COHESITY

RESILIENCE EVERYWHERE

CYBER-RESILIENZ IN DER RANSOMWARE-ÄRA

Wie Cohesity Organisationen dabei unterstützt, Cyberangriffen zu widerstehen und eine Wiederherstellung vorzunehmen und dabei die Anforderungen des NIST Cybersecurity Framework 2.0 erfüllt.

INHALT

VON DER DATENRESILIENZ ZUR CYBER-RESILIENZ

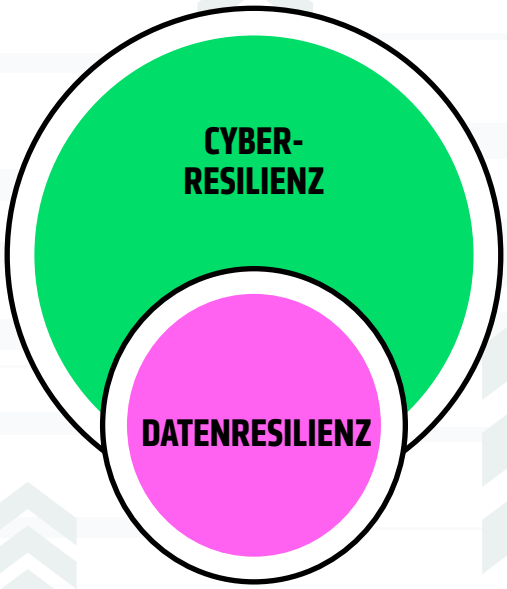
Naturkatastrophen stellen eine enorme Bedrohung für den Geschäftsbetrieb dar. Blitzeinschläge, Hurrikans, Tornados oder Überschwemmungen können schwere Schäden verursachen und Unternehmen zum Stillstand bringen. In solchen Situationen sorgen Strategien für die Datenresilienz dafür, dass die Daten auch bei Hardwarefehlern, versehentlichem Löschen oder Naturkatastrophen intakt und zugänglich bleiben.

Diese Vorfälle zielen jedoch nicht aktiv auf Ihr Geschäft ab und stellen keine fortlaufenden, gezielten Angriffe dar.

Ganz anders hingegen bei einer Cyberbedrohung. Kriminelle arbeiten ständig daran, Sie mit Ihren Daten zu erpressen und Ihr Unternehmen zu zerstören. Die Angriffsvektoren sind oft vielschichtig und schwer zu erkennen.
Das Risiko, Schwachstellen, kompromittierte Konten und andere Angriffsartefakte wieder in Ihre Umgebung einzuschleusen, ist allgegenwärtig.
Im Gegensatz zu herkömmlichen Szenarien der Geschäftskontinuität und Notfallwiederherstellung, bei denen die Ursache in der Regel offensichtlich ist, erfordert die Reaktion auf Cyberbedrohungen eine Untersuchung, um diese Ursachen aufzudecken und Abhilfemaßnahmen zu ergreifen, damit sich solche Vorfälle nicht wiederholen.

Des Weiteren können bei einem Ransomware-Angriff die Sicherheitsinfrastruktur und wichtige Nachweise von dem Vorfall betroffen sein. Dies kann die Bereitstellung von Produkten und Dienstleistungen beeinträchtigen.

Im Vergleich zu den Prozessen, die als Reaktion auf einen Standardausfall aufgrund von Naturkatastrophen oder technischen Störungen zum Einsatz kommen, benötigen IT- und Sicherheitsverantwortliche bei der Entwicklung eines cyberresistenten Unternehmens robustere, dynamischere und kooperativere Prozesse. Cyber-Resilienz baut auf den Praktiken der Datenresilienz auf und umfasst Elemente wie Cyber-Sicherheitsbereitschaft, Reaktionspläne für Vorfälle, Mitarbeiterschulung und Threat Intelligence.



Die heutigen Cyberbedrohungen erfordern moderne Lösungen. Diese müssen einen globalen Einblick in gesicherte Datenbestände ermöglichen und die Zusammenarbeit zwischen IT- und Sicherheitsexperten optimieren.

Die modernen, KI-gestützten Datensicherheitslösungen von Cohesity ermöglichen es Organisationen, ihre Cyber-Bereitschaft zu stärken, die Reaktion auf Vorfälle zu beschleunigen und eine schnelle, sichere Wiederherstellung zu gewährleisten.

MIT COHESITY KÖNNEN SIE:

- all Ihre Daten schützen
- für die Wiederherstellbarkeit all Ihrer Daten sorgen
- Einblick in Schwachstellen und Bedrohungen in Ihren Backup-Daten gewinnen
- schnell und effektiv auf Angriffe reagieren und nach Bedrohungen suchen, die bei herkömmlichen Abwehrmaßnahmen leicht unentdeckt bleiben
- Systeme und Daten schnell und sicher wiederherstellen

Das Ergebnis ist ein widerstandsfähigeres Unternehmen, das besser in der Lage ist, sich auf Cyberangriffe vorzubereiten, ihnen standzuhalten, darauf zu reagieren und sich davon zu erholen.

EIN PARADOX VON VERTRAUEN UND FÄHIGKEIT

78 % der Organisationen haben Vertrauen in ihre interne Strategie zur Cyber-Resilienz[1]. Dies ist im Allgemeinen ein gutes Zeichen, solange dieses Vertrauen durch konkrete Fähigkeiten untermauert wird. Doch zeigen die Daten eine Diskrepanz zwischen strategischer Absicht und tatsächlichen Fähigkeiten.

98 % haben das Ziel, Daten wiederherzustellen und Geschäftsprozesse nach einem Angriff innerhalb eines Tages wieder aufzunehmen[2].

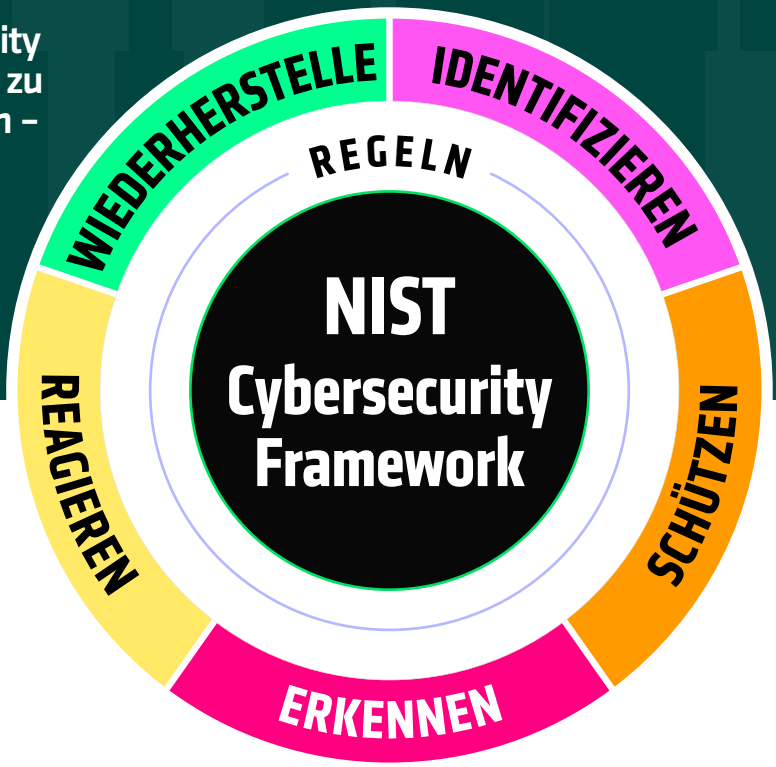
Aber nur **2 %** konnten dieses erreichen[3].

