Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

- Was ist Ransomware
- Sollten Sie das Lösegeld zahlen?
- Datensicherung
- Weitere vorbeugende Maßnahmen

Ransomware

Was ist Ransomware?

Ransomware (Verschlüsselungs- oder Erpressungstrojaner) bezeichnet eine spezielle Form von Schadprogrammen, die derzeit sehr aktiv im Internet Verbreitung findet und die Dateien und Dokumente der Opfer bedroht. Schadprogramme sind Programme, die bösartige Aktionen auf einem Computersystem ausführen. Wenngleich Ransomware nur eine von vielen verschiedenen Schadprogramm-Typen ist, ist sie bei Kriminellen sehr beliebt weil ihre Verbreitung sehr profitabel ist. Sobald Ransomware einen Computer infiziert, verschlüsselt sie bestimmte Dateitypen oder sogar gleich die gesamte Festplatte. Sie sind dann aus dem System augesperrt oder haben zumindest keinen Zugriff mehr auf Dateien, die Ihnen wichtig sind, z.B. Ihre Dokumente oder Fotos. Das Schadprogramm informiert Sie daraufhin, dass der einzige Weg zur Entschlüsselung Ihrer Dateien oder wieder Zugriff auf Ihr System zu erhalten darin besteht, den kriminellen Erpressern den geforderten Lösegeldbetrag zu zahlen (daher der Name Erpressungstrojaner). Meist muss das Lösegeld in einer Digitalwährung wie z.B. Bitcoin bezahlt werden. Ransomware wird wie viele andere Schadprogramme auch verteilt. Die gängigste Methode besteht im Versenden von speziell präparierten E-Mails, mit denen die Angreifer Sie davon überzeugen wollen, einen bösartigen Link anzuklicken oder einen infizierten Dateianhang zu öffnen.

Gastautor

Lenny Zeltser konzentriert sich auf den Schutz des IT-Betriebs von Kunden der NCR Corp und unterrichtet in der Bekämpfung von Schadprogrammen für das SANS Institut. Lenny ist auf Twitter unter **@lennyzeltser** zu finden und schreibt ein Blog über IT-Sicherheit auf **zeltser.com**.

Sollten Sie das Lösegeld zahlen?

Eine schwierige Frage. Das Problem besteht darin, dass die Cyberkriminellen um so motivierter werden Ihre Schadprogramme weiter zu verbreiten, je mehr Menschen auf ihre Forderungen eingehen. Andererseits haben Sie vielleicht keine alternative Möglichkeit, wieder Zugriff auf Ihre Dateien zu erlangen. Seien Sie aber gewarnt, auch wenn Sie das Lösegeld bezahlen besteht keinerlei Garantie, dass Sie Ihre Dateien zurückerhalten. Sie haben es hier mit Kriminellen zu tun, die keinerlei Veranlassung haben Ihnen die Dateien wieder zu entschlüsseln. Ebenso kann beim Ver- oder Entschlüsseln etwas schiefgehen, oder Ihr Computer wird mit weiteren Schadprogrammen infiziert.

Datensicherung

Der wahrscheinlich beste Weg sich von einer Infektion mit Ransomware zu erholen und kein Lösegeld zahlen zu müssen besteht in der Wiederherstellung Ihrer Daten aus einer Datensicherung (Backup). Dadurch haben Sie eine Möglichkeit,

Ransomware

nach einer Neuinstallation oder dem Säubern Ihres Computers all Ihre Dateien wieder aufzuspielen. Bedenken Sie dabei, dass auch Ihre Datensicherung von der Ransomware verschlüsselt oder gelöscht wird, wenn sie dauerhaft von Ihrem Computer erreichbar ist. Es ist daher essentiell, Dateien bei namhaften Cloud-Speicheranbietern zu sichern oder auf externe Datenträger, die nicht ständig mit Ihrem Computer verbunden sind. Eine weitere gängige Fehlannahme von Nutzern besteht darin anzunehmen, dass Datensicherungen zur Wiederherstellung von Dateien schon funktionieren werden, ohne dies je getestet zu haben. Stellen Sie daher sicher, regelmäßig zu prüfen ob Sie auf die gesicherten Daten zugreifen können, und dass Sie die benötigten Dateien wiederherstellen können wenn Ihr System mit Ransomware infiziert werden sollte. Datensicherungen sind auch bei anderen Gelegenheiten nützlich, z.B. wenn Sie aus Versehen Dateien löschen oder Ihre Festplatte defekt ist.

