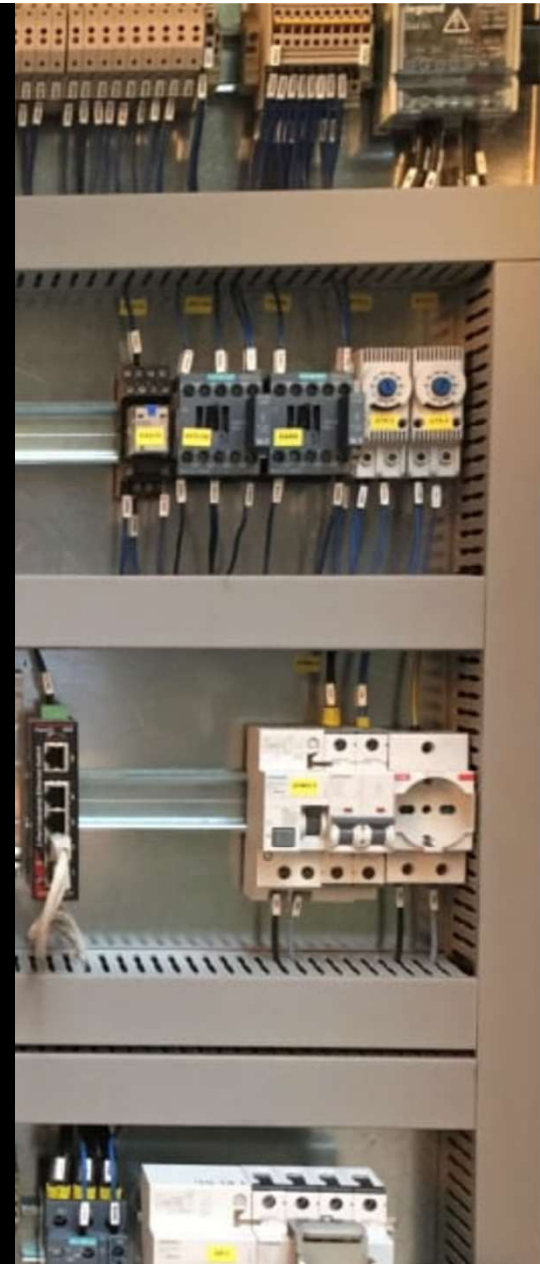




ZERO TRUST

Ing. Giuseppe Lucci

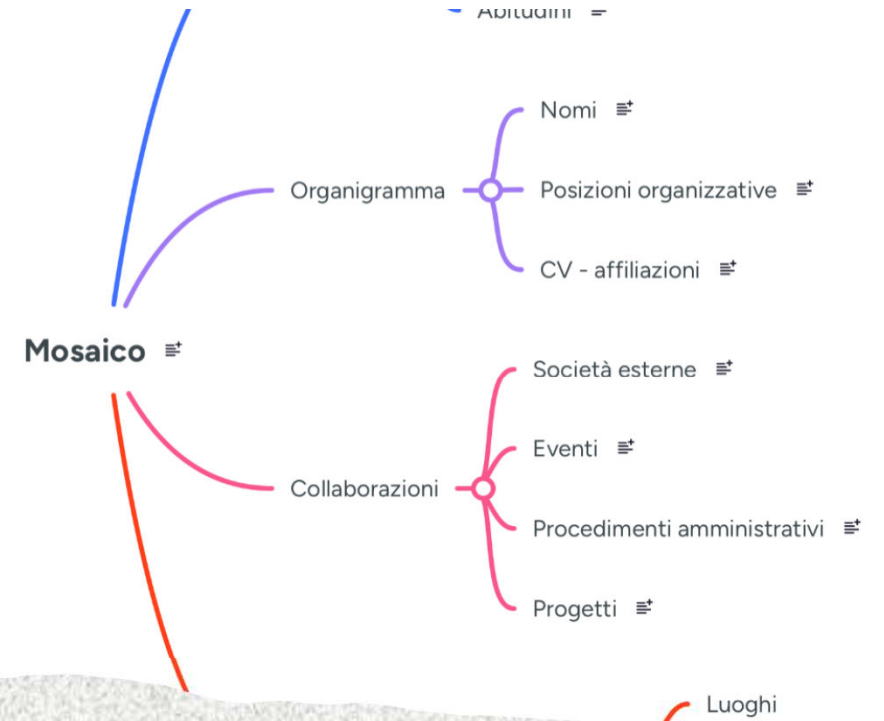
Cosa vedete ?



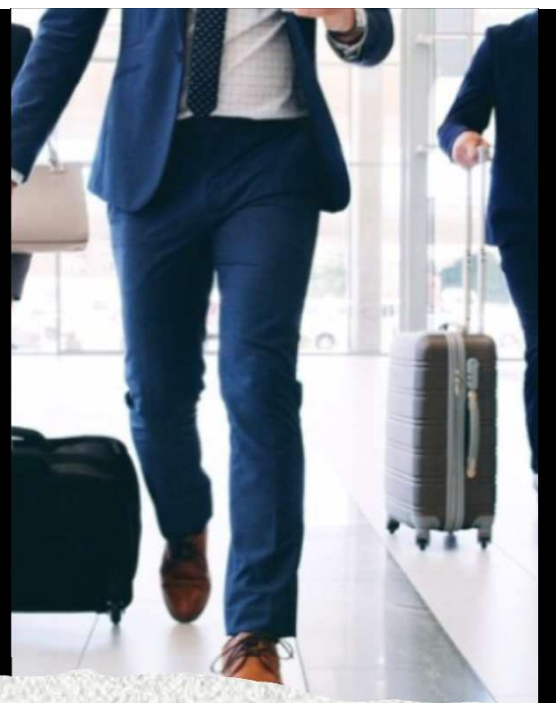


VULNERABILITA' (Database pubblici e non)

- Stuxnet, attacco informatico effettuato per causare danni cinetici agli impianti (2010)
- Attacco cyber ai sistemi di refrigerazione alimentare Francia/Olanda (Ottobre 2016)



Effetto Mosaico



Informazioni critiche condivise involontariamente

- Social network
- Call di lavoro
- Viaggio di lavoro
- File PDF inviato per e-mail



Filosofia del 'Castello e Fossato'

- Non protegge da attacchi interni
- Non si adatta al Cloud
- Basa tutto sulla fiducia

ZERO TRUST

'Non fidarti mai a prescindere, verifica sempre'

- Modello nato nel 2010
- Non è sfiducia verso i collaboratori
- Smettere di concedere privilegi permanenti
- Comprendere il valore dell'informazione
- Consapevolezza situazionale
- Abitudini e protocolli di risposta

REGOLA *‘Prima
ti identifichi, poi
verifico cosa
chiedi, poi ti
autorizzo’*

Zero Trust normalmente
presentato come modello IT

Proposta Zero Trust universale

Postura mentale e cultura
organizzativa applicabile ad ogni
processo di interazione umana

Salvaguardia contro il social
engineering

Cinque decisioni immediatamente applicabili

1. Conoscere chi sa cosa
2. Adottare una politica di minimo privilegio
3. Segmentazione delle informazioni
4. Osservazione ed apprendimento
5. Condivisione della metodologia Zero Trust con terzi e *Fornitori*



ZERO TRUST

GRAZIE PER L'ATTENZIONE