COHESITY

BERICHT ZUR CYBER-RESILIENZ

Risikobereit oder risikogefährdet:
The digitale Kluft der Cyber-Resilienz im Finanzdienstleistungssektor

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 waren 390 Teilnehmer aus Finanzdienstleistungsunternehmen. Ihre Antworten zeigen eine wachsende Kluft in der Resilienz zwischen risikobereiten Finanzdienstleistungsunternehmen, 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 Finanzdienstleistungsunternehmen 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 Finanzdienstleistungsunternehmen 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.

FÜR FINANZDIENSTLEISTUNGSUNTERNEHMEN SIND DIESE SCHWERWIEGENDEN ANGRIFFE LÄNGST KEINE EINZELFÄLLE MEHR.

77 %

der Befragten haben mindestens einen erheblichen Cyberangriff erlebt

57 %

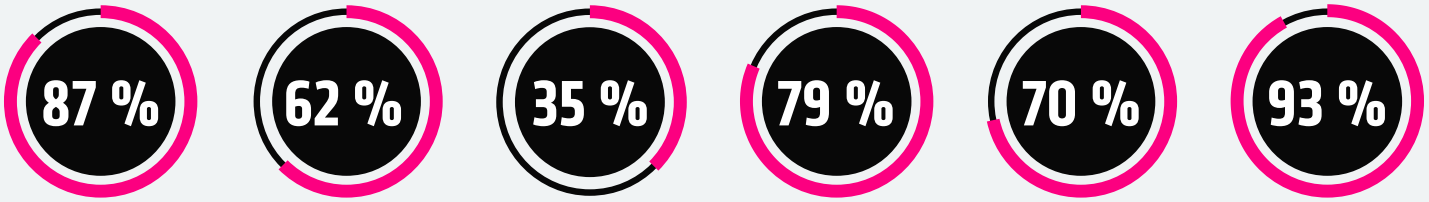
erlebten einen solchen Angriff in den letzten 12 Monaten

27 %

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 FINANZDIENSTLEISTUNGSUNTERNEHMEN ALLGEGENWÄRTIG:



87 %	62 %	35 %	79 %	70 %	93 %
meldeten Umsatzeinbußen	der börsennotierten Unternehmen 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 (51 %) sowie Klagen oder Sammelklagen (41 %)

[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

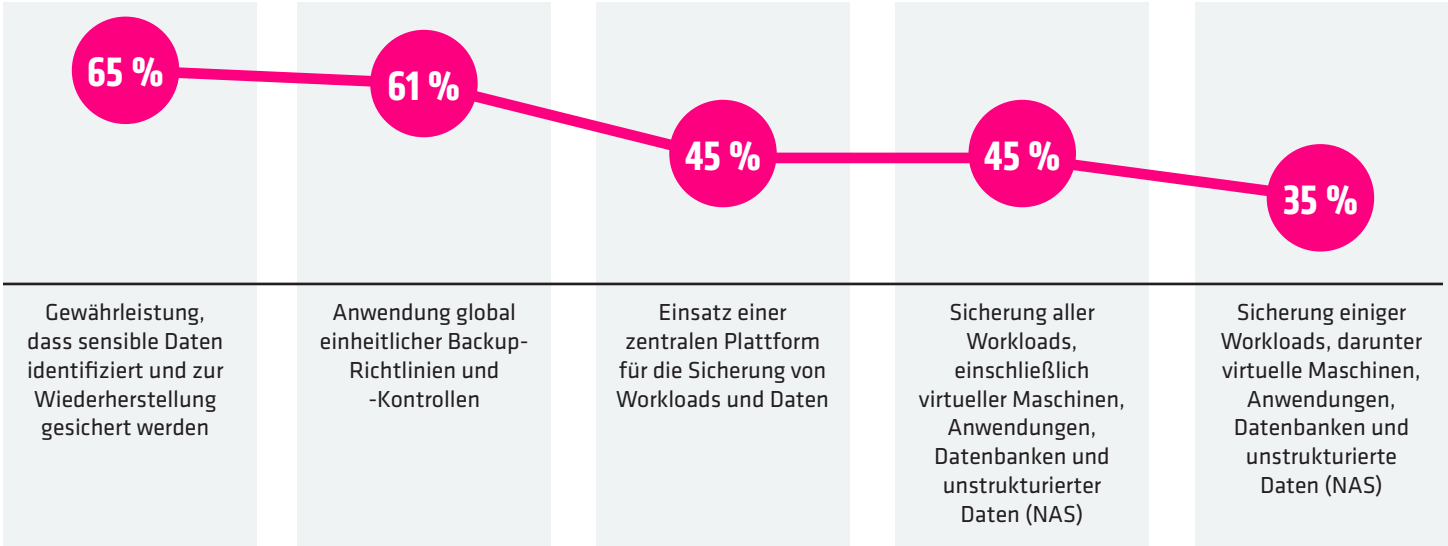
Angesichts des Ausmaßes der finanziellen und betrieblichen Auswirkungen, die unsere Nachforschungen aufgedeckt haben, könnte man erwarten, dass die Resilienz von Unternehmen weit verbreitet ist. Dennoch gab fast die Hälfte der Befragten (46 %) an, vollstes Vertrauen in ihre Cyber-Resilienzstrategie zu 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?



