heise Business Services

Ein eBook von

Powered by SOPHOS

Im Kampf gegen Erpressungstrojaner

Ransomware – vom Angriff zur effizienten Verteidigung

- **Von der Diskette zum Botnetz**
  Eine kurze Geschichte der Erpressungstrojaner
- **Künstliche Intelligenz im Kampf gegen Ransomware**
  Wie KI Erpressungstrojaner zur Strecke bringt
- **Best Practices für die Verteidigung**
  Strategien und Maßnahmen für eine effiziente Abwehr

Extra

Whitepaper

Incident Response Guide

Mehr Cyber-Resilienz für MSPs

Titelbild: Maksim Shmeljov, Shutterstock

Bild: Solarseven, Shutterstock

Editorial

Seit mehr als 30 Jahren werden Unternehmen von Erpressungstrojanern bedroht. Auch wenn sich die Angriffsmethoden drastisch verändert haben – die erste Ransomware wurde noch per Diskette ausgeliefert – so bleibt das Prinzip doch dasselbe: Kriminelle verschlüsseln Daten oder blockieren den Zugang zu ihnen und verlangen für die Freigabe Lösegeld.

Dieses Geschäftsmodell ist leider derart lukrativ und erfolgreich, dass wir wohl auch die kommenden 30 Jahre mit ihm leben müssen. Zum Glück sind Unternehmen den Angriffen jedoch nicht hilflos ausgeliefert. Vor allem die aktuellen Fortschritte bei Machine Learning und anderen Formen der künstlichen Intelligenz machen Mut. Dank KI sind Sicherheitslösungen heute sehr viel besser in der Lage, raffinierte und komplexe Bedrohungen zu erkennen und abzuwehren.

Technologie allein reicht für die Verteidigung jedoch nicht aus. Sicherheitsexperten und Anwender müssen durch kluge strategische Planung und verantwortungsvolles Handeln dazu beitragen, dass Angriffsarten wie Spear Phishing und Social Engineering ins Leere laufen, die Unachtsamkeit und menschliche Schwächen ausnutzen wollen.

Dieses eBook zeigt Ihnen, wo Ransomware herkommt und welche Entwicklung das Geschäftsmodell der Cyberkriminellen in den vergangenen Jahren genommen hat, welche Abwehrmaßnahmen wirklich helfen und wie Sie die Verteidigung gegen Ransomware effizienter und effektiver gestalten.

Dr. Thomas Hafen

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10b
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

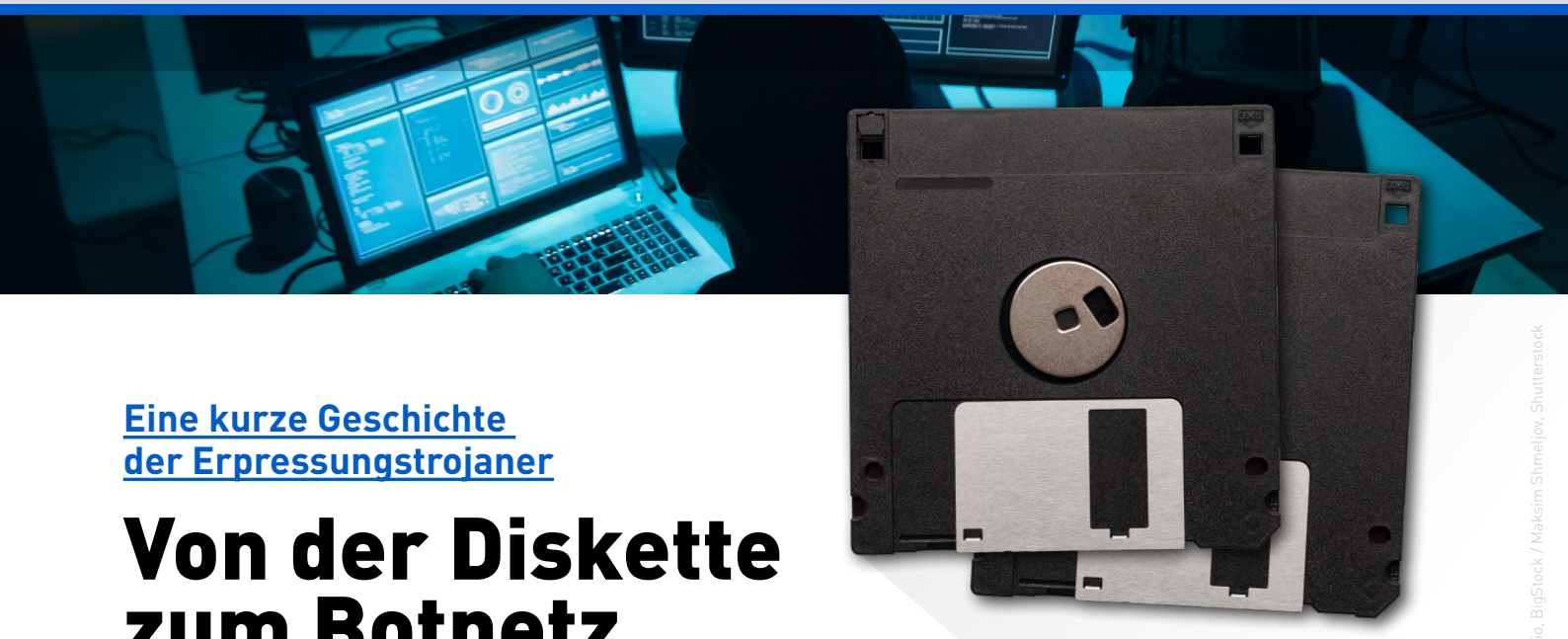
Verantwortlich für den Inhalt:
Heise Business Services
Thomas Jannot, tj@heise.de

Haben Sie Fragen zu diesem eBook oder haben Sie Interesse an einer eigenen Produktion, dann schicken Sie bitte eine E-Mail mit dem Betreff **„HBS-eBook“** an hbs@heise.de

Inhalt

ÜBER DEN AUTOR

Dr. Thomas Hafen war über 15 Jahre als Redakteur, Moderator und Manager für verschiedene IT-Fachverlage tätig. Seine fachlichen Schwerpunkte liegen in den Bereichen Digitale Transformation, Cloud Computing und Advanced Analytics. Thomas Hafen lebt und arbeitet heute als freier Journalist und Moderator in München.



Bilder: Tiko Gaspario, BigStock / Maksim Shmeljov, Shutterstock

Eine kurze Geschichte der Erpressungstrojaner

Von der Diskette zum Botnetz

Seit mehr als 30 Jahren kämpfen IT-Sicherheitsverantwortliche gegen Ransomware. Dabei haben sich die Angriffsmethoden immer weiterentwickelt und drastisch verändert.

Der Evolutionsbiologe Dr. Joseph L. Popp wurde nicht für seine Arbeiten über die Mantelpaviane Äthiopiens berühmt. Auch sein Buch „Popular Evolution" war eher kein Bestseller. In die Geschichte – zumindest die der IT – ging Popp mit einer ganz anderen Aktion ein. Der Biologe verschickte im Jahr 1989 rund 20.000 Disketten, die vorgeblich ein „AIDS-Informationssystem" enthielten. Nach 90 Starts verschlüsselte ein darin versteckter Trojaner die Festplatte des Anwenders. Für die Entschlüsselung verlangte Dr. Popp eine Jahresgebühr von 189 US-Dollar, die per Scheck auf ein Konto in Panama bezahlt werden sollten – der erste bekannte Fall von Erpressung durch Ransomware.

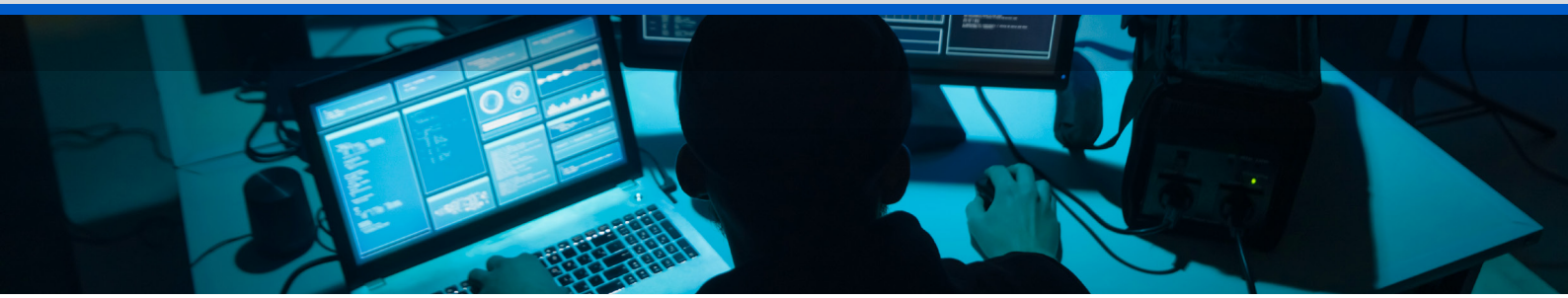
Das Geschäftsmodell des Dr. Popp hatte allerdings einige Schwächen. Seine Verschlüsselung war leicht zu knacken, die Idee, Lösegeld in Form von Schecks zu fordern, erwies sich als wenig praxistauglich, und der Aufwand für die Verbreitung des Trojaners war enorm, denn Dr. Popp musste jede Diskette selbst beschreiben und verschicken.

Die Entwicklung der Ransomware

Heute mag dieser Versuch archaisch und dilettantisch anmuten, das Prinzip von Ransomware ist aber dasselbe geblieben: Die Opfer sollen Lösegeld bezahlen, um die von einem Erpressungstrojaner verschlüsselten Dateien zurückzuerhalten. Die Angriffsvektoren, der Maßstab der Angriffe und die Professionalität der Angreifer haben jedoch ganz andere Dimensionen angenommen.

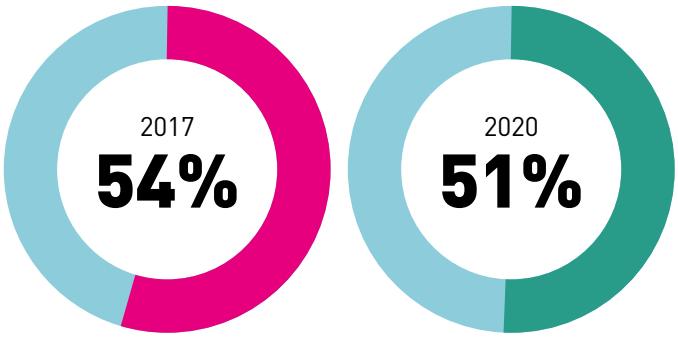
```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                        Press ENTER to continue
```

Mit diesem Text forderte die erste bekannte Ransomware der Welt zur Zahlung von Lösegeld auf.
Quelle: Sophos



Ransomware heute: Stand der Bedrohung

Für den Report „The State of Ransomware 2020" hat das Marktforschungsunternehmen Vanson Bourne im Auftrag von Sophos 5.000 IT-Manager in 26 Ländern nach ihren Erfahrungen mit Erpressungstrojanern befragt. 51 Prozent der Umfrageteilnehmer verzeichneten mindestens eine Ransomware-Attacke pro Jahr – ein leichter Rückgang im Vergleich zu 2017, wo noch 54 Prozent betroffen waren.



