des CISO verstehen:

1. Wie sieht die Charta und der Zuständigkeitsbereich des CISO in Bezug auf Ressourcen, Entscheidungsrechte, Budget, Personalausstattung und Zugang zu Informationen aus? Wie sieht dies im Vergleich zu führenden Praktiken in unserer Branche und im Allgemeinen aus?[3]

2. Wem ist der CISO unterstellt?
   → Es gibt keinen klaren Branchenkonsens zu diesem Thema. Ein großer Prozentsatz untersteht dem CIO oder dem technischen Leiter[4], obwohl sich die Meinung durchsetzt (die bereits in dieser Veröffentlichung geäußert wurde), dass die Unterstellung unter den CIO möglicherweise nicht die richtige Antwort ist. Es ist sicherlich richtig, dass ein CIO in einen Interessenkonflikt zwischen dem Druck der IT-Dienstleistungserbringung und der Sicherheit geraten kann. Dies ist abzuwägen gegen den Wert eines Vorgesetzten des CISO, der die Technologie und die Risiken versteht und in der Lage ist, Kompromisse zu schließen, ohne die Angelegenheit an den CEO weiterzuleiten. Unabhängig davon, welche Option sich langfristig durchsetzt, ist der entscheidende

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

[4] Hitch Partners (2022). Hitch Partners CISO Survey Results. Online: Hitch Partners.

Faktor nicht, wem der CISO unterstellt ist, sondern ob diese Person eine starke Stimme im Führungsteam hat, um sich für die Sicherheit einzusetzen. Wenn die Person, die den CISO auf der Führungsebene vertritt, den CEO und den CFO nicht beeinflussen kann, kann ein Sicherheitsprogramm keinen Erfolg haben.

3. Wie wird das Cyber-Sicherheitsbudget des Unternehmens ermittelt? Ein Vergleich dieser Zahl mit Ausgabentrends in der Branche ist wahrscheinlich der beste Weg, um einen Überblick über die Angemessenheit der Finanzierung zu erhalten. Wie hoch ist der Betrag (z. B. in Prozent der gesamten IT-Ausgaben), und wie verhält er sich im Vergleich zu den führenden Praktiken in der Branche des Unternehmens und im Allgemeinen?

4. Wie viel der Sicherheitsinfrastruktur liegt außerhalb des Budgets oder der Weisungsbefugnis des CISO?
   → Die Bedrohungen entwickeln sich immer schneller als der Budgetzyklus. Wenn ein CISO in der Lage ist, andere in der IT-Organisation häufig zu bitten, ihre Jahrespläne zu ändern, um neuen Sicherheitsanforderungen gerecht zu werden, erhöht sich die Wahrscheinlichkeit, dass die Änderungen abgelehnt werden. Umgekehrt gilt: Je mehr der CISO in der Lage ist, diese Budgetabwägungen intern in Echtzeit vorzunehmen, desto schneller kann er reagieren und desto geringer ist das Risiko.

5. Welche Sicherheitsinstrumente oder sonstigen Investitionen wurden im Haushalt nicht berücksichtigt?
   → Das Management ist immer bereit, der Unternehmensleitung zu sagen, was es tut, aber es ist weniger bereit, darüber zu sprechen, was es nicht tut (d.h. welche schwierigen Budgetentscheidungen es treffen musste, die zur Akzeptanz von Risiken führten). Ein Gespräch darüber, was unter die Kürzungsgrenze fiel und welcher Entscheidungsprozess zur Bewertung der Kompromisse angewandt wurde, ist immer aufschlussreich.

6. Welche Rolle spielt der CISO in der ERM-Struktur (Enterprise Risk Management) des Unternehmens und bei der Implementierung von ERM-Prozessen?

7. Welche Rolle spielt der CISO, wenn überhaupt, bei der Festlegung und Durchsetzung von Cyber-Sicherheitsrichtlinien für das Unternehmensnetzwerk und den zugehörigen Kontrollsystemen?

8. Leistet der CISO einen Beitrag zum Entwicklungsprozess für neue Produkte, Dienstleistungen und Systeme oder zur Gestaltung von Partnerschafts- und Allianzvereinbarungen usw., so dass die Cyber-Sicherheit „eingebaut“ ist und nicht nachträglich „hinzugefügt“ wird?

