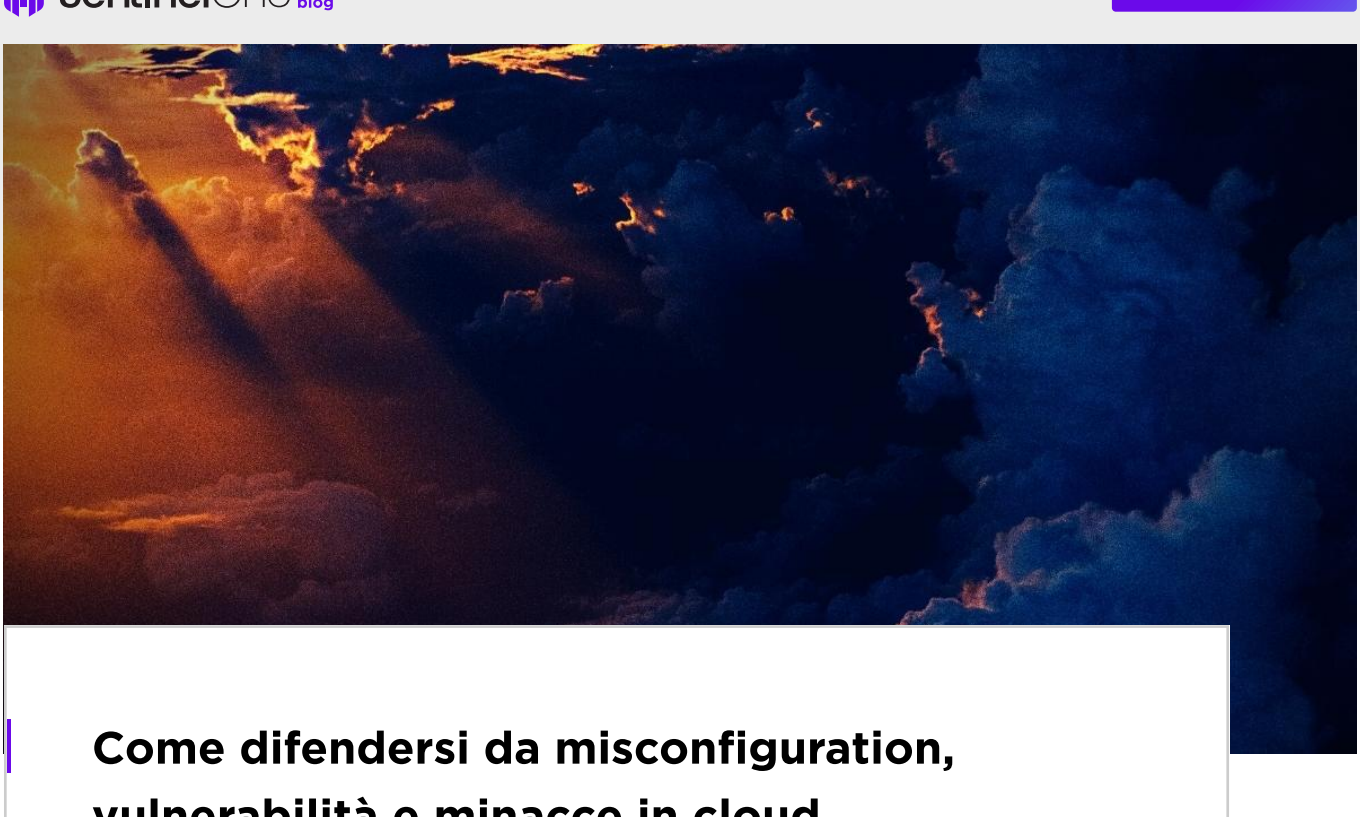


Come difendersi da misconfiguration, vulnerabilità e minacce in cloud

Luglio 5, 2022
by Marco Rottigni, Technical Director Italia di SentinelOne

Microsoft ha ampliato il portfolio di prodotti nell'ultimo decennio e, da fornitore di sistemi operativi si è trasformato in un'azienda che offre molteplici soluzioni che spaziano dalla produttività alla collaborazione e alle funzionalità in cloud. Le organizzazioni, sempre più si affidano a Microsoft 365 e Microsoft Azure per consolidare la gamma dei vendor adottati, spesso compromettendo le migliori funzionalità della categoria. Tuttavia, questo approccio ha introdotto rischi significativi per le organizzazioni, che restano eccessivamente legati a un unico software vendor.

