COHESITY

BERICHT ZUR CYBER-RESILIENZ

Risikobereit oder risikogefährdet: Die Kluft in der Cyber-Resilienz im Gesundheitswesen

DER APRIL 2026

Alle reden von der Erkennung und Prävention von Cyberangriffen, doch die Schlagzeilen zeichnen ein anderes Bild. Prävention und Erkennung allein reichen nicht mehr aus. Selbst die fortschrittlichsten Unternehmen leiden unter schwerwiegenden Störungen, die sich von der IT-Abteilung bis in die Führungsetage und darüber hinaus auswirken.

Um die Gründe dafür zu verstehen und herauszufinden, was resiliente Organisationen von denjenigen unterscheidet, die weiterhin mit Herausforderungen kämpfen, befragte Cohesity 3.200 IT und Security Operations Entscheider in 11 Ländern. Darunter befanden sich 371 Teilnehmer aus Gesundheitsorganisationen. Ihre Antworten zeigen eine wachsende Resilienzkluft zwischen risikobereiten Gesundheitsorganisationen, die sich schnell und mit hoher Sicherheit erholen können, und ihren risikogefährdeten Pendants, die weiterhin anfällig für langanhaltende Störungen und daraus resultierende finanzielle Folgeschäden sind.

Unsere Forschung untersucht die realen Auswirkungen schwerwiegender Cyberangriffe und zeigt, wie Gesundheitsorganisationen ihre Cyber-Resilienz im Vergleich zu Best Practices selbst bewertet haben und welche Schritte sie unternommen haben, um diese Vorfälle zu erkennen, darauf zu reagieren und sich davon zu erholen. Sie hebt außerdem hervor, was sie dabei gelernt haben und wie sie KI und Automatisierung nutzen, um ihre Resilienz zu beschleunigen und die Kluft zu schließen.

SCHWERWIEGENDE CYBERANGRIFFE: **DIE NEUE REALITÄT MODERNER UNTERNEHMEN**

Cybervorfälle sind nicht alle gleich. Viele Gesundheitsorganisationen haben beinahe täglich mit Phishing-Angriffen, Malware-Analysen oder Systemausfällen zu kämpfen. Schwerwiegende Cyberangriffe hingegen sind anders. In unserer Umfrage wurde ein schwerwiegender Cyberangriff als Vorfall definiert, der messbare finanzielle, reputationsbezogene, betriebliche oder kundenbezogene Auswirkungen hatte.

DIESE SCHWERWIEGENDEN ANGRIFFE SIND FÜR GESUNDHEITSORGANISATIONEN LÄNGST KEINE EINZELFÄLLE MEHR:

85 %

der Befragten waren mindestens einmal von einem schwerwiegenden Cyberangriff betroffen.

66 %

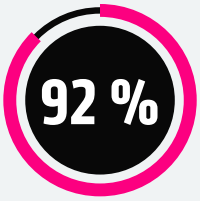
erlebten einen solchen Angriff in den vergangenen zwölf Monaten.

35 %

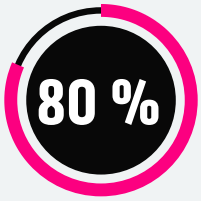
waren im selben Zeitraum von mehreren Vorfällen betroffen.

DIE TATSÄCHLICHEN KOSTEN SCHWERWIEGENDER CYBERANGRIFFE

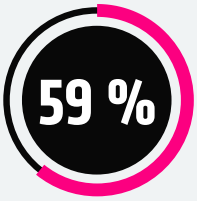
FINANZIELLER UND REGULATORISCHER DRUCK WAR IN DEN VON UNS BEFRAGTEN GESUNDHEITSORGANISATIONEN ALLGEGENWÄRTIG:



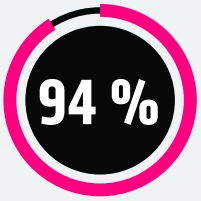
meldeten Umsatzeinbußen.



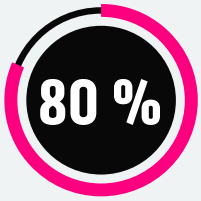
der börsennotierten Gesundheitsorganisationen gaben an, ihre Finanzprognosen angepasst zu haben[1]



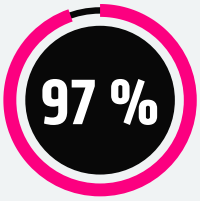
verloren Kunden



zahlten Lösegeld – im Durchschnitt 1,3 Millionen US Dollar pro Vorfall.



der privaten Gesundheitsorganisationen lenkten Budgets von Wachstumsinitiativen ab.



sahen sich mit rechtlichen oder regulatorischen Konsequenzen konfrontiert, darunter behördliche Geldbußen (54 %) sowie Rechtsstreitigkeiten oder Sammelklagen (39 %).

[1]Obwohl relativ wenige börsennotierte Unternehmen nach einem Cyberangriff Gewinnkorrekturen formell veröffentlicht haben, deuten diese Ergebnisse darauf hin, dass die finanziellen und betrieblichen Auswirkungen weit über das hinausgehen, was in den öffentlichen Berichten ersichtlich ist.

