ORDINE DEGLI INGEGNERI PROVINCIA DI MODENA

Commissione Industria 4.0

Corso di Formazione

CYBERSECURITY IN IOT E INDUSTRY 4.0

(Evento F.A.D.-COVID 19)

La Commissione Industria 4.0, organizza un corso di formazione, al fine di trattare e mettere a fuoco una tematica di particolare interesse, quale la CYBERSECURITY IN IOT E INDUSTRY 4.0.
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, in quanto dotati di un processore, di un sistema operativo e di una connessione alla rete, sono soggetti alle stesse problematiche e vulnerabilità di un computer, con l'aggravante che – essendo dispositivi in genere più semplici (o con sistemi operativi meno evoluti) – sono ancora meno protetti e quindi più attaccabili.
Questa connettività può 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".

Verranno esaminati quindi casi famosi di attacchi ICS, dai quali potremo capire le principali criticità dei sistemi iCS.
Si analizzeranno i principali punti deboli che rendono fattibile un attacco: social engineering, phishing, e-mail, uso non sicuro delle credenziali. Verranno trattati anche i rischi provenienti dai dispositivi mobili, oggi sempre più utilizzati nelle aziende.

Nella seconda parte del corso esamineremo i sistemi di protezione da adottare: i firewall ed i sistemi di tipo IPS/IDS e UBA (User Behaviour Analytics) e la segmentazione delle reti.
Ed infine, non dimentichiamo quella che è la principale fonte di rischio: il Fattore Umano.

Programma:

CYBERSECURITY IN IOT E INDUSTRY 4.0

❖ Martedì 21 settembre 2021

17:00 – 17:10 **Benvenuto e presentazione del corso.**

17:10 – 19:50 **Argomenti trattati**:

IoT e Industry 4.0: cosa sono

- *Internet of Things (IoT): cosa è e quando è nata.*
- industry 4.0, la quarta rivoluzione industriale. Le tecnologie abilitanti.
- IT vs. ICS/OT: un rapporto complicato, con priorità differenti.
- I sistemi ICS: il modello ANSI/ISA-95 (Purdue Model).
- Cosa è la IDMZ: Industrial Demilitarized Zone.
- I sistemi SCADA (Supervisory Control And Data Acquisition) e i Controllori Logici Programmabili (PLC): aspetti e criticità.

Le normative di riferimento in ambito ICS

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

Casi famosi di attacchi ICS: esempi istruttivi

- Come si è evoluto il Cybercrime: i numeri nel mondo ed in Italia
- WannaCry e NotPetya.
- Il caso più famoso: Stuxnet.
- Black Energy, attacco alle centrali elettriche ucraine: un attacco ICS "da manuale".
- *Shamoon blocca le raffinerie Saudi Aramco.*

19:50 – 20:00 Domande, Risposte e Test

❖ Giovedì 23 settembre 2021

17:00 – 19:50 **Argomenti trattati**:

Come si attacca un sistema ICS

- Un impianto disconnesso da qualsiasi rete è più sicuro? Una convinzione errata..
- Air-Gapped Systems: come attaccarli.
- I tipi e le modalità di attacco ICS: i cyber attacchi sono oggi considerati uno dei rischi più elevate in termini di probabilità e danno procurato.
- Gli attacchi APT (Advanced Persistent Threat): le caratteristiche e le fasi dell'attacco.
- Come vengono acquisite le informazioni per l'attacco: cosa è l'OSINT.
- The Internet of Health Care: i dispositivi medicali sono altamente vulnerabili.
- Gli attacchi dall'esterno e quelli dall'interno (gli "insider").

Gestione delle credenziali e Autenticazione: come usare le Password

- Gli strumenti (sempre più potenti) degli hackers: alcuni famosi casi di attacchi e "data breach".

- Le tecniche di Password Cracking
- Le regole per una Password sicura e gli errori comuni da evitare.
- Le più recenti linee guida del NIST.

Proteggersi dagli attacchi ICS

- La Mitigazione del Rischio negli attacchi ICS: i principi cardine.
- Le indicazioni del NIST Cybersecurity Framework.
- L'importanza della Detection: il monitoraggio ed il controllo.
- Monitoraggio eventi e incidenti: SIEM e SOC.
- Sistemi di protezione avanzata: IDS (Intrusion Detection System), IPS (Intrusion Prevention System) e UBA (User Behavior Analytics).
- Le verifiche di sicurezza: Vulnerability Assessment (VA) e Penetration Test (PT).
- La separazione tra la rete wireless e quella cablata e tra l'accesso "da ospite" e quello aziendale.
- La gestione degli Outsourcers (i fornitori esterni): Audit e controllo dei fornitori.
- Best practices in ambito ICS: 20 utili regole da tenere presente.
- Il pericolo arriva dall'interno: il Principio del minimo privilegio (POLP).
- L'importanza del "fattore H" (human factor): la formazione del personale.

19:50 – 20:00 **Domande, Risposte e Test**

Crediti Formativi e Attestati

Il corso ha una durata di **6 (sei) ore**, si terrà con il metodo **FAD** (Formazione A Distanza) e rilascerà **6 (sei)** Crediti Formativi Professionali a tutti gli Ingegneri iscritti ad un Ordine in Italia.

Per il rilascio è richiesta la partecipazione ad almeno il 90% delle ore di durata complessiva dell'intero webinar (tutte e due le giornate) su piattaforma GoToWebinar che permette il controllo a distanza delle presenze e il superamento del test finale.

Docente:

Giorgio Sbaraglia, ingegnere, (**www.giorgiosbaraglia.it**) svolge attività di consulenza e formazione per la sicurezza informatica e per il GDPR. Tiene corsi su questi temi per molte importanti società italiane di formazioni, tra le quali la Business School de Il Sole 24 Ore. È membro del Comitato Scientifico CLUSIT (Associazione Italiana per la Sicurezza Informatica) e certificato "Innovation Manager" da RINA. Ricopre incarichi di DPO (Data Protection Officer) presso aziende e Ordini Professionali. Autore di libri. Collabora con "Cybersecurity360" (testata specialistica del gruppo Digital360 per la **cyber security**). Scrive anche per "ICT Security Magazine", per "Agenda Digitale" e per la rivista "Class".

Organizzatore e Moderatore:

Paolo Felicani, ingegnere informatico, consulente, perito ed esperto in tematiche Industria 4.0, tecnologie abilitanti e Coordinatore della Commissione Industria 4.0 dell'Ordine Ingegneri di Modena.

Sede del corso:

In videoconferenza con la piattaforma GoToWebinar

Il giorno prima dell'evento saranno inviate a tutti gli iscritti le informazioni per la connessione in videoconferenza con la piattaforma GoToWebinar.

Modalità di partecipazione:

Quota d'iscrizione: **€ 10,00 + iva**

Apertura Iscrizioni **lunedì 23 agosto** sul portale *www.iscrizioneformazione.it*

Per ulteriori informazioni rivolgersi alla segreteria della Professione Ingegnere Associazione tra Ingegneri: Tel.059/2056370, e-mail associazione@ing.mo.it.