Cybercrime, Datenschutz, KI

Das 27. Symposium Sicherheit der Erste Group fand am 12. und 13. Oktober 2021 in Wien statt. Es nahmen etwa 120 Sicherheitsverantwortliche von Geldinstituten und deren Umfeld teil.

Expertinnen und Experten aus dem In- und Ausland referierten beim Symposium Sicherheit der *Erste Group* unter anderem zu Arbeitnehmerschutz, Business Continuity Management, Informationssicherheit, physische Sicherheit, Datenschutz, Notfall- und Krisenmanagement.

Digital fit oder fertig – wie kommt man selbst oder als Unternehmen mit der Digitalisierung zurecht? „Sicher nicht mit der Opossum-Strategie", sagte Mag. Robert Seeger, Agentur für Kommunikationskunst, also „sich auf den Rücken zu legen, sich tot zu stellen und zu hoffen, dass die Zukunft vorbeiläuft". Man müsse die Veränderung lieben. Wegrationalisiert oder vom Markt verschwinden werde der, der nicht als Besonderheit hervorgetreten sei. „Be someone's lover, not everybody's darling". Digitale Outlets, wie man sich in der digitalen Umwelt präsentiert, würden zum entscheidenden Qualitätskriterium. Mit langatmigen Stellenangeboten werde man die Generation Z nicht mehr erreichen.

BCM-Resilienz. *Business Continuity Management (BCM)* definierte Ing. Karl Weißl, *Erste Group,* in seinem Vortrag als ein Weiterführen eines Geschäfts oder eines Betriebes – trotz eingetretener Störungen – in der bisherigen Art. Es wird nach Lösungen gesucht, die bisherigen Abläufe weiter aufrecht zu erhalten. Technik wird repariert, Geräte werden ersetzt oder es werden andere verwendet. Irgendwann wird das laut Weißl nicht mehr funktionieren. Insbesondere dann, wenn technologische Sprünge auftreten oder wenn man – Stichworte Outsourcing oder Commodification – das Geschehen nicht mehr kontrollieren kann.

Transportboxen für Banknoten: Die Scheine werden im Alarmfall dauerhaft eingefärbt und sind für den Täter wertlos.

Resilienz hingegen bedeute, Dinge anders zu denken und den Ansatz zu ändern mit dem Ziel eines nahtlosen Weiterarbeitens. Zugekaufte Arbeitsleistungen (Outsourcing) und gemeinschaftlich genutzte Güter (Commodification) müssen ersetzbar gemacht werden. Es gelte, eine Konzentration gleichartiger Aktivitäten an einem Ort zu vermeiden und Know-how zu verteilen. Letztlich sollten Ressourcen geschaffen werden, die im Fall des Falles einspringen können, ohne dass nach außen hin von einem Störfall etwas bemerkt wird.

SKKM. Über das staatliche Krisen- und Katastrophenmanagement (SKKM) berichtete MMag. Harald Felgenhauer, Bundesministerium für Inneres. Krisen wie Blackouts oder Strommangel betreffen nicht nur einen Bereich, sondern sind vernetzt. Man muss mit Hilfe dynamischer Modellierungen die Auswirkungen erkennen. Als neues Thema hinzugekommen ist der Ausfall internetbasierter Dienste, etwa wenn Serverfarmen beschädigt werden.

KI. „Künstliche Intelligenz (KI) ist weder künstlich noch intelligent", sagte Dipl. Physiker Philipp Schaumann, der über Video zugeschaltet war. Es geht darum, dass mentale Funktionen von Menschen von Computerprogrammen nachgebildet werden. Der Teilbereich *Machine Learning* geht innerhalb der KI insofern weiter, als IT-Systeme automatisch aus Daten Zusammenhänge erkennen, ohne speziell dafür programmiert zu sein.

Deep Learning als weitere Untergruppe bildet neuronale Netze nach, mit der Besonderheit, dass zwischen der Datenein- und der -ausgabe „hidden layers" liegen, bei denen man nicht weiß, was sich in ihnen abspielt. Es lässt sich nicht überprüfen, was das System gelernt hat, und auch das System selbst kann nicht erklären, wie es zu einer bestimmten Entscheidung gekommen ist.

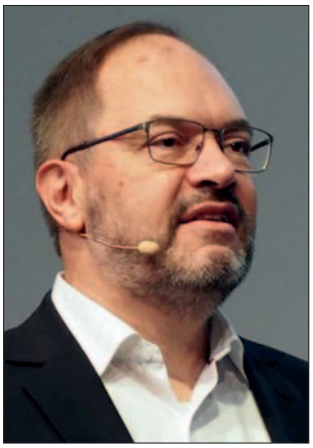
Bei *Big Data-Anwendungen* wird nach Mustern gesucht und es werden Cluster gefunden, selbst wenn sich diese nur zufällig ergeben und nur scheinbar zusammenhängen.

