Schutz für Behörden vor komplexen Cyberbedrohungen

Sophos MDR ist der **führende Managed Detection and Response Service** für den öffentlichen Sektor. Behörden sind ein Hauptziel für Cyberkriminelle. Da in diesem Bereich wertvolle Daten verarbeitet werden und eine große Angriffsfläche geboten wird, nutzen Angreifer zunehmend die lukrative Gelegenheit, Lösegeld zu erpressen. Dazu schleusen sie bei ihren Opfern Ransomware ein und drohen damit, Daten offenzulegen.

Cyberbedrohungen werden immer zahlreicher und komplexer. Daher setzen viele Behörden bereits auf den MDR-Service von Sophos, um sich vor gefährlichen Angriffen zu schützen, gegen die Technologie-Lösungen allein machtlos sind. Dieses Datenblatt beleuchtet die Cybersecurity-Herausforderungen in diesem Bereich und stellt Sophos MDR vor, den führenden MDR-Service für Behörden.

Cybersecurity-Herausforderungen im öffentlichen Sektor

Behörden sind ein Hauptangriffsziel

Über die Hälfte (58 %) der Behörden waren 2021 von Ransomware betroffen. 2020 lag der Anteil noch bei 34 %. Dieser 70%ige Anstieg innerhalb nur eines Jahres zeigt, wie schnell sich die Cyberbedrohungslage im öffentlichen Sektor zuspitzt.

Die Mehrheit der in Behörden tätigen IT-Manager meldete innerhalb des letzten Jahres einen Anstieg bei der Anzahl (59 %), Komplexität (59 %) und den Auswirkungen (56 %) von Cyberangriffen. Da Cyberkriminelle bei ihren Angriffen zunehmend auf Automatisierung und das „Malware-as-a-Service“-Modell zurückgreifen, werden diese Zahlen weiter steigen.

58 % waren 2021 von Ransomware betroffen
59 % meldeten einen Anstieg des Angriffsvolumens
59 % meldeten eine zunehmende Komplexität der Angriffe
56 % meldeten eine zunehmende Schwere der Angriffe

Die Auswirkungen komplexer Cyberbedrohungen auf Behörden sind gravierend

Ein schwerwiegender Cybervorfall hat erhebliche finanzielle und betriebliche Folgen für Behörden. 2021 beliefen sich die durchschnittlichen Kosten für die **Bereinigung eines Ransomware-Angriffs auf 660.000 US$**, wobei weit mehr als fast die Hälfte (42 %) der verschlüsselten Daten nach dem Vorfall nicht wiederhergestellt werden konnten.

Bereinigungskosten sind jedoch nur ein Teil des Problems. Die überwiegende Mehrheit (82 %) der von Ransomware betroffenen Behörden gab an, dass der Angriff ihre **Betriebsfähigkeit beeinträchtigt** habe. Beim Ausfall von IT-Systemen sind Behörden oft nur noch eingeschränkt in der Lage, kritische Dienste bereitzustellen, was letztlich zu einer Gefährdung der nationalen Sicherheit, der Infrastrukturen und der Wirtschaft führen kann.

Außerdem kann die Bereinigung zeitaufwändig sein. Über ein Fünftel (21 %) der Ransomware-Opfer in Behörden benötigen **ein bis sechs Wochen**, um den normalen **Geschäftsbetrieb nach dem Angriff wieder aufzunehmen**.

660.000 US$ Durchschnittliche Bereinigungskosten

82% der Angriffe beinträchtigen die Betriebsfähigkeit

SOPHOS

Sophos MDR

Vorteile

- 24/7 Threat Monitoring und Response in Echtzeit
- Threat Hunting aus Expertenhand
- Produktübergreifende Konsolidierung (Sophos und Drittanbieter) und Korrelation von Daten zu Sicherheitsereignisse
- Umfassende Managed Incident Response (unbegrenzte Anzahl von Stunden; keine zusätzlichen Gebühren oder Retainer-Verträge)
- Branchenführende Breach Protection Warranty
- Dedizierter Ansprechpartner
- Direkter Telefon-Support durch Sophos Security Operations Center (6 globale SOCs)

Behörden tun sich schwer, mit finanzstarken Angreifern Schritt zu halten

Die Realität zeigt, 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 einzige Möglichkeit, Cyber-Angreifer zuverlässig zu erkennen und zu eliminieren, besteht darin, einen rund um die Uhr aktiven **„Eyes on Glass"-Service** in Anspruch zu nehmen, bei dem Experten Bedrohungen mittels **Analyse von Sicherheitswarnmeldungen und Echtzeit-Bedrohungsdaten** erkennen und stoppen, bevor Schaden entsteht.