VERTRAUEN TROTZ DER FOLGEN

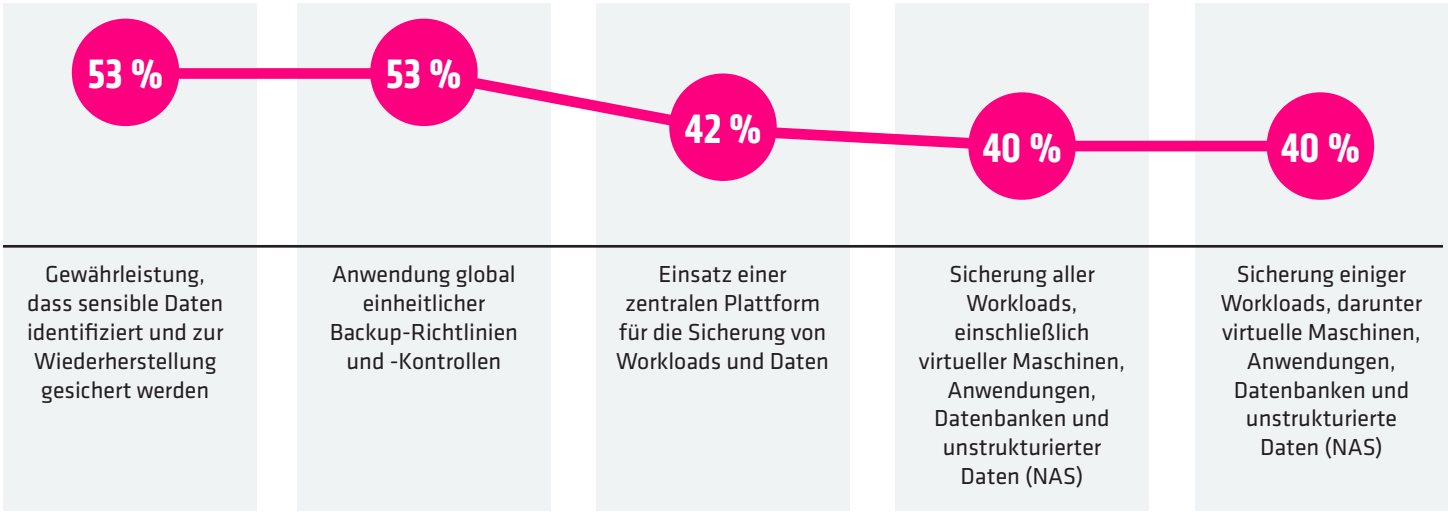
Angesichts des Ausmaßes der finanziellen und betrieblichen Auswirkungen, die unsere Nachforschungen aufgedeckt haben, könnte man erwarten, dass die Resilienz von Unternehmen weit verbreitet ist. Fast die Hälfte der Befragten (49 %) gab an, vollstes Vertrauen in ihre Cyber-Resilienzstrategie zu haben und den heutigen Bedrohungen standhalten zu können. Dieses Maß an Vertrauen steht in starkem Kontrast zu den erheblichen materiellen Einbußen, die viele dieser Unternehmen erlitten haben.

WAS UNTERNEHMEN TUN (UND WAS NICHT)

Wir wollten genauer hinschauen und die bestehenden Resilienzlücken aufdecken. Dazu baten wir die Befragten, ihren Ansatz hinsichtlich einiger wichtiger Praktiken und Fähigkeiten in den fünf Kerndimensionen der Cyber-Resilienz zu beschreiben: **Datenschutz, Datenwiederherstellung, Bedrohungserkennung und -untersuchung, Anwendungsresilienz und Optimierung der Datenrisikostrategie.**

DIE DATENSICHERUNG BLEIBT IN HYBRIDEN UND MULTICLOUD-UMGEBUNGEN FRAGMENTIERT

Welche der folgenden Maßnahmen ergreift Ihr Unternehmen, um alle Daten in Hybrid- und/oder Multicloud-Umgebungen zu schützen?



Etwas mehr als die Hälfte der Gesundheitsorganisationen stellt sicher, dass sensible Daten identifiziert und für die Wiederherstellung gesichert werden. Der gleiche Prozentsatz gilt weltweit für einheitliche Backup-Richtlinien. Allerdings sichert weniger als die Hälfte alle Workloads oder verlässt sich auf eine zentrale Plattform. Etwas mehr als ein Drittel führen nur Backups ausgewählter Workloads durch. Diese Zersplitterung schränkt die Transparenz und Konsistenz über verschiedene Umgebungen hinweg ein. Ausgereifte Cyber Resilienz hängt davon ab, Backup und Recovery in einer einzigen intelligenten, nach Zero Trust Prinzipien gesicherten Plattform zu vereinen.

MASSNAHMEN ZUR SICHERSTELLUNG DER DATENWIEDERHERSTELLBARKEIT SIND WEIT VERBREITET, DOCH DER REIFEGRAD VARIIERT.