Glücklicherweise bietet Cohesity einen bewährten Leitfaden mit Prozessen und Tools, die Kunden weltweit dabei helfen, den Betrieb schnell wieder aufzunehmen und die Auswirkungen eines Angriffs zu minimieren.

[1-3] Cohesity Global Cyber Resilience Report 2024

6 SCHLÜSSELELEMENTE ZUR SCHAFFUNG EINES CYBERRESILIENTEN UNTERNEHMENS

Unsere Datensicherheitslösungen bei Cohesity helfen Organisationen dabei, Risiken besser zu verstehen, zu verwalten und zu minimieren – und die Cyber-Resilienz im Einklang mit den Kernfunktionen des NIST Cybersecurity Framework zu stärken: Regeln, Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.



REGELN

- Klassifizierung von Backup-Daten, um die gesetzlichen Anforderungen zu verstehen
- Unterstützung der Einhaltung von Rahmenwerken für Cyberversicherungen und anderer vertraglicher Verpflichtungen im Zusammenhang mit Daten Dritter

IDENTIFIZIEREN

- Scannen empfindlicher Systeme auf Schwachstellen, ohne den Betrieb zu beeinträchtigen
- Identifizieren kritischer Systeme, die nicht gesichert sind
- Verbessern Ihrer Reaktionsbereitschaft auf künftige Vorfälle sowie Ausbau Ihrer Aktivitäten im Bereich Geschäftskontinuität und Notfallwiederherstellung
- Ermitteln von Verbesserungsmöglichkeiten in den Programmen zur Cyber-Resilienz von Organisationen

SCHÜTZEN

- Skalierbarer Schutz für Unternehmensdaten
- Schutz Ihrer Backups vor Angriffen
- Testen von Datensicherung und -wiederherstellung

ERKENNEN

- Erkennen von Ransomware-Verschlüsselung, Wiper-Angriffen und böswilliger Insider
- Proaktive Suche nach Anzeichen für eine Kompromittierung, damit Sie gegen Ausweichtechniken gewappnet sind
- Senden von Sicherheitserkennungen an SOC-Tools zur Korrelation
- Erfassen von mehr forensischen Artefakten und Auslösen inkrementeller Snapshots basierend auf EDR/XDR-Signalen
- Identifizierung von Malware in NAS-Servern

REAGIEREN

- Einbezug des CERT (Cyber Event Response Team) von Cohesity, um Ihre Reaktion zu beschleunigen und eine sichere Wiederherstellung zu gewährleisten
- Wiederherstellung der Reaktionswerkzeuge und des Active Directory auf einen vertrauenswürdigen Zustand und Gewährleistung eines schnellen Zugriffs
- Umgehende Einrichtung eines Reinraums für die Reaktion und Wiederherstellung
- Passive Suche nach Artefakten, um weitere betroffene Systeme zu identifizieren
- Kriminaltechnische Untersuchung früherer Dateisysteme
- Verschaffen eines Überblicks über bekannte Schwachstellen, die bei dem Angriff ausgenutzt wurden
- Unterstützung bei der Einhaltung gesetzlicher und regulatorischer Verpflichtungen zur Benachrichtigung von Aufsichtsbehörden, Partnern und betroffenen Datensubjekten

WIEDERHERSTELLEN

- Sicherstellung, dass die Wiederherstellung von Systemen und Daten die Minderung von Bedrohungen ermöglicht

1.

Regeln von Backup-Daten, um gesetzliche Anforderungen zu verstehen und Risiken zu minimieren

Die heutige Datenlandschaft ist unübersichtlich – wie eine überfüllte Garage –, was es zunehmend erschwert, sensible Daten aufzufinden und sicherzustellen, dass sie angemessen geschützt sind. Diese mangelnde Transparenz erhöht das Risiko der Offenlegung von Daten und Verstößen gegen gesetzliche Vorschriften.

Um dieses Risiko zu bewältigen, müssen Organisationen nicht nur gesetzliche und behördliche Anforderungen (wie HIPAA, CCPA und DSGVO) erfüllen, sondern auch durch eine wirksame Cybersicherheits-Governance strenge interne Kontrollen nachweisen. Diese Kontrollen dienen zunehmend nicht mehr nur der Einhaltung von Vorschriften – sie werden vielmehr zu einer unverzichtbaren Voraussetzung für den Abschluss einer Cybersicherheitsversicherung.

Angesichts der zunehmenden Häufigkeit und Schwere von Cyberangriffen hat sich die Cyberversicherung zu einer entscheidenden Strategie für den Risikotransfer entwickelt. Sie hilft dabei, finanzielle Verluste wie Kosten für die Datenwiederherstellung, Anwaltskosten und sonstige Folgen eines Vorfalls zu decken. Versicherer stellen jedoch höhere Anforderungen an ihre Kunden und verlangen vor dem Abschluss oder der Verlängerung von Verträgen den Nachweis solider Datenschutz- und Sicherheitsvorkehrungen.

Um diesen Anforderungen einen Schritt voraus zu sein, unterstützen wir Organisationen dabei:

Vertrauliche Daten zu entdecken und zu klassifizieren. Unsere unbegrenzten, unveränderlichen Backup-Snapshots zu nutzen, um sensible Daten in Ihrer gesamten Umgebung zu identifizieren und zu kategorisieren. Unsere integrierte Engine zur Datenklassifizierung nutzt Hunderte von Klassifikatoren und KI-gestützte Algorithmen, um regulierte und risikobehaftete Informationen zu identifizieren und zu kennzeichnen, und unterstützt Sie so bei der Bestandsaufnahme Ihrer digitalen Ressourcen und der Anwendung geeigneter Sicherheitsrichtlinien.

Die Einhaltung der Anforderungen im Zusammenhang mit Cyberversicherungen und anderer vertraglicher Verpflichtungen in Bezug auf Daten Dritter zu unterstützen. Unsere Plattform trägt dazu bei, den steigenden Anforderungen von Versicherern und Aufsichtsbehörden gerecht zu werden, indem sie bewährte Kontrollmechanismen implementiert:

- Isolierte Backup-Umgebungen, getrennt vom Produktionsnetzwerk
- Dedizierte Cloud-Backup-Dienste
- Datenverschlüsselung während der Übertragung und im Ruhezustand
- Unveränderliche Backup-Snapshots
- Rollenbasierte Zugriffe mit separaten Anmeldeinformationen
- MFA-Durchsetzung für internen und externen Zugriff
- Die Integrität der Backups wird vor der Wiederherstellung getestet, um sicherzustellen, dass sie frei von Malware sind

2.

