Planung der Active Directory-Notfallwiederherstellung für den Fall eines Ransomware-Angriffs

Ransomware-Angriffe treten immer häufiger auf. Hier erfahren Sie, wie Sie das Risiko für Ihr Unternehmen senken können.

Quest

Einführung

Akute Bedrohung durch Ransomware

Nach verheerenden Ransomware-Angriffen auf bedeutende Unternehmen und Infrastrukturen wie JBS und die Colonial Pipeline in den USA ist Ransomware heute in aller Munde. Angesichts der zunehmenden geopolitischen Spannungen hat die US-amerikanische CISA (Cybersecurity and Infrastructure Security Agency) alle Unternehmen und Organisationen in den USA – einschließlich Bundesbehörden – aufgefordert, ihre Cybersicherheit und den Schutz ihrer wichtigsten Assets zu erhöhen. Die CISA empfiehlt Unternehmen eine Bewertung ihrer Resilience durch Tests der verwendeten Sicherungsverfahren. So sollen sie sicherstellen, dass wichtige Systeme und Daten nach einem Ransomware-Angriff oder einem anderweitig zerstörerischen Cyberangriff schnell wiederhergestellt werden können.

Es besteht durchaus Grund zur Beunruhigung. Zur Veranschaulichung hier einige Zahlen:

- **69 %** der Unternehmen waren bereits von einem Ransomware-Angriff betroffen.
- Nur **8 %** der Unternehmen, die das Lösegeld zahlten, erhielten all ihre Daten zurück.
- Die durchschnittliche Ausfallzeit nach einem Ransomware-Angriff beträgt **21 Tage**.
- Die durchschnittlichen Kosten zur Behebung eines einzelnen Ransomware-Angriffs liegen bei **1,85 Millionen US-Dollar**.
- Ransomware hat Kosten in Höhe von **20,8 Milliarden US-Dollar** verursacht – und das allein bei Gesundheitsdienstleistern in den USA.

Wären Sie ausreichend vorbereitet, wenn Ihr Unternehmen heute Opfer eines Ransomware-Angriffs würde?

Bestandteile einer umfassenden Strategie gegen Ransomware

Ein umfassender Ansatz zum Umgang mit Ransomware erfordert eine tiefgreifende Verteidigungsstrategie, die alle fünf im NIST Cybersecurity Framework angegebenen Funktionen abdeckt:

- **Identifizierung –** Ermitteln Sie den aktuellen Stand der Cybersicherheit in Ihrem Unternehmen unter Berücksichtigung der vorhandenen physischen und Software-Assets und der zugehörigen Cybersicherheitsrisiken, des Kontexts und der Risikotoleranz des Unternehmens, der aktuellen Richtlinien und Kontrollen für die Cybersicherheit sowie der Compliancevorgaben und gesetzlichen Vorschriften.
- **Schutz –** Begrenzen Sie das Risiko und die Auswirkungen von Cybersicherheitsvorfällen, indem Sie Schwachstellen beheben, Ihre Belegschaft schulen, Prozesse zur Verbesserung des Informationsschutzes implementieren sowie Governance und Administration stärken.
- **Erkennung –** Nutzen Sie Funktionen wie Auditierung, Anomalieerkennung und Warnmeldungen in Echtzeit, um bei verdächtigen Aktivitäten schneller benachrichtigt zu werden.
- **Reaktion –** Sorgen Sie durch zuverlässige Kommunikation und forensische Analysen dafür, dass schnell die richtigen Maßnahmen getroffen werden, bevor der Schaden noch größer wird.
- **Wiederherstellung –** Mindern Sie die Auswirkungen eines Sicherheitsvorfalls durch die schnelle Wiederherstellung des Normalbetriebs.

Keine dieser Funktionen ist verzichtbar. In diesem Whitepaper wird jedoch hauptsächlich der letzte Aspekt – Wiederherstellung – behandelt. Sie erfahren, wie Sie einen zuverlässigen Plan zur Active Directory-Notfallwiederherstellung erstellen und die für eine schnelle, effektive Umsetzung dieses Plans erforderlichen flexiblen Wiederherstellungsoptionen erhalten.

Rechenbeispiel zu den durch einen Ransomware-Angriff verursachten Kosten

Wie wichtig ist der Aspekt der Wiederherstellung? Eine Möglichkeit zur Quantifizierung besteht darin, die durch einen Ransomware-Angriff verursachten Kosten zu berechnen. Die Grundlage dafür bildet die zur Wiederherstellung des Normalbetriebs benötigte Zeit.

Nachfolgend finden Sie ein einfaches Rechenbeispiel. Berücksichtigt werden nur drei Faktoren: die entgangene Mitarbeiterproduktivität, der entgangene Umsatz und die direkten Kosten der Wiederherstellung des IT-Betriebs.

Für die Spalte „Beispiel“ wurden folgende Annahmen getroffen:

- Das durchschnittliche Jahresgehalt pro Mitarbeiter beträgt 65.000 US-Dollar.
- Ein Jahr hat 260 Arbeitstage.
- Der jährliche Gesamtumsatz des Unternehmens liegt bei 100 Millionen US-Dollar.

Wenn Sie die Kosten für Ihr eigenes Unternehmen berechnen möchten, verwenden Sie in der Rechnung einfach die entsprechenden Zahlen Ihres Unternehmens.

> „Natürlich sind Business-Continuity-Pläne unverzichtbar. Dennoch gibt es auf jeder Unternehmensebene weitere Möglichkeiten, sich auf den schlimmsten Fall vorzubereiten – den berühmten Worst Case. Damit meine ich die größte Katastrophe, die Sie sich vorstellen können. Bereiten Sie sich auf diesen Fall vor – Sie werden es zu schätzen wissen, sobald Ihnen wirklich alles um die Ohren fliegt.“
>
> *Gavin Ashton*
> *Zuständiger IAM SME bei Maersk zur Zeit des NotPetya-Ransomware-Angriffs*

