FlexPod, die Lösung gegen Ransomware

FlexPod

NetApp
October 30, 2025

Inhalt

FlexPod, die Lösung gegen Ransomware

TR-4802: FlexPod, die Lösung gegen Ransomware

Arvind Ramakrishnan, NetApp

In Zusammenarbeit mit: 

Um Ransomware zu verstehen, ist es notwendig, zunächst ein paar wichtige Punkte zur Kryptografie zu verstehen. Kryptografische Methoden ermöglichen die Verschlüsselung von Daten mit einem gemeinsamen geheimen Schlüssel (symmetrische Schlüsselverschlüsselung) oder einem Schlüsselpaar (asymmetrische Verschlüsselungsschlüsselverschlüsselung). Einer dieser Schlüssel ist ein weit verbreiteter öffentlicher Schlüssel und der andere ist ein nicht offenbarter privater Schlüssel.

Ransomware ist eine Art von Malware, die auf Kryptovirologie basiert, die die Verwendung von Kryptografie ist, um schädliche Software zu erstellen. Diese Malware kann sowohl symmetrische und asymmetrische Schlüssel Verschlüsselung zu machen, um ein Opfer Daten zu sperren und ein Lösegeld zu verlangen, um den Schlüssel zur Entschlüsselung der Daten des Opfers.

Wie funktioniert Ransomware?

In den folgenden Schritten wird beschrieben, wie Ransomware die Daten des Opfers mit Kryptografie verschlüsselt, ohne dabei Möglichkeiten zur Entschlüsselung oder Wiederherstellung des Opfers haben zu müssen:

1. Der Angreifer generiert ein Schlüsselpaar wie bei der asymmetrischen Schlüsselverschlüsselung. Der erzeugte öffentliche Schlüssel wird innerhalb der Malware abgelegt und anschließend die Malware freigegeben.
2. Nachdem die Malware den Computer oder das System des Opfers eingegeben hat, erzeugt sie einen zufällig symmetrischen Schlüssel, indem sie einen Pseudorandom Number Generator (PRNG) oder einen anderen praktikablen Zufallszahlengenerator verwendet.
3. Die Malware verwendet diesen symmetrischen Schlüssel, um die Daten des Opfers zu verschlüsseln. Es verschlüsselt schließlich den symmetrischen Schlüssel, indem der Angreifer den öffentlichen Schlüssel verwendet, der in die Malware eingebettet wurde. Die Ausgabe dieses Schritts ist ein asymmetrischer Chiffretext des verschlüsselten symmetrischen Schlüssels und des symmetrischen Chiffretextes der Daten des Opfers.
4. Die Malware zerosiert (löscht) die Daten des Opfers und den symmetrischen Schlüssel, der verwendet wurde, um die Daten zu verschlüsseln, so dass kein Spielraum für die Wiederherstellung.
5. Das Opfer zeigt nun den asymmetrischen Chiffretext des symmetrischen Schlüssels und einen Lösegeld-Wert, der bezahlt werden muss, um den symmetrischen Schlüssel zu erhalten, der verwendet wurde, um die Daten zu verschlüsseln.
6. Das Opfer zahlt das Lösegeld und teilt den asymmetrischen Chiffretext mit dem Angreifer. Der Angreifer entschlüsselt den Chiffretext mit seinem privaten Schlüssel, was zu dem symmetrischen Schlüssel führt.

7. Der Angreifer teilt diesen symmetrischen Schlüssel mit dem Opfer, der verwendet werden kann, um alle Daten zu entschlüsseln und somit vom Angriff zu erholen.

Herausforderungen

Bei einem Ransomware-Angriff stehen Einzelpersonen und Unternehmen vor folgenden Herausforderungen:

- Die wichtigste Herausforderung besteht darin, dass sie die Produktivität des Unternehmens oder der Person sofort belastet. Es braucht Zeit, in den Status der Normalität zurückzukehren, da alle wichtigen Dateien wieder gewonnen werden müssen und die Systeme gesichert werden müssen.
- Sie könnten zu einer Verletzung der Daten führen, die vertrauliche und vertrauliche Informationen enthält, die Kunden oder Kunden gehören, und zu einer Krisensituation führen, die ein Unternehmen eindeutig vermeiden möchte.
- Es besteht eine sehr gute Möglichkeit, dass Daten in die falschen Hände geraten oder vollständig gelöscht werden. Dies führt zu einem Punkt ohne Rückkehr, der für Unternehmen und Einzelpersonen verheerend sein könnte.
- Nach der Bezahlung des Lösegeld gibt es keine Garantie, dass der Angreifer den Schlüssel zur Wiederherstellung der Daten zur Verfügung stellt.
- Es besteht keine Gewissheit, dass der Angreifer die Übertragung sensibler Daten absieht, obwohl er das Lösegeld bezahlt.
- In großen Unternehmen ist die Identifizierung von Schlupflöcher, die zu einem Ransomware-Angriff geführt haben, eine mühsame Aufgabe, und es ist mit großem Aufwand auch möglich, alle Systeme zu sichern.

Wer ist gefährdet?

Jeder kann von Ransomware angegriffen werden, auch von Einzelpersonen und großen Unternehmen. Unternehmen, die keine klar definierten Sicherheitsmaßnahmen und -Praktiken implementieren, sind noch anfälliger für solche Angriffe. Die Auswirkungen des Angriffs auf ein großes Unternehmen können mehrere Male größer sein als das, was ein einzelner ertragen könnte.

Ransomware macht ca. 28 % aller Malware-Angriffe aus. Mit anderen Worten: Mehr als jeder vierte Malware-Vorfall ist ein Ransomware-Angriff. Ransomware kann sich automatisch und wahllos über das Internet verbreiten, und, wenn es einen Sicherheitsverfall gibt, kann es in die Systeme des Opfers und weiter auf andere verbundene Systeme zu verbreiten. Angreifer neigen dazu, Personen oder Organisationen anzugreifen, die sehr viel File Sharing betreiben, sehr sensible und kritische Daten haben oder einen unzureichenden Schutz gegen Angriffe bieten.

Angreifer neigen dazu, sich auf die folgenden potenziellen Ziele zu konzentrieren:

- Universitäten und Studentengemeinden
- Regierungsbehörden und Behörden um
- Krankenhäuser
- Banken

Dies ist keine umfassende Liste von Zielen. Sie können sich nicht vor Angriffen schützen, wenn Sie außerhalb einer dieser Kategorien fallen.

Wie kommt Ransomware in ein System oder verteilt?

Ransomware kann auf verschiedene Weise in ein System eintreten oder auf andere Systeme übergreifen. In

der heutigen Welt sind fast alle Systeme über das Internet, LANs, WANs usw. miteinander verbunden. Die Menge der Daten, die zwischen diesen Systemen generiert und ausgetauscht werden, steigt nur.

Ransomware kann sich am häufigsten mit vielen Methoden ausbreiten und auf die Daten zugreifen – wir nutzen sie täglich.

- E-Mail
- P2P-Netzwerke
- Dateien werden heruntergeladen
- Soziale Netzwerke
- Mobilgeräte
- Verbindung zu unsicheren öffentlichen Netzwerken herstellen
- Zugriff auf Web-URLs

Konsequenzen eines Datenverlusts

Die Folgen oder Auswirkungen von Datenverlusten können breiter ausfallen, als Unternehmen erwarten würden. Die Auswirkungen können variieren, je nach Dauer der Ausfallzeit oder Zeitraum, in dem ein Unternehmen keinen Zugriff auf seine Daten hat. Je länger der Angriff andauere, desto größer ist der Einfluss auf die Einnahmen, Marke und den Ruf der Organisation. Zudem kann sich ein Unternehmen mit rechtlichen Fragen und einem starken Produktivitätsrückgang konfrontiert sehen.

Während diese Probleme im Laufe der Zeit weiter bestehen, beginnen sie zu vergrößern und könnten am Ende eine Kultur einer Organisation ändern, je nachdem, wie sie auf den Angriff reagiert. In der heutigen Welt verbreiten sich Informationen schnell, und negative Nachrichten über eine Organisation können ihren Ruf dauerhaft schädigen. Ein Unternehmen könnte hohe Einbußen bei Datenverlusten verzeichnen, die letztendlich zur Schließung eines Unternehmens führen können.

Finanzielle Auswirkungen

Laut einer aktuellen "McAfee-Bericht"Die durch Cyberkriminalität verursachten globalen Kosten belaufen sich auf rund 600 Milliarden US-Dollar, was etwa 0.8 % des weltweiten BIP entspricht. Wenn dieser Betrag mit der weltweit wachsenden Internetwirtschaft von 4.2 Billionen Dollar verglichen wird, entspricht dies einer Wachstumssteuer von 14 %.

Ransomware ist einen bedeutenden Anteil dieser finanziellen Kosten. Die durch Ransomware-Angriffe verursachten Kosten im Jahr 2018 belaufen sich auf ca. 8 Milliarden US-Dollar—einem Betrag, der 2019 auf 11.5 Milliarden US-Dollar geschätzt wird.

Welche Lösung bietet sich an?

Eine Wiederherstellung nach einem Ransomware-Angriff mit minimaler Downtime ist nur durch die Implementierung eines proaktiven Disaster-Recovery-Plans möglich. Die Fähigkeit, sich von einem Angriff zu erholen, ist gut, aber einen Angriff insgesamt zu verhindern ist ideal.

Obwohl es verschiedene Fronten gibt, die Sie überprüfen und beheben müssen, um einen Angriff zu verhindern, ist die Kernkomponente, mit der Sie einen Angriff verhindern oder beheben können, das Rechenzentrum.

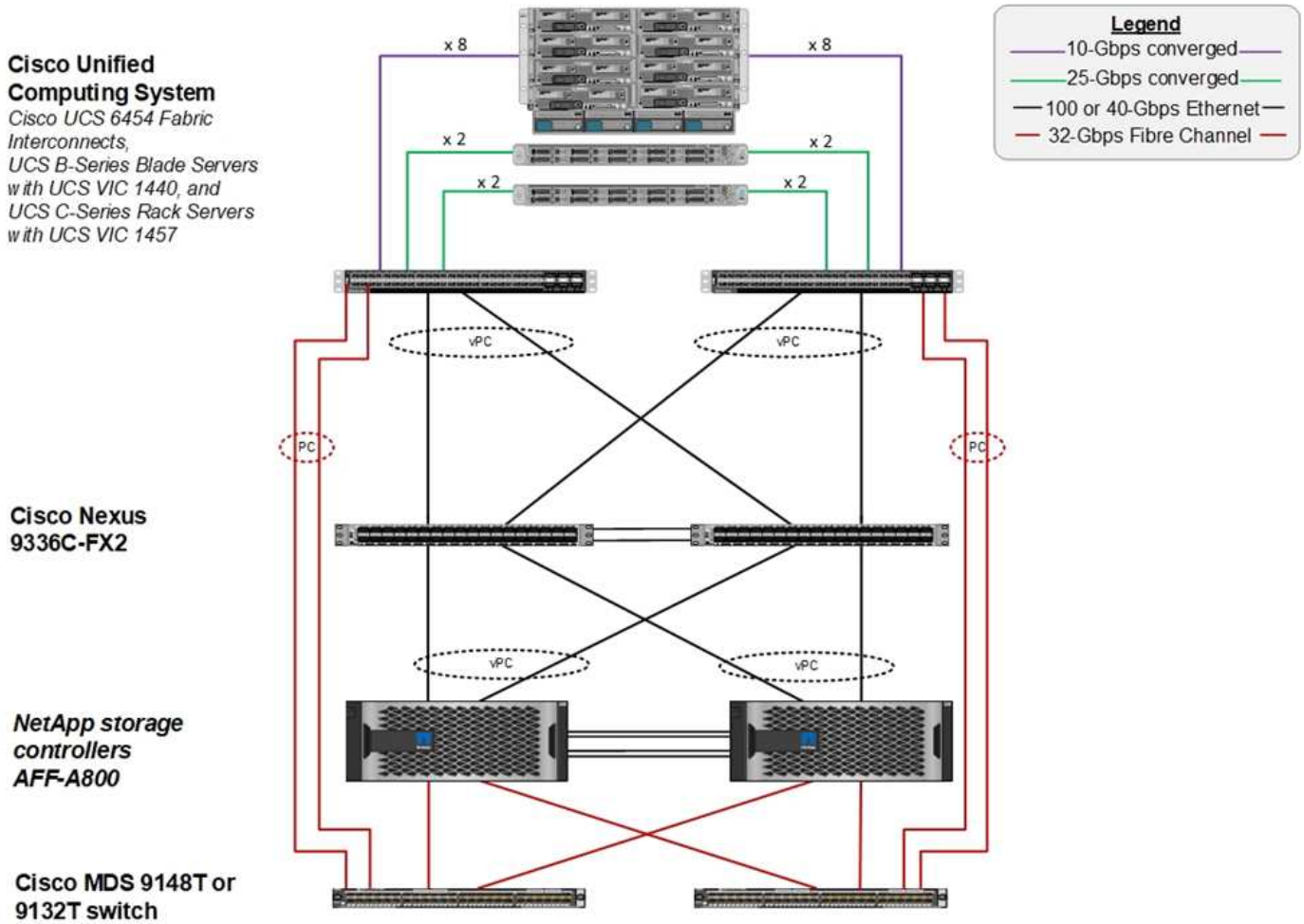
Das Datacenter-Design und die Funktionen, die es zur Sicherung von Endpunkten in Netzwerk, Computing und Storage bietet, spielen eine entscheidende Rolle beim Aufbau einer sicheren Umgebung für den täglichen

Betrieb. In diesem Dokument wird erläutert, wie die Funktionen einer Hybrid-Cloud-Infrastruktur von FlexPod bei einem Angriff eine schnelle Daten-Recovery ermöglichen und außerdem Angriffe komplett verhindern können.

