CYBER SECURITY HUB

CISO-Strategien zur präventiven Gefahrenabwehr

CISOs sehen sich immer häufiger mit komplexen und systematischen Bedrohungen konfrontiert. Deshalb denken viele über einen Wechsel von einem reaktiven zu einem präventiven Schutz nach. Und zwar mithilfe von EPP-, EDR-, MDR- und Managed XDR-Lösungen.

Aus dem Inhalt:

- Wie gelingt der Übergang von einer reaktiven zu einer präventiven Strategie?
- Dank Managed Services als CISO wirtschaftlicher arbeiten
- Warum KI ein Schlüsselelement für einen präventiven Ansatz ist

Präsentiert in Zusammenarbeit mit:

BlackBerry.
Intelligent Security. Everywhere.

Gute Gründe für einen präventiven Ansatz

Als CISO müssen Sie Ihre Organisation umfassend schützen, um nicht wegen Datenverlusten in die Schlagzeilen zu geraten. Der Druck ist hoch, doch die Bedrohungslandschaft entwickelt sich ständig weiter und wird immer ausgefeilter. Außerdem erfreut sich Ransomware-as-a-Service (RaaS) wachsender Beliebtheit. Denn die Lösegeldzahlungen aus gelungenen Ransomware-Angriffen ziehen Cyberkriminelle magisch an. Damit sich dieser Trend nicht fortsetzt, untersucht dieser Bericht, warum reaktive Strategien hier nicht greifen und was Sie tun können, um Bedrohungen im Vorfeld zu stoppen.

Reaktive Cybersecurity-Lösungen haben ein großes Manko. Zwar können Sie mit ihrer Hilfe Ihre Daten und Systeme wiederherstellen, doch nichts hindert die Angreifer daran, Sie mit den Daten zu erpressen, die sie Ihnen vor der Ausführung der Ransomware gestohlen haben. Deshalb genügt oft schon die Drohung mit der Veröffentlichung, um die Opfer zur Zahlung des Lösegelds zu bewegen. Selbst wenn es seine Systeme und Daten selbst wiederherstellen könnte.

„Bedrohungsakteure entwickeln ihre Taktiken ständig weiter, und wir müssen diesen Änderungen Rechnung tragen", erklärt Tony Lee, Vice-President – Global Services Technical Operations bei BlackBerry.

Es ist wichtig, schnell zu reagieren und mit der Wiederherstellung zu beginnen. Doch nach Ansicht von Lee ist dies nur die halbe Wahrheit. Denn die Prangermethoden und die Erpressung mit den erbeuteten Daten seien damit nicht vom Tisch.

RaaS ist so gefährlich, weil auch weniger erfahrene Bedrohungsakteure gegen Bezahlung bereits entwickelte Ransomware für einen Angriff nutzen können. Das erbeutete Geld hält dann das unselige Spiel am Laufen. Dadurch geraten auch Unternehmen ins Visier, die sich aufgrund der Unternehmensgröße nie für ein lohnendes Ziel gehalten hätten. Wer sensible Unternehmensdaten schützen will, kann sich demnach keine rein reaktive Abwehr leisten. Denn die Angreifer sind weltweit tätig und halten sich nicht an Bürozeiten. Ihre Verteidigung sollte deshalb auch rund um die Uhr funktionieren.

Tatsächlich bereiten die „neuen Ransomware-Modelle" den Unternehmen große Sorgen. Der jüngste ***Emerging Risks Monitor Report*** von Gartner zeigte, dass Ransomware für die befragten Unternehmen aktuell das größte Problem darstellt. Es übertrifft sogar pandemiebedingte Störungen, zu denen auch Probleme mit der Lieferkette gehören.

Inhalt

Moderne Unternehmen sehen sich zunehmend einem ständig wachsenden Cyberspace, riesigen Datenmengen und unzähligen Endpunkten gegenüber. Noch vor Kurzem war die Anzahl der zu verwaltenden Systeme überschaubar. Doch mittlerweile ist es unerlässlich, sich auf die explodierende Anzahl und Vielfalt der neuen Endpunkte einzustellen. Das schnelle Wachstum und die Verbreitung des IoT stellen ein erhebliches Risiko dar. Nicht nur Privatpersonen, auch Unternehmen machen sich durch die Geräte angreifbar. Ob smarte Kaffeekannen, intelligente Ladegeräte für Fahrzeuge oder **Thermometer von Aquarien**, alles kann zu einem Türöffner für Unbefugte werden. Doch mit einem präventiven Ansatz, modernen Technologien und der passenden Strategie können Sie als CISO diese Probleme lösen.

