

Krisenmanagement in Firmen

Sicherheitsbeauftragte berichteten beim 12. SIMEDIA-Forum für Sicherheitsverantwortliche über Möglichkeiten zur Prävention und Bewältigung von Krisen in anderen Ländern.

Weltweit tätige Unternehmen sind nicht nur von herkömmlichen Kriminalitätsformen wie Diebstahl, Einbruch, Überfall, Brandstiftung, Produkterpressung bedroht, sondern auch von Industrie- und Wirtschaftsspionage, Terrorismus, Extremismus, Entführungen sowie Naturkatastrophen und Pandemien. Betroffen sind nicht nur die Niederlassungen der Unternehmen in Krisengebieten oder Risikoländern, sondern auch die dorthin entsendeten Mitarbeiter („Expatriats“) und Dienstreisende.

Beim 12. SIMEDIA-Forum für Sicherheitsverantwortliche am 8. und 9. Juni 2011 in Hamburg berichteten Sicherheitsbeauftragte weltweit tätiger Unternehmen unter anderem, welche Vorkehrungen zum Schutz ihrer Mitarbeiter und des Vermögens für solche Fälle getroffen werden und welche Lehren aus Krisen gezogen werden, etwa in Ägypten, Libyen, Pakistan, in südamerikanischen Ländern oder Japan.

Nahostexperte Dr. Michael Lüders gab einen Überblick, welche Konsequenzen die gesellschaftlichen Umbrüche in Nordafrika und anderen Staaten des arabischen Raumes für Unternehmen und die Unternehmenssicherheit nach sich ziehen.

Im Allgemeinen haben Unternehmen mit Niederlassungen in kritischen Ländern Strukturen aufgebaut, wie sie Peter Speckbruck, Hauptreferent in der Konzernsicherheit der RWE AG, darstellte, unter Einbeziehung von Erfahrungen bei der Rückholung von Mitarbeitern aus Ägypten und Libyen.



Niederlassungen weltweit tätiger Unternehmen in Risikoländern können auch Opfer von Naturkatastrophen werden.

Mitarbeitersicherheit im Ausland. Mitarbeiter werden durch Schulungen und interkulturelles Training mit Security-Inhalten auf Auslandseinsätze vorbereitet, wobei auf Wunsch auch Familienangehörige einbezogen werden. Informationen in Form von Länderlisten werden im Intranet zur Verfügung gestellt. Auf Notfallkarten finden sich die wichtigsten Informationen, über die kompetente Hilfe – auch medizinische – zu erlangen ist.

Zudem haben die Unternehmen rund um die Uhr besetzte Sicherheits- und Lagezentren eingerichtet, die unter anderem durch Auswertung von Medienberichten permanent Krisenherde beobachten und die erste Anlaufstelle sind. Für bestimmte Szenarien sind Maßnah-

men und Verantwortlichkeiten bereits im Voraus festgelegt – immer mit Alternativen. Die Unterlagen müssen aktuell gehalten werden.

Evakuierungspläne sind in verschiedenen Abstufungen vorbereitet. Sie beginnen damit, die Erreichbarkeit der betroffenen Mitarbeiter sicherzustellen. Die Nutzung der Handy-Applikation des Travel-Trackings wird empfohlen, um die jeweiligen Reisebewegungen verfolgen zu können. Familienangehörige werden aufgefordert, das Land zu verlassen.

Die nächste Stufe kann darin bestehen, Mitarbeiter zum Aufenthalt zu Hause oder im Büro zu verpflichten. Es werden „Save Havens“, etwa in internationalen Hotels, vorbereitet, in die sich Mitarbeiter bei weiterer

Zuspitzung der Lage (Ausbreitungen, Plünderungen) begeben können. Standorte sind zu reduzieren, der Geschäftsübergang an eine Rumpfmannschaft ist zu regeln und für Vertretung durch lokale Mitarbeiter zu sorgen. Wohn- und Geschäftsgebäude sowie mobile Vermögenswerte sind abzusichern, etwa durch vertragliche Verpflichtung lokaler Sicherheitsdienste.

