proofpoint.

E-BOOK

Die richtigen Kennzahlen

CISO-Leitfaden für die Bewertung, Priorisierung und Begründung wirtschaftlich sinnvoller Cybersicherheits-Budgets

ABSCHNITT 1

Vom Sündenbock zum Strategen

Die Entwicklung der Rolle des CISOs (Chief Information Security Officer) in den letzten Jahren hat eine Führungskraft bei einer kürzlichen Proofpoint-Diskussionsrunde wie folgt passend beschrieben:

„Als ich in die Branche einstieg, spielten CISOs eher die Rolle des Sündenbocks. Die Unternehmensführung musste jemanden haben, dem sie die Schuld geben kann, wenn etwas schiefging. Häufig jedoch waren ihnen Haftpflichtausfallversicherungen wichtiger als Investitionen in Sicherheitsteams und -lösungen. Mit anderen Worten: CISOs waren Technologen mit äußerst begrenzten Ressourcen."

Doch so langsam dreht sich der Wind. Bedrohungen sind komplexer geworden und können weite Teile eines Unternehmens beeinträchtigen. Wenn Cyberangriffe zu großflächigen Kompromittierungen werden, können sie schnell den Ruf einer Marke beschädigen oder zerstören.

Aus diesem Grund nehmen Unternehmensführungen Investitionen in Cybersicherheit – und die Rolle des CISO – heute anders wahr. Ebenso interessieren sich die Vorstände nun viel mehr für die Arbeit des CISOs. Zudem haben CISOs ihrer Bezeichnung „Chief" (dt. Leiter) zufolge einen großen Anteil an der allgemeinen Unternehmensstrategie. Zunehmend gestalten sie die digitale Transformation auf eine Art und Weise, die Risiken reduziert, Geschäftsprozesse optimiert und vermeidbare Verluste minimiert.

„Als ich in die Branche einstieg, spielten CISOs eher die Rolle des Sündenbocks."

Wachsende Herausforderungen führen zu neuen Kosten

Diese Entwicklung geht mit neuem Finanzbedarf einher. Laut einer aktuellen Untersuchung von Forrester stockten 60 % der leitenden Sicherheitsverantwortlichen in Unternehmen ihr Sicherheitsbudget im Jahr 2020 auf.[1]

Und die, die nicht mehr Geld ausgeben, versuchen ihre Mittel so weit wie möglich zu strecken. Das Cybersicherheits-Budget muss heute folgende Bereiche abdecken:

- Veränderte Vorschriften und Anforderungen
- Die anhaltende Verlagerung in die Cloud
- Den plötzlichen Umstieg auf Remote- und Hybrid-Arbeitsmodelle
- Die sich entwickelnde Bedrohungslandschaft

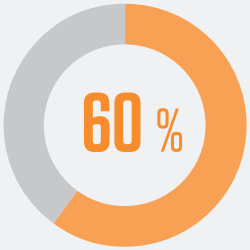
Vorbereitung auf die Zukunft

Während sich die CISOs auf diese Veränderungen einstellen, gehen viele davon aus, dass die Budgets weiter (im Durchschnitt um 11 %) steigen werden, um den anstehenden Herausforderungen gerecht zu werden. Nahezu zwei Drittel (65 %) glauben, dass sie Cyberangriffe bis 2023 besser erkennen und die Schäden schneller beheben werden können.[2]

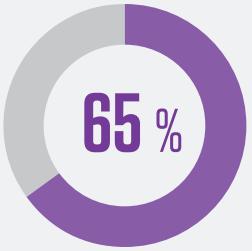
Nichtsdestotrotz ist Vorsorge immer noch ein zentrales Anliegen. Obwohl sich Führungskräfte optimistisch darüber äußern, Bedrohungen abwehren und ihre Geschäftsabläufe in Zukunft wiederherstellen zu können, sind sie derzeit noch weniger zuversichtlich. Laut unserem Voice of the CISO Report 2021 haben 66 % der CISOs das Gefühl, ihr Unternehmen sei momentan nicht für einen gezielten Cyberangriff gewappnet.[3]

Den neuen Perimeter bilden nicht die Netzwerktechnologien, sondern die Mitarbeiter. Zudem führt der Wechsel zu hybriden Arbeitsmodellen (ausgehend von überwiegender oder vollständiger Remote-Arbeit) zu zusätzlichen Sicherheitsherausforderungen und Komplexitäten.

