semperis

Deckt Ihr Active Directory-Notfallwiederherstellungsplan Cyberangriffe ab?

VON GUIDO GRILLENMEIER UND GIL KIRKPATRICK

02 WIEDERHERSTELLUNG VON ACTIVE DIRECTORY NACH EINEM CYBERANGRIFF
04 WARUM DER SCHUTZ VON ACTIVE DIRECTORY SO WICHTIG IST
06 WIE SICH DIE BEDROHUNGSLANDSCHAFT VERÄNDERT HAT
07 WARUM ACTIVE DIRECTORY ANFÄLLIG IST
11 WIEDERHERSTELLUNG VON ACTIVE DIRECTORY

WIEDERHERSTELLUNG VON ACTIVE DIRECTORY NACH EINEM CYBERANGRIFF

Vor sechzehn Jahren taten sich Gil Kirkpatrick (Semperis Chief Architect) und Guido Grillenmeier (Semperis Chief Technologist), die damals für verschiedene Unternehmen arbeiteten, zusammen, um ihre Erfahrungen und ihr Fachwissen zum Schutz und zur Wiederherstellung von Active Directory (AD) zu kombinieren. Das Ergebnis dieser Zusammenarbeit war die Veröffentlichung des Whitepapers „A Definitive Guide to Active Directory Disaster Recovery“ im Jahr 2005 Das Whitepaper sprach einen wunden Punkt in der Branche an, da die meisten Unternehmen AD inzwischen als faktischen Standard-Verzeichnisdienst für das Kontrollieren des Benutzerzugriffs auf ihr Unternehmensnetzwerk, ihre Anwendungen und ihre Dienste nutzten.

Damals war nur wenig über die vollständige oder teilweise Wiederherstellung von AD bekannt und nur wenige AD-Spezialisten waren sich der Herausforderung ganz bewusst. Im Whitepaper wurden die Mechanismen der AD-Wiederherstellung erläutert und es wurde aufgezeigt, wie wichtig es für Unternehmen ist, sich darauf vorzubereiten, Daten nach unterschiedlichen AD-Problemen vollständig wiederherzustellen. Es wurde beschrieben, wie man Daten nach unterschiedlichen Arten von Katastrophen wiederherstellen kann, etwa bei einer versehentlichen Löschung von AD-Objekten, einer falschen Gruppenrichtlinienkonfiguration oder ausgefallenen AD-Domänencontrollern. Das Dokument endete mit einer kurzen Beschreibung des Prozesses zur Wiederherstellung einer AD-Umgebung nach einem Komplettausfall, mit dem Vorbehalt: „Die Wahrscheinlichkeit, dass eine vollständige Wiederherstellung des AD Forest erforderlich ist, ist jedoch sehr gering.“

Das war damals. Heute sieht es anders aus. Die Cybersicherheitslandschaft hat sich drastisch verändert. Es vergeht keine Woche, in der nicht das lokale Windows-Netzwerk eines Unternehmens durch einen Ransomware- oder Wiper-Angriff außer Gefecht gesetzt wird. Darunter zum Beispiel im Jahr 2019 und Anfang 2020 (mit geschätzten Wiederherstellungskosten):

- Stadt New Orleans (über 3 Mio. Dollar)
- Stadt Baltimore (18 Mio. Dollar)
- Norsk Hydro (70 Mio. Dollar)
- Demant (80 Mio. Dollar)

Es gibt unzählige weitere Fälle. Die Sache ist die: Die Fähigkeit, Ihre AD-Umgebung vollständig aus einem Backup wiederherzustellen, nicht mehr nur eine nette Option als Reaktion auf ein höchst unwahrscheinliches Ereignis. Sie ist eine Voraussetzung.

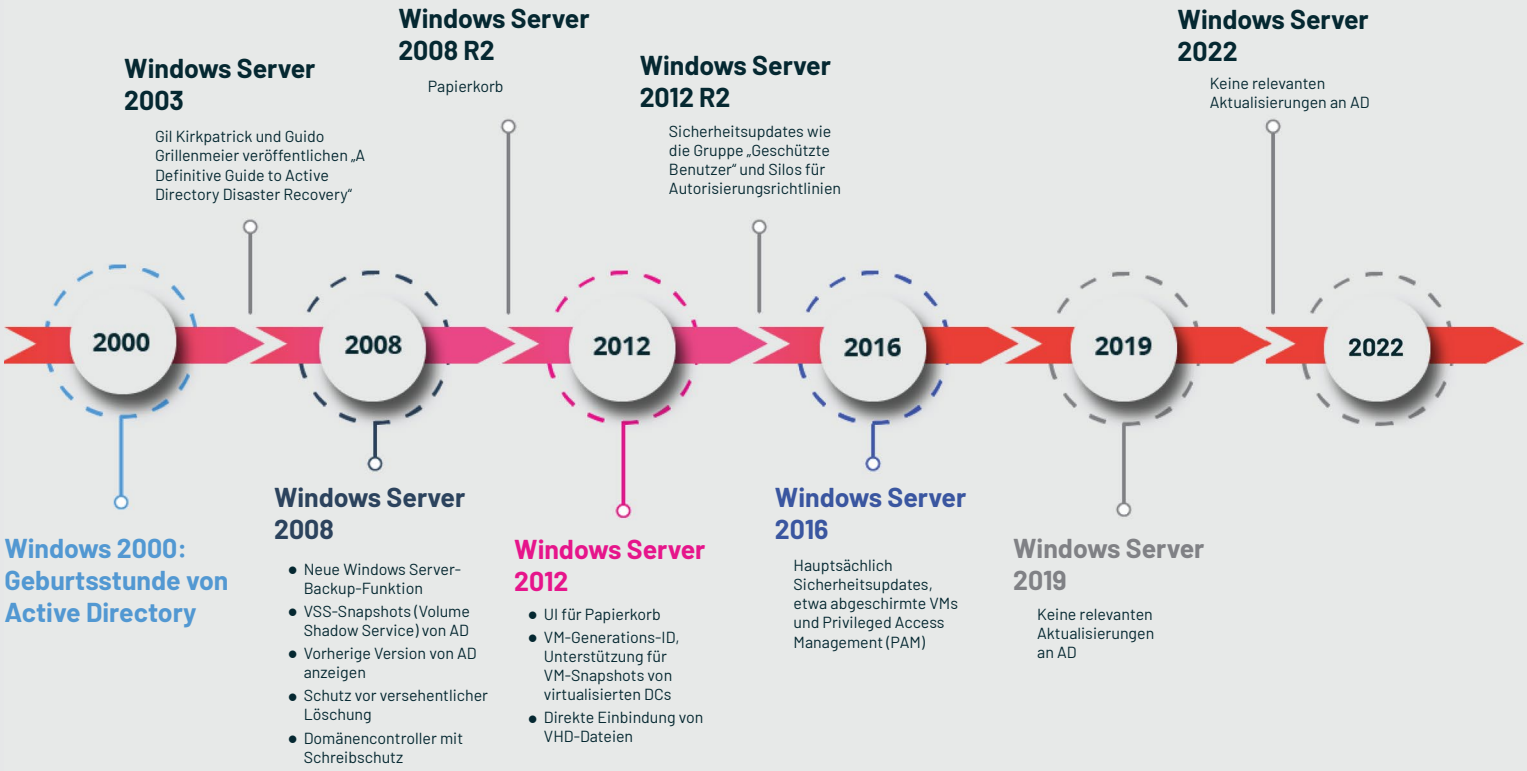
So, wie sich die Bedrohungslandschaft seit 2005 dramatisch verändert hat, hat sich auch das Windows Server-Betriebssystem und sein integrierter Active Directory-Dienst verändert. Microsoft hat die Sicherheit von Windows erheblich erhöht, Funktionen und Möglichkeiten zur Vereinfachung der Wiederherstellung von AD-Objekten hinzugefügt und das Verhalten von AD bei der Ausführung in einer virtualisierten Umgebung verbessert. Aber die grundlegenden Probleme bei der Wiederherstellung eines gesamten Active Directory Forest aus einem Backup haben sich nicht geändert. Es ist immer noch ein fehleranfälliger, komplexer Prozess, der Planung und Übung bei praktisch allen AD-Bereitstellungen erfordert.

