Prepararsi per gli attacchi che puntano a un'eliminazione globale

Il panorama delle minacce è cambiato radicalmente. Sei preparato per i nuovi attacchi distruttivi?

Scritto da Brian Hymer, Strategic Systems Architect di Quest® Software, in collaborazione con Randy Franklin Smith, esperto di sicurezza di Windows e Active Directory

INTRODUZIONE

I professionisti di IT e sicurezza stanno da tempo affrontando minacce gravi. Da un lato abbiamo rischi come interruzioni di corrente, guasti hardware e catastrofi naturali. Dall'altro, abbiamo malintenzionati all'interno delle aziende e hacker esperti, armati fino ai denti con tecniche e strumenti innovativi per sfruttare le vulnerabilità e creare virus, malware e ransomware sempre più sofisticati.

Difendersi da queste minacce non è mai facile, ma perlomeno in passato i rischi erano limitati in maniera importante. Le minacce naturali sono generalmente contenute a livello geografico, quindi basta avere un backup del data center in un'altra area per disporre di una difesa efficace. Gli attacchi da parte di persone vere si concentrano quasi sempre su un obiettivo specifico: ottenere l'accesso ai dati per rubarli o rivenderli, oppure per crittografarli e chiederne un riscatto. I professionisti di IT, pertanto, sanno dare priorità alle strategie di protezione dei dati.

Tuttavia, le cose ultimamente sono peggiorate: sempre più attacchi cercano semplicemente di eliminare l'intera infrastruttura. Purtroppo, molte organizzazioni sono impreparate. Questo white paper esamina alcuni degli attacchi recenti più distruttivi, ne analizza velocità, ambito e metodologia ed esamina le strategie migliori per difendere l'organizzazione.

VELOCITÀ E POTENZA DEGLI ATTACCHI DISTRUTTIVI

Avrai senz'altro sentito questi nomi fantascientifici: NotPetya. Shamoon. Stuxnet. Olympic Destroyer. BlackEnergy. Destover. Wiper. Triton. Ma cos'è veramente accaduto in questi attacchi distruttivi? Per avere un senso di velocità e scala, e pertanto capire l'importanza di trovare subito una strategia adeguata, è importante analizzare alcuni incidenti recenti.

Stuxnet

Poco prima del 2010, Israele e Stati Uniti erano sempre più preoccupati dal programma nucleare dell'Iran: nel 2009, tale Paese produceva così tanto uranio arricchito da poter creare potenzialmente due armi nucleari all'anno. Si ritiene che, in risposta, Israele e Stati Uniti abbiano iniziato a sviluppare un sofisticato worm per computer, Stuxnet, progettato non per violare computer o rubare dati, ma per distruggerli fisicamente. Nello specifico, quando Stuxnet infetta un computer collegato a un controller di logica programmabile (PLC) specifico che controlla macchinari industriali come centrifughe di uranio,

infetta la programmazione del PLC per forzare una rotazione eccessivamente veloce delle centrifughe, oltre che per un periodo eccessivamente lungo, il tutto assicurandosi che i PLC non segnalino malfunzionamenti in modo che chi li monitora non noti nulla di strano. Nel tempo, questo sforzo provoca la rottura delle apparecchiature. Nel 2010, più di 15 stabilimenti in Iran erano infettati da Stuxnet, con danni per quasi un quinto delle centrifughe nucleari del paese.

Stuxnet non era mai stato pensato per espandersi al di là degli stabilimenti nucleari iraniani, isolati e non collegati a Internet. Tuttavia, in qualche modo il malware ha raggiunto Internet e ha iniziato a diffondersi. Nel tempo, altri gruppi hanno modificato il virus per attaccare altri tipi di organizzazioni, come impianti di trattamento acque, centrali elettriche, enti governativi e aziende nei settori aeronautico, farmaceutico e della difesa. Questi virus modificati, chiamati a volte "i figli di Stuxnet", includono Duqu, Flame, Havex, Industroyer e Triton.

Sempre più attacchi cercano semplicemente di distruggere completamente la tua infrastruttura. Troppe organizzazioni non sono preparate a sufficienza.

