Effizientes Krisenmanagement

Krisen und ihre Bewältigung standen im Mittelpunkt des länderübergreifenden 3. D/A/CH-Sicherheitsforums der Simedia Akademie am 18. und 19. November 2015 in Going in Tirol.

Als „Welt ohne Weltordnung“ mit einem Ende der Berechenbarkeit der Politik bezeichnete Prof. Dr. Gunther Schmid, früher Referent für internationale Politik und Sicherheit beim deutschen Bundesnachrichtendienst (BND), den derzeitigen Zustand der Welt. Schmid war einer der Referenten beim *3. DACH-Sicherheitsforum* am 18. und 19. November 2015 im *Biohotel Stanglwirt* in Going in Tirol. Am Ende der Periode relativ stabiler Ordnung seit 1945 scheine nunmehr das „Age of Riots“ zu stehen, mit einem beschleunigten Machtzerfall in vielen Staaten, betonte Schmid. Mehr als ein Drittel der der UNO angehörenden Staaten seien entweder scheiternde Staaten oder schon gescheitert; ein Drittel der Fläche Afrikas befinde sich im Zerfall. Regionale Ordnungen würden ebenso zerfallen.

Globalisieren werde sich als totalitäres und expansives Projekt der islamistische Terrorismus, mit dem Ziel der Überwindung der Nationalstaaten und der Zerstörung der offenen Gesellschaften. Geopolitik im Sinne einer gewaltsamen Änderung von Grenzen lebe wieder auf (Ukraine, südchinesisches Meer). Das Gewicht der Weltwirtschaft werde sich auf die BRICS-Staaten (Brasilien, Russland, Indien, China und Südafrika) verschieben. Im Jahr 2030 würden fünf Milliarden Menschen zur globalen Mittelschicht gehören, zwei Drittel davon Asiaten. Um diese neuen Länder werde man sich kümmern müssen.

Festzustellen sei ein Rückzug der Demokratien und eine Wiederkehr nicht demokratischer Herrschaftssysteme wie Clans, Sekten, Kalifate. Autoritäre Staaten und westliche Demokratien würden als Modelle miteinander in Konkurrenz stehen. Krisen würden zur Lebensform. Das Migrationsproblem treffe auf nervöse Gesellschaften. Zu fürchten sei die „Angst vor der Angst“. Sicherheitsverantwortliche müssten strategisch über das Tagesgeschäft hinaus denken und auch Krisen in ihre Überlegungen einbeziehen.

Notstromaggregate: Ein Problem ist das Ausflocken des Biodiesels, der dem Dieselkraftstoff beigemengt ist.

FOTO: WERNER SABITZER

SIMEDIA

Veranstaltungen

Seit über 20 Jahren veranstaltet die *Simedia GmbH* (seit Dezember 2015: *Simedia Akademie*) Kongresse, Foren, Seminare und Netzwerktreffen zu Sicherheitsthemen, praxisbezogen und produktneutral.

Einige Lehrgänge können mit einem Zertifikat durch den *Bundesverband unabhängiger deutscher Sicherheitsberater und -ingenieure e. V.* abgeschlossen werden. Der Zertifikatslehrgang *Security-Engineer, BdSI* umfasst drei Module zur Objektsicherheit (Modul I: Perimeterschutz, Außenhautsicherung, Einbruch- und Brandmeldetechnik, Modul II: Zutrittskontroll- und Berechtigungsmanagement; Modul III: Videotechnik und Sicherheitsmanagement), weiters Multifunktionale Türenplanung; technischer und baulicher Brandschutz sowie homogene Sicherheitskonzepte. Die Absolventen können durch eine Kooperation mit der Hochschule Furtwangen einen hochschulqualifizierten Abschluss mit dem Titel *Certified Security-Engineer, HFU* erwerben. Dazu muss noch ein eintägiges Aufbauseminar besucht und eine Hausarbeit erstellt werden. Das erste Aufbauseminar findet am 5. Juli 2016 statt.

