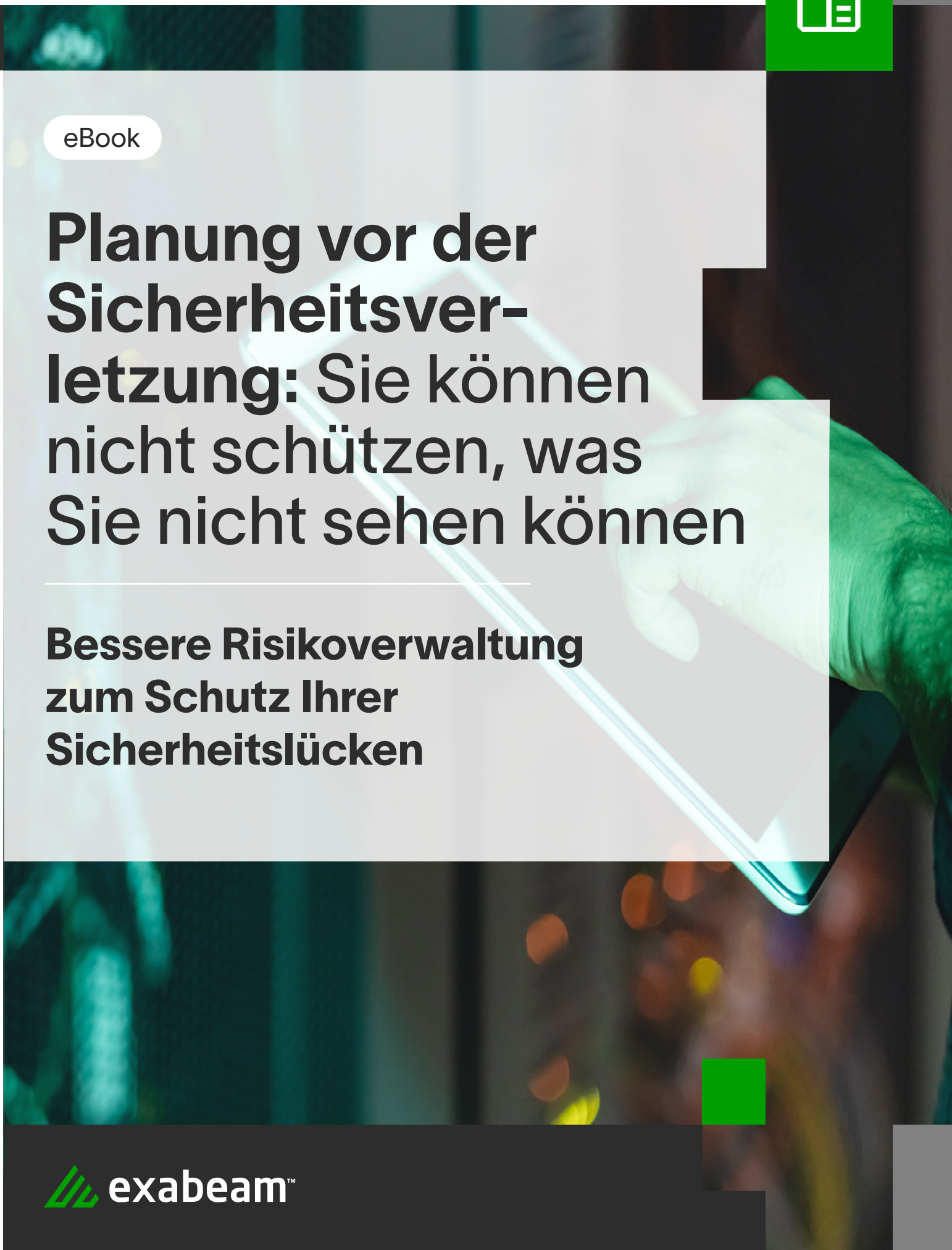


eBook

Planung vor der Sicherheitsverletzung: Sie können nicht schützen, was Sie nicht sehen können

Bessere Risikoverwaltung zum Schutz Ihrer Sicherheitslücken

exabeam™

Inhalts-verzeichnis

Planung vor der Sicherheitsverletzung:
Sie können nicht schützen, was Sie nicht sehen können

