

Wir haben für Ihre Organisation das folgende Gesamtergebnis ermittelt:

## Unvorbereitet



Erkennung



Reaktion



Recovery

[Bewertung erneut durchführen](#)



### Erkennung

In Bezug auf den proaktiven Schutz Ihrer Organisation anhand von Best Practices für die Erkennung fällt Ihre Bewertung wie folgt aus:

**Unvorbereitet**

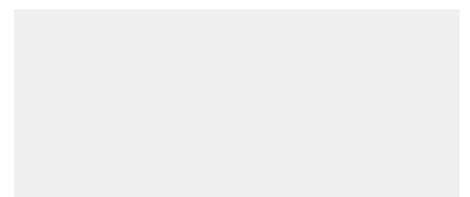
Sehen Sie sich die Videozusammenfassung an.

Cannot load video.  
This video is unavailable



### Reaktion

In Bezug auf die schnelle und effektive Reaktion auf einen Cyber-Incident mit



dem Ziel, den Schaden bzw. die negativen Auswirkungen möglichst gering zu halten, fällt Ihre Bewertung wie folgt aus:

**Unvorbereitet**

Sehen Sie sich die Videozusammenfassung an.

Cannot load video.  
This video is unavailable



### **Genesen**

In Bezug auf die Daten-Recovery und die Wiederaufnahme des Betriebs nach einem Cyber-Incident fällt Ihre Bewertung wie folgt aus:

**Unvorbereitet**

Sehen Sie sich die Videozusammenfassung an.

Cannot load video.  
This video is unavailable

## Ihr maßgeschneiderter Bericht zur Ausfallsicherheit bei Cyberangriffen

Vielen Dank, dass Sie die Selbstbewertung der Ausfallsicherheit bei Cyberangriffen von Dell Technologies (powered by ESG) durchgeführt haben. Diese Bewertung hat das folgende Ziel: Sie sollen verstehen, wie anfällig Ihre Organisation für Ransomware- und andere hochentwickelte Cyberangriffe derzeit ist, es sollen Bereiche identifiziert werden, in denen Sicherheitslücken bestehen, und Ihre Optionen zur Eindämmung dieser Risiken sollen erläutert werden. Zu diesem Zweck evaluieren wir die Bereitschaft Ihrer Organisation in den folgenden drei Hauptbereichen: proaktive Bedrohungserkennung, agile Reaktion auf Bedrohungen und Vollständigkeit der Recovery-Fähigkeiten.

Basierend auf Ihren Antworten, die Sie im Rahmen der Bewertung in diesen Bereichen auswählen, stufen wir Ihre Organisation als **Unvorbereitet** ein. Diese Kategorien stehen bei dieser Bewertung für die **niedrigste** Bereitschaftsstufe. Auf den folgenden Seiten wird ausführlich beschrieben, warum Ihre Organisation diese Bewertung erhalten hat, und sie enthalten zusätzlich die Empfehlungen für Ihre Organisation.