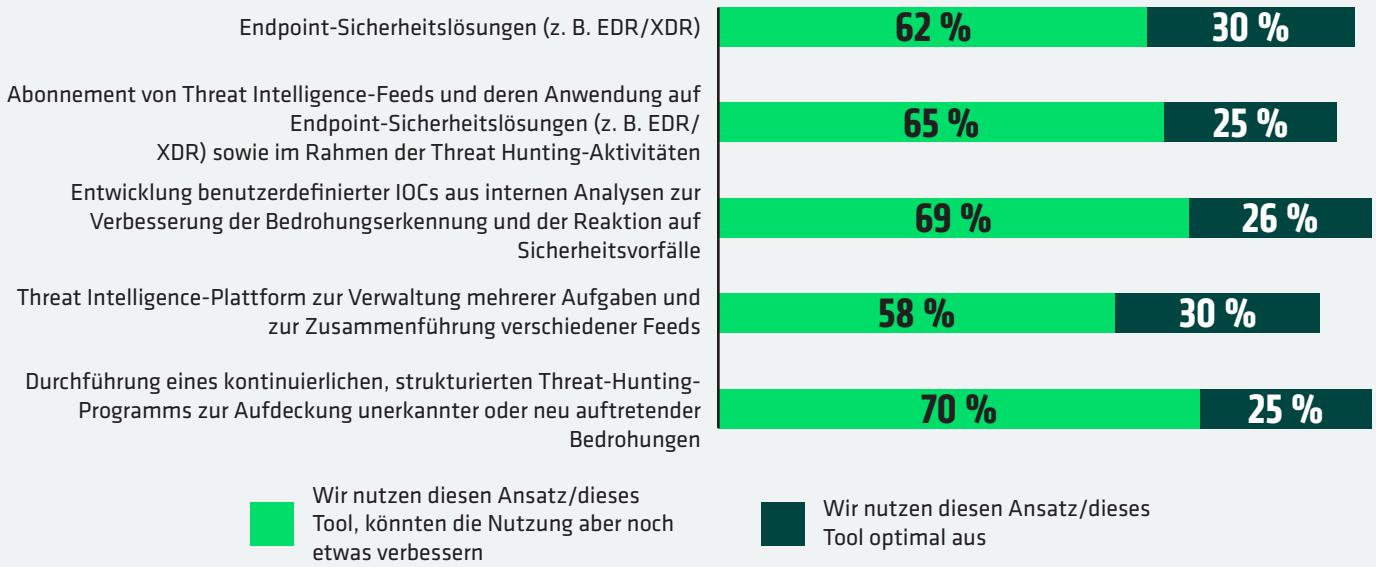
Was unternimmt Ihr Unternehmen, um die jederzeitige Wiederherstellbarkeit seiner Daten zu gewährleisten?

60 %	Zusätzliche Autorisierung für risikoreiche administrative Aufgaben im Zusammenhang mit Datensicherung und -wiederherstellungs lösungen
48 %	Multifaktor-Authentifizierung für unsere Backup-Lösung
44 %	Befolgung der „3-2-1-Backup-Regel“ (drei Datenkopien auf zwei verschiedenen Speichermedien, wobei eine Kopie extern aufbewahrt wird)
42 %	Schutz kritischer Daten durch Unveränderlichkeit
35 %	Zugriffsrechte nach dem Prinzip der minimalen Berechtigungen für gesicherte Workloads

Viele Gesundheitsorganisationen haben die Zugriffskontrollen rund um ihre Backup-Umgebungen verstärkt, sechs von 10 benötigen für risikoreiche Aufgaben eine zusätzliche administrative Genehmigung. Weniger als die Hälfte setzt Multifaktor-Authentifizierung durch, folgt der 3-2-1-Backup-Regel oder schützt kritische Daten durch Unveränderlichkeit. Nur etwa ein Drittel wendet Zugriffsrechte mit minimalen Berechtigungen an. Diese Lücken verringern die Sicherheit einer vollständigen Wiederherstellung. Ausgereifte Cyber-Resilienz hängt von verifizierten, isolierten und manipulationssicheren Wiederherstellungskopien ab.

TOOLS ZUR BEDROHUNGSERKENNUNG UND -UNTERSUCHUNG WERDEN ZU WENIG GENUTZT

In welchem Umfang nutzt Ihr Unternehmen die folgenden Methoden und Tools zur Erkennung und Untersuchung von Bedrohungen?



Tools zur Bedrohungserkennung und -analyse sind weit verbreitet, werden aber häufig nicht voll ausgeschöpft. Die meisten Gesundheitsorganisationen setzen auf Endpoint-Sicherheit, Threat-Intelligence-Feeds und strukturierte Threat-Hunting-Programme, doch nur eine Minderheit nutzt das volle Potenzial dieser Lösungen. Die Optimierung erweiterter Fähigkeiten wie benutzerdefinierter Indikatoren für Kompromittierungen (Custom Indicators of Compromise, IOCs) und Threat Intelligence-Plattformen ist nach wie vor besonders eingeschränkt. Eine ausgereifte Cyber-Resilienz erfordert die Integration dieser Tools in einen kontinuierlichen Informationskreislauf.

UNTERNEHMEN SIND ANFÄLLIG FÜR ERNEUTE INFEKTIONEN

Was unternimmt Ihr Unternehmen bzw. würde Ihr Unternehmen tun, um die Resilienz von Anwendungen gegen Cyberangriffe zu gewährleisten?