> „Der Übergang von einer reaktiven zu einer präventiven Sicherheitsstrategie ist keine leichte Aufgabe."
>
> **Tony Lee**
>
> **Vice President, Global Services Technical Operations BlackBerry**

Dieser Report zeigt, wie CISOs mittels Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR), Managed Detection and Response (MDR) und Managed Extended Detection and Response (XDR) die neuesten Strategien zur Cybersicherheit einsetzen, um sich in dieser komplexen und dynamischen Bedrohungslandschaft zu behaupten.

Managed Services bei Kompetenzlücken

Angesichts der wachsenden Bedrohungen gehören zu einer präventiven, KI-gestützten Sicherheitsstrategie neben einem 24 x 7 x 365-Monitoring auch Threat-Intel-Overlay und kontinuierliche Bedrohungssuche. KI ist dabei ein wirkungsvoller und unverzichtbarer Multiplikator, um Kompetenz- und Ressourcenlücken zu schließen und Abläufe effizienter zu gestalten. Beispielsweise ermöglichen Ihnen die prädiktiven Fähigkeiten von KI-basierten EDR- und EPP-Lösungen die Bekämpfung von Zero-Day-Bedrohungen und damit die Verfolgung einer echten Präventionsstrategie (siehe Seite 6 für Details zu KI-Lösungen).

Kaum ein CISO kann die dafür nötigen Fähigkeiten und Ressourcen intern bereitstellen. In aller Regel können dies nur die größten Unternehmen mit entsprechendem Budget. Für alle andern gibt es Managed Services, die je nach Bedarf fixe Ressourcen bereitstellen.

„Meist ist das Budget gar nicht das Problem, viel häufiger fehlt es an Personal und Zeit für den Aufbau. Unternehmen jeder Größe sparen oft viel Zeit und Kosten, wenn sie die Hilfe eines erfahrenen MDR- oder XDR-Anbieters in Anspruch nehmen“, erklärt Lee.

Managed Services sind durchaus keine neue Lösung. Doch Lee hat die Erfahrung gemacht, dass Kunden, die mit einem EDR-Produkt für mehr Transparenz in ihrer Umgebung sorgen wollen, schnell den Wert der Lösung erkennen und genauso schnell die Herausforderung bei der Implementierung bemerken. Nicht zu vergessen den Aufwand für die Optimierung eines solch leistungsstarken Produkts.

KI-basierte EDR- und EPP-Lösungen der nächsten Generation ersetzen zunehmend herkömmliche Antivirenprodukte, die selbst minimale Sicherheitsstandards nicht mehr erfüllen.

Allerdings verweist Lee darauf, dass der Einsatz herkömmlicher Lösungen oft darauf hindeutet, dass ein Unternehmen aufgrund seines hohen Risikos keine Cyberversicherung abschließen kann.

„Versicherer von Cyberrisiken wollen nicht nur Produkte der nächsten Generation sehen, sondern auch EDR- und 24 x 7-Monitoring. Denn die Kombination aus KI-gestütztem EPP und EDR ermöglicht präventive Sicherheit und sorgt für die nötige Transparenz, die im Ernstfall für eine Untersuchung und Validierung gebraucht wird“, so Lee.

Fachkräftemangel

Einerseits wird EDR immer beliebter, andererseits wird es für Unternehmen immer schwieriger, die Lösung angemessen zu bedienen. Denn sie erfordert Engagement und dedizierte Ressourcen.

„Unternehmen erkennen die Notwendigkeit [für EDR], allerdings verfügen sie oft nicht über das nötige Know-how im eigenen Haus. Statt sich ein unnötiges Shelfware-Produkt anzulachen, entscheiden sie viele für Managed Services“, fügt Lee hinzu.