Übersicht über FlexPod

FlexPod ist eine vorkonfigurierte, integrierte und validierte Architektur, die Server der Cisco Unified Computing System (Cisco UCS), Switches der Cisco Nexus Familie, Cisco MDS Fabric Switches und NetApp Storage Arrays in einer einzigen flexiblen Architektur kombiniert. Die Lösungen von FlexPod wurden für Hochverfügbarkeit ohne Single Points of Failure konzipiert und sorgen gleichzeitig für Kosteneffizienz und Designflexibilität, um eine Vielzahl von Workloads zu unterstützen. Ein FlexPod-Design kann verschiedene Hypervisoren und Bare Metal-Server unterstützen und sich ebenfalls entsprechend den Workload-Anforderungen des Kunden dimensionieren und optimieren lassen.

Die Abbildung unten zeigt die FlexPod Architektur und hebt die Hochverfügbarkeit auf allen Ebenen des Stacks deutlich hervor. Die Infrastrukturkomponenten von Storage, Netzwerk und Computing sind so konfiguriert, dass bei einem Ausfall einer Komponente sofort ein Failover zum verbleibenden Partner möglich ist.



Ein großer Vorteil für ein FlexPod System ist, dass es vorab integriert und für mehrere Workloads validiert wurde. Für jede Lösungsvalidierung werden detaillierte Design- und Implementierungsleitfäden veröffentlicht.

In diesen Dokumenten finden Sie Best Practices, die Sie für Workloads einsetzen müssen, damit sie nahtlos auf FlexPod ausgeführt werden können. Diese Lösungen basieren auf erstklassigen Computing-, Netzwerk- und Storage-Produkten sowie einer Vielzahl von Funktionen, die auf Sicherheit und Härtung der gesamten Infrastruktur liegen.

"IBM X-Force Threat Intelligence Index" staaten, „menschliche Fehler, die für zwei Drittel der kompromittierten Aufzeichnungen verantwortlich sind, einschließlich historischer 424 % Sprung in die falsch konfigurierte Cloud-Infrastruktur.“

Mit einem FlexPod-System vermeiden Sie Fehlkonfiguration Ihrer Infrastruktur, indem Sie Automatisierung durch Ansible-Playbooks verwenden, die ein lückenloses Setup der Infrastruktur gemäß den Best Practices in Cisco Validated Designs (CVDs) und NetApp Verified Architectures (NVAs) durchführen.

Schutzmaßnahmen gegen Ransomware

In diesem Abschnitt werden die wichtigsten Funktionen der NetApp ONTAP Datenmanagement-Software sowie die Tools für Cisco UCS und Cisco Nexus erläutert, mit denen Sie gegen Ransomware-Angriffe sichern und wiederherstellen können.

NetApp ONTAP

Die ONTAP Software bietet viele nützliche Funktionen für die Datensicherung, von denen die meisten für Kunden mit einem ONTAP System kostenlos sind. Sie können die folgenden Funktionen zu jeder Zeit nutzen, um Daten vor Angriffen zu schützen:

- **NetApp Snapshot Technologie.** Eine Snapshot-Kopie ist ein schreibgeschütztes Image eines Volumes, das den Status eines Filesystems zu einem bestimmten Zeitpunkt erfasst. Diese Kopien helfen, Daten ohne Auswirkungen auf die System-Performance zu sichern und belegen gleichzeitig nicht viel Storage. NetApp empfiehlt, einen Zeitplan für die Erstellung von Snapshot-Kopien zu erstellen. Sie sollten auch eine lange Aufbewahrungszeit halten, weil einige Malware kann ruhend gehen und dann wieder aktivieren Wochen oder Monate nach einer Infektion. Im Falle eines Angriffs kann das Volume mithilfe einer Snapshot-Kopie zurückgesetzt werden, die vor der Infektion erstellt wurde.
- **NetApp SnapRestore Technologie.** SnapRestore Daten-Recovery-Software ist extrem nützlich, um Daten zu beschädigen oder nur die Datei Inhalte zurücksetzen. SnapRestore setzt die Attribute eines Volume nicht zurück. Dies ist wesentlich schneller als ein Administrator, indem er Dateien aus der Snapshot Kopie in das aktive Filesystem kopiert. Die Geschwindigkeit, mit der Daten wiederhergestellt werden können, ist hilfreich, wenn viele Dateien so schnell wie möglich wiederhergestellt werden müssen. Wird ein Angriff verursacht, hilft dieser äußerst effiziente Recovery-Prozess der schnellen Wiederherstellung des Geschäftsbetriebs.
- **NetApp SnapCenter Technologie.** die SnapCenter Software nutzt Storage-basierte Backup- und Replizierungsfunktionen von NetApp, um applikationskonsistente Datensicherung zu ermöglichen. Diese Software lässt sich in Enterprise-Applikationen integrieren und bietet applikationsspezifische und datenbankspezifische Workflows, um die Anforderungen von Applikations-, Datenbank- und Administratoren virtueller Infrastrukturen zu erfüllen. SnapCenter bietet eine unkomplizierte Enterprise-Plattform zur sicheren Koordinierung und Verwaltung der Datensicherung für alle Applikationen, Datenbanken und Filesysteme. Die Fähigkeit zur applikationskonsistenten Datensicherung ist bei der Datenwiederherstellung wichtig, da Applikationen schneller in einem konsistenten Status wiederhergestellt werden können.
- **NetApp SnapLock Technologie.** SnapLock stellt ein speziellen Volume zur Verfügung, in dem Dateien gespeichert und in einen nicht löschbaren, nicht überschreibbaren Zustand versetzt werden können. Die Produktionsdaten des Benutzers, die sich in einem FlexVol Volume befinden, können durch NetApp SnapMirror bzw. SnapVault Technologie gespiegelt oder in ein SnapLock Volume archiviert werden. Die

Dateien im SnapLock Volume, das Volume selbst und das Hosting-Aggregat können bis zum Ende der Aufbewahrungsdauer nicht gelöscht werden.

- **NetApp FPolicy Technologie.** Verwenden Sie FPolicy Software, um Angriffe zu verhindern, indem Operationen auf Dateien mit bestimmten Erweiterungen dierlauben. Ein FPolicy-Ereignis kann für bestimmte Dateivorgänge ausgelöst werden. Das Ereignis ist mit einer Richtlinie verknüpft, die die Engine aufruft, die es verwenden muss. Sie können eine Richtlinie mit einer Reihe von Dateierweiterungen konfigurieren, die möglicherweise Ransomware enthalten könnten. Wenn eine Datei mit einer nicht zulässigen Erweiterung versucht, einen nicht autorisierten Vorgang auszuführen, verhindert FPolicy die Ausführung dieses Vorgangs.

Netzwerk: Cisco Nexus

Die Cisco NX OS-Software unterstützt die NetFlow-Funktion, die eine verbesserte Erkennung von Netzwerkanomalien und -Sicherheit ermöglicht. NetFlow erfasst die Metadaten jedes Gesprächs im Netzwerk, die an der Kommunikation beteiligten Parteien, das verwendete Protokoll und die Dauer der Transaktion. Nachdem die Informationen aggregiert und analysiert wurden, können sie einen Einblick in das normale Verhalten geben.

Die gesammelten Daten ermöglichen außerdem die Identifizierung fragwürdiger Aktivitätsmuster, wie etwa die Verbreitung von Malware im Netzwerk, die ansonsten unbemerkt bleiben kann.

NetFlow verwendet Flows, um Statistiken für die Netzwerküberwachung bereitzustellen. Ein Flow ist ein unidirektionaler Strom von Paketen, der auf einer Quellschnittstelle (oder VLAN) ankommt und die gleichen Werte für die Schlüssel hat. Ein Schlüssel ist ein identifizierter Wert für ein Feld innerhalb des Pakets. Sie erstellen einen Flow mithilfe eines Flow-Datensatzes, um die eindeutigen Tasten für Ihren Flow zu definieren. Sie können die Daten, die NetFlow für Ihre Ströme sammelt, mit Hilfe eines Flow-Exporterers in einen Remote NetFlow Collector, wie z. B. Cisco Stealthwatch, exportieren. Stealthwatch verwendet diese Informationen für die kontinuierliche Überwachung des Netzwerks und bietet Bedrohungserkennung in Echtzeit sowie eine Forensik zum Vorfallsreaktion, falls ein Ransomware-Ausbruch auftritt.

Computing: Cisco UCS

Cisco UCS ist der Computing-Endpunkt in einer FlexPod Architektur. Sie können mehrere Cisco Produkte verwenden, um diese Stack-Ebene auf Betriebssystemebene zu sichern.

Sie können die folgenden wichtigen Produkte auf der Computing- oder Anwendungsebene implementieren:

- **Cisco Advanced Malware Protection (AMP) for Endpoints.** Diese Lösung wird auf Microsoft Windows und Linux Betriebssystemen unterstützt und umfasst Funktionen für Prävention, Erkennung und Reaktion. Diese Sicherheitssoftware verhindert Verstöße, blockiert Malware am Einstiegspunkt und überwacht und analysiert kontinuierlich die Datei- und Prozessaktivitäten, um Bedrohungen schnell zu erkennen, einzudämmen und zu beseitigen, die den Schutz vor der Front-Line-Lösung ausweichen können.

  Die Komponente „bösartiger Aktivitätsschutz“ (MAP) von AMP überwacht kontinuierlich alle Endpoint-Aktivitäten und ermöglicht die Laufzeiterkennung und das Blockieren des anormalen Verhaltens eines laufenden Programms auf dem Endpunkt. Wenn beispielsweise das Endpunktverhalten auf Ransomware hinweist, werden die abgebrochene Prozesse beendet, um Endpunktverschlüsselung zu verhindern und den Angriff zu stoppen.

- **Cisco Advanced Malware Protection for Email Security.** E-Mails sind das erste Fahrzeug, um Malware zu verbreiten und Cyber-Angriffe durchzuführen. Im Durchschnitt werden an einem einzigen Tag rund 100 Milliarden E-Mails ausgetauscht, die Angreifern einen ausgezeichneten Penetrationsvektor in die Systeme des Benutzers bieten. Daher ist es absolut unerlässlich, sich gegen diese Angriffslinie zu verteidigen.

AMP analysiert E-Mails auf Bedrohungen wie Zero-Day-Exploits und entstickende Malware, die in bösartigen Anhängen verborgen sind. Darüber hinaus nutzt es branchenführende URL-Informationen, um schädliche Links zu bekämpfen. Anwender erhalten erweiterten Schutz vor Spear-Phishing, Ransomware und anderen anspruchsvollen Angriffen.

