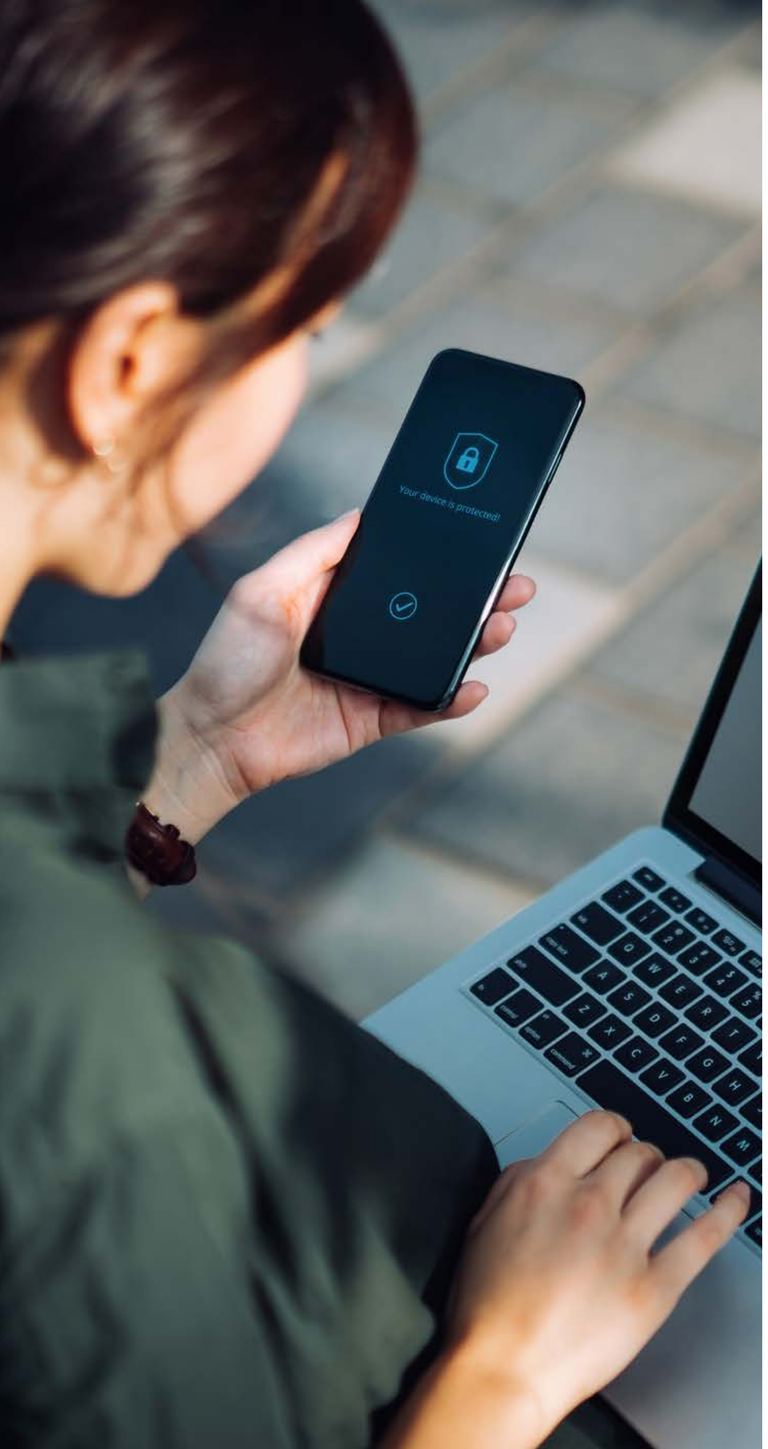
Enterprise Strategy Group | Getting to the bigger truth.™

So bauen Sie ein cybersicheres Unternehmen auf, das bereit für Innovationen und Erfolg ist

Adam Demattia, Senior Director, Custom Research

MÄRZ 2022

INHALT



Studienziele und -methodik

ZIELE:

In diesem E-Book wird erläutert, ob und in welchem Maße die Einführung einer robusten Strategie für die Ausfallsicherheit bei Cyberangriffen in einem Unternehmen mit IT-Vorhersehbarkeit, geschäftlichen Innovationen und Erfolg zusammenhängt. Diese Beziehungen werden basierend auf wettbewerbsbasierten Daten ermittelt. In diesem E-Book erfahren Sie Folgendes:

- Sie werden verstehen, wie wir die Ausfallsicherheit bei Cyberangriffen definieren und messen und wo Ihr Unternehmen heute steht.
- Sie können quantifizieren, welche Vorteile hochgradig ausfallsichere Unternehmen im Vergleich zu ihren Mitbewerbern erzielen, und zwar sowohl in Bezug auf die IT- als auch die geschäftliche Performance.
- Schließlich erfahren Sie durch die Erkenntnis, was cybersichere Unternehmen tun, wie Ihr Unternehmen seine Praktiken und Prioritäten weiterentwickeln muss, um wie ein Marktführer zu agieren.

METHODIK:

Im ersten Quartal 2022 hat die ESG eine Doppelblindumfrage[1] unter 750 IT- und SicherheitsentscheidungsträgerInnen durchgeführt, die mit den Cybersicherheits- und Ausfallsicherheitstechnologien zum Schutz von Rechenzentrums- und EndnutzerInnengeräteumgebungen vertraut sind.

Die repräsentierten Unternehmen umfassten mittelständische und Großunternehmen und die Stichprobe bestand aus einer horizontalen Mischung aus vertikalen Branchen. Die Studie war mit Unternehmen aus Nordamerika (N = 187), Westeuropa (N = 185), APAC (N = 179) und LATAM (N = 199) außerdem global ausgelegt.

[1] Die Befragten waren anonym und wurden nicht darüber informiert, dass die ESG die Umfrage durchführte oder diese von Dell Technologies in Auftrag gegeben wurde.

Zurück zum Inhaltsverzeichnis

Wichtige Erkenntnisse

In diesem E-Book werden Unternehmen, die über einen optimalen Level an Investitionen in Sicherheitstechnologie, Personaldecke und rigorosen Drittanbieterrisikoprüfungen verfügen, als vorbereitete Unternehmen kategorisiert. Unsere Studie zeigt, dass heute nur 10 % der befragten Unternehmen diesen Level an Ausfallsicherheit erreicht haben, was die Notwendigkeit einer unternehmensweiten Fokussierung und Verbesserung unterstreicht.

Cybersichere Unternehmen minimieren Unterbrechungen. Vorbereitete Unternehmen weisen folgende Merkmale auf:

7,3-mal häufigere
Bewertung ihrer Ausfallsicherheitssituation als hervorragend

2,5-mal häufigere
Bereitstellung einer Verfügbarkeit von mindestens 99,99 % für ihre geschäftskritischen Anwendungen, was einem geschätzten Kostenvorteil von 33,3 Mio. US-Dollar für Ausfallzeiten entspricht

Wesentlich mehr Agilität
bei der Erkennung von Incidents (20 % schnellere durchschnittliche Erkennungszeit [Mean Time to Detect, MTTD]) und Reaktionen (35 % durchschnittliche Zeit bis zur Wiederherstellung [Mean Time to Recover, MTTR])

Ausfallsicherheit bei Cyberangriffen hängt mit verbesserter Geschäftsperformance zusammen. Vorbereitete Unternehmen weisen folgende Merkmale auf:

8,5-mal häufigere
Angabe, dass ihre EndnutzerInnenzufriedenheitsbewertungen in der Regel ihre Ziele übertreffen, was auf einem besseren Service und EndnutzerInnenerlebnis basiert

7,7-mal häufigere
Markteinführung neuer Angebote vor der Konkurrenz im Vergleich zu gefährdeten Unternehmen

Prognose, dass der Umsatz des Unternehmens

doppelt
so schnell steigt wie bei Mitbewerbern

Zurück zum Inhaltsverzeichnis

Definieren und Messen der Ausfallsicherheit bei Cyberangriffen

Vier Merkmale eines vorbereiteten (oder hochgradig ausfallsicheren) Unternehmens

Um zu ermitteln, ob das Unternehmen von Befragten als „vorbereitet“ kategorisiert werden kann, haben wir uns die Antworten auf vier wichtige Fragen im Zusammenhang mit der Personaldecke für Ausfallsicherheitsaufgaben, mit Kompetenzlücken, Technologieinvestitionen und Risikobewertungsprozessen angesehen:

PERSONAL

Wie würden Sie die Personalausstattung in Ihrem Cybersicherheitsteam beschreiben?

- ☑ Keine offenen Stellen
- ☐ Schlecht, knapp oder ausreichend besetzt

Wie würden Sie den Kenntnisstand im Cybersicherheitsteam Ihres Unternehmens beschreiben?

