RANSOMWARE

Informationen für Unternehmen in Österreich

Beschreibung

Ransomware ist Schadsoftware, die Computer, Server oder Daten verschlüsselt. Täterinnen und Täter fordern anschließend Lösegeld – meist in Kryptowährungen – für die Entschlüsselung oder die Nichtveröffentlichung gestohlener Daten. Betroffen sind Unternehmen jeder Größe. Es wird empfohlen, kein Lösegeld zu bezahlen. Ein wirksamer Schutz besteht aus sensibilisierten Mitarbeitenden, technischer IT-Sicherheit und klaren Organisationsabläufen.

Hier einige Vorgehensweisen der Täterinnen und Täter:

- **Klassische Ransomware:** Verschlüsselung von Dateien, Servern oder gesamten IT-Systemen.
- **Double Extortion:** Diebstahl vertraulicher Unternehmensdaten mit anschließender Veröffentlichungsdrohung.
- **Triple Extortion:** Zusätzliche Erpressung von Kundinnen und Kunden, Lieferantinnen und Lieferanten oder Geschäftspartnerinnen und Geschäftspartnern.
- **Angriff über kompromittierte Zugänge:** Einstieg über Phishing, gestohlene Zugangsdaten, Sicherheitslücken oder unsichere Fernzugänge.
- **Angriff auf Datensicherungen:** Backups werden gelöscht oder verschlüsselt, um eine Wiederherstellung zu verhindern.

Achtung, wenn…

- Dateien oder Ordner nicht mehr geöffnet werden können.
- Dateiendungen plötzlich verändert sind.
- Computer oder Server ungewöhnlich langsam reagieren.
- Sicherheitssoftware deaktiviert wurde.
- Benutzerkonten gesperrt sind und mehrere Mitarbeitende keinen Zugriff auf Unternehmensdaten haben.

Wie können Sie sich schützen?

- **Sensibilisierung der Mitarbeiterinnen und Mitarbeiter**
  - Regelmäßige Schulungen durchführen.
  - Keine unbekannten Anhänge oder Links öffnen.
  - Verdächtige E-Mails sofort melden.

- **Technischer Schutz**
  - Zwei-Faktor-Authentifizierung nutzen.
  - Sicherheitsupdates zeitnah installieren.
  - Administratorrechte beschränken.
  - Netzwerke aufteilen.
  - Regelmäßige Backups erstellen und mindestens eine Sicherung offline aufbewahren.

- **Sichere Organisationsabläufe**
  - Notfallplan erstellen.
  - Zuständigkeiten festlegen.
  - Krisenübungen durchführen.
  - Externe IT-Unterstützung vorbereiten.

Besonders wichtig

Eine Lösegeldzahlung garantiert weder die Entschlüsselung der Daten noch die Löschung gestohlener Informationen oder die vollständige Wiederherstellung der Systeme. Unternehmen können dadurch erneut Ziel von Angriffen werden.

Und wenn es mal passiert ist …

- Betroffene Systeme sofort vom Netzwerk trennen.
- WLAN und Netzwerkverbindungen deaktivieren.
- IT-Abteilung oder Incident-Response-Team verständigen.
- Zugangsdaten unverzüglich ändern.
- Kein Lösegeld bezahlen.
- Beweise sichern (Screenshots, Logdateien, Uhrzeiten).
- Anzeige bei der Polizei erstatten.

Weiterführende Links

- Bundeskriminalamt Österreich – Prävention
- Watchlist Internet
- CERT.at