

Schwachstellen früh erkennen

Wie Unternehmen eine umfassende IT-Grundsicherheit schaffen können und welche Rolle dabei das Thema Outsourcing spielt, darüber sprachen wir mit Torsten Gründer, Geschäftsführer der auf IT-Sourcing spezialisierten gründer.consulting gmbh.

business guide: Demnächst wird Ihr Buch „IT-Sicherheit im Unternehmen“ erscheinen. Darin geht es auch um die Sicherheitsanforderungen an ein Unternehmen, das im IT-Bereich gut gerüstet sein will. Welche zentralen Voraussetzungen müssen gegeben sein, um eine Grundsicherheit zu gewährleisten?

Gründer: Es muss ein ganzheitliches Sicherheitskonzept für das Unternehmen entwickelt werden. Dafür ist zunächst einmal eine umfangreiche Schwachstellenanalyse nötig. Zu berücksichtigen sind dabei die physische Systemebene, die den Schutz der IT-Standorte und -Einrichtung beinhaltet, ebenso wie die logische und Prozessebene. Wichtig ist zu entscheiden, welchen Sicherheitsbedarf ein Unternehmen tatsächlich hat. Verfügt es etwa über eine

zuverlässige Datenverschlüsselung und aktuelle Firewall-Technologie oder werden zusätzliche Schutztechnologien wie ein Intrusion Detection System benötigt. Es geht natürlich auch um die Fragen, wie die notwendigen Prozesse im Unternehmen zu definieren und dokumentieren und insbesondere die Mitarbeiter zu sensibilisieren sind und welche Service-Lösungen im Bereich Sicherheit sinnvoller Weise eingesetzt werden könnten. IT-Sicherheit ist stets ein sehr komplexes, alle Unternehmensbereiche betreffendes Thema und deshalb in jedem Fall eine Management-Aufgabe. Zahllose IT-Risiken bedrohen Unternehmen und Behörden und nahezu alle hängen heute existenziell von der Funktionalität ihrer IT-Lösungen ab. Zusammenhänge verdeutlichen und Bewusstsein schaffen für IT-Sicherheit – darum geht es auch in meinem Buch. Fehlen wichtige Systeme und Prozessanweisungen, ist die Geschäftskontinuität und damit oft der Unternehmensbestand gefährdet. Da spielen auch rechtliche Vorgaben wie Datenschutz und die Pflicht zu pro-aktivem Risikomanagement – Stichwort KonTraG – eine Rolle.

business guide: Das ist auch wichtig im Hinblick auf das viel diskutierte Thema Basel II.
Gründer: Natürlich. Die Wirtschaftsprüfer schauen heute zunehmend danach, ob ein Unternehmen alles im Griff hat – auch und gerade im Bereich der IT-Sicherheit. Die Frage ist nur, nach welchen Kriterien werden die bestehenden IT-Risiken beurteilt? Eine 100-prozentige Sicherheit im Unternehmen ist objektiv unmöglich, aber es ist unverzichtbar, ein angemessenes Niveau anzustreben. Dafür ist ein geeigneter Mix aus u.a. Einrichtungen, Tools, Prozessen und qualifizierten Mitarbeiterressourcen notwendig. Das ist ein weites und kostspieliges Feld, das viele Unternehmen heute überfordert, insbesondere den Möglichkeitsrahmen eines Mittelständlers sprengt. Immer öfter greifen diese deshalb auf

spezialisierte Dienstleister zurück. Dennoch bleibt zu klären, wie mit dem verbleibenden Restrisiko umgegangen wird. Akzeptiert ein Unternehmer dieses einfach oder transferiert er es intelligent auf eine Assekuranz? Das ist nicht ohne Bedeutung. Gemäß Basel II sollen die Banken vor Gewährung von Kreditlinien im Zuge einer Gesamtbetrachtung (Ranking) genau prüfen, welche Risiken einem Unternehmen immanent sind – mithin auch und gerade wie mit dem Thema IT-Sicherheit umgegangen wird. Dann ist es ungenügend allein festzustellen, dass der Geprüfte eine Firewall einsetzt. Entscheidend ist doch, ob die verwendete Firewall-Technologie und deren Einsatz den heutigen Standards entspricht. Wenn also ein Unternehmen einen Kreditbedarf bei einem Bankhaus anmeldet, besteht ein maßgeblicher Zusammenhang zwischen der realen Qualität der IT-Sicherheitsvorkehrungen und der Höhe der Refinanzierungskosten. Die Banken sind an dieser Stelle kaum sensibilisiert – mithin zu einer objektiven und damit umfangreichen Unternehmensbewertung im Zuge eines Ratings nicht in der Lage. Für die Unternehmen aber muss es einen Unterschied machen, ob sie fünf Prozent oder acht oder zehn Prozent Kreditzinsen zahlen – je nach Stand ihrer aktuellen IT-Sicherheit.

