semperis

Sicurezza di Active Directory

Report di Metà Anno

2021

IL PUNTO DI VISTA DEL CEO:
MICKEY BRESMAN

i protocolli fondamentali di sicurezza dell'identità hanno bisogno di prestare molta attenzione per frenare i cyberattacchi

Dopo un semestre di escalation di cyberattacchi in ogni settore di attività e in tutto il mondo, il CEO Mickey Bresman riflette sulle tendenze della sicurezza informatica che definiranno la battaglia a breve termine contro gli attacchi dannosi che minacciano i fatturati aziendali, la sicurezza pubblica e la sicurezza nazionale.

Perché le aziende faticano ancora a implementare i protocolli di sicurezza fondamentali per Active Directory?

In primo luogo, Active Directory esiste da 20 anni e, all'inizio, la sicurezza non era necessariamente in cima ai pensieri dei team che configuravano AD. Uniamo a questo il fatto che oggi AD è molto più complicato: ogni ambiente ha molti livelli diversi di autorizzazioni e complessità.

AD rimane il cuore pulsante della gestione delle identità, il nucleo della piattaforma di identità per la maggior parte delle aziende, ma tutto ciò che lo circonda è cambiato rapidamente. L'igiene di base di AD non era così importante 15 anni fa, quindi molti degli errori che sono stati compiuti allora sono i problemi che dobbiamo affrontare oggi. Vorrei inoltre sottolineare la mancanza di competenze: ci sono persone che conoscono molto bene AD, ma il loro modo di pensare è più operativo. Oppure ci sono persone che conoscono molto bene il Red Teaming (un attacco senza esclusione di colpi usato per simulare un avversario reale capace di sfruttare e testare tutte le falle presenti nel sistema informativo di un'azienda) e la sicurezza, ma non sono esperti di AD. Trovare questa combinazione di competenze in una sola persona non è così semplice.

Cosa possono fare le aziende in termini di costruzione di competenze o di struttura organizzativa per abbattere i compartimenti stagni tra i team IT e di sicurezza?

L'identità dovrà sicuramente entrare a far parte della più ampia storia della sicurezza informatica in azienda. Chiunque si occupi di identità dovrà pensare per prima cosa alla cybersicurezza. Dato che sappiamo che molte aziende dipendono da Active Directory per poter proseguire le attività operative dopo un attacco informatico, come ci si assicura che, nel peggiore dei casi, si sia in grado di ripristinare la funzionalità il più velocemente possibile? Stiamo vedendo che le aziende iniziano a trasferire la responsabilità dell'identità al lato sicurezza dell'impresa. E anche nelle aziende in cui l'identità è ancora sul lato operativo, oggi vediamo una maggiore consapevolezza della sicurezza a livello di professionisti IT e una maggiore collaborazione tra il team responsabile della sicurezza e quello IT, soprattutto nella gestione delle identità e di Active Directory.

A mio parere, si tratta di una tendenza incoraggiante: chi è responsabile di qualsiasi funzione nell'ambito dell'identità deve mettere la sicurezza al centro.

Quali problematiche inerenti alla sicurezza sono intrinseche alla gestione di un ambiente a identità ibrida?

Con la gestione di ambienti a identità ibrida vediamo molte problematiche diverse, a partire dal fatto fondamentale che Active Directory e Azure Active Directory, a parte il nome, hanno ben poche cose in comune. Azure Active Directory è un diverso stack di protocolli, che richiede un approccio gestionale molto diverso, compresa la protezione del sistema di identità dai cyberattacchi. Per esempio, quando apporto modifiche alle identità nel cloud, questo influisce sulla mia postura di sicurezza generale nel data center, ossia nell'ambiente on-premise? Con uno scenario ibrido, la potenziale superficie d'attacco a disposizione degli avversari si espande. È uno scenario relativamente comune vedere gli attacchi iniziare on-premise e passare al cloud, o passare dal cloud all'on-premise. Le aziende hanno ora bisogno di pensare a quali modifiche vengono apportate ai sistemi di identità in ogni ambiente, e come la connettività tra i due elementi possa creare un punto di ingresso per gli avversari.

La gestione della sicurezza in un ambiente ibrido porta inoltre in primo piano il modello di responsabilità condivisa: la responsabilità di Microsoft è di assicurarsi che il servizio continui a funzionare. Cosa fate con l'ambiente, incluso come lo proteggete, è una vostra responsabilità.

Per quanto tempo l'ambiente ibrido sarà in gioco per la maggior parte delle aziende?

La maggior parte dei nostri clienti non abbandonerà mai completamente i data center. Potenzialmente, il modello ibrido è destinato a restare per sempre. Le aziende prenderanno in considerazione ciò che ha senso continuare ad eseguire nel data center e ciò che ha senso usare come servizio fornito da Microsoft, AWS, Google o un altro fornitore. Le aziende possono ora mescolare e abbinare la soluzione migliore per i loro scenari e requisiti. Il cloud non è la risposta a tutto.

Ma indipendentemente dal particolare mix di sistemi e risorse on-premise e sul cloud, è necessario proteggere lo store di identità. L'identità continuerà a giocare un ruolo enorme nel gioco di protezione che stiamo giocando contro gli avversari. Dovreste inoltre ipotizzare che, continuando il processo di digitalizzazione e di adozione del cloud, la protezione dell'identità diventerà ancora più essenziale per la vostra strategia operativa e di sicurezza.

UNLEASH PURPLE KNIGHT

Purple Knight consente ai team IT e di security di scoprire le lacune relative alla sicurezza di Active Directory

Con migliaia di download fino ad oggi, lo strumento gratuito di valutazione della sicurezza di Active Directory aiuta le aziende a identificare e affrontare le lacune relative alla sicurezza che gli avversari spesso sfruttano nei cyberattacchi

Il rilascio dello strumento di valutazione della sicurezza Purple Knight, avvenuto nel marzo 2021, ha risposto a un'esigenza insoddisfatta: identificare e affrontare le lacune relative alla sicurezza in Active Directory. Migliaia di professionisti IT e della sicurezza hanno scaricato questo strumento gratuito, costruito dagli esperti di identità di Semperis, che analizza l'ambiente Active Directory in base a più di 60 indicatori di esposizione (IOE) e indicatori di compromissione (IOC).

"Nessuno di noi si aspettava questo livello di accettazione di Purple Knight sul mercato", spiega Mickey Bresman, CEO di Semperis. "Ma è una bella sorpresa, perché le aziende sono ora in grado di fare un collegamento diretto tra gli attacchi che vedono sul campo e i punti deboli della sicurezza in Active Directory. Le aziende richiedono Purple Knight per assicurarsi che i loro ambienti AD siano preparati per questi tipi di attacchi".

Secondo Bresman, il feedback dei clienti indica che Purple Knight scopre vulnerabilità che persino le società di consulenza non colgono, un vantaggio che egli attribuisce alla profonda comprensione del team Semperis di Active Directory e di come le aziende lo utilizzano.

"Abbiamo visto che molte aziende non comprendono a fondo le esposizioni di Active Directory che gli avversari sono in grado di utilizzare contro di loro", spiega Bresman. "Volevamo fornire ai team di sicurezza che non hanno una profonda esperienza di Active Directory un modo per capire la loro postura di sicurezza AD, e poi colmare qualsiasi lacuna esistente in modo che gli avversari non la possano usare contro di loro".

Purple Knight esamina l'ambiente AD per identificare le lacune relative alla sicurezza dovute ad attività malevole o a configurazioni errate che potrebbero essersi annidate nel sistema per anni. Secondo Ran Harel, Senior Security Product Manager presso Semperis, molte delle configurazioni errate che riscontra nelle implementazioni di Active Directory sono il risultato di una mancata comprensione del modello di sicurezza generale o della decisione di implementare soluzioni rapide che causano vulnerabilità di sicurezza lungo il percorso.

"Questi sono gli scenari di cui gli aggressori amano approfittare, specialmente le configurazioni difettose con Kerberos e le group policy, spiega Harel.

