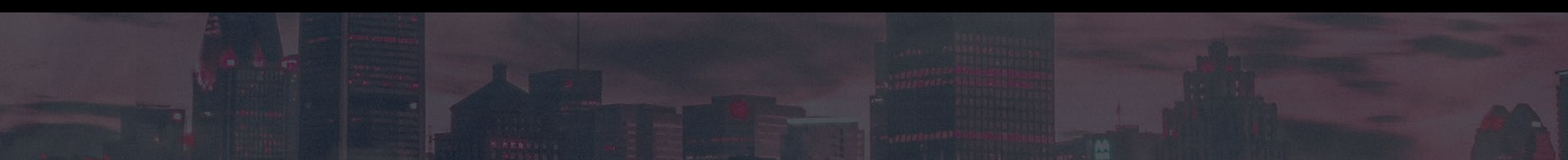
CYBER RECOVERY READINESS REPORT

2024

Commvault®

In partnership with GIGAOM



Sehr geehrte/r Leser/in,

seien Sie bei einem entscheidenden Moment in der Entwicklung der Cyber-Resilienz mit dabei. Seit der Gründung von „The Collaborative“ Anfang 2024 ist unser Ziel klar: Starke Partnerschaften mit Analysten, Branchenführern und Visionären wie Ihnen zu knüpfen, um die Cyber-Resilienz in verschiedenen Unternehmen zu erforschen und zu verbessern. Unser Grundlagenbericht „Seven Emerging Trends in Cyber Resilience (Sieben neue Trends im Bereich der Cyber-Resilienz)“ hat bereits die Richtung für dieses Jahr vorgegeben und sich, angesichts der zunehmenden Bedrohung durch Ransomware, mit kritischen Bereichen befasst.

Wir freuen uns, die Veröffentlichung des Cyber Recovery Readiness Reports 2024 ankündigen zu können, einer Zusammenarbeit zwischen Commvault und GigaOm. Ihre Führungsposition und Ihr Fachwissen in den Bereichen IT und Sicherheit sind entscheidend, um in Zukunft eine erhöhte Cyber-Resilienz erzielen zu können. Dieser Bericht ist dazu konzipiert, Ihnen wichtige Erkenntnisse und Daten zu vermitteln und Ihr Unternehmen dazu zu befähigen, in einer zunehmend volatilen Cyberlandschaft immer einen Schritt vorauszubleiben.

Unsere Erkenntnisse stammen aus einer umfassenden Umfrage unter 1.000 führenden Unternehmen im Bereich Cybersicherheit und IT auf der ganzen Welt. Dieser Bericht bietet nicht nur einen weltweiten Überblick über die Herausforderungen, sondern zeigt auch wirksame Strategien auf, die für die Cyber Recovery-Fähigkeit unerlässlich sind. Er unterstreicht den dringenden Bedarf an umfassenden Cyber Recovery-Strategien, die über herkömmliche Disaster Recovery-Pläne hinausgehen.

Zentrale Erkenntnisse

- Unglaubliche 83 % der Unternehmen haben in letzter Zeit eine schwerwiegende Sicherheitsverletzung erlitten, wobei mehr als die Hälfte davon allein im vergangenen Jahr betroffen war. Dies zeigt den dringenden Bedarf an modernen Recovery-Maßnahmen und agilen Reaktionsstrategien.
- Die widerstandsfähigsten Unternehmen nutzen gängige Praktiken, die ihre Recovery-Fähigkeit erheblich verbessern. Unsere Analyse zeigt, dass die am besten vorbereiteten Unternehmen mindestens vier der fünf Indikatoren für Cyber-Reife aufweisen.
- Es besteht ein klarer Zusammenhang zwischen Cyber-Reife und Recovery-Geschwindigkeit. Unternehmen mit einem höheren Cyber-Reifegrad erholen sich von Sicherheitsverstößen um 41 % schneller als Unternehmen, die schlechter vorbereitet sind.
- Regelmäßige Tests der Cyber-Recovery-Pläne sind nicht nur von Vorteil, sondern unerlässlich. Unsere Daten zeigen einen deutlichen Unterschied in der Testhäufigkeit bei Unternehmen, die eine Sicherheitsverletzung erlitten haben gegenüber Unternehmen, bei denen dies nicht der Fall war.

Empfehlungen:

1. Testen und verbessern Sie Ihre Recovery-Pläne regelmäßig. Häufige Übungen und Updates sorgen dafür, dass Ihr Unternehmen schnell und effektiv auf Cybervorfälle reagieren kann.
2. Priorisieren Sie den Ausbau der Cyber-Reife, indem Sie die identifizierten Indikatoren für Cyber-Fähigkeit umsetzen. Dadurch werden nicht nur Risiken minimiert, sondern auch die Auswirkungen potenzieller Verstöße erheblich verringert.
3. Entwickeln Sie eine ganzheitliche Cyber Recovery-Strategie, die über die bloße Datensicherung hinausgeht und eine vollständige Systemwiederherstellung beinhaltet sowie eine umfassende Geschäftskontinuität gewährleistet.

Wir laden Sie ein, tiefer in den Bericht einzutauchen und diese Erkenntnisse und Empfehlungen in Ihre strategische Planung zu integrieren. Unser Ziel ist nicht nur, Sie zu informieren, sondern Sie dazu anzuregen, entscheidende Maßnahmen zu ergreifen, um Ihr Unternehmen gegen zukünftige Cyberbedrohungen zu stärken.

Wir sind hier, um Sie auf dem Weg zu einer herausragenden Cyber-Fähigkeit zu unterstützen.

Vielen Dank!

