SOPHOS

Best Practices zum Schutz Ihres Netzwerks vor Ransomware

Stärken Sie Ihren Schutz gegen Ransomware und andere Angriffe

Sophos-Whitepaper, Oktober 2024

Ransomware ist noch immer auf dem Vormarsch

Ransomware zählt nach wie vor zu den größten Cyberbedrohungen. Sie kann weitreichende, oft verheerende Folgen nach sich ziehen. 59 % der im Rahmen unseres Ransomware-Reports 2024 Befragten gaben an, dass ihre Organisation im vergangenen Jahr von Ransomware betroffen war. Bei 70 % dieser Vorfälle verschlüsselten Angreifer Daten.

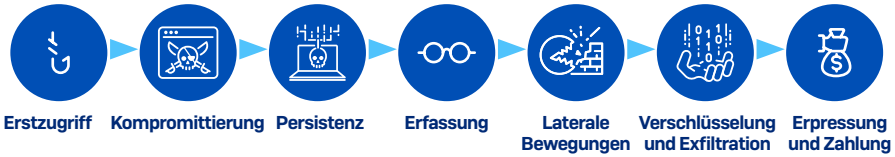
Der Anstieg der Angriffszahlen in den letzten Jahren spiegelt vermutlich den wachsenden Erfolg von Ransomware-as-a-Service wider, die Angreifern den Einstieg in die Cyberkriminalität erleichtert.

Die durchschnittlichen Kosten zur Bereinigung nach einem Ransomware-Angriff betragen mittlerweile 2,73 Millionen US$ – ein Anstieg von 50 % gegenüber dem Vorjahr. Außerdem benötigten 34 % der Unternehmen mehr als einen Monat, um sich von den Auswirkungen eines Angriffs zu erholen. Die längere Wiederherstellungszeit verdeutlicht die zunehmende Komplexität der Angriffe und die starke Belastung der Sicherheitsteams. So stufen 95 % grundlegende Sicherheitsaufgaben als Herausforderung ein[1].

Diese Trends zeigen ganz klar: Eine starke Ransomware-Abwehr und robuste Wiederherstellungsstrategien sind unabdingbar. Neben Endpoint-Schutz bieten insbesondere optimierte Netzwerk-Security-Lösungen effektiven Schutz vor Ransomware. In diesem Whitepaper erfahren Sie mehr über den Ablauf von Ransomware-Angriffen und erhalten Strategien zur Prävention sowie Tipps zum Optimieren Ihrer Netzwerksicherheit.

Wie Ransomware-Angriffe ablaufen

Um zu verstehen, wie man sich vor Ransomware-Angriffen schützt, muss man wissen, wie diese Angriffe ablaufen. In der Regel geschieht bei einem Ransomware-Angriff Folgendes:



Heutzutage nutzen Angreifer oft legitime IT- und Anwendertools wie VPN oder Remote Desktop Protocol (RDP), um sich Zugriff zu verschaffen. RDP spielte bei mindestens 90 % der von Sophos in 2023 analysierten Cyberangriffe eine Rolle. Im Vorjahr lag der Anteil noch bei 83 %.[2]

Diese Tools werden von vielen Mitarbeitern bei der täglichen Arbeit genutzt, wodurch es oft schwer ist, solche Ransomware-Angriffe direkt zu erkennen. Das Problem: Häufig wird der Verwendung dieser Tools einfach gutgläubig vertraut, d. h. jede Person, die auf ein VPN oder RDP zugreifen kann, wird als vertrauenswürdig angesehen – eine Praxis, die sich immer wieder als unklug erwiesen hat.

Best Practices zum Schutz Ihres Netzwerks vor Ransomware

Nachdem wir uns einen kurzen Überblick über die Methodik von Ransomware-Angriffen und Bedrohungsakteuren verschafft haben, erfahren Sie im Folgenden, wie Sie Ihre Netzwerksicherheit mit drei Best Practices optimieren können:

