Technical Review

Verbesserte Wiederherstellbarkeit nach Ransomware-Angriffen mit SafeMode auf FlashBlade von Pure Storage

Datum: März 2020 **Autor:** Vinny Choinski, Senior Validation Analyst, und Alex Arcilla, Validation Analyst

Kurzfassung

Dieses ESG Technical Review dokumentiert die praktische Analyse und Prüfung von Pure Storage FlashBlade mit SafeMode. Wir untersuchen, wie SafeMode Daten vor Ransomware-Angriffen oder versehentlichem Löschen schützt und sich in aktuelle Datenschutzlösungen integrieren lässt: Veeam, Veritas NetBackup und Commvault.

Die Herausforderungen

Ransomware ist allgegenwärtig und stellt sowohl für Führungskräfte aus der IT wie auch aus anderen Geschäftsbereichen ein ernsthaftes Problem dar. Die ESG hat kürzlich ihre jährliche Umfrage zu den beabsichtigten Technologie-Investitionen unter 651 führenden IT-Entscheidungsträgern in mittelständischen (d. h. 100 bis 999 Mitarbeiter) und großen Unternehmen (d. h. 1.000 oder mehr Mitarbeiter) in Nordamerika und Westeuropa abgeschlossen.[1] Laut Abbildung 1 haben zwar 40 % der Organisationen keinen Ransomware-Angriff erlitten (oder ziehen es vor, dies nicht zu sagen), aber die Mehrheit der Unternehmen gab an, dass sie 2019 mit Ransomware-Angriffen zu tun hatten. Tatsächlich meldeten 60 % einen Ransomware-Angriff zu irgendeinem Zeitpunkt während des Zeitraums von zwölf Monaten, während 29 % meldeten, dass Angriffe wöchentlich (oder sogar noch häufiger) erfolgten. Alarmierend ist, dass 13 % täglich Bedrohungen durch Ransomware ausgesetzt sind. Organisationen, die einen Fachkräftemangel im Bereich der Cybersicherheit meldeten, waren in den letzten 12 Monaten mit wesentlich höherer Wahrscheinlichkeit (67 % gegenüber 54 %) Opfer von Ransomware-Angriffen. Die ESG-Untersuchung zu geplanten Technologieausgaben im Jahr 2020 deutet auch darauf hin, dass 62 % der Organisationen ihre Ausgaben für Cybersicherheit im Jahr 2020 erhöhen werden, und es ist davon auszugehen, dass in vielen Fällen die Sorge um Ransomware-Angriffe diese Einstellung zu Sicherheitsinvestitionen zumindest beeinflusst hat.

Abbildung 1. Menge der Ransomware-Angriffe im Jahr 2019

Quelle: Enterprise Strategy Group

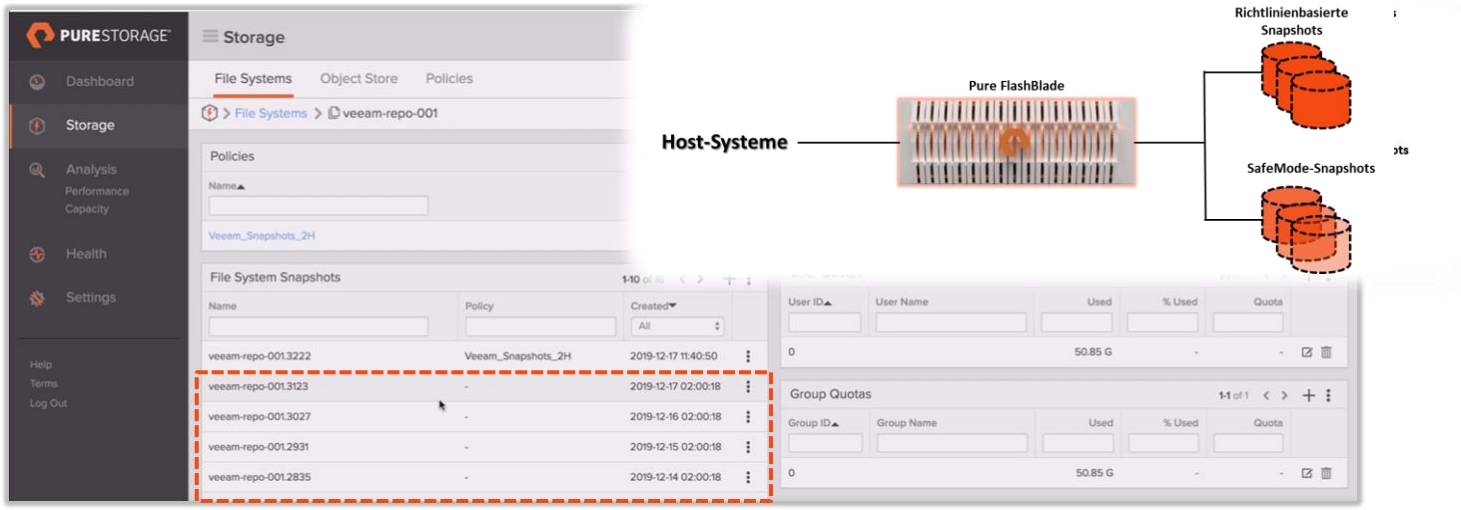
Die Lösung: Pure Storage FlashBlade mit SafeMode

[1] Quelle: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, Januar 2020. Alle anderen ESG-Forschungsreferenzen und -diagramme in diesem technischen Bericht wurden, sofern nicht anders angegeben, diesen Master-Umfrageergebnissen entnommen.

