SOPHOS

MEHR CYBER-RESILIENZ FÜR MSPS MIT SOPHOS MANAGED THREAT RESPONSE (MTR)

Sophos-Whitepaper September 2020

Einleitung

Cyberattacken nehmen massiv zu, auch MSPs rücken verstärkt ins Blickfeld der Angreifer. Denn die Verbindungen zwischen MSPs und ihren zahlreichen Endkunden bieten Cyberkriminellen ein ideales Sprungbrett, über das sie gleich mehrere Ziele auf einen Schlag erreichen.

Von Staaten wie China bis hin zu kriminellen Gruppierungen wie GandCrab und REvil: Den Angreifern ist der Vertrauensverlust, den die gesamte MSP-Branche durch die Angriffe erleidet, sehr wohl bewusst. Die damit einhergehende existenzielle Bedrohung macht MSPs sogar zu einem noch attraktiveren Ziel. Jeden einzelnen Kunden darüber informieren zu müssen, dass der Ernstfall eingetreten ist, ist der Albtraum eines jeden MSPs. Denn schon ein einziger Vorfall kann das Vertrauen der Kunden erschüttern und das endgültige Aus für einen MSP bedeuten.

Dieser enorme Druck erhöht die Chancen eines Angreifers auf lukrative Lösegeldzahlungen noch zusätzlich und verstärkt den Anreiz, MSPs ins Visier zu nehmen. Siebenstellige Lösegeldforderungen sind keine Seltenheit. Manche Angreifer exfiltrieren Terabytes an Kundendaten und drohen, diese im Internet zu veröffentlichen, sollte das Lösegeld nicht gezahlt werden.

Umso wichtiger ist es daher für MSPs, nicht nur in Abwehrtechnologien für sich selbst und ihre Kunden zu investieren, sondern auch dafür zu sorgen, dass ausgereifte Detection-and-Response-Mechanismen vorhanden sind. So lassen sich Bedrohungen, die der Abwehr entgehen, rechtzeitig identifizieren und bekämpfen.

Mit Sophos Managed Threat Response (MTR) erhalten Sie umfangreiche Unterstützung durch ein Expertenteam, das sich ausschließlich der Bedrohungsbekämpfung widmet. Der Service bietet ein Rund-um-die-Uhr-Monitoring Ihrer verwalteten Assets, einschließlich Bedrohungssuche und -erkennung sowie Analyse von Vorfällen in Echtzeit. Wenn eine Bedrohung erkannt wird, reagiert das Sophos MTR-Team in Zusammenarbeit mit Ihrem Team oder ganz eigenständig in Ihrem Auftrag. Anstatt zu warten, bis eine Sicherheitspanne eintritt, und erst dann händeringend nach Unterstützung zu suchen, ist das Sophos MTR-Team bereits zur Stelle. Neue und aufkommende Bedrohungen können so rechtzeitig abgewehrt und in enger Zusammenarbeit mit Ihrem Unternehmen eingedämmt und eliminiert werden.

- Ihre eigene Verteidigung ist die beste Verteidigung für Ihre Kunden
- Zusammenspiel von Technologien, Experten und Prozessen
- Verstärkung Ihres Sicherheitsteams mit Response-Experten
- Rapid Response für den Ernstfall
- Transparenz über Endpoints, Netzwerke und Cloud hinweg
- Relevante Signale für eine effiziente Analyse

Ihre eigene Verteidigung ist die beste Verteidigung für Ihre Kunden

MSPs stehen immer wieder im Fadenkreuz professioneller Cyberbanden und müssen daher mindestens die gleichen Anstrengungen zu ihrer eigenen Verteidigung unternehmen wie für ihre Kunden.

Durch die Zusammenarbeit mit einem Service-Provider wie Sophos MTR können Sie als MSP Ihr Risiko deutlich reduzieren. Verstärken Sie Ihre eigenen Schutzmaßnahmen durch zusätzliche Transparenz und einen Managed Service zur Bedrohungsabwehr, inklusive Expertenteam. So machen Sie es selbst den raffiniertesten Angreifern praktisch unmöglich, Ihre Abwehr zu durchbrechen.

