SIEMENS

On line-Training Configurazione e Programmazione Sicura dei Sistemi di Automazione (DI-S7HARD)

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, Drive) 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.

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 SCADA che offra maggiore protezione contro attacchi cyber
- Scrivere un'applicazione PLC che includa la sicurezza cyber "by design"
- Diagnosticare e correggere problemi di esecuzione del programma PLC con impatto sulla cyber

Gruppo target

- Programmatori PLC e HMI/SCADA
- 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

PLC Hardening (SIMATIC S7-300/400, SIMATIC S7-1200/1500)
- Protezione fisica di un sistema di controllo (lucchetto, password del display nei SIMATIC S7-1500, disabilitazione porte non utilizzate)
- Protezione di accesso all'hardware (gestione password in scrittura/lettura)
- Protezione del software (protezione del know-how, copia del progetto)
- Protezione di un progetto (definizione utenti e ruoli)
- Protezione dei dati (confidential PLC configuration, secure S7/OUC/OPC UA communication, web server)
- Accesso da remoto con CP dedicata (VPN, SINEMA)
- Monitoraggio di potenziali accessi non autorizzati (log di accesso, monitoraggio del tempo ciclo, …)

HMI Hardening (SIMATIC WinCC Comfort, SIMATIC WinCC Unified)
- Protezione fisica di un sistema di supervisione (gestione utenti per l'accesso al dispositivo, gestione porte USB)

- Trasferimento del progetto utilizzando una chiave privata
- Comunicazione sicura con un sistema di controllo (Secure S7, OPC UA)
- Protezione delle funzionalità (gestione delle autorizzazioni utenti)
- Accesso remoto (Sm@rt options)

Tipologia

Formazione online

Durata

2 giorni

Lingua

it