Die stets zunehmende Häufigkeit von Ransomware-Angriffen erfordert von Organisationen einen umfassenden Ansatz zur Abwehr solcher Bedrohungen. Diese Abwehr muss Folgendes umfassen: eine Schärfung des Bewusstseins für Cybersicherheit und die Schulung von Mitarbeitern – da viele Angriffe durch die eine oder andere menschliche Interaktion gestartet werden –, die Zusammenarbeit zwischen Cybersicherheits-, System- und Datenschutzteams zum Stärken von Infrastrukturen und einen Reaktionsplan, der ausgehend von Backups leicht ausgeführt und sicher verwahrt und validiert werden kann, falls eine Wiederherstellung erforderlich wird.

Pure Storage FlashBlade ist eine fortschrittliche Scale-Out-Plattform für Datei- und Objekt-Storage zum Konsolidieren von Datensilos wie Backup-Appliances und Datenpools. Seine hohe Performance und die Vielzahl an Funktionen bilden die Grundlage für einen Data Hub, der auch jenseits des Datenschutzes einen erheblichen Mehrwert für Workloads bieten kann, einschließlich Analysen, KI, Tests/Entwicklung und EDA. Wie in Abbildung 2 dargestellt, handelt es sich bei SafeMode-Snapshots um eine integrierte FlashBlade-Funktion, mit der Unternehmen schreibgeschützte Snapshots von Backup-Daten und zugehörigen Metadatenkatalogen erstellen können, nachdem sie ein vollständiges Backup durchgeführt haben. SafeMode-Snapshots werden unabhängig vom Administrator automatisch erstellt und verwaltet. Unternehmen können Primär- oder Sicherungsdaten direkt aus diesen Snapshots wiederherstellen und sich so vor Ransomware-Angriffen, mutwillig schädlichen Aktivitäten von Administratoren oder Mitarbeitern und sogar vor versehentlichem Löschen schützen, wenn Originalkopien beschädigt oder nicht mehr zum Ermöglichen einer einfacheren Wiederherstellung verfügbar sind.

Abbildung 2. Überblick zu FlashBlade mit SafeMode



Quelle: Enterprise Strategy Group

Dies sind die wichtigsten Lösungsmerkmale:

- **Verbesserter Schutz:** Ransomware kann SafeMode-Snapshots weder löschen noch ändern oder verschlüsseln. Außerdem kann nur ein autorisierter Beauftragter eines Unternehmens direkt mit dem technischen Support von Pure zusammenarbeiten, um die Funktion zu konfigurieren, die Richtlinie zu ändern oder Snapshots manuell zu löschen.
- **Einfachheit:** Die Einrichtung von SafeMode ist sehr einfach und die Wartung erfordert keinen täglichen Betriebsaufwand.
- **Backup-Integration:** Organisationen können unabhängig vom Backup-Produkt oder vom nativen Dienstprogramm, das zum Verwalten von Datenschutzprozessen verwendet wird, denselben Snapshot-Prozess verwenden.
- **Flexibilität:** Die Planung von Snapshot-Kadenzen und -Löschungen ist anpassbar.
- **Schnelle Wiederherstellung:** Ransomware bedeutet für Backup-Systeme die besondere Herausforderung, potenziell riesige Datenmengen wiederherstellen zu müssen. Mit FlashBlade können Organisationen eine parallele Architektur mit elastischer Performance nutzen, die entsprechend dem Datenvolumen wächst, um Backups und Wiederherstellungsprozesse zu beschleunigen.
- **Investitionsschutz:** FlashBlade umfasst SafeMode-Snapshots ohne Aufpreis. Ein aktuelles Pure-Abonnement oder ein Wartungs-Support-Vertrag deckt Erweiterungen ab.

Von ESG validiert

In diesem ESG Technical Review ist die praktische Prüfung von Pure Storage SafeMode dokumentiert. Wir haben die Lösung validiert, indem wir mehrere von Pure Storage gehostete Demositzungen nutzten, an einer Einweisung und einem Deep Dive zur Architektur teilnahmen und durch die verschiedenen Storage- und Datenschutz-Schnittstellen navigierten, die für die Integration und Verwaltung verwendet werden.

