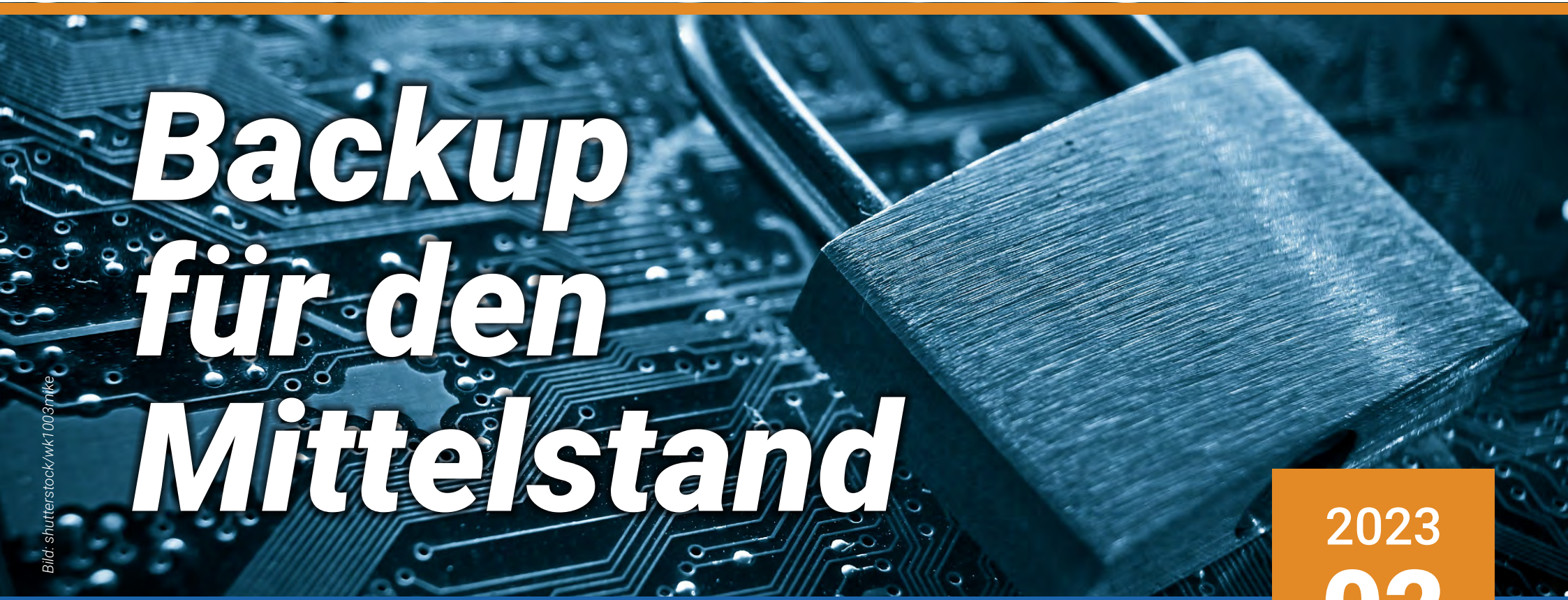
storage-magazin.de

powered by it-daily.net

Eine Publikation von speicherguide.de



Backup für den Mittelstand

Bild: shutterstock/wk1003mike

Cyberattacken: Auswirkungen & Folgekosten

2023
02

Editorial

DIE AUSMASSE EINES CYBERANGRIFFS SIND IMMENS

Karl Fröhlich
Chefredakteur
speicherguide.de

Liebe Leserinnen und Leser,

wir haben ein Problem, vermutlich sogar mehrere. Unsere Unternehmensdaten sind bedroht. Ja werden Sie sagen, »fällt uns denn nach 20 Jahren *speicherguide.de* nichts neues ein, schreibt Ihr das nicht jedes Jahr?« Da haben Sie natürlich recht, nur haben sich die Bedrohungen geändert und da nimmt das Übel seinen Lauf: Ich behaupte einfach mal übergriffig, unsere Datensicherungsstrategien basieren überwiegend auf alten Annahmen und Bedrohungsszenarien.

Natürlich sind technische Defekte, menschliches Versagen, Feuer- und Wasserschäden und Naturkatastrophen weiterhin realistische Bedrohungen. Die eigentliche Gefahr droht aber mittlerweile von Dieben. Von Datendieben. Von Cyberkriminellen, die es nicht auf die Hardware, sondern auf die Firmendaten abgesehen haben.

Nun ist auch dies nicht neu. Einigen wir uns aber darauf, dass es sich aber um ein ernsthaftes Problem handelt. Die Frage ist nun, ist Ihr Unternehmen auf einen Cyberangriff vorbereitet? Hat die Geschäftsleitung den Ernst der Lage verstanden? Herrscht nicht vielmehr der Glaube vor, »uns trifft es schon nicht« oder »wir sind (bestimmt) ausreichend vorbereitet«. Sind Sie das wirklich?

Wurde Ihr Notfallplan tatsächlich schon einmal durchgespielt? Und damit meine ich nicht nur, ob die Backups funktionieren und sich einzelne Teile wiederherstellen lassen. Würde dies auch unter Notfallbedingungen funktionieren? Ist Ihre Benachrichtigungskette krisensicher? Angenommen ein Ransomware-Angriff kommt durch und legt alles lahm. Was dann? Wer steht bereit, um die Infektion zu erkennen, zu finden und zu beheben? Wenn rufen Sie im Notfall zu Hilfe?

Wissen Sie wirklich, wie lange eine Rücksicherung aller Daten dauern würde? Passen diese angenommenen Werte zu den definierten RPO und RTOs? Kennt Ihre Geschäftsleitung die Höhe der stündlichen Verluste, wenn die IT steht?

Sie verstehen, worauf ich hinaus möchte. Und, um das Szenario auf die Spitze zu treiben, hat sich schon einmal jemand bei Ihnen mit den möglichen Folgekosten eines Ransomware-Angriffs beschäftigt? Was Kosten externe Experten, Anwälte, die sicherlich benötigt werden, mögliche Regressansprüche von Kunden bis hin zu Schadenersatzklagen und eventuellen Strafzahlungen?

Die Rechnung ist erschütternd umfangreich. Wir fassen das Wichtigste in diesem Storage-Magazin für Sie zusammen.

Ihr Karl Fröhlich,
Chefredakteur speicherguide.de

Bild: shutterstock/wk1003mike

DATENSICHERUNG MIT MAXIMALER CYBER-RESILIENZ

SEITE 5

Backup und Recovery ist nicht mehr das profane Sichern von Dateikopien und dem Rücksichern einzelner Files. Heute geht es um eine schnelle Betriebswiederherstellung. Zu groß ist die Bedrohung, dass eine Cyberattacke das ganze Unternehmen lahm legt. Die Datensicherung muss sich neu aufstellen.

Bild: shutterstock/Wolfilser

Finanzielle Auswirkungen von Ransomware

FOLGEKOSTEN UND KOLLATERALSCHADEN

SEITE 19

Ein erfolgreicher Ransomware-Angriff belastet Unternehmen schwer, vor allem finanziell. Die zu erwartenden Kosten gehen weit über die Höhe des geforderten Lösegelds hinaus. Neben der Downtime und dem mögliche Datenverlust muss mit Ausgaben für technischen und rechtlichen Beistand kalkuliert werden. Zudem werden die erbeuteten Daten zum Kauf angeboten.

Im Ernstfall helfen nur vorab definierte Prozesse

JEDES UNTERNEHMEN BRAUCHT EINEN IT-NOTFALLPLAN

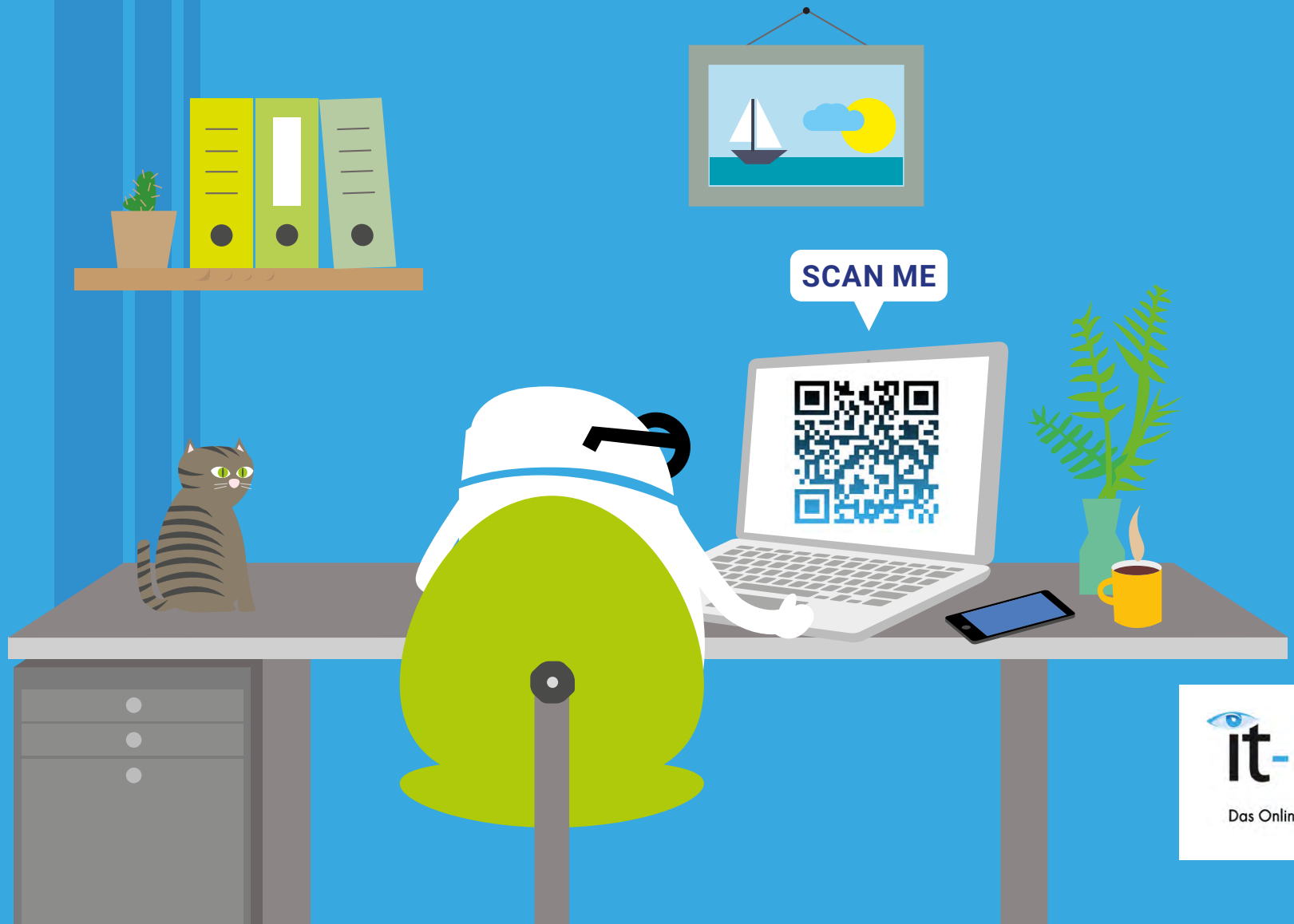
Foto: schutterstock.com / Panchenko Vladimir

SEITE 22

Übersicht **Storage-Anbieter**

SEITE 15

it-daily.net mehr als nur tägliche IT-News!



it-daily.net

Das Online-Portal von itmanagement & itsecurity

Bild: shutterstock/wk1003mike

Karl Fröhlich
speicherguide.de

Backup für den Mittelstand

DATENSICHERUNG MIT MAXIMALER **CYBER-RESILIENZ**

Backup und Recovery ist nicht mehr das profane Sichern von Dateikopien und dem Rücksichern einzelner Files. Heute geht es um eine schnelle Betriebswiederherstellung. Zu groß ist die Bedrohung, dass eine Cyberattacke das ganze Unternehmen lahm legt. Die Datensicherung muss sich neu aufstellen.