Oggi tutti i servizi Microsoft dipendono da Azure Active Directory come soluzione primaria di Identity and Access Management (IAM), con la conseguenza che l'anello più debole dell'ambiente Microsoft è diventato l'identità dell'user. Quando un cyber criminale riesce a compromettere l'identità di un utente con privilegi elevati, come il ruolo di amministratore della sicurezza, può eludere tutte le misure di difesa e gli strumenti di sicurezza di Microsoft. In questo articolo analizzeremo come identificare e difendersi da alcune vulnerabilità comuni del cloud, dalle minacce interne e da pericolose configurazioni errate in cloud.

Vulnerabilità del cloud

I servizi cloud offrono alle aziende vantaggi significativi in termini di scalabilità e costi operativi. Proprio per questo anche gli hacker stanno spostando la loro attenzione per colpire direttamente i servizi cloud utilizzati da un'impresa.

Questa tendenza rappresenta una nuova sfida per le aziende che devono combattere la superficie di attacco di Windows già piuttosto ampia e che devono gestire anche l'aumento esponenziale delle vulnerabilità nei servizi cloud e di sicurezza.

I ricercatori di Proofpoint hanno scoperto che gli hacker possono attaccare Microsoft Office 365 a causa di un difetto di progettazione che consente loro di crittografare i file archiviati su SharePoint e OneDrive. in questo caso, il cyber criminale potrebbe creare un'applicazione web OAuth dannosa e attirare un utente affinché gli conceda le credenziali per autenticarsi con l'account indicato.

Nel 2021 i SentinelLabs hanno rivelato una vulnerabilità di privilege escalation in Windows Defender che era rimasta irrisolta per 12 anni. Nel 2022, è stato mostrato come Azure Defender for IoT contenesse diverse falle che interessavano i clienti cloud e on-premise e che consentivano l'esecuzione di codice remoto da parte di hacker non autenticati.

Nel frattempo, sono state scoperte numerose varianti di attacchi NTLM relay, per i quali Microsoft ha persino dichiarato che alcune avevano lo status di "non risolvibili".

A causa della visibilità spesso limitata degli ambienti cloud, molte organizzazioni faticano a proteggere efficacemente i loro dati o si affidano a Cloud Service Provider (CSP) per proteggere le loro istanze cloud. Secondo il rapporto IBM Data Breach, solo nel 2018 e nel 2019 sono stati esposti oltre 33 miliardi di record a causa di configurazioni errate i cloud.

Tipi di minacce interne

Il rapporto 2022 sulle minacce di Cybersecurity Insiders ha rilevato che gli incidenti interni sono diventati più frequenti negli ultimi 12 mesi. Tra questi si distinguono:

Insider imprudenti: sono persone che hanno accesso all'ambiente aziendale e possono provocare un attacco informatico attraverso un semplice e incauto errore. Potrebbe trattarsi di persone che non sono consapevoli delle problematiche informatiche e che, ad esempio, cadono in una trappola mirata di social engineering.

Insider malintenzionati: sono individui che accedono all'ambiente aziendale e supportano gli hacker, spesso in cambio di un guadagno monetario. Di recente un ex dipendente del governo canadese si è dichiarato colpevole di aver lavorato per un gruppo di ransomware responsabile dell'hacking degli ospedali durante la pandemia.

Configurazioni errate in cloud

Le aziende accelerano l'adozione di servizi cloud che facilitano la loro trasformazione digitale, ma nel fare ciò spesso dimenticano la sicurezza che non è responsabilità solo dei fornitori di servizi cloud (CSP), come molti credono. Di recente un fornitore di servizi VPN ha scoperto un'errata configurazione del cloud che può consentire agli aggressori di accedere ai dati sensibili archiviati negli account Blob di Microsoft Azure. Il Cloud Security Report 2022 di Check Point conferma che il 27% delle organizzazioni ha subito un incidente di sicurezza nella propria infrastruttura di public cloud, mentre il 23% di questi è stato causato da configurazioni errate in cloud.