Fast zwei Drittel der Finanzdienstleistungsunternehmen stellen sicher, dass sensible Daten identifiziert und zur Wiederherstellung gesichert werden, während ein etwas geringerer Anteil weltweit einheitliche Sicherungsrichtlinien anwendet. Weniger als die Hälfte sichert alle Workloads oder verlässt sich auf eine zentrale Plattform. Etwa 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 einzigen intelligenten Plattform vereinigt werden, die nach Zero-Trust-Prinzipien gesichert ist.

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

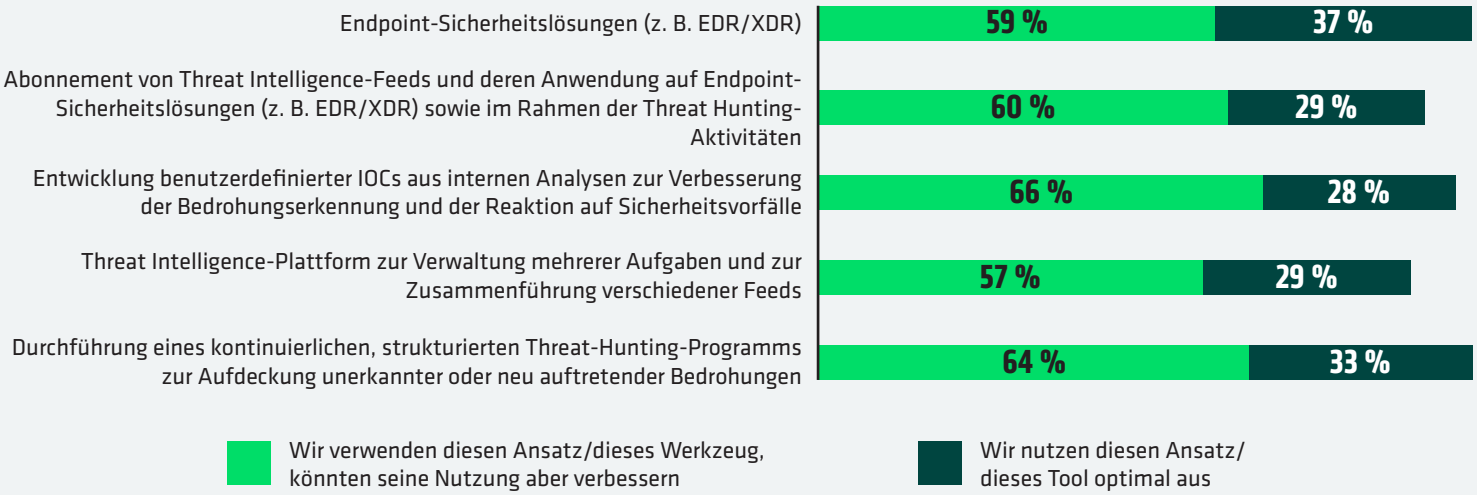
Was unternimmt Ihr Unternehmen, um die jederzeitige Wiederherstellbarkeit seiner Daten zu gewährleisten?