The Collaborative

INHALT

Aus Schaden wird man klug 4

Cyber-Herausforderungen, die es zu bewältigen gilt 7

Indikatoren für Cyber-Reife 9

Machen Sie keine halben Sachen 11

Cyber-fähige Unternehmen erholen sich schneller 12

Cyber-Recovery ist mehr als Disaster Recovery 13

Recovery-Bereitschaft braucht Fähigkeiten, Kompetenzen und Kultur 14

Tests sind die Grundlage von Cyber-Resilienz und Cyber-Fähigkeit 15

Warum Cyber-Fähigkeit wichtig ist – Die Auswirkungen eines Verstoßes minimieren 16

Zusammenfassung 17

Demografische Daten 18

AUS SCHADEN WIRD MAN KLUG

Die Erfahrung eines Sicherheitsverstoßes hat einen erheblichen Einfluss darauf, wie ein Unternehmen das Thema Resilienz angeht

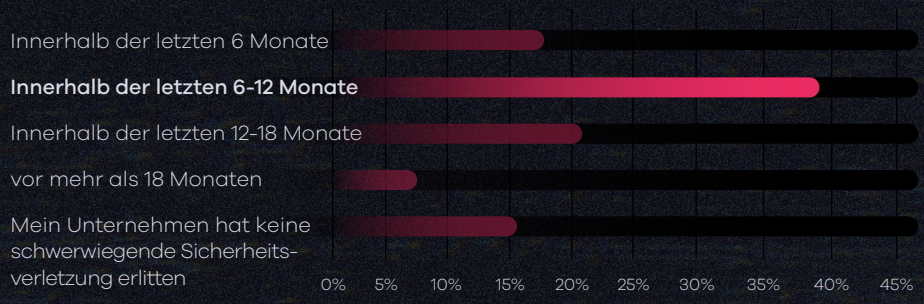
Leider passieren Verstöße viel zu häufig und betreffen Unternehmen aller Größen in allen Branchen. Wie bei jedem dramatischen Erlebnis, verändert die Erfahrung einer Sicherheitsverletzung, wie sich ein Unternehmen verhält und seine Handlungen priorisiert. Dies waren einige der Ergebnisse unseres ersten Cyber Recovery Readiness Reports, einer gemeinsamen Initiative von Commvault und GigaOm.

Wir befragten 1.000 Führungskräfte im Cyber Security und IT-Bereich aus aller Welt, um mehr über den globalen Status der Cyber-Fähigkeit zu erfahren und ein klares Verständnis dafür zu erhalten, wie Unternehmen trotz des Chaos und der Schäden, die eine Sicherheitsverletzung verursacht, widerstandsfähig bleiben. Weitere Einzelheiten zu unserer Methodik und den Befragten finden Sie auf Seite 17.

Unsere Umfrage bestätigte die weite Verbreitung von Sicherheitsverstößen. 83 % unserer Befragten gaben an, einen schwerwiegenden Sicherheitsverstoß erlitten zu haben: Über 50 % davon im vergangenen Jahr und über 75 % in den letzten 18 Monaten (Abbildung 1). Da Verstöße bis zu 12 Millionen US-Dollar pro Tag kosten, ist die Fähigkeit, sich schnell davon erholen zu können, von essenzieller Bedeutung[1].

Abbildung 1

Wann war Ihr Unternehmen das letzte Mal Opfer einer massiven Sicherheitsverletzung?



83% der Befragten meldeten eine schwerwiegende Sicherheits- verletzung. Über **50%** davon im letzten Jahr.

1 SolarWinds: Pingdom Team, Average Cost of Downtime per Industry, Jan 9, 2023.

Eine wichtige Erkenntnis unserer Umfrage ist, dass sich aus einer Sicherheitsverletzung viele Lehren ziehen lassen.

Unternehmen machen Erfahrungen, die ihre Perspektive, ihre Priorisierung und oft ihren Reifegrad verändern. So ist beispielsweise die Wahrscheinlichkeit, dass Unternehmen, die einen Verstoß zu verzeichnen hatten, bei ihrer Cyber-Recovery-Strategie das Verständnis für das Risikoprofil ihrer Daten, die Datenklassifizierung und das Risikolevel zur obersten Priorität erklären, fast 2,5-mal höher als bei Unternehmen, bei denen kein Verstoß vorliegt (Abbildung 2).

Abbildung 2

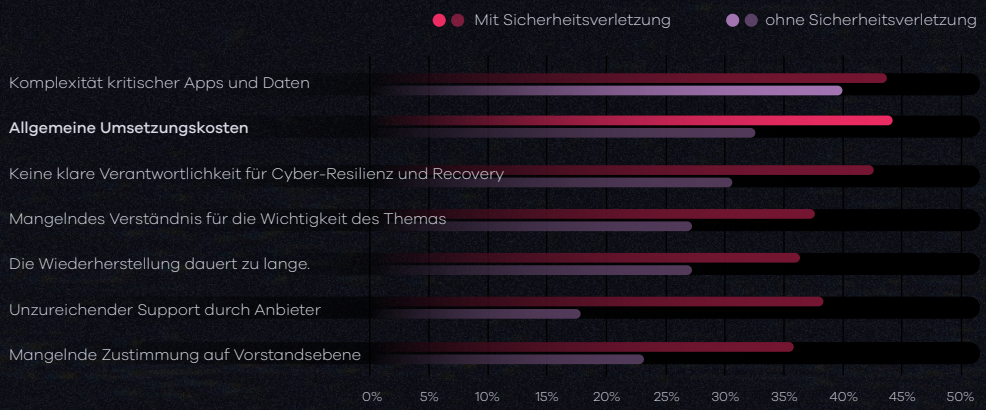
Welche Prioritäten setzt Ihr Unternehmen im Rahmen seiner Cyber-Recovery-Strategie als Reaktion auf Sicherheitsvorfälle?

Unternehmen, die Erfahrung mit einer schwerwiegenden Sicherheitsverletzung haben, im Vergleich zu allen Befragten

Abbildung 3

Welche Herausforderungen sehen Sie generell bei der Umsetzung der Cyber-Resilienz?

Datenaufteilung: Haben Sie bereits eine Sicherheitsverletzung erlitten?



Insgesamt haben Unternehmen, die keinen Sicherheitsverstoß erlitten haben, einen engeren Fokus. Bei fast 60% der Befragten landet die vollständige Sicherung und Wiederherstellbarkeit der wichtigen Daten unter den Top 3 (Abbildung 3). Unternehmen, die Opfer einer Sicherheitsverletzung wurden, setzen auf eine breitere Palette an Maßnahmen, die sich auf das Verständnis des Risikoprofils und die Klassifizierung ihrer Daten stützen.

