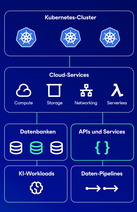
Was tatsächlich schief läuft, wenn moderne Anwendungen ausfallen

Moderne Anwendungen bewegen sich schnell. Fehler breiten sich noch schneller aus. Resilienz hält Ihr Business am Laufen.

Ausfälle moderner Anwendungen sind nicht nur Datenverlust-Events. Wenn etwas schiefgeht, handelt es sich selten um einen Einzelfall. Häufig sind es Abhängigkeitsausfälle, Konfigurationsfehler, Bereitstellungsprobleme, fehlende Transparenz oder andere Faktoren, die Ihnen Schwierigkeiten bereiten.

Was beschädigt wird — und was man dagegen tun kann



WARUM MODERNE ANWENDUNGEN AUSFALLEN

Moderne Anwendungen laufen auf einer verteilten — und nicht auf einer monolithischen — Infrastruktur. Diese verteilten Umgebungen ermöglichen Agilität und kürzere Entwicklungszyklen, bringen jedoch auch neue Komplexität und potenzielle Ausfälle mit sich, die die Grenzen traditioneller Schutzstrategien überschreiten.

Diese Strategien sind auf Ausfälle ausgelegt, die einen Server, aber nur wenige Nutzer betreffen. Dies deckt leider nicht das gesamte Ausmaß moderner Ausfälle ab, deren Auswirkungen sich auf Hunderte von Nutzern und Abhängigkeiten ausweiten können.

EIN NEUER ANSATZ FÜR RESILIENZ

Da moderne Anwendungskomponenten voneinander abhängig sind, bergen Änderungen Risiken. Es ist wichtig, dieses Gefahrenpotenzial zu verstehen.

Mit dem Aufkommen von KI und hybriden Umgebungen ist systemisches Denken unerlässlich. Um optimale Ergebnisse zu erzielen, müssen Unternehmen ihre vollständige Anwendungslandschaft schützen. Der Schutz sollte sich auf Daten, Konfigurationen, Richtlinien, Abhängigkeiten, Metadaten und Kontext erstrecken.

Proaktives Handeln ist ebenfalls wichtig, da Resilienzlücken unentdeckt bleiben können, bis etwas schiefgeht. Tools, die Einblicke zur Überwachung des Systemzustands bieten, können Sie dabei unterstützen, diese Lücken zu erkennen, bevor sie zu einem Problem werden.

Moderne Anwendungen sind häufig mit Betriebsstörungen konfrontiert.

>2/3

der Unternehmen verlieren bei IT-Vorfällen über 300.000 USD pro Stunde.

* PagerDuty-Report „State of AI-First Operations 2026"

54 %

der Opfer von Ransomware haben im vergangenen Jahr Backups genutzt, um verschlüsselte Daten wiederherzustellen.

* Sophos State of Ransomware 2025

2 Millionen USD

pro Stunde betragen die mittleren Kosten schwerwiegender IT-Ausfälle.

* New Relic 2025 Observability Forecast



Zu Störungen kommt es schnell

01
Ausgefallene Abhängigkeit

Anwendungsabhängigkeiten werden unterbrochen.
Ein ausgefallener Service führt zu einer Kaskade verzögerter Transaktionen.

02
Ransomware-Angriff

Ransomware hat Auswirkungen auf moderne Umgebungen.
Angreifer nehmen Backups ins Visier, nicht nur Daten.

03
Fehlkonfiguration

Fehlkonfigurationen verursachen Ausfälle. Kleine Fehler können dazu führen, dass Anwendungen beschädigt sind, aber dennoch als „gesund" angezeigt werden.

04
Fehlgeschlagene Bereitstellungen

Fehlgeschlagene Bereitstellungen führen zu Unterbrechungen des Business.
Fehlerhafte Releases beschädigen Daten und Konfigurationen schnell.

05
Folgewirkungen von Ausfällen

Ausfälle haben Folgewirkungen. Fragmentierte Tools in Kubernetes, VMs und SaaS verschleiern, was tatsächlich geschützt ist.

06
Dateninkonsistenz

Backups können gelingen, selbst wenn Kontext, Metadaten und Abhängigkeiten verloren gehen.

Das Risiko für Ihr Business ist real

Ausfallzeit bedeutet Risiko. Zu den Folgen zählen:

OPERATIV
Mehr Katastrophenbekämpfung, weniger Innovation.

FINANZIELL
Jede Minute Ausfallzeit verursacht Kosten.

SICHERHEIT
Größere Angriffsfläche für Ransomware und Fehler.

STRATEGISCH
Das Vertrauen schwindet auf allen Ebenen.

Moderne Resilienz ist entscheidend

Moderne Resilienz schützt das gesamte Anwendungsökosystem, indem sie Anwendungen, Daten, Governance und Vertrauen genau dann wiederherstellt, wenn Unternehmen es am dringendsten benötigen.

Die entscheidenden Kriterien für eine effektive Resilienz-Lösung

Automatisierte Wiederherstellung
Die Wiederherstellung ist wiederholbar, validiert und fest integriert; sie wird nicht erst mitten im Vorfall improvisiert.

Saubere, konsistente Daten
Schützt Daten, Richtlinien, Metadaten, Konfigurationen und Abhängigkeiten zusammen, nicht einzeln.

Richtlinienvorgaben durchgesetzt
Allgemeine Richtlinien gewährleisten Konsistenz der Workloads über alle Cluster, Clouds und Anwendungstypen hinweg.

Anwendungskontinuität
Stellt die gesamte App und ihren Betriebszustand wieder her, anstatt sie manuell neu aufzubauen.

Compliance-Validierung
Nachweisbare Compliance belegt, dass Richtlinien durchgesetzt werden und die Wiederherstellung wiederholbar ist, statt sich nur auf Annahmen zu verlassen.

Zuverlässiger Betrieb
Schaffen Sie Vertrauen und Zuverlässigkeit. Sie wissen bereits vor dem Eintreten eines Vorfalls genau, was geschützt ist, was gefährdet ist und was wiederhergestellt werden kann.

Moderne Anwendungen verlangen moderne Resilienz.

Entdecken Sie, wie Veeam Kasten Sie dabei unterstützt, Ihre modernen Anwendungen zu vereinfachen, abzusichern und zu optimieren. Entlasten Sie Ihr Team von Komplexität, verringern Sie Risiken und sorgen Sie dafür, dass Ihr Business für jede Herausforderung gewappnet ist, unabhängig davon, was auf Sie zukommt.

Sind Sie bereit, sich näher mit diesem Thema zu befassen? Vertiefen Sie Ihr Wissen mit dem E-Book „Warum moderne Anwendungen nativen Schutz benötigen", um zu erfahren, wie nativer Schutz die Daten, den Kontext, Richtlinien und Abhängigkeiten sichert, die für eine vollständige Wiederherstellung bei Ausfall moderner Anwendungen erforderlich sind.

KASTEN TESTEN

ZUM E-BOOK

© 2026 Veeam Software. Vertrauliche Informationen. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.