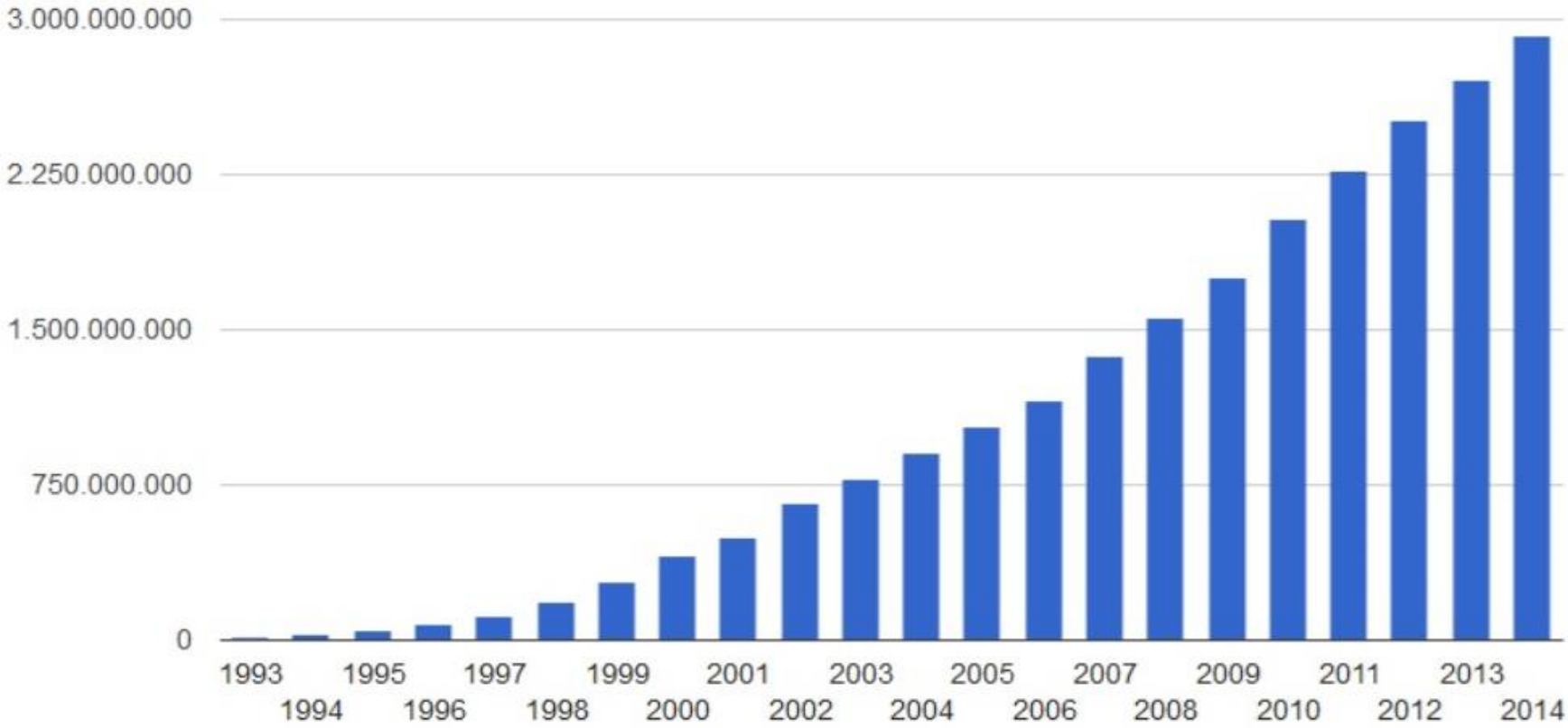
L'importanza della Cyber Security in applicazioni industriali

