

Wie man sich gegen Ransomware- Angriffe verteidigt?



Systeme und Software auf dem neuesten Stand halten

- ✓ Patchen Sie umgehend: Viele Ransomware-Angreifer nutzen bekannte Schwachstellen aus, dagegen hilft nur regelmäßige Aktualisierung von Betriebssystemen, Anwendungen und Firmware.
- ✓ Automatisieren Sie Updates, wo immer dies möglich ist, um sicherzustellen, dass keine kritischen Patches übersehen werden.
- ✓ Systeme, die keinen Support mehr in Form von Sicherheitsupdates erhalten, müssen durch supportet Versionen ersetzt werden.



Nutzen Sie “Best-Practices” fürs Backup



- ✓ Befolgen Sie die 3-2-1-Regel: Bewahren Sie 3 Kopien Ihrer Daten auf, auf 2 verschiedenen Speicherarten, wobei 1 Kopie an einer externen Lokation aufbewahrt wird.
- ✓ Testen Sie ihre Backups regelmäßig, um sicherzustellen, dass sie schnell und vollständig wiederhergestellt werden können.
- ✓ Backups sollten verschlüsselt werden, so dass Backups auch bei Diebstahl nicht missbraucht werden können.



Zugriffskontrolle ist das A und O



- ✓ Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für alle kritischen Systeme.
- ✓ Beschränken Sie Benutzerrechte: Geben Sie Ihren Mitarbeitern nur Zugriff auf die Daten und Tools, die sie benötigen (Need-to-Know Prinzip).
- ✓ Verwenden Sie einzigartige, sichere Passwörter, für kritische Systeme mit 16+ Zeichen.



Setzen Sie Sicherheitstools ein und aktive Überwachung

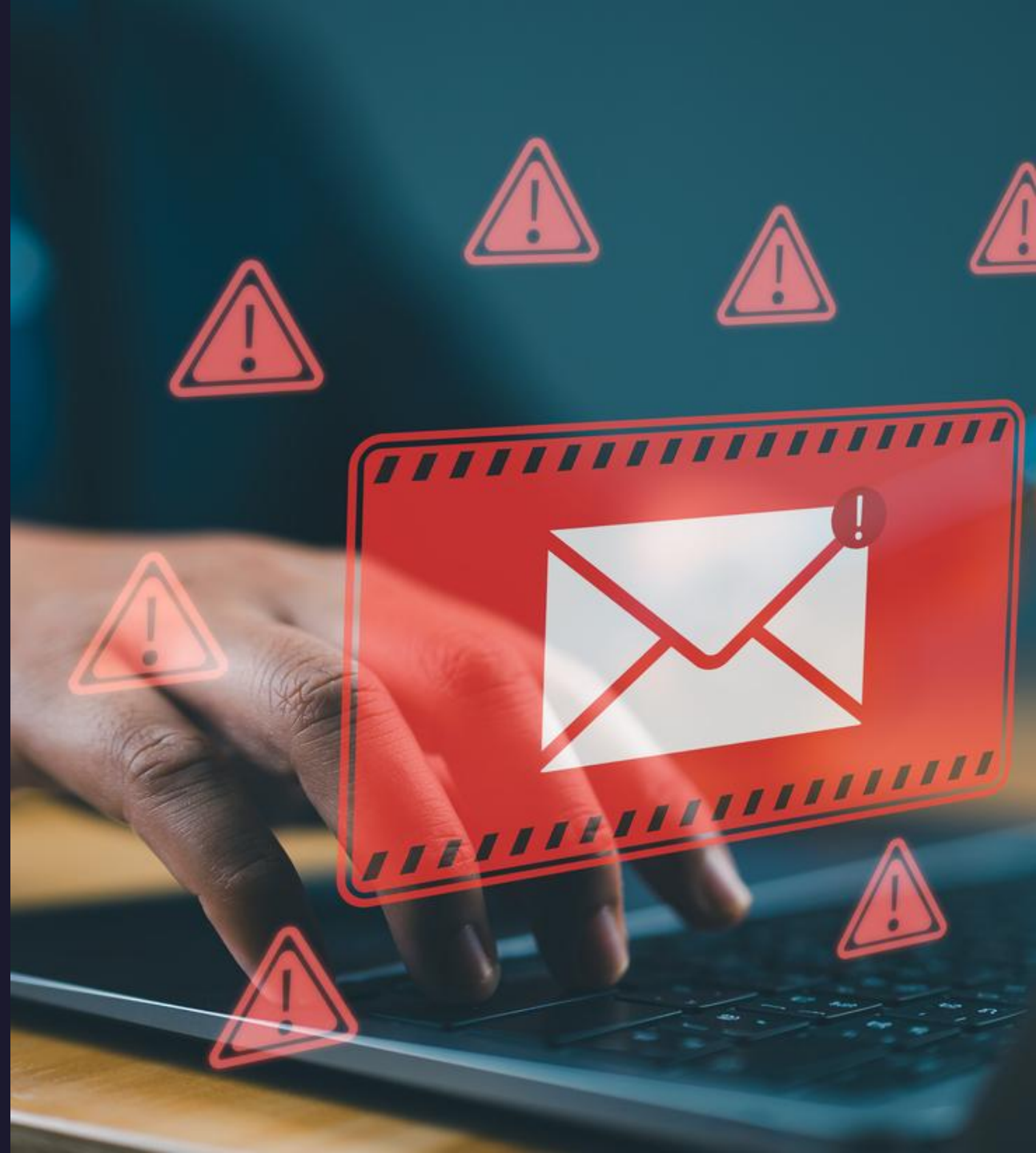
- ✓ Nutzen Sie einen effektiven Endpunktschutz, der Ransomware erkennen und blockieren kann, bevor sie ausgeführt wird.
- ✓ Nutzen Sie ein Intrusion Detection System und definieren sie Schwellwerte, um ungewöhnliche Aktivitäten frühzeitig zu erkennen.
- ✓ Segmentieren Sie Ihr Netzwerk, sodass sich eine Infektion in einem Bereich, sich nicht in andere Segmente ausbreiten kann.