Im Vergleich zu 2017 ist der Anteil der von Ransomware betroffenen Unternehmen etwas gesunken.
n (2020) = 5.000, n (2017) = 1.700,
Quelle: The State of Ransomware 2020, Sophos

Dies ist jedoch kein Grund zur Entwarnung. Der Rückgang beruht nach Analysen der Sicherheitsexperten vor allem auf Strategieänderungen der Angreifer. Von ungezielten „Schrotschuss"-Angriffen gehen die Cyberkriminellen zunehmend zu gezielten Attacken über. Daher werden zwar weniger Unternehmen getroffen, diese aber nachhaltiger.

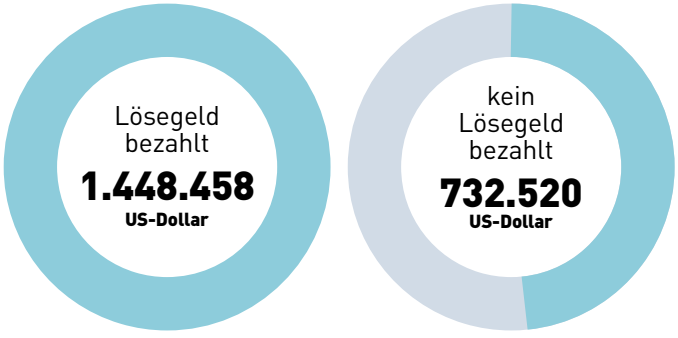
Durchschnittliche Kosten für die Behebung einer Ransomware-Attacke

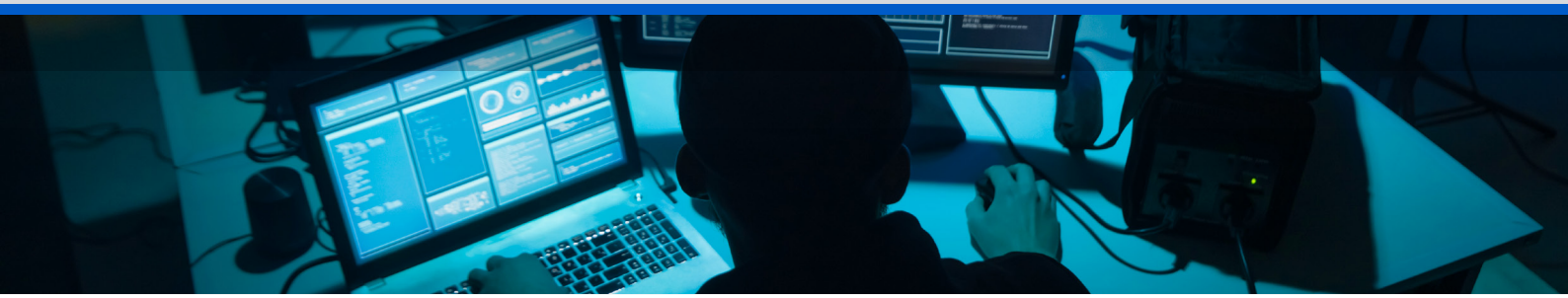
Wer Erpresser bezahlt, verdoppelt die Kosten einer Ransomware-Attacke.
n = 1.849, Quelle: The State of Ransomware 2020, Sophos

Wer Lösegeld zahlt, zahlt doppelt

In fast drei Viertel der Fälle gelingt es den Cyberkriminellen dann auch, Daten zu verschlüsseln. Allerdings erhalten 94 Prozent der Betroffenen ihre Daten wieder zurück. 56 Prozent konnten sie aus einem Backup wiederherstellen, bei 26 Prozent gaben die Erpresser die Daten nach Zahlung eines Lösegelds frei. Die durchschnittlichen Kosten einer Ransomware-Attacke beziffert Sophos auf mehr als 750.000 US-Dollar. Darin enthalten sind Umsatzausfälle, Personal- und Netzwerkkosten sowie gegebenenfalls die gezahlten Lösegelder. Wer auf die Forderungen der Erpresser eingeht, senkt im Übrigen die Gesamtkosten nicht – im Gegenteil: In Unternehmen, die Lösegeld bezahlt haben, lagen die Aufwände doppelt so hoch wie bei den Zahlungsverweigerern.

Bemerkenswert ist der hohe Anteil verschlüsselter Public-Cloud-Ressourcen. In 59 Prozent der Attacken, die von Sophos analysiert wurden, waren Daten in der Cloud betroffen. Der Report deckte außerdem eine gravierende Versicherungslücke bei vielen Unternehmen auf. Zwar sind bei 84 Prozent der Umfrageteilnehmer Schäden durch Hackerangriffe über eine Cyberversicherung abgesichert, bei einem Fünftel der Policen sind Ransomware-Attacken jedoch nicht mit abgedeckt. Unternehmen tun daher gut daran, ihre Versicherungsbedingungen zu überprüfen und diese Lücke zu schließen.





Die Zukunft von Ransomware

Worauf sich Unternehmen aktuell und in Zukunft einstellen müssen, wird im Sophos Threat Report 2021 deutlich. Die Experten identifizieren dabei vor allem folgende Trends:

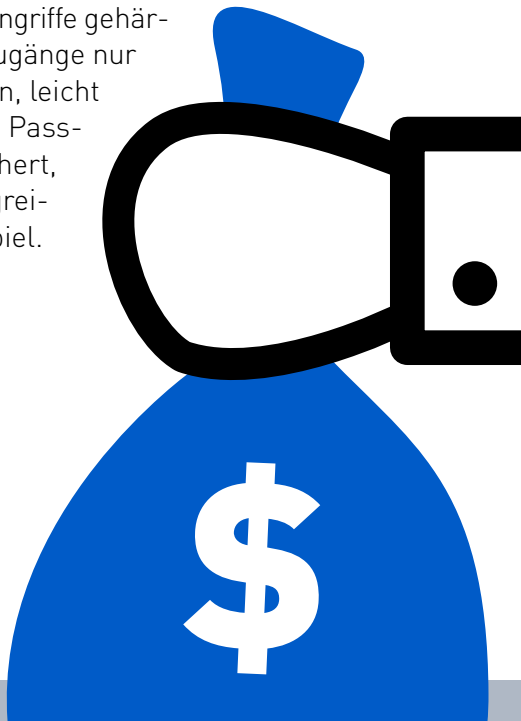
- **Ransomware-Attacken werden zunehmend diverser:** Baukästen und „Ransomware-as-a-Service" haben die Einstiegsschwelle deutlich gesenkt. Mit einfach zu bedienenden Tools wie Dharma greifen Gelegenheitserpresser vor allem kleine und mittlere Unternehmen an. Auf der anderen Seite des Spektrums stehen das organisierte Verbrechen und Geheimdienste, die gezielt und hochprofessionell agieren. Ransomware-Kategorien wie Ryuk und Ragnar Locker sind Beispiele für solche Angriffe.

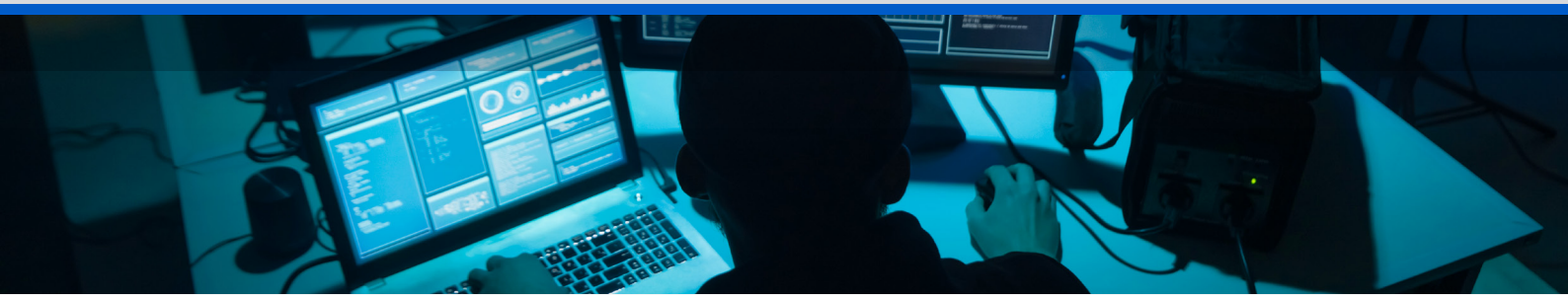
- **Zusatzgeschäft mit gestohlenen Daten:** Der Sophos Threat Report 2021 enthüllte eine weitere gefährliche Entwicklung: Erpresser bauen sich zunehmend ein zweites Standbein auf, falls die Verschlüsselung fehlschlägt oder das Opfer die Daten aus einem Backup wiederherstellen kann. Dazu stehlen sie sensible Informationen und drohen mit deren Veröffentlichung, wenn das Unternehmen nicht bezahlt.

- **Gezielte Jagd auf Backups:** Neben Cloud-Ressourcen nehmen Erpresser zunehmend auch lokale Sicherungsdateien ins Visier. Sie löschen Sicherungsdaten oder verschlüsseln sie, bevor sie ihren eigentlichen Angriff auf das Netzwerk starten. Da Backups in den meisten Unternehmen viel zu selten auf ihre Funktionsfähigkeit überprüft werden, fällt deren Ausfall erst auf, nachdem die Produktivsysteme verschlüsselt sind.

- **Vermehrte Attacken auf Windows- und Linux-Server:** Angriffe auf Server haben im Jahr 2020 erheblich zugenommen. Sie sind für Cyberkriminelle attraktive Ziele, weil sie oft über längere Zeiträume unbeaufsichtigt betrieben werden und privilegierte Rechte haben. In dieser Zeit können sich Angreifer daher unbemerkt von einem Server aus im Netzwerk ausbreiten. Sophos geht davon aus, dass Attacken auf Server weiter zunehmen werden.

- **Windows Remote Desktop Protocol (RDP) als Einfallstor:** Brute-Force-Attacken über RDP sind häufig der Beginn eines erfolgreichen Ransomware-Angriffs. Dabei verschaffen sich Cyberkriminelle zunächst über RDP Zugang zu einem Rechner, um sich von dort im Netzwerk auszubreiten und die Kontrolle zu übernehmen. Die starke Zunahme von Homeoffice-Arbeitsplätzen in der Corona-Krise hat das Problem verschärft. Viele Unternehmen nutzen RDP, um die verteilten Arbeitsplätze zu administrieren. Laut Sophos ist RDP aber nicht dafür konzipiert, aus dem öffentlichen Internet zugänglich zu sein, und daher nicht gegen Brute-Force-Angriffe gehärtet. Sind die Zugänge nur mit schwachen, leicht zu erratenden Passwörtern gesichert, haben die Angreifer leichtes Spiel.





