N-ABLE™

Endpoint Detection and Response:

Den finanziellen Nutzen vor Augen

eGuide

Einleitung

Die Pandemie hat die Art und Weise, wie wir unsere täglichen Aufgaben ausführen, grundlegend verändert. Die Menschen verbringen zunehmend mehr Zeit damit, online zu arbeiten, online einzukaufen, an virtuellen Veranstaltungen teilzunehmen und selbst Arztbesuche erfolgen immer häufiger online. Dies hat zur Folge, dass die Unternehmen ihren Wechsel in die Cloud mit Nachdruck vorantreiben. Wenn man nun noch die Arbeit im Homeoffice (WFH oder auch „working from home“) und die Nutzung privater Geräte (BYOD bzw. „bring your own device“) in die Gleichung miteinbezieht, ergibt das in Summe eine erhöhte Konnektivität und wachsende Angriffsflächen für Einzelpersonen und Unternehmen.

Nun ist es die Aufgabe von MSPs, die IT-Bestände, Daten und Geschäftsprozesse ihrer Kunden zu verwalten und zu schützen, daher haben sie häufig weitreichenden Zugriff auf die Systeme der betreffenden Kunden. Das macht die MSPs und die von ihnen verwendeten Tools natürlich zu einem attraktiven Angriffsziel. Aus einem aktuellen N-able-Bericht[1] geht hervor, dass MSPs zunehmend zum Ziel von Cyberangriffen werden, wobei die Angriffe seit Beginn der Pandemie um 90 % zugenommen haben. Und es sieht momentan nicht so aus, als würde sich dieser Trend verlangsamen.

Im Verlauf der letzten Jahre konnten wir eine rasante Steigerung der Akzeptanz von Endpoint Detection and Response (EDR) im MSP-Bereich beobachten. Mehr und mehr Serviceanbieter entschließen sich dazu, veralteten Virenschutzlösungen (AV-Lösungen)[2] zugunsten von EDR den Laufpass zu geben. So mancher stößt jedoch bei der geplanten Umstellung auf den Widerstand seiner Kunden und steht vor der großen Herausforderung, den finanziellen Nutzen dieser Maßnahmen belegen zu müssen.

In diesem eGuide beleuchten wir die bewährten Verfahren, die Ihnen dabei helfen, diese Herausforderungen zu meistern und erfolgreiche Gespräche über EDR mit Ihren Ansprechpartnern zu führen.

Bewährte Verfahren zum Nachweis des finanziellen Nutzens von EDR

Den finanziellen Nutzen zu demonstrieren kann eine gewaltige Herausforderung sein. Mit einem gut durchdachten, strukturierten Ansatz sieht die Sache jedoch schon anders aus.

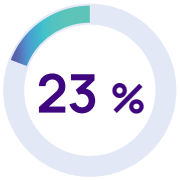
1. Klären Sie Ihre Kunden über die bestehende Cyber-Sicherheitslandschaft auf
2. Machen Sie sich ein Bild ihrer geschäftlichen Anforderungen und Perspektiven
3. Zeigen Sie die tatsächlichen Kosten eines Angriffs auf
4. Skizzieren Sie Ihre Lösung und Ihre zukünftigen Sicherheitspläne
5. Wenn sie sich dann immer noch nicht überzeugen lassen, ziehen Sie eine klare Linie

Sprechen wir über einige der wichtigsten Punkte in jedem Schritt.

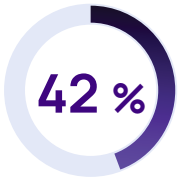
1 Klären Sie Ihre Kunden über die bestehende Cyber-Sicherheitslandschaft auf

Mit einer simplen Statistik lässt sich vielfach ein aussagekräftiges Bild zeichnen. Und falls Ihre Statistiken nicht überzeugend genug sind, können Ihnen aktuelle Nachrichten über die jüngsten Sicherheitsverstöße dabei helfen, Ihren Standpunkt zu verdeutlichen. Zum Beispiel:

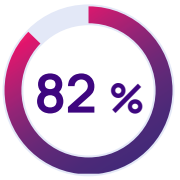
Ransomware verzeichnete 2021 neue Rekorde, mit einem **Anstieg von 105 % gegenüber 2020**[4]



