

FORUM FÜR SICHERHEITSVERANTWORTLICHE

Strategisches Denken

Terroranschläge, organisierte Kriminalität, Betriebsspionage: Wie sich Unternehmen vor existenzbedrohende Gefahren schützen können, war Thema des 5. vzm-Forums für Sicherheitsverantwortliche.

Nach den Anschlägen von Al Qaida wurde der Ruf nach mehr Bewachungspersonal laut, da wurde in bloßem Aktionismus sinnlos Geld verbrannt, ohne dass die Sicherheit substantziell verbessert wurde", sagte Rainer von zur Mühlen in der Einleitung zum 5. Forum für Sicherheitsverantwortliche, das am 20. und 21. April 2004 in Frankfurt/Main stattgefunden hat. Es komme zu einer Selbstschädigung durch eine martialische Rüstungsspirale, betonte der Sicherheitsexperte.

Das Handlungsmuster der Terrororganisation ist dadurch gekennzeichnet, dass sich keine Regel erkennen lässt. Es soll spektakulär die Verwundbarkeit der Strukturen demonstriert werden. "Gegen einen konsequent und professionell vorbereiteten Anschlag gibt es keinen hundertprozentigen Schutz", erläuterte Von zur Mühlen. Kann aber die Wahrscheinlichkeit eines Schadenseintrittes nicht weiter gesenkt werden, gilt es, zumindest die Schadenshöhe bei einem Anschlag so gering wie möglich zu halten, so dass ein Unternehmen nicht lebensbedrohlich getroffen wird. Nicht punktuell, sondern strategisch muss gedacht werden: Es muss gewährleistet sein, dass Produktion und Lieferfähigkeit erhalten bleiben. In der gesamten Prozesskette darf sich kein existenzieller Fehlerpunkt befinden.

Das kann durch Auslagerung erreicht werden. Wenn auch Zentrallager aus wirtschaftlichen Gründen am zweckmäßigsten sind, ist eine Auslagerung wichtiger Güter unter den neuen Bedrohungsbildern eine Notwendigkeit. Das betrifft etwa Ersatzteile, die innerhalb kurzer Fristen geliefert werden müssen, aber auch wesentliche Produktionsprozesse. Bei Rechenanlagen und Datenarchiven sollte die Auslagerung eine Selbstverständlichkeit sein. Gerade bei der Hochwasserkatastrophe im August 2002 hat sich die Notwendigkeit gezeigt, Datenbestände in Kopien auszulagern. Maschinen und Leistungen lassen sich zukaufen, nicht gesicherte Daten sind verloren.

An Schutz vor existenzbedrohenden Krisen muss auch aus anderen Gesichtspunkten gedacht werden: "Basel II" verpflichtet die Banken, das Kreditrisiko von Unternehmen genauer zu überprüfen, wozu auch gehört, dass die Unternehmen Vorkehrungen gegen Bestandsgefährdungen getroffen haben.

In Deutschland geht das seit 1. Mai 1998 geltende Gesetz zur Kontrolle und Transparenz in Aktiengesellschaften (KonTraG) noch weiter und verpflichtet die Vorstände von Aktiengesellschaften bei persönlicher Haftung, ein funktionsfähiges Risikomanagement-System einzurichten und den jährlichen Lagebericht um Angaben zu den Risiken einer künftigen Entwicklung zu ergänzen. Auch kann allgemein Organisationsverschulden vorliegen, wenn keine Vorkehrungen gegen Gefahren getroffen wurden.

Ein Druck, die innerbetrieblichen Sicherheitsmaßnahmen zu überprüfen und zu verbessern, ergibt sich für Firmen, die in die USA exportieren, auch aus dem Customs-Trade Partnership against Terrorism (C-TPAT). Von US-Behördenvertretern wird überprüft, ob das betreffende

Unternehmen in seiner internen Sicherheitsstruktur so gestaltet ist, dass terroristische Anschläge über seine Produkte ausgeschlossen sind. Ohne entsprechendes Zertifikat werden Waren dieses Unternehmens vom Zoll nicht mehr in das Land gelassen; die USA als Absatzmarkt gehen verloren. Dazu kommt, dass große Wirtschaftsunternehmen von sich aus bei ihren Zulieferern zunehmend regelmäßige Überprüfungen durchführen.

Die Existenz eines Unternehmens ist weniger dadurch bedroht, dass hin und wieder ein Laptop oder eine Bohrmaschine abhanden kommen. Eher geht es an die Substanz, wenn Schreibtischtäter am Werk sind oder Diebstähle und Betrügereien organisiert erfolgen. Es geht nicht darum, den Schwund von Waren bloß zu erfassen, sondern ihn auch zu analysieren, Querverbindungen zu Zeitschichten herzustellen, Verbindungen aufzudecken, Plausibilitätskontrollen einzuziehen und Auffälligkeiten herauszuarbeiten.

