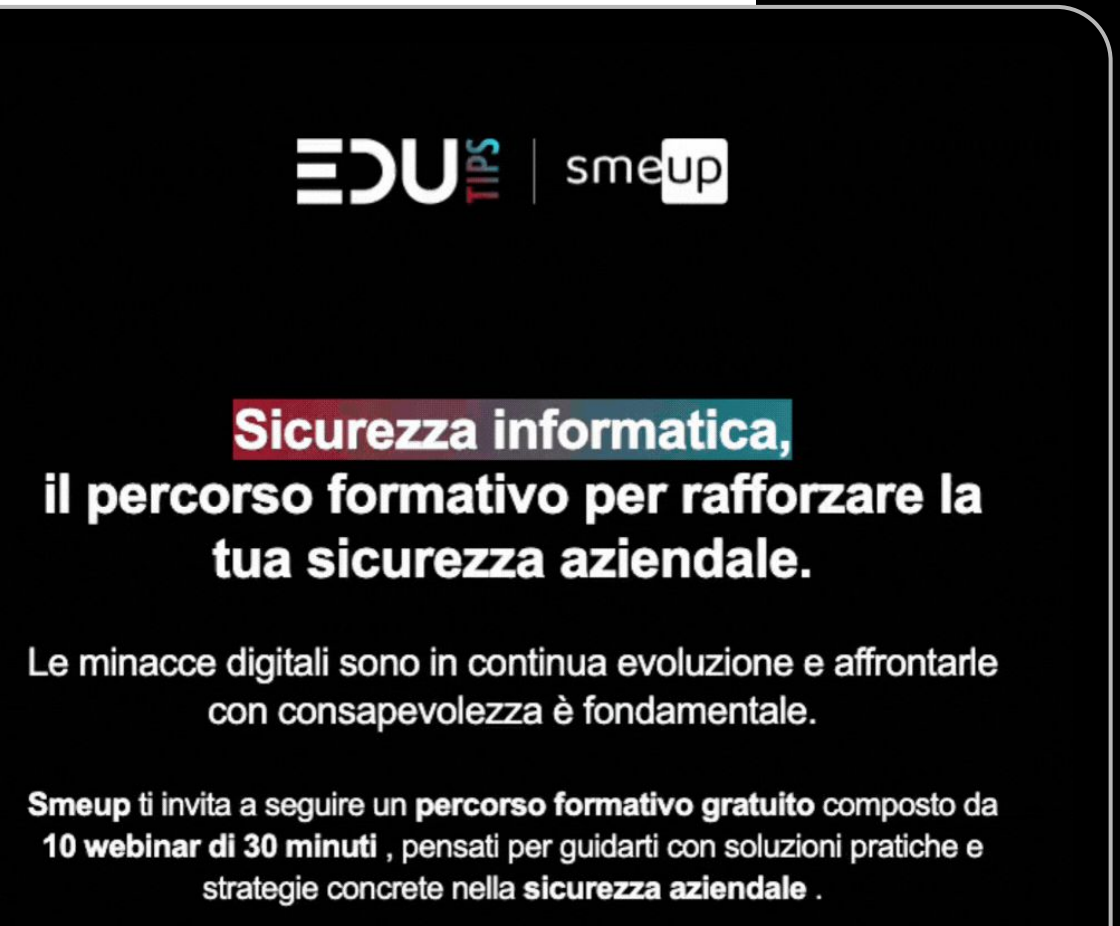
WEBINAR

Sicurezza delle reti industriali

Impara a proteggere i sistemi di controllo industriale

14 OTTOBRE
2025

EDU TIPS
CYBERSECURITY



EDU TIPS Cybersecurity

10 webinar TIPS - 30 minuti al mese
su tematiche specifiche di Cybersecurity

DATA	DESCRIZIONE
28/1	Mese 1: **Sicurezza dell'infrastruttura**
13/2	Mese 2: **Cyber Security Awareness**
13/3	Mese 3: **Data Protection**
10/4	**Mese 4: Identità e accesso**
13/5	Mese 5: **Cloud security**
12/6	Mese 6: **Incident response**
8/7	Mese 7: **Sicurezza delle applicazioni**
11/9	Mese 8: **Analisi delle minacce e vulnerability assessment**
10/10	**Mese 9: Sicurezza delle reti industriali (OT)**
11/11	Mese 10: **Sicurezza in ambito A.I.**

