WHITEPAPER

Best Practices für Cybersicherheit und Cyber-Resilienz

Ein Dokument der Data Security Alliance

Inhaltsverzeichnis

Zusammenfassung

Stellen Sie sich vor, Ihr Unternehmen oder Ihre Regierungsbehörde wäre ein Formel-1-Rennwagen. Sie verbringen täglich viele Stunden damit, sich auf den Wettbewerb in der höchsten internationalen Rennsportklasse vorzubereiten, aber keine Strecke gleicht der anderen. Auch das Rennen verläuft immer unterschiedlich. Die Fahrer sind Menschen. Das Wetter wechselt. Doch mehr als jeder andere Faktor hängt Ihr Erfolg vor allem von einem ab: einer außergewöhnlichen Boxencrew.

Gleiches gilt für die Cyber-Resilienz. Eine integrierte, technische Cyberabwehr, die außergewöhnliche Datensicherheit und Datenmanagement kombiniert, ähnelt einer Formel-1-Boxencrew: Sie trägt dazu bei, dass Ihr Unternehmen erfolgreich im Rennen bleibt.

Im November 2022 gründeten mehr als ein Dutzend Schwergewichte der Sicherheitsbranche die **Data Security Alliance**, um Unternehmen und Regierungen mehr Möglichkeiten zu bieten, den Wettlauf gegen Cyberangriffe zu gewinnen. Ihre Mission ist klar: Daten sichern und schützen. Die Alliance erreicht dies durch die Vereinheitlichung von Datensicherheit und Datenmanagement mit Cybersicherheit, um die Cyber-Resilienz zu verbessern. Sie stellt kritische technische Integrationen und Architekturen bereit, teilt Best Practices und nimmt eine Vordenkerrolle beim Erreichen des gemeinsamen Ziels ein.

Dieses Whitepaper der Data Security Alliance beschreibt, wie Führungskräfte die wichtigsten Geschäftsprioritäten angehen können, einschließlich der Reduzierung von Risiken und der Stärkung der Compliance durch intelligentere Investitionen in die Cyber-Resilienz. Mit einer Anspielung auf den neuen NIST-Fachbereich Cyber-Resilienz-Engineering hebt dieses Papier Best Practices hervor, die mit der gemeinsamen Vision und den Technologien der Data Security Alliance in Einklang stehen. Es zeigt, wie Mitgliedsorganisationen Ideen und Strategien zur Bedrohungsabwehr einzelner Unternehmen auf die Branchenebene übertragen – und dies im Einklang mit dem NIST Cybersicherheits-Framework geschieht. Der Schwerpunkt liegt hierbei auf Identifizierung, Schutz, Erkennung, Reaktion und Wiederherstellung.

Cyber-Resilienz ist wichtig

In der heutigen digitalen Welt erwarten Verbraucher und Mitarbeiter, dass Unternehmen jeder Art und Größe unterbrechungsfrei arbeiten. Vertragliche Verpflichtungen wie Service Level Agreements erfordern dies sogar. Dennoch können Vorfälle – ob geplant oder ungeplant – zu Ausfallzeiten führen. Dann kommt es auf die Cyber-Resilienz an.

> **„Daten auf sichere und ethische Weise in Werte umzuwandeln, ist das Geschäftsziel des nächsten Jahrzehnts. Wer seinen Datenlebenszyklus kontrolliert, kann sein Schicksal am besten lenken. Da der wahrgenommene Wert von Daten zunimmt, werden sie zunehmend zum Ziel von Unternehmensspionage und staatlichen Cyberangriffen.“**[1]
>
> – **Dr. Jan-Peter Ohrtmann,** Partner, PwC

Das Ziel der Cyber-Resilienz besteht darin, angesichts eskalierender Bedrohungen ein Höchstmaß an Betriebs- und Geschäftskontinuität zu erreichen. Cybersicherheit – die praktischen, unverzichtbaren Cyber-Hygienepraktiken, zu denen regelmäßige Patches, Bedrohungserkennung, Schwachstellenidentifizierung und mehr gehören – ist grundlegend für die Cyber-Resilienz, reicht aber allein nicht aus. Cyber-Resilienz geht weit über die Notfallwiederherstellung hinaus und erfordert von Unternehmen auch, Störungen schnell zu antizipieren, ihnen standzuhalten, sich von ihnen zu erholen und sich an sie anzupassen, und zwar in Minuten oder Stunden, nicht in Tagen oder Wochen.

[1] PwC. „Privacy Megatrends 2030: A Roadmap for CEOs“, Dr. Jan-Peter Ohrtmann, 21. Januar 2021.

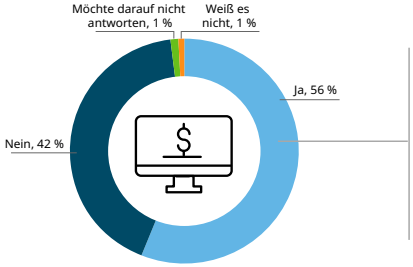
„Resiliente Unternehmen verfügen über eine Strategie und einen Rahmen für die Risikoerkennung und -minderung, eine gründliche Geschäftskontinuitätsplanung und -bereitschaft, flexible Fähigkeiten zur Reaktion auf Krisen und Vorfälle sowie Geschäftssysteme, die auf Redundanz und Zuverlässigkeit ausgelegt sind“, schrieb Stephanie Balaouras, VP und Group Director von Forrester im Mai 2020.[2] Nur wenige Jahre und Hunderttausende Ransomware-Angriffe später benötigen Unternehmen zusätzlich Cyber-resistente Strategien und Frameworks.

Cyber-Bedrohungen, insbesondere Ransomware, treten immer häufiger und und in immer raffinierterer Form auf. Daher müssen Unternehmen auf der ganzen Welt das neue Zusammenspiel zwischen ihren typischerweise isolierten Sicherheits- und Datenmanagementteams und den von ihnen verwendeten Lösungen vorantreiben, um ihre Cyber-Resilienz in rund um die Uhr verfügbaren -Umgebungen zu maximieren – und gleichzeitig den Anforderungen an die Geschäftskontinuität gerecht zu werden. Nur durch die Integration von Technologien und Prozessen können die modernen digitalen Plattformen von Unternehmen Cyberangriffen, Naturkatastrophen und Systemausfällen standhalten und sich von ihnen erholen.

Vor diesem Hintergrund wird der Datenschutz immer mehr zur obersten Priorität für Führungskräfte aus Wirtschaft und Regierung. Kundenbindung, Markenimage und nationale Sicherheit hängen von einem außergewöhnlichen Datenschutz ab und strategische Führungskräfte vertrauen auf ihre technischen Kollegen – Chief Information Officers (CIOs) und Chief Information Security Officers (CISOs) –, wenn es darum geht, die notwendigen Mitarbeiter, Richtlinien und Lösungen bereitzustellen, um die Ziele der Cyber-Resilienz zu erreichen. Es ist eine Herausforderung die oft isolierten, bedrohungszentrierten und komplexen eigenständigen Sicherheitslösungen zu verwalten, während sich die Ransomware-Bedrohungen weiterentwickeln. Datensicherheit und Datenmanagement waren ähnlich unkoordiniert und inkonsistent, wenn es darum ging, Cyberkriminelle zu erkennen, zu blockieren und daran zu hindern, große Gewinne zu erpressen.

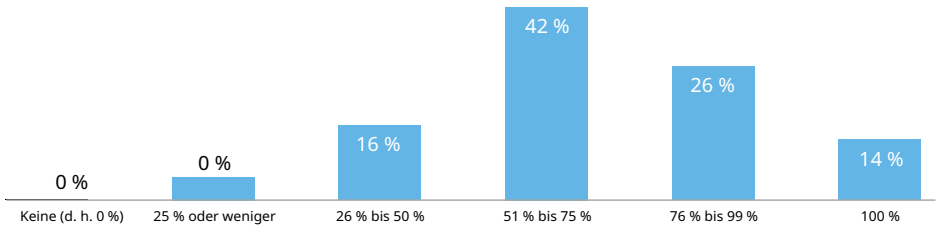
Mehr als die Hälfte der Unternehmen, die Opfer eines erfolgreichen Ransomware-Angriffs wurden, geben zu, ein Lösegeld gezahlt zu haben, um wieder Zugriff auf Daten, Anwendungen oder Systeme zu erhalten[3], wie die Enterprise Strategy Group (ESG) berichtet. Darüber hinaus stiegen die durchschnittlichen Lösegeldzahlungen in den ersten fünf Monaten des Jahres 2022 um 71 % und näherte sich laut Palo Alto Networks der beispiellosen Marke von 1 Million USD[4]. Doch selbst Unternehmen, die Lösegeld zahlen, stellen fest, dass dies keine Garantie für die Datenwiederherstellung ist. Nur 1 Unternehmen von 7 bzw. 14 % der für den ESG-Bericht befragten Unternehmen gaben an, dass sie nach der Zahlung alle ihre Daten zurückbekommen hätten.[5]

Haben erfolgreich angegriffene Organisationen Lösegelder gezahlt?



„**Mehr als die Hälfte** der Unternehmen, die Opfer eines erfolgreichen Ransomware-Angriffs wurden, gaben an, bereits Lösegelder gezahlt zu haben, um wieder Zugriff auf ihre Daten, Anwendungen oder Systeme zu erhalten.“

Prozentsatz der wiederhergestellten Daten nach Lösegeldzahlung.



[2] Forrester. „Business Resilience Is No Longer Optional“, Stephanie Balaouras, 12. Mai 2020.
[3] Enterprise Strategy Group. „The Long Road Ahead to Ransomware Preparedness“, März 2022.
[4] Palo Alto Networks. „2022 Unit 42 Ransomware Threat Report“, 7. Juni 2022.
[5] Enterprise Strategy Group. „The Long Road Ahead to Ransomware Preparedness“, März 2022.

Technische Führungskräfte können im Rahmen bestehender Budgets intelligenter arbeiten (ohne Erhöhungen der Sicherheitsbudgets beantragen zu müssen) und der zunehmenden Ransomware entgegenwirken, indem sie mit branchenführenden, datenorientierten Unternehmen zusammenarbeiten. Mit diesen gemeinsam können sie sich durch auf Cyber-Resilienz-Engineering ausgerichtete Kontrollen und Prozesse schützen und für die Wiederherstellung nach Ransomware-Angriffen sorgen. NIST definiert Resilienz-Engineering als eine aufstrebende Fachdisziplin, die in Verbindung mit Systemsicherheitstechnik eingesetzt wird, um überlebensfähige, vertrauenswürdige und sichere Systeme zu entwickeln.

Obwohl Daten die digitale Wirtschaft und staatliche Entwicklung anfeuern, muss bei Sicherheitsstrategien ein stärkerer Fokus auf Daten gelegt werden. Die Data Security Alliance stellt Daten in den Mittelpunkt, um Sicherheit mit Managementstrategien zu verknüpfen und die Ergebnisse zu verbessern.

> **„Die heutigen ununterbrochenen und immer ausgefeilteren Cyber-Bedrohungen erfordern einen praxisorientierten Ansatz. Es liegt nicht in der Verantwortung eines einzigen Anbieters, alle Cybersicherheitsprobleme zu lösen, es braucht ein ganzes Dorf, um die Übeltäter zu bekämpfen.“**
>
> – **Sanjay Poonen,** CEO und President, Cohesity

Ransomware nimmt zu

Es wird erwartet, dass Ransomware in diesem Jahr weltweit Schäden in Höhe von über 30 Milliarden USD verursacht. Prognosen zufolge wird es bis 2031 alle 2 Sekunden zu einem Angriff auf ein Unternehmen kommen, gegenüber alle 11 Sekunden im Jahr 2022.[6] Warum wird es von Jahr zu Jahr schwieriger, diese wachsende Bedrohung einzudämmen und zu stoppen? Organisationen, die Cyber-Resilienz anstreben, stehen vor zahlreichen Herausforderungen. Einige davon sind unten aufgeführt.

Herausforderungen für Mitarbeiter

Menschen sind nicht perfekt. Die häufigsten Ransomware-Angriffe erfolgen über Phishing-E-Mails und gestohlene Zugangsdaten – die letztere Form sorgt für 40 % aller Ransomware-Angriffe.[7]

- Den Unternehmen fehlen Zeit und Ressourcen, um das Sicherheitsbewusstsein der Mitarbeiter und Partner angemessen zu fördern und zu schulen, damit diese Angriffe (z. B. durch Phishing) abwehren können.
- Die IT- und Sicherheitsrollen sind isoliert. Fast ein Drittel der kürzlich befragten SecOps-Befragten (31 %) glaubt, dass die Zusammenarbeit mit der IT nicht gut sei, wobei 9 % der Befragten sie sogar als „schwach“ bezeichnen.[8]

Organisatorische und prozessuale Herausforderungen

Obwohl die Dauer der von Ransomware verursachten Unterbrechungen stetig sinkt, berichten Studien, dass es immer noch zu Verzögerungszeiten zwischen 21 und 11 Tagen kommt. Eine Hauptursache dafür ist, dass die Sicherheitsabläufe und der Informationsaustausch unzureichend auf die Abwehr dieser Bedrohungen ausgelegt sind. Beispiel:

- Das Patchen anfälliger Anwendungen und Systeme ist zeitaufwändig und kostspielig.
- Legacy-Systeme, die bei der Verteidigung helfen können, wie z. B. Datensicherungen, erfordern IT-Spezialisten.
- Die Angriffsflächen sind größer, wodurch es schwieriger wird, Daten überall zu schützen.
- „Runbooks“ für die Notfallwiederherstellung sind weit verbreitet, aber die meisten berücksichtigen nicht die Komplexität der Reaktion und Wiederherstellung nach Ransomware-Angriffen.

[6] Cybersecurity Ventures. „Ransomware will strike every 2 seconds by 2031.“ 3. Januar 2023.

[7] Verizon. „Data Breach Investigations Report“, 2022.

[8] Censuswide-Umfrage für Cohesity, Juni 2022.

Technologische Herausforderungen

Laut IDC wird sich die Größe der Global DataSphere von 2022 bis 2026 voraussichtlich mehr als verdoppeln, wobei Unternehmen den größten Anteil am Datenwachstum haben.[9] Viele Technologieumgebungen, insbesondere solche mit einem Flickenteppich aus erstklassigen Produkten und unterschiedlichen Sicherheits- und Infrastrukturplattformen, waren nicht für die Verarbeitung von Daten vor Ort, in der Cloud und am Edge in diesem Umfang ausgelegt. Angesichts der explosionsartigen Zunahme von Daten – die vielen unterschiedlichen Datentypen befinden sich an einer Vielzahl von Orten – geraten diese Umgebungen unter dem Druck von Ransomware ins Wanken.

- Bestehende Lösungen sind nicht gut integriert, was zu anhaltender Komplexität führt.
- Cloud- und Hybridumgebungen führen zu neuen Herausforderungen beim Schutz vor Ransomware und bei der Wiederherstellung.
- Wirtschaftliche Unsicherheit wirft die Frage auf, ob die Sicherheitsinvestitionen erhöht oder die bestehenden Strukturen optimiert werden sollten.
- Die meisten Technologien sind nicht in der Lage, die Effizienz und Skalierung zu nutzen, die künstliche Intelligenz und maschinelles Lernen (KI/ML) ermöglichen.

Gemeinsames Vorgehen

Zu den deutlichen Anzeichen dafür, dass Ransomware nicht abnimmt und nicht auf die leichte Schulter genommen werden sollte, zählt das kürzlich vom U.S. National Institute of Standards and Technology (NIST) herausgegebene Update „Developing Cyber-Resilient Systems: A Systems Security Engineering Approach“ mit Schwerpunkt auf Cyber-Resilienz-Engineering. Dieses aufstrebende Spezialgebiet der Systemtechnik entwickelt in Verbindung mit der Systemsicherheitstechnik überlebensfähige, zuverlässige und sichere Systeme.

Cyber-Resilienz-Engineering ist auf die Architektur, den Entwurf, die Entwicklung, die Implementierung, die Wartung und die Aufrechterhaltung der Zuverlässigkeit von Systemen ausgerichtet. Sie können schädliche Bedingungen, Belastungen, Angriffe oder Gefährdungen antizipieren, die aufgrund des Vorhandenseins oder der Nutzung von Cyber-Ressourcen auftreten könnten, ihnen standhalten sowie die Wiederherstellung und eine entsprechende Anpassung ermöglichen. Aus Sicht des Risikomanagements soll Cyber-Resilienz dazu beitragen, die Risiken zu mindern, die für Missionen, Geschäfte, Organisationen, Unternehmen oder Branchen aufgrund ihrer Abhängigkeit von Cyber-Ressourcen bestehen.