Bei der Fülle der zu verarbeitenden Daten müssen spezielle Computerprogramme (Analysts Notebook) eingesetzt werden, um Zusammenhänge zu erkennen. Schwindelfirmen ändern oft nur den Namen, nicht die Adresse oder die Kontonummer. Über gemeinsame Kontonummern werden Beziehungsgeflechte erkennbar, ebenso über das Miteigentum an Jachten oder Grundstücken.

Bei Kontrollmaßnahmen, die gegen Personen gerichtet sind, ist der Betriebsrat einzubinden und der Datenschutz zu beachten. Die Interpretation mancher Ereignisse geht durch ihre Komplexität über übliches Controlling hinaus und es darf nicht übersehen werden, dass eine Verwertbarkeit vor Gericht erzielt werden sollte, die zu einer wirtschaftlichen Lösung führt.

Mit E-Mails können leicht Dokumente versendet werden, ohne diese physisch transportieren zu müssen. Wer bei Ausschreibungen gegenüber der Konkurrenz regelmäßig das Nachsehen hat, dessen Verhandlungspartner die eigenen Vorstellungen genau kennt oder wer knapp vor der Einreichung der Patentschrift auf ein kürzlich erteiltes gleichartiges Patent stößt, sollte sich Gedanken über einen Abfluss von Information aus dem Unternehmen machen. Die Möglichkeiten, Mitarbeiter zur Ausspähung im eigenen Unternehmen zu veranlassen, sind vielfältig, und reichen von Geldüberweisungen auf verdeckte Konten über Beraterverträge und Finanzierung privater Aufwendungen bis zu "Studienreisen" mit ungewöhnlich hohem Freizeitwert, oder zu Vermögenswerten, die nicht rückverfolgbar sind, wie Schmuckstücke, Edelsteine oder gezielte Börsentipps. Blinder Aktionismus schadet in solchen subtil gelagerten Fällen nur; die Stärke liegt im Sammeln möglichst vieler Informationen bis hin zum Einsatz professioneller Ermittler, so dass sich aus einem Puzzle von Wahrnehmungen und Beobachtungen ein zusammenhängendes Bild ergibt.

Ein Betriebsgelände einzuzäunen, vermittelt keinen freundlichen Eindruck, eher den einer Kaserne. Was tun, wenn die Stadtverwaltung bei der Errichtung eines Betriebes verlangt, dass das Areal öffentlich zugänglich bleiben muss? Vor welchen Sicherheitsproblemen dabei die Heidelberger Druckmaschinen AG, ein Unternehmen mit 19.000 Mitarbeitern, gestanden ist und wie sie diese gelöst hat, hat der Leiter der Unternehmenssicherheit, Bernd Baum, dargestellt. Bei einer offenen Campus-Struktur ziehen sich die Schutz- und Verteidigungslinien für die einzelnen Gebäude auf deren Außenhaut zurück, die zugleich die juristische Abgrenzung ist – anstelle eines das Gelände umschließenden Zaunes.

Die Freiflächen zwischen den Gebäuden sind im vorliegenden Fall zwar Privatgrund, aber öffentlich zugänglich, beschränkt auf Fußgänger und Radfahrer. Die öffentliche Zugänglichkeit bedingt, dass die Haftung für die Verkehrsflächen übernommen werden muss. Zudem kommt dem äußeren Erscheinungsbild mehr Bedeutung zu: Waren können

nicht mehr auf den Verkehrsflächen gelagert werden, Staplerverkehr ist nur eingeschränkt möglich und Türen können im Sommer nicht mehr offen gehalten werden.

Die offene Struktur bietet Vorteile: Auf die Sicherheitsanforderungen der einzelnen Gebäude kann spezifisch eingegangen werden; sie sind bei einem im Gelände befindlichen Veranstaltungszentrum anders gelagert als im Forschungsbereich.

Markierungen der Wege und Hinweisschilder helfen bei der Orientierung und bieten den Vorteil, dass jemand auffällt, der sich außerhalb der üblichen Verkehrsströme bewegt. Kunden und Besucher werden auf ihren spezifischen Bereich verwiesen und lernen nur diesen kennen.

Große Bedeutung kommt der Videoüberwachung der Freiflächen zu, um Vorfälle zu dokumentieren und zur Entlastung bei Haftungsfragen. Videoüberwacht sind auch die Zugänge und Einfahrten zu den Gebäuden. Baum: "Profis gehen nicht durch Türen, die videoüberwacht sind." In Verbindung mit einem Leitstellenkonzept, in das alle Gebäude integriert sind, muss ein Mehr an Offenheit kein Weniger an Sicherheit bedeuten.

Kurt Hickisch