9. Spielt der CISO eine Rolle bei der Bewertung des Cyberrisikos von Akquisitionen während der Due Diligence?

Um Beziehungen zum CISO und zum Sicherheitsteam aufzubauen oder zu vertiefen, sollte die Unternehmensleitung einen Besuch beim Sicherheitsteam arrangieren und sich aus erster Hand von Mitarbeitenden, die an der vordersten Front der Cyber-Sicherheit stehen, informieren lassen.

Einen Einblick in das Beziehungsnetz des CISO gewinnen:

Innerhalb der Organisation:

1. Wie arbeitet der CISO oder das Informationssicherheitsteam mit anderen Abteilungen und Unternehmensfunktionen in Fragen der Cyber-Sicherheit zusammen?

2. Koordiniert der CISO beispielsweise die Due-Diligence-Prüfung mit der Unternehmensentwicklung?
   a. Übernahmeziele und Partnerschaftsvereinbarungen;
   b. die Innenrevision bei der Bewertung und Prüfung der Kontrollsysteme und -strategien;
   c. die Personalabteilung bei der Schulung der Mitarbeitenden und den Zugangsprotokollen;
   d. Einkauf und Lieferkette in Bezug auf Cyber-Sicherheitsprotokolle mit Verkäufern, Kunden und Lieferanten;
   e. Rechtsabteilung in Bezug auf die Einhaltung von Vorschriften und Berichterstattungsstandards im Zusammenhang mit der Cyber-Sicherheit und dem Datenschutz?

Außerhalb der Organisation:

1. Nimmt der CISO oder das Informationssicherheitsteam an Initiativen zum Informationsaustausch im Bereich Cyber-Sicherheit teil (z. B. branchenbezogene, auf die IT-Gemeinschaft ausgerichtete oder öffentlich-private Partnerschaften[5])? Wie werden die Informationen, die durch die Teilnahme an solchen Initiativen gesammelt werden, innerhalb der Organisation genutzt und weitergegeben?

2. Verfügt der CISO (oder das Informationssicherheitsteam) über Beziehungen zu öffentlichen Akteuren wie Strafverfolgungsbehörden (z. B. Landeskriminalamt), Cyber-Sicherheitsabteilungen von Aufsichtsbehörden, dem deutschen CERT-Bund usw.?

Innerhalb und außerhalb der Organisation:

1. Wie entwickelt und pflegt der CISO oder das Informationssicherheitsteam Kenntnisse über die strategischen Ziele, das Geschäftsmodell und die betrieblichen Aktivitäten des Unternehmens? Inwieweit versteht der CISO beispielsweise in Unternehmen, die aktiv eine „Big-Data"-Strategie zur Verbesserung der Kunden- und Produktanalyse verfolgen, die Strategie und trägt zu ihrer sicheren Umsetzung bei?

2. Welche Weiterbildungsmaßnahmen werden vom CISO oder dem Informationssicherheitsteam durchgeführt, um in Fragen der Cyber-Sicherheit auf dem neuesten Stand zu bleiben?

Leistung bewerten:

1. Wie wird die Leistung des CISOs bewertet? Wie wird die Leistung des Informationssicherheitsteams bewertet? Wer führt diese Bewertungen durch, und welche Messgrößen werden verwendet?

2. Welche Leistungsmaßnahmen und Meilensteine für die Cyber-Sicherheit wurden für die gesamte Organisation festgelegt? Verwenden wir einen risikobasierten Ansatz, der ein Höchstmaß an Schutz für die wertvollsten und kritischsten Vermögenswerte der Organisation gewährleistet?

3. Inwieweit sind die Aktivitäten zur Bewertung und Verwaltung von Cyber-Risiken in die unternehmensweiten Risikomanagementprozesse der Organisation integriert? Verwenden wir die Rahmenwerke des National Institute of Standards and Technology (NIST), der Internationalen Organisation für Normung (ISO) oder andere ähnliche Rahmenwerke, um die Cyber-Sicherheitshygiene aus einer unternehmensweiten Perspektive zu bewerten?