Bei der *Persönlichkeitsanalyse* spielen die „Big Five" eine Rolle, nämlich Offenheit, Gewissenhaftigkeit, Extraversion, Verträglichkeit und Neurotizismus. Der Auftraggeber gibt etwa bei der Personalauswahl vor, welche dieser Faktoren im Vordergrund stehen soll. Institute zur Partnervermittlung erheben pro Partner bis zu 10.000 Persönlichkeitsparameter, die über Algorithmen ausgewertet werden. Wie aber ist eine „gute Beziehung" zu definieren und wer tut das? Der Programmierer, die Firma, die allenfalls auch geschäftliche Interessen verfolgt? Auf welche messbaren Variablen kann „Kreditwürdigkeit" oder „Rückfallswahrscheinlichkeit" zurückgeführt werden? Vorurteile bei der Eingabe von Trainingsdaten spiegeln sich im Endergebnis wider. Letztlich können auch bei der Interpretation der Testergebnisse Fehler oder Vorurteile einfließen.

Regulatorische Bestrebungen in der EU laufen darauf hinaus, algorithmische Anwendungen je nach dem von ihnen ausgehenden Risiko in vier Klassen einzuteilen, von geringem bis unakzeptablem Risiko, wobei in dieser Gefahrenstufe der Einsatz dieser Anwendungen verboten werden soll.

FOTO: KURT HICKISCH

Robert Seeger: „Wie man sich in der digitalen Umwelt präsentiert, wird zum entscheidenden Kriterium."



Karl Weißl: „Es gilt, eine Konzentration gleichartiger Aktivitäten an einem Ort zu vermeiden."

Ingrid Luttenberger: „Ausreichendes Lüften hilft, um virushaltige Aerosole aus Innenräumen zu entfernen."

Joe Pichlmayr: „Pro Monat kommen cirka zehn Millionen Schadprogramme auf den Markt."

Fotos: Kurt Hickisch

Cybercrime. In die Rolle eines IT-Angreifers, konkret des Vorsitzenden der Cybercrime Unlimited Corporation, schlüpfte Joe Pichlmayr, Geschäftsführer der *Ikarus Security Software GmbH (ikarussecurity.com)*, und konnte seinen fiktiven Vorstandskollegen stolz verkünden, dass die Geschäfte blendend laufen. Die Branche sei in drei Jahren um 400 Prozent gewachsen, der Markt für Cybersecurity bloß um 40 Prozent. „Unsere Gegenspieler sprechen bereits davon, den Kampf gegen uns zu verlieren."

Große Hoffnungen seien auf das *Internet of Things* mit seinen exponentiellen Wachstumsraten zu setzen. 2025 würden 75 Milliarden Geräte miteinander über das Internet verbunden sein, Rasenmäher, Smart Homes, Transport und Logistik. Der Markt für Cybercrime, der 2015 noch bei 600 Millionen US-Dollar (USD) gelegen ist, wird für 2021 auf 2,5 Billionen USD geschätzt, immerhin 0,8 Prozent der globalen Wirtschaftsleistung. Pro Monat kommen ca. 10 Millionen Schadprogramme auf den Markt, 300.000 pro Tag und etwa 42 pro Minute. Als Hoffnungsmarkt für Kriminelle haben sich Angriffe auf Kryptowährungen entwickelt.

Der Knüller für die Branche ist *Ransomware*. Daten werden verschlüsselt und gegen Zahlung eines Lösegeldes wieder freigegeben. Das durchschnittlich bezahlte Lösegeld hat im 2. Quartal 2021 über 233.000 US-Dollar betragen, was einer Steigerung um 31 Prozent gegen dem Vergleichszeitraum des Vorjahres entspricht.

Bekannt ist die Erpressung der US-Firma *Colonial Pipeline* im Mai 2021. Treibstoffleitungen in einer Länge von 5.550 Meilen wurden lahmgelegt. Die Erstforderung der Erpresser hatte auf 30 Mio. US-Dollar gelautet. Bezahlt wurden letztlich 4,4 Millionen US-Dollar in Bitcoins. Ein Teil davon konnte vom FBI wieder beschafft werden. Auch österreichische Firmen wurden Opfer von Ransomware-Attacken. Sie finden sich, gleichsam als Referenz für gelungene Angriffe, im Darknet aufgelistet. Die Lösegeldforderungen werden anhand der für ein Unternehmen voraussichtlich entstehenden Ausfallskosten kaufmännisch mit etwa 10 Prozent davon kalkuliert. Die Wiederherstellungskosten sind erheblich höher. Dazu kommen Reputationsschäden und die Gefahr des Weiterverkaufs der Daten. Auch kann man bei Freigabe der Daten nicht sicher sein, ob sich der Angreifer nicht eine Hintertür offen gelassen hat, über die er nach wie vor Zugriff auf die Daten hat.

