Technische Prüfung

Schnelle und effiziente Wiederherstellung nach einem Ransomware-Angriff mit der unveränderlichen Architektur der Rubrik-Datenverwaltungsplattform

Datum: Mai 2020 **Autoren:** Vinny Choinski, Senior Validation Analyst, und Christophe Bertrand, Senior Analyst

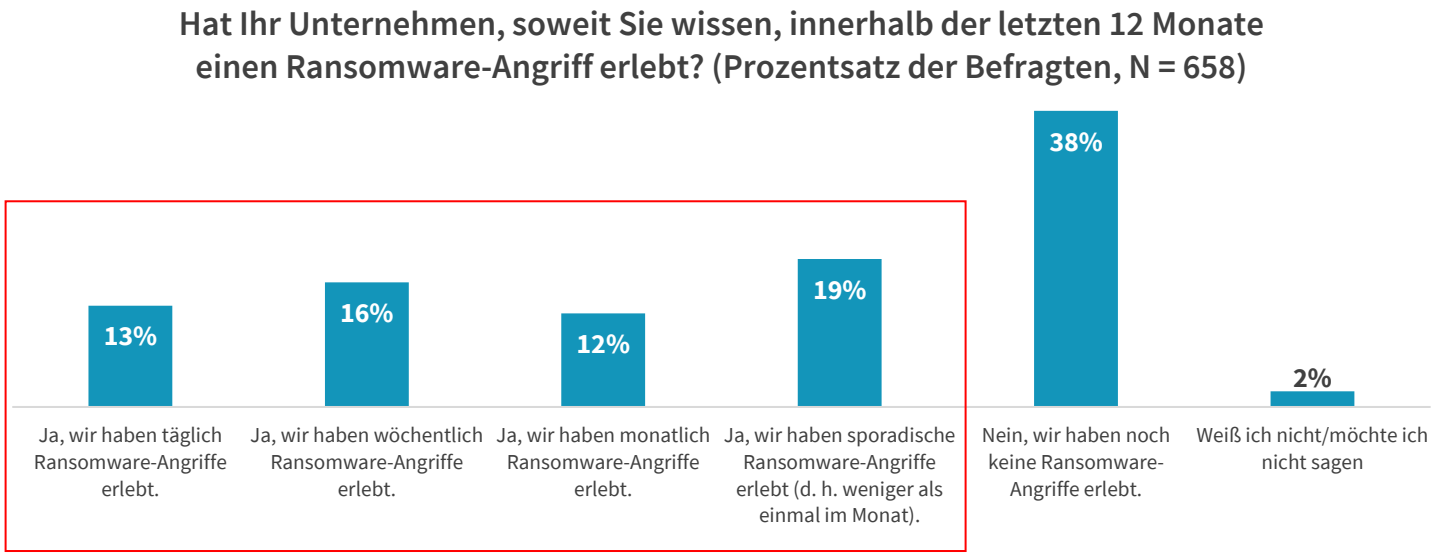
Zusammenfassung

In dieser technischen Prüfung der ESG werden praktische Analysen und Überprüfungen der Rubrik-Architektur dokumentiert. Wir untersuchen, wie Rubrik Daten vor Ransomware-Angriffen schützt und den Wiederherstellungsprozess nach dem Angriff mit seiner unveränderlichen Architektur beschleunigt.

Die Herausforderungen

Ransomware ist allgegenwärtig und stellt eine ernsthafte Bedrohung für Unternehmen jeder Größe dar. Laut FBI zahlen Unternehmen jährlich mehr als 1 Milliarde US-Dollar an Ransomware-Kriminelle, um ihre Daten wiederzuerlangen. ESG hat vor Kurzem seine jährliche Umfrage zu geplanten Technologieausgaben unter 651 leitenden IT-Entscheidungsträgern aus mittelgroßen (d. h. 100 bis 999 Mitarbeiter) und großen Unternehmen (d. h. 1.000 oder mehr Mitarbeiter) in Nordamerika und Westeuropa abgeschlossen.[1] Abbildung 1 zeigt, dass 40 % der Unternehmen keinen Ransomware-Angriff erlitten haben (oder sich nicht darüber äußern möchten), die meisten Unternehmen jedoch 2019 Probleme mit Ransomware verzeichnet haben. Tatsächlich gaben 60 % an, dass sie in einem Zeitraum von 12 Monaten Opfer eines Ransomware-Angriffs waren, wobei 29 % berichten, dass die Angriffe wöchentlich (oder sogar häufiger) stattfanden. Interessanterweise müssen sich 13 % täglich Ransomware-Bedrohungen stellen! Bei Unternehmen, die einen Mangel an Fachkenntnissen im Bereich Cybersicherheit meldeten, lag die Wahrscheinlichkeit, Ransomware in den letzten 12 Monaten zum Opfer zu fallen, deutlich höher (67 % im Vergleich zu 54 %). Die Studie von ESG zu den geplanten Technologieausgaben 2020 zeigt außerdem, dass 62 % der Unternehmen die Ausgaben für Cybersicherheit 2020 erhöhen werden. Es ist daher davon auszugehen, dass Bedenken in Bezug auf Ransomware in vielen Fällen Ransomware zumindest zur Entscheidung beigetragen haben, stärker in die Sicherheit zu investieren.