Alcune delle vulnerabilità più comuni scoperte da Purple Knight includono:

- Password che non vengono cambiate frequentemente, lasciando l'azienda esposta ad attacchi di forza bruta
- Account con privilegi elevati che non sono stati adeguatamente rivisti - per esempio, il gruppo Enterprise Key Admins
- Account Exchange con autorizzazioni AD elevate che hanno proliferato nel tempo
- Delega Kerberos impostata come "non vincolata", uno scenario facilmente soggetto ad abusi o a esposizioni involontarie a utenti inappropriati
- Configurazione debole delle group policy, che crea vulnerabilità di sicurezza quando i GPO sono collegati ad Active Directory a livello di dominio

"We wanted to give security teams that don't have deep AD expertise a way to understand their AD security posture—and then close any existing gaps so that adversaries won't use those against them."

Mickey Bresman, *Semperis* CEO

Purple Knight fornisce dati sulla sicurezza generale di Active Directory nonché singoli punteggi nelle categorie di delega AD, sicurezza degli account, sicurezza dell'infrastruttura AD, sicurezza delle group policy e sicurezza Kerberos. Nei rapporti iniziali di Purple Knight, le aziende hanno riportato punteggi medi del 61%, un voto appena sufficiente. La sicurezza Kerberos è stata la categoria con il punteggio più basso.

Punteggi medi basati sulle valutazioni iniziali

PUNTEGGIO COMPLESSIVO	61%
Delega Active Directory	**68%**
Sicurezza account	**59%**
Sicurezza infrastruttura Active Directory	**77%**
Sicurezza criteri di gruppo	**58%**
Sicurezza Kerberos	**43%**

I criminali informatici considerano le autorizzazioni di amministrazione dei domini lassiste come frutta pronta per essere colta, dichiara Darren Mar-Elia, Vice President of Products presso Semperis. "Agli aggressori piace fare così perché rende il loro lavoro più facile", spiega Mar-Elia. "Un aggressore troverà il percorso più breve per arrivare all'account admin del dominio. Questo perché, una volta che arriva a tale account, il gioco è fatto."

"Proteggersi continuamente dalle vulnerabilità della sicurezza AD richiede una buona igiene dell'account", spiega Ran Harel, principale Security Product Manager presso Semperis.

"Ma farlo è notoriamente difficile", aggiunge Harel. "Un utente può appartenere a 20 gruppi diversi, che possono avere sottogruppi con diritti di delega. È come un pacco di spaghetti: è necessario smistare le autorizzazioni degli account su base regolare In caso contrario, la gestione degli account inizia a sfuggire dai buchi (del pacco) e il problema peggiora".

I risultati dei rapporti Purple Knight evidenziano l'ironia del fatto che le aziende più grandi, spesso con più risorse, sono particolarmente soggette al rischio di rimanere indietro nella protezione dei loro sistemi di identità di importanza critica a causa delle dimensioni e della complessità dei loro ambienti, lasciandoli a rischio di un attacco simile a quello subito da SolarWinds.

ACTIVE DIRECTORY IS THE ACHILLES' HEEL OF ENTERPRISE SECURITY

Il CEO di Semperis esorta i responsabili della sicurezza a difendere Active Directory

Active Directory potrebbe sembrare uno dei tanti servizi da ripristinare in seguito a un attacco informatico, ma in realtà è un pilastro fondamentale. Se viene compromesso, identica sorte tocca a tutto il vostro ambiente.

Quasi la metà (il 47%) delle aziende usa Active Directory come archivio di identità principale. Il 51% ne fa un uso più o meno importante insieme ad altri archivi di identità, ma solo l'1% non lo usa affatto o lo sta eliminando progressivamente.

Molte aziende stanno adottando un approccio Ibrido all'identita' e iniziano a focalizzarsi sulle interdipendenze del cloud e sulle complessità che ne derivano, ignorando però un dato di fatto: la totalità delle loro identità cloud continua a essere sincronizzata on-premise con Active Directory. AD viene usata come fonte per sincronizzare gli altri archivi di identità, cosi' una sua compromissione può innescare un effetto a cascata in quanto AD è collegato ad altre applicazioni cloud. I potenziali problemi di questo collegamento tra risorse basate su cloud e on-premise iniziano a emergere con chiarezza ora che, con la pandemia, le aziende si trovano a dover supportare il telelavoro dei dipendenti tramite dispositivi mobili, con tutte le difficoltà che ne derivano.

Nel suo articolo "Rethinking Active Directory Security" su Help Net Security, il CEO di Semperis Mickey Bresman spiega quanto è importante per un'azienda disporre di un piano d'azione collaudato per il ripristino di Active Directory (AD) in caso di attacco informatico. Scoprite i suoi suggerimenti per rinforzare le difese aziendali contro gli attacchi mirati ad AD, come ad esempio l'introduzione di un monitoraggio specifico per questo sistema.

ESPERTI DI ACTIVE DIRECTORY, FUTURI PROFESSIONISTI DELLA SICUREZZA

Di **GIL KIRKPATRICK**

Negli ultimi 20 anni il mondo dei professionisti di Microsoft Active Directory (AD) ha subito grandi cambiamenti, sia per l'aumento delle applicazioni cloud sia per l'evoluzione del panorama delle minacce.

Come in qualsiasi altro settore IT, l'impulso e la curiosità di ampliare le proprie competenze per rimanere al passo con le tecnologie emergenti sono qualità importanti che non dovrebbero mai mancare ai tecnici e agli architetti di Active Directory.

Dopo due decenni sostanzialmente dedicati ai sistemi, agli utenti e alle applicazioni on-premise, la maggior parte dei professionisti di AD è oggi responsabile dell'integrazione cloud e di garantire l'accesso protetto a un ambiente in cui il tradizionale perimetro di rete non esiste più. Le loro attività si svolgono mentre gli hacker utilizzano strumenti di attacco sempre più sofisticati per approfittare degli errori di configurazione di AD e delle vulnerabilità di Windows, prendono di mira le credenziali degli utenti e tentano di stabilire una presenza persistente nei sistemi locali.

Alla luce di queste circostanze, i responsabili tecnologici riconoscono l'importanza della cooperazione dei team che si occupano di sicurezza e di identità per garantire l'accesso utente sicuro nell'era del cloud computing e del telelavoro sempre più diffuso.

In futuro, gli esperti di AD dovranno assumere un ruolo più attivo nei dibattiti inerenti alla sicurezza. È una prassi ancora poco diffusa, ma poiché AD continua a costituire una superficie d'attacco per i criminali informatici, per questi professionisti è il momento di contribuire con la loro esperienza alle attività di sicurezza aziendale. L'identità assume un ruolo sempre più cruciale nelle strategie di sicurezza delle organizzazioni e aumenta anche il coinvolgimento degli amministratori di AD nelle decisioni in merito; pertanto, chi amplierà le proprie competenze e conoscenze rappresenterà un maggior valore per l'azienda.

L'evoluzione del panorama delle minacce costituisce un'opportunità per i professionisti di AD

Sotto molti aspetti, AD non è stata concepita per far fronte alle odierne sfide alla sicurezza, e non mi riferisco solo alle vulnerabilità come quelle sfruttate dagli attacchi Zerologon dello scorso anno. Nei loro attacchi, gli hacker approfittano anche dei protocolli incorporati nel sistema operativo Windows e della stessa AD.

A ciò si aggiunge il problema del ransomware. Gli attacchi ransomware registrati negli ultimi anni hanno utilizzato tecniche APT (Advanced Persistent Threat, minacce persistenti avanzate), come quelle fornite da strumenti quali BloodHound e Mimikatz, per svolgere attività di ricognizione e di furto delle credenziali. Nel 2020 un particolare tipo di ransomware ha sfruttato la condivisione SYSVOL nei controller di dominio di AD come veicolo per diffondere il malware nell'ambiente di destinazione.

In passato, i piani di ripristino di AD erano sostanzialmente incentrati su eventi come calamità naturali, guasti della rete elettrica o errori amministrativi. Oggi, di fronte all'eventualità che il ransomware interrompa ogni attività in ambito IT, le aziende devono essere pronte ad affrontare situazioni più plausibili, ad esempio un attacco che imponga il ripristino di AD da zero.