- ☑ Keine Kompetenzlücken
- ☐ Viele, einige oder angemessene Kompetenzlücken

AUSFALLSICHERHEITSTECHNOLOGIE

Wie würden Sie die Investitionen Ihres Unternehmens in Produkte und Services zur Sicherung seiner Systeme, Anwendungen und Daten beschreiben?

- ☑ Optimal
- ☐ Schlecht, verbesserungsbedürftig oder angemessen

DRITTANBIETERRISIKEN

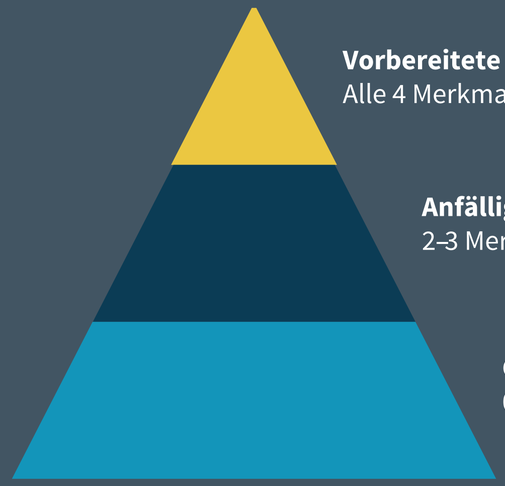
Führt Ihr Unternehmen Inspektionen oder Audits zur Sicherheit seiner Partner/IT-Anbieter durch?

- ☑ Formell und rigoros
- ☐ Informell, gelegentlich oder gar nicht

Unternehmen nach ihrer Ausfallsicherheit
(Prozent der Befragten, N = 750)

Die ESG hat ein datengesteuertes Modell entwickelt, das die Unternehmen der Befragten in drei Ausfallsicherheitsstufen unterteilt: **vorbereitete Unternehmen, anfällige Unternehmen und gefährdete Unternehmen.**

Bei diesem Modell werden die vier Fragen links aus der Umfrage als Vorgaben verwendet, um den Status eines Unternehmens zu ermitteln. Jede dieser Fragen stellt ein Merkmal eines gut vorbereiteten Unternehmens dar (d. h. ein Attribut eines Unternehmens mit hoher Ausfallsicherheit) in Bezug auf die Teams für Cybersicherheit, die Finanzierung für Technologien zur Risikominderung oder der Fokus des Unternehmens auf die Minimierung von Drittanbieterrisiken. Je mehr Merkmale das Unternehmen aufweist, desto größer ist seine Ausfallsicherheit, wie unten gezeigt:



Vorbereitete Unternehmen
Alle 4 Merkmale; 10 % des Markts

Anfällige Unternehmen
2–3 Merkmale; 26 % des Markts

Gefährdete Unternehmen
0–1 Merkmal; 64 % des Markts

Zurück zum Inhaltsverzeichnis

Cybersichere Unternehmen minimieren Unterbrechungen

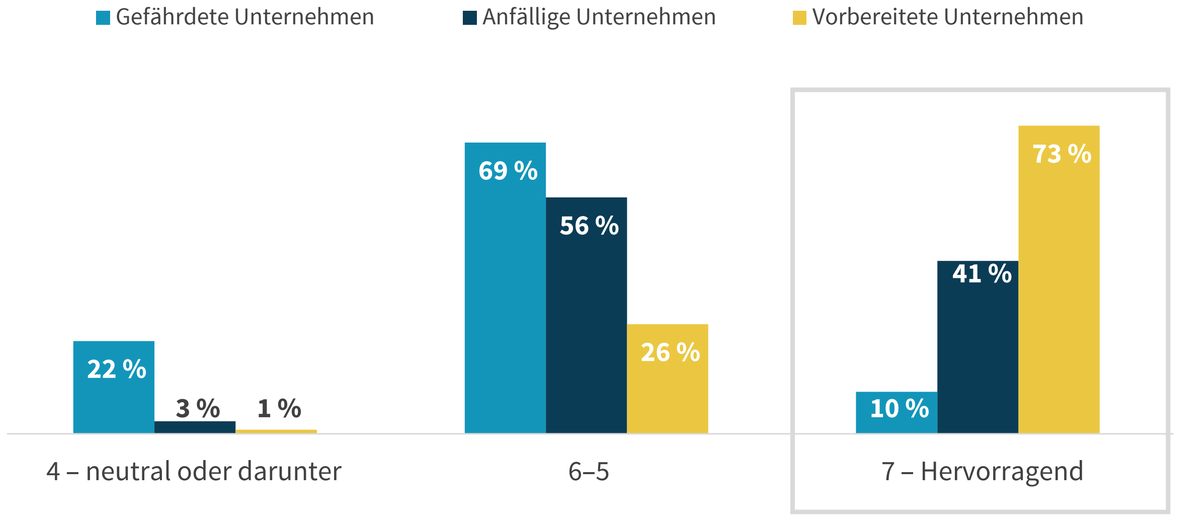
Vorbereitete Unternehmen sind im Bereich der Ausfallsicherheit bei Cyberangriffen viel zuversichtlicher als ihre Mitbewerber

Obwohl es um eine qualitative Frage geht, ist es zwar wichtig, das Vertrauen von IT- und Cybersicherheitsführungskräften in die Ausfallsicherheit ihres Unternehmens zu messen. Diese Personen gestalten und fördern die Strategien ihrer Unternehmen und sind am besten positioniert, den Erfolg bei der Umsetzung dieser Strategien zu bewerten.

Um das Vertrauen zu messen, baten wir die Befragten, ihre Ausfallsicherheit bei Cyberangriffen auf einer Skala von 7 (hervorragend) bis 1 (mangelhaft) zu bewerten. Die Befragten waren im Allgemeinen positiv gestimmt, aber nur 24 % der Unternehmen bewerteten ihre Ausfallsicherheit bei Cyberangriffen als „hervorragend“, was zusammengefasst eine vorsichtig optimistische Haltung widerspiegelte.

Allerdings variiert das Vertrauen je nach Ausfallsicherheitsstufe der Unternehmen erheblich. Fast drei Viertel der vorbereiteten Unternehmen (73 %) bewerten ihre Ausfallsicherheit als hervorragend.

Wie bewerten Sie die allgemeine Ausfallsicherheit bei Cyberangriffen Ihres Unternehmens (d. h. Ihre Fähigkeit, einem Cyberangriff standzuhalten und den Geschäftsbetrieb fortzusetzen)? (Prozentsatz der Befragten)



Vorbereitete Unternehmen sind

7,3-mal häufigere

als gefährdete Unternehmen in der Lage, ihre Ausfallsicherheit als „hervorragend“ zu bewerten.

Zurück zum Inhaltsverzeichnis

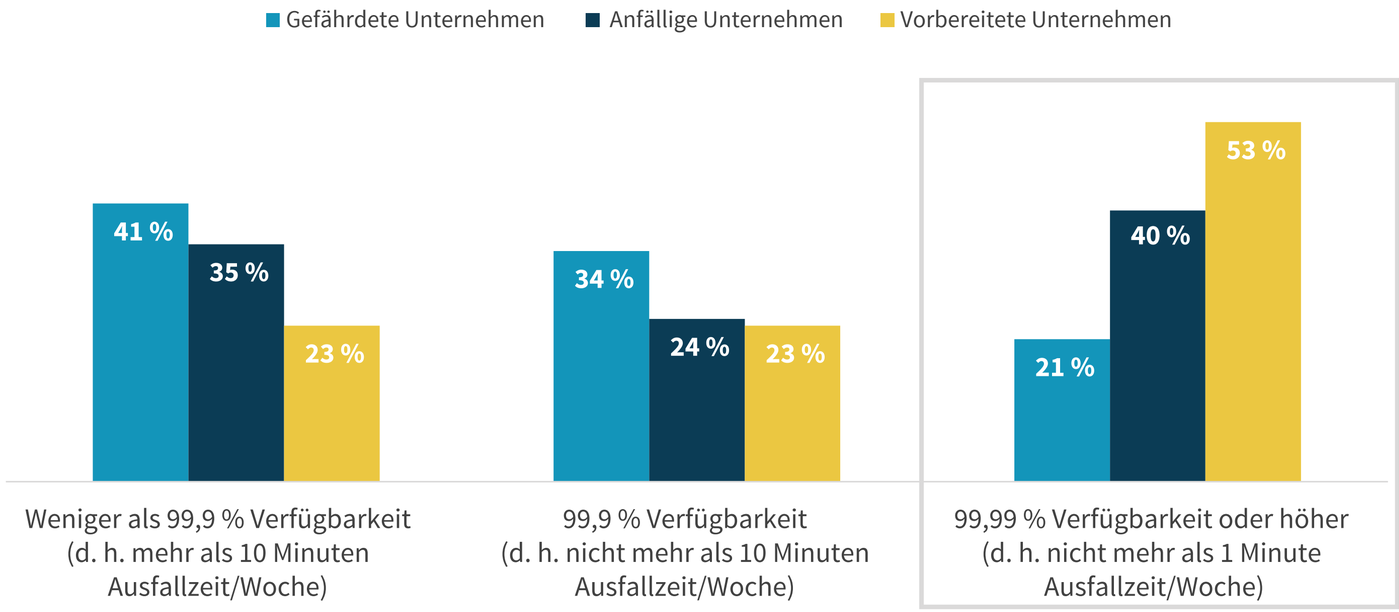
Vergleich der geschäftskritischen Anwendungsverfügbarkeit, die über die verschiedenen Stufen der Ausfallsicherheit bei Cyberangriffen hinweg erreicht wurde