Schutz bieten auf technischer Ebene Spam-, Phishing- und URL-Filter, Anti-Malware und Endpoint Protection, Intrusion-Prevention-Systeme mit Cyber Threat Intelligence. Dazu kommen als weitere Maßnahmen Awareness-Programme, eine Backup-Strategie, Klassifizierung von Daten nach Geheimhaltungs-, Integritäts- und Verfügbarkeitsanforderungen. Letztlich auch Servicevereinbarungen zu Incident Response mit kurzen Reaktionszeiten und der Abschluss von Versicherungsverträgen.

Ein großes Versicherungsunternehmen wollte den Schaden, der bei einem Kunden durch die Ransomware *NotPetya* angerichtet wurde, nicht bezahlen, weil der Angriff „kriegsähnlich" gewesen sei, berichtete Wolfgang Lehner von *Emerisis (emerisis.com)*. Lehner betonte die Wichtigkeit der Kommunikation in der Krise, und zwar über Kanäle, die sicher sind und nicht durch einen allfälligen Shitstorm überlastet werden können. Krisen erzeugen Druck, der ein starkes Team erfordere, das nach klarer Strategie zu handeln habe. Wichtig seien auch entsprechendes Training sowie Notfalls- und Krisenübungen.

NIS-Gesetz. Wolfgang Pfeiffer, *LinzNetz GmbH (linznetz.at)* ging auf die Erfordernisse ein, die sich aus dem Netz- und Informationssystemsicherheitsgesetz (NISG) und seinen Verordnungen für die Betreiber wesentlicher Dienste, darunter Finanzmarktinfrastrukturen, ergeben *(nis.gv.at)*. Das Gesetz verpflichtet diese Dienste, Sicherheitsvorfällen vorzubeugen, Störungen zu erkennen, zu beseitigen und möglichst rasch die Funktionsfähigkeit wieder herzustellen.

MMag. Stefan Unteregger, *ÖNB*, berichtete über den *Digital Operational Resilience Act (DORA)*, der in Weiterentwicklung der NIS-RL auf EU-Ebene Vorschriften zur digitalen Betriebsstabilität für Finanzinstitute vorsieht und derzeit in einem überarbeiteten Entwurf vorliegt.

In Zeiten, wo für Geldeinlagen Negativzinsen eingehoben werden, gewinnt für Banken das Mietfach (Depot)geschäft an Bedeutung. Bankenschließfächer gelten zwar als sicher, doch

verunsichern Berichte über großangelegte Einbrüche in Schließfachanlagen. Im Rechtsstreit um Schadenersatz müssen Banken beweisen, dass die Sicherungsmaßnahmen dem aktuellen Stand der Technik entsprochen haben.

Eine von Olaf Kisser, Geschäftsführer von *Safecor GmbH (safecor.de),* vorgestellte Lösung besteht darin, von begehbaren Räumen mit einer Vielzahl von Schließfächern abzugehen. Die Schließfächer befinden sich vielmehr in einer Art Hochsicherheitscontainer. Der Kunde erhält aus diesem sein Schließfach über ein elektronisch gesteuertes Transportsystem in einen gesicherten Raum geliefert, führt dort seine Manipulationen durch und schickt das Schließfach wieder zurück. Bankräume und Depot müssen nicht mehr in unmittelbarer räumlicher Verbindung stehen. Der Container selbst benötigt wesentlich weniger Platz als begehbare Anlagen und kann demgemäß mit weniger Geld besser baulich abgesichert werden.

Datenschutz. „Bei Daten aus dem Bereich der DSGVO reist diese mit", zitierte Dr. Gregor König, *Erste Group* Data Protection Officer, den EU-Justizkommissar Didier Reynders. Keine Rechtsprobleme gibt es bei der Übermittlung von Daten in die EU-Mitgliedstaaten, in Mitgliedstaaten des EWR (Island, Norwegen, Liechtenstein) und Staaten mit einem „Angemessenheitsbeschluss" der EU-Kommission (Kanada, Argentinien, Uruguay, Japan, Neuseeland, Israel, Schweiz, Andorra, Kanal- und Färöer-Inseln). Für den „Rest der Erde" hat man sich mit Standardvertragsklauseln beholfen insofern, dass sich der Verarbeiter der DSGVO unterwirft.

Symposium Sicherheit: Im Foyer wurden Sicherheitsprodukte und -lösungen präsentiert, etwa Videoüberwachungs-, Notruf-, Alarmierungs- und Zutrittskontrollanlagen.

