Schutz und Hilfe im Netz

Auf der IT-Sicherheitsmesse „it-sa 2011“ in Nürnberg präsentierten neben Unternehmen staatliche und private Organisationen ihre Beiträge zur Sicherheit im Internet.

Im Durchschnitt werden täglich 13 Schwachstellen in Standard-Programmen entdeckt. Etwa 21.000 Websites werden täglich mit Schadprogrammen infiziert“, sagte der deutsche Bundesminister des Innern Dr. Hans-Peter Friedrich am 13. Oktober 2011 in Nürnberg bei der IT-Sicherheitsmesse it-sa. Anlass war die Eröffnung des *it-sa-Campus,* einer Leistungsschau der sich mit der Sicherheit in der Informationstechnik befassenden Hochschulen und Universitäten.

Die durch Kriminalität im Internet hervorgerufenen Schäden nehmen von Jahr zu Jahr zu und es entwickle sich laut Friedrich eine *Underground Economy,* in der mit den Nummern von Kreditkarten, Zugriffscodes und Identitäten gehandelt werde.

Bereits Kleinkriminelle könnten sich über im Internet vorhandene Bauanleitungen Trojaner zusammenstellen. Spätestens seit dem Trojaner *Stuxnet* sei die Illusion verloren gegangen, dass es genüge, sich vom Netz abzukoppeln. „Sicherheitssysteme müssen ständig nachgerüstet werden, sie haben ein Verfallsdatum“, betonte der Minister. Man müsse schneller sein als die Kriminellen.

Friedrich verwies auf die Schaffung des nationalen Cyber-Abwehr-Zentrums, in dem das Know-how der Industrie gebündelt werde. Dass über 70 Prozent der Unternehmen dem Schutz der IT hohen Stellenwert einräumen und 30 Prozent diesen immerhin für wichtig erachten, zeige, dass das Problem in der Wirtschaft bekannt sei. Die Maßnahmen zur Durchsetzung seien jedoch unzureichend, wenn nur jedes dritte mittelständische Unternehmen über Abwehrsysteme verfüge. IT-Sicherheit müsse auch an den Hochschulen stärkere Verbreitung finden. Lediglich 18 Prozent der Studenten haben angegeben, auf diese Thematik angemessen vorbereitet zu werden.

it-sa 2011: Stand des Landeskriminalamts Bayern.

„Jeder fünfte PC in Deutschland ist – geschätzt – durch Schadprogramme infiziert“, sagte Prof. Dr. Sacher Paulus (Fachhochschule Brandenburg) unter Bezugnahme auf die Konferenz „Bulletproofhosting 2011“. Meist würden die Programme „schlafen“ und nur selektiv eingesetzt. Die größte Gefahr seien Drive-by-Infektionen, dass also unbewusst und unbemerkt Schadprogramme von manipulierten Websites heruntergeladen werden. Diese Infektionsart werde durch Programme gefördert, die aktive Inhalte von Websites unterstützen, und sei mittlerweile ein größeres Einfallstor für Schadprogramme geworden als bisher E-Mails und ihre Anhänge. Allein der bloße Aufruf einer solchen Website genüge, dass sich die Schadsoftware auf den Computer herunterlade. Zunehmend verbreite sich auch das Erschleichen von Zertifikaten, dass also unter Berufung auf eine vertrauenswürdige Stelle Authentizität vorgetäuscht werde, die in Wahrheit nicht besteht.

„Wir müssen gegen das Gefühl ankämpfen, dass es im Internet ohnehin keine absolute Sicherheit gebe, und dass aus dieser Einstellung heraus Sicherheitsmaßnahmen von vornherein unterbleiben“, forderte Prof. Dieter Kempf, Vorstandsvorsitzender von „Deutschland sicher im Netz e.V.“ *(DsiN.de)*. „Auch im Alltag sind wir ständig von Risiken umgeben, und haben gelernt, uns dagegen bestmöglich abzusichern, ohne deshalb auf absoluter – und in dieser Schärfe nicht realisierbarer – Sicherheit zu bestehen. IT-Sicherheit muss ein zentraler Faktor der Ausbildung sein.“

DsiN, ein 2005 zunächst aus einer Initiative heraus entstandener Zusammenschluss von Unternehmen und Verbänden und seit 2007 unter der Schirmherrschaft des deutschen BMI stehender Verein hat sich zum Ziel gesetzt, bei Verbrauchern und Unternehmen das Bewusstsein für einen sicheren Umgang mit dem Internet und der Informationstechnologie zu fördern *(www.sicher-im-netz.de)*.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) war wieder mit einem großen Ausstellungsstand vertreten. Im Rahmen der it-sa wurde die „Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen“ veröffentlicht, ein sorgfältig gestaltetes, über die Website des BSI *(www.bsi.bund.de)* abrufbares Werk. Die aus Interviews abgeleiteten Ergebnisse zeigen, dass bei den Verantwortlichen dieser Betriebe in Deutschland das Bewusstsein für die Bedeutung der IT-Sicherheit zwar hoch ist, es jedoch Nachholbedarf bei den Prozessen für ein IT-Sicherheitsmanagement sowie im personellen Bereich gibt. Nur jedes zweite Unternehmen hat beispielsweise einen IT-Sicherheitsverantwortlichen bestellt.