Shamoon

Nel 2012 è stata la volta di un'azienda petrolifera a subire un attacco informatico distruttivo. Il 15 agosto, un virus (successivamente chiamato Shamoon) ha infettato 3 quarti delle 40.000 workstation di Saudi Aramco, cancellando i dischi rigidi e visualizzando l'immagine di una bandiera statunitense in fiamme. Anche se l'azienda ha dichiarato che la produzione di petrolio e le attività di esplorazione non erano state interessate dall'attacco e che la rete interna principale era stata offline per soli dieci giorni, un consulente chiamato per le operazioni di ripristino segnalò che Saudi Aramco aveva dovuto ricreare da zero il centro per le operazioni di sicurezza e che ci sarebbero voluti cinque mesi per riportare online il sistema. Notò anche che l'attacco avrebbe potuto facilmente portare alla bancarotta un'azienda più piccola.

Shamoon è scomparso dalle prime pagine per quattro anni, ma nel 2016 una versione leggermente modificata del malware è stata usata contro più organizzazioni governative e civili in Arabia Saudita e altri paesi del Golfo. Il malware distruttivo si è ripresentato anche negli ultimi mesi del 2018, contro vari obiettivi in Medio Oriente. Questa nuova variante di Shamoon è ancora più distruttiva della precedente in quanto elimina tutti i file dai computer infetti prima di cancellare il record di avvio master, rendendo sostanzialmente impossibile recuperarli.

BlackEnergy

Il 2015 ha visto il primo attacco informatico riuscito a una rete elettrica. A dicembre, gli hacker hanno usato il malware BlackEnergy per introdursi in diversi centri di distribuzione elettrica in Ucraina e portare offline i relativi sistemi. Anche se questo attacco ha interessato solo circa 225.000 clienti ed è durato alcune ore, ha dimostrato la potenza del malware per rendere indisponibili infrastrutture critiche. Gli attacchi futuri ai fornitori di energia potrebbero essere ben più devastanti.

NotPetya

Ma è nel 2017 che probabilmente si è avuto l'attacco più costoso e diffuso. Un dirigente finanziario nella sede ucraina del gigante di spedizioni internazionali Maersk aveva di recente effettuato una richiesta di routine: aveva chiesto all'IT di installare una soluzione software di contabilità, M.E.Doc, su un singolo computer. Poiché M.E.Doc non era un'applicazione casuale ma di fatto quella usata da tutti coloro nel settore in Ucraina, l'IT ha acconsentito. Il 27 giugno, poi, i computer nella sede principale di Maersk hanno iniziato ad andare offline. Secondo gli investigatori, degli hacker pagati dallo stato avevano violato i server di aggiornamento di M.E.Doc e sfruttato una backdoor per rilasciare malware in tutte le aziende che utilizzano il software.

Nell'arco di poche ore, Maersk era nel caos. Tutti i 150 controller di dominio nel modo, ad eccezione di uno in Ghana che era fortunatamente offline al momento dell'attacco, erano offline. Per diversi giorni, i terminali di spedizione in tutto il mondo rimasero bloccati, con decine di migliaia di camion rimandati indietro e diversi container di beni deperibili senza refrigerazione. La pulizia ha interessato la ricostruzione di 4.000 server e 45.000 workstation. Un dirigente di Maersk ha riportato che NotPetya è costato all'azienda da 250 a 300 milioni di dollari, anche se altri fonti interne sospettano cifre ben più elevate.

Tuttavia i danni non si sono limitati a Maersk: NotPetya ha infettato aziende in tutto il mondo, dalla Germania agli Stati Uniti alla Tasmania, a velocità incredibili. Ci sono voluti solo 45 secondi a NotPetya per portare offline la rete di una banca ucraina di grandi dimensioni. Parte di uno dei principali hub di transito

ucraini è stata infettata completamente in soli 16 secondi. Praticamente ogni ente federale ucraino è stato paralizzato. Si stima che i danni totali ammontassero a oltre 10 miliardi di dollari.

Attacchi nel cloud.