👉 SCOPRI DI PIÙ

EDU TIPS
CYBERSECURITY

SIMONE
ZABBERONI

Presales *- smeup ICS*

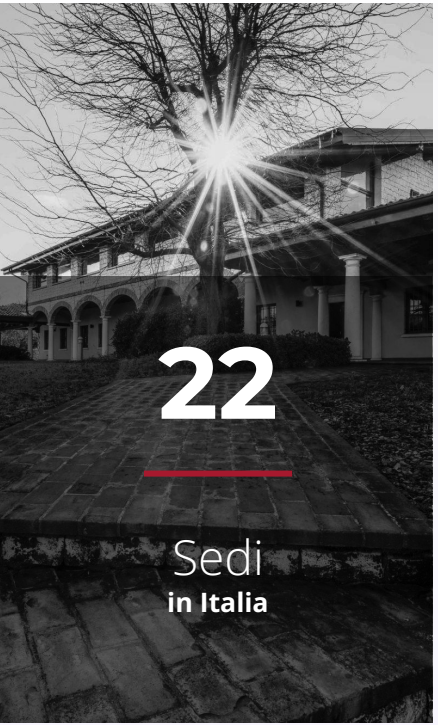
simone.zabberoni@smeup.com

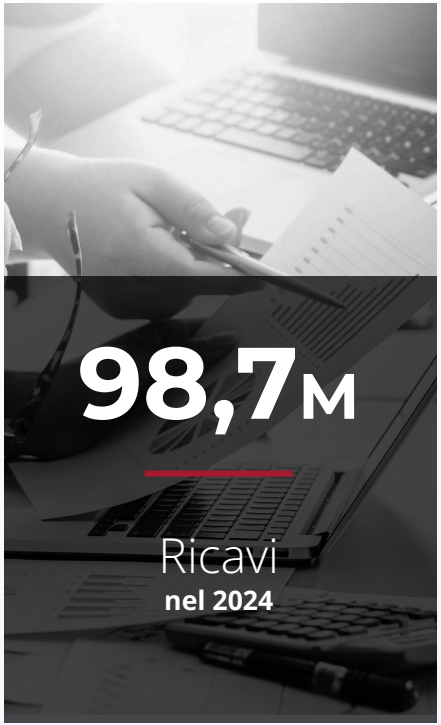
COMPANY OVERVIEW

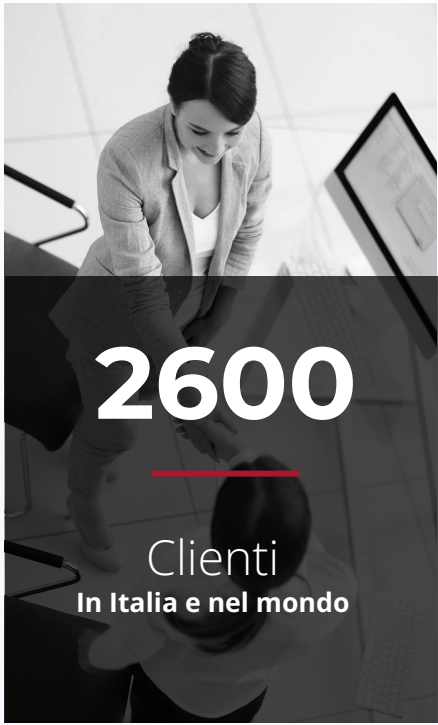
smeup in breve.

COMPANY **OVERVIEW**

smeup in Numeri.







BUSINESS SECTOR

BUSINESS SOFTWARE APPLICATION

Soluzioni **Software** per **PMI** e **grandi industrie.**

Ogni azienda è unica. smeup lo sa!
Usare la digitalizzazione per sviluppare il business e generare valore, ***insieme***.