Auffallend ist, dass die beiden neuesten Windows Server-Versionen (Windows Server 2019 und 2022) die ersten Versionen von Windows Server sind, die keine relevanten Updates für den AD-Dienst selbst enthalten. Es gibt nach Ansicht von Microsoft in AD offenbar keine Probleme mehr, die behoben werden müssten. Daher seien keine weiteren Serviceverbesserungen erforderlich. In Wirklichkeit geht es aber darum, dass die Notfallwiederherstellung von AD in Zukunft nicht einfacher werden wird.

Wir müssen jetzt die Wiederherstellungsfähigkeiten eines Unternehmens im Zusammenhang mit den neuen Cyber-Bedrohungen bewerten, die inzwischen eine Gefahr für AD darstellen und über die wir uns 2005 noch keine Gedanken machen mussten. Leider bedeutet die Zunahme der Angriffe, dass Unternehmen sich dringend auf eine schnelle Wiederherstellung nach Angriffen auf ihr Unternehmens-AD vorbereiten müssen. All die Verbesserungen, die Microsoft im Laufe der Jahre am Kern des AD-Dienstes vorgenommen hat, könnten sich beim Wiederherstellen Ihres AD als wenig hilfreich erweisen, wenn Sie Opfer eines Angriffs werden. Ist Ihr Unternehmen in der Lage, Ihr eigenes AD im Falle einer echten Katastrophe, bei der der gesamte AD-Dienst unbrauchbar gemacht wird, schnell wiederherzustellen?

„Unternehmen müssen sich dringend darauf vorbereiten, Daten nach Angriffen auf ihr Unternehmens-AD schnell wiederherzustellen.“

Änderungen im Laufe der Zeit im Zusammenhang mit dem Active Directory-Backup



Ist Ihr Unternehmen in der Lage, Ihr eigenes AD im Falle einer echten Katastrophe, bei der der gesamte AD-Dienst unbrauchbar gemacht wird, schnell wiederherzustellen?

WARUM DER SCHUTZ VON ACTIVE DIRECTORY SO WICHTIG IST

Active Directory (AD) wird seit mehr als 20 Jahren genutzt. In ihrer ursprünglichen Form bietet diese Microsoft-Serverrolle Folgendes:

Authentifizierung: Authentifiziert lokale Benutzer, die sich an ihren PCs und im Unternehmensnetzwerk anmelden, sowie Remote-Benutzer, die sich bei intern gehosteten Anwendungen oder virtuellen Desktops anmelden

Autorisierung: Steuert, für welche AD-integrierten Ressourcen – wie Dateidienste, Drucker, Exchange Server, SharePoint Server und SQL Server – sie Zugriffsrechte haben

Sicherheit und Kontrolle: Gruppenrichtlinien können Richtlinienkonfigurationen auf jeden Computer, Server und Benutzer anwenden, der mit AD verbunden ist

Verzeichnis: Ein einziger Ort für die Suche nach Benutzern und Ressourcen

DNS: AD-integriertes DNS für die Auflösung von Netzwerknamen

PKI: Active Directory-Zertifikatdienste stellen Zertifikate für Domänenbenutzer und -computer bereit

Die zunehmende Popularität des Windows Server-Betriebssystems für das Bereitstellen grundlegender Datei- und Druckfreigabedienste sowie anderer Back-Office-Dienste wie E-Mail, Messaging und Zusammenarbeit hat dazu beigetragen, dass AD zum bevorzugten Netzwerkverzeichnis wurde. Microsoft hat praktisch alle seine beliebten Anwendungen so weiterentwickelt, dass sie sich auf AD stützen, sodass AD heute einer der am weitesten verbreiteten Softwaredienste in Unternehmen ist. Mehr als 90 % aller Unternehmen weltweit mit mehr als 500 Mitarbeitern verwenden AD.

Der Aufstieg des Cloud Computing hat an dieser Abhängigkeit nichts geändert. Tatsächlich hat das Cloud Computing die Bedeutung von AD für Unternehmen gesteigert. Für die Bedeutung von AD für die Cloud gibt es zwei Gründe.

Erstens ist das Cloud-Computing-Modell nicht auf vertrauenswürdige Netze angewiesen, wie dies beim herkömmlichen lokalen Computing der Fall ist, da der Datenverkehr zwischen Kunden und den Ressourcen, auf die sie zugreifen, anders als bei herkömmlichen Unternehmensnetzen meist über das öffentliche Internet erfolgt. Dieser Datenverkehr wird nicht dadurch gesichert, WO Sie sind, sondern dadurch, WER Sie sind. Wie Microsoft es ausdrückt: „Die Identität ist die Steuerungsebene“, über die der Zugang zu Cloud-Ressourcen kontrolliert wird. Die Identität eines Benutzers steht bei der Cloud-Sicherheit im Mittelpunkt.

Zweitens bildet AD die Grundlage für die heute übliche Hybrididentitätsarchitektur. Bei dieser Architektur synchronisieren Unternehmen ihren lokalen Identitätsspeicher – in der Regel AD – mit dem Cloud-Identitätsdienst ihrer Wahl wie Azure Active Directory, Okta oder Amazon Web Services (AWS). Bei diesem Ansatz können Benutzer ihre Unternehmensidentität für den Zugriff auf Ressourcen (z. B. Office 365 oder Salesforce) verwenden, die in den Cloud-Identitätsdienst des Unternehmens integriert sind.

Darüber hinaus bringen viele Unternehmen Diensten in der Cloud noch nicht dasselbe Vertrauen entgegen wie ihren firmeneigenen kontrollierten Systemen, die vollständig von ihren eigenen IT-Mitarbeitern verwaltet werden. Daher haben sich viele dafür entschieden, für das Herstellen einer Verbindung zu Cloud-Lösungen wie Azure AD ein föderiertes Authentifizierungs-Framework mit AD Federation Services (ADFS) oder ähnlichen Lösungen einzurichten. In diesem Fall erfolgt die Validierung der Identität des Benutzers, d. h. die Authentifizierung, weiterhin anhand des eigenen lokalen AD. ADFS erstellt dann ein geeignetes Token, das SAML-Token, das dem Cloud-Dienst (z. B. Azure AD und zugehörige Anwendungen) bestätigt, dass der Benutzer, der gerade eine Verbindung herstellt, wirklich derjenige ist, der er zu sein vorgibt. Da das SAML-Token ordnungsgemäß mit einem Schlüssel verschlüsselt ist, der nur zwischen ADFS und Azure AD ausgetauscht wird, vertraut Azure AD diesem Token vollständig und gewährt dem Benutzer Zugriff auf die entsprechenden Cloud-Ressourcen. Im Wesentlichen vertraut Azure AD in dieser Konfiguration vollständig auf Ihr lokales AD.