Gli attacchi distruttivi non sono certo limitati solo agli ambienti IT locali, anche se non tutti gli incidenti nel cloud a oggi includono malware con nomi stravaganti. Ad esempio, nel 2014 il fornitore di IaaS Code Spaces è fallito dopo aver subito un attacco su più livelli ai propri server; la maggior parte dei dati, backup, configurazioni di macchine e backup fuori sito dell'azienda è stata parzialmente o completamente eliminata.

Più di recente, nel febbraio 2019, gli hacker hanno violato il fornitore di e-mail VFEmail e formattato tutti i dischi su ogni server di file e backup nella loro infrastruttura statunitense, distruggendo tutti i dati delle e-mail dei loro clienti USA. I criminali hanno anche provato a ottenere le risorse di IT aziendali localizzate nei Paesi Bassi, ma sono stati bloccati, cosa che ha permesso all'azienda di salvare alcuni dei dati di backup. In ogni caso, l'attacco ha sostanzialmente eliminato l'intera infrastruttura dell'azienda nell'arco di poche ore. Si prevedeva che l'azienda fallisse, ma tuttora sta operando anche se con numerose difficoltà.

I MOTIVI DIETRO GLI ATTACCHI DISTRUTTIVI

Gli attacchi tradizionali avevano tendenzialmente come motivazione ragioni finanziarie: ad esempio, ottenere un pagamento in cambio di una chiave di decrittazione in un attacco ransomware, l'ottenimento di informazioni confidenziali o sensibili da usare per furto di identità o rivendere sul mercato nero, oppure la raccolta di credenziali da usare in attacchi futuri per ottenere vantaggi economici. Gli attacchi distruttivi, generalmente, hanno una serie di motivazioni totalmente differente, tra cui le seguenti:

- **Motivi politici:** l'hacking da parte di stati è in aumento. Ad esempio, gli esperti ritengono che Stuxnet sia stato sviluppato congiuntamente da Stati Uniti e Israele per interrompere il programma nucleare dell'Iran, e che NotPetya sia stato un attacco politicizzato contro l'Ucraina. Alcuni ritengono che l'attacco di Shamoon nel 2012 sia stato parte di una ritorsione dell'Iran per il coinvolgimento degli Stati Uniti con Stuxnet. Gli attacchi hacker sponsorizzati dagli stati sono tipicamente altamente avanzati e finanziati, in modo da risultare particolarmente devastanti.
- **Motivi sociali:** alcuni attacchi hanno come desiderio un cambiamento sociale. Spesso chiamati "hacktivisti", questi gruppi utilizzano attacchi DoS (Denial of Service) contro organizzazioni che ritengono andare contro i loro ideali. Ad esempio, il gruppo hacktivista Anonymous è forse famoso ai più per la campagna DoS del 2010 che ha portato offline PayPal.com e interrotto i siti di Visa e MasterCard come ritorsione per i tagli ai servizi di Wikileaks operati da tali aziende, come richiesto dal governo statunitense.
- **Vendetta:** dall'altra parte, abbiamo i dipendenti interni insoddisfatti. Ad esempio, nel 2002 Roger Duronio, amministratore IT di UBS Paine Webber, ha a quanto si dice creato una "bomba logica", distribuendola in migliaia di sistemi con gli strumenti di amministrazione Unix standard. Poi si è licenziato ed è andato direttamente dal suo broker per piazzare 21.000 dollari sulla caduta delle azioni UBS/PW. Quando la bomba logica è esplosa alcune settimane dopo, ha portato offline circa 2.000 server ed eliminato tutti i file al loro interno. I danni sono stati così gravi che i dipendenti dovevano usare carta e penna per le operazioni di trading e di altro tipo. L'azienda ha speso 3 milioni di dollari solo in spese di consulenza per ripristinare i sistemi. La motivazione di Duronio? Aveva ricevuto un bonus di 18.000 dollari anziché di 50.000 come si aspettava.