business guide: Wo gibt es denn noch Sicherheitslücken?

Gründer: Eines der zentralen Sicherheitsrisiken sind stets die eigenen Mitarbeiter, etwa wie diese mit vertraulichen Daten im Unternehmen umgehen. Gefahrenherde sind auch Wireless LAN, öffentliche Hot-Spots und USB-Sticks. Damit kann man heute leicht und schnell große Datenmengen entwenden, oft ohne dass dies bemerkt wird. Deshalb müssen Mitarbeiter über Dienstverträge und Betriebsvereinbarungen verpflichtet, fortwährend sensibilisiert und in dem rechtlich zulässigen Maße auch kontrolliert werden.

business guide: Und die Kosten?

Gründer: IT-Sicherheit kostet Geld, das ist ganz klar. Die Budgets dafür werden in den Chefetagen jedoch gern als nicht vordringlich erachtet. Kommt es aber plötzlich zu einem Virenproblem oder Stromausfall, dann spielt Geld keine Rolle mehr! Das ist unbefriedigend – Sicherheit ist eben ein nach klassischen Maßstäben noch immer schwer wägbares Gut! Das Top-Management muss besser informiert werden, schließlich bestehen bei Versäumnissen Haftungsrisiken nach dem Kontroll- und Transparenzgesetz.

business guide: Das bedeutet, nicht nur im Hinblick auf die finanzielle Situation, sondern auch aus rechtlicher Sicht sollte ein Unternehmer gut aufgeklärt sein, um sich nicht durch Nachlässigkeit strafbar zu machen?

Gründer: Im Aktiengesetz heißt es in § 91, Abs. 2, dass der Vorstand geeignete Maßnahmen zu treffen hat, „damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“. Das ist eine gesetzliche Pflicht zum pro-aktiven IT-Risk-Management im Unternehmen, die übrigens auch GmbH-Geschäftsführer verpflichtet. Die Vorschrift entfaltet Wirkung u.a. im Bereich der IT-Organisationsstrukturen, erfordert strukturiertes Projektmanagement ebenso wie die Sicherstellung der Weiterentwicklung kritischer Applikationen. Ebenso muss der Schutz von Daten vor unberechtigtem Zugriff gewährleistet sein.
business guide: Sie haben bereits das Thema Datensicherung angesprochen. Können Sie den Lesern kurz schildern, welche Vorkehrungen dafür getroffen werden müssen und welche Rolle der Serverraum spielt?

Gründer: Die meisten Unternehmen, die wir kennen, führen heute professionelle Datensicherungen durch und die Daten werden wenigstens einmal täglich, bei anderen einmal wöchentlich gespeichert. Das hängt natürlich auch von der Größe des Unternehmens und

Torsten Gründer

Torsten Gründer ist Geschäftsführer und Mehrheitsgesellschafter der IT-Sourcing Beratung gründer.consulting gmbh. Er ist Experte für die erfolgreiche Umsetzung strategischer IT-Outsourcing-Projekte und die Ausgestaltung von Service Level Agreements (SLA) in der IT. Das von ihm speziell entwickelte Outsourcing Management Modell (OMM) erlaubt die strukturierte Durchführung, Steuerung und Qualitätsmanagement in IT-Outsourcing-Vorhaben. Bei einer Vielzahl von Publikationen und mehrerer Fachbücher wie etwa „IT-Outsourcing in der Praxis“ ist er Autor und Mitautor. Torsten Gründer hält verschiedene Lehraufträge, u. a. an der SAP Business School Vienna (BSV) und referiert regelmäßig auf Konferenzen und Managementseminaren zu aktuellen Entwicklungen im Bereich IT-Services.

