Erkenntnisse aus einer kürzlich durchgeführten Wiederherstellung nach einem Ransomware-Angriff

Erfahren Sie, wie ein weltweit agierendes Fertigungsunternehmen Active Directory nach einem Ransomware-Angriff schnell wiederhergestellt hat.

Quest

Einführung

Erfahrungen aus der Praxis liefern wertvolle Erkenntnisse über die Wiederherstellung nach einem Ransomware-Angriff, die eine abstrakte Strategie nicht bieten kann. In diesem Whitepaper werden die wichtigsten Erkenntnisse dargelegt, die ein weltweit agierendes Fertigungsunternehmen kürzlich bei der erfolgreichen Wiederherstellung von Active Directory nach einem Ransomware-Angriff gewonnen hat.

Jedes Unternehmen muss auf Ransomware-Angriffe vorbereitet sein

Ein Blick auf die Wirtschaftsnachrichten zeigt, dass die IT zu einem gefährlichen Pflaster geworden ist. Ransomware richtet in Unternehmen aus unterschiedlichsten Branchen verheerende Schäden an. Zu den prominentesten Opfern zählen Colonial Pipeline, JBS und Kaseya. Dieses Risiko beschränkt sich jedoch nicht auf Großunternehmen – auch KMUs, Behörden, Bildungseinrichtungen, Gesundheitsdienstleister und Organisationen aus vielen weiteren Branchen waren bereits betroffen.

Zur Veranschaulichung hier einige Zahlen:

- 69 % der Unternehmen waren 2020 von einem Ransomware-Angriff betroffen.
- Nur 8 % der Unternehmen, die das Lösegeld bezahlt haben, haben all ihre Daten zurückerhalten.
- Die durchschnittliche Ausfallzeit nach einem Ransomware-Angriff beträgt 21 Tage. (Manche Kunden vermelden allerdings deutlich längere Ausfallzeiten.)
- Die durchschnittlichen Kosten zur Behebung eines einzelnen Ransomware-Angriffs liegen bei 1,85 Millionen US-Dollar.
- Im Jahr 2020 hat Ransomware Kosten in Höhe von 20,8 Milliarden US-Dollar verursacht – und das allein bei Gesundheitsdienstleistern in den USA.

Die Bedrohung wird auch auf den höchsten Ebenen inzwischen ernst genommen. Vertreter des Weißen Hauses haben sich in einem Anschreiben an US-Unternehmen gewandt und ihnen dringend empfohlen, im Führungsteam unverzüglich die von Ransomware ausgehende Bedrohung zu besprechen, den Sicherheitsstatus des Unternehmens und seine Pläne für die Business Continuity zu bewerten und so sicherzustellen, dass sie den Geschäftsbetrieb im Ernstfall durchgehend oder mit nur kurzer Unterbrechung fortsetzen können. FBI Director Christopher Wray hat den Gesetzgebern mitgeteilt, dass sich die Cyberbedrohung fast exponentiell steigert und dass die US-Regierung aktuell 100 verschiedene Ransomware-Varianten untersucht, von denen jeweils Dutzende oder gar Hunderte Unternehmen betroffen sind.

69 %

aller Unternehmen waren 2020 von einem Ransomware-Angriff betroffen. Die durchschnittliche Ausfallzeit nach einem Ransomware-Angriff beträgt 21 Tage.

Lediglich das Lösegeld zu zahlen ist keine sinnvolle Strategie

Das Lösegeld behebt das Problem nicht. 80 % der Unternehmen, die Lösegeld bezahlt haben, wurden später erneut Opfer eines Ransomware-Angriffs. Fast jedes zweite dieser Unternehmen (46 %) vermutet, dass dahinter dieselben Angreifer steckten. Das Office of Foreign Assets Control (OFAC) des Finanzministeriums der Vereinigten Staaten hat zudem Lösegeldzahlungen bei Ransomware-Angriffen in bestimmten Fällen gesetzlich verbieten lassen. Unter Umständen werden Strafzahlungen auch dann fällig, wenn das betroffene Unternehmen nicht wusste, dass der Empfänger des Lösegelds eine laut OFAC-Auflagen verbotene Entität ist.