56 % Jährlich werden End-to-End-Simulationen durchgeführt, an denen ein funktionsübergreifendes Team aus technischen, juristischen, strategischen, leitenden und kommunikativen Stakeholdern teilnimmt

54 % Sicherheitslücken identifizieren und beheben, bevor Systeme wieder in Betrieb genommen werden

53 % Kritische Systeme und Informationen werden online und sicher gespeichert, um die Reaktion auf Vorfälle und die Wiederherstellung zu unterstützen

36 % Für die Untersuchung, Behebung und sichere Wiederherstellung von Vorfällen wird eine isolierte Umgebung genutzt

36 % Alle Backup-Daten sind unveränderlich

Gesundheitsorganisationen verbessern ihre Strategien zur Anwendungsresilienz, doch es bestehen weiterhin Lücken. Über die Hälfte identifiziert Sicherheitskontrolllücken, bevor Systeme wiederhergestellt werden, und führt jährliche Wiederherstellungsübungen durch. Ein ähnlicher Anteil unterhält Online-Tresor-Repositories, um die Reaktion und Wiederherstellung zu unterstützen. Weniger nutzen isolierte Umgebungen für sichere Untersuchungen und Wiederherstellung oder wenden Unveränderlichkeit auf alle Backup-Daten an. Dadurch sind Wiederherstellungsprozesse anfällig für erneute Infektionen oder Datenverlust. Ausgereifte Cyber-Resilienz kombiniert Vorbereitung mit sicheren, verifizierbaren Wiederherstellungszonen.

DATENKLASSIFIZIERUNG GEWINNT AN BEDEUTUNG, DOCH DER RISIKOBASIERTE EINSATZ ENTWICKELT SICH NOCH WEITER

Wie nutzt Ihr Unternehmen Ansätze/Tools zur Datenermittlung und -klassifizierung, um das Datenrisiko im gesamten Datenbestand zu minimieren?

60 %

Im Falle eines Cyberangriffs nutzen wir die Backup-Datenklassifizierung, um die Compliance-Verpflichtungen für betroffene Daten zu ermitteln

59 %

Identifizierung und Behebung von Datenschutz- und Sicherheitsverstößen in Backups zur Gewährleistung der Compliance

53 %

Definition und Analyse der Wesentlichkeit eines Cyberangriffs vor dessen Eintreten

52 %

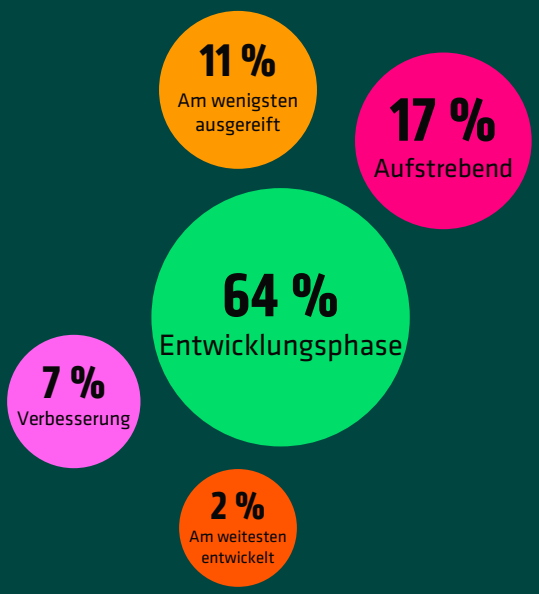
Identifizierung und Priorisierung von Backup-Systemen

Gesundheitsorganisationen setzen Datenerkennung und -klassifizierung zunehmend strategischer über Compliance, Reaktion und Wiederherstellung hinweg ein.Sechs von zehn nutzen Klassifizierungen, um die Compliance während eines Angriffs sicherzustellen, während fast ebenso viele sich mit Datenschutz- und Sicherheitsverletzungen befassen. Etwas weniger definieren die Wesentlichkeit vor einem Vorfall oder priorisieren Backups anhand des Risikos. Diese Lücken deuten darauf hin, dass sich die risikoorientierte Verwendung von Klassifizierungen noch in der Entwicklung befindet. Ausgereifte Cyber-Resilienz wandelt die Klassifizierung in einen systematischen Ansatz zur Optimierung des Datenrisikomanagements um und unterstützt so Schutz, Reaktion und Wiederherstellung.

EIN KLARERES BILD DES REIFEGRADS DER RESILIENZ

Die Antworten der Befragten dienten in ihrer Gesamtheit als grober Indikator für den Reifegrad der Cyber-Resilienz und offenbarten deutliche Muster im praktischen Aufbau – oder den Schwierigkeiten – deutscher Unternehmen beim Aufbau von Resilienz. Während sich die Mehrheit noch in der Entwicklungsphase befindet, verfügen lediglich 2 % über die ausgereiftesten, integrierten Fähigkeiten, die risikobereite Unternehmen kennzeichnen.

DIE REIFEGRADKURVE FÜR CYBER-RESILIENZ



Am wenigsten ausgereift (11 %): Datensicherungen, Richtlinien und Sicherheitsvorkehrungen fehlen weitgehend oder sind inkonsistent. MFA und administrative Kontrollen werden selten durchgesetzt, die Wiederherstellung ist oft unzureichend isoliert, und Compliance- oder Wesentlichkeitsprüfungen werden typischerweise vernachlässigt.

