ivanti

Cyber-Risiken objektiv bewerten:

Ein Leitfaden für datengestützte Risikobewertungen

ivanti.com/de

Inhaltsverzeichnis

Über dieses E-Book

Exposure Management setzt Sicherheitsrisiken in Beziehung zur allgemeinen Risikobereitschaft des Unternehmens. So können Sicherheitsverantwortliche fundierte Empfehlungen aussprechen, die bei anderen Führungskräften auf tatsächliche Zustimmung stoßen.

Dieses E-Book liefert die Tools für eine entscheidende Komponente des Exposure Management: **datengestützte Risikobewertung.**

Wir stellen eine unkomplizierte Methode zur Durchführung von Risikobewertungen und zur übersichtlichen Darstellung der Ergebnisse vor. Dabei zeigen wir konkret, welche Auswirkungen es auf geschäftskritische Assets hat, Risiken zu reduzieren – oder sie bewusst in Kauf zu nehmen.

Wir zeigen Ihnen, wie Sie den Risikobewertungsprozess in verschiedenen Szenarien anwenden, geben konkrete Beispiele und Tipps für die überzeugende Präsentation Ihrer Analyse und Maßnahmen – und helfen Ihnen, zusammen mit anderen Führungskräften ein gemeinsames Verständnis von Risiken und Exposures zu schaffen.

Einführung

Sie kennen die Cyberangriffe, denen Ihr Unternehmen ausgesetzt ist – die ‚Schwachstellen', die immer wieder Probleme verursachen, ebenso wie die Maßnahmen, mit denen sich die Sicherheitslage Ihres Unternehmens verbessern lässt.

Ihre Kolleginnen und Kollegen in anderen Unternehmensbereichen kennen ihre Ziele – und die kalkulierten Risiken, die sie bereit sind einzugehen, um diese zu erreichen.

Letztlich verfolgen Sie beide dasselbe Ziel: ein stabiles und profitables Unternehmen. Doch ohne ein gemeinsames Verständnis von Risiken reden Sie aneinander vorbei.

Damit alle Beteiligten an einem Strang ziehen, ist eine fundierte, objektive und messbare Einschätzung der Cyber-Risiken unerlässlich.

Eine Risikobewertung und ihre Ergebnisse formulieren Erkenntnisse in einer Form, die auch andere Führungskräfte verstehen – und erleichtern es Ihnen so, Unterstützung für zentrale Sicherheitsinitiativen zu gewinnen.

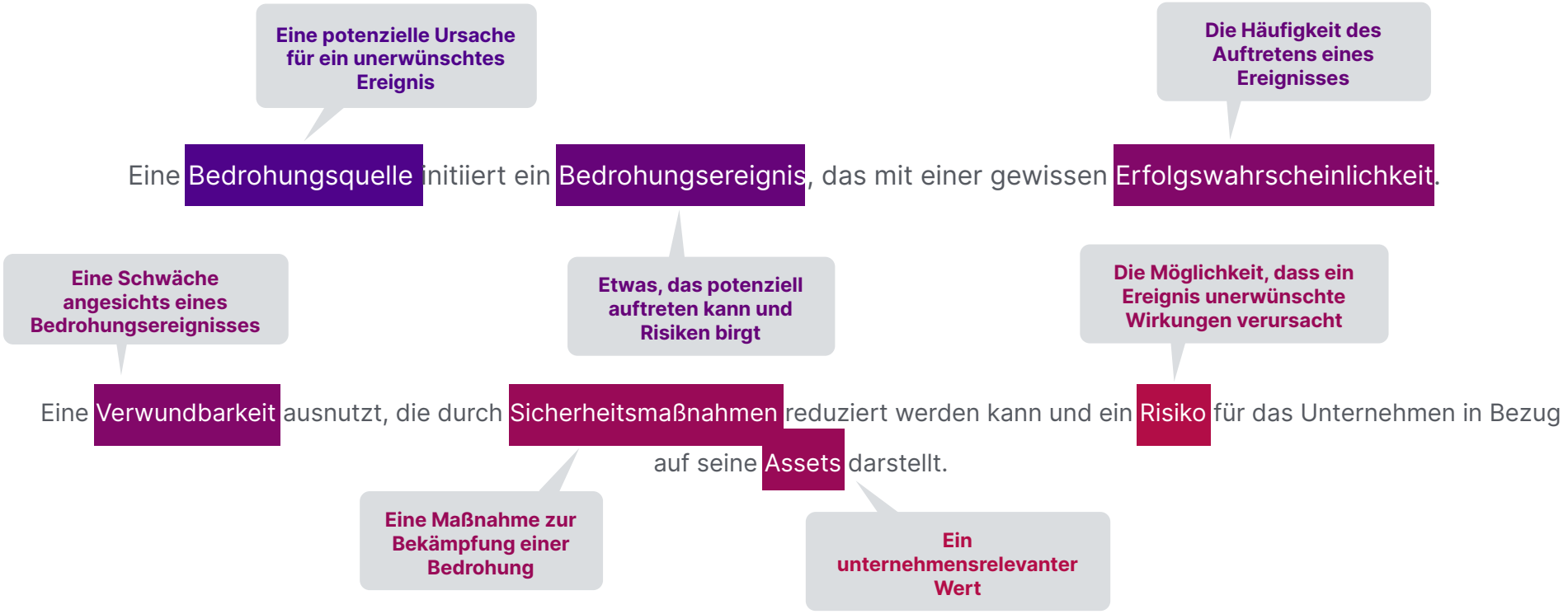
Dabei werden möglicherweise auch Ihre Annahmen darüber hinterfragt, welche Risiken gemindert und welche akzeptiert werden sollten.

Wie lässt sich also ein Sicherheitsereignis, das noch gar nicht eingetreten ist, in Zahlen fassen? Das werden wir uns genauer anschauen.

Risikobewertung

Schlüsselbegriffe und allgemeine Risikomodellierung

Ein allgemeines Risikomodell sieht etwa so aus:



Reale Ereignisse verlaufen häufig nach diesem Muster, zum Beispiel:

Die **ALPHV**-Gruppe war für mehrere **erfolgreiche Ransomware-Angriffe** auf Unternehmen in den USA, Europa und dem asiatisch-pazifischen Raum (APAC) verantwortlich. Dabei nutzten die Angreifer **Schwächen in der Zugangskontrolle und unzureichende Schulungen der Mitarbeitenden** aus. Die Angriffe führten zu tagelangen Betriebsausfällen und – in einigen Fällen – zu erheblichen **Backlogs**, da keine regelmäßigen Backups vorhanden waren. Dies hatte **finanzielle, reputationsschädigende und rechtliche Risiken** für die betroffenen Unternehmen zur Folge. Zudem besteht die Möglichkeit, dass sensible **Informationen** kompromittiert und öffentlich gemacht wurden.

Schritte der Risikobewertung

Die Risikobewertung erfolgt in fünf einfachen Schritten, die wir in diesem Abschnitt behandeln.

1. Bestimmen Sie die für Ihre Risikobewertung infrage kommenden Assets.
2. Weisen Sie diesen Assets einen Wert zu.
3. Ermitteln Sie die Schwachstellen und Bedrohungen.
4. Berechnen Sie die Risiken (Wahrscheinlichkeit multipliziert mit den Auswirkungen).
5. Führen Sie eine Kosten-Nutzen-Analyse durch.

Anschließend können Sie Handlungsempfehlungen für den Umgang mit Risiken ableiten, die durch die Ergebnisse Ihrer Risikobewertung gestützt werden. Es gibt vier mögliche Reaktionen auf Risiken, auf die wir später noch näher eingehen werden.

Sie vermeiden
das Risiko, indem die riskante Aktivität gestoppt oder das gefährdete System ganz abgeschaltet wird.

Sie akzeptieren
das Risiko und entscheiden sich, mit dem Risiko zu leben und keine Maßnahmen zu ergreifen.

Sie übertragen
das Risiko auf Dritte – in der Regel durch den Abschluss einer Versicherung zur Deckung des finanziellen Risikos.

Sie mindern
das Risiko durch zusätzliche Sicherheitsvorkehrungen.

Schritt 1
Identifizierung von Assets

Wonach suchen wir?

Assets können als **materiell** (Gebäude, Menschen, Ausrüstung) oder **immateriell** (Informationen, Patente, Marke, Lizenzen, Kundenliste, F&E) kategorisiert werden.

Die Assets können auch nach ihrer Zugehörigkeit kategorisiert werden. Auf höherer Ebene unterscheidet man dabei zwischen **Geschäfts-Assets** (z. B. Bargeld, Grundstücke, Lagerbestände, Produktionsanlagen, Fachwissen von Mitarbeitenden) und **IT-Assets** (z. B. Software, Server, Firewalls, Laptops, Monitoring-Tools).

Aber IT-Assets sind nicht nur für sich selbst da: Sie dienen letztlich dem Schutz der Geschäfts-Assets. Ihr Unternehmen verfügt möglicherweise über ein Geschäftsgeheimnis (ein immaterielles Geschäfts-Asset), das sich auf einem Server befindet (ein materielles IT-Asset). Die Sicherheitskontrollen, die auf diesem einzigen Server angewandt werden, können über Erfolg oder Misserfolg des Unternehmens entscheiden.

Nehmen wir an, es geht Ihnen um den Schutz vor Datenverlust. Ermitteln Sie, welche Geräte in Ihren Verantwortungsbereich fallen – etwa geschäftlich genutzte Laptops, private Geräte im Rahmen von BYOD, Telefone oder Drucker – und wie viele davon im Einsatz sind. Im Idealfall greifen Sie dabei auf ein regelmäßig gepflegtes Inventar zurück. Damit können Sie erklären, warum die Sicherung von x Endgeräten tatsächlich gleichbedeutend ist mit der Sicherung von Geschäfts-Assets, die vertrauliche Informationen enthalten, wie z. B. Kundendaten, Kreditkarteninformationen oder Mitarbeitergehälter.

Zwar wollen Sie in erster Linie vermeiden, dass vertrauliche Informationen nach außen dringen – doch wenn Sie das Risiko messbar machen, schaffen Sie die Grundlage für eine fundierte Risikostrategie und erhalten leichter interne Unterstützung.