Contromisure previste da Microsoft

Le ragioni per le quali gli ambienti Microsoft sono presi di mira sono tre: vulnerabilità, minacce interne e configurazioni errate del cloud. Il fattore comune è sempre la fragilità delle policy di sicurezza e il fronte delle identità. Non sorprende che Microsoft sostenga che il 99,9% delle compromissioni degli account può essere evitato con l'autenticazione a più fattori (MFA). Il problema è che solo il 22% dei clienti aziendali utilizza l'MFA e anche in questo caso l'implementazione di base è spesso insufficiente. Ad esempio, è stato recentemente scoperto come sfruttare una funzionalità integrata di WebView 2 per estrarre i cookie che consentono all'aggressore di bypassare l'autenticazione MFA.

Sono emersi nuovi rischi dal momento in cui molte imprese hanno spostato l'identità degli utenti da Active Directory on-premise a un'identità ibrida o cloud-native con Azure Active Directory (Azure AD). Ma quali sono i diversi ruoli di Azure AD e il suo rapporto con i servizi Microsoft? Oggi tutti i servizi Microsoft sfruttano Azure AD per gestire i controlli di accesso e, per aiutare a gestire i controlli di accesso, Microsoft offre diversi ruoli integrati che consentono all'utente di gestire le risorse Microsoft una volta assegnati.

"Global Administrator" è la funzionalità, integrata e protetta, che consente l'accesso completo a tutte le modalità dei servizi Microsoft. Tuttavia, Microsoft offre altre funzioni, come quella di "Security Administrator", che garantisce l'accesso completo a tutti i servizi di sicurezza Microsoft, compresi Microsoft 365 Defender, Microsoft Defender for Endpoint e Microsoft Sentinel, o quello di "Security Reader", che garantisce l'accesso in sola lettura ai prodotti di sicurezza Microsoft. Questi ruoli sono comunemente assegnati al team della sicurezza all'interno delle aziende. Anche se un'organizzazione utilizza il Role-Base-Access-Control (RBAC) in Microsoft 365 Defender o Microsoft Defender for Endpoint, qualsiasi identità utente compromessa con il privilegio di Security Administrator o Global Administrator sarà in grado di sovrascrivere i controlli di accesso e accedere alle console di gestione.

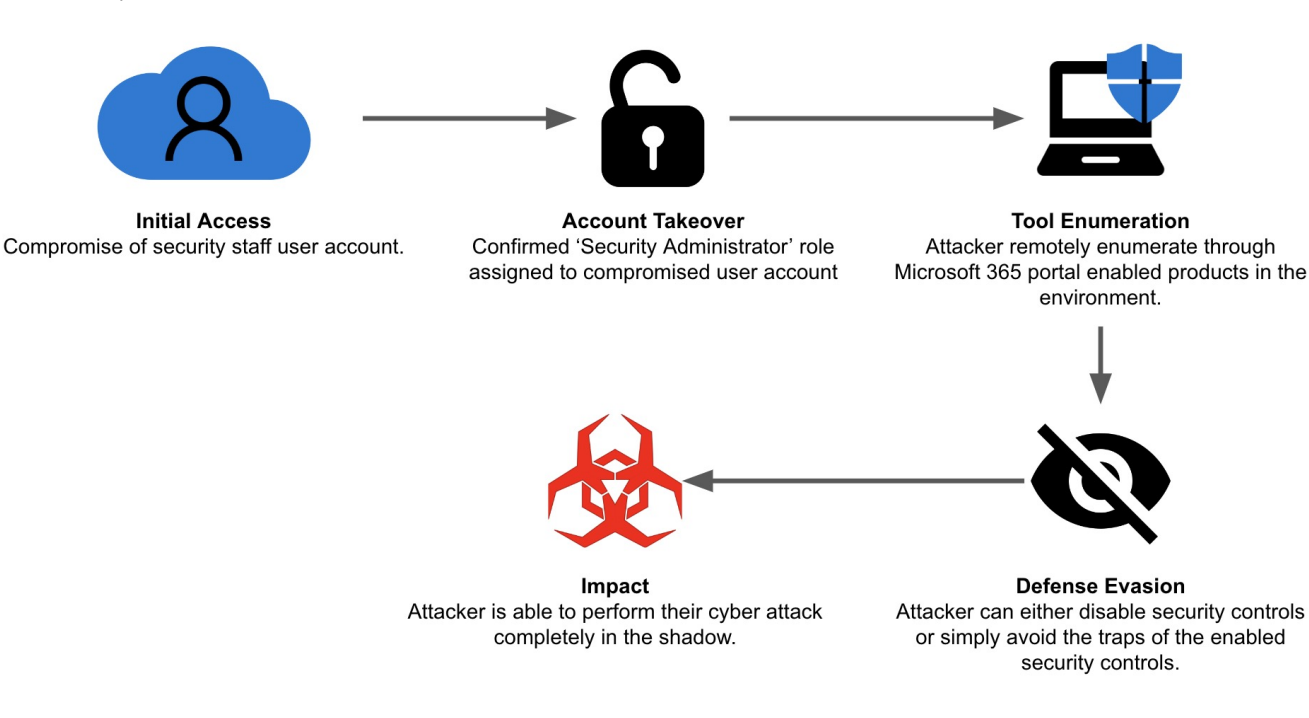
Microsoft è consapevole del fatto che queste funzioni possono causare rischi quando compromesse. Per questo motivo, Microsoft raccomanda l'utilizzo di funzionalità come Just-In-Time-Access e servizi più ampi di Privileged Identity Management (PIM). Tuttavia, come per l'MFA, solo poche organizzazioni aziendali utilizzano questi servizi a causa della complessa implementazione. Per coloro che non lo fanno, una volta che un cyber criminale riesce a compromettere un'identità utente con, ad esempio, i privilegi di amministratore della sicurezza, accede alla maggior parte dei servizi Microsoft, consentendo loro di eludere le funzionalità di sicurezza integrate.

