Report

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:

- Server interno (Application Server e-commerce)
- 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 inoltre, abbiamo aggiunto un WAF (Web Application Firewall), quest'ultimo è una soluzione progettata per proteggere le applicazioni web da eventuali minacce.
il WAF svolge 3 importanti processi:

- Monitora il traffico
- Filtra le informazioni
- Blocca i pacchetti sospetti.

Queste 3 fasi sono molto importanti per una sicurezza più ferrea.
Aggiungendo un IPS (Intrusion Prevention System), incrementiamo la sicurezza di rete, il suo compito è quello di:

- Notificare l'accesso anomalo
- Bloccare automaticamente il processo in caso di intrusione,che sia interno o esterno alla rete monitorando costantemente.

Fanno tutti parte della DMZ (Demilitarized Zone).
Potremmo definirle come 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 (Subnet) così da ampliare delle sottoreti interne per una comunicazione e uno scambio dati più sicuro in caso di eventuale attacco.
Per maggiorare il livello di sicurezza della rete,abbiamo avuto la necessità di impostare :

- Un router in ogni VLAN così facendo implementiamo una subnet mask diversa per ogni reparto aziendale.
- Un Firewall perimetrale,il quale svolge il compito di:
    - proteggere dagli accessi non autorizzati
    - difendere dagli attacchi esterni
    - filtra i dati interni ed esterni alla rete.
- Un Server Proxy svolge la funzione di:
        - Mascherare l'indirizzo IP principale dei dispositivi dell'azienda
        - Aggiunge un ulteriore filtro di protezione.

All'interno della nostra LAN possiamo trovare:

- Il server Application e-commerce (accesso riservato ai soli impiegati)
- Un NAS(server specializzato in archiviazione dati e di richieste di condivisione file)
- Un IDS (Intrusion Detenction System) per proteggere il NAS, un sistema in grado di avvisare l'utenza in caso di eventuali accessi.