Evakuierung. Die Entscheidung, ob eine Evakuierung erfolgen soll, wird nicht vor Ort, sondern von der Geschäftsleitung getroffen, weil sich gezeigt hat, dass die Lage vor Ort oft wesentlich weniger dramatisch eingeschätzt wird. Allerdings könnte ein zu früher Rückzug den Ruf des Unternehmens gefährden oder zum Verlust von Lizenzen führen sowie bei der Rückkehr und Wiederaufnahme des Betriebs nach überstandener Krise hinderlich sein. Soweit möglich, wird der Rückzug als Urlaub der Mitarbeiter deklariert.

Es hat sich als notwendig herausgestellt, auf den Entfall der Stromversorgung, der Kommunikationsmittel und des Internets vorbereitet zu sein. Vorzusorgen ist mit Satelliten-Telefonen – die allerdings nicht in Räumen verwendet werden können – und mit gedruckten, in Folie verschweißten Handlungsanweisungen sowie mit Medikamenten, Schutzausrüstung, Bargeld.

Sicherheit zur Unterstützung der Unternehmensziele. Dr. Cosima Eggers, Leiterin der Konzernsicherheit bei „Airbus“, wies darauf hin,

dass die Sicherheitsabteilung keine Verhinderungsfunktion haben dürfe, sondern im Rahmen der Unternehmensziele agieren müsse. Prävention sei wichtig, wobei auch das Image eine Rolle spielt, das sich ein Unternehmen in einem Land, etwa durch Projekte für die Jugend erworben hat.

Probleme ergeben sich in Ländern, in denen eine Verschlüsselung von Nachrichten oder Datenträgern nicht zulässig ist. Dort kann Wichtiges nicht mehr am Telefon besprochen werden, Daten am Laptop sollten gelöscht und wichtige Informationen nur mehr auf einem Stick gespeichert werden, den man am Körper trägt.

Krisen- und Business-Continuity-Management.

Über Erfahrung bei Krisen, die sich während des Reaktorunglücks im Atomkraftwerk Fukushima in Japan für das Business Continuity Management (BCM) ergaben, berichtete Wolf-Rüdiger Moritz, Leiter des Bereichs Business Continuity bei *Infinion Technologies AG*.

Informationen, etwa über Verstrahlungswerte und Ausbreitung der radioaktiven Wolke, wurden durch ständige Beobachtung ausgewählter Websites gewonnen, da offizielle Quellen nicht ausreichten.

Zur Nachverfolgung der Mitarbeiter im Großraum Tokio und zur Aufrechterhaltung der Kommandokette wurde eine Notfall-E-Mail-Adresse eingerichtet. Notunterkünfte sowie zusätzliche Büroflächen wurden in Nagoya und Osaka angemietet.

Für in Tokio verbliebene Mitarbeiter wurden Notfall-sammelplätze festgelegt. An die Mitarbeiter in Japan wurden Merkblätter mit Informationen über Schutzmaßnahmen im Fall eines radioaktiven Fallouts verteilt, nachdem irreführende Be-



Die Deutsche Bahn verstärkt die Sicherheit für ihre Kunden.

ichte über Kontamination von Wasser und Nahrungsmitteln zu einer Verunsicherung geführt hatten. Nahrung, Wasser, Schutzkleidung und Batterien wurden aus Singapur importiert und größtenteils an die Mitarbeiter verteilt. Aus Japan stammende Lieferungen wurden auf Radioaktivität überprüft.

„Es war schwer, zu wissenschaftlichen medizinischen Daten über Verstrahlung und Fallout zu kommen. Wir mussten uns im Grunde genommen die zur Beherrschung der Lage erforderlichen Kenntnisse selbst erarbeiten“, bedauerte Moritz.

Präventives Sicherheitskonzept. „Wenngleich im Bereich der Deutschen Bahn



Rainer von zur Mühlen: „Sicherheit muss mit Querschnittswissen angegangen werden, das nur mehr im Team möglich ist.“

die Kriminalität weit unter der des sonstigen öffentlichen Bereiches liegt, ist von Kundenseite her ein erhöhter Bedarf an Sicherheit festzustellen“, führte der Leiter der Abteilung für Konzernsicherheit der *Deutschen Bahn AG*, Prof. Dr. Gerd Neubeck.

