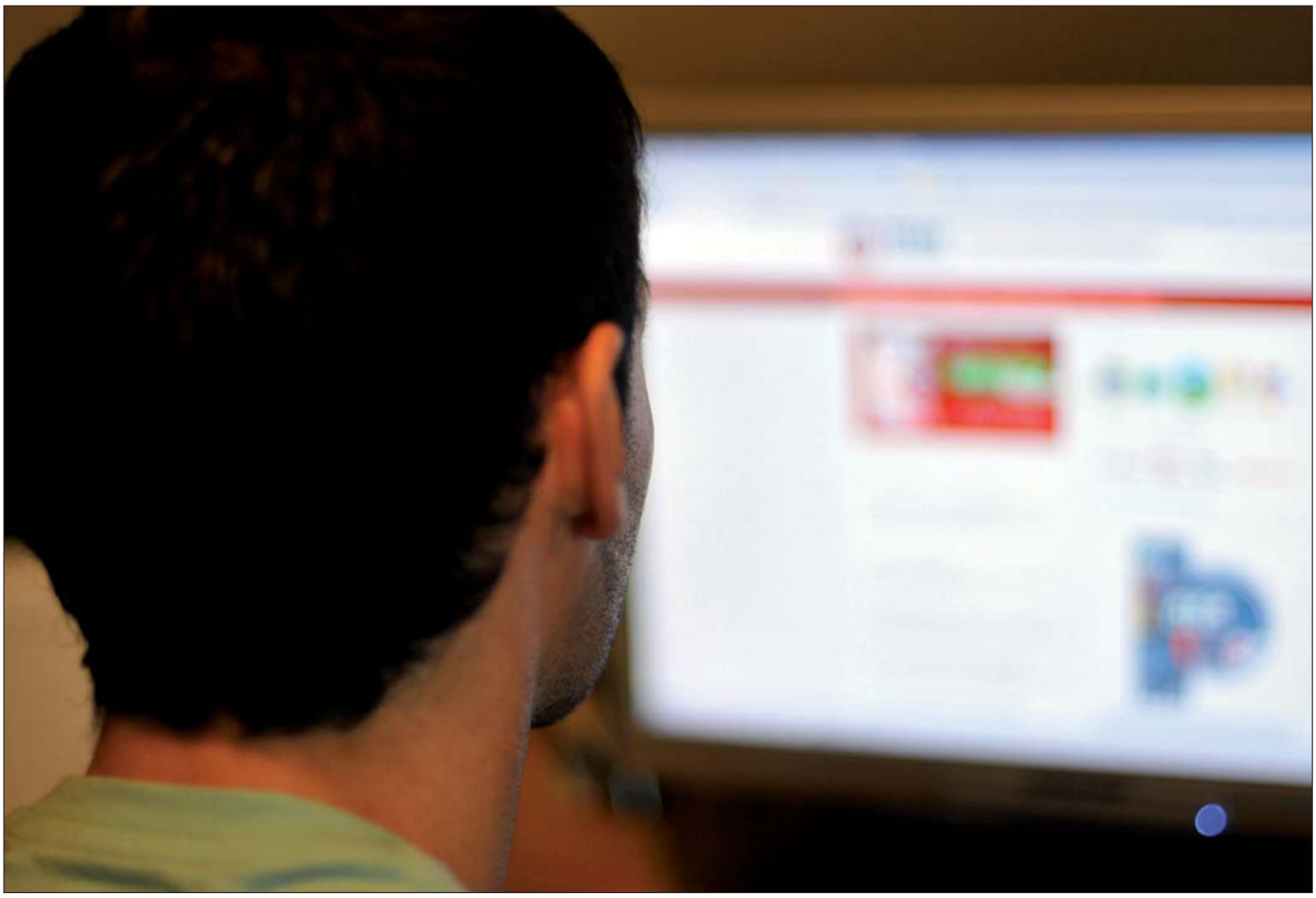

In der virtuellen Welt haben sich neue Kriminalitätsformen gebildet.

IT-Sicherheitsproblem Mensch

Menschliche Schwächen machen IT-Sicherheitssysteme angreifbar. Dieses Problem und andere Fragen der Informationssicherheit waren Schwerpunkte des 5. IT-Sicherheitstags in Klagenfurt.

