SOPHOS

Fünf gute Gründe für MDR-Services

Sophos-Whitepaper, September 2022

Einführung

Cyberbedrohungen nehmen stetig zu, werden komplexer und haben immer häufiger schwerwiegende Folgen. Unternehmen setzen daher vermehrt auf MDR-Services (Managed Detection and Response), um gefährliche Angriffe zu erkennen und zu bekämpfen. Denn Technologie-Lösungen allein können diese nicht verhindern. Gartner geht davon aus, dass bis 2025 50 % der Unternehmen MDR für Threat Monitoring, Detection and Response[1] einsetzen werden.

Angesichts der großen Auswahl an Abwehr-Lösungen auf dem Markt ist jedoch nicht immer offensichtlich, was MDR genau umfasst, wie sich MDR in Ihr Cybersecurity-Ökosystem einfügt und welche Vorteile ein MDR-Service bietet. Dieser Guide beantwortet diese Fragen und bietet praktische Tipps zur Wahl eines geeigneten MDR-Services.

Sophos MDR

Als Managed Detection and Response-Service, dem weltweit die meisten Kunden vertrauen, schützt Sophos MDR über 11.000[2] Unternehmen und Einrichtungen vor hochkomplexen Bedrohungen wie Ransomware. Mit Bestnoten von Gartner Peer Insights™[3] und der Auszeichnung als „Top Vendor" im Grid® 2022 von G2 für MDR-Services im Midmarket-Segment[4] ist Ihre Cyber-Abwehr bei Sophos MDR in den besten Händen.

Was MDR konkret umfasst

Um nachzuvollziehen, welche Vorteile MDR bietet und was sich hinter der wachsenden Nachfrage nach MDR-Services verbirgt, ist es wichtig, zu verstehen, was MDR ist – und was nicht.

Managed Detection and Response (MDR) ist ein 24/7 Fully-Managed Service durch ein Team von Sicherheitsexperten, das darauf spezialisiert ist, Cyberangriffe zu erkennen und zu bekämpfen, die Technologie-Lösungen alleine nicht verhindern können.

MDR sollte nicht mit EDR (Endpoint Detection and Response) oder XDR (Extended Detection and Response) verwechselt werden. Alle drei Lösungen unterstützen zwar Threat Hunting , und EDR- und XDR-Tools ermöglichen Analysten, nach potenziellen Kompromittierungen zu suchen und diese zu analysieren. Doch nur bei MDR-Services umfasst das Leistungsangebot die Bedrohungssuche, -analyse und -beseitigung durch Analysten eines Sicherheitsanbieters, die diese Aufgaben in Ihrem Auftrag für Sie übernehmen.

Wie der Name vermuten lässt, nutzen EDR-Tools ausschließlich Datenpunkte von Endpoint-Protection-Technologien. XDR-Tools hingegen beziehen ihre Datenquellen aus der weiteren IT-Umgebung (einschließlich Firewall-, E-Mail-, Cloud- und mobile Sicherheitslösungen) und bieten somit maximale Transparenz. Bei Sophos greifen wir zur Bereitstellung unseres MDR-Services auf unsere branchenführenden EDR- und XDR-Lösungen zurück.

Die tägliche Cybersecurity-Verwaltung, wie die Bereitstellung Ihrer Sicherheitstechnologien, die Aktualisierung von Richtlinien, die Anwendung von Patches oder die Installation von Updates, sind nicht Teil des MDR-Service. Managed Service Provider (MSPs) bieten entsprechende IT Security Management Services für Unternehmen und Einrichtungen, die Unterstützung in diesem Bereich benötigen.

Wer MDR-Services nutzt

MDR-Services werden von Unternehmen und Einrichtungen in allen Branchen genutzt – von kleinen Unternehmen mit begrenzten IT-Ressourcen bis hin zu Großkonzernen mit eigener SOC-Abteilung. Aber wie genau funktioniert hier die Zusammenarbeit? Es gibt drei wesentliche Reaktions-Modelle im Rahmen von MDR:

- Das MDR-Team verwaltet die Reaktion auf Bedrohungen komplett für den Kunden
- Das MDR-Team arbeitet mit dem IT-Team des Kunden zusammen und koordiniert gemeinsam die Reaktionsmaßnahmen
- Das MDR-Team benachrichtigt das IT-Team des Kunden und gibt Hilfestellung bei der Behebung

Bei Sophos unterstützen wir alle drei Modelle und passen diese bei Bedarf an die individuellen Kundenanforderungen an.

