SOPHOS

Endpoint Protection Best Practices zur Abwehr von Ransomware

Tipps zur Konfiguration Ihrer Endpoint-Lösung für optimalen Schutz

Sophos-Whitepaper, Oktober 2024

Einleitung

Ransomware, eine der größten Cyberbedrohungen, kann weitreichende, oft verheerende Folgen nach sich ziehen. Im Rahmen des Sophos Ransomware-Reports 2024 gaben 59 % der Befragten an, dass ihr Unternehmen/ihre Organisation im vergangenen Jahr von Ransomware betroffen war – ein Anstieg von 78 % gegenüber dem Vorjahr. Bei 70 % dieser Vorfälle wurden Daten verschlüsselt.

Insgesamt beliefen sich die durchschnittlichen Kosten für die Bereinigung eines Ransomware-Angriffs auf umgerechnet 2,6 Mio. Euro – ein 50 %iger Anstieg gegenüber dem Vorjahr. Darüber hinaus brauchte über ein Drittel (34 %) der Unternehmen/Organisationen mehr als einen Monat, um sich von Angriffen zu erholen, was die zunehmende Komplexität und Schwere dieser Vorfälle unterstreicht.

Die längeren Wiederherstellungszeiten machen deutlich, dass umfassendere Reaktionsmaßnahmen erforderlich sind. Die wachsende Komplexität belastet auch die internen Sicherheitsteams erheblich. 95 % der Unternehmen und Organisationen meldeten Schwierigkeiten beim Bewältigen grundlegender Sicherheitsaufgaben[1].

Diese Ergebnisse zeigen einmal mehr, wie wichtig es ist, dass Unternehmen und Organisationen ihre Ransomware-Abwehr und Recovery-Strategien verstärken. Denn steigende Kosten, längere Wiederherstellungszeiten und die zunehmende Belastung der Sicherheitsteams machen Ransomware zu einer gewaltigen Bedrohung, die die Aufrechterhaltung der Geschäftsprozesse gefährdet. Eine korrekt konfigurierte Endpoint-Protection-Lösung ist eine der effektivsten Methoden zur Abwehr von Ransomware. In diesem Whitepaper werden die Mechanismen von Ransomware-Angriffen, Strategien zu ihrer Abwehr und Best Practices zur Optimierung des Endpoint-Schutzes behandelt, um für maximale Sicherheit zu sorgen.

1 KMUs und Cybersecurity – Wege aus dem Fachkräftemangel – Sophos

Wie Ransomware-Angriffe ablaufen

Es gibt viele Bedrohungsakteure und viele Arten von Ransomware-Angriffen. Einige sind sehr gezielt, andere opportunistisch. Häufig durchsuchen Angreifer (manchmal auch Cyberkriminelle oder Hacker genannt) Netzwerke nach Schwachstellen oder Sicherheitslücken, um sich Zugriff zu verschaffen. Dies bestätigt auch die Aussage einer Ransomware-Gruppe, die beispielsweise eine Bildungseinrichtung angegriffen hatte:

> *„Sie hatten eine alte kritische Log4j-Schwachstelle auf Horizon nicht behoben, über diese haben wir uns Zugriff verschafft. Wir hatten Ihre Einrichtung nicht gezielt im Visier, sondern sind durch einen Massenscan auf Sie gestoßen."*

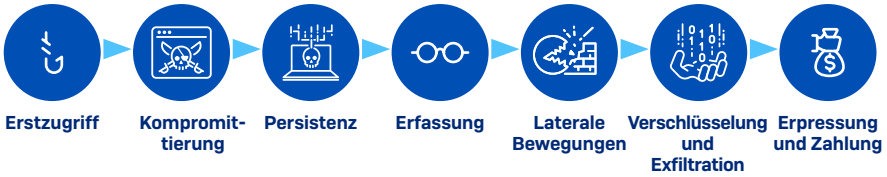
Hier wird deutlich, wie oft Schwachstellen von Angreifern als Einfallstor genutzt werden. Ungepatchte Schwachstellen waren im Jahr 2024 die häufigste Ursache von Ransomware-Angriffen.[2]

Die steigende Zahl an Ransomware-Angriffen in den letzten Jahren ist großenteils auf die zunehmende Verbreitung des sogenannten RaaS-Modells (Ransomware-as-a-Service) zurückzuführen. Dabei entwickelt eine Hackergruppe die Ransomware und vermietet diese dann an die Angreifer. Dieses Geschäftsmodell erleichtert den Einstieg ins Ransomware-Business und macht Ransomware einem immer größeren Kreis von Angreifern zugänglich.

