Unternehmen Sicherheit

Wirtschaftskriminalität ist in vielen Firmen ein unterschätztes Risiko. Dass in den vergangenen Jahren weniger Fälle erfasst wurden, ist nach Meinung von Experten trügerisch. Wer vor dem Schaden klug sein will, sorgt vor – durch technische Barrieren und klare Regeln für den Umgang mit Daten.

Elektronische Türschranken sind in vielen Unternehmen bereits Standard. *Foto: PA/ZB*

Die Frontstadt Berlin war lange Jahre ein filmreifer Tummelplatz für Spione aus Ost und West. Und heute? Mit ihren politischen Entscheidungsträgern, Vorstandsetagen, Forschungszentren ist die Hauptstadt, wie andere Metropolen auch, ein Schauplatz für Wirtschaftskrimis - mit Datenklau, Produktpiraterie, Korruption oder ganz profanen Fällen von Betrug, Diebstählen und Vandalismus?

Dabei scheint die Berliner Kriminalstatistik Entwarnung zu geben. Betrugsfälle, Straftaten im Zusammenhang mit Insolvenzen, Anlage-Finanzierungen, Beteiligungen und Kapitalanlagen oder auch Verstöße gegen das Wettbewerbsrecht gehen seit einigen Jahren zurück. 2007 sank die Zahl dieser Wirtschaftsdelikte um über 17 Prozent auf 5030 erfasste Fälle, im Jahr zuvor betrug der Rückgang sogar 30 Prozent. Der Gesamtschaden dieser Taten sank von rund 518 Mio. Euro in 2005 auf knapp 325 Mio. Euro in 2007.

Von Entwarnung will jedoch Carsten Baeck, Geschäftsführer der DRB Deutsche

Risikoberatung GmbH (Berlin), nichts wissen. „Die rückläufigen Fallzahlen der Polizeistatistiken täuschen“, so Baeck, der auch den Vorsitz des Arbeitskreises für Unternehmenssicherheit (Akus) in Berlin innehat. Zurückzuführen seien sie eher auf Modifikationen bei der statistischen Erhebung, dem wenig ausgeprägten Anzeigeverhalten der Unternehmen oder gar auf mangelnde Wehrhaftigkeit der Polizei.

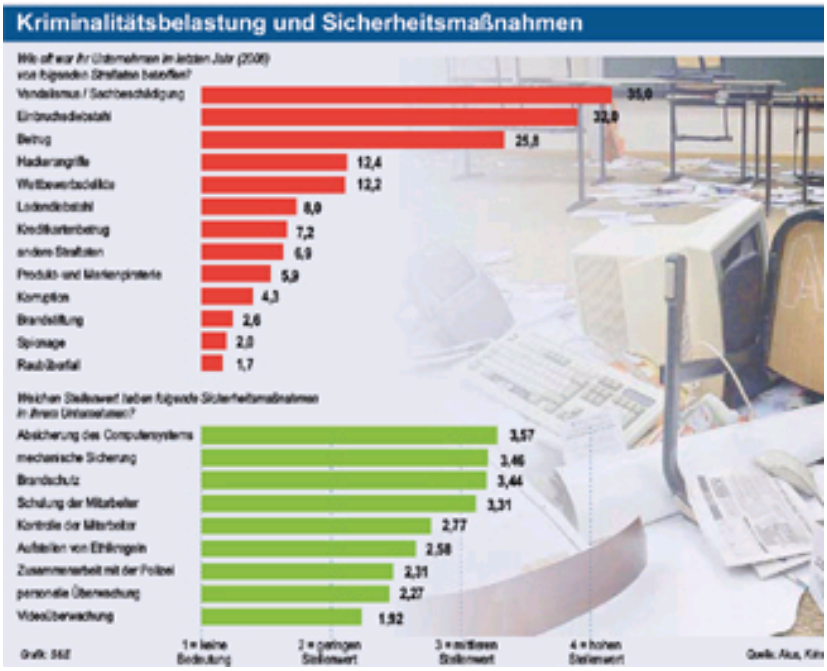
Das Landeskriminalamt seinerseits verweist darauf, dass Wirtschaftskriminalität in ihrer langjährigen Entwicklung erheblichen Schwankungen unterliegt. Kriminelle Großserien könnten das Bild rasch wieder ändern. Wie bei der Computer-Kriminalität geschehen. Nach Jahren des Rückgangs sind die Fälle, in denen das Internet als Tatmittel genutzt wird, 2007 wieder deutlich um rund 17 Prozent auf über 8000 angestiegen. Zugenommen haben vor allem Delikte durch rechtswidrig erlangte PIN-Codes, Computersabotage, Fälschung, Veränderung und Ausspähung von Daten.

