Ransomware – Erpressertrojaner auf Beutezug

Sie verschlüsselt sämtliche Dateien, infiziert Netzwerke und fordert Lösegeld – es geht um Ransomware, eine der lukrativsten Maschen der Internetkriminalität. Wenn der Privatcomputer oder das Firmennetzwerk erst einmal betroffen ist, dann ist guter Rat teuer, denn die als *Locky*, *TeslaCrypt* oder *Zepto* bezeichneten Trojaner machen sämtliche Dateien auf der Festplatte zunächst einmal unbrauchbar. Doch muss es eigentlich soweit kommen? Ist konsequenter Schutz von vornherein nicht wesentlich effektiver als das mühselige Entfernen nach der Infektion? Dieser Beitrag möchte darüber aufklären, wie zukünftig mit Ransomware umgegangen werden sollte und für Möglichkeiten bestehen, um uns effektiv vor ihr zu schützen.

Ein falscher Klick ist manchmal ein Klick zu viel

Ransomware kann überall lauern. Hauptsächlich verbreitet wird sie über E-Mail-Anhänge, bei denen es sich in nicht wenigen Fällen um infizierte Makros von Word- oder Excel-Dateien handelt. Doch auch über so genannte *„Drive-by-Downloads“*, die unbemerkt vom Benutzer auf verseuchten Webseiten stattfinden, kann ein Gerät infiziert werden.

Ein klassisches Beispiel sind E-Mails, in denen man dazu aufgefordert wird, für etwas zu zahlen, das man niemals bestellt hat. Unwissende klicken dann häufig auf die vermeintliche Rechnung im Anhang, was zur Folge hat, dass der Trojaner genau das tut, wofür er geschaffen wurde: Er verschlüsselt Festplatten oder sogar ganze Netzlaufwerke.

Freigegeben werden die Dateien erst wieder, wenn eine von Version zu Version variierende Summe Lösegeld gezahlt wird. Diese fordern die Erpresser in der Regel in Bitcoins ein, um möglichst anonym zu bleiben. IT-Security-Experten warnen allerdings einstimmig davor, dass nicht sicher sei, ob die Betroffenen nach Zahlung des Lösegeldes auch tatsächlich den versprochenen Key für die Entschlüsselung ihrer Daten erhalten. Ähnliches gilt für Schadsoftware wie den Trojaner *„Popcorn Time“*, der nach dem so genannten *„Referral-System“* funktioniert. Hier wird der Betroffene dazu aufgefordert, zwei weitere Nutzer zu infizieren, um wieder Zugriff auf seine Daten zu erhalten. Doch damit nicht genug: Besonders dreiste Versionen der Ransomware drohen sogar mit einem Zeitlimit. Sollte das Opfer in einer bestimmten Zeit nicht zahlen, werden sämtliche Dateien unwiderruflich gelöscht.

Was macht Ransomware so erfolgreich?

Ransomware lebt von der Unwissenheit, Unsicherheit und Angst vieler Computer-Nutzer. Mittlerweile kursieren massenhaft Anleitungen und Tipps im Netz, wie man die Trojaner wieder von seinem PC entfernt und seine Daten entschlüsseln kann - doch wäre es nicht klüger, es von Anfang an gar nicht erst dazu kommen zu lassen?

Zumindest eins sollte auf der Hand liegen: Schaffen es die Trojaner erst gar nicht auf unsere Endgeräte, dann bedarf es auch keiner umständlichen Entfernung der Schadsoftware und

Entschlüsselung der Dateien. Ein weiterer Pluspunkt: Die Erfolge der Cyber-Kriminellen würden signifikant schrumpfen und das Geschäft ist für sie wäre weniger profitabel.

Nutzer sollten also vor allem für das Ransomware-Problem als solches sensibilisiert werden. Weniger PC-affine Nutzer sind oft nicht genug über Risiken aufgeklärt, die im Internet oder im E-Mail-Postfach auf sie lauern können. Darüber hinaus ist der richtige Schutz elementar. Mittlerweile gibt es eine ganze Bandbreite an Präventivmaßnahmen, die wirkungsvoll gegen Ransomware eingesetzt werden können.

Wie kann ich mich gegen Ransomware schützen?

Die größte Gefahr lauert, wie schon erwähnt, im eigenen E-Mail-Postfach. Nachrichten können infizierte Links oder Dateianhänge enthalten, die besser verschlossen bleiben. Im Zweifelsfall helfen Suchmaschinen dabei, mehr über den Absender herausrauszufinden und ob bereits Beschwerden gegen ihn vorliegen.