Sobald sich Angreifer in den Umgebungen ihrer Opfer befinden, verbringen sie oft viele Tage, Wochen oder sogar Monate damit, das Netzwerk zu erkunden, Berechtigungen zu eskalieren, Daten zu exfiltrieren und Malware zu installieren. 2023 betrug die durchschnittliche Verweildauer bei Ransomware-Angriffen sechs Tage[3]. Dies verschafft der Cyberabwehr ein Zeitfenster, um Eindringlinge vor dem eigentlichen Angriff zu erkennen und zu stoppen.

2 Ransomware-Report 2024 – Sophos
3 It's Oh So Quiet (?): Active Adversary Report für das 1. Halbj. 2024 – Sophos

Typischer Ablauf eines Ransomware-Angriffs:



Angreifer greifen Unternehmen und Organisationen gezielt zu Zeiten an, in denen sie mit höherer Wahrscheinlichkeit unentdeckt bleiben. Ransomware-Angriffe finden häufig freitags oder samstags statt. Da IT-Abteilungen ihre Monitoringaktivitäten übers Wochenende möglicherweise reduzieren, bietet sich hier für die Angreifer ein günstiges Zeitfenster.

Die Analyse vom Sophos X-Ops Incident-Response-Team zeigt, dass 43 % der Ransomware-Angriffe im Jahr 2023 an diesen beiden Tagen geplant waren und 91 % der Angriffe außerhalb der regulären Geschäftszeiten (Montag bis Freitag von 8 bis 18 Uhr) in der Zeitzone des Opfers begannen, weil die Wahrscheinlichkeit in diesem Zeitraum erkannt zu werden, geringer war[4].

Remote-Ransomware

Dem Digital Defense Report 2023 von Microsoft zufolge gehen rund 60 % der manuell gesteuerten Ransomware-Angriffe mit einer Remote-Verschlüsselung einher. Bei solchen auch als Remote-Ransomware bezeichneten Angriffen nutzen Cyberkriminelle einen kompromittierten Endpoint und verschlüsseln so Daten auf anderen Geräten im gleichen Netzwerk.

Remote-Ransomware zeichnet sich vor allem durch ihre Skalierbarkeit aus: Ein nicht verwalteter oder unzureichend geschützter Endpoint kann die gesamte Organisation anfällig für Remote-Verschlüsselung machen, auch wenn auf anderen Geräten moderne Sicherheitslösungen installiert sind.

Unternehmen und Organisationen müssen sich der Bedrohung durch Remote-Ransomware-Angriffe bewusst sein, da nicht alle Endpoint-Security-Lösungen effektiv davor schützen.

Bereitstellung von Ransomware über RDP

RDP (Remote Desktop Protocol) spielte bei 90 % der von Sophos in 2023 analysierten Cyberangriffe eine Rolle. Im Vorjahr lag der Anteil noch bei 83 %[5].

RDP- und Desktop-Sharing-Tools wie Virtual Network Computing (VNC) erleichtern die Remote-Systemverwaltung. Ohne angemessene Sicherheitsvorkehrungen können sie jedoch von Ransomware-Angreifern zweckentfremdet werden, um Zugriffsrechte zu erweitern, Zugangsdaten zu stehlen, sich lateral fortzubewegen, Backdoors zu installieren, gefälschte Konten zu erstellen und unerkannt zu bleiben.

Um sich vor Angriffen zu schützen, muss folglich verhindert werden, dass Angreifer RDP für den externen Zugriff, internen Zugriff oder für laterale Bewegungen nutzen können. Viele Unternehmen und Organisationen stellen mittlerweile sicher, dass RDP nicht extern exponiert wird, aber Angreifer nutzen das Protokoll auch häufig, um sich lateral innerhalb einer Organisation zu bewegen.

