Netzwerk Südbaden

Das regionale Wirtschaftsmagazin

NUVOLIN: SANDSTEIN FÜRS FREIBURGER MÜNSTER ● BERGBAU: SCHICHT IM SCHACHT ● ALTHOLZGARAGE: MIT VIEL PATINA ● RECYCLING: DER SCHATZ IM ABWASSER ● SCHAUSTELLER HAHN: BEWEGTE FIRMENGESCHICHTE ● DAS SCHÖNE LEBEN: POP-UP-HOTEL IN HORNBERG ● YSTRAL: MISCHEN POSSIBLE ● AM FLUSS: ORTSPORTRAIT RHEINAU ● INTERVIEW: ROBERT NEISEN ÜBER DIE NAZI-VERGANGENHEIT DES SC

9 770262 777279 12

#12/2024
E2014
6,50 Euro

Ton Steine Erden

Schwerpunkt Rohstoffe

Vorbereitet auf den IT-Notfall

Montagmorgen, 8:30 Uhr. Nichts geht mehr. Die gesamte IT ist lahmgelegt. Kein Zugriff aufs ERP-System, andere Anwendungen oder das E-Mail-Programm, um mit Kunden zu kommunizieren. Niemand weiß, was zu tun ist, niemand übernimmt die Führung, Chaos bricht aus. Was tun Sie in diesem Moment?

Julian Sayer ist Vorstand für Vertrieb, Marketing und Entwicklung der Continum AG. Das Freiburger Hostingunternehmen ist AWS-, Microsoft Azure sowie IONOS Partner und unterstützt Unternehmen auf dem sicheren Weg in die Cloud.

Diese Frage sollten Sie sich nicht erst stellen, wenn es so weit ist. Denn ein IT-Notfallplan und ein vorbereitetes Notfallsystem können darüber entscheiden, ob Ihr Unternehmen eine solche Krise meistert oder scheitert. Ein IT-Notfall kann viele Ursachen haben: Ransomware, ein Stromausfall oder ein technischer Defekt. Doch die Konsequenzen sind meist ähnlich: Unterbrechungen im Geschäftsbetrieb, finanzielle Einbußen und ein potenzieller Vertrauensverlust bei Kunden.

Ein gut vorbereiteter IT-Notfallplan minimiert den Schaden und stellt sicher, dass Ihre wichtigsten Prozesse so schnell wie möglich wieder verfügbar sind. Es beginnt mit klaren Definitionen: Wann gilt ein Vorfall als Notfall? Nicht jede IT-Störung ist gleich ein Krisenszenario. Auch eine Unterscheidung in verschiedene Notfallszenarien ist sinnvoll. Ein Ransomware-Angriff verlangt andere Maßnahmen als ein technisch bedingter Serverausfall.

Ebenso entscheidend sind eindeutig definierte Zuständigkeiten. Chaos entsteht oft durch fehlende Verantwortlichkeiten: Wer entscheidet? Wer koordiniert? Wer informiert Kunden und Behörden? Klare Antworten auf diese Fragen verhindern Verzögerungen und können den Schaden minimieren. Die ersten Minuten eines Vorfalls sind oft entscheidend. Sofortmaßnahmen wie das Trennen betroffener Systeme vom Internet oder ihre Isolierung können den Schaden begrenzen. Für schnelle Handlungsmaßnahmen ist es entscheidend, diese im Vorfeld innerhalb eines Leitfadens für spezifische Szenarien zu definieren. Dieser Leitfaden sollte leicht zugänglich sein und regelmäßig aktualisiert werden, damit er im Ernstfall keine Fragen offenlässt.

Doch ein Notfallplan ist nur so gut, wie er gepflegt und getestet wird. Haben alle Verantwortlichen Zugriff darauf – auch bei einem Ausfall der IT-Systeme? Sind die hinterlegten Kontaktdaten aktuell? Nur durch regelmäßige Tests stellen Sie sicher, dass der Plan im Ernstfall funktioniert und die zuständigen Personen Ihre Verantwortlichkeiten kennen.

Neben der organisatorischen Vorbereitung ist auch die technische Absicherung entscheidend, auf die die Schlüsselpersonen im Ernstfall zugreifen können. Eine physisch getrennte Notfallinfrastruktur, beispielsweise eine unabhängige Statusseite, dazu ein separates E-Mail-System, ermöglichen es, die externe Kommunikation auch während eines IT-Ausfalls aufrechtzuerhalten beziehungsweise schnell wieder aufzunehmen. Gerade in Krisensituationen erwarten Kunden und Partner Transparenz. Vorbereitete Vorlagen für Mitteilungen helfen, schnell abgestimmt zu kommunizieren und Vertrauen zu bewahren. Es empfiehlt sich außerdem, das Notfallhandbuch in der Dokumentenablage dieser Infrastruktur zu speichern, um sicherzustellen, dass es für die Schlüsselpersonen im Ernstfall auch abrufbar ist.

Unternehmen, die gut vorbereitet sind, können IT-Krisen schneller bewältigen. Sie reduzieren finanzielle Schäden, vermeiden rechtliche Probleme durch nicht eingehaltene Meldepflichten und bewahren das Vertrauen ihrer Kunden durch schnelle, transparente Kommunikation. Wie würden Sie bei einem IT-Notfall reagieren? Was sind Ihre spezifischen Aufgaben? Nutzen Sie die Gelegenheit, Ihre Notfallstrategien zu hinterfragen und notwendige Maßnahmen zu ergreifen – bevor es zu spät ist.

Foto: PR