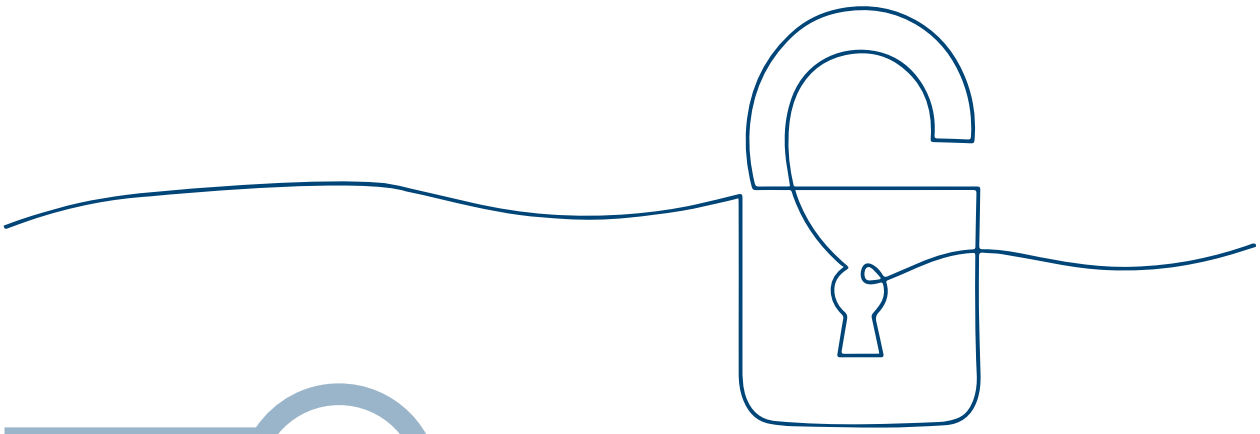
Beziehen Sie den CISO in eine Diskussion über den Zustand der Organisation ein:

1. Was war der wichtigste Vorfall im Bereich der Cyber-Sicherheit im vergangenen Quartal? Wie wurde er entdeckt? Wie haben wir darauf reagiert? Wie war die Geschwindigkeit der Erkennung und Wiederherstellung im Vergleich zu früheren Vorfällen? Welche Lehren haben wir daraus gezogen, und wie werden diese in die kontinuierlichen Verbesserungsbemühungen der Organisation einbezogen?

2. Wo haben wir in den letzten sechs Monaten die größten Fortschritte bei der Cyber-Sicherheit gemacht, und auf welche Faktoren sind diese Fortschritte zurückzuführen? Wo gibt es noch die größten Lücken und wie sieht unser Plan aus, um diese Lücken zu schließen?

3. Welche Organisationen oder Standorte wurden aus geschäftlichen Gründen von einer oder mehreren Cyber-Sicherheitskontrollen ausgenommen? Beispielsweise werden kritische Anwendungen nur während der vierteljährlichen Wartungsfenster gepatcht, Forschungseinrichtungen umgehen die Internetfilterung oder Fabriken werden nicht gescannt. Solche Ausnahmen von Richtlinien und Kontrollen erhöhen das Gesamtrisiko für das Unternehmen. Unabhängig davon, ob solche Ausnahmen berechtigt sind, müssen sich die Geschäftsleitung und der Vorstand über das Ausmaß des Risikos im Klaren sein.

[5] Siehe z. B. die Webseite der Allianz für Cyber-Sicherheit.



TOOL G

Verbesserung der Offenlegung von Informationen zur Cyber-Sicherheit – 10 Fragen für die Unternehmensleitung[6]

Nach:
Robyn Bew, Center for Board Matters, EY

Zielsetzung:
Wie in Prinzip 2 erörtert, sollten die Mitglieder der Unternehmensleitung die rechtlichen Auswirkungen von Cyber-Risiken in Bezug auf die spezifischen Umstände ihres Unternehmens verstehen, einschließlich möglicher Anforderungen in Bezug auf die Offenlegung. Dieses Tool enthält 10 Fragen, die die Unternehmensleitung stellen kann, um die Offenlegung der Cyber-Sicherheit in ihrem Unternehmen zu verbessern.

