Ein Cyber-Angriff könnte die Versorgungssicherheit im Bereich der elektrischen Energie gefährden.

Cyber-Angriffe: Angriffsmöglichkeiten werden unter anderem durch Programmierfehler geschaffen.

Krisen und Gefahren

Von Migration über Cyber-Angriffe bis zu Krisenmanagement und Krisenkommunikation spannte sich der Bogen der Vorträge beim 5. D-A-CH-Sicherheitsforum Österreich.

In den arabischen Staaten leben 5 Prozent der Weltbevölkerung, aber es ereigneten sich dort 45 Prozent aller Terroranschläge. 47 Prozent aller Binnenflüchtlinge leben in diesen Ländern. Die Bevölkerung wächst rasch. Sie weist einen überproportionalen Anteil an Jugendlichen auf, die aber kaum Zukunftsperspektiven haben. So sind im Irak 60 Prozent der Bevölkerung unter 24 Jahren alt.

Kinder würden als Altersversorgung angesehen, weil die sozialen Systeme nicht funktionierten. Die Unzufriedenheit, die sich durch wahrgenommene Korruption verstärke, richte sich gegen die herrschenden Eliten, referierte Arabien-Experte Dr. Wilfried Buchta beim 5. *D-A-CH-Sicherheitsforum,* das am 21. und 22. November 2017 im Stanglwirt in Going/Tirol stattfand. Veranstalter waren die *Simedia Akademie* und die *FH Campus Wien*.

Die nach dem Zerfall des Osmanischen Reiches nach dem 1. Weltkrieg durch die Großmächte vorgenommene territoriale Neugliederung habe auf die ethnischen und religiösen Gruppierungen kaum Rücksicht genommen, betonte Buchta. Innerhalb der damals gezogenen geografischen Grenzen habe sich durch die Vielfalt der Gruppierungen keine nationale Identität entwickelt. Ein Großteil dieser Staaten sei instabil.

Unzufriedenheit und Perspektivlosigkeit seien auch die Wurzeln der Organisation *Islamischer Staat (IS),* die, zunächst auf den Irak beschränkt, 2014 ein Kalifat ausrief. Trotz der mittlerweile erfolgten Zerschlagung des *IS*-„Staatsgebiets" seien die Kommandostrukturen noch erhalten und der *IS* noch operationsfähig. Die meisten Ableger des *IS* seien weiterhin aktiv. Opfer des islamistischen Terrors seien zumeist Muslime selbst, Polizei, Militär, Regierungsvertreter, aber auch Wirtschaftsvertreter.

Oberst Gerald Tatzgern, Leiter der Zentralstelle im Innenministerium zur Bekämpfung der Schlepperkriminalität, wies auf den raschen Bevölkerungszuwachs in Afrika hin. Bis 2050 werde sich dort die Bevölkerung von derzeit über 1,2 Milliarden Menschen auf 2,5 Milliarden verdoppelt haben. Für Afrikaner sei Europa das „neue Amerika". Nach Schätzungen unter anderem von Europol seien 2016 durch Schlepperei zwischen 6 und 9 Milliarden Euro „erwirtschaftet" worden. Die Ermittler arbeiten bei der Bekämpfung und Verhinderung der Schlepperei mit den Herkunfts- und Transitländern zusammen; die kriminalistischen Methoden wurden verbessert. Selbst für einen Massenandrang von Migranten, ähnlich der Flüchtlingswelle vom September 2015, seien entsprechende Vorbereitungen getroffen worden, sagte Tatzgern.

Gerald Tatzgern: „Für Afrikaner ist Europa das neue Amerika."

Schutz von Mitarbeitern. Die *Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ; www.giz.de),* ein gemeinnütziges Bundesunternehmen, leistet Entwicklungshilfe und unterstützt deutsche Unternehmen, Behörden und internationale Organisationen bei Tätigkeiten im Ausland. Die knapp 20.000 Beschäftigten sind zum Großteil als nationales Personal in den rund 120 Ländern tätig, zu denen die *GIZ* Verbindungen hat. In etwa 40 Ländern gibt es hauptamtliche Berater, und in 5 Ländern rund um die Uhr erreichbare Einsatzstellen.

