Protezione delle stazioni di ricarica da minacce specifiche

CSP008_S_E

PRESENTAZIONE DA PARTE DI:

- CRISTINA ALCARAZ, UNIVERSITÀ DI MALAGA, SPAGNA
- ABDELKADER SHAABAN, AIT, AUSTRIACO
- STEFAN SCHAUER, AIT, AUSTRIACO
- ELIAS ATHANASOPOULOS, UNIVERSITÀ DI CIPRO, CIPRO

Riconoscimento

- *Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione Europea o di HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili.*
- *Accordo di progetto n. 101083594*

Protezione delle stazioni di ricarica da minacce specifiche

01. Obiettivi: Chi-Cosa-Perché è necessario partecipare a questa formazione

02. Logistica della formazione: Quando-Dove-Come

03. Risultati dell'apprendimento

04. Schemi di formazione

05. Dettagli degli esercizi

06. Informazioni e requisiti pratici

07. Informazioni sulla registrazione e contatti

Obiettivi: Chi-Cosa-Perché è necessario partecipare a questa formazione

OMS

Tutti coloro che sono interessati a conoscere la sicurezza informatica delle infrastrutture di ricarica, come CISO, architetti di cybersecurity, ricercatori e risk manager, tra gli altri.

COSA

Stabilisce le basi (anche se a livello avanzato) per comprendere la rilevanza della cybersecurity in un ambito specifico del settore energetico.

PERCHÉ

Fornire ai partecipanti le conoscenze e le competenze necessarie per elaborare una strategia di protezione dei sistemi critici, dei dati e delle risorse essenziali, come il controllo e l'energia.

CSP Formazione Logistica: Quando-Dove-Come

QUANDO

Poiché il modulo si tiene più volte, si consiglia di controllare la piattaforma CyberSecPro DCM per informazioni aggiornate.

4 ore in totale con una pausa (circa 30 min.)

DOVE

Online, fisico o entrambi

Tutte le informazioni modalità di connessione saranno pubblicate sul sistema DCM.

COME

Un seminario basato su **lezioni sincrone** in cui ogni formatore spiegherà argomenti specifici; alla fine del seminario verranno proposte varie attività e verrà effettuato un test di valutazione.

Proposte di valore

Vantaggi per i partecipanti

- Esplorazione di un campo di applicazione specifico, ma molto comune, all'interno del settore energetico.
- Livello del modulo di formazione: Avanzato
- Formazione professionale sulla cybersecurity nel settore delle stazioni di ricarica
- Sviluppo di competenze pratiche e pratiche
- Radicati con i quadri di riferimento europei per le competenze di cybersecurity
- Approfondimenti all'avanguardia da parte di esperti del settore e del mondo accademico
- Contribuisce allo sviluppo delle competenze e all'avanzamento di carriera

OMS

Profilo dei partecipanti alla formazione

- Dirigenti e leader
- Dipendenti del settore energetico (operatori, ingegneri, amministratori, ecc.) e PMI
- Architetti e gestori del rischio di cybersecurity
- Ricercatori ed educatori nel campo della sicurezza informatica
- Professionisti e appassionati di cybersecurity

OMS

Profilo del formatore

- Cristina Alcaraz
  Professore associato presso l'Università di Malaga
  Dottorato di ricerca in informatica

- Abdelkader Shaaban
  Scientist Security & Communication Technologies Center for Digital Safety & Security (Centro per la sicurezza digitale)
  Dottorato di ricerca in Informatica

- Stefan Schauer
  Coordinatore tematico
  Centro per la sicurezza digitale Dottorato di ricerca in informatica

- Elias Athanasopoulos
  Professore associato presso l'Università di Cipro
  Dottorato di ricerca in informatica

COSA

Argomenti di formazione

- Introduzione alle infrastrutture di ricarica energetica
- Sfide per la sicurezza nelle stazioni di rifornimento energetico
- Cascata di energia e impatto su altre infrastrutture critiche
- Misure di sicurezza e migliori pratiche per le stazioni di ricarica

PERCHÉ

Risultati dell'apprendimento

- Comprendere la definizione, la portata e l'importanza delle stazioni di ricarica nel settore energetico e il loro impatto su altre infrastrutture critiche.
- Cogliere le sfide e le vulnerabilità di sicurezza specifiche delle stazioni di ricarica
- Sviluppare la conoscenza delle minacce informatiche e fisiche, dei vettori di attacco e delle potenziali conseguenze delle violazioni della sicurezza nelle stazioni di ricarica.
- Comprendere i principi e le metodologie per analizzare gli effetti a cascata e valutare i rischi per la sicurezza.
- Conoscere le misure di sicurezza efficaci, i controlli e le migliori pratiche per la protezione delle stazioni di ricarica.
- Rimanere informati sulle nuove minacce e tendenze nel campo della sicurezza delle stazioni di ricarica

WHY-2

Risultati dell'apprendimento

- Applicare le migliori pratiche per l'implementazione di controlli di sicurezza fisica e informatica nelle infrastrutture di ricarica.
- Identificare e utilizzare strumenti e meccanismi di sicurezza specializzati.
- Pensiero critico e risoluzione dei problemi negli scenari di sicurezza delle stazioni di ricarica.
- Capacità di analizzare e interpretare le informazioni tecniche e di sviluppare soluzioni di sicurezza basate sui dati.
- Forti capacità decisionali basate su una comprensione completa dei rischi e delle best practice

Formatori:

- Cristina Alcaraz
- Shaaban Abdelkader

Schema di formazione

Sessione-1 - circa 1 ora

Argomento-1: Introduzione alle infrastrutture di ricarica energetica

Concettualizzazione delle "infrastrutture di ricarica", dei loro componenti e del loro ambiente, nonché degli Stakeholder e degli interessi

Panoramica delle dipendenze e dell'impatto

Argomento-2: Sfide per la sicurezza nelle stazioni di rifornimento energetico

Principali sfide di sicurezza nel contesto delle stazioni di ricarica Una

panoramica delle principali minacce in questo contesto

Attacchi specifici nelle stazioni di ricarica: un'ulteriore esplorazione del problema

Allenatore:

- Stefan Schauer

Schema di formazione

Sessione-2 - circa 1 ora

Argomento-3: Energia a cascata e impatto su altre infrastrutture critiche

Introdurre le dipendenze e le interdipendenze rispetto ad altre infrastrutture critiche.