1. Verringern Sie Ihre Angriffsfläche

2. Prüfen und schützen Sie den Netzwerkverkehr beim Netzwerk-Eintritt

3. Identifizieren und stoppen Sie alle Bedrohungen, die in das Netzwerk eindringen

1 KMUs und Cybersecurity – Wege aus dem Fachkräftemangel, Sophos

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

Verringern Sie Ihre Angriffsfläche

Alle Netzwerkinfrastrukturen, die dem öffentlichen Internet ausgesetzt sind, sind ein potenzielles Ziel für Angreifer. Daher gilt es, diese Angriffsfläche so weit wie möglich zu reduzieren. Unsere Empfehlungen:

1. Konsolidieren Sie Ihre Netzwerk-Infrastruktur

Die meisten Unternehmen schützen ihr Netzwerk mit einer Firewall. Viele verfügen auch über einen VPN Concentrator oder zusätzliche Netzwerk-Gateway-Produkte. Reduzieren Sie diese Infrastruktur so weit wie möglich. Upgraden Sie zu einer Firewall mit integriertem Remote-Zugriff, die vorhandene VPN Concentrators ersetzt. Idealerweise sollte die Firewall zudem den Wechsel zu Zero Trust Network Access (ZTNA) ermöglichen (mehr dazu erfahren Sie weiter unten).

2. Halten Sie Patches und Firmware auf dem neuesten Stand

Wussten Sie schon?

Ransomware-Angriffe haben immer negative Folgen. Angriffe, die von ungepatchten Schwachstellen ausgehen, sind jedoch besonders gravierend. So meldeten Unternehmen, die von diesen Angriffen betroffen waren, viermal höhere Bereinigungskosten als solche, bei denen kompromittierte Zugangsdaten als Einfallstor dienten.[3]

Ungepatchte Schwachstellen waren 2024 die Hauptursache von Ransomware-Angriffen[4]. Daher ist es entscheidend, dass Sie Ihre Firewall und andere Infrastruktur-Firmware immer auf dem neuesten Stand halten. Prüfen Sie regelmäßig (mindestens einmal im Monat), ob Firmware-Updates verfügbar sind. Planen Sie die Installation dieser Updates zu günstigen Zeitpunkten.

3. Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur auf maximale Sicherheit ausgelegt ist

Achten Sie darauf, dass alle Netzwerkinfrastruktur-Produkte, die mit dem Internet verbunden sind, wie etwa Ihre Firewall, auf maximale Sicherheit ausgelegt sind. Entscheiden Sie sich für eine Firewall, die speziell dafür entwickelt und gehärtet wurde, um Angriffen standzuhalten. Funktionen, auf die Sie unbedingt achten sollten:

- **Keine standardmäßige Internetverbindung**: Die Firewall sollte nicht standardmäßig auf das Internet zugreifen können. Sie sollte granulare Zugriffskontrollen bieten, damit Sie genau steuern können, was exponiert ist.
- **Gehärtetes Design:** Die Firewall sollte Sicherheitsmechanismen wie Multi-Faktor-Authentifizierung (MFA) und Containerisierung aller exponierten Services oder Portale enthalten, damit Angreifer potenzielle Schwachstellen nicht ausnutzen können.
- **Automatisierte Hotfixes:** In der sich schnell entwickelnden Bedrohungslandschaft sind automatische Hotfixes von entscheidender Bedeutung. Zum Schutz vor neuen Bedrohungen muss die Firewall in der Lage sein, Updates sofort auch ohne größere Firmware-Updates zu erhalten.
- **Proaktive Überwachung**: Die herstellerseitige Überwachung des gesamten Kundenstamms kann helfen, Angriffe schneller zu erkennen und darauf zu reagieren.

4. Minimieren Sie mit dem Internet verbundene Server und Anwendungen

Wenn Sie Remote Desktop Tools (RDP oder VNC) nutzen oder eines Ihrer Systeme für das Remote-Management direkt über das Internet zugänglich ist, deaktivieren Sie den Zugriff umgehend. Wie wir bereits gesehen haben, sind diese Tools ein gängiger Vektor für Angriffe auf Netzwerke. Überprüfen Sie die NAT-Regeln Ihrer Firewall, um sicherzustellen, dass nur unbedingt erforderliche Komponenten exponiert sind. Schützen Sie Ihre Server und Admin-Systeme mit ZTNA. So sorgen Sie dafür, dass diese für Angreifer unsichtbar sind und Mitarbeiter bei Bedarf weiterhin sicher per Remote-Zugriff darauf zugreifen können.