Leider gibt es für menschliche Einfalt keinen Sicherheitspatch“, sagte Gerald Kortschak beim 5. IT-Sicherheitstag, der am 5. November 2008 an der Universität Klagenfurt stattfand. „Damit bleibt der Mensch trotz aller technischen Vorkehrungen die Schwachstelle im IT-Sicherheitskonzept.“

Was nützt die beste Firewall, wenn der *Social Engineer (Social Hacker)* durch die Herstellung von persönlichen Kontakten Passwörter in Erfahrung bringen und damit Sicherheitsmaßnahmen unterlaufen kann. Bei einem typischen Angriff dieser Art werden zunächst Informationen über Internes gesammelt, die den Angreifer bei weiteren Kontakten als Insider erscheinen lassen, dem man vertrauen kann. Dann wird eine Beziehung aufgebaut, und diese letztlich ausgenützt.

Nach achtlos weggeworfenen Papierausdrucken zu stöbern („Dumpster Diving“), kann wertvolle Informationen verschaffen. Sobald Müll nach außen geschafft wurde, ist es nicht verboten, darin herumzuwühlen.

Vermeintlich von anderen vergessene USB-Sticks wird wohl jeder einmal probeweise und aus Neugier anstecken, ohne daran zu denken, dass er sich damit Programme zum Ausspähen von Daten oder des von ihm verwendeten Passworts auf seinen Rechner laden kann.

„Über das Netz kann mehr über einen Menschen in Erfahrung gebracht werden, als diesem lieb ist“, erklärte Daniela Senger, ebenfalls Mitglied der *WKÖ IT-Security Experts Group (www.itsecurityexperts.at/wko)*. So gut Netzwerke wie *StudiVZ* unter Studenten oder *Xing* im kommerziellen Bereich geeignet sind, Verbindungen zu Menschen herzustellen, mit denen man sonst nicht zusammenkommen würde, hinterlässt man Spuren, und es ist bereits gängige Praxis von Personalbüros, einen Stellenbewerber vor der Einstellung zu „googeln“ oder in Netzwerk-Plattformen nach ihm zu suchen. Ein in launiger Runde geschossenes Partyfoto, das ins Netz gestellt wurde, Blogs oder Videos auf *YouTube* können zur Ablehnung einer Bewerbung führen. „Abwägen, welche Daten zu privat für das Internet sind“, rät Senger, „alles kann gegen einen verwendet werden.“

In den virtuellen Welten haben sich neue Formen einer Kriminalität entwickelt: Es wird bis zur Erpressung damit gedroht, die Identität, mit der jemand im Internet auftritt und sich einen Bekanntheitsgrad erworben hat (Nickname), zu missbrau-

FOTO: KURT HICKISCH

chen oder unter dem realen Namen des Betroffenen auf Plattformen aufzutreten und ihm dadurch Schaden zuzufügen (Nick-Napping). Erpresserisch gedroht wird auch damit, das, was sich jemand in der virtuellen Welt des *Second Life* aufgebaut hat, durch Löschen seines Accounts zu zerstören, sein In-Game-Konto zu leeren, oder es werden Schutzgelder dafür verlangt, dass seine Kreditkarte nicht gehackt wird. Immer mehr Fälle werden bekannt, dass kleine bis mittlere Unternehmen, die Online-Shops betreiben, mit der Drohung zu Geldleistungen veranlasst werden, dass sie bei Nichtzahlung durch *Denial-of-Service*-Attacken lahmgelegt werden.

Online-Banking. Über Rechtsfragen im Zusammenhang mit Missbrauchsfällen beim Online-Banking wie Phishing und Pharming referierte Univ.-Prof. Dr. Peter Mader der Universität Salzburg. In beiden Fällen wird versucht, an Zugangsdaten des Kontos des Opfers zu gelangen, entweder, indem ihm das Passwort (PIN) und die Transaktionsnummern (TANs) herausgelockt werden oder der Rechner des Opfers beispielsweise durch *Trojaner* so manipuliert wird, dass er bei Herstellung der Bankverbindung trotz richtiger Eingabe der Adresse auf eine nachgebildete Website umgeleitet wird. Wenn der Kontoinhaber dann auf dieser seine Zugangsdaten eingibt, werden sie dem Betrüger bekannt und zum Schaden des Berechtigten verwendet.