  In un ambiente Windows è forse ancora più semplice per un utente insoddisfatto con privilegi causare danni: tutto ciò che devono fare è portare offline Active Directory. Se AD è offline, lo è anche l'intera rete, anche se non c'è niente che non vada su server e applicazioni.
- **Cortina di fumo:** spesso, gli hacker associano un attacco progettato per rubare informazioni con uno distruttivo per far perdere le proprie tracce. L'attacco distruttivo può rallentare le analisi forensi, rendendo difficile identificare i colpevoli., impedendo così che vengano denunciati e proteggendone il modus operandi in modo che possano continuare a usare le stesse tecniche in futuro. Ad esempio, il malware Olympic Destroyer ha paralizzato i sistemi IT prima delle cerimonie di apertura ufficiali delle Olimpiadi invernali del 2018 in Corea del Sud. Tuttavia, Olympic Destroyer ha coperto così efficacemente le proprie tracce che, quando in seguito nell'anno si è ripresentato, colpendo

NotPetya ha portato offline la rete di una grande banca ucraina in soli 45 secondi. I danni globali totali dell'attacco del 2017 sono stimati a oltre 10 miliardi di dollari.

organizzazioni finanziarie e biologiche e laboratori di prevenzione delle minacce chimiche, i ricercatori non erano sicuri che fosse usato dallo stesso gruppo o da un altro con interessi diversi.

- **Danni collaterali:** non tutte le vittime di attacchi distruttivi vengono puntate nello specifico, alcune sono semplicemente parte di danni collaterali. Ad esempio, gli architetti dell'attacco NotPetya avevano chiaramente l'Ucraina come obiettivo, una stima indica che circa l'80% delle infezioni ha avuto luogo in tale paese, ma anche aziende in tutto il mondo, inclusa Maersk, hanno avuto danni esponenziali.

METODOLOGIA

Come abbiamo visto, gli attacchi distruttivi hanno varie forme. Alcuni includono malware o virus, mentre altri si basano sulla forza bruta. Alcuni tentano di eliminare dati, mentre altri vogliono causare danni fisici. Diamo un'occhiata più da vicino al loro svolgimento.

Ogni organizzazione può essere vittima di un attacco distruttivo, anche solo di danni collaterali di un attacco che puntava ad altri obiettivi.

Accesso iniziale

Solitamente, il primo passaggio in un attacco è accedere alla rete. Probabilmente conosci le varie tecniche, come quelle indicate di seguito. È importante sottolineare come gli attacchi distruttivi non puntino solo ai computer come workstation e server, ma anche a dispositivi IoT, router e altro ancora.

- **Phishing:** Shamoon si è introdotto nella rete di Saudi Aramco quando un dipendente del team di IT ha aperto un'e-mail di phishing infetta.
- **Backdoor:** una backdoor nel software di aggiornamento di una soluzione aziendale di terze parti ha permesso ai criminali di rilasciare NotPetya in Maersk e altre organizzazioni nel mondo.
- **Dispositivo USB infetto:** poiché gli stabilimenti nucleari dell'Iran non erano collegati a Internet, Stuxnet è stato probabilmente introdotto tramite un dispositivo USB fisico, in maniera deliberata o accidentale.
- **Vulnerabilità software:** una tecnica usata nell'attacco NotPetya e nell'attacco ransomware WannaCry nel 2017 era l'uso di uno strumento di penetrazione noto come EternalBlue, creato dalla NSA statunitense ma diffuso in una violazione disastrosa. EternalBlue sfrutta una vulnerabilità in un protocollo Windows specifico per permettere agli hacker di eseguire da remoto il proprio codice su una macchina non aggiornata.
- **Violazione di Wi-Fi o trasmettitori:** nel 2015, i produttori della Jeep Cherokee hanno dovuto richiamare 1,4 milioni di veicoli dopo che i ricercatori hanno dimostrato che era possibile violare da remoto i sistemi dell'automobile via Internet; i criminali potevano prendere potenzialmente il controllo delle chiusure delle portiere, dei freni, del motore o delle funzioni di guida autonoma dei veicoli. In modo simile, la FDA ha confermato che alcuni dispositivi cardiaci impiantabili dispongono di vulnerabilità che permetterebbero a un hacker di far esaurire la batteria o fornire ritmi o shock errati.
- **Vulnerabilità nei dispositivi IoT:** nell'ottobre 2016, ha avuto luogo il più ampio attacco DDoS di sempre, che ha portato offline varie parti di Internet, inclusi Twitter, Netflix, Reddit e il sito della CNN, il tutto colpendo il provider di servizi Dyn. La botnet usata nell'attacco consisteva in un gran numero di dispositivi connessi a Internet, come stampanti, fotocamere digitali, baby monitor e router per privati, infettati da un malware chiamato Mirai.
- **Vulnerabilità in altri dispositivi:** cosa succederebbe se qualcuno reimpostasse tutti i tuoi router, firewall e punti di accesso wireless alle impostazioni di fabbrica o altre impostazioni? O se li violasseper i propri scopi? Nel 2018, l'FBI ha consigliato ai consumatori di riavviare i propri router per aiutare a interrompere la diffusione di un malware chiamato VPNFilter, che i ricercatori ritenevano fosse usato da un gruppo collegato all'intelligence militare russa per lanciare attacchi informatici coordinati contro l'Ucraina. Il malware è stato aggiornato da allora, ed è in grado di sopravvivere al riavvio; chiunque usi uno degli oltre 70 dispositivi vulnerabili deve ora aggiornare quanto prima il firmware.[1]

Diffusione e danni nella rete

Una volta che il malware si è introdotto, si diffonde dalla macchina infetta in altri computer nella rete. Una tecnica implica l'uso di una vulnerabilità chiamata Mimikatz, che permette agli hacker di raccogliere le credenziali presenti nella memoria di un computer e di usarle per accedere ad altre macchine. A volte, gli hacker vincono il jackpot se riescono a ottenere credenziali di amministratori oltre a quelle degli utenti ordinari.

1 Per altre informazioni, puoi leggere il rapporto iniziale di Cisco Talus su VPNFilter e il post di blog in cui viene aggiornato l'elenco dei dispositivi interessati. Tuttavia, assicurati di cercare le informazioni più aggiornate con il tuo motore di ricerca preferito o con altre opzioni di ricerca.

Nelle organizzazioni senza una segmentazione di rete vera e propria e altri limiti di sicurezza, il malware può diffondersi rapidamente e i criminali possono spostarsi dove vogliono con molta più facilità. Le tattiche di camuffamento, oltre alla mancanza di strumenti di monitoraggio e avvisi, permettono loro di non essere scoperti.

Ed è qui che avviene la parte principale di un attacco. Spesso, lo scopo è cancellare dati specifici o l'intero file system. Per cancellare i dati, alcuni attacchi sovrascrivono interi file, ma poiché è un'operazione che richiede tempo, altri attacchi invece prendono delle scorciatoie altrettanto efficaci. Ad esempio, un attacco può sovrascrivere un blocco di 500 byte ogni coppia di megabyte, o semplicemente sovrascrivere i primi N byte di un file, cosa che elimina le informazioni di intestazione. In ogni caso, la tecnica rende inutilizzabile il file anche se non viene cancellato del tutto. Esistono anche malware distruttivi che attaccano il BIOS e malware progettati per disabilitare dei servizi specifici.

Spesso, un attacco non viene avviato finché il malware non raggiunge la saturazione, per limitare la possibilità che una vittima se ne accorga in tempo per prendere provvedimenti. Per evitare una firma di I/O che potrebbe essere rilevata più facilmente, il malware spesso sposta la maggior parte del carico sul bootloader. Inoltre, gli attacchi vengono spesso effettuati con tempistiche precise in modo da massimizzare i danni; NotPetya e Shamoon sono stati rilasciati quando molti dipendenti non stavano lavorando a causa di ferie nazionali o religiose, limitando le possibilità di scovare tempestivamente l'attacco e le possibilità di intervento.

STRATEGIE DI PREVENZIONE E RILEVAMENTO

Poiché ogni organizzazione può essere obiettivo di un attacco distruttivo o anche solo di danni collaterali di un attacco indirizzato ad altri, è necessario prendere provvedimenti per mitigare i rischi. Il primo passo sta nell'implementare best practice di sicurezza standard che aiutino a impedire l'accesso alla rete da parte dei criminali, limitandone raggio d'azione e possibilità di spostamento in caso dovessero comunque riuscirci, in modo da scoprirne le attività. Ecco alcune delle strategie principali:

- Assegnare autorizzazioni strettamente in base al principio "meno autorizzazioni possibile".
- Usare un modello di sicurezza a livelli per separare gli utenti con privilegi da quelli aziendali normali, ad esempio Microsoft Enhanced Security Administrative Environment (ESAE), spesso chiamato modello "Red Forest".
- Non consentire l'esecuzione di codice non affidabile.
- Non eseguire software obsoleto e applicare sempre le patch.
- Valutare le modifiche all'ambiente e usare strumenti che permettano di impedire modifiche agli oggetti più critici, ad esempio i gruppi con privilegi elevati.
- Monitorare da vicino le modifiche a configurazione e ad altre parti del sistema e la presenza di operazioni non comuni, ad esempio comandi che potrebbero alterare le partizioni di avvio o bloccare un sistema.
- Monitorare l'attività degli utenti, specialmente degli account con privilegi. Idealmente, usare uno strumento che crei una baseline di attività normali, cerchi quelle non comuni e le analizzi nel contesto per ridurre al minimo gli avvisi falsi e scoprire rapidamente le minacce reali.
- Automatizzare gli interventi. Gli attacchi moderni hanno luogo in pochi secondi, perciò non può bastare una dashboard nel centro delle operazioni di sicurezza: nel tempo che ci impiega un essere umano a rilevare un problema, indagarlo e prendere provvedimenti, il danno è già stato fatto. Pertanto, automazione e orchestrazione della sicurezza sono essenziali.

STRATEGIE PER IL DISASTER RECOVERY

Racchiudere una protezione efficace e strategie di rilevamento è essenziale, ma non basta di certo. In molti degli attacchi descritti prima, le vittime sono state giustamente criticate per non aver implementato basi di sicurezza, ad esempio nell'attacco NotPetya del 2017 alcuni dei server di Maersk eseguivano ancora Windows 2000, che Microsoft ha cessato di supportare nel 2010. Inoltre, l'insufficiente segmentazione della rete di Maersk ha permesso al malware di diffondersi rapidamente in tutta la rete.

Tuttavia, è bene ricordare che Maersk non ha fatto nulla di sbagliato che abbia causato in sé l'infezione. Il malware è

Tecniche di protezione e rilevamento solide sono fondamentali ma non bastano: è anche necessario disporre di una strategia di disaster recovery completa.

stato rilasciato tramite un pacchetto software di contabilità standard, usato praticamente da ogni azienda in Ucraina. Varie organizzazioni hanno subito grossi danni nell'attacco e, come Maersk, la maggior parte di loro non era un obiettivo mirato ma era parte semplicemente dei danni collaterali.

La lezione è chiara: anche se l'organizzazione ritiene di non avere nemici e implementa tutte le best practice di sicurezza consigliate dagli esperti, non è possibile garantire che non diventi vittima di un attacco distruttivo. Pertanto, è fondamentale disporre di una strategia di disaster recovery comprovata e testata.

Maersk non l'aveva. Sono riusciti a salvarsi solo per pura fortuna. Quando NotPetya ha portato offline tutti i loro 150 controller di dominio, nessuno riusciva a trovare un backup. Se l'azienda non fosse riuscita a ripristinare i controller, sarebbe fallita. Tuttavia, grazie a un'interruzione locale di corrente, un controller di dominio in Ghana, l'unico, era offline al momento dell'attacco ed è stato la salvezza per l'azienda. Sfortunatamente, la larghezza di banda dell'ufficio in Ghana era così lenta che il caricamento del controller di dominio avrebbe impiegato gironi e nessuno lì aveva un visto britannico, pertanto il team di ripristino ha dovuto fare una sorta di "staffetta" per portare il macchinario di precisione nella sede in Regno Unito. Infine, però, sono riusciti a usare il macchinario per ricostruire gli altri controller di dominio.

