Industrie, Technologie, Energie, Umwelt

2. Tag der IT-Sicherheit

14.00 Uhr **Begrüßung**
Wolfgang Grenke,
Vizepräsident der IHK Karlsruhe
Dirk Fox, Geschäftsführer der Secorvo Security Consulting GmbH und Initiator der KA-IT-Si

14.15 Uhr **China auf der Überholspur – Know-how-Diebstahl in deutschen Unternehmen**
Karl-Friedrich Fecht, Landesamt für Verfassungsschutz Baden-Württemberg

14.45 Uhr **iPhone Security – Harmloses Gadget oder Sicherheitstrauma?**
Jörg Völker, Security Consultant bei Secorvo Security Consulting GmbH, Karlsruhe

15.30 Uhr **Räumen Sie auf in Ihrem Rack! Konsolidierte Netzwerksicherheit spart Kosten und Zeit**
Enzo Sabbattini, Astaro AG, Karlsruhe

16.15 Uhr **Pause und Networking mit Ausstellung**

Best Practice Vorträge mit Diskussion:

17.00 Uhr **Kontra Produktpiraterie** – IT-Sicherheit als zwingende Voraussetzung für einen Innovationsdienstleister
Dr.-Ing. Dirk Schweinberger, Geschäftsführer, tech-solute GmbH & Co. KG, Technologiefabrik Karlsruhe

17.45 Uhr **Technik allein hilft nicht** – Umgang mit dem Faktor Mensch im Kontext der IT-Sicherheit
Andreas Fritz, IuK Security Management, EnBW Energie Baden-Württemberg AG

18.30 Uhr **Ende der Veranstaltung**

Informationen
Telefon (07 21) 174-438
birgit.strunck@karlsruhe.ihk.de

Foto: Marc Dietrich, fotolia.com

IT-Sicherheit ist Pflicht

Geschäftsführer und Vorstände sind zur Sorgfalt des ordentlichen Geschäftsmannes verpflichtet. Diese Pflicht erfordert eine ordnungsgemäße Geschäftsorganisation, bestehend aus dem Erkennen der Verpflichtung, der Strukturierung der Aufgabenerfüllung und der Kontrolle des Ergebnisses. Kommt die Geschäftsführung dieser Verpflichtung nicht nach, haftet sie persönlich für den Sorgfaltsverstoß.

Prozesse

Die Organisation der Aufgabenerfüllung und eine wirksame Umsetzungskontrolle erfordern klare Zuständigkeiten und Prozesse. Hinsichtlich der IT-Sicherheit müssen Angemessenheit und Eignung der getroffenen Schutzmaßnahmen anhand präziser Soll-Vorgaben und regelmäßiger Überprüfungen des Ist-Zustands beurteilt werden. Minimum ist ein jährlicher Bericht an die Geschäftsleitung, der eine Risikobewertung, eine Auflistung der Schutzmaßnahmen und eine Darstellung des Umsetzungsstands (möglichst das Ergebnis einer unabhängigen Prüfung) umfasst.

Sicherheitsbewusstsein

Häufig beschränken sich Schutzmaßnahmen auf technische Mechanismen wie Virenschutz, Firewalls oder Verschlüsselungslösungen. Weithin unterschätzt wird die Schaffung von „Security Awareness". Denn Menschen sind gelegentlich nachlässig oder reagieren unbedacht – und bieten so oft mehr „Angriffsfläche" als ein IT-System. Das gilt auch für den Arbeitsplatz: Ein unverschlossenes Büro, einsehbare vertrauliche Unterlagen auf dem Schreibtisch und Dokumente mit Kundendaten im Papierkorb können sensible Informationen preisgeben.

Fast 60 Prozent aller Anwender würden einer kürzlich durchgeführten Befragung zufolge einem Mitarbeiter der IT-Abteilung am Telefon ihr Passwort preisgeben – oder dem, der sich dafür ausgibt. Auch mobile Datenträger, vor allem USB-Sticks – selten gelöscht und gelegentlich vermisst – bergen Risiken: 9.000 Exemplare fanden britische Reinigungen im vergangenen Jahr in Jacketts und Hosen.

Ein sorgfältiger Umgang mit IT-Risiken erfordert klare Vorgaben (Security Policy), dokumentierte Prozesse und unabhängige Prüfungen. Die Ergebnisse sollte sich die Geschäftsleitung regelmäßig vorlegen lassen – dann kann sie sicher sein, der Sorgfaltspflicht zu genügen.

Dirk Fox, Geschäftsführer der Secorvo Security Consulting GmbH, Karlsruhe, Mitinitiator der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si)