Identifizieren von Risiken für die Cyber-Resilienz

Um Cybersicherheitsrisiken effektiv zu bewältigen, ist ein klares Verständnis der Schwachstellen in Ihrer gesamten IT-Umgebung erforderlich – einschließlich der Backup-Systeme. Dies beinhaltet auch, den Schutz der Datenbestände entsprechend ihrer Einstufung zu priorisieren und die Sicherheit durch Sicherheitstests, Übungen sowie die aus früheren Maßnahmen zur Reaktion auf Vorfälle und zur Wiederherstellung gewonnenen Erkenntnisse kontinuierlich zu verbessern.

CyberScan
Powered by tenable

Scannen Sie empfindliche Systeme auf Schwachstellen, ohne den Betrieb zu beeinträchtigen.

Nutzen Sie Cohesity CyberScan, unterstützt von Tenable, um Schwachstellen-Scans an Backup-Snapshots durchzuführen und Auswirkungen auf Produktionssysteme zu vermeiden.

Identifizieren Sie kritische Systeme, die nicht gesichert sind.

Die Integration von Cohesity mit Ihrem bevorzugten Anbieter für die Verwaltung der Datensicherheitslage (Data Security Posture Management, DSPM) ist eine wirksame Methode, um verborgene Risiken für die Cyber-Resilienz aufzudecken. DSPM-Lösungen bieten Transparenz über bekannte und vergessene Datenspeicher auf verschiedenen Cloud-Plattformen, klassifizieren die Daten, um sensible Informationen zu identifizieren, und ermitteln das Risiko einer Offenlegung.

Auch wenn ein Großteil Ihrer sensiblen Daten möglicherweise bereits durch die Cohesity Data Cloud und bestehende Backup-Richtlinien geschützt ist, bestehen oft noch erhebliche Lücken. Hier kommt die Integration des DSPM ins Spiel.

Durch die Kombination der Erkenntnisse aus dem DSPM mit Cohesity können Sie kritische Systeme und Daten identifizieren, für die noch keine Sicherungskopien erstellt wurden, und die Sicherungsrichtlinien schnell auf diese ausweiten – wodurch die Sicherheit erhöht und Risiken verringert werden.

Weitere wichtige betriebliche Vorteile sind:

- Optimierte Häufigkeit von Backups und Aufbewahrungsfristen basierend auf der Kritikalität der Daten in den von Cohesity gesicherten Datenspeichern
- Priorisierte Wiederherstellung von Daten basierend auf der geschäftlichen Kritikalität der Daten
- Optimierte Reaktion auf Vorfälle durch eine „Just-in-Time"-Analyse der betroffenen Daten (näher erläutert in der Funktion „Reaktion")

Gemeinsam tragen das DSPM und die KI-gestützte Datensicherheitsplattform von Cohesity dazu bei, Ihre Sicherheitslage in Multicloud-Umgebungen zu verbessern.

2.

Identifizieren von Risiken für die Cyber-Resilienz

Ermitteln Sie Verbesserungsmöglichkeiten in Hinblick auf das künftige Ergreifen von Maßnahmen zur Störungsbehebung sowie im Bereich BC/DR-Aktivitäten.

Bewerten Sie die aktuellen Reaktions- und Wiederherstellungsfähigkeiten Ihres Unternehmens und legen Sie mit dem **„Destructive Cyberattack Resilience Maturity Model“ (DCARMM) einen Weg hin zu branchenüblichen Best Practices fest.**

Dieses von Cohesity entwickelte Modell orientiert sich an führenden Rahmenwerken wie dem SANS 6-Step Incident Response Process, RE&CT, MITRE D3FEND und NIST SP 800-61 und ermöglicht Unternehmen Folgendes:

- Bewerten der Abwehrbereitschaft gegen zerstörerische Cyberangriffe
- Benchmark der Resilienz im Vergleich zu Branchenkollegen oder regionalen Standards
- Identifizieren der Schwachstellen und Erstellen eines Aktionsplans für kontinuierliche Verbesserungen

Ihr Unternehmen kann es als strategisches Instrument nutzen, um Ihre Cyber-Resilienz zu stärken und Investitionen in Mitarbeiter, Prozesse und Technologie gezielt zu steuern.

Ermitteln Sie Bereiche, in denen Ihr Programm zur Cyber-Resilienz verbessert werden muss, indem Sie in Bewertungen durch externe Anbieter investieren.

Die Beratungsdienstleistungen des Cohesity CERT (Cyber Event Response Team) im Bereich Cyber-Resilienz umfassen proaktive, von Experten geleitete Maßnahmen, die darauf abzielen, Ihre Cyber-Resilienz vor dem nächsten Vorfall zu stärken. Von umfassenden Resilienzbewertungen auf Basis des DCARMM bis hin zu maßgeschneiderten Aktionsplänen unterstützt Sie das CERT dabei, Schwachstellen zu identifizieren, Risiken zu minimieren und dauerhafte Schutzmaßnahmen aufzubauen.

3.

Skalierbarer Schutz für Unternehmen

Da Datenbestände – bedingt durch ihren Umfang und ihre Vielfalt – immer komplexer werden, steigt auch das Risiko schwerwiegender geschäftlicher Auswirkungen durch Cyberangriffe oder Datenausfälle.

Durch die Nutzung einer einzigen, sicheren Plattform zur Sicherung all Ihrer Datenquellen in lokalen, Cloud- und SaaS-Umgebungen können Sie den Datenschutz skalieren und gleichzeitig die Auswirkungen potenzieller Angriffe erheblich minimieren.

Verringern Sie die Angriffsfläche

Viele Umgebungen sind auf fragmentierten Einzelprodukten aufgebaut. Im Gegensatz dazu konsolidiert Cohesity alle Komponenten zur Datensicherung und -wiederherstellung auf einer einzigen, globalen Plattform. Es umfasst eine globale Deduplizierung mit variabler Länge über alle Datenquellen hinweg sowie eine Kompression zur weiteren Reduzierung der verfügbaren Angriffsflächen.

Skalieren Sie den Datenschutz über alle Datenbestände hinweg

Da die Cohesity Data Cloud auf einer Hyperscale-Architektur basiert, können IT-Administratoren ihre Cohesity-Cluster unbegrenzt erweitern und eine unbegrenzte Anzahl von Snapshots und Klonen speichern, ohne dass dies Auswirkungen auf die Leistung hat. Die beispiellose Datendeduplizierung sorgt nicht nur dafür, dass Sie mehr Daten zu deutlich geringeren Kosten speichern können, sondern ermöglicht es Ihnen auch, Snapshots zu jedem beliebigen Zeitpunkt zu erstellen, um forensische Untersuchungen zu unterstützen.

3.

Skalierbarer Schutz für Unternehmen

Ihre Backups vor Angriffen schützen

Auf der Grundlage der Zero-Trust-Prinzipien verfolgt Cohesity einen mehrschichtigen Sicherheitsansatz, der das Risiko von Ransomware-Angriffen auf Backups sowie das Risiko einer versehentlichen oder böswilligen Löschung von Daten minimiert.