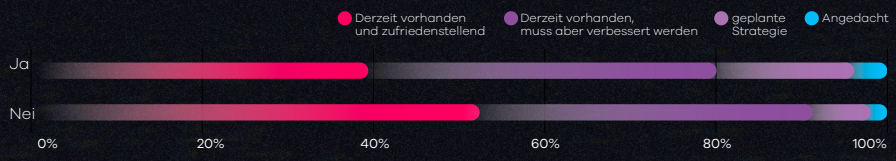
Dies zeigt uns, dass sich die Prioritäten verschieben, sobald ein Unternehmen einen Verstoß erlitten hat und weiß, was für eine angemessene Reaktion nötig ist. Diese Unternehmen haben gelernt, dass es wichtige Bereiche gibt, die berücksichtigt werden müssen, und die für jene, ohne die entsprechende Erfahrung, vielleicht weniger offensichtlich sind, z. B. die Kommunikation mit Stakeholdern, die Zusammenarbeit mit Anbietern, klare Zuständigkeiten und Aufteilung der Verantwortlichkeiten. Diejenigen, die noch nicht von einer Sicherheitsverletzung betroffen waren, konzentrieren sich in erster Linie auf die Schnelligkeit.

Unternehmen, die bereits eine Sicherheitsverletzung erlebt haben, sind zudem weniger zufrieden mit dem Status ihrer Frühwarnsysteme als Unternehmen, die noch keine Erfahrung in diesem Bereich haben (Abbildung 4), was auf ein gewisses Maß an Sorglosigkeit in der noch nicht betroffenen Gruppe hindeutet.

Abbildung 4

Inwieweit verfügt Ihr Unternehmen über die folgenden Fähigkeiten, um sich von einem Sicherheitsvorfall zu erholen?

Spezifische Maßnahmen, um die Cyber-Fähigkeit und das Risiko im Vergleich zu jenen mit Sicherheitsverletzung aufzuzeigen.



Insgesamt bereiten sich diejenigen, die einen Verstoß erlitten haben, umfassender vor – sie verfügen häufiger über Pläne, und die Pläne, die sie haben, werden öfter getestet. Als Reaktion auf einen Verstoß setzen Sie auf mehrere Funktionen und Aktivitäten und versuchen nicht nur ein paar wenige Dinge umzusetzen (Abbildung 5).

Abbildung 5

Was wären nach einem Sicherheitsvorfall die 5 Schlüsselprioritäten für Ihr Unternehmen?

Kombination aus den drei erstgereihten Antworten

CYBER-HERAUSFORDERUNGEN, DIE ES ZU BEWÄLTIGEN GILT

In einer sich schnell verändernden Risikolandschaft, hat für Unternehmen der Schutz ihrer Daten oberste Priorität.

Sicherheits- und IT-Experten machen sich, angesichts der sich ständig weiterentwickelnden Risikolandschaft, vor allem wegen externer Bedrohungen Sorgen und Unternehmen müssen davon ausgehen Opfer von Sicherheitsverletzungen zu werden. Sie wissen, dass es nicht darum geht, ***ob*** oder ***wann*** dieser Fall eintritt, sondern darum, wann sie herausfinden, ***dass sie bereits betroffen sind***.

Angesichts dieser Realität stehen Sicherheits- und IT-Experten vor einer Reihe von Herausforderungen. Zu den größten Sicherheitsherausforderungen der Befragten zählen: Immer raffiniertere Hacker und Angriffsarten, die Nutzung künstlicher Intelligenz durch Cyberkriminelle, eine größere Angriffsfläche aufgrund von Cloud und SaaS und die Einführung KI-basierter Technologien in allen Sicherheitstools (Abbildung 6).

Abbildung 6

Was sind für Sie die größten Herausforderungen für die Cybersicherheit Ihres Unternehmens?

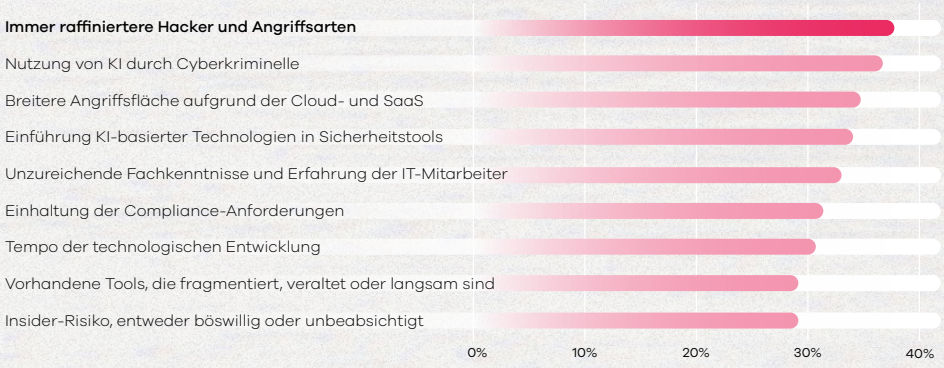
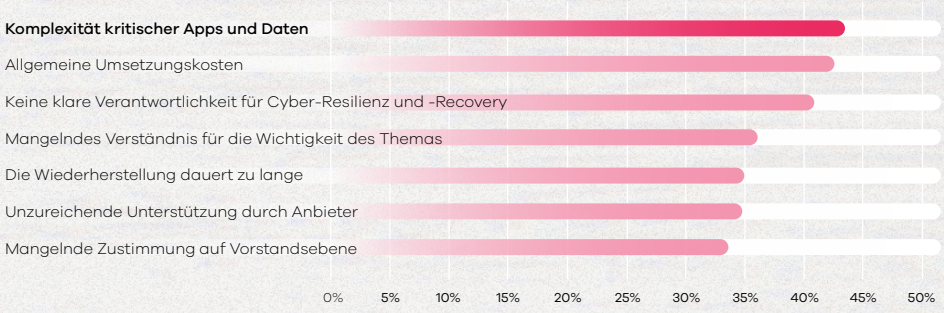


Abbildung 7

Welche Herausforderungen sehen Sie insgesamt bei der Umsetzung der Cyber-Fähigkeit?



Die in unserer Umfrage größte Herausforderung im Hinblick auf die Cyber-Fähigkeit war die Komplexität kritischer Apps und Daten, die von **44%** der Befragten genannt wurde, gefolgt von den Kosten.

