Struttura di una mail, Email secure gateway e relativo mail flow

Struttura di un'email

Come si può evincere dalla figura 8, ogni mail ha le seguenti componenti:

- **Connessioni**: da quale mail server (e relativo IP) è inviata la mail, quali eventuali "relay" ha attraversato e qual è il mail server destinatario. Di seguito alcuni esempi relativi alle connessioni:
    - **Sender HELO Domain**, informazione utilizzata per avviare una connessione SMTP e relativa conversazione con un altro mail server.
    - **Sender IP**
    - **Sender hostname**
- "**Envelope Information**": sono tutte quelle informazioni che possono essere utilizzate per filtrare le conversazioni a livello di mail server tra cui:
    - **Envelope sender**, ovvero, il reale mittente della mail. Questi potrebbe non combaciare con **l'header from**, il nome che il destinatario vedrà quando riceverà la mail. Quando queste due informazioni non combaciano c'è la possibilità che vi sia un potenziale tentativo di spoofing
    - **Envelope Recipient**.
- **Body**, tutto ciò che viene scritto e inserito all'interno di una mail tra cui: testo, URL ed eventuali allegati ma anche informazioni relative alla dimensione del messaggio.
- **"Header information"**: riguarda tutte le informazioni relative a **From, To, Date, Subject** e **Reply-To** di

un’email. I threat actors possono facilmente spoofare queste informazioni. È fondamentale che chiunque riceva mail sospette riesca a riconoscerle segnalandole prontamente ai team dedicati che procederanno poi con ulteriori analisi e relativi filtraggi.



Figura 8. Struttura di una mail

Email secure gateway e relativo mail flow

Ogni volta che si invia una mail ci sono diversi step, si veda la figura 9, che vengono effettuati. Di seguito verrà illustrato un classico invio di una mail da un sender verso un recipient:

1. Il sender invia un messaggio al recipient. Il mail server, una volta compreso che il recipient è esterno all’organizzazione, procederà col contattare il “**message trasfer agent**” (**MTA**), ovvero il mail server responsabile dello smistamento da un server a un altro della posta elettronica, per la gestione della richiesta.
2. Il sending MTA effettuerà una query DNS per ottenere tramite **l’MX** (**mail exchange**) record, ovvero il responsabile della ricezione dei messaggi indirizzati a una casella di posta elettronica, informazioni per indirizzare la mail verso il destinatario. L’MX specificherà quindi il mail server autorizzato ad accettare il messaggio inviato.
3. A questo punto il sending MTA, utilizzando le informazioni ottenute dall’MX, contatterà l’MTA del recipent per stabilire una connessione. Come si evince dalla figura 9, il recipient utilizza un email secure gateway per proteggere il proprio servizio di posta e per gestire tutti i tentativi di connessione, il sistema è anche noto come **protection server**.
4. Il protection server processerà quindi il messaggio in inbound, verificando ad esempio:

- Che il sender non sia in una blacklist/whitelist.
- Che non ci siano filtri configurati che possano bloccare la mail.
- Che la mail non contenga allegati e/o URL malevoli.
- Che i record SPF, DKIM e DMARC siano correttamente configurati.

E molte altre azioni che varieranno a seconda del vendor utilizzato.

5. Una volta completata l'analisi, il protection server classificherà la mail (spam, phishing ecc.) e se non malevola, e conseguentemente considerata legittima, procedendo quindi con l'invio al mail server del recipient che consegnerà infine la mail al destinatario.



Figura 9. Mail flow

Un **email secure gateway**, quindi, protegge le comunicazioni che avvengono tramite posta elettronica da minacce come malware, phishing, spam e simili. Di seguito alcune delle principali funzionalità:

- **Categorizzazione delle mail**: il gateway esamina tutti i messaggi in arrivo per identificare e bloccare le email indesiderate, come spam e phishing. Questo processo coinvolge l'analisi delle connessioni della mail, degli header e di eventuali URL e/o allegati per individuare potenziali minacce. Ogni mail avrà un determinato score (tipicamente da 0 a 100) e una tipologia (spam_score, phishing_score ecc) che le verrà assegnata al termine dell'analisi. In base a questo score il secure gateway procederà con una determinata azione (consegna, quarantena ecc).
- Gestione di **blacklist** e **whitelist** (note anche come **blocklist** e **passlist**). All'interno delle blacklist vengono inseriti tutti quei sender/domini/IP che sono

classificati come malevoli. Viceversa, nelle whitelist verrà inserito tuttò ciò che è considerato legittimo. Si tenga presente che inserire un sender in whitelist può esporre l'azienda a potenziali attacchi in quanto quel particolare indirizzo (mail o anche IP) verrà considerato come non malevolo anche in caso di compromissione. Inoltre, i sender in whitelist tipicamente non sono sottoposti ad alcun tipo di controllo da parte dell'antispam. Si consiglia pertanto di maneggiare le whitelist con cura ed eventualmente monitorarle periodicamente prediligendo maggiormente l'uso delle blacklist (metodologia considerata più sicura).