Bewusstsein schaffen durch Schulungen



- ✓ Schulung der Mitarbeiter über Phishing Angriffe: Viele Ransomware-Angriffe beginnen mit bösartigen E-Mail-Anhängen oder Links.
- ✓ Führen Sie regelmäßige simulierte Phishing-Angriffe durch, um die Einsatzbereitschaft zu testen.
- ✓ Etablieren Sie einen einfachen Meldeprozess, damit verdächtige E-Mails oder Aktivitäten schnell und unkompliziert gemeldet werden können.



Entwickeln und Testen Sie einen Incident-Response-Plan

- ✓ Erstellen Sie eine Schritt-für-Schritt-Anleitung für die Reaktion auf ein Ransomware-Ereignis. Vergessen Sie dabei nicht die Außenkommunikation.
- ✓ Benennen Sie ihren Krisenstab und klären Sie die Verantwortlichkeiten für den Krisenfall im Voraus, damit jeder seine Verantwortlichkeit und Aufgabe kennt.
- ✓ Führen Sie Cyberangriffssimulationen durch, um den Plan unter realistischen Bedingungen zu testen und Lücken vor einem echten Vorfall aufzudecken.



Wir empfehlen Zero-Trust-Architektur

- ✓ Überprüfen Sie jeden Benutzer und jedes Gerät, bevor Sie Zugriff gewähren.
- ✓ Überwachen Sie kontinuierlich die Vertrauensstufen, um die laterale Bewegung des Angreifers zu verhindern, sollte es zu einer Sicherheitsverletzung gekommen sein.
- ✓ Standardmäßig wird Zugriff mit den geringsten Rechten gewährt, um sicherzustellen, dass Konten und Geräte nur die erforderlichen Rechte erhalten.



Key Takeaways

Aktualisieren Sie laufend

- Patchen Sie regelmäßig veraltete Systeme, um häufige Einfallstore für Ransomware zu schließen.

Intelligentes Backup

- Erstellen Sie verschlüsselte Backups und testen Sie regelmäßig den schnellen und fehlerfreien Restore

Zugriff einschränken

- Wenden Sie den Least Privileged, MFA und Netzwerksegmentierung an, um die Auswirkung zu reduzieren.

Planen und trainieren

- Erstellen Sie einen IRP und schulen Sie Ihre Mitarbeiter, um verdächtige Aktivitäten schnell zu erkennen und zu melden.

Nehmen Sie Kontakt auf. Wir unterstützen Sie gerne.

www.patecco.com

info@patecco.com