Einer beträchtlichen Anzahl von Unternehmen (42 %) fehlt ein klares Verständnis dafür, wer für die Verbesserung der Cyber-Resilienz und der Recovery-Strategien und deren Umsetzung verantwortlich ist (Abbildung 7).

Das Vorhandensein mehrerer allgemeiner Sicherheitsfunktionen – Identitäts- und Zugriffsmanagement, Schutz vor unbefugten Zugriffen, Erkennungs- und Reaktionsmöglichkeiten, Vermeidung von/Schutz vor Datenverlusten; und Sicherheitsmanagement – bewegt sich zwischen 75 % und 80 %, wobei die aktuelle Lösung entweder zufriedenstellend ist oder verbessert werden muss (Abbildung 8).

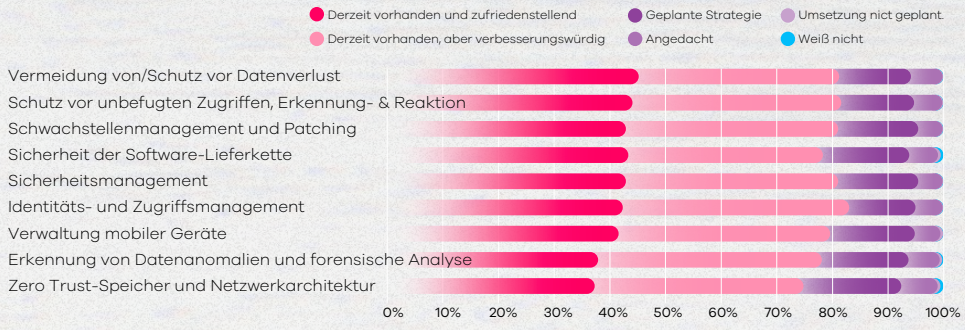
Doch im Allgemeinen finden

42% der Befragten, dass ihre Cybersicherheit zufriedenstellend ist

38% dass ihre Cybersicherheitsmaßnahmen verbessert werden müssen.

Abbildung 8

Inwieweit wurden die folgenden Schlüsselelemente für die Cybersicherheit Ihres Unternehmens geplant und/oder umgesetzt?



INDIKATOREN FÜR CYBER-REIFE

In Bezug auf Cyber-Resilienz gibt es wichtige Praktiken und Fähigkeiten, die die Reife eines Unternehmens kennzeichnen.

Auch wenn Unternehmen vielleicht bestimmte Maßnahmen als vorrangig nennen, kommt es vor allem darauf an, wie sie sich verhalten. Bei der Analyse der widerstandsfähigsten Unternehmen stellten wir fest, dass sie viele verschiedene Maßnahmen gesetzt hatten. Doch es kristallisierten sich fünf Merkmale heraus, die auf ihre wahre Resilienz hindeuteten. Wir nennen diese Merkmale Reifegrad-Indikatoren (siehe 5 Indikatoren zur Cyber-Fähigkeit, Seite 10).

Unternehmen, die vier oder fünf Indikatoren aufweisen, haben einen hohen Cyber-Reifegrad. Diese Unternehmen berichten, dass es weniger Sicherheitsverletzungen gibt und dass sie sich schneller erholen, wenn es zu einem Vorfall kommt.

Unsere Umfrage ergab jedoch, dass nur 4 % der Unternehmen alle fünf Indikatoren und nur 13 % zumindest vier davon umgesetzt haben. Am Ende der Reifegradkurve ergreifen 14 % überhaupt keine Schlüsselmaßnahmen (Abbildung 9).

Während weniger als die Hälfte aller Unternehmen vollstes Vertrauen in ihre Recovery-Pläne hat (Abbildung 10), sind mehr als die Hälfte der Unternehmen mit Cyber-Reife (54 %) deutlich zuversichtlicher, dass sie nach einem größeren Vorfall kritische Systeme und Daten wiederherstellen können (Abbildung 13, Seite 11).

Abbildung 9

Wie hoch ist die Recovery-Fähigkeit Ihres Unternehmens nach einem Sicherheitsvorfall basierend auf der Nutzung bestimmter Merkmale?

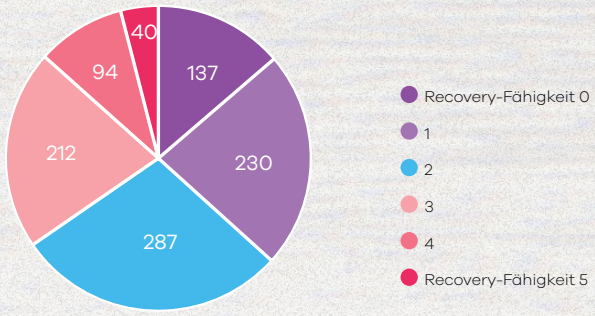
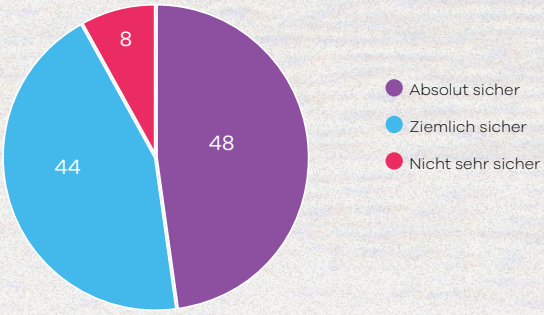


Abbildung 10

Wie sicher sind Sie, dass Sie über einen soliden Recovery-Plan im Hinblick auf Cyberbedrohungen verfügen?



5 INDIKATOREN FÜR CYBER-FÄHIGKEIT

Der Grad der Cyber-Reife eines Unternehmens lässt sich anhand von fünf Indikatoren messen. Die Unternehmen mit der höchsten Cyber-Reife weisen vier oder fünf davon auf:

1. ## Sicherheitstools, die eine frühzeitige Warnung vor Risiken, einschließlich Insider-Risiken, ermöglichen.

