„Die Risiken werden deutlich unterschätzt“

Vielen Unternehmensleitungen fehlt das fachliche Verständnis für IT-Risiken, sagt AXA-Experte Dirk Kalinowski. Dabei ist ein professionelles Risikomanagement heute zur Abwehr von Gefahren unverzichtbar.

Herr Kalinowski, das europäische Zentrum gegen Cyberkriminalität schlägt Alarm. Es beziffert die weltweiten Schäden durch Onlineattacken inzwischen auf 290 Milliarden Euro. Warum nimmt diese Form der Kriminalität solche Dimensionen an?

Dafür gibt es mehrere Gründe. Zum einen braucht heute praktisch jedes Unternehmen für den täglichen Betrieb eine Anbindung ans Internet. Immer mehr Daten werden zudem via Cloud Computing ins Netz gestellt. Das Spielfeld für Online-Kriminelle ist in den vergangenen Jahren also deutlich gewachsen. Zum anderen stellen IT-Risiken für viele Unternehmen eine vollkommen neue und komplexe Bedrohung dar, mit der sie bislang nie konfrontiert wurden. Vielfach fehlt daher das fachliche Verständnis.

Aber die Gefahr von Viren und die damit verbundene Notwendigkeit von Schutzprogrammen kennt heute doch jeder.

In vielen Unternehmen sind die Risiken äußerst komplex und mit der Installation eines Antivirenprogramms oder einer Firewall noch lange nicht ausgeschaltet. Angreifer gehen heute zudem sehr viel subtiler und intelligenter vor, um Zugang zu internen Netzwerken zu erhalten.

Was also müssten Unternehmen aus Ihrer Sicht tun?

Die erste und wichtigste aller Maßnahmen ist der Aufbau und die fortlaufende Umsetzung eines professionellen und umfassenden Risikomanagementprozesses. Der gliedert sich normalerweise in die Phasen Planung, Umsetzung, Überwachung und Verbesserung.

Kann ein solcher Prozess IT-Risiken komplett vermeiden, wenn er gut aufgesetzt ist?

Leider nicht. Wer Vermeidung zur Strategie erklärt, wird in den meisten Fällen wohl scheitern. Im Extremfall würde dies zum Beispiel bedeuten, dass ein Unternehmen auf den Anschluss ans Internet verzichten muss. Das wird tatsächlich bei

Energieversorgungsanlagen praktiziert, dient aber sicherlich nicht als Vorbild für das Gros der nationalen und internationalen Wirtschaft.

Was also ist die Alternative?

Im Idealfall sollte der Prozess aus drei Stufen bestehen: Risikovermeidung, Risikoreduzierung, Risikoübertragung. Im IT-Bereich ist eine vollständige Risikovermeidung wie schon erwähnt meist nicht möglich. Die Unternehmen können aber die Gefahren durch technische und organisatorische Maßnahmen deutlich reduzieren. Hierzu gehört z. B. ein systematisches Patchmanagement. Das bedeutet, konkret zu planen, wann welche Sicherheitsupdates installiert werden, um die Systeme gegen Angriffe zu schützen. Weitere Maßnahmen können Verschlüsselung von Daten, Überwachung der Zugriffsrechte, Erstellung von Notfallplänen etc. sein. Bei Restrisiken, die dann noch verbleiben, sollten Unternehmen abwägen, welche sie selber tragen können oder an einen Versicherer übertragen sollten.

Wie unterstützen Sie Unternehmen in diesem Prozess?

Um Unternehmen für IT-Risiken zu sensibilisieren und bei einem ganzheitlichen Risikomanagement-Prozess zu unterstützen, haben wir zusammen mit den IT-Sicherheitsexperten von 8com und dem SIZ Informatikzentrum der Sparkassenorganisation die Initiative „Lifecycle of Information Security“ gegründet. 8com bringt sein Know-how darüber ein, wie man Sicherheitslücken erkennen und schließen kann, während das SIZ als Experte berät und Lösungen zur Informationssicherheit bereitstellt. AXA schließlich bietet als einer der größten Firmenversicherer Deutschlands langjährige Erfahrung im Management und der Absicherung unternehmerischer Risiken, insbesondere auch von IT-Risiken.

Sind nach Ihrer Erfahrung Unternehmen ausreichend gegen Angriffe auf ihre IT-Systeme versichert?

Die <kes>/Microsoft-Sicherheitsstudie hat deutlich gezeigt, dass Unternehmen das Risiko zwar kennen, allerdings bislang nur die wenigsten eine klare Strategie entwickelt haben. Interessanterweise nehmen die befragten Unternehmen den Irrtum und die Nachlässigkeit der eigenen Mitarbeiter wiederholt als größte Gefahr für ihre IT-Sicherheit wahr. Da verwundert es, dass sich nur wenige Firmen gegen die finanziellen Folgen solcher Gefahren schützen.

Was wären denn aus Ihrer Sicht die wichtigsten Versicherungen?

Manche Risiken sind ganz einfach zu versichern. Eine Elektronikversicherung, die auch die Software abdeckt, greift zum Beispiel bei Bedienungsfehlern, falschen Befehlseingaben oder einer versehentlichen Datenlöschung durch eigene Mitarbeiter oder Dritte. Sofern im Vertrag vereinbart, springt die Elektronikversicherung auch ein, wenn der Ausfall der IT durch einen Sachschaden zu einer Betriebsunterbrechung führt. Zunehmend gefragt ist darüber hinaus die Vertrauensschadenversicherung. Sie

dient im Wesentlichen dem Schutz vor den finanziellen Folgen externer Hackerangriffe. Die Versicherung übernimmt auch die Kosten für die Wiederherstellung oder Wiederbeschaffung von Daten, wenn diese durch zielgerichtete Angriffe auf die IT gelöscht wurden.

Was passiert eigentlich, wenn ein Unternehmen unbewusst über seine eigenen Systeme Viren verbreitet und dadurch andere schädigt?

Der Verursacher eines solchen Schadens ist gegebenenfalls schadensersatzpflichtig. Deshalb sollte die Betriebshaftpflichtversicherung auch einen Baustein für Vermögensschäden enthalten, die aus der Nutzung des Internets bzw. der Datenübertragung entstehen. Hierdurch können nicht nur Kosten durch die Verbreitung von Viren, sondern auch andere Ansprüche z. B. durch Zugangsstörung oder Datenverlust Dritter versichert werden.

Vielen Dank für das Gespräch.