SOPHOS

Security made simple.

Anti-Ransomware-Checkliste

Schlüsseltechnologien und Security Best Practices

Ransomware-Angriffe beginnen entweder mit einem schädlichen E-Mail-Anhang oder über eine kompromittierte Website. Von dort aus arbeitet sich die Ransomware bis zu Ihren Endpoints und Servern vor. Um solche Angriffe zu stoppen, benötigen Sie leistungsstarke Schutztechnologien für jede Phase des Angriffs und müssen diese mit Security Best Practices kombinieren.

Endpoints und Server schützen

Ransomware auf Ihren Endpoints und Servern bekämpfen Sie effektiv mit folgenden Technologien:

☐ CryptoGuard-Technologie (verfügbar in Sophos Intercept X)

Schützt Ihre Endpoints und Server mit einer einzigartigen Technologie, die Ransomware bereits stoppt, bevor sie Schaden anrichten kann. CryptoGuard ergänzt Ihre bestehende Sicherheit und blockiert Prozesse, die versuchen, unbefugte Änderungen an Ihren Daten vorzunehmen.

- Wirksam gegen CryptoLocker, Locky, Zepto, Cerber etc.
- Unterbindet sowohl lokale als auch Remote-Verschlüsselungen
- Macht alle Änderungen rückgängig und verhindert somit Datenverluste

☐ Exploit Prevention (verfügbar in Sophos Intercept X)

Stoppt Ransomware, die Schwachstellen in Software-Produkten ausnutzt.

☐ HIPS-Verhaltensanalysen/Dateianalysen

Überprüft die Komponenten/Struktur von Dateien auf Schadelemente und ermittelt, ob Code enthalten ist, der versucht, die Registry zu manipulieren.

☐ Web Security

Scannt Web-Inhalte auf Ransomware-Code.

☐ Malicious Traffic Detection (MTD)

Erkennt Datenbewegungen zu Command-and-Control-Servern von Ransomware und blockiert diese.

☐ Application Control

Erlaubt nur die Ausführung bestimmter Anwendungen und kann Wcript blockieren, das oft von Ransomware verwendet wird.

☐ Application Whitelisting

Richtet eine Standard-Ablehnungsrichtlinie auf Servern ein, damit nur vertrauenswürdige Anwendungen ausgeführt werden können – so kann Ransomware gar nicht erst Fuß fassen.

E-Mail-Bedrohungen stoppen

Das E-Mail-Gateway ist Ihre erste Verteidigungslinie gegen Ransomware-E-Mails. Wichtig sind folgende Funktionen:

☐ Anti-Spam-/Anti-Virus-Technologie

Blockiert Ransomware-E-Mails (auch solche mit schädlichen Makro-Attachments) und stoppt andere E-Mail-Bedrohungen.

☐ Time-Of-Click Protection

Verhindert, dass Benutzer auf Links zu Ransomware-hostenden Websites klicken – selbst, wenn der Link sicher war, als er in den Posteingang gelangte.

☐ Cloud-Sandboxing

Testet Dateien in einer sicheren Umgebung, bevor sie von Benutzern ausgeführt werden, und fängt auf diese Weise Zero-Day-Bedrohungen wie Ransomware ab.

Web-Bedrohungen stoppen

Das Web-Gateway blockiert Ransomware aus dem Internet, bevor sie auf die Endpoints Ihrer Benutzer gelangen kann. Es sollte folgende Funktionen beinhalten:

☐ URL-Filterung

Blockiert Websites, die Ransomware hosten, und unterbindet die Kommunikation von Ransomware mit Command-and-Control-Servern.

☐ Web-Filterung

Setzt strenge Kontrollen für Dateitypen durch, die in Zusammenhang mit Ransomware stehen, und verhindert deren Download.

☐ Cloud-Sandboxing

Testet Dateien in einer sicheren Umgebung, bevor sie von Benutzern ausgeführt werden, und fängt auf diese Weise Zero-Day-Bedrohungen wie Ransomware ab.

Neun Security Best Practices

IT Security Best Practices wie regelmäßige Mitarbeiterschulungen sind unerlässlich. Befolgen Sie unbedingt die folgenden neun Best Practices:

☐ Fertigen Sie regelmäßig Back-ups an und verwahren Sie diese offline und außerhalb des Büros

So kann Ransomware nicht an diese Daten gelangen. Mit regelmäßigen Back-ups lassen sich außerdem Datenverluste verhindern.

☐ Aktivieren Sie Dateierweiterungen

Bei aktivierten Dateierweiterungen können Dateitypen, die normalerweise nicht an Sie und Ihre Benutzer gesendet werden (z. B. JavaScript) einfach erkannt werden.

☐ Öffnen Sie JavaScript (.JS)-Dateien in Notepad

Wenn Sie eine JavaScript-Datei in Notepad öffnen, können keine Schad-Skripte ausgeführt werden und Sie können den Inhalt der Datei überprüfen.

☐ Aktivieren Sie keine Makros in Dokumentanhängen, die Sie per E-Mail erhalten

Viele Infektionen funktionieren nur, wenn Sie Makros aktivieren. Aktivieren Sie also keine Makros!

☐ Vorsicht bei Attachments, die Ihnen unaufgefordert zugesendet werden

Wenn Sie Zweifel haben, sollten Sie das Attachment lieber nicht öffnen. Rückversichern Sie sich nach Möglichkeit beim Absender.

☐ Beschränken Sie Ihre Anmelderechte auf das Nötigste

Administratorrechte können dazu führen, dass eine lokale Infektion sich über das gesamte Netzwerk ausbreitet.

☐ Ziehen Sie die Installation von Microsoft Office Viewern in Betracht

Mit diesen Viewer-Anwendungen können Sie sich den Inhalt von Dokumenten anzeigen lassen, ohne sie in Word oder Excel zu öffnen.

☐ Installieren Sie Patches zeitig und regelmäßig

Je eher Sie Patches installieren, desto weniger Schwachstellen sind vorhanden, die von Ransomware ausgenutzt werden können.

☐ Halten Sie die Sicherheitsfunktionen in Ihren Geschäftsanwendungen aktuell

In Office 2016 gibt es nun zum Beispiel das Steuerelement „Ausführung von Makros in Office-Dateien aus dem Internet blockieren".

Bleiben Sie sicher mit Sophos

Um Ransomware rechtzeitig zu stoppen, benötigen Sie eine geeignete Schutzlösung. Verhindern Sie mit der CryptoGuard-Technologie in Sophos Intercept X, dass Ransomware Ihre Dateien verschlüsselt. Stellen Sie außerdem sicher, dass Sie die geeigneten Anti-Ransomware-Technologien an Ihrem E-Mail-Gateway, Web-Gateway, Ihrer Firewall und Ihren Servern implementiert haben, sodass Bedrohungen gar nicht erst auf Ihre Endpoints gelangen können. So hindern Sie Ransomware daran, Ihre Daten zu verschlüsseln und Lösegeld von Ihnen zu erpressen.

Weitere Informationen und Tipps zum Schutz vor Ransomware

unter www.sophos.de/ransomware

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

SOPHOS

2016-09-08 CL-DE (RP)