1 Gartner Market Guide for MDR 2021
2 Stand: August 2022.
3 Bewertungen der letzten 12 Monate (Stand: 1. August 2022). Gartner Peer Insights geben die subjektiven Meinungen einzelner Enduser wieder, die auf deren eigenen Erfahrungen mit den auf der Plattform aufgeführten Anbietern basieren. Sie sind in keinem Fall als Tatsachenfeststellung zu werten und repräsentieren nicht die Ansichten von Gartner oder seinen verbundenen Unternehmen. Gartner befürwortet in dieser Publikation keine bestimmten Hersteller, Produkte oder Dienstleistungen und übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus.
4 Sophos wurde im Grid® 2022 von G2 in der Kategorie MDR-Services für den Midmarket als Top Vendor eingestuft.

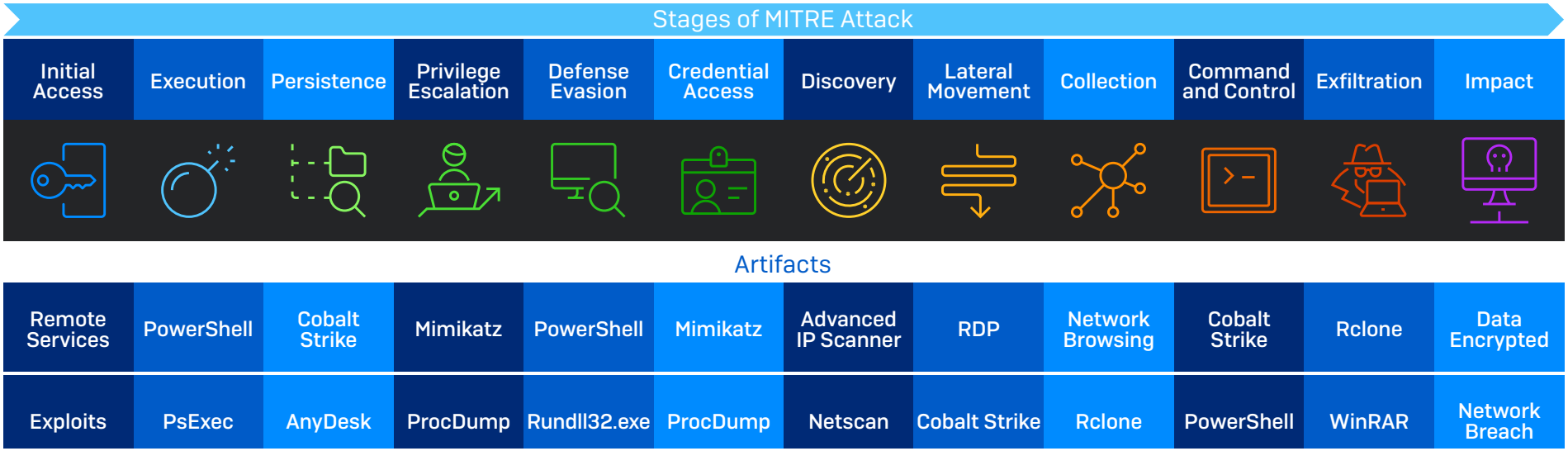
Warum Threat Detection and Response durch Experten unerlässlich ist

Die Realität zeigt uns, dass Technologie-Lösungen allein nicht jeden Cyberangriff verhindern können. Denn um von Cybersecurity-Lösungen unerkannt zu bleiben, zweckentfremden Angreifer zunehmend legitime IT-Tools, bedienen sich gestohlener Anmeldeinformationen und Zugriffsberechtigungen und nutzen ungepatchte Schwachstellen aus. Indem sie autorisierte Benutzer nachahmen und sich Sicherheitslücken in der Abwehr von Unternehmen zunutze machen, können Angreifer automatisierte Erkennungstechnologien überlisten.

