E-BOOK

Cyberresilienz: Datenschutz mit dem Inside-Out-Ansatz

NetApp

Übersicht

Der Weg in das Herz der IT-Abteilung

Es ist Zeit für den wöchentlichen Einkauf im Supermarkt. Sie schnappen sich einige Tüten und die Schlüssel und nehmen dann eine große silberne Tablette – Ihre magische Fahrsicherheitstablette –, bevor Sie das Haus verlassen.

Jetzt können Sie sicher und unbesorgt in dem Wissen fahren, dass Ihr Körper mit seinen übermenschlichen Fähigkeiten alles, was auf dem Weg passieren könnte, unbeschadet übersteht.

Wenn wir einen Resilienz-Zaubertrank trinken könnten, unsere Häuser mit Ziegeln bauen könnten, die Eindringlinge hinauskatapultieren, oder Schmuck kaufen könnten, der aus der Hand des Diebs hinausfliegt, würden wir uns wohl kaum um Anschnallgurte, Schlösser oder Alarmanlagen kümmern.

Ein neuer Ansatz für Cybersicherheit

In der realen Welt gibt es solche magischen Schutzmaßnahmen vielleicht nicht, in der virtuellen Welt tauchen aber immer mehr davon auf. Sie nähern sich der vorhandenen Schutzausrüstung immer mehr an. In den letzten Jahrzehnten hat die IT-Welt hinsichtlich Cybersicherheit auf den Ansatz „Anschnallgurte und Alarmanlagen“ gesetzt, denn es gab nur diesen.

Heute gibt es einen intelligenteren Ansatz: ***Cyberresilienz***.

Cyberresilienz kombiniert Datensicherung mit Datensicherheit, damit Unternehmen sich von Cyberangriffen schnell wieder erholen können. Selbst wenn ein Eindringling es durch die äußeren Schichten schafft oder durch einen Insider schädliche Vorgänge ausgelöst werden, sind die Daten geschützt, da der Schutz direkt integriert ist und nicht nachträglich aufgesetzt.

Warum ist das wichtig?
Cybersicherheitsmaßnahmen, die sich allein auf Abschottung konzentrieren, hinken den sich ständig weiterentwickelnden kriminellen Taktiken hinterher. Heute gilt:

Bei den meisten Sicherheitsstrategien geht es im Kern darum, den Feind am Tor zu stoppen, indem die äußeren Schichten verstärkt werden.

Aber Unternehmen verteidigen nicht nur ein Tor. Durch die Vervielfachung der Endpunkte, Bring-Your-Own-Device-Strategien und die Zunahme von Remote-Arbeit sind sie für hunderte verantwortlich.

Heute ist es für Kriminelle leichter denn je, Unternehmen zu schaden, die mit der umfassenden Überwachung komplexer Netzwerkumgebungen schon jetzt überfordert sind.

Und viele Unternehmen vergessen, dass es nicht eigentlich darum geht, ein Eindringen zu verhindern. Das Hauptziel besteht darin, das zu schützen, was für Sie am wertvollsten ist: **Ihre Daten**.

Cyberresilienz *Substantiv*

Cy·ber·re·si·li·enz

Die Fähigkeit, widrige Umstände, Belastungen, Angriffe oder Gefährdungen, die Cyberressourcen nutzen oder durch Cyberressourcen ermöglicht werden, zu antizipieren, ihnen standzuhalten und sich von ihnen zu erholen[1]

Setzt Ihre Cyberresilienz-Strategie am entscheidenden Punkt an?

Wohin Sie auch schauen, Bedrohungen lauern überall. Wo fangen Sie also an?

Sie beginnen mit einem Daten-orientierten Sicherheitsansatz – und machen diesen dann zu einem zentralen Teil Ihres Cyberresilienzplans. In der modernen Bedrohungslandschaft:

- **Der weltweite Anstieg von 62 % bei Ransomware**[2] und der Anstieg von 3,4 % bei Ransomware-Familien[3] zeigen, dass Angreifer Daten immer leichter in ihre Gewalt bekommen.
- **Ungefähr ein Drittel der Unternehmen zahlt nach einem Ransomware-Angriff schließlich,** um die verschlüsselten Daten zurückzubekommen.[4]
- **2021 verursachte ein Ransomware-Angriff im Schnitt Kosten von 1,85 Millionen US-Dollar**, gegenüber 768.106 US-Dollar im Jahr 2020.[5]
- **Ransomware-Angriffe mit Double Extortion nehmen zu**, was bedeutet, dass Unternehmen nicht mehr nur Gefahr laufen, ihre Daten zu verlieren, sondern auch noch mit der Veröffentlichung der Daten bedroht werden.[6]

Es steht mehr auf dem Spiel als jemals zuvor, und im modernen Computing stellt sich nicht mehr die Frage, ob es zu einem Ransomware-Angriff kommt, sondern wann.