Fare affidamento su una "strategia" di disaster recovery di fortuna come questa è uno scenario troppo comune e altrettanto rischioso. Come abbiamo visto, l'attacco a VFEmail ha quasi distrutto l'azienda; è riuscita a sopravvivere solo perché si sono salvati alcuni server di backup. Quest caso è particolarmente ironico, poiché il servizio era stato impostato in risposta al virus ILoveYou che si era diffuso via e-mail nel 2001, e uno dei punti cardine era la possibilità di rilevare spam e malware. Si tratta anche di un caso particolarmente triste poiché VFEmail ha subito vari attacchi DDoS gravi negli anni, non riuscendo mai a prenderli abbastanza sul serio.

Se sei vittima di un attacco catastrofico e disponi sono di strumenti nativi disponibili, devi essere preparato a un processo di ripristino delle foreste difficile, lungo e predisposto agli errori.

Strumenti nativi

Se sei vittima di un attacco catastrofico e disponi sono di strumenti nativi disponibili, devi essere preparato a un processo di ripristino delle foreste difficile, lungo e predisposto agli errori.

Poiché le foreste di AD sono complesse, con numerose interconnessioni tra controller di dominio, ripristinare una foresta di AD è difficoltoso. Tra le altre cose, è necessario:

- Ricostruire i servizi di AD
- Pulire i metadati
- Ristabilire i trust
- Reimpostare gli account
- Riavviare la replica

Tutte queste attività includono procedure complesse da completare correttamente: saltare anche un solo passaggio o effettuarli non in ordine può far fallire l'intero processo. Provare a completare manualmente un ripristino di foreste solo con strumenti nativi in caso di errori catastrofici con i piani alti che ti mettono sotto pressione è un lavoro che non fa gola a molti.

Per vedere da te quanto sia difficile, consulta la Guida al ripristino delle foreste di Active Directory di Microsoft, che offre un modello per ripristinare una foresta di Active Directory in caso di guasto ampio che rende tutti i controller di dominio impossibilitati a funzionare normalmente.[2] Ecco una panoramica dei passaggi generali dopo aver determinato la necessità del ripristino di una foresta:

1. **Determinare come ripristinare la foresta:** per prepararsi al ripristino, Microsoft consiglia di determinare prima la struttura della foresta corrente, identificare la funzione di ciascun controller di dominio e decidere quale ripristinare per ogni dominio e assicurarsi che tutti i controller scrivibili siano portati offline.

   Nota: secondo le stime di Microsoft, solo la lettura del passaggio di preparazione richiede 12 minuti; la descrizione di ogni sottopassaggio è lunga almeno una pagina.

2. **Eseguire il ripristino iniziale (un controller di dominio in ogni dominio):** a livello generale, i passaggi qui includono il ripristino del primo controller di dominio scrivibile in ogni dominio, il ricollegamento

2 La Guida al ripristino delle foreste di Active Directory di Microsoft è disponibile qui: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-guide.

di ogni controller scrivibile ripristinato alla rete e l'aggiunta del catalogo globale a un controller nel dominio radice della foresta.

Anche solo il completamento del primo passaggio (il ripristino del primo controller di dominio) richiede 13 sottopassaggi separati, alcuni dei quali a loro volta includono procedure in più passaggi documentate separatamente da Microsoft. Ad esempio è necessario creare una rete isolata, ottenere i ruoli master delle operazioni, aumentare i valori del pool RID disponibile e rimuovere i metadati di AD dai controller di dominio non ripristinati dal backup.

3. **Ridistribuire altri controller di dominio nella foresta:** una volta che si dispone di una foresta stabile con un controller per ogni dominio e un catalogo globale nella foresta, è possibile finalmente iniziare a ridistribuire gli altri controller di dominio nella foresta installando AD DS.

4. **Pulizia:** dopo aver ripristinato l'intera foresta, è necessario rendere di nuovo operative le applicazioni per utenti e line of business. Tra le altre cose, è necessario riconfigurare lo stesso DNS, e determinare quali modifiche potrebbero essere state effettuate dal momento del backup al momento dell'emergenza, quindi riapplicarle.