- **Antivirus** e **antimalware** per rilevare e bloccare malware presenti negli allegati delle email impedendo che i file malevoli raggiungano il destinatario. In alcuni casi il secure gateway supporta anche l'uso di **sandbox** per l'esecuzione degli allegati così che possa verificare se effettivamente sono malevoli o comunque effettuano comportamenti inattesi e/o sospetti.
- **Rewriting** degli **URL**: questa funzionalità riscrive tutti gli URL e analizza i link presenti nelle email una volta cliccati verificando se conducono a siti web dannosi o phishing o se vengono effettuate connessioni malevole. Se il link è sospetto, il gateway potrà quindi bloccare l'azione intrapresa per evitare l'infezione della macchina o comunque azioni nel sito sospetto.
- **Analisi comportamentale** per rilevare modelli di comportamento anomalo, aiutando a identificare attività sospette o attacchi avanzati. Può osservare, analizzare e filtrare, ad esempio, se vi è un massivo invio di mail e/o documenti verso l'esterno tramite email bloccando prontamente una potenziale esfiltrazione.
- **Gestione delle mail in outbound**, ad esempio, tramite regole che definiscono la dimensione massima di una mail in uscita verso un recipient esterno (o anche interno al perimetro di monitoraggio). Così facendo si limiterà la

quantità di documenti inviata verso l'esterno e si invoglierà l'uso di strumenti più sicuri per la condivisione di materiale sensibile e/o riservato evitando così una potenziale esfiltrazione di dati tramite mail.

- Verifica e controllo dei record **SPF, DKIM e DMARC**.
- Segnalazione della mail quarantenate, agli utenti abilitati, tramite strumenti come il **digest** così da consentire eventualmente all'utente di richiederne la rimozione al team di competenza.
- Gestione e supporto di **campagne awareness**: in questi casi si costruiscono delle campagne mail "malevole" ad hoc per comprendere quanto l'azienda è suscettibile a campagne di spam/phishing e quali sono gli utenti con minor sensibilità sulla tematica. L'obiettivo sarà quello di sensibilizzare i dipendenti verso tale tematica inducendoli a trattare le mail con la dovuta attenzione e a segnalare ogni mail malevola tramite l'apposito canale interno al team di competenza. Queste campagne sono quindi, dei veri e propri training per i dipendenti.
- **Reportistica** e **monitoraggio** per consentire agli amministratori di sistema di tenere traccia delle attività e delle minacce consentendogli anche di rispondere rapidamente a eventuali incidenti di sicurezza. Queste servono anche a comprendere se l'azienda è stata presa di mira da eventuali hackers e/o coinvolta in delle campagne malevole.

Di seguito alcuni dei principali vendor nel campo dell'email security:

- Microsoft O365
- Proofpoint Email Security
- Darktrace Antigena Mail
- Cisco Email Security
- Barracuda Email Security Gateway

- FireEye Email Security

Prima di scegliere una soluzione, è importante valutare le specifiche esigenze dell'organizzazione, tenendo conto di fattori come le dimensioni dell'azienda, il livello di protezione richiesto e il budget disponibile. Ogni fornitore ha le proprie caratteristiche e funzionalità uniche, quindi la scelta dipenderà dalle esigenze specifiche richieste.

Questo articolo è stato estratto dal white paper "Email Security: Intelligenza Artificiale, Protocolli e Best Practice Contro gli Attacchi Informatici" disponibile in maniera libera e gratuita al seguente link: https://www.ictsecuritymagazine.com/pubblicazioni/email-security-intelligenza-artificiale-protocolli-e-best-practice-contro-gli-attacchi-informatici/

Articolo a cura di **Fabrizio Giorgione**

Profilo Autore

Fabrizio Giorgione è nato a Napoli (NA) nel 1992. Si è laureato in ingegneria informatica presso l'università degli studi del Sannio il 17 dicembre del 2018 con una tesi dal titolo: "Analisi della superficie di un sistema SCADA". Ha sviluppato, presso il laboratorio ISWATlab, un'applicazione Android denominata "Privacy Guard" la quale valuta il rischio di privacy leakage, ovvero il furto di informazioni, sugli smartphone (http://www.iswatlab.eu/?page_id=499). Ha effettuato il tirocinio presso lo "ZLab" di "Cse Cyber Sec" nell'ambito "SOC", "Forensic" e "Malware Analysis". Attualmente lavora presso la società di "NTT DATA" come "Cyber security Analyst" nel SOC di Napoli. Il suo compito è quello di effettuare analisi di log, di malware e di prevenire minacce interne ed esterne alla sua azienda e ai clienti della società. Si è occupato, inoltre, del montaggio e della

gestione di sonde IDS/IPS presso Telecom Italia nella sede di Roma (RM).

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/struttura-di-una-mail-email-secure-gateway-e-relativo-mail-flow/