Aber müssen Sie nun ständig den nächsten Ransomware-Angriff fürchten? Nein. Sie können die Angst vor Ransomware ablegen und Ihre **Cyberresilienz aktivieren** – mit einem Daten-orientierten Cybersicherheitsansatz.

Bei diesem Ansatz starten Sie so nah wie möglich an Ihren Daten statt an den äußeren Schichten.

Stellen Sie die Weichen für bessere Cyberresilienz

Wenn Sie sich in das Herzstück Ihrer IT-Abteilung begeben, um Ihre Daten zu schützen, steht Ihnen Arbeit bevor. Zum Glück haben aber andere diesen Weg schon vor Ihnen beschritten und ein paar nützliche Wegweiser hinterlassen.

Ermitteln **Sichern** **Erkennen**

Reagieren **Wiederherstellen**

Selbst mit diesen hilfreichen Wegweisern ist die Entwicklung eines umfassenden Cyberresilienzplans noch immer ein schwieriges und teures Unterfangen. Ihr Team muss mit begrenzten Ressourcen zurechtkommen, Kompetenzlücken überbrücken, regulatorischen Anforderungen gerecht werden und inmitten vieler anderer Prioritäten um Aufmerksamkeit kämpfen.[7] Cyberresilienz kann dadurch schnell anstrengend werden – und genauso schnell in Vergessenheit geraten.

So arbeiten Sie sich schrittweise durch die einzelnen Phasen.

62 %

Der **weltweite Anstieg von 62 % bei Ransomware**[2] und der **Anstieg von 3,4 % bei Ransomware-Familien**[3] zeigen, dass Angreifer Daten immer leichter in ihre Gewalt bekommen.

Ermitteln: Bestandsaufnahme Ihrer Umgebung

Ermitteln Sie, was gesichert werden muss, und ordnen Sie die Punkte Ihrer Bedeutung nach. Dabei sollten Sie sich die folgenden Fragen stellen:

Kennen Sie die Speicherorte Ihrer Daten und wissen Sie, welche Datentypen es in Ihrer Umgebung gibt?

Für jeden Datentyp: Handelt es sich um sensible Daten und wer ist zugriffsberechtigt?

Welche Systeme sind für die Aufrechterhaltung Ihrer Geschäftsabläufe wesentlich?

Welche Rolle spielt die jeweilige Technologie in Ihren Geschäftsabläufen, und wie könnte sie von Cyberkriminellen eventuell ausgenutzt werden?

Werden Informationsflüsse dokumentiert?

Wie werden Rollen und Verantwortlichkeiten im Zusammenhang mit Cybersicherheit zugewiesen?

Wie sieht Ihr Plan für Gefahrenidentifizierung und Risikomanagement aus?[7]

Welche Datensicherungs- und -sicherheitslösungen nutzen Sie aktuell?

Anders gesagt: Sie müssen Ihre aktuelle Datensicherung und -sicherheit bewerten. Außerdem sollten Sie Ihre Daten in die verschiedenen Datentypen unterteilen, den Standort der jeweiligen Typen ermitteln und die damit verbundenen Rechte evaluieren.

Herausforderungen in der Ermittlungsphase

Diese Phase ist zeitaufwendig, und IT-Führungskräfte müssen sich ohnehin schon jeden Tag um enorm viele Aufgaben im Bereich Infrastruktur- und Datenmanagement kümmern. Allein die Inventarisierung der gesamten IT-Infrastruktur kann sehr viel Zeit in Anspruch nehmen, vor allem ohne Automatisierungstools.

Wenn diese Inventarisierung dann auch noch ohne einen konkreten Plan oder standardisierte Klassifizierungsprotokolle durchgeführt wird, kann dabei eine unübersichtliche Datenmasse entstehen, die Ihre Teams nur schwer entziffern und operationalisieren können.

Sichern: Aufbau von Verteidigungsmaßnahmen

In der Sicherungsphase errichten Sie Ihre Schutzmauern.

Dazu sollten Sie Ihre Daten verschlüsseln, regelmäßige Backups vornehmen, für Zugriffssteuerung sorgen, Schutzmaßnahmen für Ihre äußeren Grenzen implementieren, anfällige Betriebssysteme und Anwendungen aktualisieren und Nutzern die Best Practices der Cybersicherheit vermitteln.[7]

Jetzt gilt es, böswillige Nutzer zu blockieren, potenziell schädliche Daten zu isolieren, das Schreiben von zusätzlichen Daten auf eine Festplatte zu stoppen, granulare unveränderliche Kopien zu erstellen, um eine Infizierung der Systeme abzuwenden, und das Löschen von Daten durch nicht entfernbare Backups zu verhindern.

Herausforderungen in der Sicherungsphase
In der Sicherungsphase werden einige der jüngsten Änderungen in Sachen Cybersicherheit offensichtlich. Zwar schützen Unternehmen ihre IT-Umgebungen schon seit Jahrzehnten mit Firewalls und Netzwerk-basierten Angriffserkennungstools, aber angesichts der enormen Datenmengen der neuen Realität lassen sich diese Strategien nicht mehr so einfach anwenden. IT-Abteilungen sehen sich vor schwierige Fragen gestellt, wie:

- Wie lassen sich riesige Mengen an Daten verschlüsseln, die schneller generiert werden, als sie inventarisiert werden können?
- Wie lässt sich Zugriffssteuerung bewerkstelligen, ohne das Nutzererlebnis stark zu beeinträchtigen, weil das zu geringerer Produktivität oder unsicheren Workarounds führen könnte?
- Wie kann man angesichts der großen Anzahl entdeckter Schwächen sicher sein, alles abgedeckt zu haben?
- Welche regelmäßigen Tests der Datensicherungstechnologien müssen durchgeführt werden, um sicherzustellen, dass man seine Daten im Fall einer Bedrohung erfolgreich wiederherstellen kann?

Erkennen: Immer einen Schritt voraus

Vorbeugung ist die beste Medizin. Richten Sie also Systeme ein, die verdächtige Aktivitäten identifizieren, bevor sie zu einer existentiellen Bedrohung werden. Achten Sie auf:

- aktualisierte Erkennungsprozesse
- regelmäßig kontrollierte Protokolle zum Erkennen von und Reagieren auf untypische Aktivitäten
- ein eingehendes Verständnis regulärer Datenflüsse zur Wahrnehmung ungewöhnlicher Aktivitäten, die auf Datendiebstahl hinweisen könnten
- die Fähigkeit, eine Datenpanne nicht nur erkennen, sondern auch deren Auswirkungen oder Ausmaße zu beurteilen[7]

In anderen Worten: Sie müssen das Nutzerverhalten auf verdächtige Aktivitäten kontrollieren und Anomalien im Datenverhalten erkennen.

Herausforderungen in der Erkennungsphase

Umgang mit der Alarmflut: Die wahrscheinlich größte Herausforderung in der Erkennungsphase ist die Vielzahl der Störsignale, die Unternehmen herausfiltern müssen. Cybersicherheitsteams und Security Operations Center (SOC) werden von Gefahrenalarmen überflutet, die sie oft manuell abarbeiten müssen.

Automatisierte Gefahren-Triage: Sie brauchen eine Möglichkeit, falsche Alarme und Alarme mit niedriger Priorität automatisch zu untersuchen und zu beseitigen, damit sie ihre Aufmerksamkeit auf die brenzligeren Alarme konzentrieren können.

Schnelleres Erkennen: Cybersicherheitsteams müssen außerdem in der Lage sein, diese Alarme schneller zu erkennen, damit sie reagieren können, bevor es zu gravierenden Schäden kommt. Insbesondere müssen sie unverzüglich über unberechtigten Zugriff mit kompromittierten Zugangsdaten informiert werden, bevor ein Angreifer eine erhebliche Datenmenge verschlüsseln kann.

Reagieren: Wissen, was in einer Krise zu tun ist

Bedrohungen entwickeln sich parallel zu Sicherheitsmaßnahmen weiter. Deshalb ist es wichtig, dass Sie Ihre Pläne kontinuierlich in drei Schritten auf die Probe stellen:

1

Alle Teammitglieder müssen ihre Verantwortlichkeiten kennen. Das umfasst sowohl allgemeine Best Practices für Cybersicherheit als auch ihre jeweilige konkrete Rolle in einem Notfall.

2

Aktualisieren Sie Ihre Pläne entsprechend der Entwicklung der Bedrohungslage und anhand der aus überstandenen Angriffen gewonnenen Erkenntnisse.

3

Teilen Sie all diese Aktualisierungen mit anderen internen und externen Beteiligten, damit im Fall eines Angriffs geschlossen reagiert werden kann.[7]

Herausforderungen in der Reaktionsphase

Um die Reaktionsphase zu meistern, benötigen Sie einen guten Überblick über Ihre Systeme. So können Sie einschätzen, wo Ihre Daten sich befinden, die Aktivitäten in Ihrer Umgebung überwachen und Ihre Pläne entsprechend anpassen.

Auch dies ist eine zeitaufwendige Aufgabe für Unternehmen, die schon mit den tagtäglichen Infrastruktur- und Datenmanagementanforderungen mehr als genug zu tun haben.

Eine effektive Reaktion muss schneller sein als die manuelle Ausführung eines Plans – egal, wie gut die Vorbereitung ist. Cybersicherheitsteams brauchen daher automatisierte Tools, die vorgegebenen Schritten (beispielsweise Erstellen eines Daten-Snapshots) folgen, sobald das System eine verdächtige Aktivität entdeckt.

Wiederherstellen: Umgehend zurück zur Normalität

Wenn ein Cyberangriff die Geschäftsabläufe unterbricht, müssen Sie schnell wieder zum Normalbetrieb zurückfinden. Dafür müssen Sie unbedingt Folgendes wissen:

- Welche Informationen müssen geteilt werden?
- Wer braucht Zugang zu diesen Informationen?
- Wie stellen Sie sicher, dass diese Beteiligten die Informationen zeitnah erhalten?
- Wie teilen Sie den Vorfall der Öffentlichkeit mit und wie informieren Sie Personen, deren Daten eventuell kompromittiert wurden?
- Welche Schritte müssen unternommen werden, um Aufsichtsbehörden zu verständigen?

In der Wiederherstellungsphase geht es darum, die Ausfallzeit zu verringern, indem Sie Daten schnell wiederherstellen, nicht betroffene Anwendungen wieder online verfügbar machen und intelligente forensische Analysen einsetzen, um die Quelle der Bedrohung zu ermitteln.

Herausforderungen in der Wiederherstellungsphase
Nach einem Angriff kann es wertvolle Zeit kosten, zu ermitteln, welche Bereiche in welchem Umfang betroffen sind. Sie brauchen diese Informationen jedoch schnell, um die internen Maßnahmen und die Wirkung nach außen zu managen.[7]

Alle fünf Phasen eines Cyberresilienzplans – Ermitteln, Sichern, Erkennen, Reagieren und Wiederherstellen – werden von der NetApp Cyberresilienzlösung unterstützt. Viele Unternehmen setzen jedoch eine Kombination aus mehreren Cybersicherheitstools ein. Da kann der Gedanke, zu einem anderen Provider zu wechseln, erdrückend wirken.

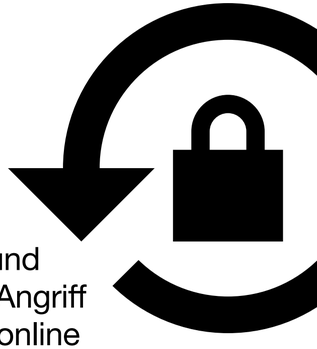
Mit NetApp muss der Wechsel aber nicht zu einer Überforderung werden, da Sie in Ihrem Unternehmen eine Ransomware-Lösung einführen können, die entweder als umfassende Lösung oder als Ergänzung zu bestehenden Investitionen genutzt werden kann.

Entwicklung eines modernen Cyberresilienz-Ansatzes – von innen nach außen

Schauen wir uns genauer an, wie Sie einen modernen Cyberresilienz-Ansatz für Ihr Unternehmen entwickeln können, einschließlich der Lösungen, die den oben beschriebenen Herausforderungen begegnen. Die Cyberresilienzlösungen von NetApp gehen diese Herausforderungen von innen nach außen an, mit Sicherheits- und Sicherungslösungen, die auf Ihre Daten zugeschnitten sind.

Das Lösungsportfolio von NetApp umfasst leistungsstarkes und robustes Datenmanagement und Benutzerüberwachung sowie professionelle Services, die Unternehmen in jeder Phase ihrer Vorbereitung und ihres Managements unterstützen.

Wenn Sie sich vorrangig auf Ihre Daten konzentrieren, können Sie Ihre Cyberresilienz-Anforderungen einfacher angehen. In einem ersten Schritt sollten Sie sich ein Bild von Ihrem aktuellen Zustand machen. Die folgenden Fragen helfen Ihnen dabei.



Vorbeugung ist die beste Medizin. Richten Sie also Systeme ein, die verdächtige Aktivitäten identifizieren, bevor sie zu einer existentiellen Bedrohung werden. Achten Sie auf:

- Wo befinden sich meine Daten? In der Cloud? On-Premises? Am Edge? Oder an mehreren geografischen Standorten?
- Welche Art von Daten habe ich?
- Welche Rechte sind meinen Daten zugeordnet?
- Wie schnell kann ich schädliche Aktivitäten ermitteln und blockieren?
- Wie kann ich sicherstellen, dass alle meine Daten geschützt sind, während die Ausmaße eines Angriffs ermittelt werden?
- Wie kann ich meine Daten und Anwendungen nach einem Angriff in wenigen Minuten wieder online bereitstellen?
- Wie kann ich die Quelle der Bedrohung untersuchen, damit ich genügend Informationen habe, um ähnliche Versuche zukünftig zu verhindern?
- Wie kann ich Schutzmaßnahmen direkt in meine Daten integrieren oder sie damit umgeben, sodass sie sich schnell „selbst schützen“ können, während ich damit beschäftigt bin, eine Bedrohung zu ermitteln und darauf zu reagieren? Wie kann ich das Nutzerverhalten in meinem globalen Netzwerk auf verdächtige Aktivitäten überwachen?

Die Antworten auf diese Fragen sind das Gerüst für einen Daten-orientierten Cyberresilienzplan, mit dem Ihr Unternehmen auf Ransomware-Angriffe vorbereitet ist.

Wenn mehr Fragen mit „unbekannt“ beantwortet werden, als es Ihnen lieb ist, hat NetApp professionelle Services für Sie, die Ihnen nicht nur Antworten, sondern auch die Tools liefern, die Sie zur Umsetzung Ihres neuen Ransomware-Schutzes und Recovery-Plans brauchen.

Ein Cyberresilienzplan in Aktion – mit NetApp

Das Lösungsportfolio von NetApp wurde ausgehend von dem Bedarf von IT- und Sicherheitsteams entwickelt, um Daten besser zu sichern und zu schützen. Mit der ONTAP Storage-Software als Fundament schichten wir Datenservices übereinander, um die Sichtbarkeit zu verbessern, Bedrohungen zu erkennen und die Reaktion und Wiederherstellung zu automatisieren.

Lesen Sie weiter und erfahren Sie, wie NetApp und ein Cyberresilienzplan, der auf den zuvor gegebenen Antworten basiert, Ihr Team bei einem tatsächlichen Ransomware-Angriff unterstützen können.

„Wir hatten kürzlich einen Ransomware-Vorfall und die Erkennungsmöglichkeiten von Cloud Insights haben uns restlos überzeugt.“

IT-Leiter eines Transportunternehmens

Ermitteln

Ihr Team muss wissen, welche Art von Daten Sie haben, ob sie sensibel sind und wo der Speicherort der Daten ist, um die Sicherung der Daten besser planen zu können. NetApp Cloud Data Sense, eine Software-als-Service-Lösung (SaaS), nutzt auf künstlicher Intelligenz (KI) basierende Algorithmen für Datenerkennung, -mapping und -klassifizierung, um diese Informationen bereitzustellen.

Währenddessen versetzt NetApp Cloud Insights, das in der hybriden Cloud-Infrastruktur für Sichtbarkeit sorgt, Ihr Team in die Lage, Ihre gesamte Umgebung zu überwachen und zu sichern. Und das ist auch gut so, denn Ihre Verteidigungsmaßnahmen können jeden Moment auf die Probe gestellt werden.

Sichern

Ihr in New York ansässiges IT-Team kommt eines Morgens zur Arbeit und erfährt, dass jemand aus dem Londoner Büro auf einen nicht sauberen E-Mail-Link geklickt hat.

Obwohl niemand anwesend war, der diesen Angriff direkt hätte beobachten können, wurden bekannte schädliche Dateiendungen durch NetApp FPolicy, Teil der Datenmanagement-Software NetApp ONTAP, mithilfe der Zero-Trust Datensicherung blockiert.

Die Hacker lassen dennoch nicht locker. Über ein manipuliertes Nutzerkonto infizieren sie Dateien durch einen Zero-Day-Malware-Exploit. Weitere Malware nutzt mehrere manipulierte Konten zur Verschlüsselung der Daten – und zwar langsam, um nicht erkannt zu werden.

Erkennen und Reagieren

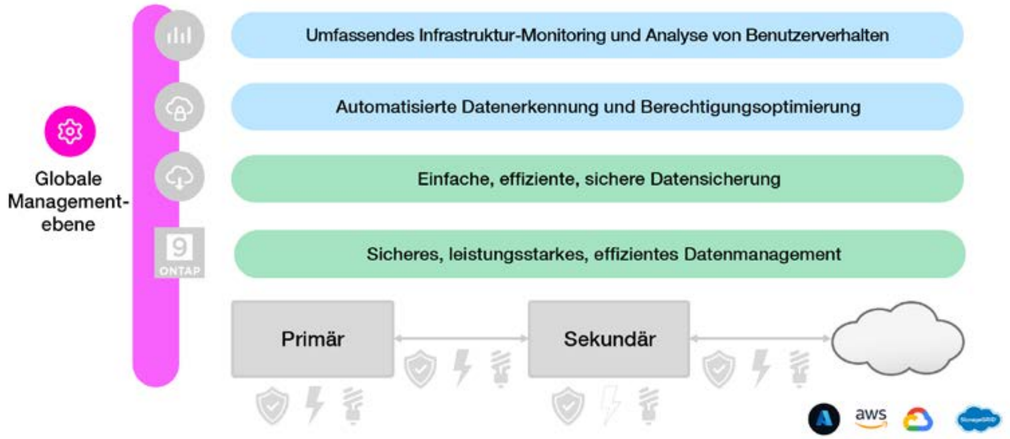
Alle diese Aktivitäten zu entdecken und zu bekämpfen, wäre mit wenigen Mitarbeitern nur schwer zu schaffen, insbesondere dann, wenn sie sich gleichzeitig auch um andere Aufgaben kümmern müssen – und das in verschiedenen Zeitzonen. Aber das IT-Team hat NetApp Cloud Insights, das sich darum kümmert, Dateifreigaben über das Netzwerk zu überwachen und anomales Nutzerverhalten zu entdecken. Selbst wenn das Team den Angriff nicht bemerkt – Cloud Insights erkennt ihn und erstellt sofort eine NetApp Snapshot Kopie, um Ihre Daten zu schützen.

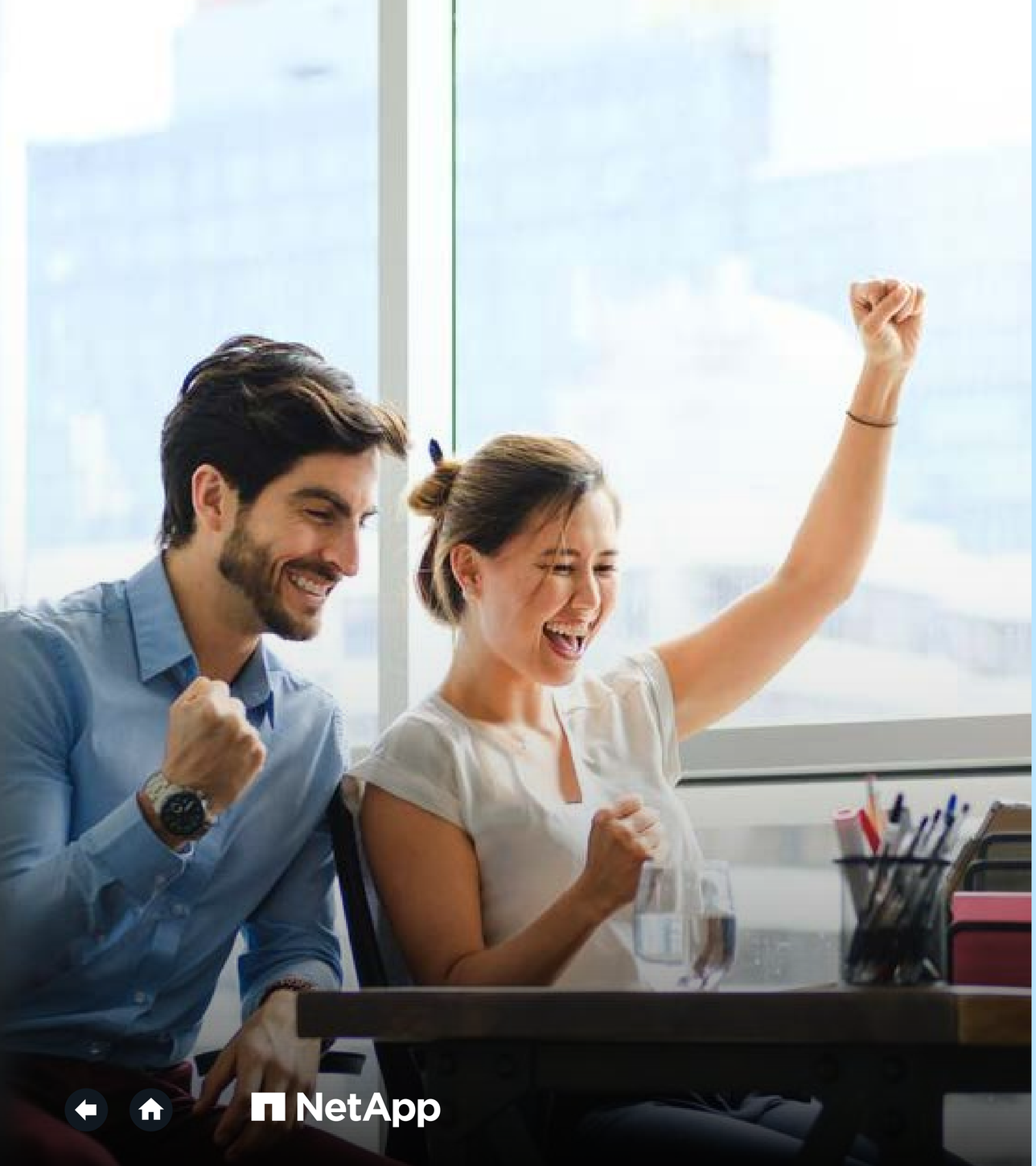
Ihr primäres Volume mag für Verschlüsselung anfällig sein, Ihre Snapshot-Kopien aber sind unveränderlich und ergeben in Kombination mit dem NetApp Cloud Backup eine sichere und effektive Datensicherungsstrategie.

Cloud Insights kann die Quelle des Angriffs identifizieren und das betroffene Benutzerkonto automatisch blockieren, um weitere Schäden und Datenexfiltration zu verhindern.

Und die Malware, die sich langsam durch Ihren File-Storage frisst? Keine Sorge. Dank des in ONTAP integrierten eigenständigen Ransomware-Schutzes wird eine Warnmeldung verschickt und die Workload-Aktivitäten sowie Datendichte werden von ONTAP mithilfe von maschinellem Lernen überwacht. Gleichzeitig wird durch den Alarm eine automatische Snapshot Kopie ausgelöst, die mehrere Wiederherstellungspunkte bereitstellt.

