Neue Ansätze

Wirtschaftskriminalität und Sicherheitsstrukturen innerhalb von Unternehmen waren Schwerpunkte des 11. Simedia-Forums für Sicherheitsverantwortliche am 29. und 30. Juni 2010 in Leipzig.

In den letzten Jahren ist im internationalen und deutschen Vergleich fast jedes zweite Unternehmen Opfer von Wirtschaftskriminalität geworden", sagte Rechtsanwalt Bernd H. Klose beim 11. Simedia-Forum unter Bezugnahme auf die Studie *Wirtschaftskriminalität 2005* von *PriceWaterhouseCoopers* und der Martin-Luther-Universität Halle-Wittenberg, „Von den deutschen Unternehmen mit über 5.000 Mitarbeitern waren 62 Prozent betroffen."

„Auffällig ist, dass Wirtschaftskriminelle aus Kontinentaleuropa ihr Geld hauptsächlich auf Standorten in der Karibik verbergen, Täter aus den USA hingegen eher in der Schweiz und Liechtenstein", berichtete Klose. „Jeder glaubt, im jeweils anderen Rechtssystem sei das Geld besser geschützt."

Im kontinentaleuropäischen Rechtsbereich erfolgt die Strafverfolgung durch die Behörden mit nur wenig Möglichkeiten für die Opfer, die Strafverfolgung zu betreiben. Der Geschädigte kann sich andererseits im zivilgerichtlichen Verfahren auf die Beweisergebnisse im Strafverfahren stützen, um sein Geld zurück zu bekommen. Im angelsächsischen Rechtsbereich *(Common Law)*, der sich auf alle Staaten des Commonwealth und somit auch auf die „beliebten" Offshore-Standorte in der Karibik (Cayman Islands, British Virgin Islands) erstreckt, gibt es zwar vorgerichtliche Ermittlungen, doch wird das Opfer straf- und zivilrechtlich weitgehend sich selbst überlassen. Es werden ihm aber massive Rechte zur Verfolgung seiner Interessen eingeräumt. Eine der Möglichkeiten, die in beiden Rechtssystemen eingesetzt werden kann, besteht darin, das Geldinstitut schriftlich auf den Umstand der unrechtmäßigen Herkunft des Geldes aufmerksam zu machen *(Mareva by letter)*. Aus strafrechtlicher Sicht hätten dann die Bestimmungen über Geldwäsche zu greifen. Zivilrechtlich kann sich das Geldinstitut nicht auf guten Glauben berufen und wird haftungs- sowie schadenersatzpflichtig. Um Informationen zu bekommen bzw. Informationen über einen künftigen Beklagten und das bei ihm verborgene Vermögen zu erhalten, gibt es im angelsächsischen Recht die *Norwich Pharmacal Order/Bankers Trust Order* – Rechtsinstitute, die erstmalig in Rechtsfällen in den Jahren 1974 bzw. 1980 entwickelt wurden und seither diese Bezeichnungen tragen. Beide Institute zusammen werden auch als *Information Injunction* bezeichnet. Anträge auf Erlassung dieser Verfügungen sind bei Gericht zu stellen, wobei der Kläger ausreichende Beweise für den Betrugsfall vorzulegen hat.

Bernd Klose: „Jede zweite Firma ist von Wirtschaftskriminalität betroffen."

Rainer von zur Mühlen: Rechenmodell zur exakten Kostenprognose.

