Ausfallsicherheit bei Cyberangriffen in Aktion

Benchmarking der globalen Unternehmensbereitschaft
für Sicherheit/Erkennung/Wiederherstellung
Informationen zu Insights
Januar 2026

DELL Technologies

Agenda

- Ziele und Firmografik
- Die Lücke in der Ausfallsicherheit bei Cyberangriffen
- Sicher
- Erkennen
- Recovery
- Komplexität, Kultur und was als Nächstes kommt

Geschäftsziele

- Positionierung von Dell als Vordenker und strategischer Partner für Ausfallsicherheit bei Cyberangriffen
- Bestätigung der Entscheidung, von „Data Protection“ zu „Ausfallsicherheit bei Cyberangriffen“ zu wechseln

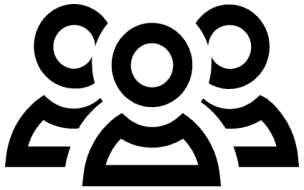
Ziele der Studie

- Einschätzung des Reifegrads und der Integration von Strategien zur Ausfallsicherheit bei Cyberangriffen
- Bewertung der Effektivität von Sicherungs-, Erkennungs- und Wiederherstellungsverfahren von Unternehmen
- Verstehen der Hürden, die der Verbesserung der Ausfallsicherheit bei Cyberangriffen im Weg stehen, darunter Kompetenzlücken, Budget und Komplexität
- Erfahren, wie Unternehmen ihre IT-Umgebung schützen und Daten vor Ransomware-Bedrohungen schützen

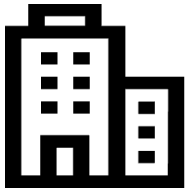
Wen haben wir befragt?

Die Teilnehmenden wurden im Juli und Oktober 2025 befragt

850 IT-EntscheidungsträgerInnen aus globalen Unternehmen



Unternehmen mit mehr als 1.000 MitarbeiterInnen



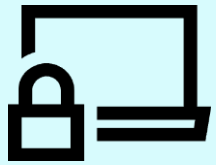
Unternehmen aus verschiedenenöffentlichen und privaten Branchen

Zu den Teilnehmenden gehören: Vorstandsmitglieder; Mitglieder der Führungsebene; Mitglieder des mittleren Managements

Die wichtigsten Erkenntnisse

39 %

Der Organisationen verfügen über eine vollständig etablierte und kontinuierlich optimierte Strategie zur Ausfallsicherheit bei Cyberangriffen



Kontinuierliche Optimierung ist entscheidend – ohne sie können Strategien schnell veralten und nicht mehr in der Lage sein, sich weiterentwickelnde Bedrohungen zu bewältigen, sodass Unternehmen einem größeren Risiko ausgesetzt sind

46 %

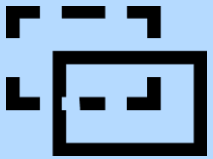
Stimmen zu, dass ihre Backup-Daten nicht so gut geschützt sind, wie sie sein sollten

Die Stärkung des Backup-Schutzes ist unerlässlich, um sicherzustellen, dass die Wiederherstellung auch dann möglich bleibt, wenn die primären Systeme beeinträchtigt werden.

Sicher

30 %

Verwenden eine umfassende Plattform für die Bedrohungserkennung, die sich über das Netzwerk, das Backup und das primäre Storage erstreckt



Ohne einheitliche Erkennung können die Erkennungs- und Reaktionszeiten bei Bedrohungen langsamer sein, was das Risiko unerkannter Sicherheitsverletzungen erhöht.

Erkennung

55 %

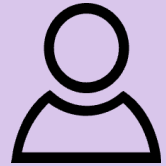
Der BefragungsteilnehmerInnen, die mindestens ein Mal pro Monat simulierte Cyberangriffe durchführten, konnten den Betrieb nach einem Drill-/Cyber-Incident erfolgreich wieder aufnehmen

Häufige Tests helfen Teams, sich auf echte Angriffe vorzubereiten. Unvorbereitete Teams haben ein höheres Risiko von Reaktions- und Wiederherstellungsverzögerungen in Krisensituationen.

Recovery

63 %

Sind der Meinung, dass Führungskräfte die Resilienz ihres Unternehmens bei einem großen Cybersicherheitsvorfall überschätzen



Selbstüberschätzung kann Investitionen verzögern, die Reaktionsplanung beeinträchtigen und kritische Sicherheitslücken unbehoben lassen.

Abschnitt 1: Die Lücke in der Ausfallsicherheit bei Cyberangriffen

Verstehen des Problems und der Notwendigkeit, sich schnell weiterzuentwickeln

Die kontinuierliche Optimierung von Ausfallsicherheitsstrategien verbessert die Wiederherstellungsprozesse, führt jedoch nicht immer zu einem Erfolg

99,5 %

Verfügen über eine Strategie zu Ausfallsicherheit bei Cyberangriffen in irgendeiner Form

39 %

Glauben, dass sie vollständig etabliert und kontinuierlich optimiert wird (= eine ausgereifte Strategie)

57 %

Konnten bei ihrem letzten Test oder Vorfall die Bedrohung nicht wirksam eindämmen und sich schnell nach dem Angriff erholen

Unternehmen mit ausgereiften Strategien zur Ausfallsicherheit bei Cyberangriffen sind **2,6-mal häufiger in der Lage**, sich erfolgreich Cyberangriffe zu überstehen

65 % im Vergleich zu. **25 %**

63 %

Sind der Meinung, dass die **Führungskräfte die Unternehmensbereitschaft** für ein großes Cybersicherheitsvorfall überschätzen