Ransomware ist aktuell klar Herausforderung Nummer eins. Die Bedrohung durch Erpresser-Software und Malware nimmt stetig zu. »Für Cyberkriminelle ist dies äußerst lukrativ«, sagt **Daniel Hofmann**, CEO bei **Hornetsecurity**. »Deswegen kommen täglich neue Methoden hinzu, schädliche Software zu übermitteln, wie zum Beispiel per QR-Code (sogenanntes Quishing).«

»Die Anforderungen reichen von Zero-Trust über Mitarbeiterschulung und Notfallplänen bis hin zu Backup und Recovery«, ergänzt **Hannes Heckel**, Leiter Marketing bei **FAST LTA**. »Gerade KMUs haben in manchen Bereichen oft Nachholbedarf, nach dem Motto `uns passiert schon nix, wir sind ja nicht interessant für Angreifer´. Dass die Hälfte deutscher Unternehmen keine echten Notfallpläne haben und bis zu 80 Prozent von sich selber sagen, dass sie sicherheitstechnisch nicht mit der Bedrohungslage mithalten können, ist alarmierend.«

Daniel Hofmann
Hornetsecurity

»Bei Cyberangriffen stehen Mitarbeiter in der ersten Reihe und müssen entsprechend trainiert werden.«

Kleine und mittlere Unternehmen (KMU) stehen vor der Aufgabe, eine Datensicherung so aufzusetzen, dass sie die maximale Cyber-Resilienz gewährleistet. »Die Datensicherung soll nach einem Desaster eine schnelle Betriebswiederherstellung gewährleisten«, erklärt **NovaStor**-Geschäftsführer **Stefan Utzinger**. »Leicht gesagt, aber Fachkräftemangel, zu geringe Budgets, Überlastung und die fortschreitende Digitalisierung machen es den Verantwortlichen nicht leicht.«

Dies sieht auch **Albrecht Hestermann**, Vertriebsleiter bei **actidata**, so: »Geschäftsführung und Vorstand sind gefordert, Budgets freizugeben. Wir verzeichnen eine steigende Anfrage zu Mietlösungen, die, kombiniert mit den Managed-Service-Leistungen unserer Partner, bei den Anwendern platziert werden. Verstärkt sehen wir, dass heute mehr Datensicherungssätze angelegt werden. Also nicht nur

Hannes Heckel
Fast LTA

»Ein kompletter Schutz vor einem Cyberangriff dürfte zunehmend unmöglich sein.«

Backup-to-Disk-to-Tape (B2D2T) mit monatlichen Auslagerungen, sondern auch eine Selektion von »besonders kritischen Daten«, beispielsweise Buchhaltung oder Kundendateien, die dann im wahrsten Sinne des Wortes doppelt und dreifach auf unterschiedlichen Medien abgelegt werden. »

Datensicherung endlich aus Recovery-Sicht betrachten

Für Fast-LTA-Manager Heckel ist das Zeitalter der Backups vorbei: »Der Fokus muss auf Recovery liegen, dabei erfordern unterschiedliche Datenklassen verschiedene Strategien und Technologien. Daten in irgendeinem Safe auf Tape nutzen nichts, wenn man schnell und wahlfrei darauf zugreifen muss, um den laufenden Betrieb zu sichern. Technologien, die nichts zur Recovery-Strategie beitragen, haben im Backups nichts mehr zu suchen.«

Wobei Magnetbänder und Tape-Automation nach wie vor fester Bestandteil einer Datensicherungsstrategie bleiben. Die Nachfrage steigt seit rund zwei Jahre kontinuierlich. »Verstärkt wird nach Lösungen mit Einzel-Streamern gefragt«, sagt Actidata-Manager Hestermann. »Hier will man dem Anspruch gerecht werden, unternehmenswichtigen Tagen regelmäßig extern an einem sicheren Ort auszulagern.«

Hinzukommt laut Hestermann die Frage, wie geht der Admin mit den so genannten unstrukturierten Daten um. »Die Einteilung nach `cold´ und `hot data´ erscheint vielen zu einfach. Immer noch wird meist alles gesichert – was natürlich den Speicherbedarf wachsen lässt. Lösungen hierzu mögen in einer Daten-Management-Software liegen, wobei das Thema von KMUs nicht wirklich angefasst wird. Budgets hierfür liegen in der Regel nicht bereit.«

Backup-Software: mehr Sicherheit & Unveränderlichkeit

In Folge wirkt sich der neue Fokus auf die Datensicherung auch auf das Ge-

Stefan Utzinger
Novastor

»IT-Verantwortliche müssen sicherstellen, dass die Firma im Ernstfall schnellstmöglich wieder arbeitsfähig ist.«

schäft mit Backup-Software aus. Die Jahre der Konsolidierung sind erst einmal vorbei. Gleichzeitig steigen die Anforderungen an die Backup-Lösung.

»Neben ausgeklügelten Backup Konzepten, die die Compliance-Anforderungen unterstützen und die Schutz gegen Ransomware bieten, sind auch die Immutable-Technologien wie *SiS* und *Blocky4sesam* zum Ransomware-Schutz der Backups sehr wichtig«, erklärt **Andreas Mayer**, Director Marketing bei **SEP**. »Hinzu kommt auch der *S3 Object Lock*, das heißt, die Immutability von S3 mit der Unveränderbarkeit der Daten mittels Lock-Retention (Vorgabe der Aufbewahrungsfrist).« Außerdem sei ein Restore-Virus-Check der Backup-Daten eine gute Möglichkeit mehr Sicherheit zu erreichen. Hier werden beim Restore die Daten noch einmal auf Viren überprüft. Sollte das Backup kompromittiert sein, werden infizierte Dateien gemeldet und lassen sich vom Restore ausschließen. Dies sei laut Mayer ein weiterer Sicherheitsvorteil, denn zum Zeitpunkt der Datenwiederherstellung sind meist mehr Virenpattern bekannt als zum Backup-Zeitpunkt.

Albrecht Hestermann
Actidata

»Ransomware ist das Thema bei allen Projektierungen rund um Secondary-Storage und Backup.«

»Wurde die Unveränderbarkeit geschriebener Daten früher eher unter dem Aspekt der Rechtskonformität gesehen, ist heute der Schutz vor Ransomware der Kerngedanke bei dieser Funktionalität«, ergänzt Hornetsecurity-CEO Hofmann. »Auch die nähere Angliederung an Applikationen dürfte mehr Fahrt aufnehmen, um das Management zu vereinfachen. Das Thema M365 im Betrieb wird auch immer stärker ganzheitlich verstanden: IT Manager möchten alle dazugehörigen Aspekte, also Security, Security-Awareness, Compliance und auch Backup zentral über eine Konsole verwalten. Das konzeptionelle Denken von Infrastruktur von der Applikation aus wird weiterhin Trend bleiben.«

Datensicherung ganzheitlich betrachtet

»Bei der Datensicherung geht es nicht mehr um die Sicherung einzelner Files«, mahnt Novastor-Chef Utzinger. »Im Vordergrund steht die schnelle Betriebswiederherstellung nach einem Desaster, wie einem Cyberangriff. IT-Verantwortliche stehen nicht vor der Aufgabe, sämtliche Daten im Unternehmen einfach zu sichern. Vielmehr stehen sie vor der Herausforderung des Disaster-Recovery-Managements. Das heißt, die müssen sicherstellen, dass die Organisation im Ernstfall schnellstmöglich wieder arbeitsfähig ist und die Daten wieder verfügbar sind.« Gerade der Ansatz, ganzheitliche Lösungen aus der Applikationssicht zu denken, soll KMUs helfen, ihre IT schlank und effizient zu gestalten. Experten zufolge bedeuten Silo-Strukturen mehr Aufwand in der Organisation, im Management und in der Administration, und seien somit ein Kostentreiber. Ziel solle sein, dass Lösungen ganzheitlich alle Aspekte und bestimmte Anwendungen abdecken, um damit starre Strukturen aufzubrechen und IT-Managern letztendlich die Arbeit zu erleichtern. ■

Andreas Mayer
SEP

»Ransomware greift auch die Datensicherung an und daher benötigen auch die Backups einen entsprechend Schutz.«

Data-Protection als übergreifendes Konzept

GANZHEITLICHE DATENSICHERUNG IST UNTERNEHMENSPFLICHT

Die Datensicherung als das schlichte Vorhalten von Datenkopien zu sehen, ist nicht mehr zeitgerecht. Vielmehr benötigen Unternehmen eine übergreifende Strategie, die alle Eventualitäten und Katastrophenszenarien abdeckt. Neben der notwendigen Technik und Ausstattung gehören auch erprobte Notfallpläne zum Konzept.

Michael Baumann
speicherguide.de

Geheimnis ist es keines mehr: Mit der wachsenden Digitalisierung und aufgrund externer und interner Gefahren wächst die Bedeutung von Backup und Disaster-Recovery für Unternehmen aller Größen, Branchen und Organisationsformen. Da auch eine Diversifizierung der Daten stattfindet, werden Box-Lösungen den Anforderungen nicht mehr gerecht. Die Datensicherung sollte vielmehr als übergreifendes Konzept angegangen werden. Doch was bedeutet das im Detail?

Die kurze Antwort sofort: Benötigt wird eine Software-Lösung für Datensicherung und -wiederherstellung im Unternehmensmaßstab, die vollständig integrierte Funktionalität für heterogene Umgebungen bietet. Sie orchestriert Datenschutz auf Band, Festplatte und Cloud aus physischen oder virtuellen Ressourcen, Daten, Betriebssystemen und Anwendungen in Rechenzentren und an entfernten Standorten.

Leitlinien für modernes Backup und Recovery

Der Branchenverband **Bitkom** in seinem »Leitfaden Backup/Recovery/Disaster-Recovery« oder auch das **BSI** (Bundesamt für Sicherheit in der Informationstechnik) im Leitfaden zum Thema Ransomware definieren die unterschiedlichen Disziplinen der Datensicherung.

Backup beschreibt dabei die Sicherung der Daten und Datenzuständen. Das primäre Ziel einer Datensicherung ist, ein Unternehmen vor dem Verlust seiner Daten zu bewahren. Im Kern gilt die berühmte, aber nicht immer befolgte 3-2-1-Regel: Drei Datenkopien, zwei Medien, ein externes Offline-Backup. Typischerweise sollte ein Medienbruch in einer Backup-Kette integriert werden, und ein separates Speichermedium für die Auslagerung (Air-Gap) verwendet werden. Insbesondere soll dies dem Schutz vor Ransomware dienen.

Beim Restore geht es darum, Datenzustände in Form von Objekten, Dateien, Datenträgern oder auch Applikationssystemen wiederherzustellen. Das Recovery geht darüber hinaus und umfasst neben dem Restore weitere IT-Prozesse zu einer vollständigen Dienst-Wiederherstellung. Dazu werden Recovery-Point-Objective (RPO) und Recovery-Time-Objective (RTO) definiert. Ersteres bestimmt die Summe der Daten, deren Verlust bei einem Ausfall noch erträglich ist, zweiteres die Zeit, die benötigt wird, um die Dienste wieder in Betrieb zu nehmen.

Da diese unterschiedlichen Aspekte der Datensicherung ineinandergreifen sollten, wird deutlich, dass einfache Silo- oder Boxlösungen für eine effektive Absicherung der Daten und damit der Geschäftsprozesse nicht ausreichen. Deshalb empfehlen Experten heute Hardware-unabhängige Software, die all diese Funktionen über Tape, HDD, SSD und Cloud mit physischen oder virtuellen Systemen abdecken kann.

