

RELAZIONE

DMZ

La DMZ, o "zona demilitarizzata", è una parte di rete per l'accesso a servizi come lo shopping online e la webmail. È cruciale proteggerla con firewall, proxy e altri dispositivi per garantire la sicurezza dei dati aziendali. Questo approccio a più livelli migliora significativamente la sicurezza complessiva della rete.

WAF

Un Web Application Firewall (WAF) protegge le applicazioni web filtrando il traffico HTTP/HTTPS per prevenire attacchi come malware, SQL injection, cross-site scripting e file inclusion tra l'applicazione e l'utente finale.

COME FUNZIONA IL WAF

1. *Ispezione del Contenuto*: Il WAF ispeziona il contenuto dei file caricati e dei dati inviati al server
2. *Analisi delle Regole*: Identifica pattern sospetti nei file caricati tramite regole preconfigurate per script PHP e eseguibili.
3. *Rilevamento dell'Attacco*: Riconosce che il file caricato contiene codice potenzialmente dannoso.

IPS

Un IPS è un sistema di sicurezza informatica che, a differenza di un IDS, non solo rileva attività sospette o intrusioni, ma può anche intraprendere azioni attive per bloccare o prevenire tali attacchi. L'IPS opera in tempo reale per interrompere immediatamente l'attività dannosa o indesiderata. Va oltre il semplice rilevamento e può agire in modo proattivo per fermare un attacco, bloccando traffico sospetto, disconnettendo utenti o inviando notifiche di allarme. L'obiettivo principale è prevenire danni causati dagli attacchi informatici, ma è importante evitare falsi positivi configurando attentamente l'IPS.

IDS

Un IDS rileva attacchi informatici analizzando il traffico di rete o i log di sistema, segnalando comportamenti anomali o violazioni delle policy. Non interviene direttamente per fermare gli attacchi, ma genera avvisi agli amministratori di sicurezza per consentire interventi appropriati.

FIREWALL

Un componente fondamentale nella sicurezza informatica è il firewall, un dispositivo o software progettato per proteggere una rete o sistema controllando il traffico in entrata e in uscita. Funge da guardiano tra la rete interna e il mondo esterno, decidendo se permettere o bloccare il passaggio dei dati in base a regole predefinite.

NAS

Il network-attached storage (NAS) è un dispositivo di archiviazione dedicato ai file che rende i dati sempre disponibili ai dipendenti per collaborare in maniera efficace in una rete. Qualsiasi rete informatica ha server interconnessi e computer client che inviano richieste ai server.