Geschäftskritischste Assets

Die **geschäftskritischsten Assets** eines Unternehmens sind jene, bei deren Kompromittierung die gravierendsten Auswirkungen auf das Geschäft entstehen würden.

Informationen zählen für Sie vermutlich zu den wertvollsten Geschäftsassets – und das zu Recht. Allerdings könnten andere Führungskräfte da anderer Meinung sein. Manche Entscheidungsträger verweisen möglicherweise auf bestimmte Geschäftsprozesse oder Systeme – ohne sich bewusst zu machen, dass diese ohne Informationen keinen eigenen Wert hätten. Informationen überdauern Systeme oft um ein Vielfaches – und sind letztlich das, was wirklich geschützt werden muss.

Sie beziehen sich letztlich auf dieselben Assets, denn Geschäftsprozesse und Informationssysteme gehören zusammen. Um jedoch Wirkung zu zeigen, muss Ihre Risikobewertung sehr spezifisch sein.

Nehmen wir an, eines der geschäftskritischsten Assets des Unternehmens ist das CRM-System sowie die damit verarbeiteten Kundendaten, die es verarbeitet. Beachten Sie den Unterschied zwischen diesen zwei Aussagen:

*„Wir riskieren, dass sensible **Daten** durch DNS-Spoofing in die Hände von Angreifern geraten."*

„Infolge einer Datenschutzverletzung – wie sie im vergangenen Jahr 45 % der Unternehmen unserer Branche betroffen hat – könnten Kundendaten (PII) sowie über Salesforce verarbeitete Transaktionen öffentlich bekannt werden. Dies hätte voraussichtlich Geldbußen in Höhe von 4,5 Milliarden US-Dollar zur Folge, einen nicht endenden administrativen Aufwand durch Klagen sowie einen Reputationsschaden, von dem sich das Unternehmen erst in 5 bis 10 Jahren erholen würde."

Der zweite Punkt ist eindeutig aussagekräftiger – und Ihre Risikobewertung wird Ihnen dabei helfen, genau dieses Maß an Konkretheit zu erreichen.

Schritt 2
Bestimmung des Asset-Wertes

Ob materiell oder immateriell, der Wert eines Assets muss klar sein. Die Bewertung des Asset-Werts fällt nicht zwingend in den Aufgabenbereich des Sicherheitsteams – dennoch ist sie ein wesentlicher Parameter für unternehmerische Entscheidungen über notwendige Sicherheitsmaßnahmen.

Bei der Bestimmung des Werts eines Assets sollten folgende Aspekte berücksichtigt werden:

- Kosten für den Erwerb oder die Entwicklung des Assets.
- Kosten für die Instandhaltung und den Schutz des Assets.
- Wert des Assets für Verantwortliche und User.
- Wert des Assets für potenzielle Angreifer.
- Preis, den andere für das Asset zu zahlen bereit sind.
- Kosten für die Wiederbeschaffung des Assets bei Verlust.
- Betriebs- und Produktionsabläufe, die durch den Ausfall des Assets beeinträchtigt würden.
- Haftungsfragen, wenn das Asset gefährdet wäre.
- Geschäftlicher Nutzen und Rolle des Assets im Unternehmen.

Jedes Asset des Unternehmens sollte einen Verantwortlichen haben, und der Wert des Assets sollte von diesem Verantwortlichen festgelegt werden, möglicherweise unter Anleitung des Sicherheitsteams.

Die entscheidende Frage lautet daher: Was würde es das Unternehmen kosten, dieses Asset NICHT zu schützen? Die Beantwortung dieser Frage beginnt mit einer Analyse der geschäftlichen Auswirkungen, der sogenannten Business Impact Analysis (BIA)

Eine ideale Analyse der geschäftlichen Auswirkungen

Eine BIA ist in der Regel ein fester Bestandteil im Lebenszyklus der Geschäftskontinuitätsplanung. Dabei handelt es sich um einen Schlüsselmoment, in dem sich die IT-Abteilung und die Fachbereiche abstimmen, um die geschäftskritischen Aktivitäten sowie die dafür erforderlichen Assets gemeinsam zu identifizieren und zu priorisieren.

Die Frage „Was genau würde passieren, wenn dieser Prozess nicht mehr funktioniert?“ veranlasst die Prozessverantwortlichen und Abteilungsleiter, über mögliche Auswirkungen, auch finanzieller Art, nachzudenken und diese anzugeben. So erhalten Sie realistische Zahlen, die Sie für Ihre Risikobewertung verwenden können.

Eine ideale BIA umfasst:

- Prozesszweck, Verantwortliche, Inputs und Outputs.
- Die Auswirkungen einer Unterbrechung, gemessen an den finanziellen, betrieblichen, rechtlichen/regulatorischen und reputationsschädigenden Folgen.
- Die schlimmstmöglichen Szenarien und Zeiten einer Unterbrechung (z. B. Spitzenzeiten).
- Wiederherstellungszeit-Ziele (RTOs), Wiederherstellungspunkt-Ziele (RPOs) und maximal tolerierbare Ausfallzeit (MTD) für Aktivitäten.
- Ressourcen, die zur Durchführung/Unterstützung des Prozesses benötigt werden: andere Organisationseinheiten, Informationen, Mitarbeitende, Infrastrukturen, Lieferantenstandorte und IT-Assets. Diese Ressourcen übernehmen die RTOs und RPOs des Prozesses und werden im Falle einer Störung entsprechend vorrangig wiederhergestellt.

Tipps

Es gibt zwar zahlreiche Vorlagen, aber es gibt kein universelles Format, die für alle passt. Deshalb bieten wir Ihnen unten eine vereinfachte, bearbeitbare Vorlage zum Download an, die als Ausgangspunkt für eine BIA dienen kann.

Geschäftskontinuität und Informationssicherheit können in verschiedenen Abteilungen angesiedelt sein. In diesem Fall sollten die Informationen ausgetauscht werden, um ein einheitliches Konzept für das Risikomanagement zu gewährleisten.

Festlegung der Kritikalität von Assets mittels BIA

Die Business Impact Analysis (BIA) ermittelt, welche unternehmenskritischen Systeme für die Geschäftsprozesse besonders relevant sind, und schätzt ab, wie lange ein Ausfall dieser Systeme maximal toleriert werden kann. Diese höchstzulässige Ausfallzeit wird als Maximum Tolerable Downtime (MTD) bezeichnet.

Einige Beispiele für MTD:

- **Unkritisch:** 30 Tage
- **Normal:** 7 Tage
- **Wichtig:** 72 Stunden
- **Dringend:** 24 Stunden
- **Kritisch:** Minuten bis Stunden

Jeder Geschäftsprozess und jedes Asset sollte einer dieser Kategorien zugeordnet werden – abhängig davon, wie lange das Unternehmen ohne sie funktionsfähig bleiben kann. Diese Einschätzungen helfen dabei, den notwendigen Schutzbedarf zu ermitteln, um die Verfügbarkeit dieser Ressourcen sicherzustellen.

Wenn ein Webserver-Ausfall innerhalb von vier Stunden 120.000 US-Dollar kosten würde, gilt der Server als kritisch – und das Unternehmen sollte einen redundanten Webserver in Betracht ziehen.

Verursacht der Ausfall eines Reporting-Tools zur Gebäudeauslastung über drei Wochen hinweg weniger als 500 US-Dollar an Kosten, gilt dies als **unkritisch** – und man kann sich auf das SLA des Anbieters oder eine Wiederherstellung nach Best-Effort-Prinzip verlassen.

Tipp

Prozess- und System-RTOs, in Verbindung mit den entsprechenden finanziellen Verlustwerten, können als Parameter in einer quantitativen Risikobewertung verwendet werden. Mit hoher Wahrscheinlichkeit liegen Ihnen diese Informationen bereits vor – etwa in bestehenden Business-Impact-Analysen (BIA) oder in Ihrem Disaster-Recover-Plan. Falls diese nicht verfügbar sind, können Sie die Analyse problemlos auf Ihren eigenen Verantwortungsbereich beschränken.

Eine vereinfachte BIA könnte folgendermaßen aussehen.

Prozessname	Prozessunterbrechung	Finanzielle Auswirkungen	Rechtliche Auswirkungen	Auswirkungen auf die Reputation
Zahlungen am selben Tag	<4 Stunden	$-$$$	n/a	n/a
	4-8 Stunden	$$$-$$$	n/a	Niedrig
	2-5 Arbeitstage	$$$-$$$$	Mittel	Mittel
	1-2 Wochen	$$$-$$$$	Medium	Hoch
	2-4 Wochen	$$$$-$$$$$$	Hoch	Kritisch
Rechtfertigung	▪ Verlust der Reputation und des öffentlichen Vertrauens: ... ▪ Verlust von Wettbewerbsvorteilen: ... ▪ Anstieg der Betriebskosten: ... ▪ Verletzung von vertraglichen Vereinbarungen: ... ▪ Verstöße gegen rechtliche und regulatorische Anforderungen: ... ▪ Kosten durch verzögerte Einnahmen: ... ▪ Umsatzeinbußen: ... ▪ Produktivitätsverluste: ... ▪ Sonstiges: ...			
Benötigte Ressourcen	Personal: mindestens vier Mitarbeitende in der ersten Woche; mindestens sechs Mitarbeitende nach einer Woche Zahlungssystem: muss verfügbar sein, keine manuellen Umgehungen Zahlungstoken: mindestens zwei Token IT-Systeme: Zahlungssystem (Server + Datenbank), Internet, Verbindung zur Clearingstelle, E-Mail Standort: kann am ersten Tag von zu Hause aus arbeiten, benötigt dann einen Büroarbeitsplatz Bürobedarf: Drucker			

Tipp

Sie können diese BIA-Vorlage als bearbeitbare Folien herunterladen.

Wie die BIA mit der Risikobewertung zusammenhängt

Die BIA ist Teil einer auf die Geschäftskontinuität ausgerichteten Risikobewertung. Sie zeigt die Auswirkungen unwahrscheinlicher, aber wichtiger Szenarien auf die Geschäftsaktivitäten auf und macht die Prioritäten der Unternehmen deutlich. Anhand dieser Ergebnisse können Sie die geschäftskritischsten Assets Ihres Unternehmens bestimmen, einschließlich der unterstützenden Informationssysteme.

