TECHNIK

Schutz vor Cyber-Erpressern

Millionen Rechner wurden bereits Opfer von Krypto-Trojanern – So können Sie den Verlust Ihrer Daten verhindern

VON STEFFEN HAUBNER

Persönliche Dokumente, private Fotos, Musik, Videos. Alles, was man so auf der Festplatte speichert, gerät derzeit ins Visier von Cyberkriminellen. Locky, TeslaCrypt und CryptoLocker heißen die Angreifer, die den PC in Geiselhaft nehmen. Über ein Infofenster wird dem Besitzer mitgeteilt, dass alle seine Laufwerke verschlüsselt wurden. Nur gegen Zahlung eines bestimmten Betrages würden die Daten wieder freigegeben – in der Regel zwischen 200 und 350 Euro. Mehr als drei Millionen Deutsche wurden 2015 von solchen Krypto-Trojanern heimgesucht. Und für 2016 registrieren die Sicherheitsdienstleister schon jetzt einen dramatischen Anstieg der Infektionen.

Von der Idee, die Sperre eigenhändig wieder aufzuheben, muss man sich verabschieden. Es gibt derzeit kaum ein Mittel, die Verschlüsselung zu knacken. Umso wichtiger ist es, sich zu schützen. Wertvolle Dateien wie Familienfotos oder amtliche Dokumente sollten stets an einem separaten Ort gesichert werden. Separat bedeutet, dass es sich dabei um einen Datenträger handeln sollte, der nicht permanent mit dem PC verbunden ist. Dateien, die nicht mehr ständig verändert werden müssen, können auf CD oder DVDs gebrannt, auf einen USB-Stick kopiert oder auf eine externe Festplatte ausgelagert werden, die man nach jeder Sicherung vom PC trennt.

Dabei sind zwei Dinge wichtig: Erstens ist ein Backup grundsätzlich nur dann ein Backup, wenn die gesicherten Inhalte hinterher mindestens zweimal vorhanden sind, und zwar auf unterschiedlichen Datenträgern. Zweitens nützt eine Sicherung nur dann etwas, wenn man sie im Notfall wiederfindet. Dafür sorgt eine eindeutige Beschriftung von Dateien und Datenträgern.

Kostenlose Backup-Programme

Für Dateien, an denen man aktuell arbeitet, bietet sich eine schnelle Sicherung in einem Cloud-Speicher wie Dropbox oder OneDrive an. Das sollte man immer nach einem größeren Arbeitsschritt tun. Spezielle Backup-Programme helfen dabei, in regelmäßigen Abständen auch größere Datenmengen oder ganze Festplattenabbilder zu sichern. Ein kostenloses Programm ist „Duplicati“ (www.duplicati.com), das es aber leider nur in englischer Sprache gibt. Für kommerzielle Backup-Programme wie etwa „Ashampoo Backup 2016“ (https://www.ashampoo.com/de) bezahlt man rund 20 Euro. Häufig bieten die Hersteller auch abgespeckte kostenlose Versionen ihrer Software an wie beispielsweise „Ashampoo Burning Studio Free“, das mit einer Backup-Funktion ausgestattet ist und für den Hausgebrauch vollkommen ausreicht.

In den meisten Fällen wird Ransomware über E-Mails auf den Rechner geschleust. Sobald man einen infizierten Anhang öffnet, startet im Hintergrund die Installation der Schadsoftware. Bei einigen Varianten versenden die befallenen Systeme automatisch E-Mails an das gesamte Adressbuch. Das bedeutet, dass die heimtückische Software auch von bekannten Absendern kommen kann. Deshalb sollte man sich vor dem Öffnen eines Anhangs stets genau überlegen, ob der Bekannte tatsächlich eine solche E-Mail verschicken würde. Im Zweifel hilft eine persönliche Nachfrage. Ein häufiger Trick sind auch gefälschte Rechnungen von Dienstleistern. Nachrichten von unbekannten Absendern sollte man deshalb unter gar keinen Umständen öffnen, das gilt insbesondere für .exe- und Office-Dateien.