5. Ersetzen Sie Remote Access VPN durch ZTNA

Zero Trust Network Access (ZTNA) ist der moderne Nachfolger von Remote Access VPN. ZTNA eliminiert das inhärente Vertrauen und den breiten Zugriff, wie es bei VPN üblich ist, und verwendet stattdessen die Prinzipien von Zero Trust – Vertrauen Sie nichts, überprüfen Sie alles. ZTNA bietet deshalb deutlich mehr Sicherheit. Zudem ist die Lösung einfacher zu verwalten, ist benutzerfreundlicher und bietet mehr Transparenz im Vergleich zu Remote Access VPN.

ZTNA eliminiert anfällige VPN-Clients, nutzt Multifaktor-Authentifizierung (MFA)

3 Ungepatchte Schwachstellen: Der verheerendste Angriffsvektor bei Ransomware – Sophos
4 Ransomware-Report 2024 – Sophos

und Gerätezustand zur Zugriffskontrolle und bietet nur Zugriff auf bestimmte Netzwerkanwendungen, wodurch Ihr Netzwerk effektiv mikrosegmentiert wird. Wählen Sie eine Firewall, die ZTNA integriert. So erhalten Sie eine Lösung mit einem einzigen Gateway, die zentral über eine einzige Konsole verwaltet wird. Im Idealfall müssen Sie dabei nur einen einzigen Agent für ZTNA und Endpoint-Schutz auf Ihren Benutzergeräten installieren.

6. Verwenden Sie starke Passwörter und Multi-Faktor-Authentifizierung (MFA)
Nach wie vor gehen zahlreiche Cyberangriffe von schwachen Passwörtern und fehlender Multi-Faktor-Authentifizierung (MFA) aus. Stellen Sie sicher, dass alle Systeme in Ihrem Netzwerk starke Passwörter und MFA verwenden, auch wenn sie nicht mit dem Internet verbunden sind, um Brute-Force-Angriffe zu verhindern.

Überprüfen und schützen Sie Ihren Netzwerkverkehr beim Netzwerk-Eintritt

Ein weiterer, bei Angreifern beliebter Angriffsvektor ist regulärer Internet- und E-Mail-Verkehr, der Ihre Infrastruktur durchläuft. Online- und E-Mail-Tools sind unverzichtbar und lassen sich nicht einfach deaktivieren. Stellen Sie daher sicher, dass dieser Datenverkehr angemessen geprüft und geschützt wird. Mit den folgenden empfohlenen Best Practices können Sie Ihren Netzwerkverkehr schützen:

1. Untersuchen Sie verschlüsselten Datenverkehr
Mehr als 90 % des Netzwerkverkehrs sind verschlüsselt. Zwar ist dies in Sachen Datenschutz positiv, sicherheitstechnisch jedoch eine Herausforderung, da herkömmliche Bedrohungserkennungsverfahren verschlüsselte Datenströme nicht erfassen. Angreifer nutzen diese Sicherheitslücke aus. Viele Firewalls stoßen bei der Entschlüsselung und Überprüfung des hohen Anteils an verschlüsseltem Datenverkehr an ihre Grenzen. Wählen Sie eine Firewall, die speziell für die stark verschlüsselte Welt von heute entwickelt wurde und entscheiden kann, welche Datenströme entschlüsselt werden müssen und welche nicht. Ihre Firewall sollte den Datenverkehr effizient entschlüsseln und prüfen, ohne die Gesamtleistung des Netzwerks zu beeinträchtigen. Außerdem muss sie in der Lage sein, verschlüsselte Bedrohungen zu erkennen.

2. Nutzen Sie IPS
Viele Systeme in Ihrem Netzwerk können ungepatchte Sicherheitslücken aufweisen. Dabei kann es sich um Windows- oder Linux-Systeme, IoT-Geräte wie Kameras, industrielle Kontrollsysteme oder sonstige Systeme handeln, die mit Ihrem Netzwerk verbunden sind – kabelgebunden oder über WLAN. Alle Firewalls verfügen in der Regel über IPS (Intrusion Prevention Systems). Dabei handelt es sich um Technologien zur Erkennung von Netzwerkangriffen, die auf Sicherheitslücken abzielen. Leider nutzen viele Unternehmen diese Technologie nicht. Vergewissern Sie sich, dass IPS Ihren gesamten Netzwerkverkehr abdeckt. Datenverkehr aus dem Internet hat natürlich besonders hohe Priorität, doch auch interner Datenverkehr ist wichtig, da Sie so potenzielle Angreifer abfangen, die sich möglicherweise bereits in Ihrem Netzwerk befinden.