Phishing-Betrügereien und E-Mail-Anhänge sind nicht die einzigen Bedrohungen. Kompromittierte Administratoren-Zugangsdaten oder – noch schlimmer – ein Administrator, der seine Position missbraucht, können Ihre Daten ernsthaft in Gefahr bringen. NetApp ONTAP kann verhindern, dass ein einzelnes Administratorenkonto Schäden verursacht, indem es mit der neuen Multi-Administratoren-Verifizierung für wesentliche Aufgaben – wie beispielsweise das Löschen von Snapshot Kopien – die Genehmigung durch mehr als ein Administratorenkonto verlangt.





Wiederherstellen

Mit Cloud Data Sense und Cloud Insights können Sie intelligente Dateiforensik einsetzen, um zu ermitteln, welche Daten betroffen sind und wer dahintersteckt. Damit fokussieren Sie Ihre Datenwiederherstellung und verkürzen die Ausfallzeit.

Ihr IT-Team kann die Daten dann mithilfe der NetApp Tools schnell wiederherstellen – Terabytes in Minuten. Protokolle können zur weiteren Analyse in führende Sicherheitsinformations- und Eventmanagementsoftware (SIEM) exportiert werden.

Und trotz der Dramatik des Augenblicks kann das gesamte Team gelassen bleiben, weil es weiß, dass die Wiederherstellung der Daten zu keinem Zeitpunkt in Frage steht, da die NetApp SnapLock Software die Löschung von Daten durch sichere WORM-Dateisperrung verhindert.

Ein Daten-orientierter Cyberresilienzplan für jeden Speicherort

Gilt das zuvor beschriebene Szenario auch für IT-Teams, die Daten lokal managen? Oder in der Cloud? In einer hybriden Umgebung? Am Edge? Absolut.

Da Cyberresilienz ein von Grund auf Daten-orientierter Ansatz ist, werden Ihre Daten stets umfassend geschützt und sind immer resilient und verfügbar – unabhängig vom Speicherort: lokal, an Remote-Standorten oder in der Cloud. Die Cyberresilienzlösung von NetApp umfasst die gesamte Hybrid Cloud und lässt sich in jede gängige Public Cloud integrieren.

Optimale Nutzung vorhandener Investitionen

Die Daten-orientierte Cyberresilienzlösung von NetApp kann Sie in allen fünf Phasen des hier beschriebenen Plans unterstützen – auch wenn Ihr Unternehmen bereits in Cybersicherheitstools investiert hat. Denn die Funktionen der NetApp ONTAP Software lassen sich in bestehende Cybersicherheitslösungen integrieren, damit Sie Lücken schließen können, anstatt bei Null anzufangen.

Datensicherung	Benutzerverhalten	Audits und Protokollierung
Integration in NetApp ONTAP Snapshot und effiziente Replizierung mit SnapMirror	Integration in FPolicy APIs für eine intelligente Einsicht in Datei- und Benutzerverhalten	Integration in forensische Syslog-Analyse- oder SIEM-Tools
COMMVAULT, rubrik, VEEAM, CLEONDRIS, CATALOGIC, IBM, ProLion, VERITAS	Brainwave GRC, CLEONDRIS, ProLion, STEALTHbits, VARONIS, VERITAS, splunk>	Brainwave GRC, CLEONDRIS, ProLion, STEALTHbits, VARONIS, VERITAS, splunk>