- **Intrusion Prevention System der nächsten Generation (NGIPS).** Cisco Firepower NGIPS kann als physische Appliance im Datacenter oder als virtuelle Appliance auf VMware (NGIPSv für VMware) eingesetzt werden. Dieses hocheffiziente Abwehrsystem für Angriffe sorgt für zuverlässige Leistung und niedrige Gesamtbetriebskosten. Der Schutz vor Bedrohungen kann durch optionale Abonnementlizenzen erweitert werden, um AMP, Transparenz und Kontrolle von Anwendungen sowie URL-Filterfunktionen bereitzustellen. Virtualisierte NGIPS überprüft den Datenverkehr zwischen Virtual Machines (VMs) und erleichtert die Bereitstellung und das Management von NGIPS-Lösungen an Standorten mit begrenzten Ressourcen. Dadurch wird der Schutz sowohl für physische als auch für virtuelle Ressourcen erhöht.

Sichern Sie Ihre Daten und stellen Sie sie auf FlexPod wieder her

Dieser Abschnitt beschreibt, wie die Daten eines Endbenutzers im Falle eines Angriffs wiederhergestellt werden können und wie Angriffe durch die Verwendung eines FlexPod-Systems verhindert werden können.

Testbed-Übersicht

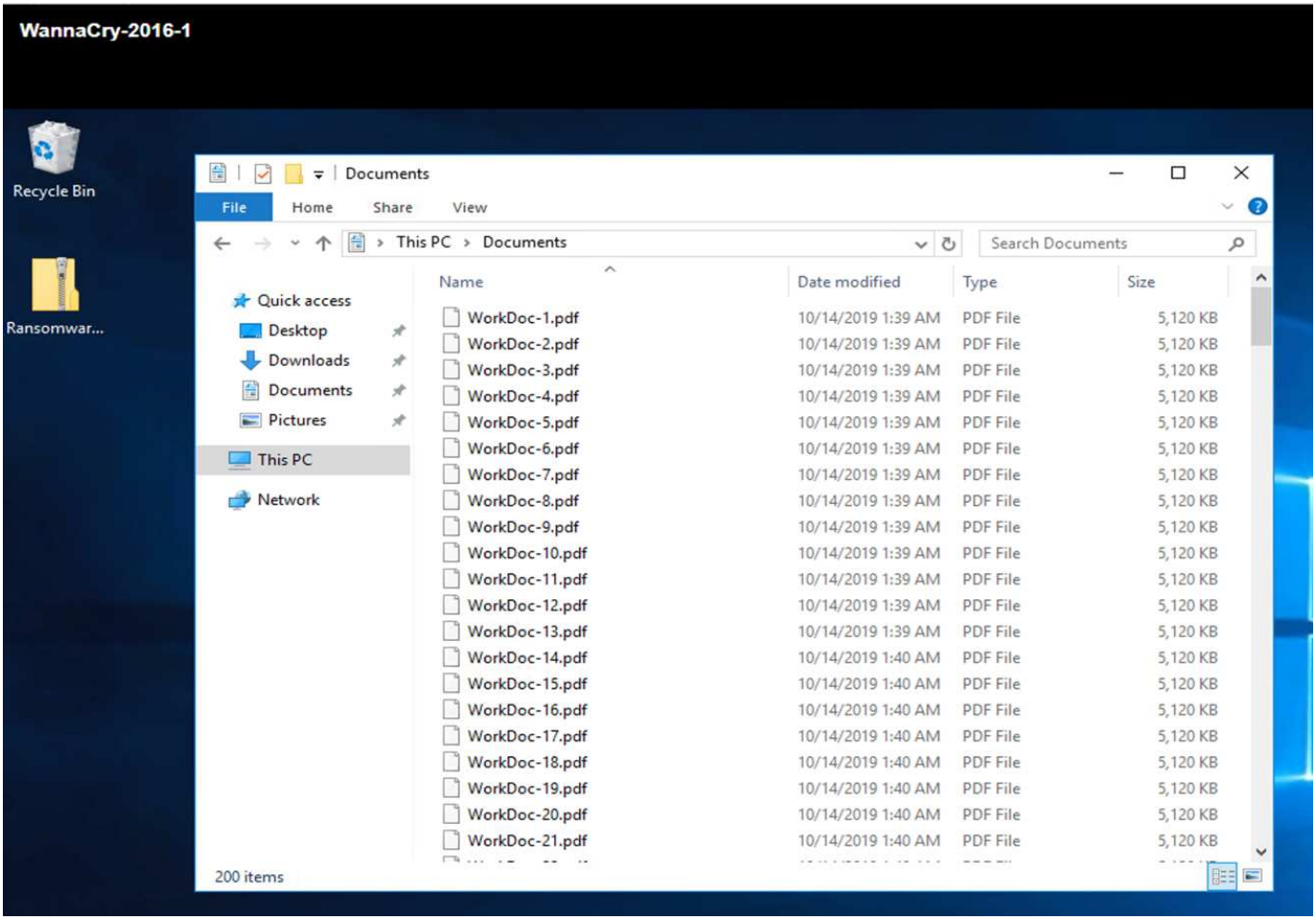
Zur Präsentation von FlexPod-Erkennung, -Korrektur und -Vorbeugung wurde ein Testbed auf Basis der Richtlinien erstellt, die in der neuesten CVD-Plattform angegeben sind, die zum Zeitpunkt der Erstellung dieses Dokuments verfügbar sind: "FlexPod Datacenter mit VMware vSphere 6.7 U1, Cisco UCS der vierten Generation und NetApp AFF A-Series CVD".

In der VMware vSphere Infrastruktur wurde eine Windows 2016 VM mit einer CIFS-Freigabe durch die NetApp ONTAP Software implementiert. Dann wurde NetApp FPolicy auf der CIFS-Freigabe konfiguriert, um die Ausführung von Dateien mit bestimmten Extension-Typen zu verhindern. Darüber hinaus wurde die NetApp SnapCenter Software implementiert, um die Snapshot Kopien der VMs in der Infrastruktur zu managen, um applikationskonsistente Snapshot Kopien zu ermöglichen.

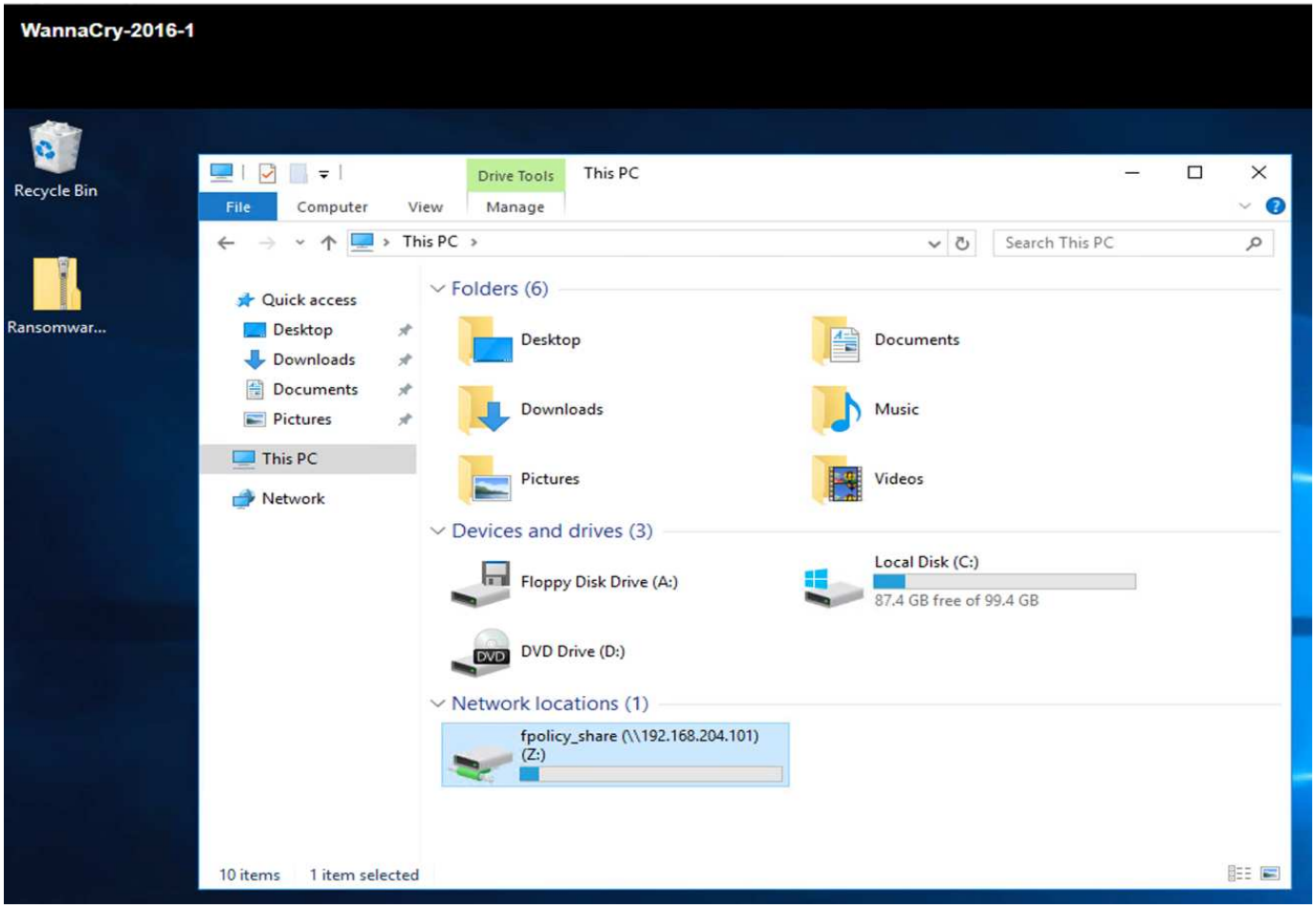
Status der VM und ihrer Dateien vor einem Angriff

In diesem Abschnitt werden der Status der Dateien vor einem Angriff auf die VM und die ihr zugewiesene CIFS-Freigabe angezeigt.