23 % aller Datenschutzverstöße sind auf menschliches Versagen zurückzuführen[5]



42 % der häufigsten Angriffe, die MSPs beobachten, erfolgen durch Ransomware.[6]



82 % der Kunden von MSPs verzeichnen eine Zunahme der Angriffsversuche[7]

Sie sollten Ihren Kunden keine Angst einjagen, sondern ihnen klar machen, dass alle Unternehmen – egal ob groß oder klein – potenzielle Zielscheiben sind und dass konventionelle Lösungen mit der rasanten Entwicklung der Cyberbedrohungen nicht Schritt halten können.

2 Machen Sie sich ein Bild ihrer geschäftlichen Anforderungen und Perspektiven

Gehen Sie sicher, dass Sie das Geschäftsmodell und die Bedürfnisse Ihrer Kunden auch wirklich verstehen. Finden Sie heraus, was wirklich wichtig für sie ist, um eine optimale Lösung anbieten zu können, und fragen Sie sie nach ihren geschäftlichen Zielen und Erwartungen. Wir haben für den Anfang ein paar Fragen für Sie zusammengestellt:

- War Ihr Unternehmen schon einmal Opfer von Ransomware oder anderer Malware?
- Haben Sie in Ihrem Unternehmen schon einmal Betriebsausfälle erlebt? Welche Auswirkungen hatten diese?
- Beschäftigen Sie die möglichen Auswirkungen von solchen Ausfällen auf Ihr Geschäft?
- Welche Kosten kämen bei Ausfällen pro Stunde auf Sie zu?
- Haben Sie einen dezidierten Plan für den Fall, dass Ihre Systeme oder Daten nicht verfügbar sind?
- Wäre Ihr Unternehmen in der Lage zu arbeiten, wenn die Systeme vorübergehend ausfallen würden? Wie lange ginge das?
- Bereitet Ihnen Ihre aktuelle Situation schlaflose Nächte?
- Drohen rechtliche Konsequenzen, wenn Services plötzlich nicht mehr verfügbar sind?
- Wie lange ist Ihr Geschäftsbetrieb ohne Datenzugriff möglich?
- Welche Auswirkungen auf Ihren Ruf hätte ein eintägiger Ausfall Ihrer Kundenbetreuung?
- Haben Sie Ihre vorhandenen Cyberversicherungen und Datenschutzversicherungsverträge geprüft und besteht das Risiko, dass kein Versicherungsschutz vorhanden ist, falls Sie nicht die neuesten auf dem Markt verfügbaren Sicherheitstechnologien nutzen?

Einwände, mit denen die MSPs in der Regel bei solchen Gesprächen mit ihren Kunden konfrontiert werden, betreffen vor allem den höheren Preis für eine fortschrittliche Lösung (wie EDR) und den Gedanken, dass das Unternehmen des Kunden ja sowieso zu klein und unattraktiv für Cyberangreifer ist. Das könnte allerdings nicht weiter von der Wahrheit entfernt sein.

Hier finden Sie einige der häufigsten Einwände, mit denen MSPs konfrontiert werden, und praktische Tipps, wie sie ihnen begegnen können:

„Ich habe bereits einen Virenschutz. Ich brauche kein EDR“

Hier werden tatsächlich Äpfel mit Birnen verglichen – die Kunden vergessen dabei, dass die unterschiedlichen Lösungen auch unterschiedliche Schutzniveaus bieten und neigen dazu, die Kosten für Mitarbeiter bzw. Arbeit unterzubewerten. Erklären Sie ihnen die Unterschiede zwischen AV und EDR und insbesondere der verschiedenen Schutzniveaus und informieren Sie sie über den mit den jeweiligen Sicherheitslösungen verbundenen Aufwand.

