Cyberrisiken begegnen

Moderne IT-Systeme mit einer schnellen Anbindung ans Internet sind für Unternehmen heute überlebenswichtig. Damit ist jedoch die Gefahr digitaler Angriffe massiv gestiegen. Schäden in Höhe von 290 Milliarden Euro verursachen Cyber-Kriminelle jedes Jahr. Auch die eigenen Mitarbeiter können Schäden oder Datenverluste verursachen. Trotzdem haben sich viele Unternehmen gegen IT-Risiken noch nicht ausreichend gewappnet.

Der Ausfall von IT-Systemen stellt für Unternehmen seit jeher ein großes Risiko dar, das Schäden in Millionenhöhe nach sich ziehen kann. Eine wachsende Bedrohung geht dabei von Datendieben aus, deren Handwerkszeug nicht Brecheisen oder Dietriche, sondern Emails, Schadcodes und weltweit verknüpfte Datennetze sind. So unscheinbar und zunächst unspektakulär Cyberkriminelle agieren, so groß ist zugleich die Gefahr, die von ihnen ausgeht. Zahlreiche Unternehmen, darunter internationale Großkonzerne, mussten in den vergangenen Jahren schmerzhaft erfahren, was es bedeutet, in ihr Visier zu geraten. So belegt eine im Oktober 2012 vorgestellte Studie des Computerherstellers Hewlett Packard, dass deutschen Großunternehmen durch Datendiebstahl, Computerviren und Internetattacken jedes Jahr ein durchschnittlicher Schaden von rund 4,8 Millionen Euro entsteht. Auch der deutsche Mittelstand ist zunehmend das Ziel von Datendieben. Weltweit entsteht nach Erkenntnissen des europäischen Zentrums gegen Cyberkriminalität jedes Jahr ein Schaden von rund 290 Milliarden Euro.

Zu einer der häufigsten Angriffsvarianten zählen sogenannte Trojaner. Diese Viren werden versteckt in einem E-Mail-Anhang oder über einen USB-Stick ins System eingeschleust und können anschließend Daten vernichten oder die Systeme lahmlegen. Viele Unternehmen, die mit Verkauf von Waren im Internet Geld verdienen, haben auch schon erleben müssen, wie Kriminelle den gesamten Web-Shop nachgebaut und mit technischen Geschick nicht nur Bestellungen, sondern vor allem Zahlungen der Kunden auf sich umgeleitet haben.

AXA Konzern AG • Konzernkommunikation
Colonia-Allee 10-20 • 51067 Köln
Internet: www.axa.de • E-Mail: presse@axa.de

Auch eigene Mitarbeiter: Gefahr für die Unternehmens-IT

Große Schäden können allerdings nicht nur Fremde anrichten, sondern vor allem auch die eigenen Mitarbeiter, die bewusst oder aus Nachlässigkeit Daten löschen oder Systeme mit Viren infizieren. Dieses Problem scheint auch den IT-Verantwortlichen in den Unternehmen bewusst zu werden. Nach der <kes>/Microsoft-Sicherheitsstudie 2012 sehen auch sie die eigenen Mitarbeiter als größte Gefahr für die IT-Systeme an.

Nur wenige Unternehmen beugen vor oder sichern sich ab

Betroffen von der steigenden Onlinekriminalität sind keineswegs nur Großkonzerne, sondern zunehmend auch kleine und mittelständische Unternehmen. „Deutsche Mittelständler gehören in vielen Branchen zu den innovativsten Unternehmen weltweit. Das weckt Begehrlichkeiten“, sagte Prof. Dieter Kempf, Präsident des Branchenverbandes BITKOM bei der Vorstellung einer repräsentativen Umfrage unter IT-Verantwortlichen. Danach verzeichneten 40 Prozent aller Unternehmen in Deutschland bereits Angriffe auf ihre IT-Systeme, viele davon mehrmals. Ein Drittel hat bereits Erfahrungen mit dem Verlust von Daten gemacht. Umso bedenklicher ist es, so der Verband, dass viele Firmen unzureichend auf solche Fälle vorbereitet sind. Fast die Hälfte (45 Prozent) der Unternehmen hat keinen Notfallplan für Datenverluste oder andere IT-Sicherheitsvorfälle. Auch Betreiber gewerblicher Internetseiten sind sich der Risiken bislang kaum bewusst. So sind nur ca. acht Prozent der Firmen gegen die Manipulation ihrer Website versichert.

„Im Vergleich zu Risiken wie Feuer oder Überschwemmung sind IT-Gefahren für Unternehmen noch relativ neuartig. Rechtsprechung, Gesetzgebung und auch die technischen Grundlagen sind im raschen Wandel“, sagt Dirk Kalinowski, der sich bei AXA seit Jahren mit Gefahren beschäftigt, die Unternehmen durch Attacken auf IT-Systeme drohen. Nach Erfahrung von Kalinowski schützen sich die meisten Firmen inzwischen zwar durch Firewalls und Antivirenprogramme, die meisten von ihnen haben aber kaum ein Gefühl dafür, welche Schäden ihnen im Ernstfall drohen. Wer sich umfassend vor den finanziellen Folgen infizierter oder einfach defekter Computersysteme schützen will, muss laut Kalinowski aber zunächst einmal den möglichen Schaden abschätzen können.