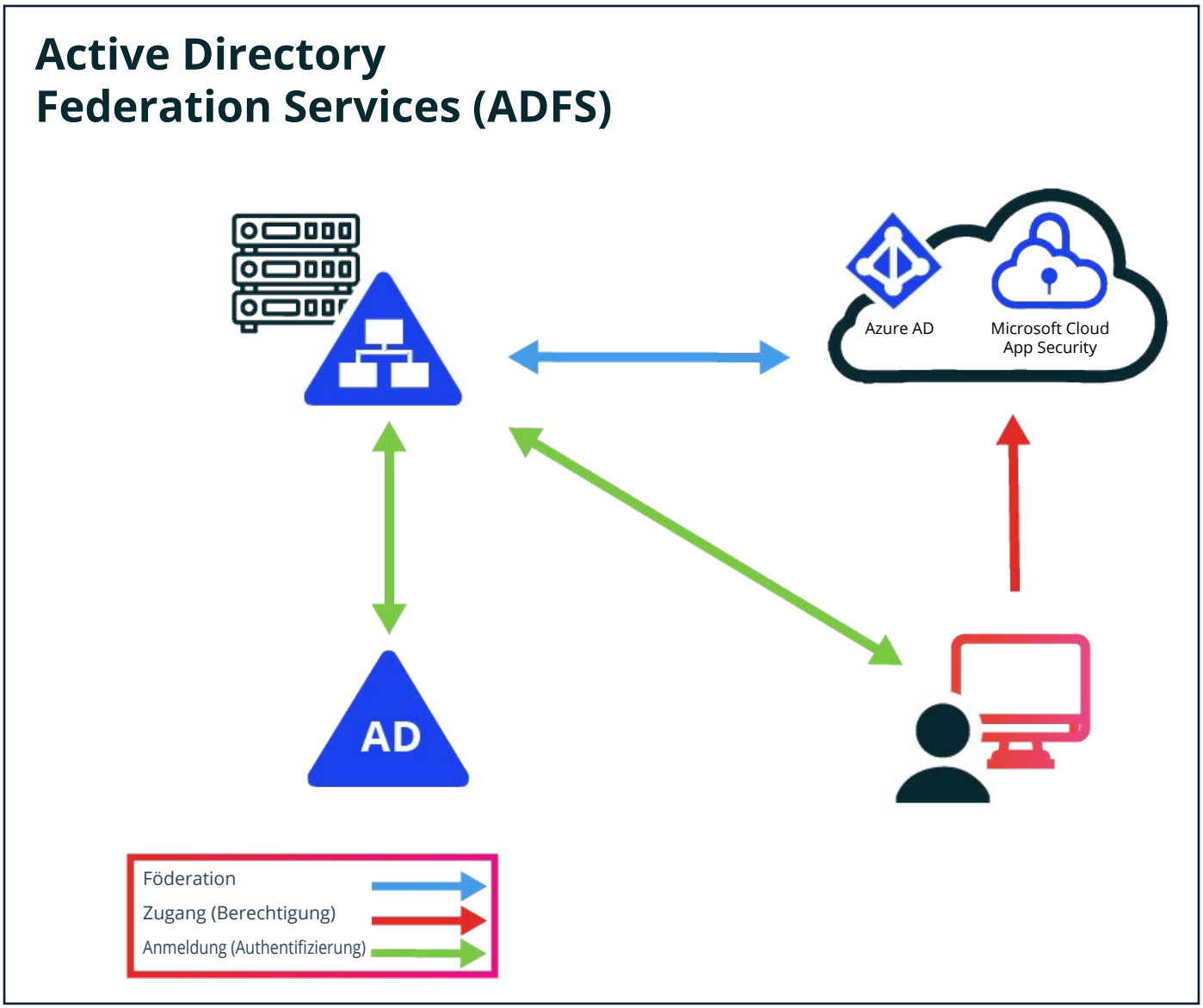


Abbildung 1: Die Föderation stützt sich in der Regel auf Ihr lokales AD, um die Identität Ihrer Benutzer zu zertifizieren

Hinzu kommt die Tatsache, dass trotz des ganzen Hypes und des Wechsels hin zu Cloud Computing alle Unternehmen, unabhängig von ihrer Größe und ihrem Alter, über umfangreiche und ständig laufende lokale Abläufe verfügen, die von AD abhängig sind. Daher ist AD heute nicht nur weiterhin für den Zugriff auf lokale Ressourcen unverzichtbar, sondern stellt auch eine wichtige Komponente des modernen hybriden Unternehmens und all seiner Anwendungen dar.

WIE SICH DIE BEDROHUNGSLANDSCHAFT VERÄNDERT HAT

Als das ursprüngliche Paper „A Definitive Guide to Active Directory Disaster Recovery“ verfasst wurde, gab es für AD-Administratoren hauptsächlich zwei Arten von Katastrophen: physische Katastrophen (z. B. Stromausfall, Festplattenabsturz oder Überschwemmung) und administrative Fehler (versehentlich oder böswillig), durch die AD-Objekte in unerwünschter Weise geändert oder gelöscht wurden. Die dritte Kategorie – ein Forest-weiter Ausfall des Dienstes – war eine interessante theoretische Möglichkeit, kam aber in der Praxis fast nie vor. Obwohl die Auswirkungen eines vollständigen Forest-Ausfalls katastrophal gewesen wären, war dieser so unwahrscheinlich, dass die meisten Unternehmen das daraus resultierende Restrisiko einfach hinnahmen.

Im Jahr 2021 sieht diese Risikokalkulation komplett anders aus. AD kommt nach wie vor gut mit physischen Server- und Standortproblemen zurecht, und nach 10 bis 20 Jahren Erfahrung können die meisten Unternehmen ihr Active Directory zuverlässig und sicher verwalten. Doch Cyberkriminelle, die mit ausgefeilten Phishing-Tools und der neuesten Aufklärungs-, Persistenz- und Datenverschlüsselungs-Malware bewaffnet sind, können die gesamte Windows-Umgebung eines Unternehmens innerhalb weniger Minuten funktionsunfähig machen. Die jüngsten Ransomware-Statistiken sind ernüchternd.

Im Jahr 2020 ...

... waren 51 % aller Unternehmen Opfer eines Ransomware-Angriffs. (PenTest Magazine)

... kostete Ransomware Organisationen etwa 75 Mrd Dollar (Datto).

... belief sich die durchschnittliche Lösegeldforderung bei Ransomware auf 178.000 Dollar, wobei die höchste bekannte Zahlung 11,8 Mio. Dollar betrug.

Das Risiko, den gesamten Active Directory-Dienst zu verlieren, ist inzwischen nicht mehr nebensächlich, sondern von größter Bedeutung.

Active Directory ist ein Hauptziel für Cyberkriminelle

Active Directory ist dafür ausgelegt, mit physischen Katastrophen umgehen zu können. Wenn ein DC ausfällt oder sogar ein ganzes Rechenzentrum offline geht, funktioniert AD mit den verbleibenden Domänencontrollern weiter. Microsoft hat die AD-Papierkorbfunktion in Windows Server 2008 R2 hinzugefügt, die die Wiederherstellung versehentlich gelöschter Objekte recht gut unterstützt. Was das Rückgängigmachen versehentlicher Änderungen an AD-Objekten angeht, sind Sie immer noch ziemlich auf sich allein gestellt.

Es ist klar, dass AD ein wichtiger Kerndienst in fast allen Unternehmen ist. AD speichert Benutzer-, Computer- und Dienstanmeldedaten und steuert die Authentifizierung und Autorisierung in der gesamten lokalen Umgebung. Dies macht AD aus drei Gründen zu einem lohnenden Ziel für Cyberkriminelle:

- Als Verzeichnisdienst ist AD eine zentrale Anlaufstelle für Informationen, die Cyberkriminelle benötigen, um sich horizontal durch das Netzwerk zu bewegen und ihre Berechtigungen zu erweitern.
- Als primärer Authentifizierungs- und Autorisierungsdienst ist AD ein einziger Angriffspunkt, der den Rest des Netzwerks praktisch unbrauchbar machen kann.
- Als faktische Lösung für die Verwaltung der Endgerätekonfiguration über Gruppenrichtlinien ist AD ein weiteres Tool, das Angreifer nutzen können, um Malware zu verbreiten und sich dauerhaft auf mehreren Computern im Netzwerk einzunisten.

Während wir in Nachrichtenartikeln über Cyberangriffe in der Regel nichts über technische Details erfahren, wird Active Directory immer häufiger erwähnt:

- Das Active Directory von Virgin Mobile wurde kompromittiert und seine Daten wurden im Dark Web verkauft.
- NTT Communication hat zugegeben, dass ihr Active Directory bei einer Datenpanne kompromittiert wurde.
- Es hat sich gezeigt, dass Ryuk-Ransomware Gruppenrichtlinien ändern kann, um sich über ein Anmeldeskript auf Endpunkte zu verbreiten.

Im Grunde wussten wir theoretisch schon immer, dass Active Directory sehr wahrscheinlich bei Angriffen eine Rolle spielte, aber jetzt haben wir Daten, die das beweisen.

WARUM ACTIVE DIRECTORY ANFÄLLIG IST

Active Directory funktioniert recht gut, und sein Design hat sich im Laufe der Zeit bewährt. Mit dem Aufkommen von Kryptoversionen, der Offenheit für Abfragen, Kerberos und der zunehmenden Raffinesse von Angriffen, die Tools wie Mimikatz einsetzen, hat sich die Welt um AD herum jedoch verändert.

