COHESITY

BERICHT ZUR CYBER-RESILIENZ

Risikobereit oder risikogefährdet: Die Kluft bei der Cyber-Resilienz in mittelständischen Unternehmen

MAI 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 befanden sich fast 1.000 Teilnehmer aus mittelständischen Unternehmen. 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 mittelständische Unternehmen 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 ANGRIFFE MIT GROSSER WIRKUNG SIND FÜR MITTELSTÄNDISCHE ORGANISATIONEN KEINE EINZELFÄLLE MEHR.

75 %

der Befragten haben mindestens einen erheblichen Cyberangriff erlebt.

55 %

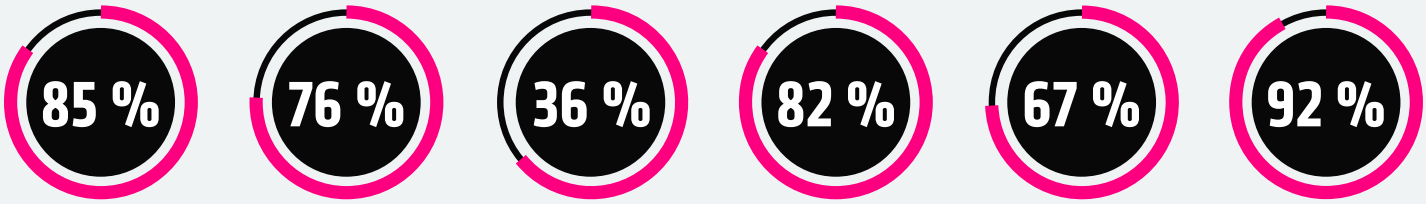
haben einen solchen Angriff in den letzten 12 Monaten erlebt.

25 %

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

DIE TATSÄCHLICHEN KOSTEN SCHWERWIEGENDER CYBERANGRIFFE

FINANZIELLER UND REGULATORISCHER DRUCK WAR AUCH IN DEN VON UNS BEFRAGTEN MITTELSTÄNDISCHEN ORGANISATIONEN ZU SPÜREN:



85 % meldeten Umsatzeinbußen

76 % der börsennotierten Organisationen gaben an, ihre Finanzprognosen angepasst zu haben[1]

36 % verlorene Kunden

82 % zahlten Lösegeld – durchschnittlich 1,3 Mio. USD pro Vorfall

67 % der privat geführten Unternehmen haben Mittel aus Wachstumsinitiativen verlagert

92 % hatten mit rechtlichen oder aufsichtsrechtlichen Konsequenzen zu kämpfen, darunter Bußgelder (46 %) sowie Klagen oder Sammelklagen (33 %)

[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

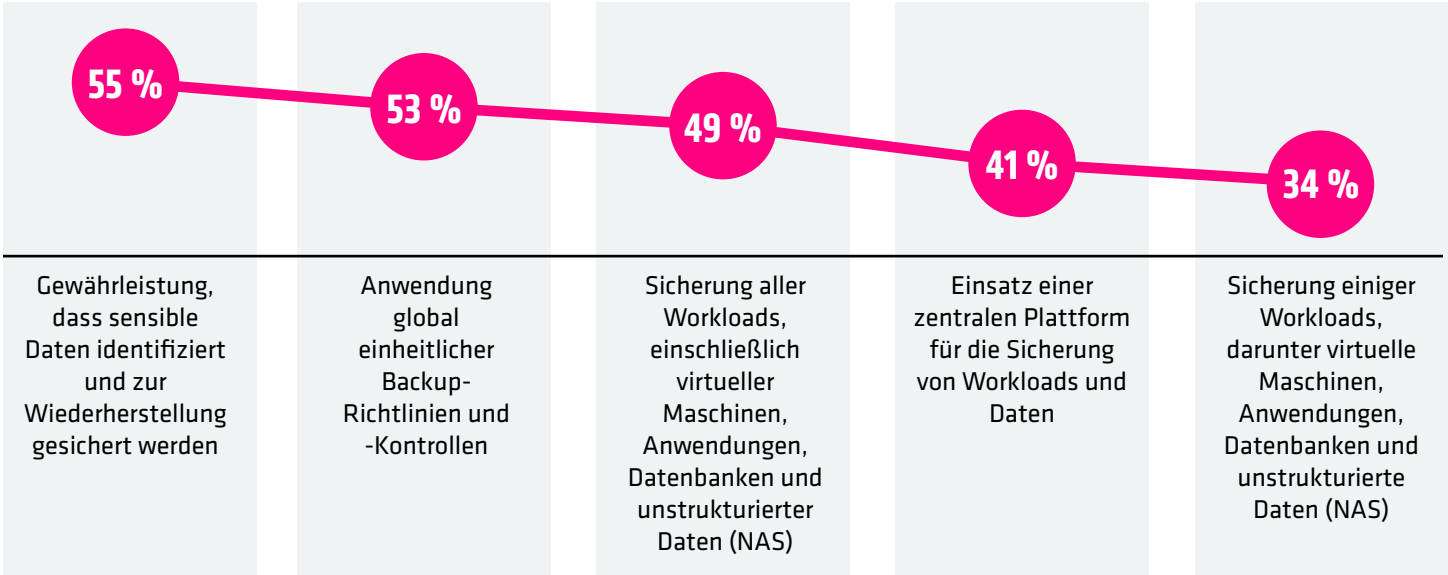
Angesichts des Ausmaßes der finanziellen und betrieblichen Auswirkungen, die unsere Nachforschungen aufgedeckt haben, könnte man erwarten, dass die Resilienz von Unternehmen weit verbreitet ist. Dennoch gaben viele Befragte (47 %) an, vollstes Vertrauen in ihre Cyber-Resilienzstrategie zu haben und den 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