Dies kann für Unternehmen eine Erleichterung bedeuten, da der Fachkräftemangel die Zusammenarbeit zwischen IT- und Sicherheitsteams erschwert. In einem aktuellen Bericht stimmten 77 % der IT-Entscheidungsträger und 78 % der SecOps-Experten zu, dass dies Auswirkungen hat.[10] Der Mangel an Koordination zwischen IT und SecOps führt laut demselben Bericht dazu, dass die Befragten glauben, ihr Unternehmen sei Cyber-Bedrohungen stärker ausgesetzt. Alle Befragten befürchten besonders:

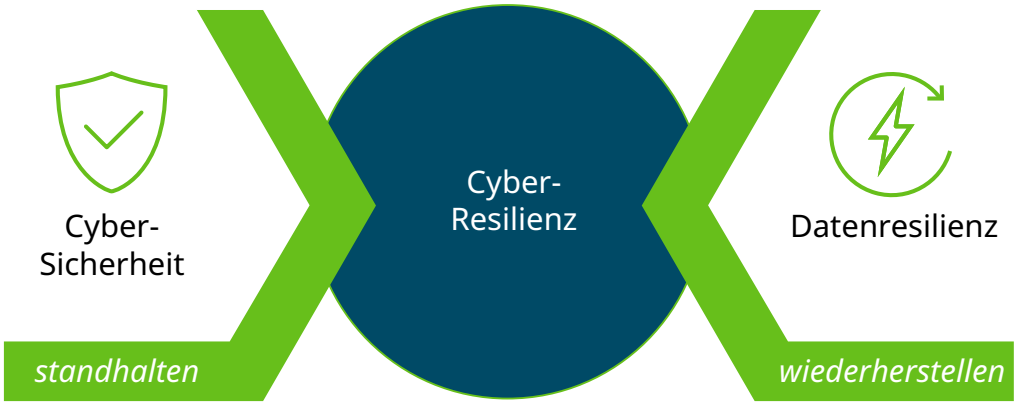
- Datenverlust (42 %)
- Geschäftsunterbrechung (42 %)
- Verlust von Kunden (40 %)
- Schuldzuweisungen des Teams, wenn Fehler auftreten (35 %)
- Bezahlen von Ransomware-Forderungen (32 %)
- Entlassung von Talenten beider Teams (IT und SecOps) (30 %).

[9] IDC. „Worldwide IDC Global DataSphere Forecast, 2022–2026“, Mai 2022.

[10] Censuswide-Umfrage für Cohesity, Juni 2022.

Ein Teil des NIST-Cybersicherheit-Resilienz-Framework-Ansatzes besteht aus einer Reihe von Richtlinien, Standards und Best Practices, die Organisationen dabei helfen sollen, Cybersicherheitsrisiken zu verwalten und zu reduzieren. Das Framework bietet eine gemeinsame Sprache und einen systematischen Ansatz für den Umgang mit Cybersicherheitsrisiken in verschiedenen Sektoren und Branchen. Es basiert auf den Kernfunktionen „Identifizieren“, „Schützen“, „Erkennen“, „Reagieren“ und “Wiederherstellen“. Diese Funktionen helfen Unternehmen, ihre Cybersicherheitsrisiken zu verstehen, ihre Vermögenswerte zu schützen, Cybersicherheitsvorfälle zu erkennen, auf diese zu reagieren und sich zeitnah von ihnen zu erholen.

Auf höchster Ebene umfasst ein robustes Cyber-Resilienz-Framework zwei Schlüsselkonzepte: Angriffen standzuhalten und die Wiederherstellung nach einem Angriff zu ermöglichen.



Modernes Denken: Richten Sie Ihre Sicherheitsstrategie auf Daten aus

Im Formel-1-Rennsport steht das Fahrzeug im Mittelpunkt. Wie maximiert man seine Geschwindigkeit? Wie optimiert man seine Leistung? Wie sorgt man dabei für umfassende Sicherheit? In Wirtschaft und Regierung sind Daten das Formel-1-Auto. Sie treiben die digitale Wirtschaft und die staatliche Führung voran. Bei vielen Sicherheits- und Verwaltungsstrategien stehen Daten jedoch nicht im Vordergrund. Ihr Fokus liegt zu sehr auf Infrastruktur und Systemen, insbesondere bei Clouds.

Die Mission der Data Security Alliance konzentriert sich auf Daten, insbesondere auf die Vereinheitlichung von Datenmanagement und Datensicherheit zugunsten der Cyber-Resilienz. Die Vision besteht darin, als Vordenker für branchenverändernde technische Integrationen und Architekturen, eine solide Zusammenarbeit in Daten- und Sicherheitsfragen sowie die Vermittlung von Best Practices zu sorgen.

Diese Vision ist nicht die gleiche wie die der Cloud Security Alliance (CSA), unterstützt jedoch deren Ziel, Best Practices zu definieren und das Bewusstsein für ihre Befolgung zu schärfen, um eine sichere Cloud-Computing-Umgebung zu schaffen. Unternehmen haben Schwierigkeiten mit der Sicherung und Nachverfolgung sensibler Daten in der Cloud. Nur 4 % glauben, dass alle ihre Cloud-Daten ausreichend gesichert sind. Über ein Viertel der Unternehmen erfassen keine regulierten Daten, fast ein Drittel keine vertraulichen oder internen Daten und 45 % keine nicht klassifizierten Daten, wie dem Forschungsbericht State of Cloud Data Security der CSA zu entnehmen ist.

Die Integrationen und Best Practices der Data Security Alliance werden Unternehmen dabei helfen, eine Reihe kohäsiver Prozesse und Kontrollen zu entwickeln, um die Auswirkungen von Cybervorfällen zu minimieren. Sie werden außerdem das Vertrauen der Unternehmen in ihre Daten stärken, die überall gespeichert sind – in öffentlichen, privaten und hybriden Computerumgebungen.