Ransomware sind Schadprogramme, die sobald sie Ihren Computer infiziert haben, alle Dateien verschlüsseln, so dass Sie keinen Zugriff mehr darauf haben.

Weitere vorbeugende Maßnahmen

Vor Ransomware können Sie sich mit den gleichen Mitteln schützen wie gegen andere Schadprogramme – lassen Sie sich gar nicht erst infizieren. Beginnen Sie damit sicherzustellen, dass Sie ein Antivirusprogramm eines renommierten Herstellers einsetzen und dies stets aktuell halten. Solche Programme, oft auch Anti-Malware genannt, sind genau darauf ausgelegt Schadprogramme zu erkennen und zu zerstören. Sie können jedoch nicht alle Schadprogramme erkennen oder entfernen, da diese von den Kriminellen in einer unglaublichen Geschwindigkeit weiterentwickelt werden. Sie sind dadurch in der Lage, die Erkennungsmechanismen der Anti-Malware Programme zu umgehen. Im Gegenzug verbessern aber auch Antivirus-Hersteller kontinuierlich ihre Produkte mit neuen Methoden zur Erkennung von Schadprogrammen. Es ist zu einem regelrechten Wettrüsten geworden, bei dem beide Seiten versuchen den anderen zu überlisten. Leider sind die Bösewichte meist einen Schritt voraus, daher ist es so wichtig dass Sie Ihre Daten sichern und noch weitere Schritte zu Ihrer Absicherung ergreifen:

- Cyberkriminelle infizieren Computer oder Mobilgeräte oft durch das Ausnutzen von Schwachstellen in installierten Programmen. Je aktueller Ihre Programme sind, desto weniger bekannte Schwachstellen weist Ihr System auf und desto schwieriger ist es für Cyberkriminelle, es zu infizieren. Stellen Sie daher sicher, dass Ihre Geräte, das Betriebssystem und alle Anwendungen „Automatische Updates“ aktiviert haben.
- Nutzen Sie auf Computern standardmäßig ein Benutzerkonto mit begrenzten Rechten anstelle von privilegierten Konten wie „Administrator“ oder „root“. Das schafft einen zusätzlichen Schutz, indem es bei vielen Schadprogrammen verhindert, dass sie sich überhaupt im System verankern können.

Ransomware

- Cyberkriminelle überlisten Anwender oft und bringen sie dazu, das Schadprogramm selbst zu installieren. Sie könnten Ihnen zum Beispiel eine E-Mail senden die legitim aussieht und einen Link oder einen Dateianhang enthält. Die E-Mail scheint vielleicht von Ihrer Hausbank oder von einem Bekannten gesendet zu sein. Wenn Sie jedoch die angehängte Datei öffnen oder den Link anklicken, aktivieren Sie die Funktion, die das Schadprogramm auf Ihrem Computer installiert. Wenn eine Nachricht eine besondere Dringlichkeit suggeriert, verwirrend formuliert ist oder zu gut um wahr zu sein erscheint, könnte es sich um einen Angriff handeln. Lassen Sie die gebotene Vorsicht walten und nutzen Sie Ihren gesunden Menschenverstand – oft Ihr bestes Mittel zur Abwehr dieser Angriffe.

Schützen Sie sich vor Ransomware indem Sie wachsam sind wenn Sie einen E-Mail-Anhang öffnen oder einen Link aufrufen, stellen Sie sicher jederzeit einen aktuellen Virenschutz zu nutzen und prüfen Sie regelmäßig Ihre Datensicherung, ob die Dateien wirklich gesichert werden und auch wiederhergestellt werden können.

Weiterführende Informationen

Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
Schadprogramme:	https://securingthehuman.sans.org/ouch/2016#march2016
Verschlüsselung:	https://securingthehuman.sans.org/ouch/2016#june2016
Datensicherung & Wiederherstellung:	https://securingthehuman.sans.org/ouch/2015#august2015
Wikipedia Artikel zu Ransomware:	https://de.wikipedia.org/wiki/Ransomware
SANS FOR610 Kurs - Reverse Engineering Malware:	https://sans.org/for610

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter securingthehuman.sans.org/ouch/archives.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley