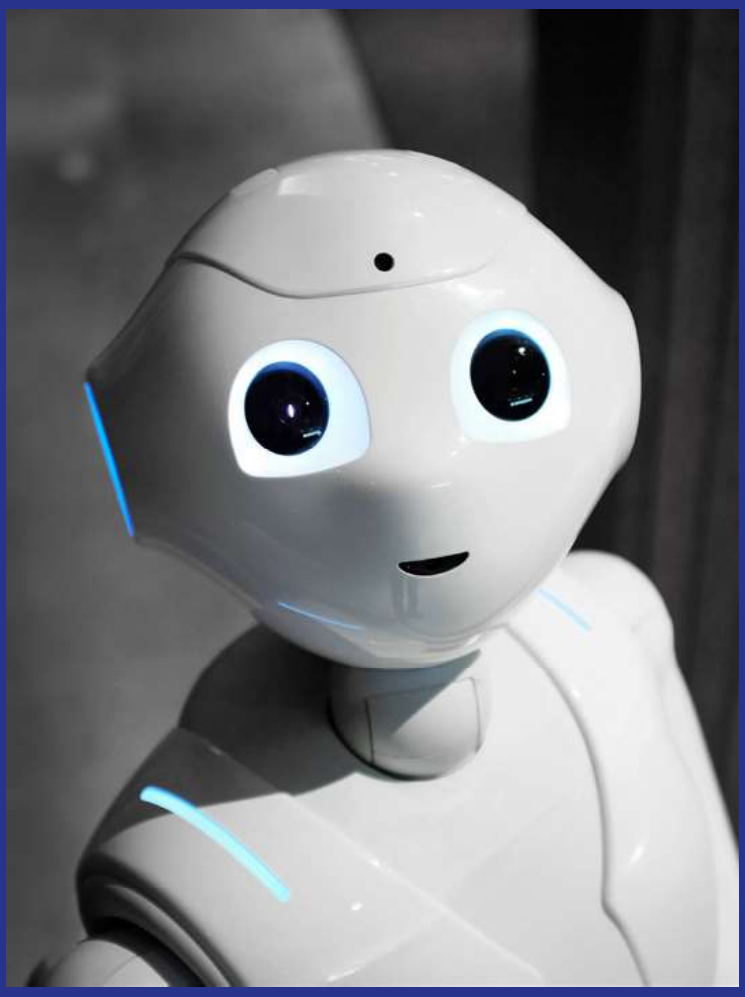
Netzwerk Südbaden

Das regionale Wirtschaftsmagazin

KUNSTSTOFF: VERÄNDERN, UM ZU BLEIBEN ● ANTONIHOF: SO KANN DIE AGRARWENDE FUNKTIONIEREN ● TRANSFORM: EINE AUSSTELLUNG ZUR ENERGIEWENDE ● MUSIKMACHER: SAUTER BAUT KLAVIERE UND FLÜGEL ● ORTSPORTRÄT OBERKIRCH: ZWISCHEN OBST UND INDUSTRIE ● INTERVIEW ZU DEN STEIGENDEN INSOLVENZZAHLEN ● BRUGGAA: NEUES PROJEKT VON HALDE-WIRT HEGAR UNTEN IM TAL

9 770262 777279 04

#04/2024
E2014
6,50 Euro



Zukunft ist jetzt

Schwerpunkt Change

Effektiver Schutzschild gegen Cyberangriffe

Das Lagebild zur Cybersicherheit in Deutschland skizziert eine besorgniserregende Situation. Die Bedrohung hat ein historisch hohes Niveau erreicht. Ein neuer Baustein kann helfen.

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.

Die größte Bedrohung bleibt dabei Ransomware. Angegriffen werden nicht mehr nur große Unternehmen, sondern zunehmend kleinere Organisationen, staatliche Institutionen und Kommunen, was direkte Auswirkungen auf die Bürgerinnen und Bürger haben kann. Angesichts dieser Bedrohungslage stellt sich die Frage: Wie wäre es, eine feste Schutzschicht zu haben, die sich um die eigenen Daten legt und damit eine robuste Verteidigung gegen Cyberangriffe bietet?

