Berlin-Brandenburgische Unternehmens- und IT-Sicherheitstage

Mangelnde Sensibilität

Ziel der dritten Sicherheitsveranstaltung war es, die Unternehmens- und IT-Sicherheit zusammenzuführen – Bereiche, die in der Wirtschaft oft noch weit voneinander entfernt sind. Die Referenten verdeutlichten, dass die Überwachung eines Unternehmens mit biometrischen Lösungen, Videotechnik und Zugangskontrolle sichere informationstechnische Anwendungen voraussetzt.

Informationen schützen

Gemeinsam hatten der Arbeitskreis für Unternehmenssicherheit der IHK Berlin-Brandenburg (AKUS), die Interflex Datensysteme GmbH & Co. KG, Stuttgart, und die TimeKontor AG, Berlin, die zweitägige Veranstaltung organisiert. Rund 170 Teilnehmer waren der Einladung in das Berliner Ludwig-Ehrhard-Haus gefolgt.

Der Parlamentarische Staatssekretär im Bundesministerium für Wirtschaft und Arbeit, *Rezzo Schlauch* (Bild ❶), unterstrich die Wichtigkeit des Internets als Produktionsfaktor. Trotzdem mangele es an der notwendigen Sicherheit. So seien bei 76 % der deutschen Firmen in den vergangenen zwei Jahren Schäden aufgetreten. Ergriffene Schutzmaßnahmen und geringe Aufwendungen für die Sicherheit sprechen dafür, dass sich Betroffene mit den vorliegenden Empfehlungen wenig beschäftigen. Deshalb strebt die Initiative „Mittelstand sicher im Internet" die Entwicklung von branchenspezifischen Modulen an, um die Zielgruppe zu sensibilisieren und motivieren.

AKUS-Vorsitzender *Carsten Baeck* wies darauf hin, dass bei der Industriespionage firmeninterne Informationen genutzt werden. Die Sicherheit in diesem Bereich beginne bei Datenbanken, schließe das Fax ein und reiche bis zum gesprochenen Wort. Es sei erforderlich, Informationen zu schützen. In Da lian, China, fahre beispielsweise das Plagiat der Siemens-Straßenbahn Combino, die in Krefeld entwickelt und hergestellt worden ist. 2001 habe der sogar gleichfarbige Nachbau die Negativauszeichnung „Plagiarius" erhalten. Wie aber gehen Informationen verloren? Mögliche Angriffszenarien sind das Erschleichen von Informationen, die „panzerbrechende Putzfrau", die überall Zugang hat, und das Risiko Beratung. Wichtig sei die Mitarbeiterschulung, um Standards (ISO 17799/BS 7799) einzuführen, die eine Risikobewertung erlauben. Die Informationssicherheit verbinde IT-Sicherheit und Unternehmensschutz.

❶ **Als Beauftragter der Bundesregierung für den Mittelstand appellierte *Rezzo Schlauch* an die Unternehmen, die vorliegenden Sicherheitsempfehlungen anzuwenden.**

Foto: Wagner

Sicherheitsmanagement

Den Begriff „Sicherheit" versuchte Dr. *Christoph Thiel,* Fraunhofer-Institut für Software- und Systemtechnik (ISST), Berlin, zu erklären: Eine beurteilende Person spricht von Sicherheit, wenn alle vorgegebenen Anforderungen erfüllt sind. Absolute Sicherheit könne es nicht geben. Ein ganzheitliches Sicherheitsmanagement habe wenig mit Sicherheitstechnik zu tun, viel mehr jedoch mit Unternehmenskultur und Organisation. Maßgeblich für die Vorbeugung bzw. Bewältigung von Notfällen ist eine Planung, um in tolerierbaren Grenzen Geschäftsprozesse aufrechterhalten zu können. Aus Bedrohungen oder Risikokategorien lassen sich Risikoparameter ableiten. Diese sind Grundlage für eine Sicherheitsmanagementstrategie, in der mögliche Gefahren zu identifizieren und einzuschätzen sind. Die vorhandenen Informationen fließen in einen Steuerungsplan ein, der umzusetzen ist. Mit der nachfolgenden Kontrolle, also entsprechenden Korrektur, beginne der Regelkreis von Neuem.

