Ihre ersten 100 Tage mit Veeam Data Platform

Guide für Führungskräfte zur messbaren Resilienz

Die meisten Organisationen gehen davon aus, dass sie geschützt sind, doch nur wenige haben dies tatsächlich überprüft.

In einer kürzlich durchgeführten Umfrage gaben 90 % der Sicherheitsverantwortlichen an, dass sie die Wiederherstellung innerhalb ihrer definierten Zielvorgaben erreichen könnten. Unter den Ransomware-Opfern konnten nur 28 % ihre Daten vollständig wiederherstellen (Quelle: Data Trust and Resilienz Report 2026). Vertrauen ist nicht dasselbe wie nachgewiesene Wiederherstellungsfähigkeit, und die Lücke dazwischen ist der Ort, an dem Ransomware die Oberhand gewinnt, Audits scheitern und Ausfälle zu Krisen werden.

90 %

der Sicherheitsverantwortlichen gaben an, dass sie die Wiederherstellung innerhalb ihrer definierten Zielvorgaben erreichen könnten.

28 %

der Ransomware-Opfer konnten ihre Daten vollständig wiederherstellen.

Denn Resilienz ist nur dann echt, wenn man sie unter Beweis stellen kann.

Dieser Guide betrachtet Ihre Veeam Data Platform-Bereitstellung aus strategischer Sicht. Während Ihr Team die technischen Bereitstellungsmeilensteine durchläuft, übersetzt dieser Guide diese in Business-Ergebnisse: die reduzierten Risiken, die gewonnenen Funktionalitäten und den Nachweis, den Sie am Ende vorlegen können.

Denn die Entscheidungen über Risikotoleranz, Wiederherstellungsverpflichtungen und Business Continuity treffen Sie selbst. Dieser Guide behandelt Ihre Verantwortlichkeiten und zeigt Ihnen, was Sie bis Tag 100 mit Zuversicht gegenüber dem Vorstand, Wirtschaftsprüfern und Versicherern kommunizieren können.

Dieser Guide stattet Sie mit Folgendem aus:

1. Die fünf Ergebnisse, die bewährte Resilienz von vermeintlichem Schutz unterscheiden
2. Was dies für Ihre Rolle bedeutet: CIO, CISO oder CFO
3. Die sieben Anwendungsfälle, die Ihre Investition abdeckt, und wie deren Umsetzung Ihren ROI steigert
4. Fragen, die Sie Ihrem Team stellen sollten, um zu bestätigen, dass die Resilienz nach Tag 100 besteht

Von der Gefährdung zum Nachweis: Die fünf entscheidenden Ergebnisse

Dies sind die fünf Ergebnisse, zu denen sich Ihr Unternehmen verpflichtet, wenn es Veeam Data Platform bereitstellt. Jedes dieser Ergebnisse stellt einen Schritt auf dem Weg von Gefährdung zu Nachweis dar und gemeinsam definieren sie, wie eine nachweislich resiliente Umgebung aussieht.

01. Bereitgestellt

Sie wissen genau, was geschützt ist, wo es sich befindet und welchem Standard es entspricht. Keine Annahmen und keine Lücken, die erst unter Druck auffallen.

02. Geschützt

Jeder kritische Workload ist durch einen Plan abgedeckt, auf den sich Ihre Business-Continuity-Strategie stützen kann. Im entscheidenden Moment wird nichts übersehen.

03. Gehärtet

Ein Angreifer kann Ihre Fähigkeit zur Wiederherstellung nicht zunichte machen. Unveränderliche Kopien existieren lokal und extern und bieten einen bestätigten sauberen Wiederherstellungspunkt, unabhängig davon, wie sich ein Vorfall entwickelt.

04. Nachweislich wiederherstellbar

Sie können nachweisen, dass die Wiederherstellung funktioniert — nicht nur behaupten. Es ist geprüft, dokumentiert und bereit, Ihrem Vorstand, Ihren Wirtschaftsprüfern und Ihrem Versicherer vorgelegt zu werden.

05. Betriebsbereit

Resilienz hängt nicht von einer Person oder einer heldenhaften Leistung ab. Es basiert auf klaren Zuständigkeiten, strukturiertem Reporting und einem festgelegten Rhythmus, den Ihr Team aufrechterhalten kann.

Was das für Ihre Rolle bedeutet

CIO/CTO

Wenn der Vorstand fragt, ob Ihre Organisation nach einem schwerwiegenden Vorfall wiederherstellen kann, haben Sie eine erprobte und dokumentierte Antwort. Das Ausfallrisiko ist nicht mehr eine Vertrauenssache, sondern eine Frage der Nachweisbarkeit.