Aufstrebend (17 %): Einige Maßnahmen zur Erhöhung der Resilienz sind vorhanden, werden aber nicht einheitlich angewendet. Unternehmen sichern möglicherweise sensible Daten, wenden globale Richtlinien an oder nutzen Multi-Faktor-Authentifizierung (MFA), jedoch selten in Kombination. Die Bemühungen hinsichtlich Threat Intelligence-Analyse und Compliance sind zwar vorhanden, aber noch nicht ausgereift und fragmentiert.

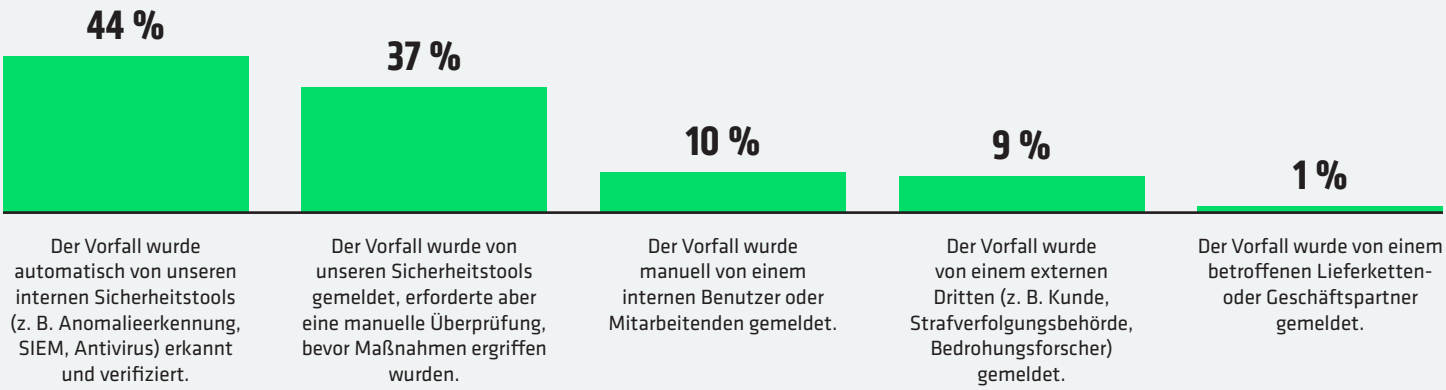
Entwicklungsphase (64 %): Kernpraktiken wie Datensicherung, administrative Kontrollen und Threat Intelligence sind zwar verbreiteter, aber noch nicht einheitlich. Wiederherstellungsumgebungen, Compliance-Prüfungen und die Behebung von Sicherheitslücken werden nur sporadisch angewendet, wodurch die Maßnahmen zur Erhöhung der Resilienz nur teilweise wirksam sind.

Verbesserung (7 %): Die meisten wichtigen Vorgehensweisen werden konsequent umgesetzt, darunter globale Backup-Richtlinien, Genehmigungen durch Administratoren und die Behebung von Sicherheitslücken vor der Wiederherstellung. Threat Intelligence wird genutzt, aber nicht vollständig optimiert, und es bestehen weiterhin Lücken hinsichtlich isolierter Wiederherstellung und vollständiger Compliance-Abdeckung.

Am weitesten entwickelt (2 %): Die Resilienz ist systematisch und umfassend. Sensible Daten werden global gesichert, MFA und administrative Kontrollen sind Standard, Threat Intelligence wird optimal genutzt, die Wiederherstellung wird durch die Behebung von Sicherheitslücken gesichert, und Compliance-Vorgaben werden konsequent eingehalten.

