kaspersky BRING ON THE FUTURE

Anti-Ransomware-Checkliste

Backups erstellen

Fertigen Sie regelmäßig Sicherungskopien der Dateien an und speichern Sie diese sowohl auf physischen Datenträgern als auch in der Cloud – stellen Sie dabei sicher, dass Sie im Notfall schnell darauf Zugriff haben.

Backups überprüfen

Überprüfen Sie die erstellten Backups regelmäßig, ob alle wichtigen Dateien gespeichert sind, das Backup nicht beschädigt ist und schnell wiederhergestellt werden kann.

Updates

Stellen Sie sicher, dass alle Software, Anwendungen und Systeme immer auf dem neuesten Stand sind. Hierzu eine Schutzlösung mit Schwachstellen- und Patch-Management-Funktionen verwenden, um nicht gepatchte Schwachstellen im Netzwerk zu identifizieren.

Authentifizierungsfunktionen nutzen

Stellen Sie sicher, dass nur starke Kennwörter für den Zugriff auf Unternehmensdienste verwendet werden und dass die Multi-Faktor-Authentifizierung für den Zugriff auf Remotedienste aktiviert ist.

Mitarbeiter schulen

Schulen Sie ihre Mitarbeiter darin, wie sich Ransomware verbreitet – unter anderem über Phishing-Mails, verdächtige Websites oder gecrackte Software, die von inoffiziellen Quellen heruntergeladen wurde. Die Mitarbeiter sollten stets wachsam sein; regelmäßige Tests helfen bei der Sensibilisierung.

Endpunkte und Netzwerke schützen

Stellen Sie sicher, dass am Netzwerk-Perimeter und an allen Netzwerkknoten, einschließlich Endpunkten und Servern, der richtige Schutz vorhanden ist. Aktivieren Sie die Schutzfunktion für Netzwerkbedrohungen, um Verschlüsselungen zu erkennen und zu blockieren, wenn Ransomware in das Netzwerk gelangt. Vergessen Sie nicht, auch eingebettete Geräte zu schützen, da Ransomware auch diese verschlüsseln kann.

Schutz vor Phishing

Setzen Sie eine Schutzlösung für Endpunkte und Mailserver mit Anti-Phishing-Funktionalität ein, um das Risiko zu verringern, dass eine Infektion über eine Phishing-Mail erfolgt.

Netzwerke prüfen

Führen Sie ein Cybersicherheitsaudit Ihrer Netzwerke durch und beheben Sie alle entdeckten Schwachstellen, die am Perimeter oder innerhalb des Netzwerks entdeckt wurden.

Spezielle Nutzer schützen

Richten Sie einen anwendungsübergreifenden Standard-Verweigerungsmodus für die Nutzergruppen ein, die Zugriff auf die sensibelsten Daten haben, wie z.B. die Finanzabteilung. Dieser Modus stellt sicher, dass ein nicht vertrauenswürdiger Prozess auf einem Rechner nicht gestartet werden kann.

Niemals Cyberkriminelle bezahlen

Erpressung über Ransomware ist eine Straftat. Zahlen Sie nie die geforderte Lösegeldsumme, wenn Sie zum Opfer werden. Denn es gibt keine Garantie, dass Sie ihre Daten zurück bekommen, die Cyberkriminellen werden allerdings in ihren Aktivitäten ermutigt und bestätigt. Zeigen Sie den Vorfall bei Ihrer örtlichen Strafverfolgungsbehörde an. Im Internet gibt es kostenfreie Entschlüsselungstools für Ransomware, beispielsweise https://www.nomoreransom.org/en/index.html