„Der Schutz von Mitarbeitern in Krisengebieten hat höchste Priorität und liegt im ureigensten Geschäftsinteresse", sagte Matthias Wagner, Gruppenleiter Sicherheitsrisiko und Krisenmanagement der *GIZ*. Wenn das Risiko zu hoch ist, wird ein Auftrag nicht angenommen. Den Arbeitgeber trifft eine Fürsorgepflicht, die über die Arbeitsschutzgesetze hinausgeht. Mitarbeiter müssen über die Sicherheitslage in den Gebieten, in die sie entsendet werden, informiert werden, und es ist zu dokumentieren, was für den Fall von Anschlägen vorgesorgt wurde. Die Verantwortlichkeit schließt auch die mitreisenden Familienangehörigen ein, die ein

Fotos: F8studio/Fotolia, Kurt Hickisch, Utamaria/Fotolia

Sicherheitsbriefing erhalten. Vor dem Einsatz eines Mitarbeiters wird erhoben, ob er bereits Erfahrung in Krisengebieten gesammelt hat. Weiters erfolgen eine Prüfung der körperlichen und psychischen Verfassung, ein Sicherheitstraining und eine umfassende, dokumentierte Aufklärung über Risiken. Der Risk Advisor evaluiert Gebäude nach Sicherheitsgesichtspunkten, gibt Handlungsanweisungen. Kommunikationswege werden festgelegt, auch zwischen den Fahrzeugen untereinander, verbunden mit Fahrzeugortung.

Während des Einsatzes geht es hauptsächlich um Schutzmaßnahmen vor Ort, Betreuung und medizinische Unterstützung. Bei Ereignissen liegt die Entscheidungsbefugnis beim *Krisenmanagement-Team (KMT)*. Die Erstbetreuung am und Bergung vom Unfallort erfolgt mit unmittelbar zur Verfügung stehenden Transportmitteln (CasEvac – Casuality Evacuation), an die sich die Verbringung in qualifizierte medizinische Versorgung (MedEvac – Medical Evacuation) anschließt. Nach dem Einsatz werden Rückkehrhilfe, ärztliche und psychologische Unterstützung sowie Maßnahmen zur Reintegration geboten. Die Beurteilung des Sicherheitsrisikos erfolgt nach *ISO 31000* ff. Im Rahmen einer Sicherheitsrisikobewertung werden die dort aufgelisteten 180 möglichen Gefahren vor Ort nach Eintrittswahrscheinlichkeit und Schadenshöhe gewichtet. Die Eintrittswahrscheinlichkeit wird von jedem Mitarbeiter selbst bewertet; daraus wird ein Mittelwert gebildet. Die Bewertung des Schadensausmaßes erfolgt durch Sicherheitsexperten.

Terror und Amok. Nach den Erkenntnissen, die der Expertenkreis Amok, Baden-Württemberg, aus dem Amoklauf in Winnenden gewonnen hat, sind Amoktaten dadurch gekennzeichnet, dass der Täter versucht, in kürzester Zeit möglichst viele Menschen zu töten oder zu verletzen. Nicht selten dauern Amoktaten nur wenige Minuten. Die Täter haben einen absoluten Tötungswillen, sie zerstören bis zur eigenen Erschöpfung, bis zum geplanten Suizid oder bis zur Intervention der Polizei. Eine freiwillige Aufgabe ist selten. Empathie des Täters gegenüber Opfern ist nicht zu erwarten. Diese Charakterisierung sei auf terroristische Angriffe übertragbar, sagte Torsten Hiermann *(Crise Consult)*. Aus taktisch-operativer

Timo Kob: „Der Wirtschaftsgrundschutz deckt die Bereiche Mensch, Infrastruktur und Prozesse ab.“

Michael Meier: „Cyber-Angriffe können automatisiert und gegen mehrere Opfer geführt werden.“

Marcus Beyer: „Das Risiko in einem Unternehmen sitzt 50 cm vor dem Bildschirm.“

Matthias Wagner: „Der Schutz von Mitarbeitern in Krisengebieten hat höchste Priorität.“

Sicht seien die wissenschaftlichen Definitionen von Amok und Terrorlage zunächst nebensächlich. Der Unterschied liege im Wesentlichen im Motiv, während die Tatausübung ähnlich erfolgen könne. In beiden Fällen komme es zwangsläufig zu einer „Polizeilage“.