Die Stakeholder wollen besser verstehen, wie sich Unternehmen auf Vorfälle im Bereich der Cyber-Sicherheit vorbereiten und darauf reagieren. Sie möchten auch verstehen, wie die Unternehmensleitung diese kritischen Risikomanagementmaßnahmen überwachen. Als Reaktion darauf verbessern viele Unternehmen ihre Angaben zur Cyber-Sicherheit, wobei die wichtigsten Änderungen die Aufsichtspraktiken des Vorstands betreffen.

Die nachstehenden Fragen können vom Management als Grundlage für Diskussionen mit der Unternehmensleitung über Möglichkeiten zur Verbesserung der Kommunikation mit Investoren und anderen Stakeholdern im Bereich der Cyber-Sicherheit verwendet werden:

1. Verstehen wir die Prioritäten der wichtigsten Investoren unseres Unternehmens in Bezug auf Cyber-Sicherheit, Datenschutz und andere wichtige Risiko- und Strategiefragen?

2. Wissen wir, wie hoch der finanzielle Wert der Cyber-Sicherheit ist? Wie kann die Organisation wirtschaftliche Risikobewertungen nutzen, um den Mehrwert von Cyber-Sicherheitskontrollen zu ermitteln und festzustellen, ob die Kontrollen wirksam und kosteneffizient sind?

3. Welche Rückmeldungen haben das Managementteam und/oder Investor Relations von unseren Hauptinvestoren erhalten? Welche Fragen stellen unsere Investoren über den Umgang des Unternehmens mit Informationssicherheit und Datenschutz?

4. Wie nutzt das Unternehmen die Offenlegung, um Investoren und anderen Stakeholdern die Strenge unseres Cyber-Sicherheits-Risikomanagementprogramms

[6] Content adapted from EY (2019). What Companies are sharing about cybersecurity risk and oversight. Online: EY.

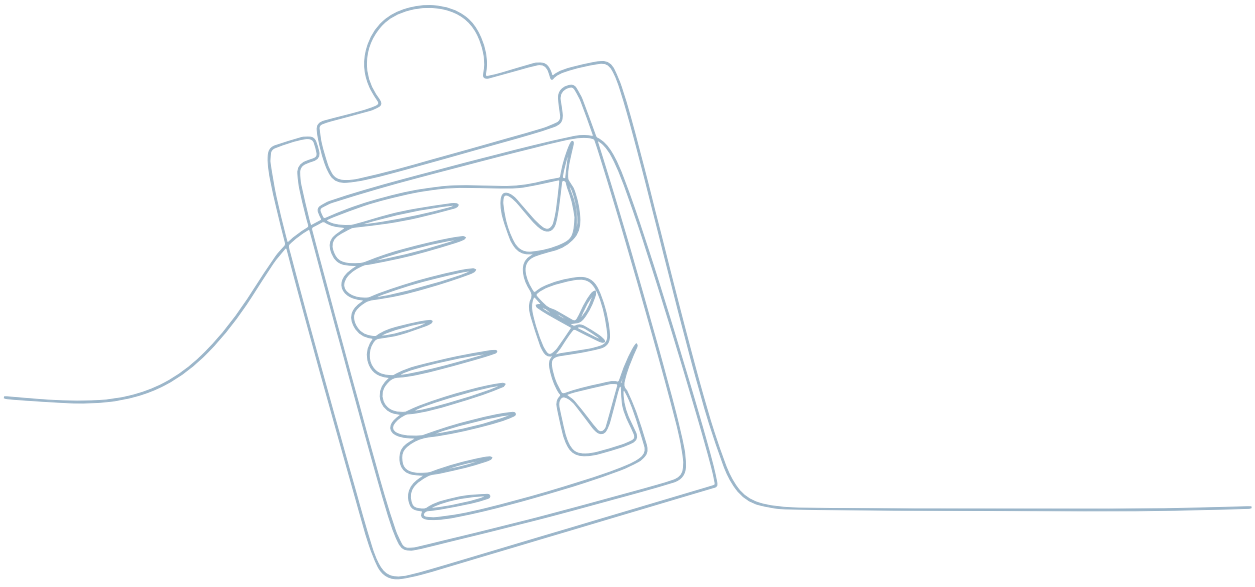
und die damit verbundenen Aufsichtsaktivitäten des Vorstands effektiv zu vermitteln? Im Einzelnen:

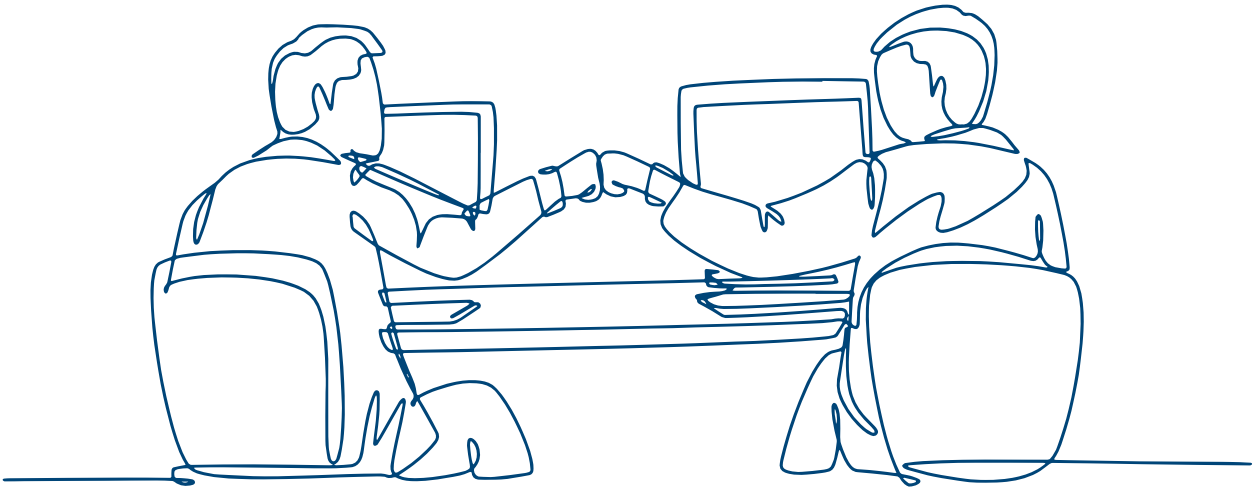
- **a.** Wird die Cyber-Sicherheit im Abschnitt über die Risikoüberwachung in der Vollmachtserklärung erwähnt?
- **b.** Beschreiben wir, welcher Teil der Unternehmensleitung für die Überwachung von Cyber-Sicherheitsangelegenheiten zuständig sind?
- **c.** Gehört die Cyber-Sicherheit zu den Fachgebieten, die wir in der Unternehmensleitung für wichtig halten, und/oder ist sie in der Biografie eines oder mehrerer Unternehmensleitenden enthalten?
- **d.** Beschreiben wir, wie die Unternehmensleitung und/oder wichtige Ausschüsse vom Management Informationen über Cyber-Sicherheitsfragen erhalten?
- **e.** Steht die Cyber-Sicherheit auf der Liste der Risikofaktoren des Unternehmens?

5. Wie beschreiben wir Aktivitäten des Cyber-Sicherheits-Risikomanagements, wie z. B. diese:
   - **a.** Grundsätze und Verfahren
   - **b.** Reaktionsplanung, Notfallwiederherstellung oder Geschäftskontinuität
   - **c.** Simulationen und Tabletop-Übungen im Zusammenhang mit Cyber-Angriffen oder Sicherheitsverletzungen
   - **d.** Bildungs- und Ausbildungsmaßnahmen
   - **e.** Informationsaustausch mit Branchenkollegen, Strafverfolgungsbehörden usw.
   - **f.** Einsatz eines externen, unabhängigen Beraters zur Unterstützung des Managements und/oder zur Bescheinigung der Ergebnisse der Cyber-Sicherheitsbewertung