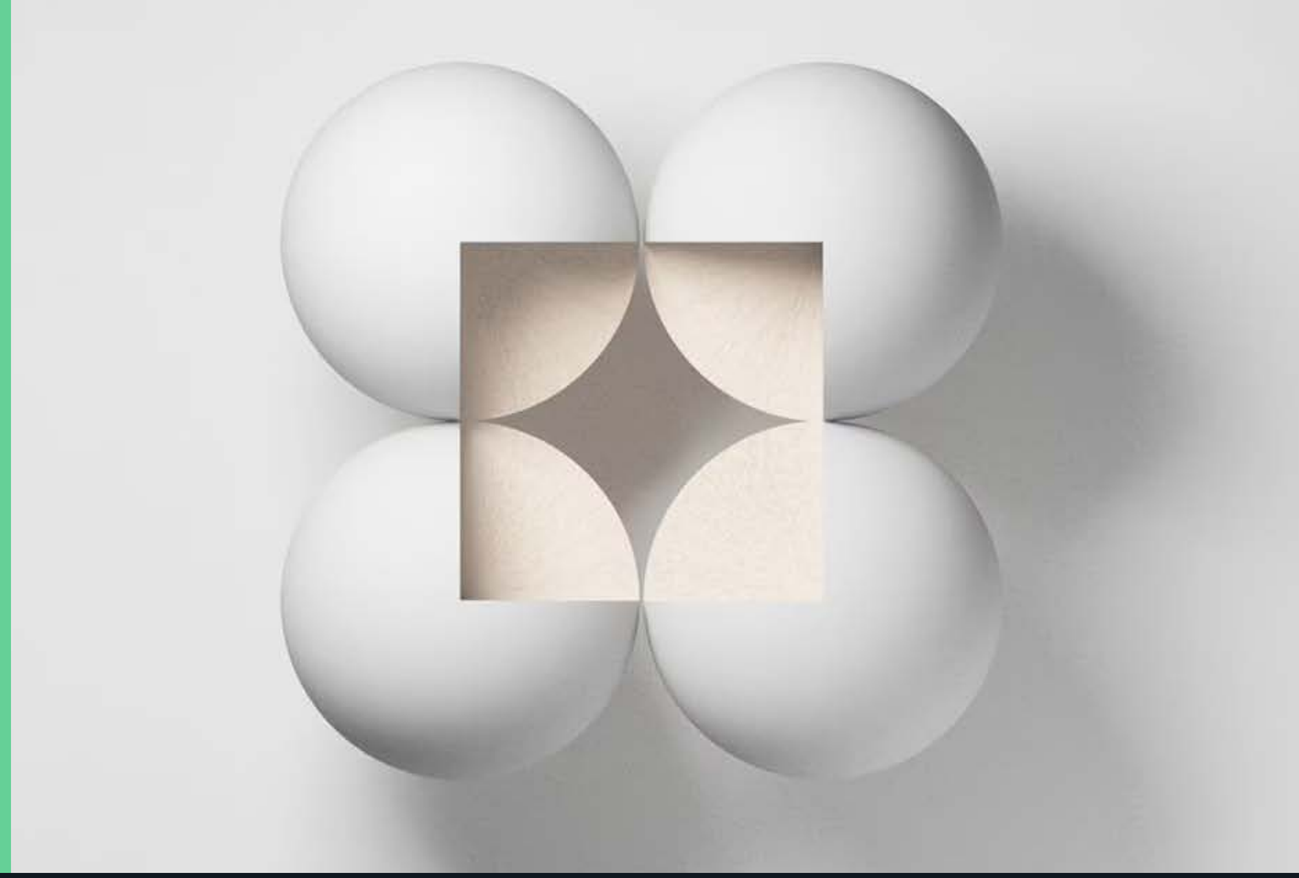
In nur wenigen Klicks zum Cyberresilienzplan

Wie können Kriminelle nicht aus der Welt schaffen, aber wir können die Cyberresilienz Ihres Unternehmens mit den richtigen Tools aktivieren.

Erfahren Sie mehr darüber, wie NetApp Ihnen dabei helfen kann, Ihren Daten-orientierten Cyberresilienzplan in die Tat umzusetzen.
netapp.com/de/cyber-resilience/

Klicken Sie auf die Links unten, um sich die neuesten Cyberresilienzlösungen, Blogs und Videos von NetApp anzusehen

- NetApp Cyberresilienzlösungen
- NetApp Datensicherungslösungen
- NetApp Ransomware-Lösungen
- NetApp Cyberresilienz-Blogs
- NetApp.tv Cyberresilienz-Videos



1. National Institute for Standards and Technology, „Developing Cyber-Resilient Systems“, Dezember 2021.
2. PBS NewsHour, „Why ransomware attacks are on the rise—and what can be done to stop them“, 8. Juli 2021.
3. Business Wire: „Ransomware Index Spotlight Report Reveals Steady Increase in Sophistication and Volume of New Ransomware Vulnerabilities and Families in Q3 2021“, 9. November 2021.
4. Statista: „Methods of organizations compromised by ransomware to get their encrypted data back as of February 2021“, 2021.
5. Sophos News, „The State of Ransomware 2021“, 27. April 2021.
6. Deloitte, „Double extortion incidents“, Oktober 2020.
7. Infosec: „NIST CSF: Implementing NIST CSF“, 19. Februar 2020.

Über NetApp
In einer Welt voller Generalisten beweist sich NetApp als Spezialist. Wir haben ein Ziel fest im Blick: Ihr Unternehmen darin zu unterstützen, Ihre Daten optimal zu nutzen. NetApp bringt die Datenservices, denen Sie vertrauen, in die Cloud und die Einfachheit und Flexibilität der Cloud in Ihr Datacenter. Selbst bei höchsten Ansprüchen lassen sich die branchenführenden NetApp Lösungen in unterschiedlichsten Kundenumgebungen und den weltweit führenden Public Clouds einsetzen.

Als Cloud- und Daten-orientierter Softwareanbieter stellt nur NetApp alle Technologien bereit, mit denen Sie Ihre eigene maßgeschneiderte Data Fabric aufbauen, Ihre Clouds vereinfachen, Ihre Public Clouds anbinden und so die richtigen Daten, Services und Anwendungen sicher bereitstellen können – immer und überall.

NetApp

+49 151 12055761