Mehr Sicherheit im Netz

Was können die User und die Wirtschaft zur Sicherheit im Internet beitragen? Antworten auf diese und andere Fragen der IT-Sicherheit gab es beim 10. Österreichischen IT-Sicherheitstag in Klagenfurt.

Wenn man genauer hinsieht, sind die Grundlagen für Systemeinbrüche und Datendiebstähle dieselben wie vor einigen Jahren“, sagte Robert Jankovics von *Kapsch BusinessCom*. „Ausprägung, Professionalität und Komplexität der Angriffe haben jedoch zugenommen und stellen neue Herausforderungen dar.“ Als Beispiel nannte Jankovics die *Watering Hole Attacks*. Der schlaue Löwe hetzt seinem Opfer nicht in der Savanne nach, sondern lauert ihm beim Wasserloch auf – daher der Name für diese Art eines Angriffs auf IT-Systeme. Der Angreifer ahnt, dass die Zielperson bestimmte Webseiten regelmäßig aufsucht. Er sucht auf diesen Seiten Schwachstellen und infiziert sie mit einem Schadcode. Übersieht die Zielperson, dass sie auf eine Webseite des Angreifers weitergeleitet wird, springt der Schadcode auf ihr IT-System über und ermöglicht dem Angreifer, es zu manipulieren und zu missbrauchen.

Ähnlich funktioniert *Social Phishing,* über das Edgar Weippl und Markus Huber von *SBA Research (www.sbs-research.org)* berichteten. Über soziale Netzwerke werden persönliche Informationen gewonnen, indem sich der Angreifer etwa mit einem erfundenen Profil als „Freund“ aufbaut.

Siegfried Schauer von *Ikarus Security Software GmbH (www.ikarussecurity.com)* warnte davor, die IKT-Sicherheit bei Handys weniger ernst zu nehmen als etwa bei PCs. Auch bei Smartphones müsse ein Virenschutzprogramm installiert werden. „Vielfach wird übersehen, dass Smartphones Computer sind, und überaus leistungsfähige noch dazu“, warnte Schauer. Beispielsweise täuscht ein speziell für Handys entwickeltes Schadprogramm das Installieren einer App vor, versendet aber im Hintergrund Mehrwert-SMS, wie man nachträglich beim Erhalt der Telefonrechnung ersehen kann. Eine sich als Antiviren-Programm tarnende Malware aus dem App-Store verlangt zur Bezahlung der Reparaturkosten, um die festgestellten Mängel zu beheben, die Eingabe der Kreditkartennummer samt Sicherheitscode – diese Daten gehen an den Angreifer. *FakeToken* tarnt sich als ein von der Bank zur Verfügung gestellter Generator für mTANs und ermöglicht dem Angreifer den Remote-Zugriff auf das Smartphone. Es gibt Programm-Bibliotheken, aus denen heraus sich Schadprogramme in Apps einbauen lassen.

Zeitgleich mit dem IT-Sicherheitstag fand in Klagenfurt die IKT-Kongress-Messe für Südösterreich und den Alpen-Adria-Raum statt (IT Carinthia) – mit rund 60 Ausstellern.

Die Schwierigkeit liege darin, dass sich Angreifer und Verteidiger in einem asymmetrischen Kräfteverhältnis gegenüberstehen, sagte Markus Robin von der *SEC Consult Unternehmensberatung GmbH (www.sec-consult.com)*. Dem Angreifer genügt eine einzige Schwachstelle, wogegen der Verteidiger alle Schwachstellen bereinigen muss. Bei Programmen stehe Funktionalität an erster Stelle, dann die Performance und erst zum Schluss die Sicherheit. In diese werde, unter dem Druck des Marktes, am wenigsten investiert. „Sicherheitsfeatures und sichere Features sind nicht das Gleiche.“ Wie bei einem Auto müsste Software einem Security-Crashtest unterzogen werden. Welchen sicherheitstechnischen Anforderungen Webapplikationen zu entsprechen haben, ist in der ÖNORM A7700 geregelt *(www.a7700.org)*.

