Symposium Sicherheit in Wien: 14 Aussteller präsentierten ihre Sicherheitsprodukte und -dienstleistungen.

Vorbereiten, schützen, sichern

Schwerpunktthemen beim 25. Symposium Sicherheit waren Informations- und physische Sicherheit, Daten- und Arbeitnehmerschutz, Notfall- und Krisenmanagement und Wirtschaftskriminalität.

Seit dem Inkrafttreten der DSGVO am 25. Mai 2018 bemerken wir im Bankenwesen ein gesteigertes Bewusstsein und größeres Interesse für den Datenschutz, insbesondere hinsichtlich der Rechte der Betroffenen", sagte Martin Knoll vom *Erste-Data-Protection-Office* beim *Symposium Sicherheit,* das vom 15. bis 17. Oktober 2018 im *Erste Campus* in Wien stattgefunden hat. Allerdings würden oft Missverständnisse hinsichtlich der Rechte auf Löschung und Vergessenwerden bestehen.

Diese Rechte stoßen dann an ihre Grenzen, wenn gesetzliche Archivierungspflichten bestehen. Das Recht auf Datenportabilität kann mit der Forderung: „Gib mir meine Daten wieder!" umschrieben werden. „Überlege dir gut, was du mit meinen Daten machst", weist auf die vorzunehmende Datenschutz-Folgeabschätzung hin. „Sag mir, was du mit meinen Daten machst", bezieht sich auf die erweiterten Informationspflichten, zu denen auch die Meldung einer Data-Breach (Datenpanne) gezählt werden kann. „Merke dir, was du mit meinen Daten machst", enthält die Aufforderung, ein internes Verarbeitungsverzeichnis zu führen.

NISG. Einen Überblick über das zu erwartende *Netz- und Informationssicherheitsgesetz (NISG)* gab Ing. Mag. Sylvia Mayer, MA, vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT). Dieses Gesetz, das sich zum Zeitpunkt des Referats noch als Ministerialentwurf im Begutachtungsverfahren befand, dient der Umsetzung der EU-Richtlinie 2016/1148 vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. Adressaten des auch als Cyber-Sicherheitsgesetz bezeichneten Gesetzes sind die Betreiber wesentlicher Dienste in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastruktur sowie neben Einrichtungen des Bundes die Anbieter digitaler Dienste. Zu diesen zählen die Anbieter von Online-Marktplätzen, Online-Suchmaschinen und von Cloud-Computing-Diensten.

Für Unternehmen dieser Kategorien legt das Bundeskanzleramt Schwellwerte fest, ab wann sie unter die Bestimmungen des NISG fallen. Dies wird im Einzelfall durch Bescheid festgestellt. Diese Unternehmen werden besondere, dem Stand der Technik entsprechende Sicherheitsvorkehrungen hinsichtlich ihrer IT-Infrastruktur zu treffen haben (§ 15 des Entwurfs), die durch Verordnung des Bundeskanzleramtes in Leitlinien festgelegt werden. Die Erfüllung dieser Anforderungen ist mindestens alle drei Jahre gegenüber dem Bundesministerium für Inneres (BMI) durch Zertifizierungen oder Überprüfungen durch qualifizierte Stellen nachzuweisen.

Ferner besteht für die Betreiber wesentlicher Dienste eine Meldepflicht (§ 16) insofern, als sie Sicherheitsvorfälle unverzüglich dem für sie zuständigen Computer-Notfallteam zu melden haben, das diese Meldung an das BMI weiterleitet. Damit soll dem partnerschaftlichen Ansatz des Gesetzes folgend die Möglichkeit geschaffen werden, andere Unternehmen warnen zu können. Je mehr Meldungen einlangen, desto qualifizierter können Informationen erteilt werden.

SYMPOSIUM SICHERHEIT

Sicherheitsthemen

Themenschwerpunkte des 25. *Symposiums Sicherheit* für Sicherheitsverantwortliche von Geldinstituten und deren Umfeld waren Informations- und physische Sicherheit, Daten- und Arbeitnehmerschutz, Notfall- und Krisenmanagement, Wirtschaftskriminalität. 14 Aussteller präsentierten Sicherheitsprodukte und -dienstleistungen. Das nächste Symposium wird vom 14. bis 16. Oktober 2019 in Wien stattfinden.

www.erstegroup.com

FOTOS: KURT HICKISCH

Referentinnen und Referenten beim 25. Symposium Sicherheit der Erste-Group in Wien: Norbert Welzl, Franz Wulz, Thomas Greis, Daniela Jordanich, Birgit Langeder und Timo Kob.