Backup-Best-Practices – Probleme und Herausforderungen

Backup ist die letzte Schutzmaßnahme, mit der im Falle eines Ransomware-Vorfalls, bei technischen Fehlfunktionen oder einer natürlichen Katastrophe (Brand, Sturm, Erdbeben, Überschwemmung), aber auch, wenn Mitarbeiter Daten absichtlich oder un-

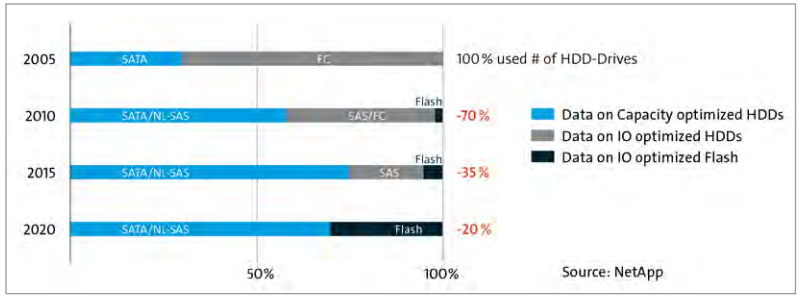
absichtlich löschen, die Verfügbarkeit der Daten gewährleistet werden kann. Jede Institution sollte daher über ein Datensicherungskonzept verfügen, wie es im »IT Grundschutz Kompendium: CON.3. Datensicherungskonzept« definiert wird.

Notstände bei der Datensicherung

Das hört sich zunächst selbstverständlich an. Jedoch sieht die Realität oftmals anders aus. Die Bundesbehörde benennt dazu die in der Praxis am häufigsten auftretenden Kardinalfehler:

- Fehlende Datensicherung
- Fehlende Wiederherstellungstests
- Ungeeignete Aufbewahrung (physisch wie elektronisch/virtuell) von Datensicherungen
- Fehlende oder unzureichende Dokumentation
- Missachtung gesetzlicher Vorschriften
- Unsichere Cloud-Anbieter für Online-Datensicherungen
- Ungenügende Speicherkapazitäten
- Unzureichendes Datensicherungskonzept

Zu letzterem gehört beispielsweise der Fehler, im Falle der Verschlüsselung von Sicherungsdaten, diese Schlüssel nicht getrennt aufzubewahren. Zudem ist es mittlerweile bei Schad-Software üblich, dass Angreifer Administrationsrechte »kapern« und



Grafik: Bitkom

Flash-Speicher ersetzt IO-optimierte HDDs

Backups ebenso infizieren wie Produktivsysteme. Eine wie auch immer geartete Offline-Kopie ist deshalb ebenso eingefordert wie die Planung und Vorbereitung des Wiederanlaufs und der Rücksicherung der Daten.

Die Mindestanforderungen an ein Datensicherungskonzept – und damit verbunden einer geeigneten Datensicherungslösung, – müssen demnach Speichervolumen, Änderungsvolumen, Änderungszeitpunkte, Verfügbarkeitsanforderungen, Integritätsbedarf, rechtliche Anforderungen sowie ausreichende Dokumentation umfassen.

Neue Technologien – neue Herausforderungen

Die Kosten von Datenverlusten und der Nichtverfügbarkeit von IT-Services werden immer höher. Deshalb gilt es nicht nur die Verfügbarkeit von Primärspeicher zu optimieren, sondern auch die Service-Level-Anforderungen bei Backup und Desaster-Recovery zu erhöhen, um die Geschäftsfähigkeit eines Unternehmens sicherzustellen. Eine Reihe technologischer bzw. datenbezogener Entwicklungen der letzten Dekade erschweren IT-Verantwortlichen aber die Umsetzung dieser Zielvorgabe erheblich.

1. Bei Harddisks (HDD) entwickeln sich die Kapazitäten pro Diskspindel deutlich schneller als deren Geschwindigkeit. Um dies zu kompensieren, werden Flash-Speicher in Form von SSDs, Flash-Karten am Storage-Controller und Applikationsserver mit ihren sehr schnellen Zugriffszeiten zusätzlich genutzt. Durch Komprimierung und/oder Deduplizierung der Daten wird das Schreiben der Daten bei der Sicherung ebenso wie das Auslesen im Falle der Wiederherstellung bei der Nutzung ungeeigneter Backup-Software erschwert oder verlangsamt.
2. Die Anzahl unstrukturierter Dateien wächst, die Sicherung von Millionen von Datei-basierten Datensätzen wird zur Herausforderung. Als Antwort darauf wurden zu den bekannten Block- und File-Systemen Objektspeicher als neue Speicherklasse entwickelt, die bevorzugt auch in Containern in der Cloud abgelegt werden. Insgesamt ist die Komplexität der Datensicherung eher gestiegen, anstatt abzunehmen.
3. Strukturierte Daten, also etwa Block-basierte Datenbanken wie *Oracle* oder *SAP HANA* weisen erhöhte Anforderungen auf. Das sind nicht nur in Kapazitätsanforderungen , sondern vor allem I/O- und Performance-Anforderungen. Dies gilt für den Produktivbetrieb ebenso wie für die Sicherung, die um IOs konkurrieren. Vor allem die Laufzeiten bei der Datenbanksicherung aufgrund des immer höheren IO-Aufwandes werden zum Problem. Größere Datenbanken benötigen zudem mehr Recovery-Points in bestimmten Zeitrahmen.
4. Zentrale Rechenzentren (Core) und Niederlassungen und entfernte Standorte (Edge) wollen in einem konsistenten Modus gesichert werden. Dies erfolgt durch eine Übertragung der Backup-Daten in einen zentralen Standort oder zu einem Cloud-Speicher. In beiden Fällen sind dafür ein einheitliches Datenformat sowie eine adäquate Netzwerkanbindung (WAN) notwendig.
5. Die Virtualisierung von Applikationsservern ist zum Standard geworden. Zu sichernde virtuelle Maschinen (VMs) und damit verbunden virtualisierter Backup-Targets wechseln dynamischer die Lokation. Dies erschwert es, die klassischen 1:1-Beziehungen zwischen lokalem Backup-Server und lokalem Backup-Client herzustellen.
6. Trotz der wachsenden Komplexität sollte eine effiziente Datensicherung regelbasiert und automatisiert erfolgen. Dazu müssen Data Protection und Disaster Recovery »as a Service« (DPaaS, DRaaS) im Verbund zu On-Premise-Sicherungen auch über die Cloud integriert werden können. Doch längst nicht alle Datensicherungslösungen verstehen sich dabei auf multiple und heterogene Cloud-Umgebungen, die auch mit On-Premises-Konzepten in Einklang zu bringen sind. Im schlechten Falle bilden sich neue Backup-Inseln, die den aktuellen Anforderungen nicht genügen. ■

Weiterführende Links:

➔ **Bitkom-Leitfaden Backup/Recovery/Disaster-Recovery**

➔ **BSI Ransomware – Bedrohungslage, Prävention & Reaktion**

Bild: shutterstock/Ar_TH

Peter Marwan
speicherguide.de

Immutability für den Mittelstand

FÜRS UNERWARTETE GEWAPPNET SEIN

Keine Branche ist vor Ransomware-Angriffen gefeit. Den Mittelstand macht die Kombination aus Fachkräftemangel, knappen Budgets und rasch komplexer werdender IT-Infrastruktur besonders anfällig. Benötigt werden nicht nur unkomplizierte und den Anforderungen gewachsene Lösungen, sondern auch moderne Bezahlmöglichkeiten, wie Pay-per-Use.

Dem aktuellen Bundeslagebild Cybercrime zufolge steigt das Bedrohungspotenzial durch Ransomware weiterhin stark an. »Ransomware bleibt der Modus Operandi mit dem höchsten Schadenspotenzial im Bereich Cybercrime«, teilte das *Bundeskriminalamt* (BKA) bei der Vorstellung seines Berichts mit. Betroffen sind Unternehmen jeder Branche sowie Behörden, Kommunen und Bildungseinrichtungen.

Die Schäden liegen in Milliardenhöhe. Konkret spricht das BKA für 2021 (für 2022 liegen die Daten noch nicht vor) von 24,3 Milliarden Euro alleine durch Erpressung mit gestohlenen oder verschlüsselten Daten in Deutschland. Besserung ist nicht in Sicht: Die Allianz-Tochter *Allianz Global Coporate & Specialty* (AGCS) nennt Zahlen, wonach Unternehmen bis Ende 2023 durch Ransomware weltweit mit Schäden in Höhe von 30 Milliarden US-Dollar rechnen müssen.

Die Bandbreite der genannten Werte erklärt sich durch unterschiedliche Definitionen und Schadensbewertungen – die Tendenz ist aber klar: Sie zeigt nach oben.

Die vom BKA genannten Zahlen zu den Profiten der Ransomware-Gruppierungen basieren auf Untersuchungen von *Chanalysis* und scheinen mit 602 Millionen Dollar dagegen fast gering. Sie zeigen dennoch, dass es sich um ein profitables Geschäft in großem Stil handelt. Auch der durchschnittliche Lösegeldbetrag nimmt immer weiter zu. Er stieg von 169.446 Dollar 2020 auf 204.695 Dollar im Jahr 2021 an.

Lösegeldforderung nur ein kleiner Teil des Problems

Der Vergleich der Zahlen macht auch deutlich, dass die Lösegeldzahlung für Unternehmen das kleinere Problem ist. Viel schwerer wiegen die Einbußen durch den Stillstand des Unternehmens, der Verlust von Geschäftsbeziehungen und die Kosten zur Wiederherstellung. Denn die Schadenssumme ist um den Faktor 40 höher als die Einnahmen der Cyberkriminellen.

Grafik: Cristie

Die wichtigsten Kriterien einer modernen Backup- und Disaster-Recovery-Lösung im Überblick.

Bild: Cristie

Schlüsselfertige Hard- und Software-Kombi: Die Rubrik RCDM-Software mit Dell Poweredge-Server als Pay-per-Use-Lösung.

Kein Wunder also, dass zum Beispiel *Mario Greco*, Chef des Versicherungskonzerns *Zurich*, im Dezember in einem Interview erklärte, dass Cyberangriffe bald »unversicherbar« werden könnten. Womöglich als Reaktion darauf berichteten Sicherheitsforscher kurz darauf von einer Ransomware-Gruppe, die ihre Opfer nach Details ihrer Cyberversicherung befragt und verspricht, die Lösegeldforderung der Deckungssumme anzupassen. Offenbar will man die Kuh nicht schlachten, die sich so gut melken lässt.

Angriffe sind kaum zu vermeiden

Das alte Credo der IT-Security-Branche – »100-prozentige Sicherheit gibt es nicht«, gilt auch für Ransomware-Angriffe. Bei ihnen gelangt die Malware oft über E-Mail- Phishing-Angriffe oder Social-Engineering ins Unternehmen – also Methoden, bei denen Unachtsamkeit oder Unwissen der Beschäftigten ausgenutzt werden. Die sind zwar aufwändig, aber die Angreifer suchen sich ihre Opfer gut aus und spekulieren auf hohe Gewinne.

Eine im Februar 2023 veröffentlichte Sonderauswertung des Mittelstandspanels der Staatsbank KfW zeigt, dass in Deutschland besonders Unternehmen mit mehr als hundert Beschäftigten und von denen solche mit besonders ausgeprägten Digitalisierungsaktivitäten ins Visier der Angreifer geraten. So wurden etwa 43 Prozent der Unternehmen attackiert, die im Jahr 2020 mehr als 10.000 Euro für Digitalisierungsprojekte ausgegeben hatten. Bei Unternehmen ohne derartige Investitionen lag der Anteil der angegriffenen Firmen dagegen bei 23 Prozent. Was zunächst paradox klingt, hat Methode: Offenbar rechnen die Angreifer damit, dass für Firmen, die Digitalisierung aktiv betreiben, Daten einen hohen Wert haben und sie daher auch eher bereit sind, das geforderte Lösegeld zu bezahlen.