Nach dem Urteil des EuGH vom 16.7.2020, C-311/18 („Schrems II") zum „Privacy Shield" der USA ist eine zusätzliche Prüfung der ausländischen Rechtsordnung erforderlich, ob das Drittland ein der EU vergleichbares, angemessenes Datenschutzniveau aufweist. Sollte das nicht der Fall sein, ist nach der Empfehlung des Europäischen Datensicherheitsrates (EDPB) 01/2020 vom 18.6.2020 zu prüfen, durch welche ergänzenden Maßnahmen (supplementary measures) technischer, organisatorischer oder vertraglicher Art ein Ausgleich geschaffen werden kann. Technische Maßnahmen wären etwa Verschlüsselung der Daten; organisatorisch käme eine Datenreduktion in Betracht. Seit Juni 2021 gibt es neue Standard-Vertragsklauseln.

Arbeitnehmerschutz – Covid-19. „Eine möglichst hohe Frischluftzufuhr ist eine der wirksamsten Methoden, potenziell virushaltige Aerosole aus Innenräumen zu entfernen", stellte Mag. Ingrid Luttenberger, Sicherheitstechnisches Zentrum *Erste Group,* fest. „Ausreichendes Lüften durch Öffnen der Fenster oder raumlufttechnische Anlagen kann durch Raumluftreinigungsgeräte nicht ersetzt werden." Filtergeräte filtern zwar Partikel einschließlich Viren aus der Luft, haben aber höhere Schallemissionen. UV-C-Technik inaktiviert Viren, die Geräte sind leiser, doch muss sichergestellt sein, dass kein Ozon erzeugt wird. Eine Luftbehandlung mit Ozon ist, wie überhaupt eine Einbringung von Chemikalien in die Atemluft am Arbeitsplatz, nicht zulässig.

Hofrat Ing. Mag. Leopold Schuster, Leiter des Arbeitsinspektorates Wien-West-Ost, erläuterte die am 1. April 2021 in Kraft getretenen Bestimmungen des „Home-Office-Gesetzes", BGBl I 61/2021. Regelmäßige Arbeitsleistungen in der Wohnung sind zwischen Arbeitgeber und -nehmer schriftlich zu vereinbaren. Der Arbeitgeber hat digitale Arbeitsmittel bereitzustellen oder trägt, allenfalls pauschaliert, die – angemessenen und notwendigen – Kosten. Unfälle im „Home Office" gelten, bei zeitlichem und ursächlichem Zusammenhang, als Arbeitsunfälle. Das ASchG gilt, soweit anwendbar, uneingeschränkt, vor allem die Arbeitsplatzevaluierung. Der Ort der Arbeitsverrichtung (Privatwohnung) gilt als auswärtige Arbeitsstelle. Mit Ausnahme der Regelungen über Pausen und Tätigkeitswechsel, Augenuntersuchungen und Sehhilfen gelten auch die Bestimmungen über Bildschirmarbeitsplätze.

Schulungen. Patrick Türl, bei der *Erste Group* zuständig für Physical Security, und Bernhard Sindl, Sicherheitsbeauftragter, berichteten über ihre Erfahrungen bei virtuellen Sicherheitsschulungen. Deren Vorteil liegt in der Ortsunabhängigkeit und sie lassen sich leichter organisieren. Es empfiehlt sich allerdings ein Testlauf vor dem Seminar. Kreative Ansätze sind gefragt, um die Aufmerksamkeit der Teilnehmer/-innen zu erhalten. Dies fällt bei Präsenzveranstaltungen leichter, die, wie betont wurde, durch virtuelle Schulungen nicht ersetzt werden können. Interessant war, wie der bisherige Lehrfilm „Bankraub Training" in Virtual Reality umgesetzt wurde. Die durch Einsatz eines Avatars ohnehin schon reduzierte Realitätsnähe der Darstellung musste gegenüber den Gefahren einer Traumatisierung abgewogen werden.

Ausstellung. Im Foyer außerhalb des Veranstaltungsraumes wurden Sicherheitsprodukte und -lösungen präsentiert, etwa Videoüberwachungs-, Notruf-, Alarmierungs- und Zutrittskontrollanlagen. Die Fa. *Cennox (cennox.com)* stellte Kassetten für Banknoten vor, die diese im Alarmfall dauerhaft einfärben und dadurch für den Täter wertlos machen. *Dallmeier (dallmeier.com)* präsentierte das Videoüberwachungssystem Panomera mit Analysefunktionen wie Objekterkennung und -verfolgung oder der Möglichkeit, Personen oder abgestellte Fahrzeuge (Parkplatzmanagement) numerisch zu erfassen.

Kurt Hickisch

FOTO: KURT HICKISCH