6. Wie sieht es im Vergleich zu unseren Konkurrenten und Branchenkollegen mit unserer Cyber-Sicherheitsoffenlegung aus?

7. Haben wir ein Verfahren, um den Wert der verbesserten Sicherheit zu verstehen?





TOOL H

Persönliche Cyber-Sicherheit für Mitglieder der Unternehmensleitung

Nach:
Melissa Hathaway, President, Hathaway Global Strategies

Zielsetzung:
Auch wenn die Cyber-Sicherheit in einem Unternehmen unglaublich wichtig ist, müssen die Mitglieder der Unternehmensleitung die richtige Cyber-Sicherheitspraxis anwenden und ihre Geräte und ihre Privatsphäre schützen. Dieses Tool enthält 10 Empfehlungen für Unternehmensleitende, um ihre eigene Cyber-Sicherheit zu verbessern.

1. Stellen Sie sicher, dass alle Ihre Geräte mit aktueller Software ausgestattet sind. Es ist wichtig, dass Sie Ihre Geräte und Anwendungen auf dem neuesten Stand der Software halten, die verfügbar ist.

2. Sperren Sie Ihr WiFi, so selbstverständlich wie Sie auch Ihr Haus abschließen. Legen Sie ein neues Passwort fest, das über die Werkseinstellung hinausgeht. Richten Sie ein Gastkonto für Hausbesucher, Auftragnehmer usw. ein.

3. Sichern Sie Ihre Daten häufig - mindestens einmal pro Monat. Nutzen Sie einen verschlüsselten Backup-Dienst, um sich vor Ransomware zu schützen.

4. Denken Sie nach, bevor Sie etwas posten, und minimieren Sie Ihr digitales Risiko. Teilen Sie nichts, was Kriminellen Aufschluss über Ihren derzeitigen oder zukünftigen Aufenthaltsort geben könnte. Sperren Sie Ihre Konten in den sozialen Medien, indem Sie Ihre Beiträge auf Freunde beschränken. Überprüfen Sie regelmäßig Ihre Datenschutz- und Sicherheitseinstellungen und setzen Sie sie um.

5. Schalten Sie die Zwei-Faktor-Authentifizierung für alles ein. Verwenden Sie biometrische Daten, wo immer es möglich ist.

6. Verwenden Sie komplexe Kennwörter für sensible Konten. Verwenden Sie (z. B.) den Schlüsselbund Ihres iPhones, um Ihre Passwörter zu sichern. Verwenden Sie die empfohlenen sicheren Passwörter.[7]

7. Bestimmen Sie einen Computer/Gerät (den Ihre Kinder nicht benutzen können), um sensible und finanzielle Transaktionen durchzuführen.

[7] Siehe z. B. die Webseite des Bundesamtes für Sicherheit in der Informationstechnik.

8. Recherchieren Sie regelmäßig und gründlich, was es über Sie und Ihre Familie zu wissen gibt.

9. Entsorgen Sie elektronische Geräte sicher; löschen oder zerstören Sie das Gerät.

10. Sperren Sie Ihr Guthaben. Eine Kreditsperre ist ein wirksames Mittel gegen finanziellen Identitätsdiebstahl und gibt Ihnen maximale Kontrolle darüber, wer Zugang zu Ihrem Kredit hat.

TOOL I

Ressourcen der Bundesregierung Deutschland

Autor:
Simona Autolitano, Bundesamt für Sicherheit in der Informationstechnik

Zielsetzung:
Alle Organisationen können davon profitieren, proaktiv Beziehungen zu Behörden auf Bundes- oder Landesebene aufzubauen. In diesem Anhang gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI), die zentrale Cyber-Sicherheits-Behörde in Deutschland, einen Überblick über relevante Ressourcen, die der Wirtschaft zur Verfügung stehen.