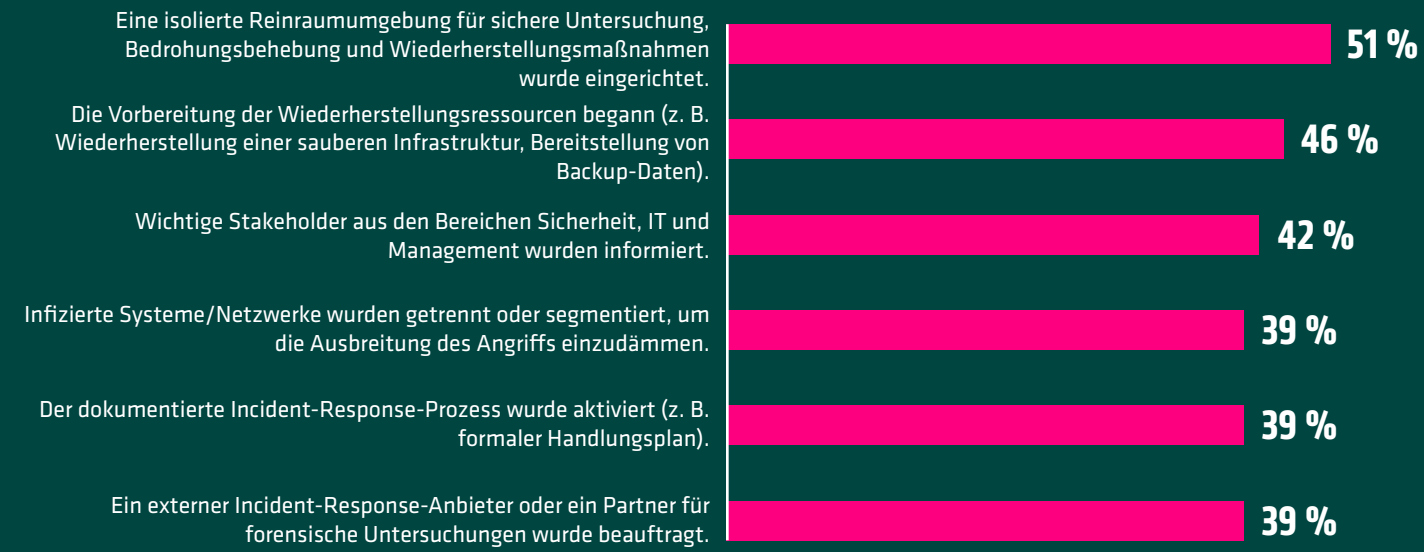
RESILIENZ UNTER BESCHUSS

WIE TEAMS ANGRIFFE IDENTIFIZIERTEN



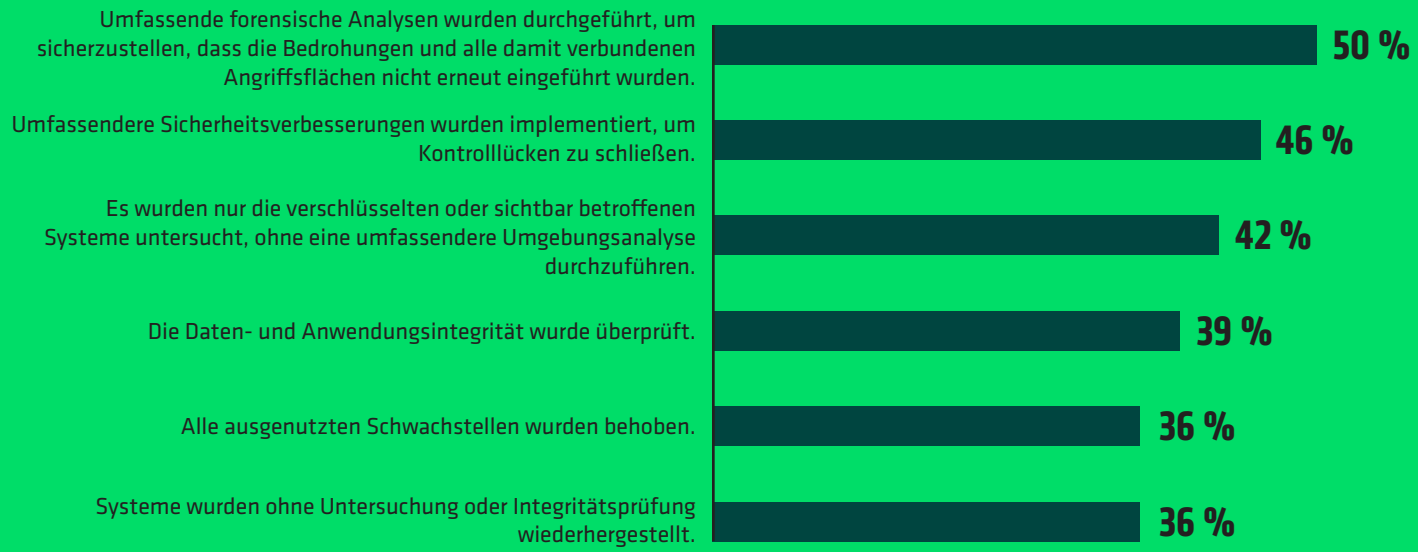
Im Falle eines Cyberangriffs gaben fast die Hälfte der Gesundheitsorganisationen an, dass Angriffe automatisch von ihren eigenen Sicherheitstools identifiziert und verifiziert wurden, während mehr als ein Drittel von den Tools gemeldet wurden, jedoch eine manuelle Überprüfung erforderten, bevor Maßnahmen ergriffen werden konnten. Warnmeldungen von Dritten waren deutlich seltener. Die Erkennung erfolgt größtenteils intern, ist jedoch weiterhin von einer menschlichen Bestätigung abhängig.