Abbildung 1. Ransomware-Angriffe im Jahr 2019



Quelle: Enterprise Strategy Group

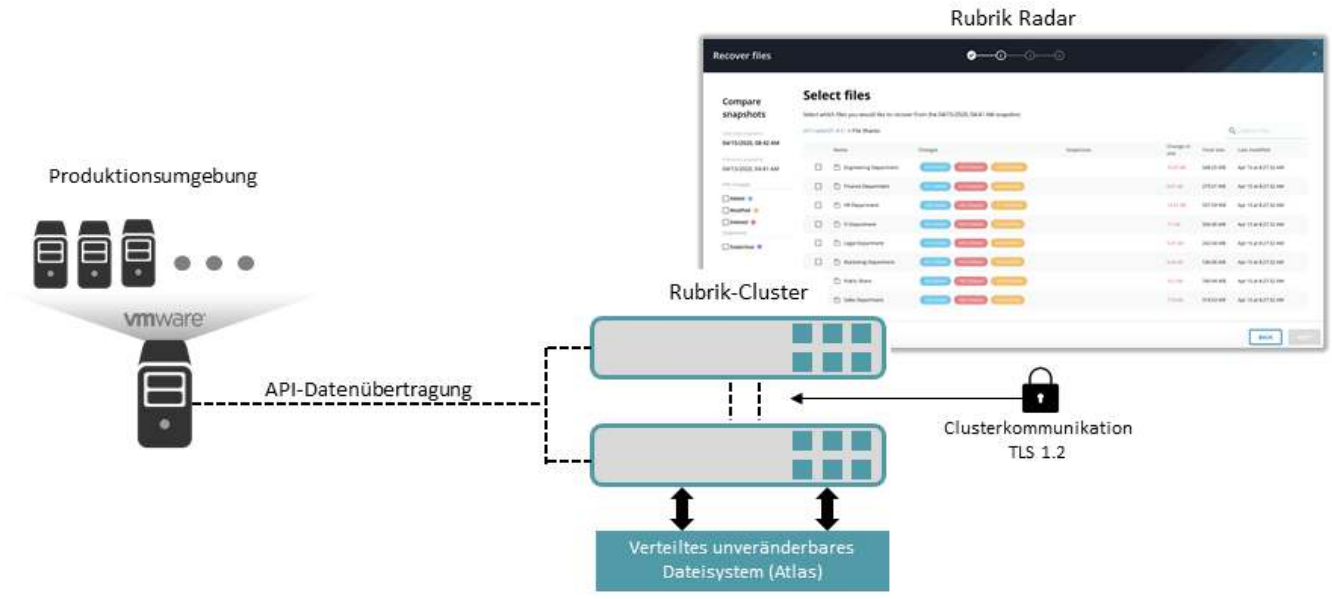
[1] Quelle: ESG Master Survey Results, *Umfrage zu geplanten Technologieausgaben 2020*, Januar 2020. Alle anderen ESG-Forschungsreferenzen und Diagramme in dieser technischen Prüfung wurden, sofern nicht anders angegeben, diesem Master-Umfrageergebnissatz entnommen.

Die Lösung: Wiederherstellung mit Rubrik Ransomware

Viele fragen sich, warum Unternehmen überhaupt auf Ransomware reagieren und das geforderte Lösegeld zahlen. Können sie ihre Daten nach einem Angriff nicht mit ihren Backups wiederherstellen? Die Wahrheit ist, dass viele Lösungen nicht über die Schutzfunktionen verfügen, die Unternehmen wirklich für ihren Malware-Schutz benötigen. Aber auch wenn entsprechende Maßnahmen implementiert wurden, sind Wiederherstellungsszenarien häufig eingeschränkt. Wenn Daten kompromittiert werden, führen die meisten Unternehmen eine schnelle Kosten-Nutzen-Analyse ihrer Optionen durch. Ist jedoch keine angemessene Datensicherheitslösung vorhanden, führt dies oft dazu, dass das Lösegeld bezahlt wird. Ein großer Teil der Analyse umfasst die Überlegung, dass es im Durchschnitt mindestens sieben Tage dauert, bis ein Unternehmen seine Daten wiederhergestellt hat. Diese Zeit ohne geschäftskritische Systeme reicht oft aus, um ein Unternehmen in den Ruin zu treiben. Fortschrittliche Ransomware zielt inzwischen auf Backups ab und verschlüsselt oder löscht sie vollständig. Die Wiederherstellung muss dann über externe Backups wie z. B. Bänder erfolgen, was meist zu lange dauert, sodass es für Unternehmen letztendlich einfacher ist, das Lösegeld hinzublättern. Die meisten Unternehmen haben auch keinen Einblick in ihre Backups und wissen daher nicht, was sie wiederherstellen können, ohne die Malware erneut in ihre Systeme zu lassen.

Rubrik schützt Ihre Backup-Daten durch cleveres Design vor Ransomware. Die Lösung gewährleistet eine mehrschichtige Datensicherheit, indem alle Daten im Ruhezustand und während der Übertragung verschlüsselt werden. Wie in Abbildung 2 gezeigt, überträgt jedes Rubrik-Cluster Daten über leistungsstarke randomisierte, kennwortauthentifizierte APIs an einen und von einem Schutz-Client. Dabei schützt das TLS 1.2-Protokoll die Datenübertragungen und zertifiziert die Knoten-zu-Knoten-Kommunikation. Alle Backup-Daten werden in einem unveränderlichen Format gespeichert, sodass sie nicht geändert werden können. Das verhindert, dass Ransomware auf die Backups zugreifen und diese verschlüsseln oder löschen kann. Dieser Ansatz ist für jede moderne Schutzstrategie unerlässlich. Mit nur wenigen Klicks kann ein Unternehmen nach einem Angriff über das inkrementelle Backup-Schema von Rubrik schnell zum letzten unkompromittierten Zeitpunkt zurückkehren.

