Großunternehmen ignorieren die Gefahren durch Hacker und Wirtschaftsspione

In den meisten DAX-Firmen fehlt ein durchgängiges Konzept für die Informationssicherheit

Düsseldorf, 2. Juli 2012 – Die großen deutschen Unternehmen vernachlässigen das Thema Informationssicherheit, wie eine Studie der Unternehmensberatung A.T. Kearney zeigt. Die meisten Organisationen verfolgen keine ganzheitliche Strategie, um ihre Daten und ihr Know-how zu schützen. Stattdessen verlassen sich die Verantwortlichen häufig auf technische Einzellösungen, die aber immer nur einen Teil der Gefahr abwehren können. Daneben fehlen in vielen Unternehmen die organisatorischen Voraussetzungen für eine wirksame Informationssicherheit „Das Thema Informationssicherheit hat trotz der Zunahmen an Hacker und Wirtschaftsspionageangriffen noch nicht den Stellenwert im Management“, sagt Michael Römer, Partner bei A.T. Kearney und Experte für IT-Strategie.

A.T. Kearney untersuchte die Jahresberichte der 30 DAX-Unternehmen. Das Ergebnis: 27 Firmen widmen sich zwar explizit dem Thema Informationssicherheit. Die im Bericht genannten Schutzmaßnahmen deuten aber auf ein veraltetes Sicherheitsverständnis hin. Meist werden allein technische Einzelmaßnahmen dokumentiert – wie etwa der Einsatz von Antiviren-Software oder der Aufbau redundanter Systeme. Ein durchgängiges und ganzheitliches Konzept lässt sich in den meisten Fällen nicht erkennen. „Lediglich jeder zehnte Bericht ist dazu geeignet, wirkliches Vertrauen aufzubauen“, sagt Dr. Boris Piwinger, Experte für Informationssicherheit bei A.T. Kearney.

Dabei stehen Deutschlands Unternehmen zunehmend im Visier von Wirtschaftsspionen, die es auf Informationen wie Marketingpläne, Kundenlisten oder Entwicklungsdaten abgesehen haben. „Vorsichtige Schätzungen gehen davon aus, dass mindestens jedes vierte Unternehmen bereits Opfer eines Computerangriffs wurde. Aktuelle

Untersuchungen zeigen, dass 95 Prozent aller Unternehmen weltweit gegenwärtig angegriffen werden oder massiv verwundbar sind“, sagt Piwinger. Auf 50 Milliarden Euro beziffert das Bundesministerium des Inneren den jährlichen Schaden in Deutschland durch Industriespionage.

„Weil sich Unternehmen aber nach wie vor scheuen, Fälle von Wirtschaftsspionage und Hackerangriffen publik zu machen, wirkt die Bedrohung kleiner als sie tatsächlich ist“, so Piwinger. „Dadurch fehlt vielen Entscheidern insgesamt eine Sensibilität für die Größe des Problems.“ Zu den betroffenen Unternehmen zählt zum Beispiel das Reiseunternehmen Neckermann; im Mai 2011 erbeuteten Unbekannte 1,2 Millionen Kundendatensätze. Sportartikelhersteller Adidas musste im Herbst vergangenen Jahres seine Website nach einer Hackerangriff vom Netz nehmen. Bei Nortel Networks hatten Datendiebe unbemerkt zehn Jahre lang uneingeschränkten Zugang.

Das Internet dient laut BKA mittlerweile in einem Viertel aller Fälle den Wirtschaftskriminellen als Tatmittel. Dennoch investieren die Unternehmen kaum in die Abwehr von Cyberangriffen und Wirtschaftsspionen. Die Ausgaben, um IT-Systeme gegen Angriffe von außen abzusichern, summieren sich lediglich auf 2,5 Milliarden Euro in Deutschland – also nicht einmal vier Prozent der Gesamtausgaben für Informationstechnologie. „Heute sind die Angriffe individuell auf das Opfer zugeschnitten und verwenden Methoden, die mit den klassischen Werkzeugen nicht abgewehrt werden können. Diese neue Realität erfordert, verstärkt auf Erkennung und Abwehr laufender Angriffe zu setzen“, beschreibt Piwinger die größte Schwachstelle.

Doch nicht nur auf der Technologieebene tun die Unternehmen zu wenig. Auch organisatorisch schaffen sie nicht die Voraussetzungen dafür, Bedrohungen im Digitalzeitalter wirksam entgegenzutreten. „Die meisten Sicherheitsverantwortlichen sind heute noch Teil der IT-Abteilung und oft auch nur auf der Sachbearbeiter-Ebene angesiedelt“, berichtet Michael Römer, Partner bei A.T. Kearney. Die Experten empfehlen, die für die Sicherheit Zuständigen ähnlich wie die Compliance-Verantwortlichen außerhalb der IT-Abteilung anzusiedeln – beispielsweise neben dem Revisionswesen. „Derjenige, der sich um die Informationssicherheit kümmert, muss dem CIO auf Augenhöhe begegnen und kritische Fragen stellen können“, so Römer.

A.T. Kearney rät außerdem dazu, in einem Assessment die wertvollen Daten im Unternehmen zu identifizieren und die Frage, wie sie abgesichert werden können, als strategisch und geschäftskritisch einzustufen. Informationssicherheit sollte als ganzheitliche Funktion betrachtet und über die Abteilungsgrenzen hinweg angegangen werden.

Über A.T. Kearney

A.T. Kearney zählt zu den weltweit führenden Unternehmensberatungen für das Top-Management und berät sowohl global tätige Konzerne als auch führende mittelständische Unternehmen und öffentliche Institutionen. Mit strategischer Weitsicht und operativer Umsetzungsstärke unterstützt das Beratungsunternehmen seine Klienten bei der Transformation ihres Geschäftes und ihrer Organisation. Im Mittelpunkt stehen dabei die Themen Wachstum und Innovation, Technologie und Nachhaltigkeit sowie die Optimierung der Unternehmensperformance durch das Management von Komplexität in globalen Produktions- und Lieferketten. A.T. Kearney wurde 1926 in Chicago gegründet. 1964 eröffnete in Düsseldorf das erste Büro außerhalb der USA. Heute beschäftigt A.T. Kearney rund 3.000 Mitarbeiter in 39 Ländern der Welt. Seit 2010 berät das Unternehmen Klienten klimaneutral.

Weitere Informationen finden Sie unter www.atkearney.de und auf Facebook: www.facebook.com/atkearney.de.

Für weitere Informationen wenden Sie sich bitte an:

Thomas A. Becker
Director Marketing & Communications
A.T. Kearney GmbH
Kaistraße 16A
40221 Düsseldorf
Germany
+49 175 2659 533 Mobile
+49 211 1377 2533 Office
+49 211 1377 2990 Fax
Thomas.Achim.Becker@ATKearney.com