Simulazioni di attacco

Esaminando alcuni possibili modelli di minaccia per un ambiente aziendale che utilizza Microsoft si distinguono:

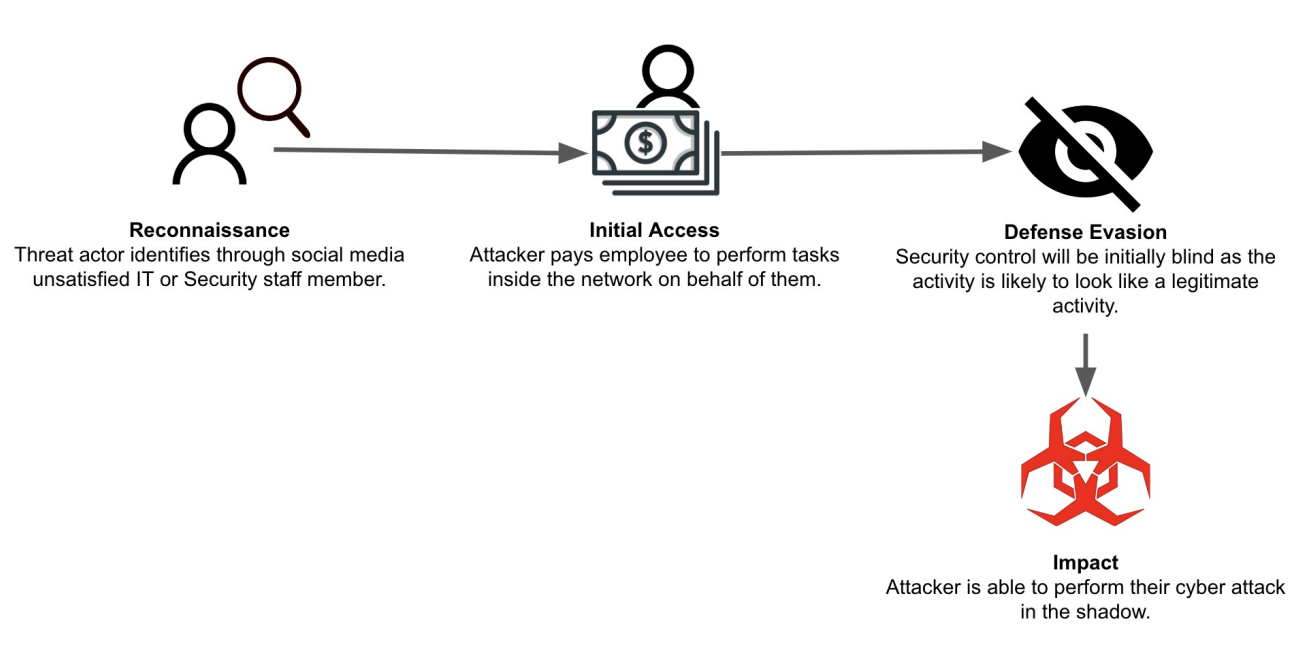
Attacco Identity-Based

l'azienda che prendiamo in esempio non dispone di autenticazione a più fattori (MFA), ha un modello Azure AD ibrido e utilizza Microsoft Defender for Endpoint. In questo caso, l'hacker compromette un'identità user del team di sicurezza, conferma che l'account user ha i privilegi di amministratore di sicurezza ed enumera attraverso il portale Microsoft 365 i controlli e i prodotti di sicurezza abilitati. I cybercriminali scelgono quindi se disattivarli o semplicemente evitarli. A causa della natura dell'attacco, Microsoft Defender for Endpoint è inefficace in quanto manca il contesto dell'identità dell'user.



Attacco Cloud-Based

l'azienda presa a esempio dispone di autenticazione MFA e gestione delle identità privilegiate (PIM) e di Microsoft Defender per le applicazioni cloud. In questo caso, l'hacker identifica uno o più dipendenti del team IT o di sicurezza e offre un compenso in denaro se questi eseguono