L'identità prima di tutto

I confini del tradizionale perimetro di rete sono oggi meno marcati a causa degli utenti mobili e del cloud computing. L'unico punto di controllo tra utenti, azioni e risorse di rete è l'identità dell'utente. L'identità digitale incide su tutti gli aspetti dell'azienda moderna. Per svolgere la propria mansione, ogni utente deve accedere ai sistemi e alle applicazioni appropriate. Controllare la sicurezza degli accessi, tuttavia, non è solo una questione di produttività. Autorizzazioni eccessive, password deboli e altri potenziali problemi possono causare violazioni dei dati, infezioni da malware, danni finanziari importanti e notti insonni per i responsabili IT e aziendali.

Con l'espansione dell'ecosistema delle applicazioni cloud utilizzate dal personale, gestire le integrazioni necessarie per AD diventa più complicato, e non solo per il team che si occupa delle identità. Anche l'estensione dei criteri di sicurezza e di accesso da AD on-premise ad AD nel cloud costituisce un problema di sicurezza. Per gli esperti di AD abituati a un modello di autorizzazione per gli ambienti on-premise, il cambio di attitudine che implica l'integrazione di AD on-premise con Azure Active Directory (AAD) può risultare sgradito. (Per un'opinione più approfondita sulle implicazioni della gestione congiunta di AD on-premise e di AAD in un ambiente ibrido, si legga "Top Risks to Watch for in Shifting to Hybrid Identity Management" di Doug Davis, Responsabile di prodotto Senior di Semperis.)

Come sempre accade, però, i cambiamenti portano con sé delle opportunità. Per chi è orientato alla trasformazione digitale, è di cruciale importanza capire i nuovi rischi a cui far fronte e il ruolo che occupa AD nel rompicapo della sicurezza. I professionisti dell'identità che, grazie alla propria esperienza, possono prendere parte alla discussione con il team della sicurezza o con la dirigenza saranno nella posizione migliore per dare il loro apporto al piano di sicurezza aziendale e migliorare le proprie prospettive di carriera.

Accrescere competenze e conoscenze in materia di identità e sicurezza

L'aggiornamento continuo è fondamentale per i professionisti di AD e di altri servizi di identità che vogliono contribuire attivamente alla strategia di sicurezza della propria azienda, ma in realtà è sempre uno degli aspetti più complessi e gratificanti delle professioni in ambito IT. Pensiamo a tutte le tecnologie che i professionisti IT hanno usato nel corso della propria carriera e che oggi non sono più utilizzate. Quante tecnologie sono giunte al termine del ciclo di vita e sono state dismesse? La formazione è la chiave per adeguarsi alla realtà in costante cambiamento della sicurezza e delle operazioni in ambito IT.

La buona notizia è che Internet mette a disposizione dei professionisti IT innumerevoli risorse, come ad esempio Channel 9, dove reperire video informativi sui prodotti Microsoft. Microsoft pubblica inoltre guide alla preparazione degli esami di certificazione. "Security, Compliance, and Identity Fundamentals" e "Security Fundamentals" sono esempi di certificazioni sulla sicurezza che i professionisti dell'identità potrebbero valutare. Oltre ad attestare le competenze maturate, queste e altre certificazioni consentono ai professionisti di acquisire quelle nozioni fondanti sulla sicurezza necessarie per un dibattito proficuo con i responsabili tecnologici.

Niente, tuttavia, vale come l'esperienza. Un'esperienza pratica in un ambiente di laboratorio, non esclusivamente con AD on-premise ma anche con gli ambienti ibridi che utilizzano Azure, AWS e Google Cloud Platform, è l'unico modo per acquisire competenze concrete nella gestione efficace e sicura di questi ambienti.

Continuare a studiare le identità e la sicurezza

In tutti i percorsi professionali in ambito IT, l'unica costante è il cambiamento. Per dominare qualsiasi aspetto di questo settore, dalla sicurezza allo sviluppo applicativo, occorre essere sempre aggiornati sulle tecnologie e le tendenze emergenti. I rischi di sicurezza correlati all'identità aumentano di pari passo con la progressiva adozione del cloud. I professionisti di AD devono comprendere a fondo e condurre il dibattito sull'importanza prioritaria della gestione delle identità nella strategia di sicurezza della propria organizzazione.

Tre modi per rafforzare Active Directory alla luce dei recenti attacchi

Di **BRIAN DESMOND**

In un recente webinar organizzato insieme a Semperis (l'azienda che ha sviluppato Purple Knight, uno strumento per la valutazione della sicurezza), abbiamo esaminato il principale denominatore comune degli ultimi attacchi di alto profilo: Active Directory (AD). Nella sessione "How Attackers Exploit Active Directory: Lessons Learned from High-Profile Breaches" ho analizzato, insieme a Sean Deuby e Ran Harel di Semperis, i quattro recenti attacchi che hanno riempito le prime pagine dei giornali: SolarWinds, l'attacco zero-day Hafnium Exchange, l'attacco Colonial Pipeline e infine quello che ha colpito il Servizio Sanitario irlandese. Ognuna di queste violazioni è stata perpetrata da autori differenti e con tattiche diverse, ma tutte hanno un punto in comune: le conseguenze devastanti. Nella nostra analisi abbiamo preso in considerazione tre delle principali misure preventive a disposizione delle organizzazioni per difendersi dagli attacchi informatici.

1 Proteggere le e-mail dalle minacce avanzate

La posta elettronica costituisce uno dei punti di accesso e di attacco più comuni. Le campagne di phishing rivolte agli utenti finali, sempre più sofisticate e convincenti, forniscono agli attaccanti un percorso facile per ottenere credenziali valide e/o infiltrare malware negli endpoint. Per proteggersi da queste minacce è assolutamente fondamentale che le organizzazioni adottino un approccio a più livelli. Formazione sulla Security Awareness e simulazioni del phishing sono importanti per informare e imparare a valutare il rischio. A prescindere dal livello di preparazione, gli hacker riusciranno comunque a superare le difese. Per far fronte a questi attacchi, la strategia di difesa deve includere una soluzione di protezione contro le minacce e-mail avanzate, che sia in grado di alzare le barriere più in alto rispetto agli strumenti antispam e antivirus. Per contrastare le minacce odierne occorre implementare un servizio che utilizzi algoritmi di machine learning e altri strumenti di rilevamento avanzato per individuare e bloccare i messaggi di phishing e gli allegati sospetti.

"Solo chi nell'ultimo anno ha vissuto isolato dal mondo non ha avuto notizia degli eventi di sicurezza informatica che si sono verificati praticamente ogni settimana. Dedichiamo molto tempo a parlare delle nuove modalità di attacco, ma in realtà i criminali non sono alla ricerca di nuovi metodi; puntano solo ad infiltrarsi, e l'enorme varco a loro disposizione è Active Directory."

Sean Deuby, *Responsabile Servizi, Semperis*

2 Prevenire il movimento laterale

Una volta compromesso un computer client o un server membro, i malintenzionati tenteranno di spostarsi lateralmente all'interno della rete e di avviare l'escalation dei privilegi. Prevenire questi movimenti laterali complica il lavoro degli hacker. A questo scopo possono essere utilizzati alcuni controlli semplici dal punto di vista tecnico, ma a volte complessi in termini operativi. Innanzitutto, la password dell'amministratore locale su ogni endpoint deve essere differente. Per facilitare questo compito, Microsoft offre gratuitamente la Soluzione password dell'amministratore locale (LAPS). In secondo luogo, non è possibile annidare gli account di dominio nel gruppo degli amministratori locali per agevolare il supporto IT. Il personale IT deve utilizzare LAPS per recuperare le credenziali amministrative per gli endpoint specifici.

3 Proteggere l'accesso alle credenziali con privilegi

Una delle prime misure di difesa consiste nell'impedire ai malintenzionati di ottenere l'accesso con privilegi, in particolar modo l'accesso come amministratore di dominio. Se l'avversario riesce ad appropriarsi dei privilegi, potrà ottenere un maggior controllo, o addirittura il controllo totale dell'intera rete. È quindi fondamentale implementare controlli efficaci che isolino e proteggano le credenziali con privilegi. Ravenswood Technology Group si avvale di due set di controll molto diffusi: i controlli di sicurezza su più livelli e le workstation ad accesso con privilegi (PAW). I controlli di sicurezza su più livelli prevengono l'esposizione delle credenziali con i privilegi più elevati nelle risorse a maggior rischio, come i computer client, da cui potrebbero essere prelevate con facilità. Le PAW isolano le attività eseguite da un amministratore nelle workstation di utilizzo quotidiano in una workstation altamente sicura, proteggendo le credenziali e la sessione dell'amministratore da vettori di attacco quali e-mail, accesso Internet e alcuni tipi di malware.