- **Angriffe auf IoT- und Smart-Home-Geräte:** Router, Telefone, Smart TVs, Lautsprecher, Überwachungskameras, Mähroboter und viele andere Geräte des Alltags sind heute mit dem Internet verbunden. Veraltete Firmware, nur schwach gesicherte Administrationszugänge und offene Ports machen es Angreifern leicht, diese Geräte zu übernehmen und beispielsweise in ein Botnetz zu integrieren. Laut Sophos nehmen aber auch sogenannte „Malvertising"-Angriffe zu, bei denen ein Malware-Befall nur vorgetäuscht wird. Die Anwender sollen so dazu bewogen werden, überteuerte Rettungs-Software zu kaufen oder Service-Verträge abzuschließen.

- **Missbrauch legaler Tools:** Cyberkriminelle setzen zunehmend Bordmittel des Betriebssystems wie PowerShell, aber auch Sicherheitswerkzeuge wie Metasploit oder Cobalt Strike ein, um Systeme zu übernehmen und Daten zu exfiltrieren. Diese als „Living-off-the-Land" (LoL) bezeichneten Angriffe sind für Sicherheitsverantwortliche besonders problematisch. Da diese Angriffe wenig oder keine Malware enthalten, schlagen Antivirenlösungen in der Regel nicht Alarm. LoL-Angriffe lassen sich daher nur über eine gezielte Verhaltensanalyse der entsprechenden Tools entdecken.

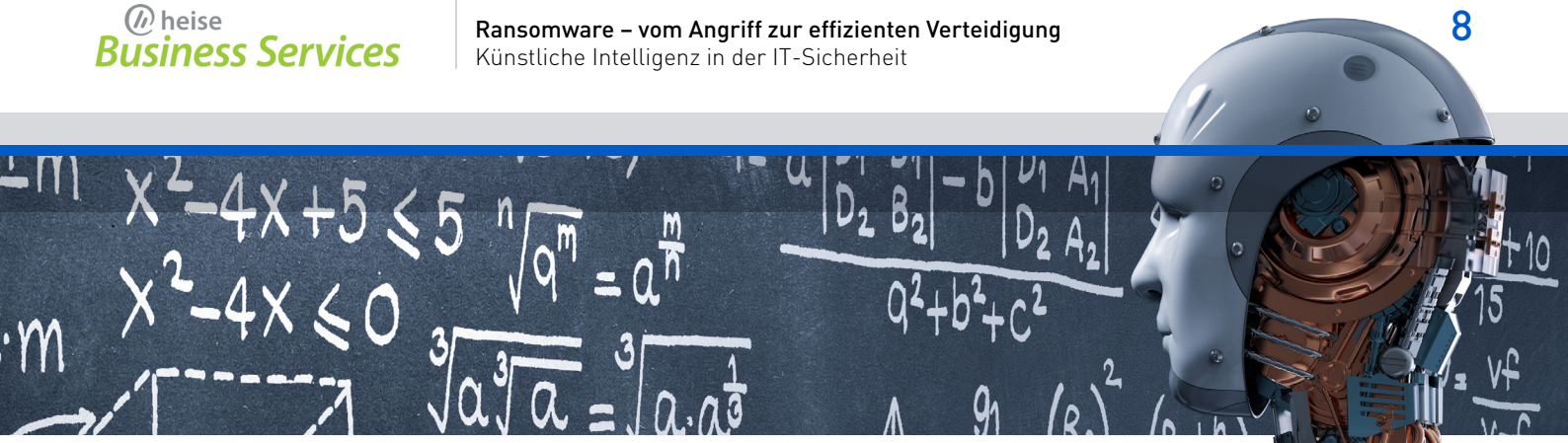
Fazit: Ransomware – eine Bedrohung mit Bestand

Ransomware richtet Jahr für Jahr Schäden in Milliardenhöhe an. Daran wird sich wohl auch in den kommenden Jahren wenig ändern. Unternehmen und öffentliche Organisationen sollten mit einem dreistufigen Konzept dagegenhalten:

1. **Verbesserung der Abwehr**
2. **Ausbau und Absicherung einer Backup-and-Recovery-Strategie**
3. **Abschluss beziehungsweise Erweiterung einer Cyberversicherung auf Schäden durch Ransomware**

Besondere Bedeutung kommt in Zukunft zudem Services wie Managed Threat Response (MTR) durch spezialisierte Threat-Hunting-Teams zu. Sie sind in der Lage, subtile Veränderungen und kleinste Anomalien zu erkennen und richtig einzuordnen und so potenzielle Eindringlinge schnell und sicher zu identifizieren. Das verringert die Gefahr, Opfer einer Ransomware-Attacke zu werden, erheblich. Der Einsatz von MTR kann sich darüber hinaus auch positiv auf die Höhe einer Versicherungspolice für Cyberschäden auswirken und so zusätzliche wirtschaftliche Vorteile mit sich bringen. ■

Cyberkriminelle setzen zunehmend Bordmittel des Betriebssystems und legitime Sicherheitswerkzeuge ein, um Systeme zu übernehmen und Daten zu exfiltrieren.



KI im Kampf gegen Ransomware und andere Bedrohungen

Künstliche Intelligenz in der IT-Sicherheit

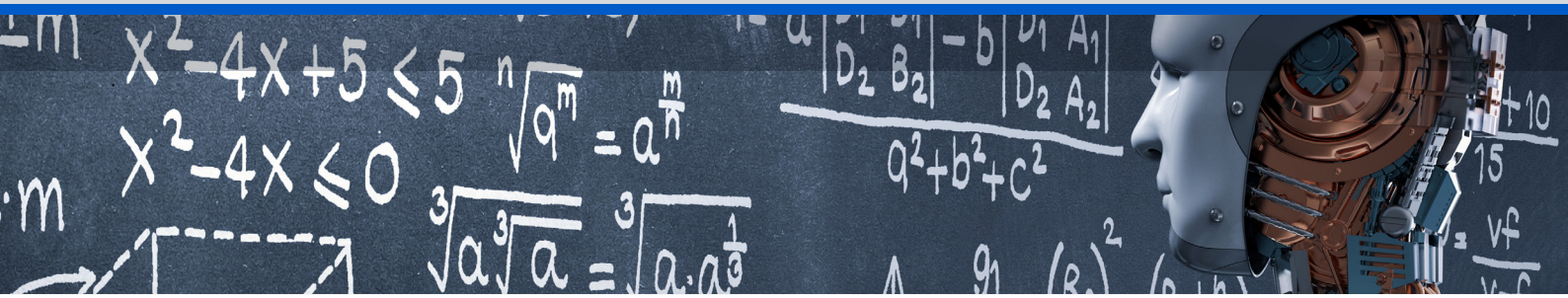
Maschinelles Lernen und andere Formen der künstlichen Intelligenz haben in den vergangenen Jahren massiv an Bedeutung gewonnen. Auch in der IT-Security übernehmen intelligente Systeme immer mehr Aufgaben.

KI-basierte Systeme sind aus unserem Alltag nicht mehr wegzudenken. Die Einsatzgebiete der künstlichen Intelligenz reichen vom autonomen Fahren über die Entwicklung von Medikamenten und Impfstoffen bis hin zur Produktionssteuerung und prädiktiven Wartung in der „Smart Factory". Auch in der IT-Sicherheit werden Machine Learning und KI immer wichtiger. Dies hat mehrere Gründe. Zum einen lässt sich die zunehmende Komplexität von IT-Umgebungen ohne die Hilfe künstlicher Intelligenz kaum mehr überblicken und managen. Die Zahl und Vielfalt von Endgeräten und Benutzerschnittstellen steigt ständig, Cloud Computing, das Internet der Dinge (IoT) und neue Technologien wie 5G vergrößern die Angriffsfläche stetig. Hinzu kommt das ungebrochene Datenwachstum. Laut einer Prognose des Analystenhauses IDC wird das weltweite Datenvolumen bis 2025 rund 175 Zettabyte erreichen – das sind 175 Billionen Gigabyte!

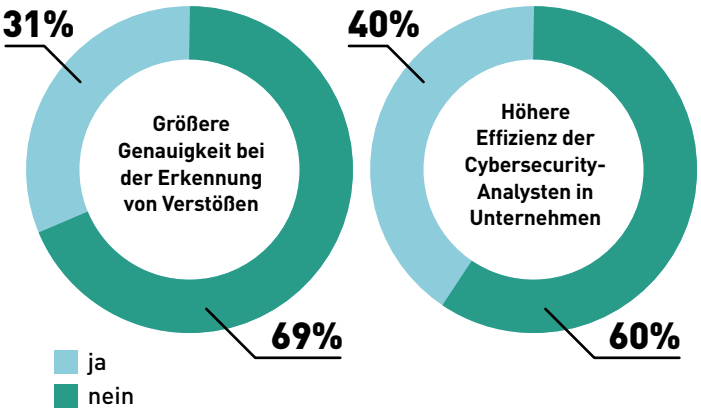
Zum anderen setzen auch Kriminelle vermehrt auf KI, um beispielsweise Angriffe effizienter zu gestalten. Wie das funktioniert, zeigen Tools, die für Schulungs- und Pentest-Zwecke auf GitHub verfügbar sind. SNAP_R kann beispielsweise die Twitter-Timeline eines potenziellen Opfers analysieren, um zielgerichtete Spear-Phishing-Tweets zu verfassen. Das Tool ist sechs Mal effektiver als ein menschlicher Hacker. Auch Social Mapper lässt sich zur Vorbereitung von Spear-Phishing-Attacken einsetzen. Es kann mithilfe der Gesichtserkennung Personen identifizieren, deren Social-Media-Kanäle zusammenführen und daraus ein Profil erstellen, das für gezielte personalisierte Angriffe genutzt werden kann.

Deepfakes – Manipulation von Bildern und Sprache

Ein weiterer Bereich, in dem KI für kriminelle Zwecke missbraucht wird, sind sogenannte „Deepfakes". Für diese Form des Betrugs werden Videos und Sprachaufnahmen mithilfe von Deep Learning so gefälscht, dass sie von echten Bildern oder Äußerungen einer Person nicht mehr zu unterscheiden sind. Deepfakes lassen sich beispielsweise für den „CEO Fraud"– auch als „Geschäftsführerbetrug" bekannt – einsetzen. Bereits 2019 berichtete die Versicherung Euler Hermes über einen Fall, bei dem Deepfakes eingesetzt wurden, um die Stimme eines Geschäftsführers täuschend echt nachzubilden. In der britischen Niederlassung eines Energie-



unternehmens hatte vermeintlich der deutsche CEO des Mutterkonzerns angerufen, und die Überweisung von 220.000 Euro auf das Konto eines ungarischen Lieferanten veranlasst. Der Mitarbeiter wunderte sich zwar über den ungewöhnlichen Auftrag, da er die Stimme aber eindeutig erkannte und die Erklärung plausibel war, folgte er den Anweisungen. Der Schwindel flog erst auf, als der „falsche" CEO noch einmal anrief, während der Mitarbeiter mit dem echten Chef sprach.