Entgangene Produktivität	Beispiel	Ihre Zahlen
Durchschnittliche Vergütung pro Tag (Gehalt + Sachbezüge)	250 USD	
Ausfallzeit in Tagen	21	
Anzahl der Mitarbeitenden, die aufgrund des Ausfalls nicht arbeiten können	10.000	
Zwischensumme	**52.500.000 USD**	
Entgangene Umsätze		
Durchschnittlicher Umsatz pro Tag	384.615 USD	
Ausfallzeit in Tagen	21	
Zwischensumme	8.076.915 USD	
Kosten für die Wiederherstellung des IT-Betriebs		
Überstunden der Mitarbeitenden oder Bezahlung von Auftragnehmenden für die Wiederherstellung	50.000 USD	
Hardwarereparaturen	25.000 USD	
Zwischensumme	75.000 USD	
Summe der grundlegenden Kosten des Zwischenfalls	**60.651.915 USD**	

Tabelle 1: Rechenbeispiel zu den durch einen einzelnen Ransomware-Angriff verursachten Kosten

Beachten Sie, dass es sich hierbei um eine stark vereinfachte und eher vorsichtige Schätzung handelt. Für eine genauere Berechnung müssten Sie unter anderem folgende zusätzliche Kosten berücksichtigen:

- Wenn die Ausfallzeit eine von Kunden genutzte Website oder Anwendung betrifft, müssen Sie die Kosten berücksichtigen, die die zu erwartende Flut an Anrufen beim Kundensupport verursacht. Auch die entgangenen Einnahmen von unzufriedenen Kunden, die zu Mitbewerbern abwandern, sind relevant.
- Wenn Sie Complianceauflagen erfüllen müssen, kommen mögliche Geldstrafen und die Kosten für zusätzliche Audits hinzu.
- Falls Kundendaten offengelegt werden (ein von Angreifern zunehmend genutztes Druckmittel, um Opfer zur Zahlung des Lösegelds zu zwingen), entstehen Ihnen unter Umständen auch Kosten für rechtliche Schritte und für Abhilfemaßnahmen wie die für Kunden kostenlose Kreditüberwachung des Unternehmens.
- Sollten Sie sich für die Zahlung des Lösegelds entscheiden, müssen Sie auch diese Summe hinzurechnen.
- Schwieriger zu quantifizieren ist der potenziell größte Kostenfaktor bei einem Angriff: die Schädigung des Unternehmensrufs. Sie verlieren nicht nur die Einnahmen von Kunden, die sofort abwandern, sondern auch von Interessenten, die sich aufgrund des Vorfalls in Zukunft gegen Ihr Unternehmen entscheiden. Es kann Jahre dauern, bis Ihr Ruf vollständig wiederhergestellt ist.

Vor diesem Hintergrund überrascht es nicht, dass 40 % der Unternehmen die Kosten einer einzigen Stunde Ausfallzeit auf eine Summe zwischen 1 Million US-Dollar und über 5 Millionen US-Dollar beziffern. Im schlimmsten Fall können sich die Verluste auf mehrere Millionen US-Dollar pro Minute belaufen.

Der Schlüssel zur schnellen Wiederherstellung nach einem Ransomware-Angriff: ein mehrschrittiger Ansatz, bei dem Active Directory im Mittelpunkt steht

Active Directory ist für nahezu alle IT-Betriebsabläufe entscheidend.

Erinnern Sie sich an den berüchtigten NotPetya-Angriff im Jahr 2017? Innerhalb weniger Stunden brachte diese Malware Unternehmen rund um die Welt zum Stillstand. Eines der Opfer war der Logistik- und Transportriese Maersk. Maersk hatte zwar Sicherungen zahlreicher Mission-Critical-Server erstellt, doch im gesamten Unternehmen war nicht eine einzige Sicherung eines Domänencontrollers aufzufinden. Mit anderen Worten: Es gab keine Sicherung von Active Directory. Das Unternehmen war praktisch handlungsunfähig.

> **Laut Gartner kann die Wiederherstellung nach Angriffen durch ein dediziertes Tool für die Sicherung und Wiederherstellung von Microsoft Active Directory beschleunigt werden.**
>
> *Gartner, Inc.,*
> *„How to Protect Backup Systems From Ransomware Attacks“, Nik Simpson, 21. September 2021.*

Active Directory (AD) bildet den Eckpfeiler einer effektiven Notfallwiederherstellung, da es den primären Mechanismus zur Benutzerauthentifizierung und Gewährung von Zugriff auf Daten und Anwendungen darstellt. Wenn AD nicht funktioniert, hat die Belegschaft keinen Zugriff auf die für ihre Arbeit benötigten Tools und Informationen. Das Unternehmen kann also den Betrieb nicht fortsetzen.

Bei Maersk hatte der AD-Ausfall verheerende Folgen. Die Mitarbeitenden konnten sich nicht bei den Systemen anmelden und daher ihren Aufgaben nicht nachkommen. Zudem musste das Unternehmen Schiffe umleiten, konnte Frachtschiffe in mehreren Dutzend Häfen weder anlegen noch entladen und war darüber hinaus nicht in der Lage, neue Aufträge zu bearbeiten. Am Ende wurde Maersk durch schieres Glück gerettet: Ein einzelner Domänencontroller an einem Remotestandort war während des Angriffs offline gewesen. Dieser wurde mit größter Sorgfalt zum Hauptsitz des Unternehmens transportiert, um als Ausgangspunkt für die AD-Wiederherstellung zu dienen.

Natürlich können sich Unternehmen nicht einfach auf ihr Glück verlassen. Um das Risiko erheblicher finanzieller Verluste durch Cyberangriffe wie Ransomware zu minimieren, benötigen sie einen zuverlässigen Plan zur Sicherung und Notfallwiederherstellung, in dessen Mittelpunkt die Active Directory-Wiederherstellung steht. Gartner zufolge wurde bei vielen gut dokumentierten Ransomware-Angriffen die Wiederherstellung dadurch erschwert, dass kein funktionierender Wiederherstellungsprozess für Active Directory vorhanden war. Gartner gibt auch an, dass die Wiederherstellung nach Angriffen durch ein dediziertes Tool für die Sicherung und Wiederherstellung von Microsoft Active Directory beschleunigt werden kann.[2]

Ein mehrere Phasen umfassender Ansatz für die AD-Notfallwiederherstellung trägt zur Verkürzung des RTO bei.

