veeam Insights

Regionsspezifische Zusammenfassung

des Reports über Datensicherungstrends 2024

Ausgabe für EMEA

1.200 IT-Führungskräfte und -Implementierer in 10 Ländern der Regionen EMEA, APJ sowie Nord-, Mittel- und Südamerika wurden von einem unabhängigen Marktforschungsinstitut zu Herausforderungen und Strategien hinsichtlich der Datensicherung für das Jahr 2024 befragt. Bei allen Befragten handelte es sich um Unternehmen mit mindestens 1.000 Mitarbeitern. Das Whitepaper beschreibt die zehn wichtigsten Aspekte, die Mitglieder der oberen Führungsebene in ihren Organisationen genauer betrachten sollten. Der Hauptteil des Whitepapers enthält aufschlussreiche weltweite Daten; regionale Statistiken für den Raum EMEA sind in der Seitenleiste aufgeführt.

1. Immer größere Lücken zwischen Geschäftsanforderungen und SLAs für die IT

Ein Hauptgrund für eine erneute Beurteilung oder die Beibehaltung von SLAs ist sicherlich die konstante Bedrohung durch Ransomware:

2. Ransomware — keine Frage, ob, sondern wann
3. Cyber-Schutz und ökologisch-soziale Unternehmensführung behindern die Digital Transformation
4. Die meisten Unternehmen erreichen ihre Cyber-/Disaster-Recovery-SLAs nicht

Darüber hinaus stellen viele Unternehmen bei der Umstellung auf cloudorientierte Strategien fest, dass ihre vorhandenen Datensicherungslösungen unzureichend sind:

5. „Hybride" Production-Architekturen zwingen dazu, das Konzept des „Backups" zu überdenken
6. 74 % nutzen Backup-Produkte von Drittanbietern oder Backup-Services für SaaS
7. Die meisten Organisationen nutzen Container, sichern sie jedoch nicht alle

Mit diesem Druck, gleichzeitig Veränderungen zu bewältigen und Risiken zu mindern, stocken Unternehmen ihre Tools auf, was sich aber möglicherweise negativ auf ihre Teams auswirkt:

8. 92 % der Unternehmen planen für 2024 eine Erhöhung ihres Datensicherungsbudgets
9. Über die Hälfte der Unternehmen planen, ihre Backup-Lösung auszutauschen
10. 2024 werden zahlreiche Mitarbeiter abwandern

Vor dem Hintergrund dieser Statistiken und deren Bedeutung schließt dieses Whitepaper mit einigen Diskussionsthemen ab, die die Geschäftsleitung eines Unternehmen mit seinem IT-Team besprechen sollte.

Immer größere Lücken zwischen Geschäftsanforderungen und SLAs für die IT

Auf die Frage, inwiefern sich die Erwartungen des für die Bereitstellung von IT-Services zuständigen Unternehmensbereichs mit der Fähigkeit des IT-Teams, seine SLAs einzuhalten, decken:

- gaben **85 %** der Unternehmen an, dass eine **„Verfügbarkeitslücke"** bestehe zwischen der Erwartung der Organisation, wie resilient ihre IT-Systeme seien und wie gut sie sich nach einem Angriff wiederherstellen ließen, und der tatsächlichen Fähigkeit der IT, die Systeme wiederherzustellen.
- gaben **76 %** der Unternehmen an, dass eine **„Sicherungslücke"** bestehe zwischen dem Datenverlust, den sich das Unternehmen leisten kann, und der Häufigkeit / den Methoden, mit denen das IT-Team die Daten tatsächlich sichert.

