

Sicherheitsfragen und Lösungen

Das 14. Forum für Sicherheitsverantwortliche der Simedia GmbH am 11. und 12. Juni 2013 in Ludwigsburg bot einen breiten Überblick über aktuelle Sicherheitsfragen und Lösungen.

In einer sich rasant verändernden Welt müssen Sicherheitsverantwortliche innovativ und zeitlich vorausschauend denken“, sagte Frank Ewald, Leiter der Konzernsicherheit bei der Deutschen Post DHL, beim 14. Forum für Sicherheitsverantwortliche.

Die Konzernsicherheit müsse Impulse setzen und als Innovationsmotor wirken. Um den Wertschöpfungsfaktor aufzuzeigen, gelte es, Sicherheitsdienstleistungen messbar zu machen. Messbar sei beispielsweise, wie sich ein Sicherheitsbericht hinsichtlich der Vermeidung von Schäden ausgewirkt habe; was durch rechtzeitige Hinweise auf dubiose Geschäftspartner oder durch die Aufdeckung krimineller Machenschaften an Schaden verhindert worden sei oder durch sicherheitstechnische Maßnahmen an Versicherungsprämien eingespart werde. Die Unternehmenssicherheit dürfe nicht im Operativen stecken bleiben, sagte Ewald, sondern müsse zu einer strategischen Unternehmensfunktion aufgewertet werden. Vom Sicherheitsverantwortlichen der Zukunft werde eine breitere akademische Ausbildung gefordert, verbunden mit Erfahrung im Konzern und mit internationalen Verbindungen.

Im Sicherheitsbereich sei die Auslagerung von Dienstleistungen (Outsourcing) zu überdenken. Beauftragte Externe könnten zwar manche Dienstleistungen, etwa Überwachungsaufgaben, billiger anbieten, doch eigene Leistungen (Inhouse-Lösungen) hätten den Vorteil, dass das eigene Personal eingearbei-



Frank Ewald: „Sicherheitsverantwortliche der Zukunft benötigen eine breite akademische Ausbildung.“

tet und im Unternehmen bekannt sei und sich mit den Firmenwerten identifiziere, wodurch der Abfluss von Informationen an die Konkurrenz weniger wahrscheinlich sei. Außerdem gehe weniger Zeit für Einschulungen verloren und die Mitarbeiter könnten flexibel auch für andere Aufgaben eingesetzt werden.

Schadensvermeidung.

Wie bereits in der Planungsphase von Bauvorhaben die Berücksichtigung sicherheitstechnischer Ideen künftige Schäden verhindern kann, zeigte Dkfm. Rainer von zur Mühlen anhand von komplexen Großprojekten auf, in die sein Planungsunternehmen eingebunden war.

Ein Schaden läuft prozesshaft ab und es gilt, möglichst schon am Anfang den Prozess zum Halten zu bringen. Der „Security-Integrator“ muss als eine Art Konsulent das Gesamtprojekt verstehen, in das Ausschreibungsverfahren und in weiterer Folge in die Planungsprozesse im Team eingebunden werden. Er muss die ex-



Wolfgang Neldner: „Ein überregionaler Stromausfall in Deutschland wird immer wahrscheinlicher.“

ternen und internen Risiken erkennen und Lösungen erarbeiten. Als Beispiel nannte von zur Mühlen feinjustierte Satellitenantennen auf dem Parkhaus einer Sendeanstalt. Ein Brand im Parkhaus würde durch die Ausdehnung des Tragwerks die Justierung der Antennen verändern, ebenso der Anprall eines Fahrzeugs. Die Bauteile wurden mit Dehnungsfugen getrennt und es wurden besondere Maßnahmen zur Unfallverhütung getroffen.

Innerhalb eines Gebäudes sind Unverträglichkeiten zu berücksichtigen. Im Umfeld von Elektronik dürfen sich keine Brandlasten befinden. Publikumsverkehr ist von sensiblen Zonen fernzuhalten. In einem Bankgebäude wird, schon auf Grund gesetzlicher Vorschriften, dafür zu sorgen sein, dass Vertrauliches dort bleibt, wo es sein soll. Das erfordert schallhemmende Bürowände und -türen, die Vermeidung von Großraum- und Durchgangsbüros, von Klarglastüren, bis zur teilweisen Autarkie einzelner Bereiche, etwa mit eigenen Sanitärräumen.