determinate azioni all'interno della rete aziendale. Di conseguenza, dato che l'utente è all'interno della divisione IT o di sicurezza, i controlli di sicurezza abilitati molto probabilmente non avviseranno per l'attività sospetta.



Persone, processi e tecnologia da adottare

Come le organizzazioni possono ridurre il rischio di configurazioni errate nel cloud, di vulnerabilità nei prodotti Microsoft e di minacce interne? Per affrontare questa problematica, è essenziale comprendere i requisiti delle persone, dei processi e della tecnologia.

Persone

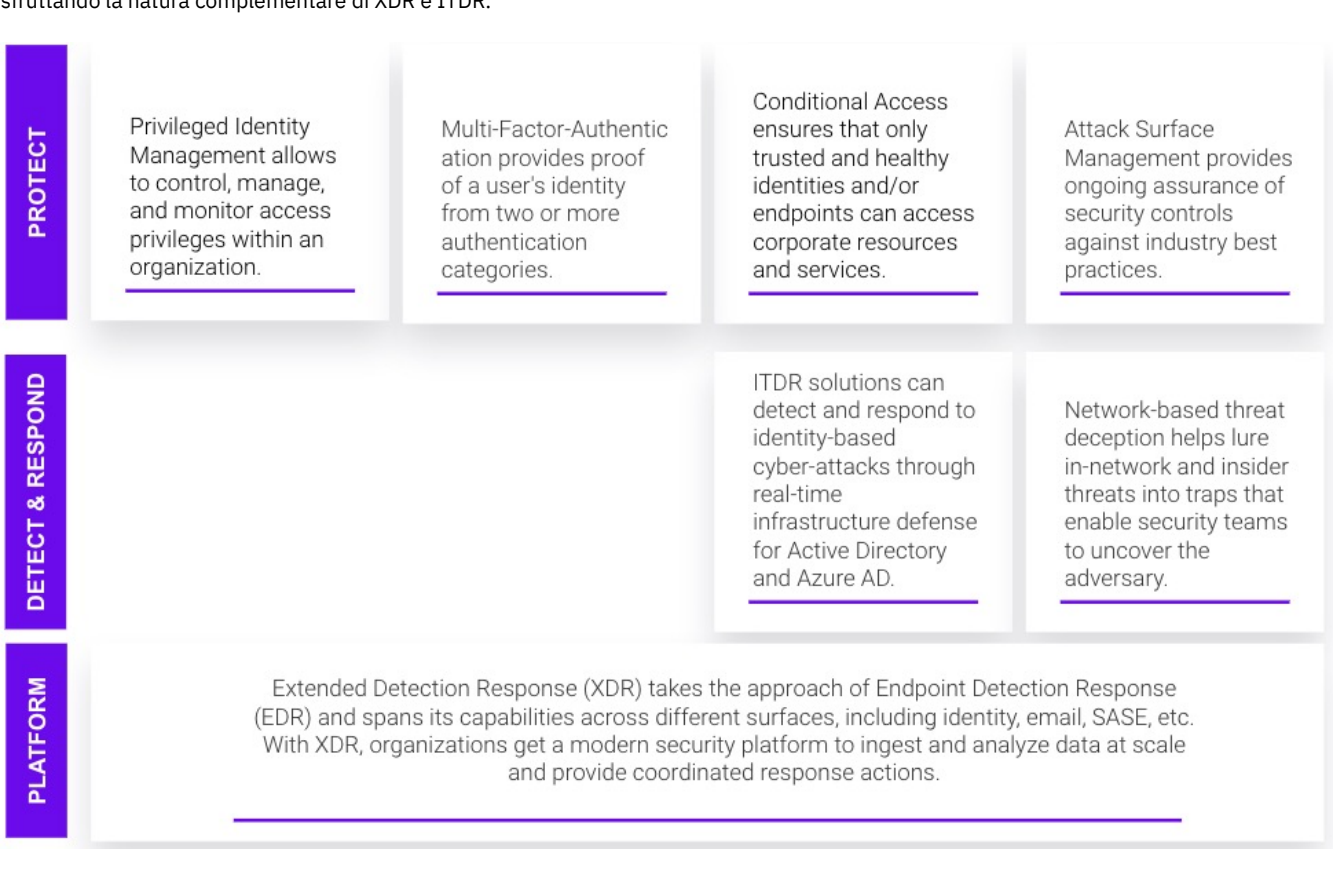
Secondo una ricerca di Mimecast, il 90% delle violazioni della sicurezza sono causate da errori umani: per questo motivo un efficace programma di sensibilizzazione alla sicurezza ridurrebbe il rischio che errori innocenti o incauti si traducano in un attacco informatico. Nessuno è immune dal commettere errori, per questo il modo in cui guidiamo la cultura interna della consapevolezza informatica è fondamentale. I dipendenti devono comprendere come possono contribuire alla sicurezza dell'azienda e segnalare le attività sospette.

