Statt Lockvogel eine Erpressungsnachricht: der CryptoLocker.

# ALLES IST VERLOREN

## HILFE, MEINE DATEN SIND VERSCHLÜSSELT!

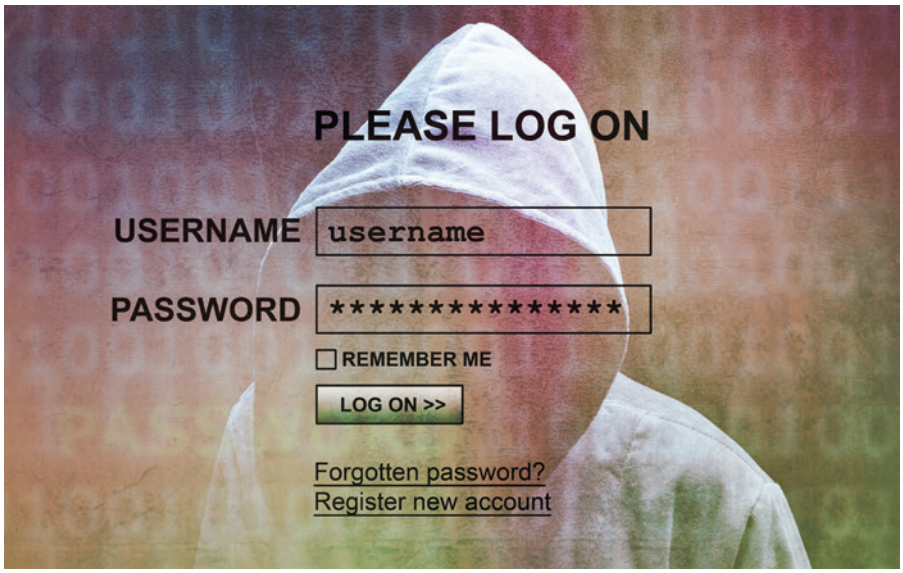
von Andreas Wisler

**Praktisch wöchentlich berichten diverse Medien über neue Varianten von Schädlingen, die die Festplatte beziehungsweise die vorhandenen Daten verschlüsseln. Oft so, dass es nicht mehr möglich ist, an die eigenen Daten zu kommen. Der Hilfeschrei ist laut: Wie komme ich wieder an meine Daten?**

Immer wieder hört und liest man von Software, die die lokalen Daten auf dem Rechner verschlüsselt. Inzwischen gibt es sogar Schädlinge, die auf verbundene Serverlaufwerke oder gar auf ein Network Attached Storage (NAS), die oft als Backup verwendet wird, zugreift. Dann sind nicht nur die eigenen Daten auf dem Rechner verloren, sondern auch gleich das Backup mit. Solche Programme werden oft als CryptoWalls bezeichnet. Vielmals ist auch von CryptoLocker zu lesen. Technisch sind diese beiden Varianten aber komplett verschieden und weisen keine Gemeinsamkeiten auf. Wer aber genau hinter diesen vielen Angriffen steht, ist unbekannt. Die Vermutung liegt nahe, dass diese aus dem Gebiet der ehemaligen Sowjetunion stammen, da Daten auf russischen Betriebssystemen nicht verschlüsselt werden.

### AUFGLEISEN EINER ERPRESSUNG

CryptoLocker wurde zum ersten Mal am 5. September 2013 im Internet erkannt. Die Verteilung erfolgte über E-Mails und das Botnet ZeuS. Ein Botnet sind von Hackern übernommene Rechner, die für die Verteilung des Schädlings genutzt werden. Wird CryptoLocker ausgeführt, sucht er bestimmte Dateitypen wie DOC/DOCX




**Wer glaubt, das Geld wiederzubekommen, täuscht sich meist.**

(Microsoft Word) und verschlüsselt diese mit einem mathematischen Verfahren (RSA, 2048 Bit). Dieses Verschlüsselungsverfahren wird auch für Webseiten genutzt, zum Beispiel wenn Kunden auf ihr Online-Banking zugreifen. Es gilt somit als sehr sicher. Eine Entschlüsselung der Daten ist nicht mehr möglich. Der Benutzer wird zu einer Webseite gelotst und erhält in einem Fenster die Anweisung, 500 Dollar in Bitcoins (eine virtuelle Währung im Internet, die anonym von einem Ort an einen anderen transferiert werden kann) zu bezahlen.