Die Mehrheit der IT-Entscheider ist überzeugt, dass KI Effizienz und Genauigkeit in der Cybersecurity verbessert.

n = 850, Quelle: Capgemini Research Institute, AI in Cybersecurity executive survey

Angesichts der zunehmenden Komplexität und der Aufrüstung auf der Gegenseite verwundert es nicht, dass die Mehrheit der IT-Sicherheitsverantwortlichen KI-Methoden zur Verteidigung als unumgänglich erachtet. Laut einer Umfrage des Beratungsunternehmens Cap Gemini unter 850 Führungskräften sind drei Viertel der Teilnehmer davon überzeugt, dass ihr Unternehmen durch den Einsatz von KI schneller auf Sicherheitsverletzungen reagieren kann. Drei von fünf Unternehmen sagen, dass der Einsatz von KI die Genauigkeit und Effizienz von Cyber-Analysen verbessert und mehr als die Hälfte gibt an, dass KI hilft, die Kosten für die Erkennung von Angriffen und die Reaktion auf Sicherheitsverletzungen zu senken.

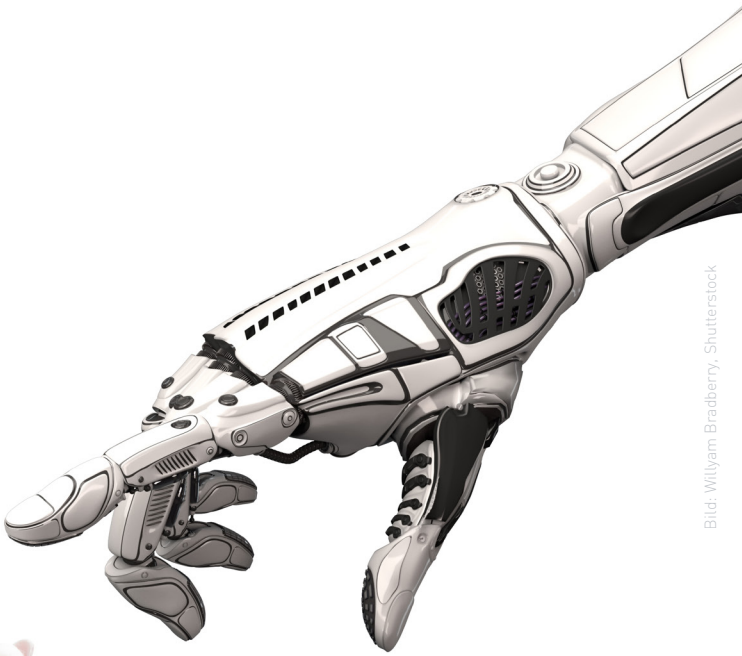
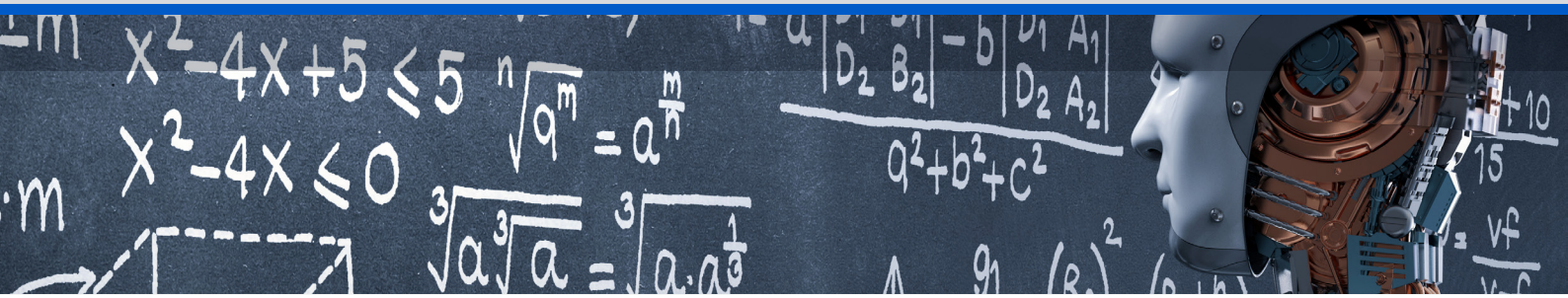


Bild: Willyam Bradberry, Shutterstock

> Drei Viertel der Unternehmen sind überzeugt, durch KI-Einsatz schneller auf Sicherheitsverstöße reagieren zu können.



Wie Unternehmen KI für die IT-Sicherheit einsetzen können

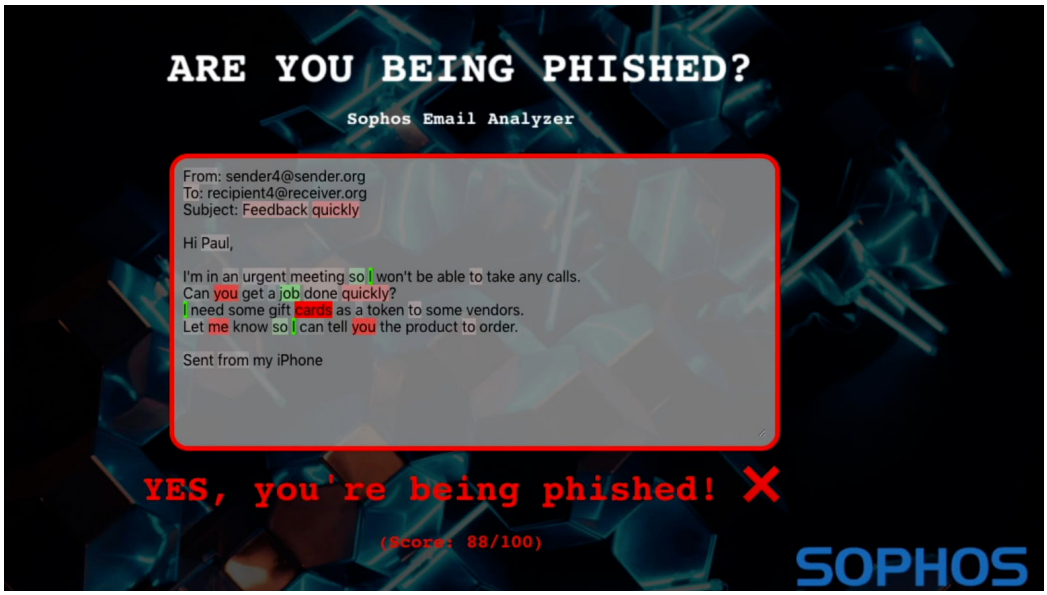
Künstliche Intelligenz und Machine Learning helfen vor allem bei der Erkennung von Mustern, der Bewertung und Priorisierung von Risiken und der Automatisierung von Analyse- und Abwehrmaßnahmen. In folgenden Bereichen ist der Einsatz von KI besonders wichtig und erfolgversprechend:

- **Netzwerkanalyse:** Durch KI lassen sich Risiken und Angriffe im Netz schneller erkennen und abwehren. Das Sophos AI Team setzt beispielsweise im Projekt Next Gen Web Deep Learning ein, um bösartige URLs zu erkennen, Benutzer vor Phishing-Seiten zu warnen und Malware bereits an der Quelle blockieren zu können.

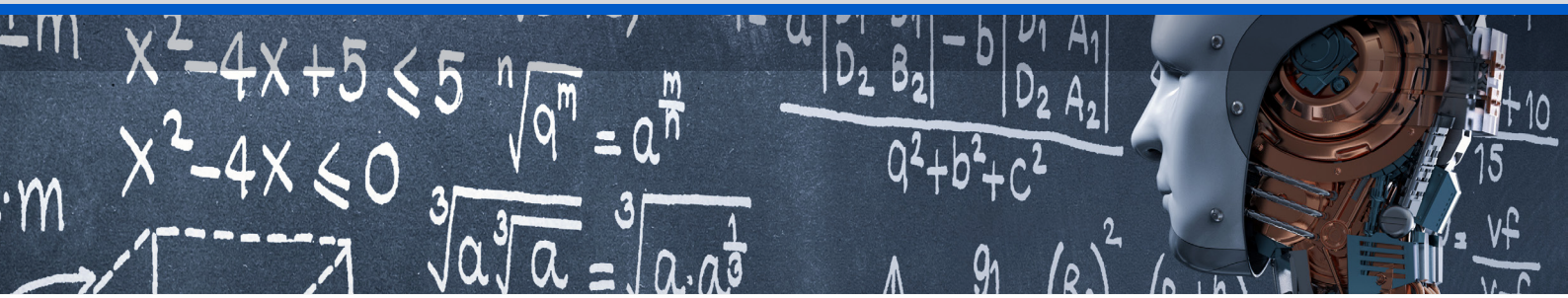
- **Verhaltensanalyse:** Viele Attacken unterlaufen herkömmliche signaturbasierte Abwehrsysteme, indem sie kaum oder gar keine Malware einsetzen, sondern sich mit Bordmitteln und legitim erscheinenden Tools im Netzwerk ausbreiten (mehr dazu im Artikel „Von der Diskette zum Botnetz“, Seite 4). Die KI-gestützte verhaltensbasierte Erkennung spielt daher eine immer wichtigere Rolle. Machine-Learning-Systeme können typisches Benutzerverhalten lernen und so Abweichungen schnell und zuverlässig erkennen. Account-Übernahmen oder maschinelle Angriffe sind damit leichter identifizierbar.

- **Betrugserkennung:** Vor allem Finanzdienstleister und E-Commerce-Anbieter, aber auch andere Unternehmen profitieren von den Fähigkeiten der KI, Millionen von Transaktionen in Echtzeit analysieren und bewerten zu können. Dabei kommen Machine-Learning-Algorithmen zum Einsatz, die zunächst anhand historischer Daten auf die Identifikation von Betrugsmustern trainiert werden. Die Danske Bank konnte beispielsweise mit Deep Learning die Erkennungsrate um 50 Prozent steigern und den Anteil an falsch-positiven Ergebnissen um 60 Prozent reduzieren.

- **Malware-Abwehr:** Die KI-gestützte Analyse bekannter Schadprogramme kann Voraussagen für neue Varianten treffen und so die Erkennung bisher nicht identifizierter Malware verbessern.