Frühwarntools sind Technologien und Systeme, die darauf ausgelegt sind, potenzielle Cyber-bedrohungen zu erkennen, bevor sie erhebliche Schäden verursachen können. Diese Tools zielen darauf ab, Risiken frühestmöglich zu erkennen, sodass Unternehmen proaktiv und nicht reaktiv reagieren können. Beispiele sind Intrusion Detection-Systeme, Deception-Technologien, Intrusion Prevention-Systeme, Sicherheitsinformations- und Ereignismanagement, User and Entity Behavior Analytics sowie Endpoint Detection and Response.

2. ## Eine bekannte saubere Darksite oder ein vorhandenes sekundäres System

Einrichten einer isolierten, vorkonfigurierten oder dynamischen isolierten Recovery-Umgebung (z. B. eines Reinraums), die von Cyber-Vorfällen am primären Standort nicht betroffen ist. Dieser sekundäre Standort kann im Falle eines Cyberangriffs oder eines schwerwiegenden Ausfalls schnell aktiviert werden, um die Geschäftskontinuität und Datenintegrität zu gewährleisten. Er verbessert die Cyber-Resilienz durch eine sichere Failover-Option, wodurch Ausfallzeiten und Komplexität eines Failovers minimiert werden.

3. ## Eine isolierte Umgebung zum Speichern einer unveränderlichen Datenkopie.

Beinhaltet die Pflege einer separaten, Air-Gap-gesicherten (d. h. unveränderlichen und unlöschbaren) Datenkopie, die auf der Infrastruktur eines Drittanbieters gesichert ist. Die Daten bleiben un-verändert und sind vor Cyberbedrohungen, einschließlich Ransomware und böswilligen Insider-aktionen, geschützt. Das führt zu einer Verbesserung der Datenintegrität und -verfügbarkeit und bietet eine zuverlässige Wiederherstellungsoption im Falle von Datenbeschädigung oder -verlust.

4. ## Definierte Runbooks, Rollen und Prozesse für die Reaktion auf Vorfälle.

Hier handelt es sich um ein entscheidendes Merkmal der Cyber-Resilienz für eine strukturierte und effiziente Reaktion auf Cybervorfälle. Getestete Runbooks bieten Schritt-für-Schritt-Anleitungen für die Handhabung verschiedener Arten von Vorfällen, wodurch Unklarheiten und Reaktionszeiten reduziert werden. Klar definierte Rollen und Prozesse stellen sicher, dass jedes Teammitglied seine Verantwortlichkeiten kennt, und fördern darüberhinaus koordinierte Bemühungen. Diese Vorsorge beschleunigt die Wiederherstellung und trägt zur Aufrechterhaltung der Betriebskontinuität während und nach Cybervorfällen bei.

5. ## Spezifische Maßnahmen zum Nachweis der Cyber-Fähigkeit und Aufzeigen von Cyber-Risiken.

Kennzahlen und Tests, die die Fähigkeit eines Unternehmens demonstrieren, sich von Cyber-Vorfällen zu erholen und damit verbundene Risiken zu bewerten. Diese Maßnahmen, wie regel-mäßige Recovery-Übungen und Risikobewertungen, bieten Einblick in die Effektivität von Recovery-Plänen und identifizieren potenzielle Schwachstellen. Sie sind insbesondere für die Cyber-Resilienz sowie für die Abwehrbereitschaft, die Validierung von Wiederherstellungsstrategien und das Aufzeigen von Verbesserungsmöglichkeiten wichtig.

MACHEN SIE KEINE HALBEN SACHEN

Cyber-fähige Unternehmen machen keine Abstriche, wenn es darum geht, Cyber-Resilienz und Cyber-Fähigkeit zu gewährleisten.

Bei vielen Unternehmen ist eine Cyber-Recovery-Strategie noch in Aufbau. 38 % unserer Befragten geben wiederholt an, dass ihre Bemühungen verbesserungswürdig sind.

Diejenigen, die Verbesserungen anstreben, sollten sich an ihre erfahreneren Kollegen wenden, die lieber mehr Maßnahmen ergreifen, als nur ein paar wenige zu priorisieren und daher im Fall einer Sicherheitsverletzung eine solidere Grundlage aufweisen.

Sie priorisieren das Testen und Sichern wichtiger Daten, legen aber fast gleich großen Wert auf die Fähigkeit, über mehrere Cloud-Anbieter hinweg arbeiten zu können, geschäftskritische Anwendungen zu kennen und zu kennzeichnen und schnell eine saubere Umgebung einrichten zu können (Abbildung 11).

Das Ergebnis ist ein verbesserter Sicherheitsstatus sowie eine bessere Cyber-Resilienz. Insgesamt ist die Wahrscheinlichkeit eines Verstoßes bei ihnen etwa halb so hoch wie bei Unternehmen mit geringerem Reifegrad (Abbildung 12).

Abbildung 11

Welche Prioritäten setzt Ihr Unternehmen im Rahmen seiner Cyber-Recovery-Strategie als Reaktion auf Sicherheitsvorfälle?

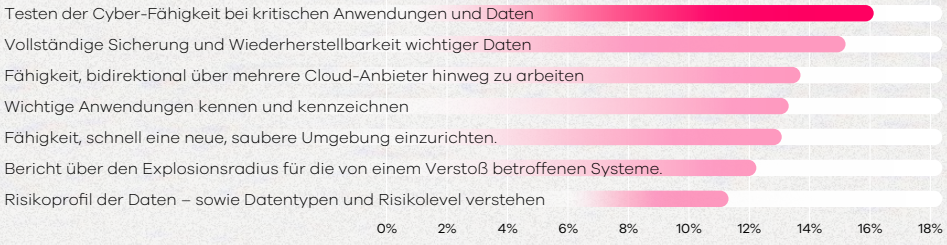
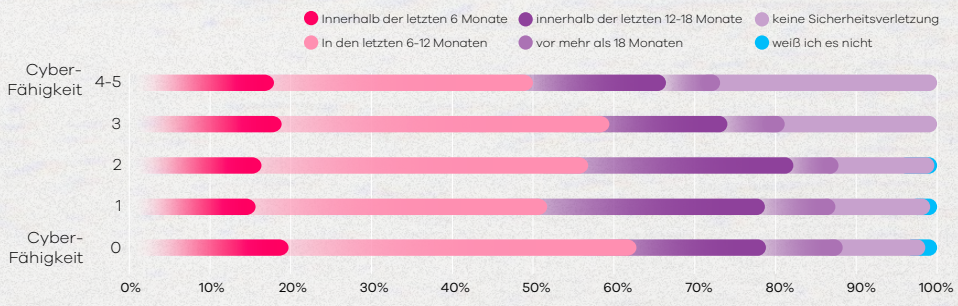


Abbildung 12

Wann war Ihr Unternehmen das letzte Mal Opfer einer massiven Sicherheitsverletzung?