Welche Strategie empfiehlt sich also?

Active Directory ist das entscheidende Element.

Für eine umfassende Ransomware-Strategie müssen Sie zahlreiche Faktoren berücksichtigen. Es gilt, die Angriffsfläche zu minimieren und eine zügige Erkennung und Reaktion sicherzustellen. In diesem Whitepaper wird ein entscheidender Bereich behandelt: die Wiederherstellung. Sie ist wichtig, damit Sie im Fall eines Ransomware-Angriffs den Geschäftsbetrieb so schnell wie möglich fortsetzen können.

Da die meisten Unternehmen Active Directory (AD) nutzen, um Identitäten zu verwalten und den Zugriff auf Unternehmensressourcen wie Datenbanken, Dateien, Anwendungen und Endpunkte zu regeln, ist AD das entscheidende Element für eine schnelle Wiederherstellung nach einem Ransomware-Angriff. Gartner zufolge wurde bei vielen gut dokumentierten Ransomware-Angriffen die Wiederherstellung dadurch erschwert, dass kein funktionierender Wiederherstellungsprozess für Active Directory vorhanden war.[1]

> **Bei vielen gut dokumentierten Ransomware-Angriffen wurde die Wiederherstellung dadurch erschwert, dass kein funktionierender Wiederherstellungsprozess für Active Directory vorhanden war.**
>
> *Gartner, Inc., „How to Recover From a Ransomware Attack Using Modern Backup Infrastructure", Fintan Quinn, 4. Juni 2021.*

Ohne AD sind die übrigen Systeme nicht nutzbar. Dies musste auch die IT-Abteilung von Maersk nach dem berüchtigten NotPetya-Angriff im Jahr 2017 feststellen: Wenn die Domänencontroller nicht wiederhergestellt werden können, ist auch keine Wiederherstellung anderer Systeme möglich.[2]

Herkömmliche Lösungen für Sicherung und Wiederherstellung haben den Nachteil, dass sie zwar die Identitäten wiederherstellen können, jedoch keine erneute Synchronisierung erfolgt. So müssen anschließend noch viele Schritte manuell auf jedem einzelnen Identitätsserver durchgeführt werden, wodurch es deutlich länger dauert, bis das Unternehmen wieder auf die Füße kommt. Mit Recovery Manager for Active Directory Disaster Recovery Edition (RMAD DRE) von Quest können Sie sichergehen, dass Sie im Fall des Falles schnell und sicher wieder einsatzbereit sind. Einer unserer Kunden hat die Wiederherstellung nach einem Ransomware-Angriff mit RMAD DRE und die daraus gewonnenen vier wichtigsten Erkenntnisse dokumentiert.

Fallstudie zur effektiven Reaktion auf Ransomware

Ransomware legt 17 DCs und nahezu alle Benutzerkonten lahm

Ein weltweit tätiger Kunde aus der Fertigungsbranche war kürzlich von Ransomware betroffen, durch die 17 Domänencontroller (DCs) auf mehreren Kontinenten ausfielen. Im Zuge des Angriffs wurden außerdem bei 98 % der Benutzerkonten die Active Directory-Kennwörter manipuliert. Auch unzählige Servicekonten waren hiervon betroffen.

Auf den ersten Blick schien es, als sei einer der 17 DCs nicht betroffen. Nachdem dieser DC im Netzwerk isoliert worden war, entdeckte das IT-Team jedoch verschlüsselte Dateien im SYSVOL. Diese hätten auch einfach Replikate von einem anderen DC sein können. Da sich Ransomware jedoch häufig über Gruppenrichtlinien verbreitet, musste sichergestellt werden, dass auf dem Server keine Malware versteckt war. Das Team musste also das Netzwerk wiederherstellen und gleichzeitig eine erneute Infektion verhindern – eine nicht zu unterschätzende Herausforderung, die aber typisch für die Wiederherstellung nach einem Ransomware-Angriff ist.

