
CERT-Leiter Robert Schischka und Roland Ledinger, Leiter des Bereichs IKT-Strategie des Bundes im Bundeskanzleramt.

Die Hälfte der Smartphone- und Tablet-Benutzer verwendet keine Passwörter, Sicherheitssoftware oder Backup-Systeme.

# Sicherheitsbewusstsein steigern

**Laut dem Internet-Sicherheitsbericht 2013 steigen die Gefahren von kriminellen Handlungen aus dem Internet, während das Sicherheitsbewusstsein vieler, vor allem Smartphone-Nutzer, hinterher hinkt.**

Jeden Tag sind weltweit etwa 150.000 Computerviren im Umlauf und rund 148.000 Computer werden täglich neu infiziert. Täglich werden etwa eine Million Menschen Opfer von Angriffen aus dem Internet. „Alle 15 Sekunden entsteht ein neues Schadprogramm", sagte Ing. Roland Ledinger, Leiter des Bereichs Informations- und Kommunikationstechnologie-Strategie (IKT-Strategie) des Bundes, bei der Präsentation des Internet-Sicherheitsberichts 2013 am 14. November 2013 in Wien.

Der jährliche Schaden durch Internetkriminalität wird in Österreich auf mehr als sechs Millionen Euro geschätzt. Im ersten Halbjahr 2013 wurden in Österreich 6.400 Delikte im Bereich der IT-Kriminalität angezeigt.

**Schadprogramme.** Zu den Gefahren aus dem Internet zählen vor allem Schadsoftware, Hacking, Spionage und Betrug. Zur Schadsoftware (Malware) gehören Computerviren und -würmer, Trojaner, Spyware, Ransomware u. a. Laut dem „Security Intelligence Report" von *Microsoft* waren im ersten Halbjahr 2013 von Malware im Schnitt 17 Prozent aller Computer weltweit befallen. In Österreich waren zwischen Jänner und Juli 2013 zwei Prozent von 1.000 gescannten Computern infiziert. Das Hauptproblem sei laut *CERT*-Experten veraltete, unsichere Software. *Windows-XP*-Nutzer sind aufgrund der veralteten Sicherheitsstruktur des Betriebssystems einer sechsfach höheren Gefahr ausgesetzt, mit Schadsoftware infiziert zu werden, als Nutzer aktueller Betriebssysteme.

Malware verbreitet sich mittlerweile immer häufiger über Social Networks wie *Facebook* und *Twitter*. „Momentan ist Java das Hauptproblem auf Kunden-Seite – weil viele Business-Applikationen Java voraussetzen", sagte Robert Schischka, Leiter des *Computer Emergency Response Teams (CERT.at)* für den Unternehmens- und Privatbereich. Viele Unternehmen hinken beim Updateverhalten hinterher. Auch das Manipulieren von Sicherheitszertifikaten habe stark zugenommen, sagte Schischka. Schadsoftware werde mit gefälschten Zertifikaten versehen und werde schwer entdeckt.

Auch die Manipulation und Veränderung von Internetseiten (Website-Defacements) entwickelte sich in den letzten Jahren zu einem ernstzunehmenden Problem. Anfang 2013 wurde ein massiver Anstieg an Website-Defacements in Österreich beobachtet, mit teilweise mehr als 1.000 Vorfällen pro Monat. Der Grund dafür war ein Fehler in einer veralteten Version eines Plugins für Joomla (ein weit verbreitetes Content Management System). Neben regelmäßigen Updates empfiehlt *CERT.at,* nicht mehr benötigte Plug-ins und solche, für die es keine (Sicherheits-)Updates mehr gibt, zu deinstallieren, um Einfallsmöglichkeiten für Angreifer zu schließen.

**DoS- und DNS-Attacken** nehmen laut *CERT* zu. Sie zählen zum Standard-Repertoire der Angreifer. Bei diesen versendet ein infizierter Computer eine Flut von Anfragen an Server, um diese zu blockieren. Ein solcher DoS-Angriff sorgte zuletzt auch in Österreich für Aufsehen. Im März 2013 kam es zu einer Serie von DoS-Angriffen auf einen Anbieter von Anti-Spam-Blocklisten. Der Angriff wurden hatte eine Verlangsamung des Internets zur Folge.

**Mobile Geräte.** Die Experten kritisieren das mangelnde Sicherheitsbewusstsein vieler Smartphone-Nutzer. Die Hälfte der Smartphone- und Tablet-Benutzer verwendet keine Passwörter, Sicherheitssoftware oder Backup-Systeme und etwas mehr als die Hälfte der Nutzer weiß nicht, dass es auch für mobile Geräte Sicherheitssysteme und -produkte gibt.

Laut der Sicherheitsfirma „Security Research Labs" können veraltete SIM-Karten als Einfallstor für Hacker genutzt werden. Durch eine Sicherheitslücke ist es möglich, dass sich Angreifer unbemerkt Zugang zu fremden Handys verschaffen und Gespräche oder Nachrichten mithören bzw. mitlesen. Mobile Malware ist vor allem auf dem Betriebssystem Android vertreten. Vielen Apps würden ohne Bedenken

Fotos: Bundeskanzleramt, Egon Weissheimer

umfassende Rechte anvertraut. Robert Ledinger rät Smartphone-Usern: „Die Apps ausmisten und sich fragen: Brauche ich das?“

Der Umgang mit Internet und Smartphone soll laut dem IKT-Leiter des Bundes ab dem Kindergarten gelernt werden, um das Bewusstsein für einen sicheren Umgang mit dem Internet zu fördern.

