Ransomware

Ein Virus auf dem Vormarsch

Im Gegensatz zu normalen Viren, die Dateien beschädigen, verschlüsselt Ransomware Ihre Daten zunächst. Der Begriff „ransom“ kommt aus dem Englischen und bedeutet „Lösegeld“ – und genau das fordert Ransomware bei einem Angriff. Dementsprechend wird Ransomware auch als Erpressersoftware bezeichnet und gilt als besonders gefährlich. Wenn Sie das Lösegeld zur Entschlüsselung Ihrer Daten zahlen sollen, so erhalten Sie – laut Angreifer - ein Passwort, mit dem Sie die zuvor verschlüsselten Dateien wieder entsperren können.

Wie erfolgen die Angriffe?

- Durch Phishing Mails werden Links zu bösartigen Websites oder infizierte Daten im Anhang verbreitet
- Durch unbewusstes und unbeabsichtigtes Herunterladen von Software
- Durch Verwendung eines infizierten USB-Sticks
- Durch Schwachstellen in Servern z.B. zu schwache Passwörter
- Durch ungeschützte Fernzugänge über unterschiedliche Remote-Desktop-Tools

Was passiert bei einem Angriff?

1. Cyberkriminelle installieren Malware über eine Sicherheitslücke auf Ihrem Gerät.
2. Die Malware wird unbemerkt heruntergeladen.
3. Wichtige Computerdaten werden gesperrt und es wird eine Meldung angezeigt, die eine Zahlung zum Entsperren der verschlüsselten Daten oder des Systems fordert.
4. Dies kann auf dem gesamten System der Organisation geschehen.

Welche Schäden drohen?

Eigenschäden

Kosten durch Betriebsbeeinträchtigung und die Behebung von Schäden.

Reputationsschäden

Kunden verlieren Vertrauen in Ihre Organisation, das Image wird beschädigt

Fremdschäden

Sie können vertragliche Verpflichtungen nicht mehr erfüllen.

Beugen Sie vor:

Der größte Risikofaktor für Cyberangriffe ist der Mensch. Vermitteln Sie daher Grundkenntnisse der IT-Sicherheit auch an die Mitarbeitenden.

Öffnen Sie keine E-Mailanhänge von unbekannten oder unseriösen Absendern.

Führen Sie regelmäßige Sicherheitsupdates auf allen Geräten durch, damit Software-Schwachstellen behoben werden.

Führen Sie regelmäßige, externe Datensicherungen durch um die Daten vor Verlust, Manipulation oder unberechtigter Kenntnisnahme durch Angreifer zu schützen.

Aktivieren Sie Virenschutzprogramme und sorgen Sie für eine funktionierende Firewall.

Nutzen Sie Zwei-Faktor-Authentisierung, die es Unbefugten erheblich erschwert in ihre Benutzerkonten einzudringen.

Reagieren Sie angemessen:

Vermeiden Sie Lösegeldzahlungen

Jede erfolgreiche Erpressung motiviert den Angreifer weiterzumachen.

Trennen Sie die infizierten Systeme vom Netz

Trennung des Netzwerkkabel Ihres Computers und Abschaltung etwaiger WLAN-Adapter.

Erstatten Sie polizeiliche Strafanzeige

Die Landes- und Bundeskriminalämter haben Anlaufstellen dafür eingerichtet.

Suche Sie sich externe Unterstützung

Teilweise kann eine bestehende Cyber-Versicherung helfen.

Warten Sie nicht, bis Sie Opfer einer Ranswomware Attacke werden. Ermitteln Sie jetzt ihren IT-Sicherheitsbedarf mit dem **kostenfreien Sec-O-Maten** der Transferstelle IT-Sicherheit im Mittelstand.

www.sec-o-mat.de

Transferstelle
IT-Sicherheit im Mittelstand
Einfach. Sicher. Machen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages