SOPHOS

Managed Detection and Response (MDR) Services Buyers Guide

Nur wenige Unternehmen haben intern die richtigen Tools, Mitarbeiter und Prozesse, um ihr Sicherheitsprogramm effizient rund um die Uhr zu verwalten und sich gleichzeitig proaktiv vor neuen Bedrohungen zu schützen. Daher vertrauen immer mehr Unternehmen auf Managed Detection and Response (MDR) Services.

Laut Prognosen von Gartner[1] werden im Jahr 2025 die Hälfte aller Unternehmen MDR-Services nutzen. Zum Vergleich: 2019 lag der Anteil noch unter 5 %.

Für viele Unternehmen ist der Security-Service-Markt allerdings noch Neuland und überzogene Werbeversprechen und Fachjargon sorgen für Verwirrung. Daher fällt es Unternehmen oft schwer, eine fundierte Entscheidung zu treffen. In unserem Buyers Guide fassen wir die zentralen Punkte zusammen, die es bei der Auswahl eines MDR-Anbieters zu beachten gilt. Zudem zeigen wir Ihnen, wie verschiedene MDR-Anbieter im Direktvergleich abschneiden.

IT-Security-Abteilungen benötigen spezialisierte Fachkräfte

Gegenwärtig verzeichnet die Cybersecurity-Branche einen enormen Fachkräftemangel. Dementsprechend fällt es Unternehmen auch schwer, handlungsfähige Security Operations (SecOps) aufzubauen, um Bedrohungen zu erkennen, zu analysieren und darauf zu reagieren, bevor Schaden entsteht.

Tools wie EDR unterstützen Unternehmen zwar bei der Suche nach Bedrohungen und der Reaktion auf Sicherheitsvorfälle. Die Tools lassen sich jedoch nur mit spezialisierten Fachkräften in vollem Umfang nutzen. Bei einer Umfrage unter 2.300 IT-Experten im Jahr 2019 [2] gaben 54 % der Befragten an, dass es ihnen an den nötigen Fachkräften fehle und sie deshalb ihre „EDR-Lösung nicht optimal nutzen" konnten.

Dieses Problem ist weit verbreitet: Laut Angaben der Analystenfirma ESG[3] fehlen 34 % aller Unternehmen Fachkräfte, um bei einem Angriff auf einen Endpoint die Ursache und die Angriffskette zu ermitteln.

Wie können Unternehmen dem rasanten Anstieg an zunehmend komplexen Bedrohungen Herr werden, ohne massiv in IT-Security-Personal zu investieren? Durch den Einsatz von Managed Security Services. Genauer gesagt: Managed Detection and Response (MDR) Services.

Was sind Managed Detection and Response Services?

Bei Managed Detection and Response (MDR) Services lagern Unternehmen den Sicherheitsbetrieb an externe Experten aus. MDR-Anbieter übernehmen dabei Aufgaben der IT-Security-Abteilung ihrer Kunden. Zu den Serviceleistungen gehören Analysen durch ein Expertenteam, Bedrohungssuche (Threat Hunting), Überwachung in Echtzeit sowie die Reaktion auf Vorfälle, kombiniert mit Technologien zum Erfassen und Analysieren von Bedrohungsdaten.

MDR-Anbieter nutzen oft eine Kombination aus Host- und Network-Layer-Technologien sowie umfassende Analysen, Bedrohungsdaten, forensische Daten und menschliche Expertise, um Bedrohungen schnell zu erkennen und zu beseitigen. Ziel dabei ist das Aufspüren und Stoppen von Bedrohungen in Kundenumgebungen, die von präventiven Sicherheitslösungen nicht erkannt wurden. Diese Lösungen – wie etwa Firewalls, Virenschutz und Inhaltsfilterung – können bekannte, gängige Bedrohungen abwehren. Sie bieten jedoch keinen verlässlichen Schutz gegen neue, komplexe Cyberangriffe. MDR-Anbieter schließen diese Lücke mit der sogenannten „Threat Detection and Response".

Warum entscheiden sich Unternehmen für einen MDR-Service?