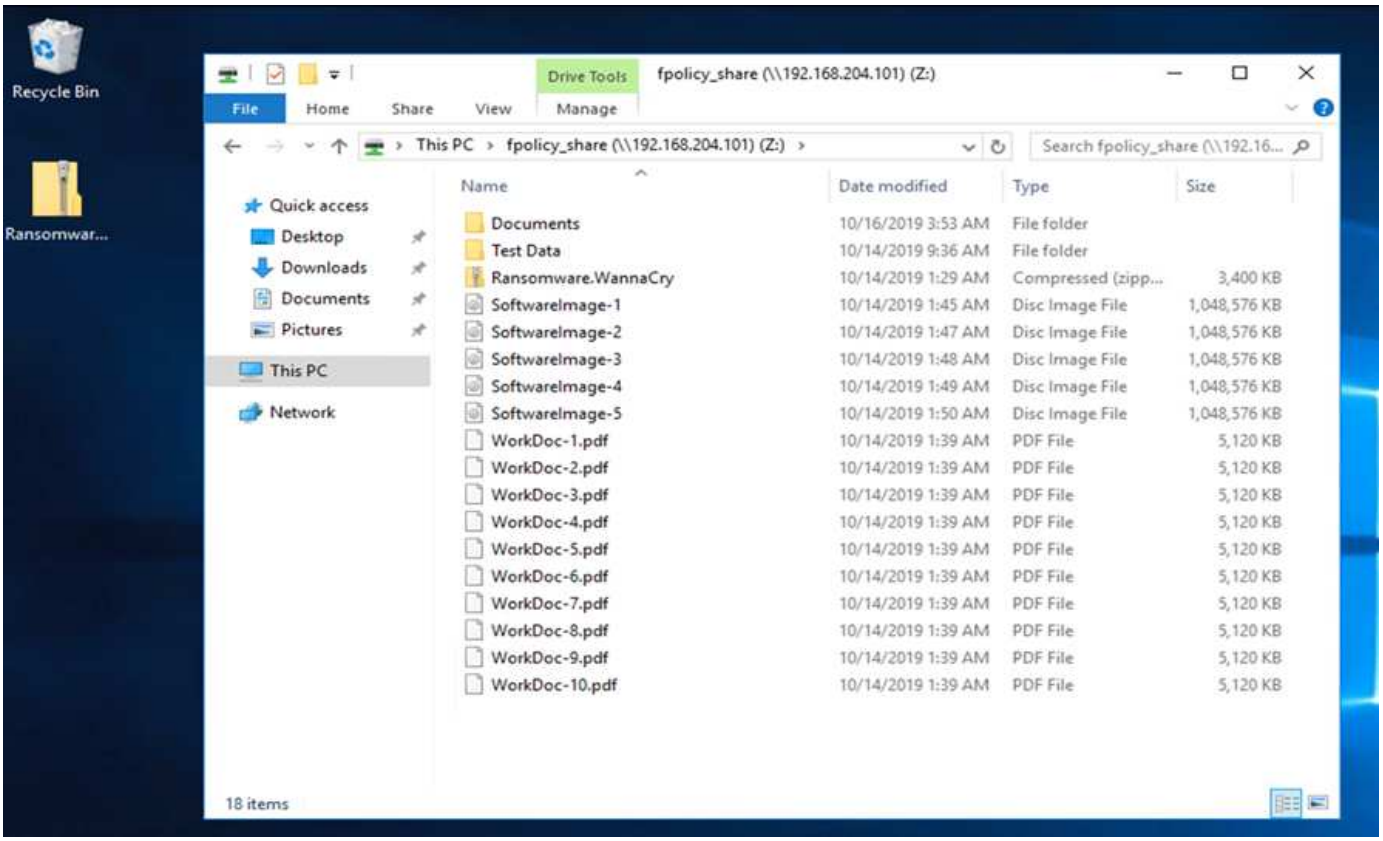
Der Ordner Dokumente der VM hatte eine Reihe von PDF-Dateien, die noch nicht durch die WannaCry Malware verschlüsselt wurden.



Der folgende Screenshot zeigt die CIFS-Freigabe, die der VM zugeordnet war.



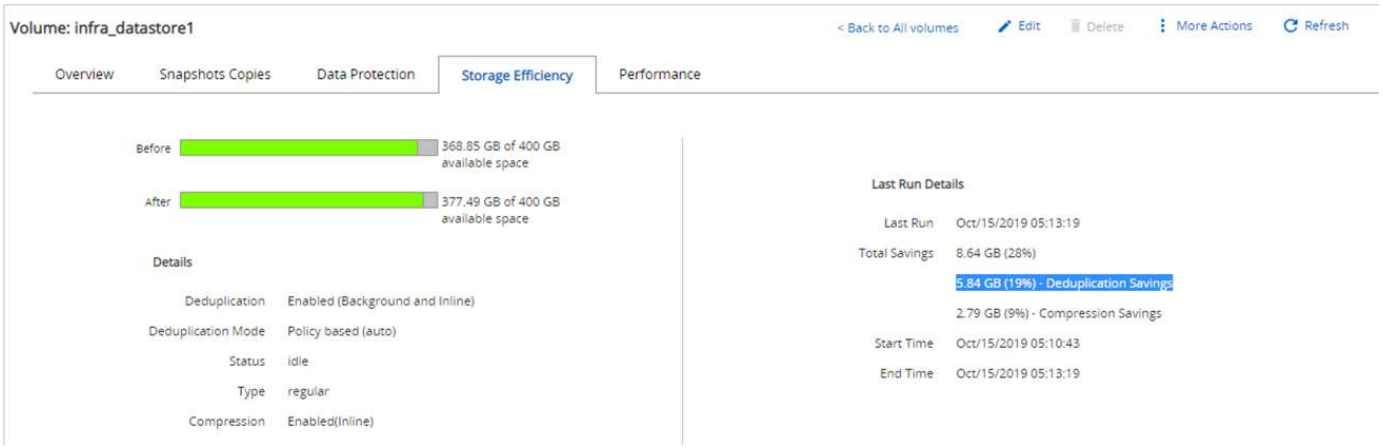
Der folgende Screenshot zeigt die Dateien auf der CIFS-Freigabe `fpolicy_share` Die noch nicht durch die WannaCry-Malware verschlüsselt wurden.



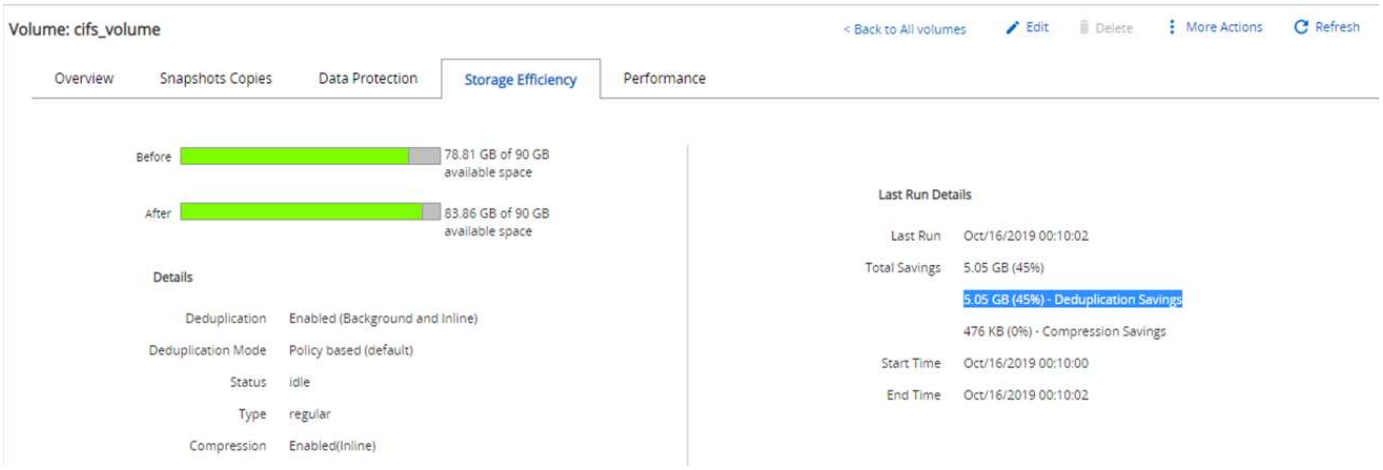
Deduplizierung und Snapshot-Informationen vor einem Angriff

Details zur Storage-Effizienz und die Größe der Snapshot-Kopie vor einem Angriff werden als Referenz während der Erkennungsphase angezeigt.

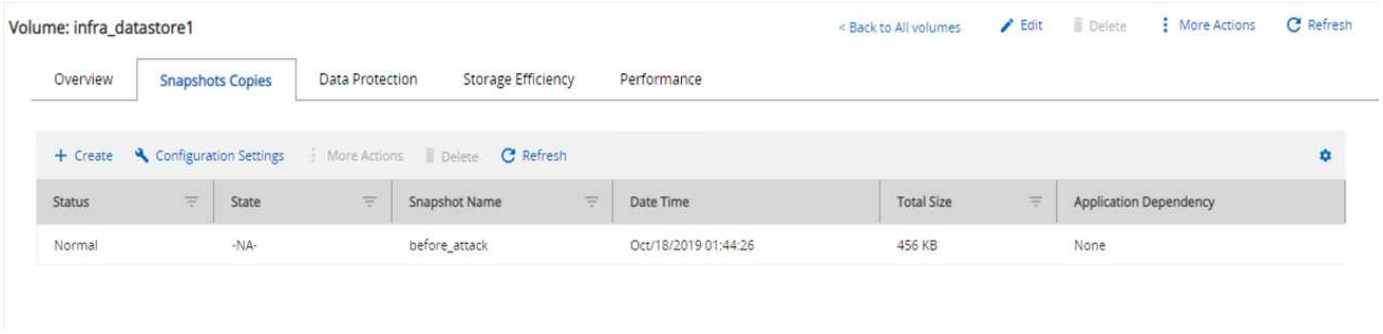
Storage-Einsparungen von 19 % wurden durch Deduplizierung auf dem Volume, das die VM hostet, erzielt.



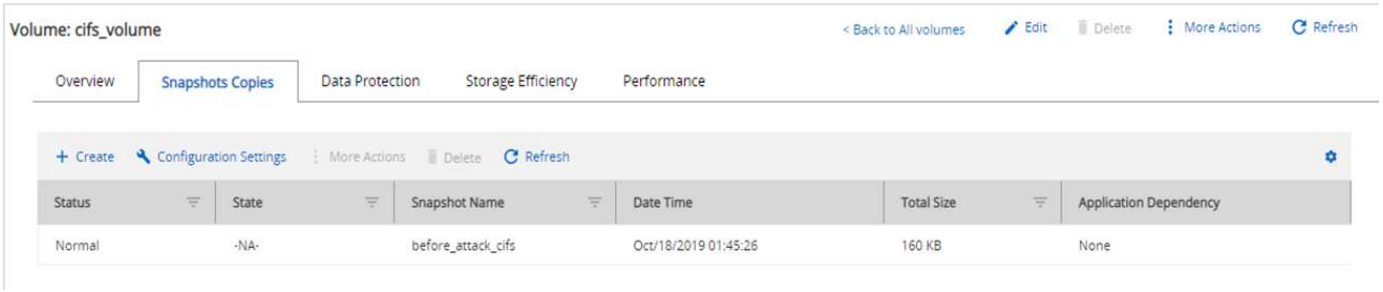
Durch Deduplizierung beim CIFS-Share wurden Storage-Einsparungen von 45 % erzielt `fpolicy_share`.



Für das Volume, das die VM hostet, wurde eine Snapshot-Kopie von 456 KB beobachtet.



Für den CIFS-Share wurde eine Snapshot Kopie von 160 KB beobachtet `fpolicy_share`.



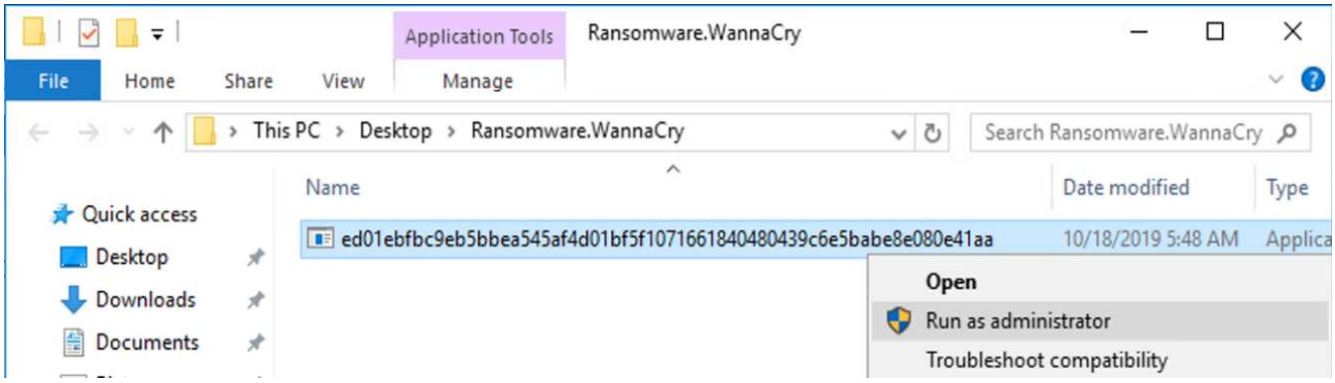
WannaCry-Infektion auf VM und CIFS-Share

In diesem Abschnitt zeigen wir, wie die WannaCry-Malware in die FlexPod-Umgebung eingeführt wurde und welche Änderungen am System beobachtet wurden.