Quest unterstützt den Kunden

Glücklicherweise konnte das Unternehmen Recovery Manager for Active Director Disaster Recovery Edition nutzen. Die Lösung ließ dem IT-Team die Wahl zwischen mehreren Wiederherstellungsmethoden wie einer stufenweisen Wiederherstellung und der Wiederherstellung von AD mit fehlerfreiem Betriebssystem, um das Risiko einer erneuten Infektion mit Malware zu minimieren. Dank RMAD DRE hatte das Wiederherstellungsteam außerdem mehr Kontrolle über den gesamten Notfall-wiederherstellungsvorgang. Durch die geringere Abhängigkeit von abteilungsübergreifenden Teams konnten Zeit und Ressourcen eingespart werden.

Wie der Projektmanager des Beratungsservice vor Ort berichtet, war der Kunde verzweifelt, bis Quest hinzukam und den Stein ins Rollen brachte. Danach war auch beim Kunden wieder Hoffnung zu spüren.

[1] Gartner, Inc., „How to Recover From a Ransomware Attack Using Modern Backup Infrastructure", Fintan Quinn, 4. Juni 2021.
[2] Wired Magazine, „The Untold Story of the NotPetya, the Most Devastating Cyberattack in History", https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Dank einer stufenweisen Wiederherstellung sind die fünf wichtigsten DCs innerhalb von weniger als zwei Stunden wieder betriebsbereit

Mithilfe von RMAD DRE leitete das Unternehmen eine stufenweise Wiederherstellung ein und konnte so festlegen, in welcher Reihenfolge die DCs wiederhergestellt werden sollen, damit wichtige Services schneller wieder verfügbar sind. Zuerst wurden alle betroffenen Benutzerkonten anhand einer fünf Tage zuvor erstellten Sicherung wiederhergestellt. Mit RMAD DRE konnte das Team sogar die Kennwörter für alle privilegierten Konten zurücksetzen. Dieser Schritt war besonders wichtig, weil der Verdacht bestand, dass mindestens ein privilegiertes Konto kompromittiert worden war.

> **Mit RMAD DRE konnte das Unternehmen fünf grundlegende DCs innerhalb von weniger als zwei Stunden wiederherstellen und dann mit dem Wiederherstellen der geschäftskritischen Anwendungen beginnen.**

Danach verlief die Wiederherstellung wie folgt:

- **Stufe 1 :** Der erste DC wurde innerhalb von einer Stunde wiederhergestellt.
- **Stufe 2:** Der zweite DC wurde innerhalb von 12 Minuten wiederhergestellt.
- **Stufe 3:** Drei weitere DCs auf zwei Kontinenten wurden innerhalb von 36 Minuten wiederhergestellt.

An diesem Punkt standen ausreichend Ressourcen in Active Directory zur Verfügung, sodass das Team seinen Fokus auf die Wiederherstellung der Geschäftsanwendungen verlagern konnte. Die Wiederherstellung der weniger wichtigen DCs wurde auf später verschoben.

Unter dem Strich konnte das Unternehmen die Ausfallzeit dank RMAD DRE erheblich reduzieren. Der Projektmanager war begeistert und sagte, ohne das Tool von Quest hätte die Wiederherstellung niemals so schnell erfolgen können.

Aus dieser Praxiserfahrung mit der Wiederherstellung nach einem Ransomware-Angriff lassen sich wichtige Erkenntnisse ableiten, die Unternehmen in ihrer Strategie zur Verteidigung gegen Ransomware berücksichtigen sollten. Lassen Sie uns einen genaueren Blick auf diese werfen.

