Rundum sicher vor Cyberangriffen
- brauche ich ein Managed SOC?

Michael Veit
Technology Evangelist, Sophos

SOPHOS

203 Mrd.€ Schaden für deutsche Unternehmen in 2021 durch Cyberangriffe[1]

84 Prozent der Unternehmen hatten Datendiebstahl, Ransomware, Sabotage[1]

6,2 Mrd.€ Investitionen in IT-Sicherheit 2021[2]

[1] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022
[2] https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/

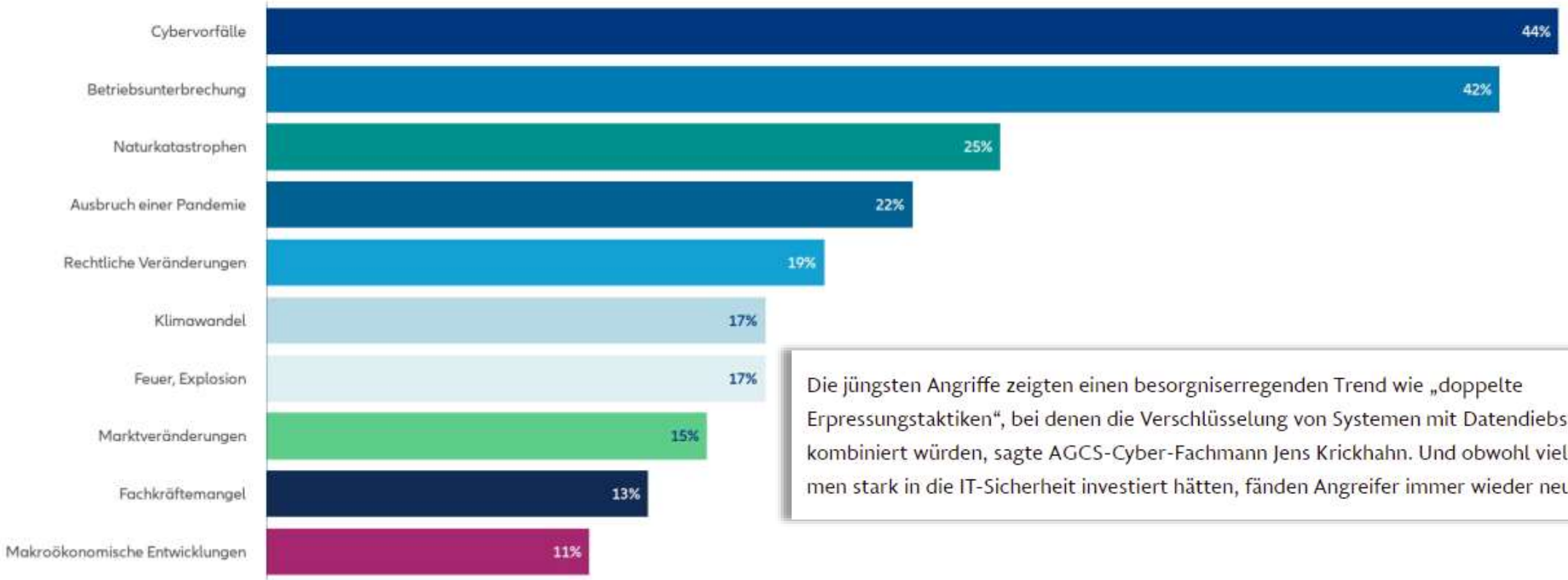
SOPHOS

Allianz

Top 10 Geschäftsrisiken weltweit in 2022

Allianz Risk Barometer 2022

Basierend auf den Antworten von 2.650 Risikomanagement-Experten aus 89 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



Die jüngsten Angriffe zeigten einen besorgniserregenden Trend wie „doppelte Erpressungstaktiken", bei denen die Verschlüsselung von Systemen mit Datendiebstahl kombiniert würden, sagte AGCS-Cyber-Fachmann Jens Krickhahn. Und obwohl viele Unternehmen stark in die IT-Sicherheit investiert hätten, fänden Angreifer immer wieder neue Lücken.