EDR bietet eine Reihe von Funktionen, die weit über simplen Virenschutz hinausgehen. Im Folgenden finden Sie eine kurze Übersicht über die Unterschiede der beiden Lösungen:

AV

- Schutz gegen Malware und Viren. In der Regel durch das Scannen von Dateien.
- Traditionell basierend auf Virensignaturen. Das heißt, die Malware muss dem AV-Anbieter bereits als solche bekannt und in einer Signaturdatenbank erfasst sein. Diese Datenbank muss auf dem Endgerät des Benutzers regelmäßig aktualisiert werden.
- Der Administrator muss regelmäßig Virenscans vornehmen.

EDR

- Schützt gegen verschiedene Bedrohungen: unter anderem gegen dateilose Angriffe, infizierte Dokumente und schädliche Skripte. Beobachtet Geräteverhalten unter Einsatz von künstlicher Intelligenz.
- Hält nach möglichen Angriffsversuchen Ausschau, statt sich auf Dateiscans zu verlassen. Wenn EDR verdächtige Vorgänge auf einem Endgerät erkennt, wird (erforderlichenfalls) in nahezu Echtzeit eine Warnmeldung ausgegeben.
- Potenzielle Bedrohungen werden automatisch behandelt. Manche EDR-Lösungen, wie N-able EDR, können Windows-Endpunkte nach einem Ransomware-Angriff in kürzester Zeit wieder in einen sicheren, einwandfreien Zustand zurückversetzen und so den entstandenen Schaden im Handumdrehen rückgängig machen.

Laut branchenweiten Umfragen[8] und den Erfahrungen unserer eigenen Sicherheitsexperten beträgt der Zeitaufwand für eine manuelle Behebung einer Bedrohung, nachdem sie von einer AV-Lösung aufgespürt wurde, im Schnitt etwa 3,5 Stunden. Im Gegensatz dazu kann die Qualität von Analysedaten und der mittels EDR aufgezeichneten Telemetrie mit der automatisierten Behebung (einschließlich Rollback) und zusätzlichen Funktionen die Reaktionszeit auf weniger als 30 Minuten verringern, manchmal sogar bis auf nur 5 Minuten.

„Das ist viel zu teuer“

Wenn der Nutzen Ihrer Leistungen klar wird, lösen sich Preisbedenken in der Regel von selbst auf. Versuchen Sie Ihren Kunden klar zu machen, welche Kosten auf sie zukommen, wenn sie nicht zu einem modernen Sicherheitsprogramm wechseln.

„Ich gehe das Risiko ein, bezahle im Fall das Lösegeld und melde einen Versicherungsfall“

Verlassen Sie sich nicht nur auf Ihre Versicherungsgesellschaft – sie wird nach fahrlässigem Verhalten suchen. Liefern Sie ihr keinen Grund, Ihren Anspruch zurückzuweisen.

„Mir passiert das nicht, unser Betrieb ist viel zu klein“

Jeder ist anfällig für Angriffe. Der kleine Kunde ist vielleicht nicht das eigentliche Ziel, könnte aber als Einfallstor genutzt werden. Sorgen Sie dafür, dass Ihr Kunde nicht das schwächste Glied wird

„Mir passiert das nicht – wer könnte mit meinen Daten schon etwas anfangen?“

Möglicherweise können die Angreifer mit Ihren Daten selbst nichts anfangen, aber sie können sie als Geiseln nehmen, weil Sie Ihre Daten dringend brauchen und bei einem vollständigen Datenverlust Ihr ganzes Unternehmen gefährdet sein könnte. Die Angreifer wollen Sie in eine Position drängen, in der Sie dann das Lösegeld bezahlen müssen.

3 Zeigen Sie die tatsächlichen Kosten eines Angriffs auf

Wenn Sie für eine neue Sicherheitslösung werben, sprechen Sie dabei am besten über Geld – bei diesem Stichwort wird jeder Geschäftsführer hellhörig.

Zwei Dinge, die den Erwerb einer EDR-Lösung auf den ersten Blick rechtfertigen, sind die Kosten für Ausfallzeiten – die sich in finanziellen Verlusten durch entgangene Geschäftsmöglichkeiten niederschlagen – und die Zeit, die nötig ist, um wieder auf die Beine zu kommen, was wiederum zusätzliche Arbeitszeit und hohen Aufwand bedeutet.