Ebenso wichtig – wenn nicht gar wichtiger als qualitative Messungen für die Ausfallsicherheit – sind quantitative Messungen wie die Verfügbarkeit, die durchschnittliche Zeit zur Erkennung (Mean Time to Detect, MTTD) von Incidents und die durchschnittliche Zeit bis zur Wiederherstellung (Mean Time to Recover, MTTR) nach Incidents. All diese Faktoren werden in der Studie als Benchmark verwendet.

Im Zentrum der Ausfallsicherheit eines Unternehmens steht der Schutz geschäftskritischer Prozesse. Für IT- und Sicherheitsteams bedeutet dies, dass geschäftskritische Anwendungs-Workloads, die diese Prozesse unterstützen, betriebsbereit bleiben müssen.

Wenn wir den Erfolg von Unternehmen in diesem Bereich vergleichen, zeigt sich eine klare Kluft: Vorbereitete Unternehmen stellen 2,5-mal eher als gefährdete Unternehmen eine Verfügbarkeit von mindestens 99,99 % für ihre geschäftskritischen Anwendungen bereit (was eine Ausfallzeit von nicht mehr als 1 Minute pro Woche bedeutet, 53 % im Vergleich zu 21 %).

Was ist das typische Verfügbarkeits-SLA, das Ihr Unternehmen für geschäftskritische Workloads bereitstellt?



Vorbereitete Unternehmen sind

2,5-mal häufigere

in der Lage, eine Verfügbarkeit von mindestens 99,99 % für ihre geschäftskritischen Anwendungen bereitzustellen.

Zurück zum Inhaltsverzeichnis

Welche Vorteile bezüglich der Kosten für Ausfallzeiten erzielen vorbereitete Unternehmen?

Dank der Studie können wir diese wichtige Frage beantworten. Natürlich haben die Personalverstärkung, die Investitionen in mehr Ausfallsicherheitstechnologien und die rigorose Überprüfung von Drittanbieterrisiken eine Kostenkomponente. Die Daten zeigen jedoch, dass dabei ein signifikanter Return on Investment erzielt wird: Vorbereitete Unternehmen reduzieren die Ausfallzeiten geschäftskritischer Anwendungen um 44 %. Wir haben diese Daten mit den von den Befragten in der Studie angegebenen durchschnittlichen stündlichen Kosten für Ausfallzeiten kombiniert und diese wirtschaftlichen Auswirkungen mit der Gesamtzahl der geschäftskritischen Anwendungen multipliziert. Die Daten zeigen, dass vorbereitete Unternehmen einen Kostenvorteil von 33,3 Mio. US-Dollar pro Jahr bei den Kosten von Ausfallzeiten gegenüber gefährdeten Unternehmen erzielen.

[1] Von den Befragten angegebener Mittelwert für die Kosten von Ausfallzeiten = 205.000 US-Dollar. [2] Angenommene durchschnittliche Anzahl der unterstützten geschäftskritischen Anwendungen: 25 (konservative Annahme).

Zurück zum Inhaltsverzeichnis

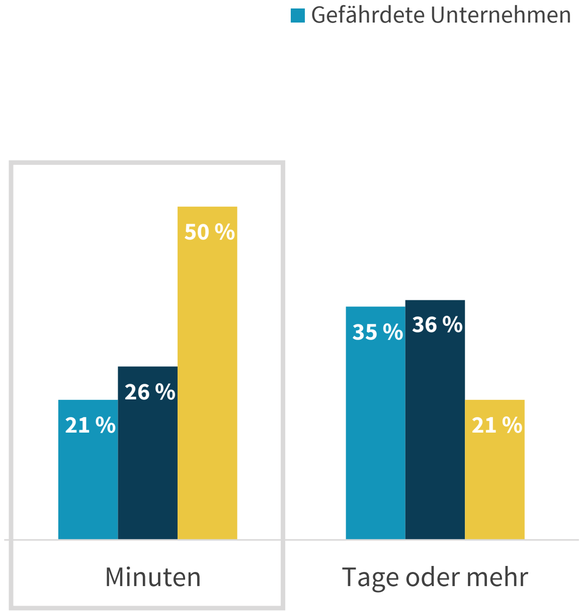
Agilität beim Umgang mit Warnmeldungen und der Reaktion auf Incidents über verschiedene Stufen der Ausfallsicherheit bei Cyberangriffen hinweg

Bei der Frage, wie vorbereitete Unternehmen eine höhere Betriebszeit und Verfügbarkeit bereitstellen, sind die Daten ebenfalls klar: Sie verfügen über eine weitaus größere Agilität als ihre Mitbewerber, wenn es um das Untersuchen und Identifizieren von sowie die Reaktion auf Incidents geht.

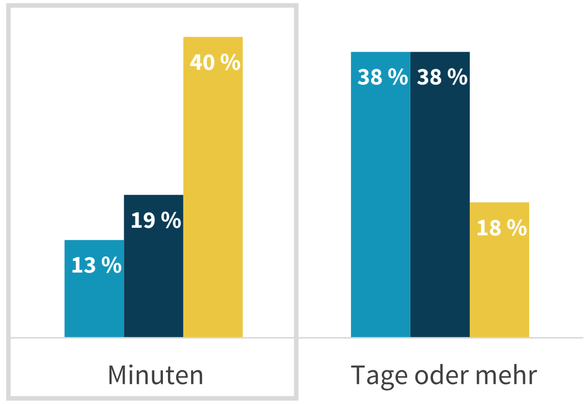
Beim Untersuchen und Identifizieren von Cyber-Incidents haben wir die MTTD wie folgt definiert: die Zeitdauer ab dem Zeitpunkt der Erzeugung einer Warnmeldung bis zu dem Zeitpunkt, an dem das Unternehmen diese Warnmeldung vollständig untersucht hat, um festzustellen, ob ein Sicherheits-Incident stattgefunden hat. Hier können vorbereitete Unternehmen Warnmeldungen 2,4-mal häufiger als gefährdete Unternehmen innerhalb weniger Minuten untersuchen (was zu einer 20 % schnelleren durchschnittlichen MTTD führt).

Zum Messen der Reaktionsagilität haben wir die MTTR als die durchschnittliche Zeitdauer ab der Cyber-Incident-Benachrichtigung bis zur vollständigen Wiederherstellung des Informationssystembetriebs definiert. Bei dieser Messung können vorbereitete Unternehmen die Wiederherstellung nach Incidents 3,1-mal häufiger in der Regel innerhalb weniger Minuten erreichen (was zu einer 35 % schnelleren durchschnittlichen MTTR führt).

Wie sieht die MTTD Ihres Unternehmens für geschäftskritische Workloads aus? (Prozentsatz der Befragten)



Wie sieht die MTTR Ihres Unternehmens für geschäftskritische Workloads aus? (Prozentsatz der Befragten)



Vorbereitete Unternehmen sind

2,4-mal häufiger

in der Lage, Warnmeldungen in der Regel innerhalb weniger Minuten zu untersuchen.

Vorbereitete Unternehmen sind

3,1-mal häufiger

in der Lage, eine Wiederherstellung nach Incidents in der Regel innerhalb weniger Minuten zu erreichen.

