Krisen wirksam managen

Das 7. D-A-CH Sicherheitsforum der Simedia-Akademie vermittelte unter anderem unkonventionelle Denkansätze zur Bewältigung von Krisen.

Bei Fragen der Unternehmenssicherheit reiche es nicht aus, bloß das eigene Unternehmen im Auge zu haben, sondern es müsse die gesamte Wertschöpfungskette einbezogen werden“, sagte Kai Pervölz, Leiter Geschäftsfeld Präventive Sicherheit des *Fraunhofer-Instituts für intelligente Analyse- und Informationssystem IAIS (www.iais.fraunhofer.de)* beim *7. D-A-CH Sicherheitsforum,* das am 19. und 20. November 2019 im *Hotel Stanglwirt* in Going, Tirol stattfand. Laut Pervölz bedarf es einer 360-Grad-Rundumsicht. Die Bedrohungslagen ändern sich, Vorgänge und Bedrohungen werden immer komplexer und auch die Gesellschaft ist durch Klimawandel und Digitalisierung im Wandel. Zulieferer werden immer mehr in die eigenen Prozesse integriert und müssen in Sicherheitsanalysen mit einbezogen werden.

Ein Mensch kann, so Pervölz, gleichzeitig nur 7 (+ 2) Informationseinheiten im Kurzzeitgedächtnis präsent halten („Millersche Zahl“) und 5 (+ 2) Einheiten gleichzeitig verarbeiten. Werden Systeme zu komplex, versteht man sie nicht mehr; die Auswirkungen von Handlungen werden kaum mehr vorhersehbar. Es gilt, Komplexitäten zu reduzieren. Dafür eignen sich TAM-Modelle. Da baumartige Abhängigkeiten am ehestens verstanden werden, werden bei der Modellierung die einzelnen Elemente in eine Baumstruktur übergeführt. Die Bäume wiederum werden durch eine Matrix miteinander verknüpft. Abhängigkeiten werden durch Attribute abgebildet. In der Matrix werden Abhängigkeiten sichtbar. Man erkennt, welche Auswirkungen der Ausfall eines Elements auf alle anderen hat. In der praktischen Umsetzung wird zunächst der Ist-Stand einschließlich der Wertschöpfungskette als TAM-Modell ermittelt, das Ergebnis auf der Basis von Bedrohungsszenarien analysiert und letztlich eine Strategie mit Maßnahmen zur Risikominimierung (Reduzierung von Komplexität, Vermeidung von Abhängigkeiten, Identifizierung besonders kritischer Prozesse) entwickelt.

Organisatoren des Sicherheitsforums Rainer von zur Mühlen, Bernhard Mayerhofer und Günter Großhanten.

Bedrohungen. Aus der Vielfalt möglicher Bedrohungen wurde bei der Tagung besonders der Ausfall elektrischer Energie thematisiert. Das Problem liegt darin, dass immer genau jene Menge an Strom erzeugt werden muss, die gerade verbraucht wird. Jede Abweichung wirkt sich auf die Frequenz des Wechselstroms (50 Hz) aus. Diese steigt, wenn weniger verbraucht wird, und sinkt, wenn mehr Leistung gefordert wird. Tolerierte Abweichungen liegen im Bereich von 0,2 Hz nach oben oder unten. Bei größeren Abweichungen kann es, in einer Pyramide von Maßnahmen, zur automatischen Abschaltung von Leitungssystemen und in letzter Konsequenz zu einem Blackout kommen. Dr.-Ing. Bernd Calaminus von der *Energie Baden-Württemberg AG (EnBW)* wies auf Fälle hin, mit Millionen Betroffenen, etwa in Venezuela 2019 (ca. 5 Tage). Auslöser können extreme Wetterbedingungen oder Naturkatastrophen sein, aber auch Cyber-Attacken. „Das nächste Pearl Harbor wird ziemlich sicher eine Cyber-Attacke auf unser Stromnetz sein“, zitierte der Vortragende eine Aussage von CIA-Direktor Leon Panetta aus dem Jahr 2010.

