proofpoint.

E-BOOK

Die Kosten „ausreichender“ Sicherheit

So viel sind Cybersicherheitslösungen wirklich wert

Cyberkriminalität und geschäftliche Risiken

Wer auch immer einst sagte, dass Verbrechen sich nicht auszahlen, hatte offensichtlich nicht mit heutigen Cyberangriffen gerechnet. Die Durchschnittskosten einer Datenschutzverletzung stiegen für die betroffenen US-amerikanischen Unternehmen von 5,4 Millionen US-Dollar im Jahr 2013 auf 9,44 Millionen US-Dollar im Jahr 2022.[1] Das übersteigt die Inflationsrate in diesem Zeitraum deutlich. Insgesamt kosten Datenschutzverletzungen die Unternehmen in den USA etwa 1,4 Milliarden US-Dollar pro Jahr – das entspricht 5.400 US-Dollar pro erwachsenem Einwohner.[2]

Prognosen zufolge wird Cyberkriminalität bis 2025 weltweite Kosten von 10,5 Billionen US-Dollar pro Jahr verursachen.[3] Andere Forscher schätzen, dass Cyberkriminalität die Unternehmen unfassbare 1,79 Millionen US-Dollar pro *Minute* kosten wird.[4]

Diese Kosten sind enorm und beschränken sich nicht auf die unmittelbaren finanziellen Verluste. Cyberkriminalität kann den Ruf Ihres Unternehmens schädigen oder zur Verhängung von Bußgeldern führen. Wenn Ihre geschäftlichen Abläufe unterbrochen werden oder Ihr Geschäftsmodell infrage gestellt wird, können Sie nicht mehr Ihrer Kernstrategie folgen.

Die Risiken von Cyberkriminalität lassen sich nicht gänzlich vermeiden – sie sind ein fester Bestandteil der heutigen Welt.

Es ist jedoch möglich, diese Risiken unter Kontrolle zu bekommen. Bei anderen Risiken, die Teil des Geschäftslebens sind, müssen Führungskräfte und Risikoverantwortliche entsprechend planen und Vorbereitungen treffen. Sie können aber auch die Anfälligkeit und Folgen von Cyberkriminalität eindämmen. Wie bei anderen Arten von Geschäftsrisiken müssen Sie die finanziellen Verluste modellieren, die Ihrem Unternehmen durch einen Cyberangriff entstehen könnten. Anschließend müssen Sie sich überlegen, wie Sie ein Gleichgewicht zwischen den Risiken und den Präventionskosten finden.

Weltweit stiegen die Durchschnittskosten durch eine Datenschutzverletzung auf

4,24 Mio. USD.[5]

Laut Expertenprognosen liegen die weltweiten Kosten für Cyberkriminalität bei

10,5 Bio. USD.[6]

Ein Prozent

des weltweiten Bruttosozialprodukts geht aktuell durch Cyberkriminalität verloren.[7]

Cyberkriminalität kostet Unternehmen pro Minute

1,79 Mio. USD.

1 IBM: „**Cost of a Data Breach Report 2022**“ (Bericht zu den Kosten einer Datenkompromittierung 2022), Juli 2022.
2 Rick Newman *(Yahoo Finance)*: „**We're all paying a cybersecurity tax**“ (Wir alle zahlen einen hohen Preis für Cybersicherheit), Mai 2021.
3 Steve Morgan *(Cybersecurity Ventures)*: „**Cybercrime to Cost the World $10.5 Trillion Annually by 2025**“ (Cyberkriminalität kostet weltweit 10,5 Billionen US-Dollar jährlich), November 2020.
4 James Coker *(Infosecurity Magazine)*: „**Cybercrime Costs Organizations Nearly $1.79 Million Per Minute**“ (Cyberkriminalität kostet Unternehmen fast 1,79 Millionen US-Dollar pro Minute), Juli 2021.
5 IBM: „**Cost of a Data Breach Report 2022**“ (Bericht zu den Kosten einer Datenkompromittierung 2022), Juli 2022.
6 Steve Morgan *(Cybersecurity Ventures)*: „**Cybercrime to Cost the World $10.5 Trillion Annually by 2025**“ (Cyberkriminalität kostet weltweit 10,5 Billionen US-Dollar jährlich), November 2020.
7 Zhanna Malekos Smith and Eugenia Lostri *(Center for Strategic and International Studies)*: „**The Hidden Cost of Cybercrime: Report**“ (Bericht zu den verborgenen Kosten von Cyberkriminalität), Dezember 2020.

