Risiken und Gefahren

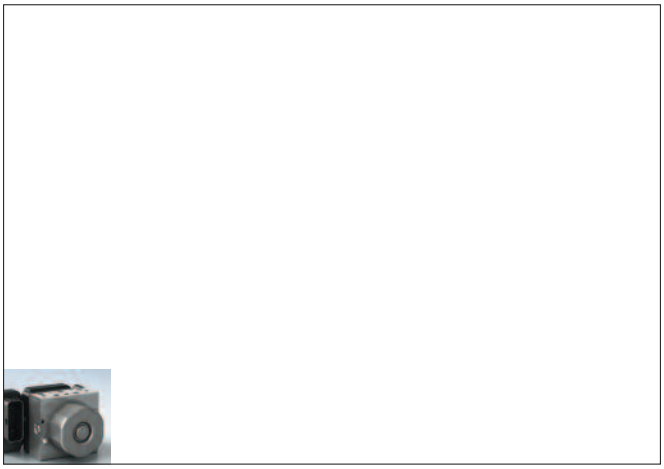
Informationssicherheit, physische Sicherheit, Datenschutz sowie Notfall- und Krisenmanagement waren die Themenschwerpunkte beim 22. Symposium Sicherheit in Wien.

Versicherung der Unsicherheit ist Sicherheit“: Dieser Sinnspruch des deutschen Aphoristikers Dr. Hanspeter Rings war das Motto des 22. Symposiums der Erste Group, das vom 21. bis 23. Oktober 2015 in Wien stattgefunden hat. Die etwa 70 Teilnehmer stammten überwiegend aus Geldinstituten.

Ein Beispiel für Unsicherheit sei die derzeitige Weltlage, referierte MMag. Harald Felgenhauer vom *Systemic Foresight Institut (www.systemicforesightinstitute.org)*. Felgenhauer sieht eine Polarisierung der Welt zwischen jenen Staaten, die dem transatlantischen Verteidigungsbündnis angehören, und denen der Shanghai Cooperation Organization (SCO). Zu dieser zählen Russland und China, Indien, Pakistan; der Iran ist assoziiert.

Die SCO versuche, ein Gegengewicht aufzubauen. So stehe die von China gegründete Asiatische Entwicklungsbank in Konkurrenz zur Weltbank. Umgelegt auf Begriffe aus der Computertechnik, werde ein eigenes Betriebssystem zu dem bereits bestehenden transatlantischen entwickelt, auf dem in beiden Fällen die Märkte, Finanzsysteme, Meinungen aufbauen würden.

Letztlich gehe es in beiden Systemen darum, die Hardware zu nutzen, die in Rohstoffen, Transportwegen, Arbeitskräften bestehe. Kristallisationspunkt einer neuen internationalen Ordnung sei das südchinesische Meer, wo die unterschiedlichen Interessen aufeinander stoßen.



Banküberfall: Technische Maßnahmen haben dazu beigetragen, die Zahl der Banküberfälle zu senken.

Im Nahen Osten stehe eine Neuaufteilung der durch den Sykes-Picot Plan 1916 geschaffenen künstlichen Grenzen bevor. Zusammen mit militärischen Auseinandersetzungen (Syrien), Migration, Wirtschafts- und Finanzkrieg (Sanktionen, Währungsabwertungen – „Race to the bottom“) und Cyberwar werde mit steigenden Turbulenzen im Außenbereich zu rechnen sein. Im Sinne des *Cynefin-Frameworks,* eines Wissensmanagement-Systems, seien die sich ergebenden Beziehungen komplex; ein Zusammenhang zwischen Ursache und Wirkung könne erst im Nachhinein wahrgenommen werden. Für Österreich ergebe sich, die Resilienz des eigenen Systems insofern zu stärken, als Veränderungen in die Erwartungshaltung aufzunehmen seien. Resilienz geht über den Begriff der Sicherheit hinaus.