CISO

Sie haben einen bestätigten, sauberen Wiederherstellungspunkt, bevor aus einem Vorfall eine Krise wird — nicht erst danach. Intelligente Bedrohungs-Scans, unveränderbare Kopien und dokumentierte Testergebnisse liefern Ihnen die Nachweise, die Ihre Versicherer, Auditoren und Ihre Rechtsabteilung benötigen.

CFO

Die Voraussetzungen für eine Cyberversicherung, die Verlängerungsbedingungen und die Verhandlungen über die Prämien verbessern sich, wenn die Wiederherstellbarkeit nachweisbar ist und nicht nur angenommen wird. Untersuchungen zeigen, dass Unternehmen, die stärker in die Datenresilienz investiert haben, nur in 33 % der Fälle Lösegeld gezahlt haben, während es bei denjenigen ohne entsprechende Investitionen 52 % waren. Ihre Investition in Veeam ist klar abgegrenzt, planbar und steht in direktem Zusammenhang mit der Verringerung des finanziellen Risikos eines ungeplanten Ausfalls.

33 %

der Zeit, in der Organisationen mit stärkeren Investitionen in die Datenresilienz ein Lösegeld zahlten.

52 %

der Zeit, in der Organisationen ohne diese Investitionen ein Lösegeld zahlten.

Quelle: Data Trust and Resilienz Report (2026).

Der generierte Mehrwert

Der von der Veeam Data Platform geschaffene Mehrwert geht weit über einzelne Rollen oder einzelne Vorfälle hinaus. Ab den ersten 100 Tagen erhält Ihr Unternehmen Zugang zu Funktionalitäten, die der tatsächlichen Komplexität moderner IT-Umgebungen gerecht werden: hybride Infrastruktur, Cloud-Wildwuchs, regulatorischer Druck und eine sich ständig weiterentwickelnde Bedrohungslandschaft.

Dies sind die sieben Anwendungsfälle, für die Ihre Investition ausgelegt ist.

Schützen, wiederherstellen

Wenn ein Vorfall eintritt, hängt die Qualität Ihrer Reaktion vollständig von der Qualität Ihrer Vorbereitung ab. Dies ist die Grundlage, die jede Organisation benötigt, unabhängig von Branche oder Infrastruktur.

1. **Bedrohungserkennung und -reaktion:** Veeam scannt Backup-Ketten auf Malware-Indikatoren und validiert die Dateiintegrität vor der Wiederherstellung, sodass Ihr Unternehmen saubere Daten wiederherstellt, anstatt eine Bedrohung erneut einzuschleusen. Dokumentierte Scan-Ergebnisse unterstützen Ihren Prozess zur Reaktion auf Vorfälle und erfüllen die Anforderungen der Versicherer.
2. **Disaster Recovery in die Cloud:** Wenn die lokale Infrastruktur ausfällt, verlagert Veeam die Workloads im Rahmen Ihrer festgelegten Wiederherstellungsziele auf Cloud-Ziele. Ihr Team verfügt über einen erprobten, umsetzbaren Plan statt eines manuellen Prozesses, der unter Druck keine guten Ergebnisse liefert.

Kontrolle und Compliance

Der regulatorische Druck und die Anforderungen an die Datenhoheit nehmen zu. Ihre Datenschutzstrategie muss mit den zunehmenden Anforderungen Schritt halten. Wenn Sie in einer regulierten Branche tätig sind oder kurz vor einem Prüfungszyklus stehen, sollten Sie sich zunächst auf diesen Bereich konzentrieren.

3. **Governance, Risk und Compliance:** Veeam erstellt das auditfähige Reporting, das Ihre Compliance- und Rechtsabteilungen benötigen — einschließlich Wiederherstellungstest-Ergebnissen, Abdeckungsinventar und Bestätigung der Aufbewahrungsrichtlinie, ganz ohne manuelle Nachweiserbringung beim Audit.
4. **Souveränität:** Veeam verschafft Ihrer Organisation Kontrolle darüber, wo Backup-Daten gespeichert und verarbeitet werden, unterstützt data residency-Anforderungen in verschiedenen Rechtsräumen, ohne dabei die Wiederherstellung zu beeinträchtigen.

