



Datenresilienz ist für heutige Unternehmen ein absolutes Muss

Das Veeam Data Resilience Maturity Model führt Unternehmen auf einen sicheren Weg zu geringeren Risiken



Was und Warum? Data Resilience Maturity Model

Als 2024 Unternehmen daran arbeiteten, ihre Datenresilienz zu verbessern, herrschte in vielen Führungsetagen noch der Irrtum, dass ihre Organisationen bei der Effizienz ihrer Leute, ihrer Prozesse und ihrer Technologien überdurchschnittlich gut aufgestellt seien. Veeam hält diese Einstellung für einen besorgniserregenden Trend und brachte daher ein Konsortium von Branchenexperten zusammen, um den allgemeinen Stand der Dinge in Unternehmen zu ermitteln und einen Konsens zu den Empfehlungen dazu zu entwickeln, wie Unternehmen ihre Datenresilienz verbessern können. Diese Umfrage ergab, dass fast drei Viertel der Unternehmen nicht auf Ausfälle vorbereitet sind. Diese Haltung führte dazu, dass die Unternehmen ihre tatsächliche Resilienz überschätzten und dadurch verwundbar wurden.

Das Veeam Data Resilience Maturity Model (DRMM)

gibt Unternehmen die notwendigen Informationen in die Hand, um sie dabei zu unterstützen, nach Störungen ihre Daten wiederherzustellen, ihre Ressourcen zu optimieren und die Betriebskontinuität sicherzustellen. Während die Ausfallsicherheit von Daten früher nur als Funktion von Backups betrachtet wurde, sind herkömmliche Backup-Strategien angesichts der sich entwickelnden Cyberbedrohungen, des regulatorischen Drucks und der zunehmenden Komplexität von Datenökosystemen unzureichend. Das Erreichen von **echter Datenresilienz** erfordert ein strukturiertes und funktionsübergreifendes Konzept, das IT-, Sicherheits- und Compliance-Bemühungen in eine zusammenhängende Strategie integriert.

Die meisten Unternehmen sind deutlich zu selbstbewusst, was ihre Datenresilienz angeht.

30%+

der Unternehmen sind der Meinung, dass sie über eine größere Resilienz verfügen, als ihre tatsächlich gemessenen Fähigkeiten belegen

74%

sind einem Risiko bei der Datenwiederherstellung ausgesetzt



Der Blueprint für Datensicherung

Das Veeam Data Resilience Maturity Model bietet einen empirischen Rahmen für Unternehmen, um ihre aktuelle Ausfallsicherheit zu bewerten, Lücken zu identifizieren und gezielte Verbesserungen umzusetzen. Veeam hat das DRMM in Zusammenarbeit mit McKinsey, Palo Alto Networks und Splunk entwickelt, wobei die Erkenntnisse von über 500 C-Level Führungskräften in den Entwicklungsprozess eingeflossen sind. Die Ergebnisse zeigen, dass 74 % der Unternehmen nicht einmal die Hälfte der von der Resilienzforschung identifizierten Best Practices anwenden, was zu erhöhten finanziellen, operativen und Compliance-Risiken führt. Das DRMM bietet ein strukturiertes Konzept, um Geschäfts- und Technologiestrategien aufeinander abzustimmen, das Risikomanagement zu verbessern und die Wiederherstellungsfunktionalitäten im großen Maßstab zu erweitern. Durch die Nutzung dieses Modells können Unternehmen von Reaktionen auf Krisen zu proaktiver Resilienz übergehen und so sicherstellen, dass Daten ein Motor für ihr Wachstum bleiben und nicht zum Ausfallfaktor werden.

Forschungsergebnisse zeigen, dass
Spitzenleister in der Regel Folgendes erleben:

7x

Höhere
Wiederherstellungs-
geschwindigkeit (MTTR)

4x

Weniger
Datenverluste (RPO)

3x

Weniger
Ausfallzeiten (RTO)

~10%

Höhere durchschnittliche
Umsatzwachstumsrate

Modell-Dimensionen

Als Veeam sich an die Entwicklung des DRMM machte, ging es zunächst darum, die besten Experten für betriebliche Effizienz zu finden. McKinsey & Company leitete die Bemühungen zur Entwicklung eines strengen, anbieterunabhängigen Frameworks. Dieses Modell wurde entwickelt, um die Fähigkeit eines Unternehmens zu bewerten, die Datenresilienz in drei Kernbereichen zu gewährleisten.