Il vostro servizio AD è pronto per affrontare il panorama delle minacce odierno?

Gli attacchi che abbiamo esaminato in questo webinar sono solo quattro tra le infinite violazioni di cui ogni giorno leggiamo sulle prime pagine. Rendere più sicuro l'ambiente IT dell'organizzazione è fondamentale e, praticamente per ogni azienda, Active Directory deve diventare una componente chiave della strategia di rafforzamento delle difese. Purple Knight è lo strumento adatto per una valutazione gratuita dei controlli di sicurezza di Active Directory. Ravenswood e Semperis sono probabilmente le due organizzazioni con la migliore esperienza in materia di sicurezza di AD, oltre alla stessa Microsoft. La nostra partnership è estremamente solida e può aiutare le organizzazioni di tutto il mondo a innalzare gli standard della sicurezza dell'identità negli ambienti ibridi.

Per ulteriori approfondimenti su come proteggere la vostra organizzazione, partecipate ai webinar on-demand. Potete inoltre scaricare gratuitamente Purple Knight: vi aiuterà ad identificare e colmare le lacune di sicurezza di AD e ad acquisire familiarità con la protezione del vostro ambiente AD, indipendentemente da quanto sia complesso, intricato o trascurato.

Il valore effettivo del ROI nel ripristino rapido di Active Directory

Di **SEAN DEUBY**

Nonostante ogni responsabile o amministratore IT sia consapevole dell'importanza di un solido piano di ripristino di Active Directory (AD) come componente essenziale di qualsiasi strategia di continuità aziendale, calcolare l'effettivo ritorno sull'investimento (ROI) di un piano di ripristino di AD ottimizzato è notoriamente complicato. Nell'elaborazione di un calcolo esatto e giustificabile entrano infatti in gioco tante variabili. Per non creare aspettative, anticipo che in questo articolo non presenterò alcun tipo di calcolatore interattivo del ROI.

Esaminerò invece alcune modalità concrete per comprendere quale sia il valore del ROI nel garantire un adeguato ripristino di AD, permettendovi di fare i vostri calcoli e trarre le dovute conclusioni in autonomia. La perdita di un controller di dominio è di per sé un problema, ma dobbiamo immaginare l'altro scenario sempre più diffuso che ha conseguenze disastrose: l'attacco ransomware che mette fuori gioco tutti i controller di dominio di tutti i siti aziendali. In una situazione di questo tipo il ripristino di AD si trasforma in una sfida da superare sotto pressione e con l'acqua alla gola.

Nell'ultimo anno abbiamo analizzato numerosi attacchi ransomware in cui i criminali informatici apportavano modifiche ad AD, in un modo o nell'altro, andando ben oltre le modifiche di base degli account o delle password utente, per ottenere l'accesso ai sistemi informatici e poi spostarsi lateralmente e propagare il malware. I gruppi di autori di ransomware accolgono oggi ingegneri che dissezionano AD e i relativi aggiornamenti di sicurezza alla ricerca di opportunità per l'escalation dei privilegi e per diffondere rapidamente il malware all'intera organizzazione. Le indagini forensi condotte dopo gli attacchi ransomware indirizzati ad AD hanno svelato che i criminali si dedicano in particolare alla modifica degli account di gruppo, degli account utente, degli oggetti Criteri di gruppo, dei volumi SYSVOL e dei controller di dominio.

Avendo presenti queste strategie di hackeraggio, nel calcolare il ROI del ripristino di AD occorre considerare i fattori seguenti:

Costo delle perdite di esercizio:

È molto probabile che una parte materiale delle vostre attività si basi sul funzionamento ottimale di AD che, sostanzialmente, autentica gli utenti per fornire loro accesso ad applicazioni, sistemi e dati. A quanto ammonta la perdita di utile o produttività generata da ogni ora di inattività di AD? Quante ore, giorni o settimane sono necessari prima che l'azienda superi il punto di non ritorno e non possa più risollevarsi finanziariamente? Ricordate l'attacco ransomware sferrato alla città di Baltimora? La ripresa delle attività ha richiesto svariati mesi ed è costata oltre 18 milioni di dollari.

Assenza di un piano di business continuity che includa AD:

Se la maturità dell'organizzazione è sufficiente, sarà stato approntato un piano di business continuity/disaster recovery che stabilisce le attività da compiere per ripristinare l'operatività aziendale in seguito a un'interruzione. Nella maggior parte dei casi il piano considera le perdite relative alle infrastrutture o agli impianti causate da calamità naturali. Sono poche le aziende che hanno previsto un piano specifico per il ripristino dell'operatività dopo un attacco informatico, soprattutto di un tipo imprevedibile come un attacco ransomware. La modalità di ripristino di AD in situazioni come queste dipende da quali modifiche hanno apportato i criminali informatici all'ambiente di AD. Si può pianificare il ripristino di una precedente versione di AD, ma come determinare quanto tornare indietro per trovare una versione sicura nota? Quali sistemi, servizi e applicazioni dipendenti da AD saranno disturbati o non funzioneranno affatto a causa del ripristino generalizzato di AD a uno stato precedente? Avete la certezza di poter individuare un backup recente e privo di malware, dal quale eseguire il ripristino? In mancanza di un piano o della possibilità di comprendere cosa sia stato modificato in AD prima di eseguire il ripristino, l'organizzazione dovrà dedicare un tempo incalcolabile a risolvere tutti i problemi che il ripristino ha causato.

Non sempre il ripristino è la giusta risposta:

Se le modifiche apportate dai criminali durante un attacco si riducono soltanto, ad esempio, all'aggiunta di un account al gruppo degli amministratori di dominio, il ripristino di AD a una versione di qualche giorno fa o del mese precedente potrebbe non essere la soluzione giusta. In questo caso, è forse più conveniente monitorare le modifiche in AD e prevedere la possibilità di non consentire le modifiche agli account "protetti", come il gruppo degli amministratori di dominio, o di ripristinare automaticamente una modifica a una configurazione approvata.

Possiamo riassumere le considerazioni fatte fin qui a tre rischi:

Il rischio di un ripristino lento, il rischio di un ripristino che produce ulteriori attività di riparazione dei danni e il rischio di un ripristino eccessivo per la natura delle modifiche apportate ad AD.

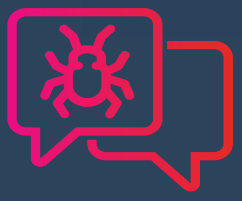
Un approccio diverso per il calcolo del ROI di un ripristino di AD

Invece di elaborare il ROI di un ripristino di AD usando uno dei tanti calcolatori reperibili online, è meglio analizzare diversi scenari reali e valutare la capacità di reazione dei sistemi di ripristino di AD in uso rispondendo alle seguenti domande, che si basano sui fattori sopra indicati:

- Quali componenti critici dell'attività dipendono da AD per il proprio funzionamento? Qual è il costo stimato della loro inattività?
- Quanto tempo occorre per ripristinare AD in base alle modifiche apportate durante un attacco?
- Qual è il livello di visibilità rispetto alle modifiche dannose apportate ad AD e, in caso di mancata visibilità, quanto occorre tornare indietro per indagare e quanto tempo sarà necessario?

  Il ripristino può incidere su altri aspetti delle attività che sarà necessario riparare? Se sì, quanto tempo sarà necessario? Va ricordato che alcuni numeri delle password degli account di utenti e computer potrebbero non corrispondere, impedendo di fatto l'acceso al dominio. In più, nelle versioni precedenti potrebbero mancare account, appartenenze a gruppi, record DNS, ecc.

