OVERLAND TANDBERG

WHITE PAPER

Die letzte Verteidigungslinie

Aufbau effektiver Business Continuity Lösungen

Februar 2024

Hintergrund

Ein Datenverlust kann jederzeit passieren. Ob Hardwarefehler, menschliches Versagen oder Viren- und Malware-Angriffe aber auch lokale Katastrophen – Unternehmen müssen darauf vorbereitet sein, Geschäftskontinuität und Datenverfügbarkeit sicherzustellen. Das Whitepaper beschreibt eine Auswahl möglicher Ursachen und Auswirkungen von Datenverlust und zeigt Lösungen, wie man sogar nach einer Ransomware-Attacke den Geschäftsbetrieb schnell wieder herstellen kann.

Herausforderungen:

- 21 % aller Datenverluste werden durch Hardwarefehler verursacht
- Täglich werden mehr als 390.000 Schadprogramme entdeckt
- Ransomware-Angriffe verursachen durchschnittlich 16,2 Tage Ausfallzeit
- 43 % der Cyberangriffe richten sich gegen kleine Unternehmen, nur 14 % sind dafür vorbereitet

Eine Betriebsunterbrechung aufgrund von Datenverlust hat zahlreiche Konsequenzen. Es besteht das Risiko von Umsatzeinbußen, die Auswirkungen auf die Bilanzen haben. Finanzielle Verpflichtungen können nicht mehr erfüllt werden, was höhere Zinsen und Schadensersatzansprüche Dritter nach sich zieht. Mitarbeiter können ihre Aufgaben nicht mehr erfüllen und befinden sich daher in Verzug.

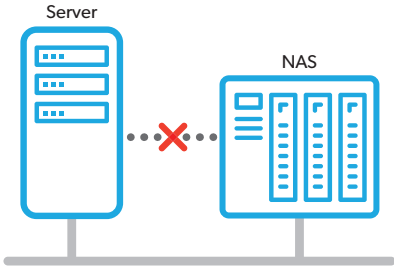
Es besteht zudem die Möglichkeit, dass ein solcher Vorfall dem Ansehen schadet. Verzögerungen bei der Betreuung von Kunden können dazu führen, dass diese zur Konkurrenz wechseln. Der vorübergehende Liquiditätsmangel verärgert Lieferanten und Banken und schränkt die Kreditwürdigkeit ein.

Finanzielle und ökonomische Herausforderungen:

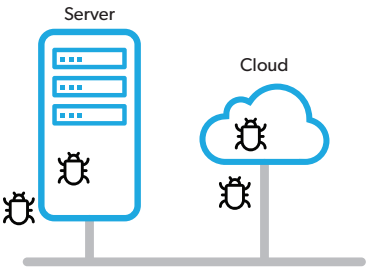
- Eine Stunde Ausfallzeit kostet kleine Unternehmen 100.000 EUR – Gartner
- Ein Cyberangriff kostet Unternehmen jeder Größe 200.000 EUR – Hiscox Business Insurance
- 98 % der Kleinunternehmen schließen, nachdem sie gehackt wurden
- 60 % der Unternehmen schließen innerhalb von 6 Monaten nach einem Datenverlust

Das Problem

Viele Unternehmen sind nicht darauf vorbereitet, die Geschäftskontinuität sicherzustellen. Sicherungen werden normalerweise auf einem Speichergerät durchgeführt, z. B. auf lokalen Festplatten oder NAS-Systemen (Network Attached Storage) oder in der Cloud. Dies ist eine praktikable Lösung, berücksichtigt jedoch nicht lokale Katastrophen oder Viren- und Ransomware-Angriffe.



Lokale Katastrophen können auch das Backup auf dem lokalen Gerät zerstören. Viren- und Ransomware-Angriffe können Backup-Sets unabhängig von ihrem Speicherort auf dem Computer, im Netzwerk oder in der Cloud infizieren und sogar löschen.



In beiden Fällen ist es eventuell unmöglich, die Daten wiederherzustellen und sich von diesen Vorfällen zu erholen. Möglicherweise lassen sich einige Daten aus Briefen, Rechnungen oder anderen Papierdokumenten rekonstruieren. Vielleicht können Kunden helfen, verlorene Informationen bereitzustellen, aber die meisten Informationen gehen verloren.