„Man kann sich natürlich völlig vom Internet abschotten, keine Daten tauschen, soziale Medien nicht benützen, keine Daten am Handy haben und mit diesem nicht fotografieren“, sagte Harald Kriener von *cloudBrokers GmbH (www.cloudbrokers.at)*. „Aber ist das noch zeitgemäß?“ Man vergebe dadurch viele Chancen und Möglichkeiten. Zu resignieren sei aber auch nicht problemlos. Das Datenschutzgesetz verpflichtet zum Schutz personenbezogener Daten. Eine Vernachlässigung der Sorgfaltspflicht kann zivilrechtliche Folgen haben. Und nicht jeder wird sich einen solchen resignierenden Ansatz leisten können; sicher nicht ein Unternehmensverantwortlicher.

Richtig ist der Mittelweg, nämlich schützenwerte Daten zu schützen. Grundsätzlich sollte mit privaten Informationen (Fotos, Videos, Texte) und Daten (Bankverbindung, Geburtsdatum, SV-Nummer, Adresse) achtsam umgegangen werden. Gelegentlich sollte man nach sich selbst oder nach Familienmitgliedern in Suchmaschinen suchen. Vorsicht ist geboten bei der Nutzung öffentlicher Computer: Die Nutzung sollte immer mit der „Logout“-Funktion beendet und es sollte nicht die Funktion „Passwort merken“ aktiviert werden. Überhaupt sollten sichere Passwörter verwendet und Tools aktuell gehalten werden. In E-Mails sollten wichtige Daten nicht als Attachment mitgesendet, sondern in sicheren Cloudstorages abgelegt werden. Als österreichisches Cloudsystem, das die Bedürfnisse von KMUs abdeckt, besteht der *Speicherblock Österreich*, dessen Rechenzentren sich in Österreich befinden *(www.speicherblock.at)*.

Smart Home. Die Heimautomatisierung schreitet voran. Die Webcam liefert ständig Bilder, wie es vor dem Haus aussieht, die

Foto: Kurt Hickisch

Alarmanlage meldet verdächtige Ereignisse. *Smart Metering* macht die Messung und Analyse des Verbrauchs beispielsweise von elektrischem Strom aus der Ferne möglich – und übermittelt dabei laufend Daten.

Der Bewohner will möglichst einfache und intuitiv zu bedienende, beliebig erweiterbare, hochverfügbare und weltweit bedienbare Systeme. Auf der Strecke bleibt, dass über Sensoren immer mehr Daten aus seinem persönlichen Umfeld übermittelt und dabei auch mitgeschnitten werden können. Eine Auswertung dieser Daten lässt Rückschlüsse auf persönliche Gewohnheiten zu (An- und Abwesenheit, Tagesrhythmus – Profilbildung) und ermöglicht Voraussagen auf künftiges Verhalten. Weiters besteht die Gefahr, dass Daten manipuliert werden, beispielsweise Alarmanlage und Außenbeleuchtung abgeschaltet werden oder die Überwachungskamera nicht Bilder von aktuellen Vorgängen liefert, sondern dass man unverfängliche Bildsequenzen eingespielt bekommt. *Smart-Metering*-Systeme könnten manipuliert werden – über falsche Rechnungen bis zum völligen Abschalten der (Strom-)Versorgung. Die Hersteller sind gefordert, die Heimautomatisierungslösungen schon von der Konzeption her möglichst sicher zu gestalten, etwa durch den Einsatz hochwertiger Verschlüsselungstechnologien.

Rechtsfragen. Dr. Wolfgang Feiel *(RTR-GmbH)* verwies auf Maßnahmen der EU wie die Modernisierung der *Europäischen Agentur für Netz- und Informationssicherheit (ENISA)* sowie die Einrichtung eines Computer-Notfallteams *(CERT)* für die EU-Organe und die am 25. August 2013 in Kraft getretene Datenschutzrichtlinie für elektronische Kommunikation, Verordnung (EU) 611/2013 der Kommission, die eine Ausweitung der Maßnahmen zur Information über Sicherheitsverstöße gegen den Schutz personenbezogener Daten mit sich gebracht hat. Vorschläge liegen vor für Regelungen zur Bekämpfung von Cyberangriffen sowie zur Gerichtsbarkeit im virtuellen Raum auf europäischer und internationaler Ebene.