Abbildung 2. Überblick über die Wiederherstellung mit Rubrik Ransomware



Quelle: Enterprise Strategy Group

Zu den wichtigsten Funktionen der Lösung gehören:

- **Unveränderlichkeit:** Sobald sie geschrieben wurden, können die Daten nicht mehr gelesen, geändert oder gelöscht werden. Echte Unveränderlichkeit ist für jede echte Ransomware-Schutzstrategie von entscheidender Bedeutung. Die Rubrik-Architektur ist darauf ausgelegt, Backups vollständig zu schützen.
- **Sichtbarkeit der Auswirkungen:** Um eine erfolgreiche Wiederherstellung durchführen zu können, müssen Unternehmen genau wissen, welche Kopie frei von jeglicher Malware ist und als Backup zur Wiederherstellung verwendet werden kann. Schnelle, präzise Transparenz spart wertvolle Zeit.
- **Sofortige Wiederherstellung:** Nach einem Angriff ist Zeit ein wichtiger Faktor für die Kosten und den Ruf eines betroffenen Unternehmens. Die Recovery Time Objective (RTO) muss auf ein Minimum beschränkt werden. Rubrik erreicht dies durch inkrementelle Backups und Point-in-Time-Wiederherstellungsoptionen, die eine schnelle und einfache Wiederherstellung ermöglichen.

Von ESG validiert

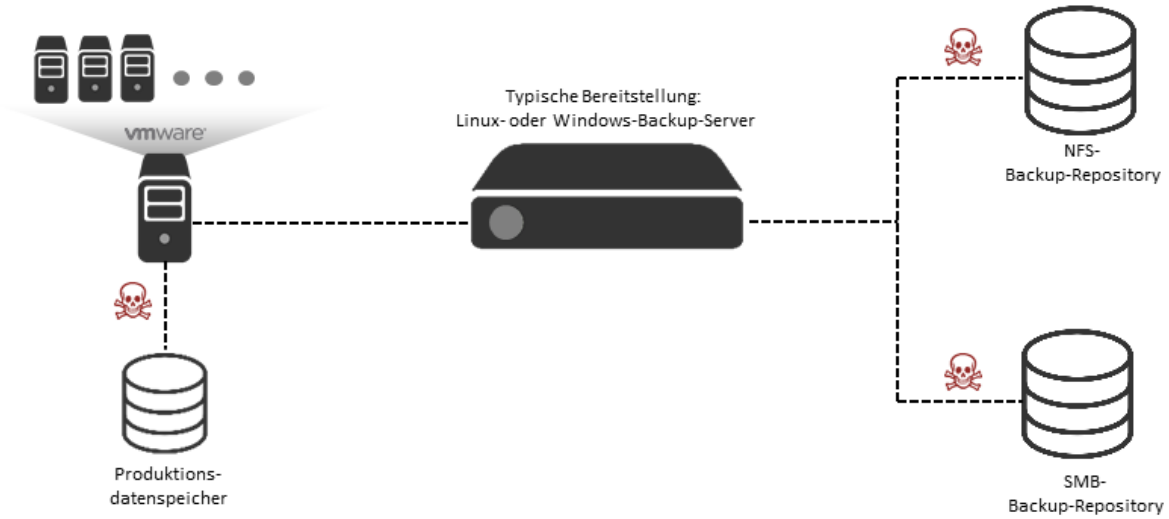
In dieser technischen Überprüfung von ESG wird die praktische Analyse der Ransomware-Lösung von Rubrik dokumentiert. Wir haben die Lösung validiert, indem wir mehrere von Rubrik gehostete Demositzungen genutzt, Fallstudien gelesen, an einem Architektur-Briefing teilgenommen und durch die verschiedenen Komponenten von Rubrik, die zusammen eine integrierte Ransomware-Schutzstrategie bilden, betrachtet haben.

Grundlagen der Ausfallsicherheit der Datenschutzarchitektur

ESG begann seine Tests damit, „herkömmliche“ Backup- und Wiederherstellungsarchitekturen zu betrachten und zu untersuchen, wo die Schwachstellen liegen, wie in Abbildung 3 dargestellt. Im Wesentlichen wollten wir besser nachvollziehen, wie ein Backup angegriffen werden kann, um Ransomware zu installieren. Ransomware ist eine Teilkategorie von Malware, bei der es sich um einen beliebigen schädlichen Code oder ein Schadprogramm handelt, das einem Angreifer die explizite Kontrolle über Ihr System verschafft. Dazu gehören Viren, Bugs, Würmer, Bots, Rootkits, Spyware, Adware und Trojaner. Sie funktioniert wie ein interner Agent, der schädlichen Code auf Ihrem Computer installiert oder Sie dazu bringt, ein Programm entweder über schädliche E-Mail-Anhänge, webbasiertes Messaging oder ein falsches Anwendungsupdate zu laden. Dadurch erhält der Angreifer Zugriff auf Ihr System, das dann nicht mehr auf Ihre Befehle reagiert. Ransomware geht aber noch einen Schritt weiter und verschlüsselt Ihre Datenbank und Dateien. Sobald ihr dies gelungen ist, verlangt der Angreifer eine Zahlung, um Ihre Dateien wieder zu entschlüsseln. Es gibt drei Hauptkategorien von Ransomware. Crypto-Ransomware greift wertvolle Dateien an und hindert Benutzer daran, darauf zugreifen. Locker-Ransomware verschlüsselt Dateien nicht, sondern sperrt das Opfer aus dem System aus und hindert es daran, darauf zuzugreifen. Doxware ist Ransomware, die Opfern droht, vertrauliche Informationen preiszugeben, wenn kein Lösegeld gezahlt wird.

Wie in Abbildung 3 gezeigt, hat ESG die Komponenten einer gängigen Datensicherheitsbereitstellung „Marke Eigenbau“ mithilfe von Tools, die von Anbieter-Websites heruntergeladen wurden, untersucht. In der Mitte sehen wir den Windows- oder Linux-Server, auf dem die Backup-Anwendung bereitgestellt wird. Normalerweise handelt es sich hierbei um einen beliebigen verfügbaren Server im Rechenzentrum, der mit demselben LAN wie die Backup-Clients verbunden ist. Genau wie die Clients, die er schützen soll, hat er in der Regel in irgendeiner Form für das Patch-Management und die Remote-Verwaltung Zugang zum Internet. Auf dem Server wird die Backup-Anwendung installiert. In der Regel übernimmt er das Anmeldedatenschema, das von der IT-Organisation standardisiert wurde. Aus diesem Grund und weil er häufig Dateisysteme (NFS und SMB) nutzt, die der Ransomware gut bekannt sind und auf denen sie gerne Backup-Images speichert, ist die Backup-Anwendung mitunter genauso anfällig wie die Systeme, die sie schützen soll.