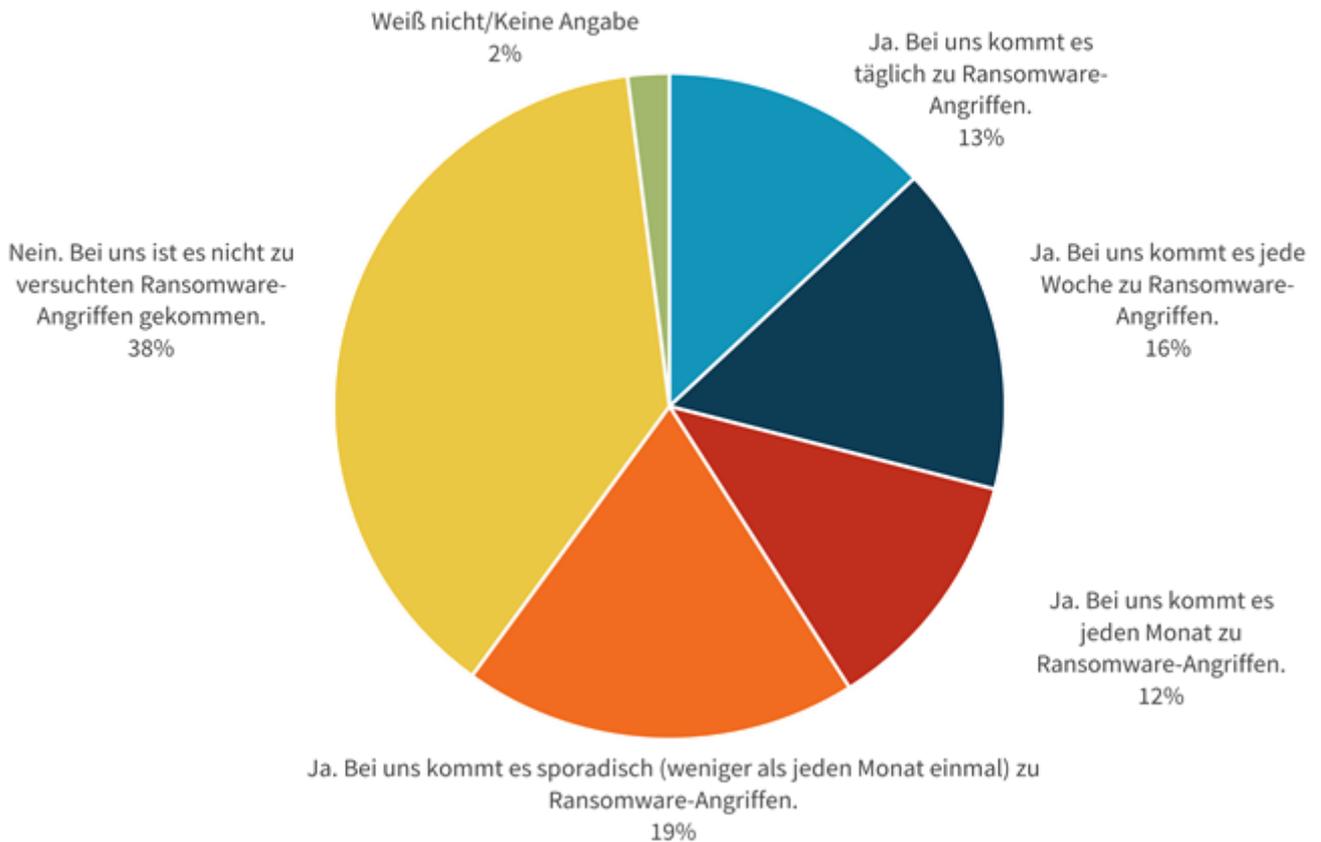
## Erkennung

Im ersten Teil der Bewertung geht es um die proaktive Bedrohungserkennung. Dies umfasst die Technologien und Prozesse, die von Ihrer Organisation genutzt werden, um einen Cyberangriff oder Ransomware-Incident zu erkennen und zu verhindern. Für diesen Teil wurde Ihre Organisation als **Unvorbereitet** eingestuft. Dies ist bei dieser Bewertung die **niedrigste** Kategorie der Bereitschaft.

- **Am Anfang der Bewertung haben wir nach den Bedrohungen gefragt, mit denen sich Ihr Team beschäftigt. Dies ist wichtig, weil eine Untersuchung von ESG zu den geplanten Ausgaben aus dem Jahr 2020 ergeben hat, dass viele Organisationen ständig mit Ransomware und anderen Arten von hochentwickelten Cyberangriffen zu kämpfen haben (siehe Abbildung 1).** Die Bedrohungslandschaft wird immer komplexer und Angreifer nutzen häufig mehrere Angriffsvektoren, um Organisationen zu kompromittieren und Eindringversuche zu unternehmen. Für die meisten Organisationen haben Ransomware und professionelle mehrstufige Angriffe mit Seitwärtsbewegungen Priorität, aber sowohl die absichtliche als auch die unabsichtliche Bedrohung durch Insider macht vielen Organisationen ebenfalls immer mehr Sorgen. Die Implementierung von Sicherheitslösungen für Endpunkte mit zuverlässigem Schutz vor Ransomware ist dringend zu empfehlen, und zwar in Verbindung mit eingeübten Plänen zur Reaktion auf Incidents und zuverlässigen Backupstrategien mit Offline-Schutzfunktionen, z. B. gemäß den Empfehlungen der Cybersecurity and Infrastructure Security Agency (CISA). Falls Sie für den Schutz Ihrer Organisation einen Serviceanbieter nutzen, ist eine Diskussion über diese Bereiche dringend zu empfehlen.