Einblicke in die derzeitige Weltlage, was etwa Kriege und Terrorismus betrifft, bietet auch die Website *www.visionofhumanity.org,* auf die Peter Aschenbrenner, MSc, bei der *OMV* global zuständig für Prävention und Bewältigung von sicherheitsrelevanten Gefährdungslagen, hinwies. Weltweit sei mit Risiken zu rechnen, darunter einem globalen Dschihad.

Krisenmanagement. Ministerialrat Mag. Robert Stocker, MBA, Leiter der Abteilung II/13 (Einsatz-, Krisen- und Katastrophenkoordination) im BMI, gab einen Überblick über die koordinierende Funktion des BMI im Rahmen des Staatlichen Krisen- und Katastrophenschutzmanagements (SKKM).

Die Tätigkeit von Behörden des Bundes und der Länder, Freiwilligenorganisationen und Unternehmen der kritischen Infrastruktur werde im SKKM zusammengefasst und sinnvoll miteinander verbunden, ohne dass eine übergeordnete Behörde entstehe.

Dem BMI, das hiezu eine Plattform bietet, komme die generelle Koordinationsverantwortung zu. Es bestehen darüber hinaus Kontakte zur EU und zur UNO. Im Einsatz- und Koordinationscenter (EKC), das ständig besetzt ist, werden täglich Lagebilder zur Sicherheit Österreichs erstellt, in das die Bundesministerien, die Landespolizeidirektionen, die Länder sowie NGOs und die Betreiber kritischer Infrastruktur eingebunden sind. Informationen gehen an die EU und Nachbarländer. Als Beispiele für die vielfältigen Vernetzungen und komplexen Abläufe nannte Stocker die Lage in Fukushima, Japan, vom 12. bis 21. März 2011 und das Hochwasser Anfang Juni 2013. Im Jänner und April 2015 wurden Übungen für den Fall eines Auftretens von Ebola in Österreich durchgeführt.

Aus Vorfällen solle man lernen; es soll sich eine Fehlerkultur entwickeln, sagte Robert Jamnik von der Zertifizierungsorganisation *CIS (www.cis-cert.com)* im Hinblick auf kontinuierliche Verbesserungen der Sicherheit in Unternehmen. Auf die Phase des Planens und Vorbereitens folge das (automatische) Erkennen und Berichten von Vorfällen. Dann sei der sicherheitsrelevante Vorfall zu untersuchen (Ausmaß feststellen, Beweismaterial sichern) und es seien in der nächsten (Response-)Stufe Sofortmaßnahmen zu treffen samt forensischen Analysen. Letztlich gelte es, Lehren zu ziehen, die Sicherheit zu verbessern und das Risiko- sowie Security-Incident-Management anzupassen.

IT-Sicherheit. „Ransomware gibt es jetzt auch für Ihr Smartphone!“ Mit dieser ironisch gemeinten Bot-

FOTO: LPD NÖ

schaft machte Sebastian Bachmann, BSc, von der *Ikarus Security Software GmbH (www.ikarus.at)* auf die Gefahren aufmerksam, die mit der Nutzung von Smartphones verbunden sind. Diese sind nicht bloße Telefone, sondern Computer, die rund um die Uhr in Betrieb sind, eine Kamera und Sensoren haben und ständig ihren Standort bekanntgeben. Das und die Möglichkeit, sie als Server zur Weiterverbreitung von Schadprogrammen einzusetzen, macht Smartphones als Angriffsobjekte für Schadprogramme begehrt. Diese Möglichkeiten werden auch genützt, „weil es leicht ist und man sehr viel Geld damit verdienen kann".

Ransomware blockiert den Computer/das Handy und gibt das Gerät gegen Bezahlung eines Lösegeldes („Ransom") wieder frei. Wenn man erkennt, dass es sich um einen Angriff handelt, ist es mitunter zu spät. Der Anwender vertraut auf den Absender einer E-Mail. Wie soll er diese auch überprüfen? Jedes Mal telefonisch nachfragen? Oder er vertraut auf Updates, die gefälscht sein können. Sobald er ein solches Update installiert, hat er das Schadprogramm auf dem Rechner.