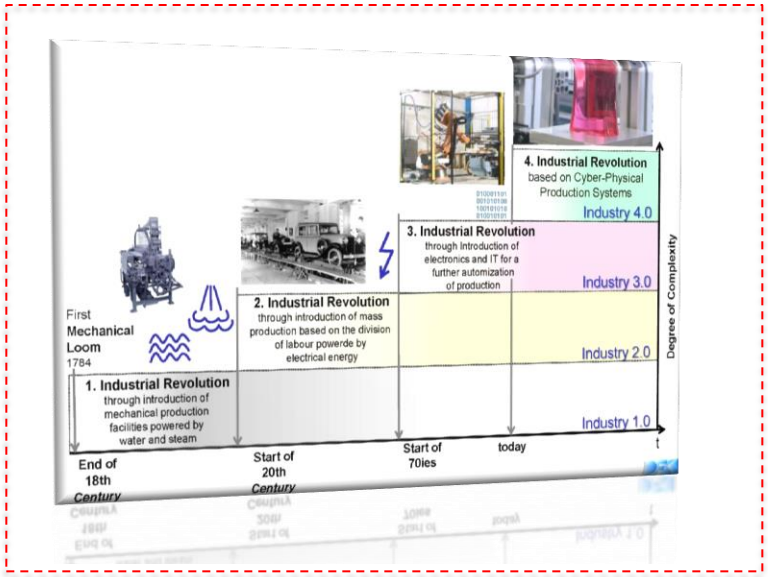
Davide Crispino

Un mondo sempre più connesso



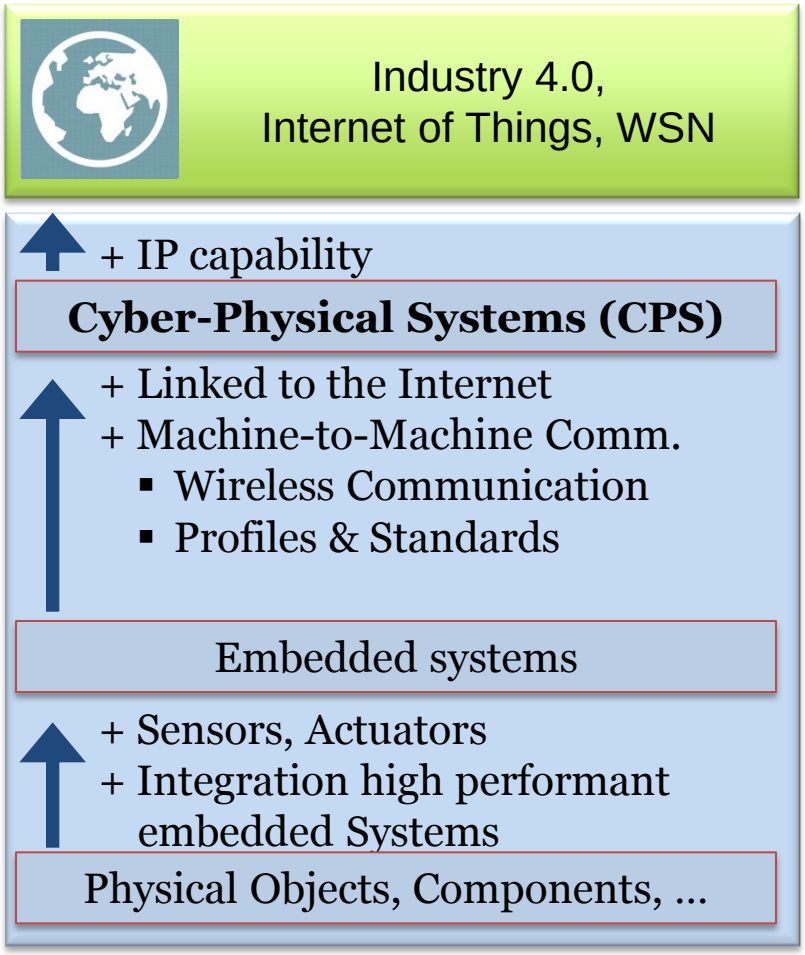
Nel 2020 gli utenti saranno circa 4 Miliardi

I Mega Trend → ancora più Internet



The INTERNET of THINGS

Road to Industry 4.0



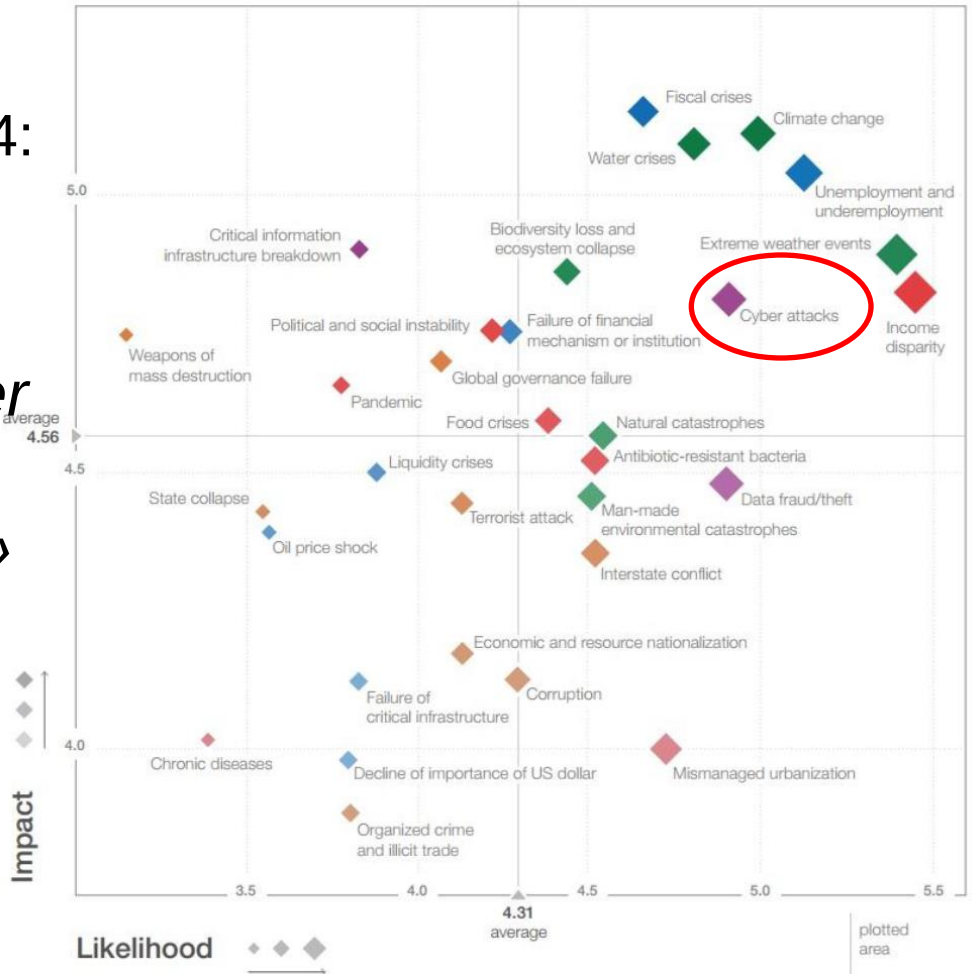
Source: Forschungsunion Wirtschaft – Wissenschaft