Systematischer Risikomanagement-Prozess wichtiger denn je

Die Bandbreite ist groß: Die Wiederherstellung von Daten ist aufwändig und teuer, auch eine Betriebsunterbrechung führt zu hohen Kosten. Wenn Diebe Daten abgreifen können, kommen dazu möglicherweise Forderungen von Geschädigten auf das Unternehmen zu, wegen Verstoßes gegen das Datenschutzgesetz. „Ein umfassender Risikomanagement-Prozess ist heute für jedes mittelständische Unternehmen unverzichtbar“, betont Kalinowski. Dabei sollten drei entscheidende Fragen beantwortet werden: Lässt sich ein Risiko zum Beispiel durch technische Maßnahmen vermeiden? Wenn es sich nicht gänzlich vermeiden lässt, wie lässt es sich vermindern? Und schließlich: Welche Risiken, die ein Unternehmen nicht vermeiden und vermindern kann, können an einen Versicherer übertragen werden?

Versicherungsschutz auf individuelle Risiken abstimmen

Vor dem Abschluss neuer Policen ist es wichtig, zunächst einmal den Leistungsumfang bestehender Versicherungen zu prüfen. Grundsätzlich in Betracht kommen für Unternehmen folgende Versicherungsformen:

- Elektronikversicherung: Sorgt ein Brand, eine Überschwemmung oder eine Fehlbedienung für den Ausfall von Computersystemen, lassen sich die finanziellen Folgen über den Abschluss dieser Versicherung abfedern.

- Softwareversicherung: Bei einem Datenverlust tritt sie für Kosten der Wiederbeschaffung oder die Wiedereingabe von Daten ein, ebenso wie für Aufwendungen, die entstehen, um eine Betriebsunterbrechung zu vermeiden oder zu reduzieren. Dabei ist es unerheblich, ob die Ursache für den Schaden ein Angriff von außen, ein interner technischer Defekt, ein Fehlverhalten von Mitarbeitern oder zum Beispiel eine zu hohe Spannung im Stromnetz war. Die Softwareversicherung wird nicht einzeln abgeschlossen, sondern ist ein Baustein der Elektronik-versicherung. Voraussetzung für die Deckung ist, dass eine Datensicherung

regelmäßig erfolgt sowie Firewall und Antivirensoftware installiert sind und aktuell gehalten werden.

- Betriebshaftpflichtversicherung: Internetseiten oder Computersysteme können nicht nur Opfer von Onlineattacken werden. Sie können ohne Wissen der Verantwortlichen auch zur Verbreitung von Viren beitragen, zum Beispiel durch den Versand infizierter E-Mails. Deshalb ist es wichtig, dass sich Firmen nicht nur gegen eigene Schäden schützen, sondern auch auf Ansprüche Dritter vorbereitet sind. Für Kosten, die durch die Beschädigung fremder Computer oder IT-Systeme oder auch durch Verstöße gegen das Datenschutzgesetz entstehen, tritt die Betriebshaftpflicht ein – vorausgesetzt, der Vertrag schließt derartige Risiken ein.

- Vertrauensschadenversicherung: Wer Verantwortung für die IT eines Unternehmens trägt, sollte zudem über den Abschluss einer Vertrauensschadenversicherung nachdenken. Sie dient im Wesentlichen dem Schutz vor Betrügern in den eigenen Reihen. Zu den häufigsten Delikten krimineller Mitarbeiter zählen Untreue, Unterschlagung, Diebstahl und Bestechung. Die Versicherung sichert auch Vermögensschäden ab, die dem Unternehmen durch Hackerangriffe von außen entstehen können und kommt – ähnlich wie die Softwareversicherung – für Kosten auf, die zum Beispiel für die Wiederherstellung von Daten anfallen.

- Rechtschutzversicherung inkl. Strafrechtschutz: Gerade wenn personenbezogene oder anderweitig schützenswerte Daten im Spiel sind, ist ein sensibler Umgang gefragt. Wird ein Laptop gestohlen oder ein Netzwerk gehackt, sind oft auch sensible Daten betroffen. Die Person, deren Rechte dadurch verletzt werden, kann in solchen Fällen Strafantrag stellen – und zwar gegen die Person oder das Unternehmen, der sie die Daten überlassen hat. In der Strafrechtschutzversicherung versichert sind zum Beispiel Kosten von Ermittlungsverfahren wegen des Vorwurfs eines solchen strafrechtlich relevanten Verstoßes.