Der erste Schritt bei der Bewertung von Lösungen ist der Vergleich des Risikominderungs-potenzials einer Lösung mit ihren Kosten. Nur so können Sie sicher sein, das bestmögliche Preis-Leistungsverhältnis zu erhalten.

Die Investition in Sicherheitstechnologien ist eine der Möglichkeiten, diese Risiken zu minimieren. Wie können Sie jedoch sicher sein, dass Ihre Investitionen wirklich effektiv sind?

Wenn Sie CISO sind, ist die Minimierung von Risiken Ihre Hauptaufgabe. Der erste Schritt bei der Bewertung von Lösungen ist der Vergleich des Risikominderungspotenzials einer Lösung mit ihren Kosten. Nur so können Sie sicher sein, das bestmögliche Preis-Leistungsverhältnis zu erhalten. Dabei sollten Sie auch Kosten berücksichtigen, die über die Lizenzierung hinausgehen, z. B. für Hardware, Implementierung, Betrieb und laufende Wartung. Beziehen Sie aber auch zusätzliche Vorteile der Lösungen ein, z. B. Effizienzsteigerungen für Mitarbeiter.

Nehmen wir als Beispiel die Belastung Ihrer internen Sicherheitsmitarbeiter. Heute kämpfen CISOs bei ihren Sicherheitsinitiativen mit Fachkräftemangel. Weltweit sind 2,72 Millionen Stellen im Cybersicherheitsbereich unbesetzt.[8] Schätzungen zufolge müsste die Zahl der Cybersicherheitsmitarbeiter um 65 % steigen, um die wichtigsten Ressourcen der Unternehmen effektiv schützen zu können.[9] Für CISOs sind diese Herausforderungen Teil des Alltags.

Es ist klar, dass die Zeit der Sicherheitsexperten wertvoll ist und der Verwaltungsaufwand in die Kosten einer Cybersicherheitslösung eingerechnet werden muss. Doch was ist mit der Produktivität der Endnutzer oder dem Aufwand für die Behebung von Zwischenfällen bzw. allein schon für ihre Meldung?

In diesem Leitfaden betrachten wir die Kosten für die Implementierung und den Betrieb einer Cybersicherheitslösung. Wir schlüsseln alle Faktoren auf, die den Gesamtnutzen einer Lösung ausmachen, darunter einige, die nur selten berücksichtigt werden. Wir berechnen, wann es kostengünstiger ist, in eine erweiterte E-Mail-Sicherheitslösung oder eine umfassende E-Mail- und Cloud-Schutzlösung zu investieren, als „preiswerte“ Add-on-Funktionen oder Legacy-Lösungen einzusetzen.

8 (ISC)²: „**Cybersecurity Workforce Study**“ (Studie zu Cybersicherheitsexperten), März 2022.
9 ebd.

Die realen Kosten für die Eindämmung von Cybersicherheitsrisiken

Ihre Investitionen in Cybersicherheit sind eine Maßnahme, um das Problem operativer und geschäftlicher Risiken mit Geld zu lösen. Es gibt jedoch keine direkte Relation zwischen investierten Geldmitteln und der Schutzabdeckung. Zuverlässiger Schutz lässt sich nur mit einem mehrstufigen Sicherheitsansatz erreichen.

Einige Sicherheitslösungen sind besonders gut dazu geeignet, Ihre Risiken zu minimieren. Kleine Unterschiede bei der Effektivität können große Auswirkungen auf das Risiko – und die potenziellen Kosten – einer Kompromittierung haben. Gleichzeitig sind die Preise der verschiedenen Lösungen sehr unterschiedlich.

Sie müssen all diese Aspekte bei Ihrer Kaufentscheidung berücksichtigen sowie Ihre potenzielle Rendite der Sicherheitsinvestition (ROSI) ermitteln.

