Cyber-Sicherheit war einer der Schwerpunkte bei den Vorträgen beim 9. D-A-CH Sicherheitsforum in Going in Tirol

Resilienz, Cyber-Angriffe, Fake News

Beim 9. D-A-CH Sicherheitsforum im November 2022 in Tirol berichteten Sicherheitsexperten über Erkenntnisse aus der Praxis.

Veranstaltet von der *SIMEDIA AkademieGmbH,* einem Unternehmen der *von zur Mühlen Gruppe (simedia.de),* fand am 15. und 16. November 2022 beim Stanglwirt in Going, Tirol, zum 9. Mal das D-A-CH Sicherheitsforum statt, das Referenten und Sicherheitsexperten im Publikum aus Deutschland, Österreich und der Schweiz zusammenführte. Im Foyer waren Aussteller von Sicherheitsprodukten und -dienstleistern vertreten.

„Durch Covid hat die Welt die globale Erfahrung der Betroffenheit und der Abhängigkeit gemacht", sagte Prof. Dr. Günther Schmid, ehemaliger Mitarbeiter des deutschen Bundesnachrichtendienstes und emeritierter Professor für internationale Politik und Sicherheit. Die De-Globalisierung und der Wettbewerb zwischen freien und autoritären politischen Systemen hätten sich beschleunigt. Es werde sich zeigen, inwieweit eine *Pax Americana* (amerikanische Weltordnung) durch eine *Pax Sinica* (chinesische Weltordnung) abgelöst wird. Im Ukraine-Krieg seien erstmals begleitend Cyber-Waffen eingesetzt worden. In der vierten industriellen Revolution würden Schlüsseltechnologien wie etwa Biotechnologie entscheidend sein; ebenso technologische Standards und wer sie bestimmen wird.

Evakuierung. Das ZDF unterhält ein weltumspannendes Netz von 18 Auslandsstudios und Außenstellen. Zudem erfolgen Drehreisen in Kriegs- und Krisengebiete. Im Sicherheitsmanagement steht der Schutz der Mitarbeiter an erster Stelle. Es geht aber auch um Vermögens- und Objektschutz, Dreh- und Reisesicherheit. Zu den Reisevorbereitungen gehört laut Frank Heider, Leiter Sicherheitsmanagement des ZDF, eine Gefährdungsbeurteilung, etwa auch über örtliche Partner. Ein gemeinsames Kommunikationszentrum (SPOC) ist einzurichten, Notfallpläne und Exitstrategien sind zu entwickeln.

In Kabul hatte sich von Juni bis August 2021 die Lage zunehmend zugespitzt. Die Amerikaner hatten ihren Rückzug angekündigt. Erste Festnahmen und Durchsuchungen fanden statt. Die Taliban rückten gegen den Flughafen vor. Ein örtlicher Mitarbeiter samt Familie mit Kindern war zu evakuieren. Reisedokumente und Begleitpapiere waren zu besorgen. Finanzen und Begleitung mussten vorbereitet werden. Jedes Familienmitglied hatte das Nötigste an Dokumenten in einem Beutel

FOTO: SCIENCE PHOTO LIBRARY/PICTUREDESK.COM

bei sich und die Informationen, auch die Planung für den Worst Case, im Kopf. Bei den beiden konzentrisch um den Flughafen angelegten Sperren war kein Durchkommen. Aber: Scheitern heißt nicht aufzugeben. Die Handy-Verbindungen funktionierten. Mit dem schon zuvor aufgebauten Netzwerk an Kontaktpersonen und -organisationen konnte in Verbindung geblieben werden. Im Menschengewühl erleichterten markante Kleidungsstücke das Erkennen untereinander und mit den Helfern. Letztlich gelang es, die Familie nach Deutschland auszufliegen.

Der Kriegsausbruch in der Ukraine im Februar 2022 war abzusehen und die Evakuierung des Personals bereits geplant. Kiew wurde mit Autos und einheimischen Fahrern verlassen. Auf dem Weg zur westlichen Landesgrenze waren in angespannter Situation etliche Straßensperren und Checkpoints zu bewältigen. Auch dabei zeigte sich die Wichtigkeit entsprechender Netzwerke.