Der erste Impuls von Betroffenen werde sein zu flüchten *(run)*. Anders als bei einem Brand wird dieses Verhalten vom Expertenkreis nur bei günstiger Gelegenheit angeraten, etwa, um die nächste Deckung aufzusuchen. Sollten mehrere Täter agieren, bestehe die Gefahr, einem anderen in die Hände zu laufen.

Bei Anschlägen mit Sprengmitteln sei es wegen der Gefahr des „Second hits“ wichtig, nicht zum Ort des Anschlags zurückzukehren *(clear the scene)*. Um Missverständnisse gegenüber anrückenden Einsatzkräften zu vermeiden, sollte man diesen gegenüber die Hände mit gespreizten Fingern langsam erheben.

Die im Amokfall auch vom Expertenkreis empfohlene Verhaltensweise ist es, sich zu verbergen *(hide)*, entweder in der Form, sich dem Blick des Täters zu entziehen *(conceal)* oder ballistische Deckung zu suchen *(cover)*. Dazu zählt, sich in einem Raum einzuschließen und sich zu verbarrikadieren. Von der Türe entfernen, auf den Boden legen, Deckung suchen, ruhig verhalten, Mobiltelefon lautlos stellen. Bei einem Kraftfahrzeug Deckung hinter dem Motorblock nehmen. Die Karosserie allein bietet zu wenig Schutz und kann durchschossen werden. Letzte Maßnahme ist, den Täter zu bekämpfen *(fight)* und ihn von seiner Waffe zu trennen.

Gegen alle Eventualfälle wird man nicht Vorkehrungen treffen können. Sinnvolle Erstmaßnahmen sind, die Polizei zu informieren, Amokalarm auszulösen, betroffene Gebäude zu sichern, Areal für Polizeikräfte bereit zu halten und diese einzuweisen. Als interne Alarmierung kann vorgesehen werden, Pop-up-Fenster mit entsprechender Meldung über alle Bildschirmfenster zu legen. Wegen der Gefahr eines Innentäters sollten die für einen Amokfall getroffenen Maßnahmen nur einem kleinen Kreis zugänglich sein.

Cyber-Angriffe. Prof. Dr. Michael Meier, Institut für Informatik an der Universität Bonn und Leiter der Abteilung *Cyber-Security bei Fraunhofer FKIE,* verglich Probleme der Sicherheit in der Informationstechnologie mit jenen der realen Welt: Auch in ein Haus oder eine Wohnung kann eingebrochen werden, weil die Haustüre zu schwach ist, die Fenster leicht zu überwinden sind oder Schlüssel verloren gehen. Zusätzliche Sicherheitsmaßnahmen wie eine Alarmanlage oder ein Wachdienst müssten getroffen werden.

In der digitalen Welt treten die Probleme verstärkt auf. Die erforderlichen Fähigkeiten und Mittel zur Durchführung von Einbrüchen und Angriffen sind einfach kopier- und vervielfältigbar. Angriffe können automatisiert und gleichzeitig gegen mehrere Opfer geführt werden. Zudem ist das Risiko für den Täter, zur Verantwortung gezogen zu werden, in der digitalen Welt um ein Vielfaches geringer als in der realen Welt.

Angriffsmöglichkeiten werden unter anderem durch Programmierfehler geschaffen, etwa dadurch, dass Befehle in den ansonsten abgeschotteten Bereich der Daten transportiert werden können *(Code-Injection)*. Im Schnitt müssten bei 1.000 Zeilen Programmcode mit einem bis zu drei Programmierfehlern gerechnet werden, die in Teilmengen sicherheitskritisch seien. Betriebssysteme

FOTOS: KURT HICKISCH

Schul-Shooting in Florida: Täter haben bei Amok- und Terrorlagen ähnliche Ziele, aber unterschiedliche Motive.