Außerdem sollten Anwender beim Surfen im Internet auf der Hut sein. Es empfiehlt sich, nicht vertrauenswürdig wirkende Webseiten am besten ganz zu meiden oder sie schnell wieder zu verlassen. Hier besteht die Gefahr eines verdeckt ausgeführten „Drive-by-Downloads", der Ransomware oder andere Malware enthalten kann. Auch durch Werbeanzeigen und Pop-Ups kann es zu diesen nicht beabsichtigten Downloads kommen. Hier sorgt ein *„Ad-Blocker"* für Abhilfe. Eine weitere Präventivmaßnahme stellen regelmäßige Backups dar. Es empfiehlt sich hierbei, eine so genannte *„Image-Sicherung"* durchzuführen. Sie kopiert nicht nur Ordner und Dateien, sondern sämtliche Bits und Bytes, die sich auf Ihrer Festplatte befinden.

Mittlerweile gibt es auch einige hilfreiche Programme, die Ihnen beim Backup behilflich sein können. Besonders gut dafür eignen sich Cloud-Speicher mit automatischer Versionierung. Sie bieten den Vorteil, dass jederzeit auf eine ehemalige Version einer Datei zurückgegriffen werden kann. Auf diese Weise kann eine Verschlüsselung durch Locky und Co. Ihren Dateien nichts anhaben, da diese dann einfach ins Leere läuft.

Des Weiteren sollte ein Auge darauf geworfen werden, dass alle sicherheitsrelevanten Programme auf Ihrem Computer stets auf dem neusten Stand sind. Dies gilt insbesondere für für das Betriebssystem. Durch veraltete Versionen entstehen Sicherheitslücken, gerade dann wenn der Support bereits eingestellt wurde. Dies war zuletzt bei Microsofts Windows Vista der Fall. Seit dem 11. April 2017 liefert der Branchenprimus aus Redmond keine sicherheitsrelevanten Updates mehr für das System, die Nutzer sind somit unzureichend gegen neue Bedrohungen geschützt.

Auch Unternehmen können mittlerweile auf eine ganze Bandbreite an Schutzmechanismen zurückgreifen. Neben klassischen Spam- und Virenfiltern, die bereits den Löwenanteil der infizierten E-Mails herausfiltern, gibt es Anbieter, die so genannte *„Advanced Threat Protection"*-Lösungen anbieten, die speziell für die Erkennung von Ransomware und gezielten Angriffen wie CEO-Fraud entwickelt wurden.

Fazit: Die richtige Vorsorge kann eine Menge Ärger ersparen

Ransomware aktiv bekämpfen heißt auch, sich intensiver mit ihr zu beschäftigen. Weitaus weniger Nutzer würden Tools für die aufwendige Entfernung der Trojaner und Entschlüsselung der Dateien benötigen, wenn sie im Vorfeld besser über die Schädlinge informiert- bzw. besser vor ihnen geschützt gewesen wären. Ein guter Mix aus Aufklärung und technischen Vorkehrungen ist dabei das A und O, um Infektionen bestmöglich auszuschließen. Bezüglich der technischen Maßnahmen gibt es, wie schon angesprochen, gerade für Unternehmen gute Möglichkeiten um die mittlerweile zahlreichen unterschiedlichen Cyber-Bedrohungen abzuwehren. Genug Wege und Mittel sich zu schützen existieren also. Doch nun liegt es in unserer Hand, ob wir sie auch tatsächlich nutzen.

Über Hornetsecurity:

Der führende deutsche Cloud-Security-Provider Hornetsecurity schützt die IT-Infrastruktur, Kommunikation und Daten von Unternehmen und Organisationen jeglicher Größenordnung. Seine Dienste erbringt der Sicherheits-Spezialist aus Hannover über redundante, gesicherte Rechenzentren in Deutschland und nach deutschem Datenschutzrecht. Das Lösungsportfolio beinhaltet Services in den Bereichen Mail Security, Web Security und File Security. Alle Services des Unternehmens sind in kurzer Zeit implementierbar und rund um die Uhr verfügbar. Bis Anfang 2015 firmierte Hornetsecurity unter dem Namen antispameurope.

Mehr Informationen finden Sie unter www.hornetsecurity.com und www.hornetdrive.com

Pressekontakt:
Hornetsecurity
Christoph Maier
Am Listholze 78
30177 Hannover
Tel.: +49 (511) 260 905-25
Fax: +49 (511) 260 905-99
E-Mail: presse@hornetsecurity.com