Geld für Daten

Die Zahl der Cyber-Angriffe nimmt laut Experten des Computer-Emergency-Response-Teams Austria zu. Betroffen sind nicht nur Firmen und Organisationen sondern zunehmend auch Privatpersonen.

Das Internet ist längst zu einer zentralen und kritischen Infrastruktur für die Gesellschaft, die Wirtschaft und für die Behörden geworden", sagte Kanzleramts-Staatssekretärin Mag.ª Sonja Steßl bei der Vorstellung des Internet-Sicherheitsberichts 2014 am 15. Jänner 2015 in Wien. „Cyber-Sicherheit ist ein Gut für alle. Deshalb ist es wichtig, dass die öffentliche Hand gemeinsam mit den Anbietern der digitalen Dienste und der IKT-Branche eine wesentliche Verantwortung und Rolle einnimmt."

Massenphänomen. Der CERT-Jahresbericht 2014 zeigt, dass Cyber-Angriffe zahlreicher und in ihrer Struktur komplexer geworden sind. Der weltweite Schaden geht in die Milliarden. Für 2015 könnten diese Angriffe laut Experten des CERT zu einem Massenphänomen werden. Die meisten Angriffe erfolgen aus wirtschaftlichen Motiven. Gehackt werden Systeme, die einen finanziellen Vorteil bringen. Auch Wirtschaftsspionage nimmt zu. „Hier gilt es, Prävention zu leisten, Sicherheitsvorkehrungen zu schaffen und das Bewusstsein in der gesamten Community und der Wirtschaft zu stärken", sagte Staatssekretärin Steßl.

Laut dem *Center for Strategic and International Studies (CSIS)* in Washington ist, gemessen an der Wirtschaftsleistung, der Schaden durch Angriffe aus dem Netz in Deutschland am größten. Die Auswirkungen von Cyber-Angriffen belaufen sich in Deutschland auf rund 1,6 Prozent des Bruttoinlandsprodukts (BIP). Damit liegt Deutschland vor den Niederlanden (1,5 %), den USA, Norwegen und China (je 0,6 %). In den USA, in China, Japan und Deutschland erreichten die Schäden eine Summe von etwa 200 Millionen US-Dollar. IT-Sicherheitsexperten gaben im Rahmen des Cyber-Security-Summits 2014 in Bonn bekannt, dass die *Deutsche Telekom* täglich bis zu eine Million Angriffe auf ihr Netz zählt. Laut dem Telekom-Report zur Cyber-Kriminalität 2014 registrierten neun von zehn deutschen Firmen Angriffe von außen. Nach einer Studie

Phishing: Cyberkriminelle „fischen" Passwörter und persönliche Daten.

des Beratungsunternehmens *KPMG* war in den vergangenen zwei Jahren jedes vierte Unternehmen in Österreich von Cyber-Angriffen betroffen. Die durchschnittliche Schadenshöhe betrug fast 400.000 Euro.

Bank-Trojaner und Adware. Experten des *G DATA Security Labs* gaben im Malware-Report für das erste Halbjahr 2014 bekannt, dass alle 8,6 Sekunden ein neuer Computerschädling für *Windows*-PCs und -Notebooks auftauchte. Besonders starke Zuwächse gab es bei „Bank-Trojanern". Eine Analyse der Top-25-Bank-Angriffsziele zeigt, dass Kunden amerikanischer Banken und Bezahldienste mit 48 Prozent am stärksten betroffen waren.

Neben den „Bank-Trojanern" wurden 2014 vermehrt „Adware"-Programme festgestellt. Sie zeigen Werbung auf dem Computer an und leiten Suchanfragen auf Werbe-Webseiten um. Diese „potenziell unerwünschten Programme" (PUP) sind keine Malware im klassischen Sinn. Anwender empfinden sie aber als störend; vor allem, da „Adware" oft schwer zu deinstallieren ist.

Ransomware. CERT-Experten registrierten 2014 Fälle von Online-Erpressungen. „Ransom" steht für „Lösegeld" und bezeichnet eine Schadsoftware, die den PC sperrt und gegen „Lösegeld" wieder freigibt. Ein aktuelles Beispiel ist „CryptoWall 2.0". Man erhält die Nachricht, dass alle Dateien verschlüsselt werden und der Entschlüsselungscode nur gegen Bezahlung zugeschickt wird. Bei Nicht-Bezahlung würden alle Dateien des PCs gelöscht werden, lautet die Drohung. Frühere Versionen von Ransomware ließen sich noch austricksen, inzwischen ist die Entwicklung so weit fortgeschritten, dass die Daten ohne Hilfe der Erpresser nicht mehr wiederherstellbar sind. Experten raten, ein regelmäßiges Backup von Daten auf einem externen Datenträger vorzunehmen, der nicht ständig mit dem Computer verbunden ist. Eine angesteckte USB-Festplatte kann ebenfalls von der Ransomware verschlüsselt werden.

Phishing war auch 2014 ein Phänomen, mit dem viele Internetnutzer konfrontiert waren. Dabei werden Passwörter „gefischt". Das geschieht mit gefälschten Webseiten und E-Mails, in denen Nutzer aufgefordert werden, ihre Zugangsdaten bekannt zu geben. Dies betrifft Online-Banking-Daten sowie Dienste wie Webmail, Social Media, Onlinespiele und E-Commerce-Seiten. Mit diesen personenbezogenen Daten versuchen die Angreifer, zu Geld zu kommen. Eine neue Form des Phishings kombinierten Cyber-Angreifer 2014 erstmals mit dem Online-Speicherdienst *Dropbox*. Dabei wurde in einem öffentlichen *Dropbox*-Ordner eine gefälschte Login-Seite hinterlegt, um die eingegebenen Daten (Username und Passwort) der Nutzer zu erhalten. Die dabei verwendete URL ähnelte jener der echten *Dropbox*-Domain.