Einführung

Es ist an der Zeit, Ihre Risikoperspektive zu ändern

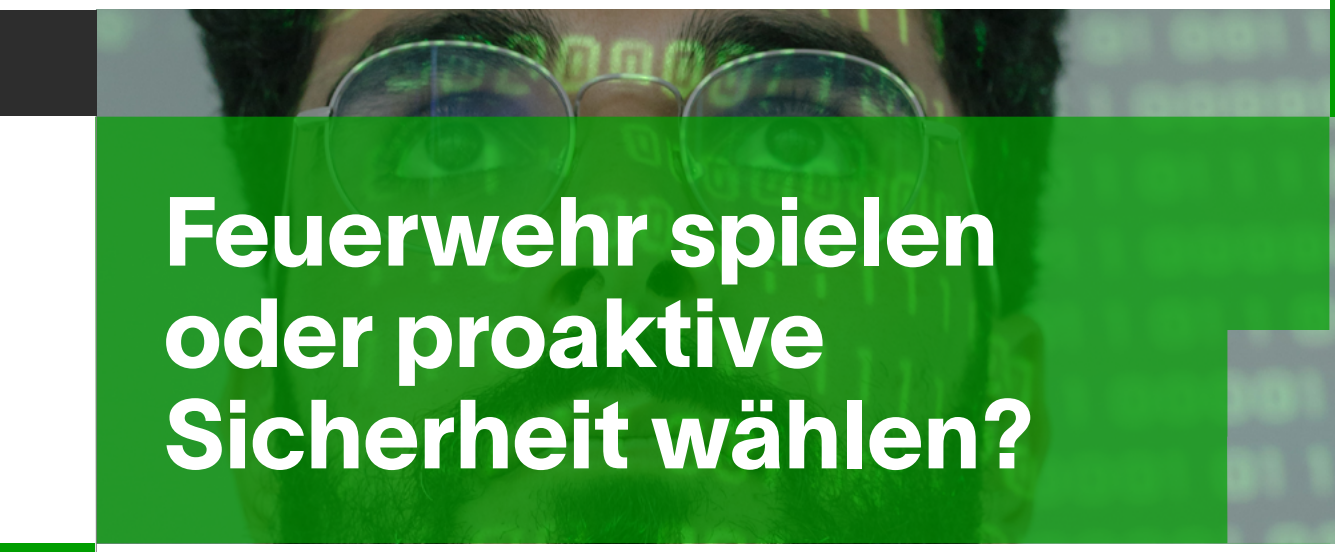
Es ist keine Neuigkeit, dass Cyberkriminelle, Nationalstaaten und böswillige Insider es aktiv auf Unternehmen abgesehen haben, um sich finanziell zu bereichern, Geheimnisse und geistiges Eigentum zu stehlen, den Betrieb zu stören und personenbezogene Daten zu sammeln. Auch der Stil und die Methoden ihrer Angriffe sind wohlbekannt – im Jahr 2020 wurden bei mehr als 80 % der gemeldeten Datenschutzverletzungen gültige Zugangsdaten oder Brute-Force-Angriffe verwendet.

Wie können Sie Schritt halten?

Dieses Paper unterstreicht die Realität, die der Gartner-Analyst Peter Firstbrook auf dem Gartner Security Summit 2021 angesprochen hat: „Die Denkweise der Annahme einer Sicherheitsverletzung ist die einzig gültige Perspektive für die Cybersicherheit." Die Strategien „Identität ist der Perimeter" und „Zero-Trust-Architektur" sind großartig, aber einfach nicht genug, um den Angreifern von heute beizukommen.

Um Schritt zu halten, ist ein tieferes Verständnis des Risikos in Ihrer Umgebung erforderlich – ein Verhaltenskontext für jeden Benutzer und jedes Asset. Die Datenwissenschaft, die hinter diesem Kontext steht, erweitert die Regeln, die Sie bereits haben, und verschafft Ihnen ein Bild der normalen Aktivitäten – wahrscheinlich die beste Verteidigung, um nicht von einem Angriff überrascht zu werden.

Dieses eBook ist ein Leitfaden für Unternehmen, die ihre Risiken besser verstehen, ihre Sicherheitserkennungs- und -reaktionsfähigkeiten verbessern und das Spielfeld gegen raffinierte Angreifer ebnen wollen.



Feuerwehr spielen oder proaktive Sicherheit wählen?

Während der weltweiten COVID-19-Krise haben die Angreifer ihre Fähigkeiten verfeinert und eine Goldmine an Möglichkeiten gefunden, Organisationen zu hacken und sensible Daten zu stehlen. Die Zahl der Angriffe nimmt stetig zu und sie werden immer raffinierter, sodass die Unternehmen Mühe haben, Schritt zu halten. Das Ergebnis? Sicherheitsteams werden von Alarmen sowie falsch-positiven (und falsch-negativen) Ergebnissen überfordert und sind gezwungen, Feuerwehr zu spielen, anstatt die Umgebung proaktiv zu sichern. Hier einige Statistiken, die Ihnen einen besseren Überblick verschaffen:

Die Zahl der Ransomware-Angriffe steigt sprunghaft an

Laut Statista gab es im Jahr 2020 weltweit 304 Millionen Ransomware-Angriffe. Das ist ein Anstieg von 62 % gegenüber 2019, aber immer noch weniger als im „Ransomware-Jahr" 2016. Ransomware-Angriffe machen 81 % aller finanziell motivierten Cyberangriffe aus.