- **e** GESTIONALI ERP
- **b** BUSINESS ANALYTICS
- **d** DOCUMENTALE
- **w** WEB & MOBILE APPLICATION
- **f** IOT E INTEGRAZIONE INDUSTRIALE
- **l** LOGISTICA E TRASPORTI

BUSINESS SECTOR

INFRASTRUCTURE, CLOUD & SECURITY

Soluzioni per **Architetture IT** e **servizi gestiti.**

Innovazione e **sicurezza** per rispondere ai bisogni delle aziende.

- i INFRASTRUTTURA
- c CLOUD
- cs CYBER SECURITY
- ps IBM POWER SYSTEMS

01

A che punto siamo

4.0 **TUTTO CONNESSO**

Dall’air-gap alla smart factory.

IERI

L'AIR-GAP

Le reti di produzione erano **isolate** in un mondo a parte, senza contatti diretti con l'esterno.

OGGI

LA CONNESSIONE (INDUSTRY 4.0)

- L'evoluzione ha portato all'uso di **protocolli Ethernet e IP**.
- **Obiettivo:** rendeva gli attaccanti meno "interessanti" (attacco locale necessario).
- **MA:** questo non le rendeva **secure *by design***.
- **Integrazione** con sistemi locali (fatturazione, mail) e servizi cloud.
- **Assistenza remota**.

VANTAGGI

MONITORAGGIO E GESTIONE CENTRALIZZATA

- **Monitoraggio** e controllo dei processi.
- Dati disponibili per la **gestione centralizzata**.
- Possibilità di **interagire** con servizi cloud.

LE **MINACCE**

Nuovi bersagli, nuove possibilità.

Questa evoluzione rende i nostri sistemi di produzione un bersaglio così appetibile e vulnerabile per il cyber-crimine.

I SISTEMI OT NON SONO NATI SICURI

- Gli apparati sono nati per la **"Safety"** (sicurezza fisica), non per la **"Security"** (sicurezza informatica).
- Sono diventati raggiungibili **dall'oggi al domani**, spesso senza seguire le best practice IT consolidate.
- Sono **privi di feature di sicurezza** e spesso carenti nel supporto alla cifratura.
- Molti sono attaccabili con **semplici attacchi DoS**.

PERCHÉ L'OT È LA NUOVA FRONTIERA DEL CRIMINE?

- Gli attaccanti usano il **"modello di business"** del Ransomware già collaudato.
- Hanno semplicemente **adattato tecniche e strumenti** di attacco al mondo OT.
- **Risultato:** hanno trovato nell'OT una **nuova frontiera** redditizia del crimine.

02

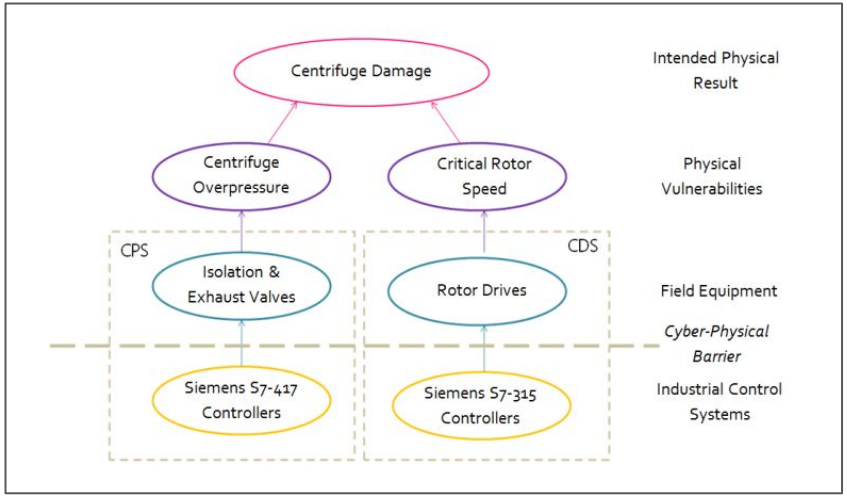
Alcuni eventi reali

ALCUNI **EVENTI REALI**

Stuxnet: danno fisico reale.

Un attacco chirurgico
e multicanale:

- **Infezione iniziale via USB.**
- Worm **auto-propagante** via rete (e via VPN!).
- Bersaglia solamente oggetti **Siemens vulnerabili.**



Fonte:
https://cyber-peace.org/wp-content/uploads/2013/06/To-kill-a-centrifuge.pdf?utm_source=chatgpt.com

Danno reale e fisico

- Invia **dati finti** ai sistemi di monitoraggio.
- **Interrompe le operazioni e danneggia le apparecchiature** (es. Centrifughe).
- Chiaro **rischio per la sicurezza umana.**

ALCUNI **EVENTI REALI**

Colonial pipeline: attacco al carburante.

L'impatto immediato dell'attacco:

- Attacco alle infrastrutture e blocco dei servizi di **billing**.
- Furto di **100GB di dati e pagamento del riscatto** ($4.4M USD).
- **Fermo fisico** totale della pipeline.

La propagazione su economia e sicurezza:

- **"Panico"** da esaurimento carburanti.
- **Aumento fuori scala** dei prezzi (i più alti in sei anni).
- Rischi legati al riempimento in **contenitori non adatti**.

ALTRI **ESEMPI**

OT: la minaccia è continua.

Gli attacchi non si sono fermati: analizziamo una rapida carrellata di esempi che dimostrano come il rischio sia continuo e miri alla sicurezza delle nostre infrastrutture e delle persone.

MALWARE CON FINI SPECIFICI

- **Duqu (2011):** malware spia per **ricognizione** prima dell'attacco.
- **Havex (2013):** trojan per **accesso remoto (RAT)** e furto di informazioni sul sistema di controllo.
- **BlackEnergy (2015):** usa macro in file Office per manipolare **infrastrutture critiche** su larga scala.

QUANDO L'ATTACCO METTE A RISCHIO LA VITA UMANA

- **TRITON (2017):** primo malware noto specificamente per attaccare i **sistemi di sicurezza industriali (SIS)** che proteggono le vite umane.
- **Attacco all'acqua (2021):** tentativo di avvelenare la **fornitura d'acqua a Tampa (FL)**.

MALWARE MODULARE E DISTRUTTIVO

- **PIPEDREAM:** framework modulare in grado di causare **disruption, degradation e *possibilmente persino distruzione.***
- **FrostyGoop (2024):** ha modificato le misurazioni dei controller ENCO causando interruzioni di riscaldamento in **oltre 600 condomini** in Ucraina durante l'inverno.

03

I rischi odierni

I **RISCHI ODIERNI**

Ma chi si interessa a me?

L'Italia è un bersaglio prioritario per il Cybercrime. Il settore Manifatturiero è al centro dell'attenzione del crimine organizzato.

I numeri sono la vostra realtà:

- **78%:** il principale attaccante in Italia è il **Cybercrime** (criminalità organizzata).
- **85%:** la maggior parte degli incidenti in OT **non inizia in produzione**, ma si propaga dagli ambienti IT (es. credenziali rubate o accessi remoti mal configurati).
- **+87%:** gli attacchi Ransomware, il loro modello di business, sono aumentati vertiginosamente contro il settore industriale.

78%

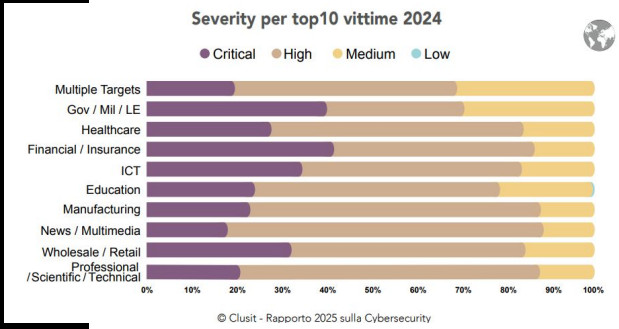
il principale attaccante in Italia è il Cybercrime