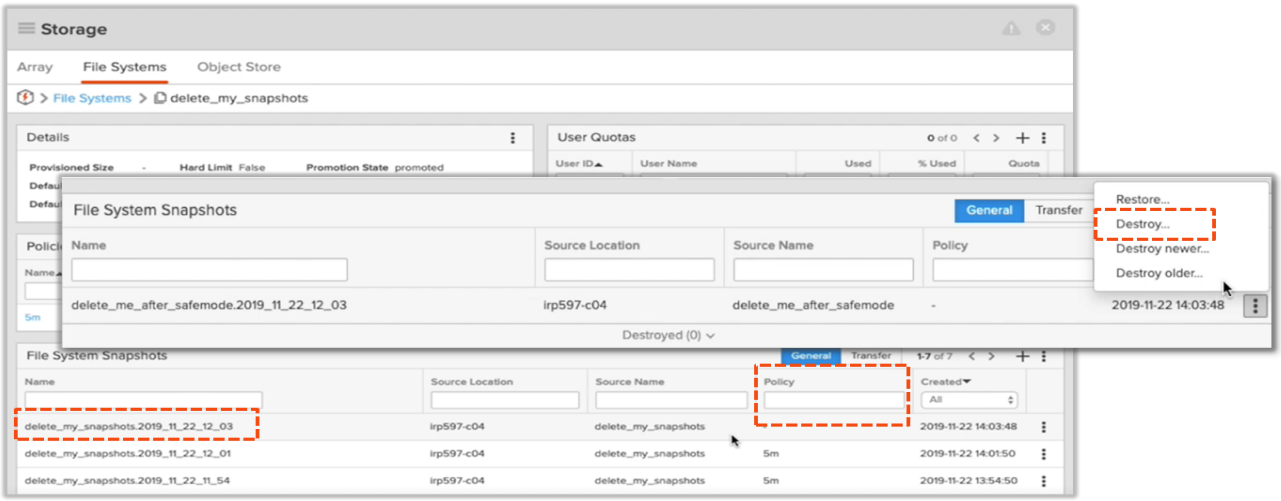
SafeMode-Grundlagen

Mit Pure Storage SafeMode können Unternehmen Datenbackups von Dateien oder Dateisystemen vor der Beeinträchtigung durch Ransomware-Angriffe, versehentliches Löschen von Backups oder mutwillig schädliche Aktivitäten von Administratoren schützen. Dadurch wird das manuelle und vollständige Entfernen (permanente Löschung) von Datenbackups von FlashBlade verhindert, sodass Organisationen ihre FlashBlade-Systeme nach derartigen Vorfällen wiederherstellen und schnell zum Produktionsstatus zurückkehren können. SafeMode darf nur durch den technischen Support von Pure Storage aktiviert werden.

Die ESG begann ihre Tests mit einer Untersuchung der Frage, wie SafeMode vor dem unbeabsichtigten Entfernen von Datei- oder Dateisystem-Snapshots schützt. Über die Verwaltungsoberfläche von Pure Storage FlashBlade wurde im Menü „Storage“ die Registerkarte „File Systems“ (Dateisysteme) aufgerufen, um die mit SafeMode geschützten Snapshots anzuzeigen. Einzelne Dateien oder Dateisysteme, die durch SafeMode geschützt sind, sind durch einen leeren Eintrag in der Spalte „Policy“ (Richtlinie) gekennzeichnet. Verwendet wurde der Snapshot namens „delete_me_after_safemode.2019_11_11_22_12_03“ (siehe Abbildung 3).

Um das Backup vollständig von FlashBlade zu entfernen, wurde zunächst auf das 3-Punkte-Symbol rechts neben dem entsprechenden SafeMode-Snapshot geklickt, um ein Popup-Menü anzuzeigen, und die Option „Destroy“ (Löschen) wurde ausgewählt. Durch diese Aktion wurde der Snapshot in den Bereich „Destroyed Snapshots“ (Gelöschte Snapshots) verschoben.

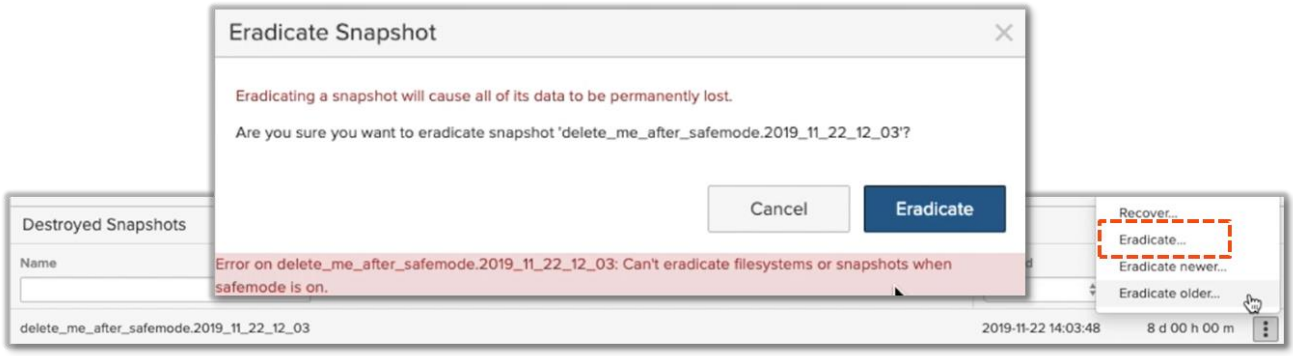
Abbildung 3. Durch SafeMode geschützter Snapshot



Quelle: Enterprise Strategy Group

Danach wurde derselbe Snapshot unter dem Bereich „Destroyed Snapshots“ (Gelöschte Snapshots) ausgewählt, auf das 3-Punkte-Symbol geklickt und „Eradicate“ (Dauerhaft löschen) aus dem Menü ausgewählt. Auf der Oberfläche wurde eine Warnmeldung angezeigt mit dem Hinweis, dass diese Aktion nicht rückgängig gemacht werden kann, nachdem sie ausgeführt wurde. Beim Klicken auf die Schaltfläche „Eradicate“ (Dauerhaft löschen) wurde die Fehlermeldung in Abbildung 4 eingeblendet, die bestätigt, dass der ausgewählte, durch SafeMode geschützte Snapshot nicht dauerhaft gelöscht werden konnte. Mit SafeMode kann ein Administrator sicherstellen, dass saubere Snapshots zur Wiederherstellung des FlashBlade-Systems verfügbar bleiben.

Abbildung 4. Versuch, einen durch SafeMode geschützten Snapshot dauerhaft zu löschen

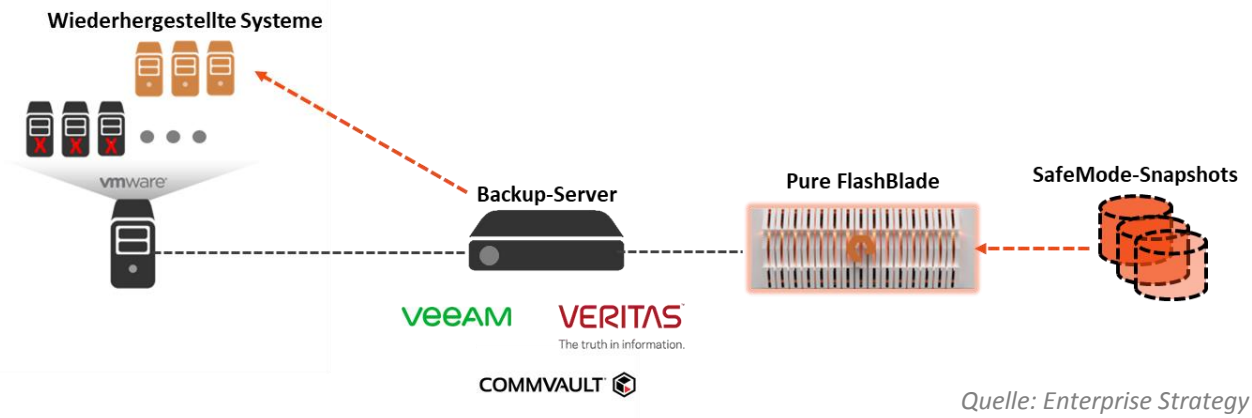


Quelle: Enterprise Strategy Group

SafeMode schützt Backups vor Ransomware, indem es automatisch schreibgeschützte Snapshots von Daten und zugehörigen Metadaten erstellt, die nicht gelöscht werden können (siehe Abbildung 5). Mit anderen Worten: Ransomware-Software kann die schreibgeschützten SafeMode-Snapshots nicht manipulieren. Im Gegensatz zu richtlinienbasierten Snapshots, die von internen Administratoren verwaltet werden, unterliegen SafeMode-Snapshots Richtlinien, die zwischen einer designierten Person und dem technischen Support von Pure Storage vereinbart werden. SafeMode verhindert, dass designierte Backups vollständig aus FlashBlade entfernt, modifiziert oder verschlüsselt werden, bis vorkonfigurierte Aufbewahrungsfristen erreicht wurden und die dauerhafte Löschung erfolgen kann.

Organisationen können auch ihre vorhandenen Datenschutzlösungen mit SafeMode nutzen, wie in Abbildung 5 dargestellt, indem sie die Lösung anweisen, SafeMode-Snapshots für die Wiederherstellung von Daten innerhalb von FlashBlade zu verwenden.

Abbildung 5. Integration mit Datenschutzlösungen anderer Anbieter



Quelle: Enterprise Strategy Group

Warum ist das wichtig?

Datenbackups, die durch Ransomware, menschliches Versagen oder mutwillig handelnde Administratoren beschädigt werden, kosten Unternehmen Zeit, Umsätze und Produktivität. Das Vorhandensein unbeschädigter und verfügbarer Backups zur Wiederherstellung und zur Wiederaufnahme des normalen Betriebs ist beim Festlegen von Sicherheits- und Datenwiederherstellungsstrategien entscheidend.