Abbildung 3. Herkömmliche Backup-Architektur



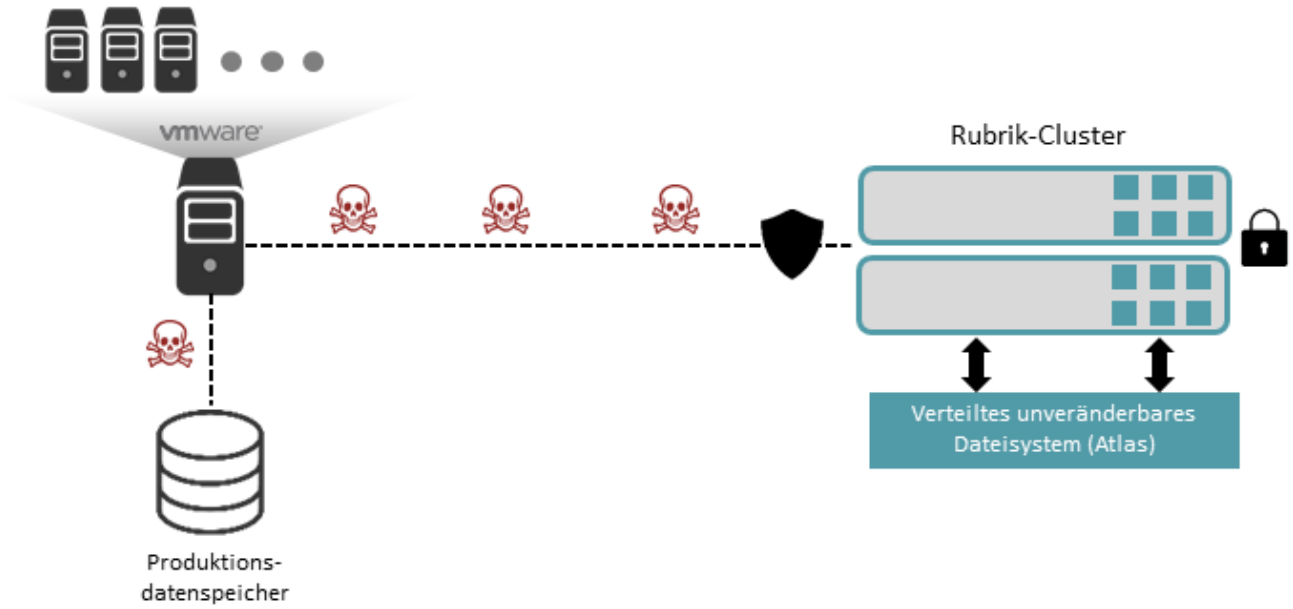
Quelle: Enterprise Strategy Group

Es ist keine leichte Aufgabe, einen Ransomware-Angriff zu verhindern. Hinzu kommt, dass Angreifer ständig auf der Suche nach neuen Schwachstellen sind. Ebenso wichtig für die Vermeidung ist die Wiederherstellung aus Ihren Backups. Die sicherste Methode für eine erfolgreiche Wiederherstellung ist eine unveränderliche Backup-Lösung. Wenn ein Backup unveränderbar ist, können die Daten nach dem Schreibvorgang nicht mehr gelesen, geändert oder gelöscht werden. ESG stellte fest, dass es in einer herkömmlichen Backup- und Recovery-Architektur, in der die Backup-Software nicht vom regulären Speichersystem getrennt ist, eine Schwachstelle gibt, die der Ransomware die Türen öffnet. Die meisten Backup-Lösungen verwenden einen NFS-Speicher als Backup-Ziel. Wenn die Ransomware auf das NFS-Dateisystem abzielt, sind diese Backups in Gefahr. Sobald die Ransomware installiert ist, kann sie die Backups verschlüsseln und den Zugriff darauf verhindern. Dieses Problem tritt bei mehreren führenden Backup-Anbietern auf. Bei der Rubrik-Lösung ist der Speicher jedoch eng in die Backup-Appliance und das Sicherheitsschema integriert, sodass diese Schwachstelle Ransomware-Angreifern nicht zugänglich ist.

Abbildung 4 zeigt einen Überblick über die Ausfallsicherheitsfunktionen der Rubrik-Lösung. Bei einem normalen Betrieb ohne echte Unveränderlichkeit laufen datenträgerbasierte Backup-Lösungen Gefahr, mit Ransomware infiziert zu werden. Dies kann Backups, die derzeit geschrieben werden, sowie vorhandene Backups betreffen. Dank der API-basierten Architektur von Rubrik ist das Client-Netzwerk vom Zugriff auf den Backup-Speicher ausgeschlossen, ganz im Gegensatz zu einigen herkömmlichen Designs, die standardmäßige Speicherprotokolle für die Konnektivität verwenden. Rubrik verfügt als Teil der Architektur über ein „API-First-Design“, das eine Authentifizierung auf allen Endpunkten erfordert, die für den Betrieb der Lösung verwendet werden. Die Authentifizierung kann über Anmeldeinformationen oder ein sicheres Token erfolgen. Dies umfasst auch Umgebungen, die eine rollenbasierte Zugriffskontrolle (RBAC) oder Mehrmandantenfähigkeit verwenden, um die verwalteten Rollen, Funktionen und Ressourcen logisch zu trennen. Die CLI, SDKs und anderen Tools von Rubrik verwenden die APIs und unterliegen denselben Sicherheitsanforderungen.