Kunden greifen vor allem aus den folgenden Gründen auf MDR-Services zurück:

- **Begrenzte IT-Security-Ressourcen:** In vielen Unternehmen beschränkt sich die IT-Security-Strategie auf präventive Maßnahmen, da es an den erforderlichen Ressourcen zum Aufbau umfassender SecOps-Programme mangelt.
- **Keine effiziente Nutzung von EDR-Tools:** Manche Unternehmen haben bereits in EDR-Lösungen investiert, um bei einem Vorfall reagieren zu können oder um proaktiv nach Bedrohungen zu suchen und sie zu stoppen. Sie können jedoch intern kein umfassendes SecOps-Programm aufbauen und benötigen deshalb Unterstützung durch externe Experten.
- **Erweiterung der vorhandenen SecOps:** Selbst Unternehmen mit internen Bedrohungsexperten haben Mühe, ihre Security-Abteilung rund um die Uhr zu besetzen (nachts, an Wochenenden und Feiertagen). Oft fehlt es zudem an Spezialisten (beispielsweise für die Malware-Analyse oder die Reaktion auf Vorfälle). Manche Unternehmen wiederum lagern SOC-Aufgaben an externe Anbieter aus, damit sich die interne IT-Abteilung auf andere Bereiche konzentrieren kann.
- **Doppelte Kontrolle:** Da vier Augen bekanntlich mehr sehen als zwei, setzen selbst Unternehmen mit internen Security Operations Centern auf zusätzliches externes Monitoring ihrer Umgebung.

Die Vorteile von MDR-Services

Rund um die Uhr verfügbares Expertenteam

Ein guter MDR-Service besitzt die nötige Expertise zum Erkennen und Stoppen aller Arten von Angriffen. Er hat die entsprechenden Fachkräfte, die auf dem Personalmarkt bekanntermaßen Mangelware sind, und ist rund um die Uhr verfügbar. Das bedeutet, diese Experten überwachen Ihre Umgebung lückenlos und können zu jeder Zeit auf Bedrohungen reagieren, also auch an Wochenenden, Feiertagen und nachts. Die Zusammenarbeit mit einem guten MDR-Service können Sie sich so vorstellen, als gäbe es in Ihrem Unternehmen ein großes, rund um die Uhr verfügbares Sicherheits-Team ohne krankheits- oder urlaubsbedingte Ausfallzeiten.

Mehr Handlungsspielraum für die IT

Die meisten Unternehmen schaffen es kaum, sich selbst um die Bedrohungssuche, Reaktion auf Vorfälle und Überprüfung der Systemintegrität zu kümmern. Durch das Auslagern von Detection-and-Response-Aufgaben ermöglichen sie es den internen IT-Mitarbeitern, sich auf andere Bereiche zu konzentrieren. Einige Unternehmen wiederum nutzen MDR-Services, um alltägliche Sicherheitsaufgaben auszulagern, damit die interne IT sich anderen Aufgaben und Projekten widmen kann.

Kosteneinsparungen

Unternehmen, die ihr eigenes SecOps-Programm implementieren möchten, erkennen schnell, wie schwierig sich der Aufbau eines Security Operation Centers (SOC) gestaltet. Selbst in kleinen und mittelständischen Unternehmen werden mindestens vier Cybersecurity-Analysten benötigt, um ein SOC rund um die Uhr, jeden Tag im Jahr zu besetzen. Größere Unternehmen benötigen noch mehr teure Fachkräfte. Darüber hinaus braucht es Teamleiter und IT-Engineers zur Anpassung und Wartung von Tools. Zu diesen Personalkosten kommen weitere Kosten hinzu für Tools, die das Team zum Arbeiten benötigt, z. B. Endpoint Protection, Network Protection, Endpoint Detection and Response (EDR), SIEM, SOAR, Datenfeeds usw.

Verlässlicher Schutz

Bei einem guten MDR-Service haben Sie die Gewissheit, dass ein Expertenteam Ihre Systeme rund um die Uhr überwacht, nach Bedrohungen sucht, verdächtige Aktivitäten prüft und auf potenzielle Vorfälle reagiert. Ein dediziertes Team von Bedrohungsexperten sorgt für Schutz, auf den Sie sich verlassen können.

Auswahl eines MDR-Anbieters: Fragen, die Sie stellen sollten

Allgemeine Kriterien

Wie viele Kunden nutzen den MDR-Service?