Die folgenden Schritte zeigen, wie die WannaCry-Malware-Binärdatei in die VM eingeführt wurde:

1. Die gesicherte Malware wurde extrahiert.

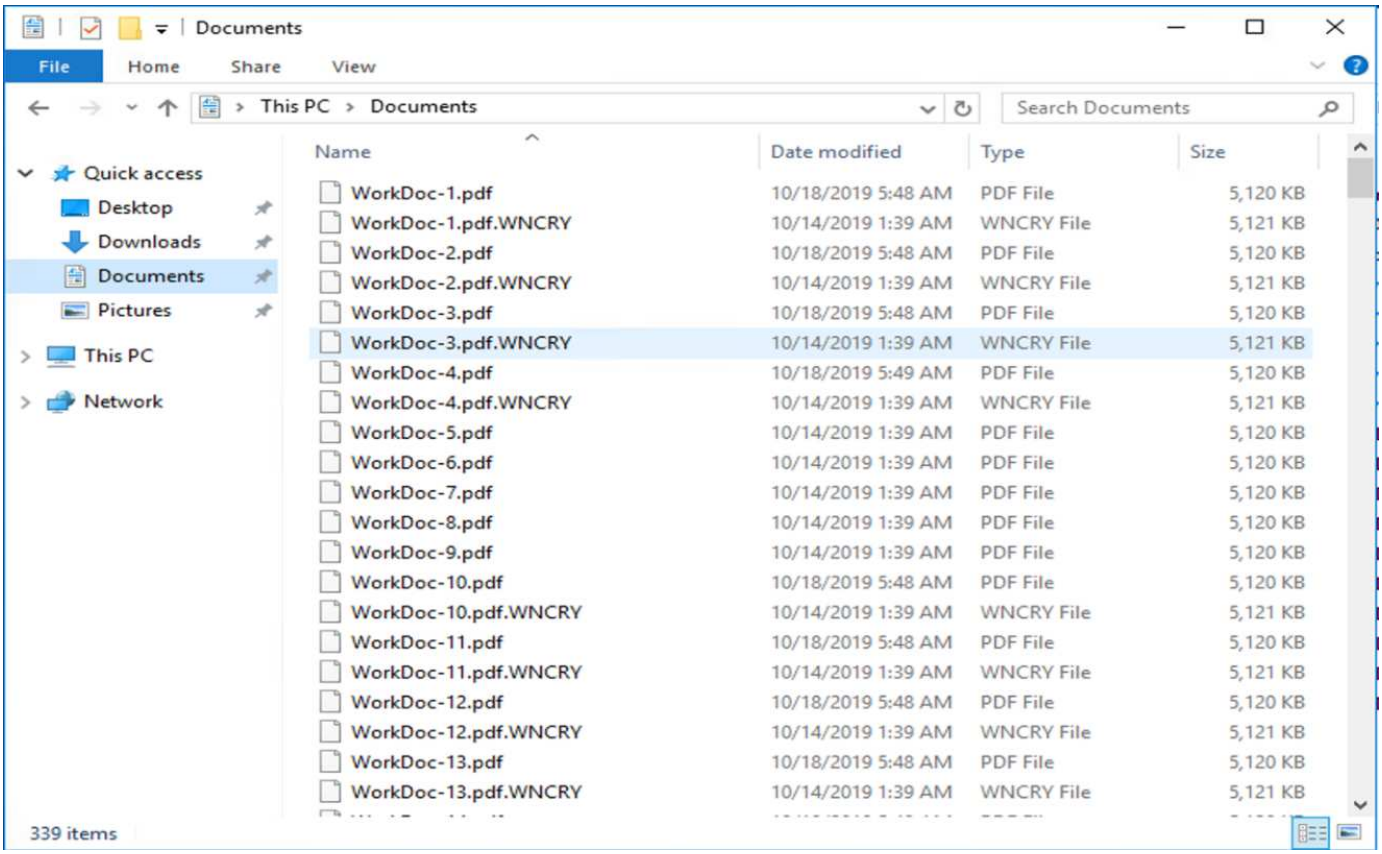
2. Die Binärdatei wurde ausgeführt.



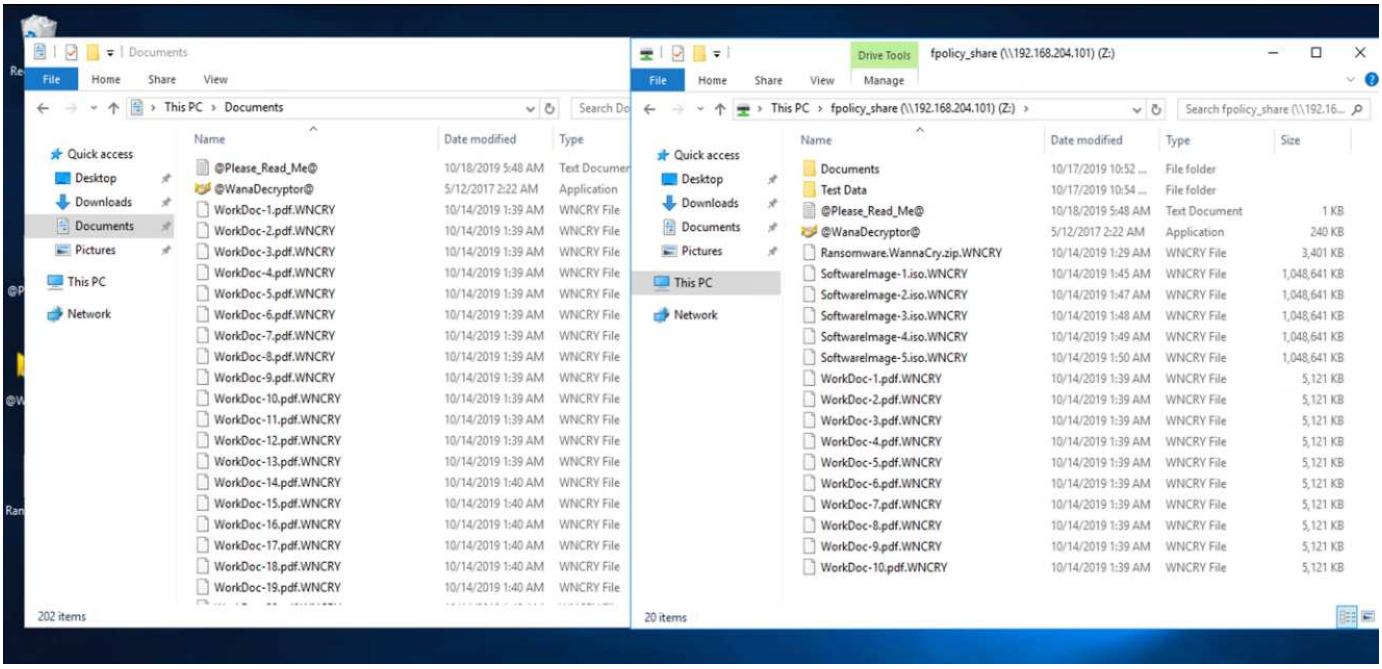
Fall 1: WannaCry verschlüsselt das Dateisystem innerhalb der VM und zugeordnete CIFS-Freigabe

Das lokale Dateisystem und die zugeordnete CIFS-Share wurden durch den WannaCry Malware verschlüsselt.

Malware beginnt, Dateien mit WNCRY-Erweiterungen zu verschlüsseln.



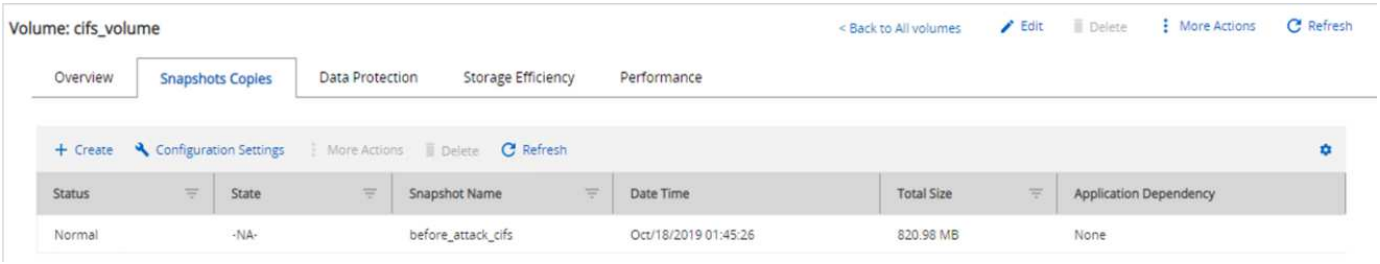
Die Malware verschlüsselt alle Dateien in der lokalen VM und der zugeordneten Freigabe.



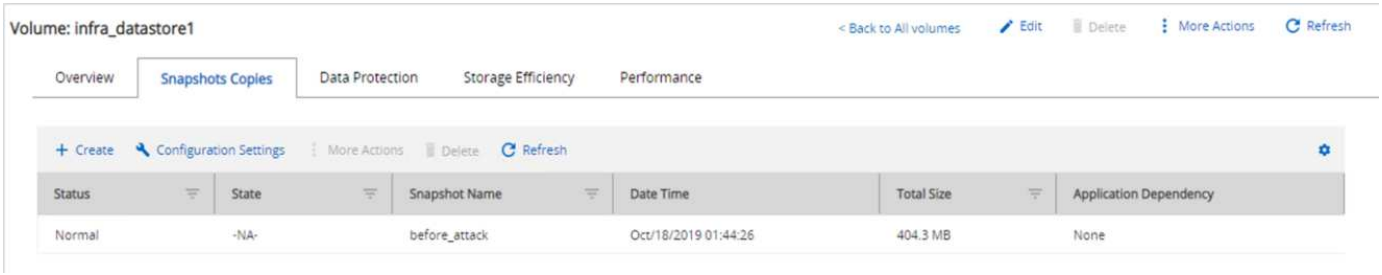
Erkennung

Als die Malware mit der Verschlüsselung der Dateien begann, führte sie zu einem exponentiellen Anstieg der Größe der Snapshot-Kopien und einer deutlichen Verringerung der Storage-Effizienz in Prozent.

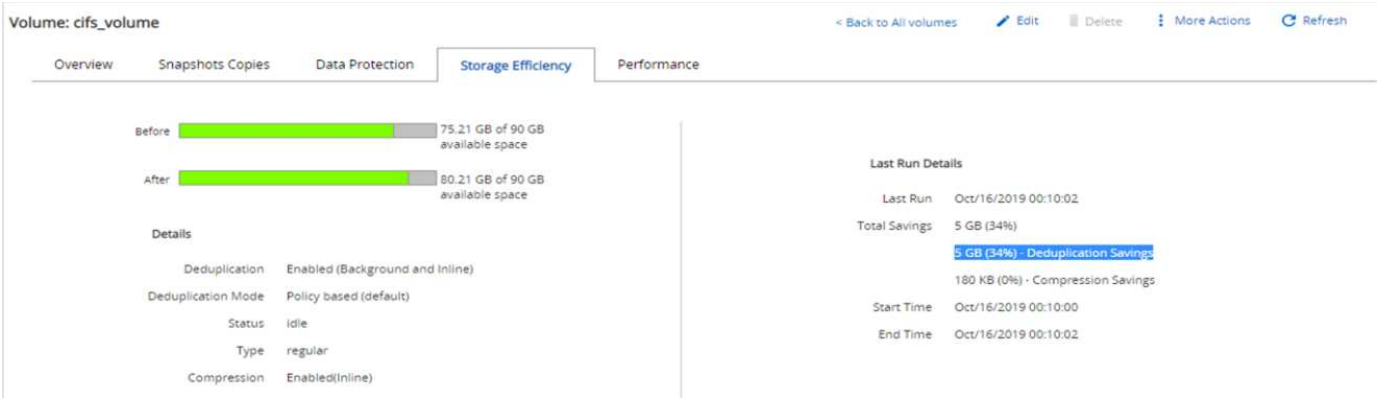
Wir erkannten eine drastische Zunahme der Snapshot-Größe auf 820.98MB für das Volume, das während des Angriffs die CIFS-Freigabe hostet.



Wir erkannten eine Erhöhung der Snapshot-Kopie auf 404,3MB für den Volumen, der die VM hostet.



Die Storage-Effizienz für das Volume, auf dem der CIFS-Share gehostet wird, sank auf 34 %.