4 So stoppen Sie aktive Angreifer: Neueste Erkenntnisse aus der Cybersecurity-Praxis – Sophos

5 It's Oh So Quiet (?): Active Adversary Report für das 1. Halbj. 2024 – Sophos

IT Best Practices zum Schutz vor Ransomware

Um sich vor Ransomware und anderen Bedrohungen zu schützen, benötigen Sie nicht nur modernste Sicherheitslösungen. Auch mit Ihrem Verhalten können Sie Ihren Schutz maßgeblich beeinflussen. Stellen Sie sicher, dass Sie diese Best Practices befolgen (die Liste erhebt keinen Anspruch auf Vollständigkeit):

1. Installieren Sie Patches frühzeitig und oft

Wussten Sie schon?
Ransomware-Angriffe haben immer negative Folgen. Angriffe, die von ungepatchten Schwachstellen ausgehen, sind jedoch besonders gravierend. So meldeten Unternehmen und Organisationen, die von diesen Angriffen betroffen waren, viermal höhere Bereinigungskosten und längere Wiederherstellungszeiten als solche, bei denen kompromittierte Zugangsdaten als Einfallstor dienten.

Die Ausnutzung ungepatchter Schwachstellen war 2024 die Hauptursache von Ransomware-Angriffen[6]. Malware und Angreifer nutzen Sicherheitslücken in gängigen Anwendungen aus. Je früher Sie Ihre Endpoints, Server, Mobilgeräte und Anwendungen patchen, desto weniger Sicherheitslücken können von Cyberkriminellen ausgenutzt werden.[7]

2. Verwenden Sie sichere Passwörter

Über ein schwaches und leicht zu erratendes Passwort können sich Hacker in Sekundenschnelle Zugriff auf Ihr Netzwerk verschaffen. Nutzen Sie deshalb komplexe Passwörter ohne Bezug auf Ihre Person mit mindestens 12 Zeichen und einer Mischung aus Groß-und Kleinschreibung sowie zufälligen Satzzeichen (z. B.: Hey527!miTn8?).

3. Aktivieren Sie die mehrstufige Authentifizierung (MFA)

MFA bietet eine zusätzliche Schutzebene nach dem ersten Faktor, der oft ein Passwort ist. MFA für alle Anwendungen und Services zu aktivieren, die diese unterstützen, ist daher von entscheidender Bedeutung. Angreifer erwerben häufig gültige Zugangsdaten im Dark Web oder versuchen aktiv, an Zugangsdaten zu gelangen, sobald sie sich in Ihrer Umgebung befinden. MFA stellt für Angreifer eine zusätzliche Hürde dar und verhindert, dass sie sich ohne weitere Prüfung als berechtigter Benutzer authentifizieren können. Verwenden Sie Phishing-resistente Passkeys, sofern Ihre Anwendungen dies unterstützen.

4. Regeln Sie den internen und externen Netzwerkzugriff

Lassen Sie Netzwerk-Ports nicht geöffnet. Sperren Sie den RDP-Zugriff Ihres Unternehmens und andere Remote-Management-Protokolle. Stellen Sie sicher, dass Remote-Benutzer eine Zero-Trust Network Access (ZTNA)-Lösung verwenden, um auf Anwendungen, Services und andere Unternehmensressourcen zuzugreifen.

5. Überwachen Sie Administrator-Rechte

Überprüfen Sie kontinuierlich die lokalen und Domain-Administrator-Rechte. Behalten Sie im Auge, wer Administrator-Rechte hat, und entziehen Sie die Rechte ggf., wenn sie nicht benötigt werden. Bleiben Sie nicht länger als nötig als Administrator angemeldet.

6. Sichern Sie Daten regelmäßig an mehreren Standorten und führen Sie routinemäßig Wiederherstellungsverfahren durch

In unserer Befragung für den Ransomware-Report 2024 konnten 68 % der IT-Manager die bei einem Angriff verschlüsselten Daten mithilfe von Backups wiederherstellen. Sichern Sie Ihre Daten regelmäßig an mehreren Standorten und schützen Sie Cloud-Backups mittels MFA. Spielen Sie die Datenwiederherstellung aus Backups durch, um im Falle eines Angriffs problemlos Ihre Daten wiederherstellen zu können. Überwachen Sie verdächtige Aktivitäten, um Backups vor potenziellen Bedrohungen zu schützen.

