CONSIGLI DI CYBERSECURITY PER LA COMPAGNIA THETA

1. Mantenere il principio di “Default Deny”

È fondamentale che la configurazione dei firewall rimanga basata sul principio di **blocco preventivo**:

- tutto il traffico deve essere negato di default;
- ogni nuova apertura di porte o servizi deve essere **giustificata, documentata e autorizzata**.

Questo riduce drasticamente il rischio di esposizione accidentale dei servizi interni.

2. Proteggere rigorosamente la VLAN di Management

La VLAN di management rappresenta il **punto più critico dell’infrastruttura**.
Si consiglia di:

- consentire l’accesso solo da host autorizzati;
- utilizzare **autenticazione forte** sugli apparati di rete;
- evitare qualsiasi accesso diretto da VLAN utente.

Un compromesso della rete di gestione comporterebbe il controllo dell’intera infrastruttura.

3. Monitorare costantemente tramite IDS / IPS

I sistemi IDS e IPS devono essere:

- mantenuti **sempre aggiornati** con firme recenti;
- monitorati quotidianamente dal personale IT;
- configurati per generare **alert immediati** in caso di traffico anomalo.

La sicurezza non è statica: il monitoraggio continuo è essenziale.

4. Limitare i privilegi degli utenti (Least Privilege)

Ogni utente deve avere accesso **solo alle risorse strettamente necessarie**:

- utenti standard limitati alla navigazione Internet;
- sviluppatori con accesso esclusivo al Web Server;
- amministratori separati dagli utenti comuni.

Questo riduce errori umani e abusi interni.

5. Aggiornare regolarmente sistemi e apparati

È consigliato pianificare:

- aggiornamenti periodici di firewall, switch, router e server;
- patch di sicurezza per sistemi operativi e servizi esposti in DMZ.

Molti attacchi sfruttano vulnerabilità già note ma non corrette.

6. Verificare periodicamente le regole firewall

Le regole di sicurezza devono essere:

- revisionate periodicamente;
- rimosse se non più necessarie;
- mantenute chiare e documentate.

Regole obsolete aumentano il rischio di falle di sicurezza.

7. Eseguire test di sicurezza ricorrenti

Oltre ai test iniziali, si consiglia di ripetere periodicamente:

- scansioni delle porte;
- test HTTP sui servizi pubblici;
- analisi del traffico con strumenti di sniffing controllato.

Questo permette di intercettare problemi prima che diventino incidenti.

8. Proteggere e testare i backup

Il NAS deve essere:

- accessibile solo tramite i protocolli necessari;
- protetto da credenziali robuste;

- verificato periodicamente con test di ripristino.

Un backup non testato equivale a non avere backup.

9. Sensibilizzare il personale

Anche la migliore infrastruttura può essere compromessa da errori umani.
Si consiglia di:

- formare i dipendenti su phishing e comportamenti sicuri;
- definire policy chiare sull'uso dei dispositivi aziendali.

La cybersecurity è anche un fattore umano.

10. Documentare e mantenere le policy di sicurezza

Ogni configurazione deve essere:

- documentata;
- aggiornata nel tempo;
- accessibile al reparto IT.

La documentazione è essenziale per interventi rapidi e sicuri.