CYBER-FÄHIGE UNTERNEHMEN ERHOLEN SICH SCHNELLER

Unternehmen mit dem höchsten Reifegrad können besser reagieren.

Aufgrund der besseren Vorbereitung sind Unternehmen mit Cyber-Reife besser in der Lage, sich von einem Cyberangriff zu erholen. Es überrascht nicht, dass diese Unternehmen mehr Vertrauen in ihre Fähigkeit haben, wieder auf die Beine zu kommen, und 54 % sich dabei absolut sicher sind (Abbildung 13).

Dieses Vertrauen ist gerechtfertigt: Die Unternehmen erholen sich um 41 % schneller als die Befragten mit keinem oder einem Indikator und um 24 % schneller als die Befragten mit zwei oder drei Indikatoren (Abbildung 14).

Offline zu sein kostet Geld und kann den Ruf eines Unternehmens und das Vertrauen seiner Kunden schädigen. Daher zählt jede Minute. Je schneller Unternehmen den normalen Betrieb wieder aufnehmen können, desto besser.

Abbildung 13

Inwieweit sind Sie sicher, dass Ihr Unternehmen kritische Systeme und Daten nach einem schwerwiegenden Vorfall wiederherstellen kann?

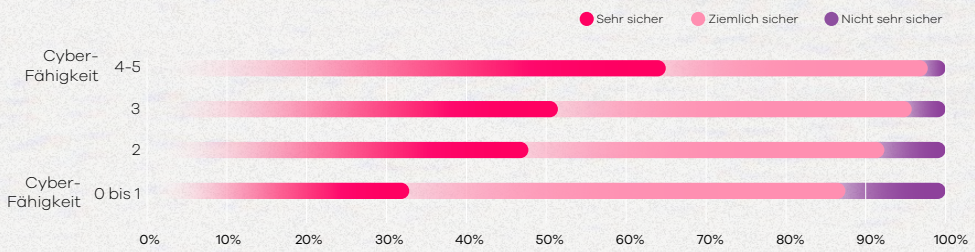
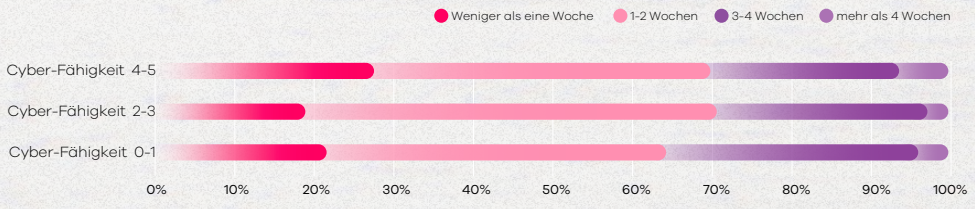


Abbildung 14

Wie lange hat es gedauert, bis Ihr Unternehmen nach der Sicherheitsverletzung den normalen Betrieb wieder aufnehmen konnte?



CYBER-RECOVERY IST MEHR ALS NUR DISASTER RECOVERY

Eine herkömmliche Disaster Recovery reicht nicht aus, um sich von einem Cyber-Vorfall zu erholen.

Es ist wichtig zu wissen, dass, auch wenn einige Unternehmen sich auf die Cyber Recovery als Bestandteil eines umfassenden Disaster Recovery-Plans vorbereiten, Cyber Recovery nicht dasselbe wie Disaster Recovery ist.

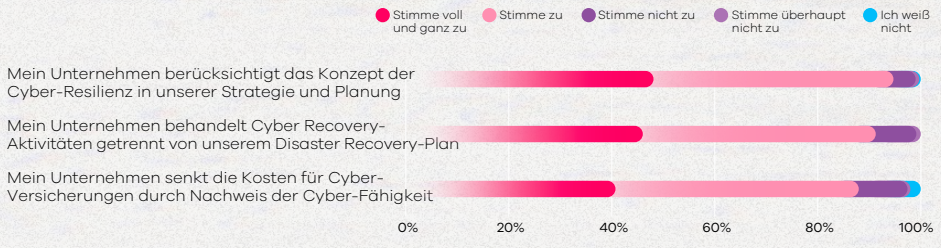
Sie benötigen einen Disaster Recovery-Plan, um vorhersehbare Ereignisse wie Hardware-Ausfälle oder Naturkatastrophen wie Brände und Überschwemmungen zu bewältigen. Obwohl solche Ereignisse sicherlich verheerend sind, sind Unternehmen in der Regel in der Lage, schneller wieder online zu gehen, weil sie die Schritte eines vordefinierten Plans befolgen. Wichtig ist, dass bei einer Naturkatastrophe die Daten wahrscheinlich vertrauenswürdig sind. Die Disaster Recovery kann sich also auf die Datenintegrität, eine rasche Wiederherstellung und das Erreichen der festgelegten Wiederherstellungsziele konzentrieren.

Cyber-Ereignisse sind anders. Bei einem Cyberangriff sind die Daten nicht vertrauenswürdig. Anhand der Recovery-Pläne müssen die wichtigen Elemente sauber und zuverlässig wiederhergestellt werden können, damit die Wiederherstellung die Situation nicht noch verschlimmert. Cyber Recovery-Pläne sollten Mechanismen zur Wiederherstellung mittels Zero Trust enthalten.

Die Befragten kennen diesen wichtigen Unterschied. In unserer Umfrage **gaben über 90 % der Teilnehmer** an, dass ihr Unternehmen **Disaster Recovery getrennt von Cyber Recovery behandelt** (Abbildung 15). Dies ist ein Zeichen dafür, dass die meisten Unternehmen die Unterschiede kennen und sich entsprechend darauf vorbereiten.