## PERFIDE STRATEGIE

Ein Counter weist darauf hin, wie lange man Zeit dafür hat. Nach Ablauf der Frist verdoppelt sich der Betrag, danach ist alles verloren, der dazu passende Wiederherstellungsschlüssel wird gelöscht. Verschiedene Quellen berichten, dass zwischen 1,8 und drei Prozent der betroffenen Personen bezahlen. Kürzlich war in der Tagespresse von einem Spital zu lesen, welches aus Verzweiflung nur eine Lösung aus der Misere sah und bezahlt hat. Je nach Quelle ergibt dies eine stolze Summe von drei Millionen Dollar. Dies alleine ist ein grosser Antrieb für professionelle Hacker, weiterhin auf diese Art Geld zu verdienen. Eine Reduktion der Angriffe ist daher nicht zu erwarten.

Doch bekommt der Benutzer nun seinen Schlüssel, um die Daten wieder herzustellen? Bei einigen Opfern war dies tatsächlich der Fall. Nach nur wenigen Stunden wurde das überwiesene Geld abgeholt und der Wiederherstellungsschlüssel, mitsamt einem Programm, übergeben. Damit konnten die Daten wiederhergestellt werden. Doch ob dies immer der Fall ist, ist eher unwahrscheinlich. Je nachdem wer hinter dem Schädling steht, kann der angebotene Weg auch ins Leere führen, und die Daten sind mitsamt dem Geld für immer verloren.

## VIER FRAGEN UND ANTWORTEN

Sind nur Windows-Benutzer davon betroffen? Nein, inzwischen sind auch Schädlinge für den Mac im Internet aufgetaucht. Die sicheren Zeiten für Mac-Benutzer sind damit definitiv vorbei, und es ist grosse Vorsicht geboten.

Wie verbreiten sich diese Schädlinge? Oft ist es der Weg via E-Mail. Aus irgendwelchen dubiosen Quellen oder dem Absuchen von Webseiten, analog wie dies Google für das Indexieren von Webseiten macht, werden E-Mail-Adressen beschafft. Diese erhalten dann die Aufforderung, eine beiliegende Datei zu öffnen. Mitte Februar 2016 wurden auch Webseiten, die mit Content-Management-System (CMS) Wordpress betrieben werden, infiziert. Durch eine vorhandene Schwachstelle kopiert sich die böse Software auf die Webseite. Besuchen Sie nun eine solche verseuchte Webseite beginnt der Schädling, ohne die Teilnahme des Betroffenen, mit der Verschlüsselung der Daten.

Wie schütze ich mich? Halten Sie Ihr System immer auf dem aktuellsten Stand. Installieren Sie die Updates (auch Patches genannt), die Microsoft und Apple herausgeben. Vergessen Sie dabei nicht die anderen Programme wie Office, Google Chrome, Firefox, Adobe Reader oder Flash. Da sammelt sich doch einiges mit der Zeit an. Eine oft mühsame, aber enorm wichtige Aufgabe. Weiter gilt es, das Antivirenprogramm aktuell zu halten. Schädlinge sind oft schon bekannt, und das Antivirenprogramm kann reagieren, sollte es in Berührung damit kommen. Und als dritter Punkt: Klicken Sie nicht alles an, auch wenn es noch so spannend erscheint.

Was ist, wenn es doch mal passiert? Da hilft oft nur eines: das Wiederherstellen des Backups. Daher gehört zu den wichtigen Aufgaben das Erstellen von regelmässigen Datensicherungen. Das reine Synchronisieren mit einem Netzwerkspeicher (NAS genannt) hat sich dabei als trügerische Sicherheit erwiesen. Ist dieser Speicher ständig verbunden oder über das Netzwerk erreichbar, verschlüsseln aktuelle Versionen der Schädlinge auch diese Daten. Sie benötigen daher ein Backup an einer externen Stelle. Dies kann zum Beispiel eine Wechselplatte oder ein grosser USB-Stick sein, den Sie wieder vom Rechner entfernen. Sollten Sie den Schädling auf dem Rechner haben, entfernen Sie diesen, bevor Sie die Festplatte anhängen. Erst wenn Sie ganz sicher sind, dass alles in Ordnung ist, spielen Sie Ihre vorher gesicherten Daten zurück.

## SCHUTZ IST MÖGLICH

Die Betrüger im Internet haben einen neuen Weg gefunden, viel Geld zu verdienen. Da es mit den heutigen technischen Möglichkeiten nicht mehr möglich ist, an die verschlüsselten Daten zu kommen, ist es enorm wichtig, im Vorfeld für eine umfassende und geschützte Datensicherung zu sorgen. Im Internet gilt es, Vorsicht walten zu lassen und nicht jedes E-Mail oder jede Webseite anzuklicken, sondern im Vorfeld zu überlegen, will ich das wirklich? Nur so können Sie sich optimal vor den aktuellen Gefährdungen schützen. ■

ANDREAS WISLER

ist CEO und Senior Security Consultant von goSecurity.

www.gosecurity.ch