Mithilfe von Natural Language Processing und Machine Learning können Phishing-E-Mails zuverlässig erkannt werden.
Quelle: Sophos



Warum KI nicht alle Security-Probleme löst

Künstliche Intelligenz kann die IT-Sicherheit wesentlich verbessern, aber sie ist kein Allheilmittel. Daher sollten sich Sicherheitsverantwortliche nicht zu sehr und nicht allein auf die Leistungsfähigkeit KI-basierter Security-Lösungen verlassen. Ein häufig auftretendes Problem sind beispielsweise falsch positive Ergebnisse wie Alarme, denen keine tatsächliche Bedrohung zugrunde liegt.

Einsatz von Machine Learning – diese Fragen sollten Sie sich stellen:

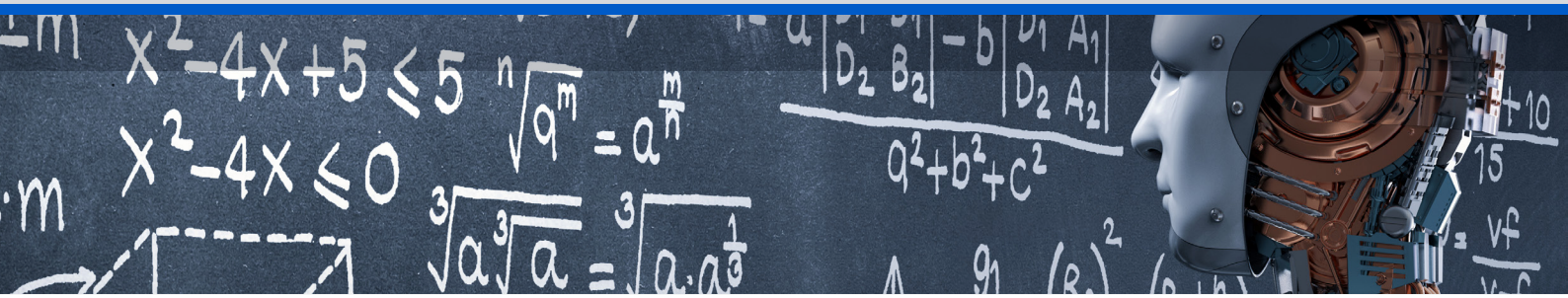
- Habe ich genug Daten, um ein gutes Modell zu trainieren? Wenn nicht Budgetgründe dagegensprechen, ist es fast immer richtig, so viele Daten wie irgend möglich zu nutzen.
- Bei überwachtem Lernen: Sind die Trainingsdaten richtig klassifiziert? Füttere ich das Modell wirklich mit den richtigen Informationen?
- Repräsentieren die Daten die reale Verteilung? Ist genügend Varianz in den Stichproben, um den Problemraum komplett abzudecken?
- Kann ich kontinuierlich neue Daten nachliefern, um das Modell immer auf dem neuesten Stand zu halten?

Hier müssen Experten entscheiden, wie valide die Ergebnisse der Algorithmen sind und eine Balance zwischen möglichst wenig Fehlalarmen bei gleichzeitig möglichst hoher Erkennungsrate finden.

Bei lernenden Systemen stellt darüber hinaus die Bereitstellung passender Trainingsdaten eine Herausforderung dar. Die Algorithmen benötigen große Mengen valider Informationen, um Muster erkennen oder Verhalten klassifizieren zu können. Bevor sich maschinelles Lernen sinnvoll einsetzen lässt, müssen Unternehmen also zunächst einmal die Daten erheben, bereinigen, klassifizieren und zusammenführen, die für das Training notwendig sind. Wie dies gelingen kann und welche Voraussetzungen dafür notwendig sind, untersucht beispielsweise das Sophos AI Team in den Projekten „Behavioral Detection“ und Infrastructure.

Werden personenbezogene Daten verarbeitet, etwa in der Benutzeranalyse oder Betrugserkennung, und haben die Entscheidungen der KI erhebliche Auswirkungen auf Betroffene, sind außerdem datenschutzrechtliche und ethische Fragen zu berücksichtigen. Anonymisierung und Verschlüsselung sind dabei wichtige Bestandteile. Entscheidungswege müssen zudem transparent und erklärbar sein. In seinem Projekt „Interpretable ML“ beschäftigt sich das Sophos AI Team damit, Methoden zu finden, um die „Denkprozesse“ selbstlernender Security-Systeme sichtbar und erklärbar zu machen.

Quelle: Sophos AI Team



Fazit: KI ist kein Allheimittel

Künstliche Intelligenz und Machine Learning (ML) spielen in der IT-Sicherheit eine zunehmende Rolle. Nur mit ihrer Hilfe lassen sich die immer größeren Angriffsflächen schützen und die zunehmend komplexen Bedrohungen abwehren. Der Einsatz von KI und ML ist jedoch nicht trivial. Vor allem bei selbstlernenden Modellen hängt das Ergebnis stark von Menge und Qualität des vorhandenen Trainingsmaterials ab. Unternehmen tun daher gut daran, mit Sicherheitsexperten wie Sophos zusammenzuarbeiten, die mit eigenen AI Teams die Herausforderungen der KI-Integration adressieren und in Produkten und Lösungen wie Sophos Intercept X oder XG Firewall vortrainierte Modelle und KI-basierte Module bieten. ■

> Algorithmen benötigen große Mengen valider Informationen, um Muster erkennen oder Verhalten klassifizieren zu können.

Bild: World Image, Bigstock

Bild: PopTika, Shutterstock

So schützen sich Unternehmen gegen Erpressungstrojaner

Best Practices für die Verteidigung

Was können Unternehmen tun, um Ransomware besser zu erkennen, erfolgreicher abzuwehren und bei einer Infektion den Schaden zu begrenzen?

Ransomware ist nach wie vor eine der größten Bedrohungen für die IT-Sicherheit. Rund 50 Prozent der Unternehmen waren im vergangenen Jahr von einer Attacke betroffen, so der von Sophos in Auftrag gegebene „State of Ransomware 2020"-Report, für den weltweit 5.000 IT-Manager befragt wurden. In fast drei Viertel der Fälle gelang es den Erpressern, Daten zu verschlüsseln. Der durchschnittliche Schaden einer erfolgreichen Ransomware-Attacke beläuft sich auf 750.000 US-Dollar, Prognosen zufolge könnten sich die durch Erpressungstrojaner verursachten Kosten für die Datenwiederherstellung im Jahr 2021 auf mehr als 20 Milliarden US-Dollar summieren.

Die acht wichtigsten Maßnahmen zum Schutz gegen Ransomware

Investitionen in eine effiziente Ransomware-Abwehr amortisieren sich deshalb schnell. Dabei sollten sich IT-Sicherheitsverantwortliche auf folgende Maßnahmen konzentrieren:

1. Patch-Management

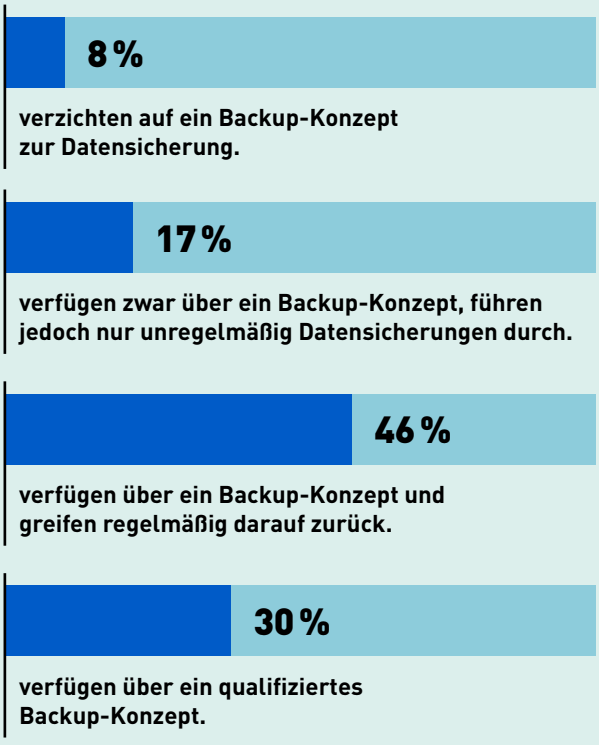
Betriebssysteme und Applikationen sollten immer auf dem neuesten Stand gehalten werden. Vor allem Sicherheits-Updates sind zeitnah einzuspielen. Diese einfache Regel wird viel zu selten befolgt, wie erfolgreiche Angriffe über teils uralte Sicherheitslücken immer wieder zeigen. Bei einem automatisierten Netzwerkscan fand beispielsweise das Security-Unternehmen Positive Technologies in 42 Prozent der Unternehmen Software, für die keine Sicherheits-Updates mehr zur Verfügung gestellt wurde. Die älteste gefundene Sicherheitslücke war 16 Jahre alt!

2. Datensicherung

Ein ähnliches Bild wie beim Patch-Management zeigt sich auch beim Thema Backup and Recovery. Natürlich sollte jedes Unternehmen seine Daten regelmäßig sichern – am besten nach der „3-2-1-Regel": Neben der Produktivversion gibt es mindestens zwei Kopien, die auf zwei unterschiedlichen Medien gespeichert sind und von denen mindestens eines an einem sicheren Ort außerhalb der Firma gelagert wird. Regelmäßige Recovery-Tests, bei denen die Funktionsfähigkeit und Vollständigkeit der Backups überprüft wird, sind ebenfalls Pflicht.

Vor allem kleine und mittlere Unternehmen (KMU) vernachlässigen diese Aufgabe oft, wie der Praxis-report 2020 Mittelstand @ IT-Sicherheit der Initiative Deutschland sicher im Netz (DsiN) zeigt. Rund ein Viertel der befragten KMU sichert Daten gar nicht oder nur unregelmäßig und nur 30 Prozent verfügen über ein qualifiziertes Backup-Konzept. Dabei kann eine gute Datensicherung bei Ransomware-Befall bares Geld sparen. Laut dem Report „State of Ransomware 2020" waren die Kosten der Wiederherstellung nur halb so hoch, wenn die Daten aus einem Backup gerettet werden konnten, als wenn sie durch Lösegeldzahlung entschlüsselt werden mussten.

Setzen Sie auf ein Backup-Konzept, um Ihre Daten regelmäßig zu sichern?



n = 1.038, Quelle: DsiN Praxisreport 2020 Mittelstand @ IT-Sicherheit

3. Kontenverwaltung

Schwache Passwörter machen es Angreifern besonders einfach, Konten zu übernehmen und Erpressungstrojaner einzuschleusen. Neben langen komplexen Passwörtern sollten Unternehmen wo immer möglich eine Mehrfaktor-Authentifizierung (MFA) nutzen, bei der zur Anmeldung neben dem Kennwort ein zusätzlicher Faktor – etwa ein von einem Hardware-Token oder einer Authenticator-App generiertes Einmalpasswort – erforderlich ist. Durch diese einfache Maßnahme lässt sich eine Account-Übernahme effizient verhindern. Laut den Microsoft-Sicherheitsexperten Lee Walker und Alexander Weinert waren von 1,2 Millionen Konten, die im Januar 2020 kompromittiert wurden, 99,99 Prozent nicht durch MFA geschützt. Oder anders ausgedrückt: MFA-gesicherte Accounts machen nur einen winzigen Bruchteil aller kompromittierten Konten aus.

