5 WICHTIGE SCHRITTE

ZUR VERBESSERUNG DER CYBER-RESILIENZ IHRES UNTERNEHMENS

COHESITY

ALLUMFASSENDE AUSFALLSICHERHEIT.

EINLEITUNG

Die Zunahme von Ransomware-Angriffen und ihre immer größeren Auswirkungen offenbaren eine unangenehme Wahrheit. Selbst mit erheblichen Investitionen in die Prävention reichen diese Maßnahmen allein nicht mehr aus, um den heutigen Bedrohungen entgegenzuwirken.

Weder Ihnen noch uns gefällt dies, aber wir müssen den Tatsachen ins Auge sehen: Es wird immer wieder zu Cyberangriffen kommen. Zudem werden die Häufigkeit, Schwere und das Ausmaß der Angriffe zunehmen.

Das waren die schlechten Nachrichten.

Kommen wir nun zu den guten. Es gibt ein bewährtes Handbuch zur Verbesserung der Cyber-Resilienz, das auch Ihr Unternehmen nutzen kann, um seinen Ansatz zu überdenken und bessere Ergebnisse zu erzielen.

In diesem E-Book stellen wir Ihnen das 5 Schritte umfassende Handbuch für Cyber-Resilienz näher vor. Wenn Sie bei allen fünf Schritten konkrete Maßnahmen ergreifen, erfüllen Sie die Best Practices für die Reaktion auf Cyberangriffe und die Wiederherstellung. Darüber hinaus werden Sie erhebliche Vorteile bei der Sicherheit, bei Kosteneinsparungen und der Risikominderung feststellen.

HIER EINIGE HINTERGRUND-INFOS IM ÜBERBLICK

Trotz des erhöhten Bewusstseins für Cyberbedrohungen wie Ransomware verursachen Cyberangriffe weiterhin enorme betriebliche und finanzielle Verluste sowie Image-Schäden. Tatsächlich sind das die größten Bedrohungen für Unternehmen weltweit.

Die finanzielle Belastung ist echt und spürbar:

540.000 US-Dollar
Verlust für jede Stunde Ausfallzeit[1]

Über 1 Mrd. US-Dollar
an Ransomware-Zahlungen pro Jahr[2]

The State of Ransomware 2024 von Sophos[3] führt ähnlich ernüchternde Statistiken auf:

Von den 59 % der befragten Unternehmen, die im letzten Jahr von Ransomware betroffen waren, gaben **94 % an, dass die Angreifer es auf ihre Backups** abgesehen hatten, wobei **57 % dieser Versuche, Backups zu kompromittieren, erfolgreich waren.**

Außerdem wurden folgende Fakten ermittelt:

- **70 % der Angriffe führten zu einer Verschlüsselung von Daten**
- **2 Mio. US-Dollar betrug die durchschnittliche Geldforderung**
- **34 % der Unternehmen benötigten für die Wiederherstellung mehr als einen Monat**

Höchste Zeit für neue und effektivere Strategien, Funktionen und Lösungen.

[1] Splunk, The Hidden Costs of Downtime: The $400B problem facing the Global 2000: https://www.splunk.com/en_us/pdfs/gated/ebooks/the-hidden-costs-of-downtime.pdf

[2] Chainalysis, Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline, 07.02.24: https://www.chainalysis.com/blog/ransomware-2024/

[3] Sophos, The State of Ransomware 2024: https://www.sophos.com/en-us/content/state-of-ransomware

ES GIBT ZWEI GRÜNDE, WARUM CYBER-RESILIENZ EINE BESONDERE HERAUSFORDERUNG DARSTELLT:

1. Die Wiederherstellung nach Cyberangriffen ist nicht mit Disaster Recovery zu vergleichen.

Selbst wenn Ihr Unternehmen über solide Disaster-Recovery-Prozesse verfügt, können Sie sich nicht darauf verlassen, dass diese Prozesse auch bei Cyberangriffen greifen.

