Risiken im Blick

UNTERNEHMENSWERTE PRÄVENTIV SCHÜTZEN

Die meisten unternehmerischen „Kronjuwelen“ wie Forschungsdaten, Produktionsverfahren oder strategische Pläne werden von Firmen in global vernetzten Computersystemen gespeichert. Dort sind sie aber nicht nur externen, sondern auch internen Gefahren ausgesetzt. Doch wie lässt sich dieses Wissen vor unerlaubtem Zugriff oder gar Diebstahl wirkungsvoll schützen? Redakteur Hendrik Fuchs sprach darüber mit Markus Geier, Geschäftsführer und Sicherheitsexperte der Comcode GmbH.

Wenn es um die Sicherheit von Daten geht, hört man meistens nur von Firewalls und Antivirenprogrammen. Reichen solche Lösungen aus technischer Sicht aus?

Markus Geier: Firewalls und Antivirenprogramme sind die Grundausstattung. Für sensible Unternehmensdaten reicht das nicht aus. Hier rate ich zu einer regelmäßigen Überwachung von Systemen und Daten (Monitoring) sowie Kontrollsystemen für die Zugriffe auf Kerndaten. Diese Mittel verschaffen dem Unternehmer einen Überblick über die Sicherheitslage im Unternehmen. Entscheidend ist, dass die technischen Lösungen an den Sicherheitsanforderungen der Firma ausgerichtet sind. Es sollten daher nur dann teure und komplexe Sicherheitssysteme eingesetzt werden, wenn Bedarf und Nutzen nachgewiesen sind.

FOTO: SHUTTERSTOCK

Unternehmensdaten sind vielen internen und externen Risiken ausgesetzt. Daher sollten Unternehmer rechtzeitig Vorkehrungen treffen.

Mobile Datenträger sind inzwischen in Unternehmen weit verbreitet. Wie muss denn ein möglichst effektiver Schutz aussehen?

Bei klassischen mobilen Datenträgern wie USB-Sticks, CDs/DVDs und externen Festplatten empfehle ich immer den Einsatz von modernen Verschlüsselungstechnologien, um darauf kopierte vertrauliche Daten wirkungsvoll zu schützen. Bei Smartphones stellt sich die Sache noch etwas komplizierter dar. Generell sollte man das Abspeichern von besonders sensiblen Daten auf den Geräten vermeiden, die auch für den privaten Gebrauch genutzt werden. Zudem ist der Einsatz eines Verwaltungssystems sinnvoll – ein so genanntes Mobile Device Management, das auch von externen Dienstleistern bezogen werden kann. Die Geschäftsleitung sollte auch darauf achten, dass alle Mitarbeiter Geräte und Betriebssysteme des gleichen Typs verwenden. Dies macht den Schutz einfacher und kostengünstiger. Wird dann noch mittels Verschlüsselung auf Unternehmensdaten zugegriffen, sind die Unternehmen gut geschützt.

Und was ist von Antivirenprogrammen für Smartphones zu halten?

Hier ist die Entwicklung noch ganz am Anfang. Dennoch bieten selbst kostenlose Lösungen einen gewissen Basisschutz.

Ein weiterer Trend ist das Cloud Computing. Wie sicher sind denn in einer Wolke abgelegte Daten vor dem Zugriff Dritter?

Das Thema wird derzeit sehr polarisiert diskutiert. Auf der einen Seite sind die Cloud-Anbieter, die vieles versprechen. Auf der anderen Seite stehen die Sicherheitsexperten, die lautstark davor warnen. Dabei gibt es insbesondere im Mittelstand durchaus Bedarf für solche externen IT Dienste. Für den Unternehmer ist jedoch letztlich entscheidend, ob seine besonders sensiblen Daten bei einem externen Anbieter liegen sollen und wenn ja, wie die Absicherung nachgewiesen und kontrolliert werden kann. Hinsichtlich der Vertraulichkeit und Verfügbarkeit müssen glasklare Vereinbarungen mit den Cloud-Anbietern getroffen werden. Im Rahmen solcher so genannten „Service Level Agreements“ muss auch geregelt sein, dass der Kunde jederzeit die Transparenz und die Kontrolle hat. Cloud-interessierte Unternehmer sollten sich mit folgenden Fragen detailliert beschäftigen:

- Sind die eigenen Sicherheitsanforderungen klar formuliert und können diese vom Cloud-Anbieter erfüllt werden?
- Bietet der Anbieter klare „Service Level Agreements“ inklusive Regelungen zum Umgang mit Daten?
- Sind die Zugangswege immer dann verfügbar, wenn auf die Unternehmensdienste zugegriffen werden soll (Funklöcher, Randgebiete)?
- Ist der Ort der Verarbeitung und Speicherung der Unternehmensdaten verbindlich geregelt? Optimal sind Cloud-Anbieter-Standorte in Deutschland.
- Sind Verschlüsselungen möglich, die der Kunde kontrollieren kann?
- Sind Exit-Szenarien möglich und klar beschrieben?