Die Abbildung unten zeigt die wichtigsten Artefakte (Tools), die von Angreifern in jeder Phase der MITRE ATT&CK Chain verwendet wurden (basierend auf den Erfahrungen von Sophos Threat Huntern im Jahr 2021). Wie Sie sehen, werden von IT-Abteilungen regelmäßig genutzte Programme wie PowerShell, PsExec und RDP häufig von Angreifern missbraucht. Automatisierte Technologien haben Schwierigkeiten, zwischen IT-Mitarbeitern, die diese Programme berechtigterweise nutzen, und Angreifern zu unterscheiden, die legitime Tools mithilfe gestohlener Anmeldeinformationen ausnutzen.

Um solche komplexen „Living-off-the-Land"-Angriffe zu stoppen, ist es erforderlich, Technologien und menschliches Know-how miteinander zu verbinden. Jedes Mal, wenn ein Angreifer eine Aktion ausführt, erzeugt er ein Signal. Durch die Kombination menschlicher Expertise und leistungsstarken Schutztechnologien sowie modernsten KI-basierten Machine-Learning-Modellen können Sicherheitsanalysten selbst hochkomplexe, von Hackern manuell gesteuerte Angriffe erkennen, analysieren und beseitigen, um Datenverstöße zu verhindern.

Theoretisch können Threat Hunting, Analyse und Reaktion ausschließlich intern mit EDR- und XDR-Tools geleistet werden. Der Einsatz eines MDR-Services, entweder parallel zu Ihrem internen Team oder als vollständig ausgelagerte Service-Leistung, bietet jedoch zahlreiche Vorteile.



In den einzelnen Phasen der MITRE-Angriffskette am häufigsten genutzte Artefakte; *Quelle: Active Adversary Playbook 2022, Sophos*

Schutztechnologien spielen bei heutigen Abwehrmaßnahmen weiterhin eine wichtige Rolle

Von Experten manuell gesteuerte Erkennungs- und Reaktionsmaßnahmen sind mittlerweile wesentlicher Bestandteil der Cyberabwehr. Trotzdem spielen hochwertige Schutztechnologien für Endpoints, Netzwerke, E-Mails und Cloud weiterhin eine wichtige Rolle bei der Abwehr heutiger Bedrohungen – und die richtigen Lösungen können die Wirksamkeit eines MDR-Services erhöhen:

- Automatisierte Schutztechnologien ermöglichen es Abwehrspezialisten, der ständig wachsenden Zahl von Angriffen auch dann einen Schritt voraus zu bleiben, wenn Angreifer Automatisierung, KI und Malware-as-a-Service nutzen, um ihre Bedrohungen zu verbreiten. Sophos Endpoint Protection blockiert 99,98 % der Bedrohungen automatisch, bevor Schaden entsteht.
- Eine der größten praktischen Herausforderungen, mit der Threat Hunter zu kämpfen haben, ist die Flut irrelevanter Informationen: Sie erhalten so viele Signale, dass es schwierig sein kann, den Wald vor lauter Bäumen zu sehen. Moderne Abwehrtechnologien reduzieren die Anzahl der Warnmeldungen, die manuell von Analysten untersucht werden müssen. Weil sich Threat Hunter auf weniger und zugleich genauere Erkennungen konzentrieren können, beschleunigen hochwertige Abwehrtechnologien die Reaktion auf Bedrohungen durch Experten.
- Analysten nutzen Erkennungen und Signale von Abwehrtechnologien, um verdächtige Aktivitäten zu identifizieren und zu analysieren. Je höher die Qualität der Erkennungen und je umfangreicher der Kontext, desto schneller und besser die Analyse und Reaktion.

Vor diesem Hintergrund werfen wir nun einen Blick auf die fünf wichtigsten Vorteile, von denen Unternehmen und Einrichtungen beim Einsatz von MDR-Services berichten.

1. Sie verbessern Ihre Cyberabwehr

Einer der Hauptvorteile von MDR-Services gegenüber unternehmenseigenen Security-Operations-Programmen ist der erhöhte Schutz vor Ransomware und anderen komplexen Cyberbedrohungen.

Außerdem profitieren Sie vom weitreichenden Erfahrungsschatz der Analysten des MDR-Anbieters, die sich im Gegensatz zu einzelnen Unternehmen fortlaufend mit verschiedensten Angriffen befassen müssen. So verfügen sie über weitreichende Kenntnisse, die sich interne IT-Teams kaum aneignen können.