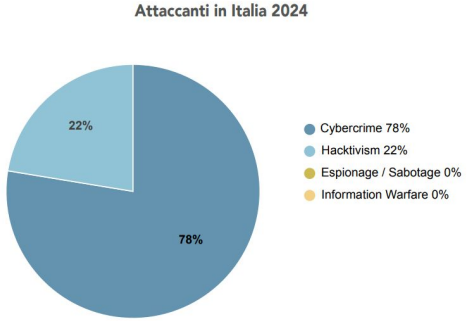
85%

degli incidenti in OT ha origine dagli ambienti IT

+87%

è l'aumento degli attacchi ransomware contro le organizzazioni industriali nell'ultimo anno





Fonte:
Rapporto clusit 2025
Dragos OT - 2025 OT Cybersecurity Report A Year in Review

QUALCHE **DATO**

Rapporto CLUSIT 2025: l'emergenza in Italia.

La minaccia in Italia è in forte crescita e ha un impatto estremamente grave sul Business.

+15%

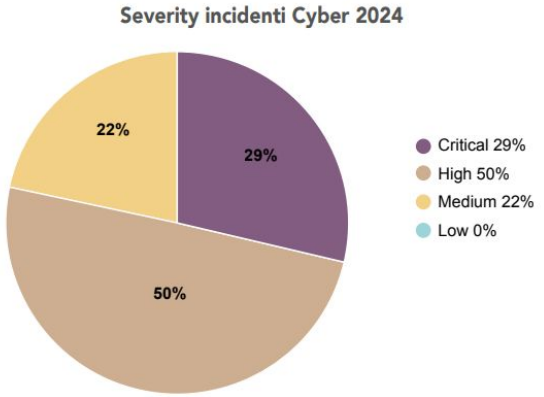
crescita degli incidenti subiti in Italia nel 2024 rispetto al 2023

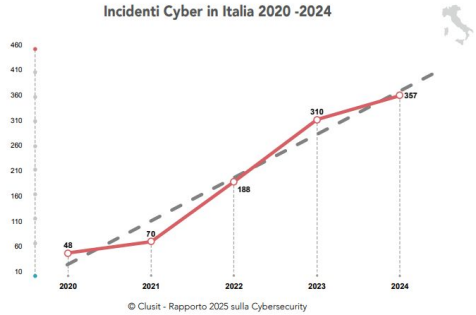
+10%

quota degli incidenti subiti in Italia nel 2024 rispetto al dato globale

79%

severità degli incidenti: critico + alto





Fonte: Rapporto Clusit 2025

Cosa può succedere?

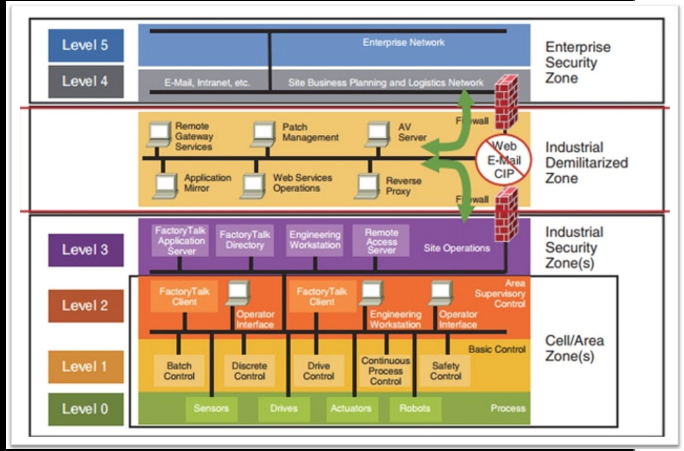
Quando viene bersagliata una rete OT dobbiamo aspettarci l'impatto "classico" di un attacco a rete IT, ma con in aggiunta ulteriori problemi:

L'IMPATTO CLASSICO (IT) Danni economici e di business:	L'IMPATTO AGGIUNTIVO (OT) Danni fisici, umani e ambientali:
Fermo dei servizi produttivi e diretto danno economico "al minuto".	**Manomissione e danneggiamento dei macchinari.**
Sottrazione dati.	**Rischio di sicurezza delle persone.**
Impatto sulla supply chain di cui si fa parte.	Problemi e tempistiche di **ripartenza**.
Danno di immagine / brand.	Impatti ambientali.
	Impatti regolamentari.

04 Protezione

PROTEGGERE LE **RETI OT**

Gli standard di riferimento.



Fonte: https://www.nist.gov/image/figure-1-purdue-model-computer-integrated-manufacturing

I DUE PILASTRI NORMATIVI

- **ISO 27001:** lo standard generale per la gestione della sicurezza delle informazioni in azienda.
- **IEC 62443:** lo standard **specifico** per la cybersecurity dei sistemi di controllo industriale (ICS).

La sicurezza OT richiede un approccio e una metodologia specifici (IEC 62443).

Differenze tra IT e OT

CARATTERISTICA	IT (INFORMATION TECHNOLOGY)	OT (OPERATIONAL TECHNOLOGY)
Obiettivo principale	Confidenzialità, integrità, disponibilità	**Disponibilità**, integrità, confidenzialità
Downtime	Spesso accettabile o pianificabile in tempi brevi	**Inaccettabile:** fermare = perdita €. pianificazione spesso difficile o in tempi lunghi.
Durata sistemi	3-5 anni	**10-30 anni**, spesso legacy
Patching/Update	Programmato, automatico, continuo	**Rarissimo**, solo in finestre manutentive ben definite. A volte non possibile (fornitori non più esistenti).
Ciclo di vita software	Aggiornato frequentemente	**Difficile da modificare**, spesso legacy
Protocolli principali	HTTPS, RDP, SSH	Modbus, Profinet, OPC UA, DNP3 **(non sicuri)**

PROTEGGERE L'OT

Capisaldi principali.

Viste le differenze tra IT e OT, ecco le sei strategie fondamentali, i 'capisaldi', che non possono mancare in una moderna strategia di sicurezza industriale.

CONOSCENZA E VALUTAZIONE

Asset inventory

Vulnerability e risk assessment

DIFESA DELLA RETE

Segmentazione e micro-segmentazione

Gestione degli account

GESTIONE ACCESSI E CULTURA

Formazione

Accesso remoto sicuro

NON PUOI PROTEGGERE **CIÒ' CHE NON VEDI**

Asset Inventory & Vulnerability Management.

Non puoi difendere ciò che non conosci. Ecco perché l'inventario degli asset OT è il primo passo.

GLI ASSET

Gli asset, ovvero le "cose" che fanno funzionare il tutto, devono essere censiti e per ciascuno deve essere chiaro:

- La **funzionalità** erogata
- Chi ne sia l'**owner**

Cosa includere:

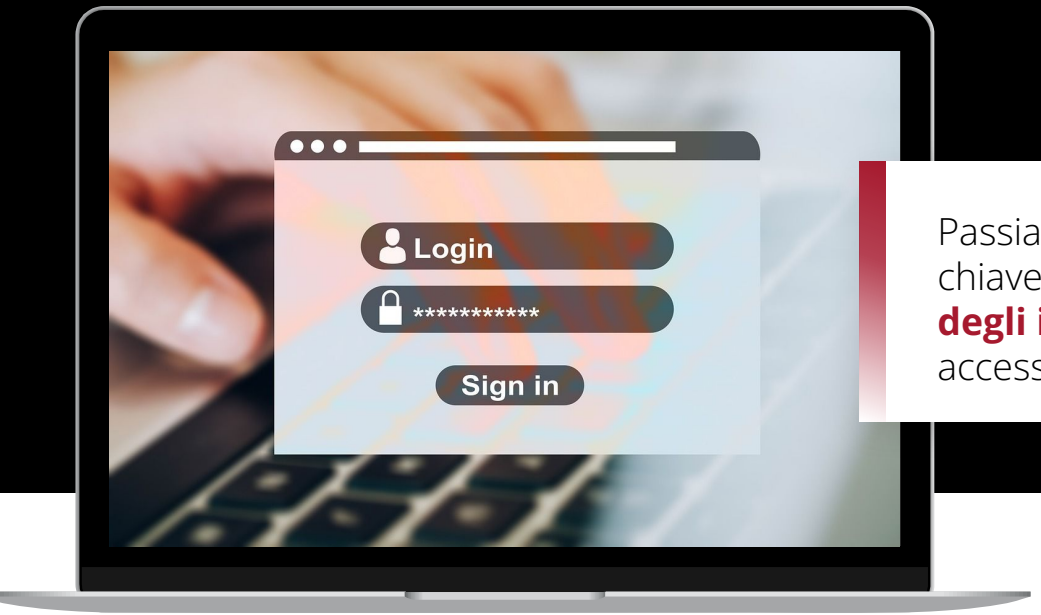
- **PLC**, PC bordo macchina, Historian
- MES, Server applicativi, Server infrastrutturali (anche se commisti con IT)
- Componenti di rete (switch, firewall, router, wireless)
- Soluzioni di **accesso remoto**.