**Betrug.** „Die größte Bedrohung für Privatpersonen im Internet stellt kommerzieller Betrug dar“, betonte Robert Schischka. Sehr verbreitet sind etwa Betrugsfälle durch Phishing sowie Ransomware. Hier werden PCs gesperrt oder die Festplatte durch Schadsoftware verschlüsselt und es wird „Lösegeld“ für die Freigabe verlangt.

Einer der verbreitesten Vertreter dieser Gattung ist der Polizei- oder Bundeskriminalamt-Trojaner. Kriminelle bedienen sich dabei psychologischer Tricks. Den Betroffenen wird häufig der Besitz von Kinderpornografie unterstellt oder durch Auslesen von Bildern über die eigene Webcam Angst gemacht. *CERT.at* rät, regelmäßige Backups der eigenen Daten zu erstellen, um diese im Notfall wieder rasch herstellen zu können.

**Phishing** – das Ausspähen von Zugangsdaten über gefälschte Webseiten und E-Mails – ist ebenfalls ein Dauerbrenner. „Auffallend dabei ist, dass Angreifer international gut vernetzt sind und verstärkt arbeitsteilig agieren. Schadprogramme oder komplette Infrastrukturen werden mittlerweile in Foren einer Untergrundwirtschaft zum Verkauf oder zur Miete angeboten“, berichtete Schischka.

**Der Schutz kritischer Infrastruktur** – dazu zählen etwa Energieversorgung, Finanzwesen, Krankenhäuser und das Internet an sich – muss gewährleistet sein, da ihr Ausfall durch Cyber-Angriffe zu Schäden und Beeinträchtigungen der Gesellschaft führen würde.

„Die Sicherung der digitalen Infrastruktur und der Schutz vor Cyber-Angriffen und Internet-Spionage gewinnen vor allem auch als Standort- und Wettbewerbsfaktoren zunehmend an Bedeutung“, erklärte Roland Ledinger. Bund und *CERT* wünschen sich eine Meldepflicht für angegriffene Unternehmen in kritischen Bereichen wie Energie oder Gesundheit.


**Kommerzieller Betrug: Größte Bedrohung für Privatpersonen im Internet.**

Foto: Egon Weissheimer

**Frühwarnsystem.** Zur Umsetzung der EU-Cybersicherheitsstrategie hat die EU-Kommission einen Vorschlag für eine begleitende Richtlinie zur Netz- und Informationssicherheit (NIS) veröffentlicht. Diese zielt auf den Aufbau von gemeinsamen Mindeststandards sowie eines europäischen Frühwarnsystems und Kooperationsnetzes ab. In den Mitgliedsländern soll es künftig eigene, für NIS zuständige Behörden geben. Außerdem hat jeder Staat eigene NIS-Strategien sowie nationale NIS- Kooperationspläne auszuarbeiten, die in einen übergreifenden Plan auf europäischer Ebene einfließen. Mit einer Verabschiedung der Richtlinie durch EU-Parlament und -Rat ist 2014 zu rechnen.

Die NIS-Richtlinie setzt mit den verankerten Regelungen auch Meilensteine für die Umsetzung der österreichischen Strategie für Cyber-Sicherheit. Österreich hat bereits bei der Erstellung der Strategie auf die sich abzeichnenden europäischen Entwicklungen im Bereich Cyber-Sicherheit Rücksicht genommen. Somit ist gewährleistet, dass Österreich bereits jetzt mit den wesentlichen Grundelementen der NIS-Richtlinie konform ist.

**Austrian Trust Circle.** Als weiteren Schwerpunkt zur Steigerung der Internet-Sicherheit hat *CERT.at* mit dem Bundeskanzleramt den „Austrian Trust Circle“ eingerichtet – für den Informationsaustausch in der strategischen Informationsinfrastruktur. Im „Austrian Trust Circle“ können sich Vertreter kritischer Infrastrukturen (z. B. Banken, Energie- oder Telekommunikationsbetreiber) zu aktuellen Sicherheitsthemen austauschen.

**CERT.at** verzeichnete 2012 rund 12.900 sicherheitsrelevante Meldungen, von denen ein Drittel als ernst zu nehmende Risiken eingestuft wurde. Dem gegenüber wurden laut Bericht bis September 2013 über 30.000 relevante Meldungen entgegengenommen, von denen mehr als 9.100 als ernsthafte Risiken gezählt wurden.

Dieser Anstieg sei neben zunehmender Netz-Kriminalität auf eine bessere Sensorik beim Entdecken von Angriffen zurückzuführen. Die Mitarbeiter von *CERT.at* beobachten die Entwicklung von Malware und anderen Bedrohungsformen im Internet und geben im Anlassfall Sicherheitswarnungen heraus. Zusätzlich unterstützt die „Internet-Feuerwehr“ IT-Verantwortliche in der Weitergabe von Know-how und leistet Präventions- und Aufklärungsarbeit in der Öffentlichkeit. *CERT.at* und *GovCERT.gv.at* führen Statistiken, mit denen sich ein aussagekräftiges und aktuelles Lagebild der Internet-Sicherheit in Österreich geben lässt.

*Siegbert Lattacher*