Abbildung 1

Wurde auf Ihre Organisation nach Ihrem Wissensstand innerhalb der letzten zwölf Monate ein versuchter Ransomware-Angriff unternommen? (Prozentsatz der Befragten)



Quelle: ESG

- Darüber hinaus haben wir Sie um eine Einschätzung gebeten, wie gut Ihre Organisation die Compliance-Anforderungen erfüllt.
- Bei der Bewertung ist es auch um die Nutzung von Risiko-Frameworks durch Ihre Organisation gegangen, die für Ihr Sicherheitsprogramm als Hilfe dienen können.
- Als Nächstes ist es in der Bewertung um die Transparenz in Bezug auf Endpunkte, die Cloud und das Netzwerk gegangen.
- Abschließend wurde in der Bewertung die Effizienz der vorhandenen Kontrollmechanismen abgefragt, mit denen vor allem ein Ransomware-Angriff verhindert werden kann.



## Reaktion

Im zweiten Teil der Bewertung geht es um die agile Reaktion auf Bedrohungen. Dies betrifft also die vorhandenen Technologien und Prozesse in Ihrer Organisation, mit denen schnell auf einen Sicherheits- oder Ransomware-Incident reagiert und die damit verbundenen Auswirkungen

eingedämmt werden können. Für diesen Teil wurde Ihre Organisation als **Unvorbereitet** eingestuft. Dies ist bei dieser Bewertung die **niedrigste** Kategorie der Bereitschaft.

- **Wir haben Ihnen die Frage gestellt, wie Ihre wahrscheinlichste Reaktion auf einen erfolgreichen Ransomware-Angriff aussehen würde.**
- **Als Nächstes haben wir gefragt, wie viel Zeit, Aufwand und Geldmittel Sie für den Schutz von sekundären Datenkopien zur Verfügung gestellt haben.**
- **Im Hinblick auf die Reaktionsbereitschaft,**
- **Im Hinblick auf bestimmte Maßnahmen zur Sicherstellung der Bereitschaft werden im Rahmen der Bewertung Ansätze wie die Planung für Incidents und Recovery-Testläufe vorrangig behandelt.**



## Wiederherstellung

Im dritten und letzten Teil der Bewertung geht es um die Vollständigkeit der Recovery-Fähigkeiten. Dies umfasst die Technologien und Prozesse, die in Ihrer Organisation vorhanden sind, um einen Recovery-Vorgang für Ihre gesamten Daten durchzuführen und die schnelle Wiederaufnahme des normalen Betriebs zu ermöglichen. Für diesen Teil wurde Ihre Organisation als **Unvorbereitet** eingestuft. Dies ist bei dieser Bewertung die **niedrigste** Kategorie der Bereitschaft.

- **Es ist von entscheidender Bedeutung, dass Sie über die richtigen MitarbeiterInnen verfügen, die nach einem Cyberangriff den Recovery-Vorgang durchführen können.**

Abbildung 2

In welchen der folgenden Bereiche verfügt Ihre IT-Abteilung Ihrer Meinung nach derzeit über einen problematischen Mangel an qualifizierten MitarbeiterInnen? (Prozentsatz der Befragten, mehrere Antworten möglich)



Quelle: ESG

- Wir haben die Frage gestellt, welchen Anteil Ihrer Daten Sie bei einem Angriff Ihrer Meinung nach wiederherstellen können.
- In der Bewertung geht es auch um die Investitionen Ihrer Organisation in eine Infrastruktur mit „Air Gap“ oder Isolation für die Kopien Ihrer kritischen Daten.
- Unabhängig davon, ob Ihre Organisation über eine isolierte Infrastruktur verfügt, haben wir abschließend die Frage gestellt, welcher Anteil der Daten in dieser Art von Umgebung Ihrer Meinung nach geschützt werden sollte.

Unterstützung von Dell Technologies

Dell Technologies ist bestrebt, Vertrauen und eine sichere vernetzte Welt zu schaffen. Wir arbeiten unermüdlich daran, dass die Sicherheit Ihrer Daten, Ihres Netzwerks, Ihrer Organisation und Ihrer Kunden an erster Stelle steht. Zu diesem Zweck haben wir unsere gesamten Produkte, Lösungen und Services so konzipiert, dass auf umfassende Weise für die Ausfallsicherheit bei Cyberangriffen und die allgemeine Sicherheit gesorgt ist. Von Dell Endpoint Security Lösungen und VMware Carbon Black Cloud bis zu unseren vertrauenswürdigen Geräten und Dell EMC PowerProtect Cyber Recovery: Wir unterstützen Sie bei der Schaffung und Aufrechterhaltung einer sicheren und ausfallsicheren Organisation, die auch auf neu entwickelte Bedrohungen vorbereitet ist.