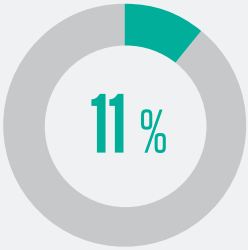
Als Sicherheitsverantwortlicher können Sie sich durch die entsprechende Verwendung Ihres Budgets an diese Veränderungen anpassen. In diesem E-Book informieren wir über empfohlene Vorgehensweisen für die Bewertung von Risiken, Ermittlung der Risikotoleranz Ihres Unternehmens, Bewertung der bestehenden Lösung sowie Priorisierung von Ausgaben und nennen Argumente für die Begründung Ihres Budgets gegenüber dem Vorstand.



der leitenden Sicherheitsverantwortlichen in Unternehmen haben ihr Sicherheitsbudget im Jahr 2020 aufgestockt



der CISOs glauben, dass sie Cyberangriffe bis 2023 besser erkennen und Schäden schneller beheben werden können



geschätzte Erhöhung des Budgets, um künftigen Herausforderungen gerecht zu werden

1 Forrester: „Global Security Budgets in 2021“ (Weltweite Sicherheitsbudgets 2021), August 2021.
2 Proofpoint: „Voice of the CISO“, Mai 2021.
3 Proofpoint: „Voice of the CISO“, Mai 2021.

ABSCHNITT 2

Bewertung der Risikotoleranz

Im ersten Schritt bewerten Sie die Sicherheitsrisiken und ermitteln die Risikotoleranz mithilfe eines für Ihr Unternehmen geeigneten Frameworks. Dabei können Sie aus einer ganzen Reihe an Frameworks wählen. Während Sie sich mit der Unternehmensführung und den Vorstandsmitgliedern um eine Einigung bemühen, sollten Sie unbedingt kommunizieren, welches Framework Sie weshalb verwenden.

In Zahlen ausgedrückt

Die Quantifizierung von Risiken ist keine perfekte Wissenschaft und kann sich als schwierig erweisen. Wenn Sie sich jedoch die Zeit nehmen, die Risiken und Risikotoleranz zu quantifizieren, fällt es Ihnen später leichter, Argumente für Ihr Budget anzubringen. Die Risikoanalyse kann auch auf qualitativer Ebene erfolgen, allerdings werden Kennzahlen in Euro und Cent bei den Führungskräften und Vorstandsmitgliedern eher Anklang finden.

Das Festlegen von Risikostufen ist unerlässlich. Die Risikotoleranz, die die Unternehmensführung während der Planungsphase angibt, muss nicht unbedingt der tatsächlichen Risikotoleranz entsprechen. Skizzieren Sie gegenüber Führungskräften und Vorstandsmitgliedern realistische Szenarien, um die wahre Risikobereitschaft Ihres Unternehmen zu ermitteln.

Wichtige Cybersicherheits-Frameworks

National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

Das NIST ist eine Abteilung des US-Handelsministeriums und bietet Empfehlungen zur Vermeidung von Cybersicherheitsrisiken sowie zur Verbesserung der internen und externen Cybersicherheitskommunikation.

NISTIR 8286: Identifizierung und Einschätzung von Cybersicherheitsrisiken zur unternehmensgerechten Risikoverwaltung

In diesem Dokument geht es um die Verringerung von Cybersicherheitsrisiken auf Unternehmensebene im Rahmen der Unternehmensmission und Geschäftsziele.

People-Centric Security Framework (PCSF)

Dieses Framework wurde in einem transparenten, auf Konsens beruhenden Verfahren mit Verantwortlichen der Privatwirtschaft und dem öffentlichen Sektor entwickelt und von Proofpoint veröffentlicht, um bessere Vorgehensweisen zur Reduzierung personenzentrierter Risiken zu fördern und Unternehmen beim Schutz der Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Umgebungen zu unterstützen.

ABSCHNITT 3

Minimierung von Risiken

Wenn Sie die Sicherheitsrisiken und Risikotoleranz identifiziert haben, müssen Sie bewerten, wie gut die bestehenden Schutzmaßnahmen die Risiken bewältigen können.