www.simedia.de
www.bdsi-ev.de

Blackout. „Eine Krise kann auch durch einen europaweiten Strom- und Infrastrukturausfall entstehen“, sagte Herbert Saurugg *(www.saurugg.net)* und warnte vor der „Truthahn-Illusion“: Mit jedem Tag, an dem der Truthahn gefüttert wird, wächst sein Vertrauen, dass dies auch weiterhin so sein wird – bis zum Thanksgiving Day. Auch andere Perspektiven müssen bedacht werden, vor allem ein Systemversagen in der Stromversorgung. Die Netze würden laut Saurugg zunehmend an der Belastungsgrenze betrieben. Vom 9. auf den 10. August 2015 stand Polen knapp vor dem Kollaps, auf Stufe 19 einer 20-stufigen Skala. Diese Stufe hätte Totalabschaltung bedeutet. Nach Erfahrungen aus dem Jahr 2006 könnte Europa in 10 bis 20 Sekunden finster sein. Es könne von einem halben Tag bis zu mehreren Tagen dauern, bis das Stromnetz wieder funktioniert. Innerhalb der ersten Stunde nach dem Blackout, der „Golden Hour“, ab der, wie bei fallenden Dominosteinen, die Eskalation nach unten einsetze, müssten Maßnahmen gesetzt werden.

Das digitale Festnetz könnte bei Stromausfall sofort zusammenbrechen, der Mobilfunk nach etwa zwei Stunden. Das analoge Festnetz sowie Untervermittlungsstellen könnten noch bis zu acht Stunden betrieben werden. Ohne Kommunikation zerfalle die Gesellschaft in Kleinststrukturen, die sich auf lokaler Ebene selbst organisiere. Ein „Management“ würde nur mehr beschränkt möglich sein. Nach zwei Stunden würde

die Wasserversorgung (somit auch die Toilettenspülung) in höheren Stockwerken nicht mehr möglich sein. Über Wasservorräte verfügen nach der Studie „Ernährungsvorsorge in Österreich“ allerdings lediglich 11 bis 26 Prozent der befragten Haushalte. Spätestens ab dem vierten Tag sind nach dieser Studie drei Millionen Menschen (1,4 Millionen Haushalte) ohne Lebensmittel, nach sieben Tagen 5,8 Millionen. Tage-, wenn nicht wochenlange Versorgungsengpässe sind möglich.

Bei Netzersatzanlagen (Notstromaggregate) hat sich das Ausflocken des dem Dieselkraftstoff beigemengten Biodiesels als Problem herausgestellt. Nach einer deutschen Studie war nur in acht Prozent der Fälle der Brennstoff uneingeschränkt verwertbar. Ein Drittel war deutlich gealtert und 60 Prozent waren nicht bzw. in naher Zukunft nicht mehr verwendbar. Deshalb gelte es, vorbereitet zu sein – sowohl im privaten als auch im Unternehmensbereich.

Krisenmanagement. Die Ursachen von Krisen können außerhalb des Einflussbereichs eines Unternehmens liegen, eine ganze Branche betreffen oder, als am häufigsten, im Unternehmen selbst entstehen, berichtete Bernhard Gupper, *Group Security Manager* bei *Magna Steyr*. Ziel des Krisenmanagements ist es, die Existenz des Unternehmens zu sichern. Im Durchschnitt investiert nur ein knappes Drittel aller Unternehmen in die Entwicklung von Krisenmanagementprozessen; am höchsten die Industrie mit 41 Prozent.

Früherkennung einer Krise samt dem Ergreifen von Gegenmaßnahmen ist wichtig. Im Zeitalter der sozialen Medien breiten sich nach einer von Gupper präsentierten

Veranstalter Rainer von zur Mühlen; Referenten Prof. Peter Heinzmann, Prof. Gunther Schmid, Herbert Saurugg.

Referenten André Duvillard, Bernhard Gupper, Elmar Rizzoli und Frank Ewald.

