Schützen von Unternehmen vor Ransomware

Warum ist DRaaS (Disaster Recovery as a Service) ein Muss?

Resilienz-Irrtümer: Wie resilient ist Ihr Unternehmen?

Es steht viel auf dem Spiel: Die Folgen von Ausfällen

Ungeplante Ausfälle aufgrund von Cyberangriffen oder anderen Zwischenfällen wirken sich unter Umständen auf Folgendes aus:

- Umsatz
- Aktienkurse
- Produktivität
- Kundenvertrauen
- Markenreputation
- Mitarbeiterzufriedenheit
- Compliance, Lizenzen oder Akkreditierungen

Noch nicht darüber nachgedacht? Jetzt ist es an der Zeit!

Schon gewusst?

der kleinen und mittelständischen Unternehmen hatten in den letzten 12 Monaten einen Verlust oder Diebstahl von sensiblen Daten zu verzeichnen.[1]

der Unternehmen haben in den letzten zwei Jahren ein Ereignis erlebt, das einen DR-Plan (Disaster Recovery) erforderte.[2]

Und dann gibt es noch Ransomwareangriffe:

Bis Ende 2021 wird **alle 11 Sekunden** ein Unternehmen Opfer eines Ransomwareangriffs werden.[3]

75% der Unternehmen werden bis 2025 von Ransomware betroffen sein.[4]

Recovery ist oft langwierig (und teuer)

Die durchschnittliche Dauer eines Totalausfalls im Rechenzentrum beträgt fast **138 Minuten**. Die gesamte Abschaltung einer Edge-Einrichtung dauert über **45 Minuten**.[5]

Die durchschnittlichen Kosten für Ausfallzeiten in Unternehmen steigen auf **250.000 USD/Stunde**.[2]

Sie möchten Ihre Cyberresilienz erhöhen?

Disaster Recovery ist die letzte Verteidigungslinie. Ein guter DR-Plan legt den Grundstein für Cyberresilienz. Er unterstützt Sie dabei, Wiederherstellungskapazitäten für den Fall eines ungeplanten Ausfalls zu konzipieren und zu entwickeln, um Unterbrechungen und Schäden für Ihr Unternehmen zu minimieren.

der Unternehmen sind im Hinblick auf ihre Disaster Recovery-Fähigkeiten schlecht aufgestellt.[6]

der Unternehmen unterliegen Irrtümern aufgrund von Selbstüberschätzung.[6]

Was hindert Sie?

Budget
Nur 45% der Unternehmen halten ihr Sicherheitsbudget für angemessen.[1]

Fachkräfte
Nur 39% der Unternehmen sind überzeugt, dass ihre Mitarbeiter über die nötige Fachkompetenz verfügen, um Angreifer erfolgreich abzuwehren.[7]

Selbstüberschätzung
Viele halten es für billiger, Lösegeld zu zahlen. Die durchschnittlichen Kosten eines Ransomwareangriffs betragen 4,62 Mio. US-Dollar.[8]

Die gute Nachricht: Sie können etwas daran ändern. Verlassen Sie sich auf VMware Cloud Disaster Recovery™.

Bis zu 60% niedrigere TCO als bei herkömmlicher DR, keine Vorabinvestitionen in Infrastruktur, geringere Personalkosten und ohne Betrieb oder Wartung eines zweiten DR-Standorts

Schützen Sie Workloads zuverlässig und nachhaltig On-Premises und in der Cloud – verringern Sie die CO2-Bilanz Ihrer DR um über 80%.

Führen Sie die Cloud in Ihrem eigenen Tempo ein, ohne dass Sie ein zweites Rechenzentrum einrichten und verwalten müssen.

VMware Cloud Disaster Recovery™

Bedarfsorientierte DR als anwenderfreundliche, anbieterseitig verwaltete SaaS-Lösung mit Cloud-Ökonomie: Sie kombiniert kosteneffizientes Cloud-Storage mit einfachem, SaaS-basiertem Management für IT-Resilienz im erforderlichen Maßstab.

- Unterbrechungsfreies Testen und Orchestrieren von Failover- und Failback-Plänen
- Failover-Kapazitätsmodell mit nutzungsbasierter Zahlung für DR-Ressourcen
- Funktionen für Ransomwareschutz: unveränderliche, Cloud-basierte Snapshots, Recovery auf Dateiebene und RPOs von nur 30 Minuten
- Automatisierte DR-Systemdiagnosen im 30-Minuten-Takt
- Integrierte Audit-Reports und RPOs von nur 30 Minuten

Planen Sie für den Optimalzustand, bereiten Sie sich auf das Schlimmste vor. Erstellen Sie einen DR-Plan, um Ihr Unternehmen – und die Daten Ihrer Kunden – vor unerwarteten Ausfällen zu schützen. Mit VMware Cloud DR setzen Sie Ihren Plan in die Tat um.

Bereit? Hier starten

Quellen:

1. Ponemon Institute, 10 schockierende Statistiken zu Datenverlust und Disaster Recovery
2. IDC-Umfrage zur IT-Infrastruktur in Unternehmen: „Insights on End-User 2021 IT Infrastructure Priorities and Adoption of Data Protection/Disaster Recovery Services and Solutions", 4. Quartal 2020
3. Cybercrime Magazine: „Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021"
4. Gartner, „Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware", veröffentlicht am 6. Januar 2021 von Nik Simpson und Ron Blair
5. Ponemon Institute: „Data Center Downtime at the Core and the Edge: A Survey of Frequency, Duration and Attitudes"
6. Gartner: „Market Guide for Disaster Recovery as a Service", veröffentlicht am 29. Juli 2021, ID G00731593, von den Analysten: Ron Blair, Jeffrey Hewitt
7. Ponemon Institute
8. IBM-Report „Cost of a Data Breach", 2021

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Willy-Brandt-Platz 2 81829 München Telefon +49 89 370 617 000 Fax +49 89 370 617 333 www.vmware.com/de