64 %	Zusätzliche Autorisierung für risikoreiche administrative Aufgaben im Zusammenhang mit Datensicherung und -wiederherstellungs lösungen
61 %	Multifaktor-Authentifizierung für unsere Backup-Lösung
48 %	Befolgung der „3-2-1-Backup-Regel“ (drei Datenkopien auf zwei verschiedenen Speichermedien, wobei eine Kopie extern aufbewahrt wird)
45 %	Schutz kritischer Daten durch Unveränderlichkeit
41 %	Zugriffsrechte nach dem Prinzip der minimalen Berechtigungen für gesicherte Workloads

Viele Finanzdienstleistungsunternehmen haben die Zugriffskontrollen für Backup-Umgebungen verschärft: Fast zwei Drittel verlangen eine zusätzliche Administratorberechtigung für risikoreiche Aufgaben, und etwas mehr als die Hälfte setzt eine Multifaktor-Authentifizierung ein. Fast die Hälfte hält sich an die 3-2-1-Backup-Regel, knapp die Hälfte schützt kritische Daten durch Unveränderlichkeit, während nur wenige den Zugriff auf das Mindestmaß an Berechtigungen beschränken. 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 Finanzdienstleistungsunternehmen setzen Endpunktsicherheit, Threat Intelligence Feeds und strukturierte Programme zur Bedrohungssuche ein, doch nur eine Minderheit nutzt das volle Potenzial dieser Tools. Die Anwendung 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, der die Transparenz, Erkennung und Reaktion verbessert.

UNTERNEHMEN SIND ANFÄLLIG FÜR ERNEUTE INFEKTIONEN

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

64 % Jährlich werden End-to-End-Simulationen durchgeführt, an denen ein funktionsübergreifendes Team aus technischen, juristischen, strategischen, leitenden und kommunikativen Stakeholdern teilnimmt

61 % Sicherheitslücken identifizieren und beheben, bevor Systeme wieder in Betrieb genommen werden

60 % Kritische Systeme und Informationen werden online und sicher gespeichert, um die Reaktion auf Vorfälle und die Wiederherstellung zu unterstützen

51 % Für die Untersuchung, Behebung und sichere Wiederherstellung von Vorfällen wird eine isolierte Umgebung genutzt

39 % Alle Backup-Daten sind unveränderlich

Finanzdienstleistungsunternehmen verbessern ihre Strategien zur Anwendungsresilienz, doch es bestehen weiterhin Lücken. Etwas mehr als die Hälfte identifiziert Sicherheitskontrolllücken, bevor Systeme wiederhergestellt werden, während fast zwei Drittel Wiederherstellungsübungen durchführen. Etwa sechs von zehn Unternehmen unterhalten Online-Speicher mit verschlüsselten Datenarchiven, und etwas mehr als die Hälfte nutzt isolierte Umgebungen für sichere Untersuchungen und Datenwiederherstellung. Weniger als die Hälfte gewährleistet die Unveränderlichkeit aller Backup-Daten. 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?

67 %

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

62 %

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

59 %

Definition und Analyse der Wesentlichkeit eines Cyberangriffs vor dessen Eintreten

56 %

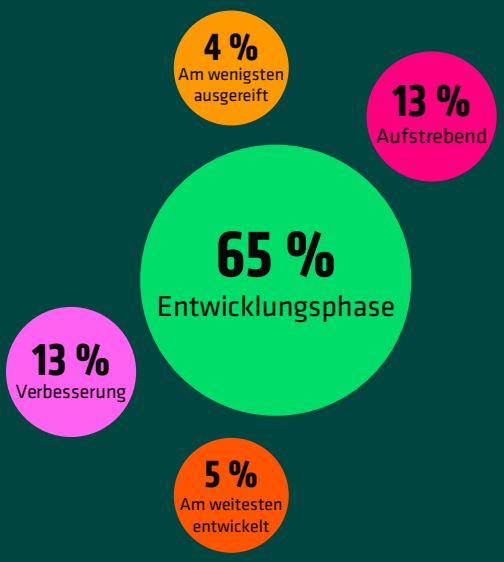
Identifizierung und Priorisierung von Backup-Systemen

Finanzdienstleistungsunternehmen nutzen Datenermittlung und -klassifizierung strategischer in den Bereichen Compliance, Reaktion und Wiederherstellung. Etwa zwei Drittel beschäftigen sich mit Datenschutz- und Sicherheitsverletzungen und nutzen Klassifizierungen, um die Compliance während eines Angriffs sicherzustellen, während weniger Unternehmen die Wesentlichkeit vor einem Vorfall definieren oder Backups auf der Grundlage des Risikos priorisieren. 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, 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 im praktischen Aufbau – oder den Schwierigkeiten – Finanzdienstleistungsunternehmen beim Aufbau von Resilienz. Während sich die Mehrheit noch in der Entwicklungsphase befindet, verfügen lediglich 5 % über die ausgereiftesten, integrierten Fähigkeiten, die risikobereite Unternehmen kennzeichnen.

