COHESITY

BERICHT ZUR CYBER-RESILIENZ

Risikobereit oder risikogefährdet: Die digitale Kluft der Cyber-Resilienz im öffentlichen Sektor

DER JUNI 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 Unternehmen von denjenigen unterscheidet, die noch immer kämpfen, befragte Cohesity 3.200 IT- und Sicherheitsentscheider in 11 Ländern. Darunter waren 399 Teilnehmer aus Organisationen des öffentlichen Sektors. Ihre Antworten zeigen eine wachsende Kluft in der Resilienz zwischen risikobereiten Unternehmen, die sich schnell und sicher erholen können, und ihren risikogefährdeten Pendants, die weiterhin anfällig für anhaltende Störungen und damit verbundene finanzielle Folgeschäden sind.

Unsere Studie untersucht die realen Auswirkungen schwerwiegender Cyberangriffe und zeigt, wie Organisationen des öffentlichen Sektors ihre Cyber-Resilienz anhand von Best Practices selbst bewertet und welche Maßnahmen sie ergriffen haben, um diese Vorfälle zu erkennen, darauf zu reagieren und sich davon zu erholen. Sie beleuchtet außerdem, was sie gelernt haben und wie sie KI und Automatisierung einsetzen, um ihre Resilienz zu stärken und die Kluft zu schließen.

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

Cybervorfälle sind nicht alle gleich. Viele Unternehmen haben fast 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 KEINE EINZELFÄLLE MEHR:

67 %

der Befragten haben mindestens einen erheblichen Cyberangriff erlebt

49 %

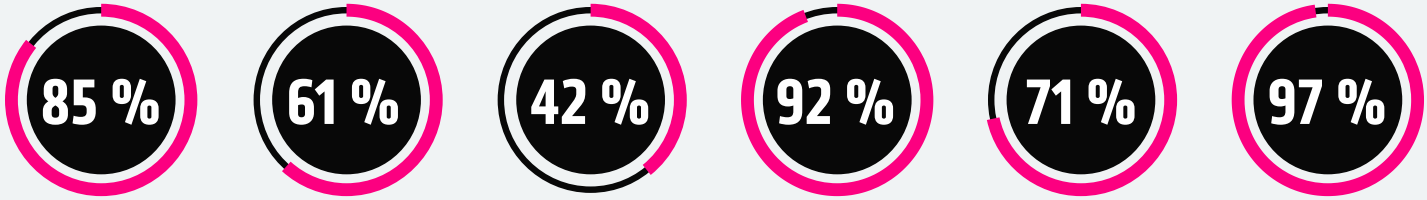
erlebten einen solchen Angriff in den letzten 12 Monaten

26 %

waren im Laufe des 12-Monats-Zeitraums von mehreren Vorfällen betroffen

DIE TATSÄCHLICHEN KOSTEN SCHWERWIEGENDER CYBERANGRIFFE

FINANZIELLER UND AUFSICHTSRECHTLICHER DRUCK WAR IN DEN VON UNS BEFRAGTEN ORGANISATIONEN DES ÖFFENTLICHEN SEKTORS ALLGEGENWÄRTIG:



85 %	61 %	42 %	92 %	71 %	97 %
meldeten Umsatzeinbußen	der börsennotierten Organisationen gaben an, ihre Finanzprognosen angepasst zu haben.[1]	verloren Kunden	zahlten Lösegeld – durchschnittlich 1,3 Mio. USD pro Vorfall	der privat geführten Unternehmen haben Mittel aus Wachstumsinitiativen verlagert	hatten mit rechtlichen oder aufsichtsrechtlichen Konsequenzen zu kämpfen, darunter Bußgelder (45 %) sowie Klagen oder Sammelklagen (40 %)

[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

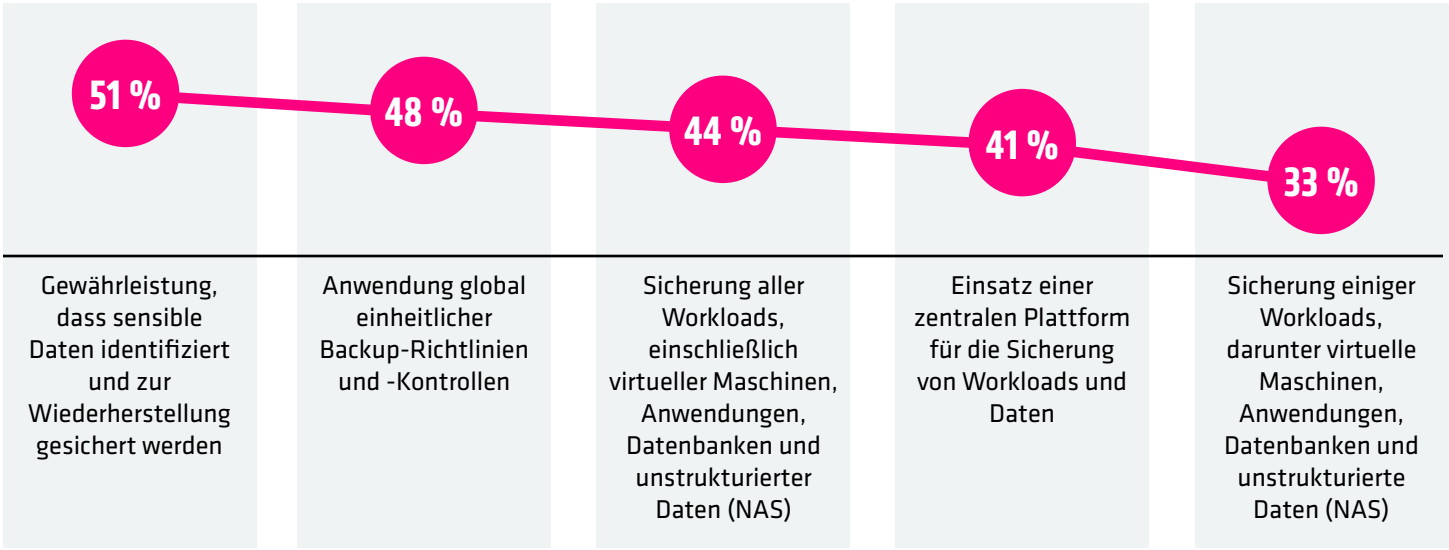
Angesichts des Ausmaßes der finanziellen und betrieblichen Auswirkungen, die unsere Nachforschungen aufgedeckt haben, könnte man erwarten, dass die Resilienz von Unternehmen weit verbreitet ist. Dennoch gab die Mehrheit der Befragten (54 %) an, vollstes Vertrauen in ihre Cyber-Resilienzstrategie zu haben 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.**

DATENSCHUTZ 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 Organisationen des öffentlichen Sektors gewährleisten, dass sensible Daten identifiziert und für die Wiederherstellung gesichert werden, während beinahe die Hälfte weltweit einheitliche Backup-Richtlinien und -Kontrollen anwendet. Weniger als die Hälfte sichert alle Workloads oder nutzt eine zentrale Plattform, um Workloads und Daten zu schützen. Ein Drittel sichert nur ausgewählte Workloads. Diese Zersplitterung schränkt die Transparenz und Konsistenz über verschiedene Umgebungen hinweg ein. Eine ausgereifte Cyber-Resilienz hängt davon ab, dass Datensicherung und -wiederherstellung innerhalb einer zentralen intelligenten Plattform vereinigt werden, die nach Zero-Trust-Prinzipien gesichert ist.

MAßNAHMEN ZUR WIEDERHERSTELLBARKEIT VON DATEN SIND ÜBLICH, DOCH DER REIFEGRAD VARIIERT

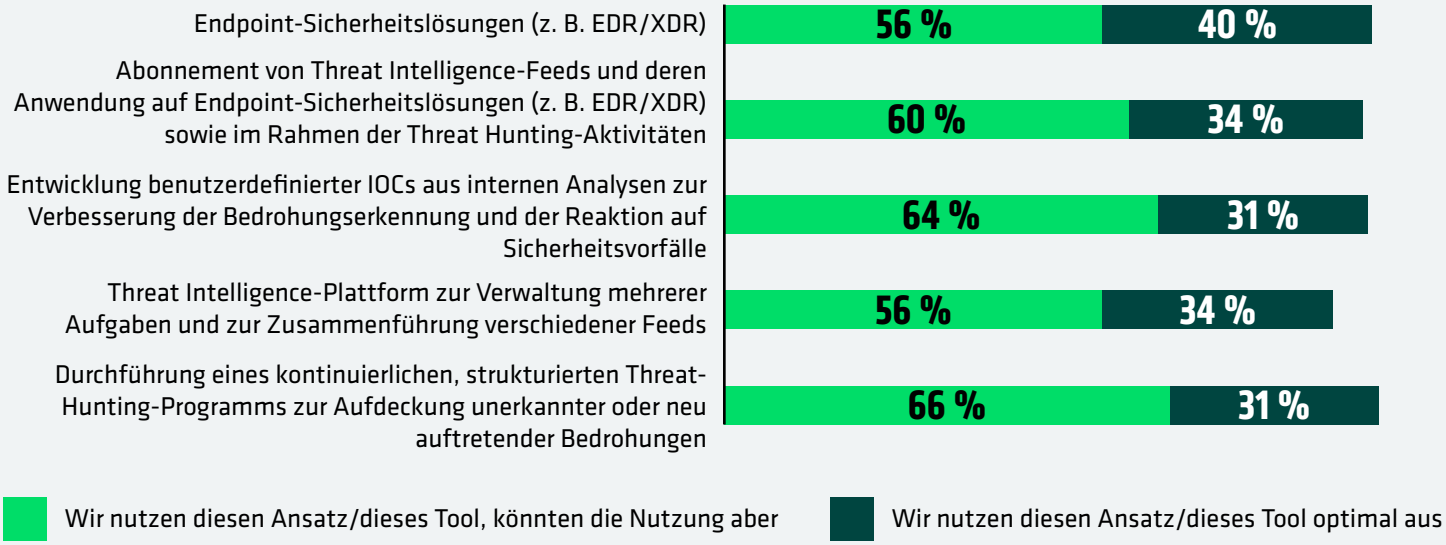
Was unternimmt Ihr Unternehmen, um die jederzeitige Wiederherstellbarkeit seiner Daten zu gewährleisten?

50 %	Zusätzliche Autorisierung für risikoreiche administrative Aufgaben im Zusammenhang mit Datensicherung und -wiederherstellungs lösungen
47 %	Befolgung der „3-2-1-Backup-Regel“ (drei Datenkopien auf zwei verschiedenen Speichermedien, wobei eine Kopie extern aufbewahrt wird)
46 %	Multifaktor-Authentifizierung für unsere Backup-Lösung
46 %	Zugriffsrechte nach dem Prinzip der minimalen Berechtigungen für gesicherte Workloads
38 %	Schutz kritischer Daten durch Unveränderlichkeit

Viele Organisationen des öffentlichen Sektors haben die Zugriffskontrollen rund um Backup-Umgebungen verstärkt; bei der Hälfte ist für risikoreiche Aufgaben eine zusätzliche Administratorautorisierung erforderlich. Etwa die Hälfte setzt Multifaktor-Authentifizierung durch, befolgt die 3-2-1-Backup-Regel und wendet Zugriffsrechte nach dem Prinzip der minimalen Berechtigungen an. Nur wenige schützen kritische Daten durch Unveränderlichkeit. 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 optimal genutzt. Die meisten Organisationen des öffentlichen Sektors setzen Endpunktsicherheit, Threat Intelligence Feeds, benutzerdefinierte IOCs, Threat Intelligence-Plattformen und strukturierte Programme zur Bedrohungssuche ein, doch nur eine Minderheit nutzt das volle Potenzial dieser Tools. Eine ausgereifte Cyber-Resilienz erfordert die Integration dieser Tools in einen kontinuierlichen Informationskreislauf, der die Transparenz, Erkennung und Reaktion verbessert.

ORGANISATIONEN SIND ANFÄLLIG FÜR ERNEUTE INFEKTIONEN

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

57 % Jährlich werden End-to-End-Simulationen durchgeführt, an denen ein funktionsübergreifendes Team aus technischen, juristischen, strategischen, leitenden und kommunikativen Stakeholdern teilnimmt

52 % Kritische Systeme und Informationen werden online und sicher gespeichert, um die Reaktion auf Vorfälle und die Wiederherstellung zu unterstützen

48 % Sicherheitslücken identifizieren und beheben, bevor Systeme wieder in Betrieb genommen werden

43 % Für die Untersuchung, Behebung und sichere Wiederherstellung von Vorfällen wird eine isolierte Umgebung genutzt

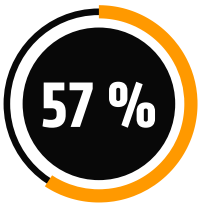
36 % Alle Backup-Daten sind unveränderlich

Organisationen des öffentlichen Sektors verbessern ihre Strategien zur Anwendungsresilienz, doch es bestehen weiterhin Lücken. Beinahe die Hälfte identifiziert Sicherheitskontrolllücken, bevor Systeme wiederhergestellt werden, und mehr als die Hälfte führt jährliche Wiederherstellungsübungen durch. Etwas mehr als die Hälfte der Organisationen unterhalten Online-Speicher mit verschlüsselten Repositories, während weniger Organisationen isolierte Umgebungen für sichere Untersuchungen und Datenwiederherstellung nutzen. Ein noch kleinerer Prozentsatz wendet Unveränderlichkeit auf alle Backup-Daten an. Diese Lücken machen Wiederherstellungsprozesse anfällig für erneute Infektionen oder Datenverlust. Ausgereifte Cyber-Resilienz kombiniert Vorbereitung mit sicheren, verifizierbaren Wiederherstellungszonen.

DIE DATENKLASSIFIZIERUNG GEWINNT AN BEDEUTUNG, DOCH DER RISIKOGESTEUERTE EINSATZ BEFINDET SICH NOCH IN DER ENTWICKLUNG

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

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



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

Identifizierung und Priorisierung von Backup-Systemen

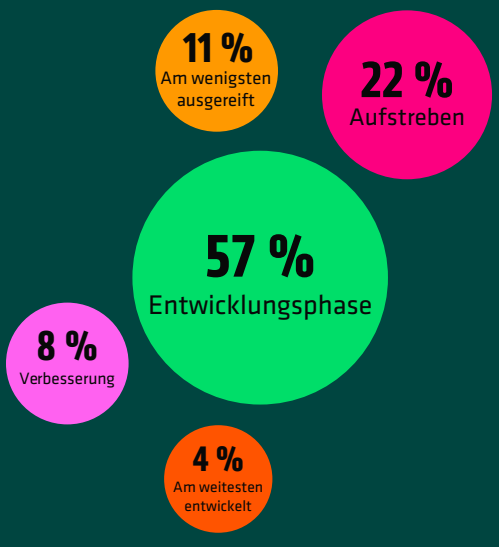
Definition und Analyse der Wesentlichkeit eines Cyberangriffs vor dessen Eintreten

Organisationen des öffentlichen Sektors nutzen Datenermittlung und -klassifizierung strategischer in den Bereichen Compliance, Reaktion und Wiederherstellung. Mehr als die Hälfte beschäftigt sich mit Datenschutz- und Sicherheitsverletzungen, während etwas mehr als die Hälfte Klassifizierungen nutzt, um die Compliance während eines Angriffs sicherzustellen, und die Wesentlichkeit vor einem Vorfall zu definieren. Ein ähnlicher Anteil legt Prioritäten für Backups auf Grundlage des Risikos fest. Diese Muster 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, der das Datenrisikomanagement optimiert und als Grundlage für Schutz, Reaktion und Wiederherstellung dient.

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 dafür, wie Organisationen des öffentlichen Sektors in der Praxis Resilienz aufbauen – oder sich damit schwer tun. Während sich die Mehrheit noch in der Entwicklungsphase befindet, verfügen lediglich 4 % 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 (22 %): 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.

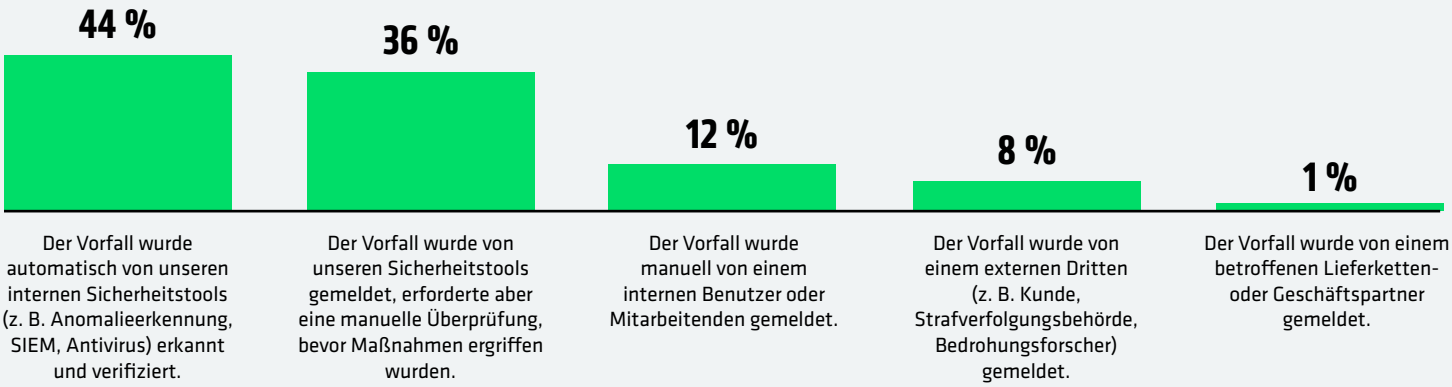
Entwicklungsphase (57 %): Kernpraktiken wie Datensicherung, administrative Kontrollen und Threat Intelligence sind zwar verbreiteter, aber noch nicht einheitlich. Wiederherstellungsumgebungen, Compliance-Prüfungen und die Behebung von Sicherheitslücken werden nur sporadisch angewendet, wodurch die Maßnahmen zur Erhöhung der Resilienz nur teilweise wirksam sind.

Verbesserung (8 %): 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 (4 %): 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.

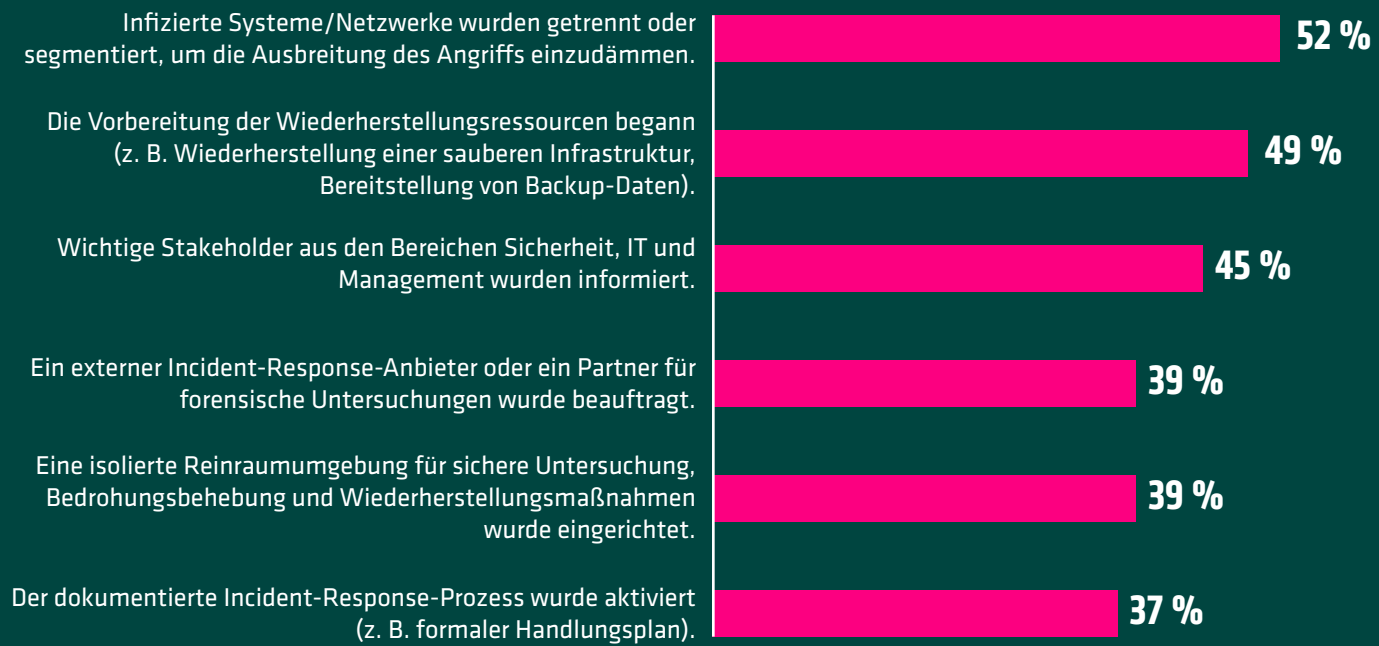
RESILIENZ UNTER BESCHUSS

WIE TEAMS ANGRIFFE IDENTIFIZIERTEN



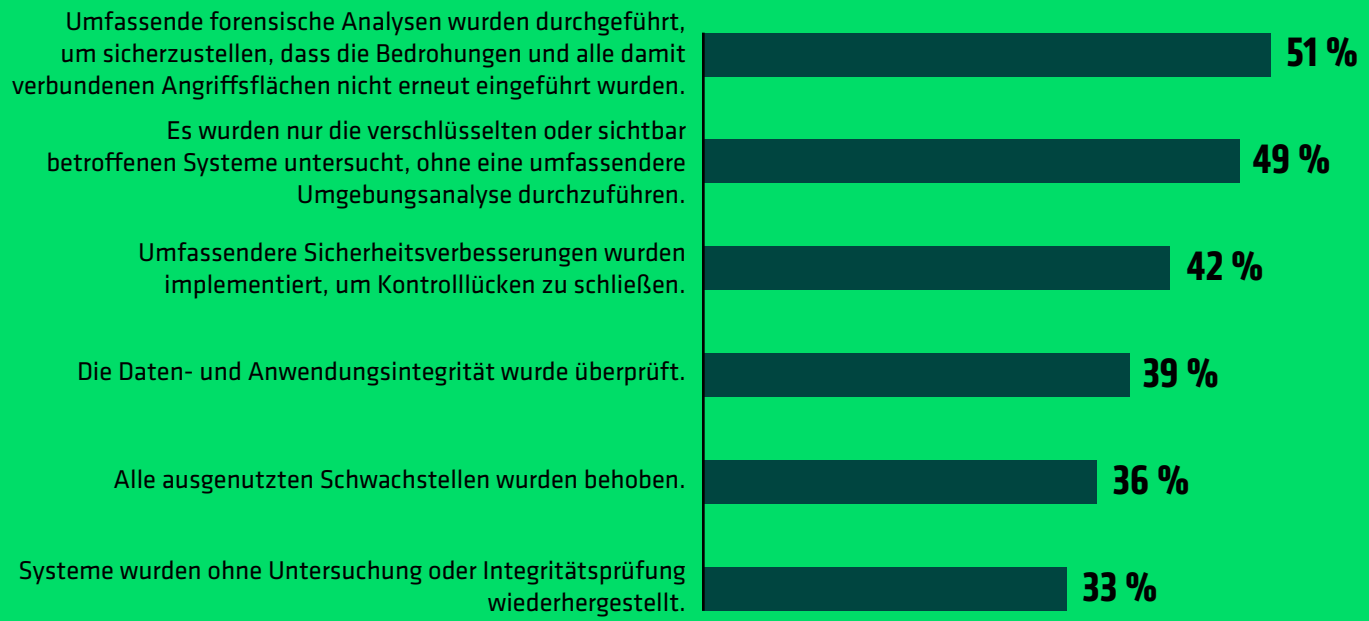
Im Falle eines Cyberangriffs erkennen die meisten Organisationen des öffentlichen Sektors die Vorfälle intern. Der größte Anteil wird automatisch von Sicherheitstools identifiziert und verifiziert, während viele andere von Tools gemeldet werden, aber eine manuelle Überprüfung benötigen. Von Mitarbeitenden oder externen Parteien werden deutlich weniger Vorfälle gemeldet. Die Erkennung übernehmen größtenteils Tools, wobei die menschliche Validierung weiterhin eine wichtige Rolle spielt.

MAßNAHMEN DER EINSATZTEAMS NACH BESTÄTIGUNG DES ANGRIFFS



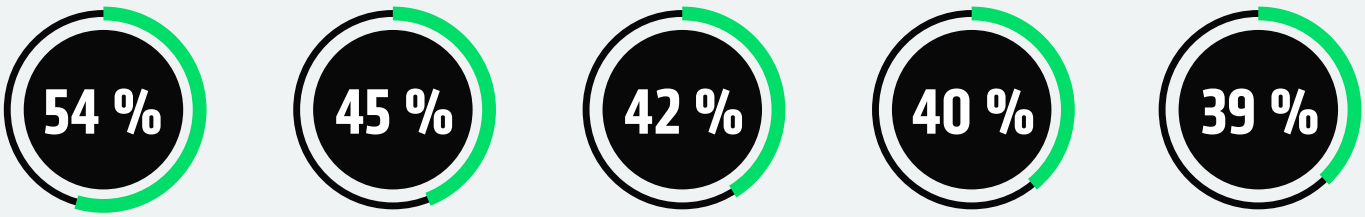
Nach der Bestätigung eines Angriffs unternahmen Organisationen des öffentlichen Sektors unterschiedliche Schritte, um die Bedrohung unter Kontrolle zu bringen und mit der Wiederherstellung zu beginnen. Etwa die Hälfte trennte infizierte Systeme vom Netz oder begann mit der Vorbereitung von Ressourcen für eine saubere Wiederherstellung, während viele wichtige Stakeholder informierten. Ein kleinerer Anteil richtete isolierte Reinraumumgebungen ein, aktivierte formale Playbooks zur Reaktion oder band externe Incident-Response-Partner ein. Diese Unterschiede deuten darauf hin, dass die Reaktionsmaßnahmen bei kritischen Aktionen noch nicht durchgängig standardisiert sind.

MAßNAHMEN VOR DER WIEDERINBETRIEBNAHME VON SYSTEMEN UND DATEN



Bevor Systeme und Daten wieder online gestellt wurden, unternahmen Organisationen des öffentlichen Sektors eine Reihe forensischer Maßnahmen und Abhilfemaßnahmen. Etwa die Hälfte der Organisationen führte umfassende forensische Untersuchungen durch oder konzentrierte sich nur auf sichtbar betroffene Systeme, während weniger Organisationen umfassendere Sicherheitsverbesserungen umsetzten, die Integrität überprüften oder ausgenutzte Schwachstellen patchten. Bemerkenswert ist, dass etwa ein Drittel der Systeme ohne weitere Untersuchung oder Überprüfung wiederhergestellt wurde, wodurch potenzielle Lücken entstanden, die das Risiko einer erneuten Infektion oder einer anhaltenden Exposition erhöhen könnten.

HERAUSFORDERUNGEN, MIT DENEN DIE TEAMS WÄHREND DES ANGRIFFS KONFRONTIERT WAREN



Die Teams standen während des Angriffs vor erheblichen betrieblichen und technischen Herausforderungen. Viele hatten Schwierigkeiten bei der Kommunikation, während wichtige Systeme ausgefallen waren, und standen unter dem Druck, die Systeme wiederherzustellen, noch bevor die Fehlerbehebung abgeschlossen war. Andere berichteten über Umgehung von Sicherheitstools, angegriffene Backups, fehlende saubere Wiederherstellungspunkte oder sogar eine erneute Infektion nach der Wiederherstellung. Diese Schwierigkeiten verdeutlichen Lücken in der Bereitschaft, die Reaktion erschweren und die Unterbrechung verlängern können.

