



Il tuo piano per il ripristino di emergenza di Active Directory ti protegge dagli attacchi informatici?

DI GUIDO GRILLENMEIER E GIL KIRKPATRICK

- 02 RIPRISTINO DI ACTIVE DIRECTORY DALLE MINACCE ATTUALI**
- 04 PERCHÉ LA PROTEZIONE DI ACTIVE DIRECTORY È COSÌ IMPORTANTE**
- 06 COME È CAMBIATO LO SCENARIO DELLE MINACCE**
- 07 PERCHÉ ACTIVE DIRECTORY È VULNERABILE**
- 11 RIPRISTINO DI ACTIVE DIRECTORY**

RIPRISTINO DI ACTIVE DIRECTORY DALLE MINACCE ATTUALI

Sedici anni fa Gil Kirkpatrick (Chief Architect di Semperis) e Guido Grillenmeier (Chief Technologist di Semperis), all'epoca dipendenti di aziende diverse, si sono seduti a tavolino per condividere la propria esperienza e competenza sulla protezione e il ripristino di Active Directory (AD). Da questa collaborazione è nato il whitepaper "A Definitive Guide to Active Directory Disaster Recovery", pubblicato nel 2005. Il whitepaper rispondeva a un'esigenza fondamentale per il settore, considerato che la maggior parte delle aziende aveva di fatto accettato AD come il servizio di directory standard da utilizzare per controllare l'accesso alla rete e alle applicazioni aziendali, nonché ai servizi per i loro utenti.

In quel periodo le informazioni sul ripristino parziale o totale di AD scarseggiavano e non erano molti i professionisti di AD che comprendevano l'entità della sfida. Il whitepaper spiegava i meccanismi del ripristino di AD e chiariva quanto fosse necessario per le aziende prepararsi a effettuarlo correttamente a seguito di vari problemi, come l'eliminazione accidentale di oggetti AD, l'errata configurazione di Criteri di gruppo e gli errori dei controller di dominio AD. Il documento si concludeva con una breve descrizione del processo di ripristino di un ambiente AD dopo un crollo completo e con una precisazione: "Tuttavia, la probabilità di [dover eseguire] un ripristino completo della foresta AD è molto bassa".

Sebbene questo fosse vero all'epoca, la situazione attuale è ben diversa. Lo scenario della sicurezza informatica è cambiato drasticamente. Non passa settimana senza che la rete Windows on-premise di qualche organizzazione venga messa in ginocchio da un attacco ransomware o wiper. Ecco alcuni esempi del 2019 e dell'inizio del 2020 (con i costi di ripristino stimati):

- Città di New Orleans (più di 3 milioni di dollari)
- Città di Baltimora (18 milioni di dollari)
- Norsk Hydro (70 milioni di dollari)
- Demant (80 milioni di dollari)

E l'elenco continua con decine di altri casi. Il punto è che la possibilità di eseguire il ripristino completo dell'ambiente AD dal backup non è più la risposta ideale a un evento altamente improbabile: è diventata un requisito.

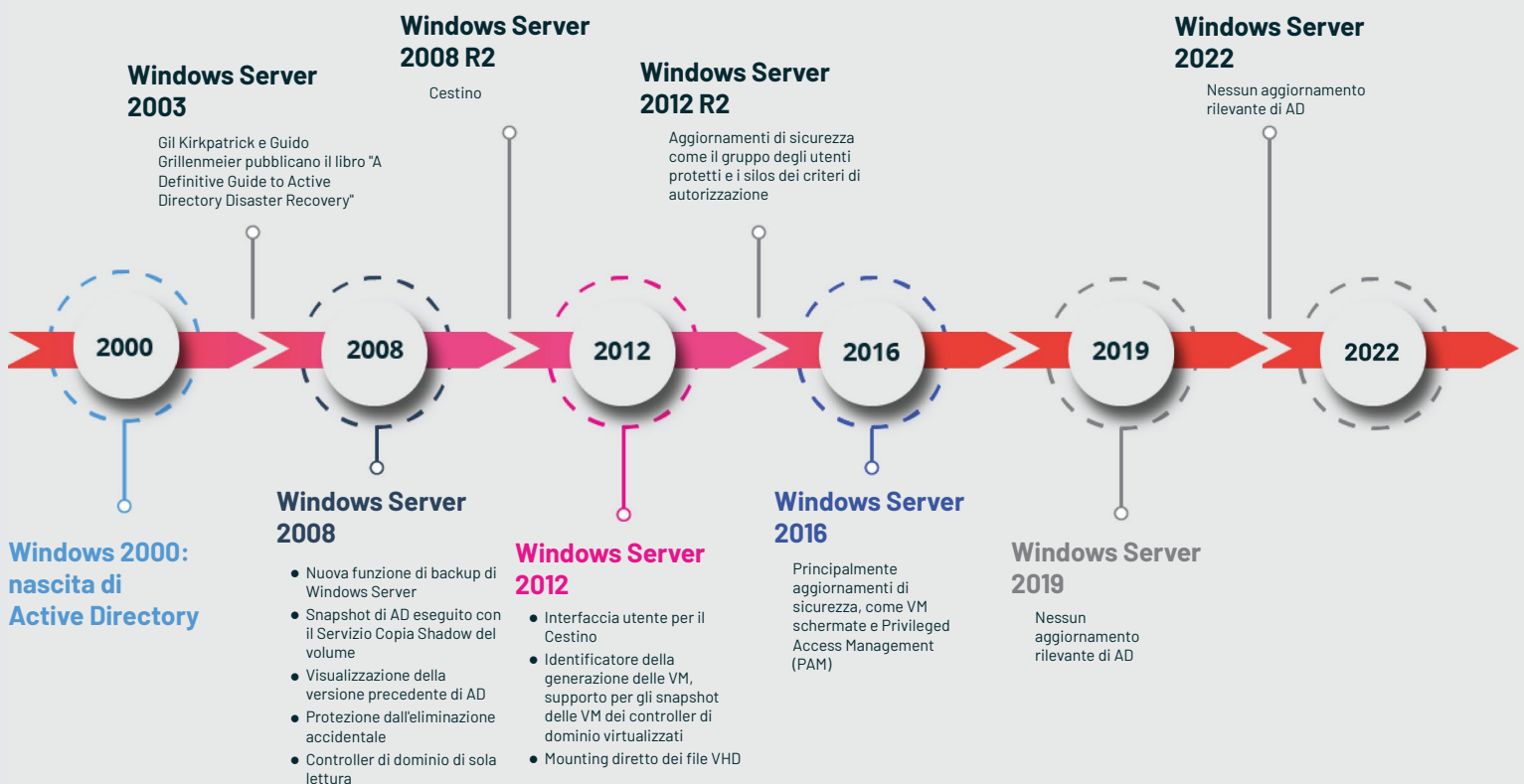
Ciò che è davvero cambiato dal 2005 non è solo il modello di minaccia, ma anche il sistema operativo (OS) Windows Server e il suo servizio Active Directory integrato. Microsoft ha migliorato la sicurezza di Windows in modo sostanziale, ha aggiunto funzionalità per semplificare il ripristino degli oggetti AD e ha migliorato il comportamento di AD quando il servizio viene eseguito in un ambiente virtualizzato. Tuttavia, i problemi fondamentali del ripristino di un'intera foresta Active Directory dal backup non sono cambiati. È ancora un processo complesso e soggetto a errori che richiede pianificazione ed esercizio per tutte le implementazioni di AD, tranne quelle più semplici.