Strategie: Ausrichtung von Geschäftstätigkeit und Risiko

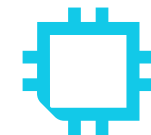
Eine klare Datenstrategie integriert **Geschäftsziele mit Resilienzplanung** und stellt sicher, dass Unternehmen Bedrohungen vorhersehen, Governance durchsetzen und Compliance-Anforderungen einhalten können.



Menschen und Prozesse: Stärkung der Widerstandsfähigkeit durch Ausrichtung und Handeln

Echte Resilienz wird durch befähigte Teams und standardisierte Ausführung erreicht. Durch Investitionen in qualifizierte Talente, eine abgestimmte Führung und klare funktionsübergreifende Protokolle können Unternehmen bei Störungen entschlossen reagieren. Definierte

Arbeitsabläufe und Governance sorgen für Kontinuität, während Zusammenarbeit und Schulung Teams in die Lage versetzen, sich schnell und sicher anzupassen und die Wiederherstellung zu gewährleisten.



Technologie: Die Grundlage der Sicherstellung der Resilienz

Technologie unterstützt die Resilienz in sechs Schlüsselbereichen:

- **Backup:** Sicherer Schutz von Daten, lokal oder in der Cloud.
- **Wiederherstellung:** Agile Wiederherstellung kritischer Systeme, auch im großen Maßstab.
- **Architektur und Portierbarkeit:** Skalierbarkeit in heterogenen und oft hybriden Umgebungen.
- **Sicherheit:** Vorbeugung und vorausschauende Fehlerbehebung gegen Cyberbedrohungen.
- **Reporting und Erkenntnisgewinnung:** Echtzeit-Transparenz und Einblicke, um die Compliance zu unterstützen, die Wiederherstellung zu verbessern und den Betrieb zu optimieren.

Durch die Integration von **Strategie, Menschen, Prozessen und Technologie** können Organisationen **Risiken reduzieren, Wiederherstellungen beschleunigen und ihre langfristige Resilienz stärken.**

Die vier Horizonte der Data Resilience Maturity

Anhand von Umfragedaten zu den Kernkategorien – Strategie, Mitarbeiter, Prozesse und sechs unterstützende Technologiedisziplinen (Backup, Wiederherstellung, Architektur, Sicherheit, Reporting und Intelligence) – hilft das DRMM Unternehmen dabei, ihre Fähigkeit zu bewerten, die Resilienz ihrer IT-abhängigen Geschäftsprozesse zu gewährleisten. Diese Bewertung ordnet Organisationen in jedem Vektor (und insgesamt) einem von vier Horizonten zu, die ihren Reifegrad in Bezug auf die Resilienz sowie die Möglichkeiten zur Verbesserung widerspiegeln:

Grundlegend

Zeigt eine grundlegende Basis mit erheblichen Verbesserungsmöglichkeiten auf.

Mittelstufe

Ein Unternehmen erfüllt die Mindestanforderungen, aber wahrscheinlich mit überwiegend manuellen Prozessen oder Ad-hoc-Ergänzungen. Es gibt immer noch viel, was verbessert werden kann, aber der Organisation fehlt vielleicht das Bewusstsein dafür, was möglich ist und was sich zu tun lohnt.

Fortgeschritten

Die Organisation beginnt, von taktischen zu strategischen Maßnahmen überzugehen und verhält sich in einigen Fällen eher proaktiv als reaktiv. Es hat in bessere Mitarbeiter und Prozesse investiert und einen Weg zu besseren Ergebnissen und Vorteilen eingeschlagen.