Zurück zum Inhaltsverzeichnis

Cybersichere Unternehmen übertreffen ihre Mitbewerber in Bezug auf Geschäftsergebnisse

Ausfallsichere Unternehmen bieten ein marktführendes EndnutzerInnenerlebnis

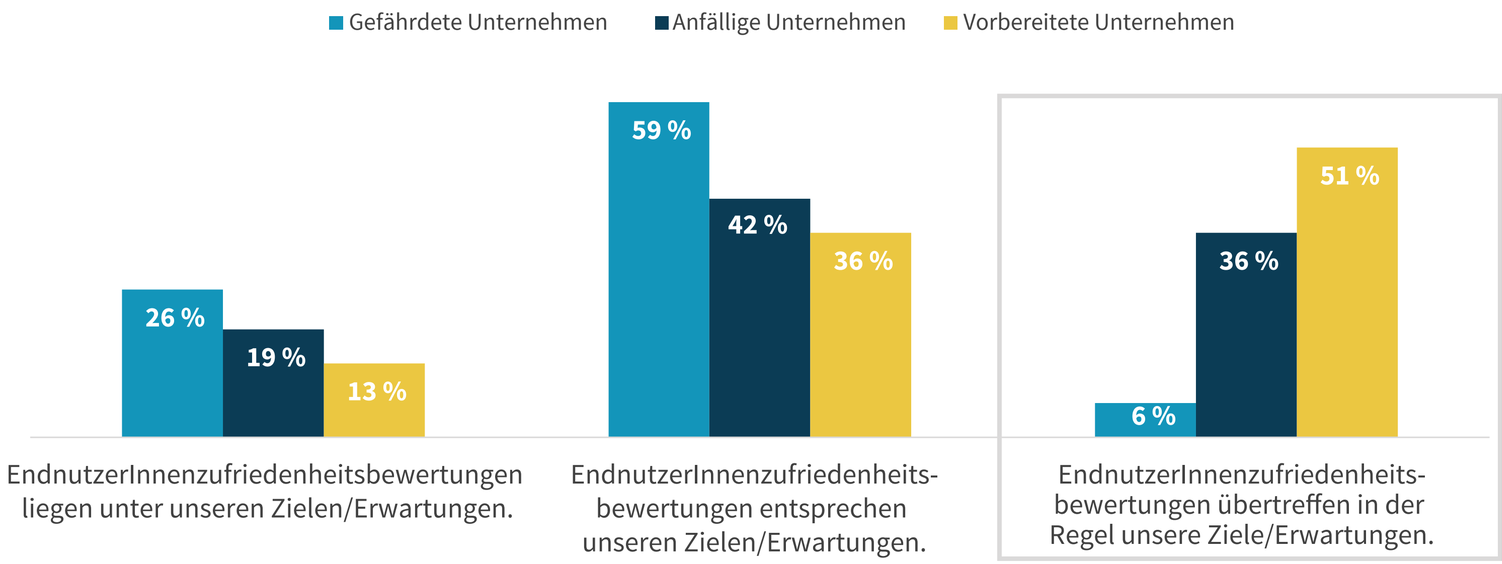
Ausfallsicherheit soll – wie viele Aspekte der IT – für EndnutzerInnen unsichtbar sein. Lücken bei der Ausfallsicherheit zeigen sich vor allem, wenn es zu unerwarteten Ereignissen kommt.

Die Daten zeigen, dass vorbereitete Unternehmen (im Vergleich zu ihren Mitbewerbern) bessere Arbeit leisten, um Unterbrechungen zu begrenzen. Die Daten zeigen auch, dass dies zu einer verbesserten EndnutzerInnenzufriedenheit führt.

Wir fragten die TeilnehmerInnen, wie die IT-Abteilung im Hinblick auf ihre Ziele für die EndnutzerInnenzufriedenheit abschneidet. Die Mehrheit der vorbereiteten Unternehmen gibt an, dass sie ihre Ziele in der Regel übertrifft. Tatsächlich sagen vorbereitete Unternehmen 8,5-mal häufiger als gefährdete Unternehmen, dass ihre Bewertungen der EndnutzerInnenzufriedenheit in der Regel ihre Ziele übertreffen.

Es besteht eine klare Korrelation zwischen der Ausfallsicherheitsstufe und der Fähigkeit der IT, das von den Geschäftsbereichen verlangte EndnutzerInnenerlebnis bereitzustellen.

Wie schneidet Ihre IT-Abteilung im Allgemeinen im Hinblick auf formale Ziele für die EndnutzerInnenzufriedenheit ab? (Prozentsatz der Befragten)



Vorbereitete Unternehmen sind

8,5-mal häufiger

in der Lage, anzugeben, dass ihre Bewertungen der EndnutzerInnenzufriedenheit in der Regel ihre Ziele übertreffen.

Zurück zum Inhaltsverzeichnis

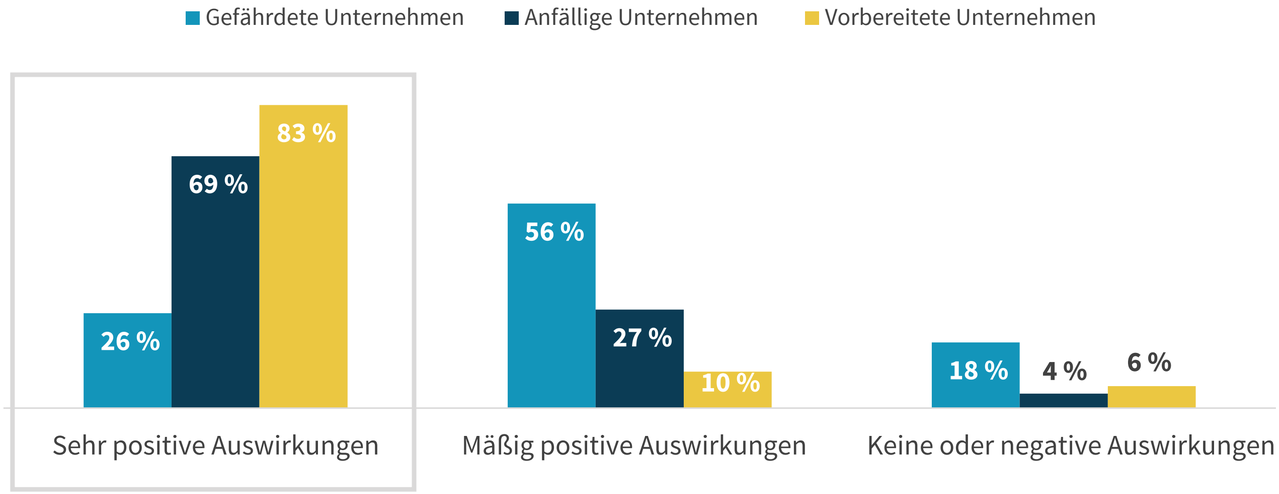
Mehr als nur Korrelation: Ausfallsicherheit fördert die Verbesserung des EndnutzerInnenerlebnisses

Natürlich ist Korrelation nicht gleich Kausalität. Aber die Studie zeigt einen definitiven kausalen Zusammenhang zwischen Investitionen in Ausfallsicherheit und einem besseren EndnutzerInnenerlebnis.

Wir haben gefragt, ob die Befragten der Ansicht sind, dass sich die Investitionen ihrer Unternehmen in Ausfallsicherheit positiv, neutral oder negativ auf Dinge wie Agilität, Innovationen und EndnutzerInnenerlebnis ausgewirkt haben. 87 % gaben eine positive Auswirkung an.

Wenn wir etwas tiefer gehen und die Daten nach Ausfallsicherheitsstufe untersuchen, zeigt sich, dass vorbereitete Unternehmen 3,2-mal häufiger als gefährdete Unternehmen eine sehr positive Auswirkung ihrer Investitionen in Ausfallsicherheit auf EndnutzerInnenerlebnis, Agilität und Innovationen sehen.

Haben sich die Investitionen Ihres Unternehmens in Ausfallsicherheit positiv/neutral/negativ auf Agilität, Innovation und EndnutzerInnenerlebnis ausgewirkt? (Prozentsatz der Befragten)



Vorbereitete Unternehmen sind

3,2-mal häufiger

in der Lage, anzugeben, dass ihre Investitionen in Ausfallsicherheit sehr positive Auswirkungen haben.

