La prevenzione prima di tutto

Prevenire le minacce via e-mail

Perché la protezione nativa di Microsoft 365 e Google Workspace non è sufficiente

ESET Digital Security
Progress. Protected.

Lacune nella protezione delle e-mail

Tra i 3 miliardi di utenti di Google Workspace (compresi gli 1,8 miliardi di utenti attivi di Gmail), i 400 milioni di utenti di Outlook o i 320 milioni di utenti dell'app di collaborazione Microsoft Teams, tutti strumenti digitali essenziali, si contano certamente numerose aziende.

A seguito dell'implementazione e impostazione di alcune regole di sicurezza, gli ambienti di collaborazione aziendale dovrebbero in teoria essere sicuri, consentendo ai team di concentrarsi sul core business.

Tuttavia, non è sempre così. Sebbene **le minacce veicolate da applicazioni cloud apparentemente legittime** siano molto diffuse, vi si può porre rimedio attraverso l'implementazione di ulteriori livelli di sicurezza.

Avvalendosi di strumenti idonei, gli amministratori possono ridurre al minimo la superficie di attacco dei servizi cloud. L'approccio preventivo consente di proteggere le app di collaborazione aziendale e la posta elettronica a monte, prima ancora che le minacce siano eseguite nel sistema.

Tra le maggiori sfide che le aziende devono affrontare nell'ambito della sicurezza delle applicazioni cloud ci sono soprattutto le minacce legate alla posta elettronica:

PHISHING E SPEAR-PHISHING

Gli aggressori utilizzano metodi innovativi, come l'uso di codici QR o omoglifi, per indurre gli utenti a scansionare e/o cliccare su link apparentemente autentici.

IMPERSONIFICAZIONE E SPOOFING DELLE E-MAIL / COMPROMISSIONE DELLE E-MAIL AZIENDALI

Le e-mail ingannevoli, che tentano di indurre il destinatario a credere di interagire con un mittente legittimo, migliorano di giorno in giorno, soprattutto con i continui progressi dell'intelligenza artificiale.

FATTORE UMANO

I dipendenti commettono errori, rendendo i gateway di posta elettronica particolarmente interessanti per gli aggressori. I corsi di formazione sulla cybersecurity restano essenziali, poiché il fattore umano è tuttora l'anello più debole della catena e nessuna tecnologia può funzionare al 100% se non viene utilizzata correttamente.

MINACCE ZERO-DAY

L'intelligenza artificiale semplifica, tra l'altro, anche la creazione di minacce nuove o sconosciute.

E-mail: Il paradiso dei criminali informatici

La posta elettronica rimane il principale vettore di minacce informatiche. Negli ultimi anni, sono milioni le minacce rilevate e bloccate da ESET dopo che avevano aggirato la protezione nativa di Microsoft 365 e di Google Workspace.

La maggior parte delle minacce bloccate erano messaggi di phishing e spam. Secondo Verizon, il tempo medio che gli utenti impiegano per abboccare all'esca delle e-mail di phishing è inferiore a 60 secondi. Secondo il rapporto 2024 Data Breach Investigations, il cosiddetto pretexting è una delle tecniche di attacco più frequenti. Il numero di casi è quasi raddoppiato dal 2022 al 2023 e attualmente il pretexting si osserva in circa il 20% di tutti gli attacchi a sfondo finanziario. La maggior parte degli incidenti di pretexting è stata causata dalla compromissione di e-mail aziendali, con un importo medio della transazione di circa 50.000 dollari secondo il dataset IC3 dell'FBI. I dati più recenti mostrano che questa tendenza non accenna a diminuire.

Secondo il rapporto sulle minacce H2 2024 di ESET, il rilevamento dello spam è aumentato del 19% e i file HTML dannosi, che indirizzano le vittime su siti web di phishing (trojan HTML/Phishing.Agent), sono tuttora la minaccia e-mail più diffusa. Nel complesso, questi **attacchi via e-mail rappresentano quasi un quarto (23,8%) di tutte le minacce informatiche** rilevate da ESET. Tra le minacce cloud rilevate dalla telemetria ESET vi sono inoltre vari tipi di malware, come backdoor, spyware, infostealer e downloader.

Più pericoli di quanto si pensi

Sebbene sia Microsoft che Google abbiano incorporato sistemi di sicurezza high-tech direttamente nelle loro applicazioni cloud, costantemente protette e aggiornate, ciò non significa che siano immuni da tutte le minacce in circolazione.

