rubrik

Die Herausforderung unstrukturierter Daten lösen

E-Book

ANFANGEN →

ZURÜCK WEITER

Zusammenfassung

Wenn Sie digitale Anwendungen haben, haben Sie auch unstrukturierte Daten. Und zwar Petabytes davon. Aber wissen Sie, was Sie da eigentlich sammeln?

Wahrscheinlich kennen Sie schon die drei wichtigen Merkmale von Daten, die drei Vs: **Vielfalt (Variety), Schnelligkeit** (Velocity) und **Volumen (Volume)**.

In diesem E-Book beschäftigen wir uns mit dem vergessenen vierten Merkmal, dem vierten V: **Wert** (Value). Wir besprechen fünf wichtige Schritte zum Erstellen einer resilienten Strategie für unstrukturierte Daten und erläutern, wie Rubrik Ihnen helfen kann, Ihre unstrukturierten Daten zu verwalten und zu schützen.

Sind Sie bereit, die unergründliche Welt der unstrukturierten Daten zu erkunden?

Los geht's!

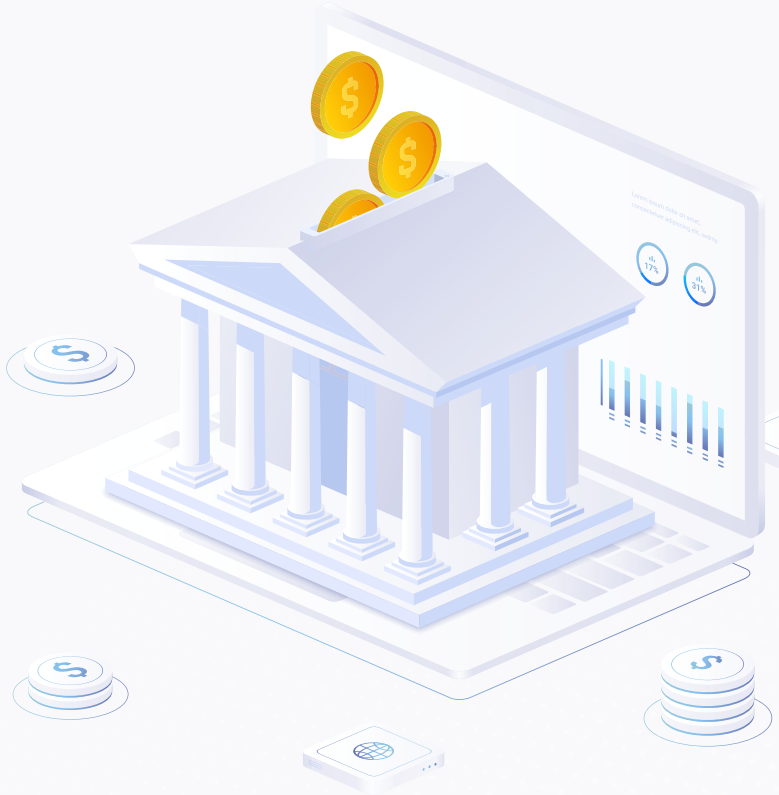
ZURÜCK WEITER

Die Geschichte der MegaBucks-Bank

Sie sind der CISO der MegaBucks-Bank, die extrem wohlhabende Kunden bedient. Sie verarbeiten täglich eine riesige Menge an Daten, von denen viele sensibel sind: Informationen zu Kundenkonten, Sozialversicherungsnummern, andere personenbezogene Daten und vieles mehr. Das ist Ihr täglich Brot.

Sie wissen, dass es extrem wichtig ist, diese Informationen zu schützen, und haben daher viel in Ihre Datensicherheitsstrategie investiert: Sie haben erstklassige Datenbanken mit modernstem Schutz, einen soliden Plan für Geschäftskontinuität und Disaster Recovery sowie ein Team, das zu den Besten in der Branche gehört, wenn es darum geht, tagtäglich Cyber-Angriffe abzuwehren. Sie sind für jeden Fall ziemlich gut abgesichert, oder?

Nicht so schnell!



ZURÜCK WEITER

Heute:

Zwei Mitarbeiter haben aus der Datenbank die vollständige Kontonummer eines Kunden entnommen und im Chat genannt.

Jemand aus dem M&A-Team hat per E-Mail eine Kopie eines drei Jahre alten Vertrags, der geschützte Informationen enthält, an einen Kollegen geschickt.

Ihre Kundendienstmitarbeiter haben Anrufe von Kunden angenommen, die allesamt aufgezeichnet wurden; in vielen davon wurden personenbezogene Daten genannt.

Außerdem haben Sie gerade erfahren, dass ein Cyber-Krimineller sich Zugriff auf Ihre Systeme verschafft hat.

Jetzt haben Sie ein Problem. Denn bei jeder dieser Interaktionen wurde eine Datei generiert, die jetzt unorganisiert und schwer zu verwalten ist, höchstwahrscheinlich sensible Daten enthält und vermutlich nicht gut genug geschützt irgendwo in Ihren unstrukturierten Daten verborgen ist.

Bis Sie diese gefunden haben, kann sehr viel Zeit verstreichen.

Vielfalt, Schnelligkeit, Volumen und … Wert?

Das war ein Albtraumszenario, oder? Aber keine Sorge! In diesem E-Book helfen wir Ihnen, eine Strategie zum Verwalten und Schützen Ihrer unstrukturierten Daten zu entwickeln, um Ihnen das Kopfzerbrechen zu ersparen, das dieses Szenario unserem fiktionalen CISO der MegaBucks-Bank bereiten dürfte.

Jeder, der in den letzten 20 Jahren in der Branche tätig war, kennt die drei wichtigen Kriterien für Daten, nämlich Vielfalt, Schnelligkeit und Volumen (English: Three V's: **Variety, Velocity, Volume).** Diese drei Vs wurden im Jahr 2001 von Doug Laney definiert[1] und bezeichnen Eigenschaften der Daten, die ein Unternehmen sammelt.[2]

VARIETY (VIELFALT)

Bezieht sich auf die **unterschiedlichen Arten** von Daten, die Sie sammeln. Wenn Sie über alle möglichen Arten von Informationen verfügen, können Sie sich ein umfassenderes Bild machen, aber Sie brauchen ein System, das folgende Herausforderungen bewältigen kann:

- strukturierte und unstrukturierte Daten
- unterschiedliche Formate
- unterschiedliche Nomenklaturen

VELOCITY (SCHNELLIGKEIT)

Bezieht sich darauf, **wie schnell** Sie Daten generieren und verarbeiten. Bei Geschäftsdaten ist Schnelligkeit das A und O.

- Eine B2C E-Commerce-Website, die innerhalb von einer Sekunde lädt, hat eine E-Commerce-Konvertierungsrate, die 2,5-mal höher ist als die einer Website, die innerhalb von 5 Sekunden lädt.[3]
- Etwa ein Drittel aller Amerikaner achten auf einen guten Schutz vor Betrug, wenn sie sich für eine Bank entscheiden.[4] Finanzinstitute müssen Daten also in Echtzeit verarbeiten, um betrügerische Aktivitäten zu verhindern.
- Hacker sind schnell und beharrlich. 99 % der IT- und Sicherheitsverantwortlichen wurden im Jahr 2022 auf mindestens einen Cyber-Angriff aufmerksam gemacht, die durchschnittlich in 52 Fällen erfolgreich waren.[5]

VOLUME (VOLUMEN)

Bezieht sich auf die **Menge** an Daten, die Sie sammeln. Kleiner Tipp: Es ist eine große Menge. Hier ein paar wirklich erstaunliche Zahlen aus unserem Rubrik Zero Labs-Bericht zum Stand der Datensicherheit 2023:

- Ein typisches Unternehmen hat durchschnittlich 239,9 Backend-Terabyte (BETB) an Daten.
- Diese Zahl ist für Unternehmen in bestimmten Branchen noch höher:
  - > Telekommunikation: 442,6
  - > IT und Technologie: 398,9
  - > Versicherung: 301,5

Sie müssen also Unmengen an Daten in allen möglichen Formaten sehr schnell verwalten.

Das ist aber noch längst nicht alles.

Wir bei Rubrik vertreten den Standpunkt, dass es ein vergessenes viertes V gibt, das Sie berücksichtigen ***müssen***, wenn Sie Ihre Daten erfolgreich verwalten und schützen möchten: **den Wert von Daten (Value)**.

VALUE (WERT)

Bezieht sich darauf, **wie nützlich** die von Ihnen gesammelten Daten für Ihr Unternehmen sind. Sie müssen wissen, was Sie haben, warum es wichtig ist und wo es gespeichert ist. Denn Sie sammeln eine Unmenge an geschäftskritischen Daten – das, was wir als die „Kronjuwelen" Ihres Unternehmens bezeichnen. Erinnern Sie sich an die 239,9 BETB an Daten? Viele dieser Daten sind sensibel.

- Global gesehen verwaltet ein typisches Unternehmen durchschnittlich 24,8 Millionen sensible Dateien.[6]
- Das von Rubrik gesicherte Unternehmen mit den meisten sensiblen Daten verfügt über mehr als 1,3 Milliarden sensible Datensätze.[7]

Wenn Ihr Unternehmen wächst, wächst auch die Menge an sensiblen Daten weiter an,

[1] 3D Data Management: Controlling Volume, Velocity, and Variety
[2] Big Data: The 3 V's Explained; 3 V's (volume, velocity and variety)
[3] Site Speed is (Still) Impacting Your Conversion Rate
[4] New FICO Survey: Americans Value Financial Fraud Prevention More Than Banking Customer Experience
[5] Rubrik Zero Labs, Bericht zum Stand der Datensicherheit 2023
[6] ebd.
[7] ebd.

24,8 MILLIONEN

durchschnittliche Anzahl sensibler Dateien in einem typischen Unternehmen

>1,3 MILLIARDEN

sensible Daten in einem einzelnen von Rubrik gesicherten Unternehmen

ZURÜCK WEITER

Fazit: Der Wert Ihrer Daten wird darüber entscheiden:

was Sie schützen

wie häufig Sie ein Backup machen

wie lange Sie Ihre Daten aufbewahren

wie Sie sie im Ruhezustand sichern, um zu vermeiden, dass Sie verschlüsselt oder exfiltriert werden oder dass Sie ein Lösegeld dafür zahlen müssen

Wahrscheinlich kennen Sie den Wert Ihrer strukturierten Daten bereits recht gut. Sie tun alles, was Sie können, um sie gut zu verwalten und zu schützen.

Aber wie sieht es mit Ihren unstrukturierten Daten aus? Können Sie derzeit herausfinden, was in Ihren unstrukturierten Daten enthalten ist, und die Resilienz Ihrer Daten im Ruhezustand steigern, um besser vor Exfiltration geschützt zu sein?

Bei den meisten Datenverantwortlichen, denen wir begegnen, lautet die ehrliche Antwort: „Nein, nicht wirklich“.

Die gute Nachricht: Wir können Ihnen helfen.

ZURÜCK WEITER

In fünf Schritten zu einer robusten Strategie für unstrukturierte Daten

Wir wissen, dass die überwiegende Mehrheit Ihrer unstrukturierten Daten weder sensible Informationen enthält noch für einen Wettbewerbsvorteil sorgt und Ihnen auch nicht hilft, Ihr Unternehmen am Laufen zu halten. Bei den meisten dieser Dateien handelt es sich also nicht um Kronjuwelen Ihres Unternehmens.

KERNPUNKT 1 – Ihre unstrukturierten Daten ***enthalten*** die Informationen, die Sie als Ihre „Kronjuwelen" bezeichnen würden.

KERNPUNKT 2 – Hacker ***wissen***, dass Ihre unstrukturierten Daten wahrscheinlich wichtige Informationen enthalten. Deshalb haben sie es gezielt auf Backups abgesehen. Böswillige Akteure ***melden sich*** inzwischen bei Ihrem Netzwerk an, anstatt es zu hacken. Sie haben heutzutage Benutzerberechtigungen für Ihre unstrukturierten Daten.

KERNPUNKT 3 – Außerdem werden in den nächsten fünf Jahren laut IDC ***90 % Ihrer Daten*** unstrukturiert sein.[7]

Wenn Sie also auf das alte Konzept „Snapshot und Replikation" oder NDMP setzen, sind Sie zum Scheitern verurteilt. Sie wissen nicht, welche Informationen wo gespeichert sind, und könnten unbeabsichtigt Malware in Ihre Backups und Archive einschleusen.

Es ist nicht mehr ratsam, unstrukturierte Daten einfach zu sichern und auf das Beste zu hoffen. Denn dabei handelt es sich um eine Daten***kontinuitäts***strategie, nicht um eine Daten***resilienz***strategie. Und im Zeitalter der Cyber-Kriminalität gilt: ***Resilienz ist alles***.

Die folgenden fünf Schritte werden Ihnen helfen, Ihre unstrukturierten Daten zu verstehen, zu verwalten und zu schützen.

Tauchen wir ein.

[7] IDC, Meeting the New Unstructured Storage Requirements for Digitally Transforming Enterprises

ZURÜCK WEITER

Schritt 1: Sie müssen Ihre Daten kennen

Daten wachsen mit schwindelerregender Geschwindigkeit. Wir bei Rubrik schätzen, dass das Gesamtvolumen an Daten, die ein typisches Unternehmen sichern muss, in den nächsten fünf Jahren um das **7-Fache** anwachsen wird.[8]

Dieser erste Schritt wird Ihnen dabei helfen, Ihren Bestand an unstrukturierten Daten so zu erfassen, dass Sie die Daten effektiv bewerten und schützen können.

SIE MÜSSEN WISSEN, WER DERZEIT für die Erfassung und Bewertung von Daten zuständig ist. Man ist schnell versucht zu denken, dass dies die Aufgabe eines Speicher- und/oder Cloud-Administrators ist, aber das sollte es nicht sein. Diese Administratoren sind nicht dafür zuständig, zu wissen, welche konkreten Daten sie verwalten und woher diese Daten kommen. Für die Erfassung und Evaluierung sollten die Dateneigentümer in Ihrem gesamten Unternehmen verantwortlich sein. Aber wer ist derzeit zuständig?

SIE MÜSSEN VERSTEHEN, WO DATEN HERKOMMEN. Wissen Sie über jede Anwendung in Ihrem Unternehmen Bescheid, die Daten generiert, oder kann die Schatten-IT nach Belieben schalten und walten? Erstellen Sie eine vollständige Liste. **Fragen Sie dann:** Sind alle Ursprungspunkte Malware-frei? Es ist extrem wichtig, dass die Generierungspunkte für alle wichtigen Datenbereiche bekannt sind, bewertet werden und sauber sind. **Prüfen Sie auch:** Sind Dateneigentümer an den Entscheidungen über die Sicherheit ihrer Daten beteiligt und/oder treffen sie diese selbst? Oder werden diese Entscheidungen von Speicher- und Backup-Administratoren getroffen?

[8] Rubrik Zero Labs, Bericht zum Stand der Datensicherheit 2023

Schritt 2: Sie müssen Ihre Daten validieren

Jetzt ist es an der Zeit, Ihren Datenbestand zu analysieren und Richtlinien festzulegen.

Verschaffen Sie sich einen Überblick darüber, **was gespeichert ist**, und bringen Sie in Erfahrung, wie **kritisch** dieses Material für Ihr Unternehmen ist. Druckerprotokolle? Wahrscheinlich nicht unverzichtbar. Aber was ist mit E-Mails? Was wäre, wenn E-Mails nicht mehr verfügbar wären? Oder was wäre, wenn Sie interne Nachrichten oder Sensordaten verlieren würden? Wenn Sie wissen, welche Anwendungen wichtige Daten produzieren, können Sie leichter eine passende Schutzstrategie entwickeln.

Bestimmen Sie **zwei Schlüsselrollen** in Ihrem Unternehmen und legen Sie deren Workflows und Aufgaben fest. Beide Rollen bieten Verantwortlichkeit und Fachwissen im Validierungsprozess und unterstützen Sie bei der Umsetzung Ihrer Strategie für die Ausfallsicherheit unstrukturierter Daten.

CHAMPION IN DER FÜHRUNGSETAGE

In nur 54 % aller externen Unternehmen gibt es eine einzelne Person in der Unternehmensführung, die für Daten und ihren Schutz zuständig ist. Aber 98 % der externen Unternehmen glauben, dass bei ihnen derzeit deutliche Herausforderungen bezüglich der Datentransparenz bestehen.[9] Wenn Ihnen das bekannt vorkommt, schlagen Sie doch eine Brücke, indem Sie Daten zur Chefsache machen. Einen Champion in der Chefetage zu ernennen wird Ihnen dabei helfen, Ihre Datenschutzstrategie zu optimieren und durchzusetzen, und es wird außerdem Mitarbeitern und Kunden sowie anderen Stakeholdern zeigen, dass Ihnen Ihre Daten wichtig sind, egal wo sie gespeichert sind.

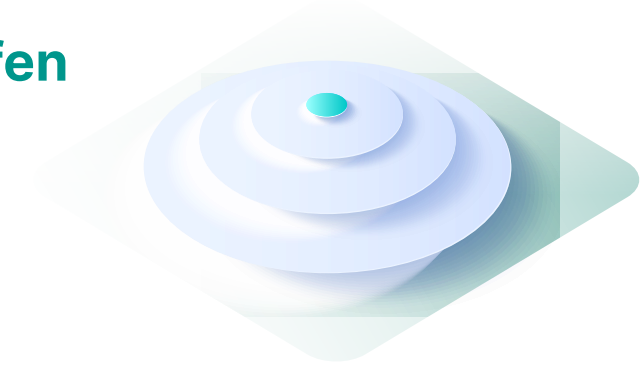
DATA CUSTODIANS

Wenn Speicher- und Cloud-Administratoren nicht die Dateneigentümer sind, wer sollte es dann sein? Wir empfehlen Datenexperten – Data Custodians –, die in Teams in Ihrem Unternehmen integriert und für das gesamte Information Lifecycle Management (ILM) ihrer Teams verantwortlich sind. Von der Datengenerierung über die Speicherung bis hin zur Löschung verstehen sie, warum diese Daten wichtig sind, stellen sicher, dass sie sauber sind, und schützen sie entsprechend.

[9] Rubrik Zero Labs, Bericht zum Stand der Datensicherheit 2023

ZURÜCK WEITER

Schritt 3: Sie müssen Ihre Anwendungen einstufen



Es ist an der Zeit, die Anwendungen einzustufen, die Ihre Daten generieren.

Dadurch können Sie einen Workflow standardisieren und verwalten, wo und wie Daten gespeichert und geschützt werden. Wie Sie Ihre Anwendungen einstufen, ist ganz von Ihrem Unternehmen abhängig. Sie wissen selbst am besten, welche Daten für Ihr Unternehmen besonders wichtig sind.

OBERE STUFE (KRITISCH)

Die Daten, die von diesen Anwendungen generiert werden, sind sehr wichtig. Vielleicht können diese Dateien nicht nachgestellt werden, wie z. B. Patientendaten aus bildgebenden Verfahren oder zeitpunktgenaue Sensor- und Navigationsdaten. Es könnten Dateien sein, die Sie zu Compliance- oder regulatorischen Zwecken aufbewahren müssen. Wahrscheinlich fallen auch Ihre E-Mails in diese Kategorie - zum einen, weil sie sensible Informationen enthalten können, und zum anderen, weil Sie Ihr E-Mail-Programm am Laufen halten müssen. Auf dieser Stufe sollten die strengsten SLA-Richtlinien gelten, mit robustem Schutz und Ausfallsicherheit, damit Sie im Falle einer Datenkompromittierung schnell auf ein aktuelles Backup zurückgreifen können.

Fazit: Wenn die Kompromittierung einer bestimmten Anwendung zu erheblichen Beeinträchtigungen führen würde, gehört diese Anwendung in diese Kategorie.

> Ihre unstrukturierten Daten kommen aus allen Bereichen Ihres Unternehmens: E-Mail-Clients, Sensoren, Social-Media-Programme, Drucker, Textverarbeitungs- und Präsentationssoftware... im Grunde aus jedem digitalen Programm, das Sie ausführen.

ZURÜCK WEITER

MITTLERE STUFE (WICHTIG)

Daten, die von Anwendungen auf dieser Stufe generiert werden, sind für Ihr Geschäft zwar wichtig, aber nicht kritisch. Darunter können Dateien wie Analysen fallen, die beim Durchführen von Verbesserungen helfen, oder (nicht sensible) Berichte, die für Ihre Teams nützlich sind. Wenn Sie diese Daten bei einem Cyber-Angriff verlieren würden, könnten Sie sie wiederherstellen und mit Ihrer Arbeit fortfahren.

Fazit: Anwendungen auf dieser Stufe generieren Daten, die nützlich, aber für Ihren täglichen Betrieb und für anhaltende Stabilität nicht unverzichtbar sind.