Für das Bankwesen bestehen bereits spezielle Regelungen (§ 85 Zahlungsdienstegesetz 2018 – ZaDiG über den Umgang mit operationellen und sicherheitsrelevanten Risiken, § 86 über die Meldung von Vorfällen). Insofern werden im Wesentlichen noch Kontaktstellen für die Kommunikation geschaffen und der NIS-Behörde gemeldet werden müssen. NIS-Behörde ist das Cyber-Security-Center im BVT. Dort werden Lagebilder erstellt, dort erfolgen die Kommunikation und das Krisenmanagement.

Wenn die Sirenen heulen: Aus diesem Blickwinkel referierte Norbert Welzl, Konzernsicherheit des ORF, über die Krisen- und Katastrophenkommunikation des ORF. Neben dem normalen Programm berichtet der ORF über wichtige Ereignisse im Internet, Teletext und in *ORF Smart*. Laufbandtexte werden in das Programm eingeblendet. Bei Bedarf werden Sondersendungen geschaltet, samt Livestreaming in das Internet.

Streaming-Dienste für Radio und Fernsehen sind Punkt-zu-Punkt-Verbindungen zum Server, was bedeutet, dass die Zugangsdienste gerade bei außergewöhnlichen Ereignissen durch zu viele Abfragen überlastet sein können und diese Dienste dann nicht mehr zugänglich sind. Mobilfunknetze und Streaming erfolgen über das Internet oder benutzen zumindest Internetkomponenten wie die DNS-Namensauflösung. Durch Cyber-Attacken oder Netzüberlastung kann es zum Ausfall dieser Dienste kommen.

Allen elektronischen Medien und Kommunikationsmitteln ist gemeinsam, dass sie von der Stromversorgung abhängig sind. Deren Ausfall würde massivste Auswirkungen auf ITK-Dienste nach sich ziehen. Störungen oder Ausfälle im Internet haben demgegenüber zwar auch erhebliche Auswirkungen, doch können Störungen einzelner Dienste teilweise oder gänzlich substituiert werden. Übrig bleibt, dass bei außergewöhnlichen Lagen die Informationsbeschaffung mit alltäglichen IKT-Mitteln extrem eingeschränkt ist.

Als noch am ehesten verfügbare Informationsebene bleibt in Krisen- und Katastrophenfällen der terrestrische UKW-Rundfunk (88 – 108 MHz). Portable UKW- und Kurzwellenempfänger sind mit Batteriebetrieb überall einsetzbar. Bei Mobiltelefonen mit eingebautem UKW-Empfänger ist immer ein UKW-Radio verfügbar, sofern die Kabelkopfhörer – die die Antenne bilden – angesteckt werden. Autoradios bieten ebenfalls einen vom Netzstrom unabhängigen UKW-Empfang.

Die UKW-Notversorgung wird vom ORF über das bundesweite Radioprogramm Ö3 und die neun ORF-Regionalprogramme in den neun Bundesländern sichergestellt. Ö3 ist 24 Stunden redaktionell besetzt und ist Ansprechpartner für die Bundeswarnzentrale. Jedes ORF-Landesstudio kann autark sein Bundesland mit seinem Regionalradioprogramm versorgen. Fast alle Landesstudios liegen in verschiedenen Erdbebenzonen und sind an verschiedene Elektrizitätsversorgungsunternehmen angeschlossen. Eine Notstromversorgung für mindestens 72 Stunden ist gesichert. Im europäischen Ausland kann, vom Sender Moosbrunn/Niederösterreich aus, das Ö1-Morgenjournal im 49-Meter-Band auf 6.155 kHz empfangen werden. Auch Überseegebiete können mit Kurzwelle erreicht werden. Außerdem betreibt der ORF-Sportverein in Moosbrunn eine notstromversorgte Amateurfunkstation auf Kurzwelle, Rufzeichen OE1XRW.