Jährliche Anzahl von Ransomware Attacken weltweit von 20016 bis 2020

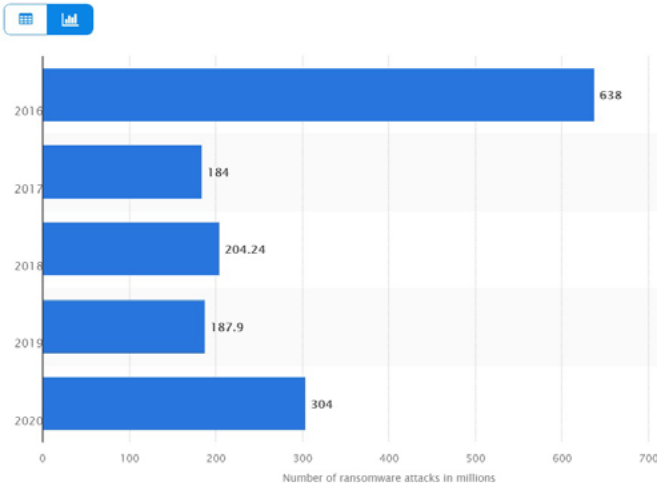


Abbildung 01 Ransomware-Angriffe nach Jahr (Bildquelle)

Warum die Verteidigung gegen Ransomware so schwer ist:

- Indicators of Compromise (IoCs) sind unzuverlässig und können nicht verwendet werden, um neue und noch nie dagewesene Ransomware-Stämme zu identifizieren
- IoCs sind unwirksam gegen einen Angriff, wenn es sich seitwärts bewegt oder die Benutzerrechte ausweitet
- Die Reaktion muss schnell erfolgen und umfasst verschiedene Produkte
- Sicherheitsteams müssen oft separate Maßnahmen in einzelnen Produkten ergreifen, wodurch Ransomware mehr Zeit bekommt um sich zu etablieren, die Systemwiederherstellung zu verhindern und Dateien zu verschlüsseln
- Ransomware nutzt bestehende Transparenzlücken aus: Fehlkonfigurationen oder Schwachstellen und machen Unternehmen anfälliger

Vorfalls-Checkliste

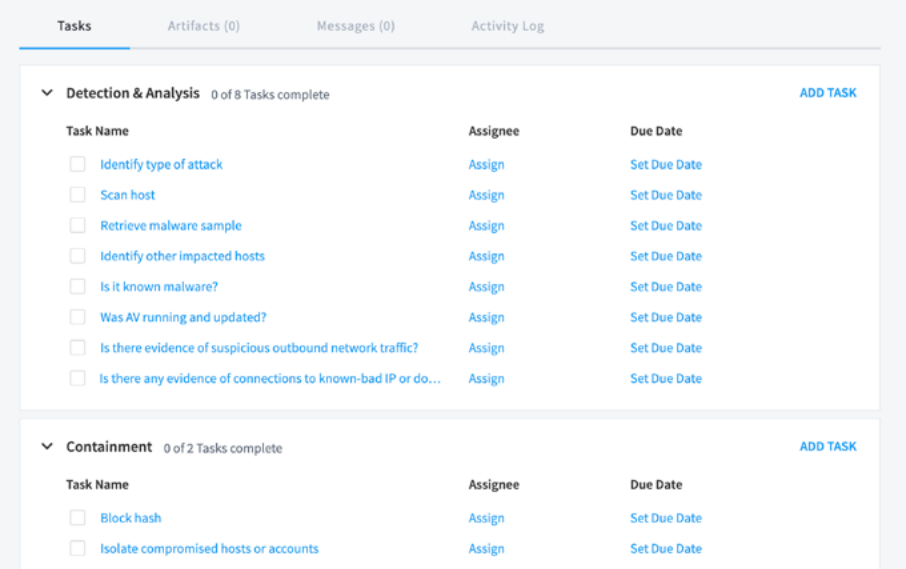


Abbildung 02 Die Ransomware-Checkliste fordert Analysten dazu auf, bestimmte Untersuchungsfragen zu beantworten und Eindämmungsmaßnahmen zu ergreifen.

Ransomware ist nur eine der Bedrohungen, bei denen Regeln und Signaturen unwirksam sind und eine automatisierte Risikotransparenz in Kombination mit Automatisierung helfen kann, eine Sicherheitsverletzung einzudämmen:

