Foto: Adobe Stock/Gorodenkoff Productions OU

Sicherheit im Unternehmen: Szenarien für die Zukunft entwickeln, um auf Krisen vorbereitet zu sein.

Krisen bewältigen

Beim 6. D-A-CH-Sicherheitsforum Österreich wurde über IT-Krisenfälle berichtet, wie diese überwunden werden konnten und welche Vorkehrungen getroffen werden können.

Die geopolitische Lage sei durch das Austesten eines Ordnungssystems zwischen drei großen Machtblöcken gekennzeichnet, sagte Dr. Gunther Schmid, emeritierter Professor für internationale Politik und Sicherheit an der Beamtenhochschule München/Berlin beim *6. D-A-CH-Sicherheitsforum,* das am 20. und 21. November 2018 in Going/Tirol, stattfand. Die drei Blöcke würden zwar über Macht, aber noch nicht über ausreichend Gestaltungsmacht verfügen. Diese Situation könnte zu einem Erstarken Europas führen. Europa werde durch sein Wirtschafts- und Gesellschaftssystem in den nächsten 30 Jahren weiterhin eine Magnetwirkung für Migrationsströme aus Afrika ausüben. 2050 werde Afrika eine Bevölkerung von 2,5 Milliarden vorwiegend junger Menschen und die EU eine solche von 450 Millionen, vorwiegend älteren Menschen haben. Derzeit würden sich 90 Prozent der Migrationsströme noch innerhalb Afrikas abspielen.

„Zur Bewältigung der Zukunft müssen wir in Zukünften denken und für jede davon Szenarien entwickeln", führte Dr. Bernhard Richter, FH Campus Wien, aus und stellte in der Folge methodische Lösungsansätze vor. Es gelte, komplexe Zusammenhänge zu verstehen und auszunutzen. Die Strategien und Handlungsoptionen orientieren sich entweder an einem (fokussierte Strategie – eher selten) oder an mehreren Szenarien (zukunftsrobuste Strategie). Erst dann sei man auf nicht in geradlinig verlaufende Entwicklungen vorbereitet.

Bewältigung von IT-Krisen. Am 27. Juni 2017 wurden mit dem Verschlüsselungstrojaner (Ransomware) *NotPetya* neben anderen großen Unternehmen Computer der Reederei *Maersk* infiziert, über die 20 Prozent des weltweiten Containerhandels abgewickelt werden. Thomas Boye Dyregaard, Leiter der Unternehmenssicherheit und des Krisenmanagements des dänischen Unternehmens, berichtete, dass die Schadsoftware über eine ukrainische Buchhaltungssoftware in die Rechner gelangt sei. 49.000 Laptops waren betroffen, die Drucker funktionierten nicht mehr. Auf 1.200 Anwenderprogramme konnte nicht mehr

zugegriffen werden, 1.000 waren zerstört. Die Anstrengungen, die Systeme wieder herzustellen, waren enorm. Die Kommunikation mit Kunden, den Mitarbeitern und den Medien erfolgte über soziale Medien. Der Schaden in Höhe von etwa 250 bis 300 Millionen US-Dollar entstand durch Verluste an Einnahmen, durch den Zukauf von Ersatz-Frachtkapazität und den Neuaufbau der IT, der nach zehn Tagen abgeschlossen war.

Durch den Erpressungstrojaner *Wannacry* wurden am 13. Mai 2017 auf Rechnern in rund 150 Ländern Daten verschlüsselt, wobei in Deutschland besonders die *Deutsche Bahn* betroffen war. Die *Innogy SE (www.innogy.com),* einer der größten Stromanbieter in Deutschland mit 23 Millionen Kunden und mehr als 40.000 Mitarbeitern, nahm diesen Vorfall zum Anlass, Abwehrstrategien zu entwickeln, über die Boris Beuster berichtete. Die Energiewirtschaft in Deutschland tauscht sich in Foren aus, in Partnerschaft mit den Behörden. Das Thema Cybersecurity wurde strategisch im Top-Management positioniert. Zur besseren Sensibilisierung der Mitarbeiter wurde ein Trainingszentrum für den Umgang mit Hacker-Attacken aufgebaut. In die Ausbildung wurden Elemente der Gamification eingebaut. Beim Brett-Spiel *What the Hack!* treten Hacker und Administrator, auch als Team, gegeneinander an. Für das Management finden Krisenstabsübungen statt.

Das von *Innogy* entwickelte *Cybersecurity-Maturity-Cockpit (CSMC)* misst den Reife- und Wirkungsgrad sowie das Kosten-/Nutzenverhältnis der Cyber-Sicherheitsmaßnahmen. Für diese Entwicklung wurde das Unternehmen auf der Sicherheitsmesse *Security* in Essen in der Kategorie *Cybersecurity/Wirtschaftsschutz* mit dem *Security-Innovation-Award 2018* in Gold ausgezeichnet.

Veranstalter Rainer von zur Mühlen (Simedia Akademie).