- **Unveränderliche, schreibgeschützte Zustands-Snapshots**
  Die Cohesity Data Cloud wurde speziell entwickelt, um Cyberangriffe abzuwehren, indem Backup-Snapshots in einem unveränderlichen Zustand gespeichert werden. Snapshots werden nicht für externe Anwendungen eingebunden, und Änderungen oder Löschungen unveränderlicher Backup-Snapshots sind ohne Genehmigung nicht möglich.
- **DataLock-Richtlinien** – Unsere WORM-Fähigkeiten (Write Once Read Many) für Datensicherungen gestatten bestimmten Rollen, unveränderliche DataLock-Richtlinien für ausgewählte Aufgaben festzulegen.
- **Multi-Faktor-Authentifizierung (MFA)**
  Jede Person, die auf ein Cohesity-Backup zugreift, muss sich anhand von zwei Verfahren authentifizieren. Cohesity unterstützt mehrere Authentifizierungsanbieter. Ihr Unternehmen kann also eine starke Authentifizierung beibehalten, selbst wenn der Hauptserver von einem Cybervorfall betroffen ist.
- **Datenverschlüsselung** – Cohesity bietet software-basierte FIPS-validierte AES-256-Standardverschlüsselung sowohl für Daten, die übertragen werden, als auch für solche, die sich im Ruhezustand befinden.
- **Rollenbasierte Zugriffskontrolle**
  Cohesity reduziert das Risiko eines unbefugten Zugriffs, da IT-Mitarbeiter den Datenzugriff auf das Mindestmaß beschränken können, das für die Ausführung einer bestimmten Aufgabe erforderlich ist.
- **Aufgabentrennung** – Mit Cohesity Quorum muss jede Root-Level- oder kritische Systemänderung von zwei oder mehr Personen autorisiert werden. So sind die Daten vor Insider-Bedrohungen und gestohlenen Anmeldedaten geschützt.

Isolation kritischer Geschäftsdaten

Sie können Daten automatisch zu einem anderen unveränderlichen Cohesity-Cluster On-Premises oder in der Public Cloud replizieren, um sicherzustellen, dass immer eine zusätzliche unveränderliche Kopie verfügbar ist.

Testen von Datensicherung und -wiederherstellung

Mithilfe der **Cyber-Recovery-Orchestrierung** können Sie anpassbare Konzepte erstellen, die Wiederherstellungsabläufe automatisieren und gründliche Tests in Nicht-Produktionsumgebungen ermöglichen. Auf diese Weise kann sich Ihre Organisation besser auf Cybervorfälle vorbereiten und die Wiederherstellung optimieren, um Ausfallzeiten und Datenverluste zu reduzieren.

4.

Erkennen potenzieller Cyberangriffe und Kompromittierungen

Cyberkriminelle schrecken vor nichts zurück, um Schwachstellen in Ihrer Datenumgebung zu finden und auszunutzen. Die frühzeitige Erkennung von ungewöhnlichen Veränderungen in den Backup-Daten oder im Nutzerverhalten ist unerlässlich, um die Auswirkungen eines Angriffs zu minimieren.

Hier spielt die KI eine entscheidende Rolle, indem sie subtile Muster in den Daten identifiziert, die dem Menschen möglicherweise verborgen bleiben. Und indem Sie zu Beginn eines Ransomware-Angriffs – der von EDR-/XDR-Tools erkannt wird – automatisch Sicherungs-Snapshots kritischer Daten erstellen, können Sie Datenverluste minimieren und die Wiederherstellung beschleunigen.

Erkennen Sie Ransomware-Verschlüsselung, Wiper-Angriffe und böswillige Insider.

Überwachen, modellieren und optimieren Sie den Betrieb proaktiv mithilfe von prädiktiven Analysen, um Trends zu erkennen. Unser KI-basierter Algorithmus ermittelt Muster und sucht kontinuierlich nach Anomalien in den Daten, die sich über verschiedene Zeitpunkte hinweg erstrecken.

Die Anomalieerkennung beschleunigt die Behebung, indem eine Benachrichtigung sowohl an Ihre IT-Administratoren als auch an das Cohesity-Supportteam gesendet wird.

Dadurch erhalten Sicherheitsteams Einblicke in Verhaltensweisen, die auf einen Ransomware- oder Wiper-Angriff hindeuten könnten – oder sogar auf die Anwesenheit eines böswilligen Insiders.

Diese Warnmeldungen können auch an Ihr Sicherheitseinsatzzentrum weitergeleitet werden, wobei dessen Tools zur Ereigniskorrelation (z. B. Sicherheitsinformations- und Ereignisverwaltung) zum Einsatz kommen.

Suchen Sie proaktiv nach Bedrohungen in den Backup-Daten.

Ransomware und andere Angriffsformen verwenden betrügerische Taktiken, um Malware zu tarnen. Die Cohesity Bedrohungserkennungs-Lösung unterstützt Sie dabei, schwer aufzuspürende Bedrohungen zu identifizieren – mithilfe einer KI-gestützten Erkennung, die die neuesten Varianten von Ransomware und anderen Cyberangriffen aufspürt.

Unsere umfassende Verhaltensmusterbibliothek wird regelmäßig mit den neuesten Bedrohungen aktualisiert.

Wir unterstützen zudem kommerzielle Threat-Intelligence-Feeds wie CrowdStrike Falcon Adversary Intelligence und nehmen alle IOCs im YARA-Format aus anderen Drittquellen auf.

4.

Erkennen potenzieller Cyberangriffe und Kompromittierungen

Senden Sie Sicherheitserkennungen an SOC-Tools zur Korrelation.

Leiten Sie kritische Sicherheitswarnungen – wie z. B. IOCs, Anomalien bei Änderungen an Backup-Daten und Warnmeldungen zu sensiblen Daten – an Ihre SOC-Tools (z. B. SIEM, SOAR) weiter, um eine schnelle Erkennung und Reaktion auf Bedrohungen zu ermöglichen.

Cohesity lässt sich in führende Plattformen wie CrowdStrike, Splunk und Microsoft integrieren, um Telemetriedaten nahtlos auszutauschen, sodass Ihr SOC die Erkenntnisse von Cohesity mit umfangreichen Protokolldaten aus Ihrer gesamten Infrastruktur zusammenführen, analysieren und in Zusammenhang bringen kann.

Das Ergebnis: eine einheitliche Echtzeit-Übersicht, die die Transparenz erhöht und die Erkennung potenzieller Ransomware oder anderer Cyberbedrohungen beschleunigt.

Erfassen Sie mehr forensische Artefakte und lösen Sie inkrementelle Snapshots basierend auf EDR/XDR-Signalen aus.

Durch die Integration zwischen der Cohesity Data Cloud und Cisco XDR können Sie die Sicherung kritischer Daten automatisieren, sobald Cisco XDR einen Ransomware-Angriff erkennt – wodurch sich die Wiederherstellungsziele (Recovery Point Objectives, RPOs) verkürzen und Betriebsunterbrechungen auf ein Minimum reduziert werden.

Diese Backup-Snapshots bieten den für die Störungsbehebung zuständigen Mitarbeitern zudem einen detaillierteren Überblick über Änderungen am Dateisystem, wodurch forensische Untersuchungen schneller und effektiver durchgeführt werden können.

