
Clusit

Maurizio Bini

- Fondatore ed Amministratore di Force 10 Consulting (20+ anni design, implementation, troubleshooting e support di network solutions.)

FORCE10 CONSULTING s.r.l.

- **Industrial Networking Certification:**
  - # Cisco Industrial Networking Specialist (IMINS)
  - # Cyber Security Certification (ISA/IEC 62443)
  - # Siemens Certified Professional for Industrial Networks – Switching & Routing
- **IT/OFFICE Networking Certification:**
  - # 3Com (MNS; Solution Expert, Wireless Solution)
  - # Aruba Networks (ACMP)
  - # Cisco (CCNP; CCDP)
  - # Enterasys/Cabletron (Switching)
  - # Fortinet (NSE4)
  - # HP (AIS)
  - # Juniper (JNCIA-EX)

1° Caso: Il «mistero della Smart TV» 1

- **Premessa:** Abbiamo una rete, sia per office sia per automazione, di circa 50 switch con oltre 1.000 device di vario genere collegati. La rete è segmentata in oltre 30 VLAN; alcune protette da firewall fisico, altre via ACL
- La rete automazione è molto «basic» (i.e. "chiavetta" per configurare i PLC e controllo di avvitatori che segnalano se e come è stato avvitato ogni bullone)
- In caso di errori il sistema blocca la catena di montaggio in automatico
- Dati raccolti su macchine virtuali e su SAP

1° Caso: Il mistero della «Smart TV» 2

- **Il Problema :** Una mattina, a caso user venivano scollegati da SAP, altri non entravano. Lo stesso per oltre 100 thinclient connessi.
- In prima battuta si pensa ad un problema di SAP
- Rete è ok: gli switch hanno configurazioni ridondate, "prive" di stp per rendere la rete più stabile e sicura.
- Dopo ore si riscontra un numero anomalo di MAC addres su una porta di uno switch periferico.
- Controllando fisicamente si trova una IP TV con OS Android. Scollegandola tutto è ripartito!
- **Perché?**

2° Caso: Progetto della rete di fabbrica MES/PLC

1. Rete con 4 server MES e 10 aree con 4 PLC/SCADA
2. Comunicazione sicura e possibilmente criptata.
3. Ridondanza e tempi di convergenza < 1 sec.
4. NB: i PLC sono distanti tra loro
5. I server MES si trovano su rete «Office»
6. SCADA e PLC sono su rete «Industrial»
7. Zone suddivise tramite una copia di firewall interni (diversi dai perimetrali)

Come segmentare e segregare ?

3° Caso: Gli operatori devono usare dei Tablet

- Alla rete del caso 2 aggiungiamo HotSpot WiFI per gestire Tablet per
  - Operatori
  - Manutentori
  - Supervisori
  - Manager
- **Come possiamo procedere?**

4° Caso: In fabbrica un armadio si è «fumato».

In Azienda produzione articoli in gomma, (100M€ fatt. 2016) una sovratensione provoca danni.

Dentro l'armadio ci sono (da verificare/sostituire):

- 2 PLC, un Siemens s7 ed un ControlLogix 5580
- 1 gateway per Profibus
- 1 gateway per Profinet
- 2 switch industriali

Come posso ripartire il più in fretta possibile?

5° Caso: Connessione remota «sospetta»

- Azienda stipula con imprese esterne contratti per manutenzione ed interventi sui PLC e SCADA su diverse zone impianti (h24-7/7).
- Le imprese chiedono di accedere da remoto per garantire il servizio in tempi brevi (h24-7/7)
- Azienda è molto sensibile a protezione I.P. sua e dei diversi fornitori di macchinari che ha in produzione

Come procedere?

6° Caso: Galeotto fu l'allegato alla email !

- Azienda alimentare media (circa 30m€ fatturato)
- Assistente amministrativa apre allegato email…
- Rete PC e Server di produzione e magazzino progressivamente si bloccano: ransomware!

Cosa è andato storto?

Come procedere?

Lesson Learned?