MDR-Anbieter unterscheiden sich unter anderem in ihrer Erfahrung bem Erkennen und Reagieren auf Bedrohungen. Die aktuelle Kundenzahl gibt Ihnen nicht nur Aufschluss darüber, wie viele Unternehmen dem MDR-Anbieter vertrauen, sondern zeigt auch, wie gut der Anbieter auf eine breite Palette an verdächtigen Aktivitäten reagieren kann. Achten Sie darauf, dass der Anbieter Erfahrung in der Zusammenarbeit mit Unternehmen hat, die Ihrem Unternehmen ähnlich sind (Größe, Branche, Sicherheitsanforderungen).

Was umfasst der Service? Ist Threat Response inbegriffen?

Die MDR-Services der verschiedenen Anbieter beinhalten teilweise sehr unterschiedliche Leistungen. Immer mehr MDR-Kunden wünschen sich, dass MDR-Anbieter im Kundenauftrag gezielte Maßnahmen ergreifen, um Bedrohungen unschädlich zu machen, anstatt nur über aktive Bedrohungen zu informieren. Doch nur wenige MDR-Services bieten diese Option an. Das Gros der Anbieter konzentriert sich vornehmlich oder ausschließlich auf das Erkennen von Bedrohungen und das Benachrichtigen der Kunden. Sämtliche Reaktions- und Bereinigungsmaßnahmen bleiben dem Kunden überlassen. Bei effektiven MDR-Services analysieren Sicherheitsexperten potenzielle Bedrohungen methodisch, minimieren False Positives, bekämpfen bestätigte Bedrohungen und unterstützen Unternehmen mit genauen Informationen und Empfehlungen bei der Verbesserung ihres allgemeinen Sicherheitsstatus.

Ist der Service rund um die Uhr verfügbar? Wer reagiert auf Vorfälle an einem Sonntag um 2 Uhr morgens?

Achten Sie darauf, dass der MDR-Anbieter Ihre Umgebung wirklich lückenlos überwacht und rund um die Uhr auf Vorfälle reagieren kann.

Welche Technologien nutzt der MDR-Service? Sind diese im Preis inbegriffen?

Bei der Auswahl eines MDR-Service gilt es zu ermitteln, ob die genutzte Technologie im Kaufpreis inbegriffen ist. Bei manchen Anbietern müssen Sie nämlich Ihre eigenen Tools (z. B. Endpoint Protection und EDR) separat erwerben. Andere Anbieter bieten die gesamte Technologie zusätzlich zur Service-Komponente.

Ist der Service proaktiv oder reaktiv?

Bei MDR geht es um proaktives Handeln. Anders als IT-Forensik und Incident Response Services, die in der Regel zur Unterstützung von Kunden dienen, wenn ein Krisenfall bereits eingetreten ist (z. B. bei Sicherheitsvorfällen oder Datenpannen), bietet MDR einen rund um die Uhr proaktiven Service. Dabei werden Kundenumgebungen kontinuierlich auf verdächtige Aktivitäten überwacht. Kommt es zu einem Vorfall, erhalten Kunden in Echtzeit Hilfe.

Wie kommunizieren Sie mit dem MDR-Team?

Informieren Sie sich darüber, wie Sie mit dem Anbieter in Kontakt treten können. Können Sie anrufen? Können Sie per E-Mail kommunizieren? Kommunizieren Sie direkt mit einem Security-Analysten oder mit einem anderen Ansprechpartner (z. B. einem Account Manager)? Die Unterschiede zwischen den MDR-Anbietern sind hier oft sehr groß: Bei einigen Anbietern können sich Kunden direkt an einen Ansprechpartner wenden, bei anderen erfolgt die Kommunikation über ein Portal. Egal, wie die Kommunikation erfolgt: MDR-Anbieter sollten zu jedem Fall eine Zusammenfassung liefern, damit Ihr Team weiß, welche Bedrohungen erkannt wurden und welche Maßnahmen noch ergriffen werden müssen.

Vorgehensweise und Effizienz

Wie geht der MDR-Anbieter im Bereich „Threat Detection and Response“ (TDR) vor?

MDR-Anbieter müssen über eine klare TDR-Strategie verfügen. Andernfalls ist der Service nur bedingt skalierbar und verdächtige Aktivitäten in Kundenumgebungen werden möglicherweise nicht erkannt.