Der Adressat der Verfügung muss in das Geschehen verwickelt und die einzige geeignete Informationsquelle sein und muss für die Kosten entschädigt werden, die ihm durch die Order entstehen. Ferner muss das Allgemeininteresse an der Auskunft gegenüber dem berechtigten Geheimhaltungsinteresse überwiegen und es muss der Kläger eine bedingte Schadenersatzverpflichtung abgeben. Mit dieser verpflichtet er sich, im Fall des Unterliegens in der Hauptsache

WORKPLACE VIOLENCE

Gewalt am Arbeitsplatz

Über Gewalt am Arbeitsplatz referierte Jens Hoffmann *(Team Psychologie & Sicherheit)*. Wenn Menschen körperlich oder seelisch verletzt werden, zieht das psychische oder körperliche Beeinträchtigungen nach sich, die sich in geringerer Arbeitsleistung, in Fehlzeiten oder Berufsunfähigkeit niederschlagen können. Eine Erhebung bei 550 Stalking-Betroffenen ergab, dass fast jedes vierte Opfer mindestens einmal krankgeschrieben war, und zwar durchschnittlich für 61 Tage.

„Es gibt Warnsignale, die sich aus erlebter Ungerechtigkeit entwickeln", erläuterte Hoffmann. „Manche sind geradezu Ungerechtigkeitensammler." Gewalt entwickelt sich und wird letztlich als „Option" angesehen. Der potenzielle Täter identifiziert sich mit anderen Gewalttätern, macht Andeutungen im Umfeld, ehe es zum offenen Ausbruch kommt. Zumeist handelt es sich um psychisch labile Menschen mit paranoiden oder querulatorischen Persönlichkeitszügen.

Im Unternehmen muss Sensibilität für solche problematischen Verhaltensweisen geschaffen werden, ebenso für Äußerungen von Hoffnungslosigkeit. Ein Bedrohungsmanagement ist einzurichten. Hoffmann wies auf die *Association of European Threat Assessment Professionals (AETAP)* hin. Ein Team, gebildet aus Unternehmenssicherheit, Personal- und Rechtsabteilung, Gesundheits- und Sozialdienst sowie dem Betriebsrat sollte sich um solche problematische Fälle kümmern und Gefahren entschärfen.

Fotos: Kurt Hickisch

Schadenersatz an den Beklagten zu leisten. Liegen diese Voraussetzungen vor, erlässt das Gericht ohne Anhörung des Betroffenen *(ex parte)* die Order, und zwar „sealed“, also bei Gericht unter Verschluss und ohne Erlaubnis des Gerichts nicht einsehbar, und „gagged“, was bedeutet, dass der Empfänger niemandem direkt oder indirekt vom Verfahren oder dem Inhalt der Order berichten und auch nicht Dritte warnen darf.

Der Order auf Herausgabe von Informationen oder den Nebenverfügungen nicht nachzukommen, wird als „Missachtung des Gerichts“ *(Contempt of Court)* angesehen und kann zu Haft, Geldstrafe, Beschlagnahme von Vermögen, Ersatzvornahme oder im Fall einer Gesellschaft zu deren Zwangsverwaltung führen.

Der Geschädigte kann ferner bei Gericht auf zivilrechtlicher Basis einen Durchsuchungs- und Beschlagnahmebeschluss erwirken *(Search Order)*, früher „Anton Piller Order“ nach einem 1976 geführten Prozess benannt, bei dem dieser Rechtsbehelf erstmals eingesetzt wurde. Er wird damit ermächtigt, vom Beklagten die Herausgabe bestimmter Gegenstände zu verlangen („kleine Anton Piller Order“) oder, sogar zur Nachtzeit, die Räume des Beklagten selbst zu durchsuchen und die einschlägigen Papiere oder Gegenstände mitzunehmen („große Anton Piller Order“). Die Verfügung ergeht ohne Einbeziehung des Beklagten. Der Antrag muss begründet sein, was den dargelegten Sachverhalt betrifft (starker Anscheinsbeweis – *strong prima facie case*), und es muss eine hohe Wahrscheinlichkeit bestehen, dass Beweise weggeschafft werden, wenn die Order nicht ergeht. Ferner muss

Dieter K. Sack: „Künftig Bachelor- und Masterstudium für Sicherheitsmanager.“

eine bedingte Schadenersatzverpflichtung abgegeben werden. Ein schuldhafter Verstoß gegen die „Search Order“ zieht die Sanktionen des *Contempt of Court* nach sich.

