

Sicherheitstag in Berlin

Mehr Unternehmenssicherheit

Etwa 140 Geschäftsführer, Ingenieure und Sicherheitsverantwortliche kamen zum 2. Berlin-Brandenburgischen Sicherheitstag. Unter dem Motto „Unternehmenssicherheit von Z bis A“ zeigten die Referenten verschiedenste Lösungen, welche sich zu umfassenden Sicherheitssystemen verbinden lassen.

Steigende Gefahr

Die Ereignisse des 11. September 2001 haben weltweit eine Sicherheitsdiskussion angestoßen. Dennoch scheinen die Großindustrie mit ihren projektbezogenen, kurzfristigen Strategien und der Mittelstand, der die Bedrohung kaum wahrnimmt, der Gefährdungslage nicht gewachsen zu sein. Anlass genug, um auf dem von der Fa. Interflex Datensysteme sowie vom Arbeitskreis für Unternehmenssicherheit der IHK Berlin-Brandenburg (AKUS) ausgerichteten Veranstaltung im Rathaus Schöneberg für unterschiedliche Lösungsansätze bzw. komplexe Sicherheitssysteme im Bereich der Unternehmenssicherheit zu sensibilisieren.

Staatliche Unterstützung

Fritz R. Körper, Parlamentarischer Staatssekretär im Bundesministerium des Innern (BMI), betonte in seinem einleitenden Grußwort, dass die Unternehmenssicherheit für das BMI ein wichtiges Anliegen sei. Er lobte „die Bereitschaft der Wirtschaft, durch Eigenschutz zur Abwehr von Kriminalitätsrisiken beizutragen“. Sicherheitstechnik lasse sich in vielen Bereichen zur Kriminalprävention einsetzen. Die Nutzung der Videoüberwachung, der Zutrittskontrollsysteme oder der Techniken zur Informationssicherung belegen dies. Nicht zu vergessen seien biometrische Identifikationsverfahren, die derzeit in Anwendungsversuchen und Pilotprojekten getestet werden. Die Sicherheitsmaßnahmen der Unternehmen dürfe der Staat jedoch nicht als Freibrief betrachten, sich nicht an diesen Anstrengungen zu beteiligen. Insbesondere das BMI könne und müsse an der Optimierung der Unternehmenssicherheit mitwirken.

Sicherheitspartnerschaft

Moderator *Heinz G. Albach*, Arbeitsgemeinschaft für die Sicherheit der Wirtschaft e. V. (ASW),

hob die Notwendigkeit hervor, bestehende Berührungspunkte gegenüber der Wirtschaft und umgekehrt auszubauen. Den Gedanken führte *Carsten Baeck*, Vorsitzender des AKUS, mit der Sicherheitspartnerschaft fort. Diese erfordert es, sich gegenseitig zu kennen, voneinander zu wissen und sich fortlaufend auszutauschen.

Strategische Maßnahmen

Mit der Sicherheitspolitik von Unternehmen beschäftigte sich der AKUS-Vorsitzende in seinem Vortrag. Der auch nach dem New Yorker Anschlag oftmals unsensiblen, leichtfertigen Umgang mit Gefährdungslagen mache Anstrengungen um eine verantwortliche Sicherheitspolitik zunichte. Dabei „ist auch Deutschland nicht nur Rückzugsraum“, wie *Baeck*, Senior Consultant bei der Control Risks Deutschland, Berlin, verdeutlichte. Während im angloamerikanischen Raum bei erhöhten Sicherheitsbudgets der Chief Security Officer auf der zweiten Führungsebene eingesetzt wird, ist diese Funktion in Deutschland meist erst dem mittleren Management zugeordnet. Darüber hinaus handelt es sich häufig nicht um ein eigenständiges Aufgabengebiet. In den USA sind langfristige, allumfassende Sicherheitskonzepte die Regel. Hierzulande schwanken die Unternehmen zwischen Aktivismus und Fatalismus. Um sich vor den global zu beobachtenden Krisen und Bedrohungen zu schützen, benötigt ein Unternehmen ein funktionierendes Risikomanagement. Für dieses ist ein Risikoportfolio zu erstellen, mit dem sich die Gefahren bewerten lassen. Aus dem Risiko Monitoring ist dann die Risikoprävention abzuleiten.