3. Nutzen Sie Zero-Day-Bedrohungsschutz
Viele Angreifer nutzen eigens für diesen Zweck entwickelte, in Dateien eingebettete Malware, die unwissentlich aus dem Internet heruntergeladen wird. Da diese Bedrohungen noch nie zuvor beobachtet wurden, werden sie als „Zero-Day" bezeichnet. Herkömmlicher Virenschutz erfasst diese Zero-Day-Bedrohungen in der Regel nicht. Um neue und entstehende Bedrohungen zu erkennen, benötigen Sie Threat-Scanning-Lösungen, die künstliche Intelligenz oder Machine Learning nutzen und anhand von Millionen von Malware-Samples trainiert wurden. Stellen Sie sicher, dass Ihre Firewall-Inspection in der Lage ist, eine Zero-Day-Analyse durchzuführen – idealerweise in Echtzeit in der Cloud. So wird Ihre Firewall entlastet und Sie profitieren sofort vom globalen Austausch von Bedrohungsinformationen.

4. Implementieren Sie robuste E-Mail-Sicherheitsmaßnahmen und schulen Sie Ihre Benutzer in der Erkennung von Phishing-E-Mails
Wir alle kennen jemanden, der schon einmal unwissentlich auf einen bösartigen Link in einer scheinbar seriösen E-Mail geklickt hat. Phishing ist und bleibt ein gängiger Angriffsvektor für Cyberkriminelle. Jedoch lässt sich das Risiko mit wirksamen Schutzlösungen und Benutzertraining minimieren.

Suchen Sie nach einer E-Mail-Security-Lösung, die proaktiv schädliche E-Mails aus den Posteingängen der Benutzer herausfiltern kann. Selbst wenn einige E-Mails durchkommen, sollte die Lösung in der Lage sein, diese rückwirkend zu entfernen oder die URLs umzuschreiben, um eine Überprüfung beim Anklicken zu ermöglichen. Ihre E-Mail-Security-Lösung sollte außerdem Benutzertests und -Trainings umfassen. So können Sie feststellen, ob Ihre Mitarbeiter Phishing-Angriffe erkennen, und Ihre Mitarbeiter lernen, worauf es zu achten gilt.

Erkennen und stoppen Sie alle Bedrohungen, die in das Netzwerk eindringen

Trotz aller Bemühungen müssen Sie davon ausgehen, dass ein Angreifer irgendwann in Ihr Netzwerk eindringen wird. Kommt es zu einem Vorfall, sind die Erkennungs- und Reaktionszeiten entscheidend. Doch genau hier stoßen die meisten Network-Security-Lösungen an ihre Grenzen. Suchen Sie nach Lösungen, die Folgendes leisten:

1. Ihr Netzwerk segmentieren

Wenn ein Angreifer in Ihr Netzwerk eindringt, wird er versuchen, sich darin zu bewegen. Dank Mikrosegmentierung Ihres Netzwerks können Sie jegliche Bewegung einschränken und Angreifer so früher entdecken. Stellen Sie sicher, dass Ihr Netzwerk in mehrere granulare Bereiche oder VLANs unterteilt ist, die über verwaltete Switches und Access Points sowie über Ihre Firewall verbunden sind, auf der IPS diesen Datenverkehr überprüft. Nutzen Sie ZTNA auch für den Remote-Zugriff, da Ihre Anwendungen so ebenfalls effektiv mikrosegmentiert werden.

2. Angreifer über mehrere Vektoren hinweg sofort erkennen

Wenn ein Angreifer in Ihr Netzwerk eindringt, ist eine schnelle Erkennung entscheidend. Da 91 % der Ransomware-Angriffe außerhalb der üblichen Geschäftszeiten[5] stattfinden, benötigen Sie eine Cybersecurity-Lösung, die rund um die Uhr aktiv ist, um Angreifer in Echtzeit zu erkennen und Bedrohungsdaten sofort auszutauschen. Dabei reicht es nicht aus, wenn Administratoren lediglich benachrichtigt werden. Ihre Lösung sollte eine nahtlose Kommunikation zwischen allen Sicherheitslösungen ermöglichen, um eine schnelle, koordinierte Reaktion und Eindämmung zu gewährleisten.