MASSNAHMEN DER EINSATZTEAMS NACH BESTÄTIGUNG DES ANGRIFFS



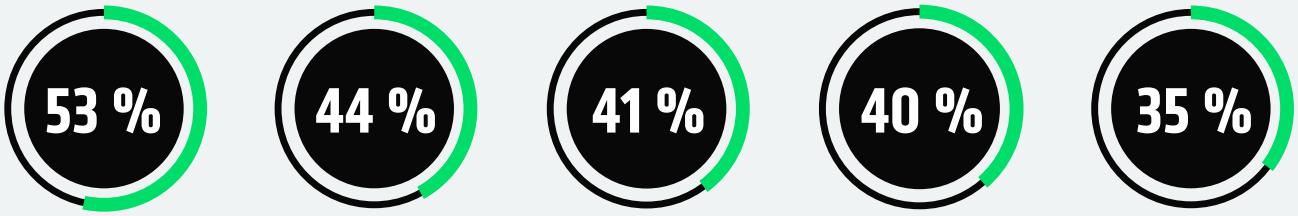
Nach der Bestätigung eines Angriffs ergriffen die Gesundheitsorganisationen eine Reihe von Maßnahmen, um die Wiederherstellung zu unterstützen. Knapp die Hälfte begann mit der Wiederherstellung einer sauberen Infrastruktur oder der Bereitstellung von Backup-Daten. Mehr als die Hälfte richtete isolierte Reinraumumgebungen für sichere Untersuchungen und Wiederherstellungen ein. Etwa vier von zehn informierten wichtige Stakeholder, isolierten infizierte Systeme, aktivierten formelle Strategiehandbücher oder beauftragten externe Experten für Vorfallsreaktion oder Forensik. Diese Abweichungen deuten darauf hin, dass die Reaktionsmaßnahmen in kritischen Schritten noch nicht vollständig standardisiert sind.

MASSNAHMEN VOR DER WIEDERINBETRIEBNAHME VON SYSTEMEN UND DATEN



Bevor die Systeme wieder online gebracht wurden, ergriffen Gesundheitsorganisationen eine Reihe von forensischen und Abhilfemaßnahmen. Die Hälfte führte vollständige forensische Untersuchungen durch, während knapp die Hälfte umfassendere Sicherheitsverbesserungen umsetzte. Weniger überprüften die Integrität von Daten und Anwendungen, patchten ausgenutzte Schwachstellen oder untersuchten Systeme, die über die sichtbar betroffenen hinausgingen. Über ein Drittel der Systeme wurde ohne vollständige Untersuchung oder Integritätsprüfung wiederhergestellt, wodurch Möglichkeiten für Neuinfektionen und Restrisiken verbleiben.

HERAUSFORDERUNGEN, MIT DENEN DIE TEAMS WÄHREND DES ANGRIFFS KONFRONTIERT WAREN



Die Teams berichteten von erheblichen Herausforderungen während des gesamten Prozesses.Viele hatten Schwierigkeiten, zu kommunizieren oder sich abzustimmen, solange kritische Systeme offline waren. Fast die Hälfte stand unter dem Druck, den Betrieb wiederherzustellen, bevor die Behebung der Sicherheitslücken abgeschlossen war. Die Umgehung von Sicherheitstools, erneute Infektionen und das Fehlen sauberer Wiederherstellungspunkte verschärften die Schwierigkeiten zusätzlich
dass stärkere Maßnahmen zur Resilienz erforderlich sind.

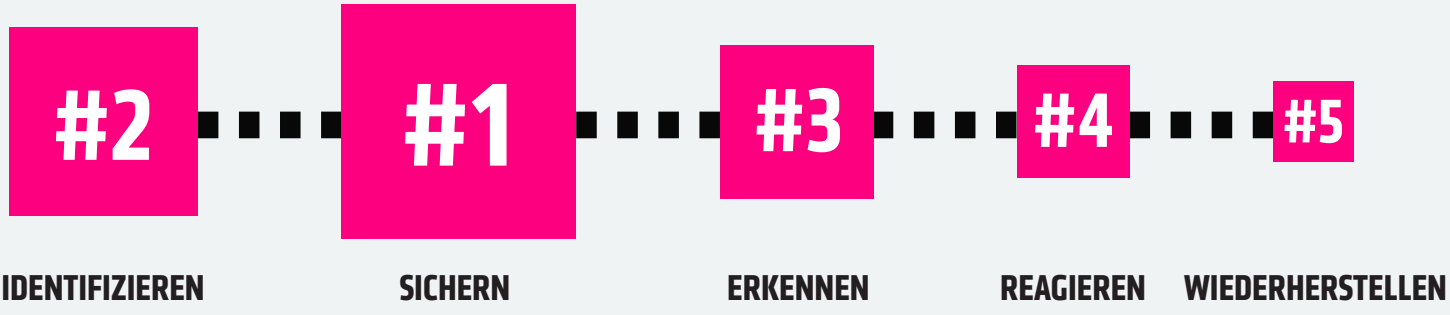
WO INVESTITIONEN IN RESILIENZ WEITERHIN UNZUREICHEND SIND

Selbst gut vorbereitete Unternehmen haben Schwierigkeiten, ihre Resilienz nach einem Angriff aufrechtzuerhalten. Operativer Druck, Kommunikationsstörungen und unvollständige Behebungsmaßnahmen decken weiterhin Schwächen in der Wiederherstellung und der Qualitätssicherung nach einem Vorfall auf. Die Ergebnisse zeigen zwar Fortschritte bei der Erkennung, aber auch einen deutlichen Bedarf an der Stärkung der Prozesse, die nach einem Angriff Vertrauen und Stabilität wiederherstellen.