Bei Katastrophen wie Bränden, Überschwemmungen, Stromausfällen oder sogar Fehlkonfigurationen können Sie schnell eine Ursachenanalyse durchführen, um herauszufinden, was schiefgelaufen ist. Bei einem Cyberangriff können Hunderte von Ereignissen stattgefunden haben, die eine gründliche Untersuchung und Behebung erfordern. Außerdem haben Sie einen Gegner, der Ihre Wiederherstellung aktiv untergräbt und Sie mit Geldforderungen unter Druck setzt.

2. Selbst erfahrene Unternehmen und Experten unterschätzen möglicherweise, wie zerstörerisch ein Ransomware-Angriff sein kann.

Vielleicht gehen Sie davon aus, dass vertrauenswürdige Systeme Ihnen helfen, wieder online zu gehen, oder Sie verlassen sich auf Daten und Beweise, um herauszufinden, was vorgefallen ist.

Bei einem Cyberangriff können allerdings genau die Systeme, auf die Sie sich zur Untersuchung des Vorfalls stützen, ausgefallen, umgangen oder kompromittiert worden sein. Wenn sich gute mit schlechten Daten vermischen, ist die Wiederherstellung länger und schwieriger. Aus diesem Grund sehen wir viele smarte Unternehmen, die immer noch Schwierigkeiten mit einer schnellen, sauberen und sicheren Wiederherstellung haben.

WERFEN WIR EINEN BLICK AUF DIE **5 WICHTIGEN SCHRITTE** ZUR VERBESSERUNG DER CYBER-RESILIENZ

Stellen Sie sich dies als einen praktischen Plan vor, bei dem Sie mit jedem Schritt weiter vorankommen.

SCHRITT 1

ALLE DATEN SICHERN.

Das klingt denkbar einfach, dennoch vollziehen viele Unternehmen noch immer nicht diesen entscheidenden ersten Schritt. Schuld daran ist wahrscheinlich die Datenflut.

Das organische Datenwachstum hat eine Fragmentierung und Silos verursacht, wodurch sich die Angriffsfläche erheblich vergrößert hat und Unternehmen angreifbarer sind als je zuvor. Gleichzeitig stellt das Management und die Sicherung von Daten in großem Umfang eine zunehmende Belastung für die Betriebseffizienz dar.

Die Kombination von mehr Daten an mehr Orten und weniger Möglichkeiten, sie effizient zu managen, bietet Angreifern perfekte Bedingungen, um Chaos zu verursachen.

SPÜRBARE VORTEILE VON SCHRITT 1

- ☑ **Erhöhte Sicherheit**
- ☑ **Reduziertes Risiko**
- ☑ **Verbesserte Compliance und Governance**
- ☑ **Geringere Kosten und verbesserter ROI**
- ☑ **Gesteigerte IT-Effizienz**

WICHTIGE MASSNAHMEN, DIE IN SCHRITT 1 IMPLEMENTIERT WERDEN MÜSSEN

1. Einsatz einer modernen Datenplattform, die mehr als 1.000 Datenquellen unterstützt, u. a.:

- Virtuelle Maschinen (VMs)
- SaaS-Anwendungen
- Datenbanken
- NAS-Umgebungen (unstrukturierte Daten)

2. Umgebungsübergreifende Plattform für On-Premise, Cloud und SaaS

Da Ihre Daten überall verstreut sind, sollte Ihre Plattform über flexible Bereitstellungsmodelle verfügen, die durch eine gemeinsame Bedienoberfläche und APIs vereinheitlicht werden.

3. Vereinfachung des Betriebs mit einer intuitiven Bedienoberfläche

Wenn Ihre Bedienoberfläche benutzerfreundlich ist, kann ein relativ kleines Team riesige Datenmengen managen, und zwar gut. Unsere Kunden profitieren von einer überragenden Betriebseffizienz mit einer zentralen Bedienoberfläche und einer Reihe von APIs für die Automatisierung von Workflows auf unserer Plattform.