Wählen Sie eine vollständig integrierte Lösungssuite, die Firewalls, Endpoint-Schutz, Switches, Wireless, ZTNA und E-Mail-Sicherheit abdeckt. Diese Tools sollten Bedrohungsdaten sowohl mit Ihrem Sicherheitsteam als auch untereinander austauschen und automatisch auf Angriffe reagieren – auch mitten in der Nacht.

3. Automatisch und adaptiv auf aktive Bedrohungen reagieren

Wenn eine Bedrohung erkannt wird – durch Sie, einen Sicherheitsanalysten, Ihre Endpoints, die Firewall oder eine andere Komponente Ihres Cybersecurity-Systems – benötigen Sie eine sofortige, koordinierte Reaktion, um die Bedrohung einzudämmen und zu beseitigen. Die Lösung? Eine Firewall (und integrierte Sicherheitslösungen) mit folgenden Funktionen:

- **Automatische Reaktion auf aktive Bedrohungen** ohne manuelles Eingreifen, sodass der Angriff sofort eingedämmt wird.
- **Dynamisches Blockieren von Bedrohungen** ohne neue Firewallregeln oder Administrator-Eingriffe.
- **Nahtlose Integration mit anderen Security-Tools**, wie Endpoint-Schutz oder ZTNA, für eine koordinierte Abwehr, die laterale Bewegungen verhindert und die Bedrohung isoliert.

5 „Übliche Geschäftszeiten" bezieht sich auf 8–18 Uhr, Montag–Freitag | So stoppen Sie aktive Angreifer: Neueste Erkenntnisse aus der Cybersecurity-Praxis – Sophos

Mehrschichtige Sicherheitstechnologien zum Schutz vor Ransomware

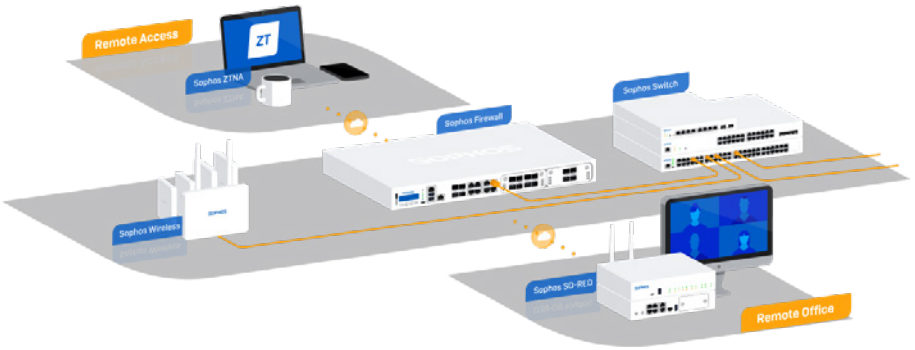
Wie das Sprichwort sagt: „*Vorsicht ist besser als Nachsicht*“. Es ist in der Tat viel einfacher, Probleme im Vorfeld zu stoppen, als den Schaden später zu beheben. Zum Schutz Ihres Unternehmens vor Ransomware eignet sich ein mehrschichtiger Sicherheitsansatz. Dabei arbeiten mehrere Technologien zusammen und sorgen so für maximalen Schutz und Transparenz. Unternehmen können zunächst eine Firewall und Endpoint-Schutz implementieren und infolge ganz nach Bedarf weitere Schichten hinzufügen, wodurch sie den Schutz und die Transparenz im Laufe der Zeit verbessern.

Beispiele:

- **Eine NDR-Lösung (Network Detection and Response)** erkennt ungeschützte Geräte und Angreifer, die sich lateral im Netzwerk bewegen. NDR bietet Einblick in den internen Netzwerkverkehr, den eine Firewall nicht erkennen kann.
- **Eine Extended Detection and Response (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 Transparenz über 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 Angreifer vollständig einzudämmen und abzuwehren. Für maximale Transparenz über Ihre gesamte 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.