Oltre a essere complessi e particolarmente sensibili all'errore umano, questi passaggi possono anche richiedere molto tempo. Microsoft stessa riconosce che "la velocità del ripristino non è l'obiettivo primario" della guida. Le FAQ a corredo notano che è possibile effettuare i passaggi di ripristino della foresta tramite strumenti a riga di comando, pertanto è possibile scrivere script che aiutino ad automatizzare alcuni parti della procedura. Tuttavia, Microsoft avvisa di testare per bene gli script prima di usarli in un ripristino effettivo, e che è necessario aggiornarli ogni volta che si apportano modifiche all'ambiente di AD, ad esempio per aggiungere un nuovo dominio o anche un nuovo controller di dominio, oppure per aggiornare a una nuova versione di Active Directory.

Recovery Manager for AD – Disaster Recovery Edition

Fortunatamente esistono degli strumenti che automatizzano il ripristino delle foreste e procedure che permettono di far tornare operativa subito l'organizzazione, con meno sforzi richiesti e rischi. Quest® Recovery Manager for Active Directory – Disaster Recovery Edition ti aiuterà a implementare una strategia di backup e ripristino completa che ti permetta di ripristinare rapidamente in caso di emergenze a livello di oggetti e attributi, a livello di directory e a livello di sistema operativo in tutta la foresta di AD. Anzi, le funzionalità di ripristino automatizzato possono ridurre i tempi di ripristino di un'emergenza di AD a livello di controller di dominio fino al 95%.

Quest On Demand Recovery estende il backup e ripristino di AD a livello di oggetti e attributi al cloud, in modo da poter proteggere non solo gli ambienti locali ma anche le distribuzioni ibride. Con On Demand Recovery puoi eseguire un backup e ripristino rapido e sicuro di Azure AD e Office 365, vedere sia gli oggetti solo nel cloud che quelli sincronizzati con Azure AD Connect, eseguire rapporti di differenza tra backup di produzione e in tempo reale, oltre a effettuare ripristini coordinati in AD locale e Azure AD.

CONCLUSIONI

Gli attacchi distruttivi si diffondono sempre di più e i loro effetti possono essere devastanti. Ogni organizzazione è vulnerabile, che sia un obiettivo specifico o parte di danni collaterali. Dopo il devastante attacco a VFEmail, il CEO e fondatore Rick Romero ha scritto su Twitter: "Non avrei mai pensato che qualcuno avesse un tale interesse nei frutti del mio lavoro al punto da volerli distruggerli in tutto e per tutto". Non fare lo stesso errore.

Per ridurre i rischi, implementa best practice di sicurezza per bloccare gli attacchi, limitarne la portata e aiutare ad assicurare un rilevamento e una risposta tempestivi. Gli esperti di sicurezza e gli attacchi nel mondo reale fanno capire come sia necessaria anche una strategia completa di disaster recovery. Per ulteriori informazioni su come Recovery Manager for AD – Disaster Recovery Edition e On Demand Recovery possano aiutarti, visita quest.com/products/recovery-manager-for-active-directory-disaster-recovery-edition e quest.com/products/on-demand-recovery.

Implementa una strategia di backup e ripristino completa nel tuo ambiente ibrido con Quest Recovery Manager for AD e On Demand Recovery.

QUEST - L'AZIENDA

Quest propone soluzioni software per il mondo in continua evoluzione dell'IT aziendale. Ti aiutiamo a gestire le difficoltà causate dall'esplosione del volume dei dati, dall'espansione del cloud, dai datacenter ibridi, dalle minacce alla sicurezza e dai requisiti normativi. La nostra azienda fornisce, a livello mondiale, 130.000 aziende in 100 paesi, come il 95% di Fortune 500 e il 90% di Global 1000. Dal 1987, abbiamo costruito una linea di soluzioni che ora includono gestione database, protezione dei dati, gestione delle identità e degli accessi, della piattaforma Microsoft ed endpoint unificata. Con Quest, le organizzazioni dedicano meno tempo all'amministrazione di IT e più per l'innovazione aziendale. Per ulteriori informazioni, visitare www.quest.com.

Per qualsiasi domanda sul potenziale utilizzo di questo materiale, contattare:
www.quest.com