UNTERE STUFE (ALLES ANDERE)

Anwendungen auf der unteren Stufe generieren Daten, die für Ihr Unternehmen kaum einen oder gar keinen geschäftlichen Wert haben. Wenn Ihr Unternehmen so ist wie die meisten, gehören auf diese Stufe wahrscheinlich Ihre Drucker- und Social-Media-Anwendungen. Daten auf dieser Stufe müssen nicht besonders stark geschützt werden. In Ihrer ILM-Strategie werden sie vermutlich archiviert und von der Quelle entfernt.

Fazit: Wenn ein Hacker Daten aus einer Anwendung kompromittieren könnte und dies kaum eine oder gar keine Geschäftsunterbrechung bewirken würde, gehört die Anwendung in diese Kategorie.

ZURÜCK WEITER

Schritt 4: Sie müssen Ihre Datenstrategie festlegen und implementieren

Nach all dieser Vorarbeit ist es nun endlich an der Zeit, sich mit dem Kern Ihrer Strategie und deren Umsetzung zu befassen. Legen Sie anhand der gesammelten und kategorisierten Informationen Ihre Datenregeln fest. Kategorisieren Sie die Personen, Prozesse und Technologien im Zusammenhang mit den Anwendungsstufen, die Sie in Schritt 3 bestimmt haben. Legen Sie also für Anwendungen der oberen, mittleren und unteren Stufe in jedem Team in Ihrem gesamten Unternehmen Folgendes fest:

Wer ist in jedem Team der Data Custodian, der für das Verwalten der Anwendungsdaten dieses Teams verantwortlich ist?

Wie häufig sollten Daten von jedem Anwendungstyp gesichert werden? Wann sollten Daten archiviert werden? Wann können sie deaktiviert (gelöscht) werden? Denken Sie daran, dass auch hier behördliche und rechtliche Anforderungen gelten können, die in Ihrer Aufbewahrungsrichtlinie zum Tragen kommen müssen.

Wie sieht Ihr Wiederherstellungsverfahren für jede Stufe im Falle eines Cyber-Angriffs aus?

Wo in Ihrer Infrastruktur sollten Daten von der jeweiligen Anwendung gespeichert werden?

- Wie viele davon sind Backup-Daten, wie viele werden archiviert?
- Können Sie es verkraften, die Daten, die Sie archivieren (und die in der Regel nicht gesichert werden und daher im Falle eines Cyber-Angriffs nicht wiederhergestellt werden könnten), zu verlieren?
- Gibt es Vorschriften, Gesetze oder Richtlinien (z. B. HIPAA oder CCPA), die beachtet werden müssen, wenn es um die Frage geht, wohin die Daten gesendet werden sollen?

Wie wird der Schutz für die Daten der unterschiedlichen Arten von Anwendungen gehandhabt?

> Vergessen Sie nicht: Nachdem Sie die Regeln festgelegt haben, ist Ihr Data Custodian für den Daten-Lebenszyklusprozess aus Verwaltung, Schutz und Sicherung **ZUSTÄNDIG**. Diese Person ist am engsten mit den Daten vertraut, die generiert werden, und muss dafür sorgen, dass sie sicher an den richtigen Speicherort gelangen.

ZURÜCK WEITER

Schritt 5: Sie müssen Ihre Strategie pflegen und überwachen

Sie haben es geschafft! Sie wissen, woher Ihre unstrukturierten Daten kommen, wer sie verwaltet und welchen Wert sie für Ihr Unternehmen haben, und Sie haben ein Verfahren entwickelt, um diese Daten sicher zu verwahren und in Ihrer Infrastruktur entsprechend unterzubringen.

Jetzt bleibt nur noch eins: die langfristige Pflege und Überwachung Ihrer Strategie für unstrukturierte Daten. Dies ist ein entscheidender Schritt, den Sie nicht auf die leichte Schulter nehmen sollten. Denn Ihre Daten wachsen exponenziell. Es kommen ständig neue Anwendungen hinzu. Mitarbeiter kommen zu Ihren Teams hinzu oder verlassen diese. Und die Cyber-Kriminalität nimmt immer weiter Fahrt auf.

Hier sind vier konkrete Maßnahmen, die Sie ergreifen können, um dafür zu sorgen, dass Ihre Strategie effektiv und resilient bleibt.