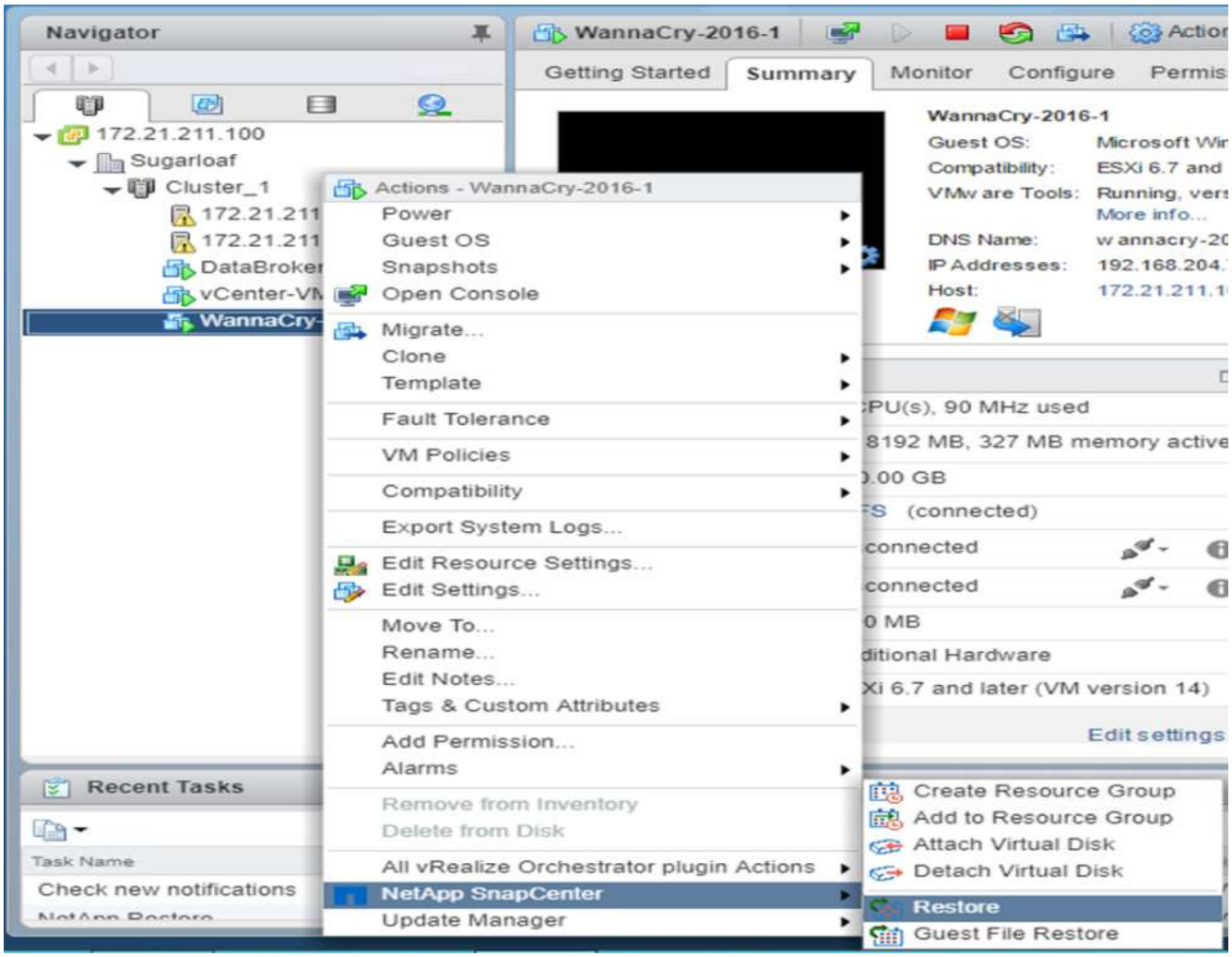
Korrekturmaßnahmen

Stellen Sie die VM wieder her und zugewiesenes CIFS Share, indem Sie vor dem Angriff eine saubere Snapshot Kopie erstellen.

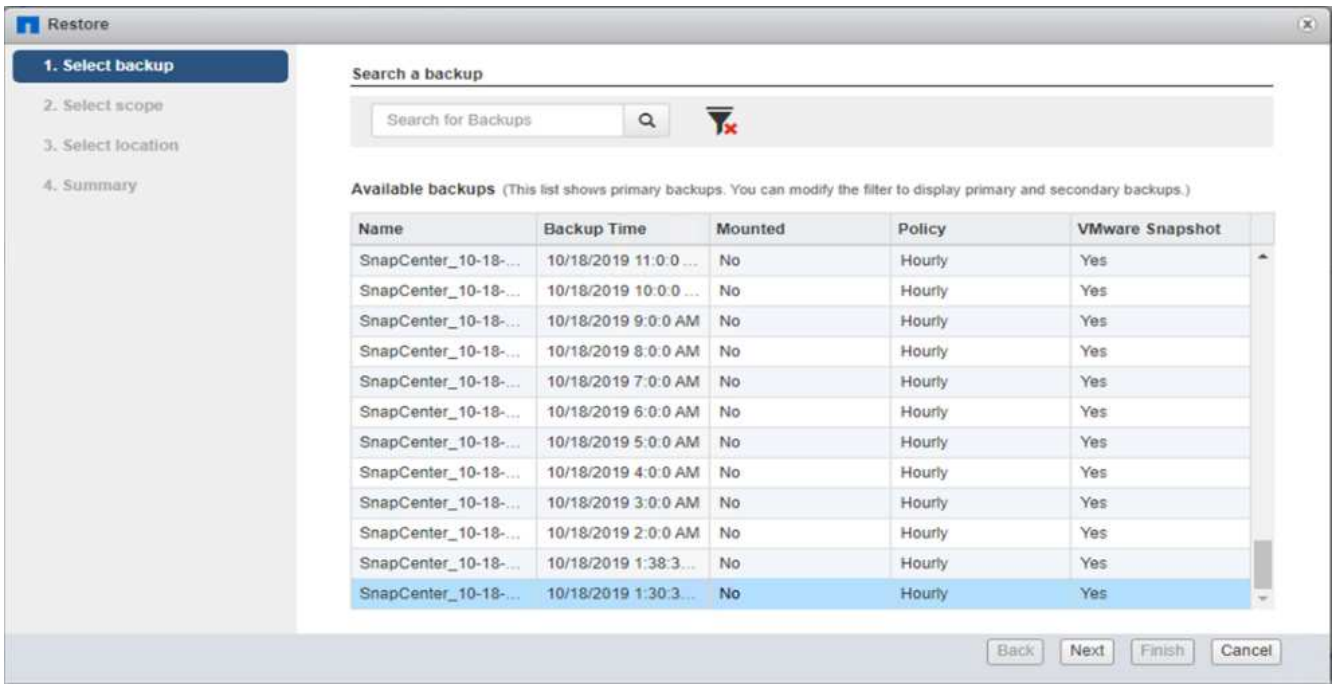
VM wiederherstellen

Um die VM wiederherzustellen, führen Sie die folgenden Schritte aus:

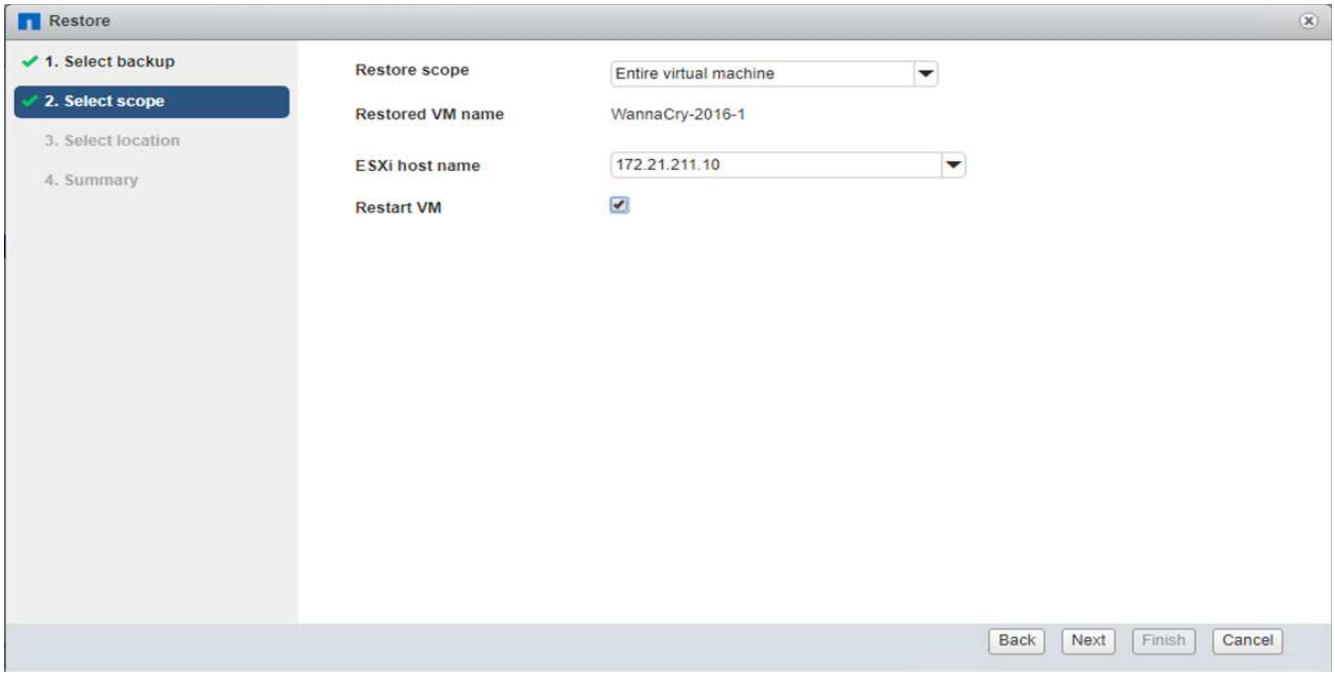
1. Verwenden Sie die mit SnapCenter erstellte Snapshot Kopie zum Wiederherstellen der VM.



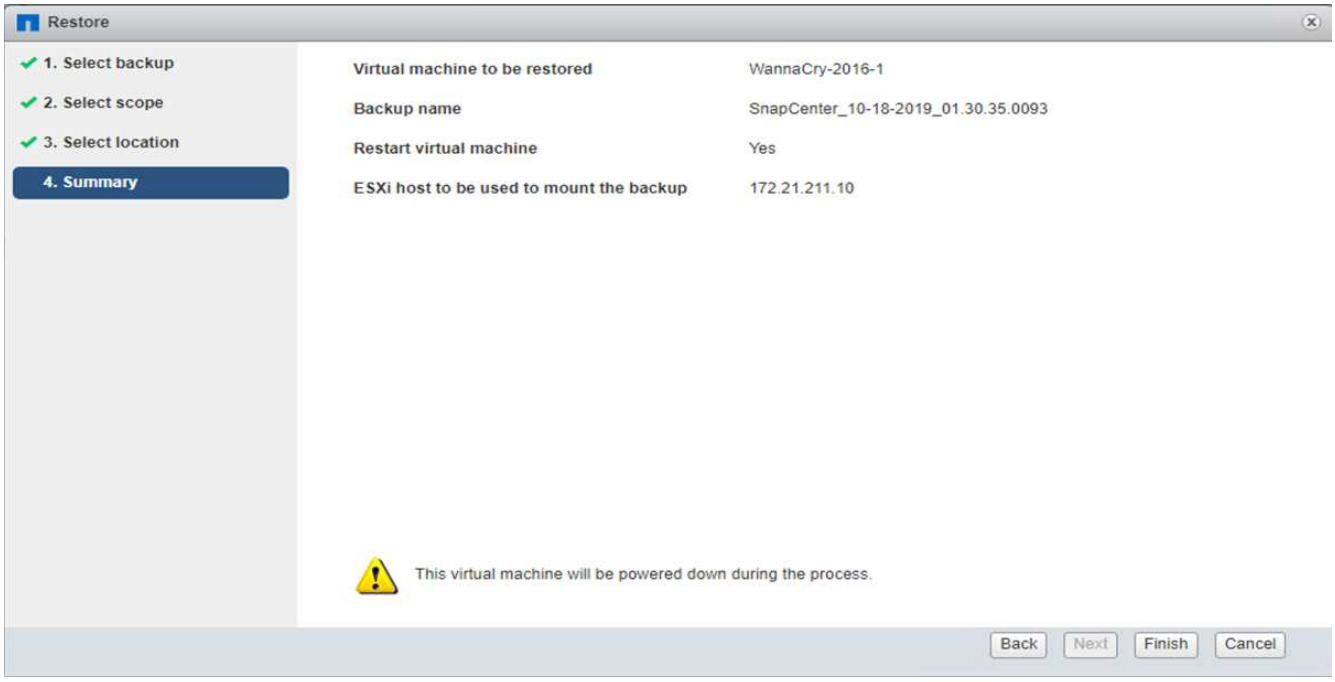
2. Wählen Sie die gewünschte VMware- konsistente Snapshot Kopie für die Wiederherstellung aus.