Foto: Ian Witlen/Zuma/Picturedesk.com

für einen PC enthalten etwa 50 Millionen *Lines of Code (LoC);* die Software moderner Autos etwa 100 Millionen LoC. Selbst in einer Welt ohne Programmierfehler sind erfolgreiche Angriffe möglich, wie Meier am Beispiel möglicher Angriffstechnologien aufzeigte. Entweder werden, wie beim Schadprogramm Rowhammer, elektromagnetische Interaktionen zwischen benachbarten Speicherzellen im Chip ausgenützt, Datenpakete injiziert *(Man-on-the-Side" – MOTS-Angriff)* oder das Internet-Routing manipuliert *(Quantum Insert)*. DDos-Angriffe werden über Verstärker, ähnlich den Boostern in der Unterhaltungselektronik, durchgeführt. Zusätzliche Schutz-Software erhöht zwar den Schutz, bietet aber durch ihre Komplexität mehr Angriffsfläche. Letztlich muss auch der Faktor Mensch in die IT-Sicherheitsbewertung einbezogen werden. Mit dem Forschungsprojekt *IT-Sicherheits-Awareness Penetration Testing (ITS.APT)* sollen Methoden zur Messung des IT-Sicherheitsbewusstseins erarbeitet und der Einfluss dieses Bewusstseins auf den Erfolg von Angriffen bewertet werden.

Bewusstseinsbildung. Für Marcus Beyer, *Resilient Workforce NCEE,* sitzt das Risiko „50 cm vor dem Bildschirm". Sicherheitsdefizite in Unternehmen seien zu etwa 70 Prozent auf fehlendes Bewusstsein der Mitarbeiter zurückzuführen. Mit Wissen vermitteln und Lernen könne zwar eine bewusste Kompetenz erworben werden, die allerdings nur kurz anhalte. Ziel müsse ein sicheres Verhalten als unbewusste Kompetenz sein, was sich entwickeln müsse und Zeit brauche. *AskitMeta* ist ein Moderationstool, mit dem in Workshops mit Elementen der Gamification Inhalte der Informationssicherheit vermittelt werden könnten.

Der Fortschritt der Bewusstseinsbildung kann in Beobachtungen verfolgt werden. Als quantitative Methoden nannte Beyer unter anderem die *TWISK*-Methode von Thomas Schlienger *(www.treesolution.ch)* und das *Security Awareness Monitoring* nach Prof. Dr. Zerr vom Steinbeis-Beratungszentrum *(www.steinbeis.de)*.

Über Messungen anderer Art, nämlich zur Ermittlung von Kennzahlen zu Kostentransparenz und -vergleich, berichtete Karl Rengstorf, Leiter Sicherheitsmanagement *Schott AG*. 12 Unternehmen mit insgesamt 27 Standorten haben sich zu einem Benchmarking jeweils für Brand- und Werkschutz zusammengefunden. Unter neutraler Koordinierung durch die Bauakademie werden Kennzahlen, die unter vergleichbaren Rahmenbedingungen ermittelt wurden, in Workshops untereinander ausgetauscht mit dem Ziel, der Ursache von Unterschieden nachzugehen, Optimierungspotenziale zu erkennen und vom Besseren zu lernen *(Benchlearning; https://benchlearning.de)*. Voraussetzung für die Vergleichbarkeit ist, dass die jeweiligen Basisleistungen von allen erbracht und detailliert dargestellt werden. Sowohl beim Werkschutz als auch bei der Werksfeuerwehr wurden 162 Kennzahlen ermittelt. Das Grundprinzip lässt sich auf andere Bereiche umlegen und ausweiten.

Wirtschaftsschutz. Ein Cyber-Angriff könnte die Versorgungssicherheit im Bereich der elektrischen Energie gefährden, sagte Dr.-Ing. Bernd Calaminus, *EnBW AG*. Dabei reichen schon

Auslandseinsatz: Mitarbeiter müssen über die Sicherheitslage in den Gebieten informiert werden, in die sie entsendet werden.