85 %

der Unternehmen im Raum EMEA geben zu, dass bei ihnen eine „Verfügbarkeitslücke" besteht

70 %

geben zu, dass bei ihnen eine „Sicherungslücke" hinsichtlich ihrer Daten besteht

Ransomware — keine Frage, ob, sondern wann

Im dritten Jahr in Folge erlitten mindestens drei von vier Unternehmen mindestens einen Ransomware-Angriff in den vorangegangenen zwölf Monaten:

- 25 % gaben an, nicht angegriffen worden zu sein. Doch Vorsicht: Viele Sicherheitsfirmen warnen, dass die Angreifer oft bereits 60 bis 200 Tage zuvor in der anvisierten Umgebung lauern, bevor sie Schaden anrichten oder Lösegeld fordern. Sollte das stimmen, dann könnte es gut sein, dass ein hoher Prozentsatz dieser Umfrageteilnehmer den Angriff einfach noch nicht bemerkt haben.
- 26 % gaben an, im vergangenen Jahr mindestens viermal angegriffen worden zu sein.

66 %

der Unternehmen im Raum EMEA erlitten mindestens einen Angriff im vorangegangenen Jahr

Cyber-Schutz und ökologisch-soziale Unternehmensführung behindern die Digital Transformation

Reaktive oder vorgeschriebene Initiativen (z. B. Compliance) im Vergleich zu proaktiven Ambitionen (Digital Transformation), die von der Geschäftsleitung vorangetrieben werden:

- Hinsichtlich der Frage zu Compliance, Governance und anderen Unternehmensinitiativen, bei denen Behördenvorgaben, geografische Datenhoheit und branchenspezifische Anforderungen zu den häufigsten fünf zählen, **war die wichtigste Initiative die Bildung im Bereich Cybersicherheit, insbesondere im Zusammenhang mit Phishing oder Prävention**.

- Auf die Frage, welche Faktoren die größten Hürden für Initiativen zur Digital Transformation (DX) **seien, wurden Cyberbedrohungen** sowie **Umwelt-, soziale und staatliche Ziele** vor den sonst üblichen Hindernissen wie mangelndes Fachwissen, wirtschaftliche Bedenken und organisatorische Herausforderungen genannt. Dies liegt jedoch nicht an widersprüchlichen Methoden oder Motivationsgründen, sondern vielmehr am Aufwand und den Ressourcen, die von DX- oder IT-Modernisierungsvorhaben abgezogen wurden.

Mit anderen Worten: Die allgegenwärtige Cyberbedrohung erschwert zahlreiche Initiativen, die im Verantwortungsbereich der Führungsebene liegen oder die für den Unternehmenserfolg entscheidend sind.

Die meisten Unternehmen erreichen ihre Cyber-/Disaster-Recovery-SLAs nicht

Angesichts der massiven finanziellen Verluste und des Image-Schadens im Zusammenhang mit großen Krisenereignissen wie Cyberangriffe (Ransomware) sowie Naturkatastrophen und andere standortweite Ausfälle betrachten die meisten Unternehmen Cyberresilienz (CR) mittlerweile als eine wesentliche Säule ihrer allgemeinen Business-Continuity- und Disaster-Recovery-Strategie (BC/DR). Leider erfüllen BC/DR-Pläne (einschließlich Cyberresilienz) oft noch nicht die Anforderungen der meisten SLAs:

- Auf die Frage nach dem letzten großen Cyber-/DR-Test gaben die Umfrageteilnehmer an, dass sich nur **58 %** der Server erwartungsgemäß wiederherstellen ließen. Stellen Sie sich einmal vor, was passiert, wenn zwei Ihrer fünf IT-Systeme nach einem Vorfall nicht wiederhergestellt werden können?
- Auf die Frage, wie lange die IT braucht, um 50 Server wiederherzustellen (was für die befragten Unternehmen keine große Menge an Ressourcen ist), gaben nur 32 % an, dass ihr Unternehmen es binnen einer Geschäftswoche (fünf Tage) schaffen könne.

Aus strategischer Sicht sind diese Schwierigkeiten wahrscheinlich die Folge von zwei weiteren Entscheidungen des IT-Teams und der Führungsebene:

- Im Durchschnitt führen Unternehmen CR/DR-Tests nur alle 8,1 Monate durch. Werden in der Zwischenzeit gravierende Veränderungen am Production-System vorgenommen, ist eine Wiederherstellung im Ernstfall nicht mehr möglich. Das öffnet Cyberkriminellen Tür und Tor, die dann unerkannt über Monate Systeme manipulieren oder beschädigen können, bevor sie überhaupt entdeckt werden.
- Derzeit nutzen 87 % der IT-Teams manuelle Wiederherstellungsmethoden oder Skripte. Diese nicht orchestrierten Aufgaben sind mühsam, sodass IT-Teams noch länger zögern, die Systeme zu testen. Auch werden die Tests und die eventuell notwendigen Wiederherstellungen dadurch uneinheitlich.

Innerhalb von EMEA waren nur

58 %

der Server erwartungsgemäß wiederherstellbar

„Hybride“ Production-Architekturen zwingen dazu, das Konzept des „Backups“ zu überdenken

Im zweiten Jahr in Folge lauten die wichtigsten Aspekte für „Enterprise-Backup“-Lösungen **Zuverlässigkeit** und der **Schutz cloudbasierter Workloads** (IaaS und SaaS). Das ist jedoch problematisch für Unternehmen, die noch mit älteren Datensicherungslösungen auf Basis von Rechenzentren arbeiten. Im Jahr 2024 wird fast die Hälfte aller Workloads über Cloud-Hosts ausgeführt (**45 %**). Demgegenüber stehen rechenzentrenbasierte Workloads mit **28 %** auf physischen Servern und **27 %** auf virtuellen Maschinen.

Wenn Unternehmen Workloads von einer Plattform oder Cloud zur anderen übertragen, wird es für IT-Teams immer schwieriger, ihre SLAs einzuhalten, da sie noch immer veraltete Backup-Lösungen nutzen, die keine angemessene Sicherung von in der Cloud gehosteten Workloads bieten. Das gilt insbesondere für SLAs mit cloudbasierten Angeboten wie Microsoft 365/Salesforce (SaaS) oder Containern.

In EMEA setzen sich Hybridarchitekturen folgendermaßen zusammen:

29 %
physische Server

28 %
virtuelle Maschinen

43 %
in der Cloud gehostete Server

74 % nutzen Backup-Produkte von Drittanbietern oder Backup-Services für SaaS

Die meisten Unternehmen haben erkannt, dass sie auch SaaS-Daten sichern müssen. In den frühen Anfängen von SaaS gingen viele Unternehmen fälschlicherweise davon aus, dass SaaS-Backups nicht nötig seien, da SaaS-Plattform von Natur aus robust sind. Deshalb weisen SaaS-Anbieter ihre Kunden immer wieder darauf hin, dass jeder Abonnent selbst für das Backup seiner Daten in SaaS verantwortlich ist — z. B. im Rahmen des Microsoft Shared Responsibility Model.

- Mittlerweile hat sich SaaS so weit etabliert, dass zentrale IT-Anforderungen wie rollenbasierter Zugriff, Zero Trust und Backup-/Aufbewahrungspflichten wieder integriert werden.
- Teil dieses Reifeprozesses sind auch Production-Plattformen, die eigene Backup-Dienstprogramme enthalten, wie das M365-Backup-Tool, das Salesforce-Dienstprogramm oder die mittlerweile Jahrzehnte alten Dienstprogramme Windows Backup und VMware Backup. Glücklicherweise sichern 2024 **74 %** der Befragten ihre Microsoft 365-Daten mit Backup-Produkten oder -Services von Drittanbietern. Lediglich 3 % verlassen sich noch auf den Papierkorb und 4 % glauben, dass Backups nicht nötig sind.

79 %
der Unternehmen in EMEA sichern Microsoft 365-Daten

Die meisten Organisationen nutzen Container, sichern sie jedoch nicht alle

Für das Jahr 2024 gaben 59 % der Großunternehmen an, dass sie Container in ihrer Production-Umgebung nutzen, und 37 % sind mit der Einführung oder der Planung von Containern beschäftigt. Das belegt die These, dass Container nicht erst „im Kommen, sondern bereits angekommen" sind. Leider nutzen aber nur 25 % der Unternehmen eine Backup-Lösung, die speziell auf Container ausgelegt ist. Die übrigen Unternehmen (71 %) sichern entweder nur die zugrunde liegenden Speicher-Repositories oder die Datenbankinhalte, wobei keins von beiden gewährleistet, dass sich die Anwendungen und Services nach einem Ausfall wieder ausführen lassen oder dass auch nur ein simpler Import-/Konfigurationsfehler rückgängig gemacht werden kann.