Business-Continuity muss das Ziel sein

Nach einem Ransomware-Angriff haben Unternehmen in der Regel mit weitreichenden operativen und logistischen Problemen zu kämpfen. Ohne externe Spezialisten lassen sich die nicht meistern. Zum Beispiel muss erst einmal festgestellt werden, wann das letzte saubere Backup erfolgte. Keine triviale Aufgabe, da die Angreifer im Schnitt 45 Tage im Netzwerk verbrachten, bevor sie zuschlagen. In der Zeit durchleuchten sie die gesamte Netzstruktur inklusive der Backup-Prozesse, versuchen, auch die Back-

Cyber-Recovery im Detail

Für weitere Kopien und Archivierung der Daten bieten Rubrik und Cristie vielfältige Optionen:

- Replication to Rubrik ist eine Backup-basierte, WAN-optimierter Replikation
- Archive to S3 – lokal oder nachhaltig bei Cristie im Windrad als Sicherungs-, Replikations- und Archivierungsziel für die Sicherungsprozesse.
- Archive to NFS ermöglicht niedrigere RTOs von Archivspeichern und macht regelmäßige, vollständige Snapshots unnötig, was auch die Storage-Kosten reduziert.
- Archive to Tape unterstützt Kunden, für die die Archivierung auf Band eine unvermeidliche gesetzliche oder Compliance-Anforderung ist
- Archive to Cloud rationalisiert die Archivierung in privaten und öffentlichen Clouds (wo möglich und erwünscht) und reduziert so Kosten bei gleichzeitig hoher Verfügbarkeit.

ups zu infizieren und ziehen oft noch Daten ab, um mit deren Veröffentlichung zu drohen. Ausfälle von bis zu drei Wochen sind keine Seltenheit. Das können sich die meisten Firmen nicht leisten.

Daher rückt der Begriff Business-Continuity immer mehr in den Vordergrund. Dabei geht es einerseits darum, die Relevanz einzelner Anwendungen für das Geschäft festzulegen und Maßnahmen zu ergreifen, die auch nach einem Totalausfall gewährleisten, dass die unverzichtbaren Prozesse möglich schnell wieder laufen. Andererseits geht es aber auch darum, das Backup als aktiv nutzbare Ressource in einer breit angelegten Cyber-Security-Strategie zu sehen, als letzte Verteidigungslinie und gleichzeitig Startpunkt für die Wiederherstellung. Experten empfehlen dafür per Air-Gap getrennte, unveränderliche, zugriffsgesicherte Backups. Sie schützen auch davor, dass Angreifer gezielt Backups verschlüsseln, um ihre Forderungen durchzusetzen. In Großunternehmen hat sich dafür unter anderem **Rubrik** als Anbieter etabliert.

Pay-per-Use: Bedarfsgerecht bezahlen

Mussten Backup-und-Recovery-Lösungen bisher komplett oder zumindest in Raten bezahlt werden, kommen nun bedarfsgerechte Bezahlmodelle hinzu. **Cristie Data** bringt die Rubrik-Lösung für Daten-, Ransomware- und Disaster-Recovery als *Cristie Cyber Recovery powered by Rubrik* nun auch im deutschsprachigen Raum als mittelstandstaugliches »True Opex«-Pay-per-Use-Angebot. Zusammen mit *Cristie Nordic* bietet Cristie das Modell schon länger an und versetzt auch Service-Provider in die Lage, Backup- und Recovery-Services anzubieten. Dafür werden auch Partner in der DACH-Region gesucht.

»Aus Sicht des Mittelstands attraktiv sind neben den Pay-per-Use-Modellen sowie den mit MSP-Partnern angebotenen SaaS-basierten Nutzungsmodellen auch die zusätzlich enthaltenen Dienste und Mehrwertfunktionen«, erklärt Cristie-Geschäftsführer **Volker Wester**. »Denn Pay-per-Use macht die Enterprise-Lösung von Rubrik für den Mittelstand erst nutzbar und bezahlbar. Die Kosteneinsparungen liegen zwischen 20 und 30 Prozent. Mit Tools zur Vorhersage der möglichen Einsparungen führen wir mit Unternehmen gerne gemeinsam eine erste Berechnung durch.«

Die Services und Mehrwertfunktionen basieren unter anderem auf dem Status von Cristie als einer der wenigen Rubrik-Partner mit der *Velocity ELITE*-Zertifizierung und dem Status als autorisierter Support-Partner. »Dadurch ist auch Support auf Deutsch gewährleistet«, sagt Wester. »Außerdem beraten und unterstützen wir vom Design über die Implementierung bis zur Wartung und Betrieb sowie bei der Auswahl der Verbrauchsmodelle, Compliance-Fragen und dem Lizenzmanagement.«

Rubrik hat zusammen mit *Dell* die Software *Rubrik Cloud Data Management* (RCDM) auf *Dell PowerEdge*-Servern validiert. Cristie bietet die Lösung als Kombination von Hard- und Software an. Da die Hardware mit dem monatlichen Pay-per-Use-Modell ebenfalls bereits abgedeckt ist, bleibt das Gesamtpaket für Firmen kalkulierbar und sind die Kosten transparent.

Schnelles Disaster-Recovery & effizienter Backup-Betrieb

Im Normalbetrieb unterstützt Rubrik Unternehmen beim umfassenden Data-Management. »Durch SLA-Automatisierung lassen sich zahllose Sicherungsjobs durch wenige Policies ersetzen, die auf alle Workloads angewendet werden«, erläutert Wester. Die Funktion *Rapid Recovery* helfe, einzelne Dateien oder Objekt schnell zu finden und wiederherzustellen. Dank der umfangreichen APIs kann jede Aktion skriptgesteuert und automatisiert ausgeführt sowie in Tools integriert werden, die Unternehmen bereits nutzen und mit denen ihre Administratoren vertraut sind.

»Im Ernstfall bietet *Cristie Recovery Assurance* durch Automatisierungs- und Orchestrierungsfunktionen für die Notfallwiederherstellung sowie die Möglichkeit, Systeme in einer Sandbox-Umgebung wiederherzustellen«, sagt Wester. »So lassen sich Anomalien feststellen und das letzte gute Backup schnell identifizieren. Dadurch reduzieren sich Wiederherstellungsprozesse von üblicherweise mehreren Wochen auf maximal wenige Tage und lassen sich kurze RTO-Ziele definieren. Das hilft Unternehmen auch bei Gesprächen mit Banken oder Cyberversicherungen.«

Bezahlbare Absicherung nach dem Stand der Technik

Selbst mit hohem technischen und administrativen Aufwand können Unternehmen nicht sicherstellen, dass sie gegen Ransomware-Angriffe immun sind. Dennoch müssen sie sich entsprechend »dem Stand der Technik« absichern, um Compliance-Anforderungen zu entsprechen. Eine wesentliche Komponente ist dabei eine moderne Backup- und Disaster-Recovery-Lösung.

»Finanziell erschwinglich und administrativ beherrschbar werden Mittelstandslösung durch Zusatz-Services und Pay-per-Use-Modelle«, meint Cristie-Chef Wester. »Sie erlauben Unternehmen die bestmögliche Vorbereitung auf einen Ransomware-Angriff und helfen ihnen im Normalbetrieb, ihre Daten unternehmensweit und unabhängig vom Speicherort weitgehend automatisiert zu verwalten.« ■

Weiterführende Links:

➔ Mehr zu Cristie Cyber Recovery und der Initiative Expect the Unexpected

Aus 3-2-1-Backup wird 3-2-1-1-0-Recovery

DESIGN FOR RECOVERY: WARUM SIE KEINE BACKUP-STRATEGIE BRAUCHEN

Die Bedrohungslage ist durch Cyberattacken so hoch wie nie. Gleichzeitig räumen viele Firmen eine deutliche Unterdeckung ihrer eigenen IT-Sicherheit ein. Helfen sollen laut BSI »Backups, die funktionieren«. Jedoch ist dieser Ansatz vom falschen Ende gedacht, vielmehr sollten IT-Manager ihren Fokus auf die Wiederherstellung richten.

Hannes Heckel
FAST LTA

Fast alle Angriffe zielen mittlerweile auf Backups, wie Backup-Spezialist *Veeam* in einer Umfrage unter 1.000 Unternehmen herausgefunden hat. Ungefähr drei Viertel sind erfolgreich, so dass Daten nicht oder nicht vollständig wiederhergestellt werden konnten. Da laut einer *Bitkom*-Studie fast die Hälfte deutscher Unternehmen keine belastbaren Notfallpläne besitzt, überrascht auch nicht, dass fast die Hälfte betroffener Unternehmen lieber Lösegeld bezahlt hat, um schneller wieder handlungsfähig zu sein. Das zeigt: Backups allein sind nicht die Lösung. Entscheidend ist der Fokus auf die schnelle und sichere Wiederherstellung der Daten. Dies gilt umso mehr, da Ausfallzeiten der IT zu den größten Kostentreibern nach einem Angriff zählen.

Aus 3-2-1-Backup wird 3-2-1-1-0-Recovery

Backup bietet einfache Antworten, Recovery stellt die richtigen Fragen

Es ist wie so oft im Leben: Einfache Antworten sind angenehm, helfen aber meist nicht weiter. Der Gedanke, für den Notfall eine Sicherheitskopie (oder mehrere) zu haben, hält den heutigen Anforderungen nicht mehr Stand. Stattdessen müssen sich IT-Verantwortliche die richtigen Fragen stellen:

- Was ist das Schlimmste, das passieren kann?
- Welche Auswirkungen hat das auf das Unternehmen, die Behörde oder die Einrichtung?
- Wie können die Folgen so weit wie möglich abgemildert werden?

Dabei werden für verschiedene Bereiche und deren Daten unterschiedliche Anforderungen entstehen, die zudem den geltenden Rahmenbedingungen angepasst werden müssen – Budget, rechtliche Vorgaben und technische Machbarkeit. Erst dann können die zu den einzelnen Anforderungen passenden Technologien und Produkte ausgesucht werden. Dabei ist besonders auf die Absicherung der Backups selbst vor Angriffen zu achten – etwa durch den konsequenten Einsatz geeigneter Immutability-Maßnahmen.

Datenklassen identifizieren

Nicht alle Daten sind gleich. Nicht alle Abteilungen und Geschäftsbereiche sind gleich. Unterschiedliche Anforderungen erfordern verschiedene Maßnahmen. Deshalb ist es entscheidend, die existierenden Daten in Klassen aufzuteilen. Dabei können Kriterien wie Wichtigkeit, Dringlichkeit, Wiederherstellbarkeit und rechtliche Relevanz herangezogen werden. Am Ende sollten mindestens drei Klassen entstehen:

1. Kritische Daten, die zum unmittelbaren und unterbrechungsfreien Betrieb notwendig sind.
2. Wichtige Daten, die zwar wichtig, aber nicht unmittelbar für den Weiterbetrieb notwendig sind.
3. Unkritische Daten, die mit vertretbarem Aufwand erneut erzeugt werden können.

Außerdem sollte möglichst frühzeitig identifiziert werden, welche Daten sich zeitnah in eine Archivierung überführen lassen. Diese verändern sich nach dem Erzeugen nicht mehr und sind nur noch selten im Zugriff. Das Verdrängen dieser Daten auf einen per Hardware-WORM abgesicherten Archivspeicher entlastet die gesamte Datensicherung.

RTO, RPO & Speichertechnologien

Für jede Datenklasse müssen nun Grenzwerte definiert werden. Dabei gilt es, die Anforderungen gemäß des zur Verfügung stehenden Budgets in Hinsicht Performance (RTO: wie schnell kann wiederhergestellt werden?) und Kapazität (RPO: wie lang darf das letzte Full-Backup zurückliegen?) abzuwägen. Während kritische Daten auf schnellem, aber teurem Flash-Storage gut aufgehoben sind, können wichtige und unkritische Daten auch auf günstigeren Speichern liegen. Auf alle Fälle muss jeder Speicherbereich mit geeigneten Maßnahmen vor Missbrauch geschützt sein. Verschiedene Immutability-Maßnahmen sind zwingend dem jeweiligen Bereich entsprechend einzusetzen. Auch hier bestimmt das Budget meist die Tiefe der Maßnahmen. Nicht vernachlässigen darf man den Schutz vor Ausfall von Komponenten und Systemen durch Redundanz und Geo-Redundanz.

Mit dem Silent Brick System lassen sich alle Recovery-Anforderungen erfüllen.

Bild: FAST LTA

Vom 3-2-1-Backup zum 3-2-1-1-0-Recovery

Das seit Jahrzehnten bewährte 3-2-1-Prinzip, um Datenverlust vorzubeugen, wird nun durch zwei wichtige Parameter zum Schutz vor den Folgen einer Cyberattacke erweitert. Weiter gilt: Mindestens drei Daten-Kopien auf mindestens zwei Medien bzw. Formaten, davon mindestens eine in einem separaten Speichersystem. Hinzu kommt mindestens eine Kopie, die komplett offline ist (Air-Gap), und vor allem die Anforderung an ein garantiert fehlerfreies Recovery. Dabei werden Worst-Case-Szenarien durchgespielt, Notfallpläne erstellt, getestet und verbessert, sowie Systeme und Prozesse optimiert. Am Ende stehen Recovery-Pläne für die einzelnen Datenklassen, die jeder Belastung standhalten.