DIE REIFEKURVE DER CYBER-RESILIENZ



Am wenigsten ausgereift (4 %): 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 (13 %): 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.

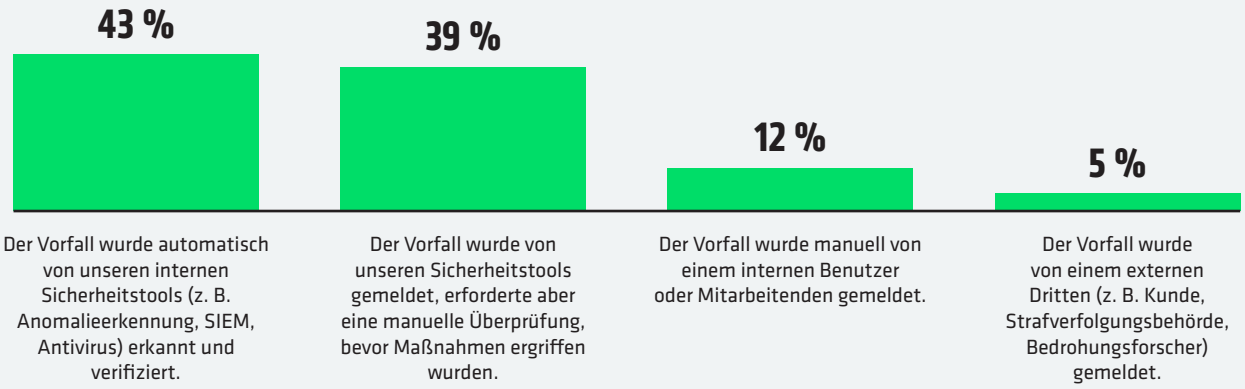
Entwicklungsphase (65 %): Kernpraktiken wie Datensicherung, administrative Kontrollen und Threat Intelligence sind zwar verbreiteter, aber noch nicht einheitlich. Wiederherstellungsumgebungen, Compliance-Prüfungen und die Behebung von Sicherheitslücken werden nur sporadisch angewendet, wodurch die Maßnahmen zur Erhöhung der Resilienz nur teilweise wirksam sind.

Verbesserung (13 %): 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 (5 %): 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.