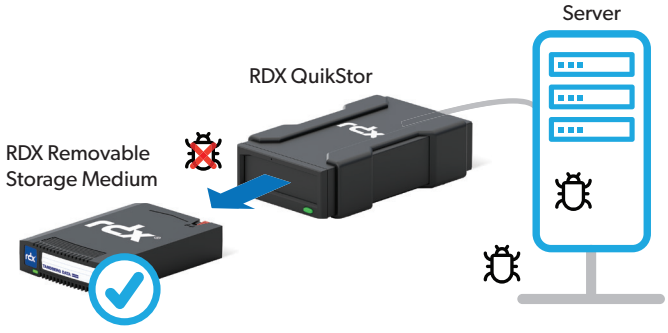
Die Lösung – Aufbau der letzten Verteidigungslinie

Wenn Speichersysteme nicht mehr mit dem Netzwerk verbunden sind, sind Daten und Backups sicher und können nicht durch Malware-Angriffe gefährdet werden. Daher sollten Unternehmen Wechselspeichermedien nutzen. Wechselspeichersysteme können die Speichermedien auswerfen und somit vom Netzwerk trennen. Dadurch ist der Zugriff auf Daten auch nach einer lokalen Katastrophe oder einem Ransomware-Angriff sichergestellt.

Dies kann entweder durch Offline-Schalten des Speichergeräts oder Entfernen des Speichermediums und Transport an einen sicheren Ort außerhalb der Betriebsstätte (Offsite) erfolgen. Auswurfvorgänge können mit den meisten Backup-Programmen konfiguriert oder per Skript ausgeführt werden.

Die RDX® Technologie

RDX ist eine proprietäre Wechselplatten-Technologie von Overland-Tandberg. Es besteht aus Wechselplattensystemen und Wechselplatten-Appliances. Das robuste Design bietet einen zuverlässigen und wertigen Datenspeicher. Durch die Portabilität eignet es sich ideal für die externe, räumlich getrennte Speicherung, um ein Air Gap für Disaster Recovery und Ransomware-Schutz aufzubauen.

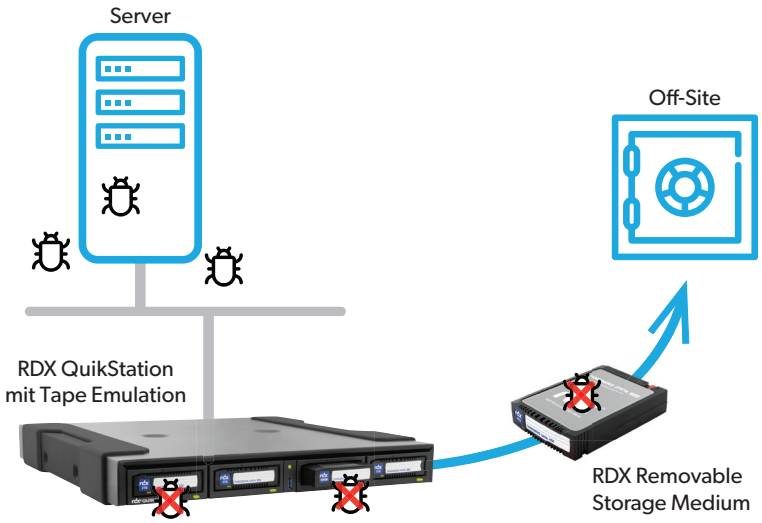


RDX QuikStor ist die ideale Lösung für Remote- und Home Office-Nutzer sowie Zweigstellen und KMU-Umgebungen. Aufgrund der herausnehmbaren Datenkassette können Backups offline und offsite gespeichert werden und sind sicher vor Ransomware-Angriffen geschützt.

Wir empfehlen die Einrichtung eines Medienrotationsschemas mit mindestens drei Datenkassetten, wobei sich eine Kassette außerhalb des Standorts, eine im Transport und eine im QuikStor-System befindet und für die nächste Sicherung bereit ist.

RDX QuikStation ist eine über iSCSI angeschlossene Wechseldatenträger-Appliance. Sie bietet eine flexible Plattform für Hybrid-Cloud-Datenschutz und externe Notfallwiederherstellung für physische oder virtuelle Umgebungen. Aufgrund der zahlreichen Konfigurationsoptionen wie einzelne Festplattenziele, logische Volumes über alle RDX-Laufwerke, Festplatten-Autoloader-, Band-Autoloader- und Bandbibliotheksemulationen, lässt sich RDX QuikStation in unterschiedlichste Umgebungen integrieren.