> „Cyber-Resilienz beginnt damit, die richtigen Grundlagen zu schaffen, insbesondere im Hinblick auf Ihre Daten. Es gilt zu verstehen, wo Ihre sensiblen Daten gespeichert sind, um was für Daten es sich handelt, wer Zugriff darauf hat und welche Risiken damit verbunden sind. Als Sicherheitsgemeinschaft müssen wir Daten in den Mittelpunkt unserer Sicherheitsstrategie stellen."
>
> – **Tyler Young,** BigID CISO

Wenn Sie Ihre Cybersicherheitsstrategie auf Daten fokussieren, erzielt Ihr Unternehmen folgende Vorteile:

- Verringerung des Risikos
- Gesteigerte Agilität
- Verbesserung der Ausfallsicherheit

Sie können sich diese Vorteile verschaffen, indem Sie den Bedrohungen in den verschiedenen Phasen der Ransomware-Reise proaktiv immer einen Schritt voraus bleiben:

Sechs Best Practices für Cyber-Resilienz

Wenn Sie sich auf Daten konzentrieren und sich von führenden Sicherheits- und Datenmanagementpartnern als Ihre architektonische Boxencrew unterstützen lassen, kann Ihr Unternehmen sich die Cyber-Resilienz-Basis verschaffen, die Sie für Ihr gesamtes Geschäft benötigen. Nachfolgend finden Sie sechs Best Practices für den Aufbau Ihrer cyber-resilienten Umgebung. (Sie ergänzen die Best Practices für Cyber-Resilienz des NIST, die ein ganzes Bündel von Maßnahmen umfassen – von der Entwicklung und Implementierung von Richtlinien und Verfahren über das regelmäßige Testen und Aktualisieren von Plänen zur Reaktion auf Vorfälle bis hin zum Aufbau von Partnerschaften mit anderen Organisationen zum Austausch von Threat Intelligence.)

1. Bleiben Sie wachsam: Überwachen Sie kontinuierlich Ihre Sicherheitslage

Die Bedrohungslandschaft entwickelt sich ständig weiter und Unternehmen haben aufgrund begrenzter Budgets und Ressourcen Schwierigkeiten, Schritt zu halten. Sie greifen auf den zeitaufwändigen manuellen Export von Daten in mehrere Tabellen zurück und verfolgen kontinuierlich Bedrohungen, anstatt potenzielle Angriffe oder Gefährdungen zu antizipieren. Dies führt zu unkoordinierter Entscheidungsfindung und unzureichender strategischer Planung auf allen organisatorischen Ebenen. Das NIST berät Teams bei der Entwicklung und Umsetzung von Cybersicherheitsrichtlinien und -verfahren. Dennoch benötigen Cybersicherheitsteams neue Ansätze, um aktuelle und aufkommende Cyber-Risiken

proaktiv anzugehen und zu bewältigen. Sie brauchen mehr Klarheit darüber, wo sie ihre Bemühungen priorisieren müssen, wie sich der Fortschritt im Laufe der Zeit objektiv messen lässt und wann sie die Ergebnisse den Stakeholdern effektiv mitteilen können, um Angriffe einzudämmen und die Anzahl der Vorfälle, auf die sie schnell reagieren müssen, drastisch zu reduzieren.

Zur Verhinderung von Cyberangriffen gehört nicht nur die Umsetzung der vom NIST empfohlenen Cybersicherheitsschulung und -sensibilisierung für Mitarbeiter, sondern auch die Implementierung von Zugriffskontrollen und Überwachungssystemen. Sie erfordert außerdem die vollständige Transparenz der Assets und Gefährdungen, eine umfassende Kenntnis der potenziellen Sicherheitsbedrohungen und klare Kennzahlen zur objektiven Messung des Cyber-Risikos. Organisationen, die Cyberangriffe vorhersehen und diese Risiken zur Entscheidungsunterstützung kommunizieren können, sind am besten für die Abwehr neu auftretender Bedrohungen aufgestellt.

Daten stellen eine besondere Herausforderung dar, da sie der dynamischste aller Vermögenswerte sind. Sensible Daten wachsen und vermehren sich schnell, und Unternehmen müssen den Speicherort der Daten, ihre Klassifizierung, die Art des Zugriffs und andere Faktoren kennen, um das Risiko und den Schutzbedarf zu verstehen.

Die erfolgreichsten Cyber-Resilienz-Pläne beginnen mit einer Bewertung. Teams müssen nicht nur Cyber-Stärken, -Schwächen, -Chancen und -Bedrohungen überprüfen, sondern auch die Lösungen identifizieren, die zum Aufbau von Cybersicherheitsabwehrmaßnahmen und zur effektiven Reaktion auf Cyberangriffe erforderlich sind. (Einzelheiten finden Sie in der Checkliste am Ende des Dokuments.) Branchenführende Bedrohungserfahrung gepaart mit Fachwissen über intelligente Datensicherheits- und Datenmanagement-Lösungen, die vor Ort und über Clouds hinweg funktionieren, helfen Unternehmen bei der Entwicklung effektiverer Cyber-Bereitschaftsprogramme.

2. Niemals vertrauen, immer überprüfen: Implementieren Sie Zero-Trust-Prinzipien

Das alte Sicherheitsmodell, das auf dem Prinzip „Vertrauen ist gut – Kontrolle ist besser“ basierte, ist in heutigen Geschäfts- und Regierungsumgebungen nicht mehr gültig, da es keine Perimeter mehr gibt. Best Practices für das digitale Geschäft erfordern eine Architektur mit Zero-Trust-Prinzipien, einschließlich „Niemals vertrauen, immer überprüfen“ und „Least Privilege“, um sicherzustellen, dass Sie wissen, wer wann auf welche Informationen zugreift.

Kompromittierte sensible Informationen schaden dem Ruf und dem Geschäft von Unternehmen sowie der Flexibilität und dem Situationsbewusstsein von Behörden. Deshalb ist es heutzutage von entscheidender Bedeutung, jede Identität – ob Mensch oder Maschine – über die unterschiedlichsten Geräte und Umgebungen hinweg zu schützen. Eine digitale Identität ist der Informationsbestand, der über eine Person, Organisation oder ein elektronisches Gerät online vorhanden ist. Da sich so viele Unternehmen einer digitalen Transformation unterziehen, ist eine Flut von Identitäten mit beispiellosem Zugriff auf Daten entstanden. Heutzutage übersteigt die Zahl der Identitäten mit privilegiertem Zugriff und Kontrolle über mehrere Geräte die Zahl der Benutzer bei weitem, sodass Ihr Sicherheitsteam eine noch größere Angriffsfläche schützen muss. Darüber hinaus führt die Verwendung mehrerer Legacy-Tools zur Verwaltung der Identitätssicherheit für Ihren Datenbestand zu Komplexität und Ineffizienzen, die Hacker ausnutzen können. Umfassende rollenbasierte Zugriffskontrollen gepaart mit „Nie vertrauen, immer überprüfen“-Richtlinien schützen Ihr Unternehmen besser vor Ransomware und Insider-Bedrohungen.