Wie schnell reagiert der Service?

In der IT-Security geht es um Sekunden. Die folgenden Kennzahlen von MDR-Anbietern sind in diesem Zusammenhang relevant:

- Durchschnittliche Zeit bis zur Erkennung
- Durchschnittliche Zeit bis zur Reaktion
- Durchschnittliche Zeit bis zur Behebung

Welche Leistungen bietet der MDR-Service genau? Können in Ihrem Auftrag Maßnahmen ergriffen werden?

Lassen Sie sich erklären, wie der MDR-Anbieter vorgeht, wenn verdächtige Aktivitäten erkannt werden. Wie bereits erläutert, erhalten Sie bei vielen MDR-Services nur eine Überwachung Ihrer Umgebung und eine Benachrichtigung, wenn eine verdächtige Aktivität bemerkt wurde. Im Idealfall kann der MDR-Anbieter jedoch auch Maßnahmen in Ihrem Auftrag ergreifen, und bei Bedrohungen erfolgt eine proaktive Reaktion durch Experten und nicht nur eine automatisch Abwehr durch ein Tool.

Ist die Bedrohungssuche indizienbasiert (Reaktion auf Warnhinweise), indizienlos (Suche nach Angriffsindikatoren auch ohne konkrete Hinweise) oder beides?

Threat Hunting ist nicht gleich Threat Hunting. Obwohl Threat Hunting definitionsgemäß eine menschliche Komponente voraussetzt, deklarieren manche Anbieter automatische, maschinelle Benachrichtigungen (fälschlicherweise) als Threat Hunting. Ein wichtiger Aspekt ist zudem die Frage, ob der MDR-Anbieter proaktiv nach Bedrohungen sucht, selbst wenn keine konkreten Hinweise auf verdächtige Aktivitäten oder Vorfälle vorliegen. Fragen Sie nach, bei welchen Aktivitäten eine Bedrohungsanalyse durchgeführt wird.

Welche Datenquellen sorgen für Transparenz? Beschränkt sich der Service auf verwaltete EDR?

Die Einblicke mancher MDR-Anbieter beschränken sich auf Endpoints. Zwar sind Endpoint-Daten sehr wichtig, doch sie alleine reichen nicht aus. Um echte MDR-Services handelt es sich in diesen Fällen nicht, sondern eher um „Managed EDR“-Lösungen. Diese bieten nur eine begrenzte Transparenz über Bedrohungen, die sich möglicherweise in Ihrer Umgebung befinden.

Verfügt der MDR-Anbieter über Bedrohungsanalysten und hat Zugriff auf Bedrohungsdaten?

Die technische Expertise von MDR-Anbietern sollte über das Know-how hinausgehen, das Unternehmen sich in der Regel selbst aneignen können. Hierzu zählen natürlich auch Sicherheitsanalysten. Darüber hinaus sollte der MDR-Service auch Zugang zu Bedrohungsdaten haben und bei neuen Bedrohungen mit Bedrohungsforschern zusammenarbeiten.

Anbietervergleich

MDR-Anbieter lassen sich im Wesentlichen in drei Kategorien einteilen:

- **Nur Überwachung:** Hier liegt der Schwerpunkt auf Priorisierung und dem Benachrichtigen der Kunden, wenn ein Produkt einen automatischen Warnhinweis anzeigt. Kunden werden zwar beraten, wie sie reagieren sollen, weitere Maßnahmen werden jedoch nicht angeboten. Außerdem geschieht das Threat Hunting nur automatisiert, d. h. Bedrohungen werden nicht proaktiv für den Kunden analysiert oder aufgespürt.
- **Eingeschränkte Reaktion:** Es werden Reaktionsmaßnahmen angeboten, allerdings handelt es sich dabei nur um automatisierte Maßnahmen. Threat Hunting wird nur bei Warnhinweisen durchgeführt.
- **Umfassende Reaktion**: Hier werden umfassende Reaktionsmaßnahmen angeboten. Experten ergreifen im Auftrag des Kunden proaktiv manuelle Maßnahmen. Das Threat Hunting erfolgt nicht nur indizienbasiert. Stattdessen sucht das MDR-Team kontinuierlich nach Bedrohungen, auch wenn keine konkreten Angriffsindikatoren vorliegen.