Resilienz. Krisen bedeuten für Unternehmen, auch mit unerwarteten und bestandsgefährdenden Ereignissen und Entwicklungen umzugehen und sich widerstandsfähig *(resilient)* zu erweisen. Diese Resilienz, erläuterte Dr. Johannes Nickel, *Corporate Resilience Academy (corporate-resilience-adademie.com),* hat einen *präventiven* Charakter in Form der Vermeidung und der Vorbereitung auf Ereignisse und Entwicklungen. Bei deren Eintritt gewinnt Resilienz einen *reaktiven* Charakter insofern, als das Überleben des Unternehmens zu sichern ist. Letztlich kommt ein *progressiver* Charakter insofern dazu, als Lehren aus diesen schwerwiegenden Ereignissen und Entwicklungen gezogen und umgesetzt werden. Die auf einen Schock folgende Reaktion kann entweder in Verarbeitung und Neuorientierung oder in die Insolvenz münden.

Resilienz kann organisatorisch durch Redundanz herbeigeführt werden. Benötigte Bestandteile werden ausreichend auf Lager gelegt, Funktionen im Unternehmen ausfallsicher besetzt und vielfältige Beziehungen aufgebaut, sodass Ausfälle leichter verkraftet werden können. Wird der Gedanke der Absicherung allerdings zu weit getrieben, kann dies zu Unwirtschaftlichkeit bis zur Verschwendung führen. Langfristige Verträge führen in der Regel zu günstigeren Preisen. Kurzfristige Verträge machen ein Unternehmen zwar flexibler, sind aber mit höheren Preisen verbunden. Entscheidend ist die Eintrittswahrscheinlichkeit, wobei auch Produktionsausfälle bei Lieferanten einzubeziehen sind, und, wie lange es dauert, bis die Wiederherstellung erfolgt ist. Entsprechend gute Rankings durch externe Bewerter bedeuten einen Wettbewerbsvorteil.

Referenten beim 9. D-A-CH Sicherheitsforum: Johannes Nickel, Frank Ewald, Johannes Strümpfel und Franz Bättig

Marco Felsberger, *Resilience Engineers (resilience-engineers.com),* ging am Beispiel von Lieferketten von der Fragilität eines Systems aus, diese verstanden als eine nicht lineare Reaktion auf Ereignisse in einer komplexen (VUCA-)Welt. VUCA bezieht sich auf

- *Volatility* (Volatilität): Das Marktumfeld verändert sich häufig und umfassend.
- *Uncertainty* (Ungewissheit): Zukünftige Marktentwicklungen können nicht vorhergesagt werden.
- *Complexity* (Komplexität): Das Umfeld besteht aus vielen Elementen, die unbekannt sind.
- *Ambiguity* (Mehrdeutigkeit): Informationen können unterschiedlich gedeutet werden.

Die (VUCA-)Welt ist zum Unterschied von der bloß komplizierten (Alltags-)Welt nicht mehr in ihren Abläufen vorhersehbar. Voraussetzung ist, das System in seinen Zusammenhängen und Abläufen zu verstehen. Dann gilt es, in einem Stress-Test die kritischen Systembestandteile zu identifizieren und fragile Reaktionen herauszufinden. Beim Transport von Gütern können dies Flaschenhälse sein, etwa Staus an den Grenzen wie beim Brexit, der Ausfall von Schiffskapazitäten (China) oder der pandemiebedingte Mangel an Lkw-Fahrern. Die von Felsberger vorgestellte Methode ermöglicht, durch Veränderung von Variablen die Auswirkungen in einem System rechnerisch darzustellen und damit auch Verbesserungen im Ablauf herbeizuführen.

Personenauswahl. Simon Carl Hardegger vom *Institut für Angewandte Psychologie (IAP)* der Zürcher Hochschule für Angewandte Wissenschaften *(zhaw.ch)* bezeichnete Situationsbewusstsein, Regelkonformität, kritische Grundhaltung, Expositionsbereitschaft und Notfalltauglichkeit als die „Save Five“ an Eigenschaften bzw. Kompetenzen, die Menschen in sicherheitssensiblen Arbeitsumgebungen dazu befähigen, zuverlässig zu handeln. Das Ausmaß, in dem diese Eigenschaften vorliegen müssen, wird unterteilt in *Beginner, Professional, Senior,* bis zum *Expert*. Hierauf werden Berufsgruppen (etwa Reaktoroperateur/-in, Polizist/-in, Pilot/-in, Anästhesist/-in) dahingehend untersucht, in welchem Ausmaß die jeweiligen Kompetenzen gefordert sind (Anforderungsprofil). Beispielsweise wird ein Reaktoroperateur in allen Bereichen mit der Kompetenzstufe Professional auskommen, lediglich bei kritischer Grundhaltung braucht es die Stufe Senior. Beim Linienpilot wird Notfalltauglichkeit in Stufe Expert gefordert, Situationsbewusstsein und Expositionsbereitschaft in Stufe Senior. Der Anästhesist muss diese Stufe in allen Bereichen, außer bei der kritischen Grundhaltung, aufweisen. Diese wird bei ihm auf Stufe Expert gefordert. Den jeweiligen Anforderungsstufen entsprechende psychologische Testprogramme liegen vor.