7. Entfernen Sie unnötige Anwendungen

In vielen Fällen zweckentfremden Angreifer regulär installierte Anwendungen für ihre böswilligen Zwecke. Dieser Ansatz wird auch als „Living-off-the-Land" bezeichnet und erschwert die Unterscheidung zwischen legitimer Nutzung und schädlichen Aktivitäten. Wägen Sie daher sorgfältig ab, welche Anwendungen auf den Computern Ihrer Benutzer wirklich notwendig sind, und unterbinden Sie die Installation aller anderen Anwendungen.

8. Identifizieren Sie ungeschützte Geräte in Ihrem Netzwerk

Angreifer suchen gezielt Geräte ohne Endpoint-Schutz, um unbemerkt in Ihrer Umgebung Fuß zu fassen. Diese ungeschützten Geräte können für Remote-Ransomware-Angriffe genutzt werden.

6 Ransomware-Report 2024 – Sophos
7 Ungepatchte Schwachstellen: Der verheerendste Angriffsvektor bei Ransomware – Sophos

Best Practices für Ihre Endpoint Protection

Eine effektive Methode zum Schutz vor Ransomware-Angriffen ist der Einsatz einer Endpoint Protection-, Endpoint Detection and Response(EDR)- oder Extended Detection and Response(XDR)-Lösung, die modernste Abwehrtechnologien und Threat-Hunting-Funktionen umfasst.

Fehlkonfigurationen von Sicherheitstools gelten als das größte Cybersecurity-Risiko für Unternehmen und Organisationen[8]. Schlecht konfigurierte Richtlinien-Einstellungen, Ausschlüsse und andere Faktoren können die Sicherheit beeinträchtigen. Stellen Sie sicher, dass der Endpoint-Schutz korrekt konfiguriert ist, um maximalen Schutz zu bieten.

Zum Schutz Ihrer Endpoints vor Ransomware empfehlen wir Ihnen diese Best Practices:

1. Aktivieren Sie alle empfohlenen Richtlinien und Funktionen

Es mag offensichtlich klingen, aber tatsächlich ist dies die effektivste Methode, um den Schutz Ihrer Endpoint-Security-Lösung optimal zu nutzen.

Richtlinien und Einstellungen sind dazu da, bestimmte Bedrohungen zu stoppen. Deshalb sollten Sie regelmäßig überprüfen, ob alle Schutzoptionen auch wirklich aktiviert sind. So stellen Sie sicher, dass Ihre Endpoints optimal geschützt bleiben – vor aktueller und neuer Ransomware. Stellen Sie sicher, dass Funktionen zum Erkennen dateiloser Angriffstechniken und Verhaltenstechnologien aktiviert sind. Außerdem empfehlen wir Folgendes:

A) Aktivieren Sie den Manipulationsschutz (Tamper Protection)

Dadurch verhindern Sie, dass Ihre Endpoint-Schutz-Software manipuliert oder komplett entfernt wird. Wenn Angreifer sich Zutritt auf ein System verschafft haben, ist ihre erste Aktion meist das Deaktivieren oder Entfernen des Endpoint-Schutzes.

B) Aktivieren Sie eine forensische Protokollierung (idealerweise in der Cloud)

Sie wurden kompromittiert? Dann möchten Sie wissen, wie es dazu kommen konnte, um ein Wiederauftreten in Zukunft zu verhindern. Angreifer löschen jedoch häufig Systemprotokolle, um ihre Spuren zu verwischen, und entfernen dabei forensische Beweise, sodass es schwierig ist, den Angriffsverlauf nachzuvollziehen. Unter Umständen verlieren Sie auch den Zugriff auf Ihr Gerät. Durch das Aufzeichnen von Aktivitäten in der Cloud behalten Sie stets Zugriff auf wichtige Informationen.