MDR-Teams untersuchen zudem täglich Vorfälle und reagieren permanent auf Bedrohungen, sodass sie über viel mehr Routine bei der Bedrohungssuche verfügen. So können sie in allen Phasen des Prozesses schneller und genauer reagieren – vom Erkennen wichtiger Signale bis hin zum Analysieren potenzieller Vorfälle und Beseitigen schädlicher Aktivitäten.

Die Arbeit in einem großen Team ermöglicht es Analysten zudem, ihr Wissen und ihre Kenntnisse auszutauschen, was wiederum ihre Reaktion beschleunigt. Das Sophos MDR-Team stellt für jede Bedrohung und jeden einzelnen Angreifer, auf den sie stoßen, sogenannte „Runbooks" zusammen. Sobald im Zuge einer Analyse ein Angreifer identifiziert wird, kann unser Team sich direkt auf das Runbook beziehen und sofort Gegenmaßnahmen ergreifen, anstatt während des Angriffs umfangreiche Untersuchungen anstellen zu müssen.

Die Runbooks werden kontinuierlich aktualisiert. Dabei erfassen die Analysten zu jedem Projekt wichtige Informationen, u. a.:

- Taktiken, Techniken und Prozesse (TTPs), die häufig angewandt werden oder spezifisch für einen bestimmten Angriff oder Bedrohungsakteur sind
- Relevante IOCs (Indicators of Compromise)
- Bekannte Proof of Concepts für Exploits, die in Zusammenhang mit offenen Schwachstellen stehen
- Nützliche Threat-Hunting-Abfragen zur Bekämpfung eines bestimmten Angriffs oder Bedrohungsakteurs

Ein weiterer Vorteil von MDR-Services besteht darin, dass sicherheitsrelevante Erkenntnisse auch auf andere Kunden angewendet werden können, die dem gleichen Zielprofil entsprechen. So lassen sich ähnliche Angriffe in dieser Community verhindern. Beispiele für Situationen, in denen das Sophos MDR-Team proaktiv die IT-Umgebungen von Kunden untersucht:

- Ein Unternehmen aus einer bestimmten Branche wurde auf eine spezielle Art und Weise angegriffen.
- Sophos X-Ops liefert Informationen über einen schweren Angriff auf eine bestimmte Branche oder ein bestimmtes Unternehmensprofil.
- In der Sicherheitslandschaft hat sich ein Vorfall mit schwerwiegenden Folgen ereignet und wir möchten prüfen, ob Kunden von uns betroffen sind.

Sollten unsere Analysten verdächtige Signale erkennen, sind sie in der Lage, die Situation schnell zu untersuchen und zu beheben, was der betroffenen Gruppe eine gemeinschaftliche Immunität verschafft.

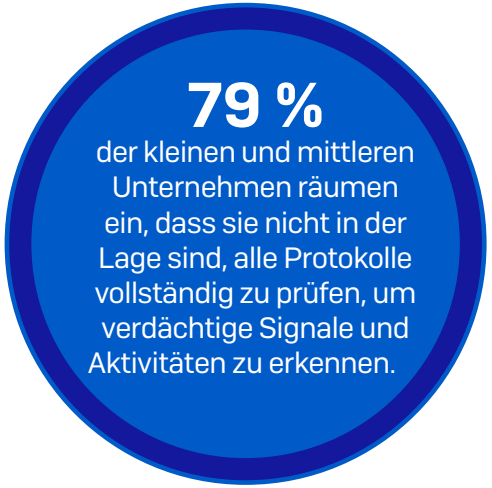
Dieser umfassende Erfahrungsschatz und die Fähigkeit, die bei einem Kunden gewonnenen Erkenntnisse auf alle Kundenumgebungen zu übertragen, ermöglichen dem Sophos MDR-Team, die Abwehr von Unternehmen und Einrichtungen in einem Maße zu verstärken, wie es einzelnen internen Security-Teams kaum möglich wäre.

2. Sie setzen IT-Kapazitäten frei

Threat Hunting ist zeitaufwändig und unvorhersehbar. IT-Experten, die mit mehreren Aufgaben und Prioritäten jonglieren, stoßen schnell an ihre Grenzen: 79 % der IT-Abteilungen räumen ein, dass sie nicht in der Lage sind, alle Protokolle vollständig zu prüfen, um verdächtige Signale und Aktivitäten zu erkennen[5].