- Utilizzare dati e servizi worldwide mantenendo un livello di complessità accettabile
- Sistemi collegati tra loro che controllano entità fisiche e comunicano tra loro
- Adattabilità a variazioni di richieste con aumento efficienza
- Controllo di sistemi e processi complessi
- Sensori

Cyber Attacks: un rischio tra i più temuti

Al World Economic Forum 2014:

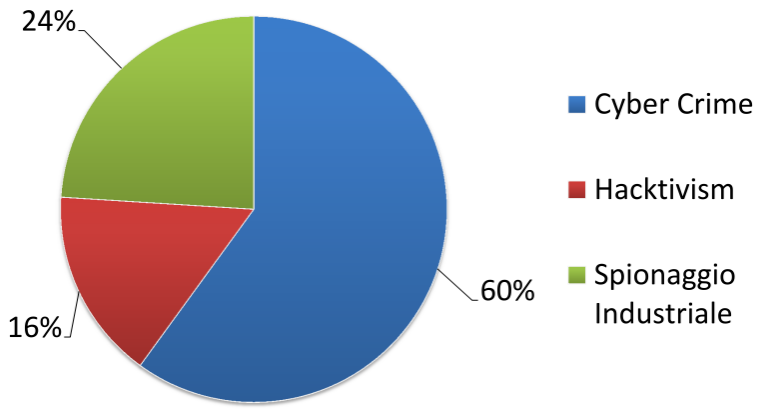
*«**Cyber Attacks** considerati uno dei **rischi più elevati** per l'economia in termini di IMPATTO e PROBABILITA'»*



E in Italia?

- Secondo un rapporto UNICRI del 2014 sulla criminalità informatica, questi sono i numeri per l'Italia:

  875 milioni di dollari all'anno di perdite per danni diretti
  - + danni di immagine e reputazionali, costi di recovery e perdita di business, 8.5 miliardi (0,6% del PIL) (dati McAfee)
  - 9 miliardi di dollari spesi per la perdita di dati sensibili
  - + perdite da interruzioni operative dei sistemi 14,1 miliardi di dollari (dati Emc)

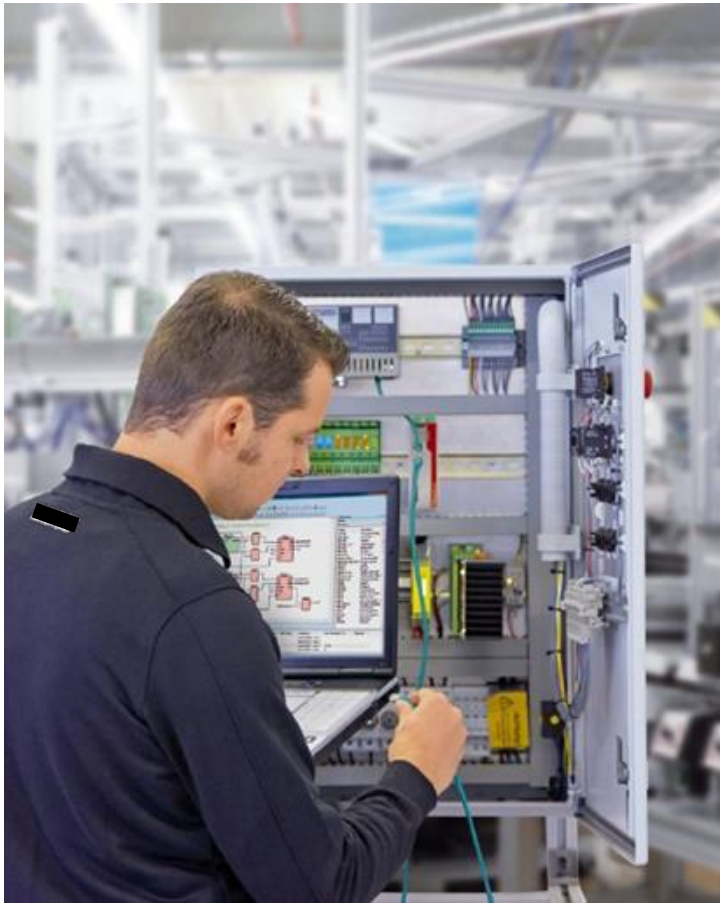


¼ degli attacchi è subito dall'industria per spionaggio !

I rischi per l’industria: dalla rete macchina

Se la rete Ethernet locale (LAN) non è connessa a Internet molti ritengono che non vi siano motivazioni valide per investire in soluzioni tecnologiche o prodotti atti a garantire la Security

Dipendenti o tecnici esterni che accedono alla rete potrebbero introdurre malware all’interno della stessa per mezzo di memorie USB o attraverso PC di servizio



I rischi per l'industria: la durata dei componenti

Il ciclo di vita di una macchina o di un'installazione è spesso superiore ai 20 anni

I produttori di sistemi operativi potrebbero dismettere il supporto per tali sistemi prima del termine del ciclo di vita della macchina (si pensi a Windows XP)

La invulnerabilità dei sistemi non viene più garantita e i rischi associati alla Security aumentano

I rischi per l’industria: l’assenza di antivirus

Programmi antivirus (virus scanner) spesso non vengono utilizzati dagli IPC di macchina

I programmi antivirus standard possono impattare in modo significativo le proprietà ‘’real time’’ dell’installazione

Il caricamento di archivi per riconoscimento virus cambia permanentemente il sistema

I rischi per l'industria: trasmissioni in chiaro

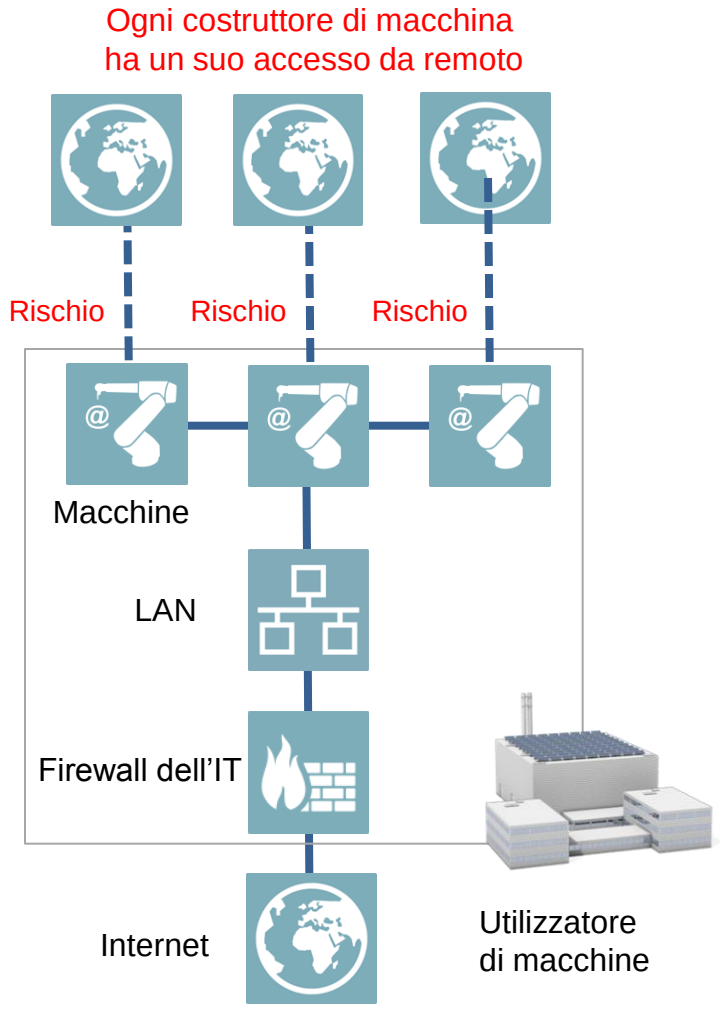
In caso di accesso da remoto, i dati spesso vengono trasferiti via Internet senza essere stati preventivamente cifrati (encryption)

In funzione della rete, i pacchetti dati vengono trasferiti via Internet attraverso diversi percorsi e paesi
Pacchetti dati non cifrati possono essere letti e modificati da un qualsiasi soggetto ovunque nel mondo senza che chi invia I dati e chi riceve gli stessi possa avere la percezione di queste azioni

I rischi per l'industria: la Teleassistenza

L'utilizzatore finale dell'impianto dispone di una rete globale che integra anche le reti disposte su macchine acquistate da diversi fornitori e ogni fornitore ha un accesso da remoto alla ''propria'' macchina

Ogni singola macchina è una potenziale fonte di rischi associati alla Security
Ogni singola rete di macchina può essere infettata o spiata attraverso le reti di tutte le altre macchine



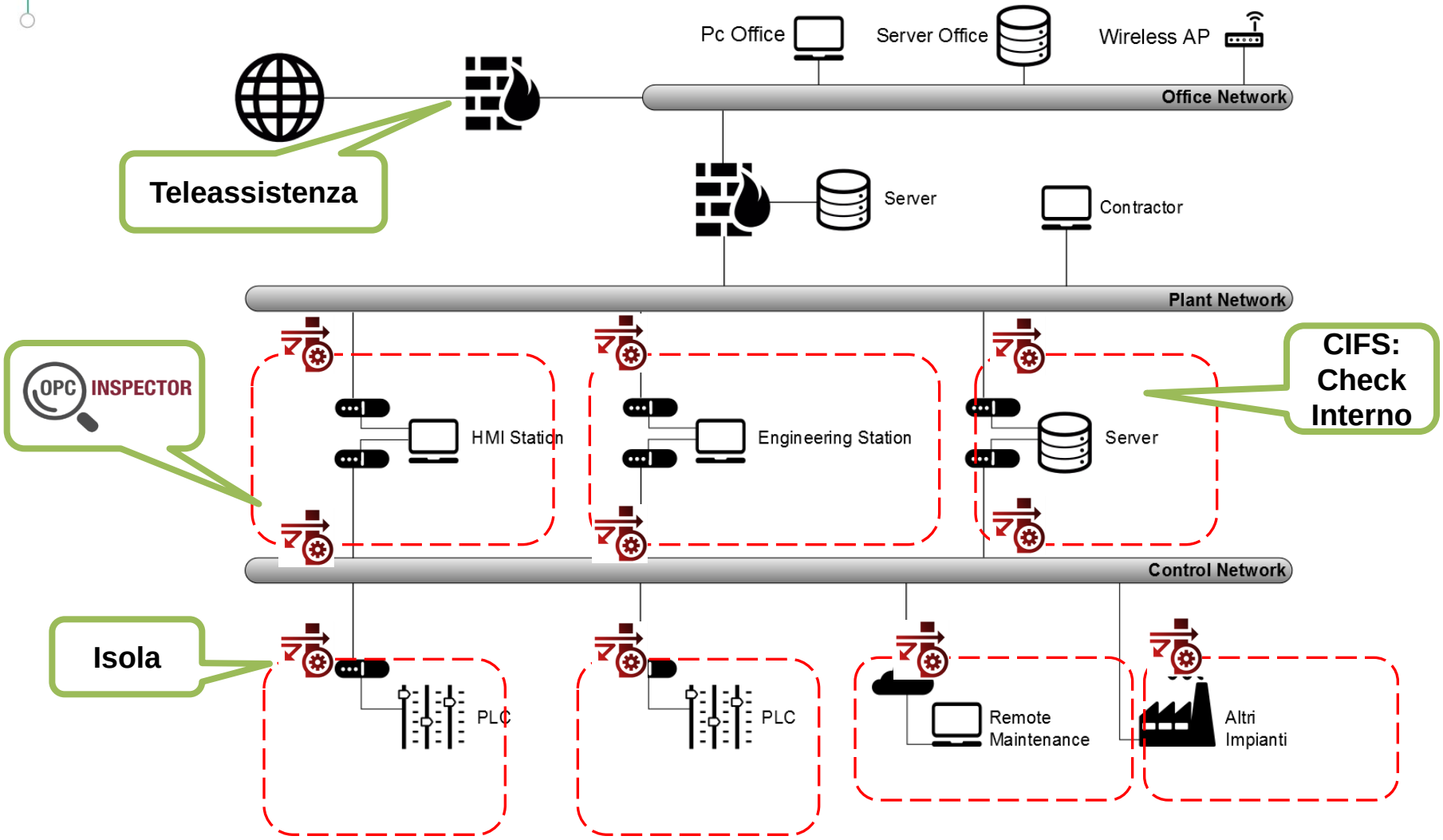
Riflessione sui costi della Security

1	**Perdita dei dati:** Improvvisamente tutti vostri dati vengono persi. Quale potrebbe essere il costo della ricostruzione di tali dati?	Euro _____
2	**Perdita di know-how:** Un vostro competitor riesce ad accedere ai vostri dati sensibili (progettazione, ingegnerizzazione, …). Quanto può economicamente valere il danno?	Euro _____
3	**Fermi di produzione:** A causa di problemi legati alla security, la produzione deve arrestarsi per alcune ore, Quanto può essere il costo di una tale mancata produzione?	Euro _____
4	**Ore lavoro dei vostri dipendenti:** Quante ore lavoro dei vostri dipendenti sarebbe necessario impiegare per risolvere i danni generati da una falla nelle vostre misure di security?	Euro _____
5	**Hijacking dai vostri computer:** Quanto potrebbe costare una campagna di comunicazione per spiegare che una terza parte ha usato i vostri sistemi per spiare o attaccare un'altra società?	Euro _____
6	**Reputazione:** Quanto potrebbe essere importante un danno alla vostra reputazione se i vostri clienti non riponessero in voi la giusta fiducia circa la protezione da Cyber attacchi?	Euro _____

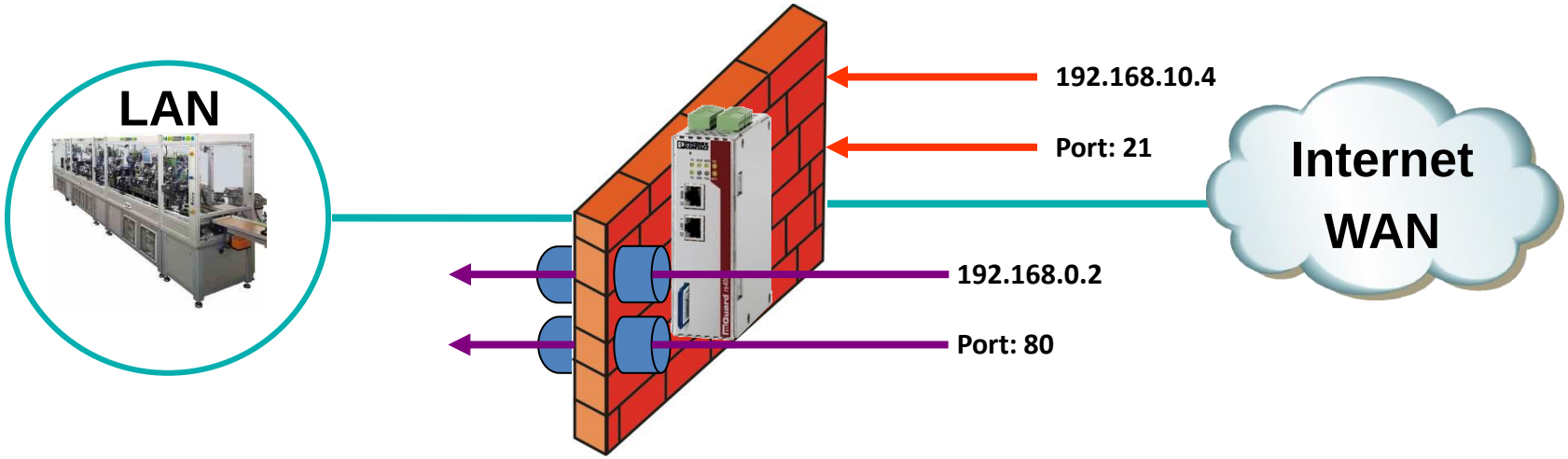
Totale: Euro

_____

Architettura Cyber Security per Impianti



Le soluzioni Cyber Security: Firewall



Defined Firewall-Rules:

1. **Accept: From TCP - Port 80**
2. **Accept: From IP - Address 192.168.0.2**

Network Security » Packet Filter

Incoming Rules | Outgoing Rules | Sets of Rules | MAC Filtering | Advanced

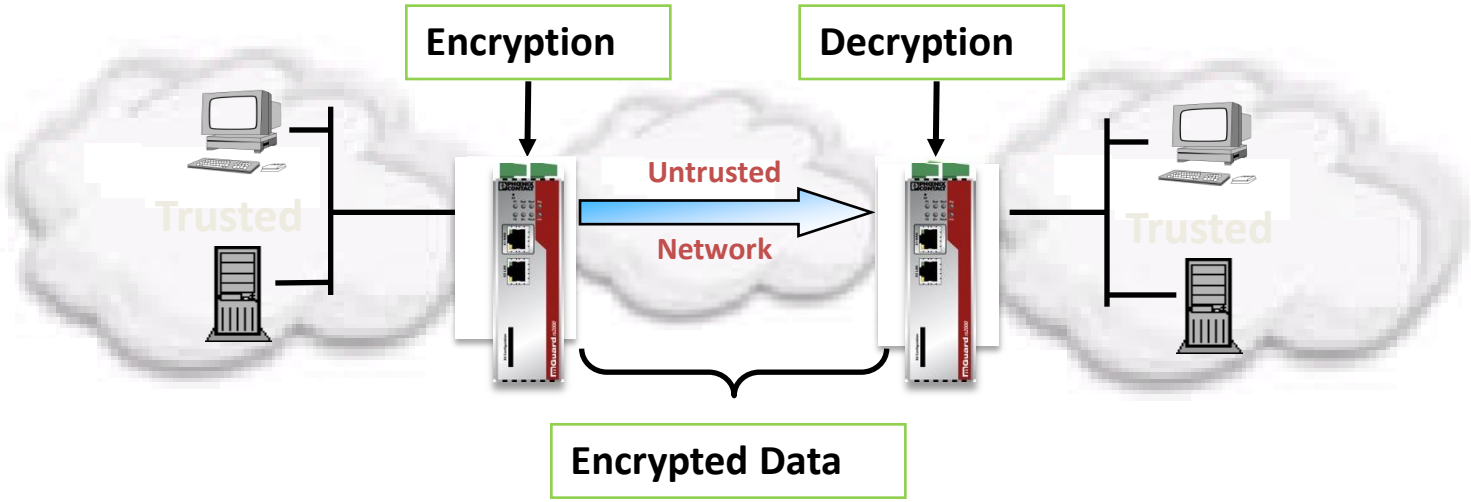
Incoming

Log ID: fw-incoming-N°-05c7bcda-8dba-17b7-981e-bbbcbeb2ac20

	Nº	Interface	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
	1	External	TCP	0.0.0.0/0	any	0.0.0.0/0	80	Accept		No
		External	All	192.168.0.2	any	0.0.0.0/0	any	Accept		Yes

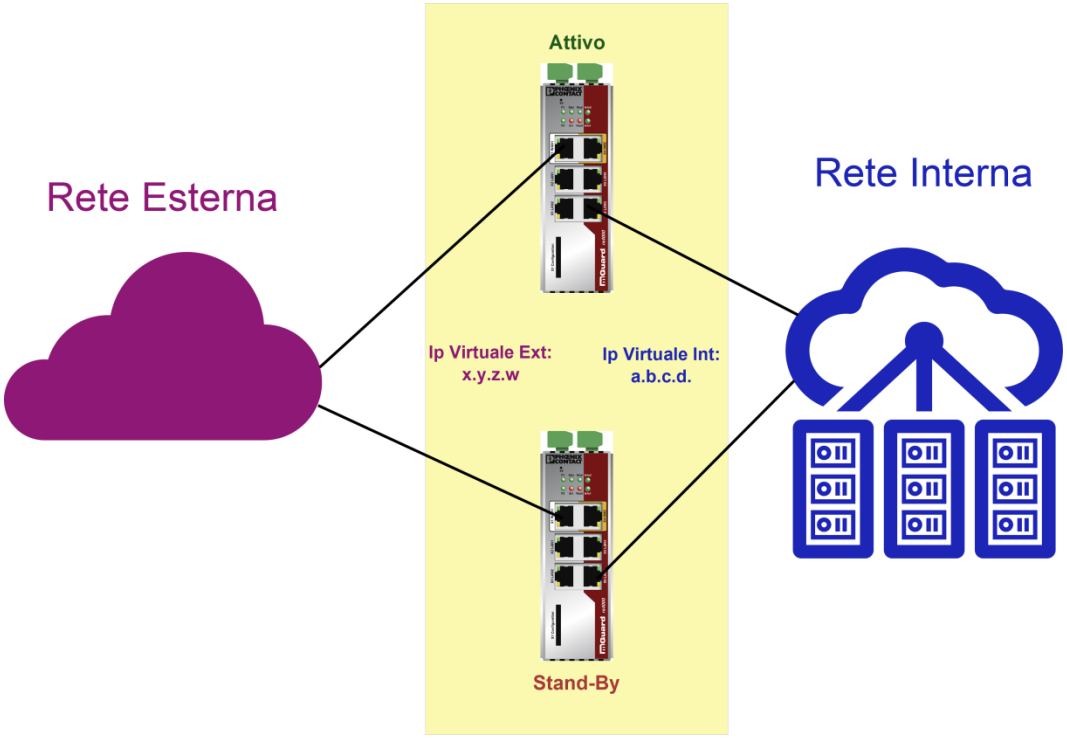
Le soluzioni Cyber Security: VPN

Un tunnel VPN consente una comunicazione crittografata e quindi sicura attraverso una rete esterna (WAN) "insicura" (ad esempio Intenet).



Le soluzioni Cyber Security: Ridondanza

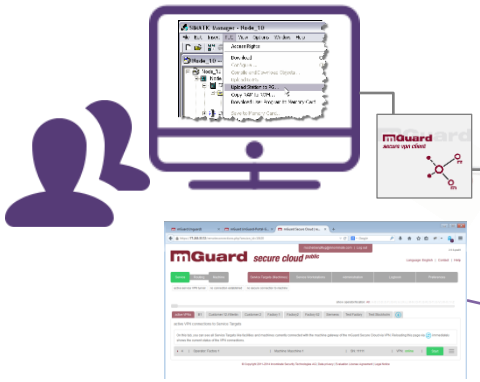
- Due Firewall possono essere collegati in modalità ridondante
- Lo stato delle connessioni viene aggiornato continuamente in modo che non ci sia interruzione in caso di switchover
- É possibile garantire la ridondanza anche per i tunnel VPN



Le soluzioni Cyber Security: Secure Cloud

Massima disponibilità per il host

Costruttore di macchina / Tecnico di servizio



VPN-Servizio:
connessione VPN criptata con IPsec dal mGuard Secure VPN Client verso il Gateway servizio

VPN: online

Gateway servizio (virtuale)

Secure Cloud App

Routing & Management

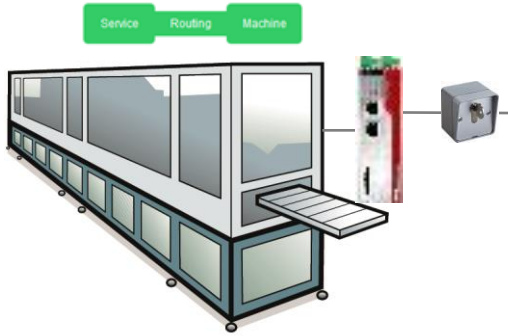
Internet

VPN: online

Gateway macchina (virtuale)

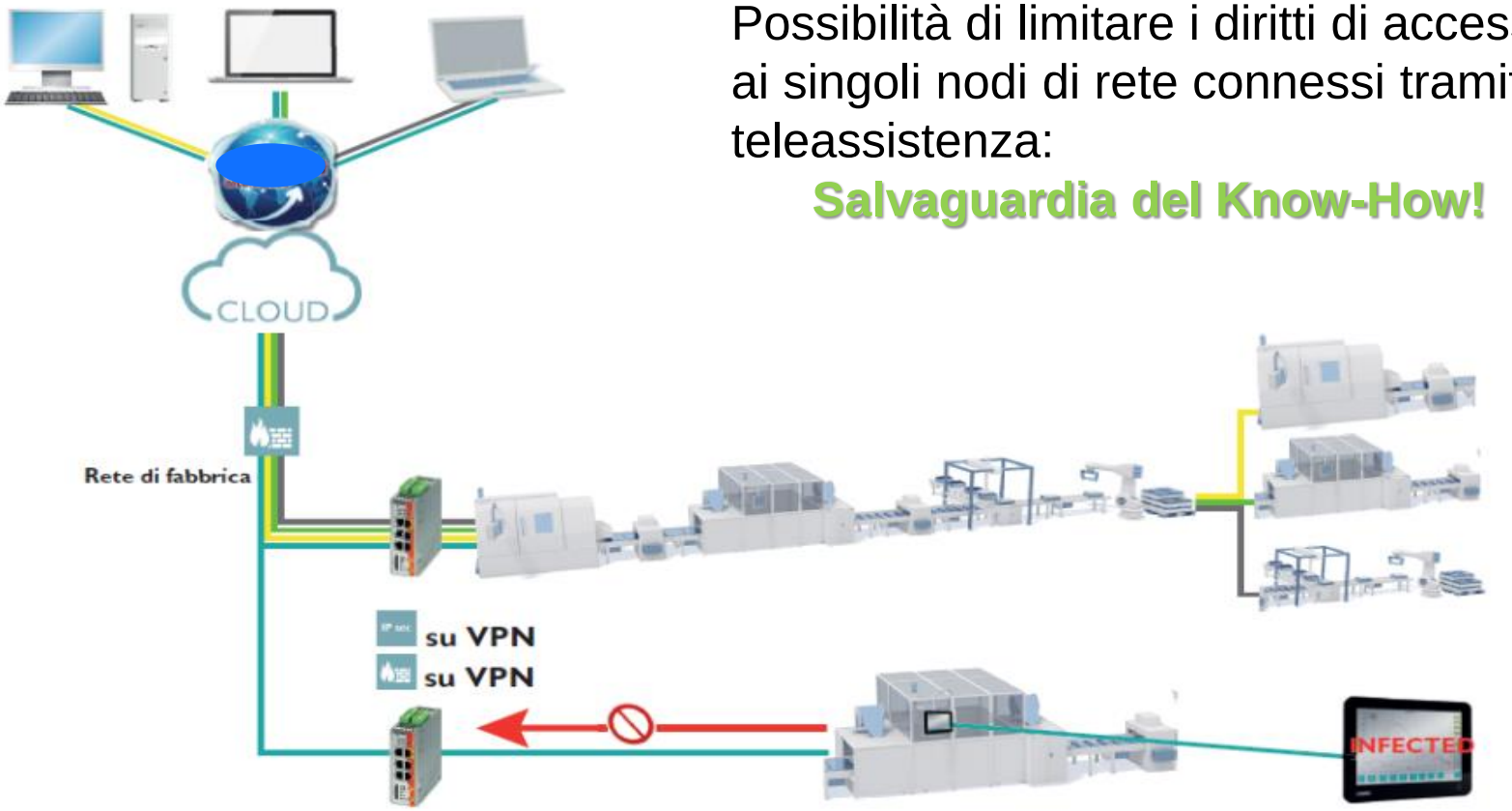
VPN macchina:
connessione VPN criptata con Psec verso il Gateway macchina