Esempi reali dimostrano che le applicazioni e i servizi cloud autentici possono essere sfruttati per diffondere malware, camuffare processi dannosi e consentire l'accesso remoto ai dispositivi aziendali:

- I ricercatori di ESET hanno individuato nuove campagne di phishing di origine sconosciuta, rivolte negli ultimi anni contro le aziende in Europa. Le e-mail contenevano allegati dannosi potenziati da AceCryptor, un malware cryptor-as-a-service progettato per nascondere altri malware agli strumenti di cybersecurity. In caso di successo, gli aggressori possono utilizzare lo strumento di accesso remoto di Rescoms (noto anche come Remcos) per spiare le loro vittime.

- Nella seconda metà del 2024, **Formbook, un infostealer** scoperto per la prima volta nel 2016, ha registrato una significativa rinascita, con un aumento dei rilevamenti di oltre il 200%. Questo malware raccoglie, tra l'altro, dati degli appunti, sequenze di tasti, screenshot e dati del browser memorizzati nella cache. Si tratta di una soluzione malware-as-a-service (MaaS), venduta su forum clandestini, che si diffonde tramite allegati malevoli nelle e-mail di phishing. I prodotti ESET hanno protetto quasi 34.000 utenti da questo malware soprattutto nell'Europa orientale e centrale, oltre che in Giappone, Canada e Spagna.

- Fortunatamente, nella maggior parte dei casi, i professionisti della sicurezza informatica scoprono le vulnerabilità prima degli attori delle minacce. Nel giugno 2023, il Red Team di Jumpsec, fornitore di servizi di sicurezza con sede nel Regno Unito, ha scoperto e poi dimostrato un modo per distribuire malware utilizzando Microsoft Teams tramite un account esterno all'organizzazione bersaglio. Il team di Jumpsec ha **aggirato la protezione integrata** ed è riuscito a ingannare il sistema, facendogli credere che l'utente esterno fosse un account interno.

ESET, fornitore leader di cybersecurity, impiega ESET Cloud Office Security per proteggere gli ambienti di collaborazione basati sul cloud.

Questa soluzione avanzata potenzia le funzioni di sicurezza integrate di Microsoft 365 e Google Workspace eseguendo scansioni dopo che i prodotti cloud office nativi hanno contrassegnato le e-mail o i file come "sicuri".

I seguenti dati* di ESET mostrano quante minacce sono riuscite a superare le difese native.

920.000
minacce via e-mail rilevate

813.000
e-mail di phishing bloccate

110.000
minacce non provenienti da e-mail che arrivano da OneDrive, SharePoint e Google Drive

75.820.000
e-mail di spam bloccate

*dati del 2024

Come migliorare le difese del cloud

È chiaro che da sola la sicurezza nativa delle applicazioni cloud non è sufficiente. Per ridurre al minimo la superficie di attacco in continua crescita, prevenendo e mitigando gli attacchi prima che possano causare danni, le aziende dovrebbero cercare di potenziare i controlli integrati di Microsoft o Google con **ulteriori livelli di protezione:**

Filtraggio dello spam

I messaggi di spam rappresentavano oltre il 46,8% dei 362 miliardi di e-mail inviate e ricevute quotidianamente nel mondo nel 2024. Con la giusta soluzione di filtraggio, le aziende possono risparmiare molto tempo ai dipendenti ed evitare problemi causati dallo spam dannoso.

Anti-phishing

Nel 2024, il phishing è stato identificato come il vettore di attacco iniziale nel 22% dei cyberattacchi subiti dalle aziende statunitensi. È assolutamente fondamentale disporre di uno strumento automatico che riconosca i link di phishing allegati alle e-mail.

Scansione antimalware

Una buona soluzione di sicurezza cloud dovrebbe eseguire automaticamente la scansione di tutti i file nuovi e modificati nello storage condiviso per impedire l'esecuzione o la diffusione di malware.

Analisi comportamentale e ambiente sandbox

Data la continua introduzione di nuove minacce, gli strumenti di cybersecurity automatizzati devono essere preparati ad affrontare attacchi mai visti prima. A tal fine è utile compiere un'analisi comportamentale approfondita dei campioni sospetti in un ambiente sandbox isolato e sicuro.

