SIEMENS

On line-Training Configurazione e Programmazione Sicura dei Sistemi a Controllo Numerico (DI-CNHARD)

Breve descrizione

Continuano a crescere in modo esponenziale gli incidenti informatici che coinvolgono impianti di automazione e di controllo di siti industriali. L'impatto che hanno può avere conseguenze molto gravi, non solo per il ciclo produttivo ma anche per la tutela delle persone e dei beni.
Malware come **WannaCry**, **Industroyer** e **Petya/NotPetya** a partire dal 2016 hanno dato origine ad attacchi su larga scala. La soluzione però non è solo l'adozione degli ultimi ritrovati della tecnologia, ma è soprattutto l'adeguata preparazione del personale di tutta l'azienda, che molto spesso rappresenta l'anello debole dell'intera catena della sicurezza.
Per questa ragione proponiamo un corso di formazione dedicato alla configurazione e alla programmazione dei sistemi di automazione (PLC, HMI, CN) con un approccio orientato alla cybersecurity, che fornisce ai programmatori le competenze necessarie a implementare l' hardening dei diversi dispositivi e la sicurezza "by design" nel software applicativo e accrescere quindi il livello di resilienza dell'intero sistema d'automazione. Il corso è frutto di oltre 20 anni di esperienza sui sistemi SCADA, PLC, fieldbus, I/O remoti e controlli numerici.

Obiettivi

Dopo aver frequentato il corso sarai in grado di:
- Comprendere gli aspetti della cybersecurity specifici per le applicazioni OT
- Individuare i potenziali rischi cyber di un impianto di automazione
- Progettare un sistema di PLC, HMI e CN che offra maggiore protezione contro attacchi cyber
- Scrivere un'applicazione industriale che includa la sicurezza cyber "by design"
- Diagnosticare e correggere problemi di esecuzione del programma di automazione con impatto sulla cyber

Gruppo target

- Programmatori CNC
- Manutentori e installatori
- Operatori e conduttori di macchine e impianti

Contenuti del corso

La cybersecurity OT
- L'impatto della sicurezza informatica
- Gli scenari e le tecnologie
- Le caratteristiche delle applicazioni ICS e SCADA
- Le diverse tipologie di attacchi
- Il MITRE ATT&CK for ICS
- Le vulnerabilità nei prodotti di automazione
- Cenni alla normativa IEC62443

Le basi di networking e sicurezza
- Gli elementi di una rete, tipologie di reti e zone
- I protocolli di comunicazione sicuri
- Concetti base di crittografia e hashing
- Segmentazione, segregazione e isolamento delle reti
- Tunneling e VPN
- I dispositivi di sicurezza
- Il monitoraggio dell'architettura OT/ICS

Programmazione sicura dei PLC
- Programmazione modulare e strutturata
- Monitoraggio del funzionamento corretto del PLC
- Gestione sicura del ciclo di esecuzione del programma e di ripristino
- Gestione e ottimizzazione della memoria del PLC
- Check di integrità del software e dei dati
- Validazione di input/output e delle risorse interne (timers, counters, blocchi funzione)
- Interazione sicura con dispositivi HMI e SCADA
- Monitoraggio, log e gestione di alerts ed eventi
- Comunicazione sicura con altri devices

CN Hardening
- Separazione fisica delle Reti macchina dalla Rete Aziendale
- Password e selettore a chiave
- Disattivazione automatica Password tramite PI_SERV
- Gestione accesso dati tramite USER_CLASS
- Customizzazione visualizzazione softkeys tramite livello di accesso
- Opzione Lock MyCycle
- Opzione CNC Lock Function (solo per SINUMERIK 828d)
- Know How protection degli azionamenti (lista eccezione parametri)
- Utilizzo del drive di rete/MMP per la condivisione dei PartProgram, evitando l'uso di USB Stick

IPC/PCU Hardening
- Prodotti obsoleti (scarsa sicurezza informatica o nulla) PCU Retrofit
- Firewall (attivazione manuale delle porte su rete aziendale)
- Aggiornamento Base Software
- Aggiornamenti di Windows
- Whitelisting

Protezione del collegamento aziendale e remoto
- Password VNC su rete aziendale
- SSH Key file per collegamento tramite Access MyMachine
- OPC UA (crittografia, accesso anonimo, diritti di scrittura dati)
- Utilizzo di SCALANCE S
- SINEMA Remote Connect

Sicurezza della macchina in caso di attacco esterno
- Backup esterno degli archivi macchina (per evitare la perdita degli archivi)
- Backup esterno dei PartProgram (per evitare la perdita dei programmi)
- Gestione centralizzata degli utensili (MMR/Tools) (per evitare la perdita degli utensili)
- Opzione Collision Avoidance/Protect MyMachine (per evitare collisioni)
- Opzione Monitoring Tool Speed/Acceleration (per evitare danni agli utensili)

Ripristino rapido del sistema
- Ripristino del CN: archivi frequenti, backup del programma PLC aggiornato (SIMATIC STEP 7, TIA Portal)
- Ripristino dell’IPC/PCU: Ghost aggiornato
- Ripristino della CF/SD Card: TGZ aggiornato, gestione cartacea delle licenze

Tipologia

Formazione online

Durata

2 giorni

Lingua

it