Die Risikobewertung erfolgt üblicherweise in Form einer Gleichung: **Risiko = Bedrohung × Auswirkung × Wahrscheinlichkeit.** Die BIA ergänzt diese Gleichung jedoch um eine entscheidende Dimension: die Zeit. Sie fokussiert sich auf jene Bedrohungen, die kritische Geschäftsprozesse am schnellsten beeinträchtigen können. Daher bildet die BIA eine zentrale Grundlage für die Auswahl geeigneter Schutzmaßnahmen – insbesondere solcher, die die **Verfügbarkeit** im Rahmen des **CIA-Modells (Vertraulichkeit, Integrität und Verfügbarkeit)** sicherstellen.

Ein **Ransomware-Angriff** passt ideal in eines der Kontinuitätsszenarien, da er die Verfügbarkeit von Daten verhindert. Allerdings wirken sich nicht alle Sicherheitsrisiken auf die **Verfügbarkeit**skomponente aus.

Ein Datenabfluss – also das unbefugte Abschöpfen von Daten ohne Einsatz von Ransomware – kann Systeme und Prozesse scheinbar ungestört weiterlaufen lassen, während die Daten weiterhin verfügbar bleiben – oder besser gesagt: auch für Unbefugte verfügbar. Damit wird das Schutzziel der Vertraulichkeitskomponente im Rahmen des CIA-Modells verletzt. Prozesse, die mit den kompromittierten Daten arbeiten, werden in diesem Szenario nicht automatisch gestoppt.

Strategisch sensible Daten gehören in der Regel zu den geschäftskritischsten Assets eines Unternehmens. Eine böswillige Veränderung (Integritätskomponente) oder die Offenlegung ist ein weiteres Beispiel, das möglicherweise nicht in der BIA erfasst wird.

Aus diesem Grund müssen Sie Ihre Risikobewertung aus zusätzlichen Blickwinkeln angehen - eine BIA bildet dafür die beste Grundlage.

Bewertung nach dem CIA-Modell

Mittels der BIA haben wir festgelegt, welche Assets zeitkritisch sind. Eine **Bewertung nach dem CIA-Modell** kann das Verständnis um eine sicherheitskritische Dimension erweitern.

ISACA empfiehlt eine Methode zur Asset-Bewertung, bei der der Wert eines Assets entsprechend seiner Sensitivität gewichtet wird.

Jedem der drei Schutzziele des CIA-Modells wird ein Wert zwischen 1 (niedrig) und 3 (hoch) zugewiesen. Die Bewertung nach dem CIA-Modell ergibt sich aus der Summe der drei Werte Vertraulichkeit (C), Integrität (I) und Verfügbarkeit (A) – also einem Score zwischen 3 und 9.

Jedem Unternehmens-Asset wird eine Bewertung nach dem CIA-Modell zugewiesen, die unmittelbar mit der risikobasierten Auswahl und Umsetzung von Sicherheitsmaßnahmen verknüpft ist. Eine Bewertung von C3-I2-A2 (7) erfordert andere Maßnahmen als ein Asset mit der Bewertung C1-I1-A2 (4).

Beide Methoden werden gemeinsam mit den Fachverantwortlichen durchgeführt, die für die Informationen verantwortlich sind, die durch ihre Assets fließen. Dies bietet die Chance, ein gemeinsames Verständnis für den Wert von Assets zu schaffen und die Diskrepanz zwischen Risikobewusstsein und geschäftlicher Zielsetzung zu verringern.

Tipps

Eine Bewertung nach dem CIA-Modell ist nicht für jedes einzelne Konfigurationsobjekt oder jede virtuelle Desktop-Infrastruktur (VDI) erforderlich. Die Assets sollten so gruppiert werden, wie es für das Unternehmen sinnvoll ist, z. B. nach einem gemeinsamen Geschäftsziel.

Falls Ihr Unternehmen eine Erklärung zur Risikobereitschaft veröffentlicht hat, nutzen Sie diese als Referenzpunkt, um die Kriterien Ihrer Bewertung nach dem CIA-Modell mit anderen Führungskräften abzugleichen. (Sie haben keine Erklärung? Verwenden Sie diese bearbeitbare Vorlage als Grundlage).

Schritt 3

Bedrohungsmodellierung und Schwachstellenanalyse

Der nächste Schritt in der Risikobewertung ist die Ermittlung von Bedrohungen und Schwachstellen mit hoher Priorität. Selbst wenn Sie bereits eine klare Vorstellung haben, was relevant ist, stärkt die Validierung Ihrer Annahmen die Aussagekraft und Glaubwürdigkeit der Risikobewertung.

Bedrohungsmodellierung (Threat Modeling)

Eine effektive Bedrohungsmodellierung (Threat Modeling) setzt fundierte Bedrohungsdaten voraus: Es berücksichtigt das globale Bedrohungsumfeld, typische Angriffsarten auf vergleichbare Unternehmen sowie die individuellen Besonderheiten Ihres Geschäftsmodells. Auf diese Weise konzentrieren Sie Ihre Bemühungen auf Bedrohungen, die mit größerer Wahrscheinlichkeit eintreten werden, anstatt sich auf weniger wahrscheinliche Bedrohungen zu konzentrieren.

Es gibt viele Methoden für die Erstellung von Bedrohungsmodellen.
Zwei gängige Methoden sind:

Attack Trees (Angriffsbäume):
Eine Bedrohungsquelle verfügt in der Regel über mehrere Angriffswege, um ein bestimmtes Ziel zu erreichen. Ein Attack Tree (Angriffsbaum) stellt mögliche Angriffspfade als verzweigte Baumstruktur mit Blattknoten dar. Diese zeigen auf, welche Bedingungen ein Angreifer erfüllen muss, um sein Ziel zu erreichen. Jeder Knoten wird dabei auf Schwachstellen hin analysiert.

Reduktionsanalyse:
Dieser Ansatz baut auf Attack Trees auf und findet Gemeinsamkeiten zwischen den Blattknoten. Auf diese Weise können Sie potenzielle Sicherheitsmaßnahmen ermitteln, die jeweils mehr als eine Schwachstelle entschärfen könnten.

Tipp

Die in der Bedrohungsmodellierung ermittelten Angriffsbeispiele verleihen Ihrer Risikobewertung und Ihren Empfehlungen zur Risikominderung mehr Anschaulichkeit – und helfen dabei, Sicherheitsbedrohungen für fachfremde Führungskräfte nachvollziehbar zu machen.

Schwachstellenanalyse

Die Bedrohungsmodellierung (Threat Modeling) betrachtet Bedrohungen von außen nach innen – es beginnt bei potenziellen Angreifern und analysiert deren mögliche Angriffswege. Die Schwachstellenanalyse hingegen geht von innen nach außen vor: Sie identifiziert Sicherheitslücken in Ihrer Angriffsfläche, die Angreifer ausnutzen könnten.

Ein zentraler Grundsatz des Exposure Managements ist eine breite Definition der Angriffsfläche. Bei der Bewertung von Schwachstellen in Ihrer Angriffsfläche sollten Sie beachten, dass diese mehr umfassen als nur Informations- und Systemschwachstellen. Schwachstellen können auch in Prozessen liegen (z. B. bei verspätetem oder fehlerhaftem Patching) oder im Verhalten von Mitarbeitenden (z. B. Anfälligkeit für Social Engineering, Verwendung schwacher Passwörter).

Software wie z.B. Netzwerk-Schwachstellen-Scanner, Anwendungssicherheitstests und External Surface Management liefern wertvolle Informationen über potenzielle Schwachstellen. Möglicherweise verfügen Sie auch über Informationsquellen wie Audit-Reports, Risikoregister, Kontrolltests, Ergebnisse von Pen-Tests, Reports über Zwischenfälle, Studien über Richtlinien und reine Beobachtungen des Unternehmensumfeldes.

Wenn es um Systemschwachstellen geht, sind die Bewertungssysteme von Anbietern – wie etwa das Common Vulnerability Scoring System (CVSS) – ein erster Schritt zur Identifikation von besonders kritischen Schwachstellen.
Um Ihre Liste jedoch weiter zu verfeinern (und dabei möglicherweise auch niedrig bewertete Schwachstellen sichtbar zu machen, die für Ihr Unternehmen besonders schwerwiegende Auswirkungen hätten), sollten Sie zwei zusätzliche Filter anwenden: den Bedrohungskontext und den Risikokontext.

Der Bedrohungskontext befasst sich mit der allgemeinen Bedrohungslandschaft:
Wird diese Schwachstelle aktiv ausgenutzt?
Eine Schwachstelle mag zwar als kritisch eingestuft sein, doch wenn sie nicht aktiv ausgenutzt wird, verliert sie an Bedeutung.
Ihre Bedrohungsmodellierung (Threat Modeling) hat diese Analyse bereits angestoßen und liefert dafür wertvolle Anhaltspunkte.

Der Risikokontext bezieht sich auf Ihr Unternehmen:
Welche Auswirkungen hätte es auf unser Unternehmen, wenn diese Schwachstelle ausgenutzt würde?
Eine Schwachstelle mag zwar nur als gering eingestuft sein, doch wenn ihre Ausnutzung ein kritisches System außer Betrieb setzen würde, verdient sie deutlich mehr Aufmerksamkeit. Dank Ihrer Business-Impact-Analyse wissen Sie bereits, welche Assets, Systeme und Prozesse im Falle einer Kompromittierung oder Störung die größten Auswirkungen auf Ihr Unternehmen hätten.

Tipp

Laden Sie diese Checkliste herunter, um sicherzustellen, dass Sie alle Facetten Ihrer Angriffsfläche berücksichtigen.

Schritt 4
Bestimmung des Risikos

Inzwischen kennen wir die Assets (AV), die Bedrohungen und die Schwachstellen. Wir können endlich damit beginnen, die Wahrscheinlichkeit und die Auswirkungen zu betrachten, um Risiken zu berechnen. Es gibt zwei Ansätze zur Messung eines Risikos: quantitativ und qualitativ.