Von Anfang an müssten sichere Systeme geschaffen werden, forderte Bachmann. Dem Anwender sollte möglichst wenig zur Kontrolle überlassen werden; sicherheitsrelevante Einstellungen ohnehin nicht. Und wenn doch, dann sollte in den Sicherheitseinstellungen die Installation von Apps aus unbekannter Herkunft gesperrt werden.

Für PCs hat sich Sicherheitsbewusstsein langsam durchgesetzt, für mobile Geräte noch nicht. Die Komplexität der Geräte macht Sicherheit „mühsam".

Harald Felgenhauer: „Die Unsicherheit zeigt sich in der Polarisierung der Welt in Ost gegen West."

Dr. Gilbert Wondracek, *Deloitte Österreich,* wies auf weitere Sicherheitsprobleme hin, die sich durch die Vernetzung und intelligente Steuerung von Gebäudefunktionalitäten wie Licht, Raumbeleuchtung, Klimaanlage, Lüftung, Sicherheits- und Alarmtechnik im Zusammenhang mit dem Internet der Dinge ergeben – Stichworte „Smart Home" und „Green Building". Ein Netzwerk von Sensoren und Steuergeräten sammelt Daten und interagiert mit der physischen Umgebung.

Wenn alles im Gebäude miteinander spricht, wird die Angriffsebene entsprechend vergrößert. Sofern die Management-Ebene mit dem Internet verbunden ist (Smart Grid, Fernwartung), können über dieses Steuerungsbefehle erteilt werden. Damit wird es möglich, Zutritts- und Steuerungssysteme (Luftzufuhr, Heizung, Jalousiensteuerung) zu manipulieren, Alarme etwa von Bewegungsmeldern zu unterdrücken und letztlich die Kontrolle über die Administrationseinheit zu übernehmen und Angriffe auf andere Server durchzuführen.

Zur Vorbeugung sollten drahtgebundene Steuerungsnetze bevorzugt werden, besonders in sensiblen Bereichen. Das Netzwerk zur Gebäudesteuerung sollte von anderen Datennetzen im Unternehmen getrennt, die Software regelmäßig aktualisiert und Zugriffe auf die Managementkonsole und -geräte eingeschränkt werden.

August Baumühlner: „Das häufigste Motiv der Täter für Banküberfälle in Wien war Spielsucht."

Banküberfälle. Chefinspektor August Baumühlner, MSc, Präventionsbeamter im Landeskriminalamt Wien, berichtete über eine Auswertung von Banküberfällen in Wien. Motiv für die Täter war am häufigsten Spielsucht, meist waren es Automatenspieler. Überfälle durch Suchtkranke verlagern sich eher auf weniger geschützte Bereiche. Technische Maßnahmen wie der Rückbau von Kassenschaltern, Verbesserungen der Videoqualität haben dazu beigetragen, die Zahl der Banküberfälle zu senken.

Analoge Leitungen zur Alarmübertragung werden in der Schweiz mit 31. Dezember 2017, in Deutschland im Jahr darauf und in Österreich auch in den nächsten Jahren abgeschaltet. Darauf wies DI Christian Sageder, Produktmanager bei *ÖWD Security Systems,* hin. Das dahinterliegende Netz (Backbone) ist bereits digitalisiert; es geht nur noch um die „letzte Meile" bis zu den Endgeräten. Teure Hochsicherheitsleitungen können dann durch IP-Leitungen und Redundanz abgelöst werden. Ein Pilotprojekt ist bei einer Bank in Salzburg bereits installiert.

Datenschutz. Die vom Rat der EU am 15. Juni 2015 beschlossene Datenschutzgrundverordnung der EU (DSGVO) befand sich zur Zeit des Symposiums im Trilog-Verfahren zwischen dem Rat der EU und dem Europäischen Parlament, mit dem Ziel einer endgültigen Einigung bis Ende 2015. Einen Überblick über die zu erwartenden Änderungen gab Dr. Gregor König von der *Erste Bank*.