Cyberangriffe zielen häufig darauf ab, Systeme zu kompromittieren, Daten und Backups zu manipulieren oder zu verschlüsseln, um Lösegeld von dem Opfer bzw. angegriffenen Unternehmen zu erpressen. Die Prävention und ein effektives Business Continuity Management (BCM) sind die Königsdisziplin für Unternehmen jeder Größe, um das Risiko von Datenverlusten, finanziellen und Reputationsschäden zu minimieren. Als neuester Baustein moderner Sicherheitskonzepte bieten sogenannte Immutable Backups eine effektive Maßnahme gegen Cyberangriffe – insbesondere gegen Ransomware.

Ein Immutable Backup, also eine unveränderbare Datensicherung, ist – wie der Name schon vermuten lässt – ein Backup, das sich nicht mehr verändern lässt, sobald es erstellt wurde. Weder von der Software noch von einem Administrator oder gar einem Angreifer. Mit dieser Unveränderlichkeit bieten Immutable Backups einen starken Schutz für gespeicherte Daten. Denn sie verhindern, dass Backup-Daten nachträglich verändert, verschlüsselt oder gelöscht werden können. Hier sind nur einige Gründe, warum Immutable Backups als effektiv gegen Cyberangriffe gelten:

Verschlüsselung: Ransomware-Angriffe zielen darauf ab, Daten zu verschlüsseln und Opfer zu Lösegeldzahlungen aufzufordern, um wieder Zugriff zu erhalten. Weil Immutable Backups nicht verschlüsselt werden können, hat man immer Zugriff auf eine saubere Kopie der Daten, ohne Lösegeld zahlen zu müssen.

Integrität: Da die Daten nicht geändert werden können, bleibt ihre Integrität erhalten. Das ist besonders wichtig, um sicherzustellen, dass die Wiederherstellung nach einem Cyberangriff auf einer vertrauenswürdigen und unberührten Datenquelle basiert.

Schnelligkeit: Nach einem Angriff ist es entscheidend, dass Unternehmen ihre Tätigkeit so schnell wie möglich wieder aufnehmen können. Da Immutable Backups vor Veränderungen geschützt sind, können sie schnell und zuverlässig wiederhergestellt werden, wodurch die Ausfallzeiten minimiert werden.

Komplementärer Schutz: Kein Sicherheitssystem ist vollständig unangreifbar. Immutable Backups fungieren daher als zusätzliche Schutzebene in einer umfassenden Cyber-Security-Strategie. Sie ergänzen andere Sicherheitsmaßnahmen wie Firewalls, Antivirus-Programme und E-Mail-Filter.

Prävention menschlicher Fehler: Nicht alle Datenverluste sind auf böswillige Angriffe zurückzuführen. Menschliche Fehler oder versehentliches Löschen von Daten können ebenso verheerend sein. Immutable Backups schützen auch hier, indem sie eine unveränderliche Sicherungskopie bereitstellen, die gegen solche Unfälle immun ist.

Ein möglichst effektiver Schutz hängt selbstverständlich von der Back-up-Historie ab. Experten empfehlen neben täglichen auch Wochen-, Monats- und Jahres-Back-ups. Eine Back-up-Historie von mindestens sechs Monaten sollte obligatorisch sein, damit man im Fall der Fälle mit einer hohen Wahrscheinlichkeit auf ein sauberes Back-up zurückgreifen kann. Unabhängig von der spezifischen Aufbewahrungsdauer hilft die 3-2-1-Regel: mindestens drei Kopien von Daten auf zwei verschiedenen Medien speichern und mindestens eine Kopie außerhalb des Standorts speichern oder aufbewahren.

Foto: PR