Gesamtgesellschaftliche Aufgabe

Weite Lebensbereiche sind von der Nutzung des Internets abhängig. Zur Sicherheit im Web beizutragen, ist eine Aufgabe für jeden.

Sicherheit im Internet hänge von jedem Einzelnen ab. Die zweite Ebene seien die Fachleute, die sich einzubringen hätten. Letztlich müssten auf struktureller Ebene alle Fähigkeiten und Kräfte zur Abwehr von Gefahren für die IKT-Sicherheit gebündelt werden, sagte der Leiter des Abwehramts des BMLVS, Generalmajor Mag. Anton Oschep, bei der Eröffnung des 10. IKT-Sicherheitsseminars am 9. November 2011 im *Austria Center Vienna*. Es gebe positive Ansätze in dieser Richtung, wobei Oschep besonders die Zusammenarbeit mit dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) hervorhob. Der Leiter des BVT, Mag. Peter Gridling, war Teilnehmer an der Podiumsdiskussion.

Angriffe im virutellen Raum. Oberst dG Mag. Walter Unger, Leiter der Abteilung IKT-Sicherheit des Abwehramts, wies darauf hin, dass durch die Vernetzung von Computern ein virtueller Raum entstanden sei, der Angriffsmöglichkeiten biete. Bedroht seien Vertraulichkeit, Integrität und Verfügbarkeit der IKT-Systeme, die für das Funktionieren der modernen Gesellschaft unerlässlich seien. Dies betreffe Grundlegendes, wie die Versorgung mit Wasser, Energie, Lebensmitteln, das Finanz- und Gesundheitswesen, Transportsysteme, Rettungs- und Hilfsdienste. Der Einzelne könnte betroffen sein von Eingriffen in seine persönlichen Daten bis hin zum Diebstahl seiner Identität und Schädigung seines Rufes, in seine Kommunikation und seinen Zugang zu Informationen. Unternehmen seien bedroht durch den Abfluss von Geschäfts- und Betriebsgeheimnissen sowie geistigen Eigentums.

IKT-Sicherheitsseminar: Stand der FH Hagenberg.

Das Bundesheer schütze seiner Aufgabenstellung gemäß die militärische Infrastruktur, den nationalen Cyberspace als Teil der umfassenden Landesverteidigung, und leiste Assistenzdienste, gemäß seinem Auftrag „schützen und helfen".

Rechtlicher Schutz. Dr. Wolfgang Feiel, Leiter der Rechtsabteilung der RTR-GmbH, betonte, dass die Sicherheit der Informations- und Kommunikationstechnik (IKT) von essenzieller Bedeutung für Gesellschaft und Wirtschaft sei. Der Schutz von IKT sei eine Aufgabe der gesamten Gesellschaft und beginne mit der Bewusstseinsbildung. IKT-Sicherheit sei auch Teil der *Digitalen Agenda* der Europäischen Kommission 2010, deren Ziel es ist, aus einem digitalen Binnenmarkt mit schnellen Internet-Verbindungen nachhaltigen wirtschaftlichen und sozialen Nutzen zu ziehen. Gegenüber dem Aufkommen neuer Verbrechensformen wie der Cyberkriminalität müssten auf EU-Ebene reaktionsfähige Mechanismen entwickelt werden. Das Internet sei zwar nie ein rechtsfreier Raum gewesen, doch hätten sich bei der Rechtsdurchsetzung Grenzen gezeigt.

Elektronische Kommunikation sei ein Massenphänomen, die Anwendungsformen (soziale Netzwerke, Medizintechnik, Unterhaltungsindustrie, Steuerungstechnik) seien unbegrenzt und grenzenlos. Das IKT-Recht sei sehr stark durch Rechtsakte der EU bestimmt – etwa 150. Entscheidend für die Sicherheit sei die Änderung des Telekommunikationsgesetzes durch BGBl I 2011/102. Durch dieses Gesetz, das großteils am 22. November 2011 in Kraft getreten ist, würden die Netzbetreiber in die Pflicht genommen. Nach § 16a TKG nF haben die Betreiber öffentlicher Kommunikationsdienste Maßnahmen zur Gewährleistung der Integrität ihrer Netze zu ergreifen und die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicher zu stellen. Die weiteren, sich aus dieser Bestimmung ergebenden Verpflichtungen sind rechtlich durchsetzbar, Verstöße mit Verwaltungsstrafe bis zu 37.000 Euro bedroht (§ 109 Abs. 3 Z 1, Z 1a, 1b und 1c TKG nF).

Jeder der etwa 600 Netzbetreiber in Österreich wird durch angemessene technische und organisatorische Maßnahmen ein Sicherheitsniveau zu gewährleisten haben, das zur Beherrschung der Risiken für die Netzwerksicherheit geeignet ist (§ 16a Abs. 2 TKG nF). Die zur Beurteilung der Sicherheit oder Integrität der Dienste und Netze erforderlichen Informationen, einschließlich Unterlagen über ihre Sicherheitsmaßnahmen, sind der Regulierungsbehörde nach Aufforderung zu übermitteln (§ 16a Abs. 3 TKG nF).