- Analysieren Sie Datei-, Web-, DNS- und Endpunktaktivitäten auf Verhaltensanomalien, um Ransomware zu erkennen, die an einem Endpunkt eintrifft oder von dort aus operiert
- Erkennen und untersuchen Sie Angriffe von bekannten und unbekannten Ransomware-Stämmen mit Verhaltensanalysen und reagieren Sie mithilfe von automatisierten Reaktions-Playbooks
- Analysieren Sie die Zusammensetzung aller Dateien, die auf einen geschützten Rechner gelangen, und blockieren Sie die jeweilige Datei, falls sie als bösartig eingestuft wird, damit sie weder auf den Rechner kopiert noch darauf ausgeführt werden kann
- Schützen Sie Infrastruktur und Systeme durch den Einsatz von Verhaltensanalysen, um Einblick in potenzielle Schwachstellen zu erhalten, die von Ransomware ausgenutzt werden könnten
- Extrahieren Sie automatisch wichtige Beweise und Links, um sie als Beweismittel für einen Rechtsfall beizufügen

Manche Angriffe können Sie sehen, andere kommen wie aus dem nichts

Ungeachtet der Behauptungen der Anbieter gibt es keine perfekte Antwort oder Sicherheitstechnologie. Ein motivierter Angreifer wird alle ihm zur Verfügung stehenden Taktiken, Techniken und Prozeduren (TTPs) einsetzen, um sein Ziel zu erreichen. Er muss nicht immer über einen Endpunkt oder eine E-Mail eindringen, so ist z. B. ein Umgehen der Identitätssysteme möglich um herkömmlichen Antivirenprogrammen durch die Maschen zu gehen.

Der 2021 Microsoft Digital Defense Report ergab, dass sie 31 Mrd. Identitätsbedrohungen und 32 Mrd. E-Mail-Bedrohungen gegenüber 9 Mrd. Endpunkt-Bedrohungen (täglich) blockieren. Hinzu kommt, dass die Anzahl der Malware-Varianten jedes Jahr schwankt. Im Jahr 2020 stieg die Zahl der entdeckten Malware-Varianten um 62 % an (Sonic Wall). Identitäts-, E-Mail-, Endpunkt- und Virenschutz sind wichtig, aber nicht ausreichend.

Da Angreifer wissen, dass ein erfolgreicher Versuch genügt, sind diese Angreifer motiviert, hartnäckig und in der Lage, mehrere automatisierte Angriffe auf ein Ziel auszuführen. Mitarbeiter und vertrauenswürdige Dritte

können unwissentlich zu Komplizen werden, indem sie einfach auf einen bösartigen Link klicken oder einen schädlichen Anhang öffnen. Diese kompromittierten Insider geben den Angreifern alles, was sie brauchen, um ihren Angriff auszuführen

Wenn jedoch ein verärgerter Mitarbeiter oder Auftragnehmer abtrünnig wird und einem Angreifer hilft, um sich einen persönlichen Vorteil zu verschaffen, kann dies sogar noch schädlicher sein. In beiden Fällen kann das Unternehmen auf dem falschen Fuß erwischt werden und die böswilligen Aktionen, die im Verborgenen stattfinden, nicht erkennen – bis es zu spät ist.

Die Verweildauer ist nach wie vor hoch

Erschwerend kommt hinzu, dass die Verweildauer (die Zeit, die Eindringlinge in einem infiltrierten System verbringen) nach wie vor hoch ist. Der 2021 Ponemon/IBM Cost of a Data Breach Report gab an, dass es 287 Tage dauerte, bis Unternehmen eine Datenschutzverletzung feststellten, 7 Tage länger als im letzten Jahr. Je länger die Angreifer im Unternehmen sind, desto mehr Zeit haben sie, die Systeme zu kompromittieren, Daten zu extrahieren und den Geschäftsbetrieb zu stören.

Angriffe wie Ransomware, bei denen die Entdeckung durch das Opfer beabsichtigt ist, verzerren die Statistik. Wichtig ist, dass die Verweildauer der Angriffe sehr unterschiedlich ist, weniger bei Ransomware (da mehr Angriffe stattfinden), aber extrem hoch bei anderen Angriffsarten („low and slow", gezielte Datenexfiltration usw.).

287 Tage Verweildauer geben Angreifern Zeit, sich seitwärts zu bewegen, Zugangsdaten zu ändern und im Netzwerk beträchtlichen Schaden anzurichten. Sie geben ihnen außerdem Zeit, sich anzupassen, indem sie die von Ihnen verwendeten Tools imitieren, was es schwieriger macht, sie zu entdecken.

Die Kosten einer Datenschutzverletzung steigen stetig

Das Ponemon Institute und IBM zeigen in ihrem Cost of a Data Breach Report, dass Datenschutzverletzungen so kostspielig sind wie eh und je. Hier sind einige der wichtigsten Erkenntnisse:

Im Jahr 2021 waren die Kosten für Datenschutzverletzungen so hoch wie nie zuvor seit Beginn der Veröffentlichung des Berichts. Die Kosten für einen Datenschutzverstoß beliefen sich auf 4,24 Mio. Dollar, gegenüber 3,86 Mio. Dollar im Jahr 2020.	**Die Cloud-Migration hat sich auf die Kosten und die Eindämmung ausgewirkt.** Unternehmen, die in ihrer Cloud-Modernisierungsstrategie weiter fortgeschritten sind, konnten die Datenschutzverletzung im Durchschnitt 77 Tage schneller eindämmen als Unternehmen, die sich noch in der Anfangsphase ihrer Modernisierungsstrategie befinden.
Künstliche Intelligenz im Bereich der Sicherheit hat die Kosten am meisten gesenkt. Unternehmen, die automatisierte und sicherheitsrelevante KI-Lösungen eingesetzt haben, gaben bis zu 3,8 Millionen Dollar weniger für die Behebung von Datenschutzverletzungen aus als Unternehmen ohne diese Lösungen.	**Remote-Arbeit war ein wichtiger Faktor für den Kostenanstieg.** Unternehmen, die von Vorfällen betroffen waren, bei denen Remote-Arbeit eine Ursache für die Datenschutzverletzung war, gaben 1 Million Dollar mehr für die Behebung aus als andere, bei denen Remote-Arbeit keine Ursache für den Vorfall war.

Tabelle 01 Faktoren für den Anstieg der Kosten einer Datenschutzverletzung.

Kontinuierliche Überwachung und Reaktion ist ein Ausgangspunkt

Der wichtigste Faktor bei der Bewältigung von Angriffen ist die Zeit, die das Sicherheitsteam benötigt, um den Angreifer zu entdecken und auf ihn zu reagieren. Eine effektive Vorfallsreaktion erfordert, dass der Angriff schnell erkannt, untersucht und gestoppt wird. Und während Sie versuchen, die Bedrohung zu stoppen, versuchen die Eindringlinge natürlich, noch weiter vorzudringen.

Abbildung 03 Je schneller die Erkennung, desto besser sind die Chancen, die Bedrohung zu beseitigen.

Die meisten SOC-Mitarbeiter verbringen mehr als 50 % ihrer Zeit mit Triage und Untersuchung. Eine wirksame Reaktion auf Vorfälle muss risikobasierte Untersuchungen umfassen, die durch Verhaltensmuster und Erkennungen ausgelöst werden, die auf einer Baseline für normale Aktivität basieren. Das Ziel – Erkennen, Untersuchen und Reagieren auf eine Sicherheitsverletzung, bevor sie Auswirkungen hat. Weitere Informationen zur Reaktion auf Vorfälle finden Sie in diesem Blog.

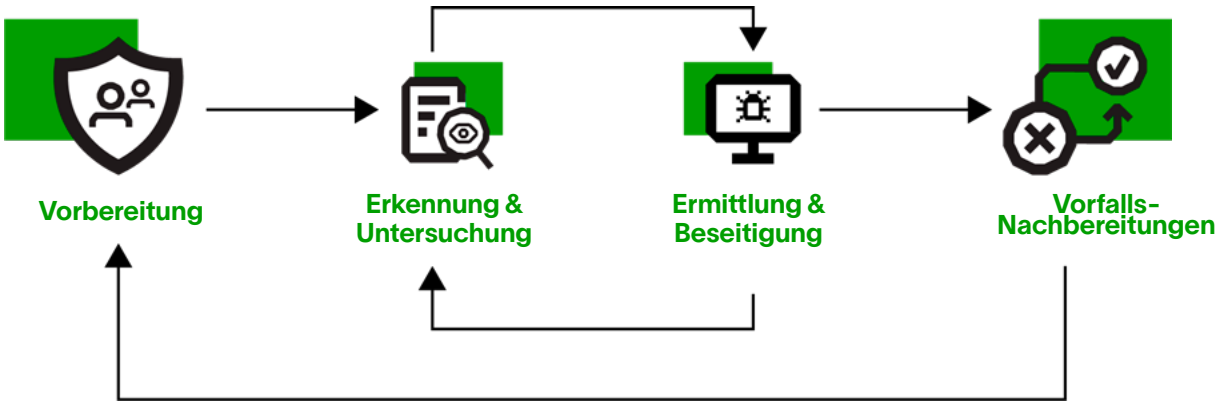


Abbildung 04 Die von NIST empfohlenen Phasen für die Reaktion auf einen Cybersicherheitsvorfall.

Der Weg zur proaktiven und effektiven Erkennung von und Reaktion auf Bedrohungen ist nicht frei von Herausforderungen. Im nächsten Abschnitt werden wir die Sicherheitslücken untersuchen, die von verschiedenen Angriffsarten ausgenutzt werden. Hier kann Exabeam helfen, wenn andere Lösungen nur wenige Antworten bieten.

Die 5 Sicherheitslücken, vor denen Sie sich schützen müssen

Neben den zusätzlichen Risiken, die Remote-Arbeit mit sich bringt, und dem Tempo, mit dem die zunehmende Cloud-Nutzung die Cloud-Sicherheit überholt, sind Unternehmen mit anderen Bedrohungen und feindlichen Aktivitäten konfrontiert, die diese Herausforderung noch vergrößert.