Dies zeigt auch eine **Studie des britischen Ministeriums für Digitales, Kultur, Medien und Sport** vom März 2020: „Annähernd 653.000 Unternehmen (48 Prozent) haben eine grundlegende Kompetenzlücke. Das heißt, den für die Cybersicherheit verantwortlichen Personen fehlt das nötige Vertrauen, um grundlegende Sicherheitsaufgaben auszuführen, die im staatlich unterstützten Cyber Essentials-Programm festgelegt sind. Sie erhalten auch keine Unterstützung von externen Cybersecurity-Anbietern.“

Selbst wer zusätzliche Mitarbeiter einstellen möchte, stößt an seine Grenzen. Denn der Fachkräftemangel in der Cybersecurity-Branche ist ein weltweites Problem.

US-Präsident Biden sagte im August 2021 in einer Rede zur Verbesserung der Cybersicherheit in den USA: „Uns fehlen qualifizierte Cybersecurity-Mitarbeiter, um Schritt zu halten [mit Hackern und Kriminellen].“

„Wir haben unser eigenes Problem geschaffen, weil wir uns auf Erkennung und Reaktion konzentriert haben und nicht auf Prävention."

Brian Robison

Vice President of Solutions Strategy bei BlackBerry

Biden stellte ferner fest, dass etwa eine halbe Million Cybersecurity-Jobs unbesetzt seien.

Statt mit dem Fachkräftemangel zu hadern, sollten Sie besser über Managed Services nachdenken, um die Bereitstellung von Cybersicherheitslösungen abzusichern.

Brian Robison, Vice President of Solutions Strategy bei BlackBerry, betrachtet den Fachkräftemangel als ein hausgemachtes Problem der Cybersecurity-Branche. „Wir haben unser eigenes Problem geschaffen, weil wir uns auf Erkennung und Reaktion konzentriert haben und nicht auf Prävention. Wir verschwenden Millionen und Abermillionen an Unternehmensgeldern, um auf Bedrohungen zu reagieren, die hätten blockiert werden können", sagt er.

„Managed Services sind unentbehrlich, um die Lücke zu schließen und um Tausende Unternehmen und Hunderttausende von Endpunkten abzudecken. Diese Services können viele Geräte schützen, indem sie eine kleinere Gruppe hochqualifizierter Experten mit modernsten Technologien und effizienten, abgestimmten Prozessen ausstattet", ergänzt Lee.

Die renommierte Beratungsgesellschaft **KPMG schrieb 2021 in einem Post**: Die Antwort auf die Frage der Kompetenzlücke lautet nicht nur mehr Mitarbeiter, sondern auch Einsatz von Technologie und Automatisierung für Routineaufgaben.

Dabei soll die Technologie nicht den Menschen ersetzen. Sie soll vielmehr bei wichtigen Aufgaben diejenigen unterstützen und entlasten, die in der Cybersicherheit arbeiten.

Warum sich ein präventiver Security-Ansatz auszahlt

Durch den kombinierten Einsatz von MDR und Managed XDR mit EDR- und EPP-Lösungen können Sie Ihre Investitionen in die Cybersicherheit optimieren.

Lee ist überzeugt davon, dass Managed Services die kostengünstigste Lösung sind, um die Cybersicherheit eines Unternehmens zu gewährleisten.

„Wir haben verschiedene Kostenmodelle für MDR/Managed XDR aufgestellt und durchgerechnet. Der interne Aufbau lohnt sich nur für die größten Unternehmen, wie sie in den Fortune 100 zu finden sind", erklärt Lee.

Das gilt speziell für kleine und mittlere Unternehmen. Denn diese Unternehmen sind nicht groß genug, um die Arbeit eines Managed Services Providers durch die Investition in eigene Mitarbeiter zu kompensieren.

KMUs müssen ihre Investitionen in die Sicherheit besonders sorgfältig abwägen, da sie einem erhöhten Risiko ausgesetzt sind. Dies sagt auch die **US- Bundesbehörde zur Unterstützung von kleinen und mittleren Unternehmen**. Sie betont, dass kleine Unternehmen für Cyberkriminelle besonders attraktiv seien, da sie wertvolle Informationen besäßen und nicht über die Sicherheitsinfrastruktur großer Unternehmen verfügten.

Managed Services bieten Ihnen nicht nur Lösungen, um Bedrohungen zu begegnen, sondern sie erleichtern Ihnen auch den Übergang zu einer präventiven, kosteneffizienten Sicherheitsstrategie.