Warum das jetzt wichtig ist

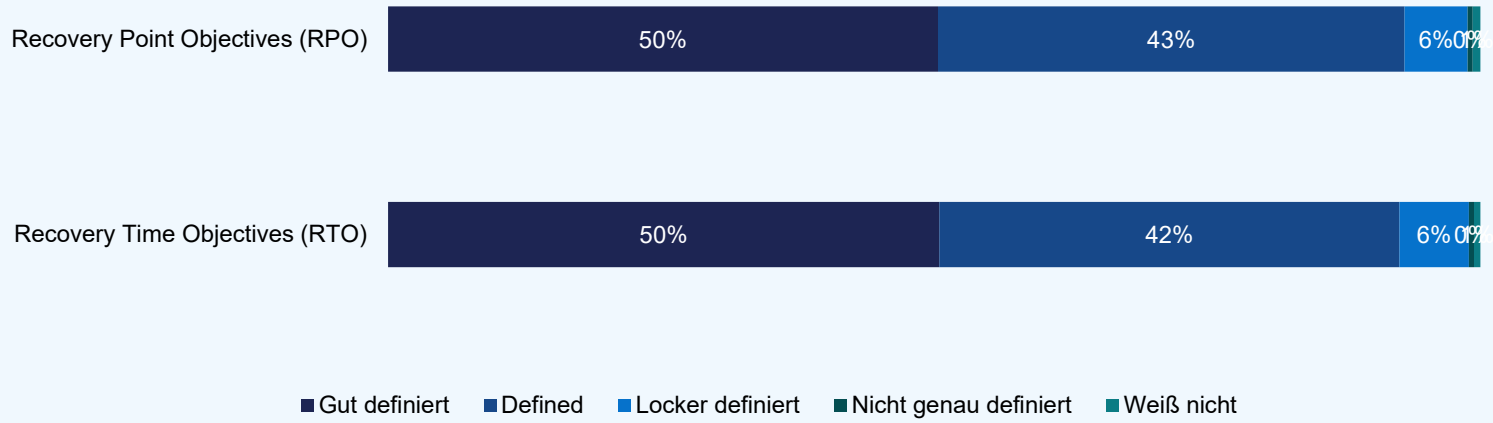
97 %

Stimmen zu, dass ihr Unternehmen seine Sicherheitsstrategien kontinuierlich weiterentwickeln muss, um mit den sich wandelnden Bedrohungen Schritt zu halten

78 %

glauben, dass sich ihr Unternehmen mehr auf die Verhinderung von Angriffen als auf Vorbereitungen für die Wiederherstellung nach einem Angriff konzentriert

Das Ausmaß, das Unternehmen Folgendes definiert haben:



32 %

Haben **beide Bereiche** klar definiert

Von denen mit einer ausgereiften Strategie für Ausfallsicherheit

58 %

Haben sowohl RTO als auch RPO klar definiert

Abschnitt 2: Sicher

Verhinderung von Angriffen und Stärkung der digitalen Infrastruktur

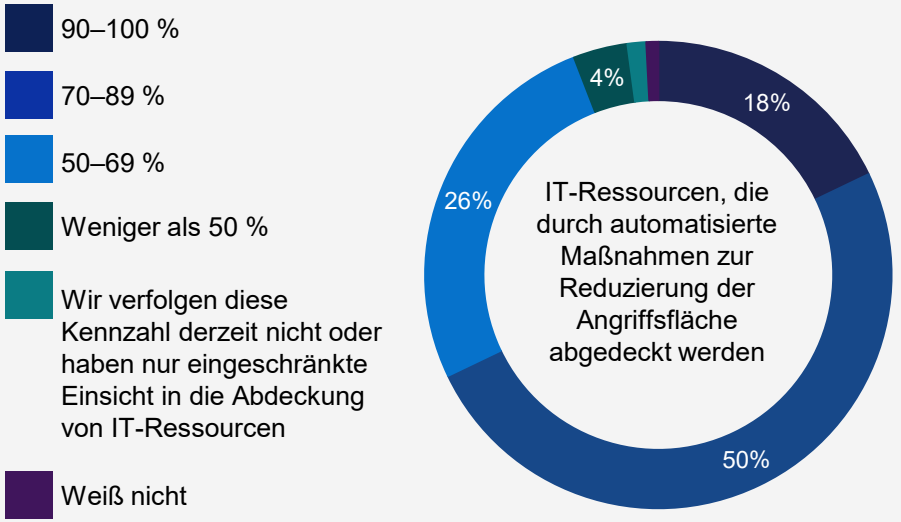
Sichtbarkeits- und Schutzlücken

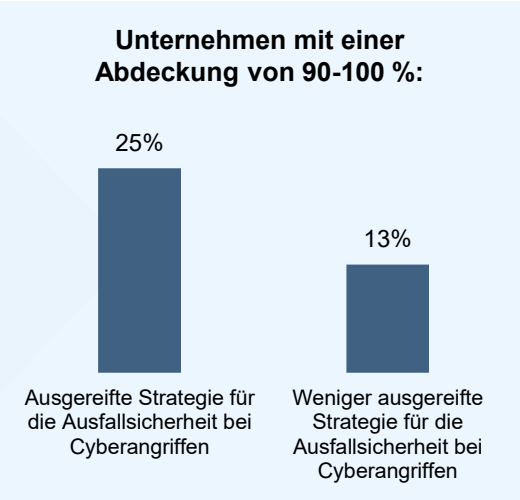
46 %

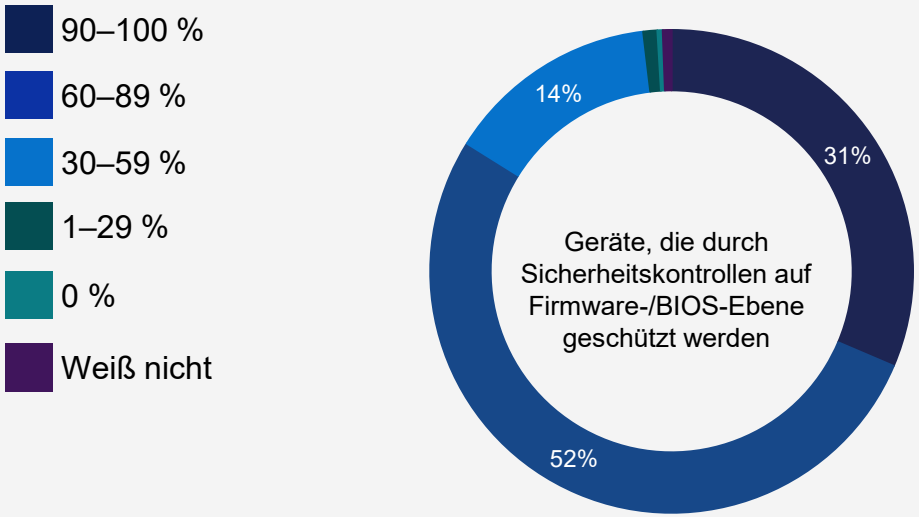
Geben zu, dass ihre Backup-Daten nicht so gut geschützt sind, wie sie sein sollten

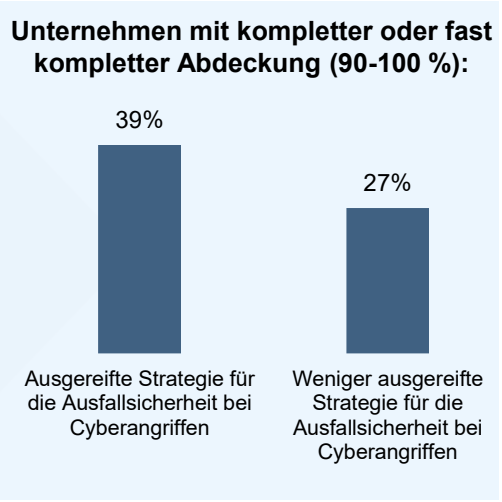
-	**59 %**
EMEA	**43 %**
LATEINAMERIKA	**41 %**
APJ	**39 %**

Kontinuierliche Optimierung beseitigt nicht die Deckungslücken, aber sie gibt Organisationen einen entscheidenden Vorteil in Bezug auf Resilienz









Von der Integrität vor der Bereitstellung bis zur Wiederherstellung nach dem Angriff: Beide Seiten der Sicherheit stärken

Prozesse/Methoden, die von Unternehmen verwendet werden, um die Integrität der IT-Hardware/-Software sicherzustellen

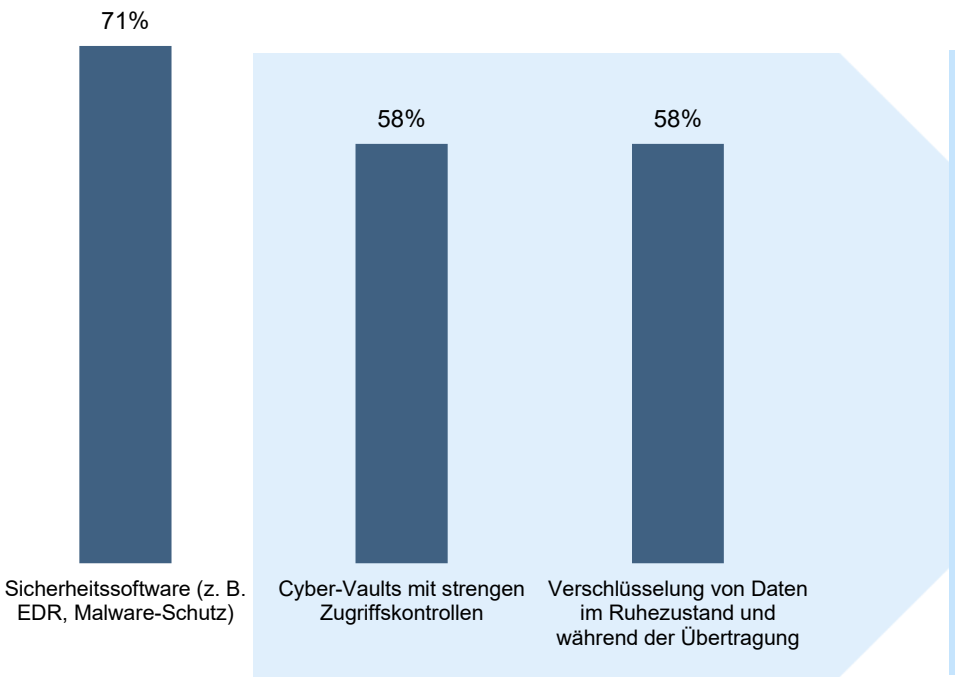
72 %

Verlassen sich auf Anbieter von Zertifizierungen und Bescheinigungen und auf Systeme mit integrierten Werkzeugen, die die Integrität der Komponenten überprüfen

64 %

Führen interne Audits oder manuelle Überprüfungen während der Bereitstellung/Einführung durch