Erkenntnis 1: AD-Sicherungen sollten mit Air Gaps geschützt werden

Das Problem liegt auf der Hand: Sie können Daten nicht anhand einer Sicherung wiederherstellen, wenn die Sicherung selbst beschädigt ist. Aus genau diesem Grund zielen viele Ransomware-Angriffe auf über das Netzwerk verbundene Sicherungen ab und zerstören diese, um die Wahrscheinlichkeit zu maximieren, dass das Unternehmen Lösegeld zahlt, um seine Daten zurückzuerhalten.

Denken Sie daher daran, Ihre regelmäßig und zuverlässig erstellten Active Directory-Sicherungen an einem Speicherort mit Air Gap aufzubewahren. Das bedeutet, der Speicherort muss „offline“ sein: vom Internet und von allen internen Netzwerken getrennt und von dort aus nicht zugänglich.

Früher wurden Sicherungen zu diesem Zweck auf Bandlaufwerken erstellt, die dann an einen externen Aufbewahrungsort versendet wurden, beispielsweise an den Anbieter Iron Mountain. Dieser Ansatz ist aufwendig und kostspielig. Noch dazu bremst er die Wiederherstellung erheblich aus, weil es lange dauert, die benötigten Bandlaufwerke zu finden, zu versenden, anzuschließen und auszulesen. Bei dieser Methode kann es schwierig werden, Wiederherstellungszeitvorgaben (Recovery Time Objectives, RTOs) einzuhalten. Wenn Sie also externe physische Speicherlösungen nutzen, sollten Sie unbedingt Ihr SLA überprüfen. Viele Unternehmen erwägen heute, ihre Sicherungen mit Cloud-Lösungen zu speichern. Zur Auswahl stehen unter anderem Amazon Simple Storage Service (Amazon S3) (sowie zusätzlich S3 Glacier und S3 Glacier Deep Archive) und der unveränderliche Objektspeicher Microsoft Azure Blob Storage.

Bei RMAD DRE hingegen wird keine separate Speicherlösung benötigt. Ab Version 10.2 ist in der Lösung ein Secure Storage-Server enthalten. Dabei handelt es sich um einen durch strikte Firewalls geschützten Server, der praktisch keinen Zugriff zulässt – sei es per Ping, RDP, PC, Remotedesktop oder SMB-Freigaben. Die SMB-Ports sind nicht einfach nur deaktiviert, sondern die Protokolle an sich sind auf dem Secure Storage-Server nicht zulässig. Die einzige Zugriffsmöglichkeit ist ein einzelner per TLS verschlüsselter TCP-Port, den Sie selbst festlegen können. Über diesen TLS-Port wird der Speicheragent benachrichtigt, wenn eine Sicherung erstellt und an den Tier-1-Speicher gesendet wurde. Die Sicherung wird dann vom Agenten selbst entgegengenommen. Sie müssen

die Firewalls somit nie deaktivieren. Zusätzlich wird die Integrität der Sicherungen von der Lösung überprüft.

Um eine Sicherung senden zu können, müssen Sie das Rechenzentrum selbst betreten und sich bei der Konsole anmelden. Dass physischer Zugang erforderlich ist, macht den Vorgang etwas unpraktischer für Sie, verhindert jedoch eine Kompromittierung der Sicherungen durch Ransomware-Angriffe fast vollständig. Anhand der so aufbewahrten Sicherungen kann Active Directory von RMAD DRE auf einem neuen Server wiederhergestellt werden, damit Ihre Systeme schneller wieder betriebsbereit sind.

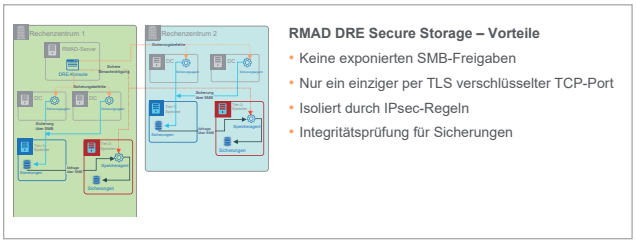

Abbildung 1: Der Secure Storage-Server von RMAD DRE schützt AD Sicherungen durch Speicher mit Air Gap vor Ransomware.