Cyber-Angriffe. Am 22. Dezember 2019 erhielt das österreichische Außenministerium Hinweise auf einen Cyber-Angriff auf sein IKT-System. Als Reaktion darauf wurden, wie Günter Reiser vom Außenministerium berichtete, erste Maßnahmen zur Minimierung des Risikos getroffen. In Zusammenarbeit mit dem *Cyber Security Center* des BMI und dem *Government Computer Emergency Response Team (GovCERT)* wurde zwischen Weihnachten 2019 und Neujahr der Angreifer laufend beobachtet und es wurden technische Gegenmaßnahmen eingeleitet. Der Durch-

FOTOS: KURT HICKISCH

bruch gelang mit der Entschlüsselung der Kommunikation des Angreifers. Die Dimension des Vorfalls wurde erkannt und es wurden erstmals Koordinationsstrukturen nach dem Netz- und Informationssicherheitsgesetz (NIS-G) eingerichtet. Am 4. Jänner 2020 wurde formell eine Cyber-Krise festgestellt. Es folgte der Aufbau einer Einsatzstruktur. Die etwa 1.600 BMEIA-Bediensteten wurden informiert, eine Meldung an die Datenschutzbehörde erstattet und die Presse informiert. Das Außenministerium wurde für die Bereinigung vorübergehend vom Internet isoliert. Alle kompromittierten Systeme wurden entfernt und neu installiert, alle kompromittierten Benutzer deaktiviert, Passwörter zurückgesetzt. Als wäre dies nicht turbulent genug, wurde an äußeren Ereignissen die Regierung umgebildet (Regierung Kurz II) und es langten aus China die ersten Meldungen über eine neuartige Lungenkrankheit ein. Am 2. Februar 2020 wurden durch das Außenministerium die ersten Österreicher aus Wuhan ausgeflogen. Weitere Flüge folgten.

Zur Bewältigung der Cyber-Krise wurden von Außen-, Innen- und Verteidigungsministerium sowie vom Bundeskanzleramt insgesamt 10.700 Personenstunden geleistet. Die unmittelbaren Kosten betrugen ca. 1,7 Millionen Euro.

Ausgelöst wurde die Krise über eine Phishing-Mail. Durch das Anklicken eines Links wurde die Schadsoftware heruntergeladen. Nach Abschluss der Systembereinigung wurden allen Bediensteten über E-Mail Sicherheitsempfehlungen übermittelt. Es hat sich allerdings herausgestellt, dass etwa 15 Prozent dieser Mails gelöscht wurden, angeblich irrtümlich. Oder weil bereits im Vorschaufenster der Inhalt als gelesen betrachtet, als irrelevant oder als ohnehin bereits bekannt beurteilt wurde; wegen generell zu vieler E-Mails oder wegen Sprachproblemen. Das Ministerium ist daher zu Plakaten übergegangen.

Einen ähnlichen Weg, das Bewusstsein der Mitarbeiter zu erhöhen, ist der Technologiekonzern *GEA (gea.com)* gegangen, über dessen Tätigkeitsbereich und Struktur Iskro Molov, CISO des Unternehmens, berichtete. Im Intranet werden den Mitarbeitern/-innen monatlich durch unterhaltsame Animationen relevante Sicherheitsthemen vermittelt und praktische Hinweise gegeben. Impact-Videos über Vorfälle sollen Betroffenheit und Verbundenheit erzeugen.

9. D-A-CH Sicherheitsforum in Going, Tirol: Referenten und Sicherheitsexperten im Publikum aus Deutschland, Österreich und der Schweiz

Schadsoftware Emotet. Durch Ransomware ist 2021 ein Schaden von ca. 24,3 Milliarden Euro entstanden; der Profit der dahinter stehenden Organisationen hat dabei 602 Millionen US-Dollar betragen, berichtete der Leitende Oberstaatsanwalt Andreas May von der Generalstaatsanwaltschaft Frankfurt am Main, *Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT),* der in der Folge die Aufdeckung eines Angreifers bis zu dessen Verhaftung schilderte.

Angriffswaffe war die Schadsoftware *Emotet,* die 2014 als Bank-Trojaner entwickelt und durch Weiterentwicklung befähigt wurde, E-Mail-Inhalte auszulesen und diese für eigene E-Mails zu nutzen, sodass die solcherart generierten Mails wie eine Antwort auf vom Nutzer kürzlich versendete Mails aussehen, allerdings ein Schadprogramm zur Verschlüsselung der Daten enthalten.