In komplexen Umgebungen agieren

Moderne Infrastruktur ist nicht ortsgebunden. Das sollte auch für Ihre Sicherheitsstrategie gelten. Wenn Sie sich mitten in einer Migration befinden oder bereits eine Multi-Cloud-Umgebung oder eine hybride SaaS-Umgebung betreiben, konzentriert sich das operative Risiko genau hier.

5. **Workload Mobility über verschiedene Umgebungen hinweg:** Während Workloads zwischen lokalen, Cloud- und Edge-Umgebungen wechseln, wandert der Schutz von Veeam mit ihnen mit. Die Abdeckung bleibt auch bei Änderungen an Ihrer Infrastruktur gewährleistet.
6. **Schutz in der Multi-Cloud-Umgebung:** Veeam gewährleistet konsistenten Schutz und Wiederherstellungsfunktionalitäten über alle Cloud-Provider hinweg und beseitigt das operationelle Risiko fragmentierter Tools und fehlender Transparenz zwischen Plattformen.
7. **Hybrid-SaaS:** Kritische Daten, die in SaaS-Anwendungen gespeichert sind, werden zusammen mit Ihren Infrastruktur-Workloads geschützt und schließen so die Schutzlücke, die viele Unternehmen erst nach einem Vorfall erkennen.

Dies sind weder zukünftige Funktionalitäten noch optionale Erweiterungen. Es sind die Fähigkeiten, die Ihr Unternehmen im Verlauf der Bereitstellung und Aktivierung gewinnt; jede einzelne reduziert eine spezifische Risikokategorie und gibt Ihrem Führungsteam Vertrauen, wenn der Druck steigt. Die Frage ist nicht, ob Ihr Unternehmen dieses Maß an Resilienz benötigt, sondern wie schnell Sie dieses erreichen können.

Tag 100 ist nicht die Ziellinie. Es ist der Ausgangspunkt.

Resilienz ist ein kontinuierlicher Prozess, kein einmaliges Projekt.

Veeam stellt die Veeam DataAI Command Platform, das bewährte Data & AI Trust Maturity Model und die technische Expertise bereit, die Ihr Team von der ersten Bereitstellung bis zur vollständig nachgewiesenen Resilienz unterstützt. Es ist uns ein Anliegen, Sie bei jedem Schritt zu unterstützen.

Stellen Sie sicher, dass Ihr Team den technischen Guide für die ersten 100 Tage hat, und beginnen Sie, Umfang, Zeitplan und Ergebnisse der Bereitstellung abzustimmen.

Resilienz auf dieser Ebene ist kein langfristiges Ziel. Mit dem richtigen Bereitstellungsplan wird dies für Ihr Unternehmen zur kurzfristigen Realität.

Der nächste Schritt liegt bei Ihnen.

Fragen, die Sie Ihrem Team in regelmäßigen Abständen stellen sollten

- Sind alle kritischen Workloads abgedeckt, und gibt es Schutzlücken oder Ausfälle, die noch nicht behoben wurden?
- Wann haben wir zuletzt eine vollständige Wiederherstellung unter realen Bedingungen getestet, und liegen uns dazu dokumentierte Ergebnisse vor?
- Wenn heute Nacht Ransomware zuschlägt, könnten wir einen bestätigten sauberen Wiederherstellungspunkt identifizieren und ohne Lösegeldzahlung wiederherstellen?
- Können unsere Compliance- und Rechtsabteilungen Prüfungsnachweise ohne manuellen Aufwand vorlegen, und erfüllt unsere Architektur weiterhin unsere aktuellen regulatorischen Verpflichtungen?
- Wer hat Administratorrechte für unsere Backup-Umgebung, und wann haben wir diese zuletzt überprüft?

Über Veeam Software

Veeam ist das führende Unternehmen für Daten- und KI-Vertrauen mit dem Anspruch, Organisationen dabei zu unterstützen, ihre Daten und KI vollständig zu verstehen, zu schützen und resilient zu halten, um die sichere Nutzung von KI in großem Umfang zu beschleunigen. Als Marktführer in den Bereichen Datenresilienz und Management der Datensicherheitslage (Data Security Posture Management = DSPM) ist Veeam auf die Konvergenz von Identität, Daten, Sicherheit und KI-Risiko ausgerichtet. Mit Hauptsitz in Seattle und Niederlassungen in mehr als 30 Ländern schützt Veeam weltweit über 550.000 Kunden, darunter 82 % der Fortune-500-Unternehmen. Erfahren Sie mehr unter www.veeam.com oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.

Mehr erfahren: veeam.com