Breites Sicherheitsspektrum

Von Datenschutz über Kommunikation, Sicherheit am Arbeitsplatz bis hin zur Krisenbewältigung spannten sich die Themen bei einem Sicherheitssymposium in Wien.

Zu den vorhandenen 125 Millionen Schadprogrammen sind 2014 34 Millionen dazugekommen. Auf jede Minute entfallen somit etwa 87 neue Schadprogramme“, berichtete Joe Pichlmayr, Geschäftsführer der Datensicherheitsfirma *Ikarus GmbH (www.ikarus.at)* und Vorstandsmitglied von Cybersecurity Austria, beim 21. „Symposium Sicherheit“ der *Erste Group Bank AG*, das vom 15. bis 17. Oktober 2014 in Wien stattgefunden hat. Das Bild über künftige Bedrohungen der IT-Sicherheit, das Pichlmayr vor den etwa 80 Sicherheitsverantwortlichen von Geldinstituten entwickelte, war alles andere als beruhigend. Man lernt nur aus Angriffen, die entdeckt wurden. Die Mehrheit der angegriffenen Unternehmen oder Organisationen bemerkt jedoch nie oder zu spät, dass sie angegriffen wurden.

Die Systeme werden immer komplexer. Selbst bei einem hochkomplizierten Uhrwerk, bei dem ein Rad in das andere greift, kann das Ergebnis vorausgesagt werden. Demgegenüber ist das Verkehrsgeschehen von einer Fülle voneinander unabhängiger Faktoren abhängig und kann nur näherungsweise prognostiziert werden. Im „Internet der Dinge“ trifft dies in noch viel höherem Ausmaß zu. Dass die Kriminalität in diesem Bereich schon angekommen ist, zeigte Pichlmayr am Beispiel eines Angriffs auf Smart-Grids. „Digitale Messzähler werden zu kommenden Angriffszielen“, betonte der IT-Sicherheitsexperte. „Die geplante Einsatzdauer von 15 Jahren ist bei der raschen

Sonja Rauschütz: „In der Kommunikation ist wichtiger, wie man etwas sagt, als das, was man sagt.“

Thomas Müller: „Mitarbeiterkriminalität entsteht auch durch Verlust des Selbstwertgefühls.“

technologischen Weiterentwicklung viel zu lang“. Was kann passieren, wenn sich über Internet oder das GSM-Netz Herd und Grill an- und abschalten lassen? Wenn das Smart Home mit dem Internet vernetzt ist? „Der steigenden Zahl, Komplexität und Intelligenz von Angriffen, dem steigenden Grad der Vernetzung und der technologischen Entwicklung steht ein sinkendes Verständnis für Sicherheit gegenüber. Es braucht das dringende Bewusstsein, dass mit diesen enormen Chancen auch enorme Risiken verbunden sind.“

Big Data. Risiken anderer Art im Zusammenhang mit Daten wurden von Dipl. Physiker Philipp Schaumann und Dr. Christian Reiser von der *Erste Group Bank AG* aufgezeigt. Algorithmen steuern die Welt, ob das den in Millisekunden ablaufenden Wertpapierhandel oder den Start von Abwehrraketen betrifft. Im Ertragsmanagement werden die Preise für Flüge oder Hotelzimmer täglich an Bedarf und Nachfrage angepasst, um eine optimale Auslastung mit bestmöglichem Gewinn zu erzielen. Das Verhalten im Netz wird beobachtet: Wie reagiert jemand auf Sonderangebote? Versandhändler wissen, was wir gerne kaufen würden. „Big Data“ ermöglicht einen Blick in die (wahrscheinliche) Zukunft des Einzelnen.