Erstklassig

Unabhängig davon, ob es um bestimmte Anwendungsfälle oder die allgemeine Landschaft geht, nutzt ein Unternehmen erstklassige Umgebungen, die zweifellos ebenso sehr das Ergebnis von Menschen und Prozessen sind wie die Technologien, für deren Einsatz es sich entschieden hat.

74%

der Organisationen fallen in die Kategorien „Grundlegend“ und „Mittelstufe“ und weisen wesentliche Verbesserungsmöglichkeiten auf

8%

Self-optimizing
Erstklassig

18%

Mature & Adaptive
Fortgeschritten

30%

Reliable But Limited
Mittelstufe

44%

Reactive & Manual
Grundlegend

Die wichtigsten Vorteile des DRMM

Die Verwendung eines branchenorientierten Modells, das auf unabhängiger Forschung basiert, kann sich als sehr nützlich für Unternehmen erweisen, die ihre Datenresilienz bewerten und stärken wollen. Einige der Vorteile des Reifegradmodells sind:

Schutz der Umsätze

Stärkung der kommerziellen Durchführbarkeit und der Wettbewerbsfähigkeit, indem wir auf die Anforderungen des Marktes reagieren und zuverlässige Produkte bereitstellen.

Kostenoptimierung

Minimierung von Ineffizienzen, IT-Ausgaben und Störfallkosten durch Optimierung von Betrieb, Infrastruktur und Risikomanagement.

Compliance und Risikomanagement

Reduzierung rechtlicher, regulatorischer und geschäftlicher Risiken durch Minimierung von Cybervorfällen, Datenverlusten und den damit verbundenen Kosten.

Markenintegrität und Verbrauchervertrauen

Schutz des Rufs des Unternehmens und des Kundenvertrauens durch Zuverlässigkeit, Verfügbarkeit und eine starke Marktpositionierung.



Erfahren Sie mehr über die [Erfolgsgeschichten](#) von Veeam-Kunden hier.

Fakten

Eine global tätige Bank stärkt ihre Ertragssicherung durch verbesserte Resilienz

Eine weltweit tätige Bank, die die Empfehlungen des Reifegradmodells befolgte, erzielte die folgenden Vorteile:

99,99%

Uptime für kritische Anwendungen

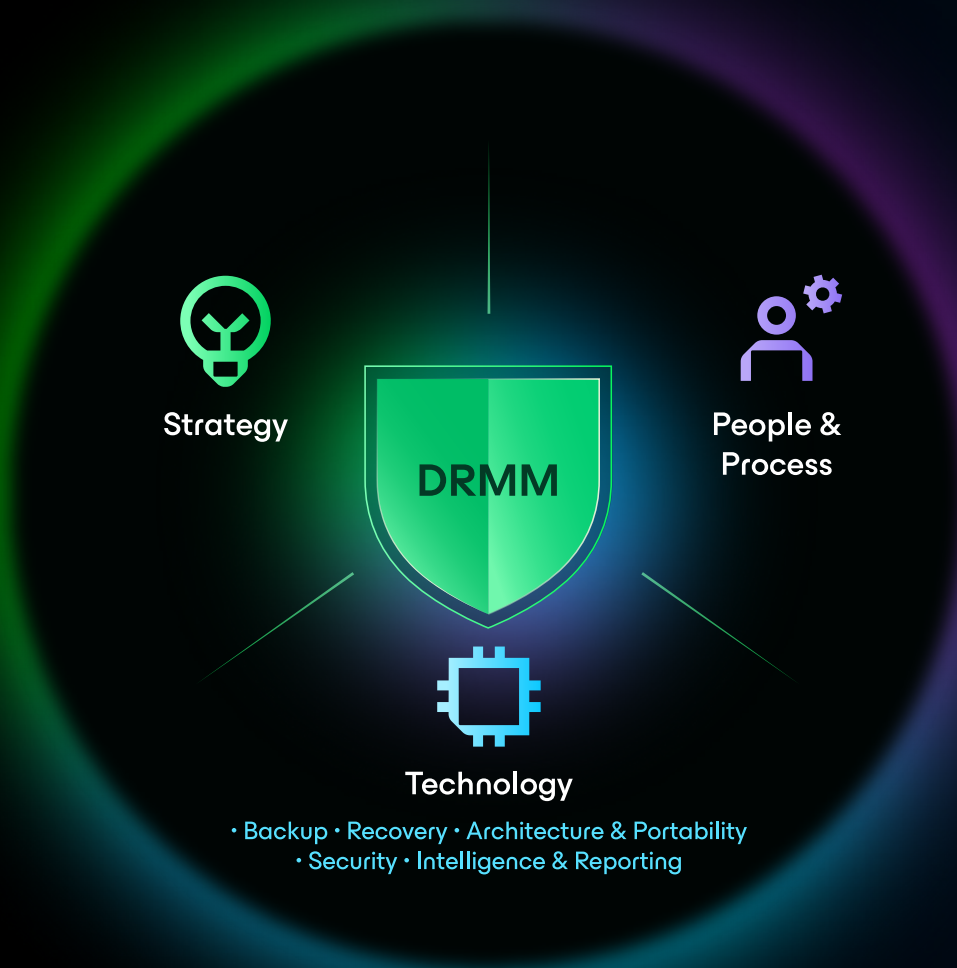
NULL

Cybersicherheitsbedingte Ausfälle in den letzten drei Jahren

\$300K

Einsparungen pro Ausfall durch die Reduzierung der MTTR für kritische IT-Systeme

„Nach oben und nach rechts“ bei der Data Resilience Maturity



Nachdem das DRMM den Stand der Resilienz einer Organisation aufgedeckt hat, gibt es auch die Methoden und Vorteile vor, die sich aus der Verbesserung der Resilienz ergeben, anstatt die Konsequenzen zu tragen, die sich ergeben, wenn die Organisation sich nicht verändert. An diesem Punkt ist wichtig, die erforderlichen Schritte zu unternehmen, um die entscheidenden Veränderungen vorzunehmen, indem Sie sich die KPIs und andere Performance-Kennzahlen genauer ansehen, um einen Einblick in die Unternehmensleistung zu erhalten.

Strategie

Damit eine Strategie zur Datenresilienz wirklich effektiv sein kann, sollten sich Unternehmen die Frage stellen, wie ihre Mitarbeiter (Führungskräfte und Teams), ihre Prozesse (intern und extern) und ihre unzähligen Technologien aufeinander abgestimmt sind, um die gewünschten Ergebnisse zu erzielen.

Menschen und Prozesse

- Wurden die Führungskräfte und Vorstandsmitglieder in die Lage versetzt, die Risiko-Resilienz und das Datenmanagement zu überwachen und entsprechende Aufgaben zu delegieren?
- Wurden für jeden Technologiebereich funktionale Teams gebildet, die auf die Gesamtprozesse und die Strategie der Datenresilienz abgestimmt sind?
- Verlangt die Führung von den Teams, dass sie stets in Bereitschaft sind, um hinsichtlich der Zielvorgaben zu handeln, integrierte Planung, Tabletops und die Vorbereitung auf den Ernstfall umzusetzen?

Technologie

- Gewährleistet die Datensicherungsarchitektur einen umfassenden Schutz im gesamten heterogenen Unternehmen, und sorgt sie für Unveränderlichkeit und die Einhaltung von Richtlinien?
- Ermöglichen die Datenwiederherstellungstechnologien eine flexible Wiederherstellung von heterogenen Schutz- und Produktionsumgebungen auf alternativen Plattformen in großem Umfang?
- Wie umfassend sind die Backup- und Sicherheitstechnologien bei der Gewährleistung effektiver Resilienz in heterogenen hybriden Clouds, einschließlich der Anpassung für die Workload-Portierbarkeit im gesamten Unternehmen?
- **Datensicherheit:** Sind die Datensicherheitstechnologien so in Sicherung und Wiederherstellung integriert, dass proaktive Resilienz oder proaktive Prävention und reaktive Resilienz innerhalb der Richtlinien und Teams aufeinander abgestimmt sind?
- Bieten die Technologien für die Datenberichterstattung angemessene Transparenz, proaktive Prävention und Governance?

