Progetto Rete Azienda Theta - Configurazione e Sicurezza Avanzata

1. Introduzione
Il progetto di rete per Azienda Theta si propone di sviluppare un'infrastruttura di rete robusta, scalabile e sicura, in grado di rispondere alle esigenze aziendali di ottimizzazione delle risorse, supporto alla crescita e protezione dei dati. La rete è progettata per separare e isolare i reparti aziendali attraverso VLAN, isolare i componenti critici tramite segmentazione, e implementare soluzioni avanzate di sicurezza come SIEM (Security Information and Event Management) e IDS/IPS (Intrusion Detection and Prevention Systems). Inoltre, la rete è progettata per essere conforme alle normative GDPR (General Data Protection Regulation), garantendo la protezione dei dati sensibili e la privacy dei dipendenti e clienti.

2. Obiettivi del Progetto
Gli obiettivi primari di questo progetto sono:

- **Separazione e Isolamento della Rete:** Ogni reparto aziendale (IT, Ricerca, Sviluppo, Servizio Clienti, Marketing e CEO/Amministrazione) è separato tramite VLAN, per garantire una gestione ottimale del traffico e ridurre la possibilità di attacchi interni. I componenti critici (come server, NAS e sistemi di monitoraggio) sono isolati da altre VLAN.
- **Sicurezza Avanzata:** Implementazione di DMZ per i server web esposti a Internet, riducendo il rischio di attacchi provenienti dall'esterno. Inoltre, l'adozione di IDS/IPS e SIEM offre una protezione proattiva e reattiva contro minacce sia interne che esterne.
- **Compliance GDPR:** Protezione dei dati sensibili e privacy, con una gestione sicura delle informazioni in linea con le normative GDPR, incluse politiche di accesso limitato e tracciabile.

3. Architettura della Rete
VLAN e Subnetting:
La rete è suddivisa in diverse VLAN, ognuna dedicata a un piano o reparto aziendale specifico. L'uso di VLAN permette una separazione fisica e logica del traffico, migliorando la sicurezza e l'efficienza della rete.

1. **Piano 1 (Componenti Critici e IT):**
    - **VLAN:** 192.168.1.0/24 (254 indirizzi IP)
    - **Dispositivi:** Firewall, NAS, IDS/IPS, SIEM, DHCP, server di gestione della rete, router e dispositivi di monitoraggio.
    - **Descrizione:** Area sicura e ventilata per i dispositivi critici e la gestione della rete aziendale. Il piano include anche i server di gestione della rete e dispositivi di monitoraggio.
2. **Piano 2 (Ricerca):**
    - **VLAN:** 192.168.2.0/24 (254 indirizzi IP)
    - **Descrizione:** Rete separata per il reparto di ricerca, dove vengono eseguite attività sensibili come l'analisi dei dati e lo sviluppo di nuovi progetti.
3. **Piano 3 (Sviluppo):**
    - **VLAN:** 192.168.3.0/24 (254 indirizzi IP)

    - **Descrizione:** Rete dedicata al team di sviluppo software, separata per evitare interferenze con altre aree aziendali.
4. **Piano 4 (Servizio Clienti):**
    - **VLAN:** 192.168.4.0/24 (254 indirizzi IP)
    - **Descrizione:** Rete per il team di servizio clienti, separata per isolare le attività legate ai clienti e garantire la protezione dei dati sensibili.
5. **Piano 5 (Marketing):**
    - **VLAN:** 192.168.5.0/24 (254 indirizzi IP)
    - **Descrizione:** Rete separata per il team di marketing e la gestione delle campagne aziendali, che non devono interferire con altre funzioni aziendali.
6. **Piano 6 (CEO e Amministrazione):**
    - **VLAN:** 192.168.6.0/24 (254 indirizzi IP)
    - **Descrizione:** Rete altamente protetta per la gestione amministrativa e decisionale dell'azienda. Separazione dei dati sensibili.
7. **DMZ per Web Server:**
    - **VLAN:** 192.168.0.0/29 (6 indirizzi IP)
    - **Dispositivi:** Web Server (esposti a Internet).
    - **Descrizione:** Isolamento dei server web da Internet, con l'intento di proteggere i sistemi aziendali da attacchi esterni.