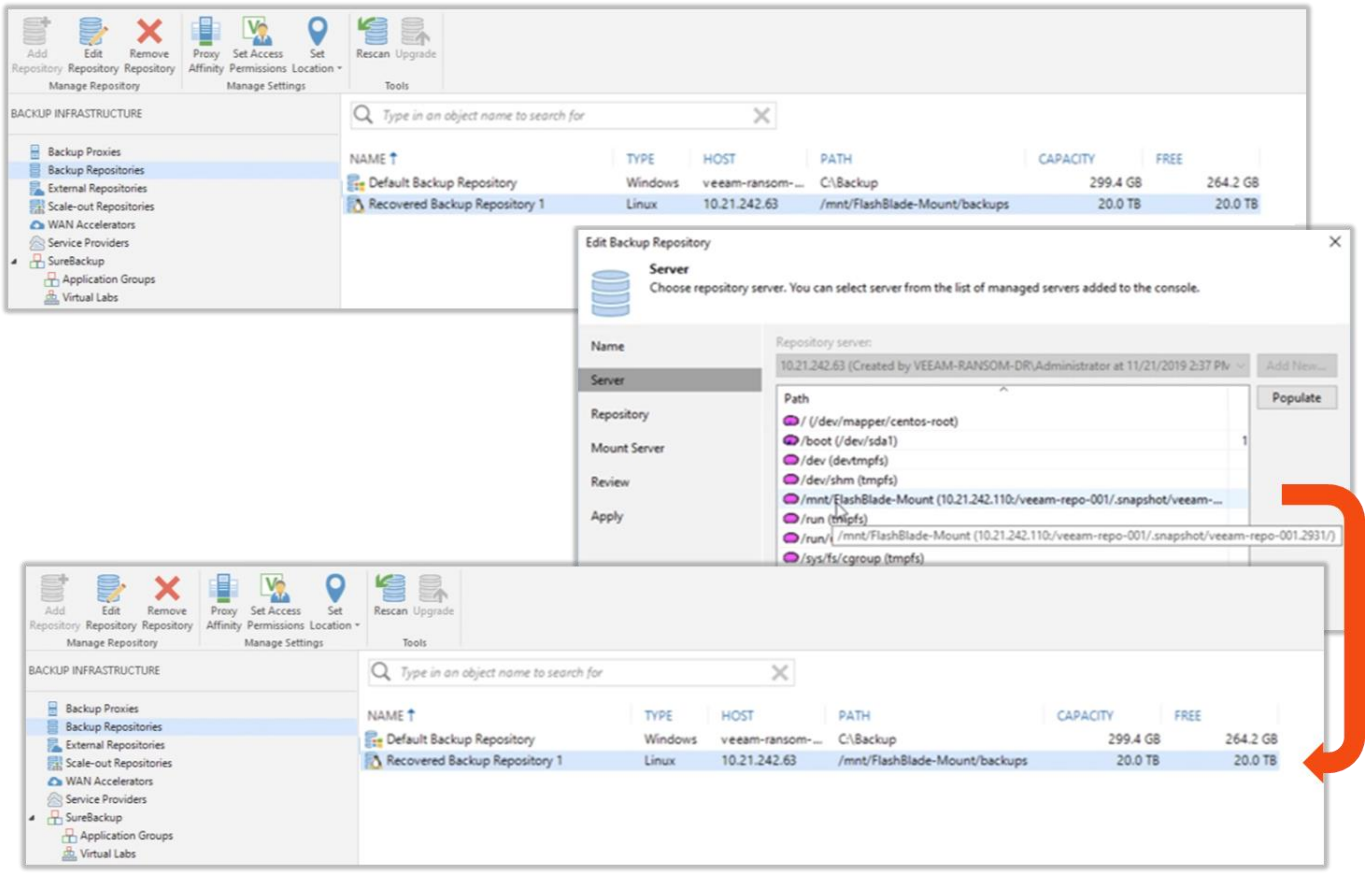
Die ESG hat bestätigt, dass Pure Storage SafeMode auf FlashBlade verhindern kann, dass Datenbackups durch Ransomware oder andere Ereignisse verändert, gelöscht oder verschlüsselt werden. Wir haben beobachtet, wie SafeMode einen verbesserten Datenschutz bietet, indem es Snapshots erstellt, die nicht geändert oder dauerhaft gelöscht werden können. Unternehmen können SafeMode einsetzen, um die Geschäftskontinuität nach Vorfällen aufrechtzuerhalten, die auf mutwillig schädliche Aktivitäten oder menschliches Versagen zurückzuführen sind.

SafeMode-Integration mit Backup und Wiederherstellung

Die ESG hat eine detailliertere Prüfung der Integration von SafeMode auf FlashBlade mit verschiedenen Datenschutzlösungen durchgeführt. Untersucht wurden hierbei Konfigurationsoptionen zum Verbessern der Wiederherstellbarkeit nach einem Ransomware-Angriff oder einem anderen böswilligen Angriff mit drei verschiedenen branchenweit anerkannten Datenschutzlösungen, darunter Veeam Backup & Replication, Veritas NetBackup und Commvault Complete Backup & Recovery.

Wie in Abbildung 6 dargestellt, begann unsere Integrationsuntersuchung mit der Nutzung einer Veeam-Umgebung mit einem Backup-Repository, das auf einem Pure Storage FlashBlade-Storage-System konfiguriert war. Oben in der Abbildung ist das Backup-Repository vor einem simulierten Angriff im blau schattierten Bereich hervorgehoben. In dieser Ansicht wurden der Repository-Name (FlashBlade SafeMode Backup Repository), der Typ (Linux), der Host (10.21.242.63) und der Pfad (/mnt/FlashBlade-Mount/Backups) angezeigt. Bei diesem Testszenario kamen wir zu dem Ergebnis, dass sowohl die Produktions- als auch die Datenschutzumgebung durch den Angriff beeinträchtigt wurde.

