

SICHERHEIT/TECHNIK

Spione, Hacker, Katastrophen

Wie erkennt man Wirtschaftskriminalität? Wie lässt sich Risiko messen? Inwieweit dürfen Mitarbeiter überwacht werden? Wie begegnet man Katastrophen? Über diese und andere Themen referierten Experten bei der Fachtagung "Security" in Wien.

Veranstalter der Fachtagung am 22. und 23. März 2000 im Hotel Modul war das Institute for International Research (IIR); die Teilnehmer waren vor allem Sicherheitsbeauftragte der Wirtschaft. Eintägige Workshops über die Vorbeugung und Abwehr von Lauschangriffen sowie zur Analyse von Sicherheitsmaßnahmen vor Ort begleiteten die Veranstaltung.

Wirtschaftskriminalität

Von der Anbotslegung bis zur Bezahlung der Rechnung können einem Unternehmen durch interne Täter Schäden zugefügt werden. Warnsignale sollten es sein, wenn beispielsweise Auftragsbedingungen so formuliert sind, dass sie nur auf einen einzelnen Anbieter zutreffen, wenn der Bestbieter eine relativ kleine und unbekannte Firma ist, oder wenn Preisänderungen oder die Änderung von Ausschreibungsbedingungen kurz nach der Auftragsvergabe akzeptiert werden. Wenn Waren geliefert oder Dienstleistungen erbracht werden, sollte überprüft werden, ob tatsächlich alle Leistungen in vereinbarter Qualität und Quantität erbracht wurden oder ob etwas abgezweigt wurde, was sich hinter doppeldeutigen oder abgekürzten Beschreibungen auf Rechnungen verbergen kann. Geprüft werden sollte, ob Firmen ungewöhnliche Adressen haben, ob unter verschiedenen Namen dasselbe Briefpapier verwendet wird. Nahe beieinander liegende Anbotspreise könnten ein Hinweis auf Preisabsprachen sein.

Die EDV wird als Black-Box empfunden; man weiß nicht mehr, was dahinter vorgeht. Sicherheit ist nicht mehr nur ein physischer Schutz wie etwa ein Zaun oder Türschlösser, sondern vielmehr die Sicherstellung von Verfügbarkeit. "Dadurch, dass erfahrene ältere Arbeitskräfte gegen jüngere ausgetauscht werden, geht unschätzbare Wissen verloren", bedauerte Diplomkaufmann Rainer von zur Mühlen, "der Schatz eines Unternehmens ist vorhandenes Wissen."

Betriebsspionage

Aus der Welt der Agenten berichtete Manfred Fink. Es muss beim Ausspionieren nicht immer High-Tech im Spiel sein. Durch das Einschleichen in das Vertrauen von Zielpersonen kann durch simple Gesprächsabschöpfung viel in Erfahrung gebracht werden. Ein weiterer Weg ist es, scheinhalber Großaufträge anzubieten, die detaillierte Angebote erfordern, aus denen ein Teil der Problembewältigung ersichtlich wird. Auch Abfall ist informationshaltig (Briefkuverts mit Adressen). Empfehlenswert ist, den Zählerstand des Kopierers vor dem Wochenende zu notieren und mit dem Stand am nächsten Werktag zu vergleichen. Über Lüftungsschächte und Klimakanäle neben Konferenzzimmern kann mitgehört werden; Sitzungszimmer mit angrenzender Toilette sind abhörgefährdet. Altleitungen sind beim Abhören dienlich, ebenso Verbindungen zu Rauch- und Bewegungsmeldern. Lautsprecher in einem Raum können zu Mikrofonen umfunktioniert werden. Künstliche Pflanzen eignen sich für die Ausspähung besonders: die Abhöreinrichtungen brauchen nicht einmal wasserdicht zu sein.

