



Tagung „Tatort Firma“: „Spionage ist das zweitälteste Gewerbe der Welt. Jeder hat seinen Preis.“

Tatort Firma

Experten referierten bei einer Tagung in Wien über Fragen der innerbetrieblichen Sicherheit und des Informationsdiebstahls in Unternehmen.

Der Sicherheitsbeauftragte ist bei manchen Unternehmen oft nur ein besserer Hausmeister“, sagte der ehemalige Generaldirektor für die öffentliche Sicherheit, Mag. Michael Sika, bei der Tagung „Tatort Firma“ am 6. Juni 2007 in Wien. Die Veranstaltung wurde von der Herausgeberin der Fachzeitschrift „Der Detektiv“, Cornelia Haupt, organisiert (www.der-detektiv.at). Dem oft gehörten Argument, was es denn bei uns auszuspionieren gebe, stellte Sika entgegen, dass auch Produktionsweisen und das hohe Know-how österreichischer Firmen lohnende Angriffsziele seien. Die Wirtschaftskriminalität schlage sich zwar nur mit etwa 3 bis 5 Prozent der Delikte in der Kriminalstatistik nieder, doch sei die Dunkelziffer hoch und die Schadenssumme für die Volkswirtschaft enorm. „Wir müssen mit allen Mitteln versuchen, die Wirtschaftskriminalität zu bekämpfen“, betonte Sika, der seit 2000 Präsident des *Kuratoriums Sicheres Österreich (KSÖ)* ist.

Wirtschafts- und Konkurrenzspionage seien nach wie vor ein wichtiges Thema, sagte Manfred Fink, Chef der *Fink Secure Communication GmbH* in Ahorn/Bayern. Nach der WIK-Sicherheits-Enquete, einer alle zwei Jahre durchgeführten Umfrage, hätten sich

2004 14 Prozent der befragten Unternehmen durch Wirtschaftsspionage, 45 Prozent durch Konkurrenzspionage und 49 Prozent durch Abhörversuche bedroht gesehen. Hauptangriffsziele seien Preisinformationen, gefolgt von Produktentwicklung und Produktionstechnik. Gefährdet seien Global Player, weiters Unternehmen in bestimmten Branchen wie Nano- und Biotechnik, Forschung, Raumfahrt, Life Science, und kleine Unternehmen dann, wenn sie in einer Marktnische erfolgreich seien.

Informationen dieser Art könnten zunächst legal aus offenen Quellen gewonnen werden (Open Source Intelligence – OSINT). „Was da im Internet an Selbstdarstellung über Firmen zu lesen ist, ist oft haarsträubend“, meinte Fink. „Da werden Fotos von Mitarbeitern ins Netz gestellt, samt Durchwahlnummern – nebenbei eine Fundgrube für Headhunter.“ Geschäftsberichte, Fachpublikationen, Pressemitteilungen, Erfolgsstorys würden auch von der Konkurrenz ausgewertet. Ausschreibungen mit der Aussicht auf lukrative Gewinne könnten nur zu dem Zweck erfolgt sein, an Know-how und technische Lösungen zu gelangen. Ähnliches gelte für Joint Ventures. Competitive Intelligence (CI), die „zivile Version“ der nachrichtendienstlichen Informati-

onsbeschaffung, dürfe nicht unterschätzt werden. „Wer über offene Wege Informationen verliert, ist selber schuld“, betonte Fink.

Brainware. Über Hard- und Software hinaus ist die „Brainware“ das möglicherweise bedeutendste Kapital eines Unternehmens, das Wissen seiner Mitarbeiter. Die Methoden, dieses Wissen abzuschöpfen, fallen unter Human Intelligence (HUMINT). Manche „Zufallsbekanntschaft“ auf Messen oder Kongressen ist nicht zufällig. Durch gezielte Lenkung eines Gesprächs merkt der arglose Partner nicht, dass er ausgehorcht wird. Ein beliebter Trick ist, in der Stadt des auszuspähenden Unternehmens verlockende Stellenangebote zu offerieren. Im vorgelieblichen Bewerbungsgespräch geht der Bewerber aus sich heraus und merkt nicht, dass er ausgehorcht wird.

Eher langfristig angelegt sind gezielte Einschleusungen von Personen. „Spionage ist das zweitälteste Gewerbe der Welt; jeder hat seinen Preis“, sagte Fink; das reiche bis zu Erpressungen.

Was die zur Informationsgewinnung durch elektronische Maßnahmen (Signal Intelligence, SIGINT) eingesetzte Technik betrifft, stellt sich für Fink nicht die Frage, ob man paranoid sei, sondern ob man „genug paranoid“ sei.