Identifizierung von Malware in NAS-Servern.

Cohesity überwacht nicht nur die Änderungsraten von Backup-Daten, um potenzielle Ransomware-Angriffe zu erkennen, sondern ermittelt und warnt auch bei Anomalien auf Dateiebene in unstrukturierten Dateien und Objektdaten.

> *Obwohl wir noch keinen größeren Cyberangriff erlebt hatten, war es für uns gut zu wissen, dass die Backups von Cohesity nicht von Angreifern verändert werden können. Außerdem werden die Daten kontinuierlich gescannt, um verdächtige Änderungen von einem Backup zum nächsten zu erkennen.*

Chris Dove

Enterprise Architect, California Department of Finance

5.

Schnelle **Reaktion** auf Cybervorfälle

Sobald ein Cybervorfall erkannt wird, muss die Organisation schnell handeln, um den Vorfall einzudämmen, dessen Ausmaß zu untersuchen und Risiken zu minimieren, damit eine sichere Wiederherstellung gewährleistet ist.

Vorfälle mit schwerwiegenden Folgen – wie Ransomware- und Wiper-Angriffe – können die Systeme lahmlegen, die für die Bereitstellung von Produkten und Dienstleistungen für Kunden erforderlich sind, sowie die internen IT-Systeme, die für deren Verwaltung von entscheidender Bedeutung sind. Diese Szenarien erfordern einen anderen, stärker strukturierten Arbeitsablauf, der über die üblichen Protokolle für Datenschutzverletzungen hinausgeht.

Wenn man sich auf die Wiederherstellung konzentriert, ohne die Bedrohung zu untersuchen und zu mindern, können zugrunde liegende Schwachstellen bestehen bleiben – was das Risiko einer erneuten Infektion und längerer Ausfallzeiten birgt.

Eine sichere Wiederherstellung nach solchen Angriffen setzt voraus, dass man versteht, wie es zu dem Vorfall gekommen ist und wie man dessen Ursachen beheben kann. Dieser disziplinierte Ansatz ist der Kern aller Best Practices für die Vorfallreaktion im Bereich der Cybersicherheit.

1. **Beziehen Sie das CERT** von Cohesity frühzeitig in den Prozess der Vorfallreaktion ein, um schnelle und kompetente Unterstützung zu erhalten. Unser Team hilft Ihnen dabei, die Bedrohung einzudämmen, Ausfallzeiten zu minimieren, die forensische Analyse der Backup-Infrastruktur durchzuführen, die Einhaltung gesetzlicher Vorschriften und die Anforderungen an die Meldung von Sicherheitsverletzungen zu gewährleisten sowie eine sichere Wiederherstellung des Produktionsbetriebs zu ermöglichen.

2. **Stellen Sie den vertrauenswürdigen Zustand der Reaktionswerkzeuge wieder her und ermöglichen Sie einen schnellen Zugriff.** Wenn ein Cyberangriff erfolgt – und Ihr Betrieb lahmgelegt ist – gibt es keine Zeit zu verlieren. Schnelles Handeln ist entscheidend, und ein **Digital Jump Bag**™ hilft Ihnen, sofort zu reagieren.

   Dieser Digital Jump Bag („digitale Notfalltasche“), die idealerweise bereits vor dem Eintreten eines Vorfalls vorbereitet wird, ist ein gesicherter und zuverlässiger Speicherort, der schnellen Zugriff auf die Tools, die Software, die Konfigurationsdateien und die Dokumentation bietet, die für die Einleitung einer wirksamen Reaktion erforderlich sind. Gespeichert an einem gesicherten, unveränderlichen Ort außerhalb der Reichweite von Angreifern, bildet diese das Fundament der gesamten Cohesity Clean Room Lösung, unterstützt die kritischen Phasen der Reaktion auf Vorfälle und ermöglicht eine sichere, zuverlässige Wiederherstellung.

3. **Stellen Sie eine saubere Active Directory (AD) Infrastruktur wieder her.** Nur wenige Systeme sind geschäftskritischer – oder werden stärker ins Visier genommen – als AD. Zu Beginn der Vorfallreaktion ist es unerlässlich, Ihre AD-Umgebung gründlich zu untersuchen und zu bereinigen, bevor Sie andere Tools zur Vorfallreaktion wieder in Betrieb nehmen und vor allem bevor Sie das AD wieder in den Produktionsbetrieb eingliedern. Wird dieser Schritt übersprungen, bleibt Angreifern die Tür weit offen, um erneut einzudringen, was die Wiederherstellungsbemühungen untergräbt und die Betriebsunterbrechung verlängert.

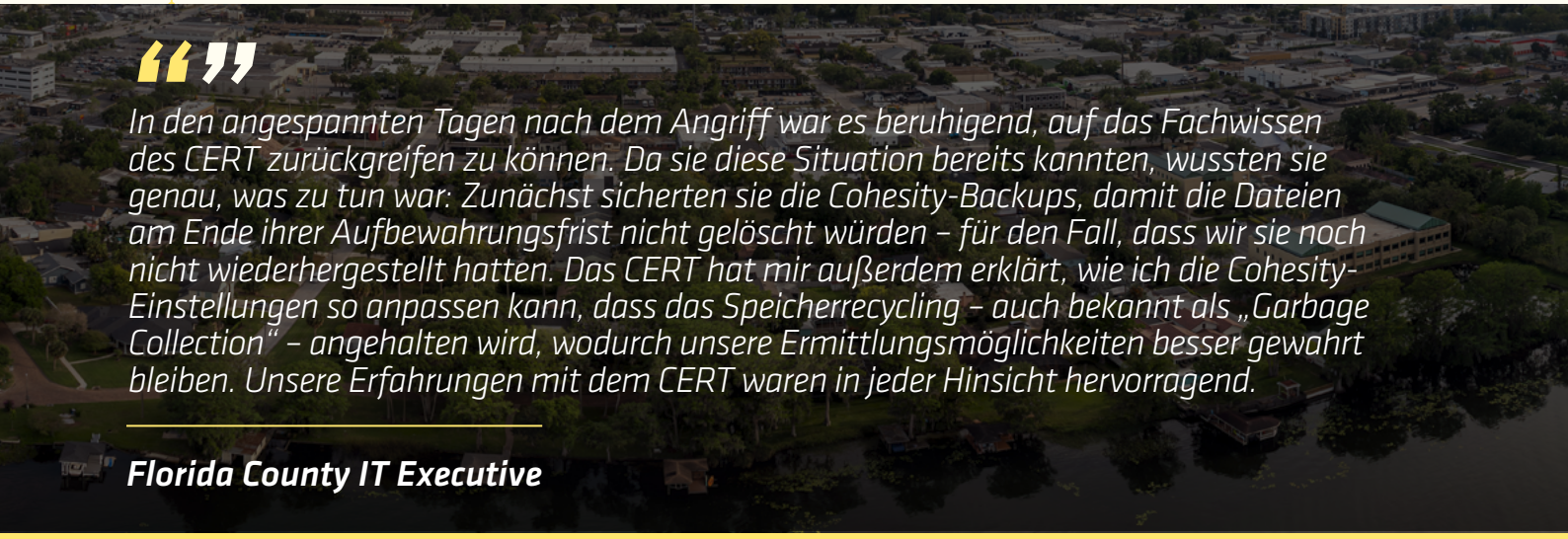
   Mit **Cohesity Identity Resilience auf Basis von Semperis** können Sie Ihr AD bis zu 90 % schneller in einen vertrauenswürdigen Zustand zurückversetzen.

