Corso - 27/02/2024

Cybersecurity applicata alle macchine e impianti

Come connettersi in sicurezza, i protocolli esistenti, le normative internazionali di riferimento per una corretta analisi dei rischi.
(Modulo destinato anche agli utilizzatori di macchine e impianti).

Obiettivi

L'avvento di Industry 4.0 sta sempre più determinando l'esigenza di connettere in rete tutte le macchine ed impianti, il più delle volte senza una precisa direttiva e protocolli tecnici e spesso in modo "non protetto".
I rischi in questo caso sono enormi: difendere le aziende e le macchine da attacchi hacker non riguarda solo l'evitare l'accesso e l'acquisizione impropria dei dati di produzione, ma anche evitare interferenze sulla parte safety dei macchinari, risvolti sulla qualità dei prodotti, fino ad arrivare ad accessi all'intera rete informativa aziendale.

Ecco quindi l'innesto della Direttiva NIS2 (Network and Information Security) che ha l'intento di rafforzare il livello globale di cybersicurezza all'interno di aziende, l'adozione di misure tecniche ed organizzative adeguate contro i rischi cyber attraverso un aumento delle capacità di resilienza aziendale su tutto il processo di gestione di tali rischi, dalla capacità di prevenire alla capacità di minimizzare l'impatto che tali incidenti possono causare.

Programma

Cenni ed evoluzione dalla NIS alla NIS 2:

- la direttiva NIS 2;
- concetto di Safety and Security ? Sinonimi o Complementari ?;
- alcuni casi di Cyber Attack, ransomware e furto di dati;
- cyber Security e GDPR.

Differenze di approccio, ed il nuovo concetto di multirischio e della filiere di approvvigionamento dei servizi informatici:

- politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
- gestione degli incidenti; (ISO 27035)
- continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi; (ISO 22301)
- sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi; (ISO 27000-1 e ISO 20000-1)
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità; (ISO 20000-1)
- strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cyber sicurezza;
- pratiche di igiene informatica di base e formazione in materia di cybersicurezza.

L'analisi dei rischi e definizione di Protection Level, Security Level Target e Maturity Level:

- distinzione IT/OT e requisiti di sicurezza associati;
- definizione IT/OT, differenze e peculiarità, defence in depth;
- struttura dello standard IEC 62443;
- concetti generali: organizzazione, ruoli (service provider, asset owner, manufacturer);
- IEC 62443-3-2 Security Risk Assessment and System Design;
- IEC 62443-3-3 System Security Requirements and Security Levels.

Destinatari

RSPP e ASPP, Responsabile manutenzione, Responsabile produzione, Responsabile Formazione, Responsabili IT, Responsabili OT, programmatori di PLC, Uffici Tecnici aziendali.

Durata
8 ore

Quota di adesione:
400,00 € + IVA a persona per le aziende associate
500,00 € + IVA a persona per le aziende non associate

Date e Sedi di svolgimento
27/02/2024 14.00-18.00 - ONLINE
28/02/2024 14.00-18.00 - ONLINE