

Netzwerk Südbaden

Das regionale Wirtschaftsmagazin

UMFRAGE: WIE FÜHREN SIE IHR UNTERNEHMEN? • ZOLLHUNDE: MEIN PARTNER MIT DER KALTEN SCHNAUZE • GRENZEN ZIEHEN: WAS TUN BEI MACHTMISSBRAUCH? • DEFENSE: SO OPERIERT DAS FREIBURGER UNTERNEHMEN LITEF • RESTAURANT GULLER: VIEL HOLZ, VIEL FLEISCH, VIELE LEUTE • REDOX-FLOW-BATTERIEN AUS DER SCHWEIZ: RIESENTANKS FÜR STROMÜBERSCHÜSSE • DREISAMSTADION: FUSSBALL MACHT SCHULE • SARAH TISCHER: „ICH WILL NICHT MEHR TEIL DIESER SHOW SEIN“



#06/2025

E2014

6,50 Euro



Wie es euch gefällt

Schwerpunkt Führung

Abhängigkeit als Risiko – Wenn das IT-Wissen das Unternehmen verlässt

Viele Unternehmen wollen wegen aktueller Unwägbarkeiten, Datensouveränität und vermeintlich höherer Datensicherheit unabhängig sein und ihre IT-Infrastruktur selbst betreiben. Doch für kleine IT-Abteilungen kann genau das zum Risiko werden.



Tobias Leinweber ist Vorstand für Vertrieb, Marketing und Entwicklung der Continuum AG. Neben eignen Cloud-Lösungen made in Germany ist der Freiburger Clouddienstleister Azure, AWS- sowie IONOS Partner und unterstützt Unternehmen auf dem sicheren Weg in die Cloud.

Wie halte ich unsere Cloud-Systeme am Laufen? Diese Frage stellte sich Matthias Berg*, Geschäftsführer eines mittelständischen Maschinenbauunternehmens im Schwarzwald, als er erfuhr, dass sein einziger IT-Verantwortlicher Daniel König das Unternehmen verlassen würde. Eine formale Nachricht – sachlich, respektvoll. Und doch der Beginn einer Krise, die niemand auf dem Schirm hatte. Denn König war nicht nur der IT-Admin. Er war der Ansprechpartner für alles Digitale: Cloud-Infrastruktur, Rechteverwaltung, Backups, VPN, Security, Updates – alles lief über ihn. Eine kurzfristige Nachbesetzung war – gerade in der aktuellen Marktsituation – nahezu ausgeschlossen.

Zunächst lief der Betrieb weiter – allerdings auf Sparflamme. Anpassungen oder Änderungen waren kaum möglich. Nach und nach häuften sich die Fragen: Wer kann neue Mitarbeitende ins System aufnehmen? Wer hat Zugriff auf die Admin-Konsole der Cloud? Wann laufen Zertifikate ab? Ist das letzte Backup vollständig beziehungsweise wurde es überhaupt durchgeführt? Gibt es sicherheitsrelevante Patches, die dringend eingespielt werden müssen? Reichen die Ressourcen für die aktuellen Anforderungen? Und wer stellt sicher, dass die VPN-Verbindung wieder funktioniert, auf die der Außendienst dringend angewiesen ist? Die eigene IT – einst als Stärke empfunden – war plötzlich ein Fremdkörper und unternehmerisches Risiko.

Matthias Berg ist mit diesem Problem kein Einzelfall. Gerade im Mittelstand liegt die Verantwortung für die IT oft bei wenigen Personen – oder sogar nur bei einer. Zusätzlich treiben geopolitische Unsicherheiten, schwankende Handelsbeziehungen, fragile Datenschutzabkommen mit den USA oder regulatorische Anforderungen wie NIS-2 viele Unternehmen dazu, ihre IT wieder enger selbst führen zu wollen. Ob bei On-Premises-Systemen oder selbst betriebenen Cloudlösungen: Das funktioniert, solange sich personell nichts verändert. Doch Fachkräftemangel, technologische Komplexität und zunehmende Abhängigkeit von digitalen Prozessen zeigen: Diese Form von Unabhängigkeit kann schnell zum strukturellen Risiko werden. Redundanz und Nachvollziehbarkeit fehlen. Doch die entscheidende Frage bleibt: Wie resilient ist ein Unternehmen, wenn sein IT-Wissen an einer einzigen Person hängt?

Matthias Berg hat eine neue Lösung gefunden. Heute arbeitet er mit einem regionalen Cloud-Dienstleister zusammen, der den Betrieb der Infrastruktur übernimmt – inklusive Monitoring, Security-Maßnahmen, Backup-Konzept und Basisbetrieb als Managed Cloud Service. Der lokale Anbieter bringt zudem umfassende Expertise in den aktuellen Themen rund um NIS-2 oder DGSVO mit. Die interne IT bleibt im Unternehmen – mit einer neuen Personalie und einem neuen Fokus: näher an Prozessen, Entwicklung und den Menschen. Dank der gewonnenen Zeit durch die Auslagerung des Infrastrukturmanagements kann sich der neue Kollege auf Themen konzentrieren, die die Digitalisierung des Betriebs und die Weiterentwicklung der Kernprozesse wirklich voranbringen. Die Systeme laufen stabil, Zugänge sind geregelt, Wissen ist dokumentiert. Und das Wichtigste: Das Unternehmen bleibt handlungsfähig – auch wenn zentrale Personen das Unternehmen verlassen.

Diese externe Absicherung schafft nicht nur Unabhängigkeit von internen Ausfällen, sondern ist kurzfristig skalierbar und bietet ein attraktives Umfeld für IT-Fachkräfte. Geboren aus der Not, entpuppte sich die neu gewonnene Flexibilität mit klarem Fokus auf geschäftsrelevante Abläufe als echter Wettbewerbsvorteil.