

Wie sicher ist das denn?

Datenschutz Unternehmen in Deutschland professionalisieren ihre Abwehr von Cyberattacken. Sechs von zehn Firmen haben laut einer Umfrage inzwischen eine IT-Sicherheitsstrategie. Die ist auch dringend geboten, sagen IT-Spezialisten.

Sobald es um IT-Security geht, wird oft nur an Viren- oder Hackerangriffe gedacht. Die eigentliche Sicherheit der Systeme beginnt jedoch viel früher: bereits bei der zugrundeliegenden Infrastruktur werden wichtige Entscheidungen getroffen. »IT-Sicherheit lässt sich nicht auf ein Thema reduzieren. Sie besteht viel-

»IT-Sicherheit lässt sich nicht auf ein Thema reduzieren.«

Thomas Feiler, »rku.it«

mehr aus einer Verbindung von organisatorischen, technischen und bedienenden, also menschlichen Faktoren«, sagt Thomas Feiler, Leiter Rechenzentrum-Services von »rku.it« in Herne.

DREITEILIGE BASIS

Das Fundament einer umfassenden IT-Security bilden laut Feiler strukturelle Elemente wie Ausfallsicherheit, Redundanz und Katastrophenschutz.

»Wir arbeiten täglich mit hochsensiblen Daten von Energieversorgern und stellen ihnen Softwarelösungen aller Art zur Verfügung. Ein Verlust oder Ausfall wäre fatal. Deshalb haben wir

bereits auf organisatorischer Ebene Standards entwickelt. Unsere Rechenzentrumsinfrastruktur ist auf zwei Standorte verteilt und wird durch einen dritten Standort zur Datensicherung ergänzt.« Dies ermöglicht die Daten- und Anwendungsspiegelung und erhöht die Ausfallsicherheit. »Auch das ist IT-Security«, betont Feiler. Diese existenziellen Aspekte würden nach seinen Worten häufig übersehen.

Katastrophenschutz und Risikomanagement vervollständigen das Sicherheitskonzept des IT-Spezialisten aus Herne. Es gelte, sich permanent neu zu hinterfragen, ob nach neuen Standards oder neuen Individualisierungen von Systemen die Verlust- und Angriffspunkte abgedeckt sind, so der Rechenzentrum-Experte.

Denn das Niveau an Sicherheit ist stets nur eine Momentaufnahme, während die permanente Ausrichtung auf die Bedrohungen hohe Standards sichert.

Ausfallsicherheit und Redundanz der Infrastruktur sind bei Cloud-Produkten elementar und auch hier bedarf es einer Back-up-Strategie, die Daten und Anwendungen sichert und jederzeit wiederherstellbar macht. Darauf aufbauend folgen technische Maßnahmen, die Unternehmen ergreifen sollten.

Die Liste aller technischen Möglichkeiten sei lang, sagt Feiler und nennt beispielhaft Patch-Management, E-Mail-Verschlüsselung, E-Mail-Gateways, Sandboxing, Mobile Device Management, Firewalls und redundante Verbindungstechnologien für den Internetzugriff.

Doch wie funktioniert die Verknüpfung sicherheitsstrategischer und technischer Aspekte im Alltag, etwa Cloud-Services? Welche Rolle spielt hier die IT-Sicherheit? »Viele Nutzer gehen bei der Auslagerung in eine Cloud davon aus, dass ihr Schutz inbegriffen ist. Das ist aber oft nicht der Fall«, so Feiler. Es dürfe nach seinen Worten nicht die Erwartungshaltung entstehen, dass beispielsweise Patches automatisch ausgeführt werden oder sicherheitsrelevante Features enthalten sind.

»rku.it« hat hier nach eigenen Angaben einen Ansatz, bei dem alle Cloud-Angebote auf den organisatorischen Standards aufbauen und als Software as a Service oder Platform as a Service gelten.

VERKNÜPFT MIT DATENSICHERUNG

Jeder Server, jeder Dienst und jede Applikation ist dabei immer mit einer der Relevanz entsprechenden Datensicherung und Redundanz verknüpft. Patchzyklen, Zugriffs- und Verbindungssicherungen, Remotezugänge und diverse weitere technische Spezifikationen werden nach Bedarf abgestimmt.

»rku.it« bietet Kunden nicht einen, sondern diverse hochwertige Standards an und sei in der Lage, spezifische Forderungen individuell umzusetzen.

»IT-Security sollte nicht auf die Technik reduziert werden«, so Feiler. »Eine tragende Rolle spielt der Nutzer vor dem Computer. Der richtige Umgang mit einer sich wandelnden Technologie will gelernt sein.« (hd)

→ www.rku-it.de



Bild: Momius/Stockadobe.com/Fotolia.de

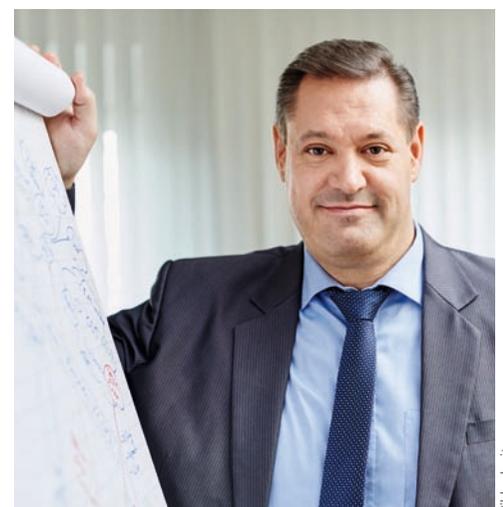


Bild: »rku.it«