Da Daten mittlerweile überall vorhanden sind, muss Ihr Unternehmen einen Weg finden, Datenmanagement und Datensicherheit umfassend zu vereinheitlichen. um böswillige Akteure zu stoppen – von den Endpunkten bis zu den Cloud-Workloads, von der Sicherung bis zur Produktion und von der Identität bis zu den Daten. Ein datenorientierter Ansatz zur Angriffsprävention – ergänzend zur Empfehlung des NIST, Verschlüsselung und andere Sicherheitskontrollen zum Schutz von Daten zu implementieren – erfordert Transparenz und Kontrolle über alle Ihre Daten. Durch vollständige Transparenz können Sie das Datenrisiko in allen Ihren Cloud- und On-Premise-Systemen hinsichtlich Datensicherheit, Datenschutz, Compliance und Governance minimieren.

3. Kennen Sie Ihre Daten: Vertiefen Sie die Intelligenz

NIST empfiehlt, Aktionspläne für Vorfälle regelmäßig zu testen und zu aktualisieren sowie regelmäßige Schwachstellenbewertungen und Penetrationstests durchzuführen. Dies ist von entscheidender Bedeutung, denn eine schnelle Malware-Erkennung hilft Ihnen, die Zahlung eines Lösegelds selbstbewusst verweigern zu können. Über diese Anleitung für Produktionssysteme hinaus können Sie Cyber-Risiken und Schwachpunkte in Ihrer Produktionsumgebung aufdecken, indem Sie bedarfsgesteuerte und automatisierte Scans der Produktionsdaten durchführen und Snapshots zum Schutz gegen bekannte Schwachstellen erstellen. Mithilfe dieser Scans können Sie zudem ganz einfach Ihre Risikolage beurteilen und strenge Sicherheits- und Compliance-Anforderungen erfüllen, ohne Ihre Produktionsumgebung zu beeinträchtigen.

Scannen Sie Produktions- und Backup-Snaps, um den Zustand und die Wiederherstellbarkeit zu beurteilen. Überprüfen Sie Backups, um sicherzustellen, dass bei Wiederherstellungen keine bekannten Schwachstellen erneut in die Produktionsumgebung gelangen. All dies bietet tiefere Einblicke und einen globalen Überblick über alle Cyber-Risiken in Ihrer Produktionsumgebung, sodass Sie diese beheben können, bevor ein Angreifer sie ausnutzt.

Die auf künstlicher Intelligenz und maschinellem Lernen (KI/ML) basierende Datenklassifizierung beschleunigt die Schutz-, Erkennungs- und Reaktionsmaßnahmen gegen Ransomware und sorgt dafür, dass Sie Cyberkriminellen immer einen Schritt voraus sind. Sie können vertrauliche und regulierte Daten, einschließlich personenbezogene Daten (PII), geschützte Gesundheitsinformationen (PHI) und PCI-Daten, kontinuierlich erkennen und Fehlalarme durch ML-basierte Datenklassifizierung reduzieren. Diese Datenintelligenz hilft dabei, die Sicherheitslage zu ermitteln und abhängige Sicherheitskontrollen, wie z. B. Data Loss Prevention (DLP), auf dem neuesten Stand zu halten. Außerdem hilft sie den Reaktionsteams, die Auswirkungen eines Ransomware-Angriffs oder Cyber-Vorfalls zu verstehen.

4. Stärken Sie die Zusammenarbeit: Machen Sie Cyber-Resilienz zum Teamsport

Resilienz erfordert Vorbereitung, Reaktionsfähigkeit, Beharrlichkeit und Anpassungsfähigkeit. In der modernen vernetzten Welt müssen Sicherheitsverantwortliche eine Architektur und Prozesse nutzen, die lokale, Cloud- und SaaS-Umgebungen einbeziehen, und gleichzeitig Sicherheitsprozesse implementieren, die auf Geschäftskontinuität ausgerichtet sind. SecOps-Programme müssen Lösungen und Prozesse nutzen, die Prävention ermöglichen, um gegnerische Aktionen nach Möglichkeit zu stoppen – sie müssen diese aber auch erkennen und bei Bedarf reagieren, wenn Prävention nicht möglich ist.

Ausfallsicherheit wird erreicht, indem Gegner gestoppt werden, bevor sie ihre Ziele in einer Zielumgebung erreichen. Um die Resilienzbemühungen zu unterstützen, müssen Unternehmen ein umfassendes Verständnis ihrer individuellen Bedrohungslandschaft und Angriffsvektoren entwickeln. Dies lässt sich durch die gezielte Nutzung verfeinerter Threat Intelligence und die Kenntnis der vorhandenen Angriffsflächen erreichen. Hierbei dürfen die Bemühungen jedoch nicht auf allgemeinen Voraussetzungen basieren, sondern müssen auf die jeweilige Organisation ausgerichtet sein. Abschließend sei bemerkt, dass Prozesse zur Unterstützung der Ausfallsicherheit des Unternehmens ein weiteres wichtiges Ergebnis des Sicherheitsprogramms sind. Notfallplanung und Partnerschaften zur Reaktion auf Vorfälle sind der Schlüssel zur Unterstützung Ihres Unternehmens und der Umsetzbarkeit Ihres Sicherheitsprogramms.

NIST empfiehlt den Aufbau von Partnerschaften und Kooperationen mit anderen Organisationen, um Threat Intelligence und Best Practices auszutauschen. Wenn Sie Ihre Prozesse neu gestalten und anpassen, um sie an die Zusammenarbeit zwischen IT und SecOps anzupassen, hat Ihr Unternehmen bessere Chancen, Ihre Daten vor Ransomware-Angreifern zu schützen. Und auch Ihre Führungskräfte werden nachts besser schlafen können.