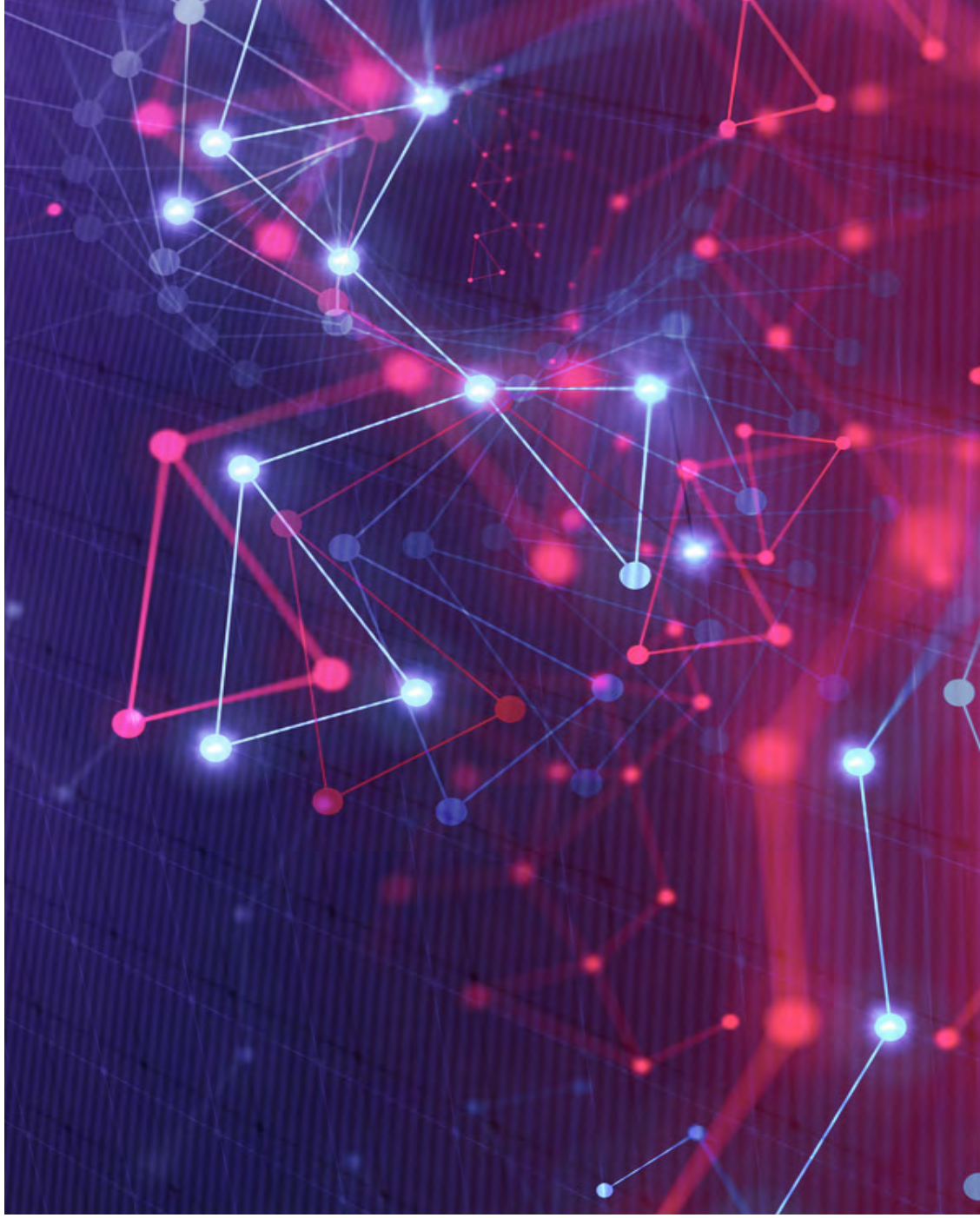
Eine quantitative Risikobewertung verwendet Berechnungen, um den einzelnen Komponenten der Analyse monetäre Werte zuzuweisen.

Eine qualitative Risikobewertung arbeitet mit Bewertungen wie niedrig/mittel/hoch, Skalen von 1 bis 10 oder Ampelmodellen.

Sie können selbst bestimmen, welche Methode für Ihr Unternehmen am besten geeignet ist. In diesem E-Book konzentrieren wir uns hauptsächlich auf die quantitative Risikoanalyse.

Tipp

Durch den Einsatz automatisierter Risikoanalysetools lässt sich der Zeitaufwand manueller Risikobewertungen deutlich reduzieren – gleichzeitig kann der Nutzen verschiedener Sicherheitsmaßnahmen quantifiziert werden.



Quantitative Risikobewertung

Ihr CEO und Ihr Vorstand erwarten, dass Ihre Analyse – wann immer möglich – in monetären und quantitativen Größen dargestellt wird. Es ist das eine, ein hohes Cyber-Risiko zu erkennen. Etwas ganz anderes ist es, konkret zu wissen, dass ein erfolgreicher Ransomware-Angriff, bei dem 15 % der Daten auf einem kritischen System verschlüsselt werden, nicht nur den Wettbewerbsvorteil gefährden würde, sondern auch dazu führen könnte, dass zentrale Geschäftsaktivitäten bis zu vier Tage lang unterbrochen werden – mit täglichen Kosten von 225.000 US-Dollar.

Die allgemein anerkannten Gleichungen zur Quantifizierung des Risikos sind eigentlich recht einfach.

Jährliche Verlusterwartung (ALE) = Einzelverlusterwartung (SLE) x annualisierte Eintrittswahrscheinlichkeit (ARO), wobei Einzelverlusterwartung (SLE) = Asset (AV) x Exposure-Faktor (EF)

Der Exposure-Faktor (EF) stellt den prozentualen Verlust dar, den eine Bedrohung auf ein bestimmtes Asset haben könnte. Wenn beispielsweise ein Geschäftsgeheimnis nach außen dringen könnte, kann der Verlust des Wettbewerbsvorteils 10 % des Asset-Werts betragen – mit anderen Worten: Der Exposure-Faktor (EF) liegt bei 10 %. Unter der Annahme, dass der Asset-Wert (AV) des Geschäftsgeheimnisses 4 Mio. USD beträgt, können Sie eine einfache Gleichung verwenden, um die Einzelverlusterwartung (SLE) zu berechnen:

AV (4 Mio. USD) x EF (10 %) = SLE (400.000 USD)

Die **annualisierte Eintrittswahrscheinlichkeit (ARO)** ist die geschätzte Häufigkeit des Auftretens der Bedrohung innerhalb eines Jahres. Anhand desselben Beispiels könnten Sie vergleichbare Vorfälle in Unternehmen wie dem Ihren betrachten und schätzen, dass alle 20 Jahre ein Geschäftsgeheimnis offengelegt werden könnte. Mit anderen Worten – seine ARO würde 0,05 (1 Jahr/20 Jahre) betragen. Jetzt können wir die jährliche Verlusterwartung (ALE) berechnen:

SLE (400.000 USD) x ARO (0.05) = ALE (20.000 USD)

Das ALE-Ergebnis unterstützt Sie dabei zu entscheiden, ob Ihr Unternehmen Maßnahmen zur Risikominderung ergreifen oder das Risiko bewusst akzeptieren sollte. In unserem Beispiel ließen sich Kontrollmaßnahmen, die weniger als 20.000 USD pro Jahr kosten, wirtschaftlich sinnvoll rechtfertigen.

Das Resultat der quantitativen Risikobewertung ist eine wesentliche Argumentationsbasis, um eine Risikominderungsstrategie wirtschaftlich zu begründen – oder solche Maßnahmen auszuschließen, deren Kosten über der jährlichen Verlusterwartung (ALE) liegen.

Beispiele für Ergebnisse der quantitativen Risikoanalyse

Asset	Bedrohung	SLE	ARO	ALE
Geschäftsgeheimnis	Kompromittiert	4 Mio. USD	0.05	20.000 USD
Datei-Server	Manipuliert	13,5 Mio. USD	0.1	1.350 USD
Betrieb	Firewall	250.000 USD	0.1	25.000 USD
Daten	Malware	7.500 USD	1	7.500 USD
Kreditkarteninformationen des Kunden	Offengelegt	300.000 USD	4	1,2 Mio. USD

Schauen wir uns ein anderes Beispiel an.

Sie wurden kürzlich als IT- und Sicherheitsverantwortlicher bei einem schnell wachsenden KI-Start-up eingestellt. Ihnen ist bewusst, welche erheblichen Risiken ein erfolgreicher Phishing-Angriff mit sich bringen kann. Im Worst-Case-Szenario könnte ein Angreifer Zugriff auf Ihre eigens entwickelten, proprietären Algorithmen erlangen, diese exfiltrieren und veröffentlichen. Das würde nicht nur Ihrem Wettbewerbsvorteil schaden, sondern auch den Unternehmenswert erheblich schmälern. Um das Risiko besser einschätzen zu können, haben Sie interne Phishing-Tests durchgeführt. Das Ergebnis: 10 % der Mitarbeitenden klicken auf verdächtige Links oder öffnen Anhänge.

Jetzt gilt es, Ihrem CEO und den Investoren – deren Fokus vor allem auf technologischem Fortschritt liegt – aufzuzeigen, dass Investitionen in Maßnahmen wie Anti-Phishing-Lösungen und Sicherheitsschulungen für Mitarbeitende notwendig sind, um das Risiko zu begrenzen. Eine quantitative Risikobewertung ist überfällig.

Bestimmen Sie die SLE:

Laut dem IBM Cost of a Data Breach Report 2024 waren Phishing-Angriffe der zweitteuerste anfängliche Bedrohungsvektor (gleichauf mit der Kompromittierung von Geschäfts-E-Mails und an zweiter Stelle nach Bedrohungen durch böswillige Insider) und erreichten im Jahr 2024 einen Durchschnittswert von **4,88 Mio. USD.** Dies ist ein durchschnittlicher SLE, den Sie entsprechend Ihren eigenen **EF**- und **AV**-Variablen anpassen sollten.

