Netzwerk Südbaden

Das regionale Wirtschaftsmagazin

ÜBEN, PROBEN UND TRAINIEREN ALS TEIL DER ARBEIT ● MEDIZIN: LABORPROBEN FÜR DIE DIAGNOSTIK ● MACK RIDES: GUT GETESTETESFAHRVERGNÜGEN ● AUFZUGSTEST:UNTERWEGSMITDEMTÜVSÜD ● DURCHBLICK:KONTAKTLINSENHERSTELLER HECHT IN AU ● SOCIAL INNOVATION LAB: UNTERSTÜTZUNG FÜR GUTE GRÜNDUNGEN ● FUSSBALL: DER KLEINE SC SAND BEI DEN PROFIFRAUEN ● SALMENGESPRÄCH: AUTORIN LENA GORELIK

9 770262 777279 10

#10/2024
E2014
6,50 Euro

Schwerpunkt Proben, Prüfen, Testen

Bereit für NIS-2 und Dora?

Diese beiden Abkürzungen treiben derzeit viele Mittelständler um. Es geht um kritische Infrastrukturen, Lieferketten und den Finanzsektor. Die Präventions- und Sicherheitsmaßnahmen, zu denen NIS-2 und DORA Unternehmen verpflichten, sollen dabei helfen, im Ernstfall schnell wieder handlungsfähig zu sein.

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.

NIS-2 steht für „Network and Information Security Directive" und betrifft kritische Infrastrukturen sowie deren Lieferketten. DORA, bedeutet „Digital Operational Resilience Act" und adressiert vor allem Unternehmen im Finanzsektor. Beide Richtlinien verpflichten betroffene Unternehmen zu Präventions- und IT-Sicherheitsmaßnahmen, um im Ernstfall schnell wieder handlungsfähig zu sein. Ein durchdachtes Business Continuity Management (BCM) hilft, den Normalbetrieb nach schweren Vorfällen zügig wieder aufzunehmen. Doch was heißt das konkret?

Stellen Sie sich vor: Sie betreten Ihren Betrieb, doch statt des gewohnten Surrens der Maschinen herrscht bedrückende Stille. Wichtige Kunden bleiben unerreichbar, Aufträge können nicht erfüllt werden. Trotz Sicherheitsmaßnahmen und Prävention hat ein Ransomware-Angriff Ihre Produktion lahmgelegt. Jede Minute Stillstand bedeutet nicht nur finanzielle Verluste, sondern auch einen enormen Vertrauensverlust bei Kunden und Partnern. Wie lange können Sie einen solchen Ausfall verkraften?

In solch einem Ernstfall stellt nur ein umfassendes BCM sicher, dass Ihr Unternehmen schnell wieder handlungsfähig wird. Ein BCM basiert auf zwei zentralen Säulen: einer durchdachten Disaster-Recovery-Strategie und einem robusten Backup-Management. Diese beiden Komponenten ermöglichen es Ihnen, kritische Systeme und Daten schnell wiederherzustellen und den Betrieb aufrechtzuerhalten respektive schnell wieder aufzunehmen.

Ein zentraler Bestandteil der Disaster-Recovery-Planung ist die Definition von Recovery Time Objective (RTO) und Recovery Point Objective (RPO). RTO beschreibt die maximale Dauer, die Ihr Unternehmen nach einem Vorfall ohne betriebswichtige Systeme überstehen kann. RPO gibt an, wie viele Daten Sie maximal verlieren dürfen. Anhand dieser Kennzahlen können Sie ableiten, welche Maßnahmen und Technologien notwendig sind, um die Anforderungen an den Wiederherstellungsprozess zu erfüllen.

Backups sind entscheidend, um nach einem Ausfall schnell wieder handlungsfähig zu sein. Die bewährte 3-2-1-Regel empfiehlt: 3 Kopien Ihrer Daten, auf 2 verschiedenen Medien, davon 1 extern gespeichert. Für viele Unternehmen stellt die Umsetzung des externen Backups eine Herausforderung dar, weil sie keinen zweiten abgetrennten Standort für ein Backup haben – hier bietet eine Cloud die ideale Lösung. Sie ist kostengünstig, flexibel und nach Bedarf skalierbar. Ihre Systeme, Daten und virtuelle Maschinen werden automatisiert in festgelegten Intervallen in die Cloud repliziert und rund um die Uhr überwacht. Zusätzlich ermöglicht ein Cloud-Backup eine georedundante Absicherung durch Speicherung in mehreren geografisch getrennten Rechenzentren. Angesichts der zunehmenden Ransomware-Bedrohung empfiehlt sich außerdem eine Kopie als sogenannte Immutable Backup abzulegen. Diese unveränderliche Kopie schützt Ihre Daten selbst dann, wenn Angreifer versuchen, gezielt Ihre Backups zu manipulieren.

Niemand kann vorhersagen, wann eingangs beschriebenes Worst-Case-Szenario eintritt – aber Sie können vorbereitet sein. Eine Kombination aus Disaster Recovery und einer soliden Backup-Strategie ist der Schlüssel, um auch in Krisenzeiten handlungsfähig zu bleiben. Statt monatelanger Ausfälle können Sie so Ihre Kernprozesse innerhalb weniger Stunden oder Tage wiederherstellen. Dies ist nicht nur essenziell für die Geschäftskontinuität, sondern erfüllt auch eine der zahlreichen Anforderungen der NIS-2-Richtlinie, deren Nichteinhaltung empfindliche Strafen nach sich ziehen kann. Sorgen Sie dafür, dass Ihr Unternehmen im Ernstfall schnell und effizient reagiert.

Foto: PR