Studie Nachrichten über Krisen zu 28 Prozent innerhalb einer Stunde grenzübergreifend aus, wogegen Unternehmen zur externen Kommunikation einer sinnvollen Reaktion durchschnittlich 21 Stunden brauchen, in 18 Prozent der Fälle sogar mehr als 48 Stunden. Innerhalb von 24 Stunden breiten sich 69 Prozent der Krisen international aus und erreichen im Durchschnitt elf Länder. Ein Jahr später haben 53 Prozent der betroffenen Unternehmen nicht wieder ihren Marktwert erreicht wie vor der Krise.

Entschließt man sich in der Führungsspitze eines Unternehmens zur Einführung eines Krisenmanagements, ist zunächst der Ist-Zustand zu erheben und hinsichtlich bestehender Risiken zu analysieren; diese sind zu bewerten. Im Sinne des *PDCA*-Verfahrens *(Plan, Do, Check, Act)* sind zunächst Pläne zur Bewältigung der erfassten Risiken auszuarbeiten. Diese Pläne sind etwa durch regelmäßige Übungen und Krisenkommunikationstraining zu implementieren und letztlich anhand der gewonnenen Erfahrungen weiterzuentwickeln und zu verbessern. Aus der Bewältigung von Krisen sollte man lernen.

Frank Ewald, Leiter der Konzernsicherheit bei der *DHL,* berichtete über den hierarchischen Aufbau eines Security-Risk-Managements. Bei einem Konzern wie der *DHL,* mit mehr als 480.000 Mitarbeitern in über 220 Ländern, bildet die umfassende Konzern-Richtlinie zur Sicherheit *(Corporate Security Policy)* die Grundlage für alle sicherheitsrelevanten Regelungen im Konzern. Die weitere Ausführung erfolgt in Security-Guidelines und Manuals. Risiken müssen erkannt und in weiterer Folge Maßnahmen zur Abwehr erarbeitet, ausgeführt, überprüft und kontinuierlich verbessert werden. Nicht die bloße Effektivität von Maßnahmen steht im Vordergrund, sondern die Effizienz, die einen Bezug zum Aufwand herstellt. Die Corporate-Security kann durch ihr Wissen über Sicherheitsverhältnisse in einem Gebiet sogar zu einem Business-Enabler werden.

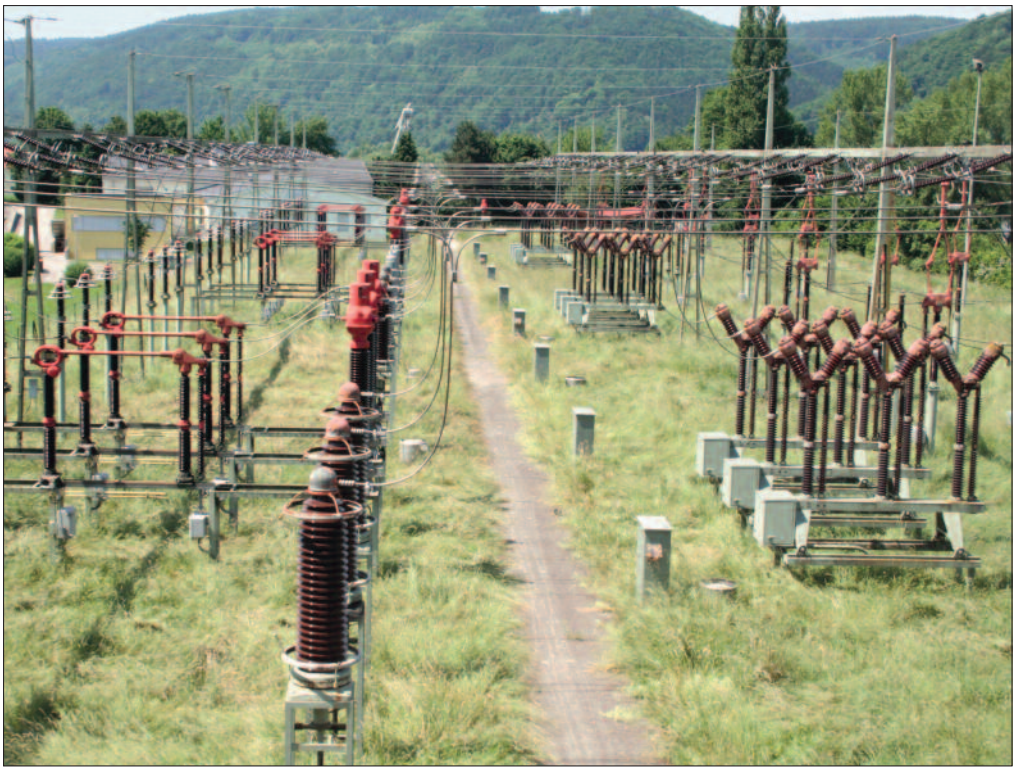
In das bestehende Krisenmanagement ist auch ein Cyber-Krisenmanagement einzubauen, forderte Eugen Leibundgut von *RM Risk Management AG (www.rmrisk.ch).* Cybercrime-Dienstleistungen können im Darknet eingekauft werden. Angriffe erfolgen gezielt und unter Kombination verschiedener Methoden. Der Kunde kauft nicht mehr Werkzeuge wie Angriffssoftware und E-Mail-Adressen, sondern den Erfolg, der zudem wie im reellen Wirtschaftsleben mit Geld-zurück-Garantie angeboten wird. Die zunehmende Vernetzung von Geräten und Systemen vergrößert die Angriffsfläche. Suchmaschinen für Geräte und Personen werden immer besser. Notwendig sind der Aufbau eines Cyber-Krisenmanagement-Teams sowie Krisenübungen.