Processi

L'utilizzo dei dispositivi da parte dei dipendenti non deve lasciare spazio alla libera interpretazione. Serve chiarire cosa i dipendenti possono o non possono fare e delineare i relativi controlli di sicurezza da effettuare. Ai dipendenti deve inoltre essere chiaro che devono segnalare prontamente eventuali incidenti di sicurezza e che questi vengano testati per garantire che il team di sicurezza possa identificare in anticipo i punti deboli.

Tecnologie

Secondo il Verizon 2022 Data Breach Investigation Report, il 61% di tutte le violazioni ha coinvolto le identità degli utenti. Non sorprende che oggi molte organizzazioni dispongano di 25-49 strumenti indipendenti, provenienti da 10 o più fornitori, per individuare o ricercare le minacce. Tuttavia, le organizzazioni che stanno valutando il consolidamento dei fornitori, sono alla ricerca di vendor di piattaforme che possano aiutarle in tutto il loro patrimonio digitale, piuttosto che concentrarsi su singoli silos. Per questo motivo, le aziende devono considerare l'integrazione di funzionalità di sicurezza in grado di rilevare, proteggere e rispondere alle minacce nell'intero patrimonio, sfruttando la natura complementare di XDR e ITDR.



Conclusioni

Comprendere i nuovi modelli di minaccia ed essere consapevoli che la protezione dei servizi cloud non è responsabilità esclusiva del CSP è diventato essenziale. E' importante guardare al quadro generale dell'ambiente aziendale e analizzare i rischi su diverse superfici (identità, e-mail, endpoint, rete) e identificare gli strumenti per proteggere, rilevare, rispondere e prevenire le minacce informatiche sull'intero patrimonio digitale.

Per ulteriori informazioni consultare it.sentinelone.com.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- 6 stereotipi sulla cybersecurity che ogni consiglio direttivo dovrebbe approfondire
- Status sulle minacce informatiche: le tecniche di attacco alle reti cloud
- Come anticipare gli hacker nel 2022: vademecum per la cybersecurity
- Difendere l'impresa nel 2022 dai rischi della Digital Supply Chain
- Come misurare l'efficacia dei controlli di sicurezza in 4 step
- SentinelOne indica le più grandi falsità sulla cybersecurity raccontate ai CISO