Abbildung 15

Inwieweit stimmen Sie den folgenden Aussagen zu oder nicht zu?



RECOVERY-BEREITSCHAFT BRAUCHT FÄHIGKEITEN, KOMPETENZEN UND KULTUR

Cyber-fähige Unternehmen optimieren ihre Mitarbeiter, Prozesse und Technologien, um Recovery-Bereitschaft zu erreichen.

Es ist wichtig zu wissen, dass **Technologie allein nicht zur Verbesserung der Resilienz und Bereitschaft beiträgt.** Unsere Forschungsergebnisse bestätigen das bewährte Paradigma: Technologie ist ein Impulsgeber für Menschen und Prozesse.

Die meisten Unternehmen sind sich bewusst, dass Cyber-Fähigkeit eine strukturierte Herangehensweise erfordert, die sowohl die Ressourcen des Unternehmens als auch die Art und Weise berücksichtigt, wie ihre Mitarbeiter sie umsetzen.

Fähigkeiten: Die Tools und Systeme, über die ein Unternehmen verfügt, um sich nach einer Sicherheitsverletzung wieder zu erholen.

Kompetenzen: Die Fähigkeit eines Unternehmens, sein Potenzial effektiv und effizient einzusetzen.

Kultur: Die Werte eines Unternehmens und die Fähigkeit, sie in die Praxis umzusetzen.

Wenn Fähigkeiten die „harten Kompetenzen" eines Unternehmens sind, umfasst die Kultur die „weichen Kompetenzen". Wie oft wird getestet?

Wie viel Wert wird darauf gelegt in Tools zu investieren und sich auch die Zeit zu nehmen, diese zu testen?

Wie effektiv kommunizieren und arbeiten Mitarbeiter zusammen, um ein strenges Testschema umzusetzen?

All diese Faktoren beeinflussen, wie gut ein Unternehmen auf Cyberbedrohungen vorbereitet ist.

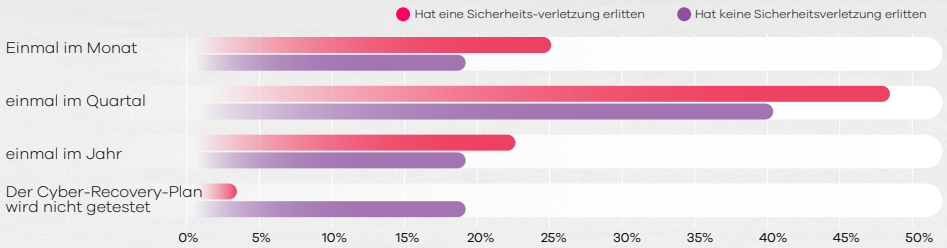
TESTS SIND DIE GRUNDLAGE FÜR CYBER-RESILIENZ UND CYBER-FÄHIGKEIT

Häufige Cyber Recovery-Tests sind eine wichtige Maßnahme, um die Cyber-Fähigkeit zu verbessern.

Ohne Tests in einem realen Szenario können Unternehmen nicht wissen, ob ihre Cyber-Recovery-Pläne funktionieren. Das sehen wir, wenn wir die Teststrategien von Unternehmen, die bereits eine Sicherheitsverletzung erlitten haben, mit denen jener vergleichen, die noch nicht betroffen waren. Zwanzig Prozent der Unternehmen ohne Sicherheitsverletzung geben an, dass sie ihren Recovery-Plan überhaupt nicht testen (Abbildung 16). Diese Zahl sinkt bei Unternehmen, die eine Sicherheitsverletzung erlitten haben, auf nur 2 %.

Abbildung 16

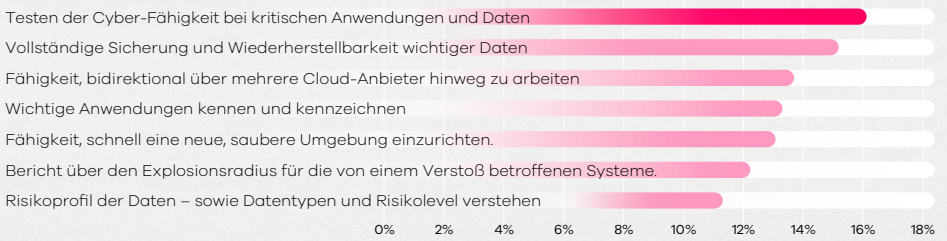
Wie oft wird der Cyber-Recovery-Plan Ihres Unternehmens getestet?



Darüber hinaus stellten wir fest, dass die Unternehmen mit dem höchsten Reifegrad Tests bei der Planung ihrer Cyber Recovery-Strategie Vorrang vor anderen Maßnahmen geben (Abbildung 17). Siebzig Prozent der Unternehmen mit dem höchsten Reifegrad testen ihre Pläne vierteljährlich, während nur 43 Prozent der Unternehmen mit keinem oder einem Reife-Indikator dies tun (Abbildung 18).

Abbildung 17

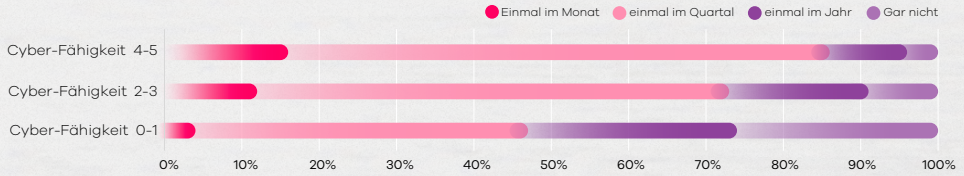
Welche Prioritäten setzt Ihr Unternehmen im Rahmen seiner Cyber-Recovery-Strategie als Reaktion auf Sicherheitsvorfälle?



Hinweis: Unternehmen mit 4 oder 5 Reife-Indikatoren

Abbildung 18

Wie oft testet Ihr Unternehmen seinen Cyber-Recovery-Plan?