Letztlich kann durch Gerichtsbeschluss das Einfrieren des gesamten, auch unbekannten, Vermögens des Beklagten erreicht werden, wenn die Gefahr besteht, dieses könnte beiseite geschafft werden (*Freezing Injunction*, früher nach einem Rechtsfall aus dem Jahre 1975 als *Mareva Injunction* bezeichnet). Eine solche Verfügung ergeht ebenfalls ex parte, und kann entweder vor oder nach dem Urteil in der Hauptsache erfolgen.

Die *Search Order* und die *Freezing Order* gelten als die wirksamsten Mittel des angelsächsischen Rechts bei der Betrugsbekämpfung. Die Effektivität der Rechtsinstrumente zeigt sich darin, dass nach der erwähnten Studie weltweit zumindest die Hälfte der befragten Unternehmen teilweise die entzogenen Vermögenswerte zurückerhalten hat, ein Viertel dieser Unternehmen mit einer Quote von 60 Prozent.

Unternehmenssicherheit. Dieter K. Sack *(Sack Security Management)* zeichnete den Weg der Unternehmenssicherheit nach, den diese

Peter Loibl: „Die neue Norm für Leitstellen legt Vorgaben auf hohem Niveau fest.“

seit den 1960er-Jahren genommen hat: Der traditionelle Werkschutz erweiterte sich auf Grund der RAF-Anschläge in den 1970ern um den Personenschutz, und durch die Ostöffnung und Globalisierung in den 1990ern standen Entführung, organisierte Kriminalität und Erpressung im Mittelpunkt. Als Konsequenz bestellten die Unternehmen als Sicherheitsverantwortliche oft ehemalige Polizeibeamte. Die neuen Herausforderungen liegen im Kampf gegen Wirtschafts- und Konkurrenzspionage, Produkt- und Markenfälschung sowie im Informations- und Know-how-Schutz. Der Informationsschutz wird häufig allein der IT-Abteilung überlassen, geht aber über den Schutz von Bits und Bytes hinaus.

Zunehmend werden diese übergreifenden Sicherheitsaspekte unter der Organisationseinheit *Corporate Security* zusammengefasst, die näher an die Führungsebene heranrückt. Damit steigt das Anforderungsprofil für den Security Manager. Er muss die Sprache der Wirtschaft sprechen und Kenntnisse in Betriebswirtschaftslehre aufweisen, Fremdsprachen beherrschen, hohe soziale und sprachliche Kompetenz haben und offen für technisch-naturwissenschaftliche Fragestellungen sein. Strategisches Denken ist gefragt, kein bloßes Trouble-Shooting im Sinn des bloßen Lösens aktueller Probleme.

Der künftige Ausbildungs- und Berufsweg eines Security Managers wird, so Sack, über ein sechssemestriges Bachelor-Studium „Security Management“ verlaufen, gefolgt von einer mehrjährigen Tätigkeit in der Praxis. Für Spitzenpositionen soll ein berufsbegleitendes, viersemestriges Masterstudium Standard werden.

Neue Norm für Leitstellen. Über die spätestens mit Ende 2010 EU-weit geltende Leitstellen-Norm EN 50518 informierte DI Peter Loibl, Geschäftsführer der „von zur Mühlen´schen GmbH“. Die Norm betrifft Alarmempfangsstellen (AES), gleichzusetzen mit *Notruf- und Serviceleitstellen (NSL),* und bezieht sich auf Alarm-, Einbruch- und Überfallmeldeanlagen, CCTV-Überwachungs- und Zutrittskontroll- sowie Personen-Hilferufanlagen und damit die betreffenden Sicherheitsdienstleister, Polizei, soziale Dienste, Werkschutzzentralen, kommunale Leitstellen, Aufzugsnotrufe und Ähnliches.

Teil 1 der Norm, der bereits fertiggestellt ist, legt die Mindestanforderungen an die Planung, Ausführung und die erforderlichen Einrichtungen für Örtlichkeiten fest, in denen im Rahmen eines einheitlichen Sicherheitskonzeptes (Alarm-)Signale überwacht, empfangen und verarbeitet werden. In den – noch in Bearbeitung befindlichen – Teilen 2 und 3 werden die technischen Anforderungen an eine AES bzw. die mindest notwendigen Abläufe und die Mindestanforderungen an deren Betrieb festgelegt. Beide Teile werden Anfang/Mitte 2011 in Kraft treten.

Die baulichen Anforderungen, denen eine der Norm

Fotos: Kurt Hickisch

entsprechende AES künftig zu entsprechen hat, sind mit jenen an ein Rechenzentrum zu vergleichen. Die Außenwände müssen aus massivem Mauerwerk oder Stahlbeton von mindestens 10 cm Stärke bestehen, die Fenster müssen durchschusshemmend (FB4 bzw., hinsichtlich des Glases BR4-S) ausgeführt sein. Toiletten und Waschgelegenheiten müssen sich innerhalb der AES befinden. Die AES muss mit einer Notstromversorgung durch Generator für 24 Stunden ausgerüstet sein und eine geschützte Lüftungsanlage haben. Türen und Schleusen müssen mit Überfalls- und Einbruchsmeldeanlagen des Sicherheitsgrades 3 ausgestattet sein, diese mit Öffnungs- und Verschlussüberwachung. Außenhaut, Zugänge und Durchreichen sind mit Videotechnik abzusichern, die ein Identifizieren von Personen zulässt.

Des Weiteren muss der Telefonsprechverkehr mit Datum und Uhrzeit automatisch aufgezeichnet und drei Monate lang gespeichert bleiben, Daten über Signale und durchgeführte Maßnahmen zwei Jahre lang. Täglich sind Funktionsprüfungen durchzuführen und Notfallpläne sind zu erstellen. Die AES ist ständig mit zwei überprüften und qualifizierten Personen zu besetzen. Betriebsabläufe sind zu dokumentieren.

Vom Betrieb her (Teil 3) werden ein jährliches Audit durch eine akkreditierte Stelle, ein dokumentiertes Verfahren für Kundenbeschwerden und für die Datenverwaltung gefordert. Ferner muss die Möglichkeit bestehen, Alarme verifizieren zu können. „Die Norm legt Vorgaben auf hohem Niveau fest, gleichgültig, ob diese, dem tatsächlichen Gefährdungsgrad nach, erforderlich sind oder nicht“, führte Loibl aus. „Wohl kaum eine Leitstelle wird EU-konform sein. Die hohen Ansprüche werden die NSL-Landschaft ausdünnen.“