Die meisten herkömmlichen Tools und Praktiken bieten einen reaktiven Sicherheitsansatz: Sie sammeln Daten aus Ihrem gesamten Unternehmen und führen statische IoC- und Korrelationsregeln aus, um Warnungen zu generieren. Dieser Ansatz ist dafür berüchtigt, dass er falsch-positive Ergebnisse erzeugt, was zu einer langsamen, ungenauen Reaktion und frustrierten Analysten führt. Wenn es zu einem Angriff kommt, hat das Team Mühe, den Angreifer zu überholen. Reaktive Sicherheit ist ein Wettlauf mit der Zeit, den man nicht gewinnen kann.

Proaktive Sicherheit hingegen erkennt Bedrohungen auf Grundlage des Risikos unter Verwendung automatisierter, auf maschinellem Lernen basierender Analysen, auch bekannt als Verhaltensanalysen. Mit einer Baseline für das normale Verhalten von Benutzern und Assets sowie einem System, das auffällige Fälle automatisch eskaliert, können Sicherheitsteams schneller, präziser und entschlossener reagieren.

Einige der Vorteile von automatisierter Risikotransparenz:

- Schnellere Erkennung und Eskalation von Bedrohungen
- Effizientere Triage von Alarmen
- Rationalisierte Untersuchungen
- Verbesserte Produktivität der Analysten

Zusätzlich zu diesen Vorteilen finden Sie hier eine Liste der 5 wichtigsten Sicherheitslücken, die durch automatisierte Risikotransparenz identifiziert werden können:

Sicherheitslücke 1: Kompromittierte Benutzerdaten

Benutzerkonto-Zugangsdaten sind der Schlüssel für legitimen Zugriff, und gestohlene Zugangsdaten sind laut dem Verizon 2021 Data Breach Investigations Report der wichtigste Angriffsvektor für Datenschutzverletzungen. Wenn ein Angreifer gestohlene Zugangsdaten verwendet, erscheint sein Verhalten legitim. Dies führt dazu, dass Sicherheits-Tools, die sich auf Regeln und Korrelationen stützen, schutzlos sind. Durch diese Sicherheitslücke kann der Angreifer nach Belieben auf sensible Daten oder interne Ressourcen zugreifen. Es liegt auf der Hand, dass die Auswirkungen von kompromittierten Benutzer-Zugangsdaten verheerend sein können, was diesen Anwendungsfall zwingend erforderlich macht.

Sicherheitslücke 2: Erkennung kompromittierter Systeme/Hosts/Geräte

Es kommt häufig vor, dass Angreifer die Kontrolle über Systeme, Hosts oder Geräte innerhalb eines Unternehmensnetzwerks übernehmen und über Monate oder Jahre hinweg heimlich Angriffe durchführen. Die durchschnittliche Zeit, die Unternehmen für die Erkennung einer Datenschutzverletzung benötigten betrug laut IBM 287 Tage. Dieses beträchtliche Zeitfenster unterstreicht, wie wichtig es ist, diese Sicherheitslücke zu beseitigen, um Angriffe schneller zu erkennen und zu stoppen. Für diesen Anwendungsfall sollte die Lösung mehrere Vektoren überwachen. Sie beginnt mit den Benutzerkonten, um anomale Aktivitäten zu erkennen, mit Servern, um Abweichungen von der Baseline-Aktivität festzustellen, und mit Netzwerkgeräten, um den Datenverkehr über einen längeren Zeitraum zu überwachen und ungewöhnliche Spitzen zu erkennen. Darüber hinaus sollte eine Überwachung von nicht vertrauenswürdigen Kommunikationsquellen, unsicheren Protokollen und Anti-Virus/-Malware vorhanden sein, um die Deaktivierung bzw. Entfernung zu erkennen oder über den Status von Bedrohungsupdates zu informieren.

Sicherheitslücke 3: Böswillige Insider

Während viele der bekanntesten Sicherheitsverletzungen von externen Angreifern verursacht wurden, sind böswillige Insider nach wie vor eine der Hauptursachen für den Verlust sensibler Daten. Zu den wichtigsten internen Akteuren bei gemeldeten Datenschutzverstößen gehörten Systemadministratoren, Auftragnehmer, Endbenutzer, Entwickler, Manager und Führungskräfte – im Grunde genommen kann jeder zu einem böswilligen Insider werden. Die Erkennung von Insider-Bedrohungen stellt eine Sicherheitslücke dar, da „vertrauenswürdiges" Verhalten in den meisten Sicherheits-Tools keine Warnungen auslöst; der böswillige Insider scheint ein legitimer Benutzer zu sein. Zu den potentiell böswilligen Akteuren gehören der böswillige Insider, der eine Sicherheitsbedrohung darstellt, die von den Mitarbeitern, ehemaligen Mitarbeitern, Auftragnehmern, Geschäftspartnern oder Partnern des Unternehmens ausgeht, sowie kompromittierte Insider – wenn ein externer böswilliger Akteur legitime Zugangsdaten verwendet, um einen Angriff auszuführen.