Anders als in Berlin zeigt die Brandenburger Statistik den Trend nach oben: Um fast 45 Prozent stiegen die Wirtschaftsdelikte allein zwischen 2004 und 2006. Und auch 2007 legten sie vor allem durch komplexe Großverfahren um rund ein Fünftel auf jetzt fast 8000 Fälle zu. „Es besteht kein Grund zum Skandalisieren und Dramatisieren“, relativiert Dr. Knuth Thiel, Geschäftsführer des Akus in Brandenburg und zuständig für das Thema Sicherheit in der Wirtschaft bei der IHK Ostbrandenburg (Frankfurt/Oder). Häufigkeit und Struktur der Wirtschaftskriminalität in der Hauptstadtregion habe sich in den letzten Jahren kaum verändert.

"Es besteht kein Grund zum Skandalisieren und Dramatisieren." Dr. Knuth Thiel, Geschäftsführer des Akus Brandenburg. *Foto: IHK Ostbrandenburg*

Bestätigt wird diese Einschätzung auch vom Kriminalitätsbarometer Berlin-Brandenburg 2007“. Diese vergleichende Studie zur Belastung der Wirtschaft mit Kriminalität wurde von der Akus in Zusammenarbeit mit den drei Industrie- und Handelskammern in Brandenburg (Potsdam, Ostbrandenburg, Cottbus) sowie der IHK Berlin durchgeführt.

Die Ergebnisse: Die über 1100 repräsentativ ausgewählten Unternehmer waren im Jahr 2006 am häufigsten betroffen von Vandalismus (35 Prozent) mit durchschnittlich 7500 Euro Schaden, dicht gefolgt von Einbruchdiebstahl (32 Prozent, Schäden: 10 bis 180 000 Euro) und Betrug (25,8 Prozent). Hackerangriffe und Verstöße gegen Wettbewerbsrecht (je 12 Prozent) sowie Ladendiebstahl (8 Prozent) und Kreditkartenbetrug (7 Prozent) rangierten im Mittelfeld. Straftaten der „klassischen“ Wirtschaftskriminalität wie Produkt- und Markenpiraterie (knapp 6 Prozent), Korruption (4 Prozent) und Spionage (2 Prozent) spielten bei den befragten Firmen eine eher geringe Rolle.

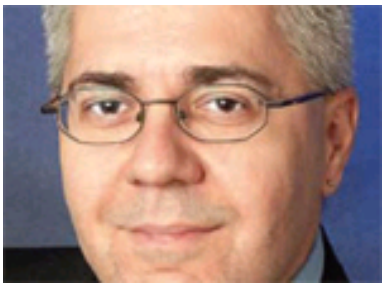


Grafik: S&E

Der Vergleich mit der Vorgängerstudie 2004 bestätigt, dass sich an dieser Grundstruktur der Delikte nichts geändert hat – allerdings mit regionalen Unterschieden. Von Betrügereien mit Kreditkarten sowie von Produkt- und Markenpiraterie etwa sind Berliner Unternehmer mehr als doppelt so häufig betroffen wie ihre Kollegen in den IHK-Einzugsgebieten Potsdam, Frankfurt/Oder und Cottbus. Diese wiederum leiden deutlich häufiger unter Vandalismus und Einbrüchen. Deutschlandweit wurden 2007 nach Angaben des Bundeskriminalamtes durch Wirtschaftsdelikte Schäden in Höhe von 4,1 Mrd. Euro verursacht. Das ist rund die Hälfte des erfassten Gesamtschadens durch Straftaten, dabei machen Wirtschaftsdelikte nur 1,4 Prozent aller Straftaten aus.

Was aber ist zu tun, um kriminelle Energie auszubremsen? Bei den befragten Unternehmen haben das Anbringen von mechanischen Einbruchssicherungen, Brandschutz, Schulung und Kontrolle von Mitarbeitern oder das Aufstellen von Ethikregeln durchaus gehobene Priorität. Am wichtigsten ist ihnen aber die Absicherung ihres Computersystems.