Erkenntnis 2: Es ist wichtig, auf Ransomware-Angriffe vorbereitet zu sein und Pläne vorab zu testen

Die Wiederherstellung der Gesamtstruktur ist ein aufwendiger, komplizierter Prozess, bei dem für jeden anhand einer Sicherung wiederherzustellenden DC mehr als 40 Schritte erforderlich sind. Daher empfiehlt es sich, eine automatisierte Lösung zu nutzen und einen dokumentierten Plan zu haben, der regelmäßig getestet wird. Achten Sie darauf, dass der Plan konkret auf die Wiederherstellung von AD nach einem Ransomware-Angriff eingeht. Zu viele Unternehmen konzentrieren sich fälschlicherweise nur auf die Anwendungswiederherstellung. Gehen Sie beim Planen unbedingt davon aus, dass zu Beginn gar keine Domänencontroller zum Ausführen der Anwendungen vorhanden sind.

> Konzentrieren Sie sich nicht nur auf die Anwendungs-wiederherstellung. Gehen Sie beim Planen unbedingt davon aus, dass zu Beginn gar keine DCs zum Ausführen der Anwendungen vorhanden sind.

Benennen Sie einen Verantwortlichen und halten Sie die Zuständigkeiten eindeutig fest

Für die Wiederherstellung werden verschiedene Teams benötigt, zum Beispiel die folgenden:

- **Sicherungsteam** – stellt die Sicherungen zur Verfügung und führt Wiederherstellungen durch.
- **Speicherteam** – sorgt dafür, dass genügend Speicherplatz zum Wiederherstellen der Server anhand von Sicherungen vorhanden ist.
- **Netzwerkteam** – ist für das Sandboxing der wiederherzustellenden Server und die Kommunikation der DCs zuständig.
- **Serverteam** – überprüft, ob die Wiederherstellung richtig und vollständig erfolgt ist, und installiert ggf. erforderliche zusätzliche Viren- oder Malwareschutzsoftware.
- **Sicherheitsteam** – überprüft, ob die wiederhergestellten Server tatsächlich frei von Ransomware sind.
- **Anwendungsteam** – überprüft, ob die Anwendungen ordnungsgemäß funktionieren.
- **Externe Beteiligte** wie Microsoft, Ihr Anbieter für Sicherung und Wiederherstellung sowie der Anbieter Ihres Cloud-Speichers.

Es ist wichtig, dass eine Person die Gesamtverantwortung trägt, die verschiedenen Teams anweist und koordiniert und bei Bedarf schnell Entscheidungen trifft. Auch alle anderen Rollen und Zuständigkeiten sollten klar dokumentiert sein.

Richten Sie einen virtuellen „War Room“ ein

Ihr Plan für die Wiederherstellung nach einem Ransomware-Angriff sollte auch einen virtuellen „War Room“ vorsehen, in dem sich die beteiligten Teams treffen können. Es sollte darin möglich sein, Untergruppen auf mehrere separate virtuelle Räume zu verteilen, damit sie die Strategie im Hinblick auf Einzelaspekte besprechen können. Hierfür eignen sich Zoom und Microsoft Teams. Auch die TeamFlow-Anwendung ist eine Option.

Berücksichtigen Sie in Ihrem Plan nicht nur die AD-Wiederherstellung

Denken Sie daran, dass die Wiederherstellung von AD nicht die einzige Aufgabe nach einem Ransomware-Angriff ist. Bedenken Sie auch die Auswirkungen auf Komponenten wie

das Netzwerk, die Router und Switches. Wie kommunizieren die VPN-Konzentratoren mit Ihrem Verzeichnis? Es ist ratsam, Server zusätzlich mit spezieller Software für noch mehr Sicherheit sowie Erkennung und Reaktion auf Endpunkten auszustatten.

Sorgen Sie dafür, dass Ihr Plan leicht zugänglich ist

Bewahren Sie Ihren Plan an einem Ort auf, an dem Sie auch nach einem sehr schwerwiegenden Ransomware-Angriff noch darauf zugreifen können. Eine bewährte Methode ist das Aufbewahren einer gedruckten Version des Plans. Sie können ihn jedoch auch in einem separaten Cloud-Speicher ablegen, beispielsweise bei Dropbox.

Erkenntnis 3: Eine stufenweise Wiederherstellung kann sinnvoll sein

Wie oben beschrieben erfolgte in dem weltweit agierenden Fertigungsunternehmen eine stufenweise Wiederherstellung: Die wichtigsten DCs wurden zuerst wiederhergestellt, um schnell zumindest einen grundlegenden Geschäftsbetrieb zu ermöglichen.

Ermitteln Sie zunächst, welche Anwendungen für Ihren Betrieb am wichtigsten sind und daher zuerst wiederhergestellt werden sollten. Benennen Sie dann die für diese Anwendungen unverzichtbaren DCs. Oft sind die Domänencontroller im Rechenzentrum wichtiger als die DCs an Remotestandorten. Sobald diese wiederhergestellt wurden, können das Anwendungsteam, das Datenbankteam und andere Beteiligte mit ihrem eigenen Wiederherstellungsprozess beginnen, während sich das Active Directory-Team mit dem Wiederherstellen der weniger wichtigen DCs befasst. Abbildung 2 veranschaulicht diese Strategie der stufenweisen Wiederherstellung.

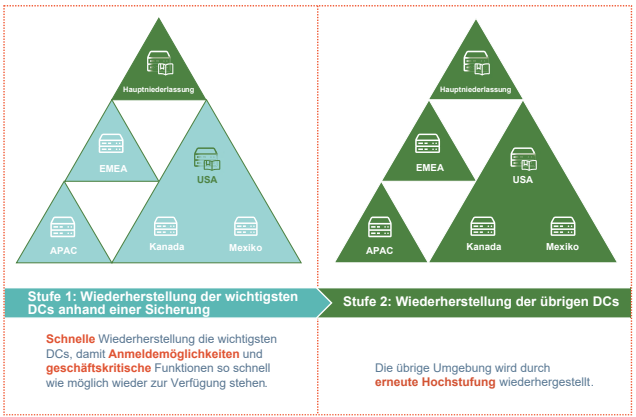

Abbildung 2: Eine stufenweise Wiederherstellung kann zur schnellen Fortsetzung wichtiger Geschäftsprozesse beitragen.

Erkenntnis 4: Geschwindigkeit ist nicht alles

Behalten Sie bei der Planung im Blick, dass es bei der Wiederherstellung nach einem Ransomware-Angriff nicht nur auf Geschwindigkeit ankommt. Es ist ebenso wichtig, dass die Wiederherstellung ordnungsgemäß verläuft und keine erneute Infektion auftritt. RMAD DRE trägt zur Risikominderung bei, da Sie die Methode zur Wiederherstellung der einzelnen DCs flexibel wählen können:

- **Bare-Metal-Wiederherstellung (Bare Metal Recovery, BMR):** Alle Volumes des DC werden auf neuer oder anderer Hardware wiederhergestellt.
- **Wiederherstellung mit fehlerfreiem Betriebssystem:** AD wird auf einem neuen Windows Server wiederhergestellt. Gleichzeitig wird das Risiko einer erneuten Infektion gemindert.
- **Installation von Active Directory:** Neue Server werden hochgestuft und übernehmen die Aufgaben der DCs, die Sie nicht anhand einer Sicherung wiederhergestellt haben.
- **Deinstallation von Active Directory:** Bei einem DC wird eine Herabstufung erzwungen und alle zugehörigen Metadaten werden aus dem Verzeichnis entfernt.
- **Erneute Installation von Active Directory:** Bei DCs wird eine Herabstufung erzwungen. Dann werden die DCs wieder hochgestuft, solange das Betriebssystem noch intakt ist.
- **Wiederherstellung von AD anhand einer Sicherung:** AD wird auf einem nicht infizierten Server wiederhergestellt.
- **Erneute Hochstufung:** Die verbleibenden DCs in einer teilweise wiederhergestellten Gesamtstruktur werden hochgestuft.