Störfall und Blackout. In Österreich waren am 30. Oktober 2018 ca. 10.000 Haushalte ohne Strom; im Jänner 2019 waren Orte tagelang durch das Schneechaos von der Umwelt und der Stromversorgung abgeschnitten und im Berliner Stadtteil Köpenick waren ab dem 19. Februar 2019 etwa 100.000 Bewohner und 2.000 Betriebe 31 Stunden ohne Strom. Das seien bloße Störfälle und kein Blackout, erklärte Oberst i. R. Gottfried Pausch. Es kam noch zu keinem längeren Ausfall der Infrastrukturen. Ein Blackout wäre ein plötzlicher, überregionaler und länger als 12 Stunden andauernder Strom- und Infrastrukturausfall, wie jener am 16. Juni 2019, der sechs Staaten Südamerikas und ca. 50 Millionen Menschen für 15 Stunden betroffen hatte. Das Stromverbundsystem hatte wegen Schwankungen der Netzfrequenz automatisch abgeschaltet, doch könnte auch ein Hackerangriff die Ursache gewesen sein.

Die Folgen eines Blackouts wären Ausfall der Informations- und Kommunikationstechnologie; weitgehender Zusammenbruch von Transport und Verkehr; Ausfall der Wasserversorgung und Abwasserentsorgung; Engpässe in der Lebensmittelversorgung; Ausfall der medizinischen Versorgung; Gefährdung der öffentlichen Ordnung und Sicherheit (zunehmende Gewaltbereitschaft, Ausschreitungen, Plünderungen). In dem Maß, in dem die organisierte Hilfe durch die Verwaltungsstrukturen nicht funktioniert, würde laut Pausch die Bedeutung von Nachbarschaftshilfe und der Fähigkeit zur Selbsthilfe steigen. In den Haushalten könnte ein Lebensmittelvorrat für zwei Wochen Engpässe in der Lebensmittelversorgung überbrücken.

Faktor Mensch. Susanne Kufeld, CSO der *Messe Berlin,* sah den Unterschied zwischen herkömmlichen und

FOTO: KURT HICKISCH

Alexander Oberkersch.

Manfred Jilg.

Sicherheitsforum: Literatur zum Thema Blackout.

Cyber-Krisen in der Geschwindigkeit und im Umfang der Ausbreitung. Der Krypto-Trojaner *Wannacry* hatte im Mai 2017 mehr als 220.000 Systeme in 150 Ländern betroffen. In Deutschland war etwa die Deutsche Bahn massiv betroffen; es kam zum Ausfall von Anzeigetafeln in vielen Bahnhöfen. Im EU-Durchschnitt wurden 2019 16 Prozent der Internetnutzer Opfer eines Viren- oder Malware-Angriffs. 45 Prozent wurden im gleichen Zeitraum Opfer eines Identitätsdiebstahls *(Quelle Statista)*. Nach einer Statistik des *VDE* bezeichneten 77 Prozent der Mitgliedsfirmen mangelnde Sensibilität der Mitarbeiter für Risken als Ursache für Cyber-Attacken; 58 Prozent, dass die Angriffe zu spät bzw. gar nicht bemerkt würden. Bei der Entwicklung einer einem Unternehmen angepassten Krisenorganisation müsse daher der Mensch im Mittelpunkt stehen *(Crew Resource Management – CRW)*.

Der Frage, wie ein Mensch als Faktor der Sicherheit in Belastungssituationen „performt" und wie dies durch Training verbessert werden kann, ging Dr. Karl Testor, *Institut für Neurokognition und Führung e.U. (www.i-n-f.at)* aus neurologischer und kommunikationswissenschaftlicher Sicht nach. Moderate Belastung führt zu einer Leistungssteigerung, wogegen bei Überforderung der Aufmerksamkeitspegel sinkt und es vermehrt zu Fehlern kommt. Im Normalfall verarbeitet der Mensch, wie Testor ausführte, drei Wörter pro Sekunde. Die Gegenwartsdauer, solange also das Gehörte im Arbeitsgedächtnis verbleibt, beträgt rund fünf Sekunden. Wird die Informationsmenge überschritten, kommt es zu Ausfällen. Gehörtes wird nicht mehr aufgenommen. In Krisensituationen wird die Gegenwartsdauer reduziert, was bedeutet, dass mit weniger Worten ausgekommen werden muss, um das Denken über die Sprache zu beeinflussen. Die Verkürzung reicht über eine standardisierte Kommunikation bis zur Kommandosprache im militärischen Bereich.

Positive Formulierungen schaffen zielfokussierte Bilder. Verben aktivieren, wogegen Adverbien dämpfen. Wichtig ist, in der Kommunikation gemeinsame Begriffe zu verwenden. Man muss seine eigenen Grenzen kennenlernen, dies aber auch bei anderen, durch Beobachtung des Sprachverhaltens, Auftreten von Ausfällen. Gegenstrategien liegen in Mentaltrainings und Entspannungstechniken wie etwa Combat Breathing sowie Einzel- und Gruppentrainings.