Krisenübung. Auf dem Gedanken von Benjamin Franklin, „by failing to prepare, you are prepairing to fail“, beruhte die *Sicherheitsverbundübung 2014 (SVU 14)* in der Schweiz, über die Oberst André Duvillard berichtete. Erprobt wurde das Zusammenwirken von Bund, Kantonen und Städten sowie Zivilschutz, Armee und Polizei in Krisensituationen. Die Übungsannahmen waren, dem wahrscheinlichsten und für ganz Westeuropa gültigen Szenario entsprechend, eine Strommangellage ab Mitte September 2014 bis Jänner 2015, mit einem dreitägigen totalen Stromausfall, sowie einer Pandemiewelle mit Höhepunkt im November 2014. Ausgegangen wurde in diesem Fall von 8.000 Toten und davon, dass 25 Prozent der Schweizer Bevölkerung infiziert worden seien. Neben der Erprobung der Führungsebenen lag das Schwergewicht auf den Themen Mobilität, Ver- und Entsorgung, Gesundheitswesen und öffentliche Sicherheit. Geübt wurde in Workshops mit über 300 Teilnehmern. Unmittelbare Außenwirkungen gab es nicht.

FOTOS: KURT HICKISCH

Bei der Elektrizitätsbewirtschaftung wurden nach Aufrufen bestimmte Verwendungsarten elektrischer Energie eingeschränkt und periodische Netzabschaltungen (33 %, 50 %) simuliert. Dabei zeigte sich, dass Straßenverbindungen durch den Ausfall der Tunnelsteuerungsanlagen unbenutzbar werden. Die *Schweizer Bundesbahnen* haben zwar ein eigenes Stromnetz, aber die Lichtsignalanlagen werden über das öffentliche Stromnetz betrieben. Schwierigkeiten in der Wasserver- und -entsorgung treten auf. Produktionsprozesse kommen zum Stillstand. In den Geschäften sind die Regale nach 24 Stunden leer. Die vollautomatisierte, IKT-gesteuerte Versorgung durch die Großhändler funktioniert nicht mehr. Kühe, die drei Tage lang nicht wie gewohnt mit Maschinen gemolken werden, gehen zugrunde. Ein Ergebnis der Übung war, dass die Bevölkerung dazu gebracht werden muss, einen Vorrat an Wasser und Konserven anzulegen sowie Gaskocher bereit zu haben.