Für dieses Beispiel passen wir die SLE an – unter der Annahme, dass Sie für ein deutlich kleineres Unternehmen arbeiten. Ihr EF, also der prozentuale Anteil der kompromittierten Daten, bleibt vermutlich gleich. Allerdings ist der AV deutlich geringer – sagen wir 10 % des ursprünglichen Werts. Daraus ergibt sich eine SLE von 488.000 USD.

Bestimmen Sie die ARO:

Im Zuge Ihrer Recherchen haben Sie herausgefunden, dass Unternehmen ähnlicher Größe in Ihrer Branche wöchentlich mit Phishing-Angriffen konfrontiert werden bzw. 52 pro Jahr. Wenn diese zu 10 % erfolgreich sind – was den Fake-Phishing-Kampagnen entspricht, die das Sicherheitsteam zu Trainingszwecken durchführt – beträgt die jährliche **ARO 5,2**.

Bestimmen Sie die ALE:

SLE (488.000 USD) x ARO (5.2)
= ALE (2,5 Mio. USD)

(Die Zahlen sind gerundet.)

Bereits im Vorfeld wird deutlich, dass es kaum vertretbar ist, ein Risiko in Höhe dieser ALE zu akzeptieren – stattdessen lässt sich ein schlüssiges Geschäftsargument für eine gezielte Risikominderungsstrategie ableiten.

Qualitative Risikoanalyse

Eine qualitative Risikobewertung beschreibt das Risiko innerhalb einer Skala von Bereichen, z. B. von sehr niedrig bis sehr hoch und/oder von 1 bis 10. Eine qualitative Risikomatrix wird häufig in folgendem oder einem ähnlichen Format dargestellt:

		Wahrscheinlichkeiten				
		1 Selten	2 Unwahrscheinlich	3 Möglich	4 Wahrscheinlich	5 Fast sicher
Auswirkung	5 Sehr hoch	5	10	15	20	25
	4 Hoch	4	8	12	16	20
	3 Mittel	3	6	9	12	15
	2 Niedrig	2	2	6	8	10
	1 Sehr niedrig	1	2	3	4	5

Risiko-Legende	Niedrig	Mittel	Hoch	Schwerwiegend

Kehren wir zu dem obigen Phishing-Beispiel zurück. In Ihrer qualitativen Risikobewertung stufen Sie das Szenario als **wahrscheinlich** ein: Als kleineres Unternehmen sind Sie zwar seltener Ziel von Angriffen als größere und bekanntere Organisationen, sind sich jedoch bewusst, dass Phishing zu den häufigsten Bedrohungsvektoren zählt. Sie stufen die Auswirkungen als **mittel** ein: Zwar könnte ein Worst-Case-Szenario Ihrer Reputation erheblich schaden und sich negativ auf Ihre Unternehmensbewertung auswirken, doch ein realistischeres Szenario wäre mit deutlich geringerem Risiko verbunden. Ihr Ergebnis ist ein **hohes** Risiko.

Um Ihre Einschätzung präziser und konsistenter zu gestalten, empfiehlt es sich, den **Wahrscheinlichkeit**srahmen anhand historischer Ereignisse einzugrenzen: Welche Szenarien in den Randbereichen sind noch realistisch und plausibel? Zudem können Sie jeder Kategorie unter dem Aspekt der **Auswirkungsgröße** einen finanziellen Richtwert zuordnen.

Sowohl quantitative als auch qualitative Risikobewertungen haben ihre Stärken und Schwächen. Ein kombinierter Ansatz ermöglicht es, auch solche Risiken angemessen zu erfassen, die sich schwer quantifizieren lassen – etwa regulatorische oder reputationsbezogene Risiken –, deren potenzielle Auswirkungen jedoch gravierend sein können.

Die vorliegende Tabelle, in der indirekte Kosten nichtfinanziellen Risiken zugewiesen werden, bietet eine solide Ausgangsbasis für weiterführende Bewertungen.

Auswirkung	Monetär	Regulatorisch	Reputationsbezogen
Sehr hoch	> 10 Mio. USD	Strafrechtliche Anklagen oder Verfahren; möglicher Entzug der Betriebserlaubnis; persönliche Haftung der Geschäftsführung	Vollständiger Vertrauensverlust; anhaltend negative Berichterstattung in lokalen und internationalen Medien; nachhaltige Schädigung des Markenimages.
Hoch	1 Mio. - 10 Mio. USD	Hohe Geldbußen, Klagen und Vergleiche mit der Staatsanwaltschaft; Einschränkung der Betriebserlaubnis möglich	Das Vertrauen ist schwer beschädigt und vermutlich nicht vollständig wiederherstellbar; negative mediale Berichterstattung nimmt zu und weitet sich international aus.
Mittel	100.000 - 2 Mio. USD	Öffentliche Verwarnungen und Bußgelder; sofortige Maßnahmen zur Behebung erforderlich	Das Vertrauen ist geschwunden und kann nur mit erheblichem Aufwand wiederhergestellt werden. Die negative mediale Berichterstattung hat zugenommen.
Niedrig	10.000 - 100.000 USD	Nichtöffentliche Verwarnungen durch Aufsichtsbehörden oder Regulierungsstellen	Das Vertrauen ist zwar erschüttert, aber mit der Zeit wiederherstellbar. Die mediale Berichterstattung erfolgt auf nationaler Ebene, teils mit neutralem Ton.
Sehr niedrig	< 10.000 USD	Keine oder nur geringe Aufmerksamkeit seitens der Aufsichts- oder Regulierungsbehörden	Das Vertrauen ist vorübergehend infrage gestellt, aber kurzfristig wiederherstellbar. Die mediale Berichterstattung beschränkt sich auf einen einmaligen lokalen Vorfall.

Unabhängig davon, für welchen Ansatz Sie sich entscheiden, bleibt eine zentrale Herausforderung jeder Risikobewertung bestehen: die Unsicherheit.

Sowohl die quantitativen als auch die qualitativen Methoden der Risikobewertung weisen gewisse Grenzen auf. Beide Ansätze – auch der numerische – enthalten ein gewisses Maß an Subjektivität, das untrennbar mit Unsicherheit verknüpft ist.

Unsicherheit beschreibt, wie wenig Vertrauen Sie in eine Schätzung haben. Bei der Durchführung einer Risikobewertung ist es wichtig, den Grad der Unsicherheit zu erfassen – denn er zeigt, wie hoch Ihr Vertrauen in die ermittelten Werte ist.

Eine vollständig objektive Analyse ist kaum erreichbar. Unsicherheit kann entstehen, wenn es nicht genügend historische Ereignisse oder Forschungsergebnisse gibt, um Ihre Daten zu untermauern, wenn keine Zeit bleibt, weitere Daten zu erheben – oder wenn ein Black-Swan-Ereignis schlicht nicht vorhersehbar ist.

Die systematische Erfassung konkreter Unsicherheitsquellen kann dabei helfen, Ihr Vertrauensniveau realistisch einzuschätzen – und zugleich Bereiche aufzeigen, in denen sich die Unsicherheit möglicherweise verringern lässt.

Nehmen wir als Beispiel für Unsicherheit die Einführung einer Bring-Your-Own-Device-(BYOD)-Richtlinie.

In sicherheitssensiblen Branchen – etwa der Verteidigungsindustrie – ist die Einführung von BYOD in der Regel wenig erwünscht. Angenommen jedoch, Mitarbeitende fordern BYOD zunehmend ein und die Unternehmensführung zeigt sich offener dafür, um die Mitarbeiterzufriedenheit zu steigern. In diesem Fall müssen Sie beurteilen, ob das zusätzliche Risiko vertretbar ist – und welche Sicherheitsmaßnahmen erforderlich wären, um dieses Risiko zu minimieren.

Was könnten Sie (noch) nicht wissen?

- Wenn Sie eine Behörde oder ein Dienstleister für Regierungsstellen sind: Werden zukünftige regulatorische Änderungen Auswirkungen auf Ihre Unternehmensrichtlinie haben?
- Wie viele Mitarbeitende werden von dieser Richtlinie tatsächlich Gebrauch machen? Welche Rollen sind betroffen?
- Wie viele Stunden wird das IT-Team benötigen, um Geräte zu registrieren und Support zu leisten?

Auch wenn sich diese Fragen nicht vollständig klären lassen, gibt es Möglichkeiten, die Ungewissheit zu reduzieren – etwa durch eine Mitarbeiterbefragung, um die potenzielle Akzeptanz einer gelockerten BYOD-Richtlinie besser einschätzen zu können.

Schritt 5
Kosten-Nutzen-Analyse

Nachdem Sie Ihr Risikolevel ermittelt haben, können Sie beginnen, mögliche Optionen zur Risikominderung abzuwägen. Auch wenn der Fokus hier auf Sicherheitskontrollen liegt, gelten dieselben Grundprinzipien für alle Formen der Schadensbegrenzung – etwa für das Beheben von Softwareschwachstellen oder das Korrigieren von Fehlkonfigurationen.

Kosten kontrollieren

Um fundierte Empfehlungen für die Reaktion auf Risiken aussprechen zu können, müssen Sie eine zentrale Frage beantworten: Wie hoch sind die tatsächlichen Kosten – einschließlich versteckter Kosten – für die Minderung dieses Risikos?

Eine Sicherheitskontrolle kann technischer Natur sein (z. B. die Implementierung von Data Loss Prevention), administrativ (z. B. ein Programm zur Sensibilisierung für Informationssicherheit) oder physisch. Solche Maßnahmen zielen darauf ab, den Angreifer zu stoppen, bevor ein Asset gefährdet wird, um deren Verwundbarkeit zu verringern. Dadurch können potenzielle Auswirkungen eines Angriffs oder Sicherheitsvorfalls minimiert werden.

Es ist wichtig, sich bewusst zu machen, dass jede Form der Risikominderung mit Kosten verbunden ist – selbst dann, wenn für die jeweilige Maßnahme keine direkten Ausgaben anfallen. Wenn Sie beispielsweise einen Server vorübergehend vom Netz nehmen, um rollenbasierte Zugriffskontrollen zu aktualisieren, verursacht auch das einen wirtschaftlichen Verlust – ebenso wie die Einführung eines neuen Sicherheitstools. Der einzige Unterschied: Die eine Maßnahme erscheint sichtbar im Budget, die andere bleibt ein versteckter Kostenfaktor – sofern sie nicht aktiv berücksichtigt wird.

