SOPHOS

Schutz für Finanzdienstleister vor komplexen Cyberbedrohungen

Sophos MDR ist der führende Managed Detection and Response Service für die Finanzdienstleistungsbranche

Finanzdienstleister sind ein Hauptziel für Cyberkriminelle. Da in diesem Bereich sensible Daten verarbeitet werden, 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 Finanzdienstleister bereits auf den MDR-Service von Sophos, um sich vor gefährlichen Angriffen zu schützen, gegen die Technologie-Lösungen allein machtlos sind. Dieser Solution Brief beleuchtet die Cybersecurity-Herausforderungen in dieser Branche und stellt Sophos MDR vor, den führenden MDR-Service für die Finanzdienstleistungsbranche.

Sophos-Whitepaper, 2023

Cybersecurity-Herausforderungen für Finanzdienstleister

Finanzdienstleister sind ein Hauptangriffsziel

Über die Hälfte (55 %) der Finanzdienstleister waren 2021 von Ransomware betroffen. 2020 lag der Anteil noch bei 34 % [1]. Dieser 62%ige Anstieg innerhalb nur eines Jahres zeigt, wie schnell sich die Cyberbedrohungslage in dieser Branche zuspitzt.

Die Mehrheit der in dieser Branche tätigen IT-Manager meldete innerhalb des letzten Jahres einen Anstieg bei der Anzahl (55 %), Komplexität (64 %) und den Auswirkungen (55 %) von Cyberangriffen. Da Cyberkriminelle bei ihren Angriffen zunehmend auf Automatisierung und das „Malware-as-a-Service"-Modell zurückgreifen, werden diese Zahlen weiter steigen.

55 % waren 2021 von Ransomware betroffen

55 % meldeten einen Anstieg des Angriffsvolumens

64 % meldeten eine zunehmende Komplexität der Angriffe

55 % meldeten eine zunehmende Schwere der Angriffe

Die Auswirkungen komplexer Cyberbedrohungen auf Finanzdienstleister sind gravierend

Ein schwerwiegender Cybervorfall hat erhebliche finanzielle und betriebliche Folgen für Finanzdienstleister. 2021 beliefen sich die durchschnittlichen Kosten für die Bereinigung eines Ransomware-Angriffs auf 1,59 Mio. US$, wobei weit mehr als ein Drittel (37 %) der verschlüsselten Daten nach dem Vorfall nicht wiederhergestellt wurde.

Bereinigungskosten sind jedoch nur ein Teil des Problems. Fast alle (91 %) der von Ransomware betroffenen Finanzdienstleister gaben an, dass sie durch den Angriff in ihrer Betriebsfähigkeit beeinträchtigt wurden. 85 % der privatwirtschaftlichen Unternehmen vermeldeten zudem, dass sie dadurch Geschäftseinbußen oder Umsatzverluste verzeichneten. Wenn IT-Systeme ausfallen, wird die Fähigkeit eines Anbieters, Dienstleistungen bereitzustellen, stark eingeschränkt, was weitreichende Folgen für Kunden haben kann.

Die Bereinigung ist oft zeitaufwändig. Mehr als ein Viertel (26 %) der Ransomware-Opfer im Finanzwesen benötigen mehr als einen Monat, um den normalen Betrieb nach dem Angriff wieder aufzunehmen.

1,59 Mio. US$ Durchschnittliche Bereinigungskosten

91 %
der Angriffe beeinträchtigten die Betriebsfähigkeit

85 %
der Angriffe führten zu Geschäftseinbußen/Umsatzverlusten

1 Ransomware-Report – Finanzdienstleister 2022, Sophos.
Unabhängige Befragung von 5.600 IT-Experten, darunter 444 aus der Finanzdienstleistungsbranche. „Von Ransomware betroffen" bedeutet hier, dass der Angriff auf ein oder mehrere Geräte erfolgte, es dabei aber nicht unbedingt zu einer Verschlüsselung kam.

Finanzdienstleister 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 zunehmend schwer, sich komplett selbst um das Erkennen und Bekämpfen von Cyberbedrohungen zu kümmern.

Unternehmen aller Branchen, auch im Finanzwesen, tun sich schwer, mit finanzstarken Angreifern Schritt zu halten, die mit zunehmend innovativen und professionellen Methoden versuchen, Abwehrtechnologien zu umgehen.

Sophos MDR: Schutz für Finanzdienstleister

Angesichts der wachsenden Cybersecurity-Herausforderungen nehmen immer mehr Finanzdienstleister den Sophos MDR-Service 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. Unsere Experten erkennen für Sie Cyberangriffe auf Ihre Computer, Server, Netzwerke, Cloud Workloads und E-Mail-Konten und ergreifen Reaktionsmaßnahmen.

- **Erkennung:** Wir überwachen Ihre Umgebung 24/7 und erfassen, kontextualisieren und korrelieren 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 unsere Fachkenntnisse über die Finanzdienstleistungsbranche und unsere 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 unsere 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 unserem 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. Unsere sechs Security Operations Center (SOCs) in Australien, Indien, Europa und Nordamerika bieten Ihnen und Ihren Kunden 24/7 lückenlosen Schutz.

Ein auf Sie zugeschnittener Service

Jeder Finanzdienstleister 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: Wir können die gesamte Incident Response und Ursachenanalyse übernehmen, Bedrohungen in Ihrem Auftrag eindämmen oder Sie lediglich über Bedrohungen informieren, damit Sie selbst Maßnahmen ergreifen können. Unsere Sicherheitsspezialisten arbeiten eng mit Ihnen zusammen, um den richtigen Ansatz für Ihr Unternehmen oder Ihre 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 der gesamten Umgebung zu erkennen und zu stoppen. Wir können Folgendes verwenden:

- **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 wir haben, desto schneller können wir 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 Finanzdienstleister

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

Sophos MDR schützt über 500 Finanzdienstleister weltweit und bietet uns eine beispiellose Tiefe und Breite an Expertise zu Bedrohungen, denen die Finanzdienstleistungsbranche ausgesetzt ist. Dank dieser umfassenden Telemetriedaten erreichen wir eine gemeinschaftliche Immunität: Aus einer einzelnen Kundenumgebung gewonnene Erkenntnisse erhöhen den Schutz für alle Kunden.

Am wichtigsten sind natürlich die Cybersecurity-Ergebnisse, die wir 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 uns 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.

Die Nummer 1 für Finanzdienstleister

- ✓ **Von allen Anbietern die meisten Kunden:**
  Über 15.000 Unternehmen nutzen Sophos MDR (Q1, 2023)
- ✓ **Am besten bewertet:**
  97 % der Kunden würden uns weiterempfehlen
- ✓ **Am häufigsten bewertet:**
  271 Bewertungen auf Gartner Peer Insights im Jahr 2022

Feedback von unseren Kunden aus dem Finanzwesen

★★★★★

„Es ist beruhigend zu wissen, dass wir erstklassige Sicherheit durch ein Experten-Team erhalten, das uns den Rücken deckt, und wir beim Schutz unserer Geschäfts- und Kundendaten nicht alleine dastehen."

Vollständige Bewertung auf Gartner Peer Insights

★★★★★

„Wir nutzen Sophos MDR nun schon seit ein paar Monaten und bislang bin ich mit dem Return on Investment mehr als zufrieden. Selbst für mich als Nicht-IT-Führungskraft sind die monatlichen Reports sehr nützlich … Dank Sophos MDR erfüllen wir unsere Branchenstandards vollständig."

Vollständige Bewertung auf Gartner Peer Insights

★★★★★

„Dank dem sofortigen Handeln von Sophos MDR konnten wir unser Netzwerk ohne Datenverluste wieder in den Normalzustand zurückbringen. Außerdem wurde uns ein ausgezeichneter Bericht vorgelegt, in dem alle Einzelheiten zum Angriffsgeschehen und getroffene Maßnahmen detailliert aufgeführt waren."

Vollständige Bewertung auf Gartner Peer Insights

Weitere Infos

Mehr zu Sophos MDR und dazu, wie wir Sie unterstützen können, erfahren Sie bei Ihrem Sophos-Ansprechpartner oder auf sophos.de/mdr

Sophos MDR

- 24/7 Threat Monitoring and Response in Echtzeit
- Threat Hunting aus Expertenhand
- Produktübergreifende Konsolidierung (Sophos und Drittanbieter) und Korrelation von Daten zu Sicherheitsereignissen
- 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)
- Wöchentliche und monatliche Aktivitätsreports
- Monatliche Intelligence Briefings
- Ursachenanalyse, um den Sicherheitsstatus zu verbessern und ein Wiederauftreten von Bedrohungen in Zukunft zu verhindern
- Regelmäßige Sophos Account Health Checks zum Überprüfen von Konfigurationen und zum Gewährleisten maximaler Performance

Gartner befürwortet in seinen Forschungsbeiträgen keine bestimmten Hersteller, Produkte oder Dienstleistungen und rät Technologie-Nutzern nicht ausschließlich zu Anbietern mit besten Bewertungen. Forschungsbeiträge von Gartner sind als Meinungsäußerungen der „Research & Advisory"-Organisation von Gartner einzustufen und in keinem Fall als Tatsachenfeststellung zu werten. Gartner übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus.

GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seiner verbundenen Unternehmen in den USA und international; MAGIC QUADRANT und PEER INSIGHTS sind eingetragene Marken von Gartner, Inc. und/oder seiner verbundenen Unternehmen und werden hier mit Genehmigung verwendet. Alle Rechte vorbehalten.
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.

2023-02-27 (WP-NP)

SOPHOS