Abbildung 6. FlashBlade SafeMode mit Veeam Backup & Replication



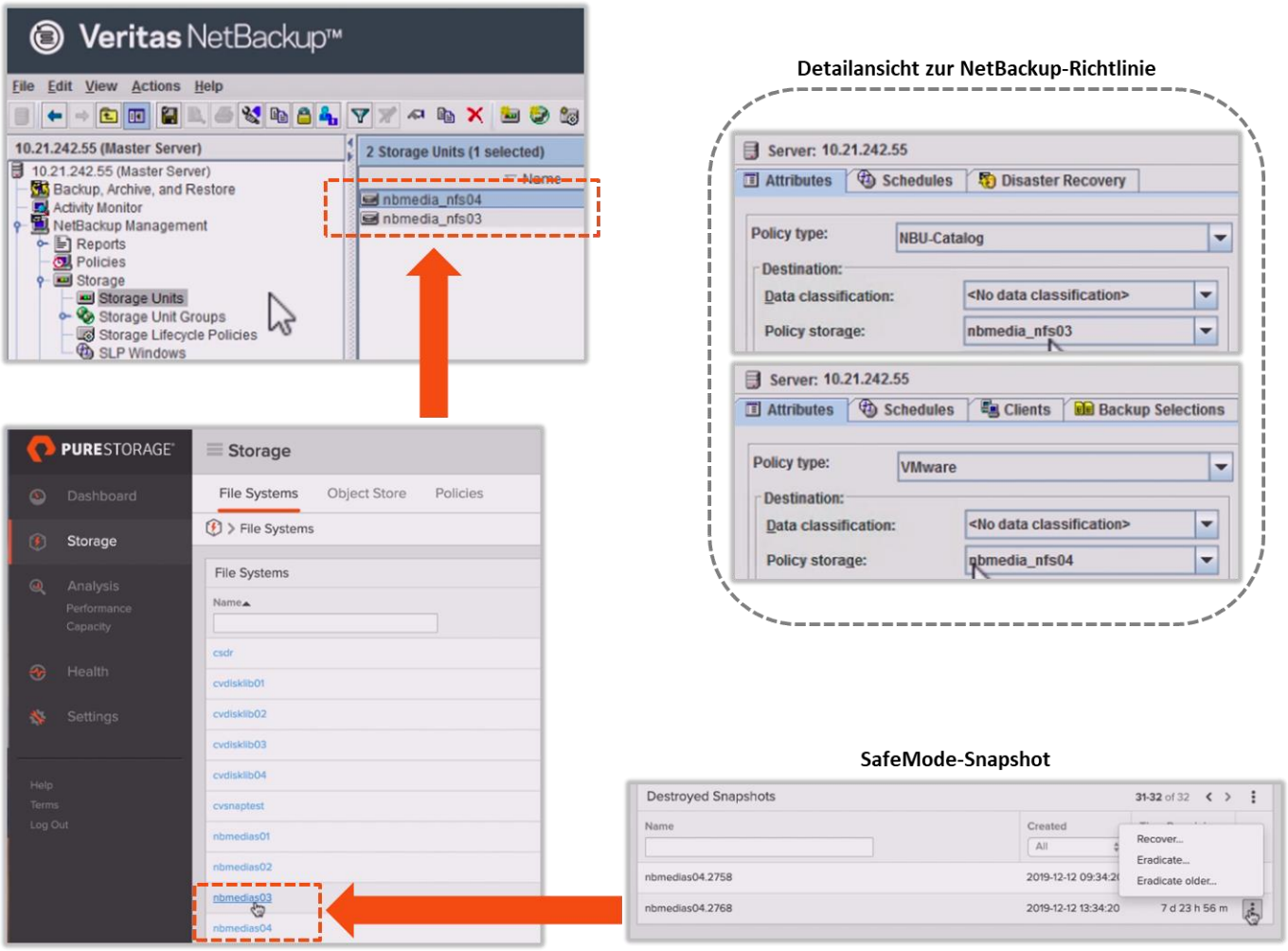
Quelle: Enterprise Strategy Group

Um den Wiederherstellungsprozess zu starten, wurde eine Neuinstallation der Anwendung Veeam Backup & Replication durchgeführt. Beachten Sie, dass diese neue Instanz von Veeam je nach Ressourcenverfügbarkeit zum Zeitpunkt der Katastrophe auf einem physischen Server oder einer virtuellen Maschine eingesetzt werden kann. Dann wurde, wie in der Mitte von Abbildung 6 dargestellt, die Veeam-Benutzeroberfläche verwendet, um den Linux-Host (10.21.242.110) nach dem schreibgeschützten, unbeschädigten SafeMode-Snapshot des FlashBlade-Dateisystem-Backup-Repositorys zu durchsuchen. Wie unten in Abbildung 6 dargestellt, erstellte die ESG einfach ein neues Backup-Repository mit dem Namen „Recovered Backup Repository 1“. Danach wurde das neue Repository gescannt, um Backup-Images zu importieren und die Kundeninformationen sowie die Historie in der neuen Veeam-Instanz zu indizieren. Nachdem der Scan abgeschlossen war, wurde mithilfe der Wiederherstellungsoption in der Veeam-Benutzeroberfläche eine vollständige VM-Wiederherstellung aus dem Backup-Image im SafeMode-Snapshot durchgeführt, um die Client-Backup-Daten in einem bekannterweise unbeschädigten Zustand wiederherzustellen.

Anschließend wurde, wie in Abbildung 7 dargestellt, der Prozess zum Konfigurieren von Veritas NetBackup mit SafeMode auf FlashBlade überprüft. Veritas NetBackup wendet das Konzept von Storage-Einheiten als Speicherort sowohl für Client-Backup-Images als auch für Backups des NetBackup-Katalogs an. Der NetBackup-Katalog enthält Anwendungskonfigurationseinstellungen sowie Informationen zu den Client-Backup-Images, die ebenfalls in Storage-Einheiten gespeichert sind.

Wie oben links in Abbildung 7 im orangefarbenen Detailausschnittfeld zu sehen, wurde die Testumgebung mit zwei Storage-Einheiten (nbmedia_nfs03 und nbmedia_nfs04) konfiguriert. Diese Speichereinheiten wurden auf einem Pure Storage FlashBlade mit konfigurierten SafeMode-Snapshots gehostet. Der Abschnitt mit Details zur NetBackup-Richtlinie in Abbildung 7 zeigt, dass für den Katalog ein Backup auf der Storage-Einheit ***nbmedia_nfs03*** erstellt wird und dass die Backup-Richtlinie ***VMware*** die Storage-Einheit ***nbmedia_nfs04*** verwendet, um virtuelle Maschinen in der Umgebung zu sichern.