Stromausfall. Ein überregionaler und länger dauernder Stromausfall in Deutschland werde immer wahrscheinlicher, sagte DI Wolfgang Neldner (*Neldner Consult, System- und Elektrizitätsnetzberatung*). „Die Netze sind hochgestresst. Ein kleiner Anstoß genügt, dass es eng wird.“ Elektrische Energie wird vornehmlich im Norden Deutschlands erzeugt und im Süden verbraucht. Wegen zu geringer Leitungskapazität muss auf Leitungen in Nachbarländern ausgewichen werden – was Auswirkungen auf das gesamte europäische Verbundnetz hat.

Wie eng die Zusammenhänge sind, zeigte sich bei der Abschaltung einer 380-kV-Doppelleitung in Norddeutschland am 4. November 2006 um 21.38 Uhr: Der Westen Europas war bis Spanien stromlos und dunkel. Erneuerbare Energien, etwa Solar- und Windstrom, erbringen Leistung nicht kontinuierlich, sondern dann, wenn die Sonne scheint oder ausreichend Windkraft zur Verfügung steht. Die Speicherung von Erzeugungsspitzen elektrischer Energie, etwa in Pumpspeicherkraftwerken, ist zunehmend erforderlich. Neldner unterscheidet zwischen dem Normal-, dem Stress-, dem Störbetrieb und dem Teil- oder Totalausfall samt Wiederaufbau.

Im Normalbetrieb sollten die Planungen erfolgen, wie es im Störfall weitergehen soll: Überprüfung der Netzanschlussverträge, Erstellung und Aktualisierung der Notfallpläne; Festlegung der Notstromanschlüsse und deren Kennzeichnung. Erfas-

sung jener Anschlüsse, an denen elektrische Leistung im Rationierungsfall, bei Stromsperre und nach Wiederversorgung vorrangig benötigt wird (z. B. Umwälzpumpe der Ölheizung).

Der in der Regel für den Verbraucher noch nicht sichtbare Stressbetrieb (Frühwarnung) wird durch Hintergrundmaßnahmen der Netzbetreiber aufgefangen. Es liegen aber konkrete und ernst zu nehmende Hinweise auf eine Verschlechterung der Versorgungslage vor (Sturmwarnungen, Hochwasser u. a.). Mit dem Versorgungsunternehmen sollte in Kontakt getreten werden, Konzepte für die unterbrechungsfreie Stromversorgung (USV) und für lokale Kooperationen sollten bereitgehalten werden.

Beim Störbetrieb (Alarm) ist es bereits zum Ausfall von Betriebsmitteln gekommen. Versorgungsunterbrechungen sind eingetreten oder müssen befürchtet werden. Die vorbereiteten Pläne treten in Kraft. Personenrettung hat Vorrang (aus Liften, von Kränen, aus Tunneln, von durch Notmaßnahmen Eingeschlossenen, von Kranken und Behinderten). Kommunikationsverbindungen sind sicherzustellen.

Ein Teil-/Totalausfall („Blackout“) stellt den Notfall dar. Heizung, Lebensmittelversorgung, Kommunikation, Verkehr, Wasserversorgung und Abwasserentsorgung brechen zusammen. Notstromaggregate können nicht mehr mit Treibstoff beliefert werden. „Es wird dunkel, kalt und stinkt“. Beim Wiederaufbau der Stromversorgung muss bei den ersten Zuschaltungen mit Überlastung der Transformatoren gerechnet werden. Das kann zu Bränden führen.

DI Dieter Zeller, Leiter des Bereichs Sicherheitslage, Krisen und Notfallmanage-

ment der *Deutschen Telekom AG*, schilderte mögliche Folgen von Zusammenbrüchen der Kommunikationsnetze durch Ausfall der Stromversorgung sowie Erkenntnisse, die man aus bisherigen Vorfällen gewonnen habe.

