Erpresserische Trojaner (kein Passwort)

a --
[LINK]

Zusammenfassung: Etzel Gysling

Ransomware: so werden bösartige «Trojaner» bezeichnet, die sich in den Computer einnisten, Dateien, Ordner oder eine ganze Festplatte verschlüsseln und dann Lösegeld dafür verlangen, dass man wieder uneingeschränkt Zugang zum Computer hat. In Gegensatz zum trojanischen Pferd der Sage – das von den Trojanern bewusst in die Stadt hineingeholt wurde – erfolgt der Import des schädlichen Codes fast ohne unser Zutun. Es scheint, dass mehr und mehr auch Rechner von kleinen Unternehmen und Privatpersonen infiziert werden. Die Ratschläge, wie man sich dagegen wehren kann, sind vielfältig – primär handelt es sich dabei um quasi selbstverständliche Massnahmen. Komplizierter wird es, wenn bereits eine Ransomware-Infektion vorhanden ist. Hier folgt eine Übersicht zu den wichtigsten Punkten, die wir beachten sollten.

Da ist zunächst die einfache Regel, das *Betriebssystem aktuell* zu halten, also das regelmässige Updating durch die Hersteller zuzulassen (gültig nicht nur für Windows-Computer, sondern auch für alle anderen). *Virenschutzprogramme*, die heute in guter Qualität auch kostenlos verfügbar sind, sollten ebenfalls unbedingt regelmässig à jour gehalten werden. Einige Fachleute empfehlen zudem, von Zeit zu Zeit den ganzen Computer auf schädlichen Code zu prüfen, was normalerweise im Virenschutzprogramm manuell initiiert werden kann. Sehr wichtig ist ferner, dass man in *E-Mails*, deren Herkunft nicht völlig eindeutig ist, keinen Links folgt und keine Anhänge öffnet. Diese supereinfache Regel wird leider recht häufig missachtet!

Leider garantieren diese Massnahmen nicht zu 100%, dass man frei von Ransomware bleibt. Es ist möglich, einfach nur

durch den Besuch bestimmter Websites infiziert zu werden. Umso wichtiger ist es, den Inhalt des Computers regelmässig mittels eines *Backups* zu sichern. Ein Teil der erpresserischen Trojaner sind aber als «Zeitbombe» eingerichtet, d.h. sie nisten sich zunächst nur ein und beginnen ihre kriminellen Aktionen erst später. Daran muss man denken, wenn man auf Backups zurückgreift, die nur einige Tage alt sind und deshalb den schädlichen Code bereits enthalten könnten. Wer essentielle Daten vor Schaden bewahren will, macht am besten Backups auf verschiedenen Medien (oder auch zusätzlich online) und bewahrt periodisch Backups z.B. auf USB-Sticks oder -Festplatten auf, die separat vom Computer aufbewahrt werden.

Was tun, wenn ein Computer offensichtlich mit Ransomware *infiziert* ist? Nicht verzweifeln, kein Lösegeld zahlen! (Lösegeld wird oft in Form von Bitcoins gefordert, die auf verschlungenen Wegen zum Cyberkriminellen gelangen, was es weitgehend verunmöglicht, die Identität des Gauners herauszufinden.) Tatsächlich gibt es keine Sicherheit, dass die Bezahlung auch wirklich zur «Befreiung» des Computers führt. Hat man die richtigen Backups zur Verfügung, so sollte einer Rettung der eigenen Dateien nichts im Wege stehen.

Anderseits ist es auch nicht ganz ausgeschlossen, dass man die Verschlüsselung der Daten wieder lösen kann. Mehrere kostenlose Rettungs-Systeme, in der Regel auf dem Linux-Betriebssystem beruhend, bieten sich an: bekannt ist unter anderem die «Kaspersky Rescue Disk» (http://goo.gl/Z3omxN); auch die Knoppix-Software (http://www.knoppix.org) kann eventuell helfen. Diese Software erfordert allerdings mehr als elementare Computerkenntnisse, damit sie erfolgreich eingesetzt werden kann.

Etzel Gysling