APTs (Advanced Persistent Threats): Infiltration und Datenpannen

Angriffe auf AD haben in den letzten Jahren dramatisch zugenommen, da Angreifer erkannt haben, dass ihnen die IT-Ressourcen eines Unternehmens gehören, wenn sie dessen AD erst einmal in Besitz genommen haben. AD nimmt eine zentrale Rolle im System ein, aber das allein ist nicht der springende Punkt. Von großer Bedeutung sind auch die zahlreichen Ressourcen des Unternehmens, die von AD abhängig sind. Auch wenn Endbenutzer sich ihrer Abhängigkeit von AD nicht bewusst sind, könnten die verschiedenen Tools und Geschäftsprozesse, die sie täglich nutzen, nicht funktionieren, wenn AD ausfällt. Dazu gehören Anwendungen für wichtige Dienste wie E-Mail (Exchange), Dateifreigabe (SharePoint, normale Dateifreigaben), Zusammenarbeit (Skype) oder sogar die Möglichkeit zu drucken. Viele Unternehmen nutzen darüber hinaus die integrierte Authentifizierung von Windows für viele ihrer Geschäftsanwendungen und Datenbanken, wobei „Windows-integriert" einfach ein anderer Ausdruck für „AD-integriert" ist. Es bedeutet, dass die Anwendungen sich nicht auf ihre eigene Benutzerliste verlassen, sondern dem Zugriffstoken eines Benutzers vertrauen, das von AD generiert wird, um berechtigten Zugriff auf eine Anwendung zu gewähren. AD kontrolliert nicht nur den Zugriff legitimer Benutzer auf diese Anwendungen, sondern ermöglicht es auch Eindringlingen, zu verstehen, welche Anwendungen in eine Infrastruktur integriert wurden, und diese gegen Sie zu verwenden.

Mit der Erkenntnis, dass AD ein wertvolles Ziel ist, ist auch das Angriffsarsenal gewachsen. PowerSploit, Bloodhound, Death Star, Cobalt Strike und vor allem Mimikatz haben es Angreifern ermöglicht, schnell Zugangsdaten zu finden, eine horizontale Erkundung des Netzwerks durchzuführen, den kürzesten Weg zu Domänenadministratorrechten zu finden und diesen Weg gezielt zu nutzen.

Diese Tools verkürzen die Zeit bis zur Domänenbeherrschung von Tagen auf Stunden. Daher ist ein erfolgreicher Angriff auf Active Directory heute einfacher als je zuvor.

Die Cyberkatastrophe: DoA-Angriffe

AD ist erstaunlich fehlertolerant gegenüber natürlichen oder physischen Katastrophen. Orkane, Tornados, Erdbeben, Stromausfälle und andere Ereignisse, die ein Rechenzentrum außer Gefecht setzen, beeinträchtigen ein gut konzipiertes AD lokal, ermöglichen aber dem Rest des Netzes, den Dienst weiterhin zu nutzen. Wenn der lahmgelegte Abschnitt des AD wieder in Betrieb genommen wird, werden alle Änderungen, die während des Ausfalls im Netz vorgenommen wurden, automatisch in den wiederhergestellten Abschnitt übernommen. Ein Vorfall, bei dem eine AD-Domäne oder einen AD-Forest komplett ausgelöscht wird, hätte sehr schwerwiegende Auswirkungen, wäre aber aufgrund der Vorsichtsmaßnahmen, die Unternehmen zur geografischen Verteilung ihrer AD-Infrastrukturen getroffen haben, auch äußerst selten. Das Risiko, dass AD nicht verfügbar ist, wurde daher immer als höchstens moderat eingestuft. In Verbindung mit der Tatsache, dass die Geschäftskontinuität und Notfallwiederherstellung von Active Directory (BCDR, Business Continuity und Disaster Recovery) sehr teuer ist (dazu später mehr), wurde die Wiederherstellung von Forests bei der BCDR-Planung in der Vergangenheit vernachlässigt.

Dann betraten DoA-Angriffe (Denial-of-Availability) die Weltbühne. Die bekanntesten Varianten dieser Art sind Ransomware und Wiperware. Fast jeder weiß, was Ransomware ist. Es vergeht kaum ein Tag, an dem nicht berichtet wird, dass Kunden, Server und Daten eines Unternehmens verschlüsselt wurden und dass die Angreifer einen gewissen Betrag in Bitcoin dafür fordern, dass sie den Entschlüsselungsschlüssel bereitstellen. Wiperware zerstört Ihre Computer und Daten, sei es durch Verschlüsselung oder durch vollständiges Löschen von Daten, ohne dass eine Wiederherstellung möglich ist.

Der NotPetya-Angriff von 2017 ist das bisher bekannteste Beispiel für einen Angriff dieser Art. Die Container-Reederei Maersk war eines der Hauptopfer. NotPetya löschte Tausende von Computern, Servern und, ja, alle AD-Domänencontroller von Maersk weltweit aus, einschließlich ihrer Backups. Maersk hatte einfach Glück, dass ein Stromausfall verhinderte, dass sich die Malware auch auf den Domänencontroller in Ghana ausbreiten konnte: So war Maersk schließlich in der Lage, diesen DC zu verwenden, um das AD wiederherzustellen. Nach einer sehr teuren Wiederherstellung, die Maersk schätzungsweise zwischen 250 und 300 Millionen Dollar gekostet hat, beschloss das Unternehmen, öffentlich über seine Situation zu sprechen, um andere Unternehmen auf die Risiken moderner Malware-Angriffe auf ihre Infrastruktur aufmerksam zu machen. Unternehmen müssen sich auf diese Bedrohung vorbereiten, denn die meisten würden einen neuntägigen Ausfall ihrer zentralen IT nicht überstehen – und so lange brauchte Maersk, um sein Active Directory vollständig wiederherzustellen.

Weitere stark betroffene Opfer des NotPetya-Angriffs waren FedEx, Saint-Gobain, Reckitt Benckiser und Mondelēz. Und der NotPetya-Angriff war bei weitem nicht der letzte Angriff auf AD. Dies war lediglich der Beginn einer neuen Ära sich schnell ausbreitender Ransomware-Angriffe, die Active Directory nutzen und beeinflussen. Leider gibt es bei AD reichlich Angriffsvektoren. Erst kürzlich konnte ein erfolgreicher Angriff von Nefilim das mit hochgradigen Berechtigungen versehene Domänenadministratorkonto eines verstorbenen Mitarbeiters nutzen, um den Eindringlingen sämtliche Türen zu öffnen.

Ihre Active Directory-Backups werden Ihnen nicht dabei helfen, Ihren AD-Dienst wiederherzustellen

Im Falle einer Cyberkatastrophe helfen normale Active Directory-Backups nicht, den Geschäftsbetrieb nach dem Angriff wiederaufzunehmen. Die Funktion „Objekte vor versehentlichem Löschen schützen" hilft, menschliches Versagen zu vermeiden, hilft aber nicht gegen bösartige Aktivitäten in Ihrem AD.

Das Gleiche gilt für den Papierkorb, aus dem Sie zwar gelöschte Objekte wiederherstellen können, der Ihnen aber nicht dabei hilft, Änderungen auf Attributebene oder Änderungen an GPOs oder der Konfiguration in Ihrem AD rückgängig zu machen. Der Papierkorb kann auch nicht bei der Wiederherstellung Ihrer gesamten Domäne oder Ihres gesamten Forest und der zugehörigen Anwendungspartitionen helfen.

Die Verwendung von Snapshots kann die Erkennung von Änderungen auf Attributebene unterstützen und dabei helfen, diese rückgängig zu machen, erhöht aber die Komplexität des Wiederherstellungsprozesses.