Zusammenspiel von Technologien, Experten und Prozessen

Um Cybersecurity-Vorfälle schnell zu erkennen und effektiv abwehren zu können, ist ein mehrschichtiger Ansatz erforderlich, bei dem Technologien, Experten und Prozesse optimal ineinandergreifen. Das NIST Cybersecurity Framework bietet hierfür ein Rahmenwerk, das aus fünf Kernfunktionen besteht: schützen, erkennen, reagieren, wiederherstellen, identifizieren. Für all diese Kernfunktionen gibt es Technologie-Lösungen, die bei der erfolgreichen Umsetzung helfen. Technologien allein können die Cybersecurity-Problematik jedoch nicht lösen.

Sophos MTR kombiniert Sophos-Technologien mit dem Know-how erfahrener Response-Experten und branchenführendem Machine Learning. Der MTR-Service umfasst unsere branchenführende Prevention-Technologie Intercept X Advanced mit einer breiten Palette an Schutz- und Erkennungsfunktionen für Ransomware, Exploits, dateilose und dateibasierte Malware, Angreiferverhalten, TTPs (Taktiken, Techniken und Prozesse) u.v.m. Ebenfalls enthalten ist Sophos EDR (Endpoint Detection and Response). Sophos EDR sammelt erweiterte System-Telemetriedaten, mit denen Bedrohungen und IT-Betriebsprobleme ermittelt werden können, und ermöglicht den Remote-Zugriff auf betroffene Systeme, um Vorfälle zu analysieren und darauf zu reagieren.

Verstärkung Ihres Sicherheitsteams mit Response-Experten

Die Reaktion auf Bedrohungen erfordert Erfahrung. Viele MSPs verfügen zwar über ausgereifte Security Operations, haben bisher jedoch nur wenige oder unwesentliche Vorfälle erlebt. Sophos MTR dient als virtuelle Erweiterung Ihres bestehenden Teams und unterstützt mit umfangreicher Erfahrung bei der Bedrohungserkennung und -bekämpfung.

Da Sophos MTR Bedrohungen aufspürt, sie analysiert und mit gezielten Maßnahmen unschädlich macht, kann sich Ihr Team strategisch wichtigeren Projekten widmen, die für das Wachstum und den Erfolg Ihres Unternehmens entscheidend sind.

Rapid Response für den Ernstfall

Für Kunden, die nicht bereits durch Sophos MTR geschützt sind, bietet Sophos Rapid Response einen blitzschnellen und kostengünstigen Service zum Erkennen und Beseitigen aktiver Bedrohungen. Bei einem Sicherheitsvorfall zählt jede Sekunde. Deshalb beginnt das Onboarding binnen weniger Stunden und die Triage ist in der Regel nach 48 Stunden abgeschlossen.

Egal, ob Sie Ihren eigenen Response-Service anbieten oder nicht – mit Sophos Rapid Response erhalten Sie Soforthilfe von Experten. So lassen sich selbst hochkomplexe Vorfälle schnell und effizient beheben.

Transparenz über Endpoints, Netzwerke und Cloud hinweg

Das Sprichwort „Eine Kette ist immer nur so stark wie ihr schwächstes Glied" lässt sich auch sehr gut auf Angriffe anwenden. Angreifer schlagen in den allermeisten Fällen dort zu, wo die Abwehrmaßnahmen eines Unternehmens am schwächsten sind. Dieser „Schwachpunkt" kann praktisch überall vorhanden sein oder entstehen. Es kann sich beispielsweise um einen falsch konfigurierten, Cloud-gehosteten Server, eine Phishing-E-Mail an einen Enduser oder eine Sicherheitslücke bei einer Webanwendung handeln.

Sophos MTR bietet Integrationen (sogenannte „MTR Connectors") mit Sophos Intercept X Endpoint Protection, der Sophos XG Firewall und Sophos Cloud Optix. Unser Security Operations Team erhält damit Einblick in alle wichtigen Bereiche, in denen ein Angreifer erstmals in Ihrer Umgebung Fuß fassen könnte. Durch diese weitreichende Transparenz lassen sich Bedrohungen früher in der Angriffskette erkennen und beseitigen. So werden Angreifer gestoppt, bevor sie ihre Ziele in die Tat umsetzen können.