Zurück zum Inhaltsverzeichnis

Wie Investitionen in Ausfallsicherheit eine messbare Auswirkung für das Geschäft erzielen

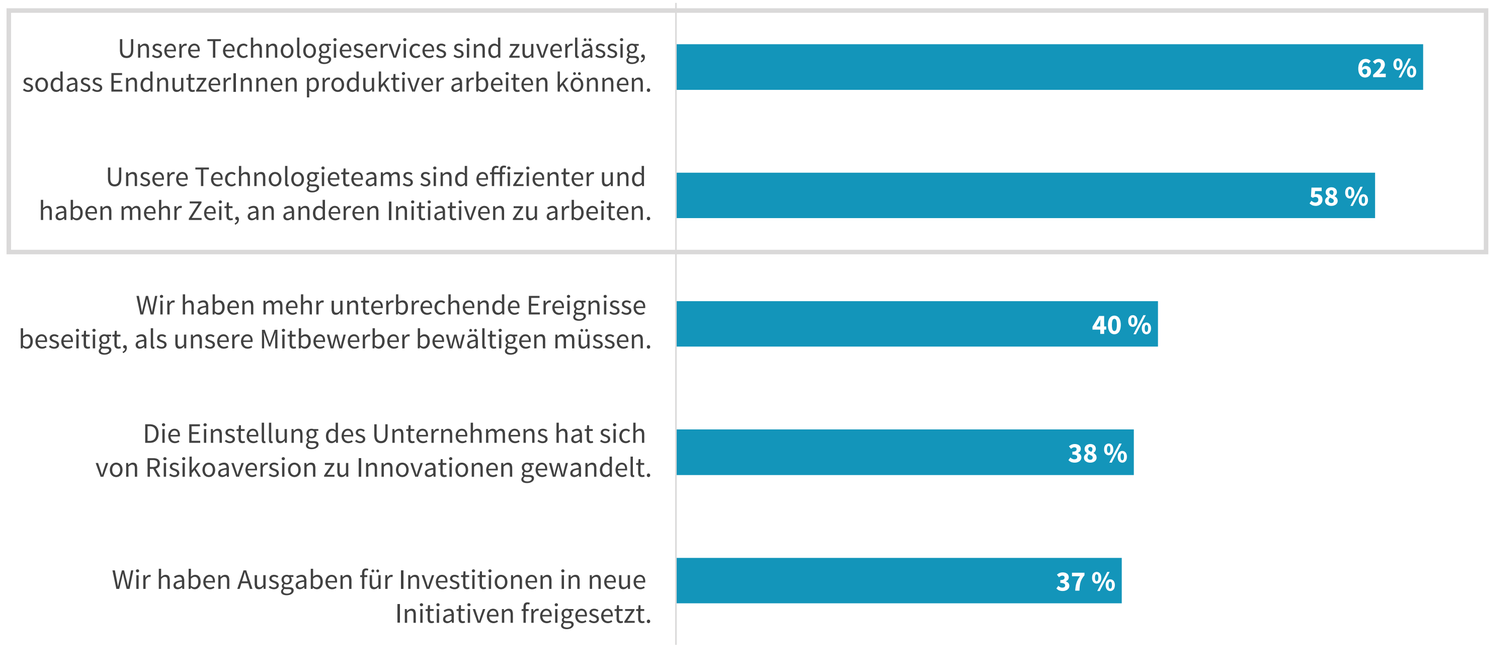
Die Frage, wie Ausfallsicherheit die geschäftlichen Fähigkeiten verbessert, ist interessant und wird in der Studie beantwortet.

Zwei wichtige und sich ergänzende Auswirkungen stechen hervor. Erstens wird Ausfallsicherheit Ihre geschäftlichen Stakeholder und Ihre Profitcenter begeistern: 62 % der Befragten geben an, dass ihre Investitionen sicherstellen, dass die Technologieservices, die EndnutzerInnen benötigen, um effektiv und effizient zu sein, verfügbar und leistungsfähig sind.

Zweitens geben 58 % der Befragten an, dass eine Investition in eine solide Grundlage für Ausfallsicherheit bedeutet, dass Technologieteams weniger Brände bekämpfen müssen. So können sie ihre Bemühungen darauf konzentrieren, innovative Projekte und Initiativen zu unterstützen und zu beschleunigen, die ihren Unternehmen einen Wettbewerbsvorteil verschaffen.

“Zwei wichtige und sich ergänzende Auswirkungen stechen hervor.“

Inwiefern tragen Investitionen in Ausfallsicherheit zum Erfolg Ihres Unternehmens bei? (Prozentsatz der Befragten)



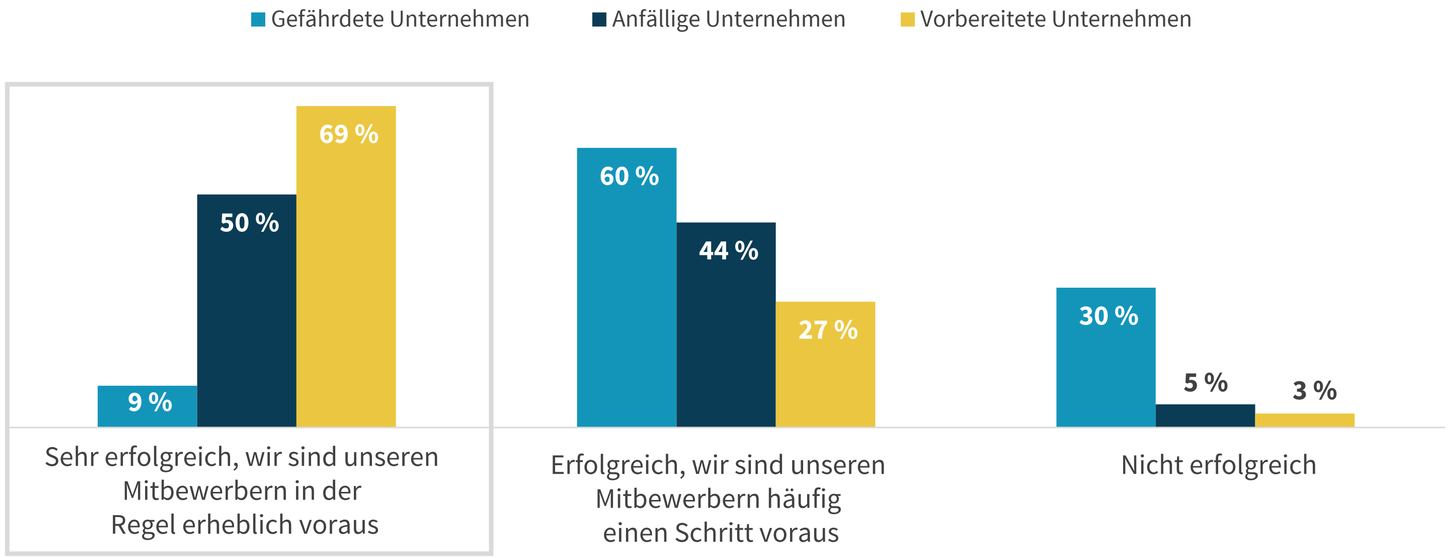
Zurück zum Inhaltsverzeichnis

Ausfallsichere Unternehmen können Innovationen besser unterstützen

Überzeugende Daten weisen darauf hin, dass Ausfallsicherheit Innovationen im Unternehmen unterstützen kann. Vorbereitete Unternehmen können 7,7-mal häufiger als gefährdete Unternehmen neue Angebote in der Regel vor der Konkurrenz auf den Markt bringen.

Auf die Bitte, diesen Vorteil ausführlicher zu erläutern, geben vorbereitete Unternehmen als Durchschnittswert an, dass ihre Unternehmen ihren Mitbewerbern bei der Markteinführung in der Regel mehr als 8 Monate voraus sind. Das ist ein signifikanter Pioniervorteil.

Wie erfolgreich ist Ihr Unternehmen im Vergleich zur Konkurrenz bei der Entwicklung und Einführung neuer Produkte und Services? (Prozentsatz der Befragten)



Vorbereitete Unternehmen sind

7,7-mal häufiger

in der Lage, neue Angebote vor der Konkurrenz auf den Markt zu bringen.

Zurück zum Inhaltsverzeichnis

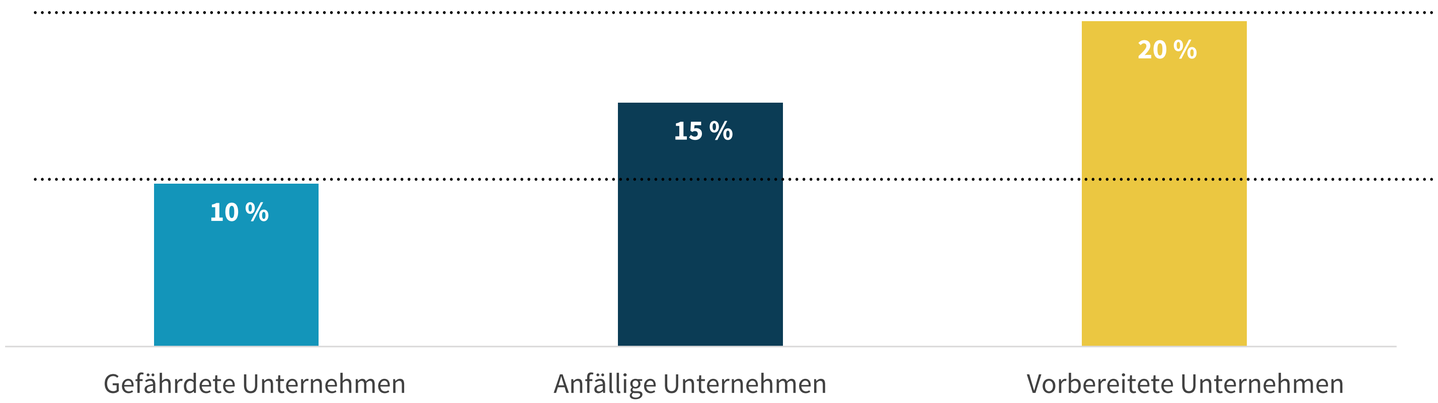
Ausfallsichere Unternehmen sind bezüglich zukünftiger Umsatzsteigerungen optimistischer

Neben Innovationen gibt es auch eine überzeugende Korrelation zwischen Ausfallsicherheit und Wachstum.

