Schützen Sie Ihre Daten vor bösartigen Ransomware-Bedrohungen

Diese Best Practices für die Datenverfügbarkeit sollen sicherstellen, dass sich Unternehmen effektiv auf potenzielle Datenverluste und Ausfallzeiten durch Ransomware-Angriffe vorbereiten und diese vermeiden können. Anhand dieser branchenspezifischen Best Practices können IT-Manager Lösegeldzahlungen vermeiden und eine absolut zuverlässige Datenverfügbarkeitslösung für den täglichen Betrieb schaffen. Hierfür steht die effektive Kombination aus HPE und Veeam® Software zur Verfügung.

„Es gibt bisher keine Methoden oder Tools, die Sie oder Ihr Unternehmen vollständig vor einem Ransomware-Angriff schützen. Entsprechende Notfall- und Korrekturpläne sind daher entscheidend für die Wiederherstellung und Kontinuität von Unternehmensprozessen. Solche Pläne müssen in regelmäßigen Abständen überprüft werden."

– James Trainor, ehemaliger FBI Cyber Division Assistant Director.

Dieses Angebot zeigt Benutzern, dass Ransomware nur ein Teil eines Bedrohungsumfelds ist, das letztendlich das Eindringen in ihr Netzwerk ermöglicht. Die beste Lösung ist der Schutz der Daten, auf die es Eindringlinge abgesehen haben.
fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

Ransomware-Angriffe nehmen weiter zu

Ransomware-Angriffe dehnen sich weiterhin auf zahlreiche Branchen aus. Ursächlich hierfür sind die Ausnutzung von gesetzlichen Bestimmungen und Compliance-Vorgaben, anfällige Netzwerke und mangelhafte Sicherungsstrategien. Durch die Zunahme dieser Bedrohungen sind immer mehr Branchen und Unternehmen aller Größenordnungen betroffen. Selbst bei leistungsfähigen Cybersicherheitslösungen und -verfahren dringen die Angreifer immer wieder in Netzwerke ein. Nach Angaben des Institute for Critical Infrastructure Technology (ICIT) wird Ransomware in den Jahren 2016 und 2017 für Unternehmen voraussichtlich verheerende Auswirkungen haben. Bedrohungen durch Ransomware sind auf dem Vormarsch. „Fast 40 % der Unternehmen werden von Angriffen betroffen sein."[1]

Geschäftliche und IT-spezifische Risiken durch Ransomware

Ransomware-Angriffe sind mehr als nur Sicherheitsrisiken. Unternehmen, die Opfer von Ransomware werden, sind nicht nur mit finanziellen und technischen Problemen konfrontiert. Die Unternehmensmarke kann so stark beschädigt werden, dass sich Unternehmen davon möglicherweise nie mehr erholen.

Gravierende finanzielle Auswirkungen

Die Kosten durch Lösegeldzahlungen, die wertvolle IT-Zeit und die möglichen Ausfälle von geschäftskritischen Anwendungen können ein Unternehmen dauerhaft schädigen.

Rückschläge im IT-Bereich

Hacker behalten die Kontrolle und den Zugriff auf das Netzwerk des betroffenen Unternehmens und nutzen dies für mögliche zukünftige Angriffe und weitere Forderungen. IT-Manager sehen sich bei Ransomware immer wiederkehrenden Bedrohungen ausgesetzt und setzen mehr Mitarbeiter ein, um dieses Problem in den Griff zu bekommen. Diese Zeit und Ressourcen fehlen dann bei den Aufgaben, die für das Unternehmen besonders wichtig sind.

Schaden für die Unternehmensmarke

Viele Unternehmen melden Ransomware-Angriffe nicht, um Schaden für die Unternehmensmarke sowie den Verlust von Kunden und Marktanteilen zu vermeiden. Unternehmen, die Lösegeld bezahlen oder ihre Daten nicht ausreichend sichern, werden letztendlich Opfer von noch ausgefeilteren Angriffen, die zu einer gravierenden Beschädigung ihrer Markenidentität und ihrem Ruf auf dem Markt führen können.

[1] **„Bedrohungen durch Ransomware sind auf dem Vormarsch. ‚Fast 40 % der Unternehmen werden von Angriffen betroffen sein'"**. The Guardian, August 2016.

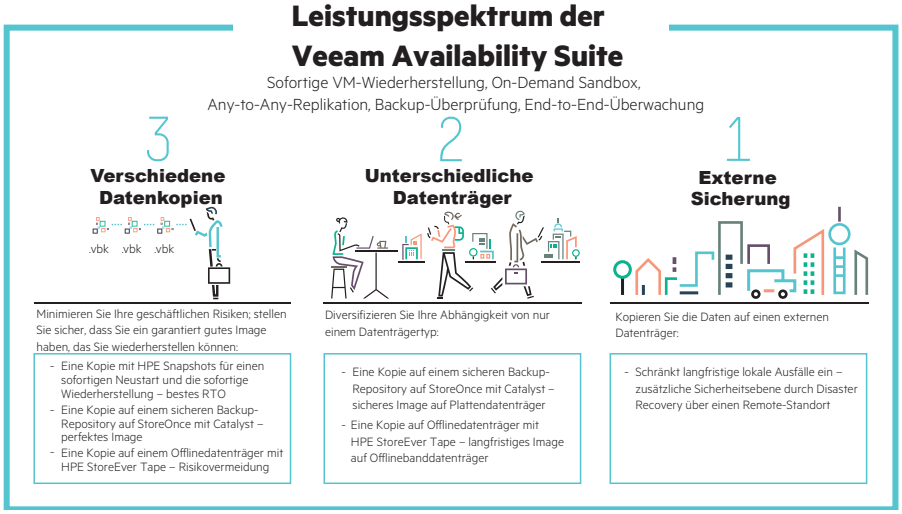
Veeam- und HPE Lösungen im Überblick

Die branchenführenden Lösungen von Veeam und HPE sind für Unternehmen jeder Größe bestens ausgestattet, um bösartige Angriffe zu bekämpfen und die Unternehmensdaten zu schützen.