Angesichts der potenziellen Auswirkungen eines Angriffs müssen Ihre Teams jedoch sofort alles stehen und liegen lassen, wenn verdächtige Aktivitäten beobachtet werden, damit die Bedrohung analysiert und umgehend bekämpft werden kann. Die Dringlichkeit der Arbeit führt daher dazu, dass sich Teams nicht mehr auf strategischere – und oft interessantere – Projekte konzentrieren können.

Die Zusammenarbeit mit einem MDR-Service ermöglicht Ihnen in diesem Fall, IT-Kapazitäten freizusetzen, um damit für Ihren Geschäftserfolg wesentliche Aufgaben voranzutreiben. Unternehmen, die Sophos MDR nutzen, berichten immer wieder von erheblichen IT-Effizienzsteigerungen, wodurch sie wiederum ihre Unternehmensziele besser erreichen können.



5 Unabhängige Befragung von 5.600 IT-Experten, Januar–Februar 2022. Im Auftrag von Sophos und unter der Leitung von Vanson Bourne.

3. Sie erhalten 24/7-Sorglos-Sicherheit

Da Angreifer rund um den Globus verteilt sind, können sie zu jeder Tages- und Nachtzeit zuschlagen. Angreifer sind besonders dann aktiv, wenn Ihre IT-Abteilung offline ist, z. B. abends, an Wochenenden und an Feiertagen. Bedrohungserkennung und -reaktion sind demzufolge eine 24-Stunden-Aufgabe und jedes Unternehmen, das diese Aktivitäten auf Bürozeiten beschränkt, geht ein hohes Risiko ein.

MDR-Services bieten einen 24/7-Schutz und sorgen so für die Gewissheit, dass zu jedem Zeitpunkt für Ihre Sicherheit gesorgt ist. Für IT-Abteilungen bedeutet dies buchstäblich, nachts besser schlafen zu können. Sie können die Verantwortung auf den MDR-Anbieter übertragen und ihre Zeit für persönliche Interessen zurückgewinnen.

Für Führungskräfte und Kunden bieten 24/7-Experten und ein hohes Maß an Cyber-Bereitschaft die starke Gewissheit, dass ihre Daten und das Unternehmen selbst gut geschützt sind.

4. Sie profitieren von mehr Expertise – ohne mehr Personal

Threat Hunting ist ein hochkomplexer Vorgang. Threat-Hunting-Experten müssen über ausgeprägte Spezialkenntnisse verfügen. Ein guter Threat Hunter zeichnet sich daher durch folgende Merkmale aus:

- **Kreativität und Neugier** – Threat Hunts gleichen nicht selten der Suche nach einer Nadel im Heuhaufen. Threat Hunter verbringen oft Tage damit, nach Bedrohungen zu suchen, und wenden dabei zahlreiche Methoden an.
- **Cybersecurity-Erfahrung** – Threat Hunting ist eine der komplexesten Aufgaben im Bereich Cybersicherheit. Daher sind Kenntnisse auf diesem Gebiet und Grundlagenwissen unerlässlich.
- **Kenntnis der Bedrohungslandschaft** – zur erfolgreichen Identifizierung und Beseitigung unbekannter Bedrohungen ist ein Verständnis der neuesten Bedrohungstrends das A und O.
- **Angreifer-Denkweise** – die Fähigkeit, wie ein Hacker zu denken, ist zur Bekämpfung heutiger aktiv gesteuerter Angriffe unentbehrlich.
- **Technische Schreibfähigkeit** – Threat Hunter müssen alle Ergebnisse im Rahmen des Analyseprozesses protokollieren. Daher ist die Fähigkeit, komplexe Informationen zu kommunizieren, entscheidend, um die Bedrohungssuche bis zu ihrem Abschluss ordnungsgemäß zu dokumentieren.
- **Betriebssystem- und Netzwerk-Kenntnisse** – fortgeschrittene praktische Kenntnisse in beiden Bereichen sind von entscheidender Bedeutung.
- **Programmier-/Skripterfahrung** – erforderlich, damit Threat Hunter Programme erstellen, Aufgaben automatisieren, Protokolle analysieren und Datenanalysen durchführen können, die sie bei ihren Untersuchungen unterstützen und voranbringen.