Keine dieser Methoden zur Wiederherstellung von Active Directory-Daten reicht jedoch aus, um den eigentlichen AD-Dienst, d. h. die gesamte Domäne oder den gesamten Forest, wiederherzustellen. Auch wenn wir alle hoffen, dass uns das nie selbst betrifft, kann eine Schemabeschädigung aufgrund einer böswilligen Änderung durch einen Eindringling oder die Verschlüsselung aller Ihrer DCs durch Malware eine Wiederherstellung Ihres AD auf Forest-Ebene erforderlich machen. Hierfür benötigen wir weiterhin ein professionelles Backup der AD-DCs.

Vorbereitung eines Backups, das die Malware-freie Wiederherstellung von Active Directory-Diensten ermöglicht

Die Wiederherstellung des Active Directory-Dienstes, d. h. die Wiederherstellung der NTDS.dit-Datei und der zugehörigen Betriebssystemdateien und -einstellungen, um eine ordnungsgemäße Replikation der AD-Daten zu ermöglichen, ist eine wesentlich anspruchsvollere Aufgabe als die Wiederherstellung einzelner AD-Objekte. Wenn alle Änderungen an allen Objekten und Attributen auf einem einzigen AD-Datenbankserver – einem einzigen Domänencontroller – gespeichert würden, wäre die Wiederherstellung des Servers eine einfache Angelegenheit, ähnlich wie bei einem Dateiserver.

Die große Stärke und der Erfolg von Active Directory beruhen jedoch auf der Tatsache, dass anders als bei seinen Vorgängern die im Verzeichnis vorgenommenen Änderungen nicht auf einen einzigen Server oder einen einzigen Master beschränkt sind. Stattdessen wurde AD als Multi-Master-Datenbankarchitektur konzipiert, die es ermöglicht, dass Änderungen auf jedem (beschreibbaren) Domänencontroller im Netzwerk eines Unternehmens vorgenommen werden können. Dies hat die Skalierbarkeit und die geografische Ausbreitung des Active Directory-Dienstes ermöglicht und erlaubt es einer AD-Domäne oder einem AD-Forest, viele Standorte zu bedienen, die über den ganzen Globus verteilt sind.

Im „Definitive Guide" werden bestimmte Punkte zum globalen DC-Backup ausführlicher behandelt. Sich über die geografische Verteilung Ihrer AD-DCs und von deren Backups Gedanken zu machen, ist aber genauso wichtig wie die Durchführung des eigentlichen Backups. Bei der Planung Ihrer AD-Backups sollten Sie immer darüber nachdenken, ob die gewählten DC-Backups ausreichen, um Ihren AD-Forest schnell wiederherzustellen. Dies ist besonders schwierig in einem Multi-Domänen-Forest, d. h. einem Forest mit mehreren untergeordneten Domänen oder parallelen Bäumen, die Teil derselben AD-Forest-Struktur sind. Sobald Ihr AD-Forest mehrere Domänen umfasst, ist der Globale Katalog eine notwendige AD-Funktionalität, die während eines Forest-Wiederherstellungsprozesses neu erstellt und neu aktiviert werden muss, damit die Authentifizierungsdienste ihre Arbeit wieder aufnehmen können. Und die erneute Erstellung des Globalen Katalogs wird viel länger dauern, wenn sich in jeder Domäne in Ihrem Forest auf derselben AD-Site nicht mindestens ein DC befindet. Weiter unten gehen wir auf weitere Herausforderungen ein, die es zu bewältigen gilt, wenn Sie Ihren Forest schnell wiederherstellen möchten.

Integration mit dem Volume Shadow Copy Service

Es versteht sich von selbst, dass das Backup-Tool, das Sie zum Sichern Ihrer Active Directory-DCs verwenden, mit der VSS-Funktion (Volume Shadow Copy Service) des Windows Server-Betriebssystems kompatibel sein sollte. Diese Integration stellt einen konsistenten Zustand Ihrer AD-Datenbank zum Zeitpunkt der Durchführung eines Backups sicher, d. h. alle laufenden Schreibvorgänge sind abgeschlossen und auf die Festplatte geschrieben, während neue eingehende Änderungen an der AD-Datenbank zum Zeitpunkt der Durchführung eines Snapshots der AD-Datenbank angehalten werden. Dieser Vorgang dauert nur wenige Sekunden. Danach hat das Backup-Tool die nötige Zeit, um den konsistenten Zustand der AD-Datenbank auf ein Ziel Ihrer Wahl zu kopieren, während die Schreiboperationen auf die ursprüngliche AD-Datenbank den AD-Domänencontroller wie gewohnt weiterlaufen lassen können.

Das integrierte Windows Server Backup (WSB) ist ein gutes Beispiel für ein Backup-Tool, das vollständig mit VSS kompatibel ist und mit dem Sie zwei Arten von Backups durchführen können:

1. SSB (System State Backup)

2. BMR (Bare Metal Recovery)

Die beiden Optionen unterscheiden sich in ihren Anwendungsfällen. Daher sollten Sie bei der Planung Ihrer Backup-Strategie die unterschiedlichen Funktionen berücksichtigen.

System State Backups können Malware enthalten

Bei System State Backups werden alle kritischen Teile des Server-Betriebssystems eines DCs gesichert, einschließlich der Datei für die AD-Datenbank (NTDS.dit), des SYSVOL-Ordners, der COM+-Klassenregistrierungsdatenbank, der Server-Registry und der Startdateien, jedoch unter Vermeidung von Benutzerdaten, zusätzlichen Datenträgern und Daten, die möglicherweise für andere Anwendungen auf demselben Server hinzugefügt wurden. Während das Backup die VSS-Funktionen nutzt, um einen korrekten Snapshot der vom Server verwendeten Festplatten zu erstellen, handelt es sich beim System State Backups um eine Übertragung einer dateibasierten Kopie der relevanten Dateien an das Backup-Ziel. Hierbei sind keine inkrementellen Backups zulässig. Sie müssen also immer den vollständigen Systemzustand an den Ziel-Backup-Speicherort übertragen. Zusätzlich zu Ihrer AD-Datenbank speichert ein System State Backup etwa 11 GB der Windows-Betriebssystemdateien in jedem DC-Backup.

Die Wiederherstellung des System State Backups ist für dieselbe Windows Server-Instanz und Betriebssystem-Installation gedacht, von der aus es erstellt wurde. Das bedeutet, dass es im Falle eines Problems auf Betriebssystem- oder Datenebene helfen soll, aber nicht im Falle eines Hardware-Problems, das eine Neuerstellung des gesamten Servers erfordert. Daher eignet sich ein System State Backup für die Wiederherstellung der AD-Datenbank in solchen Fällen gut, in denen Sie Teile einer AD-Datenbank autorisiert wiederherstellen müssen, um versehentlich gelöschte Objekte aus AD wiederherzustellen. Ein System State Backup ist jedoch nicht dazu gedacht, Ihr Backup auf einem neu installierten Server wiederherzustellen, und schon gar nicht auf einem Server mit anderer Hardware oder gar nach einem Wechsel von einer physischen zu einer virtuellen Architektur oder umgekehrt. Dennoch könnte ein System State Backup Ihre einzige Option sein, wenn Sie nach einem Cyberangriff Ihre AD-DCs sofort auf anderer Hardware oder virtuellen Maschinen wiederherstellen müssen, die Ihnen schneller zur Verfügung gestellt werden könnten. Beachten Sie in jedem Fall, dass das System State Backup verschiedene Dateien aus dem Betriebssystem enthält, die gesichert wurden. Das bedeutet, dass die Wahrscheinlichkeit einer erneuten Infektion durch Malware, die mit Ihrem AD gesichert wurde, nicht unerheblich ist.

„Beachten Sie, dass das System State Backup verschiedene Dateien aus dem Betriebssystem enthält, die gesichert wurden. Das bedeutet, dass die Wahrscheinlichkeit einer erneuten Infektion durch Malware, die mit Ihrem AD gesichert wurde, nicht unerheblich ist."

„Wie bei System State Backups ist auch bei der Wiederherstellung von AD aus BMR-Backups nach einem Cyberangriff Vorsicht geboten, um eine erneute Einschleppung von Malware zu vermeiden."

