Cybercrime: In der Europäischen Union gibt es eine Million Opfer von Cyber-Attacken pro Tag.

Präsentation des Internet-Sicherheitsberichts 2015: Staatssekretärin Sonja Steßl, Robert Schischka, CERT.at.

Angriffsziel Unternehmen

Cyber-Angriffe, Datendiebstähle und Bedrohungen über das Internet haben laut dem CERT-Internet-Sicherheitsbericht 2015 zugenommen. Betroffen sind Privatpersonen und zunehmend Unternehmen.

Das Thema Internetsicherheit sei das Zukunftsthema in Österreich und werde immer mehr einer breiten Öffentlichkeit bewusst, sagte Digital-Staatssekretärin Mag. Sonja Steßl am 15. Februar 2016 in Wien bei der Präsentation des Internet-Sicherheitsberichts 2015.

„Das Bewusstsein für Sicherheitsmaßnahmen zu steigern, ist eine wichtige Basis, um Österreich cybersicherer zu machen", sagte die Staatssekretärin. In diesem Sinne wurde auch die Österreichische Strategie für Cyber-Sicherheit erstellt, deren Ergebnis unter anderem die Schaffung eines *Cyber Security Centers* im Bundesministerium für Inneres oder der jährlich erscheinende Internetsicherheitsbericht sei. Auch das in Vorbereitung befindliche Cyber-Sicherheitsgesetz, das vom Bundeskanzleramt koordiniert und in Abstimmung mit dem Innen- und dem Verteidigungsministerium entsteht, werde zur Stärkung der Internetsicherheit in Österreich beitragen. Dieses Gesetz soll die Österreichische *Strategie für Cyber-Sicherheit* mit der Europäischen Richtlinie für Netzwerk- und Informationssicherheit zusammenführen.

CEO-Betrug. Laut dem Internet-Sicherheitsbericht 2015, der von der österreichischen Domainverwaltung *nic.at* und dem *Computer Emergency Response Team (CERT.at)* gemeinsam mit dem Bundeskanzleramt *(GovCERT Austria)* erstellt wurde, gehe es den Cyber-Kriminellen immer mehr ums Geld. Als Beispiel für das Vorgehen der Täter nannte Mag. Robert Schischka von *CERT.at* den Business E-Mail-Compromise, eine Betrugsmasche, mit der die Täter Unternehmen schädigen. Bei dieser Betrugsart, auch als „Fake President Fraud" oder „CEO-Betrug" bezeichnet, täuschen die Kriminellen Mitarbeiter von Unternehmen mit falschen Identitäten. Sie geben sich in fingierten E-Mails als Vorgesetzte aus und fordern Angestellte auf, größere Summen auf ein ausländisches Bankkonto zu überweisen. Laut Schischka spionieren die Täter vorher das Unternehmen aus und wissen dadurch Bescheid über die Geschäftsführung, Auftragslage, Geschäftspartner, geschäftliche Gepflogenheiten etc.

In Österreich gab es 2015 etwa ein halbes Dutzend derartiger Angriffe auf Unternehmen, bei denen finanzielle Schäden im sechs- und siebenstelligen Euro-Bereich verursacht worden sind.