Überwachung untreuer Mitarbeiter

Durch die fortschreitende Entwicklung der Informationstechnik bestehen weitgehende Möglichkeiten, die Tätigkeit möglicherweise untreuer Mitarbeiter zu überwachen. Rechtliche Grenzen liegen im Wesentlichen dort, wo die Menschenwürde berührt wird, erläuterte der Wiener Rechtsanwalt Dr. Alois Obereder. Genau wie die private Nutzung eines dienstlichen Telefons in geringfügigem und notwendigen Ausmaß (Arztbesuch, Behördenkontakt, Schulangelegenheiten der Kinder) nicht untersagt werden darf, gilt dies auch für die Nutzung des Internets im Büro. Es kann durchaus erwünscht sein, dass sich Mitarbeiter durch privates Surfen Kenntnisse im Umgang mit dem Internet verschaffen, die sie sonst nicht erwerben können. Durch eine lückenlose Überwachung wird die Menschenwürde zumindest berührt. Eine derartige Kontrollmaßnahme ist zustimmungspflichtig im Sinn des Arbeitsverfassungsgesetzes und ist ohne Zustimmung des Betriebsrats nicht rechtswirksam. Der Mitarbeiter könnte sogar auf Unterlassung einer derartigen Maßnahme klagen.

Quantifizierung des Risikos

Anhand des Chemiekonzerns Schering AG Berlin wurde erörtert, wie Gefahren quantifiziert werden können, um verschiedenartige Betriebe in Bezug auf das Gefahrenpotenzial miteinander vergleichen und ein Krisenmanagement entwickeln zu können.

Krisenmanagement

Welches Krisenmanagement Fluggesellschaften betreiben, wurde bei der Fachtagung "Security" von Peter Hödl (Austrian Airlines) dargestellt. Bei einem Flugzeugabsturz ist damit zu rechnen, dass innerhalb der ersten 24 Stunden Tausende besorgte Menschen anrufen. Beim Swiss-Air-Absturz am 2. September 1998 sind in dieser Zeit 12.000 Anrufe eingelangt, beim Absturz einer TWA-Maschine vor Long Island 60.000 Anrufe. In den ersten 48 Stunden waren beim Swiss-Air-Absturz zirka 1.000 Telefonbetreuer tätig, und in der ersten Woche 530 Betreuer vor Ort und auf diversen Flugplätzen. Insgesamt führten sie 59.000 Telefongespräche. Die Aufgaben der Emergency Response Organisation werden zum Teil übernommen vom TEC (Telefon Inquiry Center), wobei dem TEC-I(nformation) neben dem Erteilen allgemeiner Auskünfte das Sammeln und Weiterleiten von Informationen zukommt, dem TEC-A(ssistance) die Rückruftätigkeit und die Zusammenarbeit mit Behörden.

Das Special Assistance Team (SAT) übernimmt die Betreuung von überlebenden Passagieren und der Angehörigen, ein Go-Team ist jederzeit für die rasche Präsenz an der Unfallstelle startbereit und bereitet das Eintreffen des Field-Teams vor, das vor Ort die Aufbereitung der Katastrophe in Angriff nimmt. Für das Katastrophenmanagement sind ein bis eineinhalb Jahre zu veranschlagen. Zur Bearbeitung von Informationen wurde die Datenbank Case geschaffen (Catastrophe Administration Supporting Equipment). Die ersten 24 Stunden sind ausschlaggebend für das weitere Vertrauen und den Ruf einer Fluglinie. Oberstleutnant Gerhard Moser, Kommandant der Einsatzabteilung "Kranich" des Flughafens Wien und Leiter der Arbeitsgruppe Flugunfall im Innenministerium, hat einen Richtlinienenerlass des Innenministeriums zu Flugunfällen angekündigt, anhand dessen die Sicherheitsbehörden in Österreich Notfallpläne erstellen. Eine Sonderkommission wird zuständig sein für Bergung, Identifizierung, Vermisstenstelle und Auskunft, Ermittlung und Fahndung, Dokumentation, Logistik und Auslandseinsätze (Go-Team). Weitere mögliche Szenarien sind Zugsunglücke und Großbrände. Sinnvoll wäre ein österreichweites, einheitliches Call-Center für alle Katastrophen unter Beteiligung der Wirtschaft. Moser: "Ein funktionierendes System schafft Vertrauen in das staatliche und wirtschaftliche Gefüge."

Kurt Hickisch