È interessante il fatto che le due ultime versioni di Windows Server (Windows Server 2019 e 2022) sono le prime versioni di Windows Server senza aggiornamenti rilevanti per il servizio AD stesso. Secondo Microsoft, in AD non ci sono più problemi da risolvere e non sono più necessari miglioramenti al servizio. A dire il vero, il ripristino di emergenza di AD non diventerà più semplice.

Ora dobbiamo valutare le funzionalità di ripristino di un'azienda nel contesto delle nuove minacce informatiche che oggi prendono di mira AD e che nel 2005 non rappresentavano un motivo di preoccupazione. Purtroppo, a causa dell'aumento degli attacchi, le aziende hanno l'urgente necessità di prepararsi per eseguire il ripristino rapido del loro servizio AD societario. I miglioramenti che Microsoft ha apportato nel corso degli anni ai componenti essenziali di AD potrebbero rivelarsi comunque di scarso aiuto per ripristinare il servizio in caso di attacco. La tua azienda è pronta a effettuare il ripristino rapido del servizio AD se si verifica un evento disastroso che ne causa il crollo completo?

"Le aziende hanno l'urgente necessità di prepararsi per eseguire il ripristino rapido del loro servizio AD societario."

Modifiche correlate al backup di Active Directory nel corso del tempo



La tua azienda è pronta a effettuare il ripristino rapido del servizio AD se si verifica un evento disastroso che ne causa il crollo completo?

PERCHÉ LA PROTEZIONE DI ACTIVE DIRECTORY È COSÌ IMPORTANTE

Active Directory (AD) è in produzione da oltre 20 anni. In base alla progettazione originale, questo ruolo server Microsoft offre le seguenti funzioni:

Autenticazione: autentica gli utenti on-premise che accedono ai loro PC e alla rete aziendale, e gli utenti da remoto che accedono alle applicazioni ospitate internamente o ai desktop virtuali.

Autorizzazione: controlla quali risorse integrate in AD, come servizi di file, stampa, Exchange Server, SharePoint Server e SQL Server, dispongono di autorizzazioni di accesso.

Sicurezza e controllo: la funzione Criteri di gruppo può applicare configurazioni di criteri a ogni computer, server e utente che viene aggiunto ad AD.

Directory: una singola posizione per l'individuazione di utenti e risorse.

DNS: DNS integrato in AD per la risoluzione dei nomi di rete.

PKI: Servizi certificati Active Directory fornisce certificati per utenti e computer del dominio.

La crescente popolarità del sistema operativo Windows Server per servizi di base di condivisione di file e stampa e altri servizi di back office come e-mail, messaggistica e collaborazione ha contribuito a consolidare AD quale directory di rete preferita. Microsoft ha modificato praticamente tutte le sue applicazioni più diffuse in modo che utilizzassero AD, che pertanto è diventato uno dei servizi software più onnipresenti nelle aziende di oggi. Oltre il 90% delle organizzazioni mondiali con più di 500 dipendenti utilizza AD.

L'ascesa del cloud computing non ha influito su questa ampia adozione; al contrario, ha aumentato l'importanza di AD per le aziende. Sono due i fattori che determinano il ruolo chiave di AD nel cloud.

Innanzitutto, il modello di cloud computing non dipende da reti attendibili come avviene invece per l'elaborazione tradizionale on-premise perché, a differenza delle reti aziendali tradizionali, il traffico tra client e le risorse a cui accedono avviene con maggiore frequenza sulla rete Internet pubblica. Questo traffico non è protetto dalla POSIZIONE dell'utente, ma dalla sua IDENTITÀ. Come afferma Microsoft, "l'identità è il piano di controllo" dell'accesso alle risorse cloud. L'identità di un utente è al centro della sicurezza cloud.



In secondo luogo, AD è alla base dell'architettura di identità ibrida comunemente utilizzata oggi, in cui le organizzazioni sincronizzano il loro archivio di identità on-premise, solitamente AD, con il servizio di identità cloud scelto, come Azure Active Directory, Okta o Amazon Web Services (AWS). Questo approccio consente agli utenti di utilizzare la loro identità aziendale per accedere alle risorse (ad esempio, Office 365 o Salesforce) che sono integrate nel servizio di identità cloud dell'organizzazione.

Inoltre, numerose aziende non si fidano dei servizi cloud nella stessa misura in cui si fidano dei loro sistemi controllati in-house, che sono completamente gestiti dal personale IT interno. Pertanto in molte hanno deciso di configurare un framework di autenticazione federata utilizzando AD Federation Services (ADFS) o soluzioni simili per connettersi con le soluzioni cloud, ad esempio, Azure AD. In questo caso, la convalida dell'identità degli utenti, cioè l'autenticazione, continua ad avvenire utilizzando il servizio AD on-premise. ADFS crea quindi un token appropriato, il token SAML, per confermare al servizio cloud (ad esempio, Azure AD e le applicazioni associate) che l'utente connesso è davvero chi dice di essere. Poiché il token SAML è correttamente crittografato con una chiave condivisa solo tra ADFS e Azure AD, Azure AD considera questo token del tutto attendibile e concede all'utente l'accesso alle rispettive risorse cloud. Di fatto Azure AD considera completamente attendibile il servizio AD on-premise in questa configurazione.