GLI ASSET NON SONO TUTTI UGUALI

Bisogna classificarli per **importanza, rischio e vulnerabilità.**

Domande chiave da porsi:

- Il PLC è vulnerabile? Si può aggiornare? * Se non si può, si può spostare su una **rete blindata**?
- Quanto è importante se il PC bordo macchina viene **compromesso** o si rompe? Quanto tempo posso stare senza quel sistema?
- Come gestiamo un software di produzione **legacy** o non più supportato?
- Se c'è un guasto di rete (es. singolo switch), quanto tempo serve al ripristino?
- La produzione ha **autonomia offline**? Se sì, di quanto tempo?



Passiamo ora alla seconda strategia chiave, che attacca direttamente l'**85% degli incidenti OT**: come gestiamo gli accessi ai nostri sistemi?

UTENTI, **PASSWORD E MFA**

Gestione degli account: accesso sicuro.

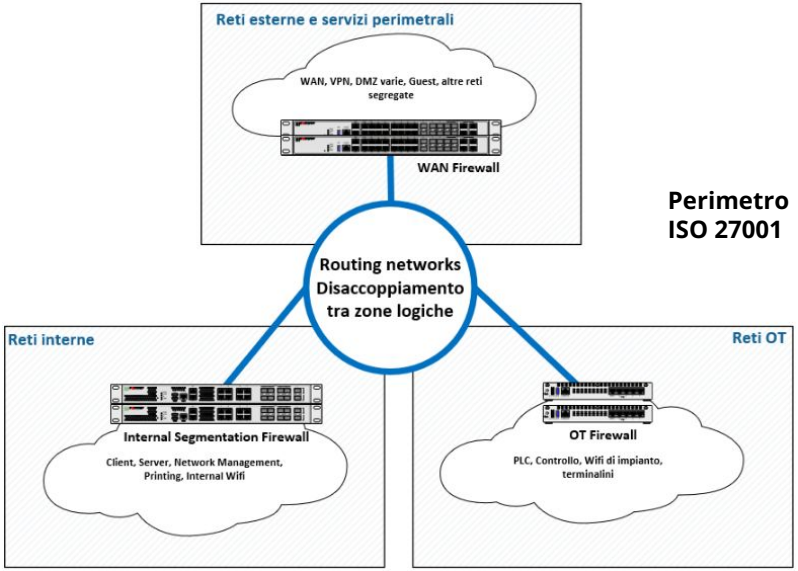
- **Gli account devono essere nominali. Mai condivisi.**
- **Eliminare gli accessi e gli utenti di default.**
- **Applicare chiare politiche su utenti e password** dei sistemi OT.
- Gestire tempestivamente le **revoche degli account**, sia interni che fornitori.
- **Usare MFA** (Multi-Factor Authentication) ove possibile.

SEPARARE GLI **AMBITI**

Network segmentation: metti i muri tra IT e OT.

La razionalizzazione delle reti IT e OT unita alla gestione sicura dei flussi dati è uno dei requisiti fondamentali.

- **Identificazione di tutti gli asset di rete.**
- **Apparati OT-Aware:** devono riconoscere i protocolli industriali (es. Modbus, Profinet).
- **A cosa serve:** virtual patching, application control e intrusion prevention.



