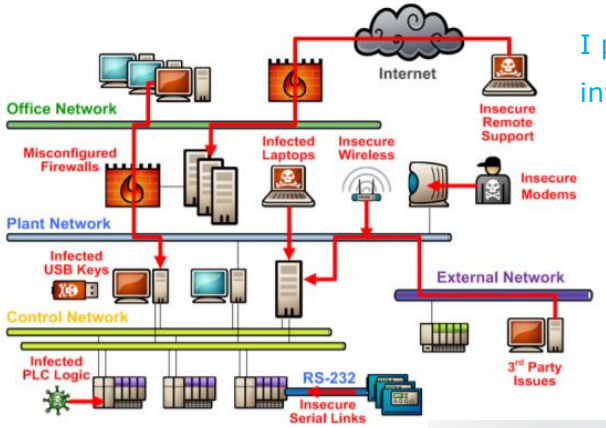
Rischi Cyber e contromisure tecnologiche per la protezione dei sistemi in ambito ICS e OT

ONE IDENTITY

Rischi “Cyber” – ICS e OT

- Il fattore umano e’ un nodo centrale. Consapevolezza dei rischi e norme di comportamento partono dal binomio “Istruzione” e “Formazione”
- I criteri di R-I-D “Riservatezza-Integrita’-Disponibilita’” risultano essere sbilanciati su “D” e “I”. Occorre pensare alla CyberSecurity con un’ottica differente.
- Le soluzioni tecnologiche tradizionali di Sicurezza IT (es. Firewall, AntiVirus) risultano inadeguate
- Occorrono competenze tecniche specifiche per proteggere l’OT e l’ICS
- I sistemi di controllo delle macchine industriali o i misuratori sono interconnessi al mondo IT: ne deriva una amplificazione del rischio Cyber
- I produttori dei sistemi di controllo devono adottare nella progettazione il principio di security “by design”
- I Ransomware possono agevolmente transitare dalla rete IT verso la rete dedicata dell’impianto industriale (caso Moller-Maersk, caso Saint Gobain, caso aziende energetiche ucraine)
- Chi amministra i sistemi di controllo e’ un potenziale insider. Esistono adeguati controlli di accesso ?

Rischi “Cyber” – ICS e OT

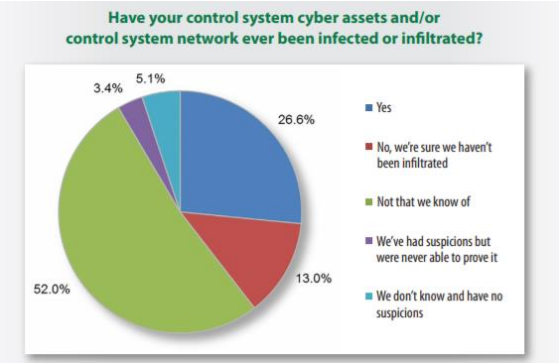


I punti di accesso per la amministrazione e la diagnostica rappresentano sorgenti di infezione o di attacco

SANS 2016 – State of ICS Security Survey

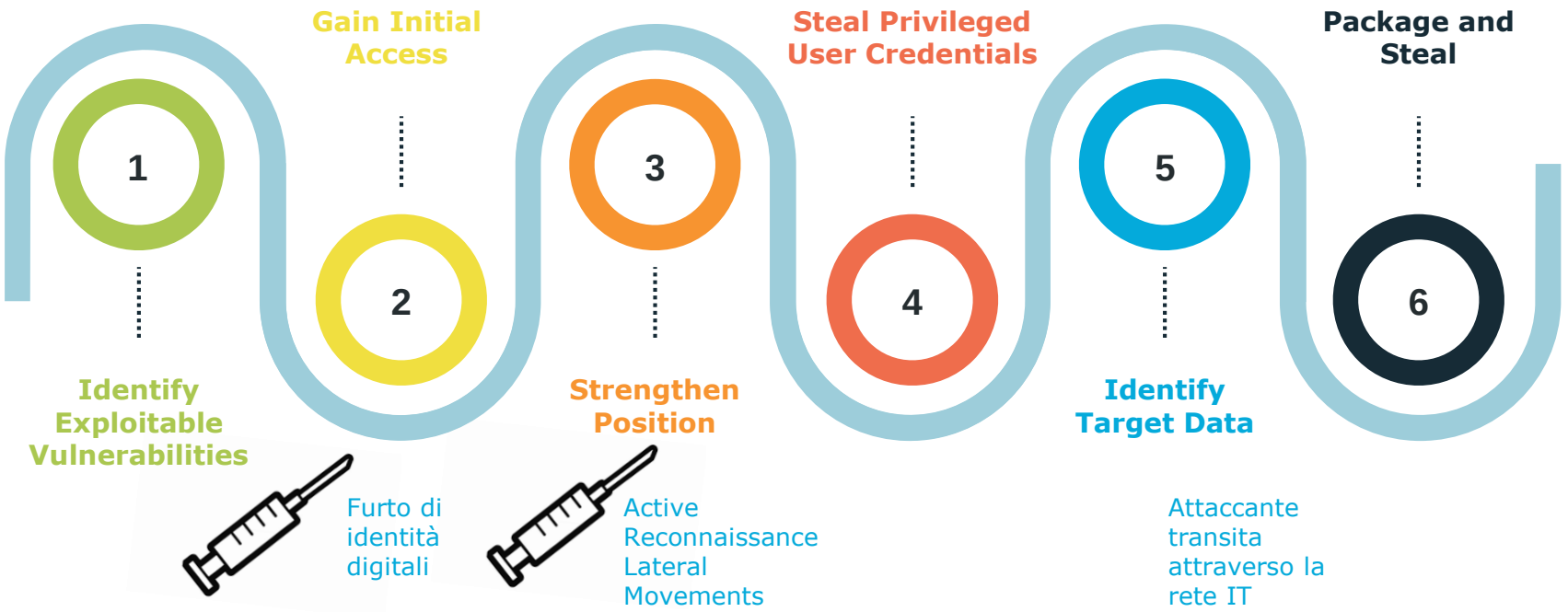
Primo posto per le minacce esterne (malware)