4. Starke Speicherkompression

Sie benötigen eine Plattform mit einer starken Speicherkompression. Dies führt zu beträchtlichen Einsparungen, wenn Petabytes verwaltet werden müssen. Wir haben ein einzigartiges Dateisystem, das dem branchenüblichen Standard entspricht. Eine wirklich starke Speicherkompression sorgt für niedrigere Gesamtbetriebskosten.

SCHRITT 2

STELLEN SIE SICHER, DASS BACKUPS IMMER WIEDERHERGESTELLT WERDEN KÖNNEN.

Angreifer nehmen Backups ins Visier. Sie wissen ganz genau, dass Sie viel eher zu Zahlungen bereit sind, wenn sie diese letzte Verteidigungslinie durchdringen können, da Ihr Unternehmen dann keine anderen Möglichkeiten hat.

Die allgemeine Annahme, dass eine moderne Datenplattform sofort wiederherstellbare Backups garantiert, wäre natürlich schön, stimmt aber nicht ganz.

Sie müssen schon mehrere Maßnahmen ergreifen, um Angreifern den Zugriff zu erschweren und im Fall eines Angriffs saubere Backups wiederherstellen zu können.

SPÜRBARE VORTEILE VON SCHRITT 2

- ☑ **Schnellere und sicherere Wiederherstellung**
- ☑ **Stärkerer Schutz gegen Angriffe**
- ☑ **Auditbereitschaft**
- ☑ **Zero-Trust-Prinzip**

WICHTIGE MASSNAHMEN, DIE IN SCHRITT 2 IMPLEMENTIERT WERDEN MÜSSEN

1. **Stärkung Ihrer Plattform durch die Konfiguration leistungsstarker Funktionen wie:**

- Multifaktor-Authentifizierung (MFA)
- Unveränderlichkeit (damit Daten nicht geändert oder gelöscht werden können)
- Rollenbasierte Zugriffskontrolle (RBAC)
- Aufgabentrennung (teilen Sie kritische Aufgaben unter verschiedenen Personen auf)

2. **Implementierung eines Datentresors**

Durch eine mit Air-Gapping verstärkte Kopie Ihrer wichtigsten Daten und der **3-2-1-1-Backup-Regel** (drei Kopien der Daten, zwei verschiedene Medien, eine extern und eine unveränderbar) steht Ihnen im Notfall immer eine Kopie Ihrer Daten zur Verfügung.

Cohesity bietet auch ein erweitertes Schlüsselverwaltungssystem, sodass wir unseren Kunden auch bei einem Angriff Zugang zu ihren Daten gewähren können.

Dieser Zugang sorgt dafür, dass Backups immer wiederhergestellt werden können.

SCHRITT 3

ERKENNEN SIE BEDROHUNGEN UND UNTERSUCHEN SIE DIESE.

Dieser Schritt bezieht sich auf die Kombination von Threat-Scanning und Threat-Hunting-Funktionen.

SPÜRBARE VORTEILE VON SCHRITT 3

- **Frühzeitige Bedrohungserkennung und -minderung**
- **Gesicherte Backup-Integrität**
- **Schnellere Wiederherstellung nach Vorfällen und kürzere Ausfallzeiten**
- **Gemeinsamer Kontext für IT- und InfoSec-Teams**

WICHTIGE MASSNAHMEN, DIE IN SCHRITT 3 IMPLEMENTIERT WERDEN MÜSSEN

1. Proaktives Handeln durch regelmäßige Überprüfung Ihrer Backups auf Bedrohungen Betrachten Sie diese proaktiven **Bedrohungsscans** als konsequente Hygiene. Dies hilft Ihnen bei Folgendem:

- Schnellstmögliche Beseitigung von Veränderungen
- Identifizierung von Malware oder anderen Schwachstellen

2. Initiierung von **Threat-Hunting**-Funktionen auf der Suche nach bestimmten Bedrohungen Unsere kuratierten Threat Feeds und Integrationen von Security-Ecosystem-Anbietern in unserer Data Security Alliance (z. B. CrowdStrike, Palo Alto Networks und Cisco) sorgen dafür, dass Sie deren kollektives Wissen mit den Daten, die wir in diese Systeme einbringen können, erhalten.