Die Erfahrungen von Maersk zeigen zum einen, welch entscheidende Rolle AD bei der Notfallwiederherstellung spielt, und verdeutlichen zum anderen, welcher Weg der schnellste zur Wiederherstellung des Betriebs ist. Das IT-Team musste nur einen einzigen Domänencontroller wieder online stellen (wenn auch auf suboptimaler Hardware), um den gesamten Prozess zur Notfallwiederherstellung anzustoßen. Anhand des letzten intakten Domänencontrollers, der mit größtmöglicher Sorgfalt vom Remotestandort eingeflogen wurde, konnte das Team einen Domänencontroller auf einem Surface Pro 4.2 wiederherstellen. Ab diesem Punkt ging es für das Unternehmen wieder bergauf.

1 Gartner, Inc., „How to Recover From a Ransomware Attack Using Modern Backup Infrastructure", Fintan Quinn, 4. Juni 2021.
2 Gartner, Inc., „How to Protect Backup Systems From Ransomware Attacks", Nik Simpson, 21. September 2021.

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

Ein mehrere Phasen umfassender Ansatz zur AD-Wiederherstellung ist die von Microsoft empfohlene Best Practice zur Wiederherstellung der AD-Gesamtstruktur und zugleich der schnellste Weg zur Wiederaufnahme des Betriebs nach einem Ransomware-Angriff. Im Prinzip besagt die Strategie, dass pro Domäne mindestens ein Domänencontroller ausgewählt wird, der im Fall einer Wiederherstellung priorisiert wird. Diese Domänencontroller müssen so schnell wie möglich wiederhergestellt werden. Danach können Sie sich den weniger wichtigen Domänencontrollern widmen:

- Phase 1: Durchführung der anfänglichen Wiederherstellung. Pro Domäne wird mindestens ein Domänencontroller wiederhergestellt.

- Phase 2: Erneute Bereitstellung der verbleibenden Domänencontroller. Die übrigen Domänencontroller werden durch Hochstufung wiederhergestellt.

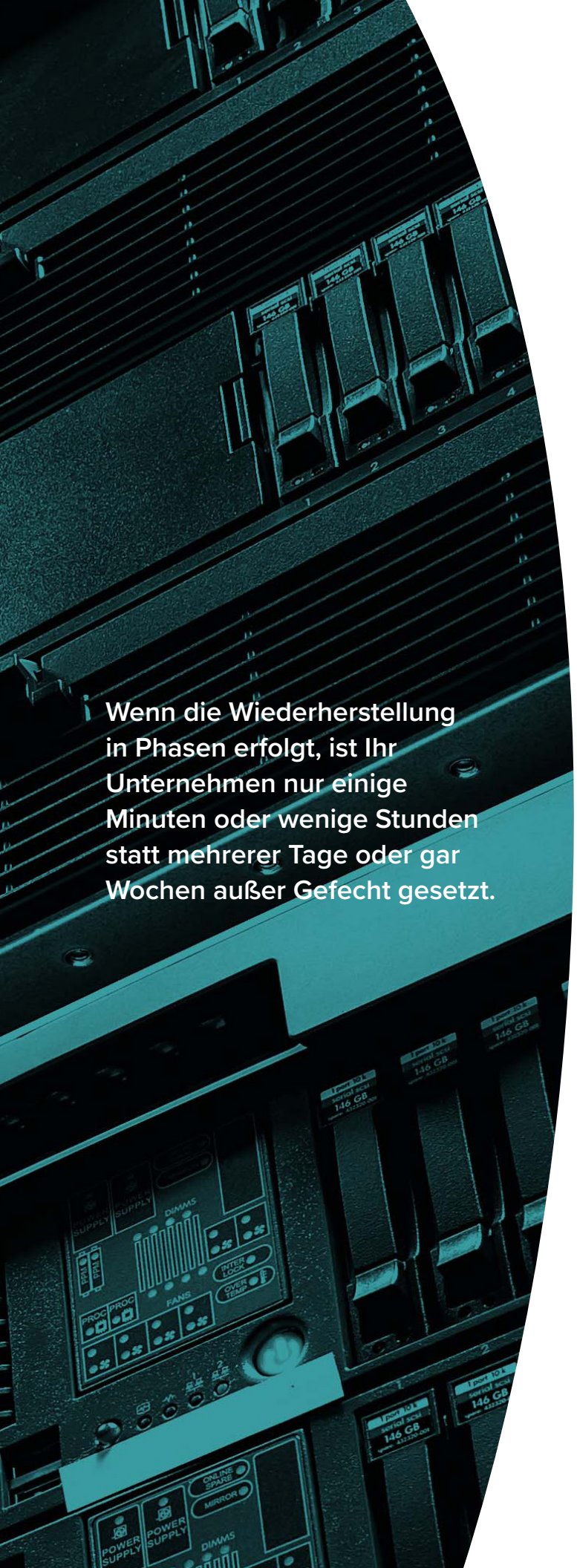
Wenn die Wiederherstellung in Phasen erfolgt, ist Ihr Unternehmen nur einige Minuten oder wenige Stunden statt mehrerer Tage oder gar Wochen außer Gefecht gesetzt.

Mit der Quest Lösung zur AD-Notfallwiederherstellung können Sie beispielsweise einen Domänencontroller in weniger als einer Stunde wiederherstellen, sodass wichtige Betriebsabläufe wieder aufgenommen werden können, während Sie die übrige Wiederherstellung durchführen.

Detailinformationen

Was genau macht eigentlich einen mehrstufigen Ansatz zur AD-Notfallwiederherstellung aus?

Quest



Voraussetzung: zuverlässige Sicherungen

Wie die Erfahrungen von Maersk mehr als deutlich zeigen, hängt die gesamte Notfallwiederherstellung vom Vorhandensein einer soliden Sicherung von Active Directory ab. Es gibt drei Arten von Sicherungen, die Sie kennen sollten:

- **Active Directory-Sicherungen –** Diese Sicherungen bilden die Grundlage für die Wiederherstellung von Active Directory. Dabei spielt es keine Rolle, ob Sie ein einzelnes Objekt, ein Attribut oder einen Domänencontroller wiederherstellen müssen oder aber im Rahmen der Notfallwiederherstellung die Gesamtstruktur. Für AD-Sicherungen sind verschiedene Komponenten von Active Directory-Domänencontrollern relevant, darunter das NTDS-Verzeichnis, SYSVOL (das die Gruppenrichtlinie und Anmeldeskripte enthält) und Aspekte der Registrierung, die mit AD zusammenhängen.

  Beachten Sie, dass AD-Sicherungen nicht dasselbe sind wie Sicherungen des Systemzustands, bei denen nicht nur die Active Directory-Komponenten gesichert werden, sondern das gesamte Betriebssystem. Der Umfang von Sicherungen des Systemzustands wurde im Laufe der Jahre erweitert, sodass diese Sicherungen jetzt zahlreiche Dateien enthalten, die eigentlich gar nicht mit dem Systemzustand zusammenhängen, beispielsweise die IIS(Internet Information Services)-Metabasis, Gerätetreiber, den DLL-Cacheordner und VSS(Volume Shadow Copy Service, Volume-Schattenkopie-Dienst)-Komponenten. Viele dieser Dateien sind für die Wiederherstellung von Active Directory irrelevant, erhöhen jedoch das Risiko, unbeabsichtigt eine infizierte Datei zu sichern (und dann wiederherzustellen). Weitere Informationen zu den Vor- und Nachteilen von Sicherungen des Systemzustands finden Sie im Whitepaper „The Varied History of System State Backups and Why You Don't Need Them for AD Recovery".

- **Azure AD-Sicherungen –** Missgeschicke und schädliche Aktivitäten geschehen nicht nur On-Premises. Aus diesem Grund muss ein umfassender Plan zur IT-Notfallwiederherstellung in Hybrid AD-Umgebungen immer auch eine Sicherungsstrategie für reine Cloud-Objekte und -Attribute beinhalten, da diese von den nativen Microsoft-Tools nicht geschützt und von On-Premises-AD-Sicherungslösungen nicht abgedeckt werden.

  Nehmen wir beispielsweise an, Sie verwenden Azure AD-Richtlinien für bedingten Zugriff, um eine zusätzliche Authentifizierungsform vorzuschreiben, wenn ein Benutzer außerhalb des Unternehmensnetzwerks auf eine sensible Anwendung zuzugreifen versucht, oder um den Zugriff über bestimmte IP-Adressen komplett zu blockieren. Dann stellen Sie fest, dass die erforderlichen Authentifizierungskontrollen für die Anwendung nicht mehr vorhanden sind. Sie können das Problem erst beheben, wenn Sie die Ursache kennen. Ist die Anwendung nicht mehr der richtigen Richtlinie für bedingten Zugriff zugeordnet? Wurde die Richtlinie geändert?

Quest

Wurde die Sicherheitsgruppe geändert, die steuert, für wen die Richtlinie für bedingten Zugriff gilt? Der Papierkorb ist in diesem Fall keine Hilfe, da er nur gelöschte Objekte enthält. Bei unsachgemäßen Änderungen an Objekten wird nichts in den Papierkorb verschoben – daher ist keine Wiederherstellung aus dem Papierkorb möglich. Um sicherzustellen, dass Sie jedes unsachgemäß geänderte Objekt wiederherstellen können, benötigen Sie eine umfassende, aktuelle Dokumentation der Konfiguration all Ihrer Azure AD-Objekte. Die Erstellung und Pflege einer solchen Dokumentation ist jedoch mit manuellen Methoden praktisch unmöglich.

- **Sicherungen für eine Bare-Metal-Wiederherstellung (Bare Metal Recovery, BMR) –** Per Bare-Metal-Wiederherstellung können Sie Ihre Active Directory-Gesamtstruktur auf unterschiedlichen Hardwareinstanzen wiederherstellen. Dies ist besonders bei physischen Beschädigungen an Domänencontrollern, Domänendaten oder Services infolge eines Ransomware-Angriffs von Vorteil. Wenn Sie zum Sichern und Wiederherstellen Ihres gesamten AD-Servers berechtigt sind, können Sie mit einer Kombination aus der erstellten BMR-Sicherung und der standardmäßigen AD-Sicherung die Active Directory-Gesamtstruktur auf anderen Hardwareinstanzen wiederherstellen.

  Selbstverständlich ist immer darauf zu achten, dass die Sicherungen intakt und tatsächlich verwendbar sind. Microsoft empfiehlt die 3-2-1-Regel: Speichern Sie jeweils drei Sicherungskopien Ihrer Daten auf zwei unterschiedlichen Speicherarten und bewahren Sie mindestens eine Kopie an einem externen Standort auf.

Phase 1: Wiederherstellung von jeweils einem Domänencontroller pro Domäne (möglichst per Wiederherstellung mit fehlerfreiem Betriebssystem)

Im ersten Schritt geht es darum, den Betrieb überhaupt wieder aufzunehmen, wenn auch noch nicht im vollen Umfang. Dazu wird zunächst ein Domänencontroller pro Domäne wiederhergestellt. Wie diese Wiederherstellung erfolgt, hängt von den vorhandenen Tools ab. Die bevorzugte Methode ist eine Wiederherstellung mit fehlerfreiem Betriebssystem. Diese Möglichkeit besteht jedoch nur, wenn Sie eine AD-Notfallwiederherstellungslösung der Enterprise-Klasse nutzen, beispielsweise Recovery Manager Disaster Recovery Edition von Quest.

Warum ist nach einem Ransomware-Angriff eine Wiederherstellung mit fehlerfreiem Betriebssystem einer BMR vorzuziehen? In erster Linie liegt es daran, dass bei einer BMR ganze Volumes (Festplattenpartitionen) wiederhergestellt werden und somit auch Dateien, die nicht zu AD gehören, wie der Boot-Abschnitt, das Verzeichnis der Programmdateien sowie die Windows- und WinSXS-Verzeichnisse. Zwischen all diesen Dateien kann sich Malware leicht verstecken. Es besteht also das Risiko einer erneuten Infektion direkt nach der Wiederherstellung (siehe Abbildung 1). Bei einer Wiederherstellung mit fehlerfreiem Betriebssystem dagegen werden nur die AD-Komponenten wiederhergestellt, wodurch weitaus weniger potenzielle „Verstecke“ für Malware vorhanden sind (siehe Abbildung 2).