Abbildung 7. FlashBlade SafeMode mit Veritas NetBackup



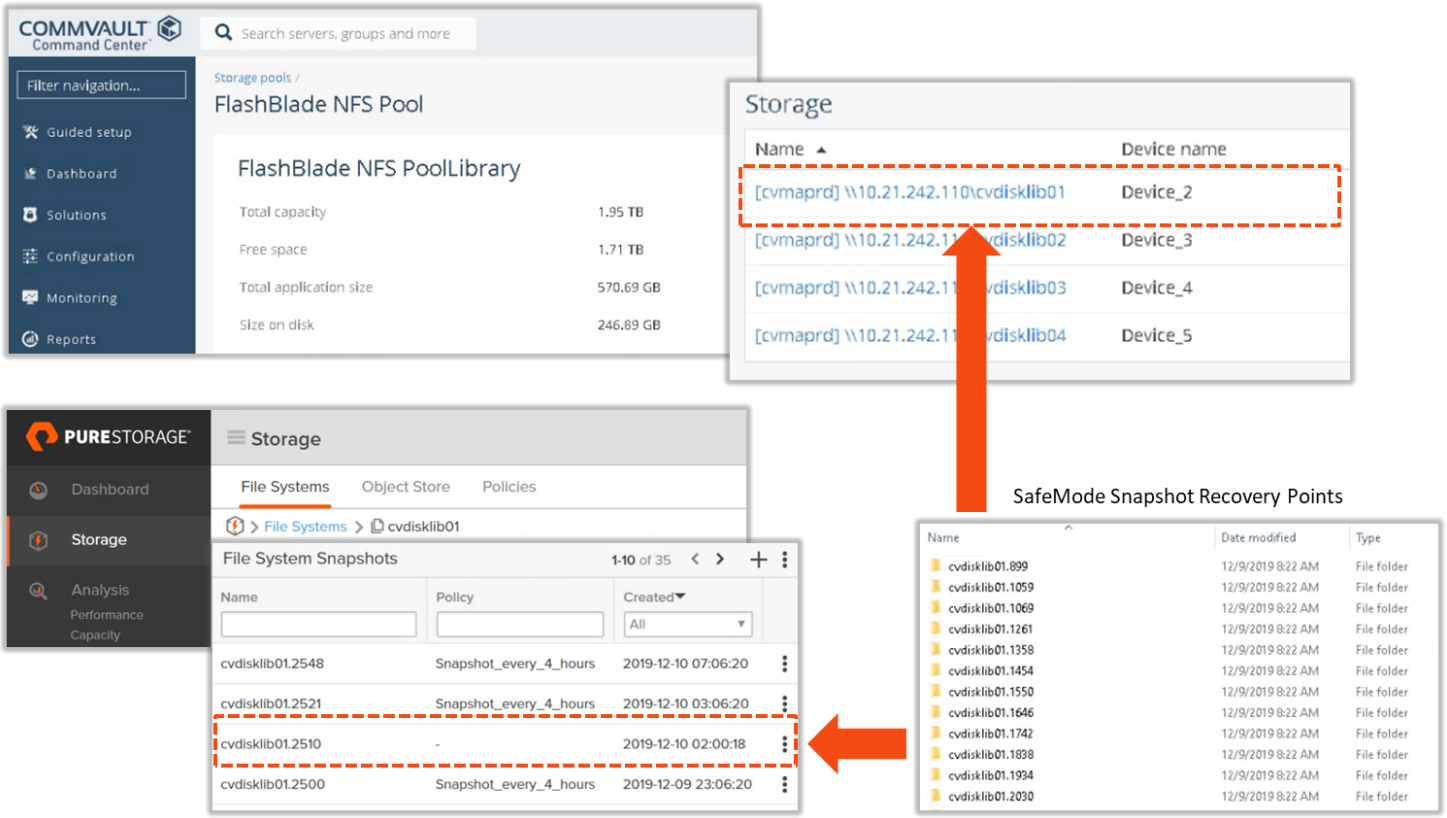
Quelle: Enterprise Strategy Group

Für NetBackup wurde dasselbe Testszenario verwendet wie für Veeam. Dieses Szenario beschreibt eine Situation, in der sowohl die Produktionssysteme als auch die Datenschutzumgebung durch Ransomware bedroht sind. Bei diesem Test haben wir tatsächlich die FlashBlade-Dateisysteme und Standard-Snapshots gelöscht und eine Wiederherstellungsanforderung initiiert, die anschließend nicht erfolgreich war. Dann wurde, wie unten in Abbildung 7 dargestellt, die FlashBlade-Benutzeroberfläche verwendet, um die Dateisysteme ***nbmedia03*** und ***nbmedia04*** aus einem SafeMode-Snapshot wiederherzustellen, und nachdem die Dateisysteme wiederhergestellt waren, wurden die NetBackup-

Dienste neu gestartet und die Benutzeroberfläche verwendet, um die Produktionssysteme in einem bekannterweise unbeschädigten Zustand wiederherzustellen.