- **Schnelle Datenwiederherstellung**
  HPE Storage Snapshots ermöglichen eine schnelle VM-basierte (Virtual Machine) und differenzierte Wiederherstellung, um verschlüsselte Ransomware-Datenbanken, -Anwendungen, -Dateien und -Betriebssysteme zu überschreiben. Dank der bewährten Integration mit HPE 3PAR StoreServ, Store Virtual, StoreOnce und StoreOnce Catalyst können Sie Anwendungen schnell wiederherstellen und Ausfallzeiten vermeiden.
- **Sperrung der Infrastruktur**
  Was Ransomware nicht erkennt, kann sie auch nicht infizieren. HPE ermöglicht dies durch die Integration mit StoreOnce Catalyst. Diese Lösung macht Backup-Images für Ransomware unsichtbar und ermöglicht so die Wiederherstellung. Eine zusätzliche Schutzebene wird durch Offlinekopien auf Band und asynchrone Remote-Replikationskopien geschaffen.
- **Testumgebung**
  Testen und entfernen Sie mit Veeam On-Demand Sandbox™ und Veeam SureBackup Ransomware-Elemente innerhalb kürzester Zeit, bevor Sie VMs in der Produktivumgebung wiederherstellen.
- **Integrierte Benutzerfreundlichkeit**
  Nutzen Sie mit dem Veeam ONE™ Tool für Überwachung, Berichterstellung und Kapazitätsplanung die integrierte Backup-Bewertung, um sicherzustellen, dass Ihre kritischen VMs ausreichend geschützt sind.

Diese Funktionen sind bei der Kombination aus Veeam Availability Suite™ und einer HPE Storage-Lösung Standardfunktionen. Die Lösung benötigt keine speziellen Skripte und nutzt Standardprodukte von HPE und Veeam.

Melden Sie sich noch heute an.



Fallstudie: Erfolgreiche Ransomware-Abwehr mit Veeam

Die Bedford School in England wurde Opfer eines bösartigen Ransomware-Angriffs durch einen CryptoLocker-Virus, der den Computer eines Mitglieds des Lehrkörpers infizierte und alle Dateien verschlüsselte. Der Schule fehlten die Mittel, um das hohe Lösegeld zu bezahlen. Gleichzeitig konnte man sich jedoch keine zusätzlichen Netzwerkausfallzeiten leisten.

Da das IT-Team der Bedford School die 3-2-1-Backup-Regel befolgte, musste kein Lösegeld bezahlt werden und es kam zu keinen Verlusten bei der Netzwerkfunktionalität. Mit Veeam konnte jede verschlüsselte Datei schnell wiederhergestellt werden.

Die Ransomware-Lösung von HPE und Veeam

Diese Datenverfügbarkeitslösung von Veeam und HPE ist so konzipiert, dass sie allen Ransomware-Versuchen von Hackern entgegenwirkt. Durch die Einhaltung der bewährten 3-2-1-Backup-Regel von Veeam können Unternehmen die Integrität und Verfügbarkeit ihrer Daten sicherstellen. Das obige Diagramm zeigt die 3-2-1-Regel zusammen mit branchenführenden Empfehlungen.

Anwendung der 3-2-1-Backup-Regel auf Ransomware

Das Ziel der 3-2-1-Regel ist es, den Kunden eine Datenschutzlösung zur Verfügung zu stellen, die die Betriebszeit der Anwendungen und die Datenverfügbarkeit maximiert. Wird sie ordnungsgemäß ausgeführt, können IT-Manager ihre Daten mit unseren 3-2-1-Richtlinien umfassend schützen:

- Pflegen Sie drei (3) Kopien Ihrer Daten – die Primärdaten und zwei Sicherungskopien – um zu vermeiden, dass Daten durch ein fehlerhaftes Backup verloren gehen.
- Speichern Sie Sicherungskopien auf zwei (2) verschiedenen Medientypen wie Band, Diskette, Sekundärspeicher oder Cloud.
- Bewahren Sie eine (1) Kopie außerhalb des Netzwerks auf – entweder auf Band oder in der Cloud – um gegen Gefahren vor Ort oder Ransomware-Infektionen innerhalb des Netzwerks gewappnet zu sein.

Zusammenfassung

Bei der Datenverfügbarkeitslösung handelt es sich um eine vollständig integrierte Lösung, die sich aus der vorhandenen Technologie zusammensetzt. Die Lösung bietet Unternehmen nicht nur die Möglichkeit, sich schnell von einem Ransomware-Angriff zu erholen, sondern ist auch als Datenverfügbarkeitslösung für das tägliche operative Geschäft in Großunternehmen zu sehen. Diese Best Practices-Lösung ist flexibel und kostengünstig und kann durch einen Veeam-zertifizierten Partner schnell implementiert werden.

Weitere Informationen

zur Einhaltung der 3-2-1-Regel finden Sie im Veeam Backup & Replication™ Blog.

Hewlett Packard Enterprise | Veeam

a00000445DEE, Januar 2017