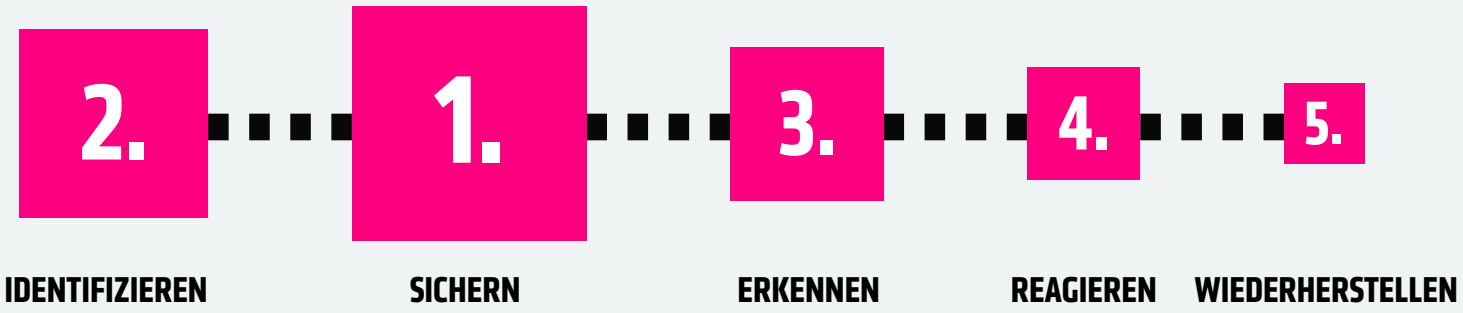
WO INVESTITIONEN IN RESILIENZ WEITERHIN UNZUREICHEND SIND

Selbst gut vorbereitete Unternehmen haben Schwierigkeiten, ihre Resilienz nach einem Angriff aufrechtzuerhalten. Angesichts des zunehmenden betrieblichen Drucks zeigen Koordinationslücken, unvollständige Abhilfemaßnahmen und das Risiko von erneuten Infektionen, wie fragil die Wiederherstellung ohne einheitliche Prozesse und kontinuierliche Qualitätssicherung sein kann.

Diese Muster spiegeln wider, wie Organisationen des öffentlichen Sektors 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 Organisationen des öffentlichen Sektors KI als wichtigen Faktor für Cyber-Resilienz betrachten, insbesondere zur Verbesserung der Erkennungsgeschwindigkeit und Reaktionspräzision. Nahezu alle Befragten bewerteten Tools wie Anomalieerkennung, Verhaltensanalyse von Nutzern sowie KI-gestützte Bedrohungsanalyse 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. 56 % der Organisationen des öffentlichen Sektors 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 so 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 spielen wird. 43 % gehen davon aus, dass KI die menschliche Entscheidungsfindung unterstützen und Analysen und Empfehlungen verbessern wird, wobei die Kontrolle über die endgültigen Maßnahmen beim Menschen bleibt. Weitere 42 % erwarten, dass KI eine zentrale Rolle bei Erkennung und Reaktion einnehmen und sogar autonome Entscheidungen treffen wird. Dies signalisiert eine klare Entwicklung: KI entwickelt sich von einem Assistenten zu einem operativen Eckpfeiler der Cyber-Resilienz und ist darauf ausgerichtet, Geschwindigkeit, Präzision und Vertrauen bei Erkennung, Reaktion und Wiederherstellung zu verbessern.

DIE ZUKUNFT DER RESILIENZ BEGINNT JETZT

Organisationen des öffentlichen Sektors erzielen zwar messbare Fortschritte in Sachen Cyber-Resilienz, doch viele haben noch Verbesserungspotenzial bei Reaktion, Wiederherstellung und der Überprüfung ihrer Einsatzbereitschaft nach einem Angriff. Cyber-Resilienz ist ein enormer Wettbewerbsvorteil. Die Zukunft gehört den Unternehmen, die in Mitarbeiter, Produkte und Prozesse investieren, um sich schneller zu erholen, das Vertrauen ihrer Kunden zu erhalten und den Geschäftsbetrieb 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.
  - Regierung/Ministerien
  - Landes-/Kommunalbehörden und Bildung

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 Unternehmen in den USA (500), Brasilien (200), Großbritannien (400), Deutschland (400), Frankreich (400), den Vereinigten Arabischen Emiraten/Saudi-Arabien (100), Australien (200), Südkorea (200), Japan (400), Indien (200) und Singapur (200). Die Unternehmen 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

2000093-001-DE 6-2026