92 % der Unternehmen planen für 2024 eine Erhöhung ihres Datensicherungsbudgets

2024 werden die Datensicherungsbudgets vermutlich um **6,6 %** steigen. Dies ist das zweite Jahr, in dem laut der Umfrage die Ausgaben für Datensicherung stärker steigen werden als das Wachstum der gesamten IT-Ausgaben. Im Vergleich dazu ging Gartner von einem Wachstum der gesamten IT-Ausgaben von 4,3 % aus[1] und IDC prognostizierte einen Ausgabenanstieg um 5,4 % im Bereich Datensicherung[2]. Den größeren Anteil dieser steigenden IT-Budgets werden Investitionen in die Datensicherung ausmachen, vermutlich um sich noch besser gegen Cyberangriffe zu wappnen, aber auch, um die sich verändernde Production-Umgebung zu berücksichtigen, die andere Datensicherungsansätze erfordert.

In EMEA werden die Datensicherungsbudgets für 2024 vermutlich angehoben um

6,0 %

Über die Hälfte der Unternehmen planen, ihre Backup-Lösung auszutauschen

54 % der Unternehmen gehen davon aus, dass sie in den nächsten zwölf Monaten auf eine andere Backup-Lösung umsteigen. Während viele erwarten, dass der Backup-Markt ausgereift und daher stabil ist, zeigen die halbjährlichen IDC-Berichte zum Marktanteil für den Markt für Datensicherung und -replikation[3] seit Jahren, dass dies ein Irrtum ist. In den letzten zwei Jahren gaben bei der Umfrage über die Hälfte der Teilnehmer (2024: 54 %, 2023: 57 %) an, dass sie „mit hoher Wahrscheinlichkeit" oder

49 %

der Unternehmen in EMEA planen, 2024 auf eine andere Backup-Lösung umzusteigen

[1] https://www.gartner.com/document/4714599

[2] https://www.idc.com/getdoc.jsp?containerId=US51037523

[3] IDC: Marktanteil 2023 H1

„definitiv“ ihre Backup-Lösung austauschen werden. Es kann natürlich auch sein, dass die Unternehmen von der „Selbstverwaltung ihrer eigenen lizenzierten Software“ zu einem „Abonnement eines Managed-Backup-as-a-Service-Angebots“ wechseln, ohne jedoch die Anbietertechnologie zu wechseln. Der Umstieg auf Managed Services würde für viele Unternehmen eine Aufwertung ihrer gerade so ausreichenden Backups auf zuverlässig wiederherstellbare Strategien bedeuten.

2024 werden zahlreiche Mitarbeiter abwandern

47 % der Umfrageteilnehmer gaben an, in den nächsten zwölf Monaten den Arbeitgeber wechseln zu wollen. Ein wesentlicher Sorgenpunkt für viele Befragten waren die *„Auswirkungen eines Cyberangriffs oder einer anderen Katastrophe“* auf das Image ihrer Tätigkeit. Darüber hinaus befürchteten viele Teilnehmer auch negative Folgen für ihren beruflichen Aufstieg, ihre Weiterbildung oder die Wahrnehmung, ob sie für das Unternehmen von Bedeutung sind. Diese Marktverschiebung ist Herausforderung und Chance zugleich:

- Es ist Aufgabe der Führungsebene, die vorhandenen Datensicherungsfachkräfte zu halten, um sich angemessen vor Cyberangriffen zu schützen und auf andere Katastrophen vorbereitet zu sein. Ein Verlust dieser Talente würde einen erheblichen Nachteil bedeuten, wenn der unvermeidliche Ernstfall eintritt.
- Es ist wichtig, Datensicherungsfachkräfte anzuwerben; mit neuen Fähigkeiten hinsichtlich einer besseren Datensicherung zum Schutz vor Cyberangriffen und mit neuen Kenntnisse zum Schutz moderner Production-Workloads in Clouds wie Microsoft 365, Kubernetes-Containern oder anderen IaaS/PaaS-Architekturen.