„Prävention ist weitaus weniger zeitaufwendig und kostspielig als die Untersuchung und Eindämmung. Je früher wir den Angriff in der Cyber-Kill-Chain stoppen können, desto weniger Ressourcen werden gebraucht. Deshalb kann eine wirksame Präventionsstrategie sowohl die Kompetenz- und Ressourcenlücke schließen als auch die Ausgaben für die Verteidigung verringern", sagt Lee.

CISOs ändern ihre Strategie

„CISOs sollten über eine Investition in eine Präventionsstrategie ernsthaft nachdenken und sich die Vorteile für ihr Unternehmen vor Augen führen", ist Robison überzeugt. Seiner Ansicht nach müssten die CISOs von heute eine proaktivere Rolle übernehmen, um nicht mehr nur als Kostenstelle wahrgenommen zu werden.

Die Überlegungen und Diskussionen sollten sich auch nicht länger um Investitionen in ältere AV-Lösungen drehen. In den Augen von Robison binden diese wichtige Ressourcen und sind ein echtes Hemmnis für präventive Lösungen, die Bedrohungen stoppen. Und zwar bevor unnötige Kosten durch Lösegeldzahlungen und Wiederherstellungsmaßnahmen entstehen.

„Dies erfordert eine enge Zusammenarbeit mit den Anbietern, die Ihnen helfen, das Geschäft auszubauen", sagt er.

Robison vergleicht die Neuausrichtung der CISOs mit den Aufgaben der CIOs beim Umstieg von lokalen Datenlösungen zu Cloud-Lösungen für Rechenzentren.

„CIOs haben aus massiven Kostenstellen ein proaktiveres Geschäftsmodell gemacht", sagt er. „Die CISOs sind noch nicht so weit."

„Den größten Paradigmenwechsel sehe ich in einer anderen Einstellung. Als CISO sollten Sie sagen können: Die Investition [in einen Managed Service] muss ich tätigen."

Seiner Meinung nach ist jetzt ein radikales Umdenken erforderlich. Genauso radikal wie damals, als es um den Umstieg von kostspieligen On-Premise-Lösungen auf effizientere cloudbasierte Services ging.

„Für CISOs ist es fraglos keine leichte Aufgabe vor dem Vorstand zu stehen und dem CEO zu sagen, dass es einen besseren Weg gibt", gesteht Robison ein. „Doch letzten Endes werden die meisten Unternehmen schnell feststellen, dass veraltete und traditionell reaktive Lösungen Vorfälle nicht verhindern. Und dass es extrem kostspielig wird, wenn es zu einem Vorfall kommt."

Auch kleine und mittlere Unternehmen sehen sich bei Vorfällen oft astronomischen Kosten gegenüber. Doch es ist möglich, sie durch Engagement und Investitionen in präventive Lösungen wie MDR/Managed XDR, EDR und EPP abzumildern.

Was KI unerlässlich macht

KI bietet sich bei Lösungen an, die große Datenmengen verarbeiten müssen und Muster erkennen sollen, um auf Basis der laufenden Analysen den weiteren Verlauf vorherzusagen und aktiv zu werden. Und zwar ohne menschliche Hilfe. Damit sind wir im Bereich prädiktiver Fähigkeiten.

Der Einsatz von KI steigert den Wert von MDR- und Managed XDR-Lösungen enorm. Denn so ist es möglich, die gewünschte 24 x 7 x 365-Überwachung auf skalierbare Weise bereitzustellen.

„Tatsächlich ist es so, dass durch menschliche Expertise ältere EPP- und EDR-Lösungen nicht skaliert werden können, es gibt mittlerweile zu viele neue Virusvarianten", sagt Robison.

Gerade bei MDR/Managed XDR, EDR und EPP ist KI unerlässlich. Nur so gewinnen Sie einen prädiktiven Vorteil gegenüber aktuellen Bedrohungen.

Im Juli 2021 **stellte das Weltwirtschaftsforum fest**, dass mit richtig eingesetzter KI aktuelle Sicherheitsbedrohungen bekämpft werden können. Außerdem betont der Bericht, dass KI dabei helfen kann, unmittelbar auf Bedrohungen zu reagieren. Insbesondere dann, wenn die Datenmenge für die Bearbeitung durch Menschen zu groß ist.

Das mathematische Modell

KI ist für den Schutz von Netzwerken unerlässlich, denn die große Flut täglicher Warnungen ist durch menschliche Expertise allein kaum zu bewältigen. Nicht wenige Unternehmen scheitern daran, alle Endpunktbedrohungen und Schwachstellen zu analysieren. Angesichts des besprochenen Fachkräftemangels ist KI auch hier ein wirkungsvoller Multiplikator.

