Mit diesen vier Schritten lassen sich die Gremlins von Unternehmensdaten fernhalten

Florian Malecki, Vice President, International Marketing, Arcserve

Halloween ist die Zeit gruseliger Monster und unheimlicher Ereignisse. Es ist auch die Zeit, in der man über die vielen Gremlins nachdenken sollte, die es auf die Daten ihres Unternehmens abgesehen haben.

Eine der fürchterlichsten Daten-Horrorgeschichte der letzten Zeit ist Pixar während der Produktion von „Toy Story 2“ passiert. Einer der Animatoren des Films gab versehentlich einen falschen Befehl ein und löschte damit 90 Prozent der Filmdateien. Schlimmer noch: Die Datensicherung hatte nicht funktioniert, weil der Speicherplatz auf der Festplatte nicht ausreichte. Für einen kurzen Moment sah es so aus, als ob fast die gesamte Produktion verloren wäre. Mit großem Aufwand gelang es dem Team schließlich, die Daten wiederherzustellen.

Fälle von Datenverlust sind inzwischen keine Seltenheit mehr, nicht zuletzt deshalb, weil hunderte von Millionen von Menschen rund um den Globus immer häufiger im Remote-Modus arbeiten. Die Verlagerung von Mitarbeitern, Computern und Daten aus einer zuverlässigen Büroumgebung in ein weniger sicheres Remote-Umfeld birgt eine Vielzahl von Risiken, sowohl hinsichtlich Datenverluste als auch menschlicher Fehler, technischer Pannen und Cyberangriffen.

Die im Folgenden beschriebenen vier Möglichkeiten zeigen, wie Unternehmen sicherstellen können, dass ihre Daten sicher und geschützt sind – an Halloween und darüber hinaus.

1. Niemals aufhören zu testen

Eine von Dimensional Research weltweit unter IT-Entscheidungsträgern durchgeführte Umfrage ergab, dass fast ein Viertel aller Unternehmen ihren Datenwiederherstellungsplan nicht testen bzw. keinen Datenwiederherstellungsplan haben. Es ist wichtig, Backups und die Fähigkeit zur Wiederherstellung für den Fall eines Datenverlusts regelmäßig zu testen. So wird sichergestellt, dass das Backup auch tatsächlich funktioniert und im Falle eines Notfalls, sei es ein Cyberangriff, eine Naturkatastrophe oder einen Systemausfall, die Daten wiederhergestellt werden

können. Unternehmen sollten es sich deshalb zur Gewohnheit machen, ihre Sicherungskopien regelmäßig zu testen, um zu gewährleisten, dass sie ihre Daten zuverlässig wiederherstellen können.

2. Auf Multi-Faktor-Authentifizierung setzen

Die Multi-Faktor-Authentifizierung (MFA) ist eine der wichtigsten Sicherheitsfunktionen zum Schutz von Unternehmensdaten. Da täglich Millionen von Passwörtern gestohlen werden, implementieren viele Unternehmen jetzt eine MFA, um eine zusätzliche Sicherheitsebene zu schaffen. Ein zweiter Authentifizierungsfaktor ist für den Schutz von Konten und die Sperrung von Daten unerlässlich. Laut jüngstem Verizon Data Breach Investigations Report ist MFA besonders wichtig, denn 61 Prozent aller Sicherheitsverletzungen sind auf gestohlene oder kompromittierte Anmeldedaten zurückzuführen.

Dadurch, dass Unternehmen von Ihren Mitarbeitern verlangen, für den Datenzugang mehr als nur ein Passwort einzugeben, erschweren sie es Kriminellen, sich als dieser Mitarbeiter auszugeben. Wenn ein Unternehmen MFA im Einsatz hat, reicht ein gestohlenes Kennwort allein dann nicht mehr aus, um Zugang zu erhalten. Damit ist die Hürde, die Cyberkriminelle überwinden müssen, bevor sie Datenzugriff bekommen, höher. Und Cyberkriminelle mögen keine Hürden. Sie lieben „low hanging fruits“.

3. Mitarbeiter ermutigen, ihre Daten zu sichern

Wenn Mitarbeiter im Remote-Modus arbeiten, sind sie oft nicht so wachsam wie im Büro. Sie verwenden ihre Heim-PCs und klicken auf Links, auf die sie vielleicht nicht klicken sollten. Dadurch sind ihre Daten einem größeren Risiko ausgesetzt. Noch schlimmer ist jedoch, dass dieses erhöhte Risiko auch auf Unternehmensdaten zutrifft. Deshalb ist es wichtig, Mitarbeiter zu ermutigen, verantwortungsbewusst zu handeln und Daten regelmäßig zu sichern.

Außerdem sollten Unternehmen die 3-2-1-1-Strategie zum Schutz der Daten anwenden. Die 3-2-1-1-Strategie sieht vor, dass drei Sicherungskopien der Daten auf zwei verschiedenen Medien (z. B. Festplatte und Band) erstellt werden und eine dieser Kopien für die Wiederherstellung im Katastrophenfall an einem anderen Ort aufbewahrt ist. Zu guter Letzt soll dann eine Kopie der Daten auf einem unveränderlichen Objektspeicher angelegt werden.

4. Datenschutz ist Chefsache
Unternehmen sollten die Implementierung einer Datenspeicherlösung in Betracht ziehen, die die Daten vor menschlichen Fehlern schützen kann, unabhängig davon, wo sie sich befinden – vor Ort, extern oder in der Cloud. Die effektivsten Lösungen können einzelne Dateien, Systeme oder auch ein ganzes Rechenzentrum in Minutenschnelle wiederherstellen und gleichzeitig gewährleisten, dass die Daten immer verfügbar sind, egal was passiert.

Mit Backup- und Recovery-Lösungen der nächsten Generation kann dieses Szenario leicht erreicht werden. Diese Lösungen bieten einen unveränderlichen Objektspeicher, der die Daten vor menschlichen Fehlern bewahrt, indem er in kurzfristigen Sekundenabständen eine Momentaufnahme der Daten erstellt. Da der Objektspeicher unveränderlich ist, kann er schnell wiederhergestellt werden, selbst wenn die Daten geändert werden.

Die Daten von Unternehmen müssen weder an Halloween noch zu einer anderen Jahreszeit Anlass zur Sorge sein. Mit den richtigen Strategien und Systemen können Datenverluste verhindert und die Gremlins in Schach gehalten werden.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de
www.tc-communications.de