5.

Schnelle Reaktion auf Cybervorfälle

4. **Richten Sie umgehend einen Reinraum für die Reaktion und Wiederherstellung ein.** Ein Reinraum sollte als vertrauenswürdige Umgebung eingerichtet werden, in der Analysten und Ermittler forensische Untersuchungen durchführen, die bei dem Angriff ausgenutzten Schwachstellen aufdecken und sicherstellen, dass infizierte Daten nicht erneut in Produktionsumgebungen gelangen.

5. **Suchen Sie passiv nach Artefakten, um weitere betroffene Systeme zu identifizieren.** Unsere Funktionen zur Bedrohungssuche erkennen Indikatoren für Kompromittierung (IOCs) in der gesamten Infrastruktur Ihrer Organisation – selbst wenn Systeme zur Eindämmung isoliert wurden. Diese Funktion ist resistent gegen gängige Techniken zur Umgehung von Sicherheitsmaßnahmen, die die Erkennung durch herkömmliche Endpunkt-Sicherheitstools verhindern oder verzögern können.



> *„In den angespannten Tagen nach dem Angriff war es beruhigend, auf das Fachwissen des CERT zurückgreifen zu können. Da sie diese Situation bereits kannten, wussten sie genau, was zu tun war: Zunächst sicherten sie die Cohesity-Backups, damit die Dateien am Ende ihrer Aufbewahrungsfrist nicht gelöscht würden – für den Fall, dass wir sie noch nicht wiederhergestellt hatten. Das CERT hat mir außerdem erklärt, wie ich die Cohesity-Einstellungen so anpassen kann, dass das Speicherrecycling – auch bekannt als „Garbage Collection" – angehalten wird, wodurch unsere Ermittlungsmöglichkeiten besser gewahrt bleiben. Unsere Erfahrungen mit dem CERT waren in jeder Hinsicht hervorragend."*
>
> ***Florida County IT Executive***

6. **Untersuchen Sie kriminaltechnisch frühere Dateisysteme.** Unser Datenschutzsystem ermöglicht über die Benutzeroberfläche und die API den Zugriff auf eine lückenlose Reihe unveränderlicher Snapshots, sodass die Verantwortlichen detaillierte kriminaltechnische Untersuchungen auf Dateiebene in den aufbewahrten Backup-Daten durchführen können.

7. **Verschaffen Sie sich einen Überblick über historische Schwachstellen, die bei dem Angriff ausgenutzt wurden.** Mit der Cohesity CyberScan Lösung können Sie Backup-Snapshots auf bekannte Schwachstellen überprüfen. Auf diese Weise können SecOps-Teams während eines Angriffs Schwachstellen identifizieren, selbst wenn ein System aufgrund von Begrenzungsmaßnahmen nicht erreichbar ist, gelöscht wurde oder vom Angreifer nachträglich gepatcht wurde.

8. **Unterstützung bei der Einhaltung gesetzlicher und regulatorischer Verpflichtungen zur Benachrichtigung von Aufsichtsbehörden, Partnern und betroffenen Datensubjekten.** Unsere KI-gestützte Datenklassifizierung durchsucht Backups, um sensible und regulierte Daten zu identifizieren, und unterstützt Organisationen dabei, gesetzliche Anforderungen zu erfüllen – selbst bei zerstörerischen Cyberangriffen, bei denen kritische Datenspeicher verschlüsselt oder gelöscht werden. Im Rahmen der Cohesity Clean Room-Lösung unterstützen wir zudem die Wiederherstellung der für das Vorfallmanagement erforderlichen Kommunikationsfunktionen. Kommunikationsvorlagen zur Benachrichtigung der Beteiligten können im Digital Jump Bag gespeichert werden, um einen schnellen Zugriff zu ermöglichen.

6.

Wiederherstellen von Systemen und Daten auf sichere Weise

Die Wiederherstellungsphase der Vorfallreaktion muss die vollständige Beseitigung von Bedrohungen gewährleisten, um eine erneute Infektion zu verhindern und die Wahrscheinlichkeit ähnlicher Angriffe in der Zukunft zu verringern.

Die Cohesity Clean Room-Lösung bietet Ihnen die Flexibilität, Ihre bevorzugte Wiederherstellungsstrategie zu wählen – ganz gleich, ob Sie bestehende Systeme wiederherstellen und bereinigen oder von Grund auf neu aufbauen möchten.

Sie unterstützt die schnelle Wiederherstellung von Datenträgern, sodass ein gesamtes Dateisystem wiederhergestellt werden kann, bevor Maßnahmen zur Beseitigung von Bedrohungen ergriffen werden. Außerdem ermöglicht sie schnelle Neuinstallationen auf Basis vertrauenswürdiger Software-Images und bewährter Konfigurationen.

“Unsere Organisation wurde Opfer eines kritischen Ransomware-Angriffs, der unsere gesamte Infrastruktur lahmlegte. Mit Cohesity waren wir in der Lage, Maschinen und Dateifreigaben wiederherzustellen, zu überprüfen, ob sie sauber sind, und die Anwendungen wieder online zu bringen.