Die Anfälligkeit eines Unternehmens zeigte Dipl.-Ing. *Torsten Lucht,* Control Risks Deutschland GmbH, Berlin, auf. Technische Schwächen ergeben sich aus der Wissensabhängigkeit und eventuellen Systemausfällen. Terroristische Anschläge und Sabotageakte, in deren Wirkungskreis eine Firma geraten kann, sind bei den politischen Risiken einzuordnen. Der Umgang mit derartigen „Einflüssen" erfordere eine gezielte Organisation der Sicherheitsmaßnahmen: Präventiv seien mögliche Schadenfälle zu inszenieren, um Handlungsabläufe planen und entsprechend reagieren zu können.

Videotechnik

Dipl.-Ing. *Rolf Senger,* SeeTec GmbH, Philippsburg, zufolge ist die Videoüberwachung der Zukunft eine digitale und netzwerkbasierte. Zentrales Element sind Netzwerk-Kameras, die mittels leistungsfähiger Datenkompression, geeigneter Schnittstellen und entsprechender Firmware Netze zur Übertragung hochwertiger Live-Bilder nutzen können. Wie bei vergleichbaren Netzknoten wählen sich autorisierte Teilnehmer über die IP-Adresse ein.

Den Kameras sind Aufträge durch Programmierung zuzuteilen, die Ausführung erfolgt selbstständig. Auswertungen, Verwaltungsaufgaben und die Sammlung von Dokumenten übernehmen allerdings die in das Netzwerk integrierten Computer.

Erstmals haben Anbieter die marktreife digitale Technologie bei der Messe „Security 2002" vorgestellt. Zwischen der Analog- und Digitaltechnik bestehen inzwischen keine qualitativen Unterschiede mehr. Es ist davon auszugehen, dass bis 2010 die analogen Kameras ausgetauscht sein werden.

Mitarbeiter – ein Sicherheitsrisiko?

Viele Vorträge stellten Angriffe verschiedenster Art von außen gegen Unternehmen dar. Die menschliche Beteiligung an diesen Schäden blieb weitgehend unberücksichtigt. Diesem Thema widmete sich schließlich Dr. *Michael Kossakowski,* Intelligenz System Transfer, Berlin, der sich mit der Risikoprävention aus psychologischer Sicht beschäftigte. Die Bereiche, die im Geschäftsalltag Gefahren bergen, sind vielfältig. Selbst die Personalauswahl zählt dazu. Statistische Erhebungen, welche Schäden ungeeignete Mitarbeiter verursachen, liegen derzeit nicht vor.

Der Ärger in einer Firma sei groß, wenn ein Kollege oder Vorgesetzter nicht so handelt, wie es die Unternehmensphilosophie erwarten lässt. Abhilfe biete das Auswahlverfahren „Jobfidence". Mit diesem bestehe eine etwa 80%-ige Chance, geeignetes Personal zu finden – Mitarbeiter, die von ihrer Persönlichkeit her für die neuen Aufgaben weder unter- noch überfordert sind. Denn jemand, dessen intellektuelle Fähigkeiten nur unter Gebühr beansprucht sind, kann ein Risiko darstellen: Sich aus Langeweile nicht an Vorgaben zu halten oder ständig neue Vorgehensweisen zu kreieren, erzeugt vermeidbare Fehlerquellen und verunsichert Mitarbeiter.

Mit einem Überblick über denkbare „Schwierigkeiten" stimmte der Psychologe auf Möglichkeiten ein, das Risikoverhalten bei Menschen wahrzunehmen.

I. Kölbl, S. Wagner