Hauptfunktionen	Nur Überwachung	Eingeschränkte Reaktion	Umfassende Reaktion
24/7 Überwachung	✓	✓	✓
Priorisierung und Benachrichtigung	✓	✓	✓
Unterstützung bei Bereinigung	✓	✓	✓
Aktivitätsreports	✓	✓	✓
Automatisiertes Threat Hunting	✓	✓	✓
Automatisierte Reaktion		✓	✓
Indizienbasiertes Threat Hunting		✓	✓
Indizienloses Threat Hunting			✓
Reaktion durch Experten			✓

Entsprechende Anbieter[4]		
Nur Überwachung	Eingeschränkte Reaktion	Umfassende Reaktion
Carbon Black Managed Detection	Arctic Wolf	Sophos MTR Standard
CrowdStrike Falcon OverWatch	eSentire	Sophos MTR Advanced
Huntress	Expel	CrowdStrike Falcon Complete
Perch	Rapid7	
	Red Canary	
	SentinelOne Vigilance Respond	

Der MDR-Service von Sophos: Managed Threat Response (MTR)

Sophos Managed Threat Response (MTR) bietet 24/7 Managed Detection and Response mit Threat Hunting durch ein Expertenteam, als Fully-Managed-Service. Das Sophos MTR-Team informiert Sie nicht bloß über Angriffe und verdächtiges Verhalten, sondern ergreift für Sie gezielte Maßnahmen, um selbst hochkomplexe Bedrohungen unschädlich zu machen.

Unsere Experten übernehmen für Sie folgende Aufgaben:

- Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen und Vorfällen
- Nutzen aller vorliegenden Informationen, um Ausmaß und Schwere von Bedrohungen zu bestimmen
- Anwenden geeigneter Maßnahmen je nach Risiko-Bewertung der Bedrohung
- Einleiten von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen
- Bereitstellen konkreter Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen

Sophos MTR: Die wichtigsten Funktionen

Sophos MTR Standard

24/7 indizienbasiertes Threat Hunting

Bestätigte schädliche Artefakte und Aktivitäten (starke Signale) werden automatisch blockiert oder beendet. So können die Bedrohungsexperten ihre Suche auf Bedrohungen konzentrieren, für die Indizien vorliegen. Bei dieser Art der Bedrohungssuche werden kausale und angrenzende Ereignisse (schwache Signale) aggregiert und analysiert, um neue „Indicators of Attack (IoA)" und „Indicators of Compromise (IoC)" zu enttarnen, die bislang nicht erkannt werden konnten.

Security Health Check

Sorgen Sie dafür, dass Ihre Sophos-Central-Produkte – allen voran Intercept X Advanced with EDR – stets mit maximaler Performance arbeiten, indem Sie proaktive Untersuchungen Ihrer Betriebsbedingungen und empfohlene Konfigurations-Verbesserungen durchführen.

Aktivitätsreports

Zusammenfassungen der Aktivitäten jedes Falls ermöglichen eine Priorisierung und Kommunikation. So weiß Ihr Team, welche Bedrohungen erkannt und welche Reaktionsmaßnahmen in den jeweiligen Reporting-Zeiträumen ergriffen wurden.

Angriffserkennung

Die meisten erfolgreichen Angriffe beruhen auf der Ausführung eines Prozesses, der für Überwachungstools seriös erscheinen kann. Mithilfe selbst entwickelter Analyseverfahren ermittelt unser Team den Unterschied zwischen seriösem Verhalten und den Taktiken, Techniken und Prozessen (TTPs) von Angreifern.

Sophos MTR Advanced

24/7 indizienloses Threat Hunting

Mithilfe von Data Science, Threat Intelligence und der Intuition erfahrener Bedrohungsexperten kombinieren wir verschiedene Informationen (Ihr Unternehmensprofil, hochwertige Assets und Benutzer mit hohem Risiko), um das Verhalten von Angreifern vorherzusagen und neue Angriffsindikatoren (IoA) zu identifizieren.

Optimierte Telemetriedaten

Bedrohungsanalysen werden um Telemetriedaten von anderen Sophos-Central-Produkten ergänzt, die über die Endpoint-Ebene hinaus ein Gesamtbild der Angriffsaktivitäten liefern.