Sophos schützt Ihr Netzwerk vor Ransomware

Sophos bietet alles, was Sie zum Schutz Ihres Netzwerks vor Ransomware und anderen Angriffen benötigen. Mit Sophos erhalten Sie eine integrierte Palette an Cybersecurity-Lösungen, inkl. Firewalls, ZTNA, Switches, Wireless, Remote Edge Devices, E-Mail-Schutz und Endpoint Protection der nächsten Generation für alle Ihre Geräte und Server.



Und das Beste ist: Sie verwalten alles über Sophos Central, eine zentrale Cloud-Management-Plattform, die alle Informationen zu Bedrohungen von unseren Lösungen und Experten zusammenführt. Dies ermöglicht eine automatische Reaktion auf Bedrohungen.

Sophos bietet ein Maß an Integration und Synchronisation, das einzigartig auf dem Markt ist. Und diese Funktionalitäten zählen unbestritten zu den wichtigsten Komponenten beim Schutz vor aktiven Angreifern.

Synchronized Security in Aktion

Wird ein kompromittierter Host erkannt, isoliert die Sophos Firewall diesen sofort. Dabei ignorieren sichere, von Sophos verwaltete Endpoints Datenverkehr von diesem Gerät automatisch. Darüber hinaus verwerfen Ihre Switches und Access Points Pakete von dem kompromittierten Host und ZTNA verhindert, dass sich ein kompromittiertes Gerät mit Ihren Anwendungen verbindet. Eine aktive Bedrohung wird sofort und automatisch im Netzwerk isoliert und kann sich nicht ausbreiten.

Network Security von Sophos auf einen Blick

Sophos Firewall

Die Sophos Firewall und die Appliances der XGS-Serie helfen Ihnen, Ihr Netzwerk vor Ransomware zu schützen, da Best Practices in das Design integriert sind:

- **Konzipiert für maximale Sicherheit**: Wir haben nicht nur viel investiert, um sicherzustellen, dass Ihre Sophos Firewall die sicherste Firewall auf dem Markt ist. Wir arbeiten auch kontinuierlich daran, sie unantastbar für Hacker zu machen und gleichzeitig Ihr Netzwerk und Ihr Unternehmen durch proaktives Monitoring vor zukünftigen Angriffen zu schützen.
- **ZTNA-Integration**: Die Sophos Firewall verfügt über ein integriertes ZTNA-Gateway. So können Sie schnell und mühelos ohne weitere Installationen von herkömmlichem VPN zu Zero-Trust wechseln. Ein weiteres Plus: ZTNA wird über die gleiche Cloud-Konsole verwaltet wie Ihre Firewall. Auf diese Weise lassen sich Ihre Anwendungen und Ihr Remote-Zugriff einfach absichern und segmentieren.
- **KI-gestützter Schutz vor Zero-Day-Bedrohungen**: Die Sophos Firewall integriert modernste KI-Technologien und erkennt und stoppt so Ransomware-Angriffe, bevor sie ins Netzwerk eindringen. Mit einer Kombination aus fortschrittlicher KI und Machine Learning, die auf Millionen von Samples trainiert wurde, sowie Echtzeit-Sandboxing erkennen unsere Lösungen auch bisher unbekannte Bedrohungen.
- **Active Threat Response**: Die Sophos Firewall erkennt sofort aktive Angreifer im Netzwerk anhand unterschiedlicher Threat Intelligence-Quellen und koordiniert Synchronized-Security-Maßnahmen, um eine aktive Bedrohung automatisch zu isolieren, bevor sie zu einem echten Problem werden kann.

Sophos ZTNA

Sophos ZTNA verbindet Ihre Benutzer einfach und transparent mit relevanten Anwendungen und Systemen dank besserer Segmentierung, Sicherheit und Transparenz als bei traditionellem Remote Access VPN.

