10 BEST PRACTICES GEGEN RANSOMWARE:
So schützen Sie sich und Ihr Unternehmen

57% der deutschen Unternehmen waren im Jahr 2019 Opfer von Ransomware.[1] Größe spielte bei den Angriffen keine Rolle – Unternehmen aller Größen landeten im Visier der Angreifer. Werden Sie nicht das nächste Opfer – stellen Sie sicher, dass Sie und Ihre Mitarbeiter diese Best Practices befolgen:

1. **Patchen Sie frühzeitig und oft:** Je früher Sie Schwachstellen schließen, desto weniger Chancen geben Sie den Angreifern.
2. **Erstellen Sie regelmäßig Backups und bewahren Sie eine aktuelle Sicherungskopie offline und außerhalb des Standorts auf:** Ist Ihr Backup offline und außerhalb des Standorts, kann Ransomware nicht darauf zugreifen. Mit aktuellen Backups können Datenverluste deutlich minimiert werden.
3. **Schützen Sie Daten unabhängig davon, wo sie gespeichert sind:** Fast sechs von zehn Ransomware-Angriffen, bei denen Daten erfolgreich verschlüsselt wurden, umfassen Daten in der öffentlichen Cloud. Ihre Strategie sollte den Schutz für Daten an allen Orten umfassen - lokal, in der privaten Cloud und in der öffentlichen Cloud.
4. **Aktivieren Sie Dateierweiterungen:** Durch die Aktivierung von Dateierweiterungen ist es viel einfacher, Dateitypen zu erkennen, die normalerweise nicht an Sie und Ihre Benutzer gesendet würden, wie z. B. JavaScript.
5. **Öffnen Sie JavaScript(.JS)-Dateien in Notepad:** Das Öffnen einer JavaScript-Datei in Notepad verhindert die Ausführung bösartiger Skripte und ermöglicht es Ihnen, den Inhalt der Datei zu untersuchen.
6. **Aktivieren Sie keine Makros in per E-Mail empfangenen Anhängen:** Viele Infektionen entstehen dadurch, dass die Angreifer Sie dazu bringen, Makros zu aktivieren – also tun Sie es nicht!
7. **Seien Sie misstrauisch bei Anhängen:** Wenn Sie nicht sicher sind, was sich im Anhang befindet und warum Sie diesen erhalten haben, öffnen Sie ihn nicht. Fragen Sie beim Absender der E-Mail nach.
8. **Aktivieren Sie nur die Zugriffsrechte, die Sie wirklich brauchen:** Administrator-Rechte können zur Folge haben, dass eine lokale Infektion zu einer Netzwerk-Katastrophe wird.
9. **Halten Sie die Sicherheitsfunktionen in Ihren Anwendungen auf dem neuesten Stand:** Zum Beispiel enthält Office 2016 jetzt ein Steuerelement mit der Bezeichnung “Blockieren der Ausführung von Makros in Office-Dateien aus dem Internet”.
10. **Investieren Sie in Anti-Ransomware-Technologie:** Mit der richtigen Technologie können Sie einen Angriff stoppen, bevor die Daten verschlüsselt werden können.

Um Ransomware-Angriffe zu stoppen, bevor sie Schaden anrichten, brauchen Sie den richtigen Schutz. Die **Sophos XG Firewall** verhindert, dass Angriffe in Ihr Netzwerk gelangen. **Sophos Intercept X** und **Intercept X for Server** stoppen die Verschlüsselung von Daten auf Ihren Endpoints und Servern. **Sophos Phish Threat** schult und testet Ihre Anwender mit simulierten E-Mail-Phishing-Kampagnen. Zusammen bieten Ihnen diese Lösungen ein starkes, effektives Schutzschild selbst gegen raffinierteste Ransomware-Attacken.

XG Firewall kostenlos testen:
sophos.de/firewall

Intercept X kostenlos testen:
sophos.de/intercept-x

Phish Threat kostenlos testen:
sophos.de/phish-threat

1 The State of Ransomware 2020

SOPHOS