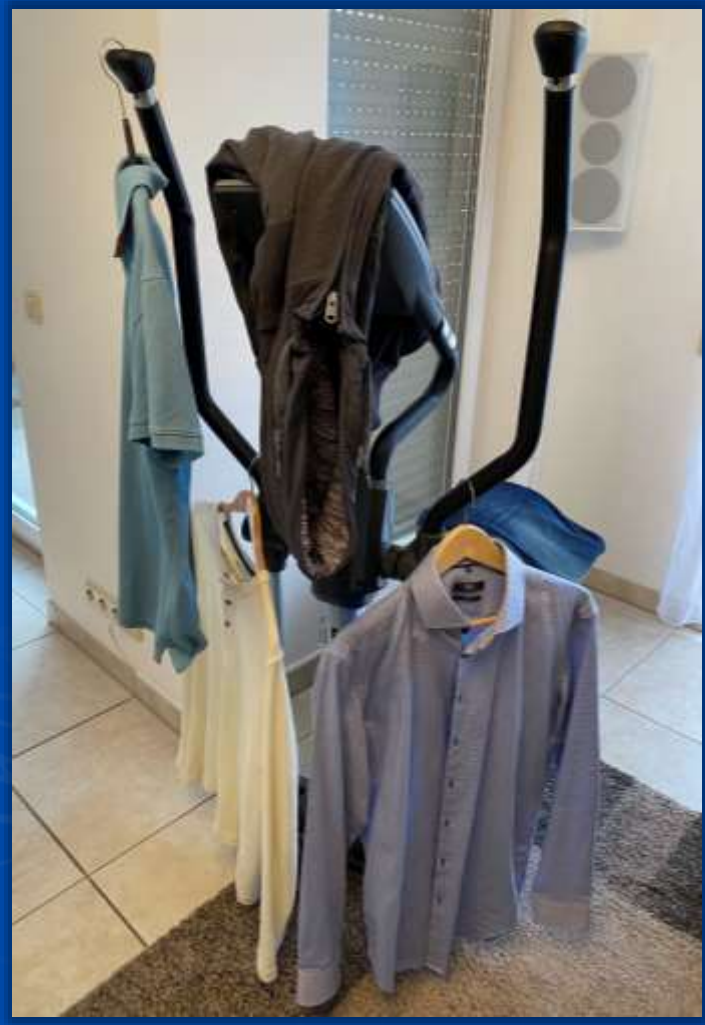
AGCS News & Insights

Source: Allianz Global Corporate & Specialty

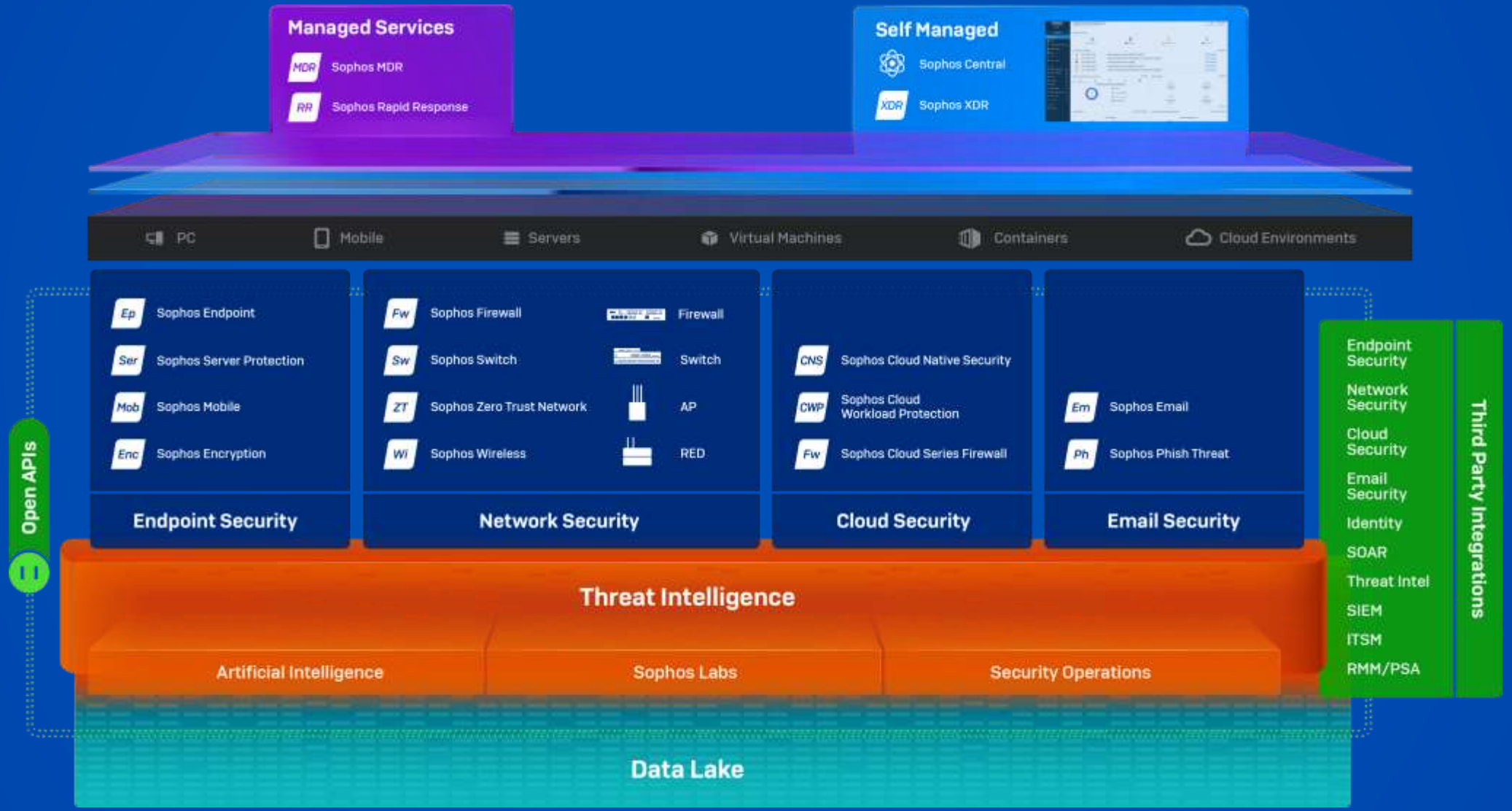
Alle Jahre wieder Ende Dezember…

SOPHOS

Eine Lösung kaufen reicht nicht mehr



SOPHOS Adaptive Cybersecurity Ecosystem

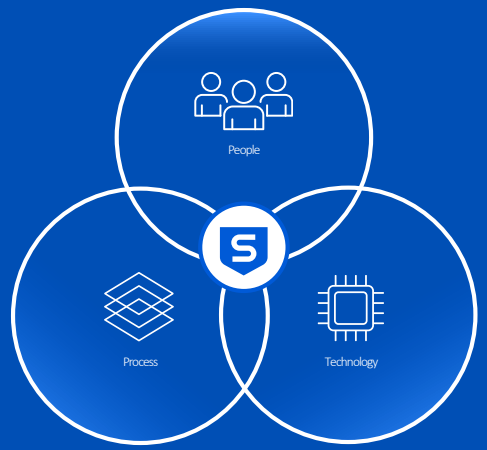


SOPHOS

Cybersecurity als Service

MANAGED DETECTION AND RESPONSE

Das Ergebnis zählt - rundum sicher durch Cybersecurity als Service



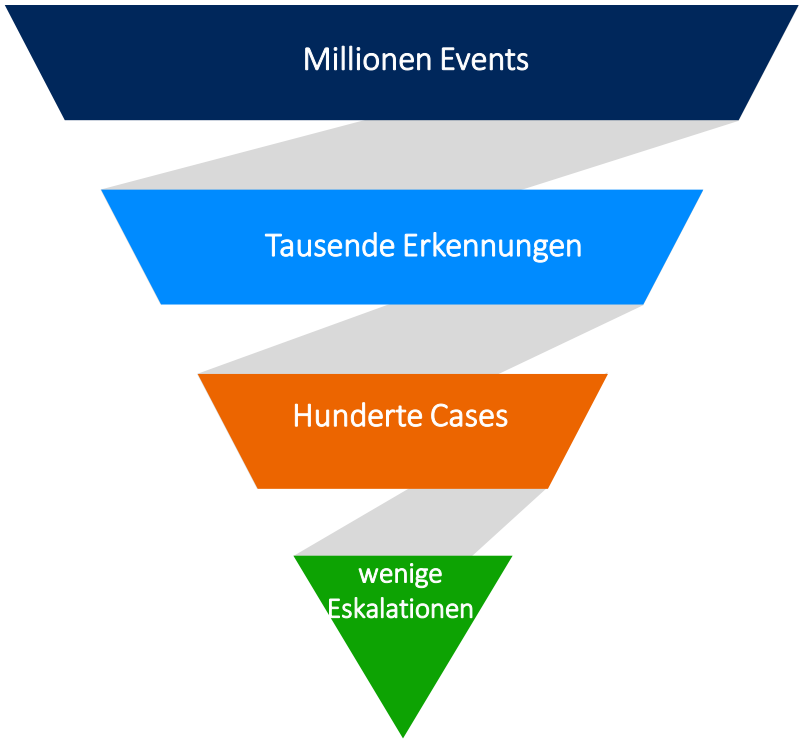
- Ihr ausgelagertes Security Operations Center (SOC)
- 24/7 Bedrohungserkennung und Reaktion
- Bedrohungssuche durch Experten
- Vollständiges Incident Response bei Angriffen
- Bestmögliches Ergebnis für Ihre IT-Sicherheit