Leider ist diese Kompetenzkombination in der IT-Branche rar gesät , sodass es für viele Unternehmen und Einrichtungen schwierig – wenn nicht fast unmöglich – ist, entsprechend qualifizierte Threat-Hunting-Experten anzuwerben.

MDR-Services liefern Ihnen dieses Know-how als Service-Leistung. Bei Sophos haben wir Hunderte von erfahrenen Analysten, die unseren Kunden auf der ganzen Welt MDR-Services bieten. Mit Sophos MDR können Kunden Ihre Security Operations ohne zusätzliches Personal aufstocken.

5. Sie steigern Ihren Cybersecurity ROI

Ein 24/7 verfügbares Team von Threat Huntern ist teuer. Um eine 24-Stunden-Abwehr zu gewährleisten, benötigen Sie mindestens fünf oder sechs Cybersecurity-Mitarbeiter, die in separaten Schichten arbeiten. Dank MDR-Services wird dieser Schutz durch die Nutzung von Skaleneffekten weit günstiger, sodass Sie mehr für Ihr Cybersecurity-Budget erhalten.

Außerdem erhöhen MDR-Services Ihren Schutz, wodurch Sie Ihr Risiko für kostspielige Datenschutzverletzungen und Bereinigungsmaßnahmen senken. Wenn man berücksichtigt, dass die Behebung eines Ransomware-Angriffs in mittleren Unternehmen im Jahr 2021 durchschnittlich 1,4 Mio. US-Dollar kostete[6], sind Investitionen in Präventionsmaßnahmen eine kluge finanzielle Entscheidung.

Wenn Sie sich für einen MDR-Anbieter entscheiden, dessen Portfolio auch Endpoint- und andere Cybersecurity-Lösungen beinhaltet, können Sie zudem Konsolidierungsvorteile nutzen und Ihr Vendor Management optimieren, wodurch Sie Ihre Gesamtkosten erheblich senken.

Und schließlich können Sie durch die Wahl eines Anbieters, der sich in Ihre bestehenden Sicherheitstechnologien integrieren lässt, den Return on Investment Ihrer vorhandenen Lösungen steigern. Bei Sophos verfolgen wir einen anbieterunabhängigen MDR-Ansatz. Bei Bedarf können Sie also auch „Threat Detection, Investigation and Response"-Produkte anderer Anbieter weiter nutzen und auf diese Weise bestehende Investitionen optimal ausschöpfen. Mit Sophos MDR können Sie unsere erstklassigen Tools von Sophos, Lösungen von anderen Anbietern oder eine Kombination aus beidem verwenden.

6 Ransomware-Report 2022, Sophos. Unabhängige Befragung von 5.600 IT-Experten aus 31 Ländern

Was Sie bei der Wahl eines MDR-Services beachten sollten

MDR-Services unterscheiden sich von Anbieter zu Anbieter. Beim Vergleich verschiedener MDR-Services gilt es mehrere Aspekte zu berücksichtigen – beachten Sie insbesondere die vier folgenden Punkte:

1. **Angebotene Support- und Interaktionsebenen**

   Möchten Sie, dass der MDR-Anbieter Ihre Reaktion auf Bedrohungen vollständig für Sie verwaltet, die Reaktion auf Bedrohungen gemeinsam mit Ihrem Team leistet oder Ihr Team nur benachrichtigt, damit Sie selbst Maßnahmen ergreifen können? Entscheiden Sie, wie viel Support und Interaktion Sie sich von Ihrem MDR-Anbieter wünschen, und vergleichen Sie die Angebote der einzelnen Anbieter.

   Bei Sophos fungieren wir als Erweiterung der IT-Abteilungen unserer Kunden – dabei entscheidet der Kunden über Art und Weise und Umfang der Unterstützung. Vom vollständig verwalteten 24/7-Support bis hin zur gezielten Ergänzung interner Security-Teams – wir bieten individuell auf Ihre Bedürfnisse zugeschnittene Service-Leistungen.