Proaktive Verbesserung des Sicherheitsstatus

Verbessern Sie Ihren Sicherheitsstatus und Ihre Abwehr proaktiv: Sie erhalten von uns Hilfestellung zur Behebung von Konfigurations- und Architektur-Schwachstellen, die sich negativ auf Ihre gesamte Sicherheit auswirken.

Dedizierter Ansprechpartner

Bei Bestätigung eines Vorfalls wird Ihnen ein dedizierter Ansprechpartner zugewiesen, der direkt mit Ihren internen und externen Mitarbeitern vor Ort zusammenarbeitet, bis die aktive Bedrohung neutralisiert wurde.

Direkter Telefon-Support

Ihr Team kann unser Security Operations Center (SOC) direkt telefonisch kontaktieren. Unser MTR-Team ist 24/7 erreichbar und wird von Support-Teams unterstützt, die weltweit auf 26 Standorte verteilt sind.

Asset-Erkennung

Von Asset-Informationen über Betriebssystem-Versionen, Anwendungen und Schwachstellen bis hin zur Identifizierung verwalteter und nicht verwalteter Assets: Wir liefern Ihnen wertvolle Detail-Informationen bei der Einschätzung von Folgen, während Bedrohungssuchen und als Teil proaktiver Empfehlungen zur Verbesserung des Sicherheitsstatus.

Sophos Managed Threat Response (MTR): Schutz, EDR und MDR			
Hauptfunktionen	Sophos Intercept X Advanced with EDR (nur Technologie)	Sophos MTR Standard (Technologie + Managed Service)	Sophos MTR Advanced (Technologie + Managed Service)
Endpoint Protection	✓	✓	✓
Endpoint Detection and Response (EDR) für IT Operations	✓	✓	✓
Endpoint Detection and Response (EDR) für Threat Hunting	✓	✓	✓
Managed Service: 24/7 Überwachung und Reaktion		✓	✓
Managed Service: Proaktive, manuelle Reaktion		✓	✓
Managed Service: Indizienbasiertes Threat Hunting		✓	✓
Managed Service: Erweitertes indizienloses Threat Hunting			✓
Managed Service: Dedizierter Ansprechpartner			✓

Sophos MTR: Die wichtigsten Unterscheidungsmerkmale

Wir handeln für Sie: Bei anderen MDR-Anbietern erhalten Sie nur eine Überwachung und eine Benachrichtigung, wenn verdächtige Aktivitäten erkannt werden. Das Sophos MTR-Team hingegen wird für Sie aktiv und ergreift Maßnahmen zum Stoppen, Eindämmen und Beseitigen selbst hochkomplexer Bedrohungen.

Spitzen-Expertise: Mit über 1.000 Kunden verfügen wir über die nötige Erfahrung: Wir haben bereits alle denkbaren Angriffe erlebt und erfolgreich gestoppt. Unser Team hochqualifizierter Bedrohungsexperten analysiert rund um die Uhr anomales Verhalten und ergreift Maßnahmen gegen Bedrohungen.

Robustes Threat Hunting: Wir führen indizienbasiertes und indizienloses Threat Hunting durch, um neue „Indicators of Attack (IoA)" und „Indicators of Compromise (IoC)" aufzuspüren, die bislang nicht erkannt werden konnten.

Verlässliche Erkennung: Wir nutzen nicht nur traditionelle Erkennungsmechanismen, sondern kombinieren deterministische und Machine-Learning-Modelle. Dadurch erkennen wir verdächtiges Verhalten sowie Taktiken, Techniken und Prozesse selbst der raffiniertesten Angreifer.

Gezielte Reaktion durch Menschen: Sophos MTR beinhaltet Intercept X Advanced with EDR, die branchenweit führende Endpoint Protection. Die Lösung stoppt automatisch Bedrohungen, die andere Anbieter nicht abfangen. Da diese umfassende, proaktive Abwehr im Service inbegriffen ist, kann sich unser Expertenteam auf komplexe Vorfälle konzentrieren und darauf reagieren.