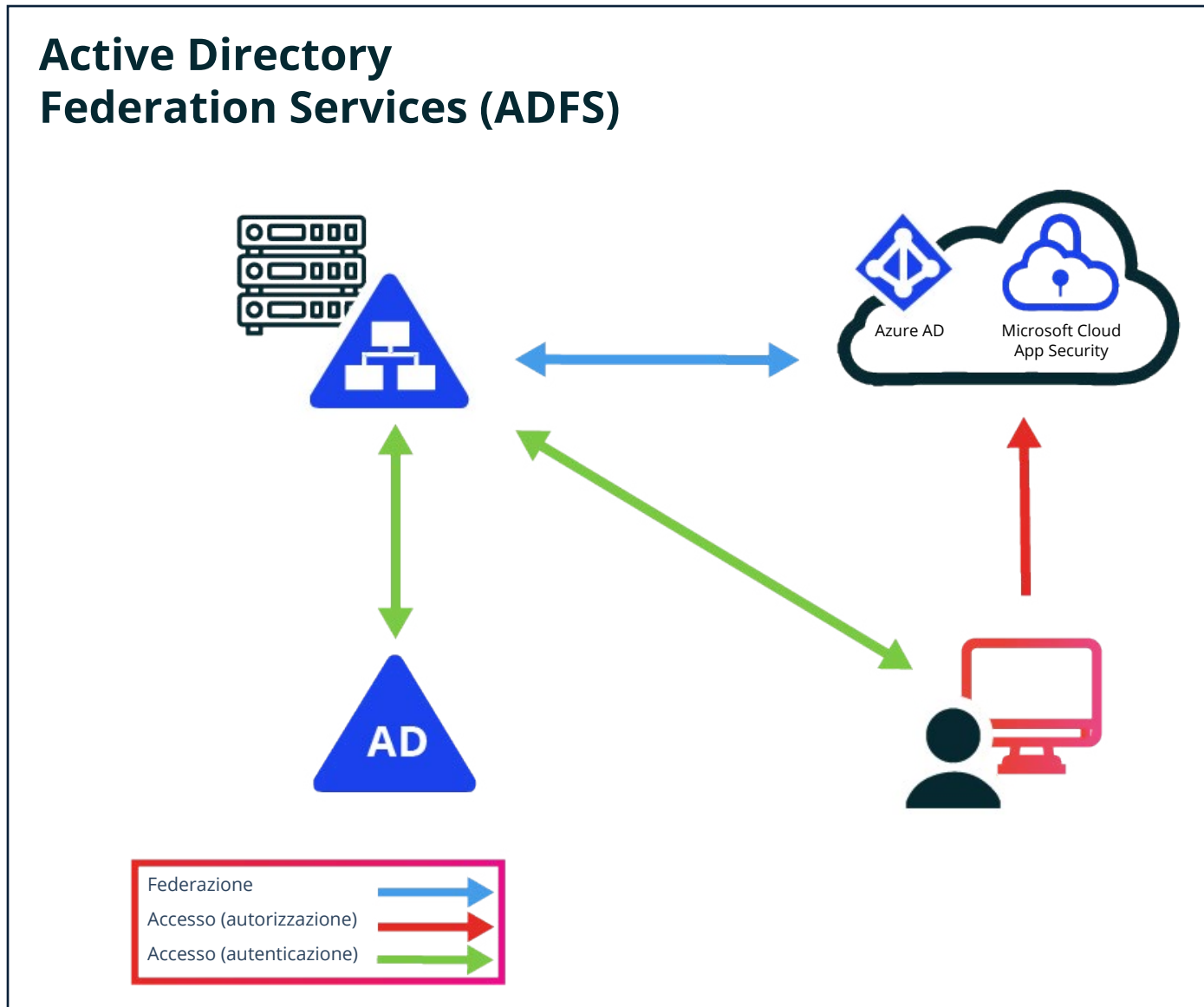


Figura 1: La federazione si basa di solito sul servizio AD on-premise per certificare l'identità degli utenti

A questo si aggiunge il fatto che, nonostante il clamore suscitato dal cloud computing e la vasta adozione di questa tecnologia, tutte le organizzazioni di qualsiasi dimensione, nuove o consolidate che siano, gestiscono on-premise operazioni continue e sostanziali che dipendono da AD. Di conseguenza, AD oggi non solo rimane essenziale per accedere alle risorse on-premise, ma è anche una componente cruciale dell'impresa ibrida di oggi e di tutte le sue applicazioni.

COME È CAMBIATO LO SCENARIO DELLE MINACCE

All'epoca della redazione del documento originale "A Definitive Guide to Active Directory Disaster Recovery", le principali situazioni di emergenza di cui gli amministratori AD dovevano occuparsi rientravano in due categorie: emergenze fisiche (ad esempio un'interruzione di corrente, un arresto anomalo del disco o un'inondazione) ed errori amministrativi (involontari o dolosi) che causavano modifiche o eliminazioni indesiderate degli oggetti AD. Vi era poi una terza categoria in cui rientrava una situazione di emergenza interessante sul piano teorico, ma che non si era quasi mai verificata nella vita reale: un errore dei servizi esteso all'intera foresta. Per quanto gli effetti di un tale errore fossero disastrosi, la probabilità che si verificasse era talmente insignificante da indurre la maggior parte delle organizzazioni a non intraprendere alcuna azione al riguardo e a convivere con il rischio residuo.

Nel 2021 quel calcolo del rischio è stato completamente ribaltato. AD continua a gestire al meglio i problemi dei server fisici e dei siti e, dopo 10-20 anni di esperienza, la maggior parte delle organizzazioni è in grado di amministrare in modo affidabile e sicuro la propria Active Directory. Tuttavia, i criminali informatici, armati di sofisticati strumenti di phishing e del più recente malware di ricognizione, persistenza e crittografia dei dati, possono annientare un intero ambiente Windows aziendale in pochi minuti. Le recenti statistiche sul ransomware sono sconcertanti.

Nel 2020:



Il 51% delle aziende è stato colpito da un attacco ransomware. ([Pentest Magazine](#))



Il ransomware costa alle organizzazioni circa 75 miliardi di dollari all'anno ([Datto](#))



La richiesta media di riscatto è stata di 178.000 dollari e il pagamento più elevato di cui si ha notizia è stato di 11,8 milioni di dollari

La perdita dell'intero servizio Active Directory è passato dal gradino più basso della scala dei rischi a quello più alto.

Active Directory è un obiettivo primario per i criminali informatici

Active Directory è progettato accuratamente per gestire le emergenze fisiche. Se si verifica un guasto in un controller di dominio, o se un intero data center non è più online, AD continuerà a funzionare utilizzando gli altri controller di dominio. Microsoft ha aggiunto la funzione Cestino di AD in Windows Server 2008 R2, che supporta abbastanza bene il ripristino di oggetti eliminati inavvertitamente, ma per quanto riguarda l'annullamento delle modifiche involontarie apportate agli oggetti AD, il servizio non è di grande aiuto.

È chiaro che AD è un servizio fondamentale in quasi tutte le organizzazioni. Memorizza le credenziali di utenti, computer e servizi, e controlla l'autenticazione e l'autorizzazione nell'ambiente on-premise; pertanto, per gli autori delle minacce è un bersaglio ambito per tre motivi:

- Come servizio di directory, AD è un punto di riferimento unico per le informazioni di cui gli autori di minacce hanno bisogno per effettuare spostamenti laterali nella rete e aumentare il livello dei loro privilegi.
- Come servizio primario di autenticazione e autorizzazione, AD rappresenta un singolo punto di attacco che di fatto può rendere il resto della rete inutilizzabile.
- Come soluzione pressoché standard per la gestione della configurazione degli endpoint tramite Criteri di gruppo, AD è un ulteriore strumento utilizzabile dagli utenti malintenzionati per distribuire malware e ottenere la persistenza in più computer della rete.

Sebbene le specifiche tecniche in genere non sono mai riportate nelle notizie sugli attacchi informatici, Active Directory inizia a essere citato molto più spesso:

- [Il servizio Active Directory di Virgin Mobile è stato compromesso](#) e i dati aziendali sono stati venduti sul dark web.
- [NTT Communication ha ammesso che il proprio servizio Active Directory è stato compromesso](#) nell'ambito di una violazione dei dati.
- [È stato dimostrato che il ransomware Ryuk modifica Criteri di gruppo](#) per propagarsi agli endpoint tramite uno script di accesso.

A dire il vero, abbiamo sempre avuto degli elementi che facevano pensare a un probabile ruolo di Active Directory in un attacco: ora abbiamo i dati che lo confermano.

PERCHÉ ACTIVE DIRECTORY È VULNERABILE

Active Directory funziona abbastanza bene e la sua base tecnica ha resistito alla prova del tempo. Tuttavia, il mondo è cambiato con l'emergere di versioni di crittografia di AD, la sua apertura alle query, Kerberos, e la crescente complessità degli attacchi che utilizzano strumenti come Mimikatz.

Minacce avanzate persistenti (APT): infiltrazione e violazione

Gli attacchi ad AD sono aumentati notevolmente negli ultimi anni perché i criminali informatici si sono resi conto che, tramite AD, possono avere il controllo delle risorse IT dell'organizzazione. Che AD sia la porta di accesso principale agli asset di un'azienda è un'ovvietà, ma anche tenendo presente questo concetto si sottovaluta un rischio: il servizio contiene infatti indicazioni precise sulla posizione di tutte le risorse integrate al suo interno e che dipendono dal servizio stesso. Per quanto gli utenti finali non siano consapevoli della loro dipendenza da AD, i vari strumenti e processi aziendali che utilizzano quotidianamente non potrebbero funzionare in caso di interruzione del servizio. Questi includono applicazioni per servizi cruciali come l'e-mail (Exchange), la condivisione di file (SharePoint, normali condivisioni di file), la collaborazione (Skype) o persino la possibilità di stampare. Numerose aziende utilizzano inoltre l'autenticazione integrata di Windows per molte delle loro applicazioni aziendali e dei loro database, dove l'espressione "integrata di Windows" è semplicemente un modo diverso per indicare l'integrazione AD. In altre parole, le applicazioni non fanno affidamento sulla propria lista di utenti, ma considerano attendibile il token di accesso di un utente che viene generato da AD per concedere l'accesso appropriato all'applicazione. AD non solo controlla l'accesso a queste applicazioni da parte di utenti legittimi, ma consente anche agli intrusi di capire quali applicazioni sono state integrate in un'infrastruttura e quindi di usarle in modo malevolo.

