CHECKLISTE: WIE SIE RANSOMWARE IM KEIM ERSTICKEN

Schlüsseltechnologien zur Bekämpfung von Ransomware

Allen Untergangstheorien zum Trotz: Ransomware ist und bleibt eine der häufigsten Cyber-Bedrohungen für Unternehmen: 57 % der deutschen Unternehmen waren im Jahr 2019 Opfer von Ransomware. Um Ihr Unternehmen vor dieser Gefahr zu schützen, benötigen Sie moderne Sicherheitstechnologien.

Angriffe stoppen und Ausbreitung im Netzwerk verhindern

Als ersten wichtigen Schritt müssen Sie verhindern, dass Ransomware in Ihr Netzwerk gelangt und sich dort verbreiten kann. Am besten erreichen Sie dies mit einer Next-Gen-Firewall. Achten Sie unbedingt darauf, dass die Lösung Ihrer Wahl über folgende Funktionen verfügt:

☐ **Leistungsstarke IPS Engine (Intrusion Prevention System)**

Eine moderne, leistungsstarke IPS Engine darf in keiner Next-Gen Firewall fehlen. Sie nimmt eine Deep-Packet Inspection des Netzwerkverkehrs vor und kann Schwachstellen-Exploits so bereits identifizieren und blockieren, bevor sie ihren Ziel-Host erreichen.

☐ **Lockdown Remote Desktop Protocol (RDP)**

Ihre Firewall sollte Ihnen ermöglichen, auf einfache Weise den Zugriff auf VPN-Nutzer zu beschränken und erlaubte IP-Adressen auf die Whitelist zu setzen.

☐ **Sandboxing-Technologie**

Ihre Firewall sollte über Sandboxing-Technologie verfügen, damit alle verdächtigen aktiven Dateien, die Sie über Web-Downloads und als E-Mail-Anhänge erhalten, hinreichend auf schädliches Verhalten analysiert werden können, bevor sie in Ihr Netzwerk gelangen.

☐ **Zonensegmentierung**

Ihre Firewall sollte Ihnen ermöglichen, laterale Bewegungen im Netzwerk zu reduzieren, indem Sie LANs in kleinere, isolierte Zonen oder virtuelle LANs segmentieren, die durch die Firewall gesichert und verbunden sind.

☐ **Identifizierung und Kontrolle von Anwendungen**

Mit Ihrer Firewall sollten Sie steuern können, welche Anwendungen im Netzwerk laufen dürfen, und diejenigen blockieren können, die häufig für Ransomware-Angriffe genutzt werden.

Endpoints und Server schützen

Sie müssen verhindern, dass Ransomware auf Ihren Endpoints und Servern Fuß fassen kann. Achten Sie daher darauf, dass Ihre Endpoint- und Server-Schutzlösung über folgende Funktionen verfügt:

☐ **Anti-Ransomware-Technologie**

Ihre Lösung sollte Ihre Endpoints mit Technologien schützen, die speziell zum Erkennen und Stoppen von Ransomware entwickelt wurden. Sie sollte in der Lage sein, Ransomware-Verhalten zu erkennen, indem sie unbefugte Verschlüsselungen blockiert, mit denen versucht wird, nicht autorisierte Änderungen an Ihren Daten vorzunehmen. Die Technologien sollten außerdem:

- lokale und Remote-Verschlüsselungen unterbinden
- datei- und festplattenbasierte Ransomware stoppen
- Dateiänderungen ohne Datenverluste rückgängig machen

☐ **Exploit Prevention**

Angreifer nutzen gezielt Schwachstellen in Software-Produkten aus, um Ransomware in Umlauf zu bringen und zu installieren. Exploit-Prevention-Technologie stoppt die Techniken, auf die Angreifer angewiesen sind, um ihre Ziele zu erreichen.

☐ **Machine Learning**

Ihre Lösung sollte in der Lage sein, Deep Learning oder andere Machine-Learning-Techniken zu nutzen, um die „DNA" von Dateien zu analysieren und neue Ransomware zu blockieren, bevor sie ausgeführt werden kann.

☐ **HIPS-Verhaltensanalysen/Dateianalysen**

Ihre Endpoint-Lösung sollte in der Lage sein, die Komponenten/Struktur von Dateien auf Schadelemente zu überprüfen und zu ermitteln, ob Code enthalten ist, der versucht, die Registry zu manipulieren.