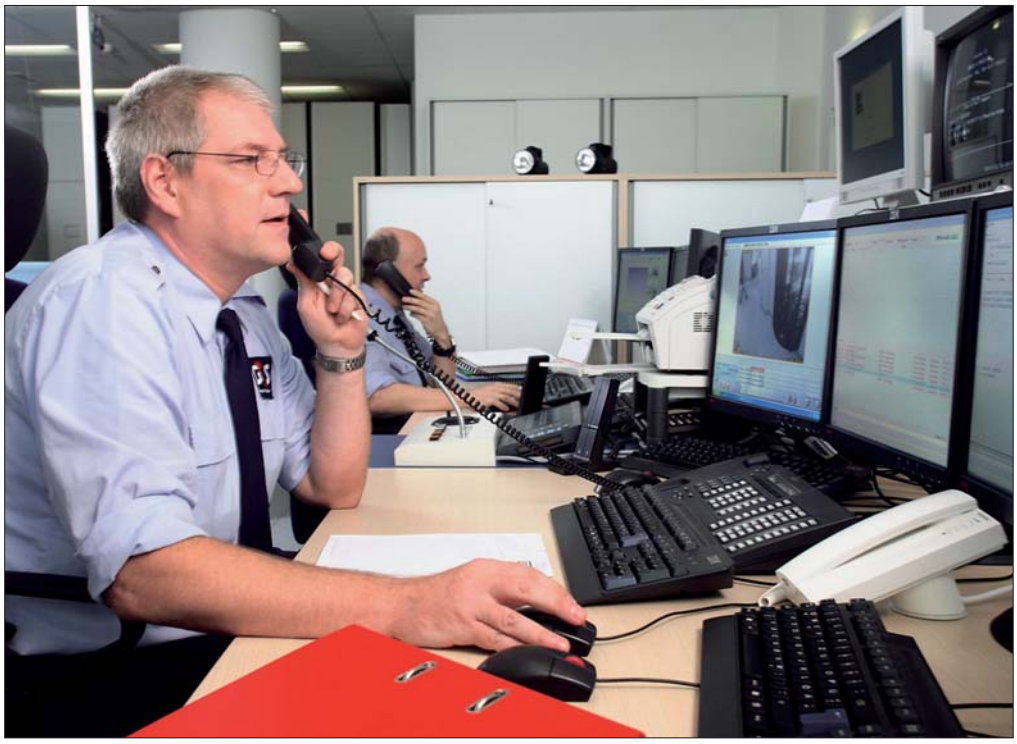

Foto: G4S

Notruf- und Sicherheitsleitstellen: Neue Norm bis spätestens Ende 2010 EU-weit in Geltung.

Normen sind anerkannte Regeln der Technik. Sie nicht einzuhalten, zieht keine unmittelbaren Sanktionen nach sich. Doch können sich vielfältige Haftungsfolgen ergeben. Es wäre eine Vertragsverletzung, wenn beispielsweise in Verträgen zur Aufschaltung von Alarmen bei der Anlage der jeweilige Stand der Technik vorausgesetzt oder ausbedungen wird, dieser aber nicht gegeben ist. Sollten Mitarbeiter durch eine solche Anlage zu Schaden kommen, kann das Auswirkungen bis ins Strafrecht haben, einschließlich vorwerfbarem Organisationsverschulden. Sollte durch eine nicht der Norm entsprechende Anlage gegenüber einem Mitarbeiter, einem Vertragspartner oder einem Dritten ein Schaden entstehen, besteht Schadenersatzpflicht. Versicherungen könnten die Schadensdeckung ablehnen. Letztlich wird die Norm die Basis von europaweiten Ausschreibungen werden.

Dipl.-Kfm. Rainer von zur Mühlen stellte ein Rechenmodell zur exakten Kostenprognose in Abhängigkeit von Modellvarianten in der Wach- und Sicherheitsdienstleistung vor. Über Lernmodelle zur Steigerung des Sicherheitsbewusstseins berichtete Dr. Christoph Schog (T-Systems International GmbH).

Kurt Hickisch
http://www.simedia.de

SECURITY MANAGEMENT

STUDIENGÄNGE

Donau-Universität Krems, MariaLukas, MSc, maria.lukas@donau-uni.ac.at
Fachhochschule Campus Wien, Martin Langer, martin.langer@fh-campus-wien.ac.at
Fachhochschule Brandenburg, Prof. Dr. Friedrich Holl, holl@fh-brandenburg.de
Fachhochschule für Verwaltung und Dienstleistung Altenholz, Dr. Ralf Kramer, kramer@fhvd.de
Hochschule der Polizei Hamburg, Jörg Feldmann, joerg.feldmann@hdp.hamburg.de
Hochschule für Öffentliche Verwaltung Bremen, Prof. Dr. Claudia Kestermann, claudia.kestermann@hfoev.bremen.de
Hochschule für Wirtschaft und Recht Berlin, Prof. Dr. Claudius Ohder, c.ohder@fhvr-berlin.de
Steinbeis Business Academy, Dr. Joachim Lindner, joachim.lindner@shb-sba.de

ZERTIFIKATSLEHRGÄNGE „SECURITY MANAGER“

BKA-FHB, Heiko Schneider, heiko.schneider@bka.bund.de
European Business School, Jasmin Engel, jasmin.engel@ebs-slie.de