Cyberresilienz: Kostspielige Ausfallrisiken minimieren

Auf Angriffe vorbereitet sein, rasch reagieren und Daten wiederherstellen

Der IDC-Report „State of Disaster Recovery and Data Protection Readiness: 2021“ zeigt deutlich die wachsende Gefahr von Ransomware und anderen Cyberbedrohungen, insbesondere das Risiko von Datenverlusten und empfindlichen Geschäftsunterbrechungen:

- **95 %** der befragten Unternehmen hatten in den letzten zwölf Monaten einen Angriff erlebt.
- **43 %** davon erlitten unwiederbringliche Datenverluste.
- **63 %** mussten aus Datengründen ihr Geschäft unterbrechen.

Cyberangriffe sind bittere Realität. Und jeden Tag kommen neue Varianten und technische Methoden hinzu, sodass die Attacken heftiger ausfallen und umfangreicher werden. Die klassischen Cybersicherheitsstrategien entwickeln sich nicht schnell genug und können uns in einer Geschäftswelt, die tägliche Verfügbarkeit rund um die Uhr erwartet, nicht mehr schützen.

Aus diesem Grund verlagern viele Unternehmen den Schwerpunkt ihrer Sicherheitsstrategien in Richtung Cyberresilienz. Sie konzentrieren sich nicht mehr auf die Netzwerkränder und deren Sicherung, sondern gehen dazu über, das Risiko für weltweit vernetzte, hybride Cloud-Umgebungen zu minimieren.

Unter Cyberresilienz versteht man die Vorbereitung und Reaktion auf Cyberangriffe sowie die Wiederherstellung nach einer Attacke. Das ist mehr als reine Prävention. Es geht vielmehr darum, die Integrität Ihrer kritischen Daten konsequent sicherzustellen. Zu Cyberresilienz gehören Mitarbeiter, Prozesse und Technologien gleichermaßen.

Menschen und Prozesse bilden die Kultur der Cyberresilienz

Ohne geeignetes Framework sind Sie anfällig für jede Art von Cyberangriffen. IT-Organisationen nutzen daher spezielle Rahmenwerke wie das von NIST und stellen damit sicher, dass sie in jeder Phase die passenden Prozesse implementiert haben. Hierzu zählen u. a. Prozesse und Methoden zum Schutz vor Bedrohungen, zur Erkennung, Identifizierung und zur Wiederherstellung.

Die Vorbereitung ist entscheidend, aber nicht alles. Ebenso wichtig ist die richtige Technologie zur Datenwiederherstellung, z.B. mit Zerto, einem Unternehmen von Hewlett Packard Enterprise. Diese Plattform arbeitet mit kontinuierlicher Datensicherung (Continuous Data Protection/CDP).

Im „Survival Kit bei Cyberangriffen“ finden Sie weitere Links und Hinweise auf Ressourcen, die Ihnen helfen, eine starke Cyberresilienz aufzubauen.

KERNFUNKTIONEN

Sekundenschnelle Wiederherstellung

Komplette Sites, Apps, VMs und Dateien feingranular und in Sekunden wiederherstellen

Applikationskonsistenz

Vollständige Multi-VM-Anwendungen aus einem einzigen Prüfpunkt konsistent wiederherstellen

Kurz- und Langzeitspeicherung

Daten mit der Journal-Technologie von Zerto vorhalten, ob kurz- oder langfristig

Durchgängig unterbrechungsfreies Testen

Wiederherstellungstests mit zusätzlichen Berichtsfunktionen in isolierten Umgebungen durchführen – ohne Beeinträchtigung der Produktion

Datenforensik

Daten nach Attacken in einem separaten Netzwerk isolieren und auf Integrität prüfen, bevor sie in die Produktion gelangen

Zerto
a Hewlett Packard Enterprise company

Lückenlose Datensicherung schützt vor Cyberbedrohungen

Die IDC-Umfrage ergab außerdem, dass 80 % der befragten Unternehmen ihre Strategie der Datensicherung überdenken mussten, weil klassische Lösungen den Wechsel zu Homeoffice und Telearbeit nicht mitmachen. Backup-Technologien mit Snapshots weisen immer Lücken in der Zeitleiste auf, was zu Datenverlusten und langen Wiederherstellungszeiten führt, die das gesamte Unternehmen lahmlegen können.