SOPHOS

Sophos Cybersecurity as a Service

GERINGES RISIKO

1.000x Reduktion von Vorfällen, die eine genaue Betrachtung benötigen



HOHE EFFIZIENZ

12.000X Effizientere IT Security Teams

Sophos MDR Spezialisten haben rund um die Uhr den Blick auf aktuell 12.000 Unternehmenskunden und nutzen Erkenntnisse über neue Bedrohungen über die Grenzen der Netzwerke hinweg. Eine Betrachtung auf eine einzige Infrastruktur lässt diesen entscheidenden Vorteil aus – vor allem bei zeitlich kritischen Ereignissen.

GERINGE KOSTEN

5X Günstiger als das eigene SOC

Ein eigenes SOC im 24/7 Betrieb ist mehr als 5x teurer gegenüber eines vergleichbaren Sophos MDR Complete Angebots. Das begründet sich in den Personalkosten für ein eigenes SOC Team und den Kosten für eine XDR und SIEM Plattform, Konnektoren, Threat Feeds, Playbooks, SOAR Werkzeugen, etc.

Wie viele IT Security Spezialisten und welche Werkzeuge benötige ich, um Millionen von Events 24/7 zu bewerten?

SOPHOS

Sophos MDR: Offen und flexibel

Sophos MDR

Kompatibel mit Ihrer Umgebung
Wir nutzen Sophos Werkzeuge, die Werkzeuge anderer Anbieter – oder eine Kombination aus beiden

Kompatibel mit Ihren Anforderungen
Wir bieten komplettes Incident Response - oder Unterstützung für Ihr Team

Kompatibel mit Ihrem Unternehmen
Unser Team hat umfangreiche Erfahrung mit Angriffen auf Unternehmen aller Branchen

Sophos

- XDR Sophos XDR
- Fw Sophos Firewall
- Cld Sophos Cloud
- NDR Sophos NDR
- Em Sophos Email
- Ep Sophos Endpoint

Endpoint

Microsoft, CROWDSTRIKE, McAfee, SentinelOne, CHECK POINT, TREND MICRO, Malwarebytes, BlackBerry

Firewall

paloalto, FORTINET, CHECK POINT, CISCO, SONICWALL

Cloud SaaS

aws, Azure, Google Cloud, orca security

Email

Microsoft 365, mimecast, proofpoint

Identity

Microsoft [Azure IDP, ATA], okta, DUO

Network

DARKTRACE, Forcepoint

Sophos Managed Detection and Response (MDR)

- 24/7 Überwachung, Bedrohungserkennung und Reaktion durch Experten
- 24/7 Stoppen und Eindämmen von Bedrohungen
- 24/7 proaktives Threat Hunting
- Sophos XDR Agent für besten Schutz, Erkennung und Reaktion*
- Vollständiges Incident-Response: komplette Neutralisierung von Bedrohungen**
- nutzt Telemetrie von Endpoints, Servern, Firewall, Email, Cloud, Identity, Netzwerk..
- All-inclusive: alle Fälle, Überwachung, Reaktion, Reporting etc.