Faktor Mensch. „Die Leute wissen nicht, was sie im Fall der Fälle tun sollen“, sagte Mag. Thomas Greis von der Sicherheitsakademie des BMI im Zusammenhang mit der persönlichen Sicherheit. Es gilt, Situationen vorauszudenken, und zwar nicht das Mögliche, sondern das Wahrscheinliche. Einem Amokläufer gegenüberzustehen, ist weniger wahrscheinlich, als es mit einem Betrunkenen zu tun zu haben oder mit jemandem, der randaliert und sich weigert, wegzugehen. Die Aussage: „Wir rufen in einem solchen Fall die Polizei“, wirft beispielsweise bereits die Fragen auf, wer übernimmt die Verständigung, wer empfängt die Polizei und wer weist sie ein. Und – was tun bis zum Eintreffen der Polizei? Sich mental auf solche Situationen vorzubereiten und sie zu antizipieren, eröffnet Handlungsoptionen, auf die man im Bedarfsfall zurückgreifen kann.

Deeskalierend zu wirken, bedeutet, ruhig zu bleiben und Haltung zu bewahren. Das Gegenüber mit „Sie“ ansprechen, nicht drohen oder beleidigen, Körperkontakt vermeiden. Sich vorwurfs- und vorurteilsfrei verhalten. Kleinigkeiten können dazu führen, dass sich eine Situation aufschaukelt. Bei allem ist die Situation als solche im Auge zu behalten. Wie groß ist das Aggressionspotenzial des Gegenübers, wie kommt es in seiner Körpersprache zum Ausdruck? Wie sind die örtlichen Gegebenheiten, wo befinden sich Notausgänge? Mit welchen Störfaktoren ist zu rechnen, etwa, wenn andere die Geschehnisse mit dem Handy filmen? Bestehen Rückzugs- und Unterstützungsmöglichkeiten? Im Training können solche Situationen durchgespielt werden, wobei wichtig ist, dass sich niemand davon ausschließt. Auch nicht jene, die glauben, niemals in solche Situationen zu kommen. Die Lage kann sich schnell ändern.

FOTOS: KURT HICKISCH

Betrugsbekämpfung. Der Mensch steht auch im Mittelpunkt bei Betrugsdelikten, worüber Birgit Langeder und Daniela Jordanich vom Fraud-Management der *Erste Bank AG* berichteten. Als 2013 eine Welle von Phishing-Attacken Österreich erreichte, wurde die Watchlist Internet als unabhängige Informationsplattform zum Thema Internet-Betrug und betrugsähnliche Online-Fallen gegründet *(www.watchlist-internet.at)*. Sie informiert über aktuelle Betrugsfälle im Internet und gibt Tipps, wie man sich vor gängigen Betrugsmaschen schützen kann. Opfer von Internet-Betrug erhalten konkrete Anleitungen für weitere Schritte.

2015 wurde eine interne „Checkliste für Polizeieinsätze in Filialen bei Betrugsfällen" erstellt, in der bei Phishing- oder Trojanerattacken die internen Arbeitsabläufe definiert und die Koordination mit den Polizeidienststellen geregelt wurde. Im Juli 2018 wurde auf Grund des Hinweises eines Mitarbeiters in Wien ohne viel Aufsehen vor einer Filiale ein von Interpol gesuchter Kreditbetrüger verhaftet, der in fast zwei Jahren durch betrügerisches Herauslocken von Krediten (Antragsbetrug) einige Millionen Euro an Schaden verursacht hatte.

Seit September 2018 wird der Kautionstrick verstärkt angewandt. Ältere Menschen erhalten einen Anruf, in dem ihnen ein angeblicher Polizist mitteilt, dass ein naher Angehöriger in einen Unfall mit mehreren Verletzten verwickelt sei und sie für ihn eine Kaution hinterlegen müssten, damit der Angehörige nicht in Haft komme. Die Täter fordern Beträge zwischen 40.000 und 80.000 Euro, die in bar einer Person zu übergeben seien, die sich bald melden und das Geld

Am Symposium Sicherheit nahmen 130 Sicherheitsverantwortliche von Geldinstituten und andere Fachleute teil.

abholen werde. Durch die bankinternen Informationen bereits sensibilisiert, fragen die Bankmitarbeiter nach, ob denn mit dem angeblich am Unfall beteiligten Angehörigen bereits in Verbindung getreten wurde. Rückfragen klären dann die Situation. Allerdings wurde den Opfern auch schon aufgetragen, das Handy auf dem Weg zur Bank mitzunehmen und nicht auszuschalten. Dadurch können die Täter mithören, was zwischenzeitig und bei der Geldabhebung gesprochen wird. In neun Verdachtsfällen konnte durch die Aufmerksamkeit der Bankangestellten ein Schaden von insgesamt 631.000 Euro verhindert werden. Informationen der Mitarbeiter in den Filialen und die Aussagen der Betrugsopfer wurden in einer Aussendung der Landespolizeidirektion Wien zusammengefasst. Die Errichtung einer institutsübergreifenden Datenbank der Banken- und Finanzindustrie im Zusammenhang mit betrügerischen Verdachtsfällen ist geplant.