Um das System der nur dem Berechtigten in Form einer Auflistung mitgeteilten Transaktionsnummern sicherer zu gestalten, muss bei *iTAN* nicht die nächste, sondern eine beliebig vorgegebene (indizierte) *TAN* aus

Daniela Senger: „Es ist bereits gängige Praxis, einen Stellenbewerber vor der Einstellung zu googeln."

der Liste verwendet werden; bei *eTAN* wird, über ein Zusatzgerät, eine aus den Transaktionsdaten erzeugte *TAN* verwendet. Bei der für den mobilen Einsatz entwickelten *mTAN (xTAN)* wird die *TAN* in der Regel per SMS übermittelt und ist nur wenige Minuten gültig.

Die elektronische Signatur wird, wie auch das „HBCI-Chipkartenverfahren", bisher kaum eingesetzt; für biometrische Verfahren (Fingerprint) zur Authentifikation bei Online-Transaktionen laufen derzeit Pilotversuche.

Online Banking bietet Vorteile für den Kunden (er braucht das Geldinstitut nicht aufzusuchen und ist nicht von dessen Öffnungszeiten abhängig) und für die Geldinstitute durch wesentliche Kostenersparnis. Allerdings ist die Frage der Haftung bei Missbrauch durch Dritte noch nicht geklärt. Generell besteht als wichtigste Kundenpflicht jene zur Geheimhaltung der ID-Merkmale wie bei der Bankomat-PIN, und dass die Bank bei Missbrauchsverdacht sofort zu benachrichtigen und die Verfügernummer zu sperren ist. Offen ist, ob bei Aufruf der Website eine Überprüfung der URL oder des SSL-Zertifikats in AGB vorgeschrieben werden kann. Eine Neuregelung ist durch die Umsetzung der

Peter Mader: „Bei Online-Banking ist die Haftungsfrage bei Missbrauch durch Dritte nicht geklärt."

„Zahlungsdienste-Richtlinie" der EU, RL 2007/64/EG, zu erwarten, die bis 1. November 2009 zu erfolgen hat. Nach dieser Richtlinie wird der Kunde nur bei betrügerischem Handeln und grob fahrlässiger Pflichtenverletzung haften und den Schaden zu tragen haben, sonst eben die Bank, und es werden Beweislastregeln aufgestellt.

„Elektronische Kommunikation ist kein und war nie ein rechtsfreier Raum", führte Wolfgang Feiel von der *Rundfunk und Telekom Regulierungs-GmbH (RTR)* aus. „Der Rechtsrahmen dafür umfasst, je nach Klassifizierung, 80 bis 150 Rechtsakte". „Sicherheit" bedeutet in diesem Bereich die öffentliche Sicherheit, die Sicherheit von Kommunikationsnetzen, von Geräten und auch von Daten. Das Kommunikationsgeheimnis, das Inhaltsdaten, Verkehrsdaten und Standortdaten betrifft, steht in einem Spannungsverhältnis dazu, dass diese Daten zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten von besonderer Bedeutung sind. Die Richtlinie 2006/24/EG über die Vorratsdatenspeicherung, die bisher in Österreich, was die Telefonie betrifft, über den vorgegebenen Termin 15. September 2007 hinaus noch nicht umgesetzt wurde und hinsichtlich des Internets bis zum 15. März 2009 noch umzusetzen ist, ist unter dem Eindruck der Terroranschläge von London und Madrid entstanden. Die Richtlinie sieht eine Speicherung von Verkehrs- und Standortdaten für einen Zeitraum zwischen sechs Monaten und zwei Jahren vor, nicht jedoch eine Speicherung von Inhaltsdaten.