Durch den Rechtsakt einer Verordnung wird eine einheitliche, EU-weit gültige, unmittelbar anwendbare Datenschutzregelung für alle personenbezogenen Daten natürlicher Personen geschaffen. Das Datenschutzrecht wird voll harmonisiert und einheitlich ausgelegt.

Durch der Kommission obliegende „delegierte Rechtsakte", „Standardformate", wird deren Stellung gestärkt. Als neue Definitionen kommen genetische, biometrische und Gesundheitsdaten hinzu (Art. 4). „Kind" ist man bis zum 18. Lebensjahr; für bis zu 13-Jährige gelten besondere Schutzbestimmungen. Zur Nutzung der Dienste der Informationsgesellschaft benötigen sie die Einwilligung der Eltern/des Vormundes. Eine „Einwilligung" ist jederzeit widerrufbar und kann auch mündlich erteilt werden; die Beweislast liegt bei dem für die Verarbeitung Verantwortlichen (Art. 6-8).

Das allgemeine Meldeverfahren wird abgeschafft. In Behörden und Unternehmen mit mehr als 250 Mitarbeitern sind Datenschutzbeauftragte zu bestellen (Art. 35 ff). Datenschutz soll des

Fotos: Kurt Hickisch, Andreas Wastian

Weiteren durch technische Vorkehrungen und Voreinstellungen erzielt werden (Privacy by design, by default; Art. 23). Ein Recht auf Vergessenwerden (Art. 17) und Datenübertragbarkeit (Art. 18) wird geschaffen. „Accountability" (Art. 22) bedeutet, dass personenbezogene Daten in Übereinstimung mit der Verordnung verarbeitet werden und dies nachgewiesen werden kann (Dokumentation, Datenschutz-Folgeabschätzung, Zu-Rate-Ziehen der Behörde; Art. 33 f). Verletzung des Schutzes personenbezogener Daten (Data breach) verpflichtet zur Meldung an die Aufsichtsbehörde und zur Benachrichtigung der Betroffenen, jeweils „ohne unangemessene Verzögerung" (Art. 31 f). Die unabhängige nationale Aufsichtsbehörde ist für Beschwerden und zur Beratung betroffener Personen zuständig, hat aber auch exekutive (Art. 46 ff) und verwaltungsstrafrechtliche Befugnisse (Art. 73 ff). Die Geldbußen können bis zu einer Million Euro reichen oder in Prozentsätzen des weltweiten Jahresumsatzes bemessen werden.

Big Data, große, komplexe Datenmengen, dienen der Erkennung statistischer Trends durch Tracking, Scoring, Personalizing, Profiling. Daten werden aus Bereichen gewonnen, die ursprünglich nicht angedacht waren, erläuterte Rechtsanwalt Mag. Gerold Pawelka. Sie erfahren, als eine Art Abfallprodukt, eine Zweitverwendung. Bei anonymisierten Daten werfen diese Verfahren keine datenschutzrechtlichen Bedenken auf – aber wann ist die Herstellung eines Personenbezuges tatsächlich verlässlich ausgeschlossen? Wenn Datenmengen zu klein und damit Rückführungen auf

Robert Jamnik: „Aus Sicherheitsvorfällen sollte man lernen; es sollte sich eine Fehlerkultur entwickeln."

Personen möglich werden, können die Daten durch „Target Swapping" verschmutzt werden.

Mit dem geltenden Datenschutzrecht (DSG 2000) ist es unvereinbar, Daten zu sammeln und einem anderen Verwendungszweck zuzuführen. Eine Zustimmung kann nicht auch künftige, noch nicht bekannte Zwecke umfassen. Für die künftige DSGVO ist im Vorschlag des Rates zu Art. 6 Abs. 4 eine Aufweichung insofern vorgesehen, als zwischen dem alten und dem neuen Zweck eine Interessenabwägung vorgenommen werden soll.