Um das Ganze zu verdeutlichen, bitten Sie Ihren Gesprächspartner doch, sich ein Szenario auszumalen, in dem die Systeme infolge eines Ransomware-Angriffs vollständig ausgefallen sind. Dann rechnen Sie aus, was das kosten wird. Im Vergleich dazu werden die Kosten für EDR vermutlich wie ein Schnäppchen aussehen.

Die Kosten der Ausfallzeit pro Tag lassen sich wie folgt berechnen: Produktivitätsverlust + entgangene Einnahmen + Kosten für die Wiederherstellung + Kosten für immaterielle Güter, wobei immaterielle Güter abhängig vom jeweiligen Fall Folgendes sein können:

- Ransomware-Lösegeld
- Gesetzlich verhängte Geldstrafen und Bußgelder
- Juristische Kosten
- Höhere Versicherungsprämien
- Beratung und Mitarbeiterschulung
- Kollateralschäden
- Umsatzverluste oder Abwanderung von Kunden
- Rufschädigung

Hier finden Sie ein Beispiel, wie das Gespräch ablaufen könnte:

Hypothetisch tritt folgendes Szenario ein:

Ein Kunde aus der Buchhaltungsbranche mit 40 Mitarbeitern wird Opfer eines Ransomware-Angriffs, der dazu führt, dass seine Systeme ganze 24 Tage ausfallen. Bei einem Arbeitstag von 8 Stunden beträgt die Anzahl der Ausfallstunden somit 192.

Wenn wir nun davon ausgehen, dass die Arbeitsleistung der gesamten Belegschaft während dieses Zeitraums von 192 Stunden beeinträchtigt wird und die durchschnittlichen Personalkosten pro Mitarbeiter und pro Stunde 50 $ betragen, könnten sich daraus folgende Kosten für den Produktivitätsverlust ergeben:

Die bewährten Verfahren und Renditebeispiele im Zusammenhang mit EDR wurden Ihnen von Stefanie Hammond, Head Nerd von N-able, nähergebracht.

Folgen Sie dem N-able Head Nerds-Team für Informationen zu bewährten Verfahren, Sicherheitsveranstaltungen und Bootcamps, mit denen Sie Ihr MSP-Business ausbauen können.

KOSTEN FÜR AUSFALLZEIT (192 STUNDEN) **1. Kosten für Mitarbeiterproduktivität** **Vom Ausfall betroffene Abteilungen:**	**ALLE**
Anzahl der Mitarbeiter im Unternehmen	40
Anzahl der Mitarbeiter in der betroffenen Abteilung	40
Durchschnittlicher Produktivitätsverlust in %	100 %
Durchschnittliche Personalkosten pro Stunde	50 $
Gesamtzahl der Ausfallstunden	192
Kosten für Mitarbeiterproduktivität	384.000,00 $

In Hinblick auf die Kosten für entgangene Einnahmen lässt sich folgende Rechnung aufstellen, wenn wir davon ausgehen, dass der Bruttojahresumsatz 1 Million USD und die effektive Anzahl der Werktage 240 (5 Tage pro Woche x 48 Wochen jährlich) beträgt und der gesamte Betrag der entgangenen Einnahmen unwiederbringlich verloren ist:

KOSTEN FÜR AUSFALLZEIT 2. Kosten für entgangene Einnahmen	
Bruttojahresumsatz	1.000.000,00 $
Anzahl der Werktage pro Jahr für das Unternehmen	240
Anzahl der täglichen Arbeitsstunden	8
Wie hoch ist der Anteil des unwiederbringlichen Geschäftsentgangs in %?	100 %
Täglicher Einnahmenentgang	4.166,67 $
Stündlicher Einnahmenentgang	520,83 $
Einnahmenentgang für die Dauer des Ausfalls	100.000,00 $

Wenn wir nun davon ausgehen, dass der durchschnittliche Stundensatz eines IT-Sicherheitstechnikers bei 150 $ liegt, lassen sich die Kosten für die Wiederherstellung folgenderweise berechnen:

KOSTEN FÜR AUSFALLZEIT (192 STUNDEN) 3. Wiederherstellungskosten	
Gesamtzahl der Arbeitsstunden bis zur vollständigen Wiederherstellung	192
Stundensatz für Wiederherstellungsdienste	150 $
Gesamtkosten für die Systemwiederherstellung (Wiederherstellungskosten)	28.800 $

Unter dem Strich können sich Gesamtkosten für die Ausfallzeit also aus den Produktivitätskosten der Mitarbeiter + entgangenen Einnahmen für die Dauer des Ausfalls + Wiederherstellungskosten zusammensetzen:

Gesamtkosten für Ausfallzeit	**512.800,00 $**
Gesamtkosten für Ausfallzeit/Stunde	**2.670,83 $**

Wenn wir die Kosten für immaterielle Güter wie oben beschrieben hinzurechnen, sind die Gesamtkosten eines Ransomware-Angriffs sogar noch wesentlich höher. Berücksichtigt man zusätzlich noch ein durchschnittliches Ransomware-Lösegeld in Höhe von 925.000 $, wie von Palo Alto berichtet, können die Kosten unter dem Strich die Grenze von 1 Million USD deutlich überschreiten.

Um die tatsächlichen Gesamtauswirkungen beurteilen zu können, muss das Unternehmen zusätzlich seine sonstigen immateriellen Kosten für sein spezielles Geschäftsfeld bewerten und sich unter anderem die folgenden Fragen stellen:

- Was passiert, wenn aufgrund des Angriffs verschiedene Projekte nicht geliefert werden können?
- Was, wenn das Unternehmen Kunden verliert?
- Wie hoch ist der Imageschaden?

Mit anderen Worten, wie könnte sich ein solches Ereignis auf die Tätigkeit des Unternehmens, seinen Ruf und schlussendlich auch auf sein Ergebnis auswirken? Die Gesamtauswirkungen umfassen die offensichtlichen und versteckten Kosten, die unter dem Strich anfallen, sowie alle durch Imageschaden, abwandernde Kunden und andere unvorhersehbare Schäden entstehenden zusätzlichen Kosten.

Wenn wir nun die im Beispiel oben angeführten Kosten mit den tatsächlichen Kosten für eine EDR-Lösung vergleichen, mit der die schlimmsten Auswirkungen eines Ransomware-Angriffs bekämpft werden können, ergeben sich beträchtliche jährliche Einsparungen.

4 Skizzieren Sie Ihre Lösung und Ihre zukünftigen Sicherheitspläne

Ihre globale Sicherheitslage ist nur so stark wie Ihr schwächstes Glied. Wenn Sie Ihren Kunden gestatten, ihre eigenen Sicherheits- und Schutzmaßnahmen basierend auf einem willkürlich vorgefassten Budget zu definieren, kann ein Angriff auf einen Ihrer Bestandskunden auch als Hintertür für einen Angriff auf Ihr MSP-Unternehmen dienen.

Bewährte Verfahren gebieten folgende Maßnahmen:

- Führen Sie ein Basisschutzprogramm ein und setzen Sie es bei allen Ihren Kunden durch. Die Cybersecurity-Landschaft wird zunehmend komplexer, daher können proaktive Lösungen wie EDR dabei helfen, sich vor den neuesten – bekannten und noch unbekannten – Cyberbedrohungen zu schützen. Solche Lösungen sollten als Basisschutz eingesetzt werden.
- Zeigen Sie Weitsicht und Fachwissen in Sicherheitsfragen – erläutern Sie Ihren Kunden Ihr Programm und animieren Sie sie dazu, es zu befolgen.

5 Wenn sie sich dann immer noch nicht überzeugen lassen, ziehen Sie eine klare Linie

Sie sind der Sicherheitsexperte für Ihre Kunden. Wenn eine Katastrophe eintritt, sind Sie derjenige, den sie um Hilfe bitten, um sie zu retten. Wenn sich Ihre Kunden nicht für das von Ihnen entwickelte Schutzprogramm entscheiden wollen, müssen sie auch die Verantwortung für die Konsequenzen tragen, die ihnen entstehen, wenn sie Ihre Ratschläge nicht befolgen.