BREVI STORIE DAL SETTORE:



Semperis offre soluzioni di disaster recovery cyber-first di altissima qualità per Active Directory. Di seguito presentiamo alcuni dei risultati ottenuti dai nostri clienti dopo l'adozione della soluzione Active Directory Forest Recovery (ADFR) di Semperis:

- La compagnia aerea israeliana El Al ha implementato Semperis ADFR e ridotto il tempo di ripristino di una foresta completa di AD da 24 a 2 ore.
- Un rivenditore internazionale, con oltre 2,2 milioni di utenti e 500 data center è passato a Semperis ADFR da una soluzione precedente e ha ridotto il tempo di ripristino di una foresta di AD da 6 giorni a 6 ore.
- Una società del settore sanitario con un database DIT da 65 GB ha ridotto il tempo di ripristino della foresta di AD dagli 1,5 giorni necessari alla soluzione preesistente a meno di 4 ore con Semperis ADFR.

- Ritenete che il ripristino vi metta in una condizione di sicurezza accertata? Occorre essere consapevoli della differenza tra la ripresa e il recupero delle attività aziendali: se non si dispone di un backup pulito e privo di malware da cui avviare il ripristino, si corre il rischio di reintrodurre le stesse vulnerabilità che vi hanno già esposto all'attacco.

In breve, il ROI di un ripristino di AD è più correlato alla capacità corrente di tornare a una condizione di produttività e di sicurezza accertata dopo un attacco di quanto non emerga da un qualsiasi calcolatore del ROI online, che non tiene in considerazione il gran numero di variabili coinvolte in un attacco ransomware. Analizzando a fondo alcune situazioni e riflettendo sulle capacità di ripristino specifiche a vostra disposizione, potrete evidenziare spese che possono essere eliminate implementando un'adeguata soluzione per il ripristino di AD, che sia progettata per contrastare, prevenire ed eseguire il ripristino in caso di modifiche dannose arrecate ad AD.

"Con ADFR abbiamo protetto 3 foreste. I nostri test di ripristino sono affidabili e sono certo che potremo ripristinare le nostre foreste AD complete in breve tempo con l'opzione Full Forest Recovery."

Leggete la recensione completa su Gartner Peer InsightsVolete approfondire l'argomento? Le seguenti risorse, redatte dal nostro team di esperti di AD, forniscono ulteriori informazioni su come elaborare un piano di ripristino di AD completo.

Come difendere Active Directory dagli attacchi che non lasciano traccia

Di **GUIDO GRILLENMEIER**

Le nuove tecniche e tattiche utilizzate dai criminali informatici per accedere ad Active Directory rendono gli attacchi sempre più pericolosi; individuarli in anticipo è ormai imprescindibile.

Il rilevamento è uno degli aspetti essenziali di qualsiasi strategia di sicurezza informatica. È possibile reagire prontamente, infatti, solo se si è in grado di individuare il malintenzionato che entra, si sposta o, peggio, gestisce la rete aziendale. I criminali sono capaci di lavorare in incognito, come dimostra il numero medio di giorni che passano prima che un hacker infiltrato in una rete venga individuato: 146, secondo Microsoft.

Per individuare azioni potenzialmente dannose contro Active Directory (AD), la maggior parte delle organizzazioni si affida al consolidamento del registro eventi del controller di dominio e alle soluzioni SIEM, per individuare accessi e modifiche anomale. Sono sistemi che funzionano, a condizione che la tecnica di attacco lasci una traccia nei registri.

Sono stati tuttavia osservati alcuni tipi di attacco che non lasciano tracce evidenti o indizi di attività pericolose, come i seguenti.

Attacco DCShadow:

Utilizzando la funzionalità DCShadow dello strumento di hackeraggio Mimikatz, questo attacco inizia con la registrazione di un controller di dominio non autorizzato, modificando la partizione di configurazione di AD. A questo punto, l'autore dell'attacco apporta false modifiche dannose, ad esempio cambia le appartenenze al gruppo degli amministratori di dominio, oppure apporta modifiche meno evidenti come l'aggiunta del SID del gruppo degli amministratori di dominio all'attributo sidHistory di un utente standard compromesso. Poiché il controller di dominio fasullo non registra le modifiche, questa tecnica di attacco aggira la registrazione convenzionale basata su SIEM. Le modifiche vengono invece introdotte direttamente nel flusso di replica dei controller di dominio in produzione.

Modifiche ai criteri di gruppo:

Un attacco documentato da parte del ransomware Ryuk ha modificato un oggetto Criteri di gruppo affinché propagasse l'installazione di Ryuk negli endpoint remoti dell'organizzazione colpita. Per impostazione predefinita, i registri eventi non includono informazioni sulle modifiche apportate a un criterio di gruppo. Se, pertanto, un hacker esegue una modifica dannosa, come nel caso di Ryuk, verrà rilevato soltanto un account con accesso al criterio di gruppo che apporta una modifica, un evento che probabilmente non attiverà alcun allarme.

Attacco Zerologon:

In seguito al rilascio pubblico di un codice di exploit proof-of-concept, un hacker con accesso alla rete per un controller di dominio è riuscito a inviare messaggi speciali del protocollo Netlogon costituiti da stringhe di zeri, forzando il computer del controller di dominio a modificare la propria password in una stringa vuota. In questo modo, senza credenziali di accesso (da qui il nome "zero logon") l'hacker si è impadronito del controller di dominio, ha potuto apportare qualsiasi modifica ad AD e quindi sfruttare questa via per attaccare gli altri sistemi dell'infrastruttura. È molto improbabile che gli strumenti di monitoraggio in uso controllino le modifiche non previste alle password nei controller di dominio.

Questi attacchi non lasciano alcuna traccia, e non per caso: sono progettati così. I cyber criminali dedicano molto tempo a ispezionare l'esatto funzionamento degli ambienti a cui puntano, alla ricerca di modalità per aggirare, offuscare e ingannare qualsiasi forma di rilevamento, inclusa la registrazione degli accessi.

Assodata l'esistenza di questo tipo di attacchi, è bene capire quali azioni intraprendere, tanto proattivamente quanto reattivamente.

Protezione contro le modifiche dannose di Active Directory

Per proteggere l'organizzazione dalle modifiche dannose di AD abbiamo a disposizione tre metodi:

- Monitorare AD per individuare modifiche dannose: poiché le soluzioni SIEM non sono sufficienti a questo scopo, è necessario avvalersi di una soluzione di terze parti progettata per visualizzare ogni modifica apportata ad AD, indipendentemente dall'utente che l'ha effettuata, su quale controller di dominio e con quale strumento. Una soluzione di questo tipo legge e analizza il traffico di replica dei controller di dominio. L'attività di monitoraggio deve coprire anche le modifiche apportate ai criteri di gruppo. In molti casi, queste soluzioni consentono di impostare specifici oggetti da proteggere monitorandone qualsiasi cambiamento, ad esempio una modifica nell'appartenenza al gruppo degli amministratori di dominio, così che l'esecuzione di una modifica su un oggetto protetto attiverà un allarme. La soluzione dovrebbe coprire le modifiche ai criteri di gruppo e offrire visibilità sulle repliche.

- Alla ricerca di DCShadow: Mimikatz lascia alcune tracce dietro di sé, e alcuni indicatori spia rivelano l'uso del comando DCShadow nella rete. L'analisi regolare della sicurezza di AD deve prevedere la ricerca di questi segnali. Una volta individuate tracce di Mimikatz o DCShadow nell'ambiente occorre agire rapidamente, perché l'attacco è già stato sferrato. A questo punto, sarebbe opportuno disporre di una soluzione che evidenzia le modifiche apportate a livello di replica, che potrebbero essere analizzate e quindi reimpostate.

- Essere in grado di ripristinare AD: alle organizzazioni è indispensabile la capacità proattiva di ripristinare ogni elemento di AD nel caso in cui ne venga scoperta la compromissione. In alcune situazioni, si può pensare ai backup e a una strategia di disaster recovery per ripristinare AD dopo un attacco informatico. È bene tuttavia sapere che, in caso di ripristino dell'intero servizio AD perché colpito da un attacco malware, un valido backup del controller di dominio non equivale a un ripristino rapido e ottimizzato del servizio AD. È opportuno esercitarsi periodicamente con l'intero processo di ripristino, seguendo le indicazioni della voluminosa Guida di Microsoft al ripristino della foresta di AD. È altrettanto utile cercare soluzioni capaci di ripristinare le modifiche fino al livello dell'attributo, o di ripristinare automaticamente quelle apportate agli oggetti protetti, se rilevate.