4. Rechtemanagement

Können Angreifer privilegierte Accounts mit Adminrechten übernehmen, haben sie leichtes Spiel und können sich nahezu ungehindert im Netzwerk ausbreiten. Nutzerkonten sollten deshalb immer nur über die absolut notwendigen Rechte verfügen. Die Privilegien sollten außerdem regelmäßig überprüft oder zeitbasiert automatisch abgeschaltet werden. Am weitesten geht dabei der Zero-Trust-Ansatz, bei dem immer nur die aktuell für eine spezifische Aufgabe erforderlichen Rechte gewährt werden.

Nur 30 Prozent der von DsiN befragten deutschen KMU nutzen ein qualifiziertes Backup-Konzept.

5. Schutz der Endpoints

Neben den Nutzerkonten stellen vor allem Endpoints eine Schwachstelle in der Ransomware-Abwehr dar. Daher sollten Unternehmen auf jeden Fall eine leistungsfähige Endpoint-Protection-Lösung wie Sophos Intercept X Endpoint einsetzen, die Ransomware-Angriffe zuverlässig erkennen und stoppen kann. Darüber hinaus sollten Betriebssysteme und Applikationen auf Endgeräten immer auf dem neuesten Stand gehalten werden – idealerweise zentral verwaltet und überwacht.

6. Effektive Perimetersicherung

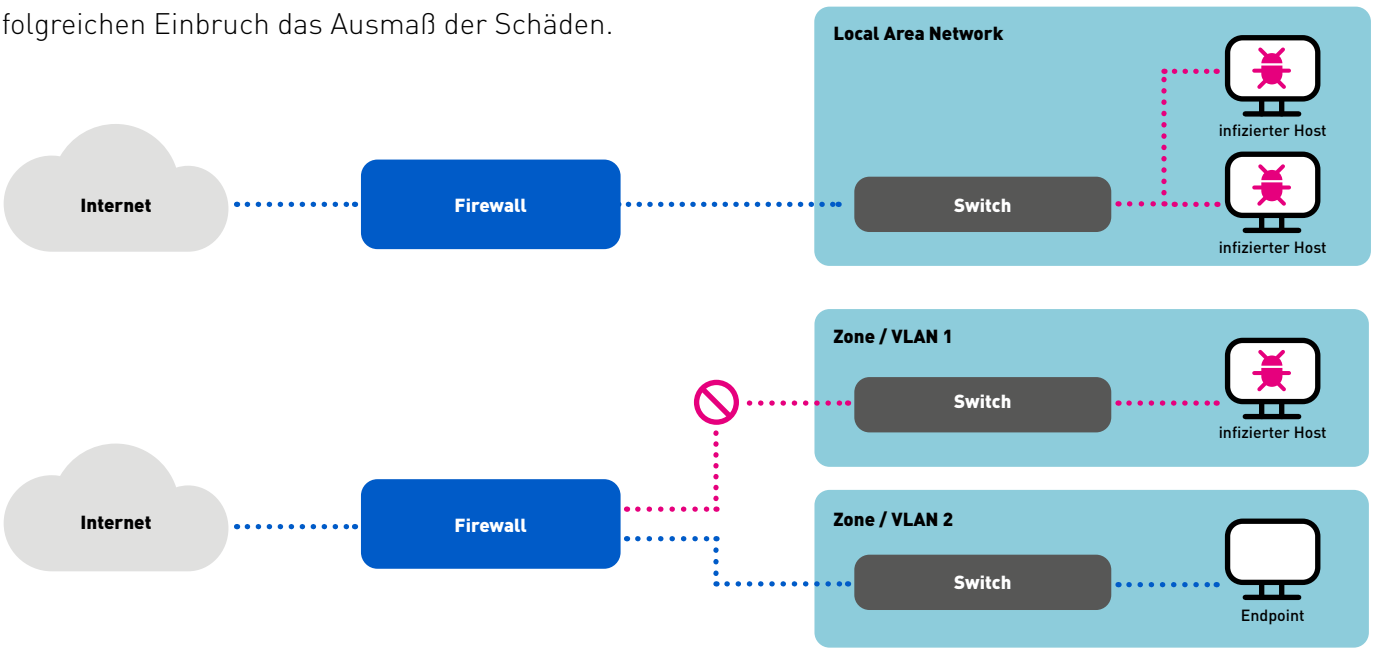
Die Firewall stellt auch heute noch die erste Verteidigungslinie dar. Die Investition in eine moderne, leistungsfähige NextGen Firewall wie die XG Firewall von Sophos ist deshalb ein wichtiger Baustein in der Ransomware-Abwehr. Moderne Technologien wie Sandboxing und KI-basierte Erkennung von Zero-Day-Varianten erhöhen die Erkennungsrate beträchtlich und minimieren bei einem erfolgreichen Einbruch das Ausmaß der Schäden.

7. Minimieren von Remote-Zugriffen

Der Homeoffice-Boom der vergangenen Monate hat IT-Administratoren vor besondere Herausforderungen gestellt. Um die verteilten Endgeräte verwalten und warten zu können, kam vermehrt das Remote Desktop Protocol (RDP) zum Einsatz. RDP ist jedoch nicht für die Nutzung über das öffentliche Internet konzipiert und stellt daher ein hohes Risiko für die IT-Sicherheit dar. Unternehmen sind daher gut beraten, RDP und andere Remote-Verwaltungsprotokolle prinzipiell zu sperren. Ein Zugriff sollte nur von bekannten IP-Adressen aus und nur über ein VPN möglich sein. Der Schutz dieser privilegierten Konten ist über komplexe Passwörter und MFA sicherzustellen.

Eine Netzwerksegmentierung verhindert, dass sich Malware ungehindert im Firmennetz ausbreiten kann.

Quelle: Sophos

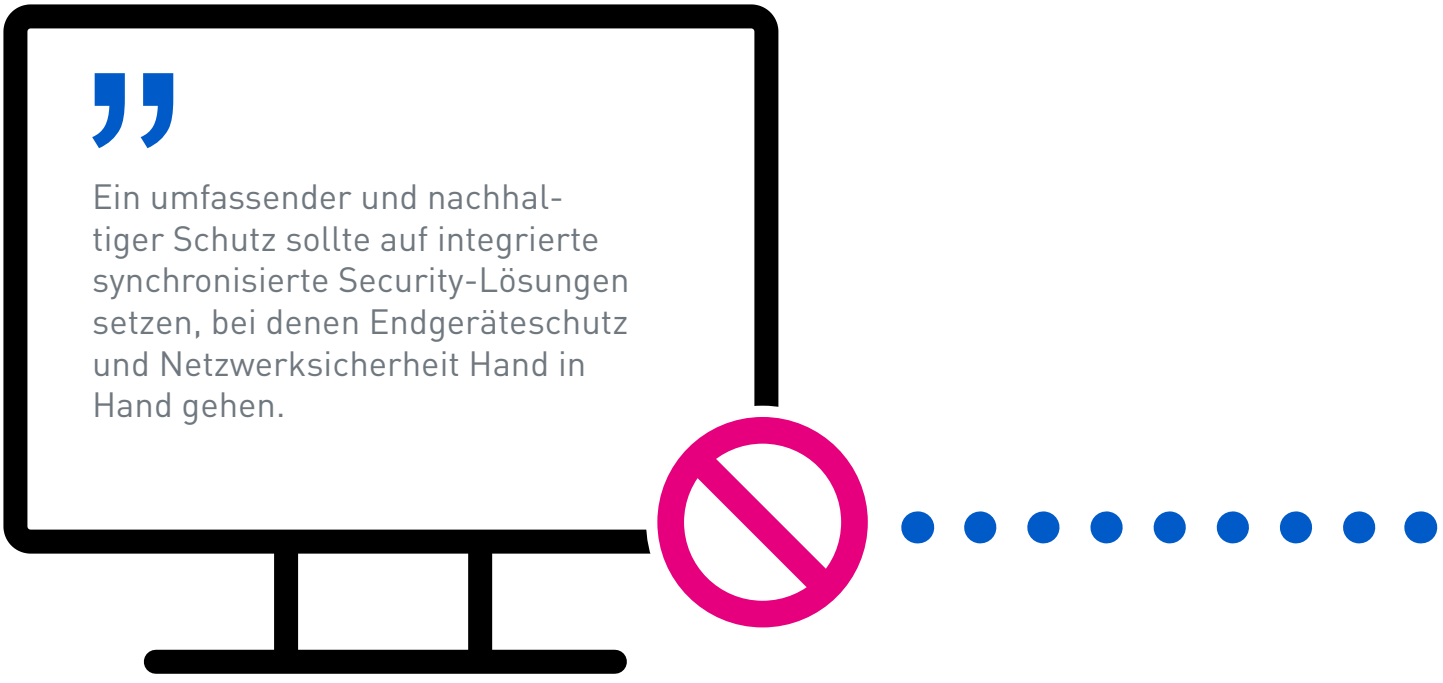


8. Netzwerksegmentierung

Flache Topologien, bei denen alle Endpoints mit einem zentralen Switch verbunden sind, machen es Angreifern besonders einfach. Einmal in das Netzwerk eingedrungen, können sie sich ungehindert ausbreiten. Firmennetze sollten deshalb durch Zonen und VLANs in kleinere Subnetze unterteilt werden. Der Verkehr zwischen den Subnetzen ist über die Firewall zu routen. So lässt sich die Infektion mit Malware auf ein Subnetz begrenzen und der Schaden minimieren.

Fazit: Ransomware-Abwehr braucht eine klare Strategie

Es ist gar nicht so schwer, den Schutz vor Ransomware und den Folgen einer erfolgreichen Infektion zu verbessern. Ein konsistentes Patchmanagement, der Schutz von Konten durch komplexe Passwörter, die Pflicht zur Mehrfaktor-Authentifizierung sowie eine konsistente Backup-Strategie senken das Risiko bereits erheblich. Allerdings greifen die Angreifer zu immer raffinierteren Methoden, und können so häufig auch in gut gesicherte Firmennetze eindringen. Ein umfassender und nachhaltiger Schutz sollte deshalb auf integrierte synchronisierte Security-Lösungen wie Sophos Synchronized Security setzen, bei denen Endgeräteschutz und Netzwerksicherheit Hand in Hand gehen. ■



SOPHOS

INCIDENT RESPONSE GUIDE

Wie Sie sich mit einem Incident-Response-Plan effektiv auf Cybersecurity-Angriffe vorbereiten

„Vor allem die Vorbereitung ist der Schlüssel zum Erfolg.“

Alexander Graham Bell

Wie verhindern Sie am effektivsten, dass sich ein Cyberangriff zu einer weitreichenden Sicherheitspanne entwickelt? Planen Sie im Vorfeld für den Ernstfall.