Datenanalyse. Daten sind im Internet im Überfluss vorhanden. Was die Auswertung offener Quellen *(Open Source Intelligence, OSINT)* hergibt, zeigte das Referat von Alexander Oberkersch, BSc, MA, *Sail Labs Technology GmbH (www.sail-labs.com)*. Weitere Quellen sind die H*uman Intelligence (HUMINT)*, bei der auch Bots und Avatare zur Informationsgewinnung eingesetzt werden, die *Measurements and Signatures Intelligence (MASINT)*, die Auswertung von Signalen *(Signals Intelligence, SIGINT)* und die Auswertung von Bildern und Geodaten *(Imagery Intelligence, IMINT)*.

Frei verfügbare Informationen etwa von sozialen Medien (Augenzeugenberichte, Fotos, Videos, Meinungen) liefern ständig die neuesten Informationen. Aktuelle Entwicklungen in Echtzeit zu verfolgen ist unerlässlich, um gezielt reagieren zu können. Dies betrifft nicht nur Nachrichtendienste, sondern auch Hilfsorganisationen oder Unternehmen, die Mitarbeiter ins Ausland entsenden. Es geht um Risikoeinschätzungen in Ländern und um Bedrohungsanalysen, etwa Naturgefahren, Seuchenausbruch, Streiks, öffentliche Meinungen und Stimmungen zu geplanten Vorhaben. Tiefergehende, mit Hilfe künstlicher Intelligenz gewonnene Erkenntnisse ermöglichen, Fake-Meldungen und -kampagnen zu identifizieren. Enorme Datenmengen werden bei militärischen Einsätzen generiert. Die Auswertung ermöglicht eine Rückverfolgung bis zur Identifikation von Soldaten und Ausrüstung.

Aus öffentlich zugänglichen Quellen, einem ins Internet gestellten Video einer Tat, konnte die Exekution einer Frau und ihrer beiden Kinder in einem zentralafrikanischen Staat aufgeklärt werden. Der Ort konnte bestimmt werden durch Vergleich der im Video sichtbaren Bergformationen mit Landschaftsbildern und weiteren Geo-Informationen wie Hütten, Wege und Bäume. Zur Bestimmung der Tatzeit wurde unter anderem die Länge des Schattens des Anführers des Trupps ausgewertet. Einer der Soldaten konnte mit seinem Namen und Foto auf Facebook ausfindig gemacht werden.

Dr. Walter Seböck, Donau Universität Krems *(www.donau-uni.ac.at)*, stellte die vielfältigen Einsatzgebiete von künstlicher Intelligenz dar; die Chancen, eine neue industrielle Revolution einzuleiten, aber auch die Bedrohungen, die sich aus dieser Technologie ergeben. Der Mensch werde zwar als Fehlerquelle aus

FOTOS: KURT HICKISCH

7. D-A-CH-Sicherheitsforum: Reza Ahmari, Susanne Kufeld, Walter Seböck, Kai Pervölz, Hannes Kern, Gottfried Pausch.

dem System genommen. Die dadurch gewonnene Sicherheit bedeute aber auch die Aufgabe der Privatsphäre.

Rechtsanwalt Dr. Ulrich Dieckert machte auf die Bedeutung des Geheimnisschutzes aufmerksam, wie er durch die EU-RL 2016/943 vom 8.6.2016 gefordert wird. Die Umsetzung dieser Richtlinie ist in Österreich durch die UWG-Novelle 2018, BGBl I 2018/109 erfolgt. Geschäftsgeheimnisse sind „angemessen" zu schützen, wobei sich diese Angemessenheit nach den Umständen zu richten hat. Die Maßnahmen können organisatorischer und technischer Art sein und werden sich zum größten Teil mit Anforderungen nach der DSGVO decken. Eine ausdrückliche Bezeichnung als „Geschäftsgeheimnis" ist nicht erforderlich; der Geheimhaltungswille kann sich aus den Umständen ergeben. § 5 GeschGehG sieht Begünstigungen für „Whistleblower" vor.

