www.insider-research.de

INSIDER RESEARCH

Notwendige Optimierungen bei der Datensicherung

Zuverlässiges Backup-Management
Maßnahmen für ein erfolgreiches Restore
Verbesserungen für das Disaster Recovery

Powered by:

NOVASTOR

Inhaltsverzeichnis

Powered by:

NOVASTOR

NovaStor GmbH
Neumann-Reichardt-Straße 27-33
22041 Hamburg
Web www.novastor.de
E-Mail kontakt@novastor.de
Telefon +49 40 638 09 0

Vogel IT-Medien GmbH
Max-Josef-Metzger-Str. 21
86157 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail zentrale.vit@vogel.de
Web www.insider-research.de
Geschäftsführer: Tobias Teske, Günter Schürger
Erscheinungstermin: Januar 2025
Titel: your123/stock.adobe.com

Das Ziel lautet: Zuverlässiges Management in der Datensicherung und -wiederherstellung

Laut aktueller Umfrage von Storage-Insider und NovaStor nennt jeder zweite Befragte die Handhabung und Verwaltung der Datensicherung als Herausforderung.

Von Oliver Schonschek, News-Analyst bei Insider Research

Offensichtlich braucht es ein besseres Management der Datensicherung. Ein besseres Datensicherungsmanagement erleichtert die strategische Einbindung in die Unternehmens-IT, vermeidet unnötige Aufwände und Kosten und hilft bei der notwendigen Transparenz in der Datensicherung. Wie aber lässt sich das Backup-Management optimieren?

Die Umfrage zeigt: Hier sind die Lücken im Datensicherungs-management, das sollte geändert werden

Die Auswertung der Datensicherungsumfrage von Insider Research im Auftrag von Storage-Insider zeigt konkreten Handlungsbedarf im Management der Backups. Im Folgenden werden die erkannten Problem-stellen erläutert und Empfehlungen zur Behebung gegeben.
Die Ergebnisse der großen Datensicherungsumfrage können Sie in diesem eBook ab Seite 10 lesen.

Bild: Murrstock/adobe.stock.com

Aktueller Status im Management der Backups (laut Umfrage)

Bei rund 30 Prozent der Befragten gibt es **keine Backup-Software unter Wartung**, bei etwa 42 Prozent **fehlt der Notfallplan**, fast 62 Prozent geben zu, **kein regelmäßiges Reporting zur Datensicherung** vorgesehen zu haben, und bei etwa 73 Prozent gibt es **keine expliziten Verantwortlichkeiten und Zuständigkeiten für die Datensicherung**, da ein dediziertes Backup-Team fehlt.

Obwohl laut Umfrage (Mehrfachantworten waren möglich) die Handhabung und Verwaltung die größte Herausforderung bei der Datensicherung ist, verzichten die meisten Befragten auf eine externe Unterstützung. 90 Prozent machen die **Datensicherung im Eigenbetrieb**. Das Outsourcing der Datensicherung an ein externes Systemhaus erscheint eher als Ausnahme. Bei zwölf Prozent hat ein Systemhaus **einzelne Dokumente** wie das Backup-Konzept erstellt, bei 14 Prozent kümmert sich das Systemhaus **nur um die Backup-Software**, bei 16 Prozent hat ein Systemhaus die Datensicherung **aufgesetzt**.

Empfehlungen zur Optimierung des Managements der Datensicherung

Datensicherungslösungen müssen einwandfrei funktionieren. Eine fehlende Wartung für die eingesetzte Backup-Lösung stellt ein hohes Risiko dar. Das Backup-Konzept muss deshalb eine **laufende und professionelle Wartung für die Backup-Lösung** vorschreiben.
Sich nicht auf den Ernstfall vorzubereiten, kann im Notfall (IT-Störungen, Systemausfälle, Cyberattacken) schwerwiegende Konsequenzen haben, darunter hohe Folgeschäden, aber auch Sanktionen wegen Compliance-Verstößen. **Ein Notfallplan ist deshalb Pflicht.**
Um die Datensicherung zuverlässig unter Kontrolle zu haben und auch um Rechenschaftspflichten aus der Compliance einhalten zu können, darf ein **vollständiges und verständliches Reporting** zu den Backups nicht fehlen. Zudem muss es **klare Rollen, Aufgaben und Zuständigkeiten im Bereich Datensicherung** geben. Können diese nicht intern übernommen werden, lautet die Option Outsourcing.

Das Backup- und Datenwiederherstellungskonzept muss **alle Aufgaben und Schritte der Datensicherung** benennen und mit Verantwortlichkeiten versehen. Können bestimmte Maßnahmen nicht intern übernommen werden, lautet die **Option Outsourcing**. Wichtig ist dabei, dass alle Aufgaben **professionell** übernommen werden, das gilt intern wie auch extern.

Aktueller Status im Management der Backups (laut Umfrage)	Empfehlungen zur Optimierung des Managements der Datensicherung
Jeder vierte Befragte sagt, dass das eigene Unternehmen oder die eigene Behörde die Backup-Software **seit mehr als zehn Jahren** einsetzt. **Mindestens vier Jahre** im Einsatz ist die Backup-Lösung bei etwa Dreiviertel der Teilnehmerinnen und Teilnehmer.	Denkt man an die hohe Dynamik der IT, impliziert das, dass die Backup-Lösung fortlaufend mit vielen neuen Anforderungen und Bedürfnissen umgehen können muss. Andernfalls droht bei einer langen Nutzungsdauer, dass die Backup-Lösung bestimmte, neue IT-Infrastrukturen nicht unterstützen kann. Deshalb gilt es, den **Funktionsumfang der eingesetzten Backup-Lösung** zu hinterfragen. Lücken in der Datensicherung darf es nicht geben, es müssen sich **alle genutzten IT-Infrastrukturen** auch in das Backup einbeziehen lassen.
Trotz der Herausforderungen bei der Datensicherung und dem erkannten Bedarf für Verbesserungen denkt mit 56 Prozent die Mehrheit der Befragten nicht daran, den Anbieter für ihre Backup-Lösung zu wechseln, oder sie hat **noch nicht darüber nachgedacht, ob ihre Datensicherung auch allen Anforderungen gerecht wird**.	Können Anforderungen an die Datensicherung von der gegenwärtigen Lösung im Backup-Bereich nicht erfüllt werden, muss an eine Veränderung gedacht werden. Ein **Wechsel im Bereich Backup** sollte nicht ausgeschlossen werden, das wäre eine riskante Einstellung.
Bei der Mehrheit stehen deshalb **erst einmal keine Veränderungen bei der Datensicherung** an. 21 Prozent haben an Veränderungen gedacht, diese **aber erst einmal verschoben**. Zwölf Prozent denken über mögliche Lücken bei ihrer Datensicherung nach, weitere zwölf Prozent sind bereits in der Planung für einen möglichen Wechsel.	Stellt man Lücken im Management der Datensicherung fest, sollte ein Wechsel der Backup-Lösung geplant werden. **Dabei drängt die Zeit**, denn die Lücken in der Datensicherung können im Ernstfall zu Datenverlust, Produktionsstillstand, wirtschaftlichen Schäden und Sanktionen wegen Compliance-Verstößen führen. Vorgaben wie die NIS2-Richtlinie fordern explizit Maßnahmen zur Gewährleistung einer Cyber-Resilienz (Widerstandskraft und Belastbarkeit bei Cyber-Vorfällen). So nennt NIS2 unter den geforderten Maßnahmen für das Risikomanagement konkret „Bewältigung von Sicherheitsvorfällen, Aufrechterhaltung des Betriebs, Backup-Management, Wiederherstellung nach einem Notfall, Krisenmanagement“.

Nicht vergessen: Entscheidend ist die erfolgreiche Wiederherstellung

Ohne zuverlässige Wiederherstellung kann ein Backup keine wirkliche Hilfe sein, denn alleine ein Backup reicht nicht für die zuverlässige und schnelle Wiederaufnahme des Betriebs.

Von Oliver Schonschek, News-Analyst bei Insider Research

Laut der aktuellen Umfrage besteht ein dringender Handlungsbedarf, um die Schäden im Ernstfall so gering wie möglich zu halten. Was ist nun zu tun?

Die Umfrage zeigt: Hier sind die Lücken in der Wiederherstellung (Restore), das sollte geändert werden

Die Auswertung der Datensicherungsumfrage von Insider Research zeigt konkreten Handlungsbedarf im Management des Restores (Wiederherstellung). Im Folgenden werden die erkannten Problemstellen erläutert und Empfehlungen zur Behebung gegeben.
Die Ergebnisse der großen Datensicherungsumfrage können Sie in diesem eBook ab Seite 10 lesen.

Bild: Parradee/adobe.stock.com

Notwendige Maßnahmen für ein erfolgreiches Restore

Aktueller Status im Restore (laut Umfrage)	Empfehlungen zur Optimierung des Restores
43 Prozent der Befragten **testen die Wiederherstellung nicht**.	Ob die Backups zur Wiederherstellung geeignet sind, ob die Prozesse im Restore wie gewünscht laufen und ein Betrieb schnell wiederaufgenommen werden kann, darf nicht dem Zufall überlassen werden. Die **Backups und die Restore-Prozesse müssen regelmäßig und realistisch getestet** werden.
Zwölf Prozent erklären, ihnen **fehlt die Transparenz** im Bereich Wiederherstellung.	Eine Wiederherstellung muss so erfolgen, dass der **Betrieb schnell und umfassend wieder aufgenommen** werden kann. Dazu bedarf es der **Transparenz bei den Backups und bei den Tests der Wiederherstellung**. Erkannte Probleme und Lücken, die die umfassende und zeitnahe Wiederherstellung behindern würden, müssen behoben werden.
Bei acht Prozent **fehlt es an Ressourcen** für die Notfalltests.	Ein Mangel an Ressourcen darf nicht dazu führen, dass es keine Notfalltests gibt. Kommt es zu einem Vorfall (Cyberattacke, IT-Ausfall), werden ebenfalls **professionelle Ressourcen** benötigt. Kann dies intern nicht geleistet werden, sollte die **Option Outsourcing** gewählt werden.

Für den Notfall gerüstet sein, auch mit externer Hilfe

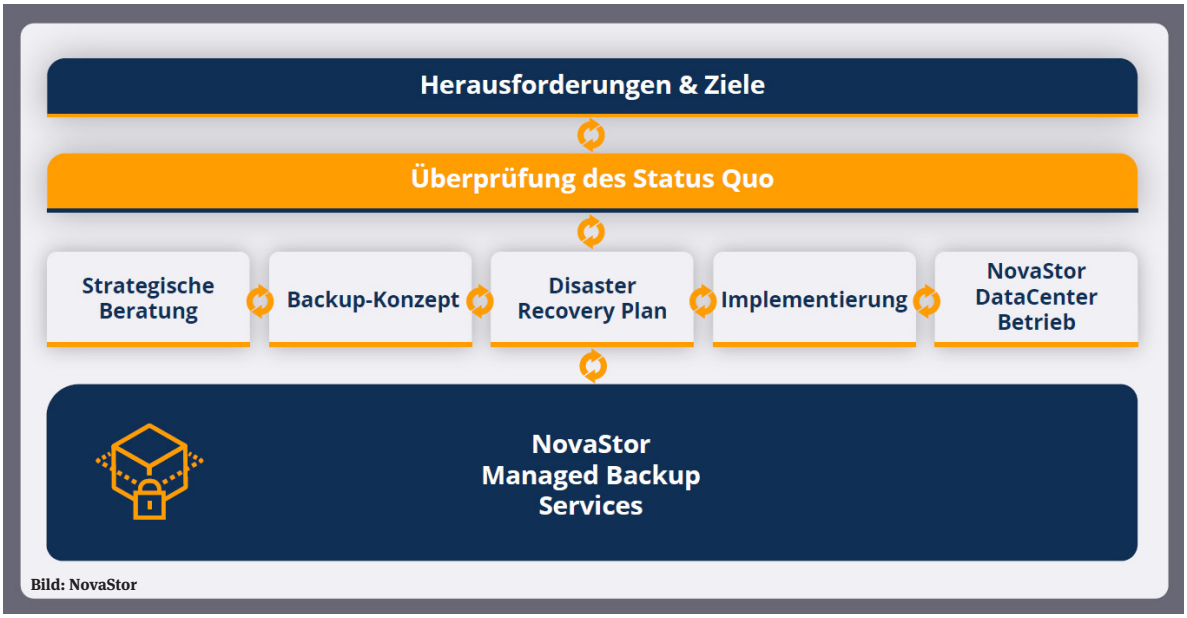
Im Ernstfall kommt es auf eine professionelle Vorbereitung und Reaktion an. Je schneller und vollständiger die Wiederherstellung gelingt, desto geringer sind die Folgeschäden.

Von Oliver Schonschek, News-Analyst bei Insider Research

Doch viele Umfrageteilnehmende haben Lücken in ihrem Notfall-Management, sie erhoffen sich Hilfe von dem Anbieter der Datensicherungslösung. Diese ist aber nicht selbstverständlich. Darauf sollte man deshalb achten.

Die Umfrage zeigt: Hier sind die Lücken im Notfall-Management, das sollte geändert werden

Die Auswertung der Datensicherungsumfrage von Insider Research im Auftrag von Storage-Insider und NovaStor zeigt konkreten Handlungsbedarf im Notfall-Management. Im Folgenden werden die erkannten Problemstellen erläutert und Empfehlungen zur Behebung gegeben.



Komplettlösungen sind gefragt: 47 Prozent der Umfrageteilnehmer haben Interesse an einem Komplettpaket mit Datensicherungslösung, Strategie und Konzept. Beispielsweise bietet NovaStor einen ganzheitlichen Lösungsansatz für die Planung und den Betrieb einer Backup-Umgebung, die auch optimal auf den IT-Notfall vorbereitet.

Aktueller Status im Notfall-Management (laut Umfrage)	Empfehlungen zur Optimierung des Notfall-Managements
Weniger als drei von zehn der Befragten erwarten nur die Backup-Software von dem Hersteller der Datensicherungslösung. Über die Hälfte wünscht sich vom Anbieter (!) **Erreichbarkeit und Hilfe im Notfall**, gefolgt von der **Einhaltung deutscher Gesetze** und einem **guten Preismodell**.	Wenn Unternehmen, Behörden und Systemhäuser in der Umfrage angeben, dass sie im Notfall Hilfe und Erreichbarkeit vom Anbieter der Datensicherungslösung erwarten, dann sollte dies auch ein **Kriterium bei der Anbieterauswahl** sein, denn dies ist keine Selbstverständlichkeit.
47 Prozent haben Interesse an einem **Komplettpaket** mit Datensicherungslösung, Strategie und Konzept.	Der Wunsch nach Einhaltung deutscher Gesetze und ein gutes Preismodell sollten ebenfalls bei der **Anbietersuche** entsprechend priorisiert werden. **Komplettpakete** können die Datensicherung deutlich vereinfachen, doch nicht jede Lösung ist als ein solches Paket zu bekommen. Hier sollte also ebenfalls bei der **Lösungssuche** darauf geachtet werden.
Wenn über einen **Wechsel des Anbieters** für die Datensicherungslösung nachgedacht wird, dann sind es für 39 Prozent **technische Aspekte**, die sie dazu bewegen, für 28 Prozent geht es um die **Kosten**, 13 Prozent suchen mehr **Transparenz**, zwölf Prozent sind unzufrieden mit ihrem gegenwärtigen Anbieter, fünf Prozent nennen Ressourcenmangel als Grund für einen möglichen Anbieterwechsel.	Wenn hohe Anforderungen an den Anbieter gestellt werden, sollte der **gegenwärtige Anbieter auch auf die Probe gestellt** werden. Ein Anbieterwechsel kann positive Veränderungen möglich machen, bei Backup, Restore und Disaster Recovery, aber auch im technischen Bereich, bei den Kosten, dem Reporting und den Nachweisen.

Die große Datensicherungsumfrage von Storage-Insider und NovaStor

Backup | Datensicherung und Restore | Disaster Recovery

Eine Umfrage unter IT-Entscheiderinnen und IT-Entscheider im DACH-Raum (Behörden, Unternehmen des Mittelstandes, Systemhäuser, die den Mittelstand bedienen)

INSIDER RESEARCH

Studiensteckbrief

Herausgeber: Vogel IT-Medien
Durchführung: Insider Research
Studienpartner: NovaStor und Storage-Insider
Teilnehmergenerierung: per E-Mail
Anzahl Teilnehmende: 143

Zielgruppe: Behörden, Unternehmen des Mittelstandes, Systemhäuser, die den Mittelstand bedienen (DACH-Raum)
Methode: Online-Fragebogen
Autor des Studienkommentars: Oliver Schonschek, News-Analyst bei Insider Research

Management Summary

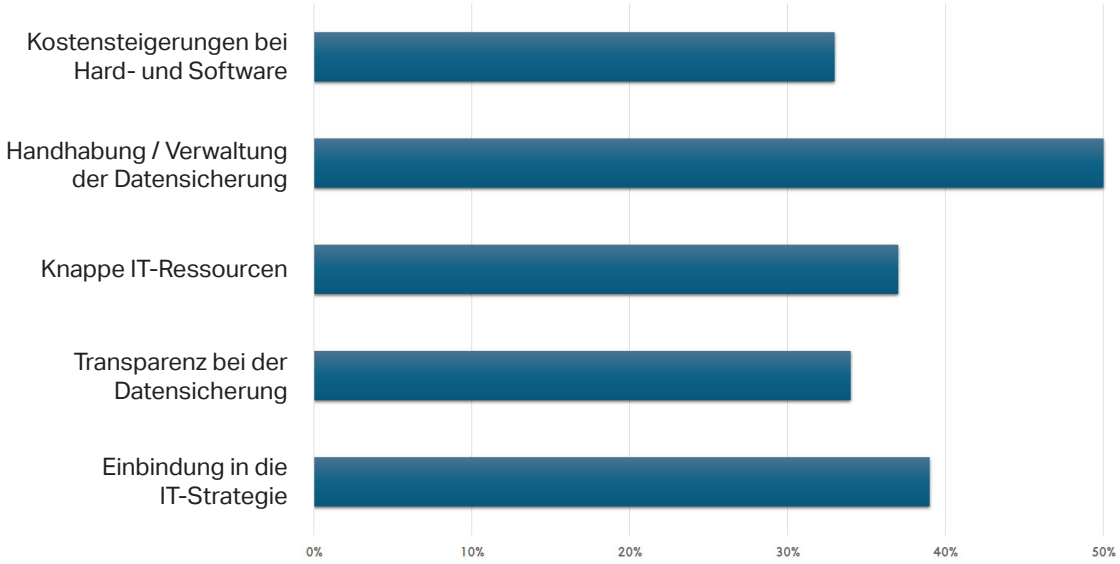
Diese Studie untersucht, welche Herausforderungen Mittelstandsunternehmen, Behörden und Systemhäuser im DACH-Raum bei der Gewährleistung der Datensicherung sehen. Die erkannten Herausforderungen werden mit dem aktuellen Status der Datensicherung bei den Befragten verglichen und der Handlungsbedarf wird abgeleitet.

Die Umfrage belegt, dass es gerade bei dem Management der Datensicherung und der Wiederherstellung Schwierigkeiten gibt, die Unternehmen aber mehrheitlich versuchen, alleine ihre Datensicherung in den Griff zu bekommen. Die Nutzung von Systemhäusern erfolgt – wenn überhaupt – nur für Teilaufgaben, dafür erhoffen sich die Unternehmen aber Hilfe vom Anbieter der Backup-Lösung, wenn es zum Ernstfall kommt. Gleichzeitig suchen die meisten Befragten keinen neuen Anbieter, wenn, dann sind es technische Gründe, gefolgt von den Kosten. Trotz des Handlungsbedarfs, den die Umfrage aufzeigt, arbeiten die Befragten aber mehrheitlich noch nicht an Veränderungen im Bereich Datensicherung.

Es ist also höchste Zeit, den Bedarf konkret zu erkennen und die Datensicherung zu optimieren. Dabei will diese Studie helfen.

Fragen, Ergebnisdiagramme und Kommentierung

1. Frage: Die Datensicherung hat heute einen sehr hohen Stellenwert. Wo sehen Sie (in Ihrer Organisation) Herausforderungen?



Jeder zweite Befragte sieht in der Handhabung und der Verwaltung der Datensicherung eine Herausforderung.

Kommentierung

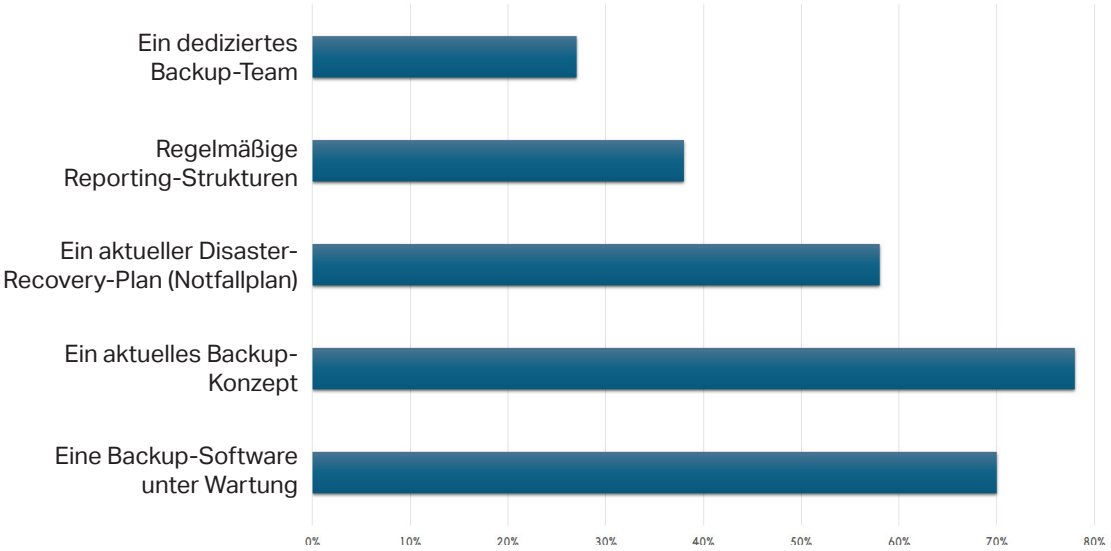
Datensicherung gehört zu den zentralen Elementen des IT-Managements und der IT-Sicherheit. Das gilt nicht erst seit der massiven Zunahme an Ransomware-Attacken, mit denen versucht wird, geschäftsrelevante Daten kriminell zu verschlüsseln und für die Entschlüsselung Lösegeld zu erpressen.

Die Verfügbarkeit der Daten ist eines der zentralen Schutzziele in der IT, die Datensicherung ein Fundament der Maßnahmen für deren Gewährleistung. Trotzdem ist es vielen der befragten Unternehmen noch nicht gelungen, die Datensicherung nicht mehr als Herausforderung zu sehen, sondern tragfähige Lösungen dafür einzusetzen.

Ein Drittel oder mehr der Befragten sehen in der strategischen Einbindung der Datensicherung, in den knappen IT-Ressourcen, in der unzureichenden Transparenz bei der Datensicherung und in den Kostensteigerungen für Hardware und Software eine Herausforderung.

Jeder zweite Befragte nennt aber die Handhabung und Verwaltung der Datensicherung als Herausforderung. Offensichtlich braucht es ein besseres Management der Datensicherung. Dieses würde auch bei den anderen als Herausforderung genannten Faktoren helfen: Ein besseres Datensicherungsmanagement erleichtert die strategische Einbindung, vermeidet unnötige Aufwände und Kosten und hilft bei der notwendigen Transparenz in der Datensicherung.

2. Frage: Welche Komponenten einer Datensicherungslösung sind in Ihrer Organisation vorhanden?



Die größten Lücken in der Datensicherung bestehen bei den notwendigen Ressourcen, dem Reporting und dem Notfallplan.

Kommentierung

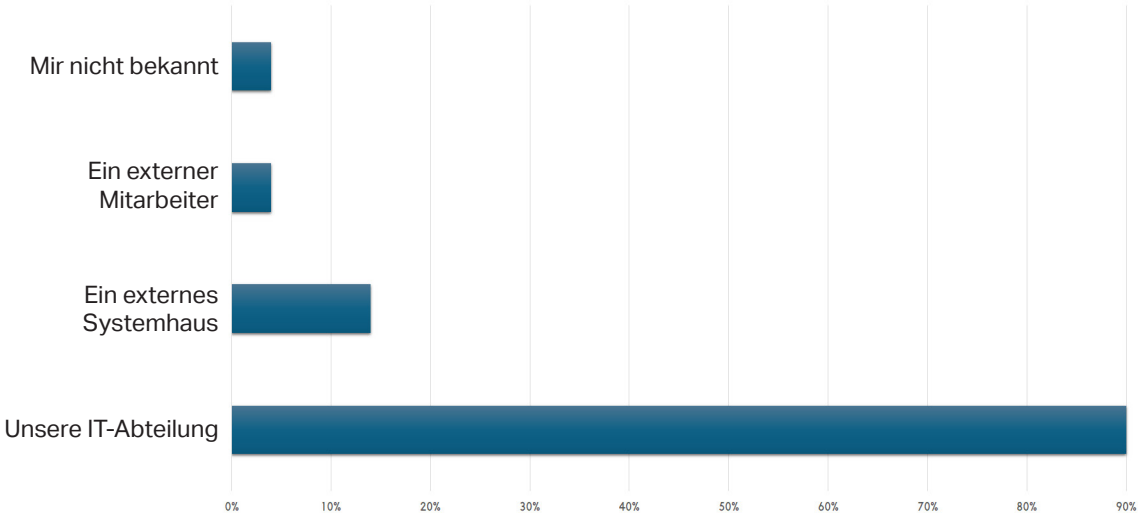
Ilmmerhin 78 Prozent der Befragten erklären, dass sie ein aktuelles Back-up-Konzept haben. Leider könnte dies eine Scheinsicherheit für die Datensicherung bedeuten. In der Praxis zeigt sich, dass viele Backup-Konzepte vor längerer Zeit einmal erstellt und dann nicht mehr gepflegt und aktualisiert wurden. Die Dynamik der modernen IT macht aber eine regelmäßige Prüfung und Aktualisierung des Backup-Konzeptes notwendig.

Bei rund 30 Prozent gibt es keine Back-up-Software unter Wartung, bei etwa 42 Prozent fehlt der Notfallplan, fast 62 Prozent geben an, kein regelmäßiges Reporting zur Datensicherung vorgesehen zu haben, und bei etwa 73 Prozent gibt es keine expliziten Verantwortlichkeiten und Zuständigkeiten für die Datensicherung, da ein dediziertes Backup-Team fehlt.

Dieses Bild spricht dafür, dass das vorhandene Backup-Konzept in vielen Fällen unvollständig sein muss und nicht für die erhoffte aktuelle Datensicherung sorgen kann.

Datensicherung erfolgt durch die eigene IT

3. Frage: Wer managt bei Ihnen die Datensicherung?



Bei neun von zehn der Befragten ist die eigene IT-Abteilung für die Datensicherung zuständig.

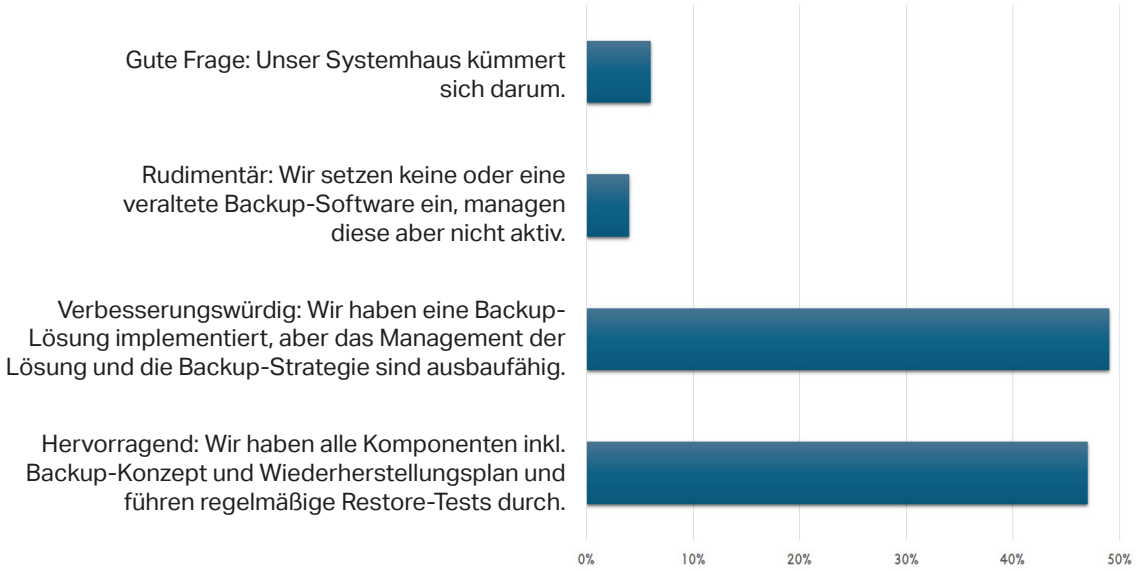
Kommentierung

Obwohl laut Umfrage die Handhabung und Verwaltung die größte Herausforderung bei der Datensicherung ist (siehe Frage 1), verzichten die meisten Befragten auf eine externe Unterstützung.

90 Prozent machen die Datensicherung im Eigenbetrieb, nur einige wenige davon greifen zusätzlich auf eine externe Hilfe zu. Das Outsourcing der Datensicherung an ein externes Systemhaus erscheint eher als Ausnahme.

Datensicherung ist verbesserungswürdig oder aber hervorragend

4. Frage: Wie bewerten Sie den Gesamtzustand Ihrer Datensicherung?



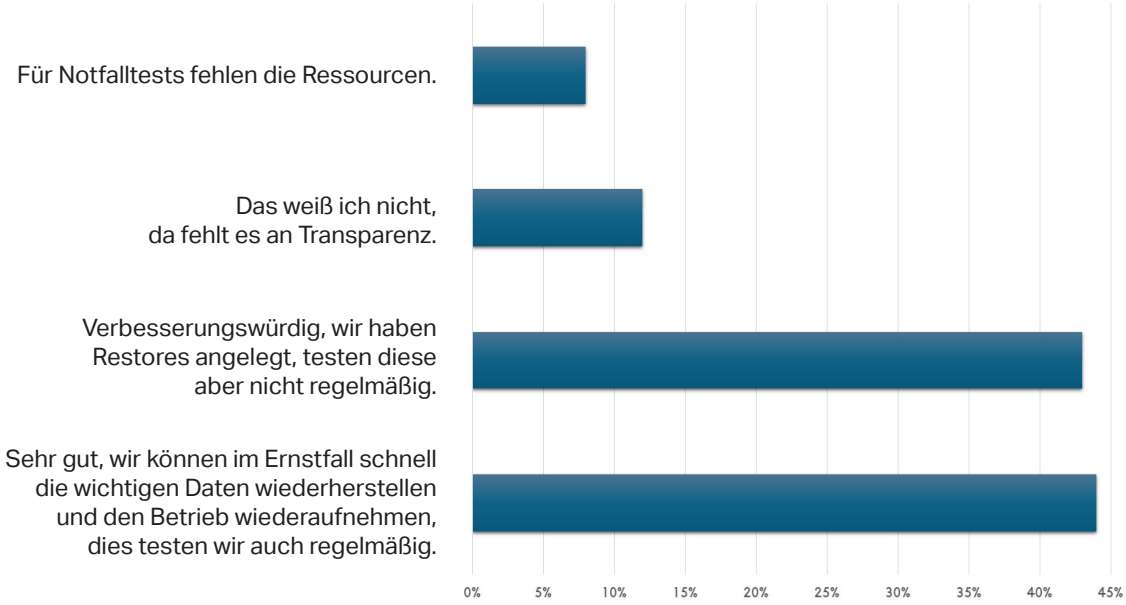
Knapp 49 Prozent der Befragten halten ihre Datensicherung für verbesserungswürdig.

Kommentierung

Nur rund vier Prozent der Befragten halten ihre Datensicherung für rudimentär, haben also keine oder eine veraltete Backup-Software und verzichten auf ein Management der Backups. Etwa sechs Prozent sind sich nicht sicher, denn sie überlassen dies ganz ihrem Systemhaus.
Die große Mehrheit der Befragten sieht die eigene Datensicherung entweder als verbesserungswürdig (Management und Strategie sind ausbaufähig) oder als hervorragend, es gibt also auch ein Backup-Konzept, einen Notfallplan und Tests der Wiederherstellung.
Denkt man aber an die enorme Bedeutung der Datensicherung, macht dies deutlich, dass bei über der Hälfte der Unternehmen ein gewisser bis großer Handlungsbedarf besteht.

Die Wiederherstellung der Daten ist oftmals nicht sichergestellt

5. Frage: Wie schätzen Sie Ihre schnelle Betriebswiederherstellung (Restore) im Desaster-Fall ein?

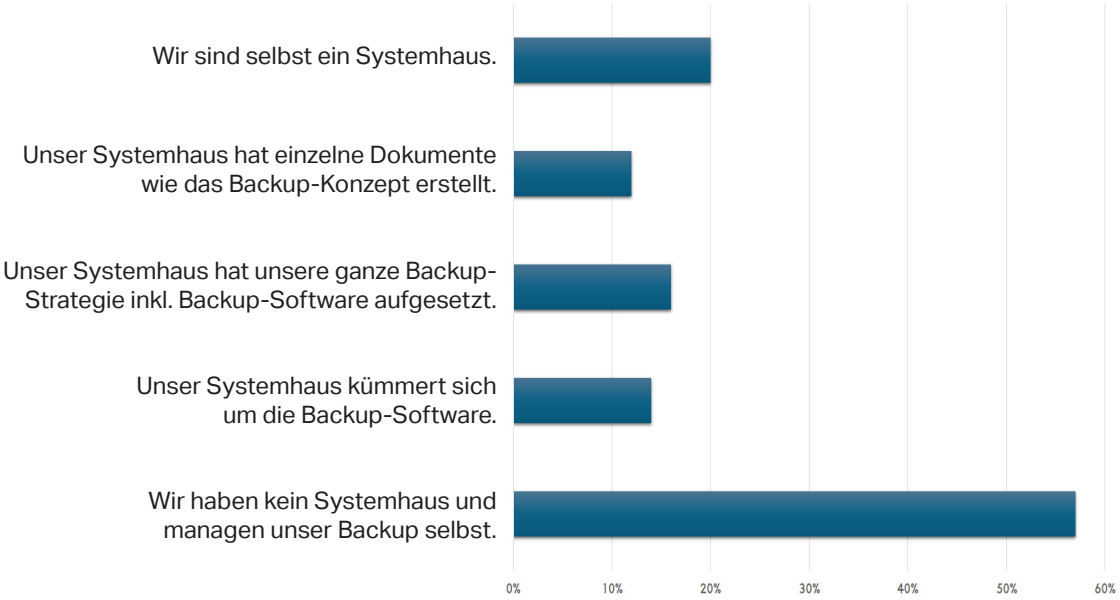


Nur knapp 44 Prozent sind im Ernstfall auf eine Wiederherstellung der Daten wirklich vorbereitet.

Kommentierung

Geht es um die Wiederherstellung der Daten im Ernstfall, fehlen regelmäßige Tests, Transparenz und/oder Ressourcen. Mehr als sechs von zehn der Befragten können also im Ernstfall ihre wichtigen Daten nicht zuverlässig wiederherstellen und den Betrieb schnell wieder aufnehmen.
Das ist ein kritisches Ergebnis mit Blick auf die Vielzahl der IT-Sicherheitsvorfälle, Störungen und Cyberattacken. Ohne zuverlässige Wiederherstellung kann ein Backup keine wirkliche Hilfe sein, denn alleine ein Backup reicht nicht für die zuverlässige und schnelle Wiederaufnahme des Betriebs.
Hier besteht somit dringender Handlungsbedarf, um die Schäden im Ernstfall so gering wie möglich zu halten.

6. Frage: Welchen Anteil an der Datensicherung übernimmt Ihr Systemhaus?



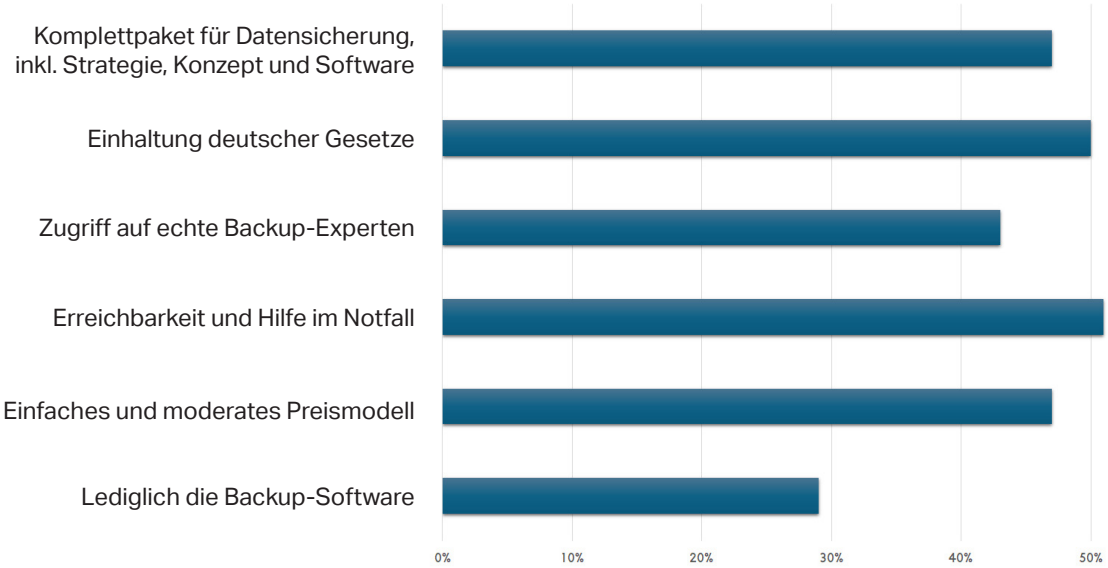
Systemhäuser übernehmen – wenn überhaupt – oft nur Teilaufgaben der Datensicherung.

Kommentierung

Unter den Unternehmen und Behörden, die zur Datensicherung befragt wurden, haben die meisten nicht einmal Teilaufgaben an Systemhäuser übertragen, wenn es um Backups geht. Bei zwölf Prozent hat ein Systemhaus einzelne Dokumente wie das Backup-Konzept erstellt, bei 14 Prozent kümmert sich das Systemhaus nur um die Backup-Software, bei 16 Prozent hat ein Systemhaus die Datensicherung aufgesetzt.

Rund 57 Prozent der Unternehmen und Behörden machen bei der Datensicherung alles selbst, sie haben sich nicht einmal initiale Hilfe beim Aufbau oder für die Konzeptarbeit geholt. Gleichzeitig bereitet vielen Unternehmen und Behörden aber das Datensicherungsmanagement Probleme (siehe Frage 1).

7. Frage: Welche Erwartungen haben Sie an einen Hersteller von Datensicherungssoftware?



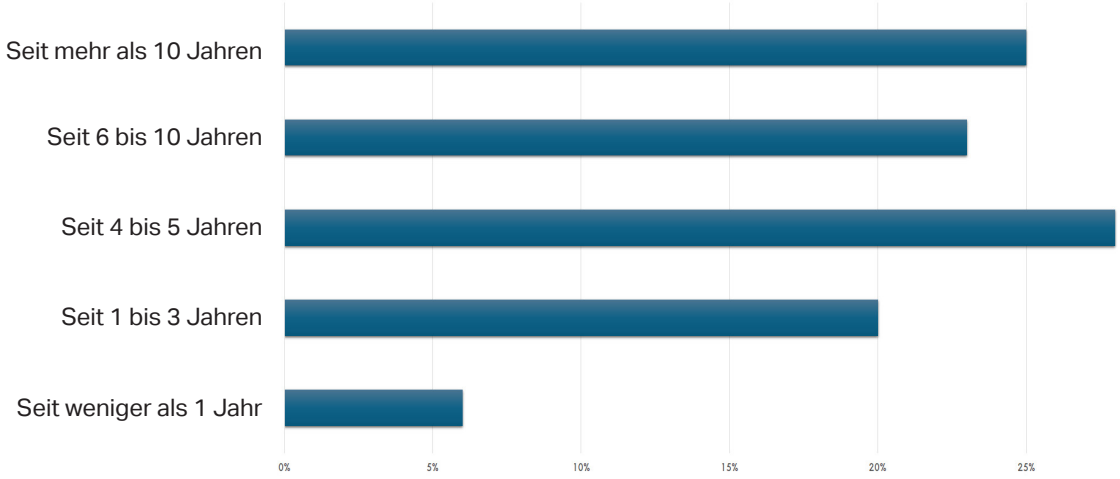
Jeder zweite Befragte wünscht sich vom Hersteller der Datensicherungslösung Hilfe im Notfall.

Kommentierung

Weniger als drei von zehn der Befragten erwarten nur die Backup-Software vom Hersteller der Datensicherungslösung. Über die Hälfte wünscht sich Erreichbarkeit und Hilfe im Notfall, gefolgt von der Einhaltung deutscher Gesetze und einem guten Preismodell.
47 Prozent hätten Interesse an einem Komplettpaket mit Datensicherungslösung, Strategie und Konzept. Interessanterweise richtet sich dieser Wunsch eher an den Anbieter der Backup-Lösung und nicht an die Systemhäuser, wie die Fragen zuvor gezeigt haben. Das gilt insbesondere für die Hilfe und Erreichbarkeit im Notfall, hier möchten die meisten den Hersteller kontaktieren können.

Backup-Lösungen werden für viele Jahre genutzt

8. Frage: Seit wann nutzen Sie Ihre aktuelle Backup-Software?

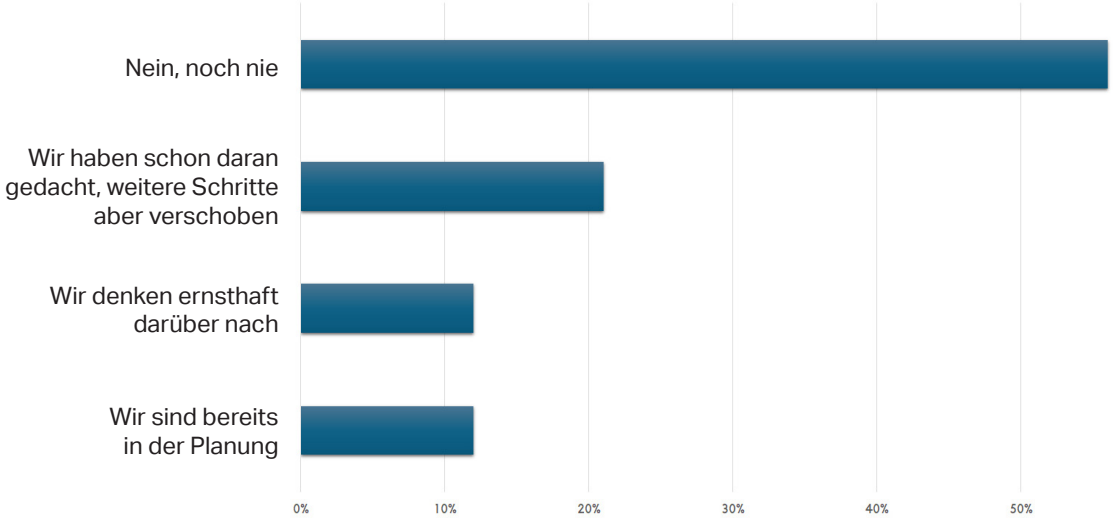


Backup-Software ist fast ein Oldtimer in der IT.

Kommentierung

Jeder vierte Befragte sagt, dass das eigene Unternehmen oder die eigene Behörde die Backup-Software seit mehr als zehn Jahren einsetzt. Mindestens vier Jahre im Einsatz ist die Backup-Lösung bei etwa Dreiviertel der Teilnehmerinnen und Teilnehmer.
Im Vergleich zu anderen IT-Bereichen finden im Bereich Backup also nicht so häufig Veränderungen statt. Denkt man aber an die hohe Dynamik der IT, impliziert das, dass die Backup-Lösung mit vielen neuen Anforderungen und Bedürfnissen umgehen können muss. Sie muss also flexibel, erweiterbar und offen sein. Andernfalls droht bei der langen Nutzungsdauer, dass die Backup-Lösung bestimmte, neue IT-Infrastrukturen nicht unterstützen kann.
Eine aktuelle, moderne Backup- und Recovery-Lösung ist auch aus Compliance-Gründen erforderlich. Rechtliche Vorgaben wie NIS2 oder DORA (Digital Operational Resilience Act, für den Finanzsektor) fordern Maßnahmen zur Gewährleistung von Cyber-Resilienz und damit Maßnahmen zur Wiederherstellung von einem Cyber-Vorfall. NIS2 zum Beispiel nennt explizit „Aufrechterhaltung des Betriebs, Backup-Management, Wiederherstellung nach einem Notfall, Krisenmanagement“ unter den geforderten Risikomanagement-Maßnahmen.

9. Frage: Haben Sie schon einmal darüber nachgedacht, ob Ihre aktuelle Backup-Lösung Ihren Anforderungen vollständig gerecht wird oder ob sich ein Anbieterwechsel lohnen könnte?



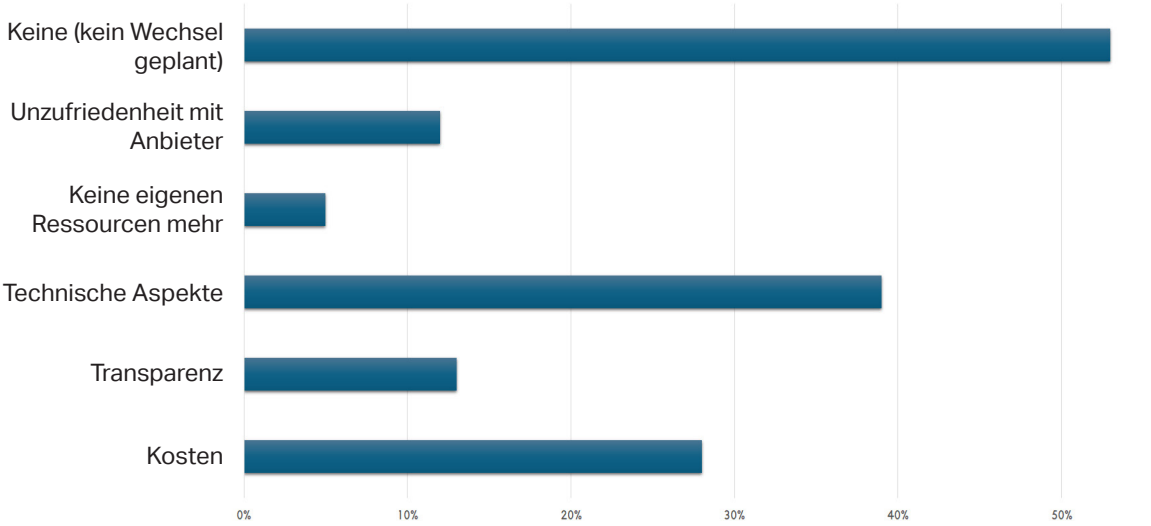
Über die Hälfte der Befragten denkt nicht an eine Veränderung bei der Datensicherung.

Kommentierung

Trotz der Herausforderungen bei der Datensicherung und dem erkannten Bedarf für Verbesserungen denkt mit 56 Prozent die Mehrheit der Befragten nicht daran, den Anbieter für ihre Back-up-Lösung zu wechseln, oder sie haben noch nicht darüber nachgedacht, ob ihre Datensicherung auch allen Anforderungen gerecht werden kann. Dies ist kritisch zu sehen, da sich die Anforderungen an eine moderne Backup- und Recovery-Lösung verändern können. Bei der Mehrheit stehen aber erst einmal keine Veränderungen bei der Datensicherung an. 21 Prozent haben an Veränderungen gedacht, diese aber erst einmal verschoben. Zwölf Prozent denken über mögliche Lücken bei ihrer Datensicherung nach, weitere zwölf Prozent sind bereits in der Planung für einen möglichen Wechsel.

Die Mehrheit will den Backup-Anbieter nicht wechseln

10. Frage: Welche Argumente sprechen aus Ihrer Sicht für einen Wechsel der Backup-Lösung?



Weniger als die Hälfte der Befragten sieht Argumente für einen Wechsel des Backup-Anbieters.

Kommentierung

Wenn denn über einen Wechsel des Anbieters für die Datensicherungslösung nachgedacht wird, dann sind es für 39 Prozent technische Aspekte, die sie dazu bewegen, für 28 Prozent geht es um die Kosten, 13 Prozent suchen mehr Transparenz, zwölf Prozent sind unzufrieden mit ihrem gegenwärtigen Anbieter und nur fünf Prozent nennen Ressourcenmangel als Grund für einen möglichen Anbieterwechsel.

Gefährlicher Stillstand bei der Datensicherung

Die große Bedeutung der Datensicherung ist unbestritten, doch in vielen Unternehmen und Behörden werden die ergriffenen Maßnahmen dem nicht gerecht.

Von Oliver Schonschek, News-Analyst bei Insider Research

Wie die Umfrage zeigt, gibt es bei den teilnehmenden Organisationen deutliche Lücken im Management von Backup, Restore und Disaster Recovery. So verfügt zum Beispiel nur eine Minderheit der Befragten über die dafür notwendigen Ressourcen, das erforderliche Reporting und einen Notfallplan. Jeder zweite Befragte sieht in der Handhabung und Verwaltung der Datensicherung eine Herausforderung. Doch obwohl die internen Schwierigkeiten im Bereich Datensicherung bekannt sind, sagen neun von zehn der Befragten, dass die eigene IT-Abteilung für die Datensicherung zuständig ist. Wenn überhaupt, dann übernehmen Systemhäuser nur Teilaufgaben bei der Datensicherung. Die Überforderung der eigenen IT und die fehlende, externe Unterstützung bleiben nicht ohne Folgen: Nur knapp 44 Prozent sind nach eigener Einschätzung im Ernstfall auf eine Wiederherstellung der Daten wirklich vorbereitet.

Kommt es zu einem Notfall, erhofft sich die Hälfte der Befragten Hilfe vom

Bild: FON's Fasai/adobe.stock.com

Hersteller der Datensicherungslösung. Trotz dieser großen Bedeutung des Software-Anbieters meint weniger als die Hälfte der Teilnehmerinnen und Teilnehmer, dass sie einen neuen Anbieter benötigen. Stattdessen setzen Dreiviertel der Befragten seit mindestens vier Jahren auf die gleiche Backup-Lösung. Veränderungen in der Datensicherung sind für weniger als die Hälfte der Befragten kein Thema, trotz der dynamischen Entwicklung der IT-Infrastrukturen und der Cyberbedrohungen.

Auch aus Compliance-Sicht zeigt sich deutlicher Handlungsbedarf: Rechtliche Vorgaben wie NIS2 und DORA fordern Maßnahmen zur Gewährleistung von Cyber-Resilienz. NIS2 schreibt konkret unter den Risikomanagement-Maßnahmen „Aufrechterhaltung des Betriebs, Backup-Management, Wiederherstellung nach einem Notfall und Krisenmanagement" vor. Für entsprechend unter NIS2 und DORA regulierte Organisationen sind Maßnahmen im Bereich Backup, Restore und Recovery also eine gesetzliche Verpflichtung.

Damit zeigt diese Studie, dass die befragten Unternehmen und Behörden vielfach mit „offenen Augen" und ihre Lücken kennend das Risiko auf sich nehmen, dass sie im Ernstfall keine zeitnahe, umfassende Wiederherstellung der betroffenen Daten leisten könnten und so unter anderem dem Risiko unterliegen, wegen Compliance-Verstößen sanktioniert zu werden.

Es erscheint notwendig, dass für die Risiken einer lückenhaften Datensicherung und Wiederherstellung sensibilisiert wird, dass auf die notwendigen Eigenschaften von Datensicherungslösungen und Anforderungen an Software-Anbieter gezielt hingewiesen und der Prozess der Optimierung im Bereich Datensicherung angestoßen wird. Andernfalls könnten vorhandene Backups eine gefühlte Scheinsicherheit erzeugen, die im Ernstfall einem hohen Risiko und Folgeschäden weichen könnte, wenn die Wiederherstellung nicht gelingt.

Es zeigt sich: In der Datensicherung herrscht bei vielen Befragten schon lange ein gefährlicher Stillstand, der im Notfall zu Datenverlust und Produktivitätsausfall sowie Compliance-Verstößen und Sanktionen führen kann. Notwendig sind nun die Prüfung und Vervollständigung der Backup-Konzepte und Notfallpläne, die Prüfung der technischen Umsetzung mit entsprechenden Wiederherstellungstests, bei Aufdeckung von Lücken in der Datensicherung die Suche nach externer Unterstützung und neuen Lösungen für Backup, Restore und Recovery. Ein „Weiter so" in der Datensicherung sollte und darf es nicht geben.

Cyber-resiliente Datensicherung und -wiederherstellung – Made in Hamburg

Daten sind das Herzstück jedes Unternehmens. Gerade in Zeiten von Cyberangriffen und Umweltkatastrophen hilft NovaStor, sie zu schützen und im Notfall schnell wiederherzustellen.

Als deutscher Softwarehersteller aus Hamburg bietet NovaStor mit seinem Komplettpaket NovaStor DataCenter eine einfache, zuverlässige und cyber-resiliente Lösung für Datensicherung und -wiederherstellung. DSGVO- und NIS2-konform. Und vor allem: 100% Made in Germany.

Die Mitarbeiter von NovaStor begleiten Kunden persönlich mit ganzheitlicher Beratung und direktem, technischen Support, um sicherzustellen, dass ihre Daten jederzeit sicher und verfügbar bleiben. Das Ganze mit transparenten Preismodellen, die auch das Controlling überzeugen.

Erfahren Sie mehr darüber, wie NovaStor Ihre Daten schützt: www.novastor.de

Bild: NovaStor