Basierend auf Ihrer Bewertung und derzeitigen Einstufung haben wir für Sie die wichtigsten Empfehlungen zusammengestellt, mit denen Sie die Ausfallsicherheit verbessern können. In unserem [Sicherheits- und Vertrauenszentrum](#) können Sie leicht auf weitere Ressourcen und Lösungen zugreifen, damit Sie schnell Antworten auf Ihre Fragen zur Sicherheit von Privatanwendern und Unternehmen erhalten.

Ob Edge, Core oder Cloud: Von unseren BranchenexpertInnen erhalten Sie eine Strategieberatung und Informationen zu bewährten praktischen Vorgehensweisen, mit denen Sie Ihr Unternehmen schützen und eine Rufschädigung durch Cyberbedrohungen vermeiden können. Vertrauen Sie Dell Technologies.

## Dell kann Sie wie folgt bei der Verbesserung Ihrer Fähigkeiten zur Angriffserkennung unterstützen:



- **Endpoint Security und Geräte:** Die Anzahl der Endnutzer, die remote und unterwegs arbeiten, hat exponentiell zugenommen. Bei den derzeitigen Sicherheitsverstößen sowohl ober- als auch unterhalb der Betriebssystemebene benötigen Sie intelligente Lösungen, mit denen Bedrohungen verhindert und erkannt werden und die unabhängig vom Ort des Auftretens die richtige Reaktion ermöglichen.
- **VMware Carbon Black™ Cloud:** Cyberkriminelle verbessern ständig ihre Taktik und verstecken ihre Aktionen in gängigen Tools und Prozessen. Sie benötigen eine Endpunktplattform, mit der Sie selbst kleinste Fluktuationen erkennen können, hinter denen sich bössartige Angriffe verbergen, damit Sie Ihre Schutzmaßnahmen entsprechend anpassen können.
- **PowerEdge – Proaktive Ausfallsicherheit:** Erhöhen Sie das Vertrauen in Ihre digitale Transformation, indem Sie eine Infrastruktur nutzen, die für sichere Interaktionen und die Fähigkeit zur Vorhersage potenzieller Bedrohungen konzipiert wurde.

## Dell kann Sie wie folgt bei der Verbesserung Ihrer Reaktionsfähigkeit unterstützen:



- **Managed Detection and Response:** Bei Managed Detection and Response (powered by Secureworks® Taegis™ XDR) werden erweiterte Analysen und Fachwissen genutzt, um eine Untersuchung auf eine potenzielle Kompromittierung durchzuführen und bei Erkennung einer Bedrohung Abhilfemaßnahmen einzuleiten.
- **Business Resiliency Services:** Dell Technologies Services ermöglichen eine hohe Ausfallsicherheit für Organisationen, die vermehrt auf Cloud-basierte IT-Services angewiesen sind und für die immer höhere Anforderungen von Stakeholdern und Regulierungsbehörden gelten.
- **Cyber Recovery-Services:** Mithilfe von Dell Technologies Services können Organisationen ihre Ausfallsicherheit bei Cyberangriffen mit einem ganzheitlichen Programm zur Cyber Recovery erhöhen, bei dem Technologien, Prozesse und MitarbeiterInnen gemeinsam eingesetzt werden, um für Ihre Organisation eine ultimative Verteidigungslinie zu bilden.

Dell kann Ihnen wie folgt bei der Verbesserung Ihrer Recovery-Fähigkeiten nach einem Angriff helfen:



- **PowerProtect Cyber Recovery:** Mit PowerProtect Cyber Recovery werden kritische Daten isoliert und vor Ransomware-Angriffen und anderen hochentwickelten Bedrohungen geschützt, damit Sie die intakten Daten wiederherstellen und die normale Geschäftstätigkeit selbstbewusst fortsetzen können.
- **Business Resiliency Services:** Dell Technologies Services ermöglichen eine hohe Ausfallsicherheit für Organisationen, die vermehrt auf Cloud-basierte IT-Services angewiesen sind und für die immer höhere Anforderungen von Stakeholdern und Regulierungsbehörden gelten.
- **PowerScale mit Superna Eyeglass Ransomware Defender:** Superna Eyeglass® Ransomware Defender ist eine hochgradig skalierbare Lösung für die Echtzeit-Ereignisverarbeitung, bei der das Nutzerverhalten analysiert wird, um einen Ransomware-Angriff zu erkennen und zu stoppen.