Was unternimmt Ihre Organisation, um alle Daten in Hybrid- und/oder Multicloud-Umgebungen zu schützen?



Etwas mehr als die Hälfte der mittelständischen Unternehmen stellt sicher, dass sensible Daten identifiziert und für die Wiederherstellung gesichert werden. Ungefähr derselbe Anteil wendet weltweit konsistente Backup-Richtlinien und -Kontrollen an. 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

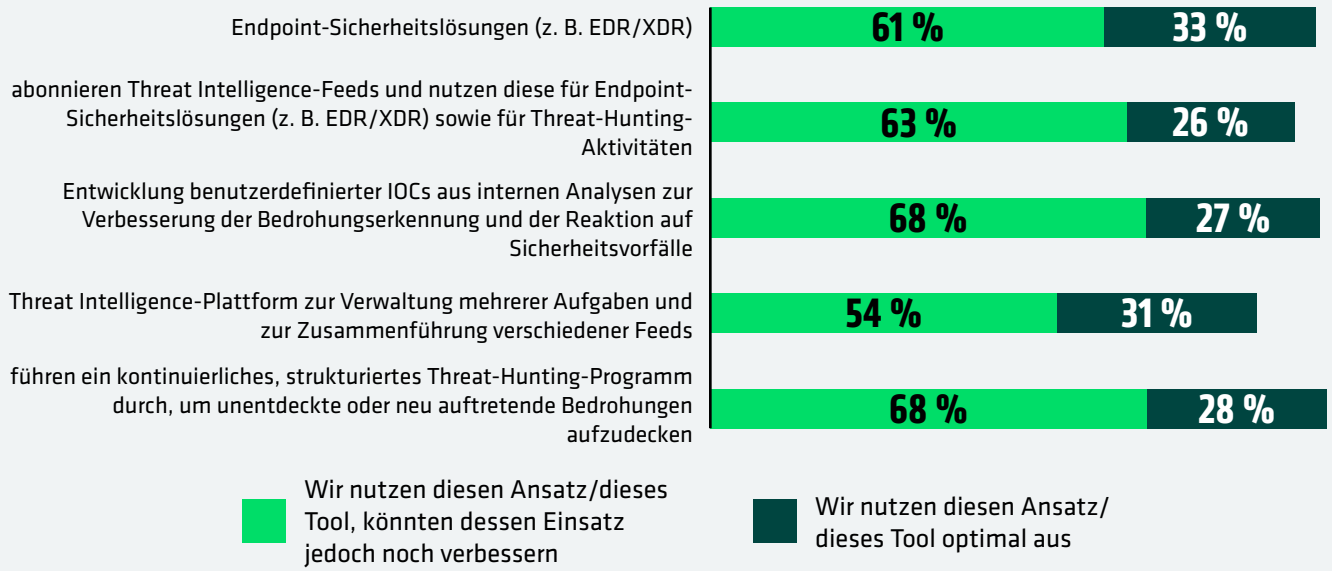
Was unternimmt Ihr Unternehmen, um die jederzeitige Wiederherstellbarkeit seiner Daten zu gewährleisten?

60 %	erfordern eine zusätzliche Autorisierung für risikoreiche Administrationsaufgaben im Zusammenhang mit Lösungen für Datensicherung und -wiederherstellung
53 %	Multifaktor-Authentifizierung für unsere Backup-Lösung
47 %	halten sich an die „3-2-1-Regel für Backups“ (drei Datenkopien, gespeichert auf zwei verschiedenen Medientypen, wobei eine Kopie außerhalb des Standorts aufbewahrt wird)
42 %	Schutz kritischer Daten durch Unveränderlichkeit
38 %	Zugriffsrechte nach dem Prinzip der minimalen Berechtigungen für gesicherte Workloads

Viele mittelständische Unternehmen haben die Zugriffskontrollen rund um Backup-Umgebungen verstärkt; bei mehr als der Hälfte ist für risikoreiche Aufgaben eine zusätzliche Administratorautorisierung erforderlich. Etwa die Hälfte setzt eine Multi-Faktor-Authentifizierung ein, und fast die Hälfte hält sich an die 3-2-1-Regel für Backups. Weniger als die Hälfte sichert kritische Daten durch Unveränderlichkeit oder wendet das Prinzip der geringsten 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 optimal genutzt. Die meisten mittelständischen Unternehmen 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.

UNVOLLSTÄNDIGE RESILIENZMASSNAHMEN ERHÖHEN DAS RISIKO EINER NEUINFEKTION

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

57 % Sicherheitslücken identifizieren und beheben, bevor Systeme wieder in Betrieb genommen werden

60 % führen jährlich End-to-End-Simulationsübungen durch, an denen ein funktionsübergreifendes Team aus technischen, rechtlichen, strategischen, leitenden und kommunikationsbezogenen Stakeholdern teilnimmt

56 % nutzen ein online verfügbares, gesichertes Repository für kritische Systeme und Informationen, um die Vorfallsreaktion und die Wiederherstellung zu unterstützen

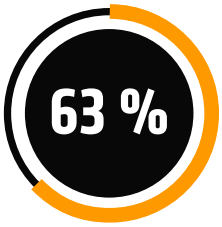
47 % Für die Untersuchung, Behebung und sichere Wiederherstellung von Vorfällen wird eine isolierte Umgebung genutzt

33 % Alle Backup-Daten sind unveränderlich

Mittelständische Unternehmen verbessern ihre Strategien zur Anwendungsresilienz, doch es bestehen weiterhin Lücken. Ein Großteil identifiziert Sicherheitskontrolllücken, bevor die Systeme wiederhergestellt werden. Ein vergleichbarer Anteil unterhält online gesicherte Tresor-Repositorys. Mehr als die Hälfte führt außerdem jährliche Wiederherstellungsübungen durch. Nur wenige nutzen isolierte Umgebungen für sichere Untersuchungen und die Wiederherstellung. 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.

DATENKLASSIFIZIERUNG GEWINNT AN BEDEUTUNG, WÄHREND SICH DIE RISIKOEXPOSITION ERWEITERT

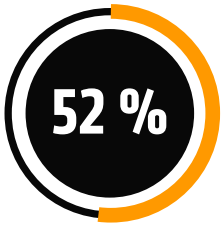
Wie nutzt Ihre Organisation Ansätze/Tools zur Datenermittlung und -klassifizierung, um das Datenrisiko im gesamten Datenbestand zu minimieren?



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

verwenden die Klassifizierung von Backup-Daten, um die Compliance-Verpflichtungen für die betroffenen Daten zu ermitteln

definieren und verstehen die Wesentlichkeit von erheblichen Cyberangriffen, bevor ein Vorfall eintritt



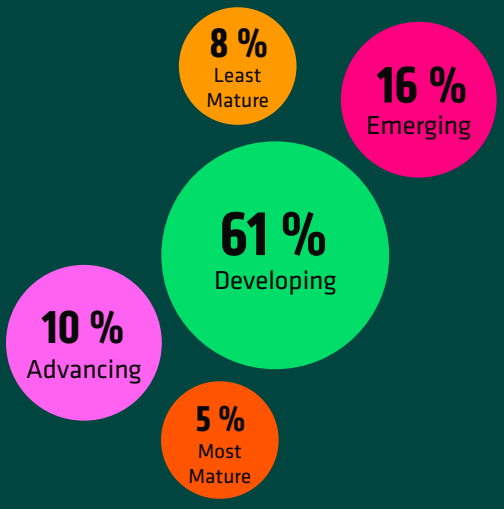
Identifizierung und Priorisierung von Backup-Systemen

Mittelständische Unternehmen nutzen Datenermittlung und -klassifizierung strategischer in den Bereichen Compliance, Reaktion und Wiederherstellung. Fast zwei Drittel befassen sich mit Datenschutz- und Sicherungsverstößen, während mehr als die Hälfte Klassifizierungen nutzt, um die Compliance während eines Angriffs sicherzustellen. Mehr als die Hälfte legt zudem bereits vor dem Eintreten eines Vorfalls fest, was als wesentlich gilt, und priorisiert Backups anhand der Risiken. 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 mittelständische Unternehmen in der Praxis Resilienz aufbauen – oder sich damit schwer tun. Während sich die Mehrheit noch in der Entwicklungsphase befindet, verfügen lediglich 5 % über die ausgereiftesten, integrierten Fähigkeiten, die risikobereite Unternehmen kennzeichnen.

DIE REIFEGRADKURVE FÜR CYBER-RESILIENZ



Geringster Reifegrad (8 %): Backups, Richtlinien und Sicherheitsvorkehrungen fehlen weitgehend oder sind uneinheitlich. MFA und administrative Kontrollen werden selten durchgesetzt, die Wiederherstellung ist oft unzureichend isoliert, und Compliance- oder Wesentlichkeitsprüfungen werden typischerweise vernachlässigt.

Im Entstehungsstadium (16 %): Einige Maßnahmen zur Erhöhung der Resilienz sind vorhanden, werden aber nicht einheitlich angewendet. Organisationen sichern möglicherweise sensible Daten, wenden globale Richtlinien an oder nutzen Multi-Faktor-Authentifizierung (MFA), jedoch selten in Kombination miteinander. Threat Intelligence-Analyse und Compliance sind zwar vorhanden, aber noch nicht ausgereift und fragmentiert.

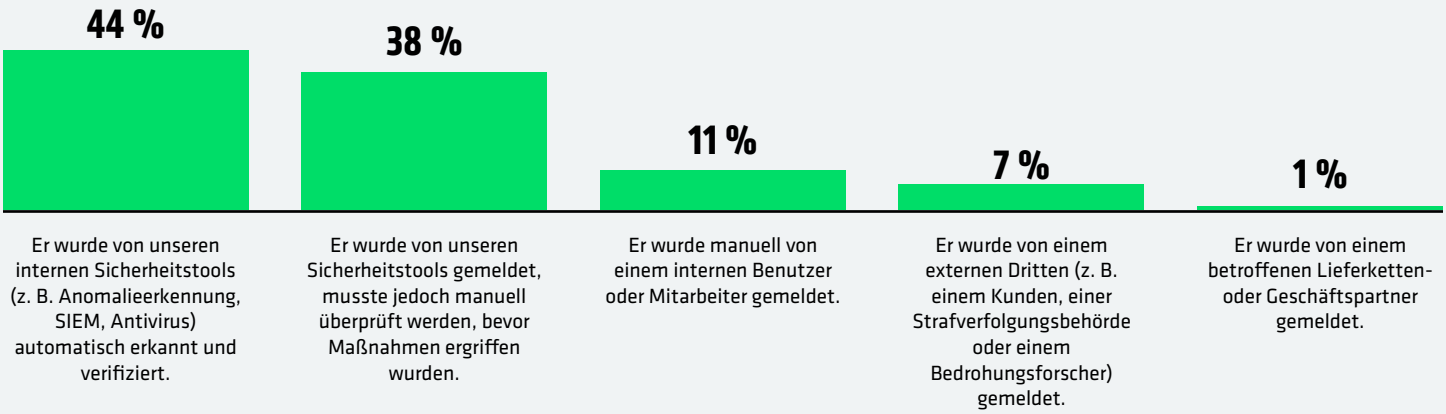
In Entwicklung (61 %): Grundlegende Praktiken wie Backups, Admin-Kontrollen und Threat Intelligence sind häufiger, wenn auch weiterhin uneinheitlich. Wiederherstellungsumgebungen, Compliance-Prüfungen und die Behebung von Sicherheitslücken werden nur sporadisch eingesetzt, wodurch die Maßnahmen zur Gewährleistung der Resilienz nur teilweise wirksam sind.

Fortgeschritten (10 %): Die meisten Schlüsselpraktiken werden konsequent durchgesetzt, einschließlich globaler Backup-Richtlinien, Admin-Genehmigungen und der Behebung von Problemen vor der Wiederherstellung. Threat Intelligence wird genutzt, aber nicht vollständig optimiert, und es bestehen noch einige Lücken bei isolierter Wiederherstellung und vollständiger Compliance-Abdeckung.

Höchster Reifegrad (5 %): Resilienz ist systemisch und umfassend. Sensible Daten werden weltweit gesichert, MFA und Admin-Kontrollen sind Standard, Threat Intelligence ist maximiert, die Wiederherstellung wird durch Behebung abgesichert, und Compliance-Schutzmaßnahmen werden konsequent eingehalten.

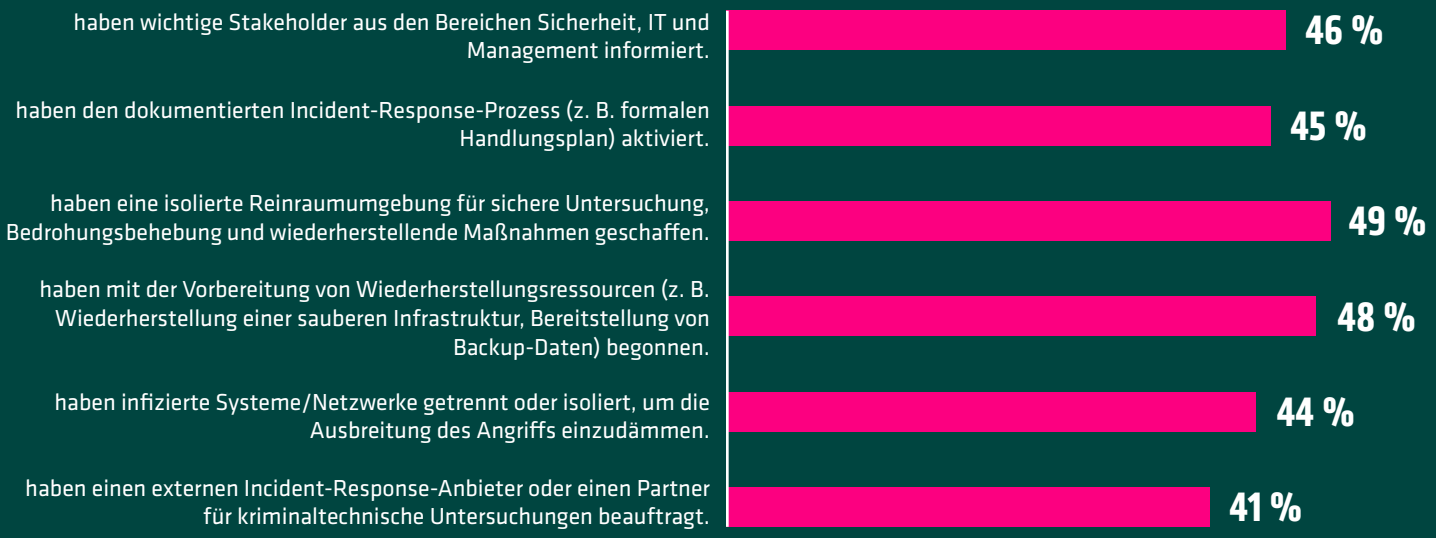
RESILIENZ UNTER BESCHUSS

WIE TEAMS ANGRIFFE IDENTIFIZIERTEN



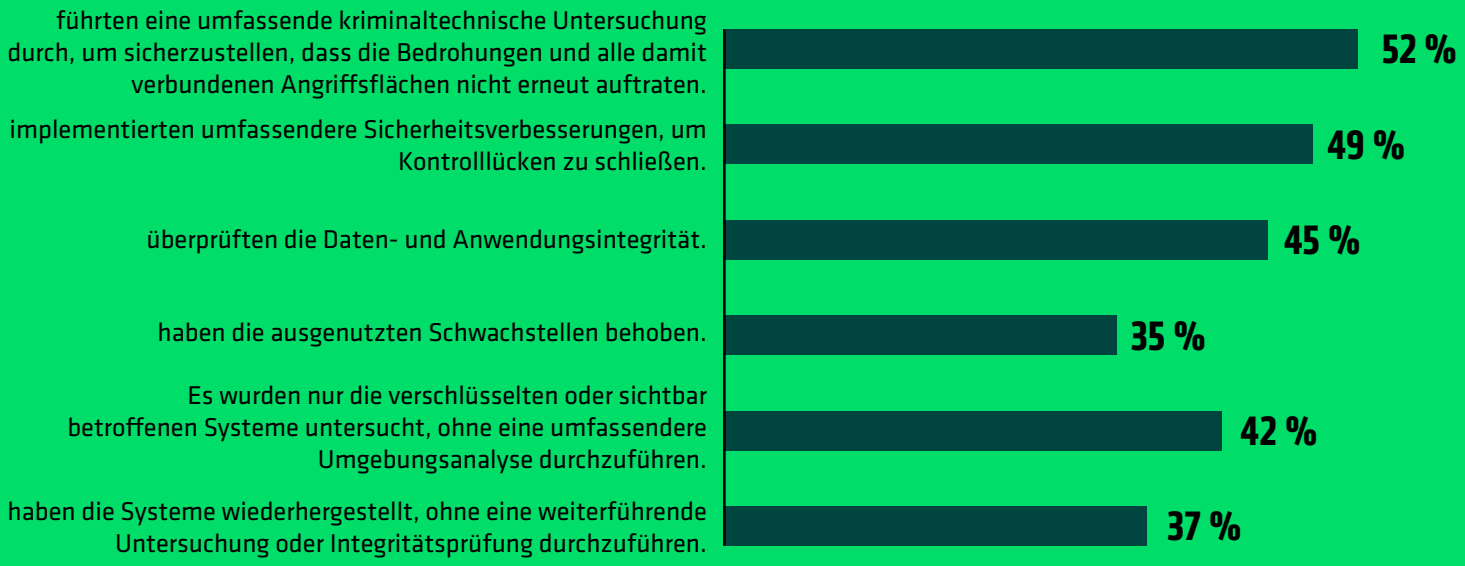
Im Falle eines Cyberangriffs erkennen die meisten mittelständischen Unternehmen Vorfälle intern, wobei der größte Teil davon automatisch identifiziert und durch Sicherheitstools überprüft wird. Viele weitere Vorfälle werden zwar von den Tools gemeldet, erfordern jedoch eine manuelle Überprüfung, bevor Maßnahmen ergriffen werden. 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



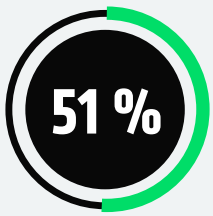
Nach der Bestätigung eines Angriffs ergriffen mittelständische Unternehmen eine Reihe von Maßnahmen, um die Bedrohung abzuschwächen und mit der Wiederherstellung zu beginnen. Ein ähnlicher Anteil begann mit der Vorbereitung von Ressourcen für die Wiederherstellung, richtete isolierte Reinraumumgebungen ein, informierte wichtige Stakeholder, schaltete infizierte Systeme ab und aktivierte Playbooks für die Vorfallsreaktion. Etwas weniger Unternehmen zogen externe Partner für die Vorfallsreaktion hinzu. Diese Muster deuten darauf hin, dass Reaktionsmaßnahmen zwar weitgehend umgesetzt werden, bei kritischen Maßnahmen jedoch noch nicht vollständig standardisiert sind.

MASSNAHMEN VOR DER WIEDERINBETRIEBNAHME VON SYSTEMEN UND DATEN

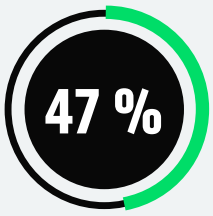


der mittelständischen Unternehmen setzten, bevor sie ihre Systeme und Daten wieder online stellten, eine Kombination aus kriminaltechnischen und Abhilfemaßnahmen ein. Etwa die Hälfte führte umfassende kriminaltechnisch Untersuchungen durch, setzte umfassendere Sicherheitsverbesserungen um oder überprüfte die Daten- und Anwendungsintegrität, während sich ein ähnlich großer Anteil ausschließlich auf die sichtbar betroffenen Systeme konzentrierte. Ein geringerer Anteil patchte ausgenutzte Sicherheitslücken oder stellte Systeme wieder her, ohne Untersuchungen oder Überprüfungen durchzuführen. Diese Lücken können das Risiko einer Neuinfektion oder einer weiteren Gefährdung erhöhen.

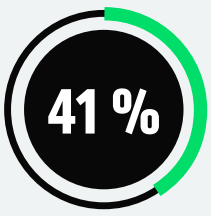
HERAUSFORDERUNGEN, MIT DENEN DIE TEAMS WÄHREND DES ANGRIFFS KONFRONTIERT WAREN



Die interne Kommunikation und Koordination waren aufgrund des Ausfalls kritischer Systeme (z. B. E-Mail, Kollaborationsanwendungen, Ticketsystem) nicht möglich.

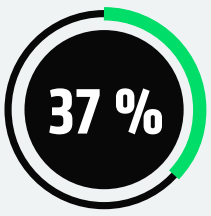


Die Führungsebene übte Druck aus, die Systeme wiederherzustellen, bevor der Angriff behoben war.



Sicherheitsmaßnahmen wurden umgangen und Backups angegriffen.

Wir konnten uns zwar erholen, wurden aber später erneut infiziert, da die Bedrohungen nicht vollständig beseitigt wurden.



Es fehlte der Zugriff auf saubere, validierte Wiederherstellungspunkte.

Die Teams standen während des Angriffs vor einer Reihe betrieblicher und technischer Herausforderungen. Etwa die Hälfte hatte Schwierigkeiten bei der Kommunikation, während die Systeme ausgefallen waren, oder stand unter dem Druck, die Systeme wiederherzustellen, bevor die Fehlerbehebung abgeschlossen war. Die Teams berichteten zudem über Umgehung von Sicherheitstools, angegriffene Backups, Neuinfektionen nach der Wiederherstellung oder fehlenden Zugriff auf saubere Wiederherstellungspunkte. Diese Herausforderungen verdeutlichen Lücken in der Bereitschaft, die die Reaktion erschweren und die Unterbrechung verlängern können.

WO INVESTITIONEN IN RESILIENZ WEITERHIN UNZUREICHEND SIND

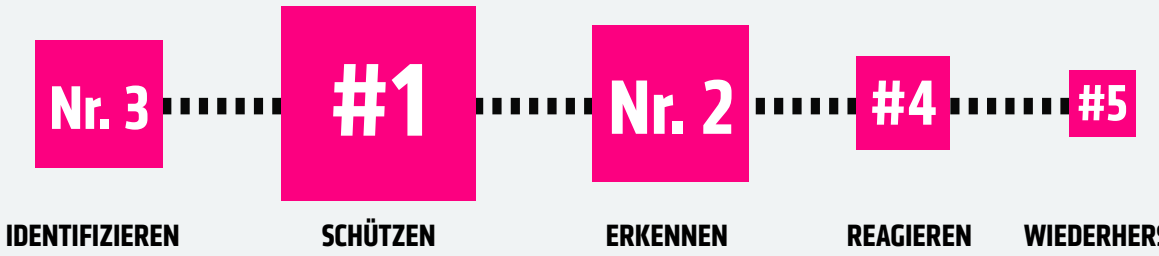
Selbst gut vorbereitete Unternehmen haben Schwierigkeiten, ihre Resilienz nach einem Angriff aufrechtzuerhalten. Angesichts des zunehmenden betrieblichen Drucks zeigen Koordinationslücken, unvollständige Abhilfemaßnahmen und das Risiko von erneuten Infektionen, wie fragil die Wiederherstellung ohne einheitliche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

Diese Muster spiegeln wider, wie mittelständische Unternehmen 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 CYBERSECURITY FRAMEWORK.

Die Größe der Kästchen zeigt den Anteil der Investitionen in Cyber-Resilienz vom höchsten zum niedrigsten an



KI UND AUTOMATISIERUNG ERWEISEN SICH ALS MULTIPLIKATOREN DER RESILIENZ

Die Ergebnisse zeigen auch, dass mittelständische Unternehmen 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 mittelständischen Unternehmen 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. 56 % geht 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 37 % 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

Mittelständische Unternehmen 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:

- Erfahren Sie mehr über die Lösungen von Cohesity zur Cyber-Resilienz für mittelständische Unternehmen
- Bewerten Sie den Reifegrad Ihrer Cyber-Resilienz mithilfe dieser Resilienz-Scorecard
- Optimieren Sie Ihre Cyber-Resilienz mit einem Fünf-Punkte-Aktionsplan

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

2000049-001-DE 7-2026