Prendere di mira Active Directory e adattarla ai propri obiettivi è la strategia più comune adottata al momento dai criminali informatici, tanto che il vecchio metodo di osservare gli eventi di controllo di AD per individuare le modifiche è diventato obsoleto. Le organizzazioni interessate alla sicurezza e all'integrità della propria AD devono individuare modalità aggiuntive per rendere visibile ogni modifica eseguita in AD, e prevedere le necessarie strategie di ripristino.

WEBINAR

HOW ATTACKERS EXPLOIT ACTIVE DIRECTORY: LESSONS LEARNED FROM HIGH-PROFILE BREACHES

Quali vulnerabilità nasconde la vostra Active Directory?

Di **SEAN DEUBY**

La protezione di Microsoft Active Directory (AD) implica diversi rischi, dagli errori di gestione alle vulnerabilità prive di patch. Molti nostri articoli si concentrano sul fatto che gli autori degli attacchi puntano ad AD per l'escalation dei privilegi e per infiltrarsi in modo persistente nell'organizzazione. È sufficiente indagare una qualsiasi violazione per scoprire che all'origine c'è l'impiego di credenziali rubate, usate a volte per il primo accesso, a volte per arrivare ai sistemi critici, ma sempre a discapito dell'organizzazione colpita.

La protezione avanzata di AD inizia dalla gestione delle vulnerabilità e dei comuni errori di configurazione e gestione che aprono le porte alle compromissioni. Per difendere AD, gli amministratori devono conoscere le modalità di cui si avvalgono i malintenzionati per infiltrarsi nel loro ambiente. Quanti di loro però sono in grado di elencare i tipi di falle nella sicurezza in cui si insidiano gli hacker nelle varie fasi della violazione?

Autenticazione non riuscita

Ironicamente, alcuni degli errori di configurazione più diffusi e potenzialmente pericolosi che interessano Active Directory sono legati al processo di autenticazione. Immaginiamo una situazione in cui un'organizzazione intende consentire sia l'uso di un'applicazione di terzi o realizzata in-house e non integrata in AD, sia l'invio di query ad AD da parte degli utenti attivi. La via più semplice è quella di abilitare l'accesso anonimo ad AD. Sebbene sia utile dal punto di vista della produttività per non gravare su amministratori già oberati di lavoro, questa modalità consente anche agli utenti non autenticati di inviare query ad AD. Se la funzionalità viene abilitata senza controlli di mitigazione, il profilo di rischio dell'organizzazione è destinato a peggiorare.

La vulnerabilità Zerologon segnalata nel 2020 è stata sfruttata dagli hacker in quanto consentiva loro di modificare o rimuovere le password degli account di servizio in un controller di dominio. Le conseguenze di un exploit di questo tipo possono essere catastrofiche. Tra i segnali di allarme di un ambiente AD non sicuro ci sono le password deboli, senza scadenza o del tutto assenti.

Criteri per le password avanzate dovrebbero invece essere all'ordine del giorno nell'intera infrastruttura di Active Directory. Qualsiasi account per il quale è impostato il flag PASSWD_NOTREQD dovrebbe richiedere automaticamente un'ulteriore analisi e dimostrare di avere una ragione giustificabile per tale configurazione. Inoltre, le password, in primis quelle degli account dei servizi, devono essere sottoposte a rotazione periodica. La mancata modifica delle password per lunghi periodi di tempo aumenta le probabilità di riuscita di un attacco di forza bruta, perché gli hacker avranno più tempo per impadronirsene.

Tra i problemi di autenticazione da tenere sotto controllo ricordiamo:

- Oggetti Account computer e Account del servizio gestito del gruppo con password impostate da oltre 90 giorni
- Oggetti Criteri di gruppo con password reversibili
- Abilitazione dell'accesso anonimo ad Active Directory
- Vulnerabilità Zerologon (CVE-2020-1472) con patch non applicata.

Concessione di autorizzazioni eccessive

La maggior parte degli ambienti AD è in produzione da molti anni, e nel tempo la loro superficie d'attacco si è estesa. Molte delle vulnerabilità accumulate in una foresta possono essere fatte risalire a un modello comune in cui un utente deve compiere un'azione, in genere in fretta, e il percorso con privilegi minimi per eseguirla richiede troppo tempo, non è facilmente disponibile o, semplicemente, non è noto. Accade quindi che all'utente, al gruppo o all'autorizzazione vengano concessi privilegi eccessivi, solo per garantire che la richiesta venga soddisfatta e che il ticket venga chiuso. In seguito, quel diritto non verrà mai rimosso, causando così la crescita a dismisura della superficie d'attacco.

Non è insolito in realtà che gli ambienti AD presentino un numero inutilmente alto di amministratori di dominio. Questa condizione, tuttavia, può rivelarsi ancor più pericolosa quando gli account non appartengono più a proprietari legittimi: significa che restano semplicemente in attesa di essere sfruttati in un attacco. Anche gli account dei servizi con autorizzazioni eccessive costituiscono un rischio elevato, in quanto le loro password sono in genere configurate per non scadere e molte di loro sono deboli, diventando così un ambito obiettivo degli attacchi di kerberoasting. In misura proporzionale all'aumento del numero di utenti con privilegi di amministratore, cresce anche la superficie d'attacco che deve essere protetta. L'appartenenza a questi gruppi deve essere rigidamente controllata.

Ovviamente, l'errore è sempre possibile. Ad esempio, mano a mano che un ambiente AD diventa più grande e più complesso, diventa difficile tenere correttamente conto dei permessi ereditati, ed è facile garantire involontariamente a un account un livello di privilegi troppo elevato. In ogni caso, se gli attaccanti sferrano un'offensiva, anche la corretta gestione della delega dei privilegi può non essere sufficiente.

Consideriamo, ad esempio, l'impatto di un attacco AdminSDHolder. Nel container AdminSDHolder viene archiviato il descrittore di sicurezza applicato ai gruppi con privilegi. Per impostazione predefinita, ogni 60 minuti il processo Security Description Propagation (SDPROP) confronta le autorizzazioni degli oggetti protetti e reimposta le eventuali discrepanze, in conformità a quanto definito in AdminSDHolder.

In un attacco AdminSDHolder, gli hacker sfruttano il processo SDPROP per mantenere la persistenza, sostituendo i permessi di un oggetto con le modifiche non autorizzate da loro disposte. Se vengono identificate e annullate le modifiche alle autorizzazioni, ma non quelle non autorizzate ad AdminSDHolder, queste ultime verranno ripristinate.

La verifica delle autorizzazioni e il monitoraggio delle attività sospette restano la miglior difesa contro l'abuso dei privilegi.

Tra i problemi delle autorizzazioni da tenere sotto controllo ricordiamo:

- Oggetti con privilegi appartenenti a proprietari senza privilegi
- Modifiche alle autorizzazioni nell'oggetto AdminSDHolder
- Utenti senza privilegi con diritti di sincronizzazione del controller di dominio
- Modifiche apportate negli ultimi 90 giorni allo schema predefinito del descrittore di sicurezza

Sintesi sulla sicurezza

Con le giuste informazioni sugli indicatori di esposizione, le organizzazioni possono rafforzare la sicurezza della propria AD. Un valido contributo è offerto da Purple Knight, uno strumento per la valutazione della sicurezza rilasciato a marzo da Semperis. Purple Knight invia query all'ambiente Active Directory in modalità di sola lettura ed esegue una serie completa di test a fronte dei più diffusi ed efficaci vettori d'attacco, per individuare configurazioni a rischio e punti deboli nelle misure di sicurezza.

La scansione di Active Directory fornisce informazioni sullo stato della sicurezza e riduce il rischio che le modifiche non autorizzate o le configurazioni errate non vengano rilevate. Gli amministratori di AD devono conoscere alla perfezione il loro mestiere, ma anche le tattiche dei propri avversari. Prestando costante attenzione ai segnali di allarme, potranno rafforzare AD e difenderla dagli attacchi più comuni.