Schließlich überprüfte die ESG, wie in Abbildung 8 dargestellt, den Prozess zum Konfigurieren von Commvault Complete Backup & Recovery mit SafeMode auf FlashBlade. Commvault-Datenschutz wendet die Konzepte eines CommServe-Servers und von MediaAgents an. Der CommServe-Server ermöglicht die administrative Steuerung der Lösung und die MediaAgents verschieben und speichern Backup-Images von Clients und stellen Daten aus Backup-Images wieder her. Obwohl beide Komponenten der Lösung während der Tests geschützt waren, liegt in Abbildung 8 der Fokus auf der Wiederherstellung von ***Storage Device_2*** aus einem Point-in-Time-SafeMode-Snapshot (von einem Zeitpunkt vor dem Ransomware-Angriff). Wie aus dem Abschnitt „SafeMode Snapshot Recovery Points“ (Wiederherstellungspunkte für SafeMode-Snapshots) rechts unten in Abbildung 8 hervorgeht, wurde ein SafeMode-Snapshot vom 9. Dezember verwendet, um eine erfolgreiche Wiederherstellung (auf einen Zustand vor dem Ransomware-Angriff) von Commvault Storage Device_2 durchzuführen.

Abbildung 8. FlashBlade SafeMode mit Commvault Complete Backup & Recovery



Quelle: Enterprise Strategy Group

Warum ist das wichtig?

Wenn man ins Büro kommt und erfährt, dass ein Ransomware-Angriff erfolgt ist, ist einem sofort klar, dass es kein guter Tag wird. Noch schlimmer wird es, wenn man feststellt, dass auch die Backups beschädigt wurden. Cyberkriminelle haben es heute nicht nur auf Primärdaten von Endbenutzern abgesehen, sondern auch auf NAS-Dateisysteme und Objektspeicher, auf die viele Datenschutzlösungen zum Speichern von Backups zurückgreifen.

Wäre es nicht großartig, ein zusätzliches Maß an Schutz mit der richtigen Performance zu haben, sodass man sicher sein kann, dass Backup-Daten jederzeit einsatzbereit sind und Wiederherstellungs-SLAs erfüllt oder übertroffen werden können, wenn dies am dringendsten nötig ist?

Die ESG hat bestätigt, dass FlashBlade mit SafeMode dazu beitragen kann, Ihre Datenschutzumgebung noch sicherer zu machen. In Kombination mit Ihrer Datenschutzanwendung kann es dazu beitragen, dass die Daten in Ihren Backup-Images so sind, wie Sie es erwarten. Mit anderen Worten: Wenn es darauf ankommt, sind sie einsatzbereit.

Die ganze Wahrheit

Es ist nicht ungewöhnlich, immer wieder Berichte über Ransomware-Angriffe zu hören, die auf Organisationen aller Größenordnungen – von staatlichen Regierungsbehörden bis hin zum Gesundheitswesen, den Medien usw. – ausgeübt wurden. Diese Angriffe sind nicht einfach nur unangenehm, sondern bedeuten, dass Unternehmen viel Zeit aufwenden und erhebliche Einnahmeeinbußen hinnehmen müssen, um sich von diesen Vorfällen zu erholen. Obwohl es ideal wäre, alle Angriffe zu verhindern, müssen Organisationen über Strategien verfügen, um im Falle eines Angriffs die Geschäfte wieder zum Laufen zu bringen. Das Sichern von Daten mithilfe von Datenschutzlösungen ist ein Anfang, doch es kann noch mehr getan werden, um unbeschädigte und unverfälschte Backups für eine schnellere Wiederherstellung verfügbar zu halten.

Pure Storage SafeMode auf FlashBlade ermöglicht es Unternehmen, Daten-Backups vor Ransomware-Angriffen sowie vor versehentlicher Löschung und mutwillig schädlichen Aktivitäten von Storage-Administratoren zu schützen. Von SafeMode geschützte Snapshots können nicht geändert oder dauerhaft aus FlashBlade gelöscht werden, was Unternehmen die schnelle Wiederherstellung von Daten erleichtert. SafeMode ist eine Funktion, die nur durch den technischen Support von Pure Storage auf Anfrage des Kunden und mit einem autorisierten Vertreter, der direkt mit dem technischen Support von Pure Storage zusammenarbeitet, aktiviert werden kann. Unternehmen können SafeMode-Snapshots auch in Kombination mit Datenschutzlösungen von anderen Anbietern verwenden, um Datenschutz- und Wiederherstellungsprozesse zu verbessern.

ESG hat bestätigt, dass Pure Storage SafeMode auf FlashBlade verhindern kann, dass Datenbackups, die durch einen SafeMode-Snapshot geschützt sind, durch Ransomware oder andere Ereignisse verändert, gelöscht oder verschlüsselt werden. Wir haben außerdem die Integration der Lösung mit drei branchenweit anerkannten Datenschutzlösungen untersucht und festgestellt, dass sie mit allen drei Schutzschemata recht einfach zu konfigurieren ist, da sie einfach als Plattensicherungsziel fungiert, jedoch mit den Vorteilen der SafeMode-Schutzfunktionen.

Wenn Sie Ihre Datenschutzinfrastruktur stärken möchten und einen besseren Schutz vor Bedrohungen wie Ransomware oder sogar Angriffen durch mutwillig handelnde Administratoren oder Mitarbeiter möchten, ist FlashBlade mit SafeMode von Pure Storage nach Ansicht der ESG eine ernsthafte Überlegung wert.