Dazu ist es auch notwendig, alle Verluste zu erfassen, die aufgrund eines schwerwiegenden Sicherheitszwischenfalls auftreten können. Häufig gehen diese weit über die Kosten durch den eigentlichen Angriff hinaus. Die langfristigen Schäden für das Unternehmen und seinen Ruf können noch jahrelang spürbar sein.

Sie müssen diese möglichen Verluste mit den Kosten der Cybersicherheitslösung ins Verhältnis setzen. Auf den ersten Blick scheint das leicht zu berechnen sein: mit einem Blick auf die Lizenzkosten.

Wenn es jedoch um den gesamten wirtschaftlichen Nutzen einer Cybersicherheitslösung geht, bilden die Lizenzkosten nur die Spitze des Eisbergs. Wenn Sie lediglich die Lizenzierung betrachten, sehen Sie nicht das Gesamtbild der Kosten einer Lösung für Ihr Unternehmen. Unter der Oberfläche lauern viele weitere verborgene Gesamtbetriebskosten, die eine Lösung erheblich verteuern können.

Dabei ist die Risikominimierung nicht immer unmittelbar spürbar. Wenn Sie den vollen Funktionsumfang einer Lösung nutzen, reduziert das vielleicht Ihr Risiko um 50 % – Ihnen stehen jedoch nur selten von Anfang an alle Vorteile eines Produkts zur Verfügung. Zudem bieten die meisten Lösungen über die reine Risikominimierung hinausgehende Vorteile, beispielsweise verbessern sie die Effizienz des Sicherheitsteams und steigern dadurch ihren Nutzen.

Die Nachwirkungen eines Angriffs

Datenverlust durch Angriffe kann folgende Auswirkungen haben:

- Entgangene Geschäfte und verlorene Kunden
- Verlorene Daten sowie Verlust des Nutzens, der sich aus der Analyse dieser Daten gewinnen ließe
- Direkte finanzielle Verluste*
- Rufschädigung
- Verlust der Produktivität von Mitarbeitern
- Ausfall geschäftlicher Abläufe
- Verringerter Share Value
- Verlust von geistigem Eigentum
- Verlust von Wettbewerbsvorteilen
- Compliance-Strafen oder Bußgelder

* Dazu gehören auch Lösegeldzahlungen sowie Arbeitskosten und Dienstleistungen für die Reaktion auf Zwischenfälle und Wiederherstellung.

Aufrechnung der Kosten

Für die meisten Unternehmen kann die Implementierung einer neuen Cybersicherheitslösung teuer und zeitaufwändig sein. Der Prozess kann auch die Produktivität der Anwender sowie reguläre IT- und Sicherheitsabläufe stören. Einige Tools sind umständlich in der Wartung, was den Aufwand für ohnehin schon ausgelastete Sicherheitsteams zusätzlich vergrößert. Um die Gesamtauswirkungen der Investition für Ihr Unternehmen abzuschätzen, müssen Sie mehrere Faktoren berücksichtigen:

Lizenzierung

Was zahlen Sie dem Anbieter pro Jahr pro Anwender für die Lösung? Ihre gesamten Lizenzierungskosten umfassen die Kosten pro Anwender pro Jahr multipliziert mit der Anzahl der Anwender.

Hardware

Für einige Lösungen ist auch zusätzliche Hardware erforderlich, was die Kosten für Ihr Unternehmen weiter steigen lässt. Das gilt insbesondere dann, wenn Sie diese Hardware lokal verwalten. Was kostet es, wenn Sie diese Hardware stets aktuell halten, Verbindungen gewährleisten, die entsprechenden Räumlichkeiten unterhalten oder Vorbereitungen für Notfälle treffen bzw. Behebungen durchführen müssen? Wie viele Ihrer Mitarbeiter benötigen Sie für die Wartung der Technik?

Fortlaufende Verwaltung

Die laufenden Verwaltungskosten entstehen durch die Zeit, die spezialisierte Mitarbeiter für die laufenden Verwaltungsaktivitäten aufwenden müssen. Dieser Faktor muss unbedingt berücksichtigt werden. Wenn zum Beispiel eine Lösung zwei Vollzeitmitarbeiter (FTE) benötigt, während für eine zweite nur eine Vollzeitstelle erforderlich ist, müssten Sie berücksichtigen, dass die laufende Verwaltung der ersten Lösung doppelt so viel kostet. So betrachtet kann eine scheinbar kostenlose Lösung schnell teurer werden als ein kostenpflichtiges Produkt, das sich leicht verwalten lässt. Das gilt insbesondere dann, wenn der Produktanbieter umfassenden Support liefert.