Man mano che è cresciuta la consapevolezza di quanto AD sia un obiettivo prezioso, sono aumentati anche i set di strumenti per attaccarlo. PowerSploit, Bloodhound, Death Star, Cobalt Strike e, soprattutto, Mimikatz hanno consentito agli aggressori di trovare rapidamente le credenziali, eseguire una ricognizione orizzontale della rete, trovare il percorso più breve per ottenere i diritti di amministrazione del dominio e prendere di mira quel percorso.

Questi strumenti riducono il tempo necessario per prendere il controllo di un dominio da diversi giorni a poche ore. Pertanto, sferrare un attacco ad Active Directory e centrare il bersaglio è più facile che mai.

L'emergenza informatica: gli attacchi DoA

AD ha una tolleranza eccezionale verso i disastri naturali o fisici. Uragani, tornado, terremoti, interruzioni di corrente e altri eventi che mettono fuori uso un data center avranno un impatto su un servizio AD ben progettato solo a livello locale, mentre il resto

della rete potrà continuare a utilizzarlo. Quando si esegue il ripristino della sezione danneggiata di AD, qualsiasi modifica avvenuta nella rete durante l'interruzione sarà applicata automaticamente alla sezione ripristinata. Un evento imprevisto che dovesse rendere inutilizzabile un intero dominio o foresta AD avrebbe un impatto molto elevato, ma sarebbe anche molto raro grazie alle precauzioni adottate dalle aziende nel distribuire geograficamente le loro infrastrutture AD. Quindi, il rischio che AD sia completamente indisponibile è sempre stato classificato al massimo come moderato. Se a questo si aggiunge il fatto che la continuità operativa e il ripristino di emergenza (BCDR) di Active Directory hanno un costo molto elevato (come vedremo più avanti), si comprende perché la pianificazione BCDR abbia storicamente trascurato il ripristino della foresta.

Gli attacchi Denial-of-Availability (DoA). Le varianti più note di questa tipologia di attacchi sono il ransomware e il wiperware. Quasi tutti sanno cos'è il ransomware. Non passa giorno senza che vengano diffuse notizie di client, server e dati aziendali crittografati da criminali informatici per fini di estorsione, con le vittime che devono pagare un riscatto in bitcoin in cambio della chiave di decrittografia. Il wiperware distrugge i computer e i dati, sia attraverso la crittografia che la cancellazione dei dati, senza possibilità di ripristino.

L'attacco del 2017 a NotPetya è a oggi l'esempio più noto di questo tipo di attacco. La [compagnia di trasporto marittimo di container Maersk è stata una delle principali vittime](#). NotPetya ha reso inutilizzabili migliaia di computer, server e tutti i controller di dominio AD di Maersk a livello globale, compresi i backup aziendali. Per fortuna un'interruzione dell'alimentazione elettrica ha impedito al malware di diffondersi al controller di dominio della sede aziendale in Ghana, che è stato utilizzato per ripristinare il servizio AD. Dopo aver effettuato un ripristino molto oneroso, che si stima sia costato a Maersk tra i 250 e i 300 milioni di dollari, l'azienda ha deciso di parlare pubblicamente della propria situazione per sensibilizzare le altre aziende sui rischi degli attacchi malware alla loro infrastruttura. Le aziende devono prepararsi a far fronte a questa minaccia, perché la maggior parte di esse non sopravviverebbe a un'interruzione di nove giorni dell'infrastruttura IT centrale, che è stato il tempo impiegato da Maersk per effettuare il ripristino completo di Active Directory.

Altre vittime gravemente colpite dall'attacco NotPetya sono state FedEx, Saint-Gobain, Reckitt Benckiser e Mondelēz. Inoltre, l'attacco NotPetya non è stato affatto l'ultimo ai danni di AD. Ha segnato in realtà l'inizio di una nuova era di attacchi ransomware a rapida diffusione che utilizzano e compromettono Active Directory. Purtroppo, i vettori di attacco ad AD sono numerosi; di recente, un attacco di Nefilim è andato a segno utilizzando un [account di amministratore di dominio con privilegi elevati di un dipendente deceduto](#) per aprire tutte le porte agli intrusi.

I backup di Active Directory non sono utili per ripristinare il servizio AD

In caso di una situazione di emergenza informatica, i normali backup di Active Directory non consentono di ripristinare le operazioni aziendali dopo l'attacco. Con la funzione di protezione degli oggetti dall'eliminazione accidentale si può evitare l'errore umano, ma non le attività malevole eseguite in AD.

Stesso discorso vale per il Cestino, che permette di ripristinare gli oggetti eliminati, ma non è di alcuna utilità per annullare le modifiche a livello di attributo, né quelle agli oggetti Criteri di gruppo o alla configurazione di AD. Inoltre, non consente di ripristinare l'intero dominio o l'intera foresta e le relative partizioni delle applicazioni.

L'utilizzo degli snapshot può supportare il rilevamento delle modifiche a livello di attributo e contribuire ad annullarle, ma rende molto più complesso il processo di ripristino.

In ogni caso, nessuno di questi metodi per il ripristino dei dati di Active Directory è sufficiente per ripristinare il servizio AD effettivo, a livello di intero dominio o di intera foresta. Anche se tutti ci auguriamo di non doverne mai avere bisogno, potrebbe essere necessario un ripristino di AD a livello di foresta, in caso di compromissione dello schema dovuta a una modifica malevola eseguita da un intruso o di crittografia di tutti i controller di dominio da parte di un malware. Per questo, serve ancora un adeguato backup dei controller di dominio di AD.

Preparazione di un backup che consenta di eseguire il ripristino del servizio Active Directory senza malware

Il ripristino del servizio Active Directory, che comporta il ripristino di NTDS.dit e dei relativi file e impostazioni del sistema operativo per consentire la corretta replica dei dati di AD, è un'attività molto più impegnativa del semplice ripristino di oggetti AD specifici. Se tutte le modifiche a tutti gli oggetti e attributi fossero mantenute su un singolo server di database AD, cioè su un singolo controller di dominio, ripristinare il server sarebbe un'operazione semplice, simile a quella di un file server.

Tuttavia, le elevate potenzialità e il grande successo di Active Directory si basano sul fatto che, a differenza dei suoi predecessori, le modifiche effettuate nella directory non devono necessariamente verificarsi su un singolo server o un singolo master. Al contrario, AD è stato progettato come un'architettura di database multi-master, che consente di implementare modifiche su qualsiasi controller di dominio scrivibile nella rete di un'azienda. È questo che ha reso possibile la scalabilità e la diffusione geografica del servizio Active Directory e che permette a un dominio o a una foresta AD di servire molti siti distribuiti in tutto il mondo.