FOTO: KURT HECKSCH

Auch hochwertige drahtgebundene Übertragungswege würden zweckentfremdet benützt ebenso Busleitungen der Gebäudeleittechnik und von Gefahrenmeldeanlagen würden zur Übertragung digitalisierter Audiosignale herangezogen. Ob Leitungen in Nebenräume gezogen werden, kann oftmals nur messtechnisch ermittelt werden, ebenso eine Anzapfung.

Dazu kommt die Nutzung drahtloser Übertragungsverfahren. Sprachsteuerung ist Standard, ebenso Fernsteuerung von Parametern wie Ein- und Ausschalten, Frequenz, Leistung.

Bei der Tarnung von Audio- und Videoaufnahmegeäten sind der Fantasie keine Grenzen gesetzt. Verborgene Abhöreinrichtungen in belanglos erscheinenden Gegenständen des Alltags wie Steckerleisten, Kugelschreiber und Stempel können nur durch Röntgentechnik entdeckt werden. Telefonhörer sind verschweißt und können nicht mehr durch Aufschrauben geöffnet werden. Für alle gängigen Modelle von Mobiltelefonen sind über das Internet manipulierte Akkus erhältlich. ISDN-Telekommunikationsanlagen sind programmierbar und weisen versteckte



**Sicherheitstechnik-
experte Manfred
Fink: „Sicherheit
muss nicht teuer
sein.“**



**Robert Goliasch:
„Bequemlichkeit
und Sicherheit
sind einander
entgegengesetzt.“**

(Export-)Leistungsmerkmale auf, die ein Mithören erlauben. Aufschaltöne können unterdrückt oder unbemerkt kurz geschaltet werden. Telefone mit Freisprecheinrichtungen können durch entsprechende Programmierung als Wanze geschaltet werden, ohne dass der Raum betreten werden muss. Fernwartung macht dies auch nachträglich möglich, wenn die ursprünglichen Zugangscodes nicht geändert wurden.

Bei Videokonferenzenanlagen findet sich häufig, dass die automatische Rufannahme freigegeben ist, sodass von außen Bild und Ton in dem betreffen-

den Raum überwacht werden können. Häufig fehlt ein Passwortschutz. Ein Auto kann leicht für Abhörzwecke genutzt werden. Peilsender ermöglichen die Erstellung eines Bewegungsprofils.

„Sicherheit muss nicht teuer sein“, fasste Fink zusammen. Man könne vorbeugen, indem man Verkleidungen und Vertäfelungen vermeidet, Abdeckungen und Geräte nach durchgeführter Kontrolle kennzeichnet, etwa mit UV-Stiften oder geheimen Kratzspuren. Funkanwendungen, auch drahtlose Mikrofone, sollten weitgehend vermieden werden. Hochwertige Aktenvernichter sollten Standard sein, die Papier nicht bloß der Länge nach zerschneiden, sondern auch noch in Schnipsel zerteilen, denn Streifen lassen sich mit Mitteln der Informationstechnik wieder sinnvoll zusammenfügen. Auch daran sollte gedacht werden, dass im Aktenvernichter ein Zeilenscanner samt Datenspeicher eingebaut sein könnte.

Für alle wichtigen Übertragungen, Fax und E-Mail inbegriffen, sollte hochwertige Verschlüsselungstechnik eingesetzt werden. Für besonders gefährdete Räume empfiehlt sich eine

FOTOS: KURT HICKISCH



www.mercedes-benz.at/vito

Ein guter Partner schaut aufs Geld.

Der Vito EcoBus schon ab 19.490,-* Euro.

► Im Geschäftsleben braucht man Partner, auf die man sich verlassen kann. So wie den Vito EcoBus. Mit ADAPTIVE ESP® bringt er bis zu neun

Personen samt Gepäck oder Arbeitsgerät sicher ans Ziel. Egal ob zur Baustelle oder zum Hotel. Serienmäßige Klimaanlage und 116 PS machen die

Arbeit zum Vergnügen. Die aktuellen Finanzierungsangebote erhalten Sie jetzt bei Ihrem Mercedes-Benz Partner. Nur ein Mercedes ist ein Mercedes.



Mercedes-Benz

*Unverb. Richtpreis exkl. MwSt. und NoVA. Richtpreis für das Modell Vito 111 CDI EcoBus in kompakter Ausführung inkl. MwSt. und 13 % NoVA: € 26.069,-. Vito: Kraftstoffverbrauch 8,2-13,2 l/100 km. CO₂-Emission 217-315 g/km

ortner - der plan
 atelier für architektur
 und innenarchitektur

gumpendorfer straße 124 . 1060 wien
 fon +43 1 2080100 fax dw 4
 mobil +43 06991 2080100
 mail office@ortner-derplan.at
 www.ortner-derplan.at