Beim Auswählen einer Wiederherstellungsstrategie sollten Sie zwei weitere Faktoren berücksichtigen. Zum einen gestaltet sich die Wiederherstellung mit einer BMR-Sicherung kompliziert. Auf dem Zielsystem muss zwar nicht zwingend ein Betriebssystem vorhanden sein, doch das physische Festplattenlayout muss identisch sein und die Kapazität der Festplatten muss mindestens der des ursprünglichen Domänencontrollers entsprechen, damit dieselben Partitionen eingerichtet werden können wie auf dem Ausgangssystem. Zum anderen stellt sich die Frage, ob Sie die in der BMR-Sicherung gespeicherten zusätzlichen Daten tatsächlich benötigen. Wenn Domänencontroller beispielsweise für Services genutzt werden, die nicht mit AD zusammenhängen (z. B. Hosting von nicht in AD integrierten DNS-Zonen, Ausführung einer Zertifizierungsstelle oder Ausführung von Datei- und Druckservices), kann eine BMR durchaus die beste Option sein.

Die Wiederherstellung mit fehlerfreiem Betriebssystem ist die bevorzugte Methode zur Wiederherstellung nach einem Ransomware-Angriff, weil bei einer BMR sehr viele potenzielle „Verstecke“ für Malware gegeben sind.

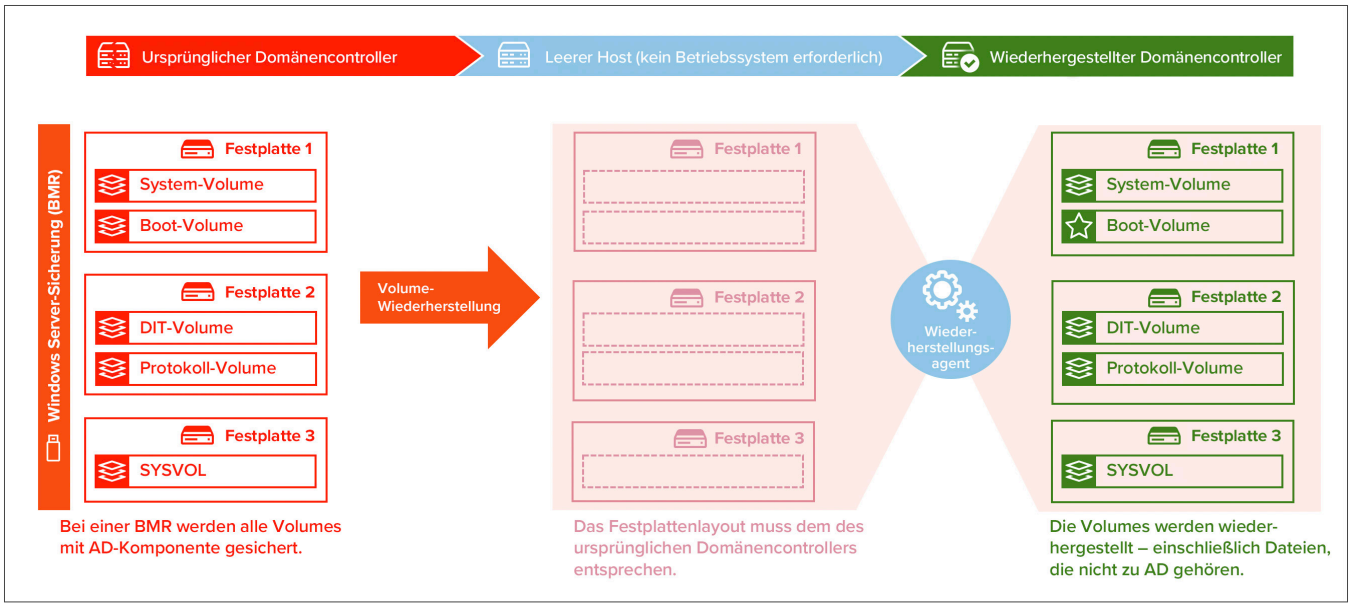


Abbildung 1: Bei einer Bare-Metal-Wiederherstellung sind sehr viele potenzielle „Verstecke" für Malware gegeben.

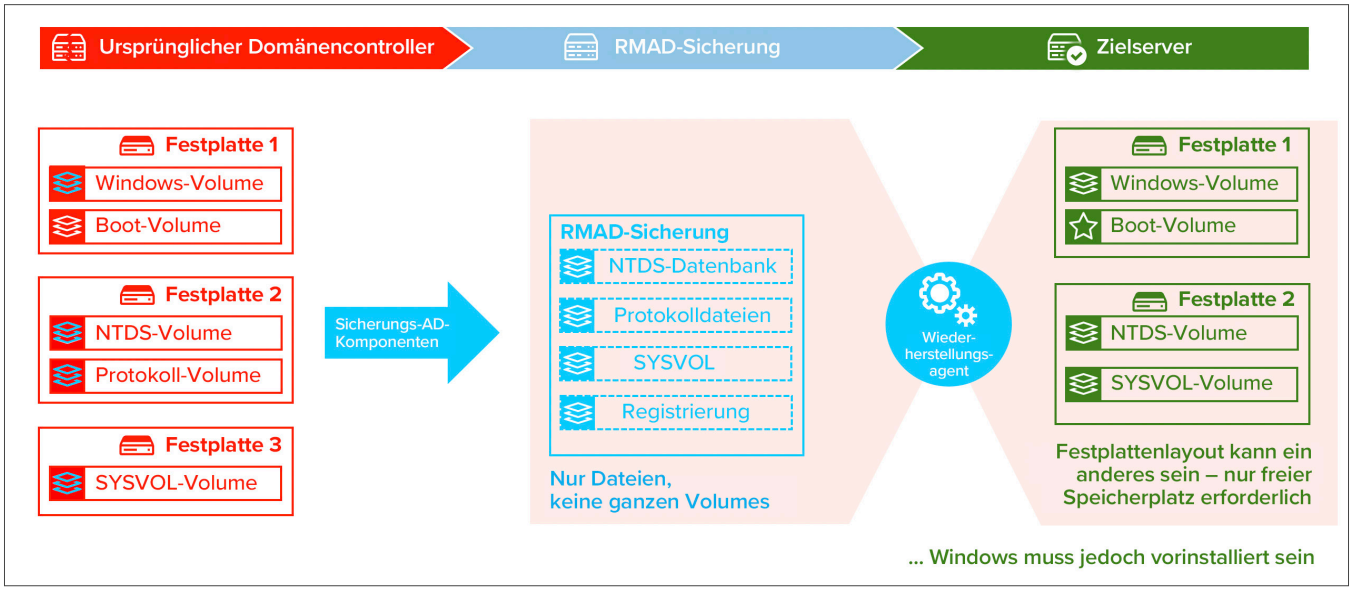


Abbildung 2: Die Wiederherstellung mit fehlerfreiem Betriebssystem (eine bei einigen Drittanbieterlösungen vorhandene Funktion) ist die bevorzugte Methode zur AD-Wiederherstellung nach einem Ransomware-Angriff.