Alcuni punti specifici sul backup globale dei controller di dominio sono trattati in modo più dettagliato nella "Definitive Guide" completa, ma una riflessione sulla distribuzione geografica dei controller di dominio AD e sui relativi backup ha la stessa importanza del backup stesso. In qualsiasi momento durante la pianificazione del backup AD, è opportuno considerare se i backup dei controller di dominio scelti sono sufficienti per ripristinare rapidamente la foresta AD. Questa operazione è davvero complessa in una foresta multi-dominio, cioè una foresta con più domini figli o alberi paralleli che fanno parte della stessa struttura della foresta AD. Non appena sono presenti più domini nella foresta AD, si rende necessaria una funzionalità AD, il Catalogo globale, che dovrà essere ricostruito e riattivato durante un processo di ripristino della foresta, prima della ripresa dei servizi di autenticazione. Inoltre, la ricostruzione del Catalogo globale richiederà molto più tempo se almeno un controller di dominio di ogni dominio della foresta non si trova nello stesso sito AD. Più avanti esamineremo altri aspetti problematici legati al ripristino rapido della foresta.

Integrazione con il Servizio Copia Shadow del volume

Va da sé che lo strumento di backup utilizzato per eseguire il backup dei controller di dominio Active Directory dovrebbe integrarsi con la funzione Servizio Copia Shadow del volume del sistema operativo Windows Server. Questa integrazione assicura uno stato coerente del database AD al momento dell'esecuzione di un backup; in altre parole, tutte le operazioni di scrittura in

corso vengono portate a termine e scritte su disco, mentre le nuove modifiche in ingresso nel database AD vengono fermate nel momento in cui si esegue uno snapshot del database AD. Questo processo richiede solo pochi secondi, dopo di che lo strumento di backup ha tutto il tempo necessario per copiare lo stato coerente del database AD sulla destinazione scelta, mentre le operazioni di scrittura sul database AD originale possono continuare a garantire la normale esecuzione dei controller di dominio AD.

Windows Server Backup (WSB) integrato è un buon esempio di strumento di backup che è completamente integrato con il Servizio Copia Shadow del volume e permette di eseguire due tipi di backup:

1. Backup dello stato del sistema
2. Ripristino bare metal

Le due opzioni sono piuttosto differenti in termini di casi d'uso, quindi è importante fare attenzione alle diverse funzioni quando pianifichi la tua strategia di backup.

I backup dello stato del sistema potrebbero contenere malware

L'opzione di backup dello stato del sistema esegue il backup di tutti i componenti critici del sistema operativo del server di un controller di dominio, tra cui il database AD (NTDS.dit), la cartella SYSVOL, il database di registrazione delle classi COM+, il registro del server e i file di avvio, ma esclude dati utente, dischi extra e dati che potrebbero essere stati aggiunti per altre applicazioni in esecuzione sullo stesso server. Mentre il backup utilizza le funzionalità Servizio Copia Shadow del volume per creare uno snapshot corretto dei dischi utilizzati dal server, il trasferimento del backup effettivo dello stato del sistema è una copia basata su file dei file pertinenti eseguita sulla destinazione del backup, che non consente l'esecuzione di alcun backup incrementale. Quindi, è necessario trasferire sempre lo stato del sistema completo nella posizione di backup di destinazione. Oltre al database AD, un backup dello stato del sistema memorizza circa 11 GB di file del sistema operativo Windows in ogni backup del controller di dominio.

Il ripristino del backup dello stato del sistema è pensato per essere eseguito sulla stessa istanza di Windows Server e sulla stessa installazione del sistema operativo da cui è stato creato. Ciò significa che è destinato a essere utilizzato qualora si verifichi un problema a livello di sistema operativo o di dati, ma non nel caso di un problema hardware che richieda la ricostruzione del server completo. Pertanto, un backup dello stato del sistema può essere utilizzato per il ripristino del database AD nei casi in cui è necessario eseguire il ripristino autorevole di parti di un database AD per ripristinare oggetti eliminati per errore da AD. Tuttavia, un backup dello stato del sistema non è pensato per eseguire il ripristino del backup su un server appena implementato, e di certo non su un server con hardware diverso, o perfino un passaggio dell'architettura da fisica a virtuale o viceversa. Sicuramente un backup dello stato del sistema potrebbe essere l'unica opzione disponibile se, dopo un attacco informatico, hai la necessità di ripristinare rapidamente i controller di dominio AD su altri hardware o macchine virtuali che potrebbero essere resi disponibili più rapidamente. In ogni caso, ricorda che il backup dello stato del sistema include vari file del sistema operativo di cui è stato eseguito il backup, il che significa che la probabilità di una reinfezione dal malware sottoposto a backup con AD è elevata.

"Ricorda che il backup dello stato del sistema include vari file del sistema operativo di cui è stato eseguito il backup, il che significa che la probabilità di una reinfezione dal malware sottoposto a backup con AD è elevata."

"Analogamente ai backup dello stato del sistema, è necessaria una certa cautela quando si esegue il ripristino di AD dai backup Ripristino bare metal dopo un attacco informatico per evitare di reintrodurre il malware."

Anche i backup Ripristino bare metal potrebbero contenere malware

I backup creati con l'opzione Bare metal recovery, definiti anche backup completo del server, permettono di ripristinare un dato server al suo stato di backup, compreso il ripristino completo del sistema operativo e dei servizi in esecuzione su di esso, nonché Active Directory. L'obiettivo è quello di fornire protezione dai classici guasti a livello di hardware, come la rottura dei dischi; tuttavia, i backup Ripristino bare metal potrebbero anche reintrodurre il malware, se usati per ripristinare AD.

L'opzione Bare metal recovery esegue il backup di tutti i dischi utilizzati dal sistema operativo, incluso lo stato del sistema. Puoi inoltre scegliere di eseguire il backup di dischi aggiuntivi sul rispettivo server. Poiché un backup Bare metal recovery viene creato con il metodo di backup basato sui blocchi, hai anche la possibilità di configurare il backup dei soli blocchi che sono stati modificati rispetto all'ultimo backup, cioè di eseguire un backup incrementale, che accelera ulteriormente l'esecuzione dell'operazione. I backup incrementali sono efficaci se hai configurato l'opzione appropriata nelle impostazioni delle prestazioni di backup sul server e se il disco di destinazione del backup è ospitato sullo stesso server sottoposto a backup. Quest'ultimo approccio potrebbe apparire controintuitivo, ma funzionerà se disponi di meccanismi aggiuntivi per archiviare successivamente i file di backup creati su un'altra destinazione di archiviazione sicura.

Al momento del ripristino, il server riparato deve essere avviato con un disco di installazione corretto del sistema operativo Windows Server, prima di poterlo ripristinare dal rispettivo file di backup. Tieni presente che questa installazione del server deve avere anche lo stesso tipo di hardware e di architettura. Per esempio, l'opzione Bare metal recovery non consente di ripristinare un backup di un server Dell su uno nuovo di HPE o di scegliere una macchina virtuale come destinazione del ripristino. A causa di questa limitazione, e poiché è disponibile un'opzione semplice per configurare una nuova replica di un controller di dominio AD innalzandone il livello dopo un'installazione pulita del sistema operativo su un qualsiasi dispositivo hardware scelto, il metodo Bare metal recovery è utilizzato raramente per il backup dei controller di dominio Active Directory. Così come accade con un backup dello stato del sistema, i backup Bare metal recovery sono soggetti allo stesso rischio di includere il malware che potrebbe aver colpito i controller di dominio AD prima di attivarsi e di danneggiare la foresta AD. Analogamente ai backup dello stato del sistema, è necessaria una certa cautela quando si esegue il ripristino di AD dai backup Ripristino bare metal dopo un attacco informatico per evitare di reintrodurre il malware.