Wir baten die Befragten, die Rate zu prognostizieren, mit der sich der Bruttoumsatz ihrer Unternehmen in den nächsten Jahren erwartungsgemäß ändert.

Im Durchschnitt (Median) gehen die Befragten aus vorbereiteten Unternehmen davon aus, dass der Umsatz ihres Unternehmens doppelt so schnell wächst wie in gefährdeten Unternehmen.
Die Fähigkeit dieser Unternehmen, Unterbrechungen zu vermeiden, die Produktivität der MitarbeiterInnen sicherzustellen und Innovationen zu unterstützen, spielt eine wichtige Rolle bei der Verbesserung des Geschäftsoptimismus der Befragten.

Wie hoch ist die erwartete jährliche Rate, mit der Ihr Unternehmen seinen Bruttoumsatz in den kommenden Jahren steigern (oder verringern) wird? (Mittlere jährliche Wachstumsrate)



Vorbereitete Unternehmen prognostizieren, dass der Umsatz ihres Unternehmens

2-mal schneller steigen wird

als bei gefährdeten Unternehmen.

Zurück zum Inhaltsverzeichnis

So werden Sie zu einem cybersicheren Unternehmen

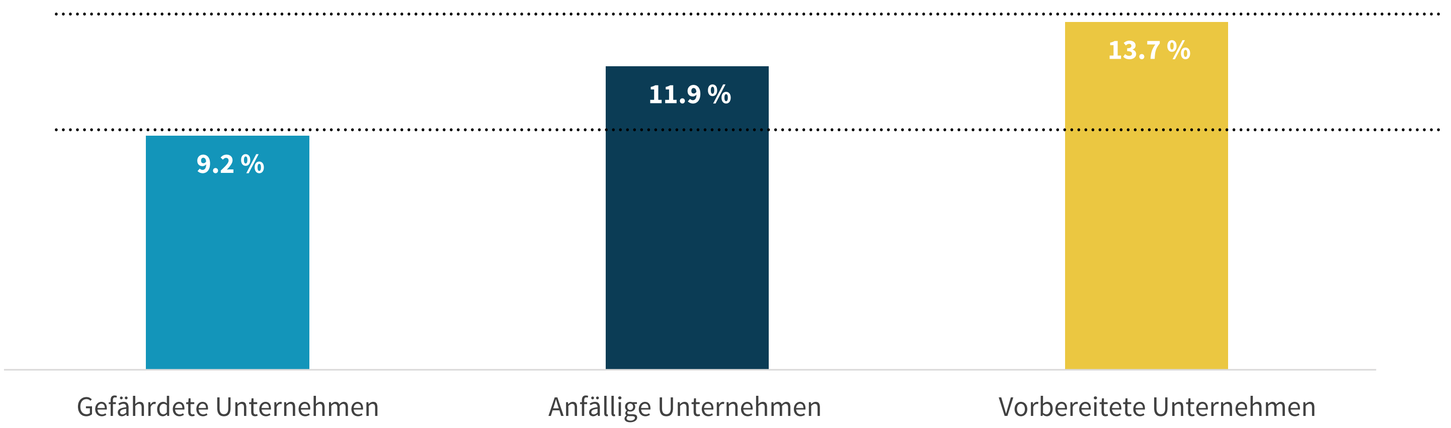
Vorbereitete Unternehmen weisen mehr ihrer Technologieausgaben der Cybersicherheit zu als ihre Mitbewerber

Basierend auf unseren Segmentierungskriterien wissen wir, dass vorbereitete Unternehmen Cybersicherheits- und Ausfallsicherheitstechnologien auf einem ihrer Meinung nach „optimalen“ Level finanzieren. Anfällige und gefährdete Unternehmen sehen dagegen Raum für Verbesserungen.

Aber diese Daten in einem Vakuum sind für IT- und Sicherheitsführungskräfte nicht verwertbar. Um etwas tiefer zu gehen, fragten wir die TeilnehmerInnen, welcher Prozentsatz der Technologieausgaben für Cybersicherheit aufgewendet wird. Wir haben festgestellt, dass vorbereitete Unternehmen fast 14 % ihres Technologiebudgets für Cybersicherheit ausgeben – 49 % mehr als ihre gefährdeten Mitbewerber.

Unternehmen mit Ausgaben unter diesem Schwellenwert sollten die Mittel neu zuweisen, um sich an den Marktführern auszurichten.

Welcher Prozentsatz des IT-Budgets Ihres Unternehmens wird der Cybersicherheit zugewiesen? (Geschätzter Mittelwert)



Im Durchschnitt investieren vorbereitete Unternehmen

49 % mehr

ihres Technologiebudgets in die Bereiche Cybersicherheit/Ausfallsicherheit.

Zurück zum Inhaltsverzeichnis

Vorbereitete Unternehmen wenden mehr Humankapital für Sicherheit und Ausfallsicherheit auf

Ähnlich wie bei der Finanzierung sind vorbereitete Unternehmen der Meinung, dass ihre Sicherheitsteams (einschließlich sicherheitsorientierter IT-ExpertInnen) gut besetzt sind. Wenn wir jedoch die durchschnittliche Anzahl zugewiesener VollzeitmitarbeiterInnen nach Ausfallsicherheitsstufe betrachten, sehen wir, wie groß der Unterschied ist.

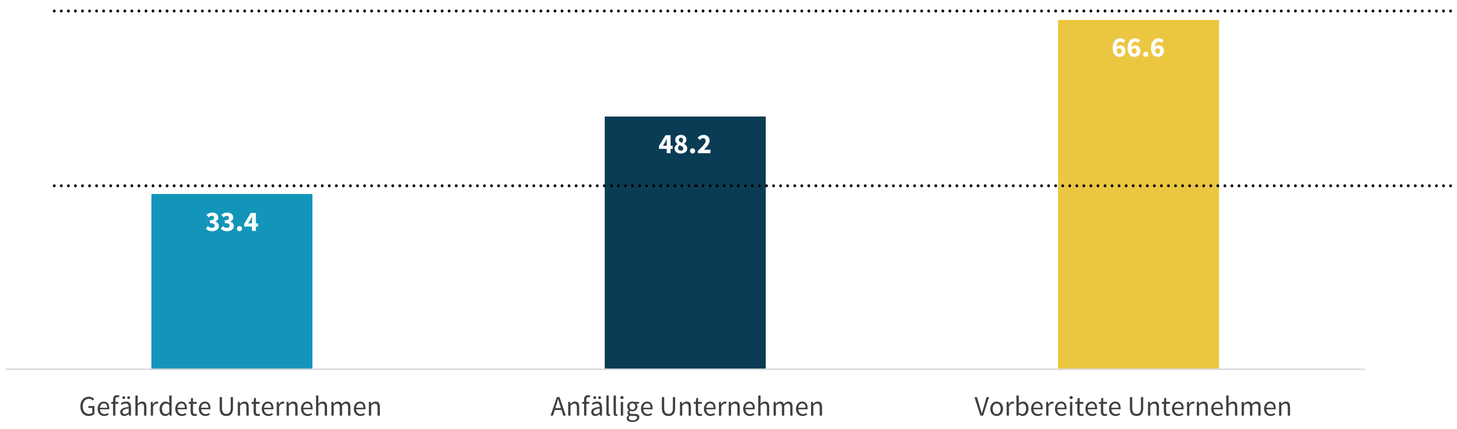
Im Durchschnitt beschäftigen vorbereitete Unternehmen doppelt so viele VollzeitmitarbeiterInnen in ihren Sicherheitsteams wie gefährdete Unternehmen (66,6 VollzeitmitarbeiterInnen im Vergleich zu 33,4).

Durch die Betrachtung dieser Daten nach Unternehmensgröße können diese Informationen noch besser verwertet werden.

- Vorbereitete Midmarket- und mittelständische Unternehmen (250 bis 4.999 MitarbeiterInnen) beschäftigen 62 VollzeitmitarbeiterInnen im Vergleich zu 27,7 VollzeitmitarbeiterInnen bei ihren gefährdeten Mitbewerbern.