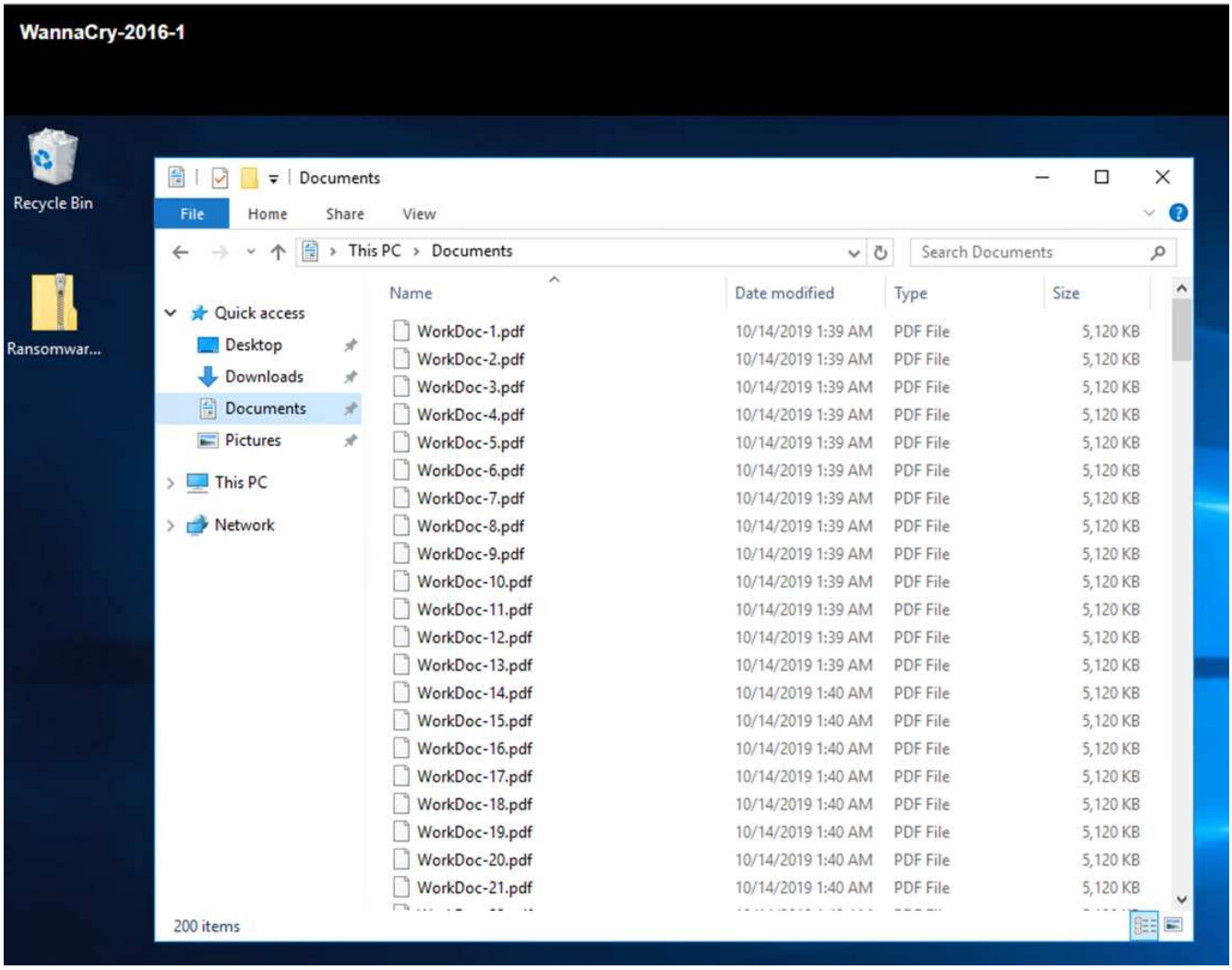
3. Die gesamte VM wird wiederhergestellt und neu gestartet.



4. Klicken Sie auf Fertig stellen, um den Wiederherstellungsvorgang zu starten.



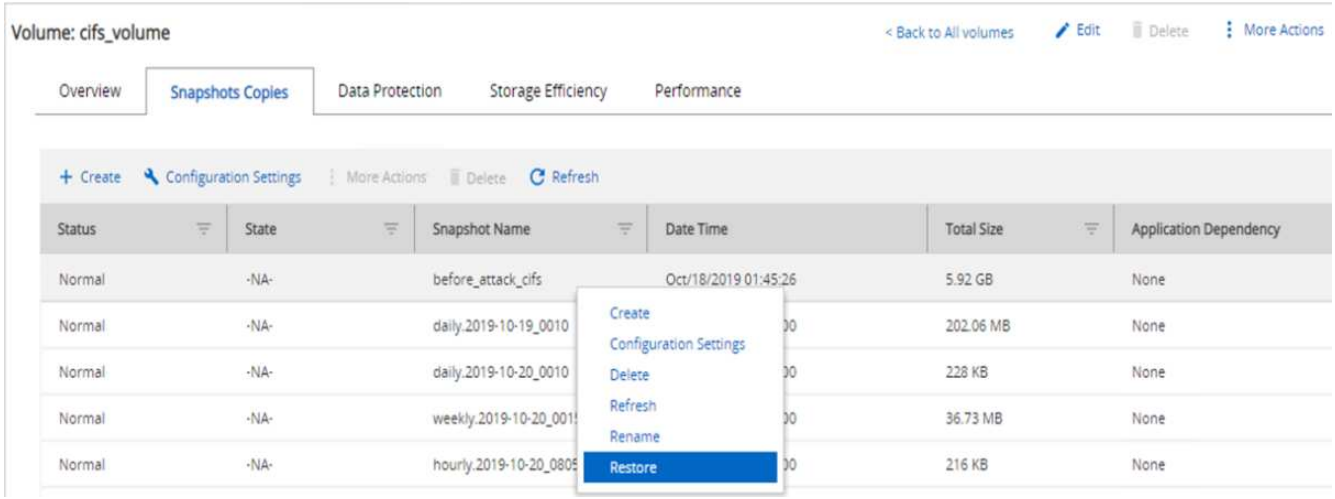
5. Die VM und ihre Dateien sind wiederhergestellt.



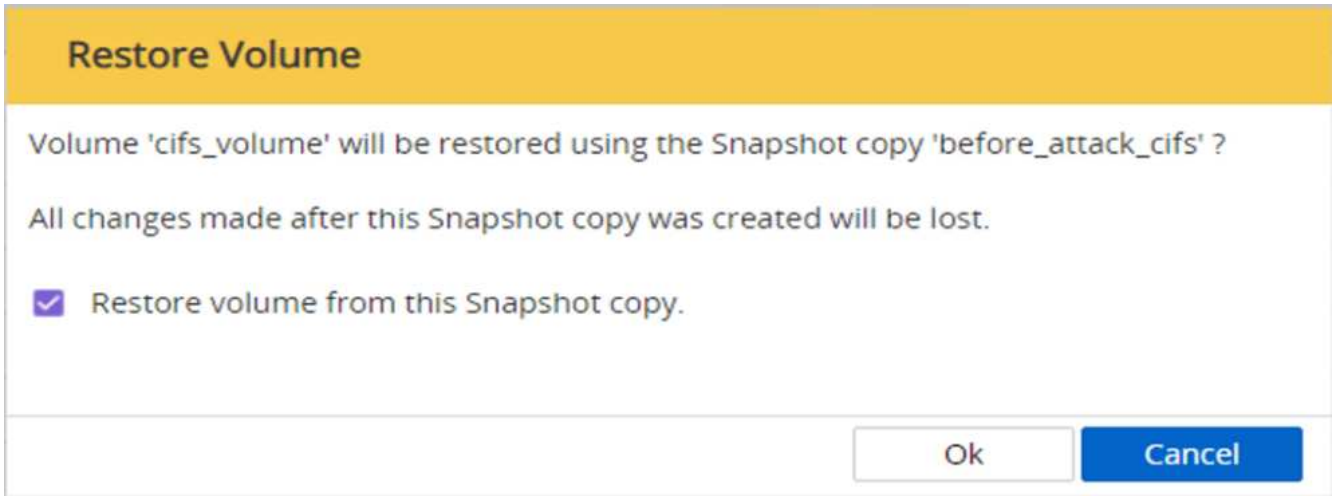
CIFS-Freigabe wiederherstellen

Gehen Sie wie folgt vor, um die CIFS-Freigabe wiederherzustellen:

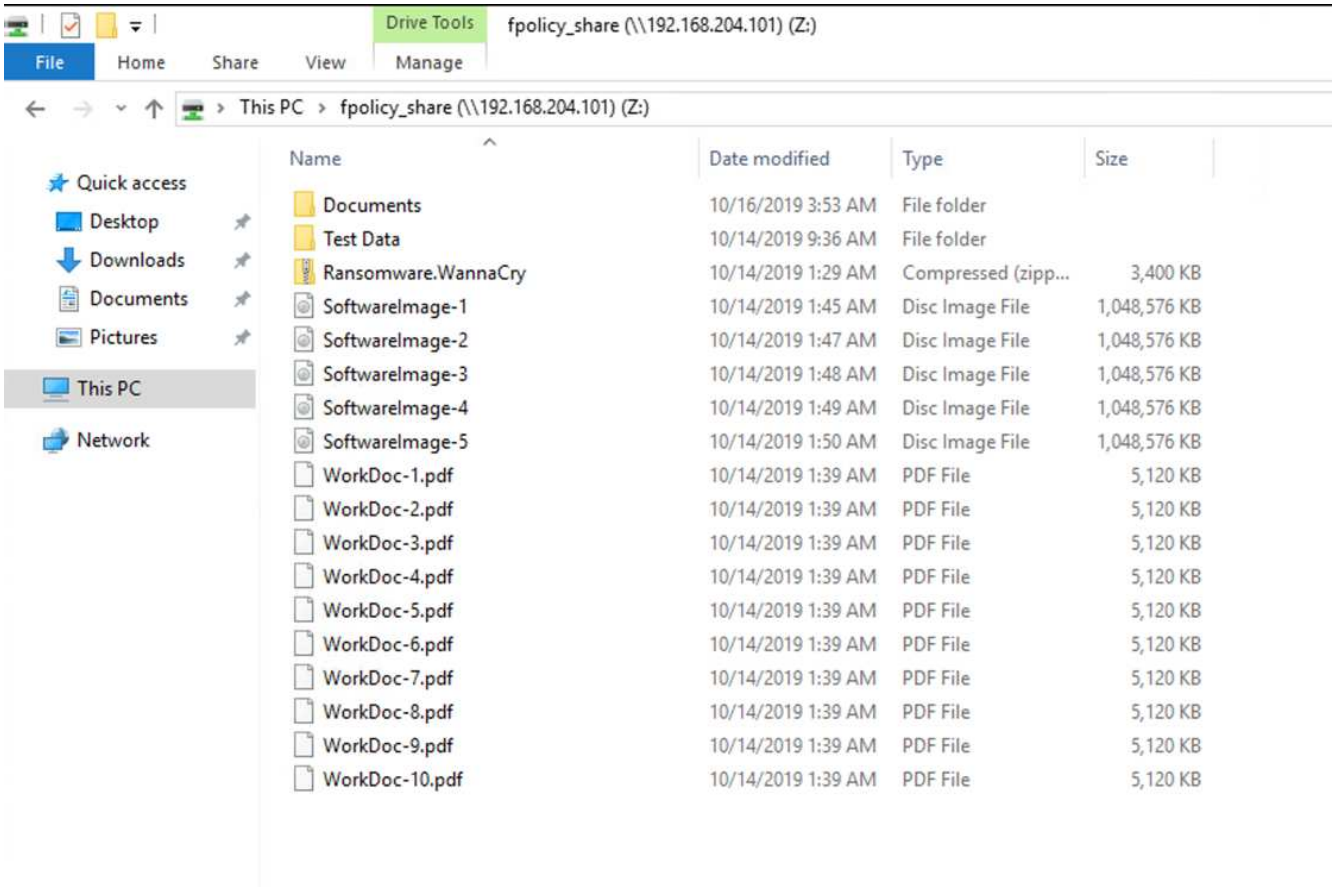
1. Verwenden Sie die Snapshot-Kopie des vor dem Angriff aufgenommene Volumes, um die Freigabe wiederherzustellen.