Ein Ausfall der Telekommunikation betrifft auch Datenleitungen zu Sensoren, beispielsweise bei Wasser- und Abwasseranlagen, was zu Abschaltungen selbst bei Notstromversorgung führt. Um die Kommunikation hilfsweise aufrecht zu erhalten, habe sich beim Hurrikan Sandy in New York der Einsatz von Bussen mit mobilen Hotspots bewährt, verbunden mit der Möglichkeit, dass dort Handys aufgeladen werden können.

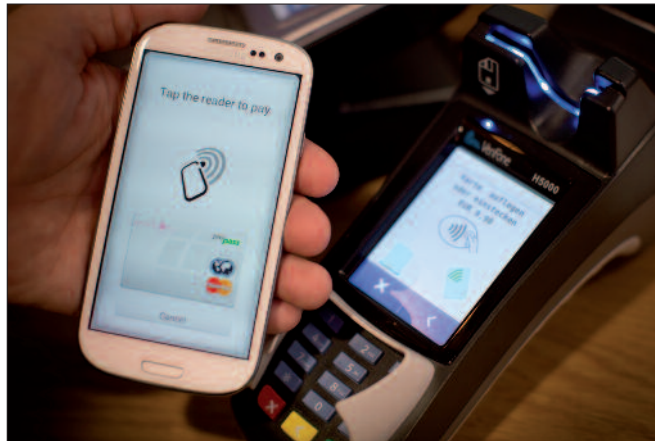
Die berührungslose Identifikation hat sich durchgesetzt, etwa zur Warenkennzeichnung oder als zusätzliches Sicherheitsfeature bei Reisedokumenten. Auch Zutrittskontrollsysteme lassen sich mit Smart Cards gestalten. Das Grundprinzip der dahinter stehenden Technik (*Radio Frequency Identification – RFID*) ist, dass ein Lesegerät Signale aussendet, auf die der Transponder antwortet. Auch wenn dieser mit eigener Rechenleistung ausgestattet ist, bleibt bei dieser Technik der Transponder immer der passive Teil. Eine Weiterentwicklung, dass beide Teile aktiv werden und beispielsweise digitale Berechtigungen übertragen werden können, ist die *Near Field Communication (NFC)*, die auf der RFID-Technologie basiert. Der Datenaustausch erfolgt wie bei dieser im Kurzwellenbereich (13,56 MHz) auf Distanzen von nur wenigen Zentimetern, wobei pro Sekunde bis zu 424 kBits übertragen werden können.

Als dem Transponder vergleichbares mobiles Gerät dient das Handy, sofern

es bereits NFC-fähig ist. Auch die praktische Anwendung ist gleich: Statt der Chipkarte wird das Handy an den Leser gehalten, der ein Bezahlterminal, etwa im Supermarkt oder bei Fahrkartenautomaten sein kann, oder ein mechatronisches Schloss, sodass sich mit dieser Technologie Zutrittskontrollsysteme aufbauen lassen.

Inwieweit dies beim Entwicklungsstand der NFC im Vergleich zu bisherigen Chipkarten sinnvoll ist, berichtete DI Klaus Behling (VZM GmbH). Selbst wenn Angriffe auf Chipkarten erfolgreich waren, reicht für Mitarbeiter bei vertretbarem Aufwand für nicht besonders zu schützende Bereiche ein als Smart Card gestalteter Ausweis.

Auch für Besucher ergibt sich durch über Handy erteilte Zutrittsberechtigungen



Near-Field-Communication: Die berührungslose Identifikation hat sich durchgesetzt, etwa zur Warenkennzeichnung oder als zusätzliches Sicherheitsfeature bei Reisedokumenten.

kein Vorteil. Sie werden ohnehin am Empfang abgeholt werden müssen, um sich zu recht zu finden. Zweckmäßig ist eine NFC-Zutrittslösung für Fremdpersonal, das nur zeitweilig und nur in bestimmten Bereichen des Unternehmens arbeitet.

