SIEMENS

On line-Training II Risk Assessment in ambito OT Cyber Security, IEC 62443-3-2 (IK-SECRISK)

Breve descrizione

In parallelo e a completamento del corso IK-SEC2, questo modulo prevede un importante approfondimento sulla valutazione dei rischi, ritenuto come strumento chiave per la predisposizione delle misure necessarie e per la conseguente gestione del rischio cyber sugli impianti industriali. Dopo aver approfondito tecniche e strumenti utilizzati per gli attacchi, con simulazioni ed esempi di attacco, sarà approfondito il processo di risk assessment. Il primo step sarà la definizione del business rationale ossia del criterio di risk assessment da utilizzare concordato con il management aziendale. Quali sono le conseguenze critiche per il business in caso di attacco? Quali sono i vari livelli? Quali sono le potenziali minacce critiche che possono compiere un attacco? La risposta a queste domande sarà l'elemento chiave per organizzare un buon processo di risk assessment. A valle della definizione dei criteri (il business rationale), il passo successivo prevede l'esecuzione dell'analisi dei rischi di alto livello, ossia dell'analisi fatta sugli asset industriali con l'obiettivo di capire dove potremo avere delle conseguenze critiche e di quale livello e quindi derivare la lista degli asset critici che meriteranno un approfondimento con l' analisi dei rischi di dettaglio. Questa analisi, molto più approfondita della precedente, richiederà una analisi specifica sugli asset critici, allo scopo di valutare architetture, dispositivi, protocolli e vulnerabilità con una analisi del traffico di rete dedicata e quindi capire quali possono essere vettori e scenari di attacco. Essendo una analisi molto complessa, si può capire come l'analisi di alto livello abbia essenzialmente lo scopo di scremare la lista degli asset critici al fine di ottimizzare il processo di assessment e quindi andare nel dettaglio solo dove utile a fare informazioni aggiuntive per valutare le problematiche e attuare le misure di contenimento de rischio più idoneo. L'obiettivo finale del processo sarà quindi la determinazione di una specifica di cyber security che a partire da una segmentazione della rete permetta di capire come e dove intervenire per la mitigazione del rischio.

Obiettivi

Dopo aver frequentato il corso sarai in grado di:
- Impostare un processo di risk assessment in ambito cyber security industriale
- Definire i criteri e i metodi per l'esecuzione di un risk assessment
- Descrivere come si valutano e presentano i rischi per il business in ambito cyber
- Capire come si acquisiscono le informazioni sulle minacce e come si può fare una valutazione delle minacce credibili
- Capire cosa è una vulnerabilità, come viene categorizzata e catalogata, come può essere sfruttata per compiere un attacco
- Capire come effettuare una analisi di vulnerabilità, con quale scopo e con quali strumenti effettuarla
- Capire come viene stimato un rischio e allocato un security level e come si arriva alla zonizzazione e segmentazione della rete
- Descrivere le architetture di riferimento presentate nella IEC 62443 e capire come utilizzarle all'interno di una specifica infrastruttura
- Capire come proteggere le aree più critiche dell'impianto
- Capire i requisiti di security organizzati nella IEC 62443-3-3 e come questi concorrono agli obiettivi di security
- Descrivere come nasce una specifica di cyber security e la sua importanza

Gruppo target

Per il livello di dettaglio attuato, questo corso si intende indirizzato a personale chiamato a effettuare valutazione del rischio in ambito cyber all'interno di una organizzazione di un end-user o ad integratori che dovranno effettuare valutazioni del rischio per dimostrare all'end user il soddisfacimento degli obiettivi di security.

Contenuti del corso

- Il processo di assessment per IEC 62443-2-1 e la contestualizzazione dei criteri e del metodo con riferimento alle IEC 62443-3-2
- Il business rationale, come criterio e step fondamentale per la determinazione dell'impatto sul business di un potenziale attacco
- L'analisi dei rischi di alto livello e la determinazione degli asset critici e delle minacce credibili
- Analisi della rete, scansioni attive e passive, analisi di vulnerabilità, penetration test, tutti strumenti per l'ottenimento di informazioni preziose su di una rete industriale
- Dinamica e simulazioni di attacco, vettori e scenari di attacco all'interno della valutazione dei rischi di dettaglio.
- Analisi dei rischi di dettaglio, come utilizzare le informazioni della valutazione dei rischi di alto livello e dell'analisi di vulnerabilità per la determinazione del reale rischio sugli impianti
- Quale è il risultato della valutazione: security level, zonizzazione e determinazione dei processi e delle misure necessarie
- Il legame fra la IEC 62443-3-3 e il risultato del risk assessment
- Dalla valutazione del rischio alle specifiche di cyber security e relativa implementazione
- Dal security level target al security level effettivamente raggiunto, come misurare le performance di security

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 e delle reti, dimestichezza con i principi e metodi di risk assessment.

Nota

Non è prevista alcuna documentazione.

Tipologia

Formazione online

Durata

8 ore

Lingua

it