Moderne Betriebsumgebungen sind jedoch hochkomplex und Cyberbedrohungen entwickeln sich permanent weiter. Das macht es Unternehmen und Behörden zunehmend schwer, sich komplett selbst um das Erkennen und Bekämpfen von Cyberbedrohungen zu kümmern.

Unternehmen aller Branchen, auch Behörden und Einrichtungen im öffentlichen Sektor, tun sich schwer, mit finanzstarken Angreifern Schritt zu halten, die mit zunehmend

Sophos MDR: Schutz für Behörden vor Cyberbedrohungen

innovativen und professionellen Methoden versuchen, Abwehrtechnologien zu umgehen.

Angesichts der wachsenden Cybersecurity-Herausforderungen nehmen immer mehr Behörden den MDR-Service von Sophos in Anspruch, um modernen Bedrohungen einen Schritt voraus zu bleiben.

Cybersecurity as a Service 24/7/365

Sophos Managed Detection and Response (MDR) ist ein Fully-Managed-Service. Die Experten erkennen für Sie Cyberangriffe auf Ihren Computern, Servern, Netzwerken, Cloud Workloads und E-Mail-Konten und ergreifen Reaktionsmaßnahmen.

- **Erkennung:** Überwachen Ihre Umgebung 24/7 und erfassen, kontextualisieren und korrelieren von Sicherheitsdaten aus dem Sophos Adaptive Cybersecurity Ecosystem und von Ihren bereits vorhandenen Cybersecurity-Lösungen, um verdächtige Aktivitäten zu erkennen
- **Analyse:** Experten analysieren potenzielle Vorfälle und nutzen dabei Fachkenntnisse über Behörden und der Bedrohungsexpertise, um nach Anzeichen schädlicher Aktivitäten zu suchen
- **Bereinigung:** Analysten können Angriffe in der gesamten Umgebung schnell beheben, bevor sie schwerwiegende Folgen haben können, wie Ransomware oder eine weitreichende Datenpanne
- **Prüfung:** Umfassende Ursachenanalysen von Vorfällen in Verbindung mit regelmäßigen Health Checks sowie wöchentlichen und monatlichen Berichten ermöglichen Ihnen, den Sicherheitsstatus zu verbessern und ein Wiederauftreten in Zukunft zu verhindern

Im Schnitt analysieren und beheben die MDR-Experten Vorfälle **in nur 38 Minuten** nach der Erkennung – also mehr als fünfmal so schnell wie selbst die effizientesten internen Teams.

Mit Sophos MDR werden Sie von einem Team aus über **500 Bedrohungsspezialisten** unterstützt, deren Know-how den gesamten Erkennungs- und Reaktionszyklus abdeckt: von der Erkennung und Beseitigung von Bedrohungen bis hin zu Malware Engineering und automatisierter Cyberabwehr. Die sechs Security Operations Center (SOCs) in Australien, Indien, Europa und Nordamerika bieten Ihnen und Ihren Kunden **24/7 lückenlosen Schutz.**

Sophos MDR

Vorteile

- 24/7 Threat Monitoring und Response in Echtzeit
- Threat Hunting aus Expertenhand
- Produktübergreifende Konsolidierung (Sophos und Drittanbieter) und Korrelation von Daten zu Sicherheitsereignisse
- Umfassende Managed Incident Response (unbegrenzte Anzahl von Stunden; keine zusätzlichen Gebühren oder Retainer-Verträge)
- Branchenführende Breach Protection Warranty
- Dedizierter Ansprechpartner
- Direkter Telefon-Support durch Sophos Security Operations Center (6 globale SOCs)

Ein auf Sie zugeschnittener Service

Jede Behörde ist anders – in Bezug auf vorhandene Security-Lösungen, IT-/Cybersecurity-Mitarbeiter und die IT-Umgebung. Sophos MDR lässt sich **individuell auf Ihre Bedürfnisse zuschneiden.** Sie bestimmen, wie Sie mit Sophos MDR zusammenarbeiten möchten: Sophos kann die gesamte Incident Response und Ursachenanalyse übernehmen, Bedrohungen in Ihrem Auftrag eindämmen oder Sie lediglich über Bedrohungen informieren, damit Sie selbst Maßnahmen ergreifen können. Die Sicherheitsspezialisten arbeiten eng mit Ihnen zusammen, um den richtigen Ansatz für Ihre Behörde oder Einrichtung zu finden.

