THEMA DES MONATS

Brandschutz und IT-Sicherheit

Wann sind Kundendaten in Rechenzentren sicher?

Das sog. IT-Outsourcing gewinnt seit Jahren an Beliebtheit. Bei der Wahl des Anbieters ist der Standort Deutschland für Rechenzentrum, Datenspeicherung und -verarbeitung, Support und Service für viele Entscheider essenziell, so die aktuelle IDG-Sourcing-Studie 2017. Detaillierte Fragen zum Brandschutz werden dagegen selten gestellt. Dabei sind Brände eine der häufigsten Ursachen für Betriebsunterbrechungen in Rechenzentren.

Dr. Michael Bürker
geschäftsführender Gesellschafter
Script Consult GmbH
München

Selten ist es ein großer Brand, der Daten in einem Rechenzentrum gefährdet. Meist entstehen kleine Schwelbrände, weil elektronische Komponenten wie Kondensatoren oder Netzteile einen Kurzschluss auslösen. Werden sie nicht fachgerecht gelöscht, können zusätzlich indirekte Schäden entstehen. Wasser und auch Löschschaum kommen als Löschmittel für einen Serverschrank oder ein Rechenzentrum keinesfalls in Frage. Beides kann die IT-Systeme unwiederbringlich beschädigen.

Es gibt, so der Branchenverband Bitkom, unterschiedliche Brandschutzkonzepte für Rechenzentren, die auf die Ausfallsicherheit abgestimmt sind. Software-Kunden sollten überlegen, welche Ausfallsicherheit ihr Unternehmen benötigt. Hätte schon eine Ausfallzeit von einer Minute hohe Umsatzeinbußen zur Folge? Oder wäre es vertretbar, wenn Kunden und Mitarbeiter erst am nächsten Morgen auf Daten zugreifen könnten?

Die effektivste Maßnahme zum Brandschutz ist die Brandfrühesterkennung. Entsprechende Anlagen saugen den Umluftstrom im Rechenzentrum kontinuierlich an und entdecken auch feinste Rauchpartikel. „Bevor ein Brand überhaupt entstehen oder sich ausbreiten kann, lassen sich auf diesem Weg bereits Maßnahmen zur Brandbekämpfung einleiten“, erklärt Klaus Nowitzky, Director Sales bei Cancom Pironet.

Eine weitere wichtige Schutzeinrichtung ist die Gaslöschanlage. Bei der Wahl des Löschgases ist zu beachten, dass die Infrastruktur nicht geschädigt wird und eine Gefährdung von Betriebspersonal ausgeschlossen werden kann. Löschanlagen arbeiten mit Gasen, die den Anteil des Sauerstoffs verringern oder die Wärme in der Flamme absorbieren. Der Vorteil der Gase ist, dass sie keine direkten oder indirekten Schäden verursachen. Ein Sauerstoffreduzierungssystem ist laufend im Betrieb und vermeidet einen Brand. Das System senkt den Sauerstoffanteil in den Räumen und leitet gleichzeitig Stickstoff ein. Die Sauerstoffkonzentration bleibt hoch genug, damit man die Räume betreten kann, und ist so niedrig, dass kein offenes Feuer entstehen kann.

Wer keine Ausfallzeit riskieren möchte, benötigt eine eigenständige Löschtechnik in redundanter Ausführung. Zu berücksichtigen sind außerdem klassische Brandschutzmaßnahmen wie Rettungswege oder die verwendeten Baustoffe. Die Anforderungen regeln die Bauordnungen der Länder und gesetzliche Vorschriften.

Nicolas Schulmann, Vorstandsvorsitzender der Fio Systems AG, beobachtet in seiner Praxis, dass Rechenzentren mit Standort in Deutschland hohe Standards setzen: „Webbasierte Software bietet eine enorm hohe Zuverlässigkeit, die mittelständische Unternehmen aufgrund der hohen Komplexität kaum selbst gewährleisten können.“

Ein Hochsicherheitszentrum erfüllt strengste Anforderungen nach Bankenstandard in puncto Datensicherheit und Datenschutz. Es ist mit einem Leitstand ausgestattet und gegen Angreifer geschützt, ganz gleich, ob jemand persönlich eindringen oder einen Angriff über das Netz starten möchte. Außerdem verfügt es über eine gesicherte Energieversorgung. Dabei stellen Anlagen zur unterbrechungsfreien Stromversorgung oder Dieselgeneratoren den Betrieb bei einem potenziellen Stromausfall sicher. Brände können gar nicht erst entstehen, da durch Reduktion nicht genügend Sauerstoff in der Luft ist, um einen Brand zu entfachen. Egal ob Klima, Strom oder Internetanschluss, alle diese Bereiche sind redundant ausgelegt.

Quelle: Cancom Pironet

Eine lückenlose Außenhaut- und Innenraumüberwachung mit 360°-Dome-Kameras schützt die im Rechenzentrum liegenden IT-Systeme

Berücksichtigt man alle Aspekte der IT-Sicherheit, wird schnell klar, dass sich diese in umgebauten Büroräumen kaum herstellen lassen.

Unter dem Strich stellt sich die Frage: Welchen Dienstleister soll man wählen? Empfehlenswert ist für Entscheider ein Besuch vor Ort, um sich von der Sicherheit des Rechenzentrums zu überzeugen und die Menschen kennenzulernen, die für die Sicherheit der Daten zuständig sind.