Das Unternehmen trägt dem seit heuer mit einem neuen Sicherheitskonzept Rechnung, das durch eine verstärkte Präsenz von Mitarbeitern der *DB* das Sicherheitsgefühl vor, während und nach der Fahrt heben soll. Bis zu 500 Sicherheitskräfte mehr werden für die Bahn im Einsatz sein. Mit der Bundespolizei wird zum Schutz der Fahrzeuge, Infrastruktur, Anlagen und Gebäude eine enge Zusammen-



Peter Speckbrück: „Mitarbeiter durch interkulturelles Training mit Security-Inhalten auf Auslandseinsätze vorbereiten.“

arbeit in Form einer Partnerschaft eingegangen. Im Hinblick auf Vandalismus-Schäden wird Präventionsarbeit geleistet: Für Jugendliche werden jährlich rund 500 Praktikumsplätze bereitgestellt.

Für Jugendliche aus Kinderheimen werden *DB-Kids-Camps* eingerichtet und über die Stiftung *Off-Road-Kids* erhalten Straßenkinder Hilfe. Für Kinder gibt es im Internet Spiele, Bastel- und Malanleitungen. Kinderheime werden mit Vorleseköffern ausgestattet.

Die Bahn unterstützt das Präventionsprogramm „Fairplayer“ (www.fairplayer.de; *Handbuch unter www.fairplayer.de/massnahmen/fairplayer_manual*), mit dem soziale Kompetenz gefördert sowie Bullying in Schulen eingedämmt werden soll.

Denken in Prozessen.

„Immer noch stehen bei Unternehmen die Abwehr und Aufklärung deliktischen Handelns im Vordergrund, obwohl mittlerweile die überwiegende Mehrzahl von Schäden aus nichtdeliktischen Ursachen resultiert“, erläuterte Rainer von zur Mühlen und forderte eine von der historischen „Werkspolizei“ gelöste Denkweise, die zudem die vielfältige Komplexität beachten sollte. „Es wird in Ereignissen und nicht in Prozessen gedacht.“ Sicherheit sei eine Querschnittsmaterie und müsse mit Querschnittswissen angegangen werden, das bei den heutigen Verhältnissen nur mehr im Team erreichbar sei. Systemanalytiker, Ingenieure und durchsetzungskräftige Manager müssten zusammenarbeiten. Um nicht immer das Rad neu erfinden zu müssen, wäre nach guten Standardlösungen zu suchen, die unternehmensweit (und nicht nur bei einzelnen Standorten) zu implementieren wären.

FOTOS: DB, KURT HUCKBISCH (2)

Krisenkommunikation.

Krisenmanagement aus ganz anderer Ursache war am 20. August 2010 an der Universitätsklinik Mainz gefordert. Damals hatten elf Kinder in der Intensivstation für Frühgeborene Infusionslösungen erhalten. Einen Tag später starben zwei Säuglinge, die schon schwere Grunderkrankungen aufgewiesen hatten. Es zeigte sich, dass die in der Klinikapotheke zubereiteten Infusionslösungen verkeimt waren.

Das am 22. August einsetzende Krisenmanagement, geleitet vom stellvertretenden medizinischen Vorstand Prof. Dr. Norbert Pfeiffer, setzte von Anfang an auf umfassende und sachliche Information der Öffentlichkeit und Kooperation mit Ermittlungsbehörden.

Am 23. August starb ein weiterer Säugling. Das internationale Medieninteresse war enorm. Die Medienpolitik der Klinik ging vom Grundsatz aus: „Wir haben nichts zu verbergen.“ Der Herstellungsprozess der Infusionen, die in einem Reinraum händisch aus etwa acht Fläschchen zusammengemischt worden waren, wurde von unabhängigen Experten überprüft. Durch die von Anfang an eingeschaltete Staatsanwaltschaft wurde ausgeschlossen, dass bei der Zubereitung ein Fehler unterlaufen war. Inwieweit und aus welchen Gründen die Bakterien schon in den angelieferten Lösungen selbst enthalten waren, ist Gegenstand laufender Verfahren.

Den Angehörigen wurde offene und ehrliche Information geboten, verbunden mit Mitgefühl sowie dem Angebot von Unterstützung durch Psychologen und Seelsorger.

Bei aller Offenheit nach außen mussten die Mitarbeiter in der Apotheke zur Wahrung des Persönlichkeitsschutzes von den Medien abgeschirmt werden.