Im Zusammenhang mit dem am 3. Mai 2011 in Deutschland in Kraft getretenen „Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften“ hat das BSI bei der it-sa die neue Broschüre „De-Mail – Sicherer elektronischer Nachrichtenverkehr – einfach und nachweisbar“ präsentiert. Mit De-Mail können Nachrichten und Dokumente verschlüsselt im Internet versendet werden. Zudem ist sichergestellt, dass Absender und Empfänger jeweils diejenigen sind, als die sie sich ausgeben – ein wesentlicher Beitrag zur Rechtssicherheit im elektronischen Geschäftsverkehr.

Foto: Kurt Hickisch

IT-Sicherheitsmesse: Stand des Bundesamts für Sicherheit in der Informationstechnik.

Smartphones: Innerhalb weniger Minuten können Daten auf einen Laptop übertragen werden.

botfrei.de. Der 1995 gegründete Verband der deutschen Internetwirtschaft e.V. *(www.eco.de),* eine Vereinigung von etwa 550 Firmen mit dem Hauptsitz in Köln, hat es sich zum Ziel gesetzt, in Deutschland die Sicherheit im Netz zu heben. In Zusammenarbeit mit dem BSI/BMI wurde Mitte September 2010 das Anti-Botnet-Beratungszentrum unter *www.botfrei.de* ins Netz gestellt, das direkt beim einzelnen User ansetzt und verhindern soll, dass dessen PC durch Schadprogramme wie Trojaner zu einem „Zombie" wird – einem Teil eines fremdgesteuerten Botnetzes.

Weiters soll ihm Hilfestellung geleistet werden, Schadprogramme wieder von seinem Rechner zu entfernen. Dadurch soll der Internetkriminalität die Grundlage entzogen werden.

Zu diesem Zweck ist eco mit den *Internet-Service-Providern (ISP)* und Finanzdienstleistern übereingekommen, dass diese einen Nutzer benachrichtigen, wenn sie feststellen, dass sein PC Teil eines Botnetzes ist. Dabei wird auch mitgeteilt, was gegen den Befall mit dem Schadprogramm getan werden muss und wie eine Neuinfektion verhindert werden kann. In Zusammenarbeit mit führenden Anti-Viren-Software-Herstellern wurden drei DE-Cleaner und eine Rettungs-CD entwickelt, die von der Website heruntergeladen werden können. Die Rettungs-CD kann nach dem Download auf CD oder USB-Stick gespeichert werden. Das Reinigungs-Programm hat sein eigenes Betriebssystem und startet sich von selbst – das auf dem Rechner befindliche Betriebssystem könnte ja kompromittiert sein.

Im ersten Jahr nach Beginn der Aktion wurden mehr als 1,2 Millionen Besucher auf der Website und mehr als 700.00 Downloads der DE-Cleaner gezählt. Über ein Call-Center und ein Forum wird zusätzlich Hilfestellung zur Nutzung der Programme geboten. Die Reaktionen waren positiv. Die Angebote wurden dankbar aufgenommen.

Einer Statistik von *Symantec* nach war Deutschland 2010 noch auf Platz zwei der Länder mit den meisten Zombie-Rechnern. Im zweiten Quartal 2011 liegt Deutschland in diesem Ranking nur mehr an achter Stelle. Wenngleich ein Teil dieses Rückgangs auch auf das Aufdecken und Abschalten einiger großer Botnetze zurückzuführen ist, kommt ein sicher nicht unwesentlicher Beitrag der eco-Initiative zu. Untermauert wird dies dadurch, dass in Deutschland die Zahl der infizierten Rechner seit dem dritten Quartal 2010 stetig gesunken ist, wogegen weltweit beträchtliche Anstiege zu verzeichnen sind.

Auch nach dem Auslaufen der durch das BSI gewährten und von vornherein nur als Starthilfe gedachten Finanzierung mit Ende 2011 wird das Projekt von Eco weitergeführt.

Smartphones und Sicherheit. „Nur ja keine Smartphones unbeaufsichtigt irgendwo liegen lassen", warnte Ronny Sackmann am Stand der *cirosec GmbH (www.cirosec.de)* und lieferte auch gleich den Beweis dafür. Mit Hilfe einer Steckverbindung wird das Handy an einen Laptop angeschlossen und innerhalb von etwa fünf Minuten ist der gesamte Dateninhalt ausgelesen. Kontakte, abgespeicherte SMS, Verbindungsdaten, der Terminkalender, Bewegungsprofile, E-Mails, unter Umständen sogar die Passwörter, die eine weitere Benutzung des Handys durch andere ermöglichen würden. Das, obwohl das Handy nur durch Eingabe eines Codes hätte verwendet werden können.