* alternativ Sophos XDR Sensor für Erkennung und Reaktion mit Endpoint Security anderer Hersteller

** Voraussetzung: voller Sophos XDR Agent für Schutz, Erkennung und Reaktion)

SOPHOS

24.2.2022

[Security Advisory] - Cyber Resiliency During the Ukraine and Russia Conflict

// Overview

The Sophos MTR team has been monitoring the situation between Ukraine and Russia and with the conflict escalating, have been staying alert and vigilant in monitoring and protecting our customers. We have thus far not seen an increase in malicious cyber activity targeting our customers but will continue to stay informed and disseminate information as it becomes relevant.

The information below from the Cybersecurity & Information Agency [CISA], provides guidance and resilience recommendations for organizations in the wake of cyber attacks affecting Ukraine. CISA suggests organizations adopt a heightened cybersecurity posture while protecting their most critical assets.

// What you should do

Review the information from the Cybersecurity & Information Agency [CISA] - Shields Up advisory [https://www.cisa.gov/shields-up], which includes guidance for organizations of all sizes.

Recommendations include:

- Validate that all remote access to the organization's network requires multi-factor authentication
- Ensure that software and applications are up to date
- Confirm that unnecessary ports and protocols have been disabled on the network
- Test and ensure that backup procedures allow for critical data to be rapidly restored

Also ensure that all devices within your estate are properly protected and configured with Sophos MTR and that your contacts and response preferences have been set appropriately in Sophos Central.

// What Sophos MTR is doing

The MTR Operations team is actively monitoring our customers' environments 24/7 for active attacks against their estates. Should our team identify suspicious activity, they will respond according to the set response preferences.

While our team is constantly performing threat hunting across the various data we collect, we have initiated focused hunting campaigns around this conflict using gathered intelligence.

Lastly, our intelligence teams are actively monitoring the event and should any new cyber activity emerge, the intelligence will be immediately fused into our ongoing processes.

// Resources

CISA | Shields Up

- https://www.cisa.gov/shields-up

Sophos MTR Operations Team

SOPHOS

30.9.2022

[Security Advisory] Zero-Day Vulnerabilities in Microsoft Exchange

// Overview

Microsoft has reported two new vulnerabilities (CVE-2022-41040 & CVE-2022-41082) affecting on-premises Microsoft Exchange Server 2013, 2016, and 2019.

Microsoft has observed limited, targeted attacks exploiting these vulnerabilities in-the-wild to compromise target systems.

Mitigations for this vulnerability are available however a patch is not available at this time.

CVE-2022-41040 is a Server-Side Request Forgery (SSRF) vulnerability while CVE-2022-41082 is a Remote Code Execution (RCE) vulnerability.

Vulnerabilities of this nature have been exploited in the past (such as with ProxyShell) to deliver web shells and perform further attacks including lateral movement within target networks along with delivery of malicious payloads (such as ransomware).

// What you should do

If you are using Microsoft Exchange Online, you do not need to take any action.