BSI als zentrale Anlaufstelle für Cyber-Sicherheit:

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gestaltet als zentrale Cyber-Sicherheits-Behörde die Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Das BSI untersucht Sicherheitsrisiken im Zusammenhang mit dem Einsatz von IT und entwickelt präventive Sicherheitsmaßnahmen. Es informiert über Risiken und Bedrohungen im Zusammenhang mit der Nutzung von Informationstechnik und sucht nach geeigneten Lösungen. Um diese Risiken zu minimieren oder zu vermeiden, bietet das BSI Dienstleistungen in den Kernbereichen Information, Beratung, Entwicklung und Zertifizierung für verschiedene Zielgruppen an, darunter Hersteller, Vertreiber und Anwender von Informationstechnik.
Die Aufgaben und Zuständigkeiten des BSI sind im IT-Sicherheitsgesetz und dem kürzlich verabschiedeten IT-Sicherheitsgesetz 2.0 geregelt und umfassen folgende Tätigkeiten:

- Das BSI als zentrale Anlaufstelle für die Meldung von Sicherheitsvorfällen sammelt und wertet Informationen über Sicherheitslücken und neue Angriffsmuster aus. Diese werden genutzt, um verlässliche Berichte über die aktuelle IT-Sicherheitslage zu erstellen, Angriffe frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten.
- Das BSI kann nach Unterrichtung der Hersteller Informationen und Warnungen über Schwachstellen in IT-Produkten oder -Dienstleistungen an Behörden oder die Öffentlichkeit weitergeben.
- Das BSI ist die zentrale Anlaufstelle für die Meldung von Sicherheitsvorfällen bei kritischen Infrastrukturen.

1. Rahmenwerke und Normen:

Mit dem **IT-Grundschutz** bietet das BSI eine bewährte Methodik zur Verbesserung der Informationssicherheit in Behörden und Unternehmen jeder Größe.

Der IT-Grundschutz ist kompatibel zu ISO/IEC 27001. Er besteht aus den BSI Standards und dem IT-Grundschutz-Kompendium:

- 200-1: Informationssicherheits-Managementsysteme (ISMS)
- 200-2: IT-Grundschutz-Methodik
- 200-3: Risikoanalyse auf Basis von IT-Grundschutz
- 100-4: Notfallmanagement der Geschäftskontinuität

Das IT-Grundschutz-Kompendium: Beschreibt spezifische Anforderungen in Form von IT-Grundschutz-Bausteinen, die verschiedene Aspekte der Informationssicherheit abdecken und bei der Umsetzung der IT-Grundschutz-Methodik helfen.

Die **IT-Grundschutz-Profile** stellen Vorlagen zur Verfügung, die es den Anwendenden ermöglichen, einen auf IT-Grundschutz basierenden Sicherheitsprozess mit Hilfe von Beispielszenarien einzurichten, die an die spezifischen Sicherheitsanforderungen ihrer Branche, ihres Unternehmens oder ihrer Organisation angepasst werden können.

Der **Cloud Computing Compliance Controls Catalogue (C5)** richtet sich in erster Linie an professionelle Cloud-Service-Anbieter, deren Wirtschaftsprüfenden und Kunden der Cloud-Service-Anbieter. Es wird festgelegt, welche Anforderungen (in diesem Zusammenhang auch als Kontrollen bezeichnet) die Cloud-Anbieter einhalten müssen bzw. welche Mindestanforderungen die Cloud-Anbieter erfüllen sollten.

2. Netzwerke:

Mit der Public Private Partnership **Allianz für Cyber-Sicherheit (ACS)** unterstützt das BSI Unternehmen in Deutschland bei der Planung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen zur Erhöhung ihrer Cyber-Sicherheit.

UP KRITIS ist eine öffentlich-private Partnerschaft zwischen Betreibenden Kritischer Infrastrukturen (KRITIS), ihren Verbänden und den zuständigen Behörden. Das gemeinsame Ziel ist es, den Schutz kritischer Infrastrukturen sektorübergreifend zu verbessern.

3. Austausch von Informationen:

CERT-Bund (Computer Emergency Response Team für Bundesbehörden) ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Computerzwischenfällen.

CERT-Bund arbeitet eng mit den mehr als 40 im CERT-Verbund organisierten CERTs sowie mit dem EU CSIRTs Network zusammen, das im Rahmen der NIS-Richtlinie geschaffen wurde.

Ziel des **IT-Lagezentrums** des BSI ist es, stets ein verlässliches Bild über die aktuelle IT-Sicherheitslage in Deutschland zu haben und den Handlungsbedarf und mögliche Gegenmaßnahmen bei IT-Sicherheitsvorfällen auf staatlicher und privatwirtschaftlicher Ebene schnell und kompetent zu bewerten.