Smartphones sind, trotz ihrer Kleinheit, mit ihrem Speicherplatz bis zu 64 GB vollwertige PCs. Während man sich in der Welt der Bürocomputer schon an zu treffende Sicherheitsmaßnahmen gewöhnt hat, steckt das Sicherheitsdenken bei Smartphones noch in den Kinderschuhen.

„Genau so, wie man beispielsweise bei Programmen, die man aus dem Internet herunterlädt, vorsichtig sein sollte, sollte man auch bei den Apps für Handys Vorsicht walten lassen. Sie könnten Schadprogramme enthalten", warnt Sackmann. Durch das Herstellen einer Verbindung mit dem Internet kann man sich genauso Malware auf das Handy laden wie beim PC.

Ein anderes Problem, auf das am Stand der Firma *Ikarus (www.ikarus.at)* hingewiesen wurde, liegt im Gebrauch des Barcode-Scanners von Smartphones. Auch in den quadratförmigen Codes mit abwechselnd hellen und dunklen Quadraten (QR-Codes) kann sich ein Schadcode verbergen, nämlich ein solcher, der auf eine Website verweist, die ihrerseits, wenn man auf sie zugreift (Drive-by) Malware auf das Handy überträgt. Das bloße Übersetzen des Codes in lesbare Form aktiviert nur dann keinen Zugriff, wenn der automatische Aufruf deaktiviert ist. Ist er das nicht oder ist ein Deaktivieren von vornherein nicht möglich, ruft das Handy die Website auf und die Schadsoftware, die die verschiedensten Manipulationen am Handy auslösen kann, wird heruntergeladen. Einen QR-Code herzustellen, der solche Funktionen auslöst, ist keine Schwierigkeit, betonte Josef Pichlmayr, Geschäfts-

Fotos: Kurt Hickisch

Barcode-Scanner von Smartphones: In den QR-Codes kann sich ein Schadcode verbergen.

führer von *Ikarus,* und warnt davor, ohne entsprechende Vorsicht – zu der eben das Deaktivieren des automatischen Aufrufs gehört – wahllos derartige Codes entschlüsseln zu wollen.

Einbruchsprävention. Erster Polizeihauptkommissar Peter Fasold vom Bayerischen Landeskriminalamt, Prävention, *(www.polizei-bayern.de),* referierte bei der it-sa über die durch Sicherungstechnik verhinderten Einbrüche in Bayern im Jahr 2010. Von den insgesamt 1.451 Fällen, in denen Einbrecher an vorhandener Sicherungstechnik gescheitert sind, war dies zu 84 Prozent (1.216 Fälle) auf mechanische Sicherungen zurückzuführen, zu 16 Prozent (235 Fälle) auf Einbruchmeldeanlagen. Zu Recht stehe die mechanische Sicherungstechnik bei der Einbruchs-Prävention an erster Stelle, betonte Fasold, doch sei auch die Einbruchmeldetechnik ein wichtiger Baustein – als Ergänzung zur mechanischen Sicherung. Von den 235 Einbruchmeldeanlagen befanden sich 203 im Gewerbebereich. 32 der insgesamt 34 auf Alarmierung erfolgten Festnahmen entfielen auf diesen Bereich. Durch aufmerksame Zeugen wurden 245 Einbrüche verhindert, und es konnten 109 Täter festgenommen werden.

Kurt Hickisch

IT-SA

IT-Sicherheitsmesse

Die vom 11. bis 13. Oktober 2011 im Messezentrum Nürnberg abgehaltene IT-Sicherheitsmesse *it-sa* hat sich zu der größten Messe für IT-Sicherheit im deutschsprachigen Raum und auch weltweit zu einer der größten Messen dieser Art entwickelt. Vertreten waren 322 Aussteller aus 15 Ländern; es wurden über 5.800 Fachbesucher gezählt. Auf der Sonderfläche „Das perfekte Rechenzentrum“ waren Aussteller zusammengefasst, die auf Planung, Bau und Technik von Rechenzentren spezialisiert sind, und am *campus@it-sa* Hochschulen mit Bezug zur IT-Sicherheit. In den Foren Blau mit Schwerpunkt Technik und Rot mit eher das Management betreffenden Themen wurden im Viertelstunden-Takt Vorträge geboten, zusammen mit den Sonderveranstaltungen im Auditorium insgesamt über 250. Die Inhalte der Vorträge samt Videostreams können über *www-it-sa.de* abgerufen werden. Die nächste *it-sa* wird vom 16. bis 18. Oktober 2012 im Messezentrum Nürnberg stattfinden.

http://www-it-sa.de

Foto: Kurt Hickisch