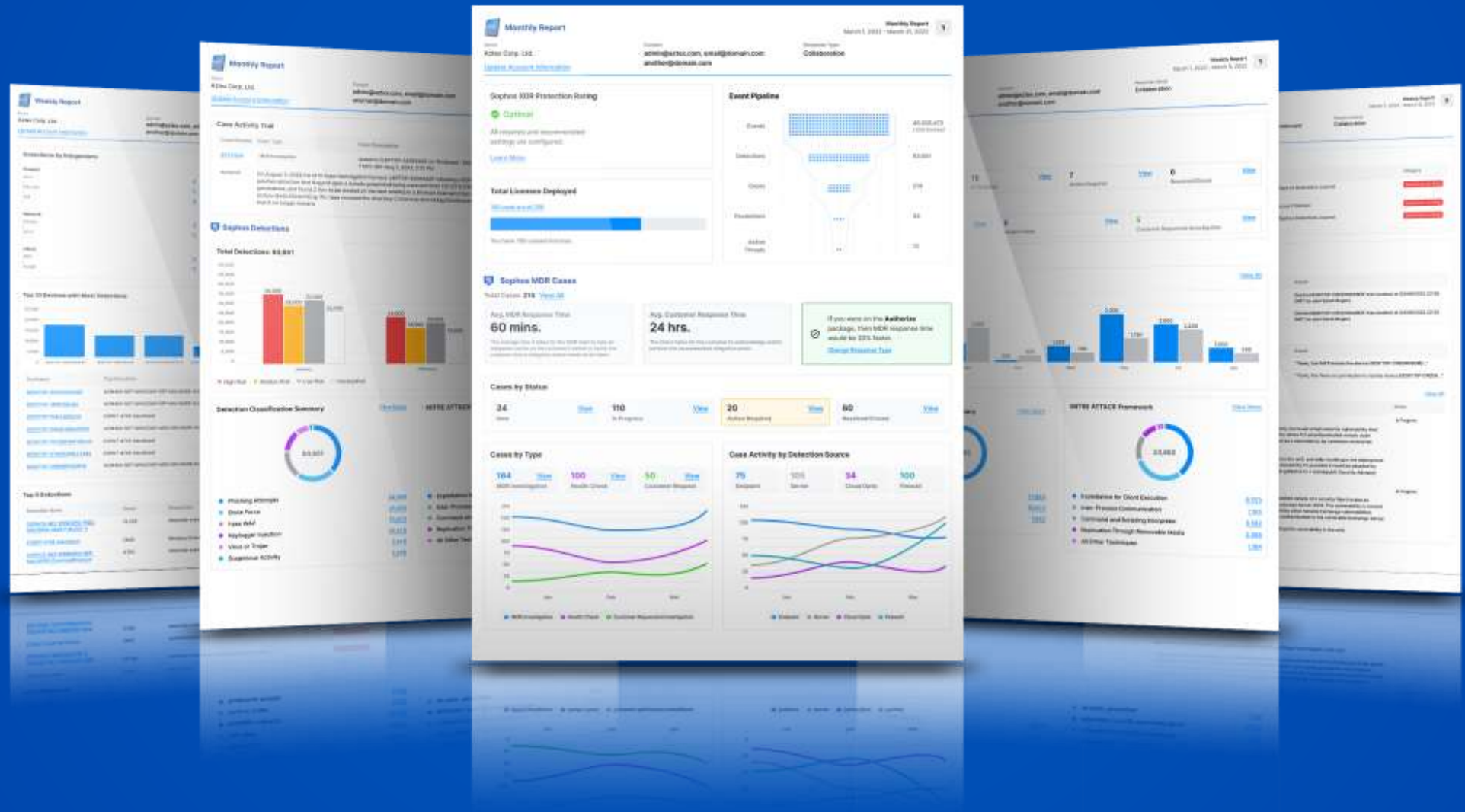
If you are using on premises Microsoft Exchange Server 2013, 2016, or 2019:

- Microsoft currently recommends adding a URL Rewrite blocking rule in IIS Manager to block exposed PowerShell ports.
- The blocking rule should be added by navigating to:
  - IIS Manager → Default Website → Autodiscover → URL Rewrite → Actions
- Review and action the guidance from Microsoft, linked in the References section below.
- Where possible, reduce the attack surface by disabling Outlook Web Access (OWA) from being exposed to the public internet.

// What Sophos MTR (Managed Threat Response) is doing

The MTR team are closely monitoring this reported zero-day. We are actively performing threat hunts on indicators of exploited Exchange servers. Our existing detection capabilities from the previous ProxyShell vulnerability will be helpful in identifying exploitation of these new vulnerabilities.

Managementtaugliche Cybersecurity Reports



SOPHOS

Nächste Schritte:

Halle 7, Stand 328

Sophos Adaptive Ecosystem (ACE)

Mit einer Kombination von Automatisierung und menschlichen Experten bietet das Sophos Adaptive Cybersecurity Ecosystem (ACE) leistungsstarken Schutz, der kontinuierlich dazulernt und sich verbessert.

➢ https://www.sophos.com/de-de/content/adaptive-cybersecurity-ecosystem

Sophos XDR - eXtended Detection and Response

Erkennen und analysieren Sie Bedrohungen lückenlos – mit Endpoint-, Server-, Firewall-, Email und weiteren Datenquellen.

➢ https://www.sophos.com/de-de/products/endpoint-antivirus/xdr.aspx

Sophos Managed Detection Response

24/7 Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen durch ein Expertenteam, als Fully-Managed-Service

➢ Mehr Infos: https://www.sophos.com/de-de/products/managed-threat-response.aspx

SOPHOS