2. Klicken Sie auf OK, um den Wiederherstellungsvorgang zu starten.



3. Zeigen Sie die CIFS-Freigabe nach der Wiederherstellung an.



Fall 2: WannaCry verschlüsselt Dateisystem innerhalb der VM und versucht, die zugewiesene CIFS-Freigabe zu verschlüsseln, die durch FPolicy geschützt ist

Prävention

FPolicy konfigurieren

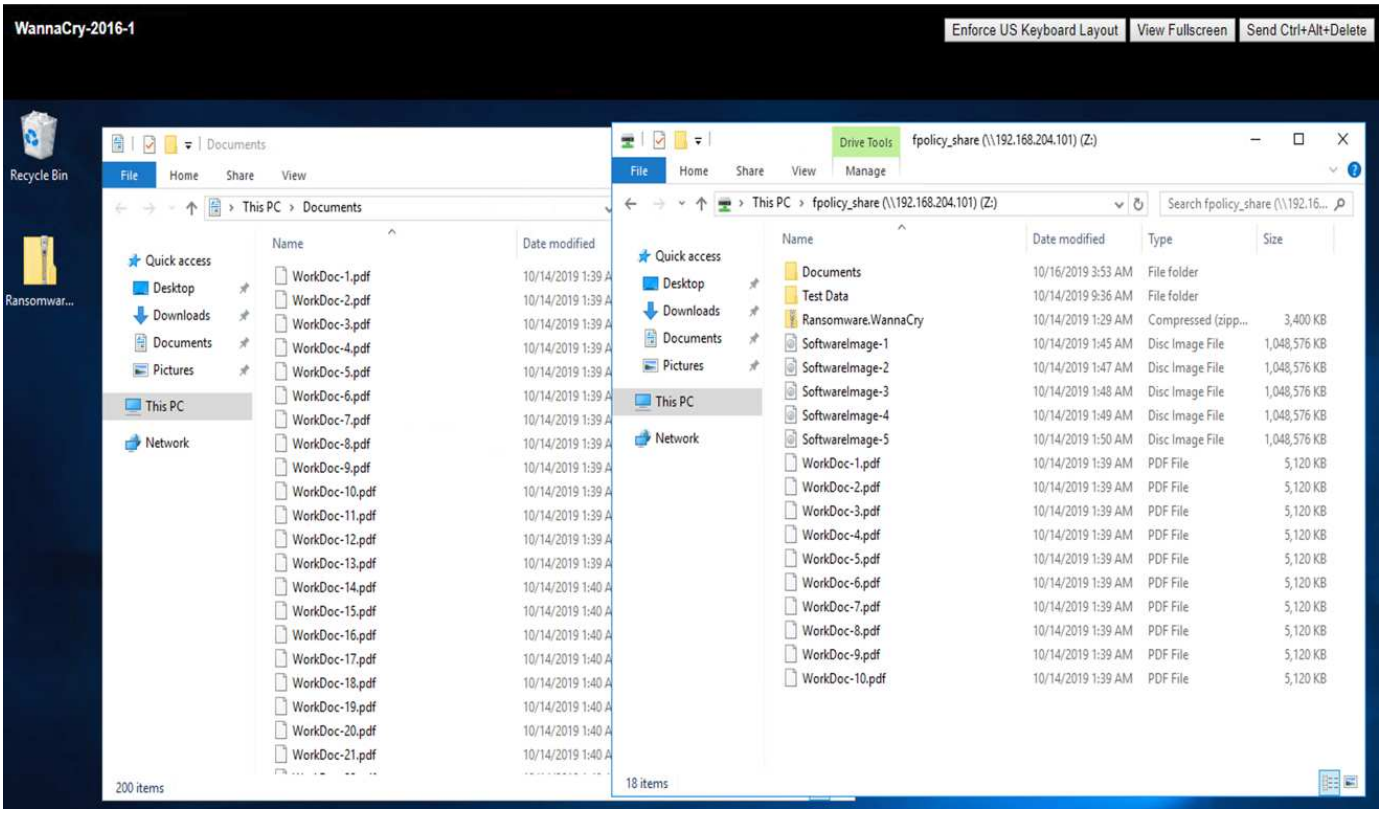
Führen Sie die folgenden Befehle auf dem ONTAP-Cluster aus, um FPolicy auf der CIFS-Freigabe zu

konfigurieren:

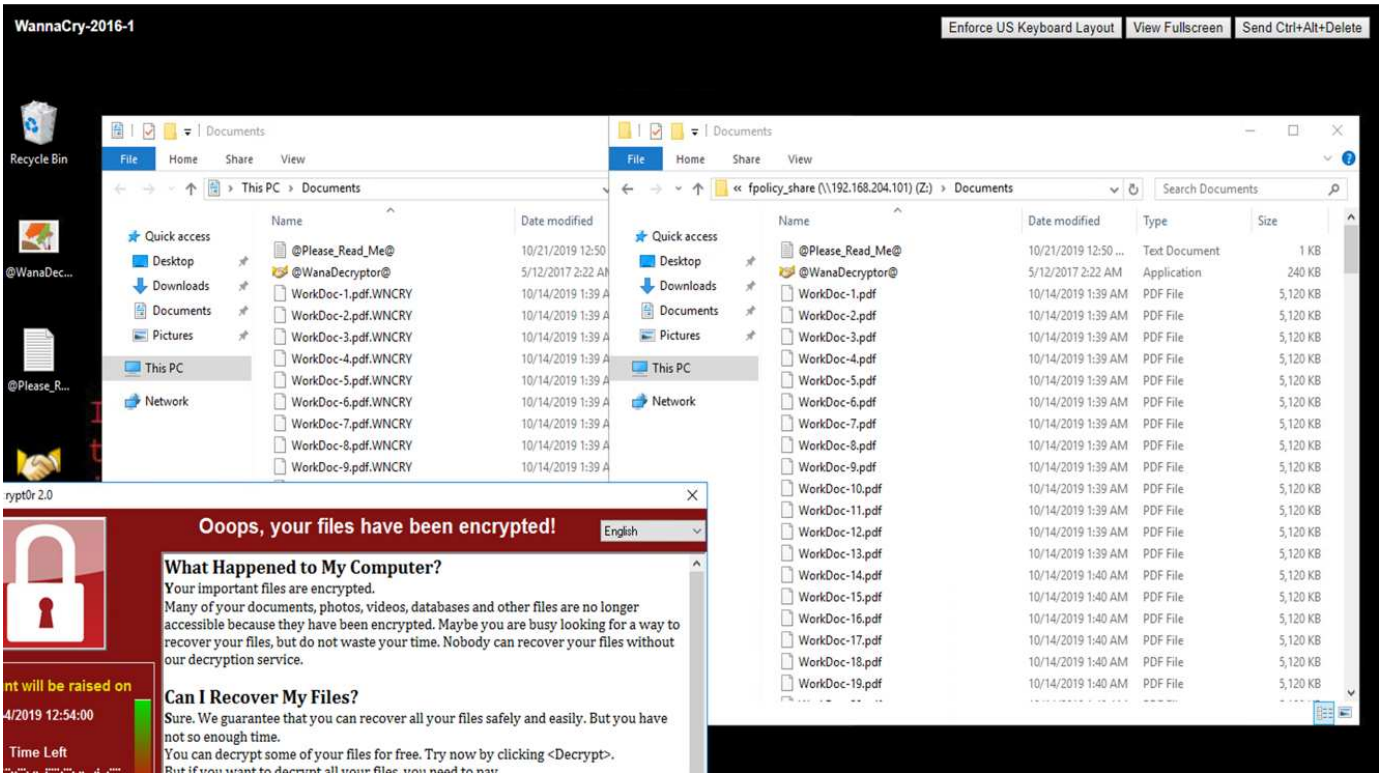
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

Mit dieser Richtlinie sind Dateien mit den Erweiterungen WNCRY, Locky und ad4c nicht berechtigt, die Dateivorgänge zum Erstellen, Umbenennen, Schreiben oder Öffnen auszuführen.

Anzeigen des Status von Dateien vor dem Angriff – sie sind unverschlüsselt und in einem sauberen System.



Die Dateien auf der VM sind verschlüsselt. Die WannaCry Malware versucht, die Dateien in der CIFS-Share zu verschlüsseln, aber FPolicy verhindert, dass sie die Dateien zu beeinflussen.



Geschäftsbetrieb ohne Lösegeld fortsetzen

Die in diesem Dokument beschriebenen NetApp Funktionen helfen Ihnen, Daten innerhalb weniger Minuten nach einem Angriff wiederherzustellen und Angriffe an erster Stelle zu vermeiden, sodass der Geschäftsbetrieb ungehindert weitergeführt werden kann.

Sie können einen Zeitplan für Snapshot Kopien festlegen, um die gewünschte Recovery-Zeitvorgabe (Recovery Point Objective, RPO) zu erfüllen. Auf Snapshot Kopien basierende Wiederherstellungsvorgänge sind sehr schnell. Somit kann ein sehr geringes Recovery Time Objective (RTO) erreicht werden.

Vor allem müssen Sie kein Lösegeld als Folge eines Angriffs zahlen, und Sie können schnell wieder zu normalen Operationen.

Schlussfolgerung

Ransomware ist ein Produkt der organisierten Kriminalität und die Angreifer arbeiten nicht mit ethischen Werten. Sie können den Schlüssel zur Entschlüsselung auch nach Erhalt des Lösegeld nicht zur Verfügung stellen. Die Opfer verlieren nicht nur ihre Daten, sondern sie gehen auch deutlich über die mit dem Verlust von Produktionsdaten verbundenen Konsequenzen nach.

Laut A "Forbes-Artikel", Nur 19% der Ransomware-Opfer bekommen ihre Daten nach dem Lösegeld zurück. Daher empfehlen die Autoren, im Falle eines Angriffs kein Lösegeld zu zahlen, weil dies den Glauben des Angreifers an ihr Geschäftsmodell stärkt.

Backup- und Restore-Prozesse spielen bei der Ransomware-Recovery eine wichtige Rolle. Daher müssen sie als integraler Bestandteil der Geschäftsplanung einbezogen werden. Die Implementierung dieser Vorgänge

sollte so geplant werden, dass die Recovery-Funktionen bei einem Angriff keine Kompromisse eingehen.

Entscheidend ist dabei, den richtigen Technologiepartner auf diesem Weg zu wählen. FlexPod stellt die meisten erforderlichen Funktionen nativ und ohne zusätzliche Kosten in einem All-Flash FAS System zur Verfügung.

Danksagungen

Der Autor dankt den folgenden Personen für ihre Unterstützung bei der Erstellung dieses Dokuments:

- Jorge Gomez Navarrete, NetApp
- Ganesh Kamath, NetApp

Weitere Informationen

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp Snapshot Software

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- SnapCenter Backup-Management

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- SnapLock Datenkonformität

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- NetApp Produktdokumentation

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco Advanced Malware Protection (AMP)

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco Stealthwatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"