Computer analysieren das Kriminalitätsgeschehen mit dem Ziel zu erkennen, an welchen Orten die nächsten Straftaten zu erwarten sind. Anhand der Vorgeschichte und des sozialen Milieus eines in Haft befindlichen Straftäters wird computerunterstützt seine Rückfälligkeit prognostiziert werden können. Aus der Analyse des Umfelds eines Menschen, seiner Wohngegend, seiner Facebook-Kontakte, seiner Vorlieben, wird die Wahrscheinlichkeit errechnet werden können, ob er einen Kredit zurückzahlen kann. Sein Verhalten im Internet, seine Vernetzungen und seine Kommunikation werden Rückschlüsse darauf zulassen können, ob jemand ein „Trouble-Maker“ ist, der auf die No-Fly-Liste kommt oder vor jedem Flug speziell befragt wird. Algorithmen finden auffälliges Verhalten.

Zielsetzungen führen uns. Viele Partnervermittlungen nutzen Algorithmen zum Bewerten von Beziehungen, wobei bis zu 10.000 Persönlichkeitsparameter pro Person verglichen werden. Der Rechner wählt den passenden Partner aus. Nur – wer entscheidet, was für eine „gute“ Beziehung notwendig ist? Der Programmierer? Das Unternehmen, das Marktinteressen verfolgt und eingegangene Partnerschaften zählt, ohne Rücksicht auf deren Dauer?

Vorausberechnete Suchergebnisse können Menschen in eine bestimmte Richtung drängen, sie „nudgen“ sie. Kleidung, Haarfarbe, Haarschnitt werden sich künftigen Erfordernissen anpassen; die Berufswahl dem vorgegebenen Muster.

Data Breach. § 24 Abs. 2a erster Satz DSG 2000 normiert, dass der Auftraggeber einer Datenverwendung unverzüglich die Betroffenen in geeigneter Form zu informieren hat, wenn ihm bekannt wird, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht.

Durch die Unbestimmtheit der verwendeten Begriffe wirft diese Gesetzesbestimmung eine Reihe von Fragen auf, betonte Dr. Gregor König von der *Erste Group Bank AG*. Eine

FOTOS: KURT HICKISCH

Gebäudemanagement mit dem Tablet: Smart-Home-Lösungen bringen Vorteile, aber auch Gefahren mit sich.

FOTO: FRAUNHOFER FKIE

schwerwiegende unrechtmäßige Verwendung kann sich aus der Anzahl der Datensätze ergeben, aus der Eingriffsintensität oder der Art der Daten, etwa Gesundheits- oder Bonitätsdaten. Die eintretenden Schäden können auch immateriell sein; dass der Betroffene bei Kenntnis des Missbrauchs den Schaden hätte abwenden können, ist nicht gefordert.

Die „unverzüglich“ und „in geeigneter Form“ zu erfüllende Informationspflicht wird primär in einer persönlichen Verständigung bestehen, aber ab einer gewissen Zahl von Betroffenen unter Einschaltung der Medien. Die Betroffenen müssen die Information tatsächlich erhalten. Inhalt der Information wird sein müssen, was passiert ist; welche Folgen eintreten könnten; nicht aber Empfehlungen über die weitere Vorgangsweise. Die Informationspflicht besteht nicht, wenn den Betroffenen nur ein geringfügiger Schaden droht oder aber die Information aller Betroffenen einen unverhältnismäßigen Aufwand erfordern würde (§ 24 Abs. 2, zweiter Satz DSG). Eine Information der Datenschutzbehörde ist derzeit nicht vorgesehen, befindet sich aber im Entwurf zur Datenschutz-Grundverordnung der EU, die die RL 95/46/EG ersetzen wird.

Für Fälle, in denen die Verständigungspflicht schlagend werden könnte, empfiehlt König vorbeugend die Erstellung eines Risikoplans mit Benennung eines Verantwortlichen für die Abwicklung und Festlegung, wer im Unternehmen wann wie beizuziehen ist. Bei Eintritt des Falls erfolgt die Erhebung des Sachverhalts (Was ist passiert? Wer ist betroffen? Was könnten die Folgen sein?) und die Dokumentation aller gesetzten Schritte.

Verhandlungsführung.

„Wie man etwas sagt, ist wichtiger als das, was wir sagen“, war die Kernthese des Vortrags von Sonja Rauschütz, MPA, Gründerin und Geschäftsführerin der „Wiener Schule der Verhandlungsführung“ *(www.vienna-school.at)*. Wie kann man erreichen, dass beim Verhandlungspartner etwas „ankommt“ und gute inhaltliche Ergebnisse erzielt werden?