In das TKG 2003 wurde § 16a eingefügt. Mit dieser Bestimmung werden Betreiber öffentlicher Kommunikationsdienste insofern in die Pflicht genommen, als sie Maßnahmen zur Gewährleistung der Integrität ihrer Netze zu ergreifen und die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen haben.

Univ.-Prof. Dr. Peter Mader (Universität Salzburg) berichtete über den Inhalt der Richtlinie 2011/83/EU vom 25. Oktober 2011 über die Rechte der Verbraucher, die nach ihrem Art. 28 bis 13. Dezember 2013 in nationales Recht umzusetzen war und ab dem 13. Juni 2014 anzuwenden ist.

Betroffen sind vorwiegend die Bestimmungen über die außerhalb von Geschäftsräumen abgeschlossenen Verträge („Haustürgeschäfte“) und Fernabsatzverträge (Vertragsabschluss ohne gleichzeitige Anwesenheit der Vertragsparteien, wie Webshopping und Katalog-Bestellungen). Ferner werden für Verträge zwischen Unternehmern und Verbrauchern (B2C) Informationspflichten eingeführt. Die Richtlinie geht von einer „Vollharmonisierung“ aus; dem nationalen Gesetzgeber verbleibt nur ein sehr eingeschränkter Regelungsspielraum. Er kann also nicht wie bisher ein höheres Verbraucherschutzniveau vorsehen.

10. Österreichischer IT-Sicherheitstag in Klagenfurt: Referenten Siegfried Schauer, Sonja Janisch, Peter Mader, Harald Kriener, Edgar Weippl, Robert Jankovics, Peter Schartner und Wolfgang Feiel.

Bei Fernabsatz- und Haustürgeschäften hat der Verbraucher künftig ein Widerrufsrecht (bisher „Rücktrittsrecht"). Die Ausübung dieses Rechtes ist an keine besonderen Gründe gebunden und auch nicht an eine besondere Form. Die Frist zum Widerruf beträgt 14 Tage (bisher sieben) und berechnet sich bei Kaufverträgen ab dem Eingang der Ware. Wurde der Verbraucher über das Widerrufsrecht nicht ausreichend belehrt, erstreckt sich die Frist auf maximal 12 Monate und 14 Tage. Bei Widerruf hat der Verbraucher bei einem Kaufvertrag die erhaltenen Waren unverzüglich zurückzusenden. Die Kosten dafür können ihm vertraglich (etwa in AGB) auferlegt werden. Der Unternehmer hat ebenso unverzüglich alle erhaltenen Zahlungen zurückzuerstatten. Die Informationspflichten sind selbst bei anderen als Fernabsatzgeschäften sehr umfangreich. Lediglich Geschäfte des täglichen Lebens, die sofort erfüllt werden, können ausgenommen werden.

Über rechtliche Stolperfallen für Webseiten-Betreiber referierte Ass.-Prof. Dr. Sonja Janisch von der Universität Salzburg. Besonders als Unternehmer kann man in „Abmahnkriege" geraten, die teuer werden können. Der Streitwert, von dem sich Anwalts- und Gerichtskosten berechnen, wird bei Urheberrechtsverletzungen vielfach mit 50.000 Euro angesetzt. „Klassiker" für Abmahnungen sind ein fehlerhaftes Impressum sowie die Verletzung fremder Urheberrechte („Fremdcontent"). Für sämtliche Websites gilt § 25 MedienG, wobei die Informationspflichten bei „kleinen Websites", die nur der Präsentation dienen, weniger umfangreich sind (Abs. 5). Unternehmer haben bei der Gestaltung ihres Webauftritts auch § 5 ECG zu beachten, und, bei Verarbeitung personenbezogener Daten, § 96 Abs. 3 TKG; Webshops zudem § 9 ECG und, wenn an Verbraucher verkauft wird, die §§ 5c und 5d KSchG. Websites von in das Firmenbuch eingetragenen Unternehmern müssen § 14 UGB entsprechen, solche von Gewerbetreibenden, die nicht im Firmenbuch eingetragen sind, § 63 GewO.

