Segmentazione di rete e gestione degli accessi privilegiati

Proponente	Marco Bianchi
Ruolo	Responsabile Sicurezza Informatica
Funzione aziendale	Sicurezza e Compliance
Email	marco.bianchi@zava-demo.example
Sponsor interno	Chiara Lombardi, Chief Information Officer
Data di presentazione	06/10/2026
Programma di riferimento indicato	PG-200 Sicurezza e Conformità
Budget richiesto	210.000 euro
Durata stimata	8 mesi

1. Contesto e problema

La rete delle sedi di Milano, Torino, Bologna e Roma è oggi una rete piatta: un dispositivo compromesso può raggiungere quasi tutti i server. Gli account amministrativi sono 140, di cui 38 condivisi tra più persone e senza rotazione delle password.

Il penetration test di marzo 2026 ha classificato come critici due rischi: movimento laterale tra le sedi e uso di credenziali amministrative condivise. Il registro dei rischi IT li riporta con codice R-SEC-07 e R-SEC-11.

2. Soluzione proposta

Segmentare la rete in zone (utenti, server, sistemi industriali, ospiti) con regole di accesso esplicite e introdurre una soluzione di gestione degli accessi privilegiati (PAM) con credenziali a tempo, registrazione delle sessioni e approvazione degli accessi amministrativi.

3. Allineamento strategico

La proposta attua l'obiettivo OS3 del Piano Strategico IT 2026-2028 (resilienza e sicurezza by design) e chiude due gap rilevati nell'autovalutazione NIS2 di giugno 2026.

4. Benefici attesi e KPI

Eliminazione dei 38 account amministrativi condivisi entro il mese 6.

Riduzione stimata del 70% dei percorsi di movimento laterale individuati dal penetration test, da verificare con un nuovo test al mese 8.

Copertura dei requisiti NIS2 sulla gestione degli accessi e sul controllo della rete; evidenze pronte per l'audit interno di fine anno.

5. Costi e pianificazione

Costo una tantum: 210.000 euro (progettazione, apparati, soluzione PAM, servizi di implementazione). Costi ricorrenti: 42.000 euro all'anno per licenze PAM e manutenzione apparati, già previsti nel budget operativo 2027.

Pianificazione: disegno delle zone (mesi 1-2), sede pilota di Bologna (mesi 3-4), estensione alle altre sedi (mesi 5-7), PAM in produzione e nuovo penetration test (mese 8).

6. Rischi, dipendenze e mitigazioni

Interruzioni di servizio durante la segmentazione: interventi nelle finestre notturne e piano di rollback per ogni sede.

Resistenza degli amministratori all'uso del PAM: formazione dedicata e periodo di affiancamento di 4 settimane.

Competenze: il team interno ha due specialisti di rete certificati; per il PAM è previsto il supporto del fornitore.

Documento fittizio creato per i laboratori Copilot Studio. Nomi, persone e importi sono inventati.