Beim Auswählen der Wiederherstellungsmethode sollten Sie berücksichtigen, dass für eine BMR das physische Layout des Zielsystems identisch mit dem Layout des gesicherten DC sein muss. Zudem beinhaltet die Sicherung Komponenten wie das Boot-Volume, die für die Wiederherstellung nicht benötigt werden und Ransomware die Gelegenheit bieten, sich darin zu verstecken und eine erneute Infektion zu verursachen.

Die Möglichkeit der Wiederherstellung mit fehlerfreiem Betriebssystem bei RMAD DRE senkt dieses Risiko erheblich, da die Sicherung nur die tatsächlich benötigten Informationen enthält (siehe Abbildung 3). Bei RMAD DRE können die Sicherungen zusätzlich auf Malware geprüft werden, bevor sie bei der Wiederherstellung zum Einsatz

RMAD DRE kann dazu beitragen, Ihre wichtigsten Geschäftsprozesse nach einem Ransomware-Angriff schnell wiederherzustellen und eine erneute Infektion zu verhindern.

kommen. Sie können im Zuge der Wiederherstellung auch die Kennwörter der Mitglieder integrierter privilegierter Gruppen zurücksetzen. Darüber hinaus bietet RMAD DRE die Möglichkeit, AD auf einer virtuellen Microsoft Azure-Maschine wiederherzustellen, also auf einem sofort verfügbaren, sicheren und kostengünstigen System, das zuverlässig frei von Malware ist.

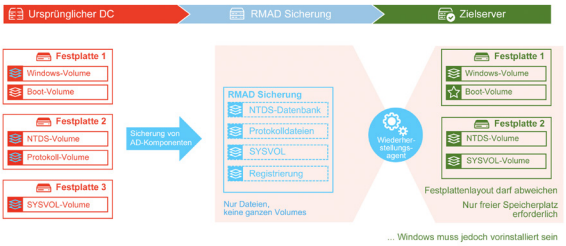

Abbildung 3: Die Option zur Wiederherstellung mit fehlerfreiem Betriebssystem bei RMAD DRE mindert das Risiko einer erneuten Infektion während der Wiederherstellung erheblich.

Fazit

Jedes Unternehmen benötigt heute eine umfassende Ransomware-Strategie, um schnell die wichtigsten Domänencontroller wiederherstellen und den Geschäftsbetrieb fortsetzen zu können. Recovery Manager for Active Directory Disaster Recovery Edition kann als entscheidende Komponente dieser Strategie fungieren. Ein weltweit agierendes Fertigungsunternehmen konnte auf diese Weise seine fünf wichtigsten DCs innerhalb von weniger als zwei Stunden wiederherstellen und so die für den grundlegenden Geschäftsbetrieb entscheidenden Anwendungen und Datenbanken ebenfalls rasch wiederherstellen.

Weitere Informationen finden Sie unter https://www.quest.com/products/recovery-manager-for-active-directory-disaster-recovery-edition/.

Quest

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das Potenzial neuer Technologien in einer zunehmend komplexen IT-Landschaft ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Verwaltung von Active Directory und Office 365 bis hin zu Cyber Resilience: Quest hilft Kunden dabei, bereits heute ihre IT-Herausforderungen von morgen zu bewältigen. Weltweit vertrauen mehr als 130.000 Unternehmen und 95 % der Fortune 500 Quest die proaktive Verwaltung und Überwachung der nächsten Unternehmensinitiative an. Quest soll außerdem die nächste Lösung für komplexe Microsoft-Herausforderungen finden, um für die nächste Bedrohung gewappnet zu sein. Quest Software: Where Next Meets Now.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an: www.quest.com/de-de/company/contact-us.aspx