Relevante Signale für eine effiziente Analyse

Viele Sicherheitsservices verlassen sich ausschließlich auf SIEM-Lösungen (Security Information and Event Management), die Protokolldaten aus mehreren Quellen aggregieren. Sie filtern diese Daten in der Hoffnung, auf Signale zu stoßen, die für die Analyse relevant sein könnten. Da von diesen Lösungen neben relevanten Signalen auch eine riesige Menge irrelevanter Daten generiert wird, geht viel Zeit für die Analyse von Signalen verloren, die letztlich keine Hinweise auf bösartige Aktivitäten liefern. Zeit ist kostbar, und wenn ein Angreifer die Abwehr überlistet hat, zählt jede Sekunde.

Um relevante Signale zu finden, bei denen sich eine tiefergehende Analyse lohnt, greift Sophos MTR sowohl auf Produkt- als auch System-Telemetriedaten von Sophos Intercept X und anderen MTR-Connector-Produkten zurück. Dank dieser effektiven Suchmethode bleibt mehr Zeit für aktive Analysen. Gleichzeitig erhalten Analysten unbeschränkten Zugriff auf ein breites Spektrum an Daten, die normalerweise in einem SIEM erfasst werden.

In Zusammenarbeit mit SophosAI werden zudem Machine-Learning-Modelle auf der Basis von Sophos-MTR-Daten trainiert und in unsere Plattform eingebettet, sodass das Fachwissen unseres Threat-Response-Teams direkt mit einfließt. Bedrohungsklassen werden somit automatisch erkannt und unsere Analysten können sich auf die nächste Bedrohungsklasse konzentrieren.

Entwickelt für MSPs

Im Gegensatz zu anderen MDR-Services, die den MSP lediglich auf die Bedrohung hinweisen, ergreift das Sophos MTR-Team proaktiv geeignete Maßnahmen – entweder in Zusammenarbeit mit Ihnen oder komplett eigenständig in Ihrem Auftrag.

Wir wissen, dass Bedrohungen zu melden nicht die Lösung, sondern nur der erste Schritt ist. Nicht alle MSPs verfügen über die richtigen Tools, Fachkräfte und Prozesse, um ihr Sicherheitsprogramm effizient rund um die Uhr zu verwalten und sich gleichzeitig proaktiv vor neuen Bedrohungen zu schützen. 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.

Die Worte „Sicherheitspanne" und „Incident Response" rufen bei MSPs nicht unbedingt Begeisterung hervor. Aktuelle Berichte und Studien zeigen, dass KMUs nach wie vor am häufigsten angegriffen und demzufolge am anfälligsten sind. Mit der zunehmenden Verantwortung für die Cyber-Resilienz ihrer Kunden wächst für MSPs auch die Notwendigkeit, möglichst gut auf Angriffe vorbereitet zu sein. Denn immer häufiger fordern von Cyber-Angriffen betroffene KMUs eine Entschädigung vom MSP ein, dem sie die Sicherheit ihres Unternehmens anvertraut haben. Cyberkriminelle bedienen sich perfider Methoden, um MSPs schlicht zu überrumpeln oder selbst hocheffektive Endpoint-Schutz-Produkte einfach zu umgehen. Hätten Sie in einem solchen Fall nicht gerne einen direkten Ansprechpartner an Ihrer Seite, der Sie mit einem Team von Bedrohungsexperten kompetent unterstützt?

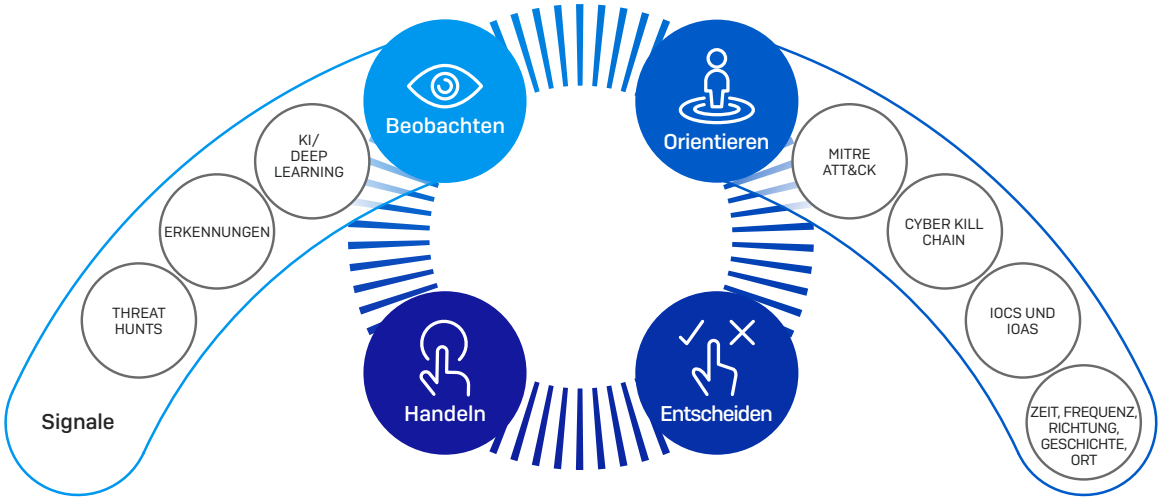
Das Analyse-Framework von Sophos MTR für Threat Hunting und Reaktionsmaßnahmen basiert auf dem als „OODA-Schleife" bekannten militärischen Konzept: beobachten, orientieren, entscheiden, handeln.