Gamification wurde auch bei der *Deutschen Post DHL-Group* zur Heranbildung einer *Security Culture* im Unternehmen eingesetzt, berichtete Christiane Hirsch von der Konzernsicherheit. Das Logistik-Unternehmen beschäftigt weltweit mehr als 520.000 Mitarbeiter, davon 1.000 in der Security. Corporate Security wird als Business-Enabler und Teil der Wertschöpfungskette angesehen. Die Konzernsicherheit ist der Ansprechpartner für alle sicherheitsrelevanten Themen im Unternehmen. Zur Steigerung des Sicherheitsbewusstseins wurde zunächst ein globaler Event mit einprägsamen Bildern und Postern gestartet, wobei auf die kulturellen Eigenheiten insbesondere des asiatischen Raumes Rücksicht zu nehmen war. Im Lauf der Jahre folgten Gewinnspiele und die Einführung eines *Security-Awards*. Eine Lunchtour wurde entwickelt, bei der Situationen wie Kontaktaufnahme, Erpressung, Social Engineering durchgespielt wurden. Bei *Security Games* wurden den Gewinnern die Preise von Mitgliedern des Vorstand überreicht. In eine globale Kommunikationskampagne *(Security-Week),* verbunden mit einem globalen Quiz, wurde auch der Vorstand eingebunden.

Medienarbeit. „Medien bestimmen das Krisenausmaß, wobei die medial aufgebauschte Krise größer sein kann als die tatsächliche", sagte Reza Ahmari, Pressesprecher der Bundespolizei Flughafen Frankfurt/Main. Krisenkommunikation sei eine wichtige Disziplin in den Chefetagen. Medien selektieren Nachrichten, man muss wissen, wie Medien „ticken". Als betroffenes Unternehmen sollte man ehrlich an die Öffentlichkeit treten, unter Rücksichtnahme auf potenziell involvierte Stakeholder (Kunden, Fachöffentlichkeit, Blogger, NGOs). Twitter sei ein geeignetes Instrument zur Kommunikation. Mit Desinformation werde zu rechnen sein. Auf keinen Fall dürfe es zu Angriffen auf die Medien kommen. Ähnliche „Todsünden" seien zu lügen, zu vertuschen, vorzuschreiben, was berichtet werden solle, Medien pauschal zu verdächtigen und Versuche, die Informationsfreiheit einzuschränken.

Red-Teams. „Denken wie der Feind" – so beschrieb Andreas Radelbauer, *Corporate Trust (www.corporate-trust.at),* die Arbeitsweise von *Red-Teams,* die im Auftrag eines Unternehmens in dieses eindringen – mit dem Ziel, Schwachstellen aufzuspüren. Es werden jene Mittel eingesetzt, deren sich auch Nachrichtendienste, organisierte Kriminalität, Konkurrenz, Hacker, Terroristen, aber auch Innentäter, die Konkurrenz oder Lieferanten bedienen. Es werden frei zugängliche Quellen wie *Google, SpiderFoot* und *Shodan* ausgewertet, Recherchen über Personen angestellt oder elektronische Auswertungen vorgenommen. Geprüft wird, wie leicht man sich physisch in ein Unternehmen einschleichen kann, um dort Lausch- und Spähgeräte einzubringen oder in die IT einzudringen. Wie angreifbar ist die Haus- und Gebäudetechnik? Gibt es Zugänge über ungeschützte IP-Adressen? Wie leicht ist es, mit Mitarbeitern in Kontakt zu treten (Kantinenge-

6. D-A-CH-TAGUNG

Sicherheitsforum

Zum 6. Mal wurde am 20. und 21. November 2018 das *D-A-CH-Sicherheitsforum Österreich* in Tirol abgehalten, veranstaltet von der *Simedia-Akademie GmbH,* Bonn. Die 80 Teilnehmer waren großteils Sicherheitsbeauftragter großer Unternehmen. Großer Wert wurde vom Veranstalter darauf gelegt, dass die Teilnehmer im Sinn eines Netzwerkens untereinander ins Gespräch kommen und wechselseitig Erfahrungen austauschen.

www.simedia.de

FOTO: KURT HICKISCH

Referenten beim 6. D-A-CH-Sicherheitsforum, das am 20. und 21. November 2018 in Going (Tirol): Gunther Schmid, Andreas Radelbauer, Felix Juhl, Christiane Hirsch, Bernhard Richter und Reza Ahmari.

spräche) und von ihnen Informationen abzuschöpfen *(Social Engineering)*? Nicht angewendet werden Abhörtechniken (Telekommunikation, Richtmikrofone), das Scannen von Funkfrequenzen, das Infizieren von Rechnern und Netzwerken, Einbringen von Lauschmitteln, Erpressen oder Nötigen von Personen.

Die Ergebnisse der Recherchen werden in einem *Scoring Report* zusammengefasst, der die Gefährdungslage des Unternehmens darstellt. Weiters werden Empfehlungen zur Beseitigung der festgestellten Mängel gegeben. Laufendes Controlling soll zu einem kontinuierlichen Verbesserungsprozess führen.