4. Beratung zur Informationssicherheit:

Das BSI berät bei der Entwicklung geeigneter Lösungen zu Fragen der Informationssicherheit, die individuelle Sicherheitsanforderungen mit wirtschaftlichen Überlegungen in Einklang bringen. Die Beratungsleistungen des BSI stehen Staat, Wirtschaft und Gesellschaft zur Verfügung.

5. Meldung von Cyber-Vorfällen:

Meldepflicht für Betreiber kritischer Infrastrukturen:

Anbietende kritischer Infrastrukturen müssen dem BSI eine erhebliche Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit oder eine außergewöhnliche IT-Störung melden. Diese Anforderung gilt derzeit für die Sektoren Energie, Informationstechnologie und Telekommunikation, Wasser, Lebensmittel, Finanzen und Versicherungen, Gesundheit sowie Transport und Verkehr.

Unternehmen, die diese Anforderung erfüllen müssen, erhalten über ihre zentrale Anlaufstelle Informationen darüber, wie sie Vorfälle melden können.

Betreibende kritischer Infrastrukturen, die nicht unter das IT-Sicherheitsgesetz fallen, können außergewöhnliche IT-Störungen auf freiwilliger Basis über das Störungsmeldeverfahren auf der Webseite der Allianz für Cyber-Sicherheit melden.

Unternehmen, die zu den IT-Sicherheitslageberichten des BSI beitragen möchten, können IT-Sicherheitsvorfälle über die Webseite der Allianz für Cyber-Sicherheit melden. Die Meldungen können anonym eingereicht werden, und alle eingereichten Informationen werden vertraulich behandelt. Die aus den Meldungen gewonnenen Erkenntnisse werden für die Erstellung von Lageberichten und Warnungen für die verschiedenen Zielgruppen des BSI genutzt. Gemeldete Schwachstellen in IT-Produkten werden nach dem Modell der „Responsible Disclosure“ auch an den Herstellenden weitergeleitet.

Was ist zu melden:

Angriffsmethoden:

- Angriffe durch Unternehmensspionage
- Angriffe auf Prozessleitsysteme
- Angriffe auf Sicherheitsinfrastrukturen
- Neue Schwachstellen
- Datenschutzverletzungen, die groß angelegte oder gezielte Angriffe ermöglichen können (z. B. Offenlegung wichtiger Passwörter, Code-Signatur-Zertifikate)

Unternehmen sollten auch in Betracht ziehen, Cyberangriffe den Strafverfolgungsbehörden zu melden. Die Liste der Zentralen Ansprechstellen für Cyberkriminalität (ZAC) auf Landes- und Bundesebene ist online verfügbar.

RAHMENWERKE UND NORMEN	
IT-Grundschutz	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
Katalog für die Kontrolle der Einhaltung der Vorschriften für das Kriterienkatalog Cloud Computing C5	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html
NETZWERKE	
Allianz für Cyber-Sicherheit	https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html
UP KRITIS	https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html
AUSTAUSCH VON INFORMATIONEN	
CERT Bund	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html
IT-Lagezentrum	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/nationales-it-lagezentrum_node.html
BERATUNG ZUR INFORMATIONSSICHERHEIT	
Beratungsdienste	Telefon: 0228 99 9582-333 E-Mail: Sicherheitsberatung@bsi.bund.de
MELDUNG VON CYBER-VORFÄLLEN:	
Obligatorische Meldung von Vorfällen	https://mip.bsi.bund.de/
Freiwillige Meldung von Vorfällen	https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html?cms_pos=4
Online-Formular für die freiwillige Meldung von Vorfällen	https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html
Meldung per E-Mail	Meldestelle@bsi.bund.de
Unternehmen im besonderen öffentlichen Interesse (UBI)	https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/UBI/ubi_node.html
Kontaktaufnahme mit den Polizeibehörden	https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Kontakt-zur-Polizei/kontakt-zur-polizei_node.html

www.allianz-fuer-cybersicherheit.de

https://isalliance.org/