Rauschitz geht von sechs Persönlichkeitstypen aus: Logiker, Beharrer, Rebell, Empathiker, Macher und Träumer. Jeder dieser Typen hat eine andere Wahrnehmung, kommuniziert anders, wird anders motiviert, lebt anders. Keiner ist besser oder schlechter als der andere; jeder Mensch hat Anteile dieser Typen in sich. „Es ist wie in einem Raum mit sechs Türen. Dort, wo eine Tür offen ist, geht man hinein“, beschreibt Rauschitz den Vorgang des Eingehens auf einen anderen; ihn so zu behandeln, wie er selbst behandelt werden möchte.

Der Logiker strukturiert, spricht auf Zahlen, Fakten, Daten, Ziele, an. Der Beharrer bewertet, baut auf Werte, Vertrauen, Loyalität, Respekt, Verlässlichkeit. Der Träumer agiert zurückhaltend („… möchte keine Umstände machen; bin mir nicht sicher …“), reflektiert, hat kein Bedürfnis zu kommunizieren. Der Macher („Wetten wir“, „Genug geredet“) setzt in die Praxis um, ist aktionistisch, ergreift Chancen. Der Empathiker ist fürsorglich, kümmert sich um andere, umsorgt sie, drückt Gefühle und Wertschätzungen aus. Der Rebell („wow“, „cool“) zeigt reaktives Verhalten, drückt starke Zu- oder Abneigung aus, geht an

Probleme kreativ und spielerisch heran. Jede dieser Typen hat laut Rauschitz ein bestimmtes, vorhersehbares Verhalten, in das er zurückfällt, wenn negativer Stress erlebt wird. Ein solcher äußert sich häufig in Verhandlungssituationen.

Logiker und Beharrer werden aggressiv. Der Beharrer sieht alles negativ, beginnt, Meinungen zu predigen. Der Logiker reagiert mit Schuldzuweisungen und Kontrolle. Beiden gemeinsam ist, dass sie Anerkennung für ihre Leistungen wollen. Sie können über den informativen Kanal angesprochen werden. Empathiker werden im Stress noch einfühlsamer. Sie wollen als Mensch gesehen werden. Zu ihnen kommt man über den fürsorglichen Kanal.

Der Macher fängt zu provozieren an. Der Träumer zieht sich noch mehr zurück, wartet ab. Er braucht klare Ansagen. Beide Typen können über den direktiven Kanal erreicht werden („Sagen Sie mir, wie es geht“).

Der – im Grunde Kontakt suchende – Rebell wird zum Kritisierer. Er ist über den spielerischen Kanal beeinflussbar, interaktiv – er hat Freude am Gespräch mit dem anderen. Die Kunst der Verhandlungsführung besteht darin, hinter der Maske den Typ des Menschen zu erkennen und sich dadurch den Zugang zu ihm zu verschaffen.

Gewalt am Arbeitsplatz. Breiten Raum, einschließlich einer Podiumsdiskussion, nahm das Phänomen Workplace Violence ein, über dessen Entstehung, Auswirkung und mögliche Prävention der Kriminalpsychologe Dr. Thomas Müller referierte. „Mitarbeiterkriminalität entsteht durch Verlust des Selbstwertgefühls“, führte Müller aus. Kommen dazu eine längerdauernde Belastungssituation, die nicht abgebaut werden kann, fehlende Identifizierung mit dem Unternehmen und private Probleme (Scheidung, Tod eines Angehörigen, Führerscheinentzug, Schulden), kann dieses verlorene Selbstwertgefühl zu destruktiven Handlungen führen.