Entdecken und investieren Sie in vertrauenswürdige Sicherheitsprodukte, die nahtlos zusammenarbeiten, um Ransomware abzuwehren. Dazu gehören Sicherheitsinformations- und Ereignisverwaltung (SIEM) und Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR)-Lösungen, die die Zeit bis zur Entdeckung, Untersuchung und Behebung von Ransomware-Angriffen verkürzen. Vorkonfigurierte, integrierte Workflows, die erweiterbar sind, helfen SecOps dabei, sie für eine automatisierte Reaktion auf Vorfälle und einheitliche Abläufe zwischen Sicherheits-, IT- und Netzwerkteams zu erweitern. Stellen Sie außerdem sicher, dass vorkonfigurierte Integrationen möglich sind, indem Sie ein sicheres Software Development Kit (SDK) und anpassbare Verwaltungs-APIs verwenden, die Ihnen die Flexibilität geben, Ihre Umgebung so zu betreiben, wie es zur Bekämpfung von Cyberkriminalität erforderlich ist.

5. Konsolidieren und vereinfachen: Nutzen Sie eine moderne Plattform für Datensicherheit und -management

Skalierbarkeit und Kompatibilität sind weitere Schlüsselelemente zur Bekämpfung von Ransomware-Angriffen. Da Cyber-Resilienz Zusammenarbeit erfordert, ist es wichtig, die Vorteile einer erweiterbaren, modernen Datensicherheits- und Datenmanagement-Plattform mit einer API-reichen und API-first-Architektur zu nutzen, die standortübergreifend funktioniert und die unterschiedlichsten Datenquellen abdeckt. Durch die Konsolidierung vieler Datenmanagement-Funktionen auf einer einzigen Plattform vereinfachen Sie den Betrieb. Anstatt Daten zu kopieren und zu verschieben, verfügen Sie außerdem über eine Lösung, mit der Sie diese direkt vor Ort wiederverwenden können. Dadurch entstehen Mehrwertanwendungen für Daten, um routinemäßige und anspruchsvollere Aufgaben durchzuführen – von Virenscan und Datenmaskierung bis hin zur Analyse von Datei-Audit-Protokollen und Datenklassifizierung. Darüber hinaus reduziert eine einzige, erweiterbare Plattform Ihren Speicherplatzbedarf und die Angriffsfläche für Ransomware.

6. Gewinnen Sie Geschwindigkeit und Vertrauen: Integrieren Sie die Backup-Infrastruktur in ihre Sicherheitsinfrastruktur und Schutzmaßnahmen

Die Komplexität der Datensicherheit und des Datenmanagements lässt sich nicht allein bewältigen, insbesondere wenn es zu einem Verstoß kommt. Um so schnell wie möglich wieder betriebsbereit zu sein – konform zu der Wiederherstellungszeit und den Wiederherstellungspunktzielen (RTOs/RPOs) – ist ein integrierter Ansatz erforderlich, bei dem die Sicherung nicht isoliert erfolgt, sondern vollständig in die Sicherheitsinfrastruktur und Betriebsabläufe integriert ist.

Unternehmen, die in Datensicherheit und Datenmanagement investieren, profitieren von eng integrierten Lösungen, die das gesamte Spektrum an Sicherheits-Frameworks abdecken. Ein beliebter Ansatz ist der Incident Response Cycle (PICERL) des SANS Institute:

- **Preparation (Vorbereitung)** – Beurteilungen, Pläne, Ausbildung, Identitätsmanagement usw.
- **Identification (Identifizierung)** – Sensibilisierungsüberwachung, Früherkennung usw.
- **Containment (Eindämmung)** – Benachrichtigung, Datensicherungen, Forensik usw.
- **Eradication (Beseitigung)** – Wiederherstellungen, Ursachenanalyse, Malware-Entfernung usw.
- **Recovery (Wiederherstellung)** – Schwachstellenscans, Wiederaufnahme des Betriebs, Baseline usw.
- **Lessons Learned (Gewonnene Erkenntnisse)** – Reporting, Verfahrensaktualisierungen usw.

Sorgfältig durchdachte Integrationen geben Ihnen und Ihrem Team die Schnelligkeit und Sicherheit, Angriffe von der Planung bis zur Wiederherstellung abzuwehren – sogar mithilfe automatisierter KI/ML. Mit ihrer Hilfe können Sie potenzielle Cyberangriffe erkennen, indem Teams auf ungewöhnliche Muster in Ihren Daten aufmerksam gemacht werden. Wenn es zu einem Sicherheitsverstoß kommt, haben Sie auch die Möglichkeit, saubere Daten – zu jedem Zeitpunkt und an jedem Ort – wiederherzustellen, die auf Schwachstellen gescannt wurden, um eine erneute Infektion des Systems zu vermeiden und Ausfallzeiten zu reduzieren.