NUTZEN SIE DATENTRANSPARENZ, UM SENSIBLE DATEN PROAKTIV REGELMÄSSIG ZU ÜBERPRÜFEN

Machen Sie sich mit Datenreduktion das Leben einfacher. Dazu könnte gehören, dass sensible Daten entfernt werden, auf die im letzten Jahr kein Benutzer zugegriffen hat, es könnten doppelte Datenkopien ermittelt und gelöscht werden oder es könnten Daten in Benutzerfreigaben für Mitarbeiter/Kunden/Partner, die im letzten Jahr ausgeschieden sind, entfernt werden. Dies gilt auch für Daten, die mehrmals in verschiedenen Datenspeichern in einem Unternehmen vorhanden sind.

ZURÜCK WEITER

HALTEN SIE AUSSCHAU NACH AUFFÄLLIGKEITEN, UM DATENRESILIENZ SICHERZUSTELLEN

Überwachen Sie Ihre Daten mithilfe von maschinellem Lernen auf ungewöhnliche Hinzufügungen, Löschvorgänge oder Verschlüsselungen. Stellen Sie sicher, dass Benutzer den Grad an Zugriff haben (d. h. Lesezugriff, Bearbeitungszugriff), den sie für ihre Arbeit benötigen. Verwenden Sie eine Lösung, die Sie proaktiv auf potenziell böswillige Aktivitäten in Ihren Backup-Daten während eines Ransomware-Angriffs hinweist.

GEHEN SIE BEIM DATENWACHSTUM BEWUSST VOR

Tun Sie, was Sie können, um das Wachstum der Daten, die Sie verwalten müssen, zu verlangsamen. Legen Sie beispielsweise fest, dass das Wachstum in der Cloud nicht mehr als 50 % des Wachstums in der gesamten Umgebung ausmachen darf, löschen Sie Daten auf Basis festgelegter Richtlinien oder platzieren Sie sensible Daten nur in einer Enklave.

ÜBERARBEITEN SIE IHRE STRATEGIE IMMER WIEDER

Ihre Strategie muss mit Ihrem Unternehmen gemeinsam wachsen. Wir empfehlen Ihnen, sie so oft wie möglich zu überprüfen (mindestens zweimal im Jahr), um sicherzustellen, dass Ihre Teams die von Ihnen festgelegten Richtlinien einhalten und Sie Cyber-Bedrohungen aktiv einen Schritt voraus bleiben.

Herzlichen Glückwunsch!

Sie sind erfolgreich von einer **Kontinuitäts**strategie für unstrukturierte Daten zu einer **Resilienz**strategie für unstrukturierte Daten übergegangen.

ZURÜCK WEITER

Rubrik: Ihr zuverlässiger Partner bei allen Herausforderungen

Nachdem Sie nun die Schritte durchgelesen haben und entschlossen sind, die Probleme zu vermeiden, mit denen unser MegaBucks-Bank-CISO konfrontiert war, lassen Sie uns darüber sprechen, wie Rubrik Ihnen helfen kann.

Rubrik NAS Cloud Direct ist die moderne Lösung zum Verwalten und Schützen Ihrer unstrukturierten Daten. Diese zustandslose VM lebt in der SaaS-Kontrollebene von Rubrik, kann nativ in der Cloud oder im Rechenzentrum eingesetzt werden und ist in der Lage, Milliarden von Dateien zu scannen – jeden beliebigen Datei-Workload und zu jeder Zeit. Sie basiert auf Zero-Trust-Prinzipien und ist bereit für Ihre größten Herausforderungen im Bereich unstrukturierter Daten:

VOLUMEN

Sie haben Milliarden Dateien und es werden jeden Tag mehr? Kein Problem.

- Schützen Sie Daten im Petabyte-Bereich über alle NAS-Technologien hinweg mit hocheffizientem Scannen, Indizieren und Verschieben von Daten.

GESCHWINDIGKEIT

Sie müssen Dateien verschieben und Backups erstellen, ohne dass es in Ihrer Produktionsumgebung zu Unterbrechungen kommt? Das können wir machen.

- Scannen, indizieren und verschieben Sie NAS-Daten in parallelen Datenströmen, um den Netzwerkdurchsatz zu maximieren.
- Eliminieren Sie negative Auswirkungen auf Benutzer mit dynamischer Drosselung.
- Verkleinern Sie Backup-Zeitfenster dramatisch und steigern Sie die betriebliche Effizienz mit wirklich dauerhaft inkrementellen Backups.