Ab 13. Juni 2014 werden die Informationspflichten nach der Richtlinie 2011/83/EU dazukommen, nämlich im Fernabsatzgeschäft noch vor Vertragsabschluss nach Art. 6 Abs. 1 lit a bis t und nach Vertragsabschluss nach Art. 8 Abs. 7. Wird der Bestellvorgang durch Aktivierung einer Schaltfläche (Button) bewirkt, muss diese Funktion mit „zahlungspflichtig bestellen" oder Ähnlichem gut lesbar gekennzeichnet sein (Art. 8 Abs. 2 RL).

Je nach verletzter Norm können Sanktionen in Verwaltungsstrafen (MedienG), Abmahnung bzw. wettbewerbsrechtlicher Unterlassungsklage, Schadenersatz, Verlängerung des Rücktrittsrechts für Verbraucher bei Fernabsatzverträgen oder in einer Zwangsstrafe vom Firmenbuchgericht bestehen. „Riskieren Sie keine kostenintensive Abmahnung durch Nichteinhaltung der Informationspflichten, zumal diese leicht zu erfüllen sind", riet Janisch.

Datenrettung. „In jeder Kaffeemaschine steckt heute fast schon mehr Rechenleistung als in einem Computer vor 20 Jahren", sagte DI Nicolas Ehrschwendner von der *Attingo Datenrettung GmbH (www.attingo.at)*. „Der Kunde kauft Geräte, ohne zu wissen, was dahinter steckt." Das liege an den eingebauten elektronischen Steuerungs- und Regelsystemen *(Embedded Systems)*, die mit entsprechend höherer Leistung als in der Haushaltselektronik vor allem in der industriellen Fertigung eingesetzt sind. Diese Systeme arbeiten im Hintergrund, sind aber auch Computer mit Massenspeichern von Disketten über CDs bis hin zu Festplatten. Vielfach sind es Systeme, die auf einen Maschinentyp hin programmiert sind, unter Umständen von einer Firma, die es nicht mehr gibt, wenn die ersten Defekte eintreten.

Daten können selbst unter widrigsten Voraussetzungen rekonstruiert werden. Beim *Attingo*-Stand auf der IT-Carinthia war ein Laptop ausgestellt, der von seinem Besitzer neben einem elektrischen Heizlüfter auf einem Schreibtisch aufgestellt war und verschmort bzw. teilweise verbrannt ist. Maus, Kugelschreiber waren in das Gehäuse eingeschmolzen. Dennoch konnte der Inhalt der Festplatte zum Großteil ausgelesen werden.

Kurt Hickisch

IT-SICHERHEITSTAG

Der Österreichische IT-Sicherheitstag wird seit 2004 jährlich von der *Forschungsgruppe Systemsicherheit (syssec – www.syssec.at)* der Universität Klagenfurt unter Leitung von Dr. Peter Schartner veranstaltet – heuer zum zweiten Mal in Kooperation mit den Kärntner Messen am 3. Oktober 2013 in der Messehalle Klagenfurt. Zeitgleich fand die *IT Carinthia,* die IKT-Kongress-Messe für Südösterreich und den Alpen-Adria-Raum statt – mit rund 60 Ausstellern. Der 11. Österreichische IT-Sicherheitstag wird am 22. Oktober 2014 an der FH Salzburg stattfinden. Die Forschungsgruppe Systemsicherheit veranstaltet zudem alljährlich die *D-A-CH Security,* bei der auf wissenschaftlicher Ebene interdisziplinär der aktuelle Stand der IT-Sicherheit in Deutschland, Österreich und der Schweiz erörtert wird. Die *D-A-CH Security 2014* wird am 16. und 17. September 2014 an der TU Graz stattfinden.

www.syssec.at/SiTag2014
www.syssec.at/dachsecurity2014).

FOTOS: KURT HICKISCH