API-Endpunkte, die das zugrunde liegende Verhalten des Systems steuern, erfordern eine zusätzliche Autorisierungsebene, die nur von einem zertifizierten technischen Support-Techniker zugewiesen werden kann. Dadurch wird verhindert, dass ein böswilliger Angreifer das Verhalten eines Rubrik-Clusters ändern kann. Dieses Design beseitigt Schwachstellen und ermöglicht Rubrik, eine echte Unveränderlichkeit zu erreichen. Gleichzeitig bietet die Lösung die Möglichkeit, den Betrieb nach einem Ransomware-Angriff über ein Backup schnell wiederherzustellen, ohne das Lösegeld zu zahlen.

Abbildung 4. Überblick über die Ausfallsicherheit der Rubrik-Lösung

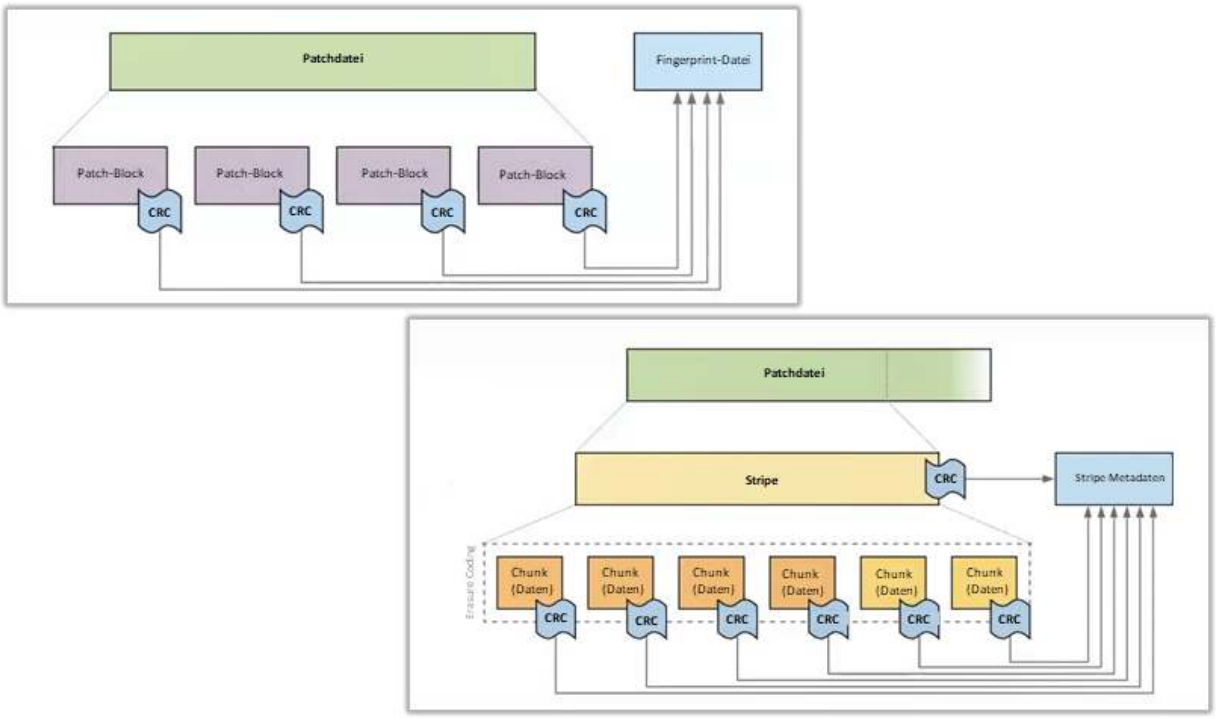


Quelle: Enterprise Strategy Group

Als Nächstes, wie in Abbildung 5 gezeigt, hat ESG einen genaueren Blick auf das Dateisystemdesign von Rubrik geworfen. Wenn ein Backup ausgeführt wird, führt Rubrik die folgenden Schritte auf der logischen Ebene aus. Alle Kundendaten werden in proprietäre Dateien mit geringer Dichte geschrieben, die so genannten „Patchdateien“. Nur-anfügen-Dateien (Append-only files; AOFs) enthalten eine Aufzeichnung aller vorgenommenen Datenänderungen, indem jede Änderung am Ende der Datei geschrieben wird. Auf diese Weise kann jede beliebige Person den gesamten Datensatz wiederherstellen, indem das Nur-anhängen-Protokoll von Anfang bis Ende wiederholt wird.

Anschließend kommen CRC-Prüfsummen (zyklische Redundanzprüfung) und Fingerabdrücke zum Einsatz, um die Integrität einer Datenübertragung oder einer Datei zu überprüfen. Prüfsummen werden als lange alphanumerische Zeichenketten dargestellt, die als digitale Fingerabdrücke fungieren und eine Originaldatei mit einer kopierten Version dieser Datei vergleichen, um sicherzustellen, dass sie identisch sind.

Abbildung 5. Details zur Unveränderlichkeit des Rubrik-Dateisystems



Quelle: Enterprise Strategy Group

Wichtige Ausfallsicherheitsfunktionen auf der physischen Ebene:

- Die AOF berechnet eine Prüfsumme auf Stripe-Ebene, die in jedem Metadaten-Stripe gespeichert wird.
- Eine Chunk-Prüfsumme wird berechnet und zusammen mit der Liste der Chunks in den Stripe-Metadaten gespeichert.
- Auf der Chunk-Ebene erfolgen die Replikation und das Erasure Coding.
- Wenn eine Datenwiederherstellung erforderlich ist, wird die Ausfallsicherheit gewährleistet, indem das Erasure Coding automatisch im Hintergrund ausgeführt wird.