Phase 2: Hochstufung der übrigen Domänencontroller (vorzugsweise mit IFM)

Wie sollten Sie zur Hochstufung der übrigen Domänencontroller vorgehen? Grundsätzlich bestehen hier verschiedene Möglichkeiten, darunter die Replikation. Die mit Abstand beste ist jedoch die IFM(Install From Media, Installation mit Medien)-Methode. Microsoft empfiehlt IFM, weil es sich um eine effiziente Vorgehensweise zur Neuinstallation von AD auf einem Domänencontroller handelt. Der Datenverkehr im Netzwerk wird dabei halbiert, sodass der Prozess deutlich schneller ablaufen kann. Wenn Sie Replikation statt IFM nutzen, kann der gesamte Vorgang je nach Standort der Domänencontroller leicht 12 bis 36 Stunden in Anspruch nehmen.

Mit nativen Tools ist IFM ein aufwendiger manueller Prozess, den Sie für jeden Domänencontroller einzeln durchführen müssen, indem Sie darauf jeweils die PowerShell-Befehle zur Installation mit Medien ausführen, um den betreffenden Domänencontroller hochzustufen. Eine Drittanbieterlösung kann die zweite Phase der Wiederherstellung erheblich beschleunigen, sodass Ihr Unternehmen wesentlich früher wieder auf die Beine kommt.

Mit IFM (Install From Media, Installation mit Medien) können Sie die übrigen Domänencontroller deutlich schneller hochstufen als mit anderen Methoden.

Auswahl der passenden Tools zum Umsetzen Ihres Plans

Viele Unternehmen überschätzen ihre Resilience gegenüber verheerenden Ransomware-Angriffen und wiegen sich fälschlicherweise in Sicherheit. Weder native Tools noch herkömmliche Datenschutzprodukte sind ein adäquater Ersatz für eine AD-Sicherungs- und -Notfallwiederherstellungslösung der Enterprise-Klasse. Dies gilt insbesondere im Fall von Ransomware. Wir sind bereits auf einige der Gründe eingegangen, sollten uns jedoch noch eingehender mit diesem Thema befassen.

Einschränkungen bei nativen Tools und manuellen Prozessen

Wie bereits erwähnt, bieten native Tools keine Möglichkeit zur Wiederherstellung mit fehlerfreiem Betriebssystem – welche das Risiko einer erneuten Ransomware-Infektion mindern würde – und das Hochstufen von Domänencontrollern per IFM gestaltet sich zeitaufwendig und mühsam. Native Methoden zur Sicherung und Wiederherstellung haben jedoch darüber hinaus weitere Nachteile, von denen einige nachfolgend erläutert werden.

Langwieriger, komplizierter Prozess zur Wiederherstellung der Gesamtstruktur

Das Wiederherstellen der AD-Gesamtstruktur mit nativen Tools und manuellen Prozessen ist kompliziert, zeitaufwendig und fehleranfällig. Microsoft listet im Microsoft-Leitfaden zur Wiederherstellung der Active Directory-Gesamtstruktur etwa 40 grundlegende Schritte auf, die durchgeführt werden müssen. Hierzu zählen u. a.:

- Isolieren der aktuell wiederherzustellenden Domänencontroller von den nicht oder erst später wiederherzustellenden
- Zurücksetzen der Kennwörter für Computer, Kerberos und Vertrauensbeziehung
- Erhöhen des RID-Poolwerts um 100.000 und Ungültigmachen der aktuellen RIDs auf den einzelnen Domänencontrollern, bevor diese genutzt werden dürfen
- Neuerstellen der globalen Kataloge

Diese Schritte sind auf jedem wiederherzustellenden Domänencontroller korrekt und in der richtigen Reihenfolge durchzuführen und der Prozess muss über die Gesamtstruktur hinweg koordiniert werden. Viele dieser Schritte beinhalten Vorgänge, mit denen AD-Administratoren nicht vertraut sind. Es handelt sich um aufwendige, oft auf Befehlszeilen basierende Schritte, bei denen schnell Fehler passieren, sodass Sie wieder von vorn beginnen müssen.

Abbildung 3: Einige der bei einer manuellen Wiederherstellung eines Domänencontrollers erforderlichen Schritte

VM-Snapshots: kein adäquater Ersatz für AD-Sicherungen

Viele Unternehmen haben zumindest einige ihrer Server virtualisiert. Eine Möglichkeit zum Sichern dieser Server sind Hypervisor-Snapshots, d. h. zu einem bestimmten Zeitpunkt erstellte Images von virtuellen Maschinen (VMs). Es ist jedoch aus verschiedenen Gründen nicht zu empfehlen, sich bei der Strategie zur AD-Notfall-wiederherstellung auf Snapshots zu verlassen.

Der wichtigste Grund: Wenn Sie Snapshots für die Wieder-herstellung der Gesamtstruktur verwenden, entstehen fast immer Probleme mit der Datenkonsistenz, die nur schwer zu beheben sind. Da die Daten auf Domänencontrollern ständig geändert werden und die Replikation einige Zeit in Anspruch nimmt, enthalten Snapshots von unterschiedlichen Domänencontrollern nahezu immer inkonsistente Informationen. Insbesondere entstehen bei der Wiederherstellung anhand von Snapshots fast immer sogenannte Lingering Objects – Objekte, die auf einem der Domänencontroller noch vorhanden sind, während sie von anderen

Domänencontrollern vollständig gelöscht wurden. Erkennung, Fehlerbehebung und Bereinigung dieser Objekte können sehr kompliziert sein.

Ähnlich wie BMR-Sicherungen können auch Snapshots Malware enthalten, die zusammen mit allen anderen Daten des Domänencontrollers wiederhergestellt wird. Zudem sind VM-Snapshots leichte Ziele für Ransomware-Verschlüsselung, sofern sie von Ihnen am Standardspeicherort ablegt werden. Die Snapshots werden dann nutzlos.