Wirtschaftskriminalität. „Gegenüber dem ersten Halbjahr 2016 ist die Zahl der Straftaten im Vergleichszeitraum 2017 um 6,5 Prozent zurückgegangen, wogegen die Zahl der Wirtschaftsdelikte um 3,3 Prozent zugenommen hat", sagte Univ.-Lektor Franz Wulz, MBA, *Campus Security & Training Group (www.campus-security.group)*. Diebstahl und Unterschlagung stehen dabei an erster Stelle.

Durch Warenschwund (31.602 Anzeigen) entstand in Österreich 2016 ein Schaden von 800 Millionen Euro. In Deutschland stieg der Schaden von 3,4 Milliarden Euro (2016) auf 4,1 Milliarden (2017). Im D-A-CH-Durchschnitt (Deutschland, Österreich, Schweiz) beträgt der Schaden durch Warenschwund (Inventurdifferenz) 1,3 Prozent des Umsatzes. Mehr als 40 Prozent der Täter kommen aus dem eigenen Unternehmen.

Die Motive liegen in Gier; darin, sich persönliche Vorteile zu verschaffen; einem Gefühl der Überlegenheit; in der betrügerischen Absprache mit anderen oder, „weil ich es kann". „Der Täter von heute stiehlt nicht mehr aus Not, sondern aus einer Form der Selbstverwirklichung", sagte Wulz. Wirtschafts-Straftäter sind zumeist männlich und zwischen 45 und 55 Jahren alt, unbescholten und unauffällig, hochangesehen, überdurchschnittlich intelligent. 41 Prozent sind mehr als sechs Jahre im Unternehmen. 70 Prozent handeln nicht alleine. „Suche den Feind im Schatten deiner Hütte", zitierte Wulz ein sudanesisches Sprichwort. Die dabei auftauchende Frage ist immer, ob diese Straftaten nicht verhindert bzw. schon früher hätten erkannt werden können. Es kommt laut Wulz auf die Art der Menschenführung an, die auf den generationenbedingten Typus eingehen und den Wertewandel berücksichtigen muss. Als Traditionalisten stuft Wulz Menschen ein, die zwischen 1922 und 1955 geboren wurden. Die Babyboomer fallen in die Geburtsjahrgänge 1955 bis 1969. Von 1965 bis 1980 Geborene bilden nach dieser Einstufung die Generation X, die Generation Y umfasst die Geburtsjahrgänge 1980 bis 2000, und die Generation Z die zwischen 1995 bis 2010 Geborenen.

Der Generation X werden Werte wie Unabhängigkeit, Individualismus und Sinnsuche zugeschrieben, Streben nach einer hohen Lebensqualität, pragmatisch und selbstständig.

Die mit den neuen Technologien aufgewachsene Generation Y ist „24 Stunden online", flexibel und anpassungsbereit, strebt nach Selbstverwirklichung und Vernetztsein. Arbeit muss Spaß machen; Führungspositionen sind nicht mehr so wichtig.

Der Generation Z wird zugeschrieben, realistisch einzuschätzen, dass Karriereversprechen vielfach nicht gehalten werden. Sie setzt auf fixe Arbeitsplätze mit fixen Arbeitszeiten. Arbeitswelt und Privatleben werden getrennt. Freizeit statt Karriere, Familie statt Firmenwagen, Sharing statt Leasing, Mietwohnung statt Eigentum. Die Risiken für ein Unternehmen liegen bei dieser Generation darin, dass sie weniger Bindungen an ein Unternehmen hat. Die Chancen liegen in der Leistungsbereitschaft und dass sie sich an Prozesse und Spielregeln hält.

Kurt Hickisch

FOTO: KURT HICKISCH