Bedeutung

Der Wechsel von physisch getrennten Bändern zu digitalen Backups führte zu einer Schwachstelle, die Ransomware-Angreifern Zugang zum Backup-System verschafft. Bei einem Bandansatz wurden Protokolle wie TAR verwendet, um Daten von Servern und aus dem Speicher auf physische und wechselbare Banddatenträger zu übertragen. Wenn eine Wiederherstellung erforderlich war, wurde das physische Band verwendet. Bei den heutigen digitalen Backups werden jedoch Protokolle wie NFS und SMB verwendet. In vielen Fällen hat dies zu einem nicht unveränderbaren Prozess mit Herausforderungen auf der physischen und logischen Ebene geführt, einschließlich Problemen mit der Transportebene, die mit NFS und SMB einhergehen.

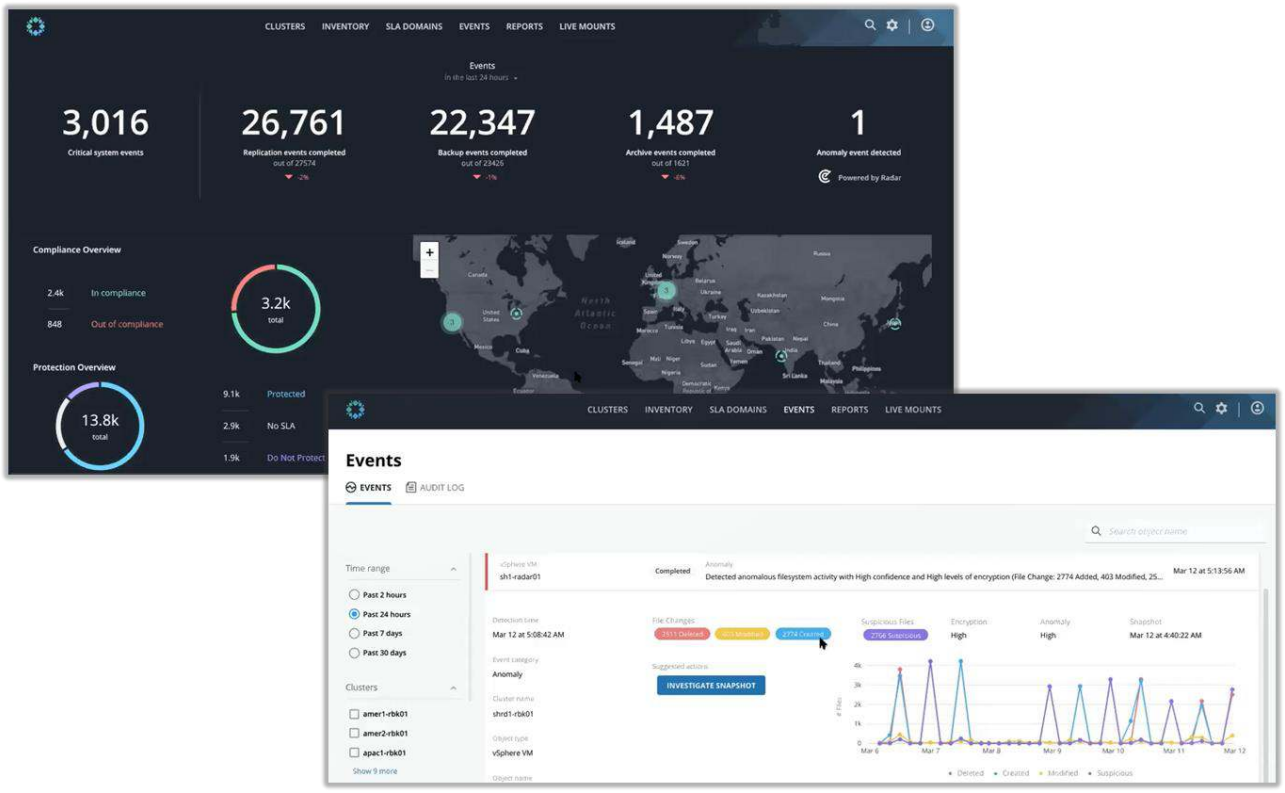
Im Gegensatz dazu wendet Rubrik einen „API-First“-Ansatz an, der die Verwendung von Protokollen wie NFS und SMB überflüssig macht. Durch die Nutzung von APIs entsteht ein vernetztes System zwischen Produktionsservern, Speicher, Datenbanken, Anwendungen und VMs. Backups werden über APIs initiiert und verarbeitet, wodurch das Rubrik-System von Natur aus unveränderbar und widerstandsfähig gegenüber Ransomware-Angriffen ist, die eine Wiederherstellung von Backup-Dateien verhindern sollen. Hinzu kommen zuverlässige Prüfsummen auf logischer und physischer Ebene und ein Fingerabdruckprozess, um die Datenintegrität zu gewährleisten.

Ransomware-Wiederherstellungsprozess

Die Wiederherstellung nach einem Ransomware-Angriff erfordert eine proaktive Datenverwaltung und -kontrolle. In den vorherigen Abschnitten haben wir uns darauf konzentriert, wie wichtig die Unveränderbarkeit ist, um Backups in Vorbereitung auf einen Angriff zu verwalten und eine schnelle Wiederherstellung einzuleiten. Für die Wiederherstellung nach einem Angriff müssen Unternehmen außerdem umfassende Einblicke in all ihre Daten und System haben. Mit Rubrik steht Unternehmen Polaris zur Verfügung – eine SaaS-Plattform, die Geschäftsinformationen organisiert und auffindbar und nutzbar macht. Rubrik Polaris bietet ML-basierte Einblicke mit speziell entwickelten SaaS-Anwendungen für Datenschutz, Governance, Sicherheit und Mobilität, um die Geschäftskontinuität zu gewährleisten, die Amortisierungszeit zu verkürzen und die Entscheidungsfindung zu verbessern.