Tieni inoltre presente che né i backup dello stato del sistema né quelli Bare metal recovery vengono crittografati dalla funzione di backup di Windows Server; pertanto, se non hai crittografato il disco contenente i backup, questi sono vulnerabili durante il transito e, sicuramente, quando sono inattivi. Ciò significa anche che è sconsigliabile copiare i file di backup su un altro sistema di archiviazione di destinazione accessibile agli amministratori non di dominio senza averli prima crittografati in modo adeguato.

Archivia i file di backup in modo sicuro, in modo che solo gli amministratori del servizio AD possano accedervi.

Gli snapshot richiedono cautela

Gli snapshot sono pericolosi! Gli snapshot ti salvano!

Entrambe le affermazioni sono in qualche modo vere. Fino al rilascio di Windows Server 2012, che ha aggiunto un opportuno identificatore della versione di una macchina virtuale quando si usano gli snapshot a livello di macchina virtuale (VMGenID), Microsoft ha dovuto continuamente mettere in guardia rispetto alla mancanza di supporto della creazione di snapshot dei controller di dominio in ambienti virtuali. Gli amministratori potrebbero commettere troppo facilmente l'errore di implementare "in modo retroattivo" un controller di dominio senza usare il metodo di ripristino di AD appropriato per informare del rollback gli altri controller di dominio presenti nell'ambiente. Questo passo falso potrebbe causare ogni genere di problema di replica poiché interrompe la logica di replica integrata del complesso ecosistema AD. Si verificherebbe il rollback del numero di sequenza dell'aggiornamento (USN) e causerebbe anche uno stato inaffidabile degli oggetti della foresta AD, con il rischio di creare SID duplicati e oggetti persistenti.

Supponendo che in tutti i controller di dominio a livello globale sia installato almeno Windows Server 2012 e che si utilizzi un hypervisor in grado di supportare la logica VMGenID (tutti i principali hypervisor lo fanno ormai da anni), possiamo risparmiarci una spiegazione dettagliata dei motivi per cui il ripristino dei controller di dominio a una versione precedente tramite uno snapshot delle macchine virtuali fosse davvero una pessima idea. Sebbene la creazione di snapshot delle macchine virtuali sia ancora ben lontana dall'essere un meccanismo di backup per la foresta AD, questa tecnologia ti consente quanto meno di non danneggiare ulteriormente AD.

Nel whitepaper di prossima pubblicazione dal titolo "The New Definitive Guide to Active Directory Disaster Recovery" prenderemo in esame i cambiamenti cruciali introdotti da Microsoft con Windows Server 2008 che hanno avuto un impatto sul backup e sul ripristino nativo di AD: l'integrazione del database AD con le funzionalità Servizio Copia Shadow del volume del sistema operativo. Tratteremo anche la funzione rinnovata di Windows Server Backup (WSB), anch'essa introdotta con Windows Server 2008, che ha reso i dati di backup accessibili come file VHD. Inoltre, forniremo una descrizione dettagliata della pratica funzione che Microsoft ha aggiunto con la versione 2012: la possibilità di eseguire il mounting dei file VHD direttamente in un client Windows esistente, consentendo la ricerca veloce di una versione precedente del database AD.

Grazie a tutte queste modifiche, gli amministratori possono svolgere più facilmente attività come, ad esempio, il ripristino di file da una versione precedente della cartella SYSVOL o l'utilizzo di una versione di sola lettura dei dati AD per eseguire il ripristino degli attributi sovrascritti di qualsiasi oggetto. L'aspetto essenziale, dal punto di vista della risoluzione delle lacune di sicurezza di Active Directory, è proteggere adeguatamente i file di backup, poiché chiunque abbia accesso a quei file sensibili può fare qualsiasi cosa, perfino usare altri strumenti di editing offline per raccogliere gli hash delle password e altri dati sensibili dal backup AD. Archivia i file di backup in modo sicuro, in modo che solo gli amministratori del servizio AD possano accedervi.

Attenzione alle limitazioni degli strumenti di terze parti

Essenzialmente, ogni strumento che, in base a quanto dichiarato, esegue il backup di AD, sarà integrato anche con le funzionalità Servizio Copia Shadow del sistema operativo o potrebbe persino sfruttare la funzione Windows Server Backup (WSB) e semplicemente includere più intelligenza per eseguire il backup centralizzato dei controller di dominio scelti.

Tuttavia, come per lo strumento WSB integrato, essere in grado di eseguire il backup dei controller di dominio AD non significa automaticamente che uno strumento può aiutarti a ripristinare rapidamente la foresta AD nel caso in cui lo schema sia danneggiato o tutti i controller di dominio siano stati infettati da malware o colpiti da altri attacchi informatici. È importante sapere che la maggior parte delle soluzioni di backup che si concentrano sui backup a livello di sistema operativo potrebbe funzionare bene per il ripristino dei singoli server, inclusi i controller di dominio; tuttavia, come vedremo nella prossima sezione, non sono in grado di coordinare il complesso processo di ripristino che è necessario per rendere nuovamente operativa la foresta AD dopo un attacco informatico.

Inoltre, c'è un'altra considerazione sconcertante: il rischio di reintrodurre il malware che potrebbe essere stato archiviato nel sistema operativo Windows dei controller di dominio AD per molte settimane o mesi senza essere stato rilevato. Questo malware verrebbe probabilmente archiviato nei backup AD se lo strumento di terze parti esegue il backup dello stato del sistema standard o Bare metal recovery dei controller di dominio, come nel caso dello strumento integrato WSB.



ALTRE RISORSE

WHITEPAPER

[Assessing the ROI of a Quick Active Directory Recovery](#)

[Report: Recovering Active Directory from Cyber Disasters](#)

WEBINAR

[A Cyber-First Approach to Disaster Recovery](#)

BLOG

[Now's the Time to Rethink Active Directory Security](#)

