SIEMENS

On line-Training OT Cyber Security lato End user, applicando la IEC 62443-2 (IK-SEC2)

Breve descrizione

A valle dell'introduzione alla cyber security in ambito industriale effettuata con il modulo 1, si entra nel dettaglio dei processi applicabili per un end user, come descritti nella IEC 62443, in particolare la sezione 2. La norma presenta infatti un life cycle che include 3 fasi principali: quella di assessment in cui l'azienda prende coscienza del rischio derivante da attacchi cyber agli impianti industriali e valutare quindi il rischio tramite un processo di risk assessment, quella relativa all'implementazione, dove l'azienda dovrà dotarsi delle necessarie figure, ruoli e responsabilità per attuare i processi di implementazione delle misure tecniche e organizzative necessarie per la mitigazione e gestione dei rischi e infine la parte di mantenimento, dove tramite audit e monitoraggi si dovrà garantire l'efficacia dei processi attuati. In questo modulo si vedranno quindi le modalità di implementazione dei processi richiesti dalla norma all'interno di un tipico end user industriale, partendo dalle necessità di gestire il rischio e quindi il problema e concentrandosi sulle modalità attuative che dovranno riguardare sia la parte di organizzazione del sistema di gestione per la cyber security, andando eventualmente ad integrare quanto già presente sotto forma di altri sistemi di gestione (ad esempio ISO 27001), sia la parte di implementazione delle misure tecniche in riferimento alla IEC 62443-3-3 che definisce i requisiti di base da attuare in funzione del security level e quindi del livello di sicurezza richiesto.

Obiettivi

Dopo aver frequentato il corso sarai in grado di:
- Capire come far prendere coscienza al management aziendale del rischio cyber sugli impianti e come presentare al management un piano ed un budget per la gestione della cyber security in ambito industriale
- Capire l'importanza di un processo di risk assessment come elemento chiave per la definizione delle misure necessarie
- Capire i processi fondamentali per l'implementazione delle misure di sicurezza, compreso quelle di emergenza
- Capire il ruolo di un integratore o un service provider e le responsabilità connesse con le attività svolte
- Capire come gestire la supply chain e la selezione dei prodotti da integrare sugli impianti in relazione alla security
- Spiegare cosa è una vulnerabilità e come può essere sfruttata durante un attacco
- Capire le metodologie di attacco informatico e gli strumenti utilizzati
- Comprendere l'importanza dell'essere umano e delle tecniche di social engineering per sottrarre informazioni rilevanti

Gruppo target

Per il livello di dettaglio attuato, questo corso si intende indirizzato a personale chiamato a gestire gli aspetti di security a livello aziendale e che si trova a lavorare con i sistemi di gestione aziendali, al personale chiamato alla gestione degli impianti di automazione, agli integratori, e alla supply chain in genere per capire le potenziali necessità di un end user.

Contenuti del corso

- La IEC 62443-2 e presentazione delle 3 fasi del life cycle: assessment, implementazione e mantenimento
- Le attività connesse al risk assessment, dal business rationale alla valutazione di alto livello e di dettaglio
- L'attacco cyber, modalità esecutive ed esempi
- Il social engineering e l'elemento umano, come anello debole della catena di security
- Interpretare i risultati della valutazione dei rischi: dal security level, zonizzazione e requisiti di security
- Architetture di riferimento e principi di security
- Gli elementi chiave di un organizzazione che lavora per processi. Dalla definizione di ruoli e responsabilità alla formazione
- Gestione degli asset e della relativa documentazione e informazioni
- Requisiti tecnici. Definizione delle specifiche in riferimento al security level tramite la IEC 62443-3-3
- Implementazione delle misure e piani di adeguamento progressivo dell'infrastruttura
- Piani di business continuity
- Ottenimento del security level target e verifiche
- Mantenimento del livello di security tramite auditing e controllo operativo, monitoraggio

Il corso comprende esempi, messi a punto su componenti e sistemi reali, seppur in ambito di laboratorio.
Durante il corso verranno svolte esercitazioni di gruppo e singole, per facilitare e verificare l'apprendimento degli argomenti descritti.

Prerequisiti partecipante

Conoscenze base dei sistemi di automazione, dei sistemi di gestione, con particolare riferimento alla security.

Nota

Non è prevista alcuna documentazione.

Tipologia

Formazione online

Durata

8 ore

Lingua

it