- **Mikrosegmentierung und Schutz Ihrer Anwendungen**: Dank der Mikrosegmentierung in Sophos ZTNA können Sie einen sicheren Zugriff auf Ihre Anwendungen gewährleisten – egal, ob Ihre Anwendungen lokal, in einem Rechenzentrum oder in Ihrer Public Cloud-Infrastruktur gehostet werden. Ihre Anwendungen sind für die Außenwelt unsichtbar.
- **Abwehr von Ransomware und anderen Bedrohungen**: Die Gefahr, dass Ransomware und andere Bedrohungen ein kompromittiertes Endgerät infizieren und sich von dort aus im gesamten Netzwerk verbreiten, besteht bei ZTNA nicht mehr. Denn Benutzer und Geräte haben nur auf bestimmte Anwendungen expliziten richtlinienbasierten Zugriff. Dadurch werden die größten VPN-Schwachstellen, wie implizites Vertrauen und weitreichender Netzwerkzugriff, eliminiert.
- **Zugriff von kompromittierten Geräte blockieren**: ZTNA ermöglicht Ihren Remote-Mitarbeitern, von überall aus sicher auf die Daten und Anwendungen zuzugreifen, die sie benötigen. Wird ein Benutzergerät kompromittiert, so wird der Anwendungszugriff des Geräts automatisch deaktiviert, bis das Gerät bereinigt wurde, um laterale Bewegungen zu verhindern.

Sophos Switches und Access Points

Sophos Switches und Access Points sind nahtlos mit der Sophos Firewall und der gesamten Cybersecurity-Plattform von Sophos integriert und überzeugt durch die automatische Reaktion auf Bedrohungen sowie die zentrale Verwaltung über eine einzige Konsole:

- **Active Threat Response**: Sophos Switches und Access Points unterstützen außerdem Active Threat Response, um aktive Angreifer zu stoppen, bevor Schaden entsteht. Ein kompromittiertes Gerät lässt sich sofort auf dem Switch oder Access Point blockieren, um laterale Bewegungen zu verhindern – auch im gleichen LAN-Segment.
- **Verwaltung über eine zentrale Konsole**: Sophos Switches und Access Points werden mit Ihrer Firewall, ZTNA und anderen Sophos-Produkten zentral in Sophos Central verwaltet. Sie profitieren dabei von maximaler Transparenz und komfortabler Verwaltung.

Sophos Email

Sophos Email bietet modernsten E-Mail- und Anti-Phishing-Schutz und wehrt E-Mail-Bedrohungen ab:

- **Phishing-Schutz**: Mithilfe KI-gestütztem Natural Language Processing (NLP) ist Sophos Email in der Lage, Betrugsversuche, wie E-Mail-Impersonation, zu erkennen, die Benutzern vortäuschen sollen, dass ein Phishing-Versuch seriös ist. Sophos Email umfasst zudem eine mehrschichtige Analyse auf Malware

und schädliche URLs mit Time-of-Click-Schutz, der URLs umschreibt und beim Anklicken eine zusätzliche Überprüfung erzwingt. Außerdem erkennt Sophos Email verdächtige Absender mit diversen Technologien, die SPF, DKIM und DMARC nutzen und Anomalien in E-Mail-Headern analysieren.

- **Mitarbeiter-Trainings in Phish Threat**: Sophos Phish Threat bietet Angriffssimulationen und Schulungen für Ihre Mitarbeiter. Die Lösung unterstützt Sie dabei, Ihre Mitarbeiter in der Erkennung von verdächtigen E-Mails und Phishing-Angriffen zu schulen. Außerdem können Sie Ihre Benutzer mit Sophos Phish Threat testen und feststellen, welche Mitarbeiter zusätzliche Trainings benötigen.

Fazit

Ransomware entwickelt sich ständig weiter. Nach wie vor sehen sich viele Unternehmen so zur Zahlung von Lösegeld gezwungen. Ihr Ziel ist es, Angreifer daran zu hindern, in Ihr Unternehmen einzudringen. Falls sie es doch tun, müssen Sie sie schnell erkennen und stoppen. Wir empfehlen Ihnen, die Best Practices für die Netzwerksicherheit in diesem Guide zu befolgen, Ihre Endbenutzer zu schulen und gegenüber Bedrohungen und Angreifern in Ihrer Umgebung immer wachsam zu bleiben. Mit einem mehrschichtigen Cybersecurity-Ansatz mit 24/7 Detection and Response ist Ihr Unternehmen 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

2024-10-14 (WP-PC)

SOPHOS