Über Technologien hinaus denken

Möglicherweise liegt die Versuchung nahe, das Problem aus der Sicht des vorhandenen Technologiepakets zu betrachten. Jeder kennt operative KPIs (Key Performance Indicators) wie die Zeit bis zur Erkennung, die Zeit bis zur Reaktion und die Zeit bis zur Behebung.

KPIs sind für allgemeine Berichte nützlich und erleichtern das Verständnis der Effektivität einer Lösung im Alltag. Mit ihnen lässt sich hingegen nur schwer bewerten und ausdrücken, wie Ihr Unternehmen generell gegenüber den übergeordneten Risiken und Geschäftsprioritäten aufgestellt ist.

Bedrohungsmodellierung

Für die Planung des Budgets und die Präsentation gegenüber Führungskräften empfiehlt es sich, den Ansatz der Bedrohungsmodellierung für die Bewertung der KRIs (Key Risk Indicators) zu wählen und die entsprechenden Zahlen zu ermitteln. Bei der Bedrohungsmodellierung wird festgestellt, welche Bedrohungen es gibt und wie sie entstehen, um die Maßnahmen zur Abwehr anschließend entsprechend zu priorisieren. Im Gegensatz zu lösungsspezifischen KPIs hilft die Bedrohungsmodellierung, einen Gesamtüberblick über die bestehenden Risiken zu erhalten und Lücken in den Sicherheitsmaßnahmen aufzuspüren.

Mithilfe der Bedrohungsmodellierung erkennen Sie, wo es gut läuft, wo weitere Investitionen nötig sind und wo möglicherweise ein Restrisiko noch hinnehmbar ist. Auf diese Weise lassen sich zahlreiche Risiken bewerten. Hier sind einige Beispiele.

Bedrohungsmodellierung in der Praxis

Hier ist ein Beispiel dafür, wie Bedrohungsmodellierung in der Praxis abläuft. Schauen wir uns dafür regulatorische Risiken an. Datenlecks sind ein potenzielles regulatorisches Risiko und können durch verschiedene Bedrohungsvektoren ausgelöst werden, zum Beispiel:

- E-Mail-Datenverlust
- Datenübertragung über die Cloud
- Speicherung von Daten auf einer lokalen Festplatte
- Nutzung von Wechselmedien
- Übertragung von Daten in eine unsichere Zone
- Verwendung einer externen Webseite zur Dateifreigabe
- Manuelles Ausschneiden und Einfügen
- Anwendungsschwachstellen

Bei der Analyse dieser Vektoren für Datenlecks können Sie bewerten, wie gut Sie jeweils davor geschützt sind, und entscheiden, wie Sie Lücken schließen wollen.

Wenn Sie jedoch gleich zur Bewertung der Leistung bestimmter Technologien (z. B. CASB (Cloud Access Security Broker), Endpunkt-Agent oder virtuelles privates Netzwerk (VPN)) übergehen, übersehen Sie womöglich Lücken bei Datenleck-Vektoren, die diese Produkte nicht abdecken.

Wenn Sie die KRIs mit einer Bedrohungsmodellierung bewerten, erhalten Sie ein umfassenderes und strategisches Bild davon, wie gut Ihr Unternehmen für diverse Risiken gerüstet ist.

ABSCHNITT 4

Auswahl der Lösungen

Basierend auf Ihrer Analyse der Risikotoleranz und KRIs können Sie die wichtigsten Bereiche für neue Investitionen in Ihrem Unternehmen identifizieren.

Bei der Suche nach geeigneten Lösungen sollten Sie folgende Fragen klären:

- Minimiert die Lösung ein Risiko?
- Löst sie ein geschäftliches Problem?
- Bringt sie Verbesserungen für das Unternehmen (neue Tools oder Prozesse)?
- Hilft sie, Sicherheitsabläufe zu vereinfachen und zu optimieren?
- Passt sie zu Ihren Geschäftszielen und Ihrer Risikotoleranz?

Dieselben Fragen können und sollten Sie auch für die vorhandenen Lösungen stellen. Bevor Sie weiter in eine bestimmte Technologie investieren, sollten Sie sicher sein, dass diese immer noch einen Mehrwert liefert.

Quantifizierung der Rendite

Um Ihre Investitionen – und das entsprechend benötigte Budget – gegenüber dem Vorstand rechtfertigen zu können, müssen Sie die Rendite der einzelnen Lösungen quantifizieren.

