

Noi della Squirtle Squad abbiamo ideato la struttura informatica in questione sotto la richiesta del committente Theta per prevenire criticità nell'ambiente lavorativo in caso di eventuali attacchi o violazioni. Ci è stato richiesto di rendere sicuri i punti critici della loro rete composta da un server interno (Application Server e-commerce) ed un Web Server (con la capacità di connettersi ad internet ergo una rete accessibile dall'esterno).

Il Web Server espone più servizi su internet e lo rende accessibile dall'esterno ed abbiamo aggiunto un WAF (Web Application Firewall), è una soluzione progettata per proteggere le applicazioni web da eventuali minacce. Monitora, filtra e blocca il traffico di informazioni e pacchetti sospetti, è cruciale per una sicurezza più ferrea.

Aggiungendo un IPS (Intrusion Prevention System) abbiamo notevolmente incrementato la sicurezza di rete, il suo compito è quello di notificare e bloccare automaticamente in caso di intrusione che sia interna o esterna alla rete monitorandola costantemente.

Fanno tutti parte della DMZ (Demilitarized Zone). Potremmo definirle delle locazioni di dati che fungono da deposito accessibile, in sintesi, una zona intermedia, uno spazio sicuro e controllato tra la rete interna e quella esterna, consentendo l'accesso a servizi pubblici senza compromettere la sicurezza dell'intera rete aziendale. Il tutto è connesso ad un router centrale dell'azienda che a sua volta è connesso alle varie postazioni. Abbiamo prontamente segmentato il dominio di broadcast così da ampliare delle sottoreti interne per una comunicazione e uno scambio dati più sicuro in caso di eventuale attacco (Subnet).

Mettendo un router in ogni VLAN abbiamo implementato una subnet mask diversa per ogni reparto aziendale. Abbiamo scelto un Firewall perimetrale perché si trova tra la rete WAN e la LAN svolge il compito di proteggere dagli accessi non autorizzati e dagli attacchi esterni e filtra i dati interni ed esterni alla rete.

Il server proxy può nascondere l'indirizzo IP originale del client, fornendo un grado di anonimato durante la navigazione su Internet. Il Server Proxy svolge la funzione di mascherare l'indirizzo

IP principale dei dispositivi dell'azienda aggiungendo un ulteriore filtro di protezione.

All'interno della nostra LAN possiamo trovare il server Application e-commerce ed un NAS collegati da uno switch.

A protezione del NAS si può trovare un IDS (Intrusion Detention System), un sistema di sicurezza estremamente simile all'IPS ma che svolge un compito minore, si limita a notificare e ad avvisare l'utenza di eventuali accessi.

Il NAS è un server specializzato in archiviazione dati e di richieste di condivisione file, essa è la zona più sensibile e delicata da proteggere.

In fine nella nostra struttura troviamo un Application Server E-commerce a cui l'accesso è riservato ai soli impiegati.