Naturereignisse wie Eisregen, Windhosen oder Starkregen mit Schlammlawinen aus, um Strommasten zu verdrehen oder zu knicken, dass es zu großflächigen Stromausfällen kommt. Das Problem ist, dass Last und Erzeugung zu jeder Sekunde ausgeglichen sein müssen. Ist das nicht der Fall, kommt es zu automatischen Abschaltungen.

Ehe es zu einer Verbraucherabschaltung kommt, gibt es eine Reihe anderer, weniger eingriffsintensiver Maßnahmen. Die zu ergreifenden Maßnahmen werden und wurden geübt, beispielsweise in großem Rahmen bei der Krisenübung „Blackout" 2017.

Für den IT-Bereich gibt es als Maßnahmenkatalog, der Gefahren entgegenwirken soll, den Grundschutz des *BSI*. Als Ergänzung dazu wurde der Wirtschaftsgrundschutz entwickelt *(www.wirtschaftsschutz.info),* über den Prof. Timo Kob berichtete. Er deckt, dem Schema des Grundschutzhandbuches mit Bausteinen und Maßnahmen folgend, die Bereiche Mensch, Infrastruktur und Prozesse ab. Als zweite Säule zum IT-Grundschutz ergibt sich ein ganzheitlicher Schutz von Werten und ein einheitliches Sicherheitsniveau.

Mit den Auswirkungen der Digitalisierung und künstlicher Intelligenz auf die Unternehmenssicherheit befasste sich Wolf-Rüdiger Moritz, *Infineon Technologies AG*. Herbert Unger setzte sich aus Sicht eines investigativen Journalisten und der Big-Data-Problematik mit den in Österreich bestehenden über 70 Datenregistern *(www.digitales.oesterreich.gv.at/register)* auseinander.

Krisenkommunikation. Oberst Mag. Michael Bauer, Pressesprecher im Bundesministerium für Landesverteidigung, berichtete über die Lehren, die das Bundesheer aus einem Vorfall im Jänner 2009 gezogen hat. In einem Nebel, der sich durch das Zünden einer Nebelgranate gebildet und sich auf die A 22 ausgeweitet hatte, war bei einer Massenkarambolage eine Frau ums Leben gekommen. Die Öffentlichkeitsarbeit des Bundesheeres wurde als zu spät (erste Aussendung erst nach zwei Tagen), unkoordiniert (13 Sprecher) und unzureichend kritisiert. Daraufhin wurde Vorsorge getroffen, dass bei ähnlichen Vorfällen (schwere Unfälle von Heeresangehörigen; Vorfälle bei Auslandseinsätzen; Zivilisten durch Bundesheer getötet oder verletzt) die erste Pressemeldung innerhalb einer Stunde erfolgt. Mythenbildung wird durch Fakten und Transparenz begegnet. Nur einer spricht und jede Aussage muss richtig und beweisbar sein. Die Hotline wird auf den Sprecher umgeleitet, die jeweilige Bezugsperson muss sofort und durchgehend ansprechbar sein. Gegebenenfalls muss ein kontrollierter Zugang zur Unfallstelle ermöglicht werden.

Das Krisenstatement muss nicht nur Mitgefühl zum Ausdruck bringen, sondern auch die Fragen wer, was, wann, wie, wo klären sowie, was funktioniert hat und wie es weitergeht. Im Krisenstab werden Aufgaben verteilt, wer was zu recherchieren hat, auch im weiteren Umfeld des Ereignisses. Die Ergebnisse werden auf Flipcharts festgehalten, die sich im Blickfeld des Sprechers befinden. Dieser ist dadurch über Ermittlungsergebnisse informiert, die für den eigentlichen Vorfall eher von peripherer Bedeutung, dennoch aber für Medien von Interesse sind.

Das nächste *D-A-CH-Sicherheitsforum* wird vom 20. bis 21. November 2018 wiederum in Going abgehalten.

Kurt Hickisch

FOTO: VERONIKA TSCHERNEY-CZAAK