- Vorbereitete Großunternehmen (über 5.000 MitarbeiterInnen) beschäftigen 76,8 VollzeitmitarbeiterInnen im Vergleich zu 47,8 VollzeitmitarbeiterInnen bei ihren gefährdeten Mitbewerbern.

Ungefähr wie viele dedizierte VollzeitmitarbeiterInnen sind Teil des internen Cybersicherheitsteams Ihres Unternehmens (einschließlich der IT-Rollen, die sich auf Cybersicherheit konzentrieren)? (Geschätzter Mittelwert)



Im Durchschnitt beschäftigen vorbereitete Unternehmen

doppelt so viele VollzeitmitarbeiterInnen

in ihrem Sicherheitsteam.

Zurück zum Inhaltsverzeichnis

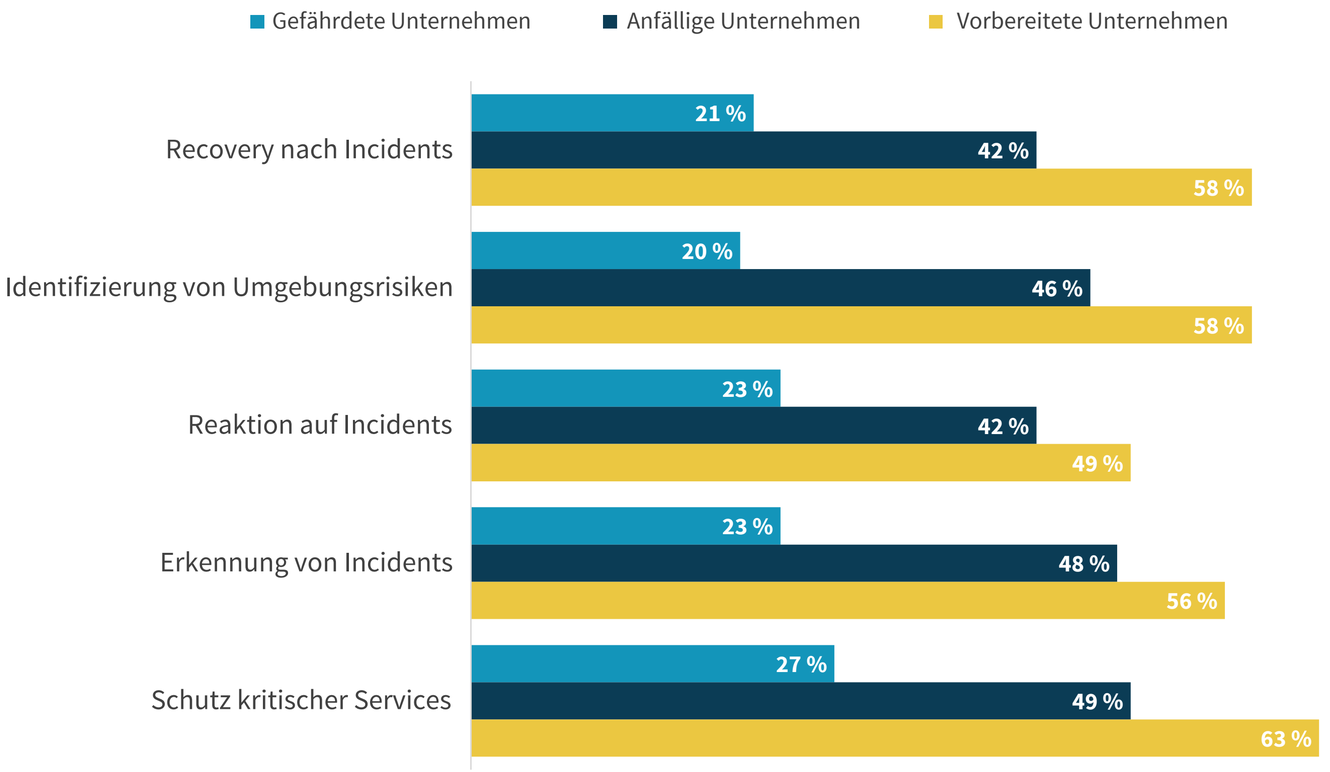
Vorbereitete Unternehmen haben ihre Investitionen über den gesamten Risikolebenszyklus hinweg verstärkt

In der Umfrage wurden die Befragten gebeten, ihre Investitionen über den gesamten Risikolebenszyklus (gemäß Definition durch NIST CSF) von der Identifizierung von Risiken bis hin zur Wiederherstellung nach Incidents zu betrachten.

Der rote Faden? Vorbereitete Unternehmen haben mit viel höherer Wahrscheinlichkeit als ihre Mitbewerber ihre Investitionen in allen Bereichen im Jahresvergleich um mehr als 15 % gesteigert.

Dieses Verhalten unterstreicht die Wichtigkeit einer Defense-in-Depth-Risikostrategie, damit Unternehmen über die Ressourcen zur Risikominderung bei jedem Schritt verfügen.

In welche der folgenden Risikominderungsbereiche hat ihr Unternehmen in den letzten 12 bis 24 Monaten mehr als 15 % im Jahresvergleich neu investiert? (Prozentsatz der Befragten)



Zurück zum Inhaltsverzeichnis

Vorbereitete Unternehmen verstärken ihre Umgebung mit intrinsisch sicheren Technologien

Dieses E-Book konzentriert sich auf das Konzept der Ausfallsicherheit von Unternehmen und die damit verbundenen allgemeinen Ergebnisse. Die Studie befasste sich weiter mit Aspekten der Umgebungen von Unternehmen – von Storage über Server bis hin zu Client-Geräten.

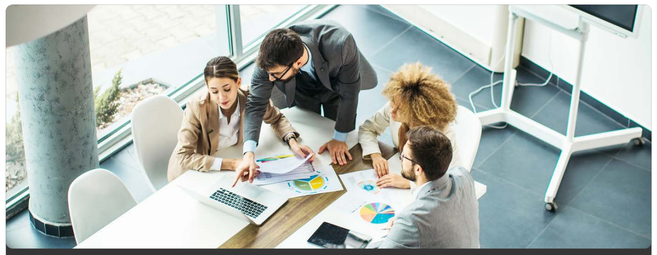
In jedem Bereich sind vorbereitete Unternehmen marktführend, wenn es um die Einführung von Technologien mit intrinsischen Sicherheitsfunktionen und eine herausragende Performance durch kürzere und weniger häufige Ausfallzeiten bis hin zu selteneren Gerätebeschädigungen geht.

Vorbereitete Unternehmen reduzieren Ausfälle und Datenverluste in ihrer Storage-Umgebung mit Storage-Lösungen mit intrinsischen Data-Protection-Funktionen.

ÜBERSICHT LESEN

Vorbereitete Unternehmen fördern Innovationen mit intelligenter Sicherheitsautomatisierung in ihrer Compute-Umgebung.

ÜBERSICHT LESEN



Vorbereitete Unternehmen reduzieren Gerätebeschädigungen und begrenzen Datenverluste durch Client-Technologien mit intrinsischen Sicherheitsfunktionen, die zu überzeugenden MitarbeiterInnenerfahrungen führen.

ÜBERSICHT LESEN

Vorbereitete Unternehmen priorisieren die Einführung von Technologielösungen mit intrinsischer Sicherheit. Erfahren Sie mehr über dieses Konzept und die Gründe.