Die Ermittlungen bis zum Ursprung gestalteten sich, ausgehend von einem infizierten deutschen System, zu einer Sisyphus-Arbeit, schilderte May. Man musste sich von einer IP-Adresse zur nächsten hangeln, bis ein Einblick in die täterseitige, wie ein Unternehmen *(Crime as a service; CaaS)* arbeitsteilig aufgebaute Infrastruktur erhalten werden konnte. Letztlich wurde als Ausgangspunkt ein Server in Kharkiv/Ukraine ermittelt und gegen den Betreiber ein Haftbefehl ausgestellt, der am 26. Jänner 2021 mit Hilfe einer Einsatzeinheit der ukrainischen Polizei im Beisein von Andreas May vollzogen wurde. Wer erwartet hatte, eine Galerie von Servern vorzufinden, wurde enttäuscht. In der in einem Hochhaus gelegenen Wohnung des Verhafteten, eines IT-Ingenieurs, befand sich lediglich ein einzelner Rechner. In der Folge wurden Maßnahmen zur De-Installation des Schadprogramms auf den betroffenen Rechnern die Wege geleitet.

Unternehmenssicherheit 4.0. „Disruptive Technologien sind nichts Neues“, sagte DI Johannes Strümpfel, stellvertretender Sicherheitschef der *Siemens AG* und Vorstandsvorsitzender des Bayerischen *Verbands für Sicherheit in der Wirtschaft (BSVW)*. Die Pferdekutsche wurde durch das mit Verbrennungsmotor angetriebene Auto abgelöst, und dieser wird durch den elektrischen Antrieb ersetzt. Die Unternehmenssicherheit 4.0 wird in Richtung Digitalisierung gehen; es werden neue Business-Modelle entstehen *(Security as a Service)*. Sicherheit wird eingekauft. Es werden eher Security Manager mit ganzheitlichem Blickwinkel als Fachexperten benötigt werden. Intelligente und autonome Fabriken werden veränderte Anforderungen an Schutz-

FOTO: KURT HICKISCH

konzepte stellen. Physische und Cyber-Sicherheit werden miteinander verschmelzen. Security wird zunehmend als signifikanter Wertbeitrag zur Erreichung von Unternehmenszielen gesehen werden.

Einen Einblick in Überlegungen zur Digitalisierung von Unternehmensprozessen bei der *Deutschen Post DHL* eröffnete Frank Ewald, Leiter der Konzernsicherheit des Unternehmens. Nicht alles muss oder kann digitalisiert werden. Die Prozesse müssen auf ihre Eignung zur Digitalisierung hinterfragt werden. „Einen Schminkroboter braucht niemand." Überprüft wurde, in welchen Bereichen der Einsatz der Blockchain-Technologie Sinn macht, deren Wesen darin besteht, dass alle Datensätze strikt dezentral gespeichert werden. Nichts kann rückwirkend verändert oder entfernt werden. Der Datensatz ist auf allen im System verbundenen Rechnern gleich.

Nach Prüfung zahlreicher in Betracht kommender Möglichkeiten hat sich der Einsatz dieser Technik bei der Verwaltung von Sicherheitszertifikaten (LBAs) und in Wächterkontrollsystemen als am sinnvollsten herausgestellt. Die Gültigkeit von Sicherheitszertifikaten ist von erfolgreich abgelegten Trainings abhängig. Das ebenfalls *proof-of-concept* vorliegende Wächterkontrollsystem bündelt die Daten von Wächterrundgängen bei jenen über 300 Objekten der DHL, die in Deutschland durch verschiedene Dienstleister bewacht werden. Jeder Scan eines Kontrollpunkts wird direkt in eine nachträglich nicht veränderbare und permanent verfügbare Blockchain eingetragen. Durch die Nicht-Fälschbarkeit der erfassten Kontrollgänge unterscheidet sich das System von einem bloßen Data-Warehouse. Vollen Wert würde das System zusammen mit s*mart contracting* bringen, dass also auch die Verträge mit den Dienstleistern der Blockchain-Technologie angepasst werden.