Kompatibel mit bereits vorhandenen Lösungen

Moderne Bedrohungen können aus jeder Richtung kommen und Angreifer setzen im Verlauf ihrer Angriffe oft mehrere Tools, Taktiken und Prozesse ein. Die Analysten von Sophos MDR können sowohl Sophos-Tools als auch vorhandene Drittanbieter-Lösungen nutzen, um Angriffe in Ihrer gesamten Umgebung zu erkennen und zu stoppen. Es wird Folgendes verwendet:

- **Endpoint-Telemetrie** zum Erkennen schädlicher Aktivitäten und Angriffsverhaltensweisen
- **Firewall-Daten** zum Erkennen von Einbruchversuchen und Beaconing
- **Netzwerk-Telemetrie** zum Erkennen nicht autorisierter Assets, ungeschützter Geräte und neuartiger Angriffe
- **E-Mail-Benachrichtigungen** zum genauen Lokalisieren des ersten Netzwerkzugangs und Zugriffsversuchen
- **Identitätsdaten** zum Erkennen von unbefugten Netzwerkzugriffen und Versuchen, Berechtigungen auszuweiten
- **Cloud-Warnmeldungen** zum Melden von unbefugten Netzwerkzugriffen und Versuchen, Daten zu stehlen

Je mehr Einblicke Sophos hat, desto schneller kann Sophos reagieren. Durch die Erkennung und Reaktion auf komplexe Angriffe mithilfe Ihrer vorhandenen Sicherheitstools reduziert Sophos MDR das Cyberrisiko und steigert gleichzeitig den ROI Ihrer Security-Investitionen.

Sophos MDR: Der führende MDR-Service für Behörden

Sophos ist der **weltweit führende MDR-Anbieter** und schützt mehr Unternehmen und Einrichtungen als alle anderen Anbieter vor Ransomware, Sicherheitsvorfällen und anderen Bedrohungen, die Technologien allein nicht stoppen können.

Sophos MDR schützt **viele Hundert Behörden** und bietet uns eine beispiellose Tiefe und Breite an Expertise zu Bedrohungen, denen der öffentliche Sektor ausgesetzt ist. Dank dieser umfassenden Telemetriedaten erreicht Sophos eine gemeinschaftliche Immunität: Aus einer einzelnen Kundenumgebung gewonnene Erkenntnisse erhöhen den Schutz für alle Kunden.

Am wichtigsten sind natürlich die Cybersecurity-Ergebnisse, die Sophos für unsere Kunden erzielen. Sophos ist die am besten und häufigsten bewertete MDR-Lösung bei Gartner Peer Insights mit einer durchschnittlichen Bewertung von 4.8/5 (271 Bewertungen insgesamt, Stand: 20. Dezember 2022). 97 % der Kunden würden Sophos weiterempfehlen. Außerdem ist Sophos Top Vendor im G2 Grid 2022 in der Kategorie MDR-Services für den Midmarket und ein MDR-Leader im G2 Grid für MDR allgemein, für Midmarket und für Enterprise.

✓ **Von allen Anbietern die meisten Kunden**
Über 15.000 Uternehmen und Einrichtungen nutzen Sophos MDR (Q1, 2023)

✓ **Am besten bewertet**
97 % der Kundn würden uns weiterempfehlen

✓ **Am häufigsten Bewertet**
271 Bewertungen auf Gartner Peer Insights im Jahr 2022

SOPHOS

Sophos MDR

Vorteile

- 24/7 Threat Monitoring und Response in Echtzeit
- Threat Hunting aus Expertenhand
- Produktübergreifende Konsolidierung (Sophos und Drittanbieter) und Korrelation von Daten zu Sicherheitsereignisse
- Umfassende Managed Incident Response (unbegrenzte Anzahl von Stunden; keine zusätzlichen Gebühren oder Retainer-Verträge)
- Branchenführende Breach Protection Warranty
- Dedizierter Ansprechpartner
- Direkter Telefon-Support durch Sophos Security Operations Center (6 globale SOCs)