Anwendungsfälle von Big Data sind etwa, dass sich durch Kombination von Aktivitäten aus dem Mobilfunknetz, soziografischen Daten und Geoinformationen in einem Kaufhaus Bewegungsmuster erkennen lassen. Oder der Erfolg von Marketingmaßnahmen: Wo bleiben Kunden stehen? Wohin wandern Kunden ab? Es lassen sich nach dem Einzugsgebiet kaufkräftiger Schichten die günstigsten Örtlichkeiten für Geschäftsansiedlungen ermitteln. Aus Analysen des Einkaufsverhaltens eines bestimmten Kunden kann diesem individuell Rabatt gewährt werden – oder auch nicht, wenn

Thomas Greis: „Für Stresssituationen muss ein Werkzeugkasten zur Verfügung stehen."

er eine Ware ohnehin immer kauft. Die Preisgestaltung bei Hotelbuchungen und Flugreisen kann von Person zu Person durch Rückschlüsse auf seine persönlichen Verhältnisse variieren („Jeder hat seinen Preis"). An der Zahl der Suchanfragen bei *Google* lässt sich erkennen, ob etwa eine Grippewelle bevorsteht und aus Auswertungen der Tweets von *Twitter*-Nutzern, welche Themen die Öffentlichkeit zu einem bestimmten Zeitpunkt bewegen.

Aggression. „Von Gewalttaten wie Raub abgesehen, entsteht Aggression nicht plötzlich, sondern ist oft ein langer Weg und multikausal", sagte Ing. Mag. Stefan Rakowsky. Es kann der nervende Kunde sein, demgegenüber sich eine Spannungssituation bis zur Belastungsgrenze aufbaut. Folgen solcher Aggression können sein Schlaf- und Konzentrationsstörungen, Aggression gegen sich und andere, Alkohol, Verschlechterung der Gesundheit, Absentismus, geringere Motivation. Präventiv wirkt Training des Verkaufspersonals hinsichtlich seines Auftretens. Jeder Mensch achtet auf Signale seines Gegenübers. Werden in der Ausbildung auch Stresssituation erlebt, können, etwa bei einem Banküberfall, Folgeerscheinungen reduziert werden. Letztlich wird psychologische oder medizinische Hilfeleistung erforderlich sein, um Langzeitfolgen zu verhindern und Funktionsfähigkeit sowie Lebensqualität wieder herzustellen.

„Für Stresssituationen muss ein Werkzeugkasten zur Verfügung stehen", forderte Mag. Thomas Greis von der Sicherheitsakademie des BMI. Dieses Instrumentarium und damit Handlungssicherheit erwirbt man sich durch mentale Vorbereitung („Was wäre, wenn …"), durch Erfahrungsaustausch, Übungen und Rollenspiele.

Wie Sicherheit die Lebensqualität entscheidend verbessern kann, schilderte Brigitte Lehner. Das Unternehmen ihres Mannes hatte 3.000 Mitarbeiter und einen Umsatz von 1,5 Milliarden Euro. Ängste vor Entführungen wurden zunächst verdrängt. Durch die Hinzuziehung der Personenschützerin Heidi Prochaska *(www.atlatusconsulting.com)* wurden präventive Maßnahmen entwickelt, wie Umbauten und Einrichtung einer Alarmanlage. Für die drei Kinder wurde ein Schutzraum geschaffen; sie wurden in präventivem Verhalten unterwiesen.

Die Personenschützerin übernahm mit dem täglichen Ausführen des Hundes die Voraufklärung der Umgebung, führte Fahrdienste durch und sonstige Dienstleistungen. Lehner und Prochaska schilderten, wie sich der Aufbau eines Vertrauensverhältnisses zwischen Beschützter und Beschützerin entwickelt hat, wie sich die Personenschützerin an die Familie anpasste, ohne ein Teil von dieser zu werden und wie die Beschützte letztlich zu einem befreiten Leben gefunden hat.

Kurt Hickisch

FOTOS: KURT HICKISCH