Eine bewährte Methode, mit der Unternehmen das Risiko eines Arbeitskräfte- oder Fachkräftemangels im Bereich der Datensicherung verringern können, ist die Beauftragung von **Managed-BaaS- oder -DRaaS-Anbietern**. Managed Serviceprovider bieten nicht nur aktuelles, tiefgreifendes Fachwissen, Überwachung des IT-Betriebs und primären technischen Support. Sie geben Unternehmen auch die Möglichkeit, dass einige ihrer internen Datensicherungsexperten nicht mehr einfach nur Prozesse „ausführen“, sondern das ausgelagerte Monitoring und Management der Datensicherung überwachen.

39 %

der Umfrageteilnehmer in EMEA gaben an, den Arbeitgeber wechseln zu wollen

Was können Sie tun?

Zum Abschluss noch einige Empfehlungen zu zentralen Fragen, die hochrangige Führungskräfte mit Verantwortung für die Bereiche Datensicherung oder Bereitstellung von IT-Services mit den IT-Implementierungsteams ihres Unternehmens klären sollten:

- Wie sicher können wir sein, dass wir unsere Daten von einem Cyberkriminellen zurückholen können, wenn dieser bereits seit mindestens drei Monaten in unserer Umgebung lauert?
- Wie schnell können wir 10 % unserer Serverfarm wiederherstellen, wenn sie mit Ransomware infiziert ist oder ein Krisenereignis die Server am Standort unbrauchbar macht?
- Wie oft testen wir diese Funktionalitäten?
- Wie beurteilen wir erfolgreiche Tests?
- Welche Prozesse haben wir für die kontinuierliche Verbesserung unserer Cyberresilienz oder BC/DR-Vorbereitung?
- Sichern wir unsere Cloud-Hosts? Unsere SaaS-Anwendungen? Unsere containerbasierten Umgebungen?

Informationen zu den Autoren

Jason Buffington
VP, Market Strategy
@JBuff

Dave Russell
VP, Enterprise Strategy
@BackupDave

Julie Webb
Director, Market
Research & Analysis

Über Veeam Software

Veeam®, weltweit marktführender Anbieter von Lösungen für die Datensicherung und die Wiederherstellung nach Ransomware-Angriffen, hat es sich zum Ziel gesetzt, jedem Unternehmen nach einem Datenausfall oder -verlust nicht nur wieder auf die Beine zu helfen, sondern auch dessen zukünftigen Erfolg zu unterstützen. Veeam ermöglicht Unternehmen einen zuverlässigen Geschäftsbetrieb durch Datensicherheit, Datenwiederherstellung und Datenfreiheit in Hybrid-Cloud-Umgebungen. Die Veeam Data Platform ist eine zentrale Lösung für cloudbasierte, virtuelle, physische, SaaS- und Kubernetes-Umgebungen, sodass Führungskräfte der IT- und Sicherheitsteams darauf vertrauen können, dass ihre Anwendungen und Daten zuverlässig geschützt sind. Veeam hat seinen Hauptsitz in Columbus, Ohio, und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit hat Veeam mehr als 450.000 Kunden, darunter 73 % der Global 2000-Unternehmen, die Veeam den zuverlässigen Geschäftsbetrieb ihres Unternehmens anvertrauen. Umfassende Resilienz beginnt mit Veeam. Weitere Informationen finden Sie unter www.veeam.com, auf LinkedIn unter @Veeam-Software und auf X unter @Veeam.

Weiteres Material zu dieser Umfrage können Sie hier herunterladen.

Bei Fragen zu dieser Studie oder zur Verwendung der Ergebnisse senden Sie bitte eine Nachricht an StrategicResearch@veeam.com.