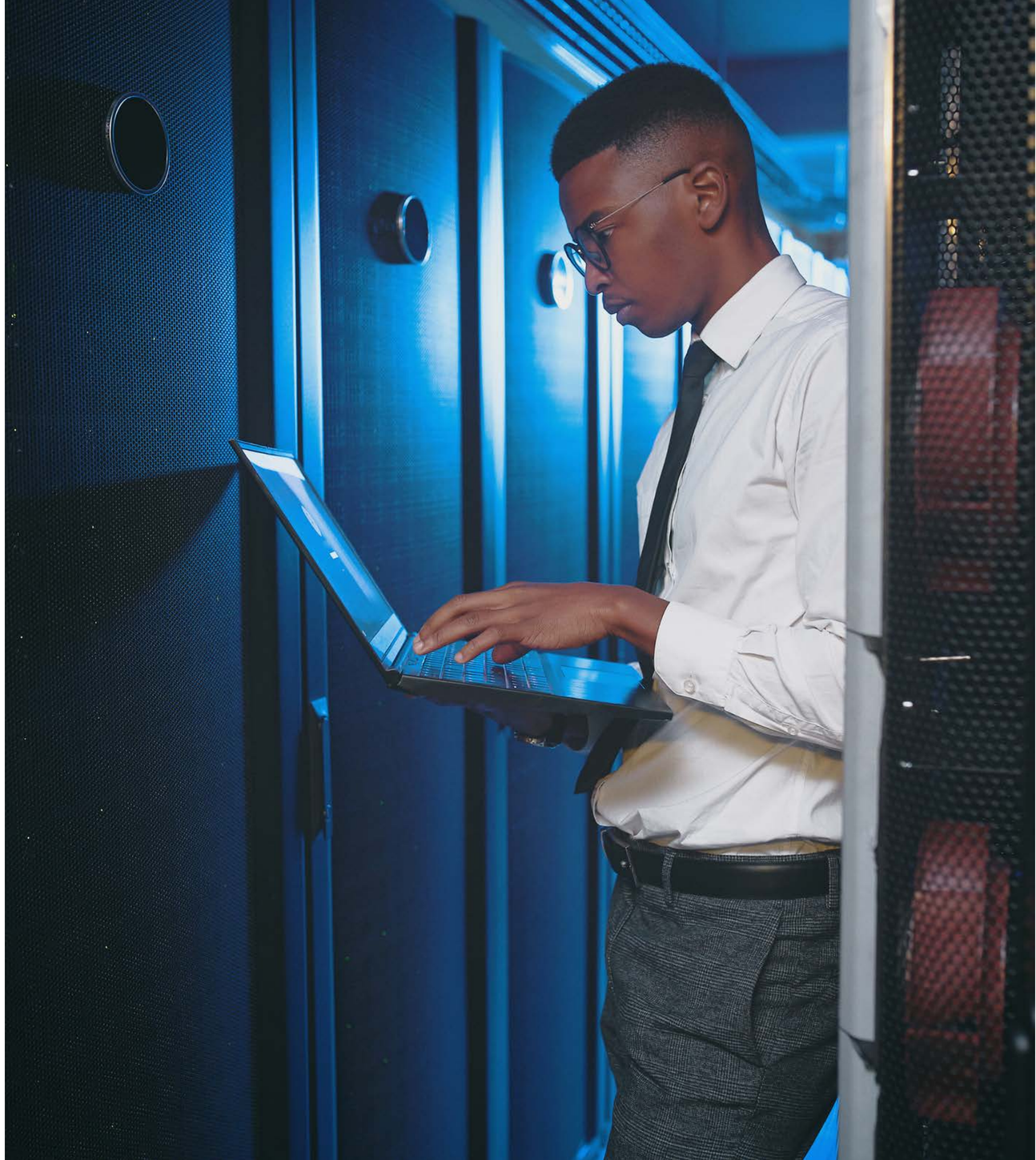
ÜBERSICHT LESEN

Zurück zum Inhaltsverzeichnis

Fazit

Ob aufgrund ihrer Fähigkeit, die Produktivität ihrer EndnutzerInnen aufrechtzuerhalten, schnell auf Sicherheits-Incidents zu reagieren oder technischen Teams Kapazitäten für wichtige IT-Transformationsinitiativen zu verschaffen – vorbereitete Unternehmen liefern überzeugende, datengestützte Argumente dafür, Ausfallsicherheit zu priorisieren. Je nachdem, an welchem Punkt sich Ihr Unternehmen heute befindet, kann diese Reise überwältigend erscheinen, aber diese Ergebnisse liefern einen überzeugenden Business Case.

Wie Dell Technologies helfen kann



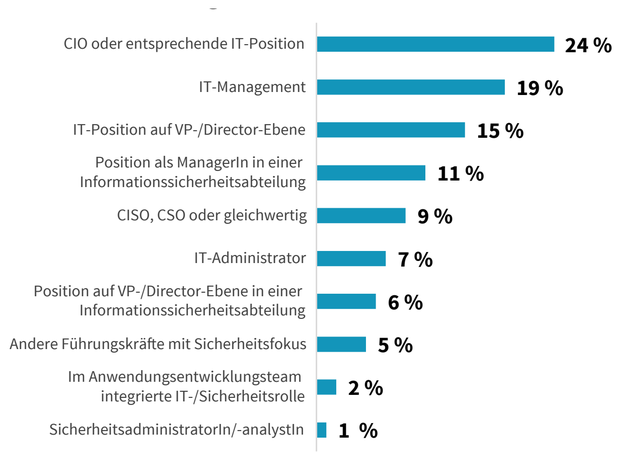
Demografische Daten

Die Daten in diesem Bericht stammen aus einer zwischen dem 11. Januar und dem 07. Februar 2022 durchgeführten Umfrage. Diese Zahlen beschreiben die demografischen Daten der Befragten in Nordamerika (N = 187), Westeuropa (N = 185), APAC (N = 179) und LATAM (N = 199).

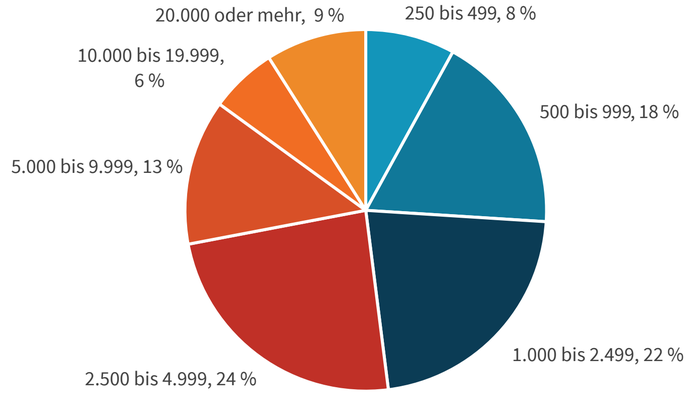
Die Gesamtsummen in den Abbildungen und Tabellen in diesem Bericht ergeben aufgrund der Rundung möglicherweise nicht 100 %.

Die Fehlermarge für eine Stichprobengröße von 750 auf einem Konfidenzniveau von 95 % liegt bei +/-4 Prozentpunkten.

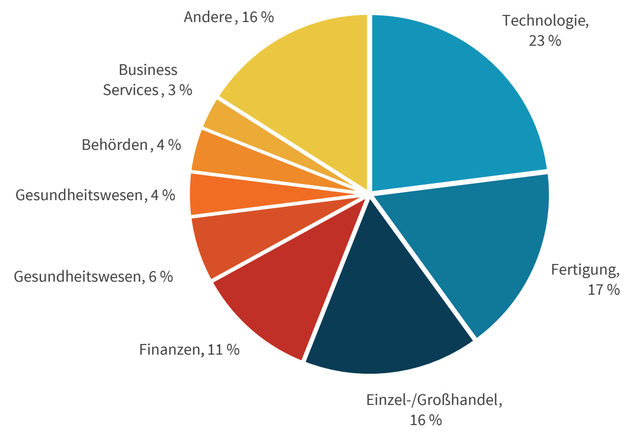
BEFRAGTE NACH POSITION



BEFRAGTE NACH UNTERNEHMENSGRÖSSE



BEFRAGTE NACH BRANCHE



Zurück zum Inhaltsverzeichnis

Informationen zu Dell Technologies, Intel und VMware

Technologie war noch nie so wichtig wie im heutigen datengesteuerten Zeitalter und Dell ist der Ansicht, dass sie eine überwältigende Kraft für das Gute ist. Wir sind bestrebt, die Rolle der Technologie beim menschlichen Fortschritt zu schützen, indem wir Ihnen helfen, Angriffe zu antizipieren und sich davor zu schützen, damit Sie selbstbewusst an Ihrer neuesten Innovation arbeiten können.

Dell Technologies und Intel arbeiten in der On-Premise-, der in der Public-Cloud- oder der Edge-Umgebung zusammen, um eine optimale Performance für ein breites Angebot an Workloads zu gewährleisten. Das datenzentrierte Portfolio von Intel basiert auf jahrzehntelangen Anwendungsoptimierungen, mit denen Ihr Unternehmen schneller vorankommen, mehr speichern und alles vom Edge bis zur Cloud verarbeiten kann.

VMware und Dell bieten gemeinsam einen einzigartigen Mehrwert für unsere gemeinsamen Kunden. Unsere integrierten Plattformen und Lösungen in Kombination mit intensiven Kundenprojekten und einem globalen Ansatz beschleunigen den Weg zur digitalen Transformation. Die innovative Anwendungsmodernisierung, Multi-Cloud und Anywhere Workspace-Software von VMware wird zusammen mit dem umfassenden IT-Portfolio von Dell Technologies, das von Endpunkten bis zur Cloud reicht, eingesetzt, um Kunden dabei zu unterstützen, einen sicheren, konsistenten Betrieb und eine schnellere Time-to-Value zu erzielen.

Zurück zum Inhaltsverzeichnis

Die Enterprise Strategy Group ist ein integriertes Technologieanalyse-, Forschungs- und Strategieunternehmen, das Marktinformationen, verwertbare Erkenntnisse und Go-to-Market-Contentservices für die globale Technologiecommunity bereitstellt.