Die Regulierungsbehörde (RTR-GmbH) hat ein Infrastrukturverzeichnis zu führen (§ 13a TKG nF), in das detailliert alle der nach Art, Verfügbarkeit und geografischen Lage sowohl vorhandenen als auch neu errichteten, für Kommunikationslinien nutzbaren Anlagen, Leitungen, Verrohrungen, Kabelschächte usw. einzutragen sind. Sinn ist es, in bereits vorhandene Strukturen Leitungen nachträglich einziehen zu können, ohne dass erneut gegraben oder gestemmt werden müsste.

Nicht ohne Grund (mögliche Ausspähung von Anlagen der Infrastruktur) sieht das Gesetz vor, dass die Daten des Infrastrukturverzeichnisses nach dem jeweiligen Stand der Technik vor dem Zugriff Unberechtigter

FOTO: KURT HICKISCH

Sicherheitslücken im Alltag: Kopien werden auf der Festplatte des Kopierers gespeichert. Die Herstellerfirma ist über das Internet mit dem Kopierer verbunden, um Fernwartung zu ermöglichen.

zu schützen sind (§ 13a Abs. 4 TKG nF) und als restriktive Umsetzung der EU-Richtlinie 2009/140/EG dass Informationen aus dem Infrastrukturverzeichnis (nur) Bereitstellern eines Kommunikationsnetzes (nur) soweit zu übermitteln sind, als der Antragsteller der Regulierungsbehörde glaubhaft macht, diese Informationen für ein konkretes Vorhaben zu benötigen (§ 13a Abs. 5 TKG nF). Insgesamt sieht Feiel einen Wandel im Kommunikationsrecht, indem nicht mehr nur repressive Vorschriften aufgestellt, sondern auch die Betreiber verpflichtet werden, an der Umsetzung von Sicherheitsmaßnahmen mitzuwirken, was die gesellschaftliche Verantwortung für IKT-Sicherheit unterstreiche.

Praxis. Über Sicherheitslücken im Alltag berichtete Paul Karrer, Obmann und Sprecher von *Cyber Security Austria (www.cybersecurityaustria.at)*. Der Verein hat sich die Förderung der Sicherheit der strategischen Infrastruktur Österreichs zum Ziel gesetzt. IKT-Einflussgrößen auf die Verwundbarkeit Österreichs und des gesellschaftlichen Lebens sollen identifiziert und bei Entscheidungsträgern ein adäquates Krisenmanagement etabliert werden.

Der Servicetechniker für die Alarmanlage hat die Daten der Anlagen aller Kunden auf seinem Laptop, einschließlich der Alarmcodes. Der Kopierer ist über das Internet mit der Herstellerfirma verbunden, um Fernwartung zu ermöglichen. Die Kopien sind auf der Festplatte des Kopierers abgespeichert. Wie oft werden beruflich genutzte Laptops von den Kindern zu Hause zum Spielen benützt – „bring your own device“ kann das Einfallstor für Schadprogramme sein. Der erstmals am 13. Juli 2010 entdeckte Virus *Stuxnet* hat gezeigt, dass auch Steuerungsanlagen von Maschinen durch Schadprogramme beeinflusst werden können. Bei einer Manipulation von Geräten der Medizintechnik (Insulinpumpen, Herzschrittmacher) könnten schwerwiegende Folgen eintreten. Bereits Hardware kann Schadcode enthalten.

Es muss nicht alles vernetzt werden. Niemand muss auf einem Steuerungsrechner auch seine E-Mails lesen oder im Web surfen. Die Kosten eines zweiten PCs stehen in keinem Verhältnis zu dem sonst drohenden Risiko.

Handys. „Jeder, der Signale aussendet, kann auch geortet werden. Umgekehrt kann man sich auch selber orten über Signale, die von bekannten Positionen kommen“, erläuterte Marco di Filippo, *Compass Security AG (www.csnc.ch)*. Über den Feldtest-Modus gelangt man zu den Daten der im Moment aktiven Funkzelle, und kann in weiterer Folge den Mobile Country Code (MCC) und den Mobile Network Code (MNC) auslesen. Mit diesem ist man auf der Ebene des Providers. Der Location Area Code (LAC) fasst mehrere Zellen organisatorisch zusammen. Die Cell ID identifiziert eine Zelle innerhalb einer LAC. Für die weitere Auswertung in geografischer Hinsicht muss dann zwar schon auf Datenbanken zurückgegriffen werden, die aber, samt entsprechenden Tools, im Internet bestehen und abgefragt werden können.