Es kommt sehr häufig vor, dass Angreifer die Kontrolle über Systeme, Hosts oder Geräte innerhalb eines Unternehmen-snetzwerks übernehmen und Angriffe heimlich über Monate oder Jahre hinweg ausführen. Was die Fristen für die Aufdeckung von Datenverstößen betrifft, so benötigten Unternehmen laut IBM durchschnittlich

Blindspot 4: Lateral Movement Detection

Ein Eindringen über den harmlosesten Eintrittspunkt des Netzwerks einer Organisation kann schnell zu einer unbemerkten Seitwärtsbewegung werden. Der Prozess der Seitwärtsbewegung beinhaltet die systematische Bewegung durch ein Netzwerk auf der Suche nach sensiblen Daten und Assets. Womöglich begann der Angriff damit, dass ein Konto eines Mitarbeiters kompromittiert wurde? Wenn der Angreifer erst einmal eingedrungen ist, überprüft er andere Assets auf Schwachstellen, um das Konto, den Rechner und die IP-Adresse zu wechseln. Sobald der Angreifer sich Administratorrechte sichert, stehen ihm alle Türen offen. Seitwärtsbewegung ist eine Sicherheitslücke, da sie von den meisten Sicherheits-Tools nur sehr schwer entdeckt werden kann, weil die scheinbar unzusammenhängenden Ereignisse alle normal zu sein scheinen. Hinzu kommt, dass diese Aktion weder konsistent noch vorhersehbar ist, sodass Regeln keinen Schutz bieten.

Vorgefertigte Inhalte für den Exabeam-Anwendungsfall „Seitwärtsbewegung“:

Datenquellen	Typen von Erkennungsregeln	MITRE-Techniken	Tools für die Untersuchung	Reaktionsmaßnahmen
• Asset-Anmeldung und -Zugriff • Authentifizierung und Zugriffsverwaltung • VPN und Zero-Trust-Netzwerkzugriff • Netzwerkzugriff, Analyse und Überwachung • Ť Endpunktsicherheit (EPP/EDR) • Betriebssystem-protokolle (z. B. UNIX/ LINUX/OSX/Windows) •	• Pass-the-Ticket • Pass-the-Hash • Abnormale Fernzugriffs- und RDP-Aktivität • Abnormale Netzwerkverbindungen und Datenverkehr	• T1090: Proxy • T1205: Traffic-Signaling • T1219: Fernzugriffs-Software • T1071: Anwendungsschicht-Protokoll • T1021: Remote-Dienste • T1078: Legitime Konten • T1550: Alternatives Auth-entifizierungsmaterial verwenden	• Gespeicherte Suchen von Threat Hunter • Smart Timelines • Checklisten für angeleitete Untersuchungen	• Benutzer/Manager/ Personalabteilung per E-Mail kontaktieren • Benutzer oder Asset zu einer Beobachtungsliste hinzufügen • Am Vorfall beteiligte Benutzer sperren, suspendieren oder ihnen Einschränkungen auferlegen • Zugangsdaten rotieren/ Passwort zurücksetzen • Aufforderung zur erneuten Authentifizierung über • 2-Faktor/Multi-Faktor-Authentifizierung • Systeme isolieren

Tabelle 02 So trägt Exabeam zum Schließen der Sicherheitslücke „Seitwärtsbewegung“ bei. (Bildquelle)

Sicherheitslücke 5: Missbrauch von Dienstkonten

Ein Dienstkonto wird anstelle eines normalen Systemkontos verwendet, um bestimmte Anwendungsdienste auszuführen. Typische Sicherheits-Tools bieten nur begrenzten oder gar keinen Einblick in Dienstkonten. Diese Einschränkung stelle eine Sicherheitslücke dar, da Dienstkonten oft über hohe Privilegien verfügen können – und damit besonders wertvolle Ziele für Angreifer darstellen. Der Missbrauch von Dienstkonten wird mithilfe von Verhaltensanalysefunktionen aufgedeckt, die automatisch Dienstkonten identifizieren und jegliches abnormale Verhalten in Verbindung mit ihnen melden.