Das größte Sicherheitsrisiko ist der Faktor Mensch. Wie sollten Unternehmen vorgehen, um die Belegschaft für das Thema zu sensibilisieren?

Richtig, daher sollten größere Investitionen in die Sicherheit der Unternehmensdaten erst getätigt werden, wenn die Mitarbeiter darauf geschult und sensibilisiert sind. Ich empfehle die Schulung des Managements inklusive der Geschäftsführung, der Anwender und der IT-Mitarbeiter. Neben gleichen Grundlagen geht es bei diesen Zielgruppen auch um spezifische Themen wie IT-Equipment und Datenzugriffe im Ausland. Die Inhalte von Sensibilisierungsmaßnahmen müssen auf existierende Sicherheitsregeln aufbauen. Oftmals ist ein Mix aus Präsenztrainings für spezielle Benutzergruppen und E-Learning sinnvoll. Mittels E-Learning können Experten in einzelnen Modulen Wissenswertes weitergeben. Das Erlernte kann anschließend in Kurz-Tests abgefragt werden. Von vorne herein sollte dem Unternehmer bewusst sein, dass es sich um einen kontinuierlichen Prozess handelt, das Wissen aktuell zu halten. Schließlich gibt es immer neue, raffiniertere Bedrohungen.

Was ist in Bezug auf Zugriffsrechte und Passwörter zu beachten?

Zugriffsrechte müssen sehr restriktiv gehandhabt werden. Es gilt das „Need to know“-Prinzip, der Mitarbeiter darf also nur auf die Daten zugreifen, die für seine Arbeit notwendig sind. Ausgeschiedene Mitarbeiter dürfen keinen Zugriff mehr auf Zugangsdaten haben. In einem von uns erlebten Fall hatte ein ausgeschiedener IT-Mitarbeiter die E-Mail-Postfächer der Geschäftsführung unwiederbringlich gelöscht. Dies war auch möglich, da er Wochen vorher die Datensicherung deaktiviert hatte, ohne dass dies bemerkt wurde. Ein weiterer Trend in den Unternehmen ist es, die Zugriffsrechte der IT-Administratoren zu beschränken, da diese häufig Zugriff auf alle Unternehmensdaten haben – also auch auf die, die mit der IT-Administration nichts zu tun haben.

„Die technischen Lösungen müssen an den Sicherheitsanforderungen der Firma ausgerichtet sein“, sagt Markus Geier, Geschäftsführer der Comcode GmbH.

Welche Instrumente empfehlen Sie, um einem Datenverlust durch Löschung vorzubeugen?

Eine tägliche Datensicherung ist unabdingbar. Zusätzlich müssen regelmäßige Rücksicherungstests erfolgen, die beweisen, dass die Sicherungen auch funktionieren. Mein Tipp: Der Unternehmer sollte sich die Protokolle von seiner IT über erfolgreiche Tests vorlegen lassen. ■

KURZ VORGESTELLT

Die „ComCode GmbH“ richtet die Umsetzung verlässlicher und sicherer IT-Systeme und -Prozesse konsequent an den Unternehmer-Anforderungen aus. 2009 in Gröbenzell bei München gegründet, schafft ein Team von praxiserprobten Beratern und Technikern Informationssicherheit in mittelständischen und großen Unternehmen. Die Experten decken dabei das notwendige Spektrum von Geschäftsprozessen bis zu komplexen Technologien ab. Zum Dienstleistungsportfolio gehören: Sicherheitsmanagement nach ISO27001 und BSI, Sicherheitsüberprüfungen, Risiko Management, Mitarbeiter-Sensibilisierung und Trainings, Optimierung des IT Betriebs, Notfallmanagement und forensische Analysen sowie Interimsmanagement im Bereich Sicherheit und Datenschutz.

► WWW.COMCODE.DE