Ist die Datenintelligenz in alle Technologiestacks innerhalb des Datenresilienzmodells integriert, und beschleunigt sie diese?

Ein präskriptives Konzept für kontinuierliche Verbesserungen

Das DRMM basiert auf Konzepten, denen einige Führungskräfte jederzeit zustimmen würden, aber erstaunlich wenige Organisationen setzen diese Ideen in ihrer Kernstrategie und ihren Prozessen um.

Keine Panik, Vorbereitung ist alles

Beginnen Sie nicht im Rechenzentrum, sondern im Konferenzraum. Der Schlüssel zur Verbesserung der Resilienz liegt in den meisten Unternehmen oft in der Einbeziehung von mehr Personen (z. B. Stakeholdern und Implementierern) sowie der Implementierung besserer Prozesse. Einige sinnvolle weitere Schritte auf dem Weg zur Weiterentwicklung einer Organisation wären die Implementierung von Prozessen und Praktiken, die über die Grundlagen hinaus proaktives Handeln ermöglichen.

Wer sollte noch einbezogen werden?

Wie bereits erwähnt, geht es bei der Datenresilienz um mehr als „nur die IT“. Daher sollten Unternehmen neben dem CIO und dem CISO eine größere Anzahl von Stakeholdern einbeziehen. Indem das Unternehmen den Kreis der Stakeholder mit Führungsverantwortung, die ein Interesse an der Datenresilienz des Unternehmens haben, deutlich erweitert, z. B. um den Chief Risk Officer und Chief Data Officer, kann es eine umfassendere

Bewertung aus unterschiedlichen Blickwinkeln vornehmen. Dadurch wird sichergestellt, dass die daraus resultierenden Strategien die Bedürfnisse der gesamten Organisation berücksichtigen und so die notwendige Unterstützung für eine bessere Resilienz bieten.

Abstimmung von Datenstrategie, Mitarbeitern, Prozessen und Technologie

Sobald die verschiedenen Interessengruppen im Raum sind, ist das DRMM eine Möglichkeit, sie miteinander bekannt zu machen und sie zur Zusammenarbeit zu bewegen. Während dieser DRMM-Arbeitssitzungen stellen viele Teams fest, dass sie voneinander isoliert arbeiten, und dass manche Mitarbeiter desselben Unternehmens in anderen Abteilungen entweder komplementäre oder kontraproduktive Arbeit leisten. Indem Organisationen alle diese unterschiedlichen Blickwinkel in einem Raum mit einem gemeinsamen Ziel zusammenbringen, können sie ein umfassendes Verständnis der Realität ihrer Situation erlangen und besser darauf vorbereitet sein, sich zwischen verschiedenen Horizonten zu bewegen.



Von der Foundation zur Revolution: Unterstützung der Datenresilienz in Ihrem Unternehmen

Resilienz ist keine einmalige Initiative – dabei handelt es sich vielmehr um einen kontinuierlichen Reifeprozess, der von Unternehmen eine ganzheitliche Bewertung ihrer Datenstrategie, ihrer Mitarbeiter, Prozesse und Technologien erfordert. Ganz gleich, ob Sie grundlegende Praktiken einführen, bestehende Arbeitsabläufe optimieren oder die Grenzen der Innovation verschieben – hier erfahren Sie, wie Sie den nächsten Schritt machen können.



Foundation

Aufbau des zentralen Frameworks für die Resilienz

- Definieren Sie eine klare Datenresilienzstrategie mit engagierter Führung und messbaren Zielen.
- Führen Sie Prozesse für den Umgang mit Vorfällen und Änderungen ein, die die Sicherheits-, IT- und Datenteams aufeinander abstimmen.
- Standardisieren Sie Backup-, Wiederherstellungs- und Sicherheits-Baselines, um das Risiko für alle kritischen Systeme zu minimieren.



Entwicklung

Erweitern Sie die Ausfallsicherheit über die Compliance hinaus zu einem proaktiven, automatisierten und skalierbaren Betrieb.