SOPHOS

☐ Web Security und Malicious Traffic Detection

Ihre Lösung sollte nach schädlichem Code suchen und den Zugriff auf Exploit Landing Pages blockieren.

☐ Device Control

Ihre Endpoint-Lösung sollte die Möglichkeit bieten, den Zugriff auf Wechselmedien wie USB-Sticks einzuschränken, um Risiken durch infizierte Medien auszuschalten.

☐ Managed Detection and Response (MDR)

Ihr Anbieter sollte als Ergänzung zu Ihrer Endpoint-Lösung einen 24/7 Monitoring- und Response-Service anbieten. MDR-Services suchen nach verdächtigen Aktivitäten und potenziellen Indicators of Compromise, die Ihr Unternehmen Ransomware-Angriffen aussetzen könnten.

Phishing-E-Mails stoppen

Phishing-E-Mails sind einer der häufigsten Übertragungswege von Ransomware. Sorgen Sie dafür, dass Ihre Benutzer sich dieser Gefahr bewusst sind:

☐ Simulierte Phishing-Angriffe

Testen Sie, wie gut Ihr Unternehmen auf gezielte Phishing-Angriffe vorbereitet ist.

☐ Individuell anpassbare Phishing-Trainings

Stimmen Sie die E-Mails inhaltlich auf Ihr Unternehmen und die Branche ab. Führen Sie zum Beispiel ein Training zum Thema Compliance durch und sensibilisieren Sie Ihre Mitarbeiter für die Gefahren.

☐ Detaillierte Infos über einzelne User

Ermitteln Sie, wie viele Mitarbeiter getäuscht wurden, wie anfällig sie für Phishing-Angriffe sind, wie die User bei den Trainings durchschnittlich abgeschnitten haben, und vieles mehr.

1 The State of Ransomware 2020

Warum Sophos Sie einfach besser schützt

Verhindert, dass Angriffe ins Netzwerk gelangen

Mit der Sophos XG Firewall erhalten Sie eine Fülle von Technologien, die Ihr Unternehmen vor ständig neuen Ransomware-Angriffen schützen. Die XG Firewall verfügt über eine der marktweit leistungsstärksten und effektivsten IPS Engines und bietet eine einfache und elegante Lösung zum Lockdown Ihrer RDP-Server.

Mit den flexiblen und einfachen Segmentierungs-Tools (z. B. Zonen und VLANs) der XG Firewall sichern Sie Ihr LAN, reduzieren das Risiko lateraler Bewegungen, verringern die Angriffsfläche und minimieren das Risiko und potenzielle Ausmaß einer Ausbreitung.

Schutz für Endpoints und Server

Sollte es Hackern gelungen sein, auf Ihr Netzwerk zuzugreifen, wendet Intercept X mehrschichtige Verteidigungsmaßnahmen an, um Ransomware bereits zu stoppen, bevor sie Schaden anrichten kann. Anti-Exploit-Technologien stoppen die Bereitstellung von Ransomware, Deep Learning blockiert die Ausführung von Ransomware und CryptoGuard verhindert unbefugte Datei-Verschlüsselungen bzw. setzt betroffene Dateien in ihren sicheren Ursprungszustand zurück. Die EDR(Endpoint Detection and Response)-Funktionalität von Intercept X erkennt zudem komplexe Ransomware-Angriffe, die möglicherweise unbemerkt geblieben sind, und sucht nach Indicators of Compromise in Ihrem Netzwerk.

Darüber hinaus ermöglicht Sophos Managed Threat Response (MTR) dank Machine Learning und künstlicher Intelligenz die Identifizierung und Ausführung von Threat-Response-Aktionen 24/7.

Anti-Phishing-Training

Sophos Phish Threat sendet simulierte Phishing-Angriffe an Ihr Unternehmen und testet damit, wie gut Ihre Mitarbeiter auf echte Angriffe vorbereitet sind. Die E-Mails lassen sich individuell an Ihr Unternehmen und die Branche anpassen. In einer detaillierten Auswertung erfahren Sie u. a., wie viele Benutzer getäuscht wurden und wie hoch das allgemeine Risiko ist, auf Angriffe hereinzufallen.

XG Firewall kostenlos testen unter www.sophos.de/firewall

Intercept X kostenlos testen unter www.sophos.de/intercept-x

Phish Threat kostenlos testen unter www.sophos.de/phish-threat

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

2019-10-07 CL-DE (NP)

SOPHOS