Auch Ihre InfoSec- und IT-Teams werden mit denselben Informationen arbeiten.

Da wir vielen unserer Kunden im Laufe der Jahre geholfen haben, sich von Cyberangriffen zu erholen, wissen wir, dass native Threat-Scanning- und Threat-Hunting-Fähigkeiten Teil Ihrer Datenplattform sein müssen.

Warum? Weil andere Sicherheitssysteme deaktiviert oder anderweitig offline sein können, wenn Sie angegriffen werden.

SCHRITT 4

ÜBEN SIE ANWENDUNGSRESILIENZ.

Wenn Sie die Schritte 1–3 durchgeführt haben, sind Sie bereits gut vorbereitet. Sie haben Ihre Plattform aufgerüstet, gehärtet und Ihre Deployment um einen Datentresor erweitert.

Außerdem haben Sie Erfahrungen mit regelmäßigem Threat Scanning und Threat Hunting gesammelt. Gute Arbeit!

Im vierten Schritt erweitern Sie Ihre Maßnahmen, indem Sie Ihre Reaktions- und Wiederherstellungsprozesse für Infrastruktur, Daten und Anwendungen üben. Schließlich wollen Sie das nicht zum ersten Mal während eines echten Angriffs tun, wenn Ihre Systeme ausgefallen sind und der Druck hoch ist.

Vielleicht denken Sie, dass es zeitaufwendig ist, alle Systeme und Daten wieder online zu bringen, und fragen sich, wie Sie bei regelmäßigen Tests Ihre alltäglichen Aufgaben erledigen können.

SPÜRBARE VORTEILE VON SCHRITT 4

- ☑ **Schnellere und sicherere Wiederherstellung**
- ☑ **Verbessertes RTO**
- ☑ **Geringeres Neuinfektionsrisiko**
- ☑ **Weniger Unterbrechungen und finanzielle Risiken**

An dieser Stelle kommt die Orchestrierung ins Spiel.

Mit der Orchestrierung können Sie Reaktions- und Recovery-Abläufe automatisieren und die Wiederherstellung Ihrer Systeme nach einem Angriff üben. Diese Tests helfen Ihnen, Ihre Reaktions- und Wiederherstellungsfähigkeiten zu verbessern, während die Orchestrierung dazu beiträgt, diese Maßnahmen mit weniger manuellem Aufwand abzustimmen.

Ein praktisches Beispiel für die Automatisierung: Mit unserer Clean Room-Lösung können Sie eine separate Umgebung einrichten, in der Sie forensische Analysen durchführen und tief in infizierte Daten eintauchen können. So können Sie verstehen, was passiert ist, und dann das schädliche Artefakt beseitigen, um Ihre Systeme sicher wiederherstellen zu können. Dieser Ansatz bietet eine einzigartige Kombination aus Schnelligkeit, Automatisierung und leistungsstarker Forensik, um die Zusammenarbeit von Incident Respondern und IT-Teams zu unterstützen. Das Ergebnis? Eine schnellere Cyberreaktion und Wiederherstellung.

In diesem Schritt werden Sie auch mit dem Cohesity CERT (Cyber Event Response Team) arbeiten. Dieses Expertenteam unterstützt Sie bei der Reaktion auf Vorfälle, von ausgeklügelter Ransomware über Datenschutzverletzungen bis hin zu gezielten Angriffen. Sie werden nie alleingelassen.