> *To defend AD, administrators* ***need to know*** *how attackers are targeting their environment.*

I PRINCIPALI RISCHI DI SICUREZZA DA TENERE SOTTO CONTROLLO NEL PASSAGGIO ALLA GESTIONE DELL'IDENTITÀ IBRIDA

Di **DOUG DAVIS**

Non è difficile capire perché le aziende si stanno orientando verso un modello di gestione dell'identità ibrida - in parte nel cloud e in parte in locale - che promette il meglio dei due mondi. In un ambiente che ruota su Active Directory, per sfruttare il cloud è necessaria l'integrazione di Azure Active Directory (ADD).

Del resto, questa soluzione è concepita con un occhio verso le applicazioni SaaS, in quanto fornisce controllo degli accessi e Single Sign-On. Con la più ampia adozione del cloud, la possibilità di gestire sia l'accesso locale che quello cloud diventa vitale per le aziende. Utilizzate insieme, AAD e Active Directory (AD) rendono possibile la gestione dell'identità ibrida.

Tuttavia, come in ogni ambito IT, il motto "pensare prima di agire" è sempre valido.

Adottare il cloud: un passaggio epocale

Spostare una qualsiasi parte di un'attività IT nel cloud richiede capacità di adattamento; l'autenticazione degli utenti non è differente. Da un punto di vista concettuale, le organizzazioni dovranno considerare tre problematiche.

1. Un nuovo modello di autenticazione

Dopo aver gestito per 20 anni le identità nello stesso modo, l'aggiunta di AAD costituirà un cambiamento importante. Per passare dall'utilizzo di AD on-premise all'autenticazione cloud occorre adottare un approccio e un'atteggiamento nuovi. AAD non prevede unità organizzative o foreste, né oggetti Criteri di gruppo. I concetti - e i conflitti - relativi alla protezione delle identità in AD non sono più validi in AAD.

All'inizio, molti amministratori ritengono che la protezione di AAD sia simile a quella di AD, ma la realtà è diversa. In alcune situazioni AAD è già utilizzata, quasi inconsapevolmente. Se, ad esempio, l'organizzazione si avvale di qualsiasi servizio cloud di Microsoft, come Office 365, AAD è già attiva in background. AAD è utilizzata anche per la connessione ad altri applicazioni SaaS non Microsoft, come Salesforce. Tutti questi fattori introducono nuove considerazioni e opportunità. Ad esempio, è meglio tenere AD e AAD separate, oppure combinarle tramite Azure AD Connect? Per decidere meglio e mantenere al tempo stesso i sistemi informatici al sicuro, occorre approfondire alcuni nuovi concetti.

2. L'estensione del perimetro

Una volta adottato il cloud, il concetto di perimetro di rete tradizionale dell'organizzazione cessa di esistere. Quest'idea rappresenta un cambiamento epocale per gli amministratori IT che hanno dedicato gli ultimi 20 anni all'esecuzione di AD in locale. In un ambiente di identità ibrida, le organizzazioni devono essere preparate per difendersi da una serie infinita di potenziali punti d'accesso.

3. Cambiamenti radicali del modello di autorizzazioni

Il passaggio ad AAD modifica drasticamente anche il modello di autorizzazioni che le organizzazioni devono proteggere. Nell'ambiente on-premise, è abbastanza semplice controllare chi ha l'accesso fisico ai controller di dominio, e i punti di accesso per la gestione sono ben definiti e documentati. In un ambiente AD ibrido, le identità sono ora archiviate anche nel cloud e vulnerabili allo sfruttamento da parte di chiunque abbia accesso a Internet. All'improvviso, gli amministratori si trovano a operare con un modello strutturalmente aperto per le connessioni di accesso iniziali, il che, insieme al numero più elevato dei servizi, ruoli e autorizzazioni richieste, incide fortemente sul rischio.

Microsoft ha messo a disposizione materiali formativi per preparare le aziende ai cambiamenti provocati dall'adozione di AAD. Molte organizzazioni IT, tuttavia, non riescono ancora ad apprezzare appieno le implicazioni della gestione dell'identità ibrida. Con l'aumento del numero di aziende che adotta l'approccio ibrido, cambia anche il modus operandi dei cyber criminali.

Nel settembre 2020, i ricercatori di Mandiant (FireEye) hanno osservato un aumento degli incidenti relativi a Microsoft 365 e Azure Active Directory, legati soprattutto ai tentativi di phishing via e-mail di convincere le vittime a inserire le proprie credenziali di Office 365 in un sito fasullo. Hanno anche notato l'utilizzo da parte degli hacker di un modulo di PowerShell chiamato AADInternals, che consente loro di spostarsi dall'ambiente locale ad AAD, per creare backdoor, rubare password e intraprendere altre azioni dannose. Queste minacce avranno una crescita esponenziale e proporzionale al maggiore interesse verso Azure e Office 365.

Autorizzazioni, autorizzazioni e ancora autorizzazioni

Senza dubbio, per i tre aspetti sopra elencati il maggior rischio per la sicurezza è rappresentato dalle modifiche al modello di autorizzazioni. Quando le organizzazioni passano a un ambiente di identità ibrida, hanno a disposizione un elevato numero di servizi. Al posto di un insieme ben definito di gruppi amministrativi in Active Directory, Azure AD utilizza i ruoli, con cui si ha poca familiarità. Qui è possibile visualizzare un elenco di ruoli, a ognuno dei quali corrisponde un lungo elenco di autorizzazioni assegnate. Dalla sola descrizione, è difficile capire le autorizzazioni assegnate a ciascun ruolo, ma molti hanno un livello di accesso elevato non sempre evidente.

Inoltre, il collegamento di qualsiasi servizio SaaS ad AAD, che è probabilmente la ragione per la quale è stata aggiunta Azure AD, implica la gestione di ulteriori modelli di autorizzazioni. Microsoft Teams, ad esempio, utilizza l'integrazione SharePoint sul backend. Una configurazione errata fa sì che l'aggiunta di un utente guest a Teams crei una condizione per cui il nuovo utente può accedere ai file archiviati in SharePoint for Teams. Gli utenti potrebbero non essere consapevoli che questi file sono disponibili a utenti guest aggiunti al proprio canale solo per una breve conversazione. Anche la possibilità di aggiungere applicazioni in Teams estende il modello di autorizzazioni a questi strumenti di terze parti. È solo un esempio dei problemi complessi che possono insorgere per ogni servizio gestito tramite AAD.

Di fatto, tenere traccia delle autorizzazioni fornite alle applicazioni di terze parti è un aspetto fondamentale e al tempo sottovalutato nella maggior parte delle implementazioni di AAD. Queste richieste di autorizzazione attivano una finestra pop-up temporanea che elenca le autorizzazioni necessarie all'app. Tali elenchi possono essere lunghi e devono essere esaminati con attenzione prima di essere accettati, una procedura che non viene quasi mai eseguita.

Alle organizzazioni possono inoltre presentarsi i due seguenti scenari, sempre legati alle autorizzazioni, che devono essere compresi nel contesto della sicurezza.

- Strumenti di terze parti che acquisiscono i dati da Azure AD e li archiviano nei propri database, come, ad esempio, un'applicazione registrata in Azure AD che consente a un sistema CRM di leggere i profili utente o che dispone di altre autorizzazioni di lettura che le permettono di recuperare e archiviare i dati in autonomia. Una volta acquisiti da Azure AD, i dati risiederanno in un database esterno e l'organizzazione dovrà fare affidamento sulla struttura di sicurezza dello strumento stesso.

- Strumenti di terze parti con accesso in scrittura, che possono apportare modifiche all'interno dello strumento stesso. In questo caso, l'autenticazione richiesta per apportare modifiche nel tenant viene trasferita da Azure AD a qualsiasi controllo appartenente allo strumento. Un utente potrebbe accedere senza l'autenticazione a più fattori, perché lo strumento non supporta l'accesso Single Sign-On (SSO), servendosi dell'applicazione come proxy dell'autorizzazione, e agendo senza alcuni dei controlli che sarebbero normalmente richiesti.

I reparti IT dovranno limitare chi può approvare le applicazioni o, almeno, dotarsi di linee guida chiare su quali autorizzazioni debbano essere considerate appropriate. Adottare un approccio all'identità ibrida significa gestire un modello di autorizzazioni molto più vasto. Per farlo al meglio, è necessario definire una governance rigida sulle app che possono essere attivate e sui diritti di accesso associati.