Als Faustregel gilt: Die Kosten für die Absicherung eines Assets sollten unter dessen Wert liegen. Andernfalls ist eine Risikominderung wirtschaftlich nicht sinnvoll.

Um die Kosten einer Sicherheitsmaßnahme zu berechnen (und auch versteckte Kosten explizit zu berücksichtigen), sollten Sie Folgendes berücksichtigen:

- Produktkosten.
- Design- und Planungskosten.
- Implementierungskosten, einschließlich Ausfallzeiten.
- Anpassungen an die Systemumgebung.
- Kompatibilität mit anderen Gegenmaßnahmen.
- Wartungsanforderungen.
- Testanforderungen.
- Kosten für Reparatur, Austausch oder Aktualisierung.
- Betriebs- und Supportkosten (einschließlich Schulung des Personals).
- Auswirkungen auf die Produktivität.
- Abonnementkosten.
- Zusätzliche Personalstunden für Überwachung und Reaktion auf Warnmeldungen.

Wert einer Sicherheitsmaßnahme

Die konzeptionelle Formel für den Wert einer Sicherheitsmaßnahme:

(ALE vor der Maßnahme) – (ALE nach der Maßnahme) – (jährliche Kosten der Maßnahme) = Wert der Maßnahme

Betrachten wir erneut das Beispiel der Datenexfiltration durch Phishing: Die Einführung eines Anti-Phishing-Tools erfolgt in Kombination mit einer **Schulung zur Informationssicherheit**, um das Risiko wirksam zu senken.

Um den Wert einer Sicherheitsmaßnahme zu ermitteln, müssen zunächst die Gesamtkosten berechnet werden. Nehmen wir an, dass sich diese – unter Berücksichtigung aller direkten und indirekten Kosten – auf 90.000 USD belaufen.

Anti-Phishing-Tool	Infosec Schulungskampagne
Bereitstellung (einmalig)	Bereitstellung (einmalig)
Integration	Integration
Lizenzgebühren/Abonnementgebühren	Lizenzgebühren/Abonnementgebühren
Benutzerschulung	Materialien für Kampagnen
Wartung und Support	Wartung und Support
Produktivitätsverlust	Produktivitätsverlust (Zeit der Mitarbeitenden für die Teilnahme an der Schulung)
Schätzung: 70.000 USD/Jahr	**Schätzung: 20.000 USD/Jahr**

Die ursprüngliche ALE war:

SLE (488.000 USD) x **ARO** (5.2) = **ALE** (2,5 Mio. USD)

(Die Zahlen sind gerundet.)

Um die neue ALE zu berechnen, muss die reduzierte ARO berücksichtigt werden, sobald die Sicherheitsmaßnahmen implementiert sind.

Ihre ursprüngliche ARO beruhte auf wöchentlichen Phishing-Versuchen mit einer angenommenen Erfolgsquote von 10 %, basierend auf den Ergebnissen Ihrer regelmäßig durchgeführten Testkampagnen. Die Häufigkeit der Angriffsversuche bleibt unverändert. Wir nehmen jedoch an, dass Sie nach Prüfung von zwei Anbietern zu dem Schluss kommen, dass die kombinierte Lösung die Erfolgsquote auf 2 % senkt. Damit reduziert sich Ihre ARO auf ein Fünftel des ursprünglichen Werts – also auf 1,04.

Jetzt haben Sie Ihre neue ALE:

SLE (488.000 USD) x new **ARO** (1.04) = **ALE** (507.500 USD)

(Die Zahlen sind gerundet.)

Sie können dann den Kontrollwert berechnen:

Ursprüngliche ALE (20,5 Mio. USD) – neue **ALE** (507.500 USD) – jährliche Kosten der Maßnahme (90.000 USD)
= Wert der Maßnahme (1,9 Mio. USD)

(Die Zahlen sind gerundet.)

Gesamtrisiko vs. Restrisiko

Wir führen Sicherheitskontrollen ein, um das Gesamtrisiko des Unternehmens auf ein akzeptables Level zu senken. Da jedoch kein System und keine Umgebung zu 100 % sicher sind, bleibt immer ein gewisses Restrisiko, mit dem man sich auseinandersetzen muss.

Die ALE nach Umsetzung der Sicherheitsmaßnahmen wird auch als Rest-ALE bezeichnet und steht für das verbleibende Restrisiko.

Quantitative residual ALE = residual ARO x residual SLE

In unserem Beispiel ist die SLE nach der Implementierung der Sicherheitsmaßnahmen gleich geblieben, aber die ARO wurde von 5,2 auf 1,04 reduziert, was zu einer Rest-ALE führt, die viel niedriger ist als die ursprüngliche (inhärente) ALE. Dies ist ein überzeugendes Argument für einen konstruktiven Umgang mit Risiken – konkret für deren Minderung.

Tipp

Möglicherweise stoßen Sie auch auf folgende Formeln – oder nutzen sie selbst:

Bedrohungen x
Schwachstelle x
Wert des Assets = **Gesamtrisiko**

Bedrohungen x
Schwachstelle x
Wert des Assets x
Lücke in der Maßnahme =
Restrisiko

Gesamtrisiko –
Maßnahmen = **Restrisiko**

Vorteile von Sicherheitsmaßnahmen

Oft geht der Nutzen einer Sicherheitsmaßnahme über die bloße Minderung einer Bedrohung hinaus – also über den zuvor erläuterten Wert. Sicherheitsmaßnahmen können auch zu Einsparungen bei den **Betriebskosten** führen, und die Berücksichtigung dieser Einsparpotenziale kann Ihre Analyse maßgeblich beeinflussen.

Beispiel: **Automatisiertes Patchen**

Angenommen, Sie erwägen die Einführung eines automatisierten Patch-Prozesses: Sicherheitsupdates könnten deutlich schneller eingespielt werden – und sowohl menschliche Fehler als auch unbeabsichtigte Schwachstellen würden seltener auftreten.

Aber das ist noch nicht alles. Nehmen wir an, Ihr Unternehmen verwaltet 75 Anwendungen, die jeweils zwei Patches im Zwei-Wochen-Rhythmus benötigen. Für jeden Patch fallen im Durchschnitt vier Stunden für Vorbereitung und Bereitstellung an – was insgesamt 600 Arbeitsstunden pro Jahr bedeutet. Ausgehend von einem voll kalkulierten Stundensatz von 100 US-Dollar für technisches Personal lassen sich die folgenden operativen Kosteneinsparungen berechnen:

Anzahl der Anwendungen	75
Anzahl der zweiwöchentlichen Aktualisierungen pro Anwendung	2
Anzahl der Stunden für die Vorbereitung einer Anwendung und ihre Bereitstellung	4
Anzahl der für die manuelle Vorbereitung aufgewendeten Stunden	600
Voll kalkulierter Stundensatz für technisches Personal	100 USD
Jährliche Kosten für die manuelle Vorbereitung	**60.000 USD**

Besonders durch Automatisierung lassen sich erhebliche Zeitressourcen einsparen – Ihr Team kann sich dadurch auf strategisch wichtigere Aufgaben konzentrieren, und das Unternehmen profitiert von spürbaren Kosteneinsparungen.

Hier sind einige weitere Beispiele für quantifizierbare Vorteile:

Vorteil	Quantifizierung
Bedrohungserkennung: Früherkennung von Anomalien	Verkürzung der Erkennungszeiten für potenzielle Bedrohungen
Reaktion auf Vorfälle: Schnelle Reaktion auf Warnmeldungen und Vorfälle	Verkürzung der Reaktionszeiten auf Vorfälle
Überwachung in Echtzeit SIEM wartet nicht auf einen Administrator, um nach neuen Aktivitäten zu suchen	Steigerung der Zeiteffizienz der Mitarbeitenden
Zentrale Ansicht: Sämtliche erfassten Geräte senden ihre Daten an ein zentrales Dashboard.	Zeitersparnis beim Wechsel zwischen den Anwendungen; Zeitersparnis beim Korrelieren von Ereignissen
Genauigkeit: Weniger False-Positives	Zeitersparnis bei der Beurteilung, ob ein Ereignis wirklich positiv ist oder nicht
Compliance: Erweitertes Reporting	Zeitersparnis bei der Erstellung von On-Demand-Reports während einer Prüfung
Forensik: Schnellere Analyse von Vorfällen; E-Discovery-Anfragen können leichter beantwortet werden	Zeitersparnis bei der Rekonstruktion von Aktivitätsprotokollen und beim Aufspüren der Bedrohungsquellen.
Verhaltensanalyse: Erkennt typische Aktivitätsmuster im System und lernt kontinuierlich dazu.	Zeitersparnis bei der Feststellung, ob eine normale Benutzeraktivität durchgeführt wird

Reaktionen auf Risiken

Nachdem Sie die relevanten Informationen zusammengetragen und die Risikobewertung abgeschlossen haben, können Sie eine fundierte, datengestützte Empfehlung für den weiteren Umgang mit dem Risiko abgeben.

Antwortmöglichkeiten

Wie bereits erwähnt, gibt es vier Arten von Reaktionen auf Risiken:

Vermeidung
des Risikos durch Schließung bzw. Stilllegung des risikobehafteten Geschäftsbereichs/ Verfahrens/Systems/ Standorts.

Übertragung
des Risikos auf eine Versicherung – Diese Option stellt lediglich einen finanziellen Risikotransfer dar. Das Unternehmen bleibt für den Eintritt des Risikos weiterhin verantwortlich und muss sich zusätzlich mit nicht versicherbaren Schäden wie Reputationsverlusten auseinandersetzen.

Akzeptanz
des Risikos. Beachten Sie, dass diese Entscheidung regelmäßig überprüft und bei Bedarf angepasst werden sollte.

Minderung
des Risikos. Dabei wird anerkannt, dass die potenziellen Kosten eines eingetretenen Risikos höher sind als die Kosten der entsprechenden Sicherheitsmaßnahmen.