GERHARD HEIMBERGER

Immobilientreuhand

A-2340 Mödling
 Frauensteingasse 7

- T: 02236/865 011-25
- F: 02236/865 011 10
- M: 0664/541 25 75

hausverwaltung@heimberger.co.at

Chirurgische Ordination
Dr. Werner SEIDL
 Facharzt für Chirurgie

2700 Wiener Neustadt
 Herrengasse 2a
 Tel.: 02622/244 44, 0664/10133 96
 Fax: 02622/856 66
 E-Mail: seidl@medicalnet.at
 Web: http://www.medicalnet.at/seidl

Ordinationszeiten:

Montag		15.00-19.00
Dienstag	8.00-13.00	
Mittwoch		14.30-17.30
Donnerstag		14.30-17.30
Freitag	8.00-13.00	

ALLE KASSEN

Raskov
Innenausbau KEG

Trennwände, Zwischendecken
 Brandschutz, Stuckarbeiten

1110 Wien
 Svetelskystraße 16/9/62
 Telefon u. Fax:
 01/33 44 988
 Mobiltelefon
 0676/322 96 82

Billini
 9. Porzellangasse 62
 315 43 64

Warme Küche täglich 11-23 Uhr

GRATIS
 Zustellservice
 (ab einem Bestellwert von € 8,40,
 darunter Zustellgebühr von € 1,50)

MENGENRABATT

- ab € 14,60 Bestellwert
 1 Dose Cola od. Fanta od. Sprite **GRATIS**
- ab € 25,50 Bestellwert
 1 Flasche Wein **GRATIS**
- ab € 36,50 Bestellwert
 1 Flasche Prosecco **GRATIS**

HAUSZUSTELLUNG
 von italienischen Spezialitäten und Qualitätsweinen (11-23 Uhr)

Baumeister und Malerbetrieb

KOPESZKY
 e-mail: bm.kopeszky@aon.at

2601 Sollenau, Böhlergasse 18/1

Zu- und Umbauten, Innenausbau,
 Sanierungsarbeiten
 Fassaden, Vollwärmeschutz
 Maler- und Anstreicherarbeiten
 für Innen und Aussen
 Tapeten, PVC- und Teppichböden

☎ Baumeister: 0699 / 107 11 431
 Fax: 0 26 28 / 615 00

☎ Maler: 0 26 28 / 624 50
 Fax: 0 26 28 / 624 50 1

TATORT FIRMA



KSÖ-Präsident Michael Sika: „Der Sicherheitsbeauftragte ist bei manchen Unternehmen oft nur ein besserer Hausmeister.“

hochfrequente Abschirmung. Auch organisatorisch kann Informationsabfließen vorgebeugt werden. Besuche von Fremden sollten nicht in den Büros, sondern in dafür vorgesehenen Räumen erfolgen. An Besucher sollten Ausweise ausgegeben werden – das schließt mit ein, dass die Mitarbeiter Ausweise tragen. Bei der Ausgabe des Besucherausweises sollte ein Personaldokument hinterlegt werden, das erst bei Verlassen des Unternehmens wieder zurückgegeben wird. Bei wichtigen, im Hotelzimmer geführten Gesprächen sollte der Fernseher und andere elektronische Geräte ausgesteckt werden.

„Bequemlichkeit und Sicherheit sind einander entgegengesetzt“, erläuterte Mag. Robert Goliash seine Erfahrungen als Berufsdetektiv, Fachberater für Sicherheitstechnik und als allgemein beideter und gerichtlich zertifizierter Sachverständiger für das Sicherheitsgewerbe. Eher selten sei Sicherheit ein finanzielles Problem; sie müsse in den Köpfen der Entscheidungsträger verankert sein. In 90 Prozent der Einbrüche genüge ein etwa 30 cm langer Schraubendreher, mit dem Zugänge aufgezwängt werden, und manchmal brauche es nicht einmal das. Goliash präsentierte einige Beispiele:

Der Schließzylinder der Tür zu einem Warenlager mit einem Warenwert über 200.000 Euro ragte 28 mm heraus, der Abreißschutz lag frei. Abdeckungen von Schließzylindern waren entweder von außen angeschraubt oder bloße Steckrosetten. Ein „Schließblech“ war aus Kunststoff. Ein von einem Staplerfahrer verursachtes Loch in einer Rolltür wurde nur mit Folie verklebt, obwohl dahinter Waren im Wert von etwa 1,5 Millionen Euro lagerten. Ein Rechenzentrum war zwar mit Zutrittskontrolle ausgestattet, eine Wand bestand aber aus Gipskartonplatten. In einem anderen Fall war eine gemeinsam genutzte Halle nur durch Hartfaserplatten abgetrennt. Verglasungen waren in Silikon eingebettet, das leicht aufgeschnitten werden konnte.

Kurt Hickisch

FOTO: KURT HICKISCH