Warum herkömmliche SIEM-Lösungen versagen

Als zentrales Sicherheitsprodukt für die Erkennung von Bedrohungen und die Reaktion auf Vorfälle ist das traditionelle SIEM eine Zielscheibe der schleichenden Ausweitung von Zuständigkeitsbereichen geworden. Das SIEM wurde in einer Welt mit begrenzten Daten und vorhersehbarer Bedrohungsüberwachung konzipiert und konnte mit statischen Korrelationsregeln erfolgreich sein. Kommen jedoch organisierte Cyberkriminalität, nationalstaatliche Akteure, Big-Data-Workloads, Cloud-Anwendungen, Remote-Mitarbeiter und Compliance-Reporting hinzu, so haben die SIEM-Anforderungen von heute kaum noch etwas mit ihrer ursprünglichen Aufgabe zu tun.Während traditionelle SIEM-Lösungen gut gegen bekannte Bedrohungen in fest definierten Perimeter funktionieren, haben sie Schwierigkeiten, eine überzeugende Verteidigung gegen die 5 Sicherheitslücken zu bieten, die wir soeben behandelt haben.

Herkömmlichen SIEMs fehlt das Verständnis dafür, wie das normale Verhalten von Benutzern und Assets aussieht. Dies ermöglicht es Angreifern, sich Zugang zu verschaffen, sich seitwärts zu bewegen und möglicherweise wochen- oder monatelang in einem Netzwerk zu verweilen, während sie den Angriff ausweiten. Nur Produkte der nächsten Generation mit Verhaltensanalysen können einen tieferen Einblick gewähren, automatisch zwischen verschiedenen Verhaltensweisen unterscheiden und Anomalien effektiv eskalieren.

Die Exabeam Fusion Plattform ist modular aufgebaut und ermöglicht es Ihnen, ein SIEM mit XDR zu erweitern, anstatt es zu ersetzen. Die Erweiterung mit Exabeam Fusion XDR ermöglicht es einem Unternehmen, die Erkennungs- und Reaktionsfähigkeiten seines alten SIEM schnell zu verbessern, sodass Zeit bleibt, den zukünftigen Weg fortzusetzen. Wenn Sie hingegen einen vollständigen SIEM-Ersatz anstreben, ist Exabeam Fusion SIEM Ihre Antwort. Das Resultat ist:

- Verbesserte Bedrohungserkennung. Die Verhaltensanalyse von Exabeam erkennt Bedrohungen auf Grundlage von abnormalem Verhalten von Benutzern und Entitäten, unabhängig davon, ob diese neu sind oder bereits beobachtet wurden.
- Verbesserte Produktivität. Exabeam Smart Timelines automatisiert den Untersuchungsprozess und vereinfacht die Analyse, sodass das Sicherheitsteam einen umfassenden Überblick erhält und Rätselraten, Fehlalarme und manuelle Untersuchungsschritte vermieden werden.
- Schnellere Reaktionszeiten. Der ergebnisorientierte Ansatz von Exabeam und die Automatisierung der Prozesse zur Bedrohungserkennung und Vorfallsreaktion ermöglichen es Unternehmen, tiefergehende Untersuchungen durchzuführen und schneller auf Bedrohungen zu reagieren.

Exabeam Fusion SIEM and XDR

Als führendes SIEM und XDR der nächsten Generation bietet Exabeam Fusion eine über die Cloud bereitgestellte Lösung für die Erkennung von und Reaktion auf Bedrohungen.

Exabeam Fusion SIEM und XDR kombinieren Verhaltensanalysen und Automatisierung mit bedrohungsorientierten Anwendungsfall-Paketen, die darauf ausgerichtet sind, greifbare Resultate zu liefern. Die Produkte von Exabeam Fusion sind modular aufgebaut. Wir können Ihren bestehenden Data Lake oder Ihre SIEM-Bereitstellung mit XDR ergänzen oder Ihr SIEM vollständig ersetzen.

Es liegt ganz bei Ihnen.

Um mehr darüber zu erfahren, wie Exabeam Fusion SIEM oder XDR Ihnen dabei helfen kann, Sicherheitslücken zu schließen und Datenschutzverletzungen einzudämmen, fordern Sie noch heute eine Demo an.

Über Exabeam

Exabeam ist ein weltweit führendes Unternehmen im Bereich Cybersicherheit, das jeden IT- und Sicherheits-Stack intelligenter macht. Als Marktführer im Bereich der nächsten Generation von SIEM und XDR erfindet Exabeam die Art und Weise neu, wie Sicherheitsteams Analysen und Automatisierung nutzen, um Bedrohungen zu erkennen, zu untersuchen und zu bekämpfen (TDIR), von gewöhnlichen Sicherheitsbedrohungen bis hin zu den kritischsten, die schwer zu erkennen sind. Exabeam bietet eine umfassende, über die Cloud bereitgestellte Lösung, die maschinelles Lernen und Automatisierung mit einem präskriptiven, ergebnisorientierten TDIR-Ansatz nutzt. Wir konzipieren und entwickeln Produkte, die Sicherheitsteams dabei helfen, externe Bedrohungen, kompromittierte Benutzer und böswillige Gegenspieler zu erkennen, Fehlalarme zu minimieren und ihre Unternehmen bestmöglich zu schützen.

Weitere Informationen finden Sie unter exabeam.com.