Desinformation. Über Bedrohungen durch Fake-News, Manipulation und Propaganda referierte Felix Juhl, leitender Direktor der schweizerischen *Fachstelle für Ermittlungsunterstützung und Begutachtung IT-Kriminalität (FEBIT; www.febit.ch)*. „Menschliches Denken ist fehlertolerant", betonte Juhl. Kurzzeitig projizierte Sätze mit jeweils einer Wortverdoppelung wurden von den Teilnehmern dem Sinn nach wiedergegeben. Nachgefragt war aber, wie der tatsächliche Wortlaut war. Diese Fehlertoleranz ermöglicht es zwar, Wichtiges von Unwichtigem zu trennen, verringert aber andererseits die Fähigkeit zur Trennung von Wahrem und Falschem. Das macht Beeinflussung möglich. Dinge, die falsch sind, werden als wahr gedacht. „Desinformation ist die neue Bedrohung."

Juhl fächerte den Begriff des maschinellen Denkens in *KI, ML* und *DL* auf. *Künstliche Intelligenz (KI)* ähnelt dem Vorgang, einem Schüler genau die Information zu vermitteln, die er lernen soll. Ein Schachroboter hat trotz seiner imponierenden Rechenleistung nur eine marginale KI insofern, als alle Züge, die er setzt, vorher schon gezogen wurden. Er schöpft lediglich aus dem großen Reservoir von Spielvarianten. Beim *Maschinellen Lernen (ML)* erarbeitet ein Schüler sich den Lehrstoff selbst. Bestehendes Wissen wird mit neuem gemischt. *Deep Learning (DL)* geht nach dieser Definition über das maschinelle Lernen insofern hinaus, als der Schüler in der Lage ist, aus seinen Fehlern zu lernen und sich kontinuierlich zu verbessern.

Man kann einem Rechner beibringen, *Captchas* zu verstehen. *Captchas* sind bildhafte Darstellungen, die sicherstellen sollen, dass ein Mensch und nicht eine Maschine (Roboterprogramm) einen Computer bedient und Handlungen setzt. Es muss eine für Menschen einfache Aufgabe gelöst werden, etwa, dass Buchstaben oder Ziffern verzerrt dargestellt werden oder Bildinhalte erkannt werden müssen. Mit *Re-Captcha* kann diese Hürde übersprungen werden. Das Programm erkennt beispielsweise bei einem Bild alle Quadrate, die bestimmte, nachgefragte Inhalte aufweisen, wie etwa Straßenverkehrszeichen.

Das Programm *Libertatus* hatte im Wettkampf mit den besten Pokerspielern nicht nur dieses Spiel, sondern auch die Strategien der Spieler einschließlich bluffen erlernt, dann zwei Monate gegen sich selbst gepokert und ist nun der weltbeste Pokerspieler. *Duplex,* die Sprach-KI von *Google,* kann auf Fragen antworten und etwa – wie bereits praktisch vorgeführt – bei Telefonanruf einen Termin beim Friseur vereinbaren, und wird Call-Center ersetzen können. Je größer die Wissensbasis, desto leichter wird die Verständigung. Es wird möglich werden, Nachrichten so umzuformulieren, dass sie anderen Kulturkreisen entsprechen und von diesen akzeptiert werden.

„Denken ist ein Prozess, der in der Evolution in einer Situation das Überleben gesichert hat", sagte Juhl. „Auch die Lüge ist ein Zeichen von Intelligenz. Jede Art von Information kann ein trojanisches Pferd sein."

„Sockenpuppen", Maschinenprogramme, die gesteuert Informationen verbreiten, lassen sich nicht oder nur mehr schwer von menschlichen Teilnehmern eines Chats unterscheiden. *Dark Posts* richten sich nur an bestimmte Internet-Gruppen. Die Posts verschwinden wieder; man weiß nicht mehr, woher man die Information hat. Gesichter können erkannt und verändert werden. Mit *Deep Fakes,* künstlichen neuronalen Netzwerken, können falsche, aber täuschend ähnliche Bilder oder Videos automatisiert erzeugt werden. Man kann nicht mehr sicher sein, dass eine dargestellte Person tatsächlich die ist, als die sie sich ausgibt. „Die Wahrheit fängt an zu verschwimmen", sagte Juhl. Es hat sich ein *Deception-Management* entwickelt, das in der Lage ist, etwa durch Beeinflussung von Wählern in Weltgeschehnisse einzugreifen. Die Psychometrie ist in der Lage, eine Persönlichkeit zu vermessen. Mussten früher etwa 200 Parameter einer Person bekannt sein, reichen heute bereits 15 Merkmale, um eine Person etwa nach politischen Präferenzen einzustufen. Und Material gibt es genug, Lebensläufe, ausgefüllte Fragebögen, Postings.

Als Gegenmaßnahme rät Juhl, sich umzusehen und frühzeitig zu reagieren. Eine Kaffeehauskette hatte bei verspäteter Reaktion Wochen gebraucht, dem Gerücht zu begegnen, jeder Migrant würde dort kostenlos eine Tasse Kaffe bekommen, was einerseits heftig akklamiert, andererseits ebenso heftig abgelehnt wurde. Man müsse die sozialen Medien im Blick haben und sie monitoren, um Entwicklungen frühzeitig zu erkennen.

Kurt Hickisch

FOTOS: KURT HICKISCH