IT-Sicherheit

Schon einleitend hatte *Körper* auf die oftmals vernachlässigte IT-Sicherheit hingewiesen. Vor allem



1 *F. R. Körper*, Parlamentarischer Staatssekretär im Bundesministerium des Innern (li.), und der AKUS-Vorsitzende *C. Baeck* befürworten den stärkeren Austausch zwischen Staat und Wirtschaft im Sinne einer Sicherheitspartnerschaft

Foto: S. Wagner

bekannte (40 %) und interne User (30 %) attackieren diesen Bereich. Wie *Gunter Hink*, Geschäftsführer der Fa. BIM Business Information Management, Wildau, erläuterte, ist alles angreifbar, womit kommuniziert wird. Angesichts der vielfältigen Möglichkeiten des unerwünschten Zugriffs – Viren, Trojaner, Keylogger, Mail- und SMS-Bomber u. a. – sind fachliche Beratung und ein sensibler Umgang mit den zur Verfügung stehenden Techniken unerlässlich. In einem gezielten „Hackertraining“ lehrt BIM Systemadministratoren und Datenschutzbeauftragte, sich in die Denk- und Handlungsweise von Angreifern hineinzuversetzen und Abwehrmaßnahmen zu ergreifen.

Zutrittskontrolle

Die Interessenlagen von Personal- und Betriebsräten bei Zutrittskontrollsystemen beleuchtete *Thomas Reuschenbach*, Geschäftsführer der DGB Technologieberatung e. V. Bei einer Zutrittskontrolle haben die Angestellten- und Arbeitnehmervertreter zwischen der Bedrohungslage und den demokratischen Grundrechten abzuwägen. Die Arbeitnehmervertretung ist gegenüber sicherheitstechnischen Maßnahmen häufig zuerst misstrauisch, da sie eine heimliche Mitarbeiterkontrolle auch über die Zeiterfassung hinaus befürchtet. Nur im Rahmen einer vertrauensvollen Zusammenarbeit zwischen Unternehmensleitung und Personalvertretung sind sicherheitstechnische Aspekte vermittelbar und erfolgreich umzusetzen. Als ein sicheres biometrisches Zutrittskontrollsystem stellte Dipl.-Betw. *Thomas Brenner* von der Fa. byometric systems, Mitterfelde, die Iriserkennung vor. Da das Irismuster mit mehr als 240 Einzelmerkmalen sich nach dem 18. Lebensmonat bis zum Lebensende nicht mehr verändert, ist die Erfassung grundsätzlich nur einmal erforderlich. Mit einer Videokamera lässt sich dieses Muster kontaktlos selbst durch Brillengläser, Kontaktlinsen und viele Sonnenbrillen

aufnehmen. Nach der Umwandlung der Merkmale in einen Iris-Code erfolgt der Abgleich mit den Aufzeichnungen in der Datenbank sowie der Zutritt oder die Zurückweisung.

Ausweissysteme

Über die Multifunktionalität von Ausweisen referierte Dipl.-Inform. *Karlheinz Bold* von der Fa. V.P.S. Video Print Systeme, Ettlingen. Ausweissysteme haben heute eine immer größere Anzahl von Schnittstellen zu unterschiedlichen Systemen zu berücksichtigen. Daneben beinhaltet der vorgegebene „Lebenszyklus“ jeder aktiven Karte, dass kein zweiter Ausweis mit den gleichen Daten produziert werden kann. Die s. g. Public-Key-Infrastrukturen (PKI) machen Ausweise fälschungs- und identifizierungssicher.

Erfolgreiche Präsentation

Die durch den AKUS geforderte Neukonzeption des Sicherheitstages im Sinne einer „firmenneutralen“ Veranstaltung hat sich nach Einschätzung von *Baeck* bewährt. Allgemeine bzw. grundlegende Informationen im Wechsel mit Workshops zu den Themen Glas-Nachrüstung, Risikomanagement, Videoüberwachung, Fluchttürsteuerung und Zutrittskontrolle bildeten wichtige Fragenkomplexe zur (Unternehmens-) Sicherheit ab und zeigten mögliche Lösungen. Zweifellos ist die konzeptionelle und strategische Vorbereitung auf Gefährdungen die wichtigste Voraussetzung für ein funktionierendes Sicherheitssystem.

Von allen Seiten gelobt wurde die Qualität des in den Pausen möglichen Austausches mit zahlreichen Ausstellern: Die konkreten Fragen des Fachpublikums fanden überall kompetente Ansprechpartner. Das große Interesse und das Feedback der Teilnehmer sind Wegbereiter für weitere Veranstaltungen dieser Art.

I. Köhl und S. Wagner