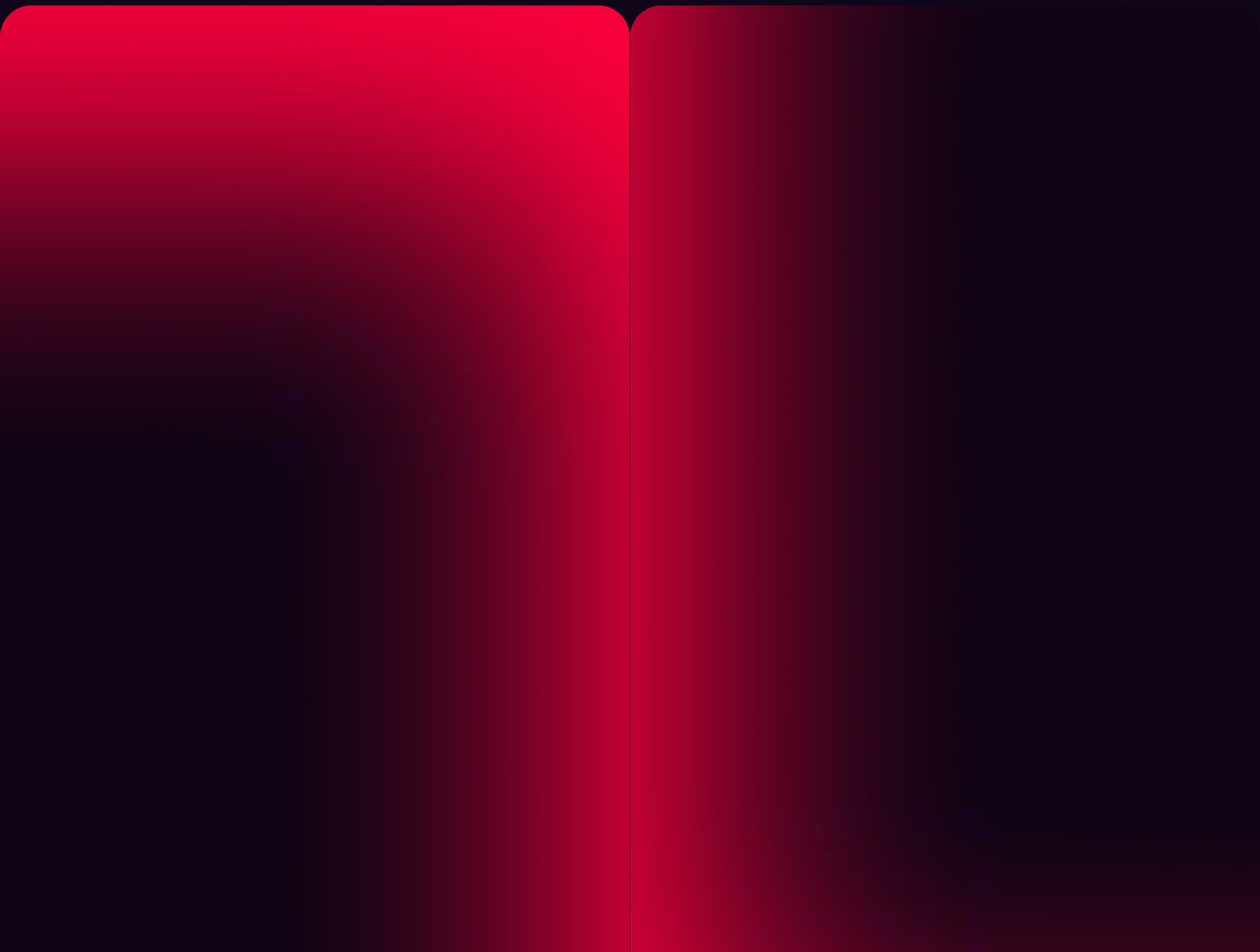
HADRIAN

GUIDE

Über den ROI hinaus: Ein Leitfaden zum Wert der Verlustvermeidung



Eine bessere Kennzahl für offensive Cybersicherheit

Sie beobachten ständig den Return on Investment (ROI) Ihrer Tools. Wenn es jedoch um offensive Cybersicherheit geht, lässt sich deren Wert am besten anhand der Kosten einer Datenverletzung belegen. Der ROI ist zwar in bestimmten Kontexten nach wie vor wertvoll, gibt jedoch nicht das gesamte Bild wieder. In diesem Dokument erfahren Sie, wie Sie mit einer neuen Gleichung den Wert Ihrer Tools für offensive Cybersicherheit ermitteln können.

Kosten von Datenverletzungen

DIE DURCHSCHNITTLICHEN GESAMTKOSTEN EINER VERLETZUNG.