Wie oben links in Abbildung 6 gezeigt, dient die über die Polaris-Plattform bereitgestellte Radar-Anwendung von Rubrik dazu, anormales Verhalten, wie Ransomware, zu identifizieren und die Wiederherstellung nach Ransomware-Angriffen zu beschleunigen und zu vereinfachen. Dabei ist darauf hinzuweisen, dass die Radar-Anwendung für die Wiederherstellung nach einem Ransomware-Angriff nicht zwingend erforderlich ist, jedoch einen besseren Einblick in die Wiederherstellungsoptionen bietet. Radar überwacht das Verhalten aller Cluster und erstellt so eine Baseline. Baselines basieren auf der Analyse des historischen Verhaltens und berücksichtigen Häufigkeiten, Zeit und Volumen. Anschließend sucht die Anwendungen nach Abweichungen von der Baseline, um festzustellen, ob eine Anomalie vorliegt, wie z. B. eine ungewöhnlich hohe Anzahl von hinzugefügten, gelöschten oder geänderten Dateien – im Grunde Veränderungen des normalen Backup-Verhaltens. Es gibt zwei Möglichkeiten, wie Rubrik Anomalien erkennt: über Dateisystemanalysen und Dateiinhaltsanalysen. Dieser Ansatz trägt entscheidend dazu bei, die Zuverlässigkeit des Erkennungsmodells zu erhöhen. Wenn eine Anomaliewarnung generiert wird, können Unternehmen mithilfe von Radar-Analysen den Inhalt der Dateien genauer untersuchen und nach Anzeichen für eine schädliche Verschlüsselung suchen. Die Lösung kann dann mithilfe eines statistischen Modells eine Verschlüsselungswahrscheinlichkeit berechnen. So kann die Analyse-Pipeline Entropiemerkmale berechnen, um den Grad der Verschlüsselung im Dateisystem ganz ohne problematischen Brute-Force-Workflow messen.