Für Social-Engineering-Angriffe über Handys eignen sich Anrufe oder SMS über eine gefälschte Rufnummer

FOTO: ALEXANDER TUMA

Anton Oschep: „Alle Fähigkeiten und Kräfte zur Abwehr von Gefahren für die IKT-Sicherheit müssen gebündelt werden.“

Marco di Filippo: „Jeder, der zum Beispiel über Handys oder Computer Signale aussendet, kann auch geortet werden.“

Wolfgang Feiel: „Der Schutz von IKT ist eine Aufgabe der gesamten Gesellschaft und beginnt mit der Bewusstseinsbildung.“

Walter Unger: „Durch Vernetzung von Computern sind Vertraulichkeit, Integrität und Verfügbarkeit der IKT-Systeme bedroht.“

(Call-ID-Spoofing, SMS-Spoofing). In beiden Fällen wird dem Angerufenen ein bekannter Absender vorgetäuscht, was eine Kontaktaufnahme erleichtert. Damit rückt auch Phishing über SMS in den Bereich des Möglichen. Nach einer Studie des *Bundesamtes für Sicherheit in der Informationstechnik (BSI)* haben 47 Prozent aller Handynutzer noch nie ein Sicherheits-Update aufgespielt.

Soziale Netzwerk-Dienste wie *Facebook, Myspace, XING, LinkedIn, studiVZ* ua. dienen dem Austausch von Informationen, von Fotos, Videos, und enthalten große Mengen persönlicher Daten. Wie Mag. Markus Klemen, SBA-Research *(www.sba-research.org)*, ausführte, loggen sich 400 Millionen User täglich ein, 800 Millionen zumindest einmal in 30 Tagen.

7,5 Milliarden Fotos werden pro Monat gespeichert (rund 18.000 Fotos pro Sekunde), 700 Milliarden Minuten Zeit wird pro Monat in der *Facebook*-Welt verbracht. Das entspricht 1,3 Millionen Lebensjahre pro Monat. 550.000 Programme haben Schnittstellen mit *Facebook*.

Da die meisten sozialen Netzwerke kostenlos sind, muss das Geld entweder mit Informationen über User verdient werden oder durch den Verkauf von Werbung. „Like-Buttons“ zielen auf ein virales Marketing ab. Wenn ein Produkt vielen anderen gefällt, muss es wohl gut sein. Hintergrund der meisten Apps ist hingegen die Informationsgewinnung.

Daten aus sozialen Netzwerken können untereinander verknüpft werden, sodass sich letztlich durch Zusammenfügung von Einzelinformationen ein Persönlichkeitsprofil ergibt. „Crawler“ (z. B. *80legs.com*) nutzen solcherart erarbeitete Profile kommerziell. Nicht einmal der Auftritt unter verschiedenen Nicknames hilft, da durch Gesichtserkennung Zusammenhänge sichtbar werden. Gleiches ergibt sich durch den Einsatz von – immer besser werdenden – Textanalyseverfahren.

Aus dem auf Fotos sichtbaren Umfeld lässt sich durch Vergleichsverfahren mit den übrigen Millionen Bildern erkennen, wo sie gemacht wurden, auch wenn den Fotos keine Geo-Daten beigefügt sind. Dies kann zur Standortermittlung herangezogen werden. Die digitalen Bildern beigefügten Metadaten geben neben den technischen Daten der Aufnahme wie Blende Verschlusszeit, Objektiv Aufschluss über die verwendete Kamera, wenn nicht sogar über deren Seriennummer.

Phishing. Über soziale Netzwerke können mit steigender Erfolgsrate Phishing-Angriffe durchgeführt werden, indem sich der Täter Vertrauen erschleicht. Auch falsche Freunde können sich einschleichen. Wer denkt schon daran, wenn sich jemand als Freund anbietet, diesem nur eingeschränkte Rechte einzuräumen. Der vorgebliche Freund ist bei bloßem, gedankenlosen Akzeptieren voll in die Kommunikation mit den anderen eingebunden – ein „Friend-in-the-middle“-Angriff.

Dass Arbeitgeber, Personalagenturen und Versicherungen auf soziale Netzwerke zurückgreifen, um zu Informationen über bestimmte Personen zu gelangen, muss bei der Teilnahme an solchen Netzen ebenfalls berücksichtigt werden.

Während die geschilderten Szenarien Angriffe auf personenbezogene Daten betreffen, gibt es auch Angriffe auf das soziale Leben. Orte mit Informationen über Dritte ohne deren Wissen zu verknüpfen, ermöglicht Stalking.

Cybermobbing. In den USA wurde im Jahr 2006 wurde die erst 13-jährige Megan Meier in den Tod getrieben. Sie war das erste Opfer dieser neuen Angriffsart. Das Beispiel Robin Sage, einer real nicht existenten 25-jährigen angeblichen Angehörigen eines Network-Warfare-Kommandos der US-Marine, hat gezeigt, dass, im Vertrauen auf die erfundene Lebensgeschichte und das beigefügte attraktive Bild, aus dem Kontakt anderer mit dieser – nicht näher hinterfragten – Kunstfigur Informationen abgeschöpft werden konnten.

Abhilfe könnten Peer-to-Peer verschlüsselte Netzwerke bieten, wie etwa das Projekt *Diaspora (http://diasporafoundation.org)*. Die Entwicklung steht hier jedoch erst am Anfang.

Dipl. Inf. Horst Bliedung von *Atos (www.atos.net/iam)* hat beim Seminar ein Identity- und Access Management vorgestellt. Gunnar Porada hat vorgeführt, wie in schlecht gesicherte Datenbanken eingedrungen werden kann. *Kurt Hickisch*

Fotos: Kurt Hickisch