Implementierung

Professional Services
Viele Anbieter empfehlen die Einrichtung und Bereitstellung der Lösung durch ihr Professional Services-Team oder schreiben dies vor. Diese Services sind natürlich ebenfalls mit Kosten verbunden.

Zeitaufwand
Unabhängig davon, ob das Professional Services-Team des Anbieters involviert ist, erfordern neue Produktbereitstellungen zumindest einige Mitarbeit Ihres internen Teams. Wer genau muss sich an der Implementierung beteiligen und wie viel Arbeitszeit nimmt das Projekt in Anspruch? Die Schätzung der Arbeitsstunden Ihrer eigenen Mitarbeiter ist dabei nur der erste Schritt. Welche anderen Aufgaben müssen sie zurückstellen, um sich auf diese Initiative zu konzentrieren? Berücksichtigen Sie auch, was Sie verlieren könnten, wenn Ihre Fachkräfte sich nicht ihren eigentlichen Tätigkeiten widmen.

Wenn Sie die Gesamtbetriebskosten einer Cybersicherheitslösung im Detail analysieren, zeigt sich schnell, dass der Aufwand für Implementierung und laufende Wartung die Lizenzierungskosten bei Weitem übersteigen kann.

Berücksichtigung der Vorteile

Um den Gesamtnutzen einer Lösung zu erfassen, müssen Sie alle oben genannten Kosten berücksichtigen und sie mit den Produktangeboten gegenrechnen. Der wichtigste Vorteil jeder Sicherheitslösung ist in jedem Fall die Risikominimierung. Ebenso wie bei den Kosten müssen jedoch auch weitere Faktoren berücksichtigt werden.

Diese Vorteile spielen eine wichtige Rolle:

- **Risikominimierung**

  Um die Risikominimierung einer Lösung ermitteln zu können, müssen Sie zuerst verstehen, welche potenziellen Verluste auf Ihr Unternehmen zukommen könnten. Wie hoch sind die Durchschnittskosten einer Datenschutzverletzung in Ihrer Branche und Region sowie speziell für Unternehmen Ihrer Größe? Setzen Sie das mit Ihrer Anfälligkeit und dem Absicherungspotenzial der Lösung ins Verhältnis. Berücksichtigen Sie auch, dass es einige Zeit dauern kann, bis die Lösung vollständig bereitgestellt ist und Sie alle ihre Vorteile nutzen können.

- **Effizienzsteigerungen für Mitarbeiter**

  Anwenderproduktivität
  Produktivität kann vielerlei Formen annehmen. Für Sicherheitsverantwortliche spielen hier vor allem die Produktivität der Nutzerbasis insgesamt sowie die Produktivität der Sicherheits- und IT-Teams eine wichtige Rolle. Eine Cybersicherheitslösung kann die Produktivität der Mitarbeiter auf vielfältige und komplizierte Weise beeinflussen und betrifft sowohl Endnutzer als auch Cybersicherheits- und IT-Teams. Wie viele Minuten oder Stunden am Tag verliert beispielsweise ein Business-Analyst, wenn er seinen Laptop nicht nutzen kann, weil dieser von Malware bereinigt werden muss? Wie viel kostet es Ihr Unternehmen, wenn Mitarbeiter des Vertriebsteams sich nicht mit Kunden in Verbindung setzen können, weil ein Cloud-Konto kompromittiert ist? Jedes Mal, wenn eine Spam-Nachricht und eine schädliche E-Mails blockiert wird, verhindert das schmerzhafte Ausfälle geschäftlicher Abläufe. Hinzu kommt: Wenn eine schädliche E-Mail durchkommt, kostet das die Helpdesk-Experten und IT-Administratoren wertvolle Zeit.