Methoden, die von Unternehmen verwendet werden, um kritische Daten vor Ransomware-Angriffen zu schützen



Unternehmen mit ausgereiften Ausfallsicherheitsstrategien nutzen häufiger:

- **Datenverschlüsselung (59 % vs 57 %)**
- **Cyber Vaults (63 % vs 55 %)**

als Unternehmen mit weniger ausgereiften Ausfallsicherheitsstrategien

Abschnitt 3: Erkennung

Die Erkennung und Reaktion auf Bedrohungen, bevor sie Schaden anrichten

Durch den Einsatz von KI und Automatisierung können Bedrohungen aufgedeckt werden, bevor sie Backups gefährden

38 %

Der Unternehmen verwenden KI-/ML-Tools mit proaktiven Playbooks für Schadensminderung und Bedrohungsreaktion

Unternehmen mit einer ausgereiften Strategie für Ausfallsicherheit bei Cyberangriffen nutzen diesen Ansatz **3,1-mal häufiger**

65 % im Vergleich zu. **21 %**

48 %

Der Unternehmen nutzen **KI/ML umfassend**, um Backup-Daten auf Gefährdungsindikatoren zu scannen

Die umfassende Nutzung von KI/ML erfolgt **2,3-mal häufiger in Unternehmen mit einer ausgereiften Strategie für Ausfallsicherheit bei Cyberangriffen**

72 % im Vergleich zu. **32 %**

83 %

Glauben, dass Bedrohungsakteure bei Ransomware-Angriffen **zunehmend auch Backups** angreifen

62 % priorisieren Investitionen in Automatisierung und KI-/ML-gestützte Bedrohungserkennung

Unvollständige Transparenz erhöht die Risiken

54 %

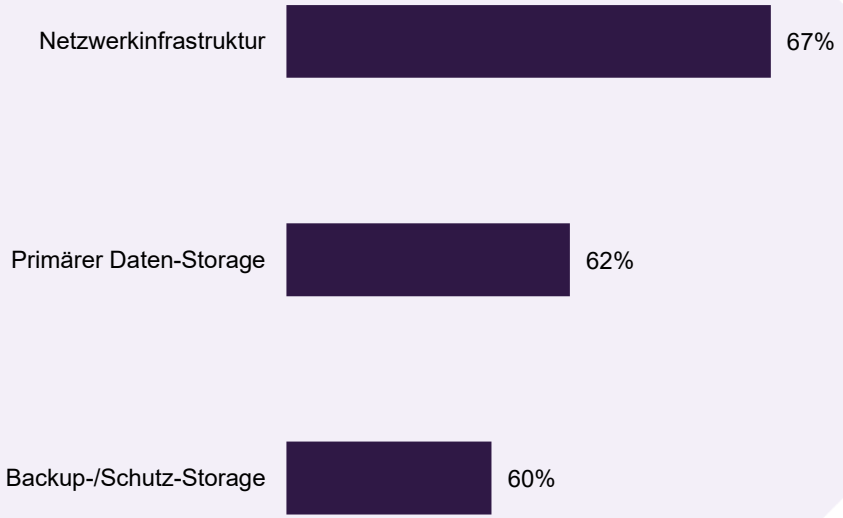
Geben an, dass sie einen guten Einblick in verdächtige Aktivitäten oder kompromittierte Daten in ihren Backup-Systemen haben

74 % Unternehmen mit einer ausgereiften Strategie für die Ausfallsicherheit bei Cyberangriffen

im Vergleich mit

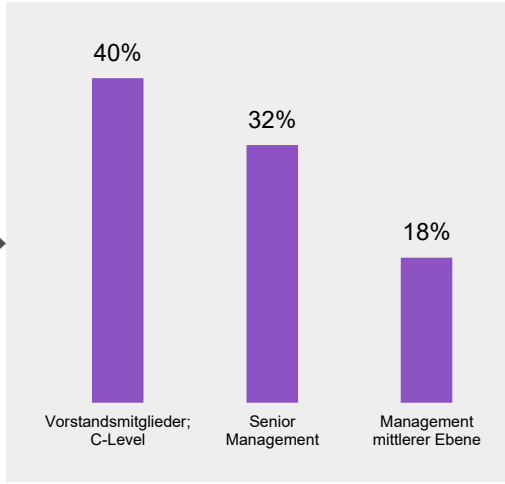
42 % Organisationen mit einer weniger ausgereiften Strategie für die Ausfallsicherheit bei Cyberangriffen

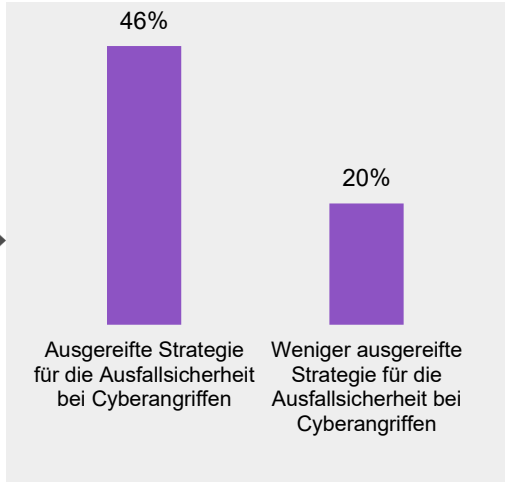
Unternehmen mit einer robusten Plattform für die Bedrohungserkennung in den folgenden Bereichen



30 %

Verfügen über eine umfassende Plattform **für alle 3 Bereiche**





Abschnitt 4: Wiederherstellung

Schnelle Wiederherstellung innerhalb der SLA-Erwartungen

Recovery-Status: Viele Unternehmen erreichen ihre Ziele, aber kontinuierliche Verbesserungen sind unerlässlich, um mit der Bedrohungslandschaft Schritt zu halten

40 %

Haben einen Vorfall **erfolgreich eingedämmt und sich mit minimalen Auswirkungen erholt**

Dabei gaben **Vorstandsmitglieder (53 %)** dies häufiger an als **Mitglieder des mittleren Managements (30 %)**

54 %

Der Unternehmen haben ihre **RTO- und RPO-Ziele erreicht**

Nach Position: Vorstandsmitglieder (66 %) vs. Mitglieder des mittleren Managements (45 %)

Nr. 4

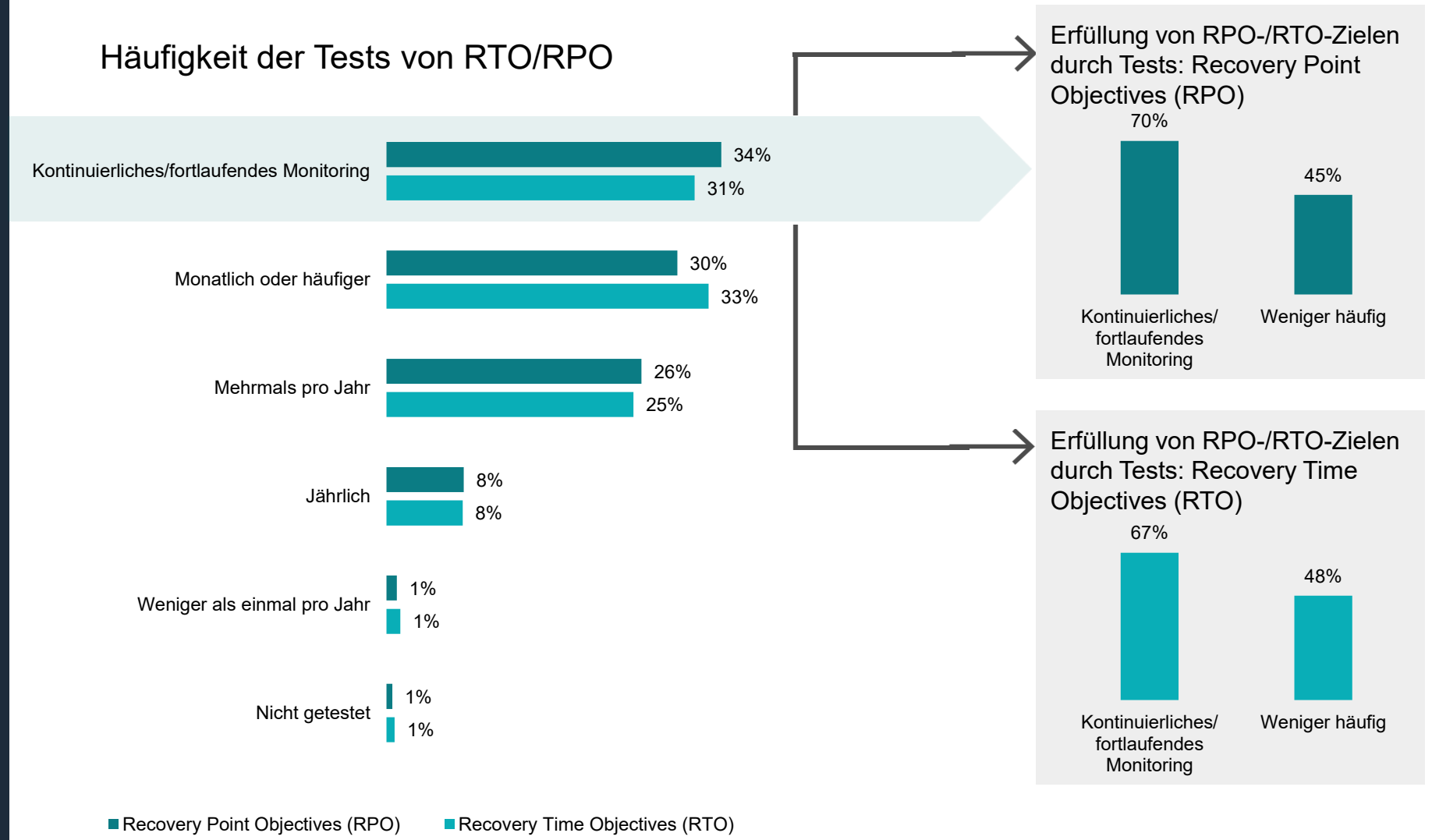
Der Hauptgrund für Investitionen in Cybersicherheit ist ein **kürzlich eingetretener oder knapp abgewendeter Cybersicherheitsvorfall** in unserem Unternehmen

57 % der Unternehmen verbessern ihre Ausfallsicherheit, um **behördliche Anforderungen oder Compliance-Vorgaben zu erfüllen**

Regelmäßige Tests könnten die Wiederherstellung verbessern

> Letztendlich ist es eine Kultur der Wachsamkeit und ständigen Verbesserung, die Resilienz schafft.
>
> *Senior Managerin, Verbraucherdienstorganisation, Brasilien*

Testen ist entscheidend für die Widerstandsfähigkeit und gibt Organisationen eine bessere Chance, sich von einem Angriff zu erholen



Tests sind von grundlegender Bedeutung für die Ausfallsicherheit

48 %

Gaben an, dass die Cybersicherheitstests ihres Unternehmens moderne Angriffstechniken nicht realistisch simulieren

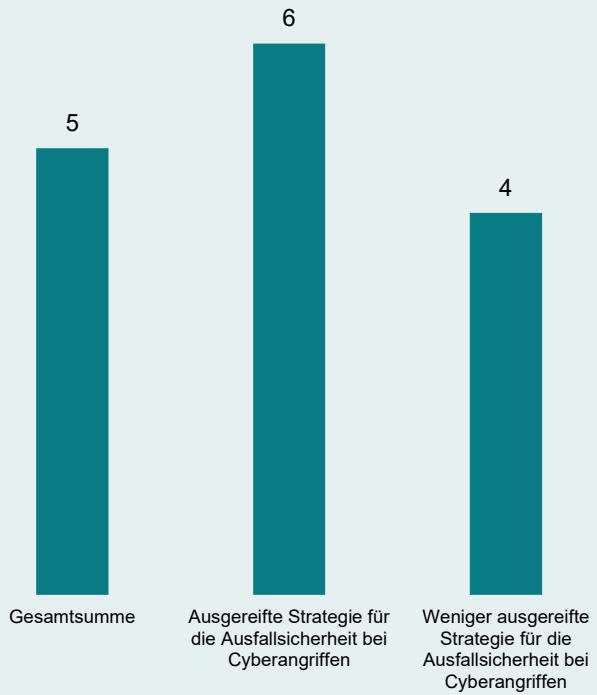
53 % der Vorstandsmitglieder/C-Level

im Vergleich mit

48 % der Manager mittlerer Ebene

Regelmäßige Übungen sind entscheidend, um die Wiederherstellung zu beschleunigen, Unternehmen sollten sich jedoch kontinuierlich auf sich entwickelnde Bedrohungen vorbereiten

Durchschnitt von simulierten Cyberangriffen pro Jahr



55 %

der BefragungsteilnehmerInnen, die **mindestens ein Mal pro Monat** simulierte Cyberangriffe durchführten, konnten den Betrieb nach einem Drill-/Cyber-Vorfall erfolgreich wieder aufnehmen

35 %

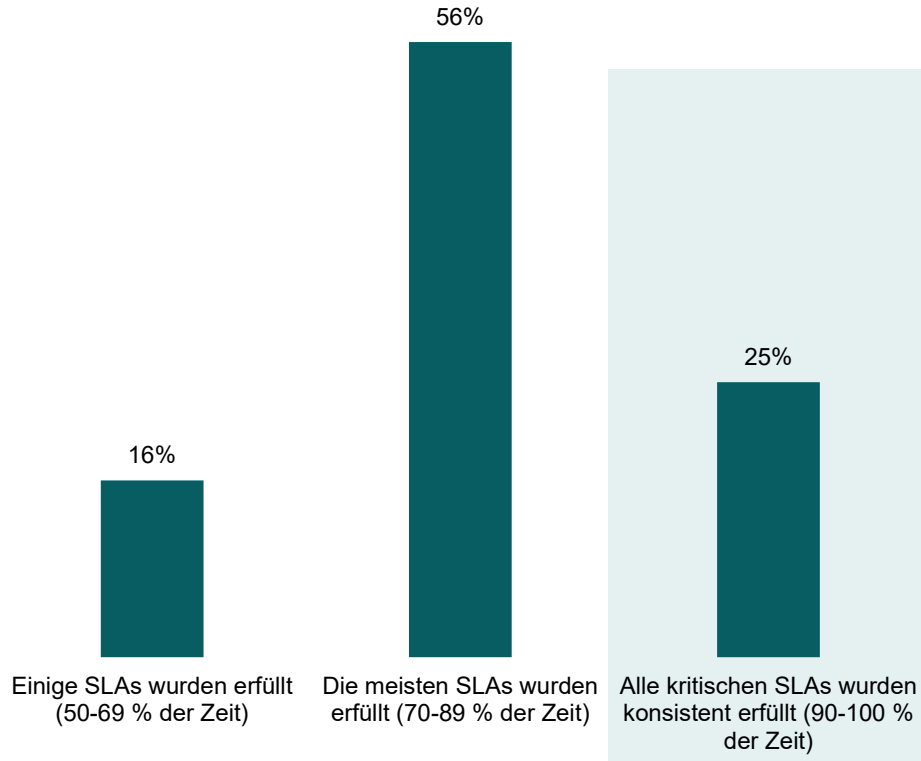
der BefragungsteilnehmerInnen, die **seltener als ein Mal pro Monat** simulierte Cyberangriffe durchführten, konnten den Betrieb nach einem Drill-/Cyber-Vorfall erfolgreich wieder aufnehmen

> *Die Notwendigkeit, ganzheitliche Tests und Bewertungen über alle potenziellen Bedrohungsflächen hinweg durchzuführen, anstatt sich auf die Punktabdeckung/Tests zu konzentrieren.*
>
> Senior ManagerIn, IT-Technologie und Telekommunikation, Vereinigtes Königreich

> *Cyberangriffe erinnern uns daran, wie wichtig es ist, regelmäßige Sicherheitsübungen durchzuführen.*
>
> *Wir haben unsere Schulungen zur Sicherheitssensibilisierung intensiviert, sodass alle MitarbeiterInnen potenzielle Bedrohungen identifizieren können.*
>
> Vorstandsmitglied, Bauwesen und Immobilien, Australien

SLAs sind der Beweis: Unternehmen mit ausgereiften Strategien erfüllen ihre Recovery-Versprechen

Häufigkeit, mit der Unternehmen Recovery-SLAs für kritische Systeme erfüllen

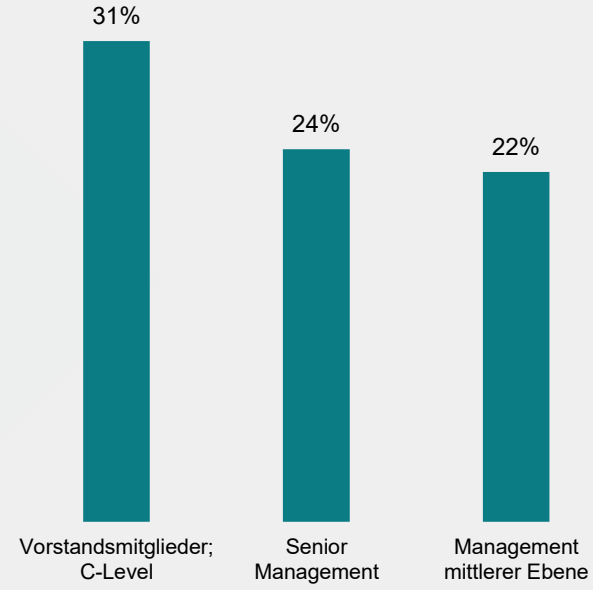


2-mal

Unternehmen mit einer ausgereiften Strategie für Ausfallsicherheit bei Cyberangriffen sind eher in der Lage, ihre SLAs konsistent einzuhalten

36 % im Vergleich zu **18 %**

Nach Position:



Abschnitt 5: Komplexität, Kultur und die Zukunft

Organisatorische Hürden und zukünftige Investitionspläne

Komplexität, Kompetenzlücken und Selbstüberschätzung bedrohen die Ausfallsicherheit bei Cyberangriffen, aber KI und Schulungen könnten helfen

Größte Herausforderungen:

Komplexe IT-Umgebungen	49 %
Begrenzte Budgets	42 %
Mangel an qualifiziertem Personal	39 %
Anbieter-/Tool-Fragmentierung	38 %
Geringe Priorisierung im Unternehmen	23 %

Größere Unternehmen sind mit höherer Wahrscheinlichkeit damit konfrontiert:

- 50 % 5.000 oder mehr MitarbeiterInnen
- 50 % 3.000 bis 4.999 MitarbeiterInnen
- 46 % 1.000 bis 2.999 MitarbeiterInnen

63 %

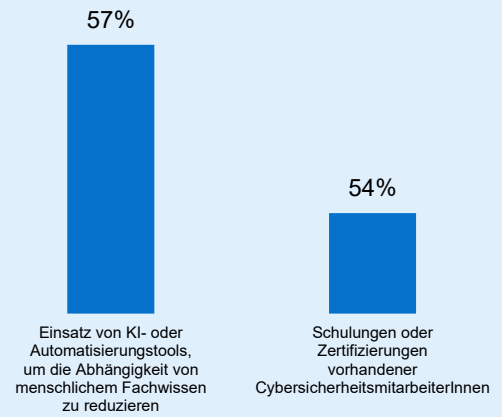
Sind der Meinung, dass Führungskräfte die Resilienz ihres Unternehmens bei einem großen Cybersicherheitsvorfall überschätzen

96 %

Erkennen an, dass sie Defizite in ihren Cybersicherheitskompetenzen oder ihrem Fachwissen haben

ABER …

Unternehmen ergreifen folgende Maßnahmen:



Ausblick auf Investitionen

Nr. 1

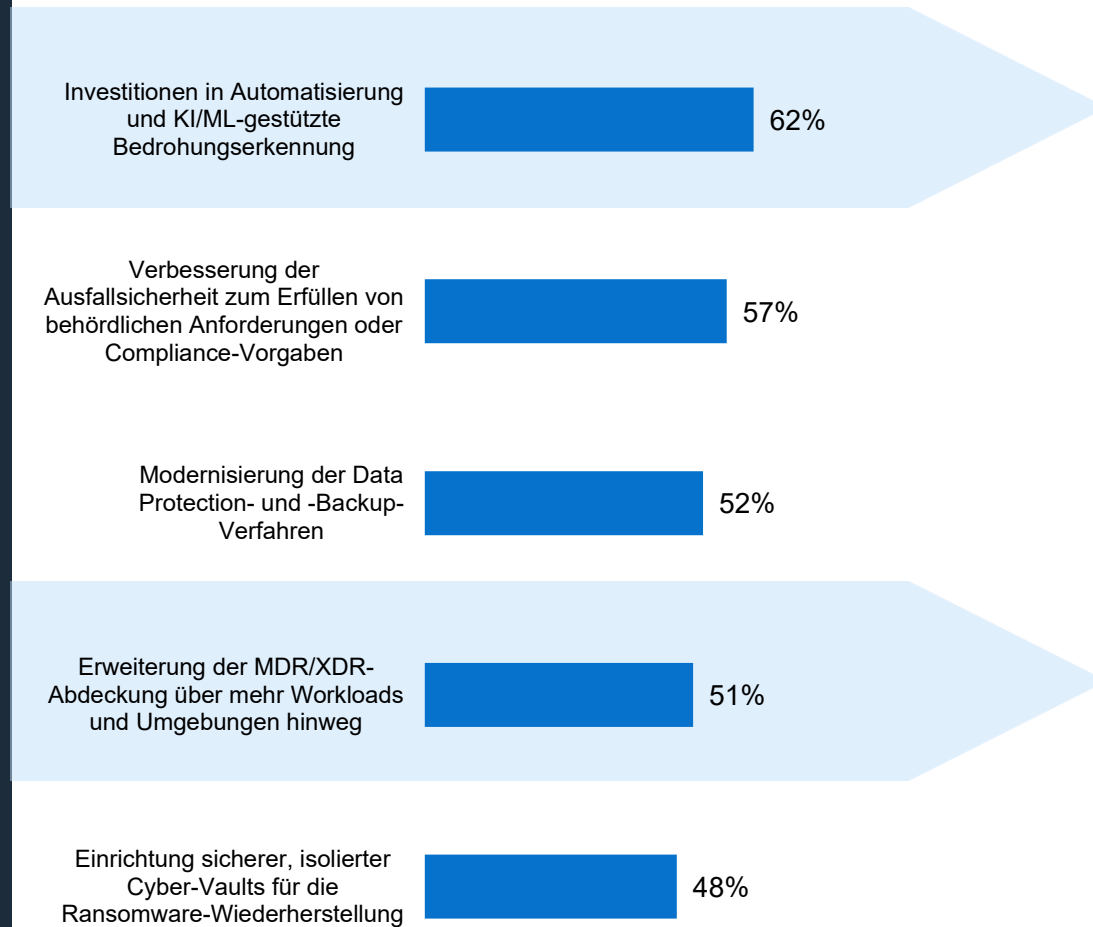
Der Hauptgrund für Investitionen ist die sich entwickelnde Bedrohungslandschaft

97 %

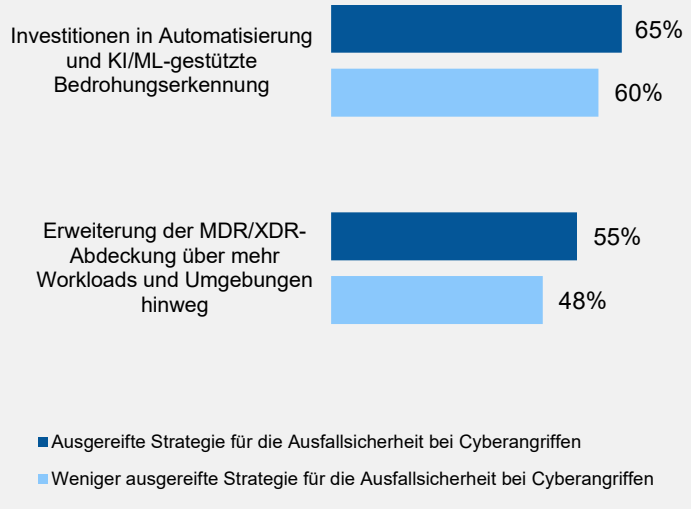
„Mein Unternehmen muss seine Sicherheit kontinuierlich stärken, da sich Bedrohungen weiterentwickeln.“

Um eine ausgereifte Strategie aufrechtzuerhalten, sind kontinuierliche Investitionen und Optimierung ein erfolgversprechender Ansatz

Priorisierte Investitionen in die Ausfallsicherheit bei Cyberangriffen in den nächsten 12 Monaten



Unternehmen mit einer ausgereiften Ausfallsicherheitsstrategie investieren kontinuierlich in:

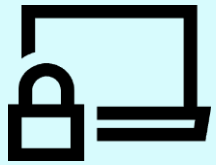


Wichtigste Erkenntnisse

Die wichtigsten Erkenntnisse

39 %

Der Organisationen verfügen über eine vollständig etablierte und kontinuierlich optimierte Strategie zur Ausfallsicherheit bei Cyberangriffen



Kontinuierliche Optimierung ist entscheidend – ohne sie können Strategien schnell veralten und nicht mehr in der Lage sein, sich weiterentwickelnde Bedrohungen zu bewältigen, sodass Unternehmen einem größeren Risiko ausgesetzt sind

46 %

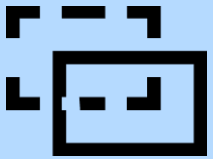
Stimmen zu, dass ihre Backup-Daten nicht so gut geschützt sind, wie sie sein sollten

Die Stärkung des Backup-Schutzes ist unerlässlich, um sicherzustellen, dass die Wiederherstellung auch dann möglich bleibt, wenn die primären Systeme beeinträchtigt werden.

Sicher

30 %

Verwenden eine umfassende Plattform für die Bedrohungserkennung, die sich über das Netzwerk, das Backup und das primäre Storage erstreckt



Ohne einheitliche Erkennung können die Erkennungs- und Reaktionszeiten bei Bedrohungen langsamer sein, was das Risiko unerkannter Sicherheitsverletzungen erhöht.

Erkennung

55 %

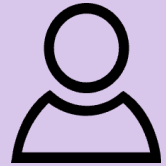
Der BefragungsteilnehmerInnen, die mindestens ein Mal pro Monat simulierte Cyberangriffe durchführten, konnten den Betrieb nach einem Drill-/Cyber-Incident erfolgreich wieder aufnehmen

Häufige Tests helfen Teams, sich auf echte Angriffe vorzubereiten. Unvorbereitete Teams haben ein höheres Risiko von Reaktions- und Wiederherstellungsverzögerungen in Krisensituationen.

Recovery

63 %

Sind der Meinung, dass Führungskräfte die Resilienz ihres Unternehmens bei einem großen Cybersicherheitsvorfall überschätzen



Selbstüberschätzung kann Investitionen verzögern, die Reaktionsplanung beeinträchtigen und kritische Sicherheitslücken unbehoben lassen.