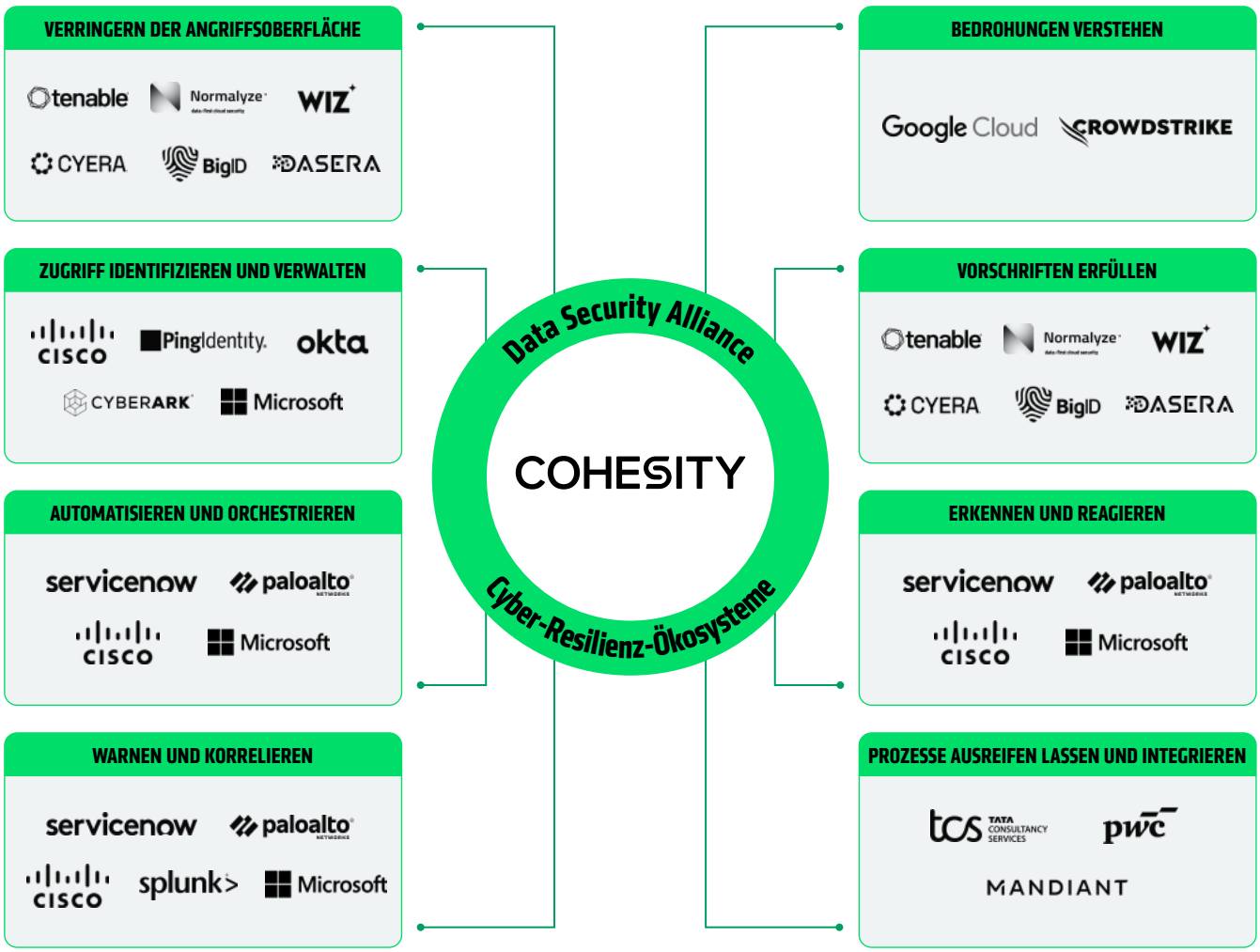
Cohesity hat uns regelrecht Hunderte von Arbeitsstunden erspart und ich würde sagen, es hat uns davor bewahrt, die Lösegeldforderung tatsächlich bezahlen zu müssen. Wir haben alle noch unsere Jobs und die Gemeinde hat ein funktionierendes Krankenhaus, weil wir mit Cohesity so viel Erfolg hatten.“

Sam Stewart
Network Systems Analyst,
Sky Lakes Medical Center

STÄRKUNG DER CYBER-RESILIENZ DURCH PARTNERSCHAFTEN

Cyber-Resilienz ist ein Teamsport. Keine Lösung eines einzelnen Anbieters kann einen Vorfall in seiner Gesamtheit untersuchen und beheben.

Aus diesem Grund haben wir die Data Security Alliance ins Leben gerufen – ein Netzwerk führender Unternehmen aus den Bereichen Sicherheit und Cyber-Recovery, das Ihnen dabei hilft, Risiken bei der Cyber-Recovery zu minimieren, die Effizienz Ihres Security Operations Center zu steigern und einen größeren Teil Ihrer Datenbestände mit den Ihnen bereits zur Verfügung stehenden Tools zu schützen.



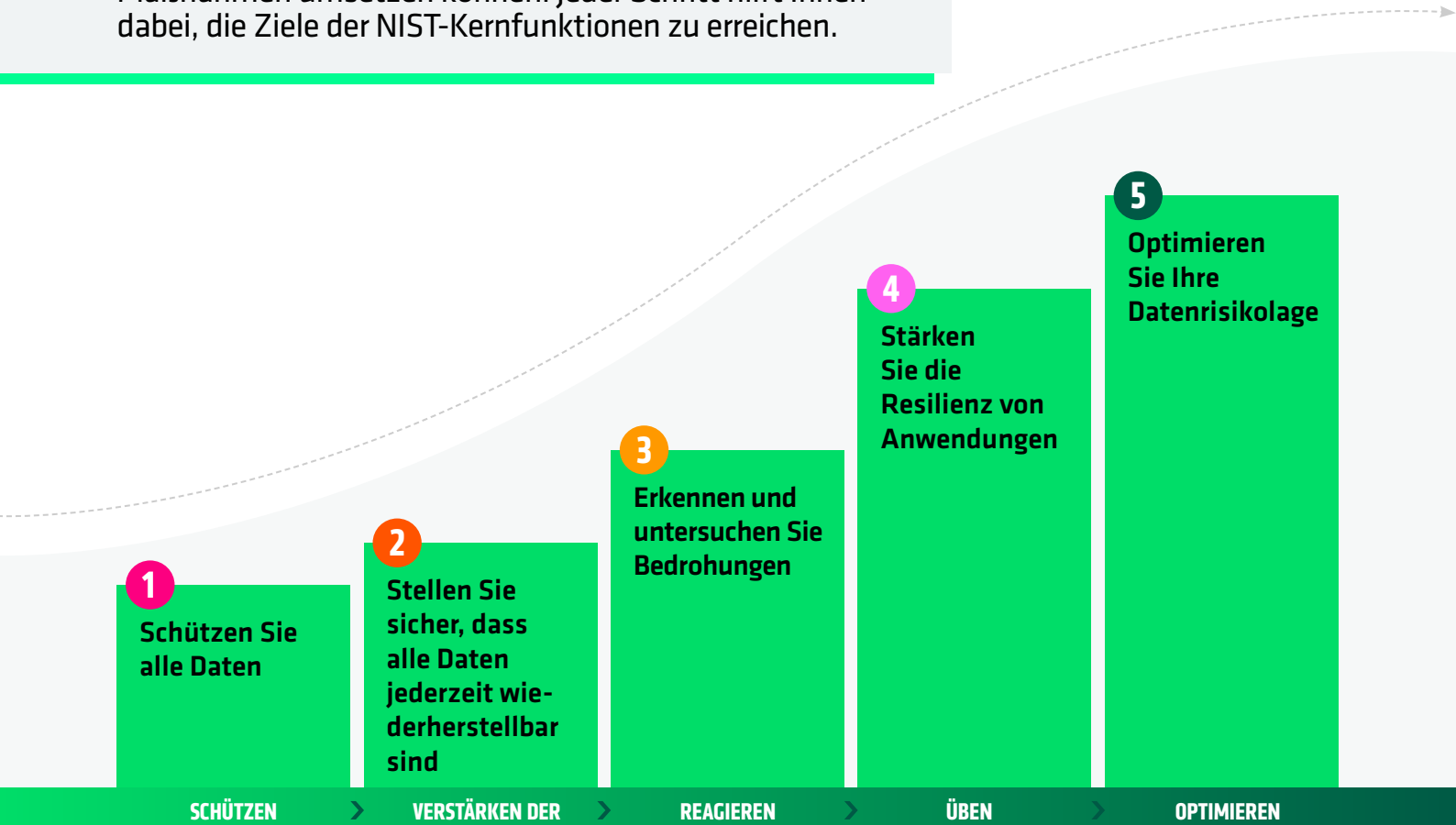
WIE GEHT ES WEITER

FÜR IHRE ORGANISATION?