Risikoanalytik. „Bei der Abschätzung von Folgen neigt das menschliche Denken zu einer linearen oder auch exponenziellen Fortschreibung von Erfahrungswerten; bestätigende Informationen werden bevorzugt", sagte Ass.-Prof. DI Dr. Hannes Kern, Montanuniversität Leoben. Dass die Entwicklung nicht immer in diesen Bestätigungsfeldern verlaufen muss, zeigt sich in der Truthahnillusion: Die von Tag zu Tag steigende Zuversicht des Truthahns, täglich gefüttert zu werden, endet jäh am Thanksgiving Day. Man sollte bei der Beurteilung von Risiken nicht nach Bestätigungen seiner Ansicht suchen, sondern, der Philosophie Karl Poppers folgend, danach trachten, die eigenen Vorstellungen zu widerlegen. Querdenken ist angesagt. Die Non-Success-Stories sind die eigentlich bedeutsamen; Erfolgsgeschichten verzerren die Wahrnehmung. Wichtig ist, was eine Katastrophe verhindert hat.

Das Risiko kann mathematisch als Produkt von Schadenshöhe und Wahrscheinlichkeit des Eintritts dargestellt werden. Während die Auswirkungen eines Schadensereignisses relativ gut eingeschätzt werden können, ist die Wahrscheinlichkeit des tatsächlichen Eintritts ungewiss. Die Risikoanalyse funktioniert gut bei weniger komplexen Systemen und guter Datenlage, verschlechtert sich aber bei sehr komplexen oder chaotischen Systemen sowie bei schlechter Datenlage.

Krisenmanagement. So nützlich Drohnen etwa in der Logistik seien, stellten Drohnen im Luftraum von Flughäfen eine Gefahr dar, sagte Reza Ahmari, Sprecher der Bundespolizei Flughafen Frankfurt. In der Regel würden sie von Piloten der Flugsicherung gemeldet. Die Gefahrenabwehr obliege der Polizei. Es könnten harte Mittel, die zur Zerstörung der Drohne führen, eingesetzt werden (Abschuss), oder weiche wie Störsender. Technisch ausgereift seien die Abwehrsysteme noch nicht. Maßnahmen wie *Geofencing* könnten zwar von vornherein verhindern, dass Drohnen in gesperrte Lufträume eindringen, doch würden Kriminelle diese Systeme wohl außer Betrieb setzen können.

„Bei BASF Ludwigshafen – einem Industriegebiet etwa in der Größe Manhattans – unterscheiden wir nicht zwischen Notfall- und Krisenmanagement", führte Manfred Jilg, Leiter der Standortsicherheit BASF SE, aus. „Die Organisation ist in beiden Fällen gleich." Der Lenkungsausschuss Gefahrenabwehr ist rund um die Uhr in Bereitschaft und innerhalb einer Stunde einsatzbereit. Bei einem Schadensereignis hat nach einer Richtlinie des Konzerns innerhalb der ersten halben Stunde eine Information der Medien zu erfolgen. Die Medien werden von einer bestimmten Person informiert. Die Berichterstattung hat auf gesicherten Erkenntnissen zu beruhen, muss wahr und in der Sprache einfach gehalten sein.

Stephan Hummel und Johannes van Galen, *Currenta (www.chempark.de),* berichteten, dass ihr Konzern ein mobiles Krisenkommunikations-Tool für die schnelle Reaktion bei Ereignissen entwickelt hat. Die Devise lautet: offen, ehrlich, schnell. Es handelt sich um einen Notfall-Navigator für Handys, in dem ein Krisenhandbuch auf Abruf gespeichert ist. Auf der Basis vorbereiteter Textbausteine können verschiedene Meldungstypen erstellt und an die ebenfalls gespeicherten Ansprechpartner und Verteiler versendet werden. Der Versand erfolgt in alle relevanten Kanäle, ohne in Facebook, Twitter, Presseserver usw. wechseln zu müssen.

Auf totale Transparenz setzte auch ein großer Buchhändler in Deutschland, dessen ITK-Systeme im Mai 2019 durch einen Virus-Angriff zusammengebrochen waren. Drei Wochen hindurch konnten von den 70 Filialen weder Bestellungen annehmen noch Bücher ausliefern. Die Kunden wurden durch Pressemitteilungen informiert und laufend über Fortschritte im Wiederaufbau. Innerbetrieblich wurde während der drei Wochen die Erfahrung gemacht, dass die Mitarbeiter wieder miteinander redeten, statt über Mails zu kommunizieren, und dass ein direkter Kundenkontakt entstanden ist. Dies soll, wie Geschäftsführer Christian Riethmüller, berichtete, als „lesson learned" beibehalten werden.

Das 8. D-A-CH Sicherheitsforum Österreich wird vom 17. bis 18. November 2020 wiederum in Going in Tirol abgehalten.

Kurt Hickisch

Fotos: Kurt Hickisch