Das Beziffern der Rendite für eine Sicherheitsinvestition (Return on Security Investment, ROSI) ist zwar nicht immer ganz leicht, doch häufig ist es dadurch einfacher, die Unterstützung der Führungsebene zu erhalten. Eine Möglichkeit besteht darin, die Vorteile der Lösung gegen die Kosten abzuwägen.

Suchen Sie nach den verborgenen Kosten einer Lösung, zum Beispiel:

- **Hardware**
- **Implementierung**
- **Software**
- **Fortlaufende Verwaltung**

Vergleichen Sie die Kosten und Vorteile jeder Lösung (z. B. in Bezug auf Risikominimierung und Effizienzsteigerung für Mitarbeiter). Zudem sollten Sie darlegen, was passiert, wenn Sie nichts tun. Erläutern Sie dazu die potenziellen Gefahren und bringen Sie einige Beispiele an.

Wenn Sie sich beispielsweise dafür entscheiden, die Folgen eines Ransomware- oder Malware-Angriffs nicht zu minimieren, könnte das folgende Auswirkungen haben:

- Geschäftsunterbrechung
- Produktivitätsverlust der Anwender
- Zeitverlust durch Bedrohungsuntersuchung und Berichterstellung
- Zeitverlust durch Abwehr oder Behebung von Bedrohungen
- Zeitaufwand für manuelle Aufgaben wie Entfernen von Nachrichten aus Postfächern oder Reagieren auf gemeldete Phishing-Nachrichten

Dokumentieren der Restrisiken

Informieren Sie sich, welche Cyberversicherung Sie haben und welche Restrisiken bleiben, d. h. welche Gefahren trotz Ihrer Investitionen bestehen bleiben. Es ist nahezu unmöglich, die Risiken für ein Unternehmen auf null zu senken. Selbst wenn Sie es könnten, wäre es den Preis wahrscheinlich nicht wert. Allerdings sollten Sie dafür sorgen, dass das Restrisiko im Rahmen der Risikotoleranz Ihres Unternehmens liegt.

ABSCHNITT 5

Kalkulation und Kommunikation der geschäftlichen Anforderungen

Nachdem Sie Ihren Finanzbedarf und die Investitionsbereiche festgelegt haben, müssen Sie Ihren Vorgesetzten und Vorstandsmitgliedern alles überzeugend vermitteln. Sie werden dabei wahrscheinlich mit mehreren verschiedenen Führungskräften sprechen:

- Mit dem Vorstand
- Mit der operativen Führung, z. B. Chief Operating Officer (COO) oder Chief Information Officer (CIO)
- Mit Finanzführungskräften, z. B. Chief Financial Officer (CFO)

Anpassen der Botschaft

Es ist sinnvoll, das Anwendungsszenario für Ihre Sicherheitsinvestitionen an Ihr Publikum anzupassen. Konzentrieren Sie sich auf die Auswirkungen in den Geschäftsbereichen, die von der jeweiligen Person geleitet werden. Es ist in etwa so, als würden Sie das gleiche Thema in drei verschiedenen Sprachen ausdrücken:

- **Der Vorstand:** Betonen Sie im Gespräch mit dem Vorstand, dass Ihr Plan der Risikotoleranz des Unternehmens entspricht, und zeigen Sie das für das Unternehmen hinnehmbare Restrisiko auf.
- **Operative Führung:** Konzentrieren Sie sich im Gespräch mit dem COO oder dem CIO auf Lücken, verbleibende Schwachstellen und darauf, wie Ihr Plan die Risiken für den Geschäftsbetrieb verringert.
- **Finanzführungskräfte:** Betonen Sie im Gespräch mit dem CFO, wie Sie die Ausgaben verteilt haben und wie Sie eventuelle Lücken schließen werden.

Kommunizieren Sie in allen Gesprächen die Rendite der Lösungen, die Sie während der Planungsphase errechnet haben. Erläutern Sie, welche Vorteile das Unternehmen für die bereitgestellten Mittel erhält.

Abfallende Rendite

Seien Sie darauf vorbereitet, das Konzept der „abfallenden Rendite“ zu erklären. Möglicherweise ist für die Behebung großer offensichtlicher Probleme ebenso viel Aufwand nötig wie für kleinere unscheinbarere, die gleichermaßen kritisch sind. Eine scheinbar kleine Bedrohung kann für das Unternehmen zu einem großen Risiko (z. B. eine Datenschutzverletzung) werden, und muss daher mit entsprechendem Aufwand vermieden werden. Auch hier können Sie auf Ihre Renditeberechnungen zurückgreifen, um die Kosten der Lösung und das verringerte Risiko in Verhältnis zu setzen.