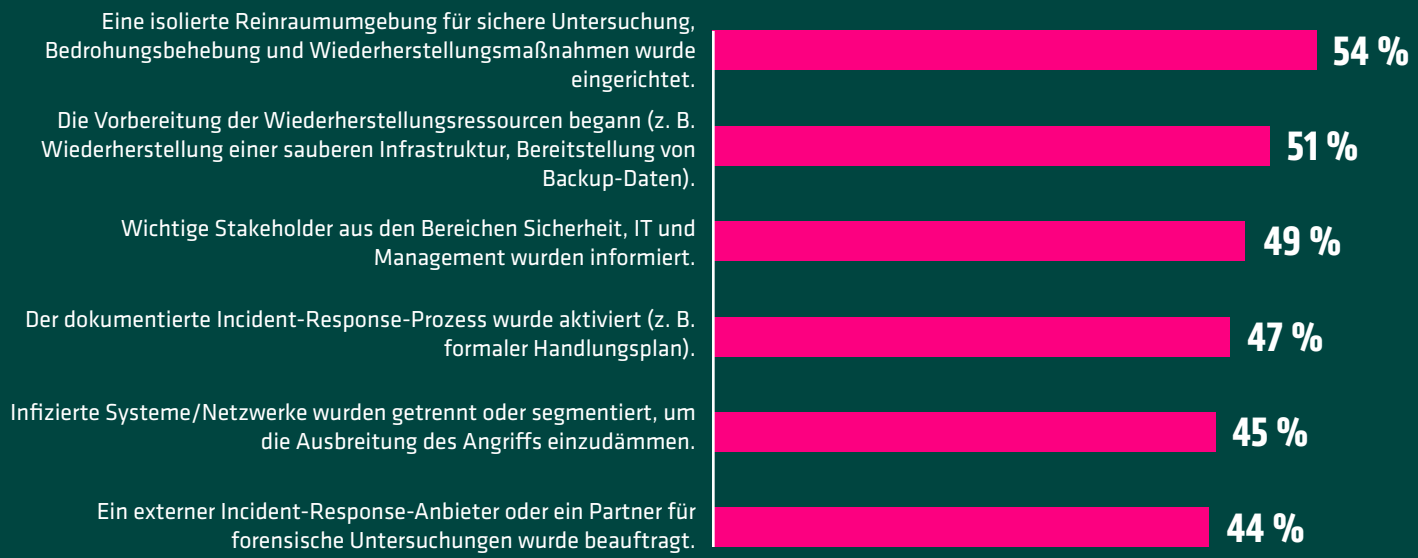
RESILIENZ UNTER BESCHUSS

WIE TEAMS ANGRIFFE IDENTIFIZIERTEN



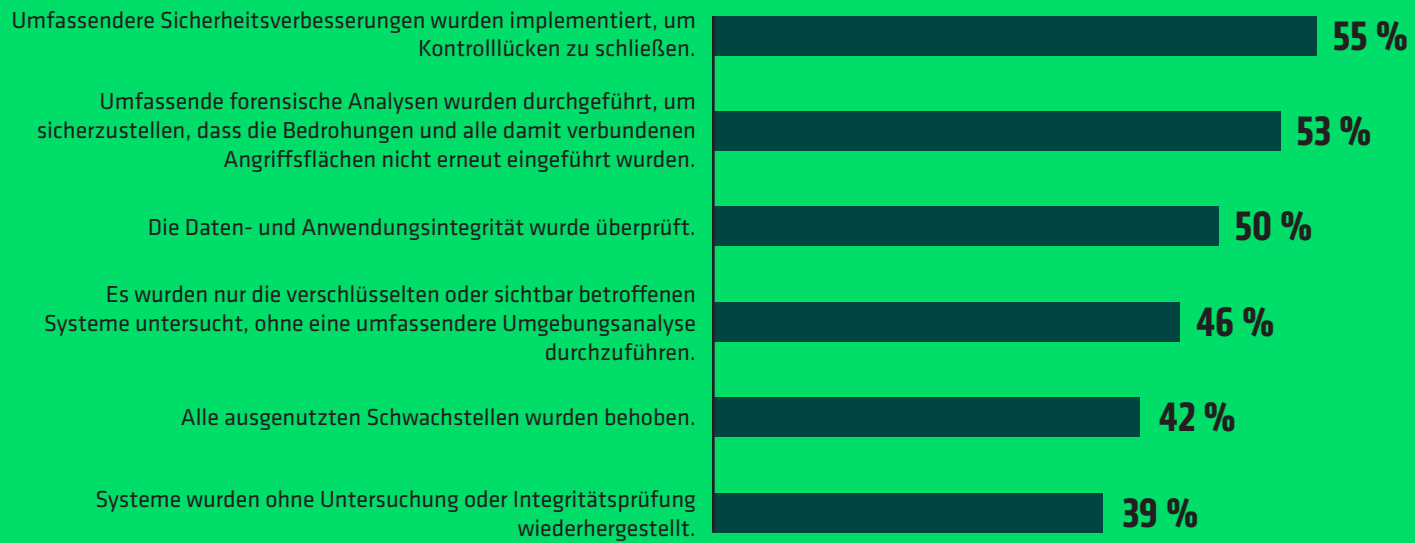
Im Falle eines Cyberangriffs erkennen die meisten Finanzdienstleistungsunternehmen die Vorfälle intern. Fast die Hälfte gab an, dass Angriffe von ihren eigenen Sicherheitstools automatisch erkannt und verifiziert wurden, während etwas weniger angaben, dass Angriffe zwar von den Tools gemeldet wurden, jedoch eine manuelle Überprüfung erforderlich war, bevor Maßnahmen ergriffen wurden. Nur ein kleiner Teil wurde von Dritten identifiziert, was darauf hindeutet, dass die Erkennung größtenteils intern erfolgt, jedoch weiterhin von einer menschlichen Bestätigung abhängt.