Investition in Recovery – nicht (nur) in Backup

Reine Backup-Medien (z. B. Tapes), auf denen Daten nicht verfügbar sind, genügen heutigen Ansprüchen nicht mehr. Selbst Air-Gap-Medien und Objektspeicher müssen die Daten so vorhalten, dass im Ernstfall ohne Verzögerung und wahlfrei darauf zugegriffen werden kann. Außerdem muss das Prinzip der Datenhoheit gelten, ein Delegieren der Verantwortung auf Dienstleister ist aus Sicht der DSGVO nicht vertretbar. Am Ende stehen Storage-Systeme, die größtmögliche Sicherheit und Flexibilität bieten, bezahlbar in Anschaffung, Wartung und Betrieb sind, und rechtlichen Auflagen genügen. ■

Immutable-Storage: Nur im Mix sicher

Backup-Daten sind nur sicher, wenn sie trotz erfolgtem Angriff nicht manipulierbar oder löschbar sind. Genau dazu dient Immutable-Storage – unveränderbares Speichern. Um tatsächlich cyber-resilient zu sein, ist aber eine Kombination aus verschiedenen Technologien notwendig: Ständige, kurzfristige Backups müssen per Continuous-Snapshots geschützt werden – so ist eine schnelle Wiederherstellung der am dringendsten benötigten Daten möglich. Air-Gap oder die Auslagerung auf Objektspeicher mit Object-Locking schützen eher die langfristigen Datensicherungen als »Last Line of Defense«. Hardware-WORM kommt überall da zum Einsatz, wo Daten auf keinen Fall verloren gehen dürfen.

Weitere Informationen:

FAST LTA GmbH

Rüdesheimer Str. 11
80686 München
Tel. 089/89 047-0
E-Mail: info@fast-lta.de
www.fast-lta.de

FAST LTA

www.fast-lta.de

Sitz der Gesellschaft:
München

Niederlassung in Deutschland:
München

Jahr der Gründung:
1999

Zielgruppe:
KMUs, VARs und Industriekunden

Wir sind die Spezialisten für Sekundärspeicher, für Archivierung und Backup.

Unsere Produkte und Services helfen mittelständischen Anwendern, Datensicherung und Datenmigration zu vereinfachen, rechtliche und regulatorische Risiken zu minimieren, und das langfristige Risiko, Daten zu verlieren, nachhaltig zu verringern.

Holstein IT-Solutions

truenas.de/

Sitz der Gesellschaft:
Hagen

Jahr der Gründung:
2015

Zielgruppe:
mittelständische Industrieunternehmen, Behörden, Bildungseinrichtungen, Gesundheitswesen, Energiesektor, Mediendienstleister

Holstein IT-Solutions aus Norddeutschland vereint kompetente IT-Experten unter seinem Dach. Das junge und motivierte Team unterstützt Behörden, Bildungseinrichtungen sowie mittelständische und große Unternehmen bei Infrastrukturprojekten von der Planung über die Umsetzung bis hin zum Betrieb. Die Stärken sind Enterprise-grade Storage-, Security-, Netzwerk- und Virtualisierungslösungen. Der IT-Systemspezialist setzt bevorzugt auf Open Source sowie offene Standards für mehr Kompatibilität und Investionsschutz.

N-TEC GmbH

n-tec.eu

Sitz der Gesellschaft:
Ismaning

Jahr der Gründung:
2001

Zielgruppe:
Vor allem KMU + öffentliche Auftraggeber

N-TEC konzentriert sich auf universell einsetzbare und skalierbare Speicherlösungen für Unternehmen und setzt dabei auf sorgfältig ausgewählte, namhafte Hersteller. Im Fokus stehen Object Storage Lösungen für Private Clouds und Storage Systeme mit hoher Verfügbarkeit. Klassische Server, SAN und Unified Storage Systeme, sowie revisionssichere WORM Archive und Backup Lösungen runden die Produktpalette ab. Kunden erhalten bei N-TEC alles aus einer Hand – vom Pre Sales bis zum After Sales und langjährigen Support. N-TEC ist immer der zentrale Ansprechpartner für alle Belange.

Quantum

quantum.com/de

Sitz der Gesellschaft:
San Jose, USA

Niederlassung in Deutschland:
München

Jahr der Gründung:
1980

Zielgruppe:
Mittelständische und große Unternehmen

Mit Technologien und Services von Quantum lassen sich digitale Inhalte erfassen, verarbeiten und gemeinsam nutzen – und außerdem für Jahrzehnte vorhalten und sichern. Unsere Plattformen bieten die schnellste Performance für große Datenmengen, industrielles IoT und hochauflösendes Film- und Bildmaterial – für jede Phase des Datenlebenszyklus – von der Kollaboration und Analyse in Echtzeit bis zur kostengünstigen Archivierung.

Absicherung der Infrastruktur nicht ausreichend

CYBERATTACKEN: SCHUTZ GEGEN DIE AUSWIRKUNGEN ERHÖHEN

Cyberangriffe sind inzwischen die wichtigste treibende Kraft für die Datenwiederherstellung. Die meisten Abwehrstrategien sind aber nicht darauf abgestimmt. Die richtige Vorbereitung darf zudem nicht nur die Absicherung der Infrastruktur berücksichtigen, sondern vor allem auch Maßnahmen gegen die Bekämpfung eine Attacke.

Karl Fröhlich
speicherguide.de

Deutsche Unternehmen sind nicht ausreichend vor Schäden durch Cyberattacken geschützt. Eine andere Interpretation lassen aktuelle Zahlen nicht zu. Laut dem Digitalverband **Bitkom** entsteht ein Schaden von 203 Milliarden Euro pro Jahr durch Angriffe auf deutsche Unternehmen. Im Vergleich dazu wächst der IT-Sicherheitsmarkt viel zu langsam. Die Ausgaben für Hardware, Software und Dienstleistungen im Bereich IT-Sicherheit lagen laut Bitkom 2022 bei knapp acht Milliarden Euro. Für 2023 wird ein 10-prozentiges Wachstum erwartet und im Jahr 2025 soll der Sprung über die 10-Milliarden-Euro-Marke geschafft werden. Eine viel zu große Diskrepanz.

»Cyberattacken können für Unternehmen aller Branchen existenzbedrohend sein«, sagt Bitkom-Hauptvorstand **Udo Littke**. »IT-Sicherheit muss Thema des Top-Managements sein und mit entsprechenden personellen und finanziellen Ressourcen ausgestattet werden.«

Der NIST-Standard (National Institute of Standards and Technology) gewichtet alle Cyber-Security-Maßnahmen gleich, um eine Cyber-Resilience zu erreichen. »In der Praxis ist es allerdings so, dass 85 bis 95 Prozent der Investitionen in die Absicherung der Infrastruktur fließen«, erklärt **Frank Schwaak**, Field CTO bei **Rubrik**, »und nur fünf bis 15 Prozent in Maßnahmen gegen die Bekämpfung eines Angriffs.« Der Schutz vor Auswirkungen durch Cyber-Attacken ist in den meisten Firmen absolut unzureichend.

Datenresilienz: schnell reagieren

Unter **Datenresilienz** versteht man die Fähigkeit eines Unternehmens, schnell auf Angriffe auf seine Daten zu reagieren und den normalen Betrieb wiederherzustellen. Die Herausforderung besteht darin, dass Unternehmen in der heutigen Zeit mit einer wachsenden Anzahl von Bedrohungen konfrontiert sind, die von Ransomware-Attacken bis hin zu Naturkatastrophen reichen können. Deswegen ist es unerlässlich, dass Unternehmen Maßnahmen ergreifen, um ihre Daten zu schützen und sicherzustellen, dass sie im Notfall wiederhergestellt werden können.

Um Datenresilienz in Unternehmen zu erreichen, empfiehlt das NIST einen Rahmen, der sich aus fünf Kernkomponenten zusammensetzt:

- Das **Identifizieren** (Identify) aller IT-Security-Risiken für kritische Systeme und Daten im Unternehmen.
- Der Implementierung von **Schutz**-Systemen und Sicherheitsmaßnahmen zur Vermeidung von Datenverlusten und -angriffen (Protect).
- Dem **Erkennen** von allen IT-Security-Ereignissen (Detect), die eine Bedrohung darstellen sowie von Datenverlusten und -angriffen.
- Dem Ergreifen von Maßnahmen zur schnellen **Reaktion** auf Angriffe, Bedrohungen und Datenverluste (Respond).
- Die **Wiederherstellung** von Daten, Geschäftsabläufen und aller Dienste, die durch eine Cyberattacke beschädigt wurden (Recover).

In der Praxis können Unternehmen diese Komponenten durch eine Kombination von technischen und organisatorischen Maßnahmen umsetzen. Technische Maßnahmen können zum Beispiel Firewalls, Verschlüsselung, regelmäßige Backups und redundan-

te Systeme umfassen. Zu den organisatorischen Maßnahmen gehören unter anderem Schulungen für Mitarbeiter, Notfallpläne und regelmäßige Überprüfungen der getroffenen Sicherheitsmaßnahmen.

»Für eine ausreichende Datenresilienz empfehlen wir für Backup-Daten ein unveränderliches Dateisystem zu verwenden«, rät Schwaak. »Zudem gilt es, ein richtiges Air-Gap zu implementieren sowie offene und auffindbare Protokolle wie SMB und NFS zu vermeiden.«

Datensichtbarkeit: alles im Überblick

Die Datensichtbarkeit bezieht sich auf die Fähigkeit eines Unternehmens, jederzeit den Überblick über seine Daten zu haben. Die Herausforderung besteht darin, zum Teil enorme Volumen und eine Vielzahl von Datenquellen zu verwalten. Es kann daher schwierig sein, den Überblick über die Daten zu behalten, die im Unternehmen vorhanden sind, wo sie sich befinden und wer darauf zugreift.

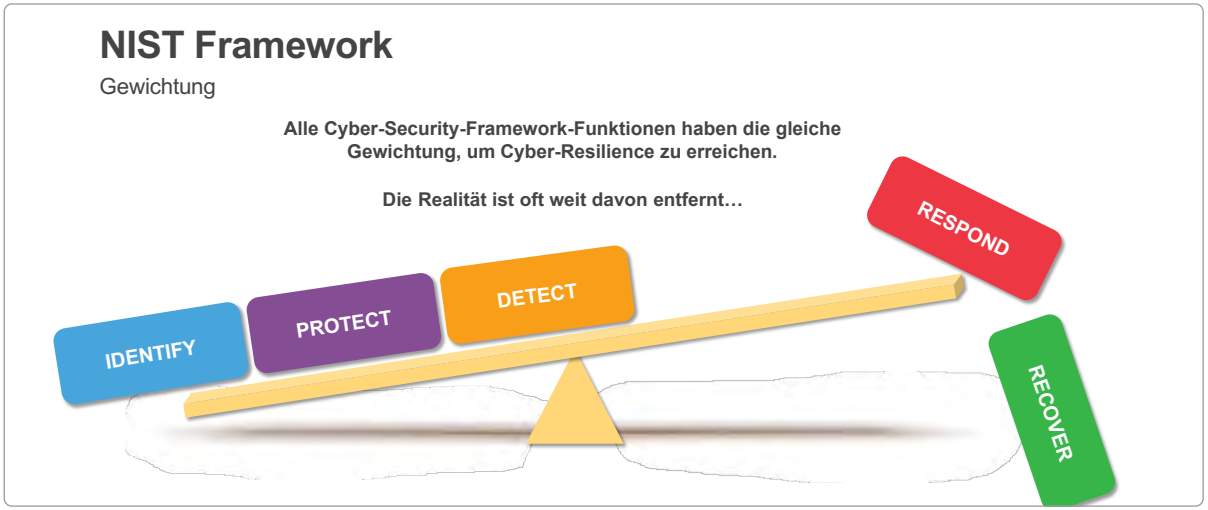
Um **Datensichtbarkeit** in Unternehmen zu erreichen, empfiehlt das NIST einen Rahmen, der sich aus fünf Kernkomponenten zusammensetzt:

1. **Identifizierung**: Identifizierung aller Datenquellen im Unternehmen und Kategorisierung der Daten nach Sensitivität und Kritikalität.
2. **Schutz**: Implementierung von Sicherheitsmaßnahmen zur Vermeidung von Datenlecks und unbefugtem Zugriff auf Daten.
3. **Erkennung**: Implementierung von Maßnahmen zur schnellen Erkennung von Datenlecks und unbefugtem Zugriff auf Daten.
4. **Reaktion**: Implementierung von Maßnahmen zur schnellen Reaktion auf Datenlecks und unbefugtem Zugriff auf Daten.
5. **Wiederherstellung**: Implementierung von Maßnahmen zur Wiederherstellung von Daten und Systemen nach einem Datenleck oder unbefugtem Zugriff auf Daten im Unternehmen.