Beobachten: Wählen Sie wichtige Datenpunkte, die helfen, das Aktivitätsgeschehen auf den Geräten Ihrer Kunden oder innerhalb einer Umgebung nachzuvollziehen.

Orientieren: Analysten prüfen die Beobachtungsdaten und stoßen ggf. auf Indikatoren. Dabei werden die Datenpunkte mit der MITRE-ATT&CK-Matrix und der Cyber Kill Chain abgeglichen. Natürlich fließt dabei auch das Know-how unserer Analysten mit ein.

Entscheiden: Analysten überprüfen die zuvor zusammengestellten Datenpunkte, um festzustellen, welche Schritte in der nächsten Phase erforderlich sind, um schädliche Aktivitäten zuverlässig zu identifizieren.

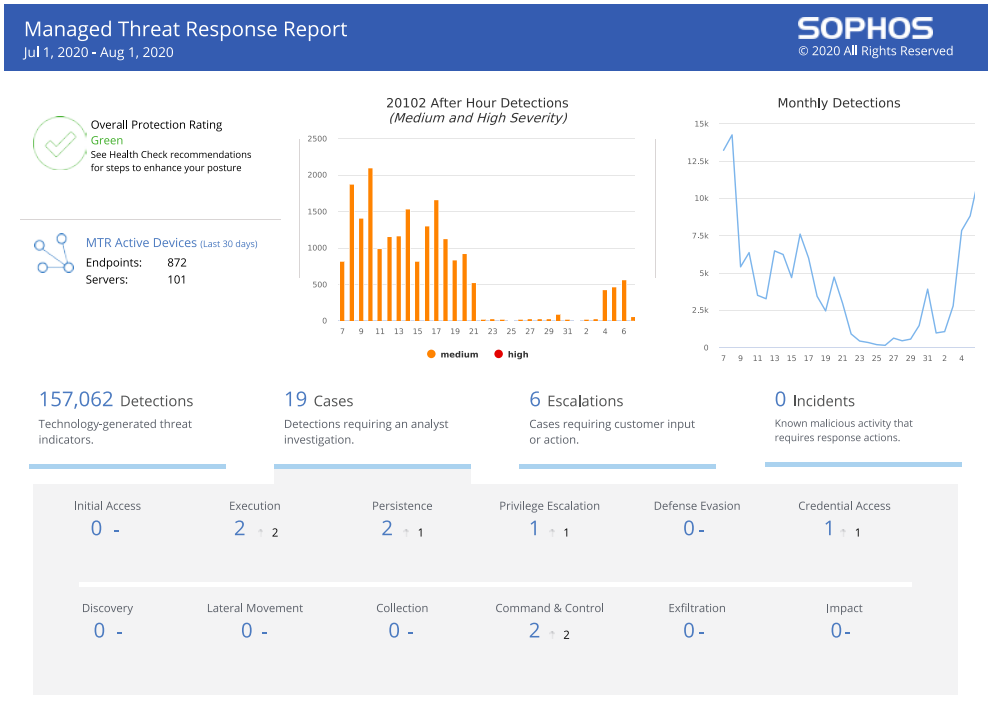
Handeln: Wenn ausreichend Informationen zur Beantwortung der Fragen in der „Entscheiden"-Phase vorliegen, ergreift der Analyst die erforderlichen Maßnahmen.