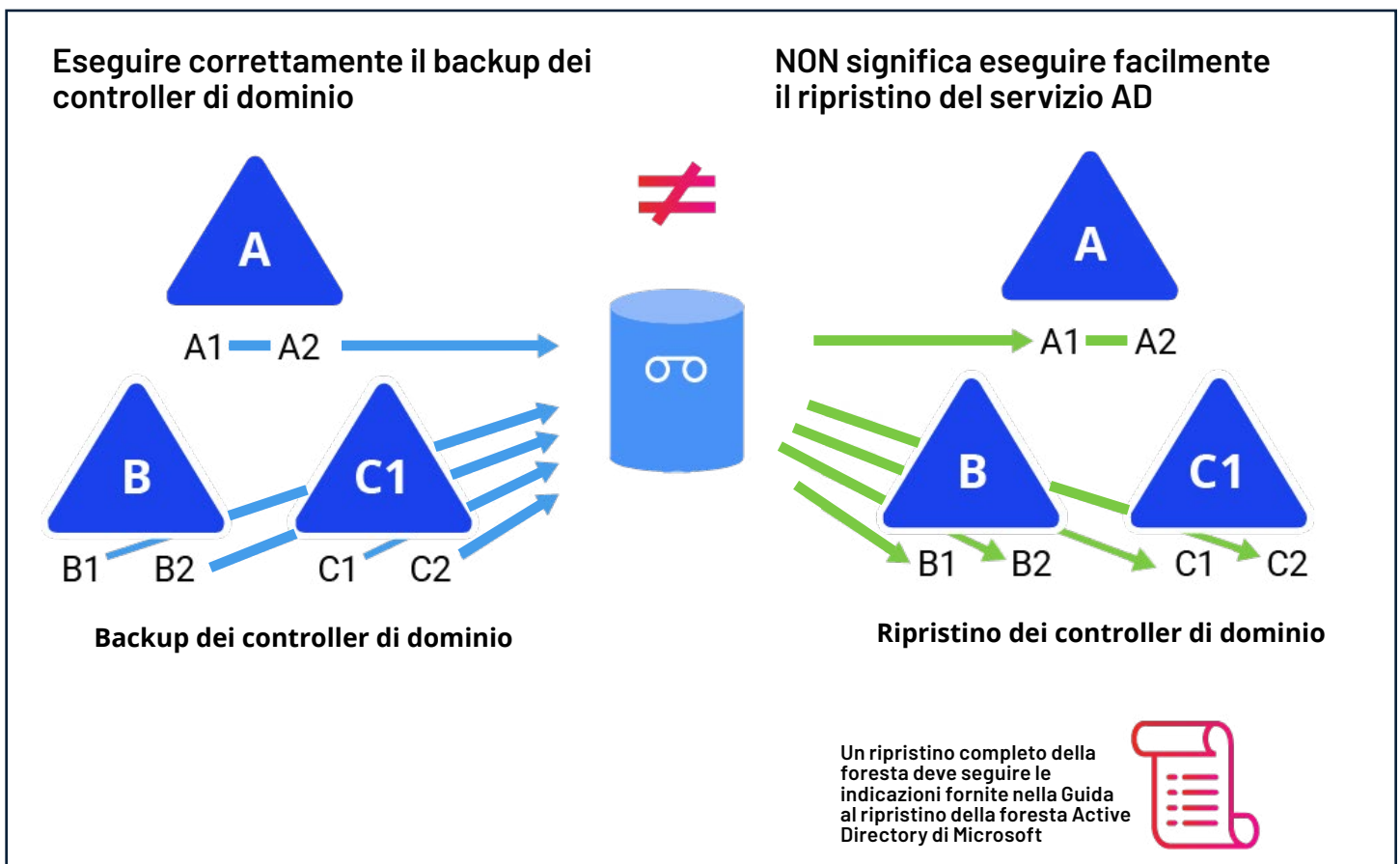
[Time to Leave ADFS Behind for Authenticating in Hybrid Environments?](#)

[The Dos and Don'ts of Active Directory Recovery](#)

[Timeline of a Hafnium Attack](#)

RIPRISTINO DI ACTIVE DIRECTORY

Quando si parla di ripristino di Active Directory, è importante distinguere tra ripristino dei dati (utenti, gruppi, computer, Criteri di gruppo e così via) e ripristino del servizio AD, l'applicazione distribuita in esecuzione su più server designati che contengono il carico di lavoro dei servizi di dominio Active Directory, configurati in una topologia specifica. Il fatto che tutti i controller di dominio della foresta condividano la configurazione della topologia AD, e lo schema del database all'interno del proprio database AD, non rende il compito più semplice.



Il semplice fatto di aver eseguito il backup di tutti i controller di dominio AD necessari non significa disporre di un "modo semplice" per ripristinare il servizio AD completo, cioè l'intera foresta AD, se necessario qualora si verificasse una vera emergenza informatica. Quando il malware ha reso inutilizzabili tutti i tuoi controller di dominio, dovrai seguire il gravoso processo di ripristino AD da un'installazione minima.

Il processo di ripristino della foresta Active Directory può essere gravoso

Come abbiamo visto, nel contesto delle minacce sempre più sofisticate che prendono di mira i sistemi IT, la portata di una situazione di emergenza è determinata dalle reti, dalle applicazioni e dalla sicurezza delle identità, non dalla geografia. La tolleranza agli errori stabilita dalla presenza di più data center diventa inutile a fronte di malware sofisticati che si diffondono in una rete nel giro di pochi minuti.

Di conseguenza, lo spettro della distruzione totale della foresta AD non è più il peggior incubo degli amministratori AD, ma è una possibilità molto concreta.

Solo di recente i clienti Microsoft hanno affrontato un nuovo grave attacco a un prodotto strettamente integrato con AD on-premise: [quattro nuove vulnerabilità zero-day di Microsoft Exchange](#) hanno consentito al gruppo di criminali informatici cinesi noto come "Hafnium" di iniettare codice dannoso nei server Exchange di [oltre 30.000 organizzazioni](#), prima che i server potessero essere sottoposti alle patch appropriate. L'attacco offre agli intrusi il controllo totale, da remoto, dei sistemi colpiti. A causa delle autorizzazioni pervasive di Microsoft Exchange in Active Directory, quest'ultimo è diventato l'ennesimo facile obiettivo. La fase iniziale prevede di solito un'infiltrazione di AD per elevare ulteriormente i privilegi degli intrusi, allo scopo di raccogliere dall'organizzazione colpita dati sensibili che vengono copiati in un obiettivo esterno, controllato dagli intrusi. In una fase successiva, gli intrusi in genere impiegano un giorno o alcune settimane per diffondere e distribuire il ransomware al maggior numero possibile di sistemi. Nel frattempo, l'organizzazione presa di mira non si rende ancora conto di aver subito una violazione e continua, ignara, a condurre le routine di backup quotidiane, includendo in tal modo anche il backup dei sistemi infettati ([secondo FireEye, un aggressore rimane in media circa 72 giorni in una rete compromessa senza essere rilevato](#)). Alla fine, attivano il ransomware che esegue la crittografia dei sistemi colpiti, inclusi tutti i sistemi membri dell'organizzazione in AD, nonché tutti i controller di dominio AD stessi. Infine, i criminali informatici responsabili della violazione richiedono un enorme riscatto all'organizzazione colpita in cambio della promessa (ma non della garanzia) di fornire una chiave di decrittografia e di non vendere i dati rubati.

Perché non limitarsi a eseguire il ripristino dai backup?

La domanda è legittima: nel caso di un'autentica situazione di emergenza del servizio AD, perché non ripristinare semplicemente tutti i controller di dominio dai backup? Come detto prima, eseguire correttamente il backup di quei servizi con il ruolo Servizi di dominio Active Directory, cioè con i controller di dominio, non significa eseguire facilmente il ripristino del servizio Active Directory. Il ripristino del servizio AD a uno stato attendibile richiede numerosi passaggi.

Eseguire con successo il processo di ripristino richiede il coordinamento tra gli ingegneri AD, i team delle operazioni di ripristino e, verosimilmente, i team di gestione della virtualizzazione, in ogni posizione in cui si intende ripristinare i controller di dominio.

Il processo di ripristino di AD

Nel corso del tempo, molti amministratori AD si sono convinti di avere tutto sotto controllo, ma, al momento dell'emergenza, non ci si può limitare a "seguire il documento" nella [Guida al ripristino della foresta Active Directory](#) online. Inoltre, il ripristino della foresta è reso difficile non solo da processo in sé, ma anche da problematiche logistiche e di formazione. Eseguire con successo il processo di ripristino richiede infatti il coordinamento di ingegneri AD, team delle operazioni di ripristino e, verosimilmente, team di gestione della virtualizzazione, in ogni posizione in cui si intende ripristinare i controller di dominio. Ognuno deve eseguire i propri compiti in modo impeccabile, nell'ordine giusto, in quello che probabilmente sarà l'ambiente a più alto tasso di stress della loro vita professionale.