NIST: Leitfaden für IT-Sicherheit & Datenschutz

Der NIST-Standard (National Institute of Standards and Technology) bietet Unternehmen bewährte Verfahren und Richtlinien, um ihre IT-Sicherheit zu verbessern und ihre Daten vor Bedrohungen zu schützen. Er ist international anerkannt und unterstützt Firmen in verschiedenen Branchen und Größenordnungen dabei, ihre Compliance-Anforderungen zu erfüllen. Eine strukturierte Methodik soll bei der Planung, Umsetzung und Überwachung helfen.

Entwickelt wurde das Rahmenwerk von der US-Regierung. Es enthält eine umfassende Sammlung von Best-Practices, Richtlinien und Empfehlungen. Der NIST-Standard gliedert sich in verschiedene Kategorien, wie zum Beispiel Risikomanagement, Identitäts- und Zugriffsverwaltung, Datenverschlüsselung und Datenwiederherstellung. Er bietet Unternehmen einen strukturierten Ansatz zur Implementierung von Sicherheitsmaßnahmen. **www.nist.gov/**



Für eine ausreichende Widerstandsfähigkeit gegen Angriffe sollten alle Cyber-Security-Framework-Funktionen gleich gewichtet sein: Respond und Recover werden jedoch meist vernachlässigt.

Grafik: Rubrik

Technische Maßnahmen können beispielsweise Zugriffskontrollen, Verschlüsselung und Überwachung von Netzwerkverkehr umfassen. Zu den organisatorische Maßnahmen gehören unter anderem Schulungen für Mitarbeiter, regelmäßige Überprüfungen der Sicherheitsmaßnahmen und Notfallpläne.

Datenwiederherstellung: schnelles Recovery

Die **Datenwiederherstellung** bezieht sich auf die Fähigkeit eines Unternehmens, nach einem Systemausfall oder einer Datenpanne seine Daten schnell und vollständig wiederherzustellen. Auch hier spricht das NIST Empfehlungen aus, die sich aus vier Kernkomponenten zusammensetzen:

1. **Planung**: Entwicklung eines Wiederherstellungsplans, der Maßnahmen und Verfahren zur Wiederherstellung von Daten und Systemen nach einem Ausfall oder einer Datenpanne umfasst.
2. **Umsetzung**: Implementierung des Wiederherstellungsplans durch regelmäßige Schulungen und Übungen, um sicherzustellen, dass das Personal in der Lage ist, im Ernstfall schnell und effektiv zu handeln.
3. **Überprüfung**: Regelmäßige Überprüfung und Aktualisierung des Wiederherstellungsplans, um sicherzustellen, dass er den aktuellen Bedürfnissen des Unternehmens entspricht.
4. **Verbesserung**: Identifizierung von Verbesserungsmöglichkeiten und Aktualisierung des Wiederherstellungsplans, um sicherzustellen, dass er kontinuierlich den Bedürfnissen des Unternehmens entspricht.

»Nur richtig vorbereitet lässt sich sicherstellen, dass schnell und effektiv auf Datenpannen oder Systemausfälle reagiert werden kann«, mahnt Rubrik-Manager Schwaak. »Wir empfehlen Wiederherstellungsszenarien realitätsnah nachzustellen, und zwar so lange, bis die Reaktion auf Notfälle automatisch abläuft.«

Backup und Recovery ist nicht gleichzusetzen mit Cyber-Recovery. Es ist etwas anderes, sich gegen technische Defekte zu erwehren bzw. einzelne Datensätze wiederherzustellen, als unter Hochdruck einen Cyberangriff einzudämmen. Zum Schutz der Daten ist ein echtes Air-Gap unerlässlich. »Wir setzen hier auf ein unveränderbares Dateisystem für die Backups mit logischem Air-Gap, damit die Angreifer nicht die *Last Line of Defense* zerstören können«, sagt Schwaak. »Zur Vorbereitung gehört zudem eine Anomalie-Erkennung (kann auf Verschlüsselung hindeuten), Pro-Active Threat-Hunts, um den Blast-Radius festzustellen und zu erkennen, welche Daten genau zu restaurieren sind, sowie ein sensitives Data-Discovery, um einen Angriff DSGVO/NIS2-konform anzuzeigen.«

Für das Unternehmen sind im Schadensfall eine detaillierte Vorbereitung und eingespielte Abläufe bares Geld. Cyber-Notfallübungen sind mindestens genauso wichtig, wie die jährliche Brandschutzübung. ■

Bild: shutterstock/Wolfilser

Karl Fröhlich
speicherguide.de

Finanzielle Auswirkungen von Ransomware

FOLGEKOSTEN UND KOLLATERALSCHADEN

Ein erfolgreicher Ransomware-Angriff belastet Unternehmen schwer, vor allem finanziell. Die zu erwartenden Kosten gehen weit über die Höhe des geforderten Lösegelds hinaus. Neben der Downtime und dem mögliche Datenverlust muss mit Ausgaben für technischen und rechtlichen Beistand kalkuliert werden. Zudem werden die erbeuteten Daten zum Kauf angeboten.

Ein Ransomware-Angriff ist nicht nur lästig, sondern vor allem teuer. Für die betroffenen Unternehmen geht es bei den finanziellen Folgen nicht um die Höhe des Lösegelds selbst oder darum, ob sie die Erpressung bezahlen sollten oder nicht. Die schwerwiegendste finanzielle Belastung durch einen Ransomware-Angriff sind der Kollateralschaden und die damit verbundenen Folgekosten.

In punkto Lösegeld sind sich die Experten einig: »nicht bezahlen«. Letztendlich gibt es keine Garantie, dass die Erpresser tatsächlich den Entschlüsselungscode herausgeben. Allerdings, und auch da sind sich die Experten einig, handelt es sich bei den Erpressern mittlerweile um bestens aufgestellte Organisationen, mit eigenen Support, der betroffene Unternehmen zum Teil beim Entschlüsseln unterstützt. Es würde sich schnell herumsprechen, wenn Lösegeldzahlungen nutzlos wären.

Womit zu rechnen ist, sind beschädigte Dateien und Datensätze. Eine Datenbank, die im laufenden Betrieb verschlüsselt wird, ist meistens korrupt und muss wieder repariert werden. Es gilt, einen Datenverlust so weit wie möglich zu vermeiden, die Wiederherstellung kostet auf jeden Fall Zeit und Geld. So lange die Systeme bzw. Daten ausfallen, steht der gesamte Betrieb. Das Unternehmen kann seine Kunden nicht oder nicht in vollen Umfang bedienen, keine Produkte verkaufen oder produzieren.

Folgekosten einer Ransomware-Attacke

- Betriebliche Ausfälle in der Firmenzentrale, in Filialen und Niederlassungen
- Produktions- und Umsatzeinbußen
- Interne Personalkosten durch Überstunden
- Kosten für externe Experten und forensische Untersuchungen
- Verlust von Kunden
- Langfristiger Reputationsschaden
- Anwalts-/Rechtshilfekosten
- Behördliche Geldbußen
- Schadenersatzforderungen von Kunden und Betroffenen bei Datenschutzverletzungen

Mögliche Bußgelder wegen Datenschutzverletzung

Sollten den Erpressern personenbezogene Daten in die Hände fallen, muss das betroffene Unternehmen binnen 72 Stunden die zuständigen Aufsichtsbehörden informieren. In einigen Branchen kann eine Datenschutzverletzung oder ein Datenverlust zu Geldstrafen führen. Gleichzeitig können Kunden eine Entschädigung fordern. Summen, die sich möglicherweise schnell aufaddieren. Sollten aufgrund des Ransomware-Angriffs beispielsweise Kreditkarteninstitute gezwungen sein, den Kunden neue Karten auszustellen, werden diese sicherlich dem betroffenen Unternehmen in Rechnung gestellt.

Grafik: speicherguide.de/B4Restore

Die finanzielle Auswirkungen eines Ransomware-Angriffs summieren sich schnell.

Betroffene Firmen müssen herausfinden, wie sich die Cyberkriminellen Zugang zu den Daten verschafft haben. Hierzu werden in der Regel externe Sicherheitsexperten hinzugezogen, die ebenfalls bezahlt werden möchten. Neben den Kosten ist mit einem Reputationsverlust zu rechnen, gegenüber Kunden, den eigenen Mitarbeitern, Investoren und Stakeholdern.

Doch selbst wenn das Problem gelöst und die Einfallstore geschlossen wurden, besteht immer noch das Risiko, dass Anmeldeinformationen gestohlen wurden oder andere Sicherheitsmaßnahmen durchgesickert sind. Die Erfahrung zeigt, dass selbst nach einer Lösegeldzahlung die Schwachstellen und der Angriffsweg im Darkweb angeboten werden. Dies führt dazu, dass die Informationen für andere Arten von Angriffen oder für einen künftigen Ransomware-Angriff genutzt werden.

Mögliches Verlustpotenzial vorher identifizieren

Wichtig ist, dass sich die Geschäftsleitung vorher – in der »Friedenszeit

vor einem Angriff« einen Überblick über mögliche Kosten verschafft:

- Welche Abteilungen sind von einem Ausfall der IT betroffen?
- Wie hoch ist der Umsatzverlust pro Stunde und Tag?
- Inwieweit können Außenstellen und Filialen ohne IT arbeiten?
- Sollen Filialen geöffnet werden?

Auch wenn alle dazu raten, kein Lösegeld zu bezahlen, eventuell ist dies zwar schmerzhaft aber die preiswerteste Lösung. Geschäftsführer, die ihre Zahlen kennen, können im Angriffsfall schneller Entscheidungen treffen. Mit der Lösegeldzahlung erkauft man sich Zeit. Sofern die Daten entschlüsselt werden, verkürzt es die Dauer des Ausfall.

