arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Backup dient auch dem Schutz vor internen Gefahren

Es besteht kein Zweifel daran, dass Cyberbedrohungen zu einem der größten Risiken für Unternehmen avanciert sind. Doch wie verhält es sich mit den internen Gefahren und hausgemachten Risiken für Daten und Systeme, denen Unternehmen heute nicht weniger als früher gegenüberstehen? Fakt ist, dass die internen Gefahren durch Mitarbeiter, Spionage oder schlichtes Fehlverhalten nach wie vor existent sind und dass Unternehmen diese neben den Cyberrisiken nicht außer Acht lassen sollten. Im „Verizon Data Breach Investigations Report (DBIR) 2023" beispielsweise wurde festgestellt, dass immerhin 19 Prozent der Sicherheitsverletzungen auf interne Akteure zurückzuführen sind. Auch das BSI zählt die internen Risiken zu den wichtigen Gefahrenquellen und rät zu einer sorgfältigen Analyse, um einen Ausfall von Geschäftsprozessen möglichst zu verhindern.

Gefahr aus den eigenen Reihen

Wichtige, unternehmenskritische Daten können sehr leicht absichtlich oder versehentlich kompromittiert oder zerstört werden, wie eines der jüngsten Beispiele bei einem Unternehmen, das Informations- und Kommunikationstechnologie anbietet, zeigt. Im Juni 2024 wurde ein Fall bekannt, bei dem sich ein enttäuschter Mitarbeiter aufgrund einer Kündigung am ehemaligen Arbeitgeber rächen wollte. Aus Frust hatte der Mitarbeiter 180 virtuelle Server im Testsystem seines Ex-Arbeitgebers gelöscht und damit einen Schaden von über 620.000 Euro verursacht; der ehemalige Mitarbeiter hatte nach wie vor Admin-Zugang zu den Systemen, auch nachdem ihm gekündigt worden war. Dieses Beispiel zeigt, wie fragil und anfällig die IT-Systeme sind, wenn Unternehmen nicht die nötigen Schutzmaßnahmen treffen und das Prinzip der geringstmöglichen Rechte strikt befolgen. Allerdings müssen Schäden durch interne Akteure nicht zwangsweise aufgrund einer bösartigen Motivation entstehen. Denkbar sind ebenso Fehler

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

der Administratoren oder der Anwender. Zu viele Rechte, ein falscher Klick und schon kann es passieren, dass unternehmenskritische Daten und Systeme unwiderruflich gelöscht sind.

Nach dem Desaster kommt das Recovery

Je nach Unternehmensgröße sind die Kosten derartiger Vorfälle vielleicht nicht das größte Problem. Viel wichtiger ist es, Daten und Systeme schnell wiederherzustellen, und zwar möglichst in dem Zustand, in dem sie sich kurz vor der Kompromittierung oder Löschung befunden haben. An dieser Stelle hilft eine gute und vor allem erprobte Backup- und Disaster-Recovery-Strategie. Und es helfen Datensicherungssätze, die weder manipuliert noch gelöscht werden können. Für das zuvor genannte Beispiel hieße das, dass die Backups der Testsysteme möglichst kurz vor der Löschung angefertigt werden und dass diese auf einem nicht löschbaren und unveränderlichen Speicher liegen. Erst dann ist garantiert, dass die Daten und Testsysteme in Gänze wiederhergestellt werden können und dass dem Unternehmen wenig Produktivzeit verloren geht oder gar Testresultate von Monaten und Jahren abhandenkommen.

In diesen Fällen sind Backup-Lösungen nötig, die durch eine orchestrierte Wiederherstellung die Wiederherstellungszeiten und -punkte (RTOs / RPOs) auf Minuten reduzieren und die gewünschten Service Level Agreements (SLAs) mit Assured Recovery validieren. Um dies zu erreichen, eignet sich eine einheitliche Plattform für die Datensicherung, wie beispielsweise Arcserve UDP. Mit einer integrierten Plattform erhalten Unternehmen eine umfassende Lösung, die Backup, Disaster Recovery sowie das Datenmanagement übergreifend vereint. Derartige Lösungen sind auch in der Lage, Auswirkungen von Datenkompromittierung oder gar -zerstörung effizient vorzubeugen – unabhängig davon, ob dies durch eine externe Cyberattacke, durch interne Akteure oder durch einen Bedienungsfehler

arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

hervorgerufen wird. Maßgeblich ist die Umsetzung und das regelmäßige Testen der 3-2-1-1-Regel für Backups. Diese geht von insgesamt drei Kopien der Backupdaten aus, wobei zwei Backups auf zwei unterschiedlichen Medienträgern und eine extern gespeichert werden soll. Die letzte 1 steht für die Speicherung einer Kopie auf einem unveränderlichen Speichermedium. Unveränderliche Backups werden in einem einmalig beschreibbaren und mehrfach lesbaren Format gesichert, das weder geändert noch gelöscht werden kann - auch nicht von Hackern, internen Akteuren oder Administratoren. Unternehmen, welche diese Regel mit einer dafür geeigneten Backup- und Disaster-Recovery-Lösung kombinieren, können im Ernstfall auf eine gesicherte Wiederherstellung aller Daten und Systeme bauen.

Folgen Sie Arcserve auf LinkedIn oder X und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Über Arcserve
Arcserve ist der Pionier für einheitliche Daten-Resilienz-Lösungen. Seit mehr als 40 Jahren vertrauen fast 150.000 Kunden und über 30.000 Vertriebspartner in 150 Ländern auf Arcserve, um ihre Datenresilienz zu stärken, verlorene Daten wiederherzustellen und die Kontinuität ihres Geschäftsbetriebs zu gewährleisten. Mit einem einheitlichen Ansatz für Datensicherung und -wiederherstellung, erstklassigem technischen Support und dem niedrigen Total Cost of Ownership (TCO) hilft Arcserve Unternehmen, ihre Daten zu verwalten, zu schützen und - was am wichtigsten ist - in jeder Situation wiederherzustellen.
Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf Twitter oder LinkedIn.

Unternehmenskontakt
Alex Plotnikov
Arcserve
alex.plotnikov@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 157 524 437 49
Thilo Christ
+49 171 622 06 10
arcserve@tc-communications.de