Hinzu kommt das logistische Problem. In der Regel hat das Virtualisierungsbetriebsteam die Kontrolle über die VM-Snapshots. Dies erschwert dem AD-Team bei der Wiederherstellung die Arbeit. Möglicherweise ist sich das Virtualisierungsteam gar nicht bewusst, wie wichtig die AD-Snapshots für die Strategie des Unternehmens zur Notfallwiederherstellung sind, und schützt sie daher nicht ausreichend.

Kein angemessener Schutz für reine Cloud-Objekte und -Attribute

Wir haben bereits erwähnt, wie wichtig Azure AD-Sicherungen in hybriden Umgebungen sind. Es gibt jedoch weitere Gründe, aus denen die nativen Microsoft-Tools keinen angemessenen Schutz für rein Cloud-basierte Objekte und Attribute bieten. Hierzu zählen:

- Für einige Objekte, darunter Azure AD-Gruppen, die Gruppenzugehörigkeit und dauerhaft gelöschte Benutzer, besteht keine Möglichkeit zur Wiederherstellung.
- Wiederherstellbar sind nur kürzlich (innerhalb der letzten 30 Tage) gelöschte Objekte.
- Auch bestimmte Attribute wie MFA-Einstellungen und Richtlinien für bedingten Zugriff lassen sich grundsätzlich nicht wiederherstellen.
- Eine Massenwiederherstellung ist nur per PowerShell-Skript möglich.
- Es gibt keine Änderungsprotokolle oder Vergleichsberichte für Azure AD, die Ihnen Anhaltspunkte dafür liefern könnten, was wiederhergestellt werden muss und was nicht.

Diese Auflistung ist längst nicht erschöpfend. Weitere Informationen finden Sie im Whitepaper „Was Sie über die Office 365 Und Azure AD Migration noch nicht wissen“.

VM-Snapshots sind kein Ersatz für eine AD-Notfallwiederherstellungslösung der Enterprise-Klasse.

Einschränkungen bei herkömmlichen Datenschutzlösungen

Viele Unternehmen haben als Reaktion auf die Einschränkungen bei nativen Tools gezielt in Sicherungstools oder andere Datenschutzlösungen investiert. Diese Produkte können in bestimmten Wiederherstellungsszenarien, beispielsweise zur Wiederherstellung des Betriebssystems, durchaus ausreichend sein. Manche Lösungen bieten sogar die Möglichkeit einer Bare-Metal-Wiederherstellung für Server.

Die meisten Datenschutztools sind allerdings für die Notfallwiederherstellung bei Active Directory schlichtweg ungenügend. Wie oben erwähnt, muss beim Wiederherstellen der Gesamtstruktur die Konfiguration über mehrere Domänencontroller hinweg koordiniert werden. Ohne diese Koordinierung besteht das Risiko von USN-Rollbacks, RID-Bubbles, RID-Wiederverwendung, im globalen Katalog verbleibenden Objekten (Lingering Objects) und anderen Problemen, die die Funktionstüchtigkeit von Active Directory erheblich beeinträchtigen können. Bei den meisten herkömmlichen Datenschutzlösungen geht es nur darum, die einzelnen Domänencontroller wieder zum Laufen zu bringen. Die Koordinierung bleibt Ihnen selbst überlassen.

Außerdem unterstützen manche Datenschutzlösungen zwar IFM, erfordern aber dennoch, dass jeder Domänencontroller einzeln hochgestuft wird. Diese Vorgehensweise ist sicher nicht die schnellste, um Ihr Unternehmen wieder auf die Beine zu bringen. Abschließend ist darauf hinzuweisen, dass rein Cloud-basierte Objekte und Eigenschaften von On-Premises-AD-Sicherungslösungen nicht abgedeckt werden.

Quest Recovery Manager for Active Directory Disaster Recovery Edition

Recovery Manager Disaster Recovery Edition optimiert die Wiederherstellung nach einem Ransomware-Angriff. Zum einen bietet die Lösung zuverlässige Sicherungen genau derjenigen Elemente, die für die AD-Wiederherstellung benötigt werden. Da irrelevante und riskante Komponenten wie Boot-Dateien und die IIS-Metabasis außen vor bleiben, werden die Sicherungen mit der Lösung kleiner, der Sicherungsprozess gestaltet sich effizienter und die Versteckmöglichkeiten für Malware werden reduziert. Darüber hinaus bietet Recovery Manager mit Secure Storage einen robusten Server, der nach IPsec-Regeln isoliert wird. Selbst wenn Sie Ihre Domänencontroller, den Tier-1-Speicher oder gar den Recovery Manager-Server verlieren, ist immer noch die Recovery Manager Secure Storage-Sicherung vorhanden, die zuverlässig vor Ransomware geschützt ist.

Wenn es zu einem Ransomware-Angriff kommt, wird mit Recovery Manager der gesamte Prozess zur AD-Wiederherstellung automatisiert, einschließlich der mehr als 40 Schritte aus dem Microsoft-Dokument zum Wiederherstellen von AD-Gesamtstrukturen. Unter anderem werden folgende Schritte durchgeführt:

- Automatischer Neustart der einzelnen Domänencontroller in DSRM
- Automatische Isolierung aller Domänencontroller während der Wiederherstellung
- Automatische Kennwortzurücksetzung
- Automatische Übernahme der FSMO-Rollen von Domänencontrollern, die nicht wiederhergestellt werden können
- Automatische Neuzuweisung von globalen Katalogen, falls der letzte globale Katalog eines Standorts nicht wiederhergestellt werden kann
- Automatische Löschung von im globalen Katalog verbleibenden Objekten (Lingering Objects)
- Automatische Bereinigung der Metadaten nach Abschluss der Wiederherstellung

Sie können dank flexibler Wiederherstellungsoptionen die Methode wählen, die sich in einer bestimmten Situation am besten eignet – ganz gleich, ob es sich um eine mehrere Phasen umfassende Wiederherstellung, eine Wiederherstellung mit fehlerfreiem Betriebssystem oder eine Bare-Metal-Wiederherstellung handelt. Die Wiederherstellung mit fehlerfreiem Betriebssystem ist auf jedem System möglich, ob physisches Gerät, virtuelle Maschine vor Ort oder in der Cloud gehostete VM. Recovery Manager bietet sogar eine automatisierte Malware-Erkennung, mit der das Risiko des erneuten Ladens infizierter Dateien auf wiederhergestellten Domänencontrollern minimiert wird. Nach dem Sichern von Active Directory können Sie Ihren Plan zur AD-Notfallwiederherstellung durch den Aufbau einer separaten virtuellen Gesamtstruktur-Testumgebung demonstrieren und validieren, um Notfallszenarien zu testen und sichere Tests durchzuführen, bevor Sie Änderungen in der Produktionsumgebung vornehmen.

