ALFA-ACADEMY

INDUSTRIA 4.0

La sicurezza nelle tecnologie IoT

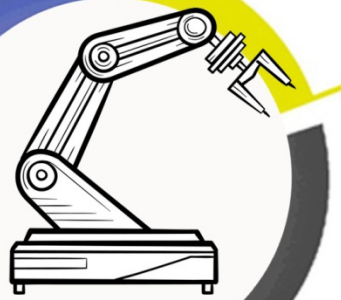
A CHI SI RIVOLGE

Il corso è rivolto a persone che devono interagire in maniera costante con macchine, processi e prodotti, operatori con compiti nella filiera produttiva, chiunque svolga mansioni per cui sia necessario acquisire o consolidare le conoscenze delle tecnologie previste dal Piano Transizione 4.0.

OBIETTIVI

Nell'Industry 4.0 l'infrastruttura IoT/M2M rischia di essere carente in sicurezza, per mancanza di conoscenza da parte degli utilizzatori. I dispositivi IoT, sono soggetti alle stesse problematiche e vulnerabilità di un computer, con l'aggravante che – essendo dispositivi in genere più semplici – sono ancora meno protetti e quindi più attaccabili. Questa connettività potrebbe consentire agli "aggressori" di utilizzare un dispositivo IoT compromesso per bypassare le impostazioni di sicurezza della rete e lanciare attacchi contro altre apparecchiature di rete come se fosse "dall'interno". I dispositivi IoT andrebbero quindi protetti come si protegge un computer, con un uso attento delle password e firewall e con sistemi di tipo UBA (User Behaviour Analytics) posti in una rete separata. L'obiettivo di questo

TIPOLOGIA DI EROGAZIONE
Courseware multimediale



FRUIZIONE
6 mesi

REQUISITI
Sistema operativo:
WINDOWS, MAC
browser:
FIREFOX (ultima versione)
Requisiti da installare:
Adobe Flash Player, Java (ultime versioni)

DURATA
7 ore

CODICE CORSO
0IN4029

INDUSTRIA 4.0

ALFA-ACADEMY

CONTENUTI

Internet of Things (IoT) e Industry 4.0: considerazioni preliminari
- Intervento dell'autore
- IoT e Industry 4.0: introduzione
- IT vs. ICS/OT: un rapporto complicato con priorità differenti
- I sistemi ICS: modello ANSI/ISA-95 e IDMZ (Industrial Demilitarized Zone)

Le norme di riferimento in ambito ICS
- NIST, ISO e la ISA99/IEC62443
- La Direttiva NIS 2016/1148 ed il Cybersecurity Act

Come si è evoluto il Cybercrime
- I numeri nel mondo ed in Italia
- Il Rapporto Clusit

Attacchi ICS: alcuni casi famosi
- Tanti tipi di attacchi
- Un caso inquietante… ma possibile
- L'attacco Stuxnet
- Shamoon colpisce Saudi Aramco
- BlackEnergy in Ucraina

I tipi e le modalità di attacco ICS
- Gli attacchi APT (Advanced Persistent Threat): fasi e caratteristiche
- Come vengono acquisite le informazioni per l'attacco: cosa è l'OSINT
- Monitoraggio del dark web, ma non solo…
- Le fasi successive e finali dell'attacco APT

Il Fattore Umano: il rischio più frequente
- I rischi del "fattore umano": social engineering, phishing, spear phishing
- Le varianti del phishing
- Gli attacchi omografici e il Typosquatting

L'email non è uno strumento sicuro
- L'email non è uno strumento sicuro. La Business Email Compromise (BEC)
- Lo spoofing
- Una Email sicura: come fare?

Gestione delle credenziali e Autenticazione. Le Password
- Gestione delle credenziali e Autenticazione
- Gli errori da non fare… e che tanti fanno!
- Come vengono scoperte (rubate) le password?
- Le tecniche di Password Cracking
- Come è fatta una password: le caratteristiche
- Le regole per una password SICURA
- I Password Manager
- Quali Password Manager usare

La Mitigazione del Rischio negli attacchi ICS
- La Mitigazione del Rischio negli attacchi ICS: i principi cardine
- Il pericolo arriva dall'interno. Il Principio del minimo privilegio (POLP)
- L'importanza della Detection: il monitoraggio ed il controllo
- Sistemi di protezione avanzata: IDS, IPS e UBA
- La gestione dei fornitori esterni
- Le verifiche di sicurezza
- Best practices in ambito ICS
- L'importanza del "fattore H" (human factor)

I VANTAGGI DELL'E-LEARNING

- Risparmio in termini di tempi/costi - Piattaforma AICC/SCORM 1.2 conforme agli standard internazionali - Accessibilità ovunque e in ogni momento
- Possibilità di rivedere le lezioni anche dopo aver terminato il corso

INDUSTRIA 4.0

ALFA-ACADEMY

ESERCITAZIONI

All'interno del corso vi saranno momenti di verifica aventi come oggetto domande attinenti all'argomento appena trattato. In caso di risposta errata, l'utente non potrà proseguire o concludere la formazione se non affrontando nuovamente il momento di verifica.

SUPERAMENTO

Una volta seguite tutte le lezioni proposte nella loro interezza di tempo è possibile ottenere l'attestato di superamento del corso.
Gli attestati conseguibili sono nominali per singolo corso ed è possibile ottenerli solo al corretto completamento del momento formativo finale.

CERTIFICAZIONI

Gli attestati rilasciati permettono di acquisire competenze secondo quanto indicato dal Framework DigComp 2.1 e, quindi, sono in grado di attestare in maniera oggettiva le competenze digitali necessarie per operare correttamente a livello professionalizzante nel lavoro in Europa.

I VANTAGGI DELL'E-LEARNING

- Risparmio in termini di tempi/costi - Piattaforma AICC/SCORM 1.2 conforme agli standard internazionali
- Accessibilità ovunque e in ogni momento - Possibilità di rivedere le lezioni anche dopo aver terminato il corso