Anti-spoofing e rule engine

È necessario bloccare le e-mail avverse che mascherano la propria identità spacciandosi per un mittente legittimo. Con questo controllo, solo le e-mail che sembrano provenire da fonti affidabili sono effettivamente consentite.

Protezione dagli omoglifi

Gli aggressori utilizzano caratteri simili per creare indirizzi e-mail o domini ingannevoli che sembrano autentici. Il rilevamento e il blocco di questi attacchi omografi aiuta a prevenire lo spear-phishing e altre attività dannose, garantendo la sicurezza delle comunicazioni aziendali.

Email Clawback

Questa funzione migliora la sicurezza consentendo agli amministratori di mettere in quarantena le e-mail direttamente dal registro di scansione. In questo modo, l'e-mail esce dalla casella di posta del destinatario, consentendo un'azione immediata in caso di sospetto attacco come lo spear-phishing.

Cosa fa ESET

Avere a disposizione così tanti strumenti e gestire un solido sistema di sicurezza può sembrare una sfida qualsiasi, ma la messa in campo di una sicurezza aggiuntiva non deve necessariamente aumentare la complessità del lavoro di un amministratore IT.

ESET Cloud Office Security offre una protezione preventiva avanzata per le app di Microsoft 365 e Google Workspace con tutte le caratteristiche sopra menzionate. Migliora la sicurezza aziendale con una protezione avanzata dalle minacce, oltre alla visibilità e al controllo di e-mail, condivisione di file e strumenti di collaborazione e dati basati sul cloud. Oltre a semplificare le operazioni e a migliorare la sicurezza, ESET Cloud Office Security contribuisce a **ridurre la complessità centralizzando e automatizzando i processi di routine**:

- I nuovi utenti all'interno dell'ambiente aziendale non devono essere aggiunti manualmente da un amministratore IT in una console, ma vengono protetti automaticamente dopo la creazione del loro account.
- Gli amministratori IT possono impostare intervalli di notifica per evitare che gli avvisi più importanti siano erroneamente trascurati, data la grande mole di segnalazioni irrilevanti.
- I file sospetti possono essere facilmente gestiti in quarantena a livello centralizzato, con la possibilità di autorizzarli/eliminarli o di compiere ulteriori indagini, se necessario.
- La soluzione consente la gestione multi-tenant per decine di migliaia di utenti di account creati all'interno delle due piattaforme più utilizzate, Microsoft 365 e Google Workspace.

Concentrandosi in particolare sugli utenti finali e sui loro dispositivi, ESET Cloud Office Security garantisce livelli più elevati di protezione per le aziende riducendo al minimo le superfici di attacco legate al cloud, alleggerendo così il carico degli amministratori IT con una console di gestione in cloud di facile utilizzo.

Come soluzione indipendente o componente della piattaforma ESET PROTECT, ESET Cloud Office Security rafforza la protezione antivirus, riduce al minimo le interruzioni del lavoro dovute a messaggi indesiderati e aiuta a prevenire attacchi mirati e tipi di minacce mai viste prima, in particolare il ransomware.

INTEGRAZIONE

Infine, ESET Cloud Office Security offre il vantaggio dell'integrazione gratuita con **ESET LiveGuard Advanced**, una tecnologia basata sul cloud che utilizza scansioni avanzate, AI all'avanguardia, sandboxing nel cloud e analisi comportamentale approfondita per prevenire attacchi mirati e minacce nuove o sconosciute, tra cui il ransomware.

ESET

Difesa proattiva. Il nostro obiettivo è ridurre al minimo la superficie di attacco.

Rimanete un passo avanti rispetto alle minacce informatiche note ed emergenti con il nostro **approccio prevention-first**, **basato sull'intelligenza artificiale e sull'esperienza umana**.

Avvalendovi del nostro supporto beneficiate di una protezione best-in-class, basata su un'**intelligence interna sulle minacce informatiche** globali maturata in oltre 30 anni all'interno della nostra rete di ricerca e sviluppo sotto la guida di **ricercatori rinomati nel settore**. ESET protegge la vostra azienda per consentirvi di sfruttare appieno il potenziale della tecnologia.

ESPLORA

Tecnologia multilivello

L'Intelligenza Artificiale incontra l'esperienza umana

In prima linea nella ricerca sulla cybersecurity

Assistenza personalizzata e locale

Digital Security
Progress. Protected.