peterschreiber.media – stock.adobe.com ©
IT-Risiken – wie lassen sich Daten retten?

IT-NOTFALLPLANUNG: Naturkatastrophen und andere Extremsituationen bergen für Betriebe ein enormes Gefährdungspotenzial. Wie Firmenchefs vorsorgen können.

Unternehmer Boris Bärmichl (55) weiß aus eigener Erfahrung um die Risiken, die IT- und Kommunikationssysteme lahmlegen können. Nach einem Stromausfall war sein Betrieb einmal sechseinhalb Stunden lang komplett vom Internet getrennt, auch Festnetz und Mobilfunk waren ausgefallen. „Für Kunden und Partner sind wir nicht mehr erreichbar gewesen, der Zugriff auf Computer und Daten war nicht mehr möglich“, erinnert sich der Inhaber des Beratungsunternehmens TechnologieScout, Schöngeising.
Doch nicht allein Stromausfälle gefährden die betrieblichen Abläufe. Angriffe aus dem Internet zum Beispiel, aber auch Wasserschäden, Blitzeinschläge oder Brandunfälle bedrohen die Betriebs-IT samt Computern und wichtigen Daten.
Bärmichl hat sich für künftige Störfälle gerüstet und im Jahr 2020 ein Notstromaggregat angeschafft, das er mit verschiedenen Kraftstoffen betreiben kann, sogar mit Frittierfett. 8 000 Liter Heizöl stehen im Keller als Reserve bereit. Das würde zwei Monate lang reichen, um per Notstromaggregat genug Strom für Computer und andere Geräte zu erzeugen. Nach tagelangem Starkregen, der seinen Keller unter Wasser setzte, ließ er zudem die gesamte EDV-Anlage aus den Kellerräumen in das erste Stockwerk und das neu ausgebaute Dachgeschoss verlegen. Parallel hat er die Blitzschutzanlage und Dachziegel zum Schutz bei Unwettern erneuert.
Um auf Extremsituationen vorbereitet zu sein, die im Zuge des Klimawandels häufiger werden, rät Bärmichl zu einer Umgebungsanalyse mit anschließender Risikobewertung. Drohen Sturmschäden, etwa durch umstürzende Bäume? Wie steht es um die Kanalisation in der Umgebung, um

Wasserleitungen und Stromnetz? Liegt das Unternehmensgebäude in einem Gebiet, in dem Bergbau betrieben wurde? Was ist über etwaige Erdbebengefahren bekannt? Wie ist die Bodenbeschaffenheit?
Auch Cyberattacken stellen eine ernstzunehmende Bedrohung dar. Erpressungstrojaner, sogenannte Ransomware, verschlüsseln IT-Systeme und sperren diese bis zur Zahlung eines Lösegelds. Der Schadcode versteckt sich etwa in E-Mail-Anhängen und in Internetdownloads und infiziert ganze Computernetze nach dem Öffnen der verseuchten Dateien. Bärmichl: „Hierzu muss in den Betrieben noch viel mehr Gefahrenbewusstsein entstehen."

Bausteine einer IT-Notfallplanung

- Mögliche Schäden von IT-Ausfällen mit damit einhergehenden Folgen ermitteln, gesetzliche Vorgaben für Notsituationen beachten.
- Interne und externe Mitarbeiter bestimmen, die im Notfall für die Leitung verantwortlich sind und die IT-Systeme wiederherstellen.
- Handbücher für Computer und Software, Lizenzverträge, Lage- und Raumpläne sowie andere relevante Dokumente sammeln und sicher verwahren.
- Sämtliche für den IT-Wiederanlauf wichtigen Systeme und Geräte erfassen, zum Beispiel Anwendungen, Schnittstellen und Computer, organisatorische Maßnahmen und Wiederanlaufprozeduren erstellen.
- Regelmäßige Backups mit mehreren Sicherungskopien anfertigen. Hilfreich sind von den betriebseigenen Systemen getrennte Speichermedien und Cloud-Dienste.

(Quelle: Bayerischer Verband für Sicherheit in der Wirtschaft e.V./eigene Recherche)

Die IHK für München und Oberbayern hilft mit Basiswissen zur Vorbereitung auf IT-Notfälle: www.ihk-muenchen.de/informationssicherheit

IHK-Zeitung Ausgabe 04/2021
