

Industrie, Technologie, Energie, Umwelt



4. Tag der IT-Sicherheit

Der Tag der IT-Sicherheit am 12. Juli im Karlsruher IHK Haus der Wirtschaft zeigt aktuelle IT-Sicherheitsbedrohungen für Unternehmen auf.

Programm:

- 14.00 Uhr Begrüßung**
Richard Schmitz, Erster Vizepräsident der IHK Karlsruhe
David Hermanns, Geschäftsführer CyberForum e. V.
Moderation: Dirk Fox, Geschäftsführer der Secorvo Security Consulting GmbH und Mitinitiator Karlsruher IT-Sicherheitsinitiative KA-IT-Si
- 14.10 Uhr Keynote: Hacking 2012 – Aktuelle Entwicklungen bei Angriffsmethoden**
Sebastian Schreiber, Geschäftsführer der SySS GmbH
- 15.00 Uhr Tatsachen, Techniken und Tücken – Sicherheit auf Hardwareebene**
Prof. Dr.-Ing. Tim Güneysu, Ruhr-Universität Bochum
- 15.40 Uhr Wunder durch Kryptographie**
Prof. Dr. Jörn Müller-Quade, Leiter des Instituts für Kryptographie und Sicherheit am Karlsruher Institut für Technologie
- 16.20 Uhr Pause mit Networking und Ausstellung**
- 17.10 Uhr Security by Design**
Wolfgang Reibenspies, EnBW Energie Baden-Württemberg AG
- 17.50 Uhr Sicherheit im Onlinebanking 2.0**
Boris Hemkemeier, Commerzbank AG
- 18.30 Uhr Ende der Veranstaltung**



Foto: elypse, fotolia.com

IT-Wirtschaftsspionage wird zur Regel

Zu diesem Ergebnis muss man kommen, wenn man die kürzlich veröffentlichte Studie „Industriespionage 2012“ von Corporate Trust liest: Anfang des Jahres 2012 wurden mehr als 6.900 Unternehmen mit mindestens zehn Mitarbeitern und über eine Million Euro Umsatz aller Branchen nach ihren Erfahrungen mit Wirtschaftsspionage befragt. Etwa neun Prozent der Unternehmen nahmen zu den Fragen differenziert Stellung; knapp 50 Prozent der antwortenden Personen gehörten dem Vorstand oder der Geschäftsleitung an.

Selbst wenn man annimmt, dass die Antworten eher von Unternehmen stammen, die bereits für das Thema Informationsschutz sensibilisiert sind, sind einige der Ergebnisse dennoch erschreckend. Mehr als 21 Prozent der Unternehmen waren danach in den vergangenen drei Jahren Opfer eines Falls von Wirtschaftsspionage; der Mittelstand war mit 23,5 Prozent überproportional betroffen. Die von den Unternehmen angegebenen Schadenshöhen lagen um durchschnittlich 50 Prozent über den Vergleichswerten einer Befragung aus dem Jahr 2007.

In den meisten Fällen (48 Prozent) waren eigene Mitarbeiter vorwiegend oder durch nachlässiges Verhalten ursächlich beteiligt, dicht gefolgt von Hackerangriffen (42 Prozent) und gezieltem Diebstahl von IT-Systemen (Laptops, Smartphones – 33 Prozent). Angriffe durch „Social Engineering“ lagen auf Platz fünf der Ursachen (23 Prozent), Einbruchdiebstahl hingegen „abgeschlagen“ auf Platz acht (11 Prozent).

Trotz dieser ernüchternden Zahlen fehlen in den meisten Unternehmen selbst grundlegende Schutzmaßnahmen wie klare Informationsschutzregeln (nur bei 46 Prozent vorhanden) oder die Verschlüsselung von Daten auf Notebooks und Laptops (nur bei 47 Prozent) – während zugleich in immer mehr Unternehmen die Nutzung von Privatgeräten der Mitarbeiter zugelassen wird (32 Prozent). Offenbar muss noch immer in vielen Unternehmen erst etwas passieren, damit die „Hausaufgaben“ im Informationsschutz gemacht werden. Eine zunehmend riskante Strategie, wie die Zahlen belegen.

Dirk Fox, Geschäftsführer der Secorvo Security Consulting GmbH, Mitinitiator der Karlsruher IT-Sicherheitsinitiative, einer Special Interest Group des Cyberforum e. V.



Veranstalter sind die Karlsruher IT-Sicherheitsinitiative KA-IT-Si, das CyberForum Karlsruhe und das Kompetenzzentrum für Angewandte Sicherheits-Technologie (KASTEL) am Karlsruher Institut für Technologie sowie die IHK Karlsruhe.

[i] Informationen
Telefon (07 21) 174-190
anna.hetenyi@karlsruhe.ihk.de
www.karlsruhe.ihk.de
Dokumenten-Nummer 13852153