Locky & Co

Sensibilisierung und Schulung schützt vor Verschlüsselungs-Trojanern

Von Dirk Munker, Inhaber Munker Privacy Consulting und LSWB-Datenschutzbeauftragter

Wer Besuch von Petya und Mischa bekommt, hat ein Problem – denn es handelt sich um Schadsoftware. Petya will Rechner komplett sperren, bis man bezahlt. Mischa verschlüsselt alle Datenbestände, auf die er Zugriff bekommt. Aber schon eine einfache Maßnahme kann den Geschwistern das Handwerk legen: die Schulung und Sensibilisierung von Mitarbeitern.

IT-Experten sind sich einig: Erpresser-Software – wie zum Beispiel Verschlüsselungs-Trojaner – wird auch 2016 die größte Gefahr unter den Cyberbedrohungen bleiben. Gezielte Angriffe auf Personengruppen mit hoher Zahlungsbereitschaft, die mit vielen vertraulichen und sensiblen Daten umgehen, sind ein neuer Trend. Für Steuerberater ist also Vorsicht geboten. Die Erpressungs-Trojaner kommen bestens getarnt. Sie hängen an E-Mails, verstecken sich auf Homepages und lauern in Downloads. Wer geschützt sein will, muss konsequent handeln.

Neben den technischen Möglichkeiten zur Absicherung der Kanzlei steht der Faktor Mensch im Rampenlicht. Selbst wenn die Kanzlei zu einem IT-Fort-Knox gemacht wird, reicht ein falscher Mausklick aus, um Trojanern Tür und Tor zu öffnen. Schulung und Sensibilisierung sind also unerlässlich, um sich zu schützen.

Umgang mit E-Mails: Worauf ist zu achten?

E-Mail-Anhänge sollten nicht geöffnet werden, wenn sie nicht absolut vertrauenswürdig sind. Dabei spielt es keine Rolle, ob der Absender bekannt ist oder nicht. Im Zweifel darf ein Anhang nur geöffnet werden, wenn man sich rückversichert hat.

Auch in E-Mails enthaltene Links sind zu hinterfragen. Bevor ein Link angeklickt wird, sollte geprüft werden, ob die E-Mail echt ist. Ein Hinweis auf eine sogenannte Phishing-Mail ist zum Beispiel oft das Fehlen der persönlichen Anrede. Am sichersten ist es, Links aus E-Mails nicht zu folgen, sondern direkt auf der Seite des Anbieters nach Informationen zu suchen.

Dubiose Internetadressen meiden!

Werden besonders günstige Produkte oder Downloads angeboten, oder wird man zum Beispiel auf unbekannte Internetadressen weitergeleitet, ist Vorsicht geboten. Grundsätzlich sollte man sorgfältig darauf achten, welche Webseiten man besucht. Beim Surfen sollte man im Auge haben, ob im Hintergrund automatische Installationen oder Downloads stattfinden. Möglichkeiten zur Anzeige solcher Aktivitäten kann der Systempartner einrichten.

Technische Schlupflöcher schließen

Veraltete, schlecht konfigurierte Systeme bieten Angriffsflächen. Updates und Patches der Softwarehersteller sollten immer zeitnah installiert werden, hier werden oft Sicherheitslücken geschlossen. Viel Sicherheit kann auch durch einen sauberen technischen Umgang mit E-Mails gewonnen werden, zum Beispiel durch die Verhinderung der automatischen Ausführung von Makros in Office-Dokumenten oder die Nutzung von Anti-Spam-Filtern. Wer zusätzlich sein Benutzerkonzept überprüft, macht einen weiteren wichtigen Schritt zur Abwehr der Trojaner. Schließlich können diese nur Datenbestände verschlüsseln, auf die der angemeldete Benutzer Zugriff hat.

Besonders wichtig ist die Prüfung des Backups. Mit fehlenden oder nicht ausreichenden Datensicherungskonzepten steht man im Ernstfall ohne Fangnetz da. Was gerne vergessen wird: Auch das Wiedereinspielen der Daten sollte wenigstens einmal jährlich getestet werden, sonst hilft die beste Sicherung nichts.

Die Palette an Maßnahmen ist hier nicht zu Ende. Am besten lässt sich ein Systembetreuer zu den individuell notwendigen und sinnvollen Schutzmaßnahmen beraten.

Was tun, wenn es doch passiert?

Auch die Maßnahmen im Ernstfall müssen mit den Mitarbeitern besprochen werden. Bei Verdacht trennt man den PC am besten sofort vom Netzwerk und informiert die Kanzleileitung. Der Aufwand für die Prüfung eines Fehlalarms ist minimal, verglichen mit dem Ernstfall.

So wird die Sache rund

Cybergefahren sind alltägliche Herausforderungen geworden. Dabei ist die Lösung ist recht einfach. Wer seine Mitarbeiter regelmäßig schult und die grundlegenden Maßnahmen zu Datensicherheit und Datenschutz umsetzt, hat gute Karten, dass es nicht zum Ernstfall kommt. ■

Kontakt

Munker Privacy Consulting GmbH
Tel. 08152 9998412
Fax 08152 9998413
E-Mail: info@munker.info
www.munker.info