MAßNAHMEN DER EINSATZTEAMS NACH BESTÄTIGUNG DES ANGRIFFS



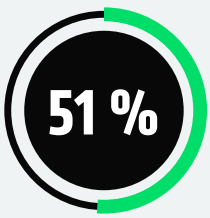
Nach der Bestätigung eines Angriffs ergriffen die Finanzdienstleistungsunternehmen eine Reihe von Maßnahmen, um die Wiederherstellung zu unterstützen. Etwas mehr als die Hälfte begann mit der Wiederherstellung einer reinen Infrastruktur oder der Bereitstellung von Sicherungsdaten, während etwas mehr Unternehmen isolierte Reinraumumgebungen für eine sichere Untersuchung und Wiederherstellung einrichteten. Ein kleinerer Teil informierte wichtige Stakeholder, isolierte infizierte Systeme, aktivierte formelle Strategiehandbücher oder beauftragte 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

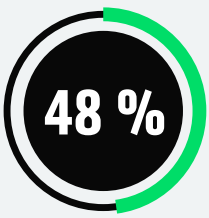


Bevor die Systeme wieder online gebracht wurden, ergriffen Finanzdienstleistungsunternehmen eine Reihe von forensischen und Abhilfemaßnahmen. Mehr als die Hälfte führte umfassendere Sicherheitsverbesserungen durch oder führte vollständige forensische Untersuchungen durch. Die Hälfte überprüfte zudem die Daten- und Anwendungsintegrität, während nur wenige über die sichtbar betroffenen Systeme hinaus untersuchten oder gepatchte Sicherheitslücken, die ausgenutzt worden waren, überprüften. Über ein Drittel der Systeme wurde ohne vollständige Untersuchung oder Integritätsprüfung wiederhergestellt, wodurch Möglichkeiten für Neuinfektionen und Restrisiken verbleiben.

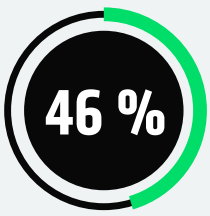
HERAUSFORDERUNGEN, MIT DENEN DIE TEAMS WÄHREND DES ANGRIFFS KONFRONTIERT WAREN



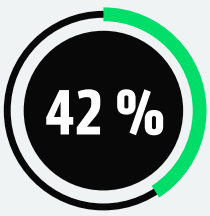
Die interne Kommunikation und Koordination waren aufgrund des Ausfalls kritischer Systeme (z. B. E-Mail, Kollaborationsanwendungen, Ticketsystem) nicht möglich.



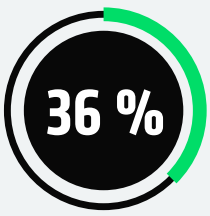
Die Führungsebene übte Druck aus, die Systeme wiederherzustellen, bevor der Angriff behoben war.



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 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, Neuinfektionen und das Fehlen sauberer Wiederherstellungspunkte erschwerten die Situation zusätzlich und machten deutlich, dass stärkere Maßnahmen zur Resilienz erforderlich sind.

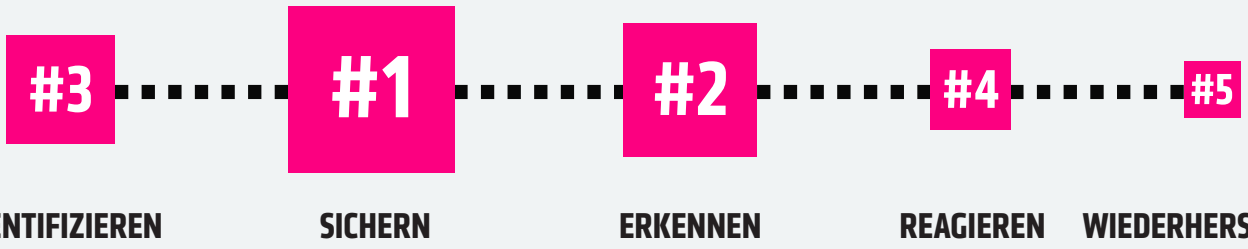
WO INVESTITIONEN IN RESILIENZ WEITERHIN UNZUREICHEND SIND

Selbst gut vorbereitete Finanzdienstleistungsunternehmen 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 Finanzdienstleistungsunternehmen 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 der Box zeigt das Verhältnis der Investitionen in Cyberresilienz von der größten bis zur kleinsten



KI UND AUTOMATISIERUNG ERWEISEN SICH ALS MULTIPLIKATOREN DER RESILIENZ

Die Ergebnisse zeigen auch, dass Finanzdienstleistungsunternehmen 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 Finanzdienstleistungsunternehmen 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. 49 % 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 39 % 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

Finanzdienstleistungsunternehmen 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 Lösungen von Cohesity zur Stärkung der Cyber-Resilienz für Finanzdienstleistungen.

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

2000085-001-DE 5-2026