Das ist verständlich. „Hackerangriffe treffen die Seele des Unternehmens“, so Akus-Experte Dr. Knuth Thiel. Bei den meisten Unternehmen laufe jede Kommunikation, jeder Transfer durch Computer und IT-Netzwerke. Wichtigste Präventionsmaßnahme ist hier, so Michael Taube, Senior Consultant der Teko Systemkonzept GmbH (Potsdam) und Vorsitzender des Akus-Fachausschusses IT-Sicherheit, die Einführung eines wirksamen Sicherheitsmanagements etwa beim Umgang mit dem Internet. Hierdurch kann nicht nur das Herunterladen von Schaddateien wie Viren und Trojanern vermieden werden. Auch der durch private Nutzung des World Wide Web verursachte Zeitklau, die Verschwendung von Arbeitszeit, stelle für manche Unternehmen ein Problem dar. Taubes Tipp: Abschalten, den Internetzugang reglementieren oder übers Betriebssystem technisch unmöglich machen. Wie bei solchen Maßnahmen das Betriebsklima retten? „Wichtigstes Mittel ist die Aufklärung der Mitarbeiter durch fortlaufende Schulungen zu den verschiedenen Aspekten der Internet- und Computersicherheit, nicht zu vergessen auch das Nachfassen und erinnern etwa per Mail“, so Taube.



"Wichtigstes Mittel ist die Aufklärung der Mitarbeiter." Michael Taube, Senior Consultant er Teko Systemkonzept GmbH (Potsdam) *Foto: Teko Systemkonzept*

Mindestens ebenso wichtig ist die Datensicherheit. Immer neue Hiobsbotschaften gehen durch die Presse: Betrugszahlen beim Online-Banking auf Rekordhoch. Kundendaten samt Kreditkartennummern von Hackern in einem Berliner Hotel ausgespäht. Illegaler Datenhandel weitet sich aus und ruft Politiker auf den Plan. Was aber können Unternehmen tun, um sich vor Datenklau zu schützen? IT-Experte Taube sieht zwei Ansatzpunkte. Zum einen könne mit einfachen technischen Mitteln unmöglich gemacht werden, externe mobile Datenträger wie Notebooks und USB-Sticks an die Computer im Unternehmen anzuschließen. Zum anderen gehe es darum, die Mitarbeiter für den sicheren Umgang mit kritischen Daten zu sensibilisieren. Hier würden Sicherheitsrichtlinien, die die Zugriffsrechte etwa auf Daten der Lohnbuchhaltung steuern, helfen. Es empfehle sich, rät Michael Taube, Kennwörter regelmäßig zu ändern und Zugriffe auf sensible Daten sorgfältig zu dokumentieren. In vielen Unternehmen gehören jedoch auch mobile Laptops zum Arbeitsalltag. Um sie vor Daten-Dieben zu schützen, gehen Hersteller wie Fujitsu Siemens, Dell oder Hewlett Packard immer mehr dazu über, ihre Notebooks mit Lesegeräten von Fingerabdrücken auszurüsten. Wirksame „Fingerprinter“ gibt es bereits ab 20 Euro. Das Mindestmaß für kleine und mittelgroße Unternehmen: Der Einsatz von Virenscannern und Firewall, mit deren Hilfe kontrolliert werden kann, welche Datenpakete durchgelassen werden. Wichtige Daten sollten zudem zentral gespeichert und regelmäßig durch Backups gesichert werden.

„Wir haben ein riesiges Problem mit der Wahrnehmung von Sicherheitsrisiken im Mittelstand“, so der Akus-Vorsitzende Carsten Baeck. Um sich die eigenen Risiken bewusst zu machen, seien drei Fragen entscheidend: Was sind unternehmenskritische Prozesse? Wo sind Angriffspunkte mit hoher Schadenwirksamkeit? Wie wird entsprechend dem Gefährdungsgrad geschützt? Häufig fehlt es jedoch noch an den einfachsten Vorsorge-Maßnahmen. „Das fängt bei der Außenhaut des Gebäudes an“, so René Etzdorf, Sicherheitsberater und Vorsitzender des Akus-Fachausschusses Sicherheitstechnik. „Eingangstüren, Fenster und Tore sind in null Komma nichts überwunden.“ Dabei gebe es einfache Sicherungstechniken mittels Querriegeln oder senkrecht angebrachten Stangen bereits ab 300 Euro. Sicherungen mit Metallplatten seien für rund 1000 Euro zu haben.

Wenn der Einbrecher erst einmal drin ist, geht es mit der Unachtsamkeit weiter. Sensible Produkte, Muster, Konstruktionszeichnungen und auch Daten liegen häufig offen herum. „Industriespionage ist ein kriminelles Betätigungsfeld, das die Zukunft bestimmen wird“, sagt Etzdorf. Sein Tipp für den Grundschutz: Anschaffung von Tresoren und Sicherheitsschränken. Zusätzliche Sicherheit biete der Einbau von Einbruchmeldeanlagen, ausgestattet mit Öffnungskontakten zu Türen sowie mit Glasbruchsensoren,

Bewegungsmeldern und als Zusatznutzen mit Rauchmeldern. Einfache Systeme zur Innenraumüberwachung gebe es schon ab 400 Euro. Auch auf Mietbasis seien sie erhältlich. Bei Geschäften mit Publikumsverkehr seien zudem Überfall-Tasten unerlässlich.