Aktuell liegen die jährlichen Kosten von Phishing-Angriffen bei durchschnittlich mehr als

14,7 Mio. USD.[10]

Jeder Wissensspezialist verliert jedes Jahr im Durchschnitt

sieben Stunden

produktiver Zeit aufgrund von Phishing.[11]

Ein Ransomware-Angriff kostete das Opfer im Jahr 2021 durchschnittlich

4,54 Mio. USD.[12]

Opfer von Business Email Compromise (BEC) haben von 2016 bis 2021 mehr als

43 Mrd. USD

an Kriminelle gezahlt.[13]

10 Ponemon Institute: „**2021 Cost of Phishing Study**“ (Studie zu Kosten durch Phishing 2021), Juni 2021.
11 ebd.
12 IBM: „**Cost of a Data Breach Report 2022**“ (Bericht zu den Kosten einer Datenkompromittierung 2022), Juli 2022.
13 Federal Bureau of Investigation: „**Business Email Compromise: The $43 Billion Scam**“ (BEC: Der 43 Milliarden US-Dollar-Betrug), Mai 2022.

Überwachung, Triage und Analysen
Cybersicherheitsanalysten gehören zu den fähigsten – und bestbezahlten – Fachleuten in der IT-Branche. Und es gibt nicht genug von ihnen. Es ist für Ihr Unternehmen strategisch wichtig, welchen Aufgaben sich Ihre Sicherheitsteams widmen. Wird deren Arbeit durch die Lösung vereinfacht oder erschwert? Lässt sich die Lösung in bereits in Ihrer Umgebung eingesetzte Systeme zur Ereignisüberwachung oder Erkennung und Reaktion integrieren? Möglicherweise lagern Sie diese Aufgaben an einen Dienstleister aus. Würde die Lösung in diesem Fall die Transparenz und Abdeckung für Ihren Partner verbessern?

Reaktions- und Behebungsmaßnahmen
Wenn Ihr Sicherheitsteam Maßnahmen ergreift, um laterale Bewegungen krimineller Akteure in Ihrer Umgebung zu verhindern, kommt es auf jede Minute an. Bietet die Lösung eine konsolidierte Plattform? Können Sie mithilfe von Richtlinienverwaltung auch Konfigurationsänderungen beschleunigen? Je schneller Sie eingehende Bedrohungen blockieren und beheben, desto geringer ist die Wahrscheinlichkeit schwerwiegender Kompromittierungen.

Automatisierung
Bietet die ins Auge gefasste Lösung vordefinierte Automatisierungs-Workflows für reguläre IT- oder E-Mail-Sicherheitsaufgaben? Wenn für die Einrichtung automatisierter Workflows erheblicher Design- und Konfigurationsaufwand entsteht, müssen Sie das ebenfalls berücksichtigen. Falls zwei Lösungen dieselbe Aufgabe übernehmen können, aber eine aufwändiger konfiguriert werden muss, umfangreiche Programmierung erfordert oder ständig verwaltet werden muss, ist sie mit höheren Kosten verbunden.

Bedrohungsdaten
Die Bedrohungssuche ist eine hochspezialisierte Sicherheitsaufgabe, die Schwachstellen aufdeckt und die Eskalation kleiner Zwischenfälle zu echten Kompromittierungen verhindert. Dazu sind jedoch Kompetenzen und Erfahrungen notwendig, die in Ihrem Unternehmen vielleicht nicht vorhanden sind. Bietet die potenzielle neue Lösung Bedrohungsanalysen und -daten, mit denen der Aufwand für Ihr Team verringert wird? Liefert sie einen nützlichen Überblick, sodass die Bedrohungssuche für Ihre Mitarbeiter weniger zeit- und arbeitsintensiv ist bzw. sie mit dem gleichen Aufwand mehr Details erhalten?

Ausgleich der Kosten und Vorteile in der Realwelt

Nachdem wir die Kosten und Vorteile einer Sicherheitslösung für Ihr Unternehmen aufgezählt haben, sehen wir uns nun genauer an, wie Sie den realen Gesamtnutzen einer Lösung ermitteln können.

Wie groß ist der *reale* Unterschied im Nutzen, wenn Sie „kostenlose“ oder „preiswerte“ Lösungen mit branchenführenden Produkten vergleichen?