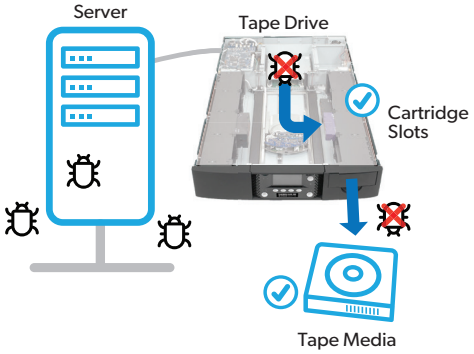
Die Festplattenmodi bieten die gleiche Funktionalität wie im Abschnitt RDX QuikStor beschrieben. Im Festplatten-Autoloader-Modus ist nur eine Kassette physisch einem RDX-Dock zugewiesen, die anderen sind vom Netzwerk getrennt, da sie sich in einem logischen Slot befinden. In den Emulationsmodi der Bandautomatisierung wird das Medium als LTO-Band behandelt und bietet vollständigen Viren- und Ransomware-Schutz.



Allerdings sollten auch lokale Katastrophen berücksichtigt werden, bei denen auch Medien zerstört werden. Daher sollten die RDX-Medien auch extern außerhalb des Rechenzentrums gelagert werden.

Die NEO® Tape Libraries

LTO-Bandlaufwerke und LTO-Band-Automatisierungssysteme von Overland-Tandberg basieren auf 45 Jahren Erfahrung in der Datenspeicherung. Durch den Einsatz branchenführender LTO-Bandtechnologie bietet die Familie der NEO-Serie geringere Betriebskosten, verbesserte Datenverfügbarkeit, hohe Zuverlässigkeit, einfache Datenverwaltung und Schutz vor Cyberangriffen.



Overland-Tandberg bietet Bandlösungen für jede Anwendung und jede Unternehmensgröße. Angefangen bei eigenständigen Bandlaufwerken über Autoloader und kleine Bibliotheken bis hin zu skalierbaren Bandbibliotheken der NEOxl-Familie wird jeder Bedarf an Kapazität und Leistung abgedeckt.

Die Kassettenschächte und I/O-Ports der Band-Autoloader und Bandbibliotheken bilden ein Air Gap, indem sie Offline- und Off-Site-Speichermöglichkeiten bieten. Solange sich ein LTO-Bandmedium in einem Kassettenschacht oder sogar außerhalb des Bandsystems befindet, hat Ransomware keine Chance, die Daten zu beschädigen.

Zusammenfassung

Die Sicherstellung der Geschäftskontinuität ist die wichtigste Aufgabe für Unternehmen jeder Größe. Datenverlust und Betriebsunterbrechungen führen zu finanziellen Verlusten oder sogar zur Schließung des Unternehmens.

Der Aufbau einer letzten Verteidigungslinie mithilfe von Wechselmedien ist für die Aufrechterhaltung des Geschäftsbetriebs und die Vermeidung von Ausfallzeiten von entscheidender Bedeutung. Wechselmedienspeichersysteme wie die RDX- und NEO-Bandbibliothekslösungen von Overland-Tandberg gewährleisten den Zugriff auf Ihre Daten nach einem Angriff.

Wir empfehlen, regelmäßig ein Backup durchzuführen und dieses auch extern zu speichern, um nicht nur vor Malware-Angriffen, sondern auch vor lokalen Katastrophen geschützt zu sein.

Weitere Informationen

Wenn unser White Paper nicht alle Ihre Fragen zu Ihren Backup-Herausforderungen beantwortet hat, stehen Ihnen die Speicherspezialisten von Overland-Tandberg gerne zur Verfügung, um Ihnen bei der Suche nach der besten Lösung für Ihr Unternehmen behilflich zu sein. Besuchen Sie hierzu unsere Kontakt-Seite.

Vertrieb und Support für Overland-Tandberg-Produkte und Lösungen stehen in über 100 Ländern zur Verfügung. Kontaktieren Sie und noch heute über sales@overlandtandberg.com.
Besuchen Sie OverlandTandberg.com/de.

WP_v1_feb05_2023