Tückisch bei Office-Dateien sind automatisch ausgeführte „Makros“. Diese kann man in der jeweiligen Office-Anwendung unter „Datei“, „Optionen“, „Trust Center“ und „Einstellungen“ deaktivieren. Auch pdf-Dateien dienen häufig der Verbreitung von Schädlingen. Deshalb sollte man auch den Acrobat-Reader immer auf dem neusten Stand halten. Tauscht man regelmäßig mit anderen Dokumente aus, benutzt man dafür am besten einen Cloud-Speicher.

Vorsicht beim Surfen

Auch über mit Schädlingen präparierte Webseiten kann man sich infizieren. Download-Buttons für kostenlose E-Books, Klingeltöne oder ähnliches sollte man im Zweifel unbedingt meiden. Teilweise genügt aber auch schon das Aufrufen einer Seite im Browser, damit die schädliche Software installiert wird. Dabei werden bekannte Sicherheitslücken gezielt ausgenutzt. Deshalb ist es wichtig, dass nicht nur das Betriebssystem, sondern auch alle darauf installierten Anwendungen und insbesondere die Surfsoftware regelmäßig aktualisiert werden. Dazu sollte man bei allen Programmen die Auto-Update-Funktion aktivieren. Bei Windows 10 geht das zum Beispiel über „Einstellungen“, „Windows Update“ und „Erweiterte Funktionen“.

Ist der PC einmal infiziert, bleibt im Grunde nur Schadenbegrenzung. Das „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) rät davon ab, auf Lösegeldforderungen einzugehen. Dateien oder Programme würden in vielen Fällen nämlich trotz Bezahlung nicht entschlüsselt. „Stattdessen sollten betroffene Nutzer den Bildschirm samt Erpressungsnachricht fotografieren und bei der Polizei Anzeige erstatten“, so die Behörde. Anschließend helfe meist nur ein komplettes Neuaufsetzen und Aufspielen eines Daten-Backups. Ärgerlich ist das natürlich auf jeden Fall.

Doch immerhin muss man sich so nicht in die Hände von Erpressern begeben, die nach der ersten Zahlung möglicherweise weitere Forderungen stellen. Und jedes Opfer, das auf die Forderungen eingeht, trägt dazu bei, dass die Bedrohung weiter fortbesteht.

FOTO: DPA

> In den meisten Fällen wird Ransomware über E-Mails auf den Rechner geschleust

Die wichtigsten Schutzmaßnahmen

Installieren Sie regelmäßig von den Herstellern bereitgestellte Sicherheitsupdates für Ihr Betriebssystem und alle Programme. Das gilt besonders für Internet-Browser, Office, Flash Player und Adobe Reader. Die Funktion „Automatische Updates“ findet sich im jeweiligen Programm, meist unter „Optionen“ und „Einstellungen“.

Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie es regelmäßig.

Aktivieren Sie eine Personal Firewall. Diese ist in den meisten aktuellen Betriebssystemen wie Windows 10 bereits enthalten und kontrolliert alle ein- und ausgehenden Verbindungen mit anderen Netzwerken.

Nutzen Sie, insbesondere für den Zugriff auf das Internet, ausschließlich ein Benutzerkonto mit eingeschränkten Rechten. Sie können ein solches Standard-Konto unter „Systemsteuerung“, „Benutzerkonten“ und „Kontotyp ändern“ zusätzlich zum Administrator-Konto einrichten. Danach melden Sie sich mit diesem Konto an und haben trotzdem weiter Zugriff auf die wichtigsten Funktionen.

Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen. Seien Sie misstrauisch – insbesondere beim Öffnen von Mail-Anhängen und beim Herunterladen von Software. Laden Sie diese möglichst nur von der Webseite des Herstellers herunter.

Diese Empfehlungen beruhen auf den vom BSI gegebenen Hinweisen zur Sicherheit von privaten PCs. Weitere Informationen finden Sie unter der Adresse
https://www.bsi-fuer-buerger.de