Perimetro ISO 27001

Fonte:
https://csrc.nist.gov/CSRC/media/Projects/operational-technology-security/documents/NIST_Control_Systems_Tips_and_Tactics_Infographic.pdf

RESTRICT ACCESS TO THE CONTROL SYSTEM NETWORK & NETWORK ACTIVITY

Implement a layered network topology with a Demilitarized Zone (DMZ) to restrict access to control system networks. Restrict control system access to only users that require it. Consider requiring two-factor authentication for remote access instead of only a password.

GESTIONE DELLA **MANUTENZIONE**

Accesso remoto sicuro: stop alla manutenzione "selvaggia".

Affrontiamo ora un punto critico, da cui arriva gran parte del rischio: come gestiamo l'accesso da remoto ai sistemi di controllo da parte di fornitori e manutentori?

STOP ALLA MANUTENZIONE SELVAGGIA

Cosa dobbiamo rimuovere subito:

- Rimozione **VPN**.
- Rimozione **NAT entranti**.
- Rimozione **utenti e password condivisi**.
- Rimozione di **SIM o apparati per tunnel**.

GOVERNANCE DI TUTTE LE SESSIONI REMOTE

Protezione tramite punti chiave:

- **Portale web dedicato** e protetto da WAF.
- **Accesso manutentivo personale.**
- **Multifactor authentication di default.**
- Accesso **selettivo** alle destinazioni.
- **Registrazione** sessioni testo e video.

SECURITY AWARENESS

Da “user” a “human firewall”

Gli utenti sono sempre stati considerati l’ultimo anello della catena tra gli attaccanti e i nostri dati, spesso considerato il più debole.

Bisogna cambiare punto di vista.

L’utente non deve più essere un anello debole, deve diventare uno “Human Firewall”
Quando le altre misure di sicurezza sono state superate, è l’utente ad essere il bastione di difesa che protegge i dati.

Non esiste una soluzione magica o una formazione one-shot: l**a chiave è la formazione continua unita ad una misurazione continua**.

Il ciclo di misurazione e formazione degli utenti deve diventare cultura aziendale e deve essere periodico e frequente.

ALLENA GLI UTENTI

Forma i dipendenti aziendali attraverso la più grande libreria al mondo di contenuti sulla sicurezza, tra cui moduli interattivi, video, giochi, poster e newsletter.

ANALIZZA I RISULTATI

Report dettagliati sull’andamento della formazione e dei test di phishing

METTI ALLA PROVA GLI UTENTI

Crea attacchi di phishing completamente automatizzati per mettere alla prova gli utenti, attraverso migliaia di template.

LA STRATEGIA **CONTINUA**

Evoluzioni ulteriori: strumenti avanzati e continuità.

Oltre ai capisaldi che abbiamo visto, una strategia moderna di sicurezza industriale richiede l'adozione continua di strumenti di visibilità e di un'infrastruttura resiliente.

VISIBILITÀ E RILEVAMENTO CONTINUO

- **Asset inventory informatizzato e continuo** (visibility).
- **Vulnerability management continuo.**
- **Tracciamento dei changes.**
- **NDR** (Network Detection and Response) **Passive**.
- **EDR** (Endpoint Detection and Response) (dove possibile nel mondo OT!).
- **Logging centralizzato**.

DIFESA, RESILIENZA E GOVERNANCE

- **NAC** (Network Access Control).
- **Strategie di patching** (mirate all'OT).
- **Hardening dei dispositivi.**
- **Architetture di rete resilienti** (SD-WAN, geografiche, ecc.).
- **Infrastrutture resilienti** (datacenter ridondati, host multipli).
- **Servizi SOC** (Security Operations Center).

*E non dimentichiamoci della **sicurezza fisica**, del **controllo accessi**, della **chiusura a chiave dei rack**, ecc...*


EDU TIPS
Q&A

Thank you!

SIMONE **ZABBERONI**

Presales - smeup ICS

simone.zabberoni@smeup.com