Jedes fünfte Unternehmen stand 2022 nach einem Cyberangriff am Rande der Insolvenz. Getroffen hat es beispielsweise den deutschen Fahrrad-Hersteller *Prophete*. Die Liste betroffener Firmen ist lang und reicht von kleinen Familienunternehmen bis hin zu Großkonzernen

Einer Studie des Branchenverbands **Bitkom** zufolge, müssen deutsche Unternehmen im Durchschnitt fast 150.000 Euro für die Bewältigung eines Ransomware-Angriffs ausgeben. Aufgrund der begrenzten Ressourcen und Fähigkeiten zur Bekämpfung von Cyberangriffen fallen die Kosten in mittelständischen Unternehmen eher noch höher aus. ■

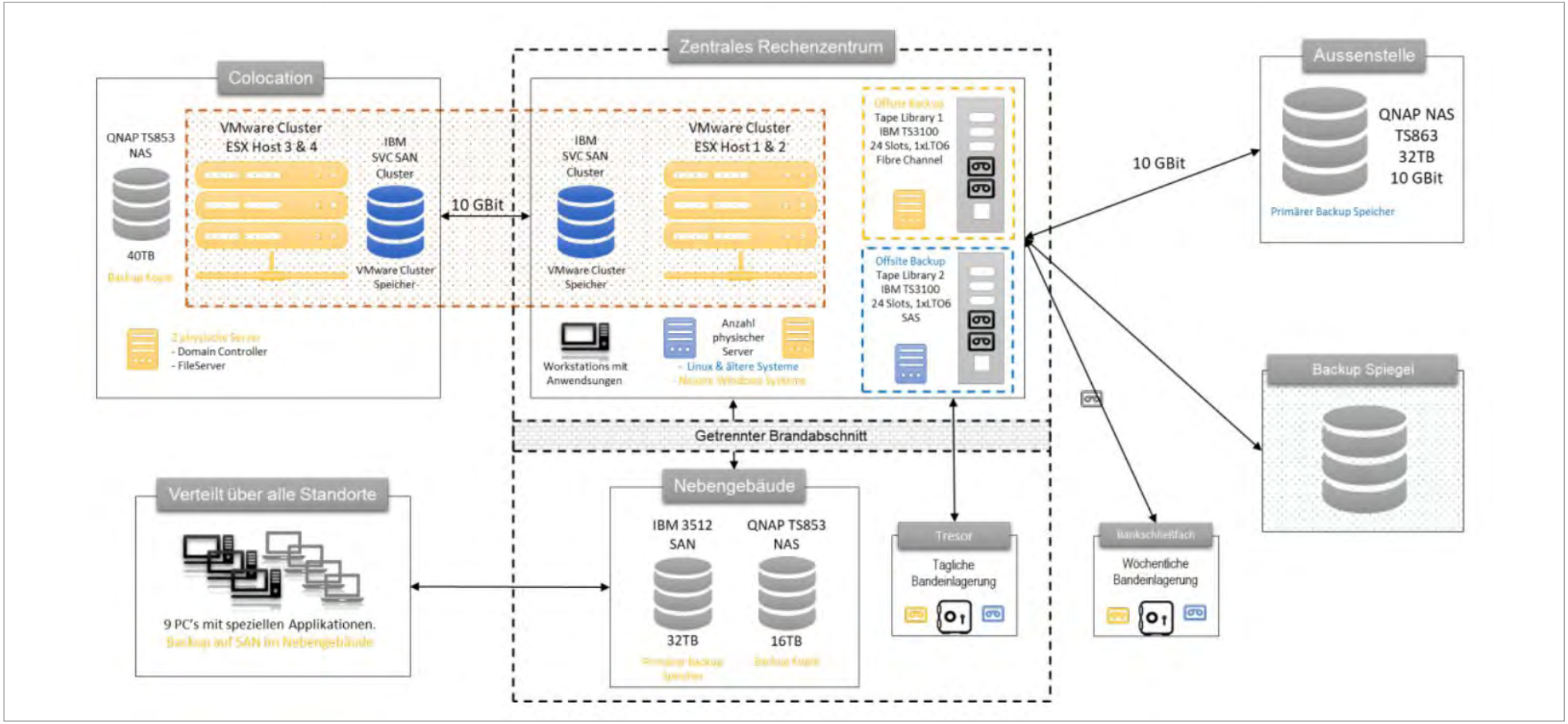
Foto: schutterstock.com / Panchenko Vladimir

Peter Marwan
speicherguide.de

Im Ernstfall helfen nur vorab definierte Prozesse

JEDES UNTERNEHMEN BRAUCHT EINEN IT-NOTFALLPLAN

Bei einer IT-Störungen im Unternehmen entscheidet eine schnelle und richtige Reaktion über das Ausmaß des Schadens. Ein IT-Notfallhandbuch bietet die erforderliche Orientierung. Tritt der Ernstfall ein, bleibt meist keine Zeit, sich zu überlegen, was nun zu tun sei. Hier bekommen Sie Hinweise, was im IT-Notfallhandbuch Ihres Unternehmens enthalten sein muss.



Grafik: Novastor

Ein Backup-Konzept dokumentiert die aktuelle Infrastruktur und sollte Teil eines IT-Notfallhandbuchs sein.

Das bekannteste Notfallhandbuch ist wahrscheinlich »The Hitchhiker's Guide to the Galaxy«. Ganz wichtig auf dem Einband sind die beruhigenden Worte »Don't Panic«. Im Inneren finden sich umfangreiche Hinweise und Handlungsempfehlungen für alle möglichen Ereignisse bei Reisen »per Anhalter durch die Galaxis«. Den Leser bewahren sie aber nicht davor, immer wieder in neue Schwierigkeiten zu geraten – wie jeder weiß, der das Buch gelesen oder den Film gesehen hat. An ein IT-Notfallhandbuch hat man andere Erwartungen: Es soll dazu beitragen, dass bei einer Störung des IT-Betriebs alle Personen im Unternehmen richtig reagieren und genau wissen, was zu tun ist. Das IT-Notfallhandbuch ist somit eine taktische Maßnahme und unterstützt strategische Bemühungen um Business-Continuity-Management und Cyber-Resilienz. Beides sind nicht nur modische Schlagworte, sondern Ausdruck der Tatsache, dass Firmen immer stärker von funktionierender IT abhängig sind.

Die Aufgabe des IT-Notfallmanagements

IT-Notfallmanagement ist Teil eines Business-Continuity-Management-Systems (BCMS). Dessen Aufgabe ist es, die Ausfallsicherheit der Geschäftsprozesse zu erhöhen und die

Voraussetzungen dafür zu schaffen, in einer Krise schnell, zielgerichtet und angemessen zu reagieren. Es soll also sowohl die Widerstandsfähigkeit (Resilienz) des Unternehmens erhöhen, als auch dafür sorgen, dass die Geschäftstätigkeit nach einem Ausfall so schnell wie möglich wieder aufgenommen werden kann.

Die Verfügbarkeit von IT ist dazu ein entscheidender Baustein. Wichtige Normen in dem Umfeld sind ISO 22.301 (Business Continuity), ISO 27.031 (IT-Service-Continuity-Management / ITSCM) und der BSI-Standard 100-4 (Notfallmanagement). Das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) erarbeitet mit dem BSI-Standard 200-4 (Business-Continuity-Management) derzeit zudem eine weiteres Dokument, dass bei der strukturierten Planung von Notfallmanagement und Disaster-Recovery helfen kann.

Ohne Risikoanalyse kein IT-Notfallmanagement

Ein IT-Notfall kann viele Ursachen haben. Erfolgreiche Cyberangriffe, etwa mittels Ransomware, sind nur eine davon. Auch technische Probleme, Naturkatastrophen, Stromausfall oder ein Brand im Unternehmen gehören dazu. Mit der Nutzung externer Ressourcen bei Cloud- und SaaS-Anbietern können dieselben Ursachen auch dort zu einem Notfall für das eigene Unternehmen führen. Denn in der Regel sagen Cloud-Dienstleister nur die Verfügbarkeit ihrer Dienste und Services zu. Sicherung und Wiederherstellung der Daten liegen dagegen in der Verantwortung der Nutzer. Notfallkonzepte und dementsprechend auch das Notfallhandbuch müssen also auch diesen Bereich abdecken. IT-Risiken zu definieren, ist eine wichtige Voraussetzung für ein gutes IT-Notfallhandbuch.

Denn im Notfall lassen sich Prioritäten nur dann sauber festlegen, wenn bekannt ist, welche Auswirkungen einzelne Aspekte auf den Betrieb haben. Dazu wird in einer Risikoanalyse ermittelt, welche Geschäftsprozesse unverzichtbar sind und welche Ressourcen dafür benötigt werden.

Als Grundlage für das Risikomanagement bietet sich unter anderem der BSI-Standard 200 – 3 als Orientierungshilfe an. Für kleine und mittelgroße Unternehmen hat der Bitkom **einen Leitfaden zum IT-Risikomanagement** erstellt, der kostenlos als PDF zum Download bereitsteht. Einen guten Einstieg und hilfreiche Anregungen auch für kleinere Firmen bietet zudem das von der *Allianz für Cyber-Sicherheit für Unternehmensvorstände und Aufsichtsräte* angebotene **Handbuch zum Management von Cyber-Risiken.**

Grafik: BSI

Die IT-Notfallkarte des BSI bietet eine erste Orientierung.

Richtige Alarmierung ist der erste Schritt

Bei einem IT-Notfall ist schnelles und zielgerichtetes Handeln gefragt. Erster Schritt dazu ist die richtige Reaktion aller Beteiligten – auch derjenigen, die nicht zur IT-Abteilung gehören. Dafür hat das BSI die IT-Notfallkarte erarbeitet. Ähnlich wie das bekannte Hinweisschild »Verhalten im Brandfall« führt sie kurz auf, was im IT-Notfall zu tun ist.

Die IT-Notfallkarte gibt knapp und übersichtlich Informationen dazu, wer auf welchem Wege zu alarmieren ist, welche Bedeutung die Weitergabe wichtiger Informationen zu IT-Notfällen hat und warnt vor womöglich kontraproduktiven, eigenmächtigen Maßnahmen. Hinweise zur Verwendung der IT-Notfallkarte und den Nutzungsbedingungen finden sich auf der **Webseite des BSI.**

Arten von IT-Notfallplänen

In einem IT-Notfallplan ist detailliert festgehalten, wie bei einem Störfall weiterhin auf wichtige Systeme zugegriffen, die Informationssicherheit aufrechterhalten und der Betrieb schnell und effektiv wiederhergestellt wird. Viele wünschen sich dafür eine konkrete Anleitung, am besten als PDF zum Download. Das ist jedoch der falsche Ansatz. Ein gutes IT-Notfallhandbuch muss die individuellen Unternehmensstrukturen berücksichtigen. Manche Unternehmen sind zum Beispiel ohne E-Mail-Zugriff handlungsunfähig. Andere können mehrere Stunden darauf verzichten – nicht dagegen auf ihren Webshop, ihre Call-Center-Anwendung oder eine branchenspezifische Software. Außerdem unterscheiden sich Zuständigkeiten und Informationswege in allen Unternehmen.

Generell gibt es mehrere Ansätze, ein IT-Notfallhandbuch aufzubauen. Welcher gewählt wird, ist teilweise Ansichtssache, teilweise durch die Strukturen im Unternehmen bedingt. Die Einteilung nach Prozessen scheint aus Sicht von Business-Continuity-Management sinnvoll, wo es um die Verfügbarkeit von Geschäftsprozessen geht. In der Praxis können prozessübergreifende oder nicht den ganzen Prozess erfassende Zuständigkeiten jedoch zu Schwierigkeiten führen.

Die Gliederung nach Phasen setzt das Verständnis der Mitarbeiter dafür voraus, in welcher Notfallphase sie sich gerade befinden, um richtig handeln zu können. Möglich ist auch eine Unterteilung des IT-Notfallhandbuchs nach Ebenen der Verantwortlichkeit. Vorteil dabei: Jede Ebene (Mitarbeiter, Führungskräfte, Support und IT-Mitarbeiter) kann Informationen in der für sie verständlichen und erforderlichen Detailtiefe erhalten. Nachteil: An Schnitt-

stellen drohen Informationsdefizite. Auf jeden Fall zu empfehlen ist ein modularer Aufbau: Niemand liest das Handbuch in einem Notfall in aller Ruhe von vorne nach hinten durch. Bewährt hat sich ein zweigliedriger Aufbau: Der erste Teil bietet allgemeine Informationen wie Begriffsdefinitionen, Zuständigkeiten, Kontaktmöglichkeiten und Meldeketten. Der zweite Teil behandelt konkrete Schadensereignisse – und verweist gegebenenfalls auf die relevanten Stellen im ersten Teil.