Kehren wir noch einmal zu unserem Beispiel der Bekämpfung von Datenexfiltration durch einen Phishing-Angriff zurück – jenem Szenario, in dem wir das Gesamtrisiko, die Implementierungskosten der Sicherheitsmaßnahmen sowie das verbleibende Restrisiko nach Einführung der Sicherheitsmaßnahme berechnet haben.

Das Risiko zu **vermeiden** würde bedeuten, jeden externen E-Mail-Austausch zu unterbinden, was eindeutig nicht machbar ist.

Das Risiko zu **akzeptieren** ist sinnvoll, wenn der Wert des Assets nicht hoch genug ist, um die Kosten für dessen Schutz zu rechtfertigen. In unserem Beispiel haben wir die Kosten für das eingetretene Risiko berechnet, d.h. die ALE, mit 2,5 Mio. $, die durch Ausgaben von 90.000 USD/Jahr um etwa 80 % reduziert werden könnten für Sicherheitsmaßnahmen – ein starkes Argument gegen die Akzeptanz des Risikos.

Das Risiko auf eine Versicherungsgesellschaft zu **übertragen**, mag zunächst mit geringen Einstiegskosten verbunden sein – in diesem Fall ist sie jedoch keine besonders geeignete Option. Eine Cyber-Versicherung würde die finanziellen Schäden voraussichtlich abdecken – nicht jedoch die übrigen Auswirkungen. In unserem Beispiel beziehen sich die größten Bedenken auf die bevorstehende Finanzierungsrunde – ein Reputationsrisiko, das sich nicht durch die Übertragung auf Dritte absichern lässt.

Schließlich können wir das Risiko durch die Umsetzung von Sicherheitsmaßnahmen **mindern** – in diesem Fall durch eine Kombination aus einem Anti-Phishing-Tool und einer Informationssicherheitskampagne –, ein Vorgehen, das durch unsere Risikobewertung eindeutig gestützt wird.

Berücksichtigung der Risikobereitschaft

Nicht jede Risikobewertung führt zu einer eindeutigen Handlungsempfehlung – selbst dann nicht, wenn die Kosten für eine Sicherheitsmaßnahme klar unter den potenziellen Schadenskosten liegen. Der Grund: Ressourcen sind stets begrenzt, und jede Risikominderungsstrategie ist mit einem Opportunitätskostenfaktor verbunden. Die Entscheidung lautet daher nicht immer: „Handeln oder akzeptieren?“, sondern häufig: „Welche Investition ist in diesem Moment die sinnvollere?“

Ein klares Verständnis der **Risikobereitschaft** Ihres Unternehmens hilft insbesondere bei Grenzfällen – also dort, wo die Risikobewertung zwar eine Sicherheitsmaßnahme nahelegt, die Opportunitätskosten jedoch hoch sind.

Die Risikobereitschaft beschreibt das Maß an Risiko, das ein Unternehmen im Rahmen seiner Zielverfolgung bereit ist, einzugehen. **Eine hohe Risikobereitschaft** bedeutet, dass ein Unternehmen bereit ist, größere Risiken einzugehen, um potenziell höhere Erträge zu erzielen. Eine **geringe Risikobereitschaft** hingegen deutet darauf hin, dass Risiken möglichst vermieden oder minimiert werden sollen..

Die Risikobereitschaft variiert stark – je nach Branche, Unternehmensgröße, Geschäftsmodell oder Wachstumszielen. Dabei ist sie selten eindimensional: So kann ein Unternehmen im operativen Bereich risikobereit sein, während es in Bezug auf regulatorische oder Compliance-Risiken eine eher konservative Haltung einnimmt.

Eine Erklärung zur Risikobereitschaft ist in der Regel wie folgt aufgebaut:

Allgemeine Risikobereitschaft **[Unternehmen XYZ] verfolgt einen ausgewogenen Ansatz in Bezug auf Risiken und erkennt an, dass nicht alle Risiken gleich sind und ein gewisses Maß an Risiko notwendig ist, um die strategischen Ziele zu erreichen.**	
Innovationsrisiko	Wir haben eine hohe Risikobereitschaft, wenn es um Investitionen in fortschrittliche Technologien und innovative Lösungen geht, die unsere Produkte im Wettbewerbsumfeld differenzieren. Wir sind uns darüber im Klaren, dass dies ein gewisses Maß an Unsicherheit in Forschung & Entwicklung sowie der Produktentwicklung mit sich bringt.
Operatives Risiko	Wir haben eine niedrige bis mäßige Risikobereitschaft. Während wir nach operativer Exzellenz streben, setzen wir Prioritäten auf Initiativen, die Effizienz und Servicequalität steigern, ohne unsere Lieferstandards zu beeinträchtigen.
Sicherheitsrisiko	Unsere Risikobereitschaft im Hinblick auf Sicherheitsbedrohungen und -verletzungen ist äußerst gering. Der Schutz der Netzwerksicherheit und der Datenschutz genießen bei uns höchste Priorität. Wir investieren gezielt und umfassend in den Schutz unserer Systeme sowie der Daten unserer Kundinnen und Kunden.
Compliance-Risiko	Wir haben eine geringe Risikobereitschaft in Bezug auf die Nichteinhaltung gesetzlicher und regulatorischer Anforderungen. Die Einhaltung relevanter Gesetze, Standards und Best Practices in allen operativen Bereichen hat für uns höchste Priorität.

Innerhalb jeder dieser Dimensionen sind mehrere Schlüsselfaktoren zu berücksichtigen:

- **Risikokapazität** ist die maximale Höhe des Risikos, das ein Unternehmen tragen kann; sie wird in der Regel durch die finanziellen Ressourcen, die operativen Fähigkeiten und die gesetzlichen Beschränkungen bestimmt.
- **Risikotoleranz** ist eine akzeptable Abweichung vom gesetzten Ziel.
- **Risikoschwellen** sind „rote Linien", die die Notwendigkeit eines Strategiewechsels anzeigen.

Die Schwelle zwischen Risikotoleranz und Risikokapazität – oder auch zwischen unterschiedlichen Toleranzgraden – kann dabei helfen, sogenannte „Grenzfälle" einzuordnen, bei denen unklar ist, ob Risikoakzeptanz oder Risikominderung die angemessene Reaktion darstellt.

Um auf unser Phishing-Beispiel zurückzukommen: Es ist denkbar, dass ein wachstumsorientiertes Start-up eine so hohe Risikobereitschaft aufweist und nur über ein derart knapp bemessenes Cybersicherheitsbudget verfügt, dass ein erfolgreicher Phishing-Angriff als tolerierbares Risiko eingestuft wird – obwohl geeignete Schutzmaßnahmen vergleichsweise kostengünstig wären.

Tipps

Falls Ihr Unternehmen über eine zentrale Funktion für das unternehmensweite Risikomanagement verfügt, sollten Sie sich dort Orientierung einholen. In der Regel ist die Risikobereitschaft dort dokumentiert und Bestandteil des übergeordneten Risikomanagement-Frameworks.

Falls Ihr Unternehmen noch über keine formelle Erklärung zur Risikobereitschaft verfügt, können Sie diese bearbeitbare Vorlage als Grundlage verwenden.

Beispiele

Bisher haben wir den Assets Werte zugewiesen, Bedrohungen und Schwachstellen bewertet, Eintrittswahrscheinlichkeit und Auswirkungen qualitativ erfasst, das Risiko mittels ALE berechnet und sowohl die Kosten von Sicherheitsmaßnahmen als auch die Folgen ihrer Nichtumsetzung abgeschätzt.

Da uns die Daten nun vorliegen, können wir mit einigen End-to-End-Beispielen arbeiten.

Tipp

Laden Sie eine editierbare Vorlage herunter, mit der Sie Ihre eigene Bewertung in diesem Format darstellen können.

Beispiel 1: Vermeidung von Datenlecks bei BYOD

Problemstellung:

Die Mitarbeitenden nutzen zunehmend die Vorteile unserer BYOD-Richtlinie (Bring Your Own Device). Für BYOD-Geräte wenden wir derzeit nicht dieselben Sicherheitsmaßnahmen an wie für firmeneigene Geräte, was das Risiko eines Datenabflusses erhöht.

Mitarbeitende könnten die unzureichenden Sicherheitsmaßnahmen ausnutzen, um Unternehmensdaten außerhalb unserer geschützten Umgebung zu verarbeiten – etwa durch das Weiterleiten an private E-Mail-Adressen oder Cloud-Speicher, über Datentransferdienste oder durch die Nutzung externer KI-Tools.

Empfehlung::

Die Ausweitung der Endgeräte-DLP, die derzeit auf firmeneigene Geräte beschränkt ist, auf BYOD-Geräte würde das Risiko von Datenverlusten – ob versehentlich oder vorsätzlich – deutlich verringern und die Einhaltung regulatorischer Vorgaben verbessern.

Risikobewertung

AV: Durch unsere BIA berechnen wir den Wert der sensiblen Daten des Unternehmens auf 1 Mio. USD.
EF: Falle eines Datenlecks ist davon auszugehen, dass bis zu 60 % des Werts unserer sensiblen Daten verloren gehen könnten.
ARO: Die Datenanalyse unseres Risikoregisters und der Helpdesk-Tickets zeigt, dass ein schwerwiegender Vorfall im Schnitt zweimal pro Jahr zu erwarten ist.

AV x EF = SLE ⇒ 1 Mio. USD x 0,6 = 600.000 USD SLE x ARO
= ALE ⇒ 600.000 × 2 =1,2 Mio. USD

Unsicherheiten: Das Vertrauensniveau in die zugrunde liegenden Daten liegt bei 85 %.
Dieses Niveau kann durch verschiedene Faktoren beeinflusst werden, darunter beispielsweise:

- Art und Umfang der geleakten sensiblen Daten.
- Potenziell unzufriedene Mitarbeitende.
- Neue Mitarbeitende, die an der Schulung zur Sensibilisierung im Umgang mit Daten – eine derzeit eingesetzte kompensierende Maßnahme – möglicherweise nicht teilnehmen.

