Angriffe, Betrug, Erpressung

Die Zahl der Fälle von Erpresser-Trojanern, Cyber-Angriffen und Betrügereien nahm laut dem Internet-Sicherheitsbericht des „Computer Emergency Response Teams“ zu.

Cybercrime hat sich zu einem lukrativen illegalen Geschäftszweig entwickelt – ähnlich dem Menschen- oder Drogenhandel. 2016 standen vor allem Bedrohungen durch Ransomware und DoS/DDoS-Angriffe im Fokus. 2016 wurden verstärkt kleine und mittelgroße Unternehmen Opfer des „Geschäftsführerbetrugs“ („CEO-Fraud“). Das geht aus dem Internet-Sicherheitsbericht 2016 des *Computer Emergency Response Teams (CERT.at)* hervor, der am 20. Jänner 2017 in Wien präsentiert wurde.

Ransomware gilt mittlerweile als die „profitabelste Schadsoftware“. Bei Angriffen mit Ransomware werden Computernutzer erpresst, indem die Angreifer das Gerät sperren oder Daten verschlüsseln. Für die Entschlüsselung wird Lösegeld (Ransom) verlangt – meist in Form von *Bitcoins*. Die Höhe der geforderten Summen bewegt sich von 500 bis zu 140.000 Euro. Die Schäden bei Firmen durch Ransomware reichen von Umsatzverlusten bis hin zur Unterbrechung der Geschäftstätigkeit. Das Security-Software-Unternehmen *IKARUS* verzeichnete in Österreich Anfang 2016 bis zu 25.000 Infektionsversuche durch Erpresser-Trojaner pro Tag. Im Sommer 2016 wurde im Bundeskriminalamt (BK) im Cybercrime-Competence-Center (C4) eine Sonderkommission einrichtete. Die Soko-Mitarbeiter übernehmen seither die Bearbeitung aller bundesweit angezeigten Ransomware-Fälle – rund 30 neue Vorfälle pro Woche.

Digitale Erpressung: Die Zahl der Fälle von Daten-Verschlüsselungen durch Ransomware nahm zu.

In Österreich waren 2016 vor allem zwei Angriffsvarianten vorherrschend. Bei der als Bewerbungsschreiben getarnten Variante versandten die Täter E-Mails mit schadhaftem Inhalt. Wurde eine Datei in einem Anhang oder ein Downloadlink geöffnet, installierte sich ein Ableger der Ransomware „Cerber“. Die Folge: Die Daten auf Computern und Laufwerken wurden verschlüsselt und waren nicht mehr abrufbar. Das Gleiche passierte bei Phishing-Mails, die als Online-Rechnung des Stromversorgers *Verbund AG* getarnt waren. Sie enthielten die Schadsoftware „Cryptolocker“, die Dateien auf dem PC verschlüsselt. *CERT.at*-Leiter Mag. Robert Schischka warnt davor, auf Lösegeldforderungen einzugehen. „Jeder Cent fließt in den Aufbau von Infrastruktur, um stärkere Angriffe zu fahren.“

DDos-Attacken (Distributed Denial of Service) und DoS-Attacken (Denial of Service) zählen zu den häufigsten Cyber-Angriffen. Im Visier der Kriminellen sind vor allem Industrie- und Finanzbetriebe. Typische DDoS-Angriffe zielen auf die Überlastung der Internetanbindung, der Netzwerke sowie der Web- und Datenbankserver ab. Im Gegensatz zu einer einfachen DoS-Attacke haben DDoS-Angriffe eine höhere Schlagkraft. Mehrere Computer greifen dabei gleichzeitig und im Ver-

RANSOMWARE

Präventionstipps

Ransomware-Angriffe können eingedämmt werden, wenn die Code-Ausführung verhindert wird. Folgende Strategien sind hilfreich:

- Eine verdächtige E-Mail, die ungelesen gelöscht wird, richtet keinen Schaden an.
- Effektive Filterung von E-Mails: Im besten Fall werden E-Mails mit gefährlichem Inhalt bereits am E-Mail-Gateway aussortiert.
- Schutz des Browsers: Die Software sollte immer auf dem neuesten Stand sein. Auf Erweiterungen wie *Flash* und *Java* sollte verzichtet werden. Darüber hinaus empfiehlt sich der Einsatz von Script-Blockern.
- Automatische Ausführung von Makro-Code in Office-Programmen deaktivieren: Makros werden häufig in Office-Dateien eingesetzt. Es besteht Infektionsgefahr, wenn *Office*-Programme so eingestellt sind, dass sie Makro-Codes ohne Nachfrage ausführen. Man sollte in *Outlook* und *Word* das automatische Ausführen von Makro-Codes deaktivieren.
- Back-up: Aktuelle, sichere, verfügbare und getestete Sicherheitskopien der Daten sind eines der wirkungsvollsten Mittel gegen die Auswirkungen von Ransomware.
- Die Back-ups sollten nicht von der Ransomware mitverschlüsselt werden können. So ist etwa eine dauerhaft an den PC/Server angesteckte USB-Platte für solche Fälle kein wirksames Back-up.
- Bei Back-ups in die Cloud muss sichergestellt werden, dass auch auf „alte“ Versionen der gesicherten Dateien zugegriffen werden kann. Ein tägliches Back-up ist in den meisten Fällen sinnvoll. Regelmäßiges Testen und Üben der Wiederherstellung von Daten gehören ebenso zu einer guten Back-up-Strategie wie längerfristiges Aufheben von einzelnen Back-up-Ständen.
- Rettung der Daten: Manchmal machen die Programmierer von Ransomware Fehler bei der Umsetzung der Verschlüsselung oder dem Schlüsselmanagement. Daher gelingt es Sicherheitsforschern immer wieder, Werkzeuge zur Datenrettung zu erstellen. Die zentrale Anlaufstelle dazu ist die Webseite *www.nomoreransom.org*, die von Europol koordiniert wird. Zur Identifikation der Ransomware dient die Seite *https://id-ransomware.malwarehunterteam.com*.

FOTO: EIBNER/EXPA/PICTUREDESK.COM

bund (beispielsweise über ein Botnetz) eine Webseite oder eine Netzinfrastruktur an. Das angegriffene System wird mit teils sinnlosen Anfragen überflutet, die mit den dort zur Verfügung stehenden Ressourcen nicht mehr schnell genug abgearbeitet werden können. Ziele derartiger Angriffe waren 2016 in Österreich das Außenministerium, das Bundesheer, die Nationalbank, der Flughafen Wien und das Telekomunternehmen *A1*. Von *A1* wollten die Angreifer 100.000 Euro in *Bitcoins* haben. Sie gaben auf, als die Techniker des Unternehmens die Attacken abwehrten. DDoS-Angriffe können im Darknet „eingekauft" werden.

Betrug. *CERT.at* stellte 2016 vermehrt Fälle des „Business-E-Mail-Compromises" und des „CEO-Frauds" fest. Beim Business-E-Mail-Compromise stellt ein Unternehmen zunächst per Mail eine „normale" Rechnung an ein anderes Unternehmen. Nach ein paar Stunden wird eine zweite E-Mail gesandt – diesmal von einem neu registrierten, gefälschten Domain-Namen, der sich oft nur durch einzelne Buchstaben unterscheiden lässt. Im Vorfeld haben die Angreifer die Kommunikation zwischen den Unternehmen abgefangen. Die Folge-E-Mails zeichnen sich dadurch aus, dass sie mit der vorherigen E-Mail ident sind, jedoch auf ein geändertes Empfängerkonto hinweisen, was in der E-Mail auch begründet wird. Beispielsweise wird eine Kontosperre durch die Finanz aufgrund eines Audits angegeben. Kommen Rückfragen von Rechnungsempfängern, wird wiederum vom Angreifer mit gefälschten Dokumenten geantwortet. Wird der Betrugsversuch durch den Rechnungsempfänger nicht erkannt, erfolgt eine Überweisung auf ein Konto des Angreifers.

Beim „CEO-Fraud" geben sich Betrüger als Geschäftsführer oder Finanzvorstand eines Unternehmens aus und fordern von Mitarbeitern eine dringende Überweisung auf ein falsches Konto, beispielsweise durch eine gefälschte E-Mail an die Buchhaltung. Die Betrüger spionieren die firmeninterne Struktur aus, sodass der Auftrag des „Chefs" glaubwürdig erscheint. „Business-E-Mail-Compromise" und „CEO-Fraud" sind keine Cyber-Kriminalität im klassischen Sinne, sondern eine Betrugsform.

Internet-Sicherheitsbericht 2016: www.cert.at