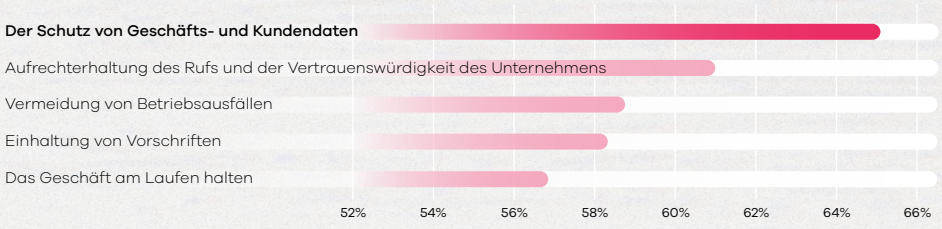
WARUM CYBER-FÄHIGKEIT WICHTIG IST - DIE AUSWIRKUNGEN EINES VERSTOSSES MINIMIEREN

Cyber-fähige Unternehmen können darauf vertrauen, auch bei Angriffen widerstandsfähig zu bleiben.

Verstöße treten nicht nur sehr häufig auf, sondern bedrohen auch die Ressourcen und die Marke eines Unternehmens. In der Umfrage haben wir erfahren, dass die größte Priorität für Unternehmen der Schutz von Geschäfts- und Kundendaten ist, gefolgt von der Aufrechterhaltung des Rufs und der Vertrauenswürdigkeit des Unternehmens (Abbildung 19).

Abbildung 19

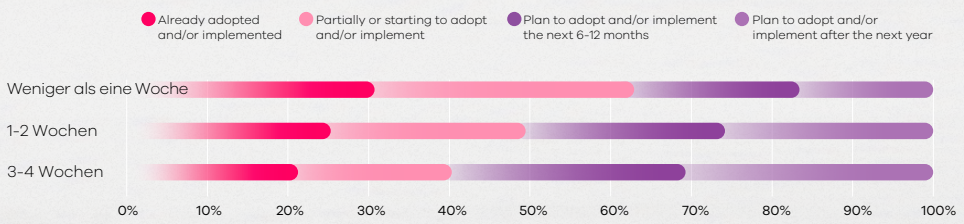
Was sind die wichtigsten Sicherheitsprioritäten Ihres Unternehmens aus geschäftlicher Sicht?



Diese Angriffe haben offensichtliche Auswirkungen auf den normalen Geschäftsbetrieb. Wir stellten fest, dass diejenigen, die bereits über einen vollständigen oder teilweisen Recovery-Plan verfügen, sich in der Regel um 41 % schneller erholen als diejenigen, die keinen Plan haben (Abbildung 20).

Abbildung 20

Wie lange hat es gedauert, bis Ihr Unternehmen nach dem Verstoß den normalen Betrieb wiederaufnehmen konnte?



Aus diesem Grund ist das Vertrauen in die Cyber-Fähigkeit von größter Bedeutung. Jene mit dem höchsten Reifegrad sind in ihrer Cyber-Resilienz fast doppelt so sicher wie diejenigen mit keinem oder einem Indikator (Abbildung 13, Seite 11). Diese Bereitschaft hilft Unternehmen mit Cyber-Reife dabei, sich schneller von einem Verstoß zu erholen und insgesamt weniger Sicherheitsverletzungen zu erleiden.

ZUSAMMENFASSUNG

Wie sieht es allgemein mit der Cyber-Fähigkeit aus?

Die Ergebnisse unserer Umfrage zeigen, dass **Unternehmen, die eine Sicherheitsverletzung erlitten haben, und jene, die noch nicht davon betroffen waren, eine unterschiedliche Perspektive einnehmen.** Aber vergessen Sie nicht, dass Taten mehr sagen als Worte. Es reicht nicht, sich vorzunehmen sich anders zu verhalten. Unternehmen müssen ihre Verhaltensweisen ändern, um ihre Chancen zu verbessern, eine Sicherheitsverletzung erfolgreich zu überstehen und ihre Systeme und Daten wiederherzustellen.

Wenn Sie zu den 38 % gehören, **die der Meinung sind, dass ihre Cybersicherheitsmaßnahmen verbessert werden könnten**, oder wenn Sie zur Mehrheit gehören, die **sich nicht ganz sicher ist, dass sie nach einem Verstoß in der Lage wäre, sich davon zu erholen**, gibt es Maßnahmen, die Sie ergreifen können.

Verfügt Ihr Unternehmen über einen Plan zum Erreichen der **fünf Indikatoren für Cyber-Resilienz**, sind Sie besser vorbereitet. Wenn Sie in ein Testprogramm investieren und sicherstellen, dass jeder seine Rolle darin versteht, erhöhen Sie Ihre allgemeinen Chancen, einen Cyberangriff erfolgreich zu überstehen.

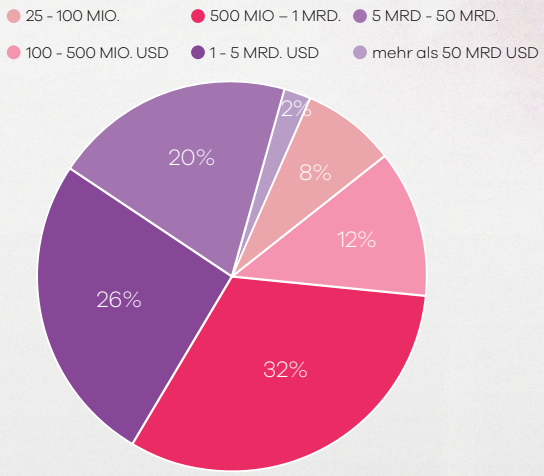
Sie können sich nicht auf Ihren Lorbeeren ausruhen und dem Irrtum unterliegen, dass Sie gegen die Gefahr immun sind. **Wenn Sie die Risiken verstehen und anerkennen, sind Ihre Daten - und Ihr Ruf- auch nach einer Sicherheitsverletzung intakt.**

DEMOGRAFISCHE DATEN

Abbildung 1

GigaOm führte diese Studie im April 2024 unter 1.000 Befragten aus 11 Ländern durch.

Die Befragten stammten von Unternehmen, die einen Jahresumsatz von mindestens 10 Millionen US-Dollar erwirtschafteten, wobei die **Mehrheit 500 Millionen US-Dollar oder mehr erwirtschaftete.**



35 % der Befragten waren Vorstandsmitglieder oder C-Level-Führungskräfte, **48 % waren Führungskräfte im Top-Management** und die restlichen 17 % im mittleren Management.