> Wir konnten die letzte Ransomware-Attacke in 15 Minuten stoppen und unsere Systeme nach drei Stunden wieder in Betrieb nehmen! Ohne Zerto hätten wir Lösegeld zahlen müssen – und zwar ohne die Garantie, unsere Daten zurückzubekommen.
>
> RUBYANNE O'BRYAN
> Systemadministrator
> ClearPath Mutual

Der Zerto-Unterschied: Kontinuierliche Datensicherung

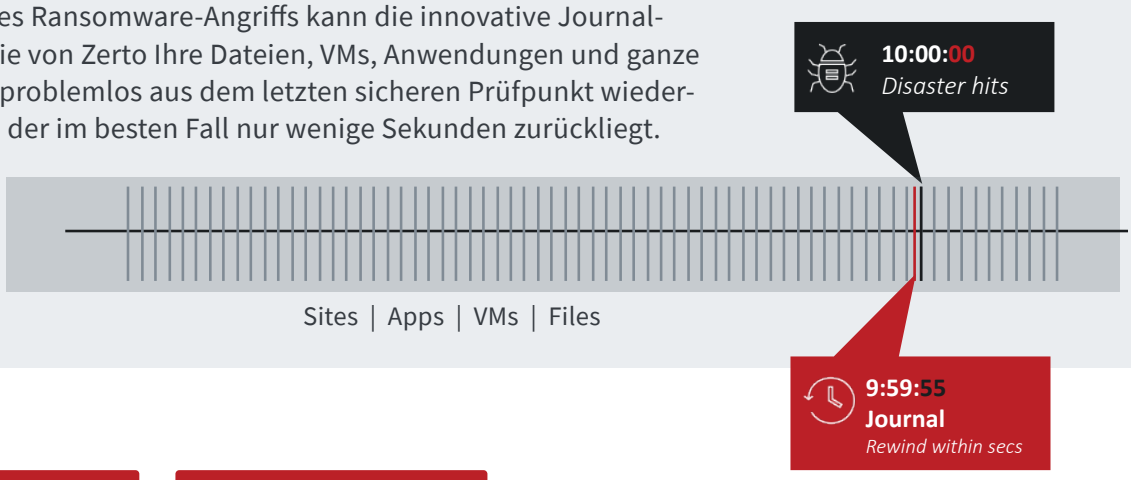
Kontinuierliche Kette von Wiederherstellungspunkten: Das Elastic Journal verbindet die granulare Journal-Technologie mit Langzeitspeicher-Repositories zu einer lückenlosen Kette von Wiederherstellungspunkten, auf die Sie einfach zurücksetzen können – wenige Sekunden, Stunden oder gar Jahre.

Applikationskonsistenz: VPGs (Virtual Protection Groups) stellen sicher, dass sich komplette Anwendungsstapel garantiert konsistent schützen und wiederherstellen lassen. Die konsistente Wiederherstellung einer Anwendung ist unabhängig von der Anzahl der virtuellen Maschinen und deren Ort in der Infrastruktur.

Durchgängig unterbrechungsfreie Tests: Die IT Resilience Platform™ von Zerto ermöglicht orchestrierte und automatisierte Disaster-Recovery-Tests – jederzeit und mit nur vier einfachen Klicks.

Wiederherstellung nach Ransomware in Sekunden

Im Fall eines Ransomware-Angriffs kann die innovative Journal-Technologie von Zerto Ihre Dateien, VMs, Anwendungen und ganze Standorte problemlos aus dem letzten sicheren Prüfpunkt wiederherstellen, der im besten Fall nur wenige Sekunden zurückliegt.



DEMO ANFORDERN | **TOUR STARTEN**

Über Zerto

Zerto ist ein Unternehmen von Hewlett Packard Enterprise, das Schutz, Wiederherstellung und Mobilität von On-premises- und Cloud-Anwendungen vereinfacht und so dafür sorgt, dass seine Kunden „always on" sind. Die Zerto-Plattform für Datenmanagement und Sicherheit in der Cloud minimiert die Risiken und die Komplexität von Modernisierung und Migration bei Private, Public und hybriden Clouds. Die einfache, rein Software-basierte und frei skalierbare Plattform führt mit kontinuierlicher Datensicherung Disaster Recovery, Backup und Datenmobilität zusammen. Auf Zerto vertrauen bereits über 9500 Kunden weltweit. Die Plattform unterstützt Lösungen mit Microsoft Azure, IBM Cloud, AWS, Google Cloud und Oracle Cloud sowie von über 350 Managed-Service-Providern. **www.zerto.com**

Copyright 2022 Zerto. Änderungen vorbehalten.

IS-13875