Checkliste für Cyber-Resilienzfähigkeiten

Wichtige automatisierte und umfassende Funktionen bekämpfen Ransomware wirksam. Dazu gehören:

	Voraussetzungen	Wichtige Funktionen
Cybersicherheit (widerstehen)	Strategie	• Beratung, Implementierung und Managed Security Services zum Aufbau Ihrer Cybersicherheitsabwehr und zur effektiven Reaktion auf Cyberangriffe
	Identitätsmanagement und Sicherheit	• Eine Plattform und Dienste für die Mitarbeiter- und Kundenidentität • Übergreifender Identitätsschutz – Mensch oder Maschine – über die unterschiedlichsten Geräte und Umgebungen hinweg
	Sichtbarkeits- und Expositionsmanagement	• Die Möglichkeit, alle IT-Assets zu inventarisieren – Hardware, Software, Anwendungen, Daten • Eine Plattform zur Risikobewertung über die gesamte Angriffsfläche hinweg – in der Cloud oder lokal, von der IT bis zur OT und darüber hinaus. Sie bietet Ihnen die nötige Transparenz und Einblicke, um Ihren Sicherheitsstatus zu validieren und priorisieren zu können. • Management der Datensicherheitslage (DSPM), um eine starke Datenerkennung, -klassifizierung und -intelligenz zu ermöglichen – zu wissen, wo Daten gespeichert sind, um was für Daten es sich handelt, wer Zugriff darauf hat, zu welchem Workflow sie gehören und welche Risiken mit ihnen verbunden sind
	Extended Detection and Response (XDR)	• Eine cloudnative Lösung mit XDR (Extended Detection and Response, erweiterte Erkennung und Reaktion)-Funktionen für die gesamte Sicherheitsinfrastruktur zum Beschleunigen von Erkennung, Reaktion und Wiederherstellung • Eine Möglichkeit, bei einem Ransomware-Angriff Workflows zur Wiederherstellung von Daten und Workloads zu initiieren
	Sicherheitsinformations- und Ereignisverwaltung (SIEM) der nächsten Generation	• Eine Lösung zur Abwehr komplexer Bedrohungen in den heutigen komplexen Hybridumgebungen, die modernste Analysen nutzt und auf einer skalierbaren, flexiblen cloudnativen Architektur aufbaut
	Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR)	• Automatisierung und Flexibilität, die es Ihnen ermöglichen, Cyber- und Ransomware-Angriffe schneller zu bewältigen
	Zielführende Threat Intelligence	• Umfassende Intelligenz und Expertise, die dynamische Lösungen vorantreiben, mit deren Hilfe Sie effektivere Programme entwickeln und Vertrauen in Ihre Cyber-Bereitschaft schaffen können • Transparenz und Kontrolle für alle sensiblen und kritischen Daten, um Datenrisiken in der Cloud und vor Ort mit einem Data-First-Ansatz zu verstehen und zu minimieren – für Datensicherheit, Datenschutz, Compliance und Governance
	Umfassende Beobachtbarkeit	• Eine erweiterbare Datenplattform, die einheitliche Sicherheit, vollständige Beobachtbarkeit und benutzerdefinierte Anwendungen bietet
	Zero Trust (ZT)/Perimeter- und Endpunktschutz	• Eine Möglichkeit, die kritischsten Bereiche des Unternehmensrisikos – Endpunkte, Cloud-Workloads, Identität und Daten – zu schützen, um Gegnern einen Schritt voraus zu sein und Sicherheitsverletzungen zu stoppen
	Forensik	• Sicherheitslösungen, die Ihnen vor der Ransomware-Beseitigung dabei helfen, die Grundursachen und die Ransomware-Signaturen für eine mögliche Strafverfolgung zu ermitteln

	Voraussetzungen	Wichtige Funktionen
Cyber-Resilienz (wiederherstellen)	Datensicherung und -wiederherstellung	• Umfassender Schutz vor Cyber-Bedrohungen, ML-basierte Anomalieerkennung, schnelle Ransomware-Wiederherstellung und hybride Cloud-Mobilität • Unveränderlichkeit der Daten • Datenisolierung: Die physische und logische Trennung von Daten schafft eine zusätzliche Sicherheitsebene • Zero-Trust-Prinzipien (z. B. Multifaktor-Authentifizierung [MFA]) • Quorum: Es sind mehrere Personen erforderlich, um Verwaltungs- oder Konfigurationsänderungen zu autorisieren
	Überprüfung auf Schwachstellen und Wiederherstellung	• Reinraum, Wiederinbetriebnahme, zusätzliche Wiederherstellungen von Daten und/oder Konfigurationen, Freigabe durch das Anwendungsteam, möglicherweise Rechenzentrumsbetrieb zum Verschieben von Systemen zwischen Umgebungen, Sicherheit und Vernetzung, um die Zugänglichkeit zum neuen Betriebsbereich sicherzustellen
	Bedrohungsschutz	• Erkennung von Malware und Indicators of Compromise (IOCs) mit ML-basierter Threat Intelligence und Scans zur Identifizierung von Bedrohungen in Backup-Daten
	Sicherheitsintegrationen	• APIs, SDKs und Integrationen in Sicherheitsabläufe und Sicherheitskontrollen, um die Reaktion auf Vorfälle zu beschleunigen und bestehende Kontrollen und Prozesse zu nutzen

Wenn Sie Daten in den Mittelpunkt Ihrer Cyber-Resilienz-Strategie stellen, können Sie sicher sein, dass Ihre Architektur auf maximalen Schutz und optimale Wiederherstellung ausgerichtet ist. Die Data Security Alliance empfiehlt IT- und Business-Entscheidungsträgern, sich unter www.cohesity.com/de/company/data-security-alliance genauer über Cyber-Resilienz zu informieren.

Über die Data Security Alliance

Die Mission der Data Security Alliance ist die Sicherheit und der Schutz von Daten. Die Allianz erreicht dies durch die holistische Vereinheitlichung von Data Security and Data Management mit Cybersicherheit, um die Cyber-Resilienz zu verbessern. Sie sorgt als Vordenker für branchenverändernde technische Integrationen und Architekturen, eine solide Zusammenarbeit in Daten- und Sicherheitsfragen sowie die Vermittlung von Best Practices. Die Data Security Alliance kombiniert erstklassige Lösungen von branchenführenden Cybersicherheits- und Dienstleistungsunternehmen mit der außergewöhnlichen Expertise in Datensicherheit und -management von Cohesity. Zu den Mitgliedern der Data Security Alliance gehören: BigID, Cisco, Cohesity, CrowdStrike, CyberArk, Okta, Palo Alto Networks, Securonix, Splunk, Tenable, Mandiant, Qualys, Netskope, ServiceNow, Zscaler und PwC.

2000046-001-DE 5-2023