- Führen Sie jährliche Analysen der Auswirkungen auf die Geschäftstätigkeit durch, um die Risikotoleranz zu verfeinern und Verbesserungen nachzuverfolgen.
- Implementieren Sie funktionsübergreifende Schulungen zur Reaktion auf Vorfälle, einschließlich Simulationen und War-Gaming.
- Automatisieren Sie Data Governance und die Nachverfolgung von Wiederherstellungen, um sicherzustellen, dass die Richtlinien in allen Geschäftseinheiten durchgesetzt werden.



Revolution

Erreichen Sie unternehmensweite Resilienz durch Integration von Intelligenz, Automatisierung und strategischer Führung.

- Ernennen Sie einen Chief Resilience Officer, um ein kohärentes und auf das Unternehmen ausgerichtetes Konzept zu verfolgen.
- Entwickeln Sie eine durchgehende Wiederherstellungsstrategie, einschließlich Multi-Cloud-Workload-Mobilität und KI-gesteuerter Risikobewertung.
- Setzen Sie Echtzeit-Monitoring und prädiktive Analysen ein, um Ausfälle zu erkennen und zu verhindern, bevor sie auftreten.

Jede Organisation wird einen anderen Weg einschlagen. Einige brauchen vielleicht Nachbesserungen, während andere schon für fortgeschrittene Strategien bereit sind. Wo steht Ihr Unternehmen heute, und wie können Sie den nächsten Schritt tun?

Wie **Veeam** Sie unterstützen kann

Veeam war der führende Anbieter, der McKinsey & Partners sowie Experten der IT-Branche zur Entwicklung des DRMM hinzuzog. Das DRMM bietet präskriptive Anleitungen dazu, wie Unternehmen ihre Datenresilienz verbessern können, wobei der Schwerpunkt auf zusätzlichen Funktionalitäten liegt, die die Resilienz einer Organisation verbessern würden. Diese Empfehlungen sind aufgrund der ursprünglichen Natur des Modells anbieterunabhängig. Veeam kann Sie dabei unterstützen, indem es spezifische Empfehlungen aus seinem Produkt- und Serviceportfolio anbietet, die mit den Richtlinien des DRMM übereinstimmen. Bitte wenden Sie sich an Ihren Veeam-Partner oder Ihr Veeam-Kundenteam, um mehr zu erfahren.

➔ Für weitere Informationen zu Veeam Enterprise Solutions [klicken Sie hier.](#)

Über Veeam Software

Veeam®, der Weltmarktführer Nummer eins im Bereich Datenresilienz, ist der Ansicht, dass jedes Unternehmen in der Lage sein sollte, nach einer Unterbrechung des Geschäftsbetriebs mit der Gewissheit und Kontrolle über alle seine Daten weiterzuarbeiten, wann und wo immer es diese benötigt. Veeam nennt dies maximale Ausfallsicherheit, und wir arbeiten kontinuierlich daran, innovative Lösungen zu entwickeln, mit denen unsere Kunden diese Zielvorgabe erreichen.

Veeam-Lösungen wurden speziell für die Datenresilienz entwickelt, indem sie Daten-Backup, Datenwiederherstellung, Datenfreiheit, Datensicherheit und Datenintelligenz bereitstellen. Mit Veeam können Verantwortliche im IT- und Sicherheitsbereich darauf vertrauen, dass ihre Anwendungen und Daten in allen Umgebungen in der Cloud, in virtuellen, physischen, SaaS und Kubernetes sicher und jederzeit verfügbar sind.

Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit hat Veeam mehr als 550.000 Kunden, darunter 74 % der Global 2000-Unternehmen, die auf Veeam vertrauen, um einen zuverlässigen Geschäftsbetrieb zu gewährleisten. Maximale Ausfallsicherheit beginnt mit Veeam.

Weitere Informationen finden Sie unter www.veeam.com/de, oder folgen Sie Veeam auf LinkedIn [@veeam-software](https://www.linkedin.com/company/veeam) und X [@veeam](https://twitter.com/veeam)