<table>
<tr><th colspan="4">Reaktion auf Risiken</th></tr>
<tr><th>Option</th><th colspan="2">Durchführbarkeit</th><th>Restrisiko</th></tr>
<tr><td>Vermeidung</td><td colspan="2">Möglich: Vermeidung würde das Risiko auf null senken – allerdings nur durch die Abschaffung von BYOD, was zu Unzufriedenheit bei den Mitarbeitenden führen könnte.</td><td>0</td></tr>
<tr><td>Akzeptanz</td><td colspan="2">Möglich: Akzeptanz ist grundsätzlich möglich, könnte jedoch außerhalb unserer definierten Risikobereitschaft liegen. Risikoakzeptanz bedeutet, dass direkte finanzielle Kosten und indirekte Auswirkungen wie Reputationsschäden, Gerichtsverfahren, Geldbußen, behördliche Überprüfung, negative Darstellung in den Social Media usw. in Kauf genommen werden.</td><td>ALE = 1,2 Mio. USD</td></tr>
<tr><td>Übertragung</td><td colspan="2">Möglich: Eine Risikoübertragung auf eine Versicherung würde die Kosten bis zu einem bestimmten Betrag abdecken. Die Deckungssummen für die Cyber-Haftpflicht liegen in der Regel zwischen 500.000 und 5 Millionen USD pro Vorfall. Allerdings:
Kosten durch Reputationsschäden, behördliche Geldbußen und Klagen von Kunden sind zusätzliche Risiken, die nicht durch die Versicherung abgedeckt sind.
Die Versicherung stellt die Deckung für erneute Vorfälle unter Umständen ein, wenn keine eindämmenden Maßnahmen ergriffen werden.</td><td>Ungewiss. Abhängig von der Versicherungsprämie und der Anzahl der Vorfälle. Es wird nur das finanzielle Risiko reduziert.</td></tr>
<tr><td rowspan="7">Mindern (empfohlen)</td><td colspan="2">Möglich – siehe unten</td><td rowspan="7">Eine Reduktion der ARO um 80 % ergibt einen neuen ARO-Wert von 0,4. Die restliche SLE bleibt gleich.

Neu (Rest-)
ALE = 600.000 USD
x 0,4 = 240.000 USD</td></tr>
<tr><td>Kosten</td><td>Vorteile</td></tr>
<tr><td>Zusätzliche Lizenzen
30.000 USD</td><td rowspan="5">Geschätzte Reduktion der Wahrscheinlichkeit von Insider-Bedrohungen um 80 %.</td></tr>
<tr><td>Für die Bereitstellung erforderliche Personalstunden
10.000 USD</td></tr>
<tr><td>Benutzerschulung
10.000 USD</td></tr>
<tr><td>Erstes Jahr insgesamt
50.000 USD</td></tr>
<tr><td>Folgejahre insgesamt
50.000 USD</td></tr>
</table>

Beispiel 2: Überarbeitung der rollenbasierten Zugriffskontrolle

Problemstellung:

Die rollenbasierten Zugriffskontrollen in unserem CRM-System wurden seit fünf Jahren nicht mehr überarbeitet – obwohl sich unsere Organisationsstruktur in dieser Zeit erheblich verändert hat. Die definierten Rollen und die zugewiesenen Berechtigungen entsprechen nicht mehr den tatsächlichen Aufgaben der Nutzerinnen und Nutzer. In vielen Fällen bestehen dadurch überflüssige Zugriffsrechte, die ein potenzieller Angreifer ausnutzen könnte, sollte er Zugangsdaten kompromittieren.

Empfehlung

Auch wenn die Neuzuordnung der rollenbasierten Zugriffsrechte einen erheblichen abteilungsübergreifenden Aufwand erfordert, ist dafür keine Systemabschaltung notwendig. Eventuelle kurzfristige Produktivitätseinbußen während der Umstellung lassen sich rasch auffangen. Diese Kosten stehen in keinem Verhältnis zur annualisierten Verlusterwartung. Wir empfehlen daher, dieses Vorhaben zügig umzusetzen und bitten um die Unterstützung unserer Kolleginnen und Kollegen aus Vertrieb, Marketing und operativem Bereich.

Risikobewertung

AV: Mittels unserer BIA berechnen wir den Wert der Daten in unserem CRM auf 1,5 Mio. USD.
EF: In Anbetracht der von uns implementierten Kontrollmechanismen – wie Protokollierung, Überwachung und Multi-Faktor-Authentifizierung – wäre ein erfolgreicher Angriff voraussichtlich in der Lage, auf etwa 10 % der sensiblen Daten zuzugreifen und diese zu exfiltrieren.
ARO: Die Ergebnisse der Pen-Tests der letzten fünf Jahre (zwei Tests pro Jahr mit unterschiedlichem Umfang) lassen den Schluss zu, dass pro Jahr mit einem Vorfall zu rechnen ist, bei dem ein privilegierter Zugang genutzt wird.

AV x EF = SLE ⇒ 1Mio. USD x 0,1 = 600.000 USD
SLE x ARO = ALE ⇒ 600.000 USD x 1 = 1,2 Mio. USD

Unsicherheiten: Das Vertrauensniveau in die zugrunde liegenden Daten liegt bei 80 %. Dieses Niveau kann durch verschiedene Faktoren beeinflusst werden, darunter:

- Art und Umfang der kompromittierten Kundendaten.
- Potenziell unzufriedene Administratoren.
- Durch einen anderen Sicherheitsvorfall kompromittierte Zugangsdaten.
- Bedrohungsakteure, die ihre Angriffstechniken weiterentwickeln, um privilegierte Zugriffe zu umgehen.

<table>
<tr><th colspan="5">Risikobewältigung</th></tr>
<tr><th>Option</th><th colspan="3">Durchführbarkeit</th><th>Restrisiko</th></tr>
<tr><td>Vermeidung</td><td colspan="3">Keine: Eine vollständige Umgehung würde das Risiko zwar auf null senken, gleichzeitig aber auch verhindern, dass privilegierte Aktionen im CRM-System ausgeführt werden können.</td><td>0</td></tr>
<tr><td>Akzeptanz</td><td colspan="3">Möglich: Eine Risikoakzeptanz ist grundsätzlich möglich und könnte innerhalb unserer Risikobereitschaft liegen. Dennoch müssen auch indirekte Kosten berücksichtigt werden – etwa Reputationsverluste oder regulatorische Prüfungen.</td><td>ALE = 150.000 USD</td></tr>
<tr><td>Übertragung</td><td colspan="3">Möglich: Die Übertragung auf die Versicherung würde die direkten Kosten eines Ereignisses decken (SLE = 150.000 USD). Die Deckungssummen für die Cyber-Haftpflicht liegen in der Regel zwischen 500.000 und 5 Millionen USD pro Vorfall. Die Versicherung stellt die Deckung für erneute Vorfälle unter Umständen ein, wenn keine abmildernden Maßnahmen ergriffen werden.</td><td>Ungewiss. Abhängig von der Versicherungsprämie und der Anzahl der Vorfälle.</td></tr>
<tr><td rowspan="5">Mindern (empfohlen)</td><td colspan="3">Möglich – siehe unten</td><td rowspan="5">Die restliche ARO bleibt gleich.

Eine Verringerung der ARO um 50 % ergibt einen neuen ARO-Wert von 0,4.

Neue (Rest-)
ALE = 75.000 USD
x 1 = 75.000 USD</td></tr>
<tr><td colspan="2">Kosten</td><td>Vorteile</td></tr>
<tr><td>Personalzeit in den Bereichen IT, Betrieb, Marketing und Vertrieb, um die neuen Rollen abzubilden</td><td>10.000 USD</td><td rowspan="3">Schätzung. 50%ige Verringerung der Gefährdung im Falle eines erfolgreichen Angriffs.</td></tr>
<tr><td>Produktivitätsverluste bei der Anpassung von CRM-Usern an neue Rollen</td><td>5.000 USD</td></tr>
<tr><td>Gesamt</td><td>15.000 USD</td></tr>
</table>

Schlussfolgerung

Sie verfügen nun über die nötigen Tools, um eine datengestützte Risikobewertung durchzuführen und Ihre Ergebnisse darzustellen. Sie sind Ihrem Ziel einen wichtigen Schritt näher gekommen, die unternehmensweiten Ziele mit den Sicherheitszielen in Einklang zu bringen und ein gemeinsames Verständnis von Risiken zu schaffen.

Wenn Sie auf Augenhöhe mit CEO und Vorstand kommunizieren, erreichen Sie mehr als nur das operative Ziel – Sie fördern ein gemeinsames Verständnis und erhalten aktive Unterstützung.

In diesem E-Book haben wir zusätzliche Tools und Vorlagen verlinkt, die Ihnen bei Ihrer Risikobewertung helfen können. **Hier geht's zum Download.**

Vorlage für eine Business Impact Analyse

Vorlage für eine Erklärung zur Risikobereitschaft

Checkliste für Angriffsflächen

Vorlage zur Zusammenfassung der Risikobewertung

Viel Erfolg!

Über Ivanti

Ivanti ist ein Anbieter von Unternehmenssoftware und bietet eine umfassende cloudbasierte Plattform für IT- und Sicherheitslösungen. Mit skalierbaren Softwarelösungen unterstützt Ivanti seine Kunden dabei, die Effizienz in IT und Sicherheit zu steigern, Kosten zu senken und Sicherheitsrisiken proaktiv zu minimieren. Die cloudnative Plattform Ivanti Neurons bildet das Fundament für einheitliche, wiederverwendbare Dienste und Tools. Sie ermöglicht eine konsistente Transparenz, hohe Skalierbarkeit und eine sichere Bereitstellung von Lösungen. Mehr als 34.000 Kunden, darunter 85 der Fortune-100-Unternehmen, haben sich für Ivanti entschieden, um die Herausforderungen mit den eigenen End-to-End-Lösungen zu meistern. Unser Ziel bei Ivanti ist, ein Umfeld zu schaffen, in dem alle Meinungen gehört, respektiert und geschätzt werden. Und wir setzen uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und unseren Planeten ein. Weitere Informationen finden Sie unter ivanti.com und folgen Sie @GoIvanti.

ivanti

Für weitere Informationen oder um Ivanti zu kontaktieren, besuchen Sie bitte ivanti.com.