Defacements, die Manipulation und Veränderung von Webseiten, haben sich in den letzten Jahren zu einem ernstzunehmenden Problem entwickelt. 2014 gab es Angriffe auf frei erhältliche CMS-Systeme über Erweiterungen wie Add-ons, Vorlagen, Designs und dergleichen. Vor allem die Installation von manipulierten Erweiterungen zu Webservern hat sich 2014 als neuer Trend herauskristallisiert.

Hacking. Bei einem Cyber-Angriff 2014 auf die Firma Sony ist es Hackern gelungen, in das Netz von Sony Pictures Entertainment einzudringen, Terabytes an Firmendaten zu kopieren und

FOTOS: MAHO/FOTOLIA.COM

Angriffe auf Computer könnten 2015 laut Experten des CERT zu einem Massenphänomen werden.

Foto: Artur Marciniec/Fotolia.com

das dortige Netz lahmzulegen. Unveröffentlichte Filme, E-Mails und vertrauliche Geschäftsdokumente wurden illegal im Internet verbreitet. Laut Sicherheitsexperten des FBI wäre die dabei verwendete Schadsoftware von 90 Prozent der im Privatsektor verwendeten Sicherheitsprogramme nicht entdeckt worden. Auch der öffentliche Bereich hätte diese Malware mit hoher Wahrscheinlichkeit nicht bemerkt. Ein ähnlicher Fall ist jener, der unter dem Namen „iCloud-Hack" Anfang September 2014 bekannt wurde: Hackern war es gelungen, die Passwörter zahlreicher US-Stars zu knacken und Nacktfotos aus der iCloud zu entwenden, die anschließend im Internet verbreitet wurden.

Laut dem IT-Sicherheitsanbieter *Trend Micro* soll die Zahl an Hackerangriffen 2015 zunehmen. Gemäß dem *Microsoft Security Intelligence Report 2014* sollen vor allem Industrie-Unternehmen verstärkt von Cyber-Angriffen und Wirtschaftsspionage betroffen sein. Dabei werden lediglich sechs Prozent der Unternehmen als „sehr sicher" eingestuft, neun Prozent als „wenig sicher" und 60 Prozent werden als „mittelmäßig sicher" angesehen.

Begehrte Daten. Neben persönlichen Daten werden Software, Malware-as-a-service und Hosting-Dienste gehandelt. Zu den häufigsten Formen von Datenhandel zählen der Verkauf von E-Mail-Listen an Spammer und die Weitergabe von Zugangsdaten an Identitätsdiebe. Dadurch lässt sich Malware installieren, die beispielsweise die Grundlage für Spionage mittels Webcam und Mikrofon oder für Kreditkartenmissbrauch ist.

Besonders beliebt unter Angreifern ist die Installation von Programmen, die jeden Tastendruck und somit alle Passwörter und Login-Daten mitschreiben. Betroffene können auf vielfältige Weise geschädigt werden – vom Online-Shopping bis hin zur Erpressung mit kompromittierenden Bildern und Informationen.

Jede Aktivität im Netz kann in Geld umgewandelt werden, egal ob es sich um Zugangsdaten für Facebook, E-Mail-Accounts oder die Umwandlung eines PCs in einen Webserver handelt. Letzteres kann dazu führen, dass man unwissend als Plattform für Kinderpornografie oder Phishing-Angriffe missbraucht wird.

Smartphones rücken verstärkt in den Fokus der Angreifer. Neben Angriffen auf herkömmliche PC-Systeme standen 2014 vermehrt mobile Geräte im Visier der Kriminellen. Bei Smartphones, Tablets & Co. wird immer noch weniger auf Sicherheit geachtet als bei PCs oder Laptops. Aus dem *Norton Report 2013* geht hervor, dass 63 Prozent der Smartphone-Nutzer und 30 Prozent der Tablet-Nutzer über keine grundlegenden Sicherheitsvorkehrungen verfügen. Oft fehlt sogar das Setzen eines PIN-Codes zum Entsperren des Smartphones. Betriebssysteme und Anwendungen sowie den Virenschutz sollte man regelmäßig updaten. Nicht benötigte Software und Dienste sollte man deaktivieren.

WLAN und Bluetooth. Funktionen wie GPS, Bluetooth und WLAN sind Schlupflöcher für schadhafte Software und vereinfachen Datenspionage. Der Datenaustausch über WLAN oder Bluetooth ist oft mangelhaft gesichert und kann leicht ausspioniert werden. Bleiben diese Funktionen eingeschaltet, kann schadhafte Software auf Geräte zugreifen. Deshalb sollte die WLAN-Funktion nur dann eingeschaltet werden, wenn auf ein lokales Netzwerk zugegriffen wird. Die Bluetooth-Funktion sollte aktiviert werden, wenn sie unmittelbar benötigt wird.

„Böse" Apps (Malware) speichern Informationen über das Benutzerverhalten und geben Benutzerdaten an Dritte weiter. Apps sollten daher nur aus einem offiziellen App-Store bezogen werden. Eine hundertprozentige Garantie für schadfreie Apps ist das zwar nicht, jedoch hat man über einen offiziellen Store zumindest die Möglichkeit, Apps innerhalb eines gewissen Zeitraums wieder zu deinstallieren. Gratis-Apps bzw. deren Zugriffsberechtigungen sollten generell hinterfragt werden. *Siegbert Lattacher*

www.cert.at