Vorteile der NFC-Technologie bei der Zutrittskon-

trolle sieht Behling vor allem in der hohen Speicherkapazität eines Handys, wodurch starke Verschlüsselungen möglich werden. Zudem bemerkt man im Regelfall das Fehlen des Handys sehr rasch und kann eine Sperre veranlassen, wogegen der Verlust des Mitarbeiterausweises möglicherweise erst

nach dem Wochenende entdeckt wird. Ferner können viele „ältere“ RFID-Leser mit NFC kommunizieren.

Nachteile ergeben sich hinsichtlich der Verfügbarkeit. Das System funktioniert nicht, wenn der Akku leer oder das Handy beschädigt ist oder wenn kein Mobilfunkempfang besteht (Netzüberlastung, abgelegenes Gebiet). Zudem bestehen in manchen Unternehmensbereichen Handyverbote.

Dazu kommen Haftungsfragen: Wem gehört das Smartphone? Wer bezahlt die Rechnung? Noch unterstützen nicht alle Smartphone-Hersteller NFC und Anwendungen zur Zutrittskontrolle. Der Durchbruch wird erst erfolgen, wenn sich die Technologie über andere Massen Anwendungen durchgesetzt haben wird, wie Bezahlungsfunktionen und Ticketsysteme. *Kurt Hickisch*

SICHERHEITSVERBÄNDE IN DEUTSCHLAND

Die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e.V. (ASW) in Berlin – ein Zusammenschluss aller regionaler Sicherheitsverbände Deutschlands – besteht seit 1993. Sie unterstützt gemeinsam mit Behörden, die Wirtschaft in Sicherheitsfragen, insbesondere bei der Bekämpfung der Wirtschaftskriminalität, einschließlich neuer Deliktformen wie Wirtschafts- und Konkurrenzspionage, Cyber-Kriminalität, Produktpiraterie und Geldwäsche. Vorsitzender des Verbandes ist Volker Wagner. www.asw-online.de

Der Bundesverband der Sicherheitswirtschaft (BDWS), bis August 2011: „Bundesverband Deutscher Wach- und Sicherheitsunternehmen e.V.“, mit Sitz in Bad Homburg vertritt die Interessen der Sicherheitswirtschaft in Deutschland und hier insbe-



Verbandsvorsitzende Oliver Klein, Volker Wagner, Rainer von zur Mühlen (Simedia), Harald Olschok.

sondere der Sicherheitsdienstleister, für die er Tarifvertragspartner ist. Auf Sicherheitsdienstleister entfällt etwa die Hälfte des Gesamtumsatzes des deutschen Sicherheitsmarktes von 12 Milliarden Euro. Der Tätigkeitsbereich dieser Unternehmen umfasst Geld- und Wertdienste, die Überwachung von Banken und Museen,

Alarmübertragung, den Schutz von Industrie- und militärischen Anlagen, Kernkraftwerken, die Flughafensicherheit sowie die Abwehr von Wirtschafts- und Konkurrenzspionage. Der Verband bildet Fachkräfte aus und zertifiziert Sicherheitsfachschulen. Hauptgeschäftsführer des Verbandes ist Dr. Harald Olschok. www.bds.de

Die American Society for Industrial Security (ASIS) wurde im Jahr 1955 zur Standardisierung für das Sicherheitsgewerbe gegründet und ist mittlerweile zu einer weltweit vertretenen Organisation mit 38.000 Mitgliedern geworden, weshalb 2002 die Umbenennung des Verbandes in *ASIS International* erfolgte.

In den einzelnen Ländern bestehen Chapters, zum Beispiel in Deutschland das Chapter 251 mit 172 Mitgliedern und dem Vorsitzenden Oliver Klein.

Ziele der Organisation sind die Verbreitung von Standards sowie die Zertifizierung und Qualifizierung von Sicherheitspersonal. Regional werden Chapter-Meetings abgehalten, überregional (Europa, Mittlerer Osten, Asien-Pazifischer Raum) Sicherheits-Konferenzen.

www.asis-germany.org