Fake News. „Die letzten drei Jahrzehnte haben eine neuartige Medien-Umwelt mit sich gebracht", stellte Mag. Stefan Auer, *Austrian Center for Intelligence, Propaganda and Security Studies (ACIPSS; acipss.org)* fest. Das Internet wurde kommerzialisiert. Einige große globale Unternehmen würden entscheiden, welche Inhalte man zu sehen bekommt. Die Unabhängigkeit des Journalismus habe massiv gelitten, auch

Branchenexperten als Vortragende: Günther Schmid, Stefan Auer, Teresa Mayerhofer und Simon Hardegger

durch den Versuch, neue Kundensegmente zu binden. Der Diskurs spiele sich im Bereich der sozialen Medien ab, wobei die klassische Streitkultur durch eigene Wahrnehmungsräume ersetzt werde. Die Verifikation von Behauptungen werde durch den Einfluss von Trollen und Informationskriegen schwieriger. Reaktionen des Staates würden verspätet, dann aber überbordend erfolgen.

Fake News hätten den Zweck, billig und schnell die Wahrnehmung und damit auch das Handeln zu beeinflussen. Bestehendes soll entweder verstärkt oder, als künstlich geschaffener Protest, abgeschwächt werden. Als bewusst falsche Informationen sind Fake News zu trennen von unbeabsichtigten Fehlinformationen (Zeitungsente). Filterblasen umschreiben ein Informations-Universum, in dem sich der Nutzer immer bestätigt fühlt, wogegen Echo-Kammern einen abgeschotteten Bereich ideologisch Gleichgesinnter darstellen.

Als „menschlichen Makel" bezeichnete Auer das Streben nach Moralisierung, das aus einem Gefühl der Überlegenheit den öffentlichen Diskurs aggressiver werden lasse, Kompromisse erschwere und den rationalen Diskurs zur Illusion werden lasse. Ein weiterer Makel sei das vorgefasste Denken (Bias), das Wahrnehmung und Urteilsvermögen verzerre.

Behavior-Detection. Mit dem Ziel, Straftäter und/oder verdächtige Situationen schon vor der Tat zu erkennen und die Straftat zu verhindern oder zumindest den Täter nach der Tat zu ermitteln und festzunehmen, wurde für den Zeitraum 2009 bis 2016 zwischen der Kantonspolizei Zürich und der Universität Zürich ein Kooperationsvertrag abgeschlossen, in dessen Rahmen das Projekt *ASPECT (Analysing Suspicious Persons und Cognitive Training)* entwickelt wurde. Mit Hilfe dieses Projekts, über das Franz Bättig, ehemals Kantonspolizei Zürich, berichtete, sollten unnötige Personen- und Fahrzeugkontrollen vermieden, der Arbeitsaufwand reduziert und Beschwerden insbesondere wegen angeblicher racial profilings minimiert werden. Ähnliche Techniken sind unter Behaviour Detection oder als *SPOT (Screening Passengers by Observation Technique)* auf Flughäfen verschiedener Länder im Einsatz.

Neben dem Wissen, wie Täter vorgehen, sind das Erkennen der Baseline, also des gewöhnlichen Zustands an einem Ort, und das Wahrnehmen von Abweichungen grundlegende Voraussetzungen. Die Baseline kann verändert werden, indem etwa in Einkaufszentren Polizeibeamte in Uniform auftreten oder im Straßenverkehr auf Verkehrskontrollen hingewiesen wird. Ein Beobachter im Vorfeld meldet daraufhin erfolgende auffällige Verhaltensweisen des Lenkers oder der Insassen eines Fahrzeugs. Dieses wird dann kontrolliert. Ähnlich verhält es sich bei plötzlichen Verhaltensänderungen eines Fußgängers (abruptes Anhalten, Tempo- und Richtungsänderungen), wenn jemand einen uniformierten Polizisten sieht. Beim Ladendiebstahl oder in Juweliergeschäften wird auf die Stimmigkeit der Kleidung oder auf Tarnkleidung wie Mütze, ins Gesicht gezogener Schal, Perücke, Sonnenbrillen zu achten sein wie auch, ob die Kleidung vor Betreten des Geschäftes geändert wurde. Vom ruhigen und abgeklärten Berufskriminellen unterscheidet sich der Anfänger durch nervöses und unsicheres Auftreten. Der psychisch oder durch Suchtmittel beeinträchtigte Täter ist eher ängstlich und unsicher, allerdings unberechenbar. Es wurden Originalfilme aus Überwachungskameras unter anderem von Juweliergeschäften vorgeführt, die zeigen, wie sich die Täter vor der Tat einen Überblick verschaffen, sich im Geschäft mit Bandenmitgliedern verbal oder nonverbal absprechen und dann rasch, auffällig zurückblickend, sich vom Tatort entfernen.

Kurt Hickisch

Fotos: Kurt Hickisch