Nach einer Sicherheitspanne stellen Unternehmen oft fest, dass ihnen ein effektiver Incident-Response-Plan für Cybersecurity-Vorfälle viel Kosten, Probleme und Betriebsunterbrechungen erspart hätte.

Dieser Guide soll Sie bei der Aufstellung Ihres eigenen Incident-Response-Plans unterstützen, damit Sie im Bedarfsfall bestmöglich auf Vorfälle reagieren können. Diese Empfehlungen basieren auf den realen Erfahrungen der Teams Sophos Managed Threat Response und Sophos Rapid Response, die zehntausende Stunden Erfahrung im Umgang mit Cyberangriffen gesammelt haben.

Incident-Response-Plan für Cybersecurity-Vorfälle

Berücksichtigen Sie bei der Erstellung Ihres Incident-Response-Plans die folgenden 10 Punkte:

Incident-Reponse-Plan in 10 Schritten

1. Wichtigste Stakeholder bestimmen
2. Kritische Ressourcen identifizieren
3. Ernstfall durchspielen
4. Security-Tools bereitstellen
5. Für maximale Transparenz sorgen
6. Zugriffskontrolle implementieren
7. In Analyse-Tools investieren
8. Reaktionsmaßnahmen festlegen
9. Awareness-Trainings durchführen
10. Managed Security Service in Anspruch nehmen

1. Wichtigste Stakeholder bestimmen

Für die ordnungsgemäße Vorbereitung auf einen potenziellen Sicherheitsvorfall ist nicht allein Ihr Sicherheitsteam verantwortlich. Tatsächlich wird sich ein Vorfall wahrscheinlich auf fast jede Abteilung in Ihrem Unternehmen auswirken, insbesondere dann, wenn sich der Vorfall zu einer weitreichenden Sicherheitspanne entwickelt. Um Ihre Reaktionsmaßnahmen effektiv zu koordinieren, müssen Sie zunächst festlegen, wer beteiligt werden soll. Häufig werden Vertreter der Geschäftsleitung, der Sicherheits-, IT-, Rechts- und PR-Abteilungen hinzugezogen.

Die Entscheidung, wen Sie in Ihre Planungaktivitäten einbeziehen wollen, sollten Sie bereits im Vorfeld treffen. Darüber hinaus muss eine Kommunikationsmethode eingerichtet werden, um eine schnelle Reaktion zu gewährleisten. Dabei sollte die Möglichkeit berücksichtigt werden, dass Ihre normalen Kommunikationskanäle (z. B. Unternehmens-E-Mails) von einem Vorfall betroffen sein können.

2. Kritische Ressourcen identifizieren

Um Ihre Schutzstrategie zu erarbeiten und im Ernstfall das Ausmaß und die Folgen eines Angriffs bestimmen zu können, müssen Sie ermitteln, welche Ressourcen für Ihr Unternehmen die höchste Priorität haben. Wenn diese Ressourcen schon im Vorfeld klar definiert sind, kann sich Ihr Incident-Response-Team bei einem Angriff gezielt auf unternehmenskritische Ressourcen konzentrieren und Unterbrechungen des Geschäftsbetriebs auf ein Minimum reduzieren.

3. Ernstfall durchspielen

Auch bei der Reaktion auf Vorfälle gilt „Übung macht den Meister". Natürlich ist es schwierig, den intensiven Druck, dem Ihr Team bei einem Sicherheitsvorfall ausgesetzt sein könnte, eins zu eins nachzuspielen. Trotzdem sorgen Theorieübungen dafür, dass Sie im Ernstfall koordinierter und effektiver reagieren können. Neben Theorieübungen (oft im Rahmen von Red-Team-Übungen) sollten Sie jedoch auch weitreichendere Übungen durchführen, in die verschiedene Stakeholder aus dem gesamten Unternehmen mit einbezogen werden.

Im Rahmen von Theorieübungen sollten die Reaktiosmaßnahmen Ihres Unternehmens auf eine Vielzahl möglicher Incident-Response-Szenarien durchgespielt werden. Jedes dieser Szenarien kann auch Stakeholder umfassen, die über das unmittelbare technische Team hinausgehen. Ihr Unternehmen sollte im Voraus festlegen, wer bei der Erkennung eines Angriffs informiert werden muss, auch wenn der Angriff erfolgreich abgewehrt wurde.

Zu den häufigsten Szenarien bei der Reaktion auf Vorfälle gehören:

- **Ein aktiver Angreifer wird in Ihrem Netzwerk erkannt:** In einem solchen Fall ist entscheidend, dass das Response-Team ermittelt, wie ein Angreifer Ihre Umgebung infiltrieren konnte, welche Tools und Techniken verwendet wurden, welche Ressourcen anvisiert wurden und ob Persistenz etabliert wurde. Diese Informationen helfen, die richtige Vorgehensweise zu bestimmen und den Angriff zu neutralisieren.

  Es mag offensichtlich erscheinen, Angreifer so schnell wie möglich aus der Umgebung zu entfernen. Einige Sicherheitsteams entscheiden sich jedoch dafür, den Angreifer zunächst zu beobachten, um wichtige Informationen über seine Ziele und seine Methoden zu sammeln.

- **Datenpanne:** Wenn eine Datenpanne festgestellt wird, sollte Ihr Team ermitteln können, was und wie exfiltriert wurde. Aus diesen Informationen ergibt sich anschließend die angemessene Reaktion, einschließlich der potenziellen Notwendigkeit zur Einhaltung von gesetzlichen und Compliance-Vorschriften, die ggf. eine Benachrichtigung von Kunden oder die Einbeziehung von Rechts- oder Strafverfolgungsbehörden vorsehen.

- **Ransomware-Angriff:** Wenn kritische Daten und Systeme verschlüsselt wurden, muss Ihr Team nach einem Plan vorgehen, um die betroffenen Ressourcen so schnell wie möglich wiederherzustellen. Dazu sollte ein Prozess zur Wiederherstellung von Systemen aus Back-ups gehören. Um sicherzustellen, dass der Angriff nicht wiederholt wird, sobald Sie wieder online sind, sollte das Team untersuchen, ob der Zugriff des Angreifers auch wirklich gekappt wurde. Darüber hinaus sollte eine unternehmensweite Entscheidung darüber getroffen werden, ob Ihr Unternehmen in Extremsituationen bereit wäre, ein Lösegeld zu zahlen, und wenn ja, in welcher Höhe.

- **Kompromittierung eines Systems mit hoher Priorität:** Sollte ein System mit hoher Priorität kompromittiert werden, ist Ihr Unternehmen möglicherweise nicht in der Lage, seinen Geschäftsbetrieb wie gewohnt aufrechtzuerhalten. Zusätzlich zu allen Schritten, die im Rahmen eines Incident-Response-Plans erforderlich sind, sollte Ihr Unternehmen auch die Erstellung eines Business-Recovery-Plans in Betracht ziehen, damit Unterbrechungen des Geschäftsbetriebs im Ernstfall auf ein Minimum reduziert werden.

4. Security-Tools bereitstellen

Am besten schützen Sie sich vor Vorfällen, imdem Sie bereits im Vorfeld Vorkehrungen treffen. Stellen Sie sicher, dass Ihr Unternehmen über geeigneten Schutz für Endpoints, Netzwerk, Server, Cloud, Mobilgeräte und E-Mails verfügt.

5. Für maximale Transparenz sorgen

Ohne die erforderliche Transparenz über alle Vorgänge während eines Angriffs wird Ihr Unternehmen Schwierigkeiten haben, angemessen zu reagieren. Bevor es zu einem Angriff kommt, sollten IT- und Sicherheitsteams sicherstellen, dass sie über das nötige Handwerkszeug verfügen, um das Ausmaß und die Folgen eines Angriffs bestimmen zu können, einschließlich der Ermittlung von Eintrittspunkten und Persistenzpunkten der Angreifer. Um sich vollständige Transparenz zu verschaffen, müssen Sie auch Protokolldaten sammeln, wobei der Schwerpunkt auf Endpoint- und Netzwerkdaten liegt. Viele Angriffe werden erst nach Tagen oder Wochen entdeckt. Daher sollten Sie Verlaufsdaten unbedingt über mehrere Tage oder Wochen (ggf. sogar Monate) speichern und Back-ups erstellen, um im Bedarfsfall zur Vorfallsanalyse darauf zurückgreifen zu können.

6. Zugriffskontrolle implementieren

Angreifer können schwache Zugriffskontrollen ausnutzen, um die Abwehr Ihres Unternehmens zu unterwandern und Berechtigungen auszuweiten. Stellen Sie daher regelmäßig sicher, dass Sie über wirksame Zugriffskontrollen verfügen. Hierzu gehören unter anderem die Bereitstellung einer mehrstufigen Authentifizierung, die Beschränkung von Administrator-Rechten auf möglichst wenige Konten (nach dem Prinzip „Principle of Least Privilege"), die Änderung von Standard-Passwörtern und die Reduzierung der Anzahl der zu überwachenden Zugriffspunkte.

7. In Analyse-Tools investieren

Neben der Sicherstellung der erforderlichen Transparenz sollte Ihr Unternehmen in Tools investieren, die während einer Untersuchung den erforderlichen Kontext liefern.

Zu den am häufigsten verwendeten Incident Response Tools zählen EDR (Endpoint Detection and Response) oder XDR (Extended Detection and Response), mit denen Sie in Ihrer gesamten Umgebung nach Indicators of Compromise (IOCs) und Indicators of Attack (IOA) suchen können. Mithilfe von EDR-Tools können Analysten ermitteln, welche Ressourcen kompromittiert wurden, wodurch sich wiederum Ausmaß und Folgen eines Angriffs bemessen lassen. Je mehr Daten – von den Endpoints und darüber hinaus – erhoben werden, desto mehr Kontext steht für die Analyse zur Verfügung. Dieser Kontext verschafft Ihrem Team mehr Transparenz, um wichtige Fragen zu beantworten: Welche Ressourcen hatten die Angreifer im Visier, wie haben sie sich Zugang zur Umgebung verschafft und besteht die Möglichkeit, dass sie erneut auf die Umgebung zugreifen?

Neben EDR-Tools können moderne Sicherheitsteams auch eine SOAR(Security Orchestration, Automation, and Response)-Lösung zur Unterstützung von Reaktionsworkflows bereitstellen.