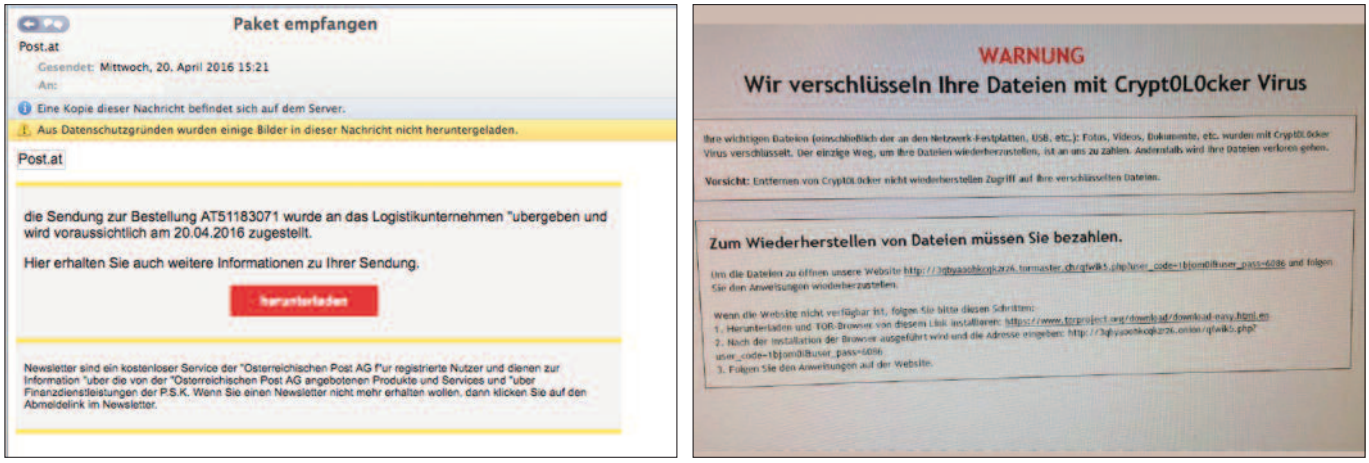
Unternehmen sind eine beliebte Zielscheibe für Cyber-Kriminelle. Laut dem auf Sicherheitssoftware spezialisierten Softwarehersteller *Kaspersky Lab* hatte 2015 über die Hälfte der weltweiten Rechner in Unternehmensnetzwerken mindestens eine Malwareattacke zu überstehen. Gegen Firmenrechner werden dreimal häufiger Exploits (Schadprogramme, die Sicherheitslücken ausnutzen) zu Office-Anwendungen eingesetzt, als bei Angriffen auf private Computer.

Ransomware befällt den Rechner und verschlüsselt in der Folge Dateien auf der lokalen Festplatte und auf erreichbaren und für den jeweiligen Nutzer berechtigten Netzwerklaufwerken. Bezahlt man das Lösegeld (Ransom), versprechen die Täter ein Werkzeug zur Wiederherstellung der Dateien. Der tatsächliche Schaden durch diese Programme kann nur geschätzt werden, da viele der Betroffenen den Fall nicht zur Anzeige bringen. Ransomware gehört mittlerweile auch in Österreich zu den gefährlichsten Angriffsformen.

Der Ransomware-Trojaner „CryptoLocker" war im Frühjahr 2015 stark verbreitet. Über E-Mail-Anhänge, gefälschte Paketdienst-Links und Webseiten verbreitet, befiel „CryptoLocker" zahlreiche Rechner, darunter viele kleine und mittelgroße Unternehmen. Im Durchschnitt wurden 500 Euro – meist in Bitcoins – für den Entschlüsselungscode gefordert.

DDoS-Attacken. Bei Ransomware droht ein Angreifer mit dem Verlust der eigenen Daten, bei DDoS-Attacken (Distributed Denial of Service) richten sich Angriffe auf die Verfügbarkeit der Online-Dienste und der dahinterliegenden Systeme seiner Opfer. Werden durch eine solche Attacke die Systeme

FOTO: BKA/REGINA AIGNER, FOTOLIA/GLEBSTOCK



Angebliche Paket-Verständigung von der „Post“: Beim Herunterladen des Versandscheines wird eine Zip-Datei ausgeführt, die Daten durch Verschlüsselung unbrauchbar macht.

des Opfers überlastet, können Kunden des Opfers dessen Online-Dienstleistungen nur mehr eingeschränkt oder schlimmstenfalls gar nicht mehr nutzen. In den letzten zwei Jahren hat sich der Kreis der DDoS-Opfer stark erweitert, insbesondere nehmen diesbezügliche Erpressungen stark zu. Im Juli 2014 tauchte die Gruppe *DD4BC (DDoS for Bitcoins)* zum ersten Mal auf. Sie richtete ihre Attacken auf Bitcoin-Webseiten, dann auf Finanzdienstleister, *E-Commerce*-Webseiten und Internet-Service-Provider.

Auch in Österreich wurden Systeme überlastet und Erpressungs-E-Mails versendet. Die Erpressungssummen bewegten sich oft im fünfstelligen Bereich und wurden in Form von Bitcoins verlangt. Für den Fall ausbleibender Zahlungen wurden weitere DDoS-Angriffe angedroht.