4,88 MILLIONEN USD

DURCHSCHNITTLICHES JÄHRLICHES WACHSTUM DER KOSTEN FÜR DATENVERSTÖSE.

10 % UND STEIGEND

KOSTENEINSPARUNGEN DURCH DEN UMFASSENDEN EINSATZ VON KI ZUR PRÄVENTION.

2,2 MILLIONEN USD

Quelle: IBM Cost of a Data Breach Report, 2024

Wert der Verlustvermeidung

Während die mit einer Datenverletzung verbundenen erheblichen Kosten greifbar sind, kann der Wert proaktiver Prävention abstrakt erscheinen, was die Darstellung eines klaren finanziellen Arguments für Sicherheitsinvestitionen erschwert. Traditionelle Kennzahlen zur Kapitalrendite (ROI) sind zwar in vielen Geschäftsbereichen effektiv, reichen jedoch im Bereich der Cybersicherheit nicht aus, da es schwierig ist, die Auswirkungen verhinderter Vorfälle genau zu quantifizieren. Hier bietet der **Wert der Verlustvermeidung (Value of Loss Avoidance, VLA) eine überlegene Lösung, indem er die Investitionen in die Minderung von Risiken direkt gegen die potenziellen finanziellen Verluste durch Cybervorfälle** quantifiziert und somit eine klare Methode liefert, um zu zeigen, wie Sicherheitsausgaben Unternehmen aktiv vor erheblichen Verstößen schützen.

Der VLA ist eine einfache Iteration des ROI, bei der Sie den Nettogewinn durch vermiedene Verluste ersetzen.

Einfach, oder? Nicht so schnell.

Um eine genauere Berechnung auf der Grundlage von Daten und nicht von Durchschnittswerten oder Spekulationen zu erhalten, gibt es eine praktische Tabelle, mit der Sie den genauen Umfang der Kosten ermitteln können.

Skala für die Wahrscheinlichkeit der Ausnutzung (LES)

Die Skala für die Wahrscheinlichkeit der Ausnutzung (LES) hilft bei der Bewertung der Wahrscheinlichkeit, dass eine bestimmte Schwachstelle erfolgreich ausgenutzt wird. Diese Skala reicht von 0 bis 10 und bietet einen klaren Rahmen für das Verständnis der Dringlichkeit und der potenziellen Auswirkungen verschiedener Schwachstellen.

Sehr hohe Wahrscheinlichkeit (10 – 8)

Diese Schwachstellen werden mit ziemlicher Sicherheit von Angreifern ins Visier genommen und oft aktiv ausgenutzt. Zu dieser Kategorie gehören Zero-Day-Schwachstellen, öffentlich bekannt gewordene Fehler mit funktionierenden Exploits und Schwachstellen bei der nicht authentifizierten Remote-Codeausführung, die häufig bei Angriffen genutzt werden.

Hohe Wahrscheinlichkeit (8 – 3)

Schwachstellen in dieser Kategorie sind sehr anfällig für Ausnutzung. Angreifer zielen häufig auf remote zugängliche Fehler, Schwachstellen in weit verbreiteten Technologien und Probleme ab, deren Ausnutzung nur minimalen Aufwand erfordert.

Mäßige Wahrscheinlichkeit (3 – 1)

Schwachstellen in diesem Bereich haben eine angemessene Chance, ausgenutzt zu werden, sind jedoch in der Regel von zusätzlichen Bedingungen abhängig. Angreifer können Fehler ausnutzen, die eine Benutzerinteraktion, eine bestimmte Netzwerkpositionierung oder ungewöhnliche Konfigurationen erfordern, um erfolgreich zu sein.

Geringe Wahrscheinlichkeit (1 – 0,2)

Diese Schwachstellen können ohne erheblichen Aufwand wahrscheinlich nicht ausgenutzt werden. Die Ausnutzung erfordert in der Regel komplexe Angriffsketten, Spezialwissen oder privilegierten Zugriff, was ihre Attraktivität für Angreifer einschränkt.

Sehr geringe Wahrscheinlichkeit (0,2 – 0)

Schwachstellen in dieser Kategorie werden aufgrund starker Schutzmaßnahmen, minimaler Sichtbarkeit oder spezieller Angriffsanforderungen nur selten ausgenutzt. Angreifer ignorieren in der Regel Schwachstellen in isolierten Systemen, Legacy-Umgebungen mit strengen Zugriffskontrollen oder solchen, die sehr spezifische Bedingungen für einen Angriff erfordern.

Berechnung des geminderten Verlusts auf der Grundlage identifizierter Risiken

Bei der Schätzung geminderter Verluste ist es entscheidend, die Wahrscheinlichkeit einer Ausnutzung innerhalb des Investitionszeitraums zu berücksichtigen. Um den geminderten Verlust für jede Risikoschweregrad genau zu berechnen, beginnen wir damit, die Anzahl der identifizierten Risiken zusammen mit einer Annahme zur Auswirkung einer Sicherheitsverletzung abzubilden. Dies ist der geschätzte finanzielle Aufwand einer Sicherheitsverletzung bei diesem Schweregrad. Anschließend wird der LES verwendet, um die Wahrscheinlichkeit einer erfolgreichen Ausnutzung für jede Expositionsschwere zu quantifizieren. Der LES stellt die Wahrscheinlichkeit dar, dass eine Exposition innerhalb eines definierten Zeitraums ausgenutzt wird. Diese Berechnung ergibt den geminderten Verlust pro Risiko. Der Verlust pro Risiko kann anhand der durchschnittlichen Kosten für Folgendes berechnet werden:

- Kosten für die Datenwiederherstellung
- Rechtskosten
- Compliance- und Bußgelder
- Kosten für Betriebsunterbrechungen
- Forensische Untersuchungen
- Erhöhte Versicherungsprämien

Dadurch werden abstrakte Wahrscheinlichkeiten in quantifizierbare Finanzzahlen umgewandelt. Betrachtet man beispielsweise eine Stichprobe identifizierter Risiken, würde die Berechnung wie folgt aussehen:

EXPOSITIONSBEWERTUNG	LES	LOSS PER EXPOSURE
Kritisch	3	146.400 $
Hoch	1	34.160 $
Mittel	0,5	4.880 $
Niedrig	0,1	195 $

Unterschiede je nach Branche

Leider sind nicht alle Cyberangriffe gleich, und es gibt bestimmte Branchen, die aufgrund hoher Margen, wertvoller Daten oder vertraulicher geistiger Eigentumsrechte stärker im Fokus von Cyberkriminellen stehen als andere.

Unabhängig von den Gründen sollten bestimmte Branchen darauf vorbereitet sein, einen Multiplikator auf ihre Gesamtzahl an Risiken anzuwenden, um dem erhöhten Druck, dem diese Branchen ausgesetzt sind, Rechnung zu tragen. Sie können diese Tabelle als Referenz verwenden:

BRANCHE	Multiplikator
FERTIGUNG	x7 Gesamtzahl der Risiken
FINANZWESEN	x7 Gesamtzahl der Risiken
GESUNDHEITSWESEN	x5 Gesamtzahl der Risiken
REGIERUNG	x4 Gesamtzahl der Risiken
ENERGIE	x3 Gesamtzahl der Risiken
EINZELHANDEL	x2 Gesamtzahl der Risiken
SONSTIGE	Kein Multiplikator

Berechnung des VLA

Da Risiken selten isoliert auftreten, sondern oft in Verbindung mit anderen Risiken, können sich Ihre Kosten sehr schnell summieren. In einem konservativen Fall, wenn Sie 3 kritische Risiken, 5 hohe Risiken, 8 mittlere Risiken und 12 geringe Risiken mit den oben aufgeführten LES-Werten haben, kommen Sie schnell auf Datenverletzungskosten in Höhe von **636.380 $.**

$566,380

=

636.380 - 70.000

Kehren wir zu unserer Gleichung für den Wert der Verlustvermeidung zurück:
VLA = Gesamtverlust, der vermieden wurde – Kosten für die Investition in Tools

Und wenn wir unsere Annahmen mit durchschnittlichen Kosten für ein proaktives Sicherheitstool in Höhe von 70.000 $ einfügen, ergibt sich Folgendes.

Der VLA beläuft sich in dieser Schätzung auf über eine halbe Million Dollar. Der durch die Verletzung verursachte Verlust übersteigt bei weitem die Kosten für das Tool, das die Verletzung von vornherein hätte verhindern können.

Sorgen Sie für messbare finanzielle Einsparungen für Ihren Vorstand

Der Wert der Verlustvermeidung ermöglicht es Sicherheitsteams, Budgetanträge effektiv zu begründen, indem sie die potenziellen finanziellen Auswirkungen geminderter Risiken quantifizieren. Dieser Ansatz zeigt, wie strategische Investitionen in Sicherheitstools kostspielige Vorfälle proaktiv verhindern, indem abstrakte Sicherheitsrisiken in klare finanzielle Kennzahlen übersetzt werden, die bei Führungskräften und Vorstandsmitgliedern direkt Anklang finden.

Im Gegensatz zu herkömmlichen Kennzahlen wie der Anzahl der verhinderten Vorfälle oder dem Prozentsatz der geminderten Risiken, die oft nicht in der Lage sind, ihre finanzielle Bedeutung für Führungskräfte zu vermitteln, verlagert VLA den Fokus auf messbare finanzielle Ergebnisse. Dies veranschaulicht genau, wie Investitionen in Cybersicherheit direkt zum Geschäftsergebnis eines Unternehmens beitragen.