6 Regeln für den Schutz vor Ransomware & anderer Schadsoftware

1. Seien Sie misstrauisch

Kriminelle wählen oft scheinbar seriöse Betreffzeilen und Dateinamen, nicht selten mit korrekten Fachtermini. Fragen Sie sich also jedes Mal wenn Sie bspw. eine Rechnung erhalten, ob sie diese erwarten und ob Sie diese im angegebenen Dateiformat erwarten. Häufig versenden Kriminelle Word-Dateien, die sie als unbezahlte Rechnungen deklarieren. Besonders bei unbekannten Absendern ist höchste Vorsicht geboten.

2. Deaktivieren Sie Makros & blocken Sie Dateianhänge

Insbesondere Makros in Word- und Excel-Dateien waren in jüngster Vergangenheit Einfallstore bspw. für den Verschlüsselungstrojaner „Locky". Sollten Makro-Funktionen nicht zwingend benötigt werden, sollten diese in Word und Excel deaktiviert werden.

3. Arbeiten Sie nur mit notwendigen Systemberechtigungen

Anwender sind häufig unwissentlich mit umfassenden Schreib- und Administrationsrechten ausgestattet. Mit minimalen Benutzerrechten hat auch Schadsoftware nur begrenzte Angriffsmöglichkeiten. Systemrechte sollten daher so sparsam wie möglich vergeben werden.

4. Offline Backup

Verschlüsselungstrojaner sind zunehmend auch in der Lage Netzwerkspeicher zu verschlüsseln. Ein regelmäßiges Offline-Backup auf Speichermdien die nach der Sicherung vom Netzwerk getrennt werden ist daher eine unverzichtbare Versicherung für den Fall der Fälle.

5. Halten Sie Software auf dem neuesten Stand

Softwarehersteller stellen regelmäßig Sicherheitsupdates bereit um Sicherheitslücken in Betriebsystemen, Firewalls, Virenschutzprogrammen etc. zu schließen. Besonders Flash-Player und PDF-Reader sind im Fokus von Schadsoftware-Entwicklern und benötigen daher häufig Sicherheitsupdates.

6. Mitarbeiter aufklären

Zeigen Sie Ihren Mitarbeitern den richtigen Umgang mit E-Mails, und erarbeiten Sie einen Verhaltensleitfaden.

ARCONDA.systems
Aktiengesellschaft

Sportalllee 6
22335 Hamburg I Germany

Tel. (+49) 40 823 158 50
E-Mail: info@arconda.ag
Web: www.arconda.ag