Mit einem KI-gestützten Endpunktschutz, der auch maschinelles Lernen nutzt, können Sie Malware, dateilose und anwenderbasierte Bedrohungen in Ihrer Umgebung aufdecken. Die Vorteile der KI zeigen sich mittlerweile auch in der Praxis. 2019 gaben **64 Prozent der von Statista befragten IT-Führungskräfte** an, dass KI in ihrem Unternehmen dazu beigetragen hat, die Kosten für Vorfälle zu senken.

Laut Statista stimmten 83 % der Befragten der Aussage zu: „Ohne KI sind wir nicht in der Lage auf Cyberangriffe zu reagieren." Doch KI ist nicht gleich KI. „Viele Anbieter werben mit künstlicher Intelligenz in ihren Produkten, um auch ein Stück vom Kuchen zu bekommen", so Lee. Deshalb sollten Sie sich für einen Anbieter entschieden, der seit geraumer Zeit KI-Expertise vorweisen kann und über ausgereifte mathematische KI-Modelle verfügt.

„Das Schöne am mathematischen Modell sind die Vorhersagemöglichkeiten. Selbst bei ganz neuen Bedrohungen ist die Wahrscheinlichkeit sehr groß, dass das mathematische Modell bereits die neue Bedrohung erfasst hat, ohne dass sie überhaupt bekannt ist", erklärt Lee.

> „Der Einsatz von KI ist entscheidend, da es sonst nicht möglich ist, effizient zu skalieren."
>
> **Tony Lee**
>
> **Vice President, Global Services Technical Operations, BlackBerry**

KI kann etwas, was Menschen nicht können. Sie kann riesige Datenmengen durchforsten, um Bedrohungen aufzudecken. Und anhand der Befunde kann sie Vorhersagen darüber treffen, wie die zukünftigen Bedrohungen aussehen.

Fazit

Damit der Übergang von einer rein reaktiven zu einer präventiven Strategie gelingt, heißt es Abschied nehmen von herkömmlichen AV-Technologien. Nur mit Lösungen der nächsten Generation können Sie Angriffe verhindern, bevor sie auftreten.

Mithilfe der richtigen Kombination von MDR-, Managed XDR-, EPP- und EDR-Lösungen können Sie eine effektive Sicherheitsstrategie verfolgen, die Ihre Ressourcen nicht belastet und die Alarmmüdigkeit minimiert.

All diese Lösungen müssen perfekt harmonieren.

„Die vollständige Integration von EPP, EDR und Managed Service ist zur Korrelation von Vorfällen zwingend notwendig. Der Versuch, EPP- und EDR-Ereignisse in zwei verschiedenen Systemen zu korrelieren, ist nicht skalierbar", weiß Lee. „Die Managed Services Experten können alles in einem Paket bereitstellen, denn sie wissen genau, wie man die Produkte am besten einsetzt. EPP allein reicht nicht. Erst mit EDR lassen sich Beweise sammeln, Bedrohungen jagen und sogar erweiterte Maßnahmen ergreifen."

„Durch die Kombination dieser beiden Technologien mit Managed Services verstärken Spezialisten für IR und Security-Prävention Ihr Sicherheitsteam sinnvoll. Dadurch können Sie wichtigere Sicherheitsinitiativen vorantreiben, ohne Zeit und Ressourcen zu verschwenden, um Warnungen zu selektieren oder sich von einem Angriff zu erholen", ergänzt er.

Für die Beurteilung und die Einschätzung des Ausmaßes von Vorfällen ist KI unerlässlich. Auch zur Identifizierung von Bedrohungen genügt menschliche Expertise allein nicht. Es ist die prädiktive Natur der KI, die Bedrohungen aufdecken kann, bevor ein Schaden entsteht.

Angesichts des weltweiten Mangels an Cybersecurity-Experten ist eine Präventionsstrategie die einzige Möglichkeit für Unternehmen, um sich in der heutigen Bedrohungslandschaft zu verteidigen.

Wichtig: Alle Kommentare in diesem Report geben die persönliche Meinung der Personen wieder und haben keinen Bezug zu ihren Arbeitgebern, Institutionen oder Geschäftspartnern.