Diese Muster spiegeln wider, wie Gesundheitsorganisationen heute ihre Budgetmittel für Cyber-Resilienz zuweisen. Wir haben die Befragten gebeten anzugeben, wie sie ihre Ausgaben auf die fünf Core-Funktionen des NIST-Cybersicherheits-Frameworks – Identifizieren, Sichern, Erkennen, Reagieren und Wiederherstellen – verteilen. Die meisten investieren weiterhin stark in Prävention, Schutz und Erkennung, während vergleichsweise weniger Mittel für Reaktion und nachgewiesene Wiederherstellung bereitgestellt werden. Das Ergebnis ist eine Reifekurve, die nach wie vor eher auf Abwehr als auf Wiederherstellung ausgerichtet ist und eine ungenutzte Chance zur Stärkung der Resilienz dort aufzeigt, wo es am wichtigsten ist: nach dem Angriff.

NIST-CYBERSICHERHEITSRAHMEN

Die Größe des Kastens zeigt den prozentualen Anteil der Investitionen in Cyber-Resilienz vom höchsten zum niedrigsten Wert an.



KI UND AUTOMATISIERUNG ERWEISEN SICH ALS MULTIPLIKATOREN DER RESILIENZ

Die Ergebnisse zeigen auch, dass Gesundheitsorganisationen KI als wichtigen Faktor für die Cyber Resilienz betrachten – insbesondere zur Verbesserung der Erkennungsgeschwindigkeit und der Präzision bei der Reaktion. Nahezu alle Befragten bewerteten Tools wie Anomalieerkennung, Verhaltensanalyse von Nutzern sowie KI gestützte Bedrohungsanalyse, -untersuchung und abwehr als wirksam zur Stärkung ihrer Sicherheitslage.

Auch neuere GenAI basierte Assistenten, die Bedrohungsabfragen in natürlicher Sprache und Kontextanalysen durchführen können, gewinnen zunehmend an Bedeutung, da sie die Entscheidungsfindung vereinfachen und beschleunigen. 61 % der Gesundheitsorganisationen gaben an, dass eine der wichtigsten Erkenntnisse nach einem Cyberangriff der Bedarf an mehr Automatisierung in den Bereichen Erkennung, Reaktion und Wiederherstellung war. Dies spiegelt die wachsende Nachfrage nach integrierten Automatisierungs und Orchestrierungsplattformen wider, bei denen KI als Kraftmultiplikator fungiert und für mehr Effizienz, Konsistenz und Effektivität aller dieser Prozesse sorgt.

Mit Blick auf die Zukunft erwarten die meisten, dass KI bis Ende 2026 eine zunehmend strategische Rolle in der Cyberabwehr einnehmen wird. 54 % gehen davon aus, dass KI die menschliche Entscheidungsfindung unterstützen und Analysen sowie Empfehlungen verbessern wird, wobei die Kontrolle über Maßnahmen weiterhin beim Menschen bleibt. Weitere 37 % erwarten, dass KI eine zentrale Rolle bei Erkennung und Reaktion spielt und sogar autonome Entscheidungen treffen kann. Dies signalisiert eine klare Entwicklung: KI entwickelt sich von einem Assistenten zu einem operativen Eckpfeiler der Cyber Resilienz – mit dem Potenzial, Geschwindigkeit, Präzision und Vertrauen über die gesamte Kette von Erkennung, Reaktion und Wiederherstellung hinweg zu verbessern.

DIE ZUKUNFT DER RESILIENZ BEGINNT JETZT

Während Gesundheitsorganisationen zwar messbare Fortschritte in der Cyber-Resilienz erzielen, haben viele weiterhin Verbesserungspotenzial bei Reaktion, Wiederherstellung und der Überprüfung ihrer Einsatzbereitschaft nach einem Angriff. Cyber-Resilienz ist ein enormer Wettbewerbsvorteil. Die Zukunft gehört den Organisationen, die in Mitarbeiter, Produkte und Prozesse investieren, um sich schneller zu erholen, das Vertrauen ihrer Patienten und Partner zu bewahren und den Betrieb aufrechtzuerhalten, wenn andere scheitern. In Zeiten nahezu unvermeidbarer Störungen bedeutet Resilienz nicht nur Schutz, sondern auch Leistungsfähigkeit.

Stärken Sie Ihre Widerstandsfähigkeit, bevor es zu einer Krise kommt:

- Buchen Sie einen Workshop zum Thema Ransomware-Resilienz.
- Optimieren Sie Ihre Cyber-Resilienz mit einem Fünf-Punkte-Aktionsplan.
- Erfahren Sie mehr über die Cyber-Resilienz-Lösungen von Cohesity.

VORGEHENSWEISE

COHESITY

Cohesity beauftragte Vanson Bourne mit einer Umfrage unter 3.200 IT- und Sicherheitsentscheidern im September 2025. Die Ergebnisse dieser Studie basieren auf den vorliegenden Daten. Die Befragten repräsentieren Organisationen in den USA (500), Brasilien (200), Großbritannien (400), Deutschland (400), Frankreich (400), den Vereinigten Arabischen Emiraten (100), Australien (200), Südkorea (200), Japan (400), Indien (200) und Singapur (200). Die Organisationen beschäftigen mindestens 1.000 Mitarbeiter und stammen aus verschiedenen Bereichen des öffentlichen und privaten Sektors, mit einem Schwerpunkt auf Finanzdienstleistungen, dem öffentlichen Sektor und dem Gesundheitswesen.

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000078-001-DE 4-2026