Dettaglio del Subnetting:

- **Piano 1:** 192.168.1.0/24
- **Piano 2:** 192.168.2.0/24
- **Piano 3:** 192.168.3.0/24
- **Piano 4:** 192.168.4.0/24
- **Piano 5:** 192.168.5.0/24
- **Piano 6:** 192.168.6.0/24
- **DMZ:** 192.168.0.0/29

4. Access Point e Wi-Fi
Gli access point sono distribuiti in modo uniforme su ogni piano, con una configurazione che garantisce l’accesso Wi-Fi sicuro separato tramite VLAN. Ogni piano avrà una VLAN Wi-Fi dedicata, e la gestione del DHCP garantisce l'assegnazione sicura degli indirizzi IP. Inoltre, i dispositivi Wi-Fi sono limitati all'accesso alle risorse aziendali necessarie, riducendo i rischi legati a dispositivi non autorizzati.

5. Sicurezza e Monitoraggio

- **IDS/IPS:** Gli IDS (Intrusion Detection Systems) monitorano il traffico per rilevare comportamenti sospetti, mentre gli IPS (Intrusion Prevention Systems) intervengono per bloccare attivamente il traffico dannoso. La loro implementazione all'interno della rete permette di identificare e prevenire attacchi come SQL injection, brute force e DDoS.
- **SIEM:** Il sistema SIEM raccoglie e analizza i log provenienti dai dispositivi di rete, server e applicazioni. Grazie alla correlazione degli eventi, il SIEM è in grado di rilevare anomalie e attività sospette, generando allarmi in tempo reale e migliorando la risposta agli incidenti di sicurezza.

- **Firewall e ACL:** I firewall segmentano la rete e proteggono i dispositivi aziendali da attacchi esterni. L'uso di Access Control Lists (ACL) permette di creare regole granulari che gestiscono il traffico tra le diverse VLAN, limitando la comunicazione solo a quella necessaria e migliorando la sicurezza complessiva.
- **Proxy e DPI (Deep Packet Inspection):** Il proxy è utilizzato per monitorare e filtrare il traffico HTTP/HTTPS in entrata e in uscita dalla rete aziendale. Attraverso la Deep Packet Inspection (DPI), il proxy analizza il contenuto del traffico e blocca minacce come malware, phishing, e tentativi di accesso non autorizzato. Inoltre, il proxy consente di implementare politiche di URL Filtering, evitando l'accesso a siti dannosi o non aziendali.

6. Compliance GDPR
La rete è progettata per garantire la protezione dei dati sensibili e la privacy in linea con le normative del GDPR. Gli accessi alle informazioni aziendali sono limitati e tracciabili, e tutte le comunicazioni tra i dispositivi della rete sono protette tramite crittografia. La gestione dei diritti di accesso è centralizzata, assicurando che solo gli utenti autorizzati possano accedere ai dati sensibili.

7. Considerazioni sulla Sicurezza Aggiuntive

- **Autenticazione Multifattoriale (MFA):** Per rafforzare la sicurezza, è raccomandato implementare l'autenticazione multifattoriale (MFA) per l'accesso ai sistemi aziendali critici, inclusi accessi remoti, server e applicazioni.
- **Backup e Disaster Recovery:** Implementare soluzioni di backup regolari e strategie di disaster recovery per garantire la protezione dei dati in caso di guasti, attacchi ransomware o incidenti gravi. Testare periodicamente i piani di recupero per ridurre i tempi di inattività.
- **Aggiornamenti e Patching Regolari:** Mantenere tutti i dispositivi di rete, server e applicazioni costantemente aggiornati con le ultime patch di sicurezza. La gestione automatica degli aggiornamenti riduce i rischi legati a vulnerabilità conosciute.
- **Monitoraggio Proattivo:** Implementare un sistema di monitoraggio continuo per rilevare eventuali anomalie nella rete, con particolare attenzione alle attività insolite, ai comportamenti sospetti e alle possibili vulnerabilità.
- **Protezione Anti-DDoS:** Integrare sistemi di protezione contro attacchi DDoS per proteggere la rete da tentativi di saturazione della larghezza di banda, che potrebbero compromettere i servizi aziendali.

8. Conclusione
La rete progettata per Azienda Theta offre una struttura robusta, sicura e scalabile. La separazione tra i vari reparti aziendali, l'uso di VLAN per il traffico interno e l'isolamento dei componenti critici garantiscono un ambiente protetto. L'integrazione di soluzioni avanzate come IDS/IPS, SIEM, proxy con DPI e il monitoraggio continuo forniscono una protezione efficace contro le minacce interne ed esterne. Il rispetto delle normative GDPR assicura che i dati aziendali siano trattati in modo sicuro, proteggendo la privacy dei clienti e dei dipendenti.