Macchina presso il cl. finale



Raggungibile tramite il indirizzo IP reale

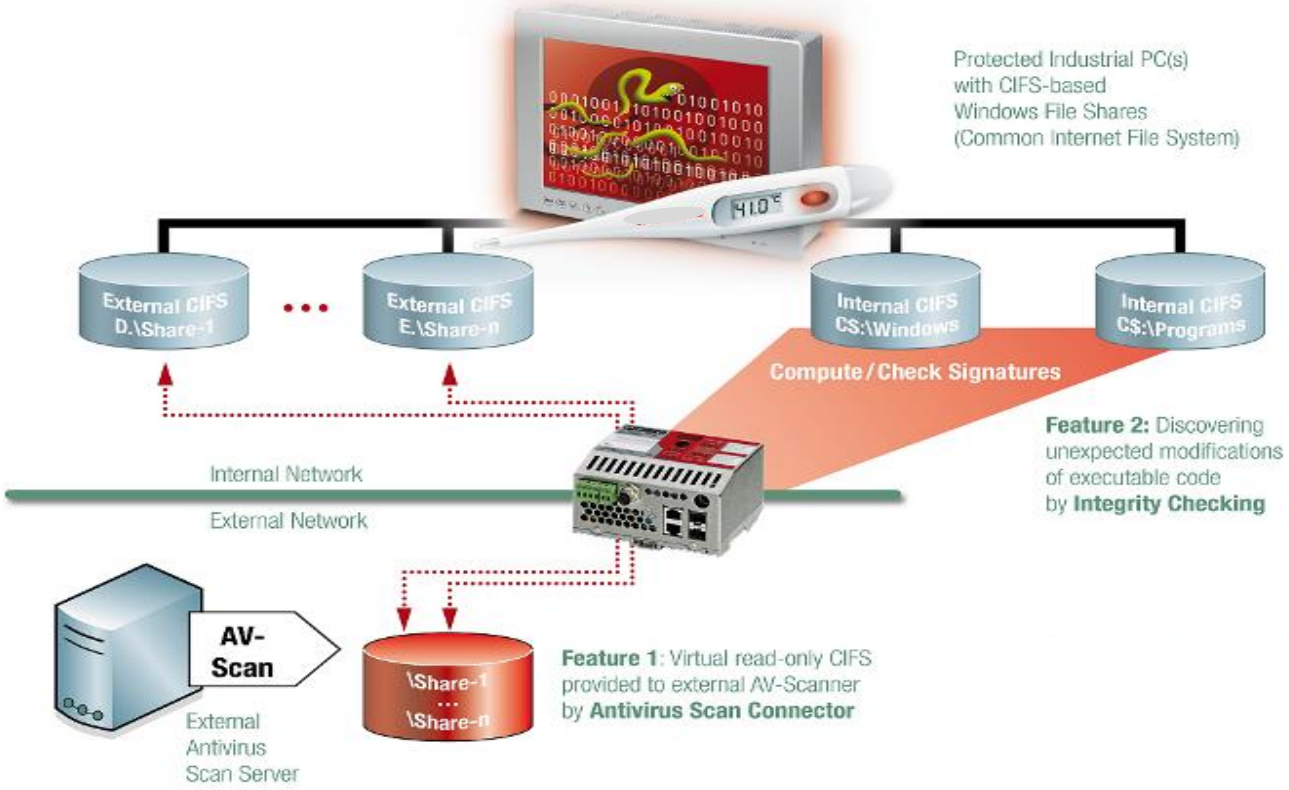
Le soluzioni Cyber Security: Regole di Accesso



Possibilità di limitare i diritti di accesso ai singoli nodi di rete connessi tramite teleassistenza:

Salvaguardia del Know-How!

Le soluzioni Cyber Security: CIFS

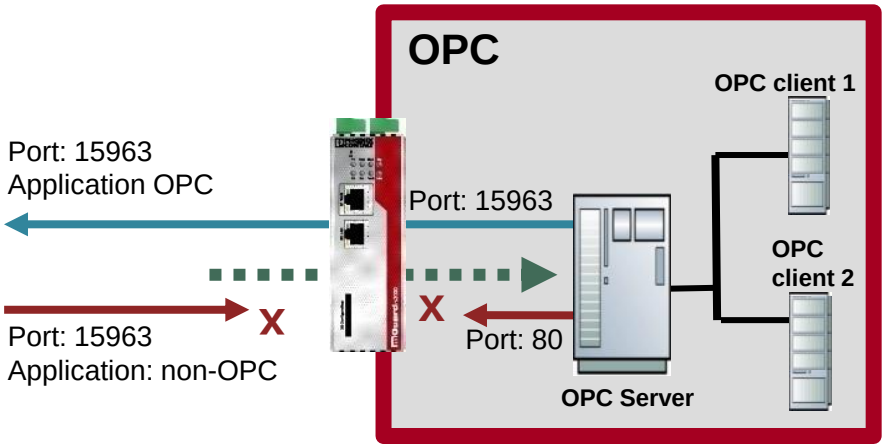


Possibilità di rilevare automaticamente tutti i cambiamenti apportati ai file dei PC di macchina senza necessità di installare Antivirus a bordo

Le soluzioni Cyber Security: Deep Packet Inspection

- Utilizzare firewall che siano in grado, dinamicamente, di creare delle regole di firewall per protocolli che cambiano continuamente le porte in uso; classico esempio la comunicazione OPC DA.

- Identificare e bloccare tutto il traffico che non corrisponde alla porta aperta nel firewall



Grazie dell'attenzione