Comprendere i rischio di gestione delle identità ibride

La sicurezza deve essere sempre prioritaria, che l'autenticazione sia gestita nel cloud, on-premise o in entrambi gli ambienti. Sebbene la gestione delle identità in un ambiente ibrido possa sembrare semplice come aggiungere un dispositivo Windows ad AAD, non tenere conto dei nuovi rischi espone l'organizzazione a problemi futuri. La conoscenza è sempre la prima linea di difesa, anche se il volume della documentazione necessaria a capire bene la sicurezza in AAD è imponente. Per ridurre le complessità della sicurezza e automatizzarne la comprensione durante e dopo l'implementazione dell'ambiente ibrido sono disponibili strumenti nativi o di terze parti.

NUOVE PROSPETTIVE SULLA PROTEZIONE DEI SISTEMI A IDENTITÀ IBRIDA

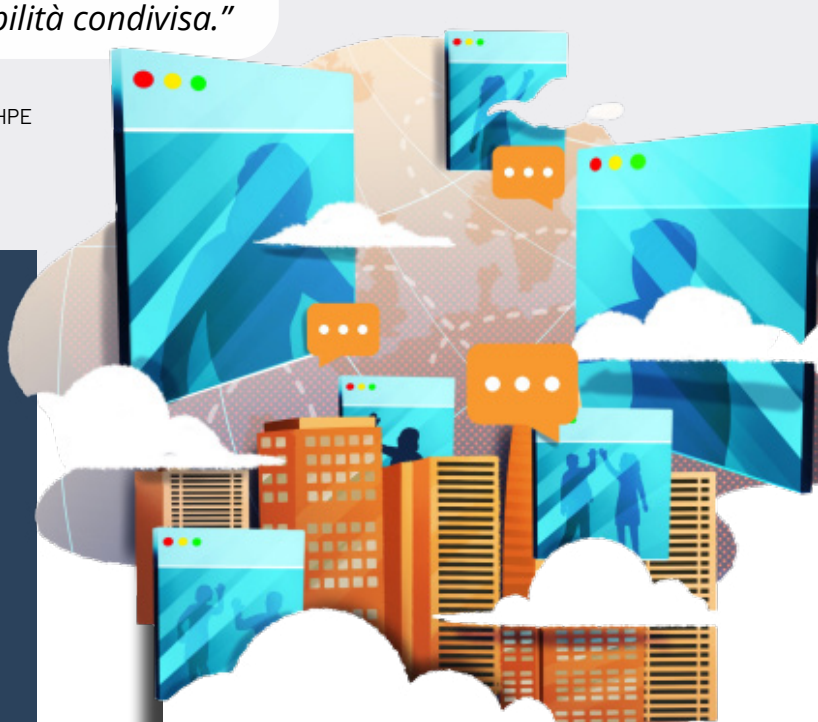
Presentazioni di esperti in materia di sicurezza dell'identità in occasione di #HIPEurope2021

"Quando un aggressore ha ottenuto l'accesso ad Active Directory, è tutta una questione di tempo. Dobbiamo assicurarci che l'aggressore non possa diffondersi in tutte le foreste di Active Directory. Dobbiamo analizzare la violazione, vedere il potenziale impatto e implementare una rete di sicurezza. Dobbiamo ripristinare l'Active Directory nel giro di ore, e non di giorni."

Ben Cauwel
Security Delivery Manager presso Accenture

"Oggi, uno dei grossi problemi con la sicurezza del cloud è che alcune persone non capiscono ancora il modello di responsabilità condivisa."

Jan de Clercq
Senior Security Architect presso HPE



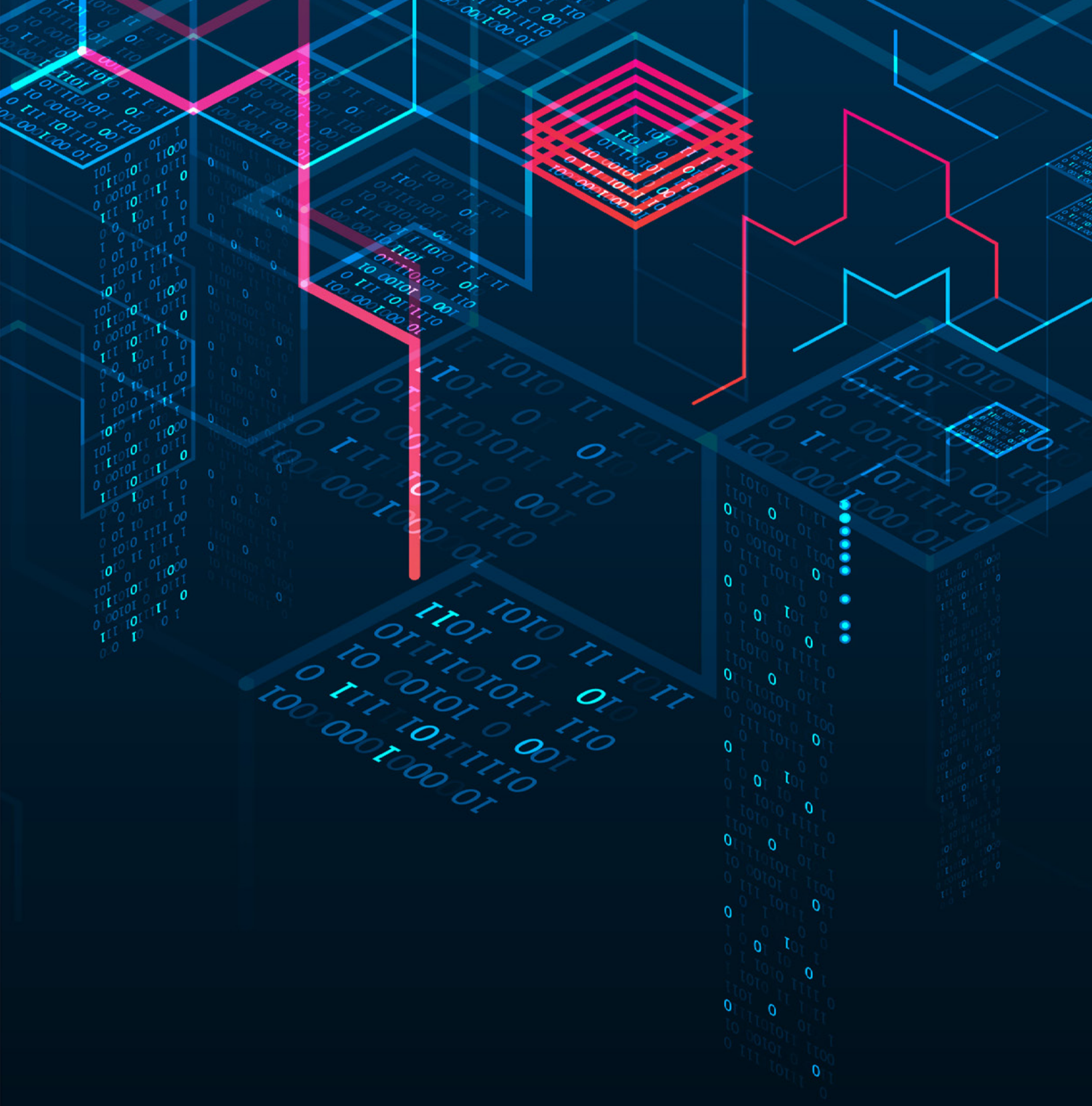
Join us for HIP Global 2021

DECEMBER 1-2

REGISTER →

Pamela Dingle
Direttrice del segmento
Identity Standards
presso Microsoft

“Messaggio per tutti coloro che non hanno implementato l’autenticazione multifattoriale (MFA): dovete mettere ordine nelle vostre priorità. Gli aggressori stanno trovando il modo di entrare nella vostra infrastruttura on-premise e quindi sfruttare il fatto che alcuni di voi hanno questa folle idea che gli utenti siano affidabili solo perché sono on-premise. Subire una violazione è complicato, costoso e dannoso. Non sto dicendo che implementare l’MFA non sia difficile, ma l’alternativa è estremamente problematica.”



semperis

semperis.com