Relazione progetto

L'obiettivo è progettare una rete informatica sicura e segmentata per garantire la protezione dei dati sensibili. Il design prevede la suddivisione della rete in tre zone (Internet, DMZ e zona interna) con un firewall perimetrale per controllare gli accessi.

I motivi per i quali ho scelto di suddividere la rete in tre zone sono:

1. Miglioramento della sicurezza (separare i servizi pubblici, HTTP/SMPT, dalla rete interna minimizza il rischio di attacchi che possano compromettere dati sensibili)
2. Gestione del traffico (le comunicazioni tra le zone sono filtrate tramite regole di firewall, limitando il traffico ai soli protocolli necessari)
3. Affidabilità (in caso di attacco a un server nella DMZ, la rete interna rimane isolata e protetta).

La zona internet rappresenta la rete pubblica da cui provengono richieste di accesso ai servizi esposti nella DMZ. Nel disegno di rete è rappresentata da un cloud collegato al firewall e permette il collegamento alla rete aziendale per l'accesso ai servizi web e email.

La zona DMZ (Demilitarized zone) è progettata per ospitare i server che devono essere accessibili dall'esterno, riducendo il rischio di accesso non autorizzato alla rete interne. Ho inserito un server HTTP che ospita siti web e applicazioni pubbliche e un server SMTP che gestisce l'invio e la recezione di email, tutti e due collegati ad uno switch a sua volta collegato al firewall. Saranno configurati per consentire solo il traffico HTTP, HTTPS e SMTP da internet verso la DMZ.

La zona interna ospita i dati sensibili e dispositivi aziendali, come pc e laptop per i dipendenti, ed è isolata da internet per evitare compromissioni dirette. Nella rete interna ho messo un server per la gestione e l'archiviazione dei dati sensibili aziendali e due dispositivi per i dipendenti collegando tutto ad uno switch che a sua volta è collegato al firewall perimetrale. Qui è consentito il traffico interno

verso la DMZ per accedere ai servizi ed è bloccato qualsiasi traffico diretto da internet verso la rete interna.

Il firewall è la componente centrale della sicurezza della rete e l'ho posizionato al centro tra tutte le zone per filtrate il traffico e applicare le policy di sicurezza. Collegato a tutte e tre le zone, bisogna configurarlo in modo da consentire il traffico HTTP e SMTP e bloccare tutto il traffico non autorizzato.

Questo design di rete garantisce un alto livello di sicurezza grazie alla segmentazione delle zone, al firewall e alle regole di accesso e blocco ben definite. Con questo modello di rete possiamo avere una protezione di dati sensibili aziendali e la disponibilità dei servizi pubblici consentiti minimizzando i rischi.