8. Reaktionsmaßnahmen festlegen

Einen Angriff zu erkennen, ist nur ein Teil des Prozesses. Um angemessen auf einen Angriff zu reagieren, müssen Ihre IT- und Sicherheitsteams in der Lage sein, eine Vielzahl von Reaktionsmaßnahmen zum Stoppen und Beseitigen von Angreifern einzuleiten. Zu diesen Reaktionsmaßnahmen zählen u. a.:

- Isolieren betroffener Hosts
- Blockieren schädlicher Dateien, Prozesse und Programme
- Blockieren von Command and Control (C2) und schädlichen Website-Aktivitäten
- Einfrieren kompromittierter Konten und Zugriffssperrung für Angreifer
- Beseitigen von Artefakten und Werkzeugen des Angreifers
- Schließen von Eintrittspunkten und Persistenzbereichen, die von Angreifern (internen und externen) genutzt werden
- Anpassen von Konfigurationen (Bedrohungsrichtlinien, Aktivieren von Endpoint-Security und EDR auf ungeschützten Geräten, Anpassen von Ausschlüssen usw.)
- Wiederherstellen betroffener Ressourcen über Offline-Backups

9. Awareness-Trainings durchführen

Kein noch so gutes Trainingsprogramm bietet hundertprozentigen Schutz gegen fest entschlossene Angreifer. Schulungssprogramme (z. B. Phishing Awareness) tragen jedoch dazu bei, Ihr Risiko zu verringern und die Anzahl der Warnmeldungen zu begrenzen, auf die Ihr Team reagieren muss. Mit Tools zur Angriffssimulation können Sie ohne Sicherheitsrisiko reale Phishing-Angriffe auf Ihre Mitarbeiter starten. Diejenigen, die auf die Angriffe hereinfallen, müssen ein Trainingsprogramm absolvieren, und Sie können gezielt Benutzergruppen identifizieren, die weitere Schulungen benötigen.

10. Managed Security Service in Anspruch nehmen

Viele Unternehmen sind nicht in der Lage, ohne fremde Hilfe angemessen auf Vorfälle zu reagieren. Eine schnelle und effektive Reaktion erfordert erfahrene Sicherheitsexperten. Um sicherzustellen, dass Sie die richtigen Maßnahmen ergreifen, sollten Sie ggf. einen externen Dienstleister wie einen MDR-Provider (Managed Detection and Response) hinzuziehen.

MDR-Provider bieten 24/7 Threat Hunting, Analysen und Reaktion auf Vorfälle als Managed Service. MDR-Services helfen Ihrem Unternehmen nicht nur, auf Vorfälle zu reagieren, bevor sich diese zu weitreichenden Sicherheitspannen entwickeln. Sie senken auch die generelle Wahrscheinlichkeit eines Vorfalls. MDR-Services werden immer beliebter: 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 %.

DFIR(Data Forensic Incident Response)-Services werden gelegentlich auch nach einem Vorfall weiter genutzt, um Beweise zum Geltendmachen eines Rechts- oder Versicherungsanspruchs zu sammeln.

Zusammenfassung

Bei einem Cybersecurity-Vorfall zählt jede Sekunde. Ein gut vorbereiteter und durchdachter Reaktionsplan, den alle betroffenen Parteien sofort umsetzen können, kann die Folgen eines Angriffs auf Ihr Unternehmen erheblich abmildern.

Wie Sophos helfen kann

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 Ursachen wiederholt auftretender Vorfälle zu bekämpfen

Weitere Informationen finden Sie unter www.sophos.de/mtr.

Sophos Rapid Response

Sophos Rapid Response bietet Soforthilfe durch ein Expertenteam beim Erkennen und Beseitigen aktiver Bedrohungen. Das Onboarding beginnt binnen weniger Stunden und die Triage ist in der Regel nach 48 Stunden abgeschlossen. Der Service steht sowohl Sophos-Kunden als auch Nichtkunden zur Verfügung.

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

- Schnelles Priorisieren, Eindämmen und Beseitigen aktiver Bedrohungen
- Stoppen von Angreifern in 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 zur Vorgehensweise

Weitere Informationen finden Sie unter www.sophos.de/rapidresponse.

Sophos Intercept X Advanced with EDR

Sophos Intercept X Advanced with EDR hilft dabei, dass Ihre Threat-Hunting-Aktivitäten und IT Operations in Ihrer gesamten Umgebung reibungslos funktionieren. Mit Sophos EDR kann Ihr Team detaillierte Fragen stellen, um komplexe Bedrohungen, aktive Angreifer und potenzielle IT-Schwachstellen zu identifizieren und anschließend schnell geeignete Gegenmaßnahmen zu ergreifen. So können Sie Angreifer in Ihrem Netzwerk aufspüren, die sich bislang unauffällig verhalten haben, aber nur auf eine gute Gelegenheit warten, um Ransomware zu installieren.

Weitere Informationen und eine kostenlose Testversion finden Sie unter www.sophos.de/edr.

* 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

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

SOPHOS

20-10-09 WPDE (DD)

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?

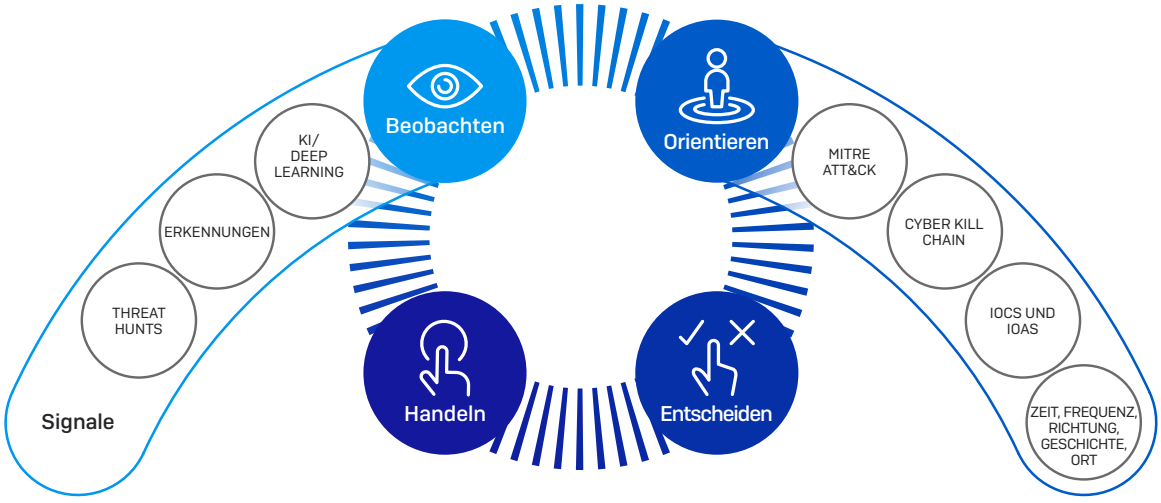
Das Analyse-Framework von Sophos MTR für Threat Hunting und Reaktionsmaßnahmen basiert auf dem als „OODA-Schleife" bekannten militärischen Konzept: beobachten, orientieren, entscheiden, handeln.

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.

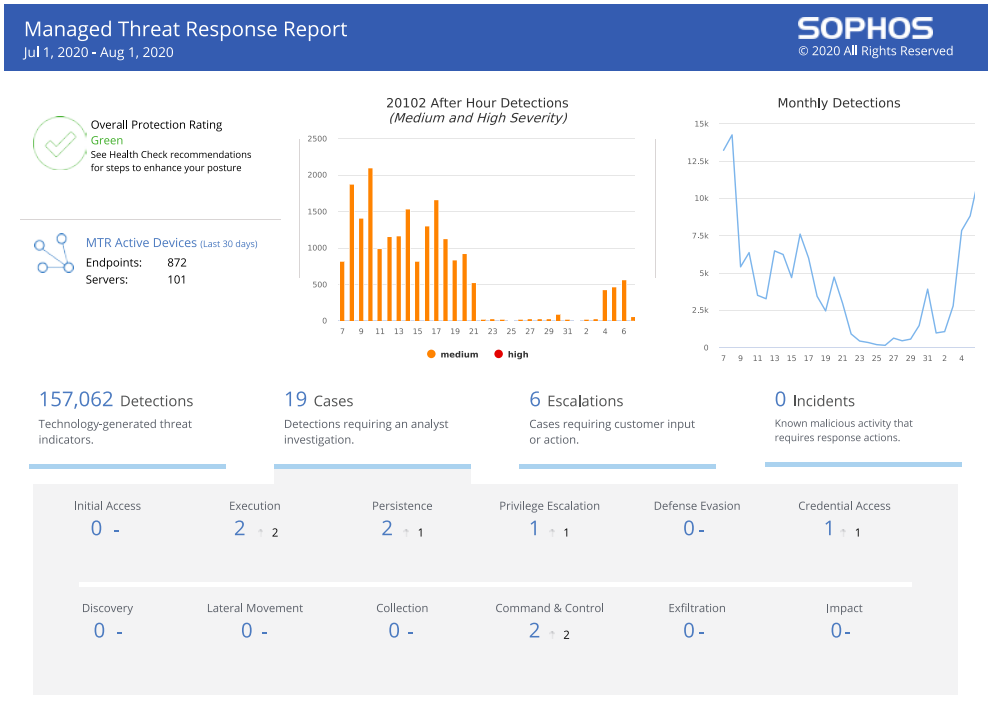
Handeln: Wenn ausreichend Informationen zur Beantwortung der Fragen in der „Entscheiden"-Phase vorliegen, ergreift der Analyst die erforderlichen Maßnahmen.



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:*

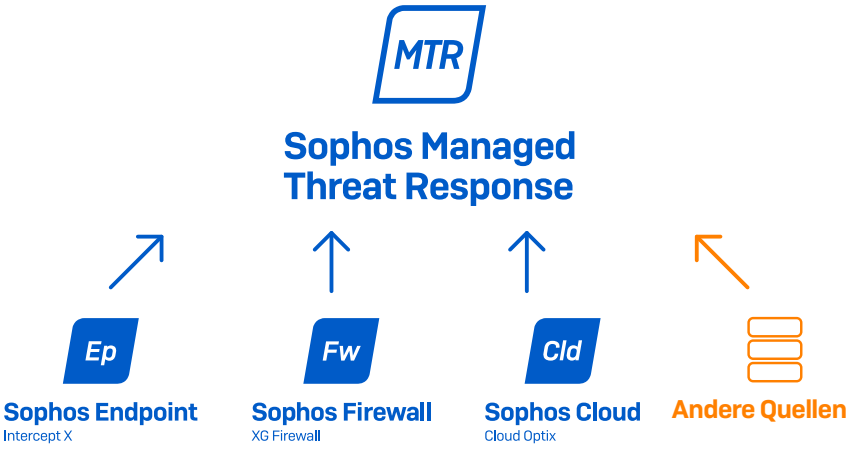
24/7 indizienloses Threat Hunting
Mithilfe von Data Science, Threat Intelligence und der Intuition erfahrener Bedrohungsexperten kombinieren wir verschiedene Informationen (Ihr Unternehmensprofil, hochwertige Assets und Benutzer mit hohem Risiko), um das Verhalten von Angreifern vorherzusagen und neue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