Elmar Rizzoli, Leiter des Amtes für allgemeine Sicherheit und Veranstaltungen des Stadtmagistrats Innsbruck, berichtete über den Aufbau und die rechtlichen Grundlagen des Katastrophenschutzes in Österreich. Jedes Bundesland hat ein eigenes Katastrophenschutzgesetz. In die Zuständigkeit des Bundes fallen die allgemeine Sicherheitspolizei, militärische Angelegenheiten, Zuständigkeiten nach der Gewerbeordnung, Veterinärwesen (Seuchen) und Strahlenschutz. Der Umgang mit sozialen Medien ist für Behörden und Einsatzorganisationen nicht gesetzlich geregelt; es ergeben sich Fragen der Haftung und des zu leistenden Aufwandes. Eine Betreuung der sozialen Medien, wie sie vom Magistrat Innsbruck aufgebaut wird, erfordert eine durchgehende Präsenz; es muss Vertrauen entwickelt werden. Das Team wird unter anderem darin geschult, Anzeichen eines Shitstorms sowie Fake-Meldungen zu erkennen, Trolle zu identifizieren und Suchfunktionen einzusetzen. In der gesamten Verwaltung sollten sich „Ambassadors“ herausbilden, die die Ideen der sozialen Medien verbreiten.



Stromversorgung: „Die Netze werden zunehmend an der Belastungsgrenze betrieben.“

FOTO: WERNER SABITZER

Geschäftsreisen. Andreas Radelbauer, Geschäftsführer der *Result Group,* hob wichtige Gesichtspunkte bei der Planung und Durchführung von Geschäftsreisen in Länder mit geringem Sicherheitsniveau hervor – unterlegt mit Erfahrungsberichten von Auftragsreisen nach Kabardino Balkarien, in den Sudan und nach Kabul. Es gilt, sich mit dem Land vertraut zu machen, Sicherheitshinweise zu beachten, die jederzeitige Erreichbarkeit sicherzustellen, für einen medizinischen Notfall Vorsorge zu treffen und einen Exitplan aufzustellen. Eine persönliche Notfalltasche sollte immer griffbereit gehalten und auf Überlandfahrten mitgeführt werden. Für die Abholung vom Flughafen sollte zuvor mit dem Abholenden ein Losungswort vereinbart werden. Die Unterkunft im Hotel sollte wegen möglicher Sprengstoffanschläge zwischen dem 3. und 5. Stock gewählt werden, aber nicht höher, weil die Leitern der Feuerwehr nicht höher reichen. Ansonsten sollte man sich in Bekleidung und Auftreten möglichst unauffällig verhalten, auf Kameras, Laptops, Telefone und Kommunikationsmittel achten und bei Überlandfahrten Ortskundige als Begleitung mitnehmen.

Über eine erfolgreiche Evakuierung von EUBAM-Mitarbeitern aus Libyen im Juli 2014 berichtete Sicherheitexperte Gerhard Gerber.

Informationssicherheit. Prof. Dr. Peter Heinzmann von der *Hochschule für Technik Rapperswil (www.cnlab.ch)* zeigte die steigende Verletzlichkeit der digitalen Welt auf und forderte organisatorische und technische Maßnahmen in den Bereichen der Infrastruktur, bei Prozessen und beim *Human-Security-Layer,* also beim Mitarbeiter.

Internet, soziale Medien und Personen-Suchmaschinen könnten zur Informationsbeschaffung über Menschen genützt und zum Social Engineering eingesetzt werden, um also durch Täuschungshandlungen zu Informationen oder Zutrittsberechtigungen zu gelangen. Abwehrmaßnahmen seien unter anderem der Aufbau einer *Mental Firewall* und ein *Person-Hardening*, also entsprechende Sensibilisierung der Mitarbeiter, Förderung eines „gesunden Misstrauens“. Soziale Automatismen, wie Respekt vor Autoritäten, Neugier, Hilfsbereitschaft und Streben nach Anerkennung, müssten beherrscht und etwaige Fehlhandlungen aus diesen Motiven mit technischen Maßnahmen abgefangen werden.

Kurt Hickisch