Neben Österreich und Deutschland war die Gruppe *DD4BC* vor allem in Skandinavien, Australien und den Vereinigten Staaten aktiv. Im Dezember 2015 konnten im Zuge einer Aktion von Europol – unter Federführung des österreichischen *Cybercrime-Competence-Centers (C4)* im Bundeskriminalamt – die Täter gefasst werden.

CERT-Experten raten im Falle einer DDoS-Attacke das verlangte Lösegeld auf keinen Fall zu bezahlen. Es sei durch eine Zahlung nicht garantiert, dass keine weiteren Angriffe folgen würden. Außerdem steige die Wahrscheinlichkeit für Nachahmungs- und Wiederholungstäter. In jedem Fall sollte Kontakt mit *CERT.at (www.cert.at)* aufgenommen werden oder mit der Meldestelle des Bundeskriminalamts zur Bekämpfung der Cyber-Kriminalität *(against-cybercrime@bmi.gv.at)*.

Betrug. Immer mehr Betrugsvarianten tauchen im Internet auf. Das reicht von Vorschussbetrug, über den Neffentrick bis hin zum Versuch, mit gefälschten Rechnungen an Geld zu gelangen – wie zum Beispiel mit gefälschten Rechnungen für Partezettel. Regelmäßig sind Kunden großer Online-Unternehmen von derart gefälschten Rechnungen betroffen. Es bestehen auch Varianten, bei denen Opfern eine E-Mail von einem angeblichen Anwalt des Online-Unternehmens erhalten. Die Anwalt-Variante ist zwar neu, die Ziele bleiben jedoch die alten, nämlich das Erspähen von Kontodaten oder das Drängen zur Überweisung.

Weiters sind gefälschte E-Mails von Paketdienstleistern, Mobilfunkanbietern oder Banken im Umlauf. Über die E-Mails wird versucht, die Nutzer auf Webseiten zu locken, die Schadsoftware verbreiten. Wer den Link in der E-Mail anklickt, wird auf eine Webseite weitergeleitet, die eine .zip- oder .exe-Datei bereitstellt. Nach deren Ausführung wird der Schadcode unbemerkt installiert. Oft erfolgt eine Infektion aber durch den Besuch der manipulierten Website; eine User-Interaktion ist in solchen Fällen nicht mehr erforderlich.

Externe Back-ups schützen Daten vor Verschlüsselung nur, wenn sie nicht mit dem Computer verbunden sind.

Mobile Internetnutzung. Mobile Geräte werden – neben der klassischen Sprachtelefonie – vorwiegend für Online-Einkäufe und soziale Netzwerke genutzt. Der hohe Anteil an persönlichen Daten in den Geräten steigert deren Attraktivität für Cyber-Attacken. Laut dem New Yorker Analyseunternehmen *Forensiq (https://forensiq.com)* wurde 2015 durch In-App-Betrug mit Werbung eine Schadenshöhe von über einer Milliarde US-Dollar verursacht. Die Betrüger verschaffen sich unter anderem über manipulierte Apps Zugang zu Smartphones und Tablets und laden unsichtbar für den Nutzer im Hintergrund mobile Werbeanzeigen. Dabei simulieren sie Klicks auf Werbeanzeigen in Apps und erreichen in kurzer Zeit unzählige Aufrufe, die von den Werbetreibenden bezahlt werden.

Sicherheitsbewusstsein. Mit der im Februar 2015 veröffentlichten Eurobarometer-Umfrage zum Thema Cyber-Sicherheit erhob die EU-Kommission das Thema „Sicherheit im Internet“ aus der Perspektive der Bevölkerung. Mit über 150.000 Viren und über einer Million Opfern von Cyber-Attacken pro Tag spielen Cyber-Bedrohungen in der EU eine wesentliche Rolle.

Die häufigsten Aktivitäten der Nutzerinnen und Nutzer im Netz sind das Abrufen von E-Mails (86 %), das Lesen von Online Zeitungen (63 %), soziale Netzwerke (60 %) und Online-Einkäufe (57 %). Nur 61 Prozent aller Internetnutzerinnen und -nutzer in Europa haben eine Anti-Virus Software installiert – in Österreich sind es 73 Prozent.

Internet-Sicherheitsbericht: www.cert.at

Fotos: Fotolia/Nomad_Soul, Bundeskriminalamt (2)