C) Stellen Sie sicher, dass Content- und Produktupdates für Ihre Endpoint Protection aktiviert sind

Um mit der sich schnell entwickelnden Bedrohungslandschaft Schritt zu halten und sich vor neuen Bedrohungen zu schützen, ist es von entscheidender Bedeutung, Sicherheitsprodukte regelmäßig mit neuen Daten zu aktualisieren. Wenn Sie Produkt- und Content-Updates deaktivieren, verliert Ihr Schutz im Laufe der Zeit an Wirksamkeit.

2. Überprüfen Sie regelmäßig Ihre Ausschlüsse

Mit Ausschlüssen legen Sie fest, dass vertrauenswürdige Verzeichnisse und Dateitypen nicht auf Malware überprüft werden müssen. So können Sie beispielsweise Systemverzögerungen reduzieren und das Risiko von falsch-positiven Sicherheitswarnungen minimieren.

Im Laufe der Zeit führt eine wachsende Liste von Ausschlüssen zu Sicherheitslücken, die Gegner ausnutzen könnten. Malware, die es schafft, in ausgeschlossene Verzeichnisse zu gelangen – vielleicht versehentlich von einem Benutzer verschoben – kann erfolgreich sein.

Überprüfen Sie regelmäßig Ihre Liste von Ausschlüssen in Ihren Richtlinien-Einstellungen und entfernen Sie so viele wie möglich. Alle unverzichtbaren Ausschlüsse sollten so spezifisch definiert werden wie möglich. Anstatt beispielsweise das Verzeichnis oder Laufwerk einer Datenbank auszuschließen, schließen Sie nur bestimmte Dateien mit ihrem vollständigen Pfad aus. Dadurch wird verhindert, dass Malware Ihre Sicherheitsmaßnahmen umgeht und aus demselben Ordner ausgeführt wird.

3. Aktivieren Sie MFA für Ihre Sicherheitskonsole

Dadurch wird ein sicherer Zugriff auf die Plattform gewährleistet, über die Ihr Endpoint-Schutz und andere Sicherheitskontrollen verwaltet werden. So verhindern Sie, dass Angreifer mutwillig Ihre Einstellungen ändern oder den Schutz deaktivieren/entfernen, wodurch Ihre Endpoints und Server anfällig für Angriffe werden.

4. Achten Sie auf eine gute IT-Praxis und Sicherheitsvorgaben

Überprüfen Sie regelmäßig, dass alle Sicherheitsvorgaben eingehalten werden. Dies ist wichtig, damit Ihre Endpoints und die installierte Software effizient laufen. So senken Sie nicht nur Ihr Cybersecurity-Risiko, sondern können auch viel Zeit bei der Bereinigung eventueller Vorfälle sparen.

8 KMUs und Cybersecurity – Wege aus dem Fachkräftemangel – Sophos

Die Implementierung eines gezielten Programms für diese Überprüfung ist besonders wichtig für den Schutz vor Ransomware-Angriffen und anderen Cybersecurity-Bedrohungen. So können Sie beispielsweise sicherstellen, dass RDP nur dort ausgeführt wird, wo Sie es benötigen und erwarten. Außerdem können Sie regelmäßige Überprüfungen auf Konfigurationsprobleme durchführen, die Geräteleistung überwachen und unerwünschte oder nicht benötigte Programme entfernen. Im Rahmen einer solchen Überprüfung können Sie ermitteln, ob Software-Anwendungen aktualisiert werden müssen. Außerdem können Sie so auch sicherstellen, dass regelmäßig Daten-Backups erstellt werden.

5. Suchen Sie proaktiv nach Angreifern in Ihrer Umgebung

Cyberkriminelle gehen immer raffinierter vor und nutzen oft legitime Tools und gestohlene Zugangsdaten, um unerkannt zu bleiben. Um diese „Living-off-the-Land"-Angriffe zu erkennen und zu stoppen, ist es wichtig, proaktiv nach komplexen Bedrohungen und aktiven Angreifern zu suchen. Sollten Sie fündig werden, müssen Sie auch in der Lage sein, diese schnell zu stoppen.

Technologien wie Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR) bieten Ihrem internen Sicherheitsteam Funktionen zur Bedrohungssuche, -analyse und -beseitigung. Da Angreifer jedoch häufig außerhalb der Bürozeiten zuschlagen, ist Ihr Sicherheitsteam möglicherweise gar nicht anwesend und kann demzufolge auch keine Gegenmaßnahmen ergreifen. Viele Unternehmen tun sich schwer, ihren Schutz rund um die Uhr zu gewährleisten, um komplexe Ransomware-Angriffe auch außerhalb der Geschäftszeiten erfolgreich abzuwehren. Deshalb werden sogenannte MDR Services (Managed Detection and Response) für viele Unternehmen und Organisationen immer wichtiger.

Mehrschichtige Sicherheitstechnologien zum Schutz vor Ransomware

„Vorbeugen ist besser als heilen" – dies trifft auch im Bereich Cybersicherheit zu. So ist es einfacher, ein Problem frühzeitig zu beseitigen, als später den Schaden zu beheben. Zum Schutz Ihres Unternehmens/Ihrer Organisation vor Ransomware eignet sich ein mehrschichtiger Sicherheitsansatz. Dabei arbeiten mehrere Technologien zusammen und sorgen so für maximalen Schutz und Transparenz. Unternehmen und Organisationen können zunächst Endpoint-Schutz implementieren und infolge ganz nach Bedarf weitere Funktionen hinzufügen, wodurch sie den Schutz und die Transparenz im Laufe der Zeit verbessern.

Beispiele:

- **Eine Firewall** zum Erkennen und Blockieren von verdächtigem Netzwerkverkehr und zur Abwehr von Bedrohungen. Eine Firewall hat Einblick in Datenverkehr, der in Ihr Netzwerk eingeht oder von ihm abgeht. Über dieses Tool haben Sie jedoch keinen Einblick in den Netzwerkverkehr innerhalb der Umgebung.
- **Lösungen zur Network Detection and Response (NDR)** können ungeschützte Geräte und Angreifer erkennen, die sich lateral in Ihrem Netzwerk bewegen. NDR bietet Einblick in den internen Netzwerkverkehr, den eine Firewall nicht erkennen kann.
- **Eine XDR-Plattform** kann Funktionen zur Bedrohungssuche, -analyse und -beseitigung bereitstellen. Zudem lässt sie sich in andere IT-Security-Lösungen integrieren und liefert über eine zentrale Plattform einen umfassenden Einblick in alle Sicherheitskontrollen.
- **MDR Services** bieten 24/7 Threat Hunting durch ein Team von Sicherheitsexperten. Diese sind darauf spezialisiert, Cyberangriffe zu erkennen und zu bekämpfen, gegen die reine Technologie-Lösungen machtlos sind. Ihr MDR Service sollte eine umfassende Reaktion auf Vorfälle ohne Zusatzkosten bieten, um Angriffe vollständig einzudämmen und abzuwehren. Für einen vollständigen Einblick in verdächtige Aktivitäten in Ihrer gesamten Umgebung muss sich ein MDR Service in Ihre vorhandenen Cybersecurity-Tools integrieren lassen. MDR bietet den besten Schutz vor komplexen, manuell gesteuerten Ransomware-Angriffen.
- **External Attack Surface Management (EASM)- und Vulnerability Management (VM)-Lösungen** dienen der Erkennung und Priorisierung von Schwachstellen. So können Sie fehlende Patches ermitteln und installieren, bevor Angreifer diese ausnutzen können.

Effektiver Schutz vor Ransomware mit Sophos

Sophos Endpoint nutzt ein umfassendes Sicherheitskonzept, das auf präventiver Cybersecurity gründet und sich nicht auf eine einzelne Sicherheitstechnologie verlässt. Mit hochmodernen Technologien blockiert Sophos Endpoint die meisten Angriffe, u. a.:

- **Lückenlose Ransomware-Abwehr** schützt vor lokalen und Remote-Ransomware-Angriffen, einschließlich neuer Varianten. Schädliche Verschlüsselungen werden in Echtzeit erkannt und betroffene Dateien automatisch in ihren Ursprungszustand zurückversetzt, wodurch geschäftliche Auswirkungen minimiert werden.
- **Anti-Exploit-Technologie** schützt vor dateilosen Angriffen und Zero-Day-Exploits, indem die von Angreifern verwendeten Techniken entlang der gesamten Angriffskette gestoppt werden.
- **Adaptive Attack Protection** bietet einmalige adaptive Abwehrmechanismen, die sich dynamisch an aktive und manuell gesteuerte Angriffe anpassen. Verstärkte Abwehrmaßnahmen, die dynamisch aktiviert werden, verhindern, dass Angreifer weitere Maßnahmen ergreifen, da die Angriffsfläche reduziert und der Angriff unterbrochen wird.

Sophos Endpoint lässt sich sehr einfach einrichten und verwalten. Sophos Endpoint installieren und loslegen! Die empfohlenen Schutztechnologien sind standardmäßig aktiviert. So verfügen Sie sofort über die stärksten Schutzeinstellungen, ohne eine Feinabstimmung vornehmen zu müssen. Bei Bedarf ist auch eine granulare Kontrolle verfügbar.

Sie verwalten Sophos Endpoint über **Sophos Central,** die Cybersecurity-Plattform, der weltweit die meisten Kunden vertrauen. Diese leistungsstarke, cloudbasierte Cybersecurity-Management-Plattform bringt alle Sophos Next-Gen-Sicherheitslösungen an einem zentralen Ort zusammen und setzt für den Zugriff MFA voraus.

Sophos-Kunden verwalten ihren Endpoint-Schutz über Sophos Central und profitieren von der Funktion „Account Health Check". Dadurch werden Security-Posture-Abweichungen in Richtlinien und Ausschlüssen sowie andere Fehlkonfigurationen mit hohem Risiko identifiziert, sodass Administratoren Probleme mit nur einem Klick beheben können.

Sophos XDR – Proaktive Tools für Threat Hunting und Durchsetzung von Sicherheitsvorgaben

Sophos XDR ist eine Unified Detection and Response Plattform, die auf dem präventiven Cybersecurity-Konzept von Sophos Endpoint basiert. Mit dieser Lösung können Sie in kürzester Zeit mehrphasige Bedrohungen an allen wichtigen Angriffsflächen erkennen, analysieren und aktiv bekämpfen.

Die Sophos-Technologien sind vollständig in die Sophos XDR-Plattform integriert und ermöglichen durch ihr nahtloses Ineinandergreifen bestmögliche Sicherheitsergebnisse. Durch schlüsselfertige Integrationen mit einem umfassenden Ökosystem von Endpoint-, Firewall-, Netzwerk-, E-Mail-, Identity-, Produktivitäts-, Cloud-Security- sowie Backup- und Recovery-Lösungen anderer Anbieter steigern Sie zudem den ROI Ihrer bestehenden Cybersecurity-Investitionen.

Die Tools und Funktionen von Sophos XDR sind gezielt darauf ausgelegt, die Effizienz von Sicherheitsanalysten und IT-Administratoren zu steigern.

- Mithilfe von KI-priorisierten Erkennungen auf allen wichtigen Angriffsflächen können verdächtige Aktivitäten erkannt werden, die sofortige Aufmerksamkeit erfordern.
- Erkennungen und Fälle werden automatisch MITRE ATT&CK-Taktiken zugeordnet, sodass Sie Lücken in Ihrer Abwehr leicht identifizieren können.
- Mit automatisierten Aktionen wie Prozessbeendigung, Ransomware-Rollback und Netzwerk-Isolierung dämmen Sie Bedrohungen blitzschnell ein und sparen wertvolle Zeit. Mit ergebnisorientierten generativen KI-Funktionen von Sophos XDR können Sicherheitsanalysten Angreifer schneller aus der Umgebung entfernen. So steigern Sie die Effizienz der Analysten und stärken das Vertrauen der Unternehmen in ihre Cybersicherheit.

Sophos MDR – Managed Detection and Response 24/7

Sophos MDR ist ein 24/7 Managed Security Service, der von hochqualifizierten Experten bereitgestellt wird und Sie vor neuartigen Bedrohungen und aktiven Angreifern mit hohem Gefährdungspotenzial schützt. Der Sophos MDR-Service bietet optimalen Ransomware-Schutz.

Mit der Servicestufe MDR Complete erhalten Sie eine umfassende Reaktion auf

Vorfälle ohne Obergrenze oder weitere Gebühren. Unsere Experten können umfangreiche Threat-Response-Maßnahmen für Sie ergreifen, um Angreifer remote zu stören, einzudämmen und vollständig aus der Umgebung zu entfernen.

Wie Sophos XDR ist Sophos MDR eng mit allen anderen Sophos-Produkten verknüpft und erfasst von diesen Telemetriedaten. Außerdem kann Sophos MDR auch auf dieselbe Weise mit einer Vielzahl von Sicherheitsprodukten anderer Hersteller kombiniert werden, um die Transparenz und Sicherheit in Ihrer gesamten Umgebung weiter zu erhöhen.

Sophos Incident Response Services Retainer – ein Incident Response Service auf Standby

Ein jederzeit abrufbereites Incident-Response-Team in der Rückhand zu haben, bevor Angreifer zuschlagen, ist die einzige Möglichkeit, Zeit zu sparen, Kosten zu senken und die Auswirkungen einer Sicherheitsverletzung (z. B. Ransomware-Angriffe) abzumildern.

Der **Sophos Incident Response Services Retainer** ist eine jährliche Subscription. Diese bietet im Bedarfsfall Zugang zu Incident-Response-Experten, die umgehend in Ihrer Umgebung aktiv werden, um Angreifer zu stören, einzudämmen und vollständig aus der Umgebung zu entfernen. Die Subscription umfasst auch Ressourcen zur Vorbereitung auf kritische Vorfälle, mit denen Sie Ihren Sicherheitsstatus verbessern und die Wahrscheinlichkeit von Sicherheitsvorfällen minimieren.

Hinweis: Der Sophos Incident Response Service Retainer ist nicht erforderlich, wenn Sie die Servicestufe Sophos MDR Complete abonnieren, in der eine umfassende Incident Response standardmäßig enthalten ist.

Sophos Managed Risk – Service zum Management von Schwachstellen und externen Angriffsflächen

Ungepatchte Schwachstellen sind die Hauptursache für Ransomware-Angriffe. Daher ist es wichtig, alle kritischen Risiken in Ihrer Umgebung zu identifizieren, zu analysieren und zu priorisieren, bevor sie zum Problem werden. Sophos Managed Risk basiert auf branchenführender Tenable-Technologie und kann Sie hierbei unterstützen.

Mit **Sophos Managed Risk** erkennen unsere erfahrenen Analysten gefährliche Cybersecurity-Schwachstellen und potenzielle Angriffsvektoren in Ihrer Umgebung. So lassen sich Angriffe verhindern, bevor Ihr Geschäftsbetrieb gestört wird.

Fazit

Ransomware entwickelt sich ständig weiter. Nach wie vor sehen sich viele Unternehmen und Organisationen so zur Zahlung von Lösegeld gezwungen. Daher ist es für Sie entscheidend, Angreifer daran zu hindern, in Ihr Unternehmen oder Ihre Organisation einzudringen. Falls sie es doch tun, müssen Sie die Bedrohung schnell erkennen und stoppen. Wir empfehlen Ihnen, IT und Endpoint Best Practices zu befolgen, Ihre Endbenutzer zu schulen und gegenüber Bedrohungen und Angreifern in Ihrer Umgebung immer wachsam zu bleiben. Mit einem präventiven, mehrschichtigen Cybersecurity-Ansatz mit 24/7 Detection and Response ist Ihr Unternehmen/Ihre Organisation bestens aufgestellt, sich vor Ransomware und den neuesten Bedrohungen zu schützen.

Sie möchten mehr darüber erfahren, wie Sophos Sie bei der Optimierung Ihrer Ransomware-Abwehr unterstützen kann? Sprechen Sie mit einem unserer Ansprechpartner oder besuchen Sie unsere Website unter www.sophos.de

2024-10-01 (WP-NP)

SOPHOS