AIS COMPUTER AG
Schalten Sie die Profis ein
www.ais-computer.ch

Was ist Ransomware?

Vorsicht bei verdächtigen E-Mails!

Ransomware (Erpresser-Software) wurde in den letzten Jahren zu einer der berüchtigtsten Cyber-Bedrohungen.

Sobald Ransomware-Trojaner in ein System eindringen können, verschlüsseln sie heimlich Dateien – inklusive wichtiger Dokumente, Videos und Fotos. Das passiert im Hintergrund, so dass das Opfer zunächst gar nichts davon bemerkt.
Nachdem der Trojaner sein schädliches Werk getan hat, informiert er das Opfer, dass die Dateien verschlüsselt worden sind. Um die Dateien wieder verwenden zu können, muss der Anwender ein Lösegeld bezahlen, das meist mehrere Hundert Dollar beträgt und in Bitcoins zu bezahlen ist. Es wird allgemein abgeraten das Lösegeld zu bezahlen.

Seien Sie vorsichtig

Cyberkriminelle verbreiten oft gefälschte E-Mails mit schädlichen Links oder Datei-Anhängen. Vertrauen Sie niemandem: schädliche Mails können auch von Freunden und Geschäftspartnern kommen! Öffnen Sie keine Dateianhänge von Mails, an deren Vertrauenswürdigkeit auch nur der geringste Zweifel besteht. Nehmen Sie sich insbesondere vor Rechnungs- und Bewerbungs-Mails in Acht. Starten Sie keine ausführbaren Dateien an deren Vertrauenswürdigkeit Sie zweifeln.

Halten Sie Ihre Systeme aktuell

Aktualisieren Sie regelmässig das Betriebssystem, den Browser, die Antivirus-Software und alle anderen installierten Programme wie Adobe Reader, Flashplayer, Java etc. Denn Cyberkriminelle missbrauchen gerne Sicherheitslücken in diesen Programmen, um in Computer einzudringen.

Sichern Sie Ihre Daten

Legen Sie regelmässig Backups Ihrer Dateien an auf externe Datenträger oder in die Cloud. Der Backup-Datenträger darf aber nicht dauerhaft mit dem Rechner verbunden sein, da er sonst ebenfalls verschlüsselt werden könnte. Sichern Sie auch Daten aus der Cloud (Dropbox, OneDrive etc.), denn auch diese sind gefährdet.

Wenn's schon zu spät ist…

Ist der Übeltäter bereits aktiv, dann kann man nur noch versuchen zu retten, was noch zu retten ist. Ertappt man den Schädling auf frischer Tat, sollte man Windows umgehend herunterfahren oder notfalls den Stecker ziehen um die Verschlüsselung zu stoppen. Bringen Sie das betroffene Gerät zu Ihrem PC-Spezialisten. Er kann Ihnen die hoffentlich noch unverschlüsselten Daten in Sicherheit bringen und den betroffenen PC säubern oder neu installieren.

Rufen Sie uns an. Wir beraten Sie gerne!

Daniel Aemmer
Geschäftsinhaber
AIS-Computer AG
Untere Bönigstrasse 33
3800 Interlaken
Telefon 033 826 11 22
ais@ais-computer.ch
www.ais-computer.ch