Beim Einschätzen der Lösungsoptionen können Sie den Gesamtnutzen jeder Lösung berechnen, indem Sie die Kosten von den Vorteilen subtrahieren. Wir demonstrieren das an zwei Beispielen:

Beispiel 1

E-Mail-Sicherheit

Heutige E-Mail-Angriffe richten sich nicht gegen Technologien, sondern gegen Menschen. Dabei kommen Social-Engineering-Taktiken zum Einsatz, mit denen Anwender zum Aufrufen schädlicher Websites und Eingeben von Anmeldedaten verleitet werden sollen. Eine effektive E-Mail-Sicherheitslösung muss Angriffe gegen Ihre Mitarbeiter verhindern, erkennen und abwehren können. Gleichzeitig muss sie Sicherheitsteams die Übersicht und Erkenntnisse liefern, die sie zum effektiven Arbeiten benötigen. Dabei darf ihre Konfiguration und Verwaltung nicht kompliziert sein.

Bewertung der Kosten

Angenommen, Ihr Unternehmen ist ein Finanzdienstleister in den USA mit 15.000 Angestellten und Sie sollen zwei E-Mail-Sicherheitslösungen bewerten. Eine der beiden ist eine „kostenlose“ Lösung im Paket mit einem vorhandenen Produkt, das Sie bereits lizenzieren. In diesem Beispiel wird angenommen, dass ein Vollzeitmitarbeiter (FTE) das Unternehmen 150.000 US-Dollar im Jahr kostet.

Ihre Kosten (für drei Jahre) könnten wie folgt aussehen:

KOSTENKATEGORIE	E-MAIL-SICHERHEITSLÖSUNG A	E-MAIL-SICHERHEITSLÖSUNG B
Lizenzierungskosten	–787.500 $	–0 $ (die neue Lösung ist ein Add-on und Sie behalten das Paket)
Professional Services	–27.000 $	–0 $ (bereits implementiert)
Mitarbeiterzeit: Implementierung	–6.250 $ (1 FTE für 0,5 Monate)	–0 $ (bereits implementiert)
Mitarbeiterzeit: Betrieb	–450.000 $ (1 FTE pro Jahr)	–450.000 $
Gesamt	**–1.270.750 $**	**–450.000 $**

In diesem Fall scheint ein erster Blick auf die Kosten nahezulegen, dass Lösung B den größeren Nutzen bietet, da Lösung A mit Mehrkosten von über 700.000 US-Dollar verbunden ist. Die Professional Services sowie die Bereitstellung für die vorhandene Lösung sind frühere Ausgaben und hier nicht relevant.

Vorteile der E-Mail-Sicherheitslösung

Um den Gesamtnutzen der Lösungen zu ermitteln, müssen Sie auch die jeweiligen Vorteile berücksichtigen, z. B. Risikominimierung sowie Effizienzsteigerung für Mitarbeiter.

Im Laufe der drei Jahre könnte das so aussehen:

VORTEILKATEGORIE	E-MAIL-SICHERHEITS-LÖSUNG A	E-MAIL-SICHERHEITS-LÖSUNG B
Risikominimierung	5.707.901 $	4.442.698 $
Anwenderproduktivität	1.200.208 $	974.788 $
Überwachung, Triage und Analysen	1.532.510 $	1.224.135 $
Reaktions- und Behebungsmaßnahmen	2.651.671 $	2.153.641 $
Automatisierung	0 $	756.685 $
Bedrohungsdaten	0 $	0 $
Gesamt	**11.092.290 $**	**9.551.947 $**

Lösung A bietet eine erheblich bessere Risikominimierung und verbessert die Mitarbeitereffizienz, was die Situation verkompliziert. Lösung B bietet eine Zusatzfunktion, sodass wir in diesem Fall untersuchen sollten, ob diese Option bei Lösung A hinzugefügt werden könnte, was unsere Rendite der Sicherheitsinvestition (ROSI) verbessern könnte.

Abschließend sollten Sie die Gesamtkosten mit den Vorteilen beider Lösungen vergleichen, um den Gesamtnutzen jeder Lösung zu erhalten:

KATEGORIE	E-MAIL-SICHERHEITS-LÖSUNG A	E-MAIL-SICHERHEITS-LÖSUNG B
Vorteile	11.092.290 $	9.551.947 $
Kosten	–1.270.750 $	–450.000 $
Gesamtnutzen	**9.821.540 $**	**9.101.947 $**

Hier zeigt sich nun das gesamte Bild. Lösung A ist zwar teurer, doch der Gesamtnutzen ist mehr als 700.000 US-Dollar höher als bei der „kostenlosen“ Option von Lösung B. Für den Vergleich sollten Sie auch Ihre geschäftlichen Anforderungen berücksichtigen.

Beispiel 2

Cloud-Sicherheit

Moderne Cloud-Sicherheitslösungen helfen Unternehmen dabei, personenzentrierte Risiken in der Cloud einzudämmen. Unternehmen setzen heute Cloud-Plattformen und -Dienste in immer größerem Maßstab ein. Damit unterstützen sie ihre remote und hybrid arbeitenden Angestellten und profitieren von der Flexibilität und geschäftlichen Agilität durch die Cloud. Bei allen Vorteilen erzeugen Cloud-basierte Anwendungen und Services aber auch neue Risiken. Ein CASB (Cloud Application Security Broker) sichert von der IT-Abteilung genehmigte Anwendungen in der Cloud ab. Eine solche Lösung kann jedoch auch Transparenz und Kontrolle darüber bieten, wie Mitarbeiter auf diese Anwendungen zugreifen und sie nutzen – und wie sie vertrauliche Daten weitergeben.

Im Jahr 2021 war die Zahl der Kompromittierungen von Cloud-Ressourcen zum ersten Mal größer als die von lokalen Assets.[14] Unternehmen wechseln in die Cloud – und die Angreifer folgen ihnen. Da die Geschäftswelt immer stärker auf Software-as-a-Service-Anwendungen wie Microsoft 365 und Google Workspace setzt, rechnen wir mit einer Fortsetzung dieses Trends.

Wenn Sie einen erheblichen Teil Ihrer Infrastruktur in die Cloud verlagern, ist die Frage nicht, *ob* Sie eine Cloud-Sicherheitslösung benötigen, sondern welche.

Bewertung der Kosten

In diesem Beispiel ist Ihr Unternehmen im Gesundheitssektor in den USA tätig, verfügt über 15.000 Angestellte und Sie interessieren sich für eine neue Cloud-Lösung (Lösung A), die Sie mit Ihrer vorhandenen Lösung (Lösung B) vergleichen. In diesem Beispiel wird außerdem angenommen, dass ein Vollzeitmitarbeiter (FTE) das Unternehmen 150.000 US-Dollar im Jahr kostet.

Die Kostenaufstellung innerhalb von drei Jahren könnte wie folgt aussehen:

KOSTENKATEGORIE	CLOUD-SICHERHEITSLÖSUNG A	CLOUD-SICHERHEITSLÖSUNG B
Lizenzierungskosten	–776.250 $	–765.000 $
Professional Services	–26.000 $	–0 $ (bereits implementiert)
Mitarbeiterzeit: Implementierung	–6.250 $ (1 FTE für 0,5 Monate)	–0 $ (bereits implementiert)
Mitarbeiterzeit: Betrieb	–450.000 $ (1 FTE pro Jahr)	–450.000 $
Gesamt	**–1.258.500 $**	**–1.215.000 $**

In diesem Fall liegen die Kosten von Lösung A etwas oberhalb der Kosten von Lösung B. Die Professional Services sowie die Bereitstellung für die vorhandene Lösung sind frühere Ausgaben und hier nicht relevant. Der echte Unterschied zwischen den Lösungen zeigt sich beim Vergleich der Vorteile.

WICHTIGER HINWEIS: Wenn Sie bereits eine Identitäts- und Zugriffsverwaltungslösung einsetzen und zu einem CASB wechseln möchten, müssen Sie möglicherweise zusätzliche Hardware-Kosten berücksichtigen. Der Wechsel in die Cloud ist meist mit geringeren Ausgaben für Hardware verbunden, Ihre Gesamteinsparungen hängen jedoch vom gewählten Cloud-Anbieter ab.

14 Verizon: „**2021 Data Breach Investigations Report**“ (Untersuchungsbericht zu Datenkompromittierungen 2021), Mai 2021.