BMR-Backups können auch Malware enthalten

Wie der Name schon andeutet, können Sie mit Backups, die mit der BMR-Option (Bare Metal Recovery) erstellt wurden, einen bestimmten Server in seinem gesicherten Zustand wiederherstellen, einschließlich der vollständigen Wiederherstellung des Betriebssystems und der darauf laufenden Dienste sowie von Active Directory. Ziel ist es, Sie vor den klassischen Ausfällen auf Hardwareebene zu schützen, z. B. vor defekten Festplatten. Mit BMR-Backups kann aber auch Malware eingeschleppt werden, wenn sie zur Wiederherstellung von AD verwendet werden.

Mit der BMR-Option werden alle Festplatten gesichert, die vom Betriebssystem verwendet werden, also auch der Systemzustand. Sie können auch zusätzliche Festplatten auf dem jeweiligen Server sichern. Da ein BMR-Backup mit der blockbasierten Backup-Methode erstellt wird, haben Sie auch die Möglichkeit, Backups nur der Blöcke zu konfigurieren, die seit dem letzten Backup geändert wurden: Sie können ein inkrementelles Backup durchführen, um Ihre Backups weiter zu beschleunigen. Inkrementelle Backups funktionieren, wenn Sie die entsprechende Option in den Einstellungen für die Backup-Performance auf Ihrem Server konfiguriert haben und sich das Ziellaufwerk für das Backup auf dem Server befindet, auf dem Sie auch das Backup erstellen. Der letztgenannte Ansatz mag nicht unmittelbar einleuchten, funktioniert aber, wenn Sie zusätzliche Mechanismen zur Hand haben, um die erstellten Backup-Dateien anschließend auf einem anderen sicheren Speicherziel zu speichern.

Zum Zeitpunkt der Wiederherstellung müssen Sie den reparierten Server mit einem geeigneten Windows Server OS-Installationsdatenträger starten, damit Sie ihn aus der entsprechenden Backup-Datei wiederherstellen können. Beachten Sie, dass auch diese Serverinstallation den gleichen Hardwaretyp und die gleiche Architektur aufweisen muss. Mit der BMR-Option ist es beispielsweise nicht möglich, ein Backup eines Dell-Servers auf einem neuen Server von HPE wiederherzustellen oder eine virtuelle Maschine als Ziel für die Wiederherstellung auszuwählen. Aufgrund dieser Einschränkung und weil es eine einfache Möglichkeit gibt, ein neues Replikat eines AD-Domänencontrollers zu erstellen, indem Sie es nach einer sauberen Betriebssysteminstallation auf eine beliebige Hardware übertragen, wird die BMR-Methode nur selten zum Sichern von Active Directory-DCs verwendet. Wie bei einem System State Backup besteht auch bei BMR-Backups das Risiko, dass sie Malware enthalten, die Ihre AD-DCs befallen haben könnte, bevor sie aktiv wurde und Ihren AD-Forest beschädigte. Wie bei System State Backups ist auch bei der Wiederherstellung von AD aus BMR-Backups nach einem Cyberangriff Vorsicht geboten, um eine erneute Einschleppung von Malware zu vermeiden.

Beachten Sie auch, dass weder SSB- noch BMR-Backups von der Windows Server-Backupfunktion verschlüsselt werden. Das bedeutet, dass Ihre Backups bei der Übertragung und ganz bestimmt auch im Ruhezustand angreifbar sind, wenn Sie den Datenträger, auf dem sich Ihre Backups befinden, nicht verschlüsselt haben. Das bedeutet auch, dass Sie die Backup-Dateien nicht auf ein anderes, für andere Personen als Domänenadministratoren zugängliches Zielspeichersystem kopieren sollten, ohne sie zuvor ordnungsgemäß zu verschlüsseln.

Achten Sie darauf, die Backup-Dateien sicher zu speichern, und sorgen Sie dafür, dass nur die Administratoren des AD-Dienstes Zugriff darauf haben.

Seien Sie vorsichtig bei der Verwendung von Snapshots

Snapshots sind gefährlich! Snapshots sind die Rettung!

Beide Aussagen sind in gewissem Maße berechtigt. Bis zur Veröffentlichung von Windows Server 2012, bei dem eine ordnungsgemäße Kennung der Version einer VM bei der Verwendung von Snapshots auf VM-Ebene (VMGenID) hinzugefügt wurde, musste Microsoft ständig auf die fehlende Unterstützung für Snapshots von DCs in virtuellen Umgebungen aufmerksam machen. Administratoren konnten allzu leicht den Fehler machen, einen DC „in der Zeit zurückzuversetzen", ohne die richtige AD-Wiederherstellungsmethode zu verwenden, bei der andere Rechenzentren in der Umgebung über dieses Rollback informiert wurden. Dieses Versäumnis konnte zu allen möglichen Replikationsproblemen führen, da die integrierte Replikationslogik des komplexen AD-Ökosystems unterbrochen wurde. Dadurch erfolgte ein USN-Rollback (Update Sequence Number), was zu einem unzuverlässigen Objektstatus im AD-Forest führte mit der Gefahr, dass doppelte SIDs erstellt und veraltete Objekte beibehalten werden.

Unter der Annahme, dass mittlerweile alle Ihre DCs weltweit mindestens mit Windows Server 2012 betrieben werden und Sie einen Hypervisor verwenden, der die VMGenID-Logik unterstützt (alle großen Hypervisoren tun dies seit Jahren), können wir uns die Details dazu ersparen, weshalb das Zurücksetzen von DCs auf eine frühere Version über einen VM-Snapshot in der Vergangenheit wirklich nicht optimal war. Es handelt sich zwar immer noch keineswegs um einen Backup-Mechanismus für Ihren AD-Forest, aber Sie können Ihrem AD zumindest keinen Schaden mehr zufügen, wenn Sie die VM-Snapshot-Technologie verwenden.

In dem demnächst erscheinenden Whitepaper „The New Definitive Guide to Active Directory Disaster Recovery" werden wir kritische Änderungen behandeln, die Microsoft mit Windows Server 2008 eingeführt hat und die sich auf die native AD-Sicherung und -Wiederherstellung auswirken: Die Integration der AD-Datenbank mit den VSS-Funktionen des Betriebssystems. Wir werden auch die überarbeitete WSB-Funktion (Windows Server Backup) behandeln, die ebenfalls mit Windows Server 2008 eingeführt wurde und mit der Backup-Daten als VHD-Datei zugänglich gemacht wurden. Außerdem werden wir die praktische Funktion erläutern, die Microsoft mit der Version 2012 hinzugefügt hat: die Möglichkeit, VHD-Dateien direkt in einen vorhandenen Windows-Client zu mounten, was die schnelle Suche nach einer früheren Version der AD-Datenbank ermöglicht.

All diese Änderungen machen es für Administratoren einfacher, beispielsweise Dateien aus einer früheren Version Ihres SYSVOL-Ordners abzurufen oder eine schreibgeschützte Version Ihrer AD-Daten zu verwenden, um überschriebene Attribute Ihrer Objekte wiederherzustellen. Im Hinblick auf das Schließen von Active Directory-Sicherheitslücken liegt der Schlüssel hier darin, Ihre Backup-Dateien richtig zu schützen, da jeder, der Zugriff auf diese sensiblen Dateien hat, damit alles tun kann, was Sie tun können. Eine solche Person kann sogar andere Offline-Bearbeitungstools verwenden, um die Passwort-Hashes und andere sensible Daten aus dem AD-Backup abzurufen. Achten Sie darauf, die Backup-Dateien sicher zu speichern, und sorgen Sie dafür, dass nur die Administratoren des AD-Dienstes Zugriff darauf haben.

Beachten Sie die Einschränkungen bei Backup-Tools von Drittanbietern

Im Grunde muss jedes Backup-Tool, das heute dazu dienen soll, AD zu sichern, auch in die VSS-Funktionen des Betriebssystems integriert sein oder sogar die WSB-Funktion (Windows Server Backup) nutzen und einfach mehr Intelligenz einsetzen, um eine angemessene Auswahl Ihrer DCs zentral zu sichern.

Wie bei dem integrierten WSB-Tool bedeutet die Möglichkeit, AD-Domänencontroller zu sichern, jedoch nicht automatisch, dass ein Tool Ihnen helfen kann, Ihren AD-Forest schnell wiederherzustellen, falls Ihr Schema beschädigt ist oder alle Ihre DCs von Malware oder einem anderen Cyberangriff infiziert wurden. Beachten Sie, dass die meisten Backup-Lösungen, die sich auf Backups auf Betriebssystemebene konzentrieren, zwar gut für die Wiederherstellung einzelner Server und sogar Domänencontroller geeignet sind, aber (wie im nächsten Abschnitt erläutert) den komplexen Wiederherstellungsprozess, der erforderlich ist, damit Ihr AD Forest nach einem Cyberangriff wieder einsatzbereit ist, nicht koordinieren können.

Zudem besteht die Gefahr einer erneuten Einschleppung von Malware, die möglicherweise viele Wochen oder Monate lang im Windows-Betriebssystem Ihrer AD-DCs gespeichert war, ohne entdeckt zu werden. Solche Malware würde wahrscheinlich in Ihren AD-Backup gespeichert, wenn das Tool eines Drittanbieters das standardmäßige System State Backup oder BMR-Backup Ihrer DCs durchführt, wie es bei dem integrierten WSB-Tool der Fall ist.

WEITERE RESSOURCEN

WHITEPAPERS

Assessing the ROI of a Quick Active Directory Recovery

Report: Recovering Active Directory from Cyber Disasters

WEBINAR

A Cyber-First Approach to Disaster Recovery

BLOGS

Now's the Time to Rethink Active Directory Security

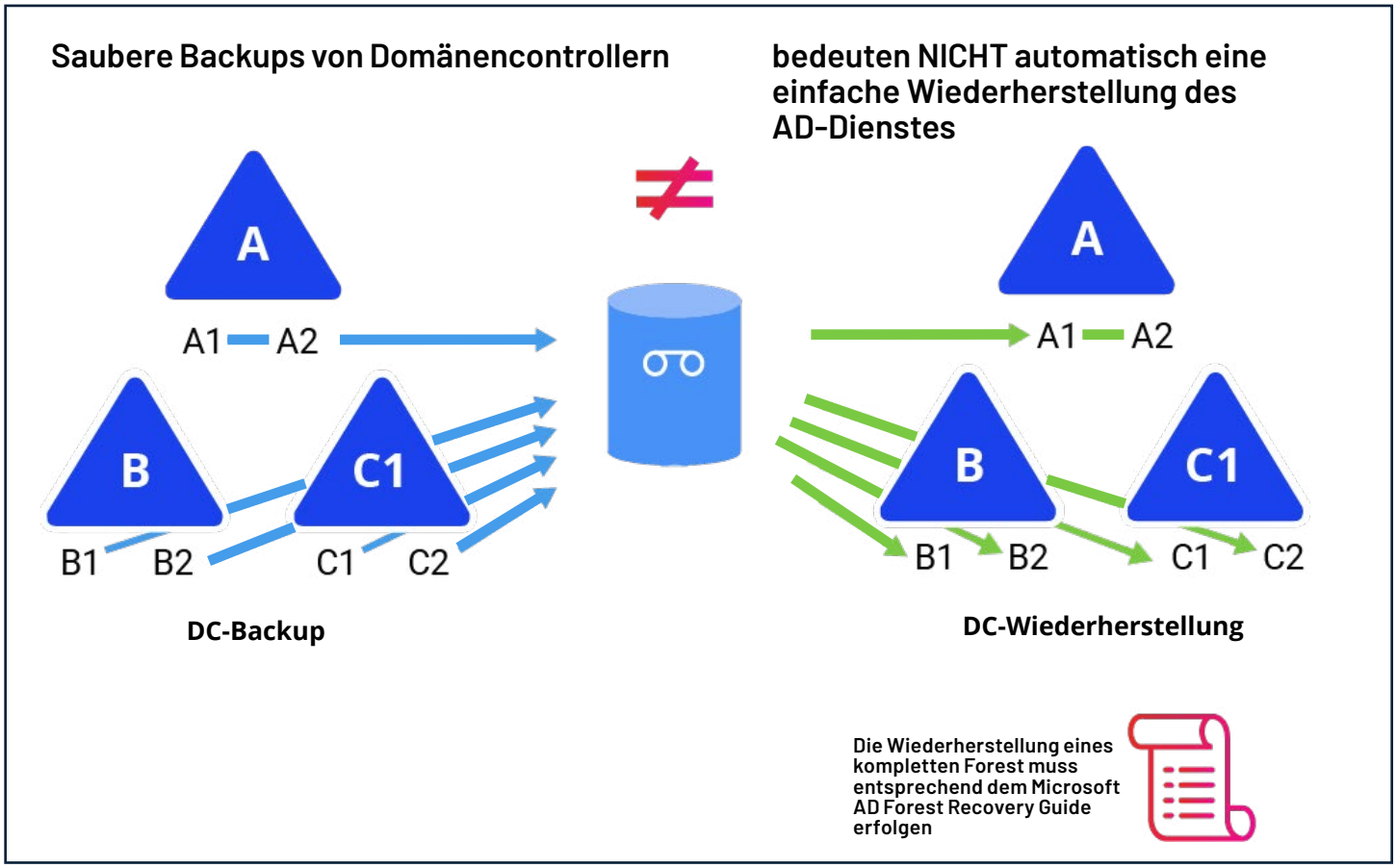
Time to Leave ADFS Behind for Authenticating in Hybrid Environments?

The Dos and Don'ts of Active Directory Recovery

Timeline of a Hafnium Attack

WIEDERHERSTELLUNG VON ACTIVE DIRECTORY

Bei der Wiederherstellung von Active Directory muss zwischen der Wiederherstellung von Daten (Benutzer, Gruppen, Computer, Gruppenrichtlinien usw.) und der Wiederherstellung des AD-Dienstes, d. h. der verteilten Anwendung, die auf mehreren Servern läuft, die die Arbeitslast der Active Directory-Domänendienste enthalten und in einer bestimmten Topologie konfiguriert sind, unterschieden werden. Die Tatsache, dass alle Domänencontroller im Forest die Konfiguration der AD-Topologie und das Datenbankschema innerhalb ihrer eigenen AD-Datenbank gemeinsam nutzen, macht diese Aufgabe nicht einfacher.



Nur weil Sie alle notwendigen AD-Domänencontroller gesichert haben, bedeutet das nicht, dass es jetzt ganz einfach ist, den kompletten AD-Dienst – den gesamten AD-Forest – wiederherzustellen, falls Sie dies im Falle einer echten Katastrophe tun müssen. Wenn Malware alle Ihre DCs auslöscht, müssen Sie Ihr AD wohl oder übel aus einer Minimalinstallation wiederherstellen.

Der Prozess zum Wiederherstellen von Active Directory-Forests kann mühsam sein

Wie bereits erwähnt, bestimmen in der zunehmend anfälligen Bedrohungslandschaft, der IT-Systeme ausgesetzt sind, Netzwerke, Anwendungen und Identitätssicherheit – und nicht etwa die Geografie – das Ausmaß einer Katastrophe. Die durch mehrere Rechenzentren geschaffene Fehlertoleranz ist nutzlos angesichts ausgeklügelter Malware, die sich innerhalb von Minuten über ein gesamtes Netzwerk verbreitet.

Die Folge: Das Schreckgespenst eines völlig zerstörten AD-Forest geistert nicht mehr nur durch die Albträume von AD-Administratoren, sondern ist eine sehr reale Gefahr.