Die 5 Schritte von Cohesity zur Cyber-Resilienz

Sie haben diese sechs Schlüsselelemente zum Aufbau eines cyberresilienten Unternehmens kennengelernt und erfahren, wie wir jede Phase des NIST Cybersecurity Framework (CSF) unterstützen. Nun ist es an der Zeit, diese Erkenntnisse in die Tat umzusetzen.

Um Ihnen den Einstieg zu erleichtern, haben wir einen **fünfstufigen Leitfaden zur Cyber-Resilienz** entwickelt, der sich an den bewährten Verfahren der Branche für die Reaktion auf Cybervorfälle und die Wiederherstellung orientiert. Es handelt sich um einen praktischen Leitfaden, der Ihnen zeigt, wie Sie mithilfe der Cohesity Data Cloud und der dazugehörigen Dienste konkrete, wiederholbare Maßnahmen umsetzen können. Jeder Schritt hilft Ihnen dabei, die Ziele der NIST-Kernfunktionen zu erreichen.



Die 5 Schritte ***von Cohesity*** zur Cyber-Resilienz

1. SCHÜTZEN SIE ALLE DATEN

NIST CSF-Ausrichtung: ***Schützen***

Stärken Sie Ihre Widerstandsfähigkeit, indem Sie Daten überall dort schützen, wo sie gespeichert sind – auf Unternehmensebene. Die Cohesity Data Cloud unterstützt **mehr als 1.000 Datenquellen**, darunter VMs, SaaS-Anwendungen, Datenbanken und NAS-Umgebungen, und senkt gleichzeitig Kosten und Risiken durch globale Deduplizierung und Komprimierung.

Dieser Ansatz senkt die Speicherkosten für die IT-Abteilung und verringert die Angriffsfläche für die Sicherheitsteams – zwei entscheidende Faktoren für eine stärkere Schutzfunktion.

2. STELLEN SIE SICHER, DASS DATEN WIEDERHERSTELLBAR SIND

NIST CSF-Ausrichtung: ***Sichern und wiederherstellen***

Schutz ist nur so stark wie Ihre Fähigkeit zur Wiederherstellung.

- **Stärken Sie Ihre Plattform:** Aktivieren Sie Sicherheitsmaßnahmen wie MFA, rollenbasierte Zugriffskontrolle und Quorum, um die Aufgabentrennung durchzusetzen und das Insiderrisiko zu minimieren.
- **Isolieren Sie kritische Daten:** Erstellen Sie sichere, wiederherstellbare Kopien mit dem Datentresor von Cohesity – erhältlich als von Cohesity verwalteter Cloud-Tresor oder als selbstverwaltete Lösung.

Diese Schritte stellen sicher, dass Sie vertrauenswürdige Kopien wiederherstellen können, wenn es darauf ankommt.

3. BEDROHUNGEN ERKENNEN UND UNTERSUCHEN

NIST CSF-Ausrichtung: ***Identifizieren und erkennen***

Widerstandsfähigkeit hängt von der Früherkennung ab. Mit Cohesity können Sie:

- ☑ **Schwachstellen**, einschließlich Lücken im Datenschutz identifizieren;
- ☑ **Datensicherungen** kontinuierlich auf Ransomware- und Malware-Indikatoren überprüfen;
- ☑ **In den Backup-Daten** gezielt nach bestimmten Bedrohungen suchen, damit Sie gegen Umgehungstechniken gewappnet sind;
- ☑ **Die Ergebnisse** an Ihre SIEM-/SOAR-Tools weiterleiten, um eine schnelle Korrelation und Reaktion im SOC zu ermöglichen.

Das Ergebnis: Bedrohungen werden früher erkannt und die Einsatzteams handeln schneller.

4. ANWENDUNGSRESILIENZ ÜBEN

NIST CSF-Ausrichtung: ***Reagieren und wiederherstellen***

Entdecken Sie den letzten Schritt >

Warten Sie nicht auf einen Angriff, um Ihren Wiederherstellungsplan zu testen.

- **Üben Sie regelmäßig:** Üben Sie Ihre Wiederherstellungspläne, als ob Sie unter Angriff stehen, um Ihre Wiederherstellungsprozesse und Ihre Einsatzbereitschaft zu überprüfen.
- **Automatisieren Sie die Wiederherstellung:** Nutzen Sie die Wiederherstellungsorchestrierung unserer Plattform, um Arbeitsabläufe zu optimieren und die Systemwiederherstellung nach einem Vorfall zu beschleunigen.

Dieser Schritt verwandelt die Wiederherstellung von einem manuellen, stressigen Prozess in ein wiederholbares, gut eingespieltes Verfahren.

Die ***5 Schritte*** von Cohesity zur Cyber-Resilienz

5. OPTIMIEREN SIE IHRE DATENRISIKOPOSITION

NIST CSF-Ausrichtung: ***Verwalten, identifizieren und reagieren***

- **Stärken Sie die Datensicherheits-Governance:** Nutzen Sie Ihre Cohesity-Daten und unsere Funktionen zur Datenklassifizierung, um einen Überblick über Ihre Datenbestände zu gewinnen, deren Risikograd einzuschätzen und die richtigen Sicherheitsmaßnahmen zu ergreifen.
- **Identifizieren Sie kritische Systeme, die nicht gesichert sind:** Identifizieren Sie sensible Daten in Ihrem gesamten Bestand – einschließlich Datensicherungen – und stellen Sie sicher, dass diese angemessen geschützt sind. Sie können diesen Prozess optimieren, indem Sie die Funktionen Ihres bevorzugten DSPM-Tools (Data Security Posture Management) mit unserer Plattform kombinieren.
- **Bewerten Sie die Auswirkungen von Vorfällen:** Sollte es zu einer Sicherheitsverletzung kommen, insbesondere wenn Ihre kritischen Datenspeicher verschlüsselt oder gelöscht wurden, können Sie anhand Ihrer Datensicherungen schnell feststellen, welche sensiblen und regulierten Daten möglicherweise offengelegt wurden, um Ihren gesetzlichen und Compliance-Verpflichtungen zur Benachrichtigung von Aufsichtsbehörden, Partnern und betroffenen Personen nachzukommen.

Erleben Sie Cyber-Resilienz in der Praxis

Erfahren Sie, wie sieben Organisationen aus verschiedenen Bereichen sich schnell und sicher von Ransomware-Angriffen erholt haben.

E-BOOK HERUNTERLADEN

ALLES ZUSAMMENFÜHREN

Unser fünfstufiger Leitfaden zur Cyber-Resilienz bietet Ihnen einen klaren, umsetzbaren Weg zur Operationalisierung des NIST CSF.

Mit der modernen Datensicherheitsplattform von Cohesity können Sie nicht nur schützen und wiederherstellen, sondern Ihre Cyber-Resilienz auch kontinuierlich optimieren.

ERFAHREN SIE MEHR ÜBER UNSERE CYBER-RESILIENZ-LÖSUNGEN

COHESITY
RESILIENCE EVERYWHERE

6100008-006-EN 11-2025