Bewertung der Vorteile

Ebenso wie bei der Evaluierung der E-Mail-Sicherheitslösungen müssen Sie auch hier die Vorteile jeder Lösung vergleichen, um den Gesamtnutzen jeder Option zu ermitteln. Im Laufe der drei Jahre könnte das so aussehen:

VORTEILKATEGORIE	CLOUD-SICHERHEITS-LÖSUNG A	CLOUD-SICHERHEITS-LÖSUNG B
Risikominimierung	6.137.377 $	3.625.216 $
Anwenderproduktivität	42.684 $	34.667 $
Überwachung, Triage und Analysen	104.339 $	84.742 $
Reaktions- und Behebungsmaßnahmen	94.853 $	77.038 $
Bedrohungsdaten	**1.264.707 $**	**1.027.174 $**
Gesamt	**7.643.961 $**	**4.848.837 $**

In diesem Fall bietet Lösung A erheblich eine bessere Risikominimierung sowie größere Effizienzsteigerungen für Mitarbeiter.

	CLOUD-SICHERHEITS-LÖSUNG A	CLOUD-SICHERHEITS-LÖSUNG B
Vorteile	**7.643.961 $**	**4.848.837 $**
Kosten	–1.258.500 $	–1.215.000 $
Gesamtnutzen	6.385.461 $	3.633.837 $

Wegen der besseren Risikominimierung und den Effizienzsteigerungen für Mitarbeiter bietet Lösung A fast den doppelten Nutzen von Lösung B.

Die Fakten

Bei der Entscheidung über die Investition in eine Sicherheitslösung müssen Sie sorgfältig die Kosten und Vorteile der jeweils verfügbaren Optionen abwägen. Sie benötigen eine Lösung, die einerseits Ihren kurzfristigen Budgetrahmen einhält, gleichzeitig jedoch auch langfristige finanzielle Risiken für Ihr Unternehmen minimiert.

Optionen mit geringen Lizenzierungskosten können auf den ersten Blick lohnenswert scheinen. Wenn Sie die bestmögliche Entscheidung treffen möchten, müssen Sie jedoch etliche weitere Faktoren berücksichtigen. Entscheiden Sie sich für einen Anbieter, dessen Lösung umfassende und vollständige Abdeckung für die häufigsten Angriffsvektoren bietet.

Berücksichtigen Sie dabei, dass Integrationen mit anderen Sicherheitslösungen Ihrem Team die dringend benötigte Transparenz bieten und damit die notwendigen Bedrohungsdaten liefern, anhand derer Sie Kontrollen zur Risikominimierung implementieren können.

Ebenso wichtig sind Workflows, die sich leicht bedienen und verwalten lassen, sowie zuverlässige und hochleistungsfähige automatisierte Bedrohungsblockierung. Da heute ein Mangel an Sicherheitsexperten herrscht, können Sie mit allem, was Ihrem Team die Arbeit erleichtert, die Arbeitskosten reduzieren. Gleichzeitig können Ihre Mitarbeiter dadurch einen größeren Beitrag zum Nutzen der Lösung liefern.

Dank Transparenz erhalten Sie auch Erkenntnisse über personenzentrierte Risiken, die andernfalls Ihrer Aufmerksamkeit entgehen. Angreifer wissen heute, dass Ihre Mitarbeiter den leichtesten Weg ins Unternehmen darstellen. Deshalb konzentrieren sich die effektivsten Lösungen darauf, diese Risiken zu identifizieren und zu minimieren. Und mit einem Fokus auf personenzentrierte Risiken können Sie bestmöglich von Ihren Sicherheitsinvestitionen profitieren.

Gehen Sie den nächsten Schritt

Proofpoint bietet umfassende und intelligente E-Mail- und Cloud-Sicherheitslösungen, um Ihre Mitarbeiter vor den gefährlichsten aktuellen Bedrohungen zu schützen. Wenn Sie mehr erfahren möchten und an einer Risikoschnellanalyse für Ihr Unternehmen interessiert sind, **besuchen Sie proofpoint.com/de**.

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 75 Prozent der Fortune-100-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.

0501-012-04-01 09/22