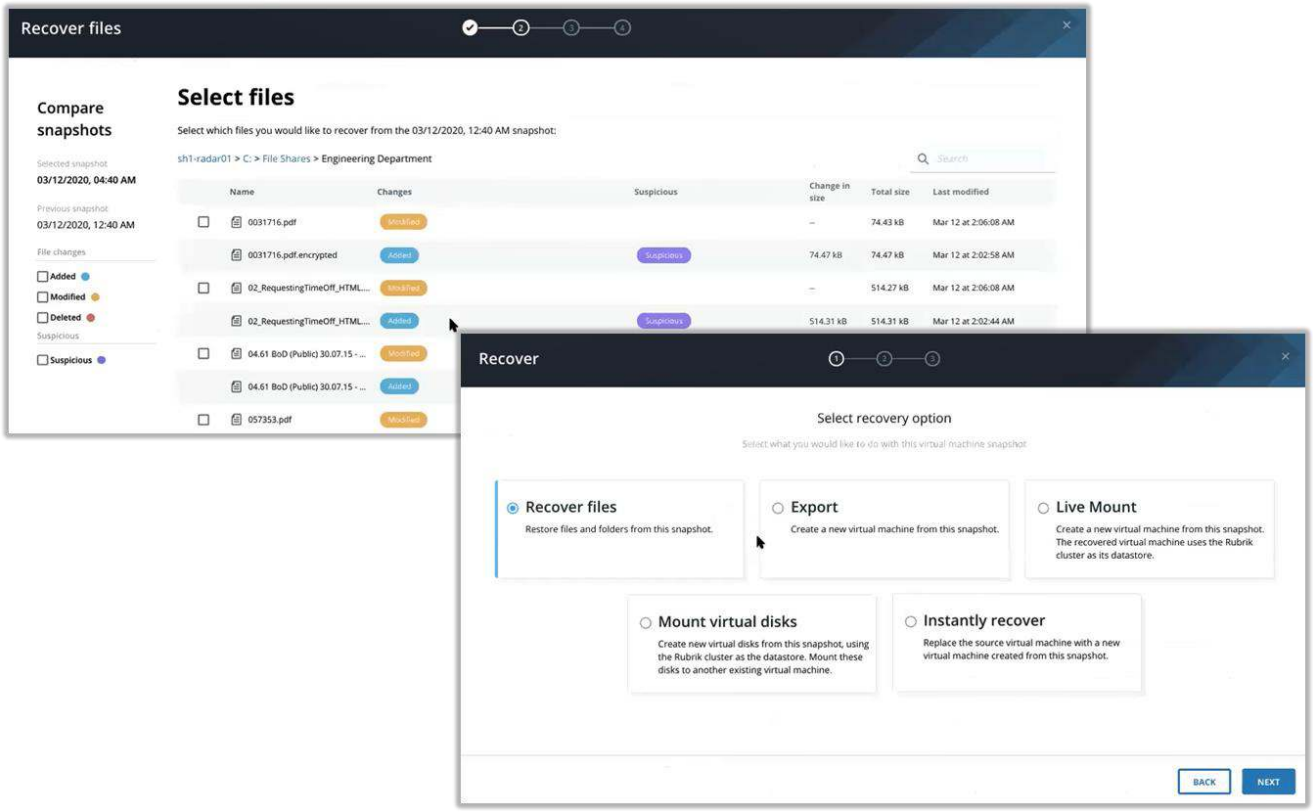
Abbildung 6. Transparenz mit Rubrik



Quelle: Enterprise Strategy Group

Nach einem Angriff auf das Hauptsystem eines Unternehmens kann ein Administrator auf Radar zugreifen und den Wiederherstellungsprozess starten. Wie unten rechts in Abbildung 6 zu sehen ist, kann ein Administrator die Ereignisseite nutzen, um schnell die besten Backups und Maßnahmen für die Wiederherstellung zu ermitteln. In der Mitte der Ereignisseite befinden sich drei farbcodierte Kennungen: Rot kennzeichnet gelöschte Dateien, Blau kennzeichnet erstellte Dateien und Gelb kennzeichnet geänderte Dateien. Der Administrator kann diese Werte und den Verlauf überprüfen, um festzustellen, ob sich das Verhalten verändert hat. Radar zeigt verdächtige Aktivitäten in Violett an, wenn eine Anomalie erkannt wird. Daraufhin kann der Administrator feststellen, ob dies auf normale Vorgänge oder schädliche Aktivitäten zurückzuführen ist. Wie in Abbildung 7 oben rechts gezeigt, kann der Administrator bei verdächtigen Volumes einen Drilldown auf Dateiebene durchführen, um eine tiefergehende Analyse durchzuführen. Für Administratoren sind die folgenden wichtigen Fragen zu berücksichtigen: Gab es einen Angriff? Wie und wann ist dieser passiert? Wie lautet der richtige Wiederherstellungspunkt und sollte eine Dateiwiederherstellung oder eine vollständige Snapshot-Wiederherstellung durchgeführt werden? Wie in Abbildung 7 unten rechts dargestellt, haben Administratoren viele Optionen für die Wiederherstellung, darunter Dateiwiederherstellung, Export, Live Mount, Bereitstellen von virtuellen Laufwerken und Instant Recovery. Die Rückkehr zum frühesten bekannten unkompromittierten Snapshot kann der sicherste Ansatz sein. Es stehen aber auch Optionen zur Verfügung, um einen neueren Snapshot zu verwenden, nachdem überprüft wurde, worauf sich die Anomalien oder Bedenken beziehen, um dann einzelne Dateien von einem anderen Zeitstempel wiederherzustellen und die beste RPO zu erreichen.

Abbildung 7. Wiederherstellungsvorgang mit Rubrik Ransomware



Quelle: Enterprise Strategy Group

Bedeutung

Unternehmen verlassen sich stark auf ihre Datenschutzanbieter, um die Wiederherstellbarkeit zu gewährleisten und die Wiederherstellungszeit im Falle einer Datenintegritätsverletzung zu verkürzen. Um zu verhindern, dass ein Opfer eine Wiederherstellung ohne Lösegeld vornimmt, greifen neue Malware-Angriffe jedoch nicht nur Produktionsdaten an, sondern auch die Backup-Datensätze. Rubrik ermöglicht es Unternehmen, Daten-Backups vor Malware und Ransomware-Angriffen zu schützen.

ESG konnte bestätigen, dass Rubrik mit unveränderlichen Backups und Transparenz über Polaris und Radar Unternehmen eine schnelle und einfache Wiederherstellung nach einem schädlichen Ransomware-Angriff ermöglicht. Detaillierte Einblicke in die betroffenen Daten ermöglichen eine präzise Wiederherstellung, um den mit dem Angriff verbundenen Datenverlust zu minimieren. Wenn Ransomware nur einen Teil der Umgebung betrifft, können Unternehmen gezielt diesen Teil wiederherstellen. Die RTO ist in diesen Situationen ebenfalls entscheidend. Eine proaktive Verwaltung von Backup-Daten mit Rubrik kann ein Unternehmen bestens vorbereiten, um den Schaden zu begrenzen.

Die übergreifende Erkenntnis

Ransomware-Angriffe gehören zu den stressigsten Ereignissen, mit denen ein datenorientiertes Unternehmen zu kämpfen hat. Sie stören den Betrieb auf allen Ebenen. Wenn Unternehmen nicht angemessen vorbereitet sind, können die Kosten für die Wiederherstellung enorm ausfallen – ganz zu schweigen von der Rufschädigung, die sie mit sich bringen. Es ist nicht immer möglich, einen Ransomware-Angriff zu vermeiden, und es fühlt sich manchmal an, als wären wir den Angreifern nur einen winzigen Schritt voraus. Wenn Angreifer eine Lücke finden, müssen Unternehmen sich schnell auf ihren Backup- und Wiederherstellungsprozess verlassen können.

ESG stellte fest, dass die Datenverwaltungsplattform von Rubik aufgrund ihrer Designelemente im Gegensatz zu vielen anderen Anbietern, die auf Hardware- und Softwareprodukte von Drittanbietern oder Bandlösungen zum Schutz vor Ransomware setzen, robuste Ransomware-Funktionen bietet. Die umfassende Nutzung von APIs, unveränderlichen Backups und der Visualisierung mit Polaris Radar bildet eine ganzheitliche Ransomware-Reaktionsstrategie, die darauf ausgelegt ist, Unternehmen aller Größen zu schützen. Unsere Analyse wurde weiter anhand von Praxisbeispielen von Kunden geprüft, die nach Ransomware-Angriffen eine sofortige Wiederherstellung durchführen konnten, sowie von anderen, die noch keine Rubrik-Strategie implementiert hatten und teuer bezahlen mussten, um ihre Systeme nach einem Angriff wiederherzustellen.

Wir haben festgestellt, dass einige Unternehmen sogar glauben, dass die Zahlung des Lösegelds eine tragfähige Strategie darstellt. Dabei ist jedoch zu bedenken, dass dies Angreifer nur noch ermutigt. Zudem gilt: Nur weil Sie einen Angreifer bezahlen, bedeutet das noch lange nicht, dass er nicht mehr Geld verlangt oder, was sogar noch schlimmer ist, einfach Ihr Geld nimmt und Ihre Dateien nie entschlüsselt. Ihr einzig vernünftiger Notfallplan muss daher einen bewährten Anbieter für Backup und Wiederherstellung einbeziehen, der die Herausforderungen versteht und über Technologien verfügt, die genau die Ergebnisse liefern, die Sie benötigen. Wenn Sie sich auf eine schnelle, nahtlose Wiederherstellung nach einem Ransomware-Angriff vorbereiten möchten, ist ESG der Meinung, dass Sie Rubrik ernsthaft in Betracht ziehen sollten.