ABSCHNITT 6

Umgang mit außerplanmäßigem Bedarf

Die Budgetierung findet jährlich oder vierteljährlich statt. Probleme wie neue Bedrohungen oder neue Taktiken von Bedrohungsakteuren werden zwangsläufig auch außerhalb des Standardzyklus auftauchen. Unerwartete Zwischenfälle lassen sich praktisch nicht vermeiden, doch sie können eine Gelegenheit sein, die Sicherheitsmaßnahmen neu zu bewerten und die Ausgabeprioritäten zu überdenken.

Berücksichtigen verborgener Kosten

Vergessen Sie nicht, die verborgenen Kosten zu bedenken, die jede implementierte Lösung mit sich bringt. Die meisten Unternehmen planen Lizenzkosten ein, doch häufig vergessen sie, die anfallenden Wartungskosten oder das erforderliche Personal zu berücksichtigen. Beziehen Sie diese verborgenen Kosten in Ihre Planung ein, um außerplanmäßige Überraschungen zu vermeiden.

ABSCHNITT 7

Beschleunigung des Prozesses

Die Budgetierung kann leicht zu einem mühsamen und langwierigen Prozess werden. Es gibt jedoch Wege, dem entgegenzuwirken.

Strategisch denken

Nehmen Sie zunächst Ihre Rolle als strategischer Geschäftspartner an und denken Sie daran, dass die Rolle des CISO sich stets weiterentwickelt. Finden Sie heraus, welche Ziele die Beteiligten verfolgen, und helfen Sie ihnen, diese mit minimalem Risiko zu verwirklichen.

Denken Sie nicht nur an die für den Betrieb und die Technik verantwortlichen Führungskräfte, sondern überlegen Sie sich, wie Sie das Unternehmen dabei unterstützen können, die digitale Transformation voranzutreiben und die Geschäftsziele umzusetzen.

Ein Gleichgewicht zwischen Risiko und Produktivität finden

Bedenken Sie zudem, dass Sie Risiken nicht völlig ausschließen können. Als Sicherheitsexperte bevorzugen Sie womöglich eine eher zurückhaltende Risikotoleranz, doch der Vorstand und andere Führungskräfte wollen ein Gleichgewicht zwischen Sicherheitsrisiken und Geschäftszielen herstellen. Ein Beispiel dazu: Nehmen wir an, die Effektivität Ihres E-Mail-Gateway beträgt 99,1 %. Für einen Ransomware-Angriff ist jedoch nur eine E-Mail nötig, womit ein Restrisiko von 0,9 % bleibt. Das Restrisiko wird in der Regel durch mehrschichtige Sicherheitsmaßnahmen wie Isolierung oder Datenverlustprävention (DLP) eingedämmt. Allen Beteiligten sollte jedoch klar sein, dass Risiken nicht vollständig ausgeräumt werden können.

Finden Sie eine gemeinsame Basis und versuchen Sie, Kompromisse zu schließen. Ihr Budget und Ihre Pläne sollten ein Gleichgewicht zwischen den Risiken und den Unternehmensprioritäten darstellen und zudem das Risiko für Kompromittierungen innerhalb der Risikotoleranz des Unternehmens minimieren.

Die richtigen Erwartungen setzen

Schrauben Sie nebenbei die Erwartungen herunter. Die meisten Unternehmensabteilungen arbeiten nach einem Produktionsmodell, das sich an KPIs wie Ertrags- und Leistungssteigerung orientiert. Cybersicherheit arbeitet nach einem Resilienzmodell.

So wie die Feuerwehr unabhängig von tatsächlichen Bränden bereitstehen muss, erfordert die Cybersicherheit ein Budget, das sich nicht immer in höheren Erträgen widerspiegelt. Niemand würde behaupten, dass die Feuerwehr unnötig ist. Es ist Ihre Aufgabe, Ihren Geschäftspartnern zu erklären, dass Cybersicherheit auf die gleiche Weise funktioniert.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0500-000-01-01 03/22