der Datenmenge ab. Es macht erkennbar wenig Sinn, seine Daten auf einem Server zu sichern, der mit dem Produktivsystem im selben Raum steht, ohne die Datenträger auszulagern. Entsteht dort ein Brand, ein Wassereintrich oder ein Rauchschaden, sind nicht nur die Daten auf den Festplatten verloren, sondern natürlich auch vom Sicherungs-Robby. Hohe Sicherheit bietet nur die regelmäßige Auslagerung von Daten an einen anderen Ort.

business guide: Ist Outsourcing eine Maßnahme für die IT-Sicherheit, die Sie empfehlen würden und wenn ja, warum?

Gründer: Wenn die richtigen Voraussetzungen geschaffen wurden, ja. Outsourcing ist schließlich nicht per se erfolgreich, sondern es muss gestaltet werden. IT-Outsourcing erfordert Handwerk – es muss strukturiert, qualitätsorientiert und mit Erfahrung umgesetzt werden, sonst führt es am gewünschten Erfolg weit vorbei. Der Auftraggeber will seine Kosten senken und idealer Weise zugleich die IT-Qualität verbessern. Der Dienstleister hingegen will Kunden gewinnen und binden, aber kann natürlich nur wettbewerbsfähig sein, wenn er Skaleneffekte erzielt. Da entstehen schnell handfeste Probleme, die nur durch ein vernünftiges Projektmanagement in den Griff zu bekommen sind. Dann ist Outsourcing eine echte Chance und eine gute Sache. Ein partielles Outsourcing (Outtasking) im Bereich Sicherheit kann besonders im Mittelstand zweckmäßig sein, wenn das Fach-Know-how oder das nötige Geld fehlt. Das Management aller Sicherheitsaspekte ist eine Mammutaufgabe und Mittelständler fragen sich zunehmend, wie sie den richtigen Grad an Schutz zu tragbaren Kosten erreichen können. Hier werden Unternehmer zunehmend IT-Sicherheit im Sinne von Managed Security Services bei Dienstleistern beziehen. Das Thema IT-Sicherheit ist bei einem professionellen Dienstleister oft besser aufgehoben.

business guide: Firmeninterne Rechenzentren sind ein neuralgischer Punkt in Sachen Sicherheit. Wie können sie geschützt werden?

Gründer: Ein Rechenzentrum sollte natürlich nicht in der Nähe von einem Flussbett, einer Raffinerie, einem Kraftwerk und nicht unbedingt unmittelbar an einer großen Fernverkehrsstraße stehen. Neben der reinen Standortthematik sind für die RZ-Sicherheit auch andere Aspekte wichtig, etwa die Sicherung des Geländes, explosionsssichere Fenster und der Serverraum sollte sich nicht im Tiefgeschoss befinden. Zudem ist ein mehrfach gestuftes Zugangssystem mit einem gut definierten Berechtigungskonzept nötig. Zu den Maßnahmen gehören zudem Bewegungsmelder, Videokameras, Doppelböden und Rauchfrüherkennungssysteme. Von der Verkabelung und Versorgung eines Rechenzentrums über redundante Stromversorgung bis hin zu zwei verschiedenen Versorgungsunternehmen ist vieles zu beachten. Alles muss auf ein minimiertes Ausfallrisiko hin konzipiert sein.

business guide: Wie sehen Sie die Zukunft. Werden Unternehmen in den nächsten Jahren mehr investieren?

Gründer: Ja und nein. Wenn es einen Ausfall gab, kann man sicher sein, dass die betroffenen Unternehmen wach werden. Bis dahin herrscht eher Zurückhaltung. Das Gute am deutschen Mittelstand aber ist, dass sich die Unternehmer untereinander stetig austauschen. Sie sprechen sowohl über ihre Erfahrungen mit Outsourcing als auch über Sicherheitsvorfälle. Das sensibilisiert viel mehr als jede verbale Warnung des eigenen IT-Leiters. Ich bin mir sicher, dass die Mittelständler in den nächsten Jahren agiler werden und auch werden müssen, weil sie im Security-Bereich einiges nachzuholen haben. Im Zuge der Globalisierung sind die Gefährdungen für die Unternehmen rasant gewachsen – dazu gehört etwa auch das Spionagerisiko. ■