42% delle minacce provengono dall’interno delle organizzazioni



10% «intenzionali» -> sabotaggi
15% «non intenzionali» -> errate configurazioni, scarsa competenza

Abuso di credenziali amministrative



Protezione degli accessi

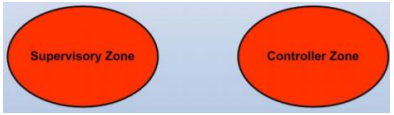
NIST 800-82 “Guide to Industrial Control Systems (ICS) Security”

- Rotazione periodica delle password di amministrazione
- Principio del “Minimo privilegio” e controlli di accesso basati sul “Ruolo” (RBAC)
- Autenticazione robusta (MFA)
- Tracciamento e monitoraggio degli accessi nella rete segregata di ICS
- Rilevamento delle minacce e tentative di attacco (Behavioural Analytics)
- Network segregation

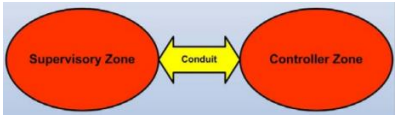
ISA/IEC 62443 “Industrial Automation and Control Systems Security”

Introduce i concetti di “zones” e “conduits”

Le zone sono gruppi di sistemi fisici o logici che condividono i medesimi requisiti di sicurezza

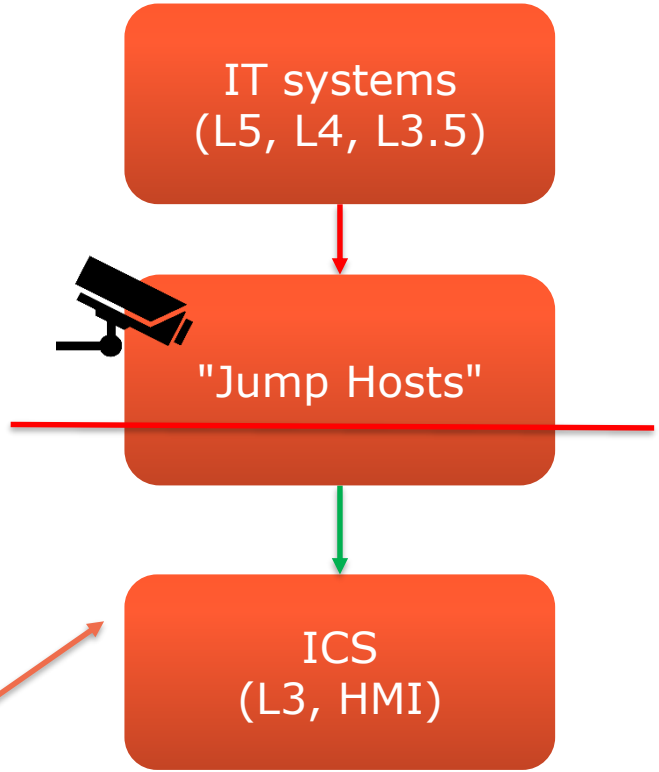


Qualsiasi comunicazione tra le zone deve avvenire tramite i “conduits”. Controllano gli accessi alle zone ed evitano il propagarsi dei malware. I controlli che implementano mitigano le differenze tra i livelli di sicurezza delle zone.



Protezione dei sistemi di controllo industriale

- L’accesso a ICS/OT puo’ avvenire solo attraverso sistemi IT dedicati
  - Secure Jump Server
  - L’elusione deve essere impedita
- "Registrazione e monitoraggio della sessione"
  - Registrazione delle azioni amministrative
  - Immodificabilita’ della registrazione
- "Isolamento della sessione"
  - No alla connessione diretta tra sistemi IT e rete OT



Applicazione del «Application White-Listing» sulle HMI (Human – Machine Interface)
+ rimozione privilegi amministrativi

Why worry about privileged accounts?

80

Forrester estimates 80% of all data breaches involve misuse of local endpoint administrative privileges

- No individual accountability
- Embedded in applications and scripts
- External access by vendors/developers
- Internal threats


ONE IDENTITY™