Darüber hinaus sollten Sie sich eine Strategie überlegen, was Sie tun können, damit Ihre Kunden zu einem geringeren Risiko für Ihr Unternehmen werden. Ein Element dieser Strategie könnte beispielsweise ein neuer Dienstleistungs-Rahmenvertrag mit einer Klausel zur Haftungsbeschränkung oder Haftungsfreistellung sein, ein Risikoakzeptanzschreiben oder auch neue Service-Level-Ziele, die unterschiedliche Preise im Falle eines Ausfalls vorsehen, falls keine angemessene Deckung besteht.

Fazit

Während des Verkaufsprozesses den finanziellen Nutzen hervorzuheben ist wie ein Bild zu malen, das die Geschichte der Cybersicherheit erzählt. Die oben skizzierten Strategien sollten Ihnen dabei helfen, Ihre Gespräche klar zu umreißen und verständlich zu gestalten. Sie können Ihre Argumente zusätzlich untermauern, indem Sie positive Bewertungen und Erfolgsgeschichten weitergeben, die zeigen, wie andere Kunden von Ihren Serviceleistungen profitiert haben. Oder Sie sprechen über die exorbitanten Forderungen von Hackern bei kürzlich erfolgten Ransomware-Angriffen und zeigen Sie Statistiken, welche Kosten einem Unternehmen durch einen Ransomware-Angriff entstehen können, wenn es nicht angemessen geschützt ist. Alle Einzelheiten, die dazu beitragen, den Vertriebsprozess greifbarer zu gestalten, erhöhen die Seriosität des Gesprächs und verleihen Ihrem Unternehmen Glaubwürdigkeit.

Um die Ratschläge in diesem Leitfaden optimal umsetzen zu können, müssen Sie eine hervorragende Endpunktsicherheitslösung für Ihre Ansprechpartner im Programm haben.

Mehr erfahren

Weitere Informationen finden Sie unter
https://www.n-able.com/de/products/endpoint-detection-and-response.

Quellen

[1]https://www.n-able.com/de/resources/state-of-the-market-the-new-threat-landscape

[2]https://www.n-able.com/de/press/press-releases/n-able-partners-worldwide-say-goodbye-to-legacy-av-solutions-in-favor-of-sentinelone-edr-to-protect-over-1-million-customer-endpoints

[3]https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2022-97-million-records-breached

[4]https://www.sonicwall.com/de-de/2022-cyber-threat-report/

[5]https://www.ibm.com/security/data-breach

[6]State of the Market: The New Threat Landscape. Pushing MSP Security to the Next Level, N-able-Bericht, März 2022: https://www.n-able.com/de/resources/state-of-the-market-the-new-threat-landscape

[7]State of the Market: The New Threat Landscape. Pushing MSP Security to the Next Level, N-able-Bericht, März 2022: https://www.n-able.com/de/resources/state-of-the-market-the-new-threat-landscape

[8]https://blog.barracuda.com/2019/09/26/threat-spotlight-inefficient-incident-response/#:~:text=Inefficient%20incident%20response%20%E2%80%94%20Suspicious%20emails,click%20on%20a%20malicious%20link.

[9]Laut einem Bericht von Coveware aus dem Jahr 2022 beträgt die durchschnittliche Ausfallzeit 24 Tage: https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

[10]https://www.paloaltonetworks.com/blog/2022/06/average-ransomware-payment-update/#:~:text=The%20numbers%20are%20startling%3A%20The,rose%2071%25%20from%20last%20year

Über N-able

N-able bietet MSPs und IT-Serviceanbietern leistungsstarke Software zur Überwachung, Verwaltung und Absicherung von IT-Infrastrukturen und Netzwerken. Unser Angebot umfasst eine skalierbare Plattform, eine sichere Infrastruktur, Tools für die einfachere Verwaltung komplexer IT-Umgebungen und Ressourcen für die digitale Transformation. Wir unterstützen unsere Partner in jeder Wachstumsphase beim Schutz ihrer Kunden sowie beim Ausbau ihres Angebots – durch das ständig wachsende flexible Portfolio an Integrationen führender Anbieter. n-able.com/de