EFFIZIENZ

Möchten Sie Komplexität ausräumen und Ihre Prozesse optimieren? Wir können Ihnen dabei helfen.

- Nutzen Sie Integration mit SecOps-Tools wie SIEM/SOAR zum Fördern der Zusammenarbeit zwischen ITOps- und SecOps-Teams, um Bedrohungen schnell zu erfassen und zu identifizieren.
- Archivieren Sie Daten von jeder NAS-Quelle direkt auf ein beliebiges lokales Ziel, auf eine Cloud oder auf privaten Speicher, basierend auf den von Ihnen definierten Richtlinieneinstellungen.

VERWALTUNG

Suchen Sie nach einer Möglichkeit, Ihre unstrukturierten Daten zu verwalten, anstatt ein wildes Durcheinander hinzunehmen? Auch hier können wir helfen.

- Suchen und verorten Sie bestimmte Dateien mit Leichtigkeit und rufen Sie jede zuvor geschützte Version Ihrer NAS-Dateidaten ab.
- Erkennen Sie durch Überwachung sensibler Daten, wo sich sensible Daten befinden, und gewinnen Sie Einblicke in den Zugriffssicherheitsstatus, um das Risiko einzugrenzen.
- Identifizieren Sie schnell veraltete oder wachsende Datensätze mit NAS CD Data Discover, damit sie archiviert, migriert oder deaktiviert werden können.

SICHERHEIT

Möchten Sie über erstklassigen Schutz verfügen? Dafür sind wir da.

- Sichern Sie NAS-Daten mit verschlüsselten, unveränderlichen Backups im Ruhezustand, einschließlich der Isolierung von Anmeldedaten für höhere Cyber-Resilienz.
- Nutzen Sie individuell entwickelte NFS- und SMB-Clients, die speziell für die schnelle Datensicherung im großen Maßstab entwickelt wurden.

RESILIENZ

Sind Sie Opfer eines Cyber-Angriffs geworden und müssen den Betrieb schnell wieder zum Laufen bringen? Wir sind für Sie da.

- Ermitteln Sie mit der Anomalie-Erkennung von Rubrik schnell, welche Anwendungen und Dateien von Ransomware betroffen sind, und machen Sie sie ausfindig.
- Stellen Sie betroffene NAS-Daten mithilfe der Auswirkungsanalyse der Anomalie-Erkennung von Rubrik präzise wieder her.
- Automatisieren Sie Wiederherstellungs-Workflows – z. B. die Massenwiederherstellung von NAS-Daten – für die Produktion, einschließlich Aufgaben nach der Wiederherstellung, um diesen Prozes zu beschleunigen und die Ausfallzeiten zu verringern.

Mit Rubrik NAS Cloud Direct können Sie Ihre unstrukturierten Daten zuversichtlich besser verwalten und schützen.

Erleben Sie es in Aktion.

ZURÜCK WEITER

Rubrik NAS Cloud Direct: Dividenden für einen Finanzdienstleister

Akuna Capital, ein Hedgefonds mit Sitz in New York und Chicago, betreibt ein Hochfrequenzhandelssystem, das 400 TB an Daten speichert – das sind zwei Milliarden Dateien.

Beim Hochfrequenzhandel kann ein Handel innerhalb von Mikrosekunden erfolgen. Es zählt also jeder Augenblick. Bevor Rubrik ins Spiel kam, waren die von Akuna Capital verwendeten Backup-Lösungen nicht in der Lage, die Daten des Unternehmens schnell und ohne Leistungsunterbrechung zu scannen und zu schützen. Dieses langsame und ineffiziente Backup hätte zu einem ernsthaften Risiko für die Geschäftstätigkeit des Unternehmens werden können.

Mit Rubrik NAS Cloud Direct, das in Pure Flashblade integriert ist, kann Akuna Capital nun 400.000 Dateien pro Sekunde scannen und Backups in weniger als zwei Stunden pro Tag abschließen. Und das Beste: Das Unternehmen ist vor Cyber-Bedrohungen geschützt.

Haben wir Sie überzeugt? Es freut uns, das zu hören!

Revolutionieren Sie die Datensicherheit in Ihrem Unternehmen noch heute mit Rubrik NAS Cloud Direct.

MEHR ERFAHREN →

rubrik