WICHTIGE MASSNAHMEN, DIE IN SCHRITT 4 IMPLEMENTIERT WERDEN MÜSSEN

1. Übungen mit Orchestrierung und Proben

- Automatisierung Ihrer Reaktions- und Wiederherstellungs-prozesse
- Durchführung von Tests, um Ihre Reaktionspläne zu verfeinern, u. a. die Reihenfolge, in der Sie Infrastruktur, Datenquellen und Anwendungen wiederherstellen

2. Verwendung eines Reinraums

- Einrichtung einer separaten, sicheren Umgebung für forensische Analysen
- Identifizierung und Beseitigung von Bedrohungen, bevor Ihre Infrastruktur, Datenquellen und Anwendungen wiederhergestellt werden

3. Support von Experten

- Wenden Sie sich an Cohesity CERT, wenn Sie angegriffen werden

SCHRITT 5

OPTIMIEREN SIE IHRE DATENRISIKOLAGE

Auf der einen Seite werden die Kriminellen, die Ransomware einsetzen, immer aggressiver. Auf der anderen Seite haben Sie mehr Daten zu verwalten als jemals zuvor: On-Premise, SaaS, Cloud und Edge. Vielleicht fragen sich viele, was sich in ihren ungeschützten S3 Buckets befindet, von denen niemand etwas weiß oder die niemand überwacht.

Neben ungeschützten S3 Buckets können zu den versteckten Risiken auch verwaiste Datenbanken, ungeschützte Anmeldedaten und vieles mehr gehören.

Proaktive Maßnahmen wie Data Security Posture Management (DSPM) und Datenklassifizierung können diese Risiken reduzieren.

SPÜRBARE VORTEILE VON SCHRITT 5

- ☑ **Verbesserte Sichtbarkeit und Klassifizierung von Daten**
- ☑ **Proaktive Risikoidentifizierung und -minderung**

WICHTIGE MASSNAHMEN, DIE IN SCHRITT 5 IMPLEMENTIERT WERDEN MÜSSEN

1. Welche Daten befinden sich wo?

- Scannen Sie Ihre Umgebung und erfassen Sie, welche Daten sich wo befinden und welches Schutzniveau sie haben. Die gesamte Tool-Klasse mit DSPM macht es möglich.
- Verstehen Sie, was sich in Ihrem Backup-Bestand befindet und stellen Sie sicher, dass alle Daten auf die richtige Art und Weise geschützt werden, mit unseren umfassenden Integrationen von einigen der besten Anbieter der Branche, darunter Cyera und BigID.

2. Bewerten Sie, was von einer Sicherheitsverletzung betroffen oder was bei einer Datenexfiltration passiert sein könnte.

- Holen Sie sich den nötigen Schutz und verringern Sie Ihr Risiko mit der in unseren Produkten integrierten Datenklassifizierung.
- Reagieren Sie schnell, wenn es zu einem Vorfall kommt und Juristen fragen: Welche Daten sind betroffen? Wie sensibel sind sie? Was ist unser Risiko? Wie viele Kunden sind betroffen? Welche Arten von Datensätzen sind betroffen?

FAZIT

Sie kennen nun die fünf entscheidenden Schritte zur Verbesserung der Cyber-Resilienz Ihres Unternehmens und verfügen über die praktischen Informationen, die Sie zu deren Umsetzung in Ihrer Umgebung benötigen.

Cohesity befindet in der einzigartigen Lage, Sie auf diesem Weg zu begleiten, damit Sie die größtmögliche Cyber-Resilienz erlangen.

Für weitere Informationen über die sichere und schnelle Wiederherstellung nach Ransomware-Angriffen empfehlen wir folgende Lektüre:

„AUFBAU EINER GEZIELTEN REAKTIONSSTRATEGIE FÜR DESTRUKTIVE CYBERANGRIFFE“

COHESITY

ALLUMFASSENDE AUSFALLSICHERHEIT.