Monatliche Aktivitätsreports

Unser MTR-Team analysiert fortlaufend Warnmeldungen sowie ungewöhnliche Aktivitäten und reagiert entsprechend der von Ihnen gewählten Reaktions-Option schnell und präzise auf aktive Bedrohungen. Dabei informieren wir Sie ausführlich über Angriffe und ergriffene Reaktionsmaßnahmen. Außerdem erhalten Sie monatliche Aktivitätsreports zu Fällen, Hintergrundinformationen zu Bedrohungen, Einschätzungen zum Unternehmensrisiko sowie Unterstützung bei der Priorisierung von Maßnahmen.

Diese monatlichen Reports liefern MSPs eine allgemeine Schutzbewertung in Form einer zusammenfassenden Analyse. Dabei werden die bereits umgesetzten Empfehlungen zur Verbesserung des Sicherheitsstatus mit den noch nicht umgesetzten Empfehlungen verglichen. Im Rahmen solcher Health-Check-Empfehlungen raten wir Ihnen, Funktionen wie beispielsweise Anti-Exploit zum Schutz vor Zugangsdatendiebstahl und Rechteausweitung oder auch die Erkennung schädlichen Datenverkehrs zum Blockieren der Kommunikation mit Command-and-Control-Servern zu aktivieren.



Beispiel eines monatlichen MTR-Service-Reports

Flexible Lizenzierungssoptionen

Wir bieten Sophos MTR in zwei Servicestufen an: Standard und Advanced. So können Unternehmen das für sie optimale Service-Angebot auswählen. Unabhängig von der gewählten Servicestufe können MSPs zwischen drei Reaktions-Optionen wählen (Benachrichtigung, Zusammenarbeit oder Autorisierung).

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 *Alle Funktionen der „Standard"-Version, plus:*

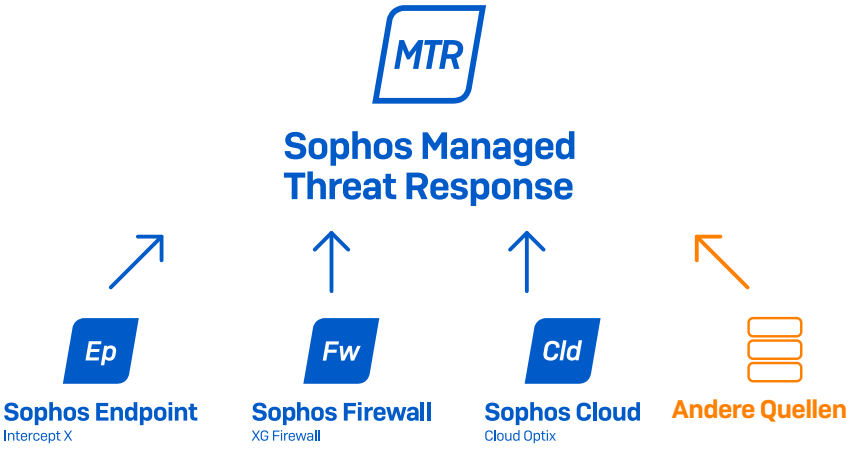
24/7 indizienloses Threat Hunting
Mithilfe von Data Science, Threat Intelligence und der Intuition erfahrener Bedrohungsexperten kombinieren wir verschiedene Informationen (Ihr Unternehmensprofil, hochwertige Assets und Benutzer mit hohem Risiko), um das Verhalten von Angreifern vorherzusagen und neue 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.

Sophos Next-Gen macht den Unterschied

Sophos kombiniert alle für eine mehrschichtige Schutzumgebung erforderlichen Komponenten in einer übersichtlichen Plattform, die skalierbare Transparenz und Sicherheit bietet. Diese innerhalb von Sophos Central kombinierten Schutzschichten werden zudem synchronisiert, um zwischen den einzelnen Produkten Informationen auszutauschen und so Bedrohungen in Echtzeit zu stoppen. Diese Synchronisierung macht Sophos Central zu einem der marktweit effektivsten und umfassendsten Cybersecurity-Systeme. Mit dem Managed Threat Response Service von Sophos können MSPs ihr IT-Sicherheitsportfolio entscheidend erweitern. Unabhängig von ihrer Größe erhalten sie damit den verlässlichen Service eines Security Operation Centers (SOC).



Erfahren Sie mehr über den Sophos Managed Threat Response Service oder lassen Sie sich von einem Cybersecurity-Experten beraten.

Mehr über Managed Threat Response erfahren Sie unter

www.sophos.de/MTR

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

20-09-10 WPDE (DD)

SOPHOS