Cosima Eggers: „Die Sicherheitsabteilung einer Firma darf keine Verhinderungsfunktion haben.“

Auch diesen Mitarbeitern wurde mentale Betreuung angeboten. Um bei der gebotenen Sachlichkeit zu bleiben, wurden auch keine Bilder aus dem Krankenhaus zugelassen. Klargestellt wurde, dass Verantwortung zu übernehmen nicht bedeutet, sich schuldig zu bekennen. Für alle Mitarbeiter wurde ein Informationsdienst eingerichtet, der sie auf dem Laufenden hielt.

Datenschutz und Datensicherheit. In Deutschland ist der Entwurf für eine Neufassung des § 32 BDSG durch Bestimmungen zum Beschäftigtendatenschutz in Diskussion. Die vorgesehenen Regelungen zur Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten gliedern sich in solche vor Begründung des Beschäftigungsverhältnisses und betreffen in diesem Fall die ärztliche Untersuchung (§ 32a Abs. 1 BDSG-E), Eignungstests (§ 32a Abs. 2) und Background-Checks (§ 32 Abs. 6). Im Beschäftigungsverhältnis werden geheime Erhebung (§ 32e) geregelt, Videoüberwachung (§ 32f), Ortungssysteme (§ 32g), biometrische Verfahren (§ 32h) und die Nutzung betrieblicher Kommunikationsmittel (§ 32i).



Katherine Timmel Zamboni: „Niederschwellige Signale für auffälliges Verhalten möglichst früh erkennen.“

Ziel des Entwurfs sei es, die bisher vornehmlich durch Gerichtsentscheidungen erfolgte Rechtsentwicklung zusammenzufassen, berichtete Manfred Jilg, Leiter des Bereichs Werkschutz der BASF AG.

Der Schwerpunkt liege darin, aus dem Gesichtspunkt der Verhältnismäßigkeit noch mehr auf die Gegebenheiten im Einzelfall abzustellen, sodass etwa bei Bewerbungen, Eignungstests oder ärztlichen Untersuchungen auf die beabsichtigte Verwendung des Bewerbers abzustellen ist und kein allgemeines Screening mehr erfolgen soll.

Ein automatisierter Datenabgleich in anonymisierter Form zur Aufdeckung von Compliance-Verstößen wird zwar als zulässig erklärt (§ 32d Abs. 3 BDSG-E), doch wird Unternehmen die – von der Judikatur bisher als letztes Mittel zur internen Aufklärung von Delikten zugelassene – verdeckte Videoüberwachung ihrer Mitarbeiter generell verboten. Sie wird laut Entwurf den Strafverfolgungsbehörden vorbehalten bleiben.

Gewalt am Arbeitsplatz. „Die Ereignisse an der Virginia Tech sowie die Amok-

läufe an Schulen in Deutschland und Finnland haben die Eidgenössische Technische Hochschule Zürich (ETH) dazu veranlasst, ein Bedrohungsmanagement-Team zu installieren“, berichtete die Leiterin Stab Sicherheit, Gesundheit und Umwelt der ETH Zürich, Katherine Timmel Zamboni (www.sicherheit.ethz.ch).

„Es gilt, niederschwellige Signale für auffälliges Verhalten möglichst früh zu erkennen und das Risiko einer Eskalation zu minimieren.“ In Workshops wurde ein Leitfaden entwickelt, an Hand dessen und mit standardisierten Instrumentarien Bedrohungen eingeschätzt werden können, um in weiterer Folge Betroffene in belastenden Bedrohungssituationen zu unterstützen.

Das Kernteam, das sich aus zwei Psychologen, zwei Vertretern des Rektorats und der Personalabteilung zusammensetzt, hält je nach Sachlage enge Verbindung mit Polizei, Staatsanwaltschaft, Stadtarzt, Vormundschaftsbehörde, Amt für Immigration.

Fallmanager. Jede relevante Risikosituation wird einem Fallmanager übertragen, über den als Ansprechpartner die gesamte Kommunikation nach innen und außen verläuft. In den zwei Jahren des Bestehens des Bedrohungsmanagement-Teams wurden bereits einige Fälle erfolgreich abgeschlossen, die zur Eskalation hätten führen können.

Im Gegensatz zu den USA ist an europäischen Universitäten ein Bedrohungsmanagement noch kaum verbreitet. Schwierigkeiten ergeben sich durch die dezentrale Organisation der Hochschulen, die große Zahl der Studierenden und die fehlende Vernetzung der weitgehend autonomen Bereiche. Kurt Hickisch