Ganz wichtig ist, das IT-Notfallhandbuch regelmäßig und zentral zu pflegen: Veraltete Informationen sind fast noch schlimmer als fehlende Informationen, gaukeln sie doch eine trügerische Sicherheit vor. Mindestens ebenso wichtig ist, zumindest gelegentlich stichprobenartige Notfallübungen durchzuführen. Durch sie zeigt sich schnell, ob die im Notfallplan angebotenen Informationen verständlich sind und die Reaktionen planmäßig verlaufen – oder ob Nachbesserungen erforderlich sind. Einen guten Einstieg in die Entwicklung des eigenen IT-Notfallhandbuchs bietet der **Maßnahmenkatalog zum Notfallmanagement des BSI.**

Die wichtigsten Punkte eines IT-Notfallplans

IT-Notfallhandbücher müssen die individuellen Bedürfnisse des Unternehmens berücksichtigen. Einige Aspekte sollten jedoch immer enthalten sein. Dazu gehören:

- **Sofortmaßnahmen:** Darunter fallen einerseits Maßnahmen zur Rettung oder Evakuierung von Personen zum Beispiel bei Brand oder Wassereinbruch im Rechenzentrum, andererseits aber auch klassische IT-Maßnahmen, etwa die Trennung vom Netz oder zumindest Netzsegmenten bei einem erkannten Angriff, um ihn einzudämmen.
- **Notfallkommunikation:** Klare und verständliche Kommunikation ist im Notfall Trumpf. Dazu muss geregelt sein, wer wen in welcher Form informieren muss – aber auch, was vielleicht nicht gesagt werden darf, etwa in der Kommunikation mit Kunden und Lieferanten. Je nach Situation ist in diesem Teil auch festgelegt, wie Öffentlichkeit und Medien sowie wie und wann Datenschutz- und andere Aufsichtsbehörden zu informieren sind.
- **Leitfaden für den Krisenstab:** Unvorhergesehene Notfälle lassen sich am besten durch ein zuvor festgelegtes Team mit allen relevanten Experten meistern. Widersprüchliche Anordnungen lassen sich vermeiden, Lagebeurteilungen schneller abgeben, wenn mögliche Optionen bereits vor dem Notfall übersichtlich zusammengefasst wurden. Auch abzuarbeitende Aufgaben, die dazu erforderlichen Rechte und die richtigen Ansprechpartner sollten hier vermerkt sein.
- **Business-Continuity-Pläne:** Als Ergebnis der Risikoanalyse ist bekannt, welche Geschäftsprozesse welche Ausfallzeiten verkraften. Daraus leitet sich die Priorisierung der Maßnahmen zur Wiederherstellung des Normalbetriebs ab. Gleichzeitig ist dadurch klar, für welche Bereiche der – hoffentlich vorher geplante – Notbetrieb aufzunehmen ist, um die Zeit bis zum Normalbetrieb zu überbrücken.
- **Rückkehr zum Normalbetrieb:** Hat sich die Lage stabilisiert, ist es meist noch ein weiter Weg bis zum Normalbetrieb. Nach einem Cyberangriff steht oft eine forensische Analyse an, bei Brand und anderen physischen Ursachen der Ersatz oder die Neuanschaffung von Hardware. Außerdem ist zu prüfen, ob durch die Unterbrechung Daten verloren gingen.

Dabei hilft ein vorher erarbeitetes Backup-Konzept. Es dokumentiert die jeweils aktuelle Backup-Infrastruktur mit sämtlichen Systemen und Datenmengen.

Ein Backup-Konzept stellt zudem sicher, dass alle Ausfall-Szenarien abgedeckt sind, die relevanten Business-Anforderungen und gesetzlichen Vorgaben erfüllt werden und die Backup-Infrastruktur bestmöglich geschützt ist. ■

Einfache aber effektive Backup-Strategie plus Unveränderlichkeit

UNERSETZLICH: DIE 3-2-1-(1-)BACKUP-REGEL

Der Daten-Gau lauert immer und überall und betrifft geschäftliche wie auch private Daten gleichermaßen. Vor Hardware-Defekten, amoklaufenden Programmen und Benutzerfehlern ist keiner gefeit. Außerdem dürfen Feuer- und Wasserschäden sowie neuzeitliche Bedrohungen wie Cyber- und Ransomware-Attacken nicht außer Acht gelassen werden. Um sich vor Datenverlust zu schützen, ist die 3-2-1-(1-)Backup-Regel daher unersetzlich.

Karl Fröhlich
speicherguide.de

Egal für welche Backup-Strategie man sich entscheidet, die 3-2-1-Backup-Regel gilt als kleinster gemeinsamer Nenner, den es zu erfüllen gilt. Das heißt, drei Kopien der Daten, gespeichert auf zwei unterschiedlichen Speichermedien (Medienbruch) und mindestens einer Offsite-Kopie. Im Detail kommt es natürlich auf die Art und Menge der Daten an und welche Technologien vorwiegend zum Einsatz kommen. Hat dies früher ausgereicht, empfiehlt sich in Zeiten von Cyberattacken eine zusätzliche unveränderliche Kopie (Offline/Immutable).

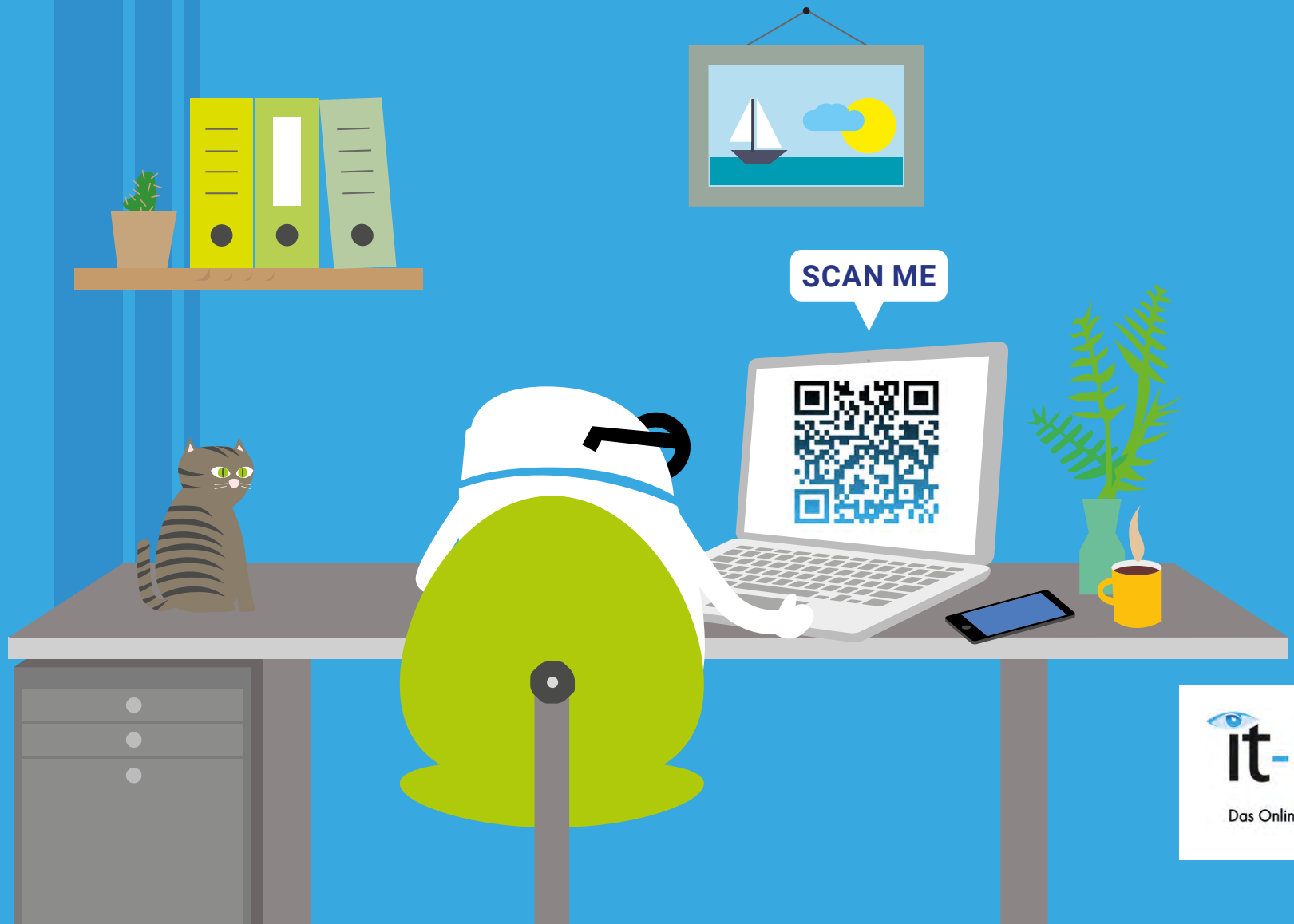
Unabhängig von der IT-Umgebung, gehören unternehmenskritische Daten so gut es geht geschützt. Wobei dies natürlich auch für die Daten von Einzelpersonen gilt. Je mehr Kopien von einem Datensatz vorhanden sind, desto größer ist der Schutz vor Datenverlust. Risikofaktor Nummer eins ist ein möglicher Hardware-Defekt. Speichermedien jeglicher Art wie Festplatten, Disk-Arrays, SSDs, Speicherkarten, aber auch der interne Speicher von Smartphones und Tablets, sind als mechanische und/oder elektronische Bauteile nicht vor einem Ausfall gefeit. Ohne Kopie sind die Daten unweigerlich verloren. Datenrettungsdienste erreichen heutzutage durchaus kleine Wunder, verlassen kann man sich darauf aber nicht. Zudem ist Datenrettung ein mitunter kostspieliger Service. Je nach Art und Beschädigungsgrad des Mediums beginnen die zu kalkulierenden Einstiegskosten im vierstelligen Bereich. Zudem müssen Betroffene Zeit mitbringen. Die Wiederherstellungszeit bemisst sich in der Regel in Wochen. Für eine größtmögliche Sicherheit sollten für die Datenkopien zwei unterschiedliche Speichertechnologien genutzt werden. Man spricht hier vom sogenannten Medienbruch. Dies soll die Ausfallwahrscheinlichkeit verringern und für eine Risikoverteilung bei systembedingten Fehlern sorgen und vor Ransomware-Attacken schützen. Jede Internet-Anbindung ist ein potentielles Einfallstor für Cyberangriffe.

Grafik: speicherguide.de

Daher sollte sich eine ausgelagerte Kopie zudem an einem anderen geographischen Standort befinden. Alle vorangegangen Bemühungen bringen nichts, wenn Originaldaten und Backups am gleichen Ort beispielsweise einem Brand oder Wasserschaden zum Opfer fallen. Auch ein Diebstahl lässt sich nie ganz ausschließen.

Speziell als Rückversicherung gegen Verschlüsselungsattacken ist die 3-2-1-Backup-Regel aktueller denn je bzw. nun als 3-2-1-1 mit einer Offline-Kopie. ■

it-daily.net mehr als nur tägliche IT-News!



it-daily.net

Das Online-Portal von itmanagement & itsecurity

Newsletter-Abonnenten erhalten die neue Ausgabe jeweils »linkfrisch« an ihren Mail-Account. Registrieren Sie sich bitte hier. Beachten Sie auch unser Archiv im Download-Bereich.

storage-magazin.de
eine Publikation von speicherguide.de
Karl Fröhlich
Ginsterweg 12, 81377 München
Tel. +49 (0) 89-740 03 99
E-Mail: redaktion@speicherguide.de

Chefredaktion, Konzept:
Karl Fröhlich *(verantwortlich für den redaktionellen Inhalt)*
Tel. 089-740 03 99
E-Mail: redaktion@speicherguide.de

Redaktion:
Michael Baumann, Karl Fröhlich, Peter Marwan

Schlussredaktion:
Peter Marwan, Brigitte Scholz

Titelbild:
shutterstock/wk1003mike

Layout/Grafik:
Uwe Klenner, Layout und Gestaltung,
Rittsteiger Str. 104, 94036 Passau,
Tel. 08 51-9 86 24 15
www.layout-und-gestaltung.de

Mediaberatung:
Kerstin Fraenzke
Head of Media Consulting
Tel: 08104 / 6494-19
E-Mail: fraenzke@it-verlag.de

Karen Reetz
Media Consulting
Tel: 08121 / 977594
E-Mail: reetz@it-verlag.de

Webkonzeption und Technik:
IT Verlag GmbH
Ludwig-Ganghofer-Str. 51
Otterfing 83624
E-Mail: webmaster@speicherguide.de

Unser Team

Karl Fröhlich
Chefredakteur
speicherguide.de

Michael Baumann
Redaktion
speicherguide.de

Peter Marwan
Redaktion
speicherguide.de

storage-magazin.de powered by it-daily.net

Eine Publikation von **speicherguide.de**