Transparenz und Kontrolle: Mit Sophos behalten Sie die Entscheidungsgewalt: Sie kontrollieren, wie und wann potenzielle Vorfälle eskaliert werden, welche Maßnahmen wir ggf. einleiten sollen und wer über die einzelnen Schritte informiert wird. Unternehmen können zwischen unseren drei Reaktions-Optionen wählen (Benachrichtigung, Zusammenarbeit oder Autorisierung).

Outcome-Focused Security™: Jede Aktion bei der Bedrohungssuche, Analyse und Reaktion generiert entscheidungsrelevante Daten, mit denen Konfigurationen und automatische Erkennungsfunktionen optimiert werden.

Sophos MTR in Zahlen

Sophos Rapid Response

Sophos Rapid Response bietet Soforthilfe durch ein Expertenteam bei der Erkennung und Beseitigung aktiver Bedrohungen. Der Rapid-Response-Service richtet sich an Unternehmen, bei denen gerade ein Cyberangriff stattfindet. Sophos-MTR-Kunden benötigen den Rapid-Response-Service nicht, da die Reaktion auf Vorfälle als Serviceleistung in Sophos MTR inbegriffen ist.

Der Rapid-Response-Service liefert Soforthilfe bei aktiven Vorfällen. Das Onboarding beginnt binnen weniger Stunden und die Triage ist in der Regel nach 48 Stunden abgeschlossen.

Das Sophos Rapid-Response-Team besteht aus unterschiedlichen Experten, die rund um die Uhr per Remote-Zugriff auf Vorfälle reagieren, Bedrohungen analysieren und aufspüren:

- Schnelles Priorisieren, Eindämmen und Beseitigen aktiver Bedrohungen
- Entfernen von Angreifern aus Ihrer Umgebung, um weitere Schäden zu vermeiden
- 24/7 Überwachung und Reaktion, um Ihren Schutz zu optimieren
- Empfehlung von Präventiv-Maßnahmen in Echtzeit, um die Ursache zu bekämpfen
- Detaillierte Bedrohungs-Übersicht nach dem Vorfall mit Informationen zu unserer Vorgehensweise

Sophos Rapid Response steht sowohl Sophos-Kunden als auch Nichtkunden zur Verfügung.

Weitere Informationen zu Sophos MTR finden Sie auf unserer Produktseite. Natürlich können Sie sich auch jederzeit an einen Sophos-Ansprechpartner wenden.

Sie machen sich lieber selbst auf Bedrohungssuche? Sophos EDR bietet Ihnen die Tools, die Sie für erweitertes Threat Hunting und zur Aufrecherhaltung Ihres Sicherheitsstatus benötigen. Jetzt unverbindlich 30 Tage testen.

Quelle:

1 Gartner, Market Guide for Managed Detection and Response Services, 26. August 2020, Analysten: Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneider

2 Befragung von 3.100 IT-Managern, 2019 https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/uncomfortable-truths-of-endpoint-security.aspx

3 https://www.esg-global.com/blog/soapa-discussion-on-edr-and-xdr-with-jon-oltsik-and-dave-gruber-video-part-1

4 Der Vergleich sowie die Informationen im vorliegenden Dokument basieren auf der Auslegung zum Zeitpunkt der Verfassung des Vergleichs öffentlich verfügbarer Daten durch Sophos. Dieses Dokument wurde von Sophos und nicht von den anderen darin aufgeführten Anbietern erstellt. Änderungen der Eigenschaften und Funktionen der verglichenen Produkte, die direkten Einfluss auf die Richtigkeit und/oder Gültigkeit dieses Vergleichs haben können, sind vorbehalten. Die in diesem Vergleich enthaltenen Informationen sollen ein allgemeines Verständnis sachlicher Informationen zu verschiedenen Produkten vermitteln und sind möglicherweise nicht vollständig. Alle dieses Dokument verwendenden Personen sollten auf Basis ihrer Anforderungen ihre eigene Entscheidung treffen und sollten auch Originalinformationsquellen zu Rate ziehen und sich bei der Wahl eines Produkts nicht nur auf diesen Vergleich verlassen.

Weitere Informationen zu Sophos Managed Threat Response (MTR) unter:

www.sophos.de/mtr

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +44 (0)8447 671131
E-Mail: sales@sophos.de

14.09.2020 BG-DE (DD)