Erst kürzlich wurden Microsoft-Kunden mit dem nächsten großen Angriff auf ein Produkt konfrontiert, das sehr eng mit ihrem On-Prem-AD integriert ist: Vier neue Zero-Day-Schwachstellen in Microsoft Exchange ermöglichten es der cyberkriminellen Gruppe „Hafnium" aus China, Schadcode in Exchange-Server von mehr als 30.000 Organisationen zu injizieren, bevor die Server ordnungsgemäß gepatcht werden konnten. Die Angreifer erhalten dadurch die vollständige Fernkontrolle über die betroffenen Systeme. Aufgrund der umfassenden Berechtigungen, die Microsoft Exchange in Active Directory hat, ist Letzteres ein einfach zu erreichendes nächstes Ziel. In der Regel wird zunächst AD infiltriert, um den Eindringlingen umfassendere Zugriffsberechtigungen zu verschaffen und sensible Daten aus dem angegriffenen Unternehmen zu erbeuten, die dann auf ein externes Ziel unter der Kontrolle der Eindringlinge kopiert werden. Im nächsten Schritt benötigen die Eindringlinge in der Regel einen Tag oder mehrere Wochen, um die Ransomware auf alle Systeme zu verteilen, die sie erreichen können. In der Zwischenzeit weiß das Zielunternehmen noch nicht, dass es gehackt wurde, und sichert die infizierten Systeme fröhlich bei seinen täglichen Sicherungsroutinen (laut FireEye bleibt ein Angreifer in einem kompromittierten Netzwerk durchschnittlich 72 Tage unentdeckt). Irgendwann aktivieren sie die Ransomware, die die betroffenen Systeme verschlüsselt, darunter alle AD-Mitgliedssysteme der Organisation sowie alle AD-Domänencontroller selbst. In einem letzten Schritt fordern die verantwortlichen Cyberkriminellen von der betroffenen Organisation ein hohes Lösegeld für das Versprechen (aber keine Garantie), dass sie einen Entschlüsselungsschlüssel enthält und dass die gestohlenen Daten nicht verkauft werden.

Warum nicht einfach von Backups wiederherstellen?

Warum also im Falle einer echten Katastrophe Ihres AD-Dienstes nicht einfach alle Ihre DCs aus Backups wiederherstellen? Wie bereits erwähnt, ist ein „sauberes Backup" der Dienste, auf denen die AD-DS-Rolle installiert ist – der Domänencontroller – nicht gleichbedeutend mit einer einfachen Möglichkeit zur Wiederherstellung des Active Directory-Dienstes. Es sind viele Schritte erforderlich, um Ihren AD-Dienst wieder in einen vertrauenswürdigen Zustand zu versetzen.

> ***Ein erfolgreicher Wiederherstellungsprozess erfordert die Koordination zwischen AD-Entwicklern, Wiederherstellungsoperations-Teams und höchstwahrscheinlich Virtualisierungsmanagement-Teams – und zwar an jedem Standort, an dem Sie Ihre DCs wiederherstellen möchten.***

Der AD-Wiederherstellungsprozess

Im Laufe der Zeit haben sich viele AD-Administratoren eingeredet, dass sie alles im Griff haben, aber wenn tatsächlich ein Problem auftritt, genügt es nicht, sich einfach an den online verfügbaren AD Forest Recovery Guide zu halten. Und nicht nur der Prozess erschwert die Forest-Wiederherstellung, sondern auch Herausforderungen im Hinblick auf Logistik und Know-how. Ein erfolgreicher Wiederherstellungsprozess erfordert die Koordination zwischen AD-Entwicklern, Wiederherstellungsoperations-Teams und höchstwahrscheinlich Virtualisierungsmanagement-Teams – und zwar an jedem Standort, an dem Sie Ihre DCs wiederherstellen möchten. Jeder muss seine Aufgaben fehlerfrei und in der richtigen Reihenfolge ausführen, und das in der wahrscheinlich stressigsten Situation seiner beruflichen Laufbahn.

Überblick über die Roadmap für die Wiederherstellung eines AD-Forest

Dies sind die Schritte, die erforderlich sind, um einen AD-Forest wieder in einen bekannterweise sicheren Zustand zu versetzen:

1. Forest-Struktur und verfügbare Backups ermitteln
2. Einen einzelnen DC für jede Domäne mit gültigem Backup identifizieren
3. Alle DCs im Forest abschalten
4. Zuerst Forest-Rootdomäne wiederherstellen
5. Dann einen DC jeder untergeordneten Domäne wiederherstellen
6. Aller anderen DCs im Forest bereinigen und erneut heraufstufen

- ↗ Die Wiederherstellung der Vertrauenshierarchie und kritischer DNS-Ressourceneinträge sicherstellen
- ↗ Die Wiederherstellung von übergeordneten Domänen vor ihren untergeordneten Domänen sicherstellen, um die Vertrauenshierarchie aufrechtzuerhalten

Die Notfallwiederherstellung von AD ist nicht einfach

Die AD-Notfallwiederherstellung ist keine einfache Aufgabe. Idealerweise bereiten Sie sich mit einer gründlichen Risikoanalyse für Ihr eigenes Umfeld vor: Ist die Schadensminderungsstrategie zu teuer oder das Restrisiko zu hoch?

Neben dem Team, das Active Directory verwaltet, müssen Sie auch andere Teams, wie z. B. Ihr Incident Response Team, in die Planung dieser Aufgabe einbeziehen. Legen Sie klare Kriterien für die Umsetzung des AD-DR-Plans und eindeutige Zuständigkeiten für dessen Ausführung fest. Verbinden Sie dies mit einer klaren Kommunikationsstrategie.

Überlegen Sie sich vor allem, ob Sie nicht mehr in die Katastrophenprävention investieren möchten. Das kann billiger sein als die Wiederherstellung nach einer Katastrophe.

ÜBER DIE AUTOREN

GUIDO GRILLENMEIER ist Chief Technologist bei Semperis. Grillenmeier lebt in Deutschland und war 12 Jahre lang MVP für Directory Services bei Microsoft. Er war über 20 Jahre bei HP/HPE als Chief Engineer tätig. Er ist ein häufiger Referent auf Technologiekonferenzen und Verfasser von Beiträgen in Fachzeitschriften und ist Mitverfasser von Microsoft Windows Security Fundamentals. Er hat unterschiedlichen Kunden geholfen, ihre Active Directory-Umgebungen zu sichern, und sie beim Übergang zu Windows 10/m365 und Azure-Cloud-Diensten unterstützt.

GIL KIRKPATRICK ist Chief Architekt für Produkte bei Semperis. Kirkpatrick entwickelt seit vielen Jahren kommerzielle Produkte für die Unternehmens-IT und konzentriert sich dabei vor allem auf Produkte im Zusammenhang mit Identitätsmanagement und Sicherheit. Er war 15-mal Microsoft MVP für Active Directory und Enterprise Mobility, ist Autor von „Active Directory Programming" und Gründer der Directory Experts Conference. Kirkpatrick spricht auf IT-Konferenzen auf der ganzen Welt über Themen wie Cybersicherheit, Identität und Notfallwiederherstellung.

+1-703-918-4884
info@semperis.com
www.semperis.com

221 River Street
9th Floor
Hoboken, NJ 07030

Für Sicherheitsteams, die mit der Verteidigung von Hybrid- und Multi-Cloud-Umgebungen betraut sind, stellt Semperis die Integrität und Verfügbarkeit von wichtigen Unternehmensverzeichnisdiensten bei jedem Schritt in der Cyberangriffskette sicher und verkürzt die Wiederherstellungszeit um 90 %. Die patentierte Technologie von Semperis wurde speziell für die Absicherung hybrider Active Directory-Umgebungen entwickelt und schützt mehr als 50 Millionen Identitäten vor Cyberangriffen, Datenpannen und Betriebsfehlern. Weltweit führende Unternehmen setzen auf Semperis, wenn es darum geht, Schwachstellen in Verzeichnissen aufzuspüren, laufende Cyberangriffe aufzuhalten und Daten bei Ransomware-Angriffen und anderen Datensicherheitsproblemen wiederherzustellen. Semperis hat seinen Hauptsitz in New Jersey und ist international tätig, wobei das Forschungs- und Entwicklungsteam auf San Francisco und Tel Aviv aufgeteilt ist.

Semperis veranstaltet die preisgekrönte Hybrid Identity Protection-Konferenz (www.hipconf.com). Das Unternehmen hat die höchsten Auszeichnungen der Branche erhalten, zuletzt Platz 157 im Inc. 5000 und als das am viertschnellsten wachsende Unternehmen in der Tri-State-Area, und nimmt Platz 35 in Deloittes 2020 Technology Fast 500™ ein. Semperis ist von Microsoft akkreditiert und von Gartner anerkannt.

semperis