2. **Breite und Tiefe der Fachkompetenz**

   Ein umfassenderer Erfahrungsschatz auf dem Gebiet der Bekämpfung von Cyberbedrohungen führt zu besseren Abwehrmaßnahmen. Ermitteln Sie deshalb, auf wie viel Erfahrung die Analysten der einzelnen MDR-Anbieter zurückgreifen können, und wie sie kollektive Erkenntnisse auf die Gesamtheit aller Kundenumgebungen anwenden.

   Beleuchten Sie außerdem, wie tiefgehend die Sicherheitsexpertise des MDR-Teams eines Anbieters ist und wie hochwertig die kontextbezogenen Erkenntnisse sind, die Analysten zum Priorisieren und Analysieren von Warnmeldungen zur Verfügung stehen.

   Sophos MDR schützt weltweit über 11.000 Unternehmen und Einrichtungen in verschiedenen Branchen – u. a. dem Gesundheits-, Bildungs- und Finanzwesen, dem Einzelhandel, dem verarbeitenden Gewerbe, dem Technologie- und Dienstleistungssektor sowie Behörden. Durch diese umfassende Erfahrung können wir unseren Kunden einzigartigen Schutz bieten.

   Hinter Sophos MDR steht das Sophos X-Ops-Team. Mit mehr als 30 Jahren Malware-Expertise und weltweit führenden KI-Funktionen bietet Sophos X-Ops umfassende Daten und Analysen, die MDR-Agenten dabei unterstützen, Angriffe schnell zu erkennen und zu beseitigen.

3. **Kundenerfahrungen aus der Praxis**

   Ein effektiver MDR-Anbieter fungiert als Erweiterung Ihres eigenen Security-Teams – entscheiden Sie sich also für einen Anbieter, mit dem Sie auf lange Sicht eng zusammenarbeiten möchten. Sprechen Sie mit bestehenden Kunden über deren Erfahrungen und besuchen Sie unabhängige Bewertungsseiten, um Feedback von Kunden zu erhalten.

   Sophos MDR ist der am häufigsten und am besten bewertete MDR-Anbieter auf Gartner Peer Insights (Stand: 1. August 2022 mit einer durchschnittlichen Bewertung von 4.8/5*). Lesen Sie hier unabhängige Kundenrezensionen.

4. **Quantität und Qualität der Telemetriedaten**

   Angreifer setzen nicht auf einen einzigen, sondern auf mehrere Technologiepfade – genau das sollte auch Ihr MDR-Anbieter beim Threat Hunting tun. Je größer die Transparenz der Analysten in Ihrer Umgebung ist, desto besser können die Analysten schädliche Aktivitäten erkennen und darauf reagieren. Fragen Sie Anbieter nach ihren Sicherheitsintegrationen und wie weit sie Signale aus Ihrer gesamten IT-Umgebung integrieren können.

   Sophos MDR bietet umfassende Integrationen über den gesamten IT Stack hinweg, einschließlich nativer und Fremdanbieter-Integrationen mit Endpoint-, Netzwerk-, Cloud-, E-Mail- und Microsoft-365-Technologien. Unser anbieterunabhängiger Ansatz bietet unseren Analysten eine hohe Transparenz über die gesamte Kundenumgebung, was wiederum zu einer schnelleren Bedrohungserkennung, -analyse und -reaktion führt.

Zusammenfassung

Da sich Cyberbedrohungen unaufhaltsam weiterentwickeln, wird MDR für immer mehr Unternehmen jeder Größe unverzichtbar. Die Zusammenarbeit mit einem bewährten MDR-Anbieter bietet zahlreiche Vorteile – ganz gleich, ob Sie Ihr Threat Hunting komplett auslagern oder Ihre internen Services ergänzen und verbessern möchten:

1. Sie verbessern Ihre Cyberabwehr.
2. Sie setzen IT-Kapazitäten frei.
3. Sie erhalten 24/7-Sorglos-Sicherheit.
4. Sie profitieren von mehr Expertise – ohne mehr Personal.
5. Sie steigern Ihren Cybersecurity ROI.

Weitere Informationen zu Sophos MDR erhalten Sie bei Ihrem Sophos-Partner oder unter www.sophos.de/mdr

www.sophos.de/mdr

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2022-09-16 DE-WP (DD)

SOPHOS