netzwerk südbaden

SPORT

Wer und was die Region bewegt

August 2021 | Preis: 5,50 Euro | E 2014 www.netzwerk-suedbaden.de

9 770262 777279 08

Das regionale Wirtschaftsmagazin

CONTINUM

UNTERNEHMEN ALS ZIELSCHEIBE

Ransomware Angriffe haben in Deutschland stark zugenommen. Wie sieht pragmatische Notfallhilfe für den Mittelstand aus?

Julian Sayer Foto: ZVG

Jedes Unternehmen sollte sich darauf vorbereiten, früher oder später Opfer eines Hacker-Angriffes zu werden. Nicht selten trifft es Mittelständler, denen Notfallpläne und Krisenkonzepte fehlen. Was dann zählt, ist die systematische Abarbeitung von Notfallschritten, um schnell einen sicheren Arbeitsmodus wiederherstellen zu können.

Rund die Hälfte (48 Prozent) der mittelständischen Unternehmen hat keinen IT-Notfallplan, wie eine Forsa-Umfrage im Frühjahr 2020 ergab. Besonders kritisch: sechs von zehn der befragten Unternehmen behaupten, bei einem Ausfall ihrer IT-Systeme kaum noch operieren zu können.

Das G4C – German Competence Center against Cybercrime - schreibt im Oktober 2019 in ihrer Information für Unternehmen und in Kooperation mit dem Bundeskriminalamt (BKA) sowie dem Bundesamt für Sicherheit in der Informationstechnologie (BSI), dass ein neuer Trend bei Ransomware-Attacken darin besteht, das Erpressungspotenzial gezielt bis auf die nachhaltige Vernichtung nahezu aller Datenbestände inklusive der Backups auszudehnen.

Gelingt den Tätern eine solche Vollverschlüsselung, können sie deutlich höhere Lösegeldsummen fordern. Die Einschränkungen würden nicht nur kurze Zeit andauern, sondern es droht im schlimmsten Fall der dauerhafte Verlust aller vorhandenen Daten. Laut dem Verband Deutscher Maschinen- und Anlagenbau (VDMA) zahlen bis zu 70 Prozent der betroffenen Unternehmen die geforderte Lösegeldsumme. Dies sollte jedoch um jeden Preis vermieden werden, da dadurch die Gefahr für Folgeangriffe massiv ansteigt.

Deutlich wird, dass die Art der Notfälle, die bei IT-Systemen auftreten können, immer komplexer und die Cyberattacken immer raffinierter werden. Das BSI schreibt im Online-Kurs Notfallmanagement: „Zum Notfallmanagement gehört die Aufgabe, Pläne zu entwickeln und Vorkehrungen zu treffen, um angemessen auf Notfälle, Krisen und Katastrophen reagieren zu können. Je besser vorbereitet ein Unternehmen auf solche Herausforderungen ist, desto handlungsfähiger ist es und desto leichter kann es mögliche Schäden begrenzen."

Ein Notfallhandbuch sollte IT-Sofortmaßnahmen konkret beschreiben sowie Geschäftsfortführungspläne und Wiederanlaufpläne enthalten. Ebenso sollten Geschäftspartner, wie Kunden und Lieferanten, über den Notfall informiert werden. Das Handbuch und weitere kritische Daten für den Notfall müssen zwingend außerhalb der Unternehmens-IT aufbewahrt werden und im Falle schnell zugänglich sein. Nur so kann sichergestellt werden, dass die Informationen nach einem Angriff tatsächlich noch verfügbar sind.

Bewährt hat sich das Auslagern eines separaten kleinen Notfall-Blogs auf Basis einer einfach zu pflegenden Wordpress-Seite bei einem Rechenzentrumsdienstleister außerhalb des Unternehmens. Ebenfalls sollte auf dem Internetserver ein Dokumenten-Safe bereitgestellt werden, in dem das Notfallhandbuch und alle wichtigen Dokumente liegen, die bei einem Notfall benötigt werden. Der Zugriff zur Pflege des Notfall-Blogs sowie zum Dokumenten-Safe ist ausschließlich für die zuvor definierten Mitarbeiter des Krisenstabs vorgesehen, der Zugang sollte auf jeden Fall über eine 2-Faktor Authentifizierung abgesichert sein.

Julian Sayer ist Vorstand für Vertrieb, Marketing und Entwicklung des Freiburger Hostingunternehmens und Cloud Solution Providers Continum AG. Als AWS und Microsoft Azure Partner versteht sich die Continum AG als „Anwalt" des Kunden und unterstützt Unternehmen auf dem sicheren Weg in die Cloud.