Roadmap generale per il ripristino della foresta AD

Ecco un rapido schema della procedura di ripristino di una foresta AD a uno stato noto e sicuro:

1. Determinare la struttura della foresta e i backup disponibili
 2. Identificare un singolo controller di dominio per ogni dominio con backup valido
 3. Arrestare tutti i controller di dominio della foresta
 4. Eseguire prima il ripristino del dominio radice della foresta
 5. Quindi, eseguire il ripristino di un controller di dominio di ciascun dominio figlio
 6. Pulire e innalzare nuovamente il livello di tutti gli altri controller di dominio della foresta
- Garantire il ripristino della gerarchia di attendibilità e dei record critici delle risorse DNS
 - Garantire il ripristino dei domini padre prima dei relativi domini figlio per mantenere la gerarchia di attendibilità

Il ripristino di emergenza di AD non è semplice

Eseguire il ripristino di emergenza di AD non è un compito semplice. Idealmente, ci si prepara con un'analisi approfondita dei rischi per il proprio ambiente: la strategia di attenuazione è troppo costosa o il rischio residuo troppo elevato?

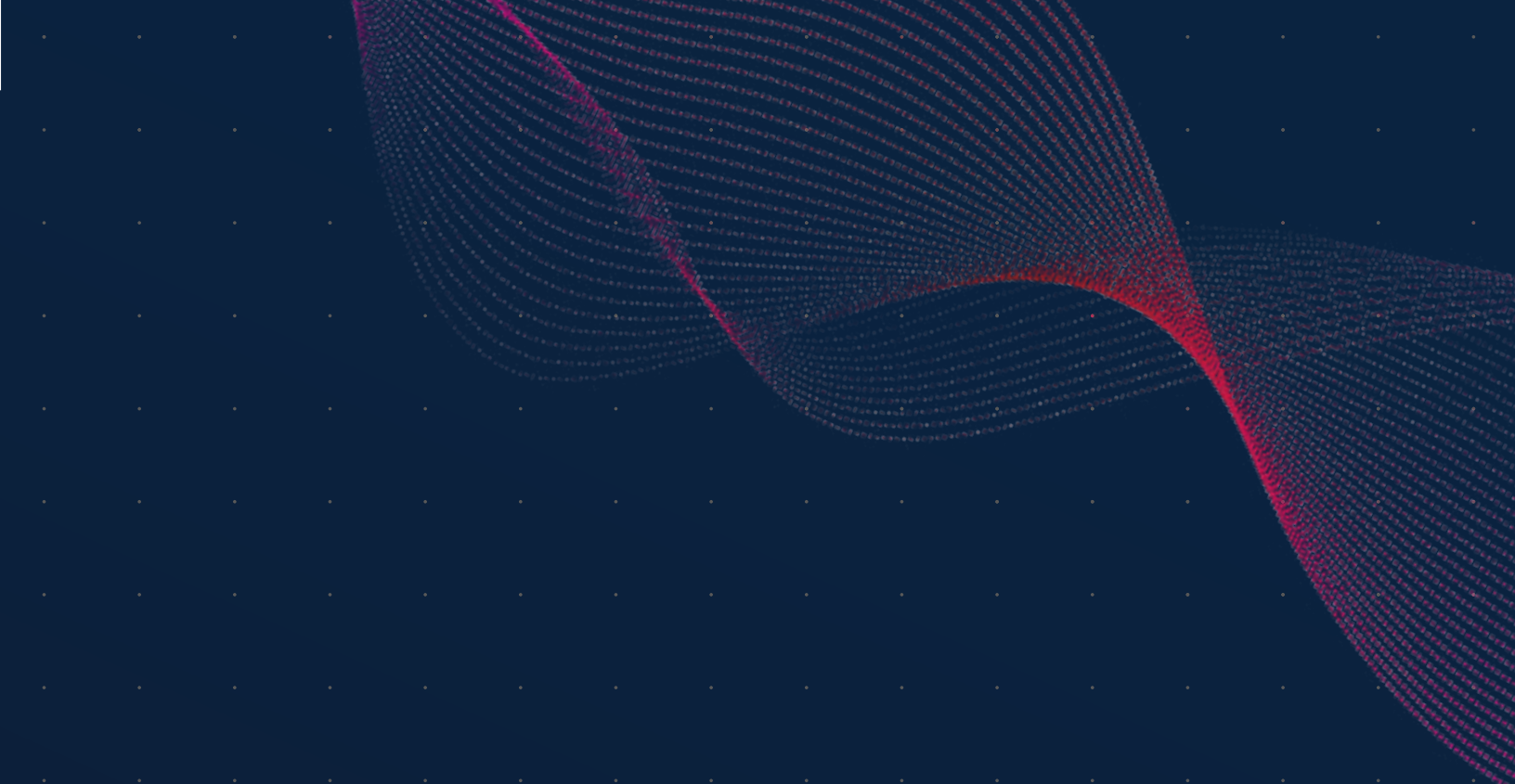
Oltre al team che gestisce Active Directory, è necessario coinvolgere altri team, come il team di risposta a eventi imprevisti, nella pianificazione per affrontare questo compito. Per chiamare in causa il piano di ripristino di emergenza di AD è importante aver definito criteri chiari e responsabilità chiare per la sua esecuzione. A questo bisogna aggiungere una strategia di comunicazione chiara

e, soprattutto, occorre considerare attentamente gli investimenti per la prevenzione delle situazioni critiche, che possono essere più convenienti rispetto al ripristino di emergenza.

INFORMAZIONI SUGLI AUTORI

GUIDO GRILLENMEIER è il Chief Technologist di Semperis. Risiede in Germania e ha lavorato per 12 anni in qualità di MVP Microsoft per i servizi di directory. Ha trascorso più di 20 anni presso HP/HPE come Chief Engineer. Partecipa spesso in veste di relatore alle conferenze tecnologiche e collabora con riviste tecniche, oltre a essere il co-autore di Microsoft Windows Security Fundamentals. Ha aiutato diversi clienti a proteggere i loro ambienti Active Directory e ne ha supportato la transizione a Windows 10/M365 e ai servizi cloud Azure.

GIL KIRKPATRICK è il Chief Architect per i prodotti di Semperis. Crea prodotti commerciali per l'IT aziendale da molti anni, con una particolare attenzione alla gestione delle identità e ai prodotti legati alla sicurezza. È stato nominato per 15 volte Microsoft MVP per Active Directory ed Enterprise Mobility, ed è l'autore di Active Directory Programming nonché il fondatore della Directory Experts Conference. Gil interviene come relatore sui temi della sicurezza informatica, dell'identità e del ripristino di emergenza alle conferenze IT di tutto il mondo.



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

221 River Street
9th Floor
Hoboken, NJ 07030

Per i team incaricati della protezione degli ambienti ibridi e multcloud, Semperis garantisce l'integrità e la disponibilità dei servizi directory aziendali cruciali in ogni fase della cyber kill chain, con tempi di ripristino ridotti del 90%. Studiata appositamente per difendere gli ambienti ibridi di Active Directory, la tecnologia brevettata di Semperis protegge oltre 50 milioni di identità da attacchi informatici, violazioni di dati ed errori operativi. Le più importanti organizzazioni a livello mondiale si affidano a Semperis per rilevare le vulnerabilità nelle directory, intercettare gli attacchi informatici in corso e ripristinare in tempi rapidi l'ambiente in caso di ransomware e altre minacce all'integrità dei dati. Semperis ha sede in New Jersey ma lavora a livello internazionale: il suo team di ricerca e sviluppo è distribuito tra San Francisco e Tel Aviv.

Semperis organizza la pluripremiata conferenza Hybrid Identity Protection (www.hipconf.com). Ha ricevuto i più importanti riconoscimenti del settore e di recente si è posizionata al 157° posto nella classifica Inc. 5000 e al quarto posto tra le aziende in maggior crescita nell'area Tri-State, nonché al 35° nella classifica Technology Fast 500™ 2020 di Deloitte. Semperis è accreditata da Microsoft e riconosciuta da Gartner.