Irland hat gegen diese Richtlinie vor dem EuGH Nichtigkeitsklage erhoben; ein Urteil ist noch nicht ergangen. Das deutsche Bundesverfassungsgericht hat mit Urteil vom 11. März 2008, 1 BvR 256/08, die vollständige Umsetzung der Vorratsdatenspeicherungs-Richtlinie wegen erheblichen Eingriffs in Persönlichkeitsrechte vorläufig ausgesetzt. Die Europäische Kommission hat den Auftrag, Teile des Rechtsrahmens für die elektronische Kommunikation zu überprüfen; ab Mitte 2009 wird ein Beschluss erwartet. Die Mitgliedstaaten werden dann eine Frist bis 2010/11 zur Umsetzung haben.

E-Card. Zahlen und Fakten zur E-Card hat Karl Scheibelhofer von der *Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft mbH (SVC)* geboten. Die im Jahr 2005 erfolgte Einführung der E-Card, die jeder in Österreich Sozialversicherte erhält, gründet sich auf § 31a ASVG; sie ist der Schlüssel zum österreichischen Gesundheitssystem.

Mitte 2008 waren rund 8,4 Millionen Karten in Umlauf; insgesamt ausgegeben wurden elf Millionen, etwa als Ersatz für verlorene oder unbrauchbar gewordene Karten oder infolge Namensänderung. Pro Jahr erfolgen 90 Millionen Konsul-

FOTOS: KURT HICKISCH

Wolfgang Feiel: „Elektronische Kommunikation findet nicht im rechtsfreien Raum statt.“

Gerald Kortschak: „Für menschliche Einfalt gibt es leider keinen Sicherheitspatch.“

tationen, zu Spitzenzeiten mehr als eine halbe Million pro Tag. Hinter dem System stehen 11.000 Clients in Ordinationen, etwa 15.000 netzwerkfähige Chipkartenleser, ferner hochverfügbare Rechenzentren und gesicherte Netzwerke. Auf der Karte sind mit Ausnahme des Geschlechts nur jene Daten abgespeichert, die auch außen aufgedruckt sind, also Name, Titel, Geburtsdatum, Sozialversicherungsnummer. Auf der Rückseite befindet sich die Europäische Krankenversicherungskarte (EKVK), die zusätzlich die international eindeutige Kartennummer, den Versicherungsträger und ein Ablaufdatum enthält.

Auf dem Chip befindet sich außerdem die Bürgerkartenfunktion, die der Inhaber kostenlos freischalten kann. Das kann entweder online über Finanz-Online erfolgen, bei einer Registrierungsstelle der Sozialversicherung oder im Wege einer elektronischen Anforderung. Die Freischaltungsinformationen werden in diesem Fall, da ja die Identität des Antragstellers, anders als bei einer persönlichen Vorsprache oder bei einer schon erfolgten Registrierung, vorerst nicht überprüft ist, mit einem RSa-Brief übermittelt, der nur dem namentlich angeführten und ausgewiesenen Empfänger ausgehändigt wird. Mit der Bürgerkartenfunktion können mit Hilfe eines Kartenlesers und der kostenlos über *www.buergerkarte.at* downloadbaren Bürgerkartensoftware unter anderem Dokumente digital unterschrieben (signiert) und verschlüsselt werden. Bisher wurde diese Funktion der E-Card nur in etwa 20.000 bis 30.000 Fällen aktiviert.

Aus abgaberechtlichen Gründen muss der Liefervertrag für die E-Card alle fünf Jahre neu ausgeschrieben werden. Daher wird ab Anfang 2010 eine neue Generation dieser Karten ausgegeben. Sie werden äußerlich gleich aussehen; die Frage, ob sie auch ein Lichtbild des Berechtigten enthalten, ist noch nicht entschieden. Technisch wird die neue Generation dafür ausgestattet sein; sie wird mehr Speicherplatz enthalten und stärkere kryptografische Algorithmen (auf der Basis elliptischer Kurven) verwenden.

Die von der *Forschungsgruppe Systemsicherheit* der Universität Klagenfurt *(syssec – www.syssec.at)* von Prof. Dr. Patrick Horster und Ass.-Prof. Dr. Peter Schartner organisierte Veranstaltung wurde von etwa 80 Teilnehmern besucht. Der nächste IT-Sicherheitstag ist für Anfang November 2009 vorgesehen. *Kurt Hickisch*

Fotos: Kurt Hickisch