Hannes Gulnbrein: „Eine Amoklage in einem Bankinstitut hat es in Österreich bisher nicht gegeben.“

Sylvia Mayer: „Kritische Infrastrukturanlagen sind in einem Objektschutzkatalog zusammengefasst.“

Diese können sich äußern im Absenden anonymer Schreiben, Entwendung von Unterlagen, Mobbing, Erpressung, Nötigung, aber auch in körperlicher Gewalt. Warnzeichen sind Verhaltensänderungen, entweder extrem kontaktsuchend oder sich zurückziehend; Isolation von den anderen, indem die Arbeitszeit in die Morgen- oder Abendstunden verlegt wird; abnehmende Produktivität, schlechte Gesundheit und Hygiene, unerklärliches wechselhaftes Verhalten. Derartige Fälle der Rechtsabteilung zuzuweisen, sei der falsche Weg, betonte Müller. Es handle sich um psychologische Probleme, deren Lösung in den Bereich der Psychologie fällt.

Krisensituationen. Mag. Sylvia Mayer vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) gab einen Einblick in das Österreichische Programm zum Schutz kritischer Infrastruktur, zu der auch das Bankwesen gehört. Besonders schützenswerte Objekte sind in einem Objektschutzkatalog zusammengefasst, in dem auch die zu ergreifenden Maßnahmen festgelegt sind. Informationen über Bedrohungen im In- und Ausland und Lagebilder werden weitergeleitet. Zentrale Kontaktstellen bei den Unternehmen stehen in Verbindung mit der zentralen Meldestelle beim BVT. Dort wird derzeit ein Cyber-Security-Center aufgebaut.

„Bei einer Amoklage handelt ein Täter in Verletzungs- oder Tötungsabsicht, will nicht unerkannt bleiben. Bei einer Geiselnahme dient die Geisel als Druckmittel zur Zielverwirklichung; der Täter möchte unerkannt entkommen“, erläuterte Oberst Hannes Gulnbrein, Kommandant des EKO Cobra Wien, das Thema Einsatzlagen.

Eine Amoklage in einem Bankinstitut hat es in Österreich bisher nicht gegeben – abgesehen von einer Ankündigung 2009 in Graz. Bei einem Amoklauf gilt es, aus dem Aktionsradius des Täters zu kommen oder sich zu verbarrikadieren, keinesfalls aber das Gespräch zu suchen. Der Täter lässt sich von seinem Plan nicht abhalten. Bei einem Banküberfall handelt es sich zumeist um Gelegenheitstäter mit akutem Geldbedarf, die meist keine einschlägige Vorerfahrung haben. Nur 14 Prozent aller Täter gehen professionell vor. International gesehen, nehmen Angriffe auf Geldtransporte zu. Ein Banküberfall kann von vornherein mit Geiselnahme geplant sein; sich zur Geiselnahme entwickeln („Anschlussgeiselnahme“) oder es nimmt der Täter beim Betreten oder Verlassen des Bankinstituts Bankangestellte als Geiseln.

Geiseln sollten nicht durch Widerstand aggressive Reaktionen des Geiselnehmers erzeugen, ihm gegenüber nicht den Helden spielen und ihn in seiner Rolle akzeptieren. Es wäre sonst mit einer Machtdemonstration zu rechnen. Sich „lässig“ oder „cool“ zu geben, würde den Geiselnehmer verwirren und verunsichern. Ihm das Gefühl zu geben, die Situation unter Kontrolle zu haben, beruhigt und stabilisiert die Lage. Über private Bereiche zu reden, würde Vertrauen aufbauen. Unüberlegte Fluchtversuche würden zumeist misslingen und hätten „Bestrafungen“ anderer Geisel zur Folge. Ziel der Polizei ist es, zu verhandeln und den Täter zur Aufgabe zu bewegen. Ist eine Verhandlungslösung nicht möglich, erfolgt der polizeiliche Zugriff. Der Schutz des Lebens der Geisel geht der Festnahme des Täters bevor.

Als wichtig bezeichnete es Gulnbrein, Checklisten für die Zusammenarbeit mit der Polizei vorzubereiten, mit den Daten der Mitarbeiter, einschließlich medizinischer Informationen, benötigter Medikamente und Kontaktpersonen. Ohne Abstimmung mit der Polizei sollten Informationen nicht an Medien weitergegeben und auch keine Interviews gegeben werden.

Kurt Hickisch

FOTOS: KURT HICKISCH