Auch die Video-Überwachung gewinnt zunehmend an Bedeutung, nicht nur zum Schutz vor Ladendieben. René Etzdorf: „In letzter Zeit hatten Straftäter vermehrt Autohäuser und auch Baumaschinenhändler im Visier. Die Maschinen tauchen dann irgendwann in Osteuropa auf.“ Hier seien Systeme zur Videoüberwachung angebracht, vor allem wenn sie digital aufzeichnen können und über eine intelligente Auswertungssoftware verfügen. Diese Technik sei inzwischen so ausgereift, dass sie nur Alarm schlage, wenn sie bestimmte Bewegungsszenarien erkenne.

Bei der Zutrittskontrolle etwa zu Büroräumen werden normale Sicherheitsschlösser zunehmend durch elektronische Lösungen ersetzt. Zutritt erhält nur, wer über einen Transponder oder eine Chip-Karte verfügt, die berührungslos über ein elektronisches Lesegerät eindeutig identifiziert werden. Zusatznutzen ist, bei Verlust muss nicht mehr das gesamte Schließsystem ausgetauscht werden. Die Umprogrammierung des Zugangscodes reicht. Für Unternehmen mit besonderen Sicherheitsbereichen etwa für Forschung oder Produktentwicklung werden biometrische Erkennungssysteme zunehmend interessanter. „Auch hier macht die Technik Fortschritte“, weiß René Etzdorf. Das gelte vor allem für die sichere Detektion von Fingerabdrücken und Augenhintergrund oder Iris. Hier fangen die Kosten für technisch hochwertige Anlagen jedoch bei 10 000 Euro an – nach oben offen.

Bei der Entwicklung derartiger Hightech tut sich in Berlin etwa die Bundesdruckerei besonders hervor. Bei den Olympischen Spielen in Peking hat sie mit einem biometrischen Akkreditierungssystem für sicheren Zutritt ins „Deutsche Haus“ gesorgt. Besucher mussten sich zu Beginn akkreditieren. Benötigt wurden hierfür ein Foto und die einmalige Vorlage des Personalausweises. Zudem wurden Fingerabdrücke genommen, die für die Dauer der Spiele auf der biometrischen ID-Karte gespeichert blieben. Wer das Haus betreten wollte, musste seine Karte auslesen lassen und die Identität zudem mit dem Fingerabdruck bestätigen. Großunternehmen haben in der Regel schon ein ausgeprägtes Sicherheitsbewusstsein. Sicherheitsabteilungen werden bereits dem Compliance-Officer unterstellt, so Akus-Vorsitzender Baeck. Ziel sei, das Handeln nach Sicherheitsvorschriften auf allen Konzern-Ebenen durchzusetzen. Mit dem Berliner Innensenat hat der Akus vor zwei Jahren eine Sicherheitspartnerschaft geschlossen, insbesondere um den Informationsaustausch zwischen privater Wirtschaft und öffentlichen Behörden zu fördern. Vertreter beider Seiten treffen sich alle zwei bis drei Monate.

"Die rückläufigen Fallzahlen der Polizeistatistiken täuschen." Carsten Baeck, Geschäftsführer der DRB Deutsche Risikoberatung GmbH (Berlin). *Foto: DRB*

Carsten Baeck: „Die Zusammenarbeit ist sehr intensiv.“ Aktueller Themen- Schwerpunkt: Krisen-Kommunikation. Hierzu gab es in diesem Jahr bereits drei Workshops. Im Fokus stehen vor allem kritische Infrastrukturen wie die Bahn, Wasser- und Energie-Versorgung. In öffentlicher Hand gab es da eingespielte Krisenpläne, Privatisierungen stellen neue Herausforderungen an Kommunikation und abgestimmtes Handeln. 2009 ist ein Symposium zu Pandemien geplant. Denn die großflächige und rasante Ausbreitung von Krankheitserregern gefährdet nicht nur das öffentliche Gemeinwesen, sondern auch die Wirtschaft.

Heinz-Wilhelm Simon

Leserbrief an die BERLINER WIRTSCHAFT versenden	
Weitere Artikel der Oktober-Ausgabe 2008	zum Archiv

Mehr zum Thema:

- "Kriminelle Hacker lieben alles, was Geld bringt" (Dokument-Nr. 53937)

Dokument-Nummer: 53944

Industrie-und Handelskammer zu Berlin I Fasanenstraße 85 I 10623 Berlin
Tel. (030) 31 51 0-0 I Fax (030) 31 51 0-166 I E-Mail:service@berlin.ihk.de I Internet: http://www.berlin.ihk24.de