Darüber hinaus beschleunigt Recovery Manager die zweite Phase des Notfallwiederherstellungsprozesses erheblich, weil die Lösung automatisiertes Massen-IFM ermöglicht: Mit nur einem Klick stoßen Sie den IFM-Prozess auf allen ausgewählten Domänencontrollern an. Fehleranfällige manuelle Prozesse und das zeitaufwendige Aufrufen jedes einzelnen Domänencontrollers entfallen. Die zur Wiederherstellung verwendete Sicherung kann auf einem beliebigen Medium (z. B. Band, CD, DVD) oder auf einer freigegebenen Netzwerkressource vorliegen. So profitieren Sie von maximaler Flexibilität und Kontrolle.

Ein weltweit tätiges Fertigungsunternehmen konnte nach einem Ransomware-Angriff die grundlegenden Betriebsabläufe mit Recovery Manager innerhalb von weniger als zwei Stunden wiederherstellen.

Beispiel: Beschleunigung der Wiederherstellung mit Recovery Manager nach einem Ransomware-Angriff

Ein weltweit tätiges Fertigungsunternehmen war von Ransomware betroffen, durch die 17 Domänencontroller auf mehreren Kontinenten ausfielen. Im Zuge des Angriffs wurden außerdem die AD-Kennwörter nahezu aller Benutzerkonten manipuliert. Auch Servicekonten waren hiervon betroffen.

Mit Recovery Manager for Active Directory Disaster Recovery Edition konnte das IT-Team die Betriebsfähigkeit schnell wiederherstellen: Der wichtigste Domänencontroller war schon nach etwa einer Stunde wieder verfügbar. Ein zweiter Domänencontroller wurde innerhalb von nur 12 Minuten wiederhergestellt, zwei weitere auf zwei Kontinenten in nur 36 Minuten. Das Unternehmen konnte seine Arbeit fortsetzen und die Wiederherstellung der verbleibenden Domänencontroller für einen späteren Zeitpunkt einplanen.

Der Projektmanager sagte dazu: „Ohne das Quest Tool wäre diese schnelle Wiederherstellung [...] unmöglich gewesen!“

Weitere Best Practices für die Notfallwiederherstellung

Ein Plan zur Notfallwiederherstellung kommt nicht ohne eine zuverlässige Strategie und entsprechende Tools zur Wiederherstellung nach einem Ransomware-Angriff aus. Beachten Sie für eine umfassende Strategie außerdem folgende Best Practices:

- Definieren Sie RTOs (Recovery Time Objectives, Ziele für die Wiederherstellungszeit) und RPOs (Recovery Point Objectives, Ziele für den Wiederherstellungszeitpunkt). Das RPO bestimmt, wie oft Sie Ihr AD sichern und replizieren, während das RTO Ihnen zeigt, welche Domänencontroller im Ernstfall zuerst wiederhergestellt werden müssen, damit die wichtigsten Unternehmensprozesse so schnell wie möglich fortgesetzt werden können.
- Richten Sie separate Kommunikationsmechanismen für den Notfall ein, die nicht von AD abhängig sind. So stellen Sie sicher, dass die Geschäftsbereiche, die IT und die für die Wiederherstellung zuständigen Personen weiterhin miteinander kommunizieren können.
- Legen Sie den Eskalationspfad und die wichtigsten Entscheidungsträger für jeden wichtigen Punkt im Notfallwiederherstellungsprozess fest. Sorgen Sie dafür, dass bekannt ist, wie die erforderlichen Mitarbeitenden überall und jederzeit erreicht werden können.
- Testen Sie den Plan mit Personen, die nicht an seiner Entwicklung beteiligt waren. Falsche Annahmen über die Verständlichkeit von Informationen können die Wiederherstellung zum Erliegen bringen oder in eine falsche Richtung lenken.

- Führen Sie mindestens zweimal im Jahr einen Testdurchlauf des Plans aus. Wie die Berechnung der Kosten von Ausfallzeit weiter oben in diesem Whitepaper eindrucksvoll gezeigt hat, zählt bei der Wiederherstellung jede Sekunde. Die beste Möglichkeit, wertvolle Zeit zu sparen: Üben Sie die Prozesse so lange ein, bis Sie sie quasi blind befolgen können.
- Aktualisieren Sie den Plan regelmäßig unter Berücksichtigung von Systemänderungen, aktuellen Compliancevorgaben, Änderungen beim Wiederherstellungsteam usw.

Fazit

Ransomware ist heute ein klares, nicht von der Hand zu weisendes Risiko für jedes Unternehmen. Sie müssen sicherstellen, dass Ihr Unternehmen so schnell wie möglich wieder auf die Beine kommt. In der Regel wird dazu eine mehrere Phasen umfassende Wiederherstellung durchgeführt.

Recovery Manager for Active Directory Disaster Recovery Edition bietet ein beispielloses Maß an Stabilität, Flexibilität und Optionen. Sie erhalten eine absolut zuverlässige Lösung zur Sicherung von Active Directory sowie flexible Wiederherstellungsoptionen wie die Wiederherstellung mit fehlerfreiem Betriebssystem, die das Risiko einer erneuten Malware-Infektion minimiert. Die Wiederherstellung von AD mit fehlerfreiem Betriebssystem ist auf jedem System unabhängig von Standort und Art (physisch, virtuell oder in der Cloud gehostet) möglich.

Kurz: Wenn der Ernstfall eintritt, können Sie als Held auftreten, statt zum Sündenbock zu werden. Weitere Informationen finden Sie unter https://www.quest.com/products/recovery-manager-for-active-directory-disaster-recovery-edition/.

Mit Recovery Manager können Sie sichergehen, dass Ihr Unternehmen nach einerm Ransomware-Angriff schnell wieder handlungsfähig ist.

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 System-verwaltung über die Verwaltung von Active Directory und Office 365 bis hin zur zuverlässigen 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