IT-Security: Zwischen Unsicherheit und Unvorsichtigkeit

Wie sicher sind meine Daten? Und wie gut kann ich mein Wissen überhaupt schützen? Das fragen sich Unternehmen nicht nur seit der NSA-Affäre, sondern spätestens seitdem russische Hacker im Juni dieses Jahres den deutschen Bundestag attackierten. Wenn selbst Verfassungsorgane Zielscheibe von Hacker-Attacken werden und es gelingt, Systeme mit höchster Sicherheitsstufe anzugreifen – wie sollte dann IT-Sicherheit im Unternehmen gelingen? Mit der zunehmenden Digitalisierung und Vernetzung der Daten macht sich folglich Unsicherheit breit. Laut der Studie „IT-Sicherheit und Datenschutz 2015", durchgeführt von der Nationalen Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS), bereitet 84 Prozent der Unternehmen die zunehmende Cyberkriminalität Kopfzerbrechen. 60 Prozent fühlen sich nicht ausreichend gegen Datendiebstahl, Wirtschaftsspionage oder Sabotageakte geschützt. Das ergab eine repräsentative Umfrage im Auftrag des Bitkom. Hauptgeschäftsführer Dr. Bernhard Rohleder schlussfolgert daraus: „Die Unternehmen müssen mehr in die technische, organisatorische und personelle Sicherheit investieren." Und das tun sie, wie die Studie des NIFIS herausfand. Demzufolge plante fast die Hälfte der deutschen Firmen, die Investitionen im Laufe des Jahres um 50 Prozent zu erhöhen. 17 Prozent konnten sich sogar eine Verdoppelung der Ausgaben für IT-Sicherheit vorstellen.

Neben der real existierenden Gefahr vor Hackerangriffen sind es aber vor allem der Kontrollverlust über die Daten sowie die Unwissenheit über potenzielle Risiken, die das Thema IT-Security weiter antreiben. Vor allem beim Thema Cloud Computing befürchten viele Unternehmenslenker ungeahnte Sicherheitslecks. Was passiert mit meinen Daten? Auf welchen (Um-)Wegen werden sie gespeichert? Welche Länder passieren sie auf dem Weg durch die Cloud – und welche Gesetze gelten dort?

Doch Sicherheitsrisiken lauern nicht nur von außen – durch Hacker, Cloud-Anbieter oder Wirtschaftsspione. Nach wie vor kommen die größten Gefahren aus dem Inneren. Zum einen durch die IT selbst: So geschehen beispielsweise in der Kommunalpolitik der Stadt Landsberg. Hier waren im Frühjahr 2015 aufgrund einer Fehlkonfiguration auch alle nicht öffentlichen Sitzungsunterlagen, unter anderem die Erlöse von Grundstücksan- und -verkäufen sowie die Besoldungsgruppen der Verwaltungsmitarbeiter, vorübergehend öffentlich zugreifbar. Etwa zeitgleich führte ein Systemfehler an der Universität Bern dazu, dass die Prüfungsnoten des Vorjahres sowie die dazugehörigen Adressdaten online eingesehen werden konnten.

Doch auch wenn die IT nicht unfehlbar ist, so heißt es doch zu Recht: Irren ist vor allem menschlich. Und damit sind wir beim Mitarbeiter als dem größten Sicherheitsrisiko. Gerade in Zeiten von BYOD verlassen Daten schnell (und oft ungewollt) die geschützte Unternehmens-IT. Ein vergessener USB-Stick, ein verlorenes Smartphone oder ein mangelhaft geschützter Filehosting-Dienst – und schon geht wertvolles Wissen seine eigenen Wege. Wobei nicht nur IT-Schnittstellen und mobile Devices können im Handumdrehen zum Sicherheitsrisiko werden. Auch klassische Papierdokumente können sensible Daten ungewollt öffentlich zu machen, denn – einmal ausgedruckt – gibt es für sie in der Regel keine Passwörter, keine Sicherheitsschranken und keine Zugriffsbeschränkungen mehr. Das zeigte eine Datenpanne beim Hamburger Sportverein im August. In einem Park tauchten Gehaltslisten und Vertragsdetails des Fußballclubs auf. Der Grund: ein gestohlener Rucksack.

Sicherheitslücken sind facettenreich. Genauso vielseitig sind die Lösungen aus dem Bereich der IT-Sicherheit, sodass es für jede Bedrohung den richtigen Schutz gibt. Die Kunst besteht jedoch darin, die Anwendungen so zu kombinieren, dass sie die verschiedenartigen Angriffe gezielt und wirkungsvoll abwehren. Doch auch das gelingt nur dann, wenn alle Beteiligten für das Thema sensibilisiert und sich ihrer Verantwortung für den Schutz wertvoller Daten bewusst sind. Im Titelthema ab Seite 22 diskutieren IT-Sicherheitsexperten die momentane Bedrohungslage und stellen praxiserprobte Wege hin zu einer sicheren Unternehmens-IT vor.

→ Ihr Herausgeber

Oliver Lehnert