Fornire studi pratici basati su simulazioni e analisi degli effetti a cascata

Allenatore:

- Shaaban Abdelkader
- Elias Athanasopoulos

Schema di formazione

Sessione-3 - circa 1 ora

Argomento 4: Misure di sicurezza e migliori pratiche per le stazioni di ricarica

Introdurre le dipendenze e le interdipendenze delle stazioni di ricarica rispetto ad altre infrastrutture critiche.

Fornire studi pratici basati su simulazioni e analisi degli effetti a cascata

Argomento-1: Introduzione alla ricarica di energia Infrastrutture

Tratteremo queste competenze

- Introduzione al concetto di "stazioni di ricarica": In questa sezione si conosceranno i principali sistemi che conformano un'infrastruttura di ricarica, nonché i loro principali componenti, protocolli e tecnologie.
- Soggetti interessati e interessi: In questa sezione sono indicati i principali soggetti interessati all'utilizzo o alla gestione delle stazioni di ricarica, sia a fini di consumo che di gestione o manutenzione.
- Rapporti con altre infrastrutture critiche: Questa sezione mostra una semplice panoramica del rapporto diretto tra le stazioni di ricarica e la rete principale, con un impatto su altre infrastrutture critiche.

Argomento-2: Sicurezza Le sfide delle stazioni di trasporto dell'energia

Tratteremo queste competenze

- Principali sfide per la sicurezza: Questa sezione illustra le principali sfide per la sicurezza in molti aspetti legati al tipo di implementazione, ai componenti cyber-fisici e alle comunicazioni.
- Sfide per la sicurezza e la privacy nelle CS: Questa sezione affronta gli attacchi tipici e specifici alle stazioni di ricarica, mostrando la suscettibilità del contesto a molteplici attacchi contro il controllo e l'alimentazione.

Argomento 3: Energia a cascata e impatto su altre criticità Infrastrutture

Tratteremo queste competenze

- Dipendenze e interdipendenze: Questa sezione comprende lo studio necessario per comprendere l'effetto a cascata tra le infrastrutture critiche, come i settori sanitario e marittimo.
- Effetto a cascata da un punto di vista pratico: Questa sezione sottolineerà l'importanza di prevenire, e in ultima analisi di mitigare, gli effetti che possono avere un grave impatto su altre infrastrutture critiche.

Argomento 4: Misure di sicurezza e migliori Pratiche per le stazioni di ricarica

Tratteremo queste competenze

- Migliori pratiche e raccomandazioni: In questa sezione verranno trattate una serie di buone pratiche e raccomandazioni fornite da organizzazioni internazionali come l'ENISA.
- Contromisure di sicurezza più personalizzate: Questa sezione affronterà misure specifiche in termini di distribuzione, comunicazione e componenti.

Esercitazioni pratiche di formazione

Durante 'intero modulo verranno proposte diverse attività:

- **Analisi di casi di studio** incentrati sul settore energetico - compito opzionale
- **Un test di valutazione** - compito obbligatorio

Metodo di valutazione

Delineare gli elementi di valutazione e il processo di valutazione

Elemento di valutazione	Come	Note
Relazione finale su un caso d'uso	Rapporto individuale presentato nei tempi previsti	Analisi e discussione richieste su un argomento specifico
Test (OBBLIGATORIO)	Test di valutazione, che può includere casi di studio in cui i discenti devono dimostrare la loro conoscenza pratica.	In presenza dei formatori (circa 10-15 minuti)

Conoscenze di base e prerequisiti

Conoscenze di base:

- Conoscenza di base dei fondamenti della sicurezza informatica (in relazione al modulo 1 del CSP).
- Conoscenza di base di computer e reti
- Esperienza con i sistemi operativi

Prerequisiti:

- Conoscenza di base degli elementi essenziali di IT e cybersecurity
- Esperienza con i sistemi operativi, le configurazioni di rete e i protocolli di comunicazione

Strumenti tecnici e altri requisiti

Strumenti tecnici

- Computer con accesso a Internet per la connessione
- Accesso alla piattaforma DCM
- Software d'ufficio per i rapporti
- Strumenti tecnici: Nessuno al momento

Altri requisiti

- **Volontà di imparare e sperimentare**
- **Consapevolezza delle pratiche di sicurezza di Internet e della sua cautela.**
- **Partecipazione attiva**

Risorse: Libri e materiali di riferimento

1. AIE, Veicoli elettrici, https://www.iea.org
2. Global Market Insigths (GMI), "Dimensioni del mercato europeo delle stazioni di ricarica per veicoli elettrici", 2022, https://www.gminsights.com/industry-analysis/europe-electric-vehicle-charging-station-market
3. C. Alcaraz, J. Lopez e S. Wolthunsen, "Il protocollo OCPP: Security Threats and Challenges", IEEE Transactions on Smart Grid, vol. 8, pp. 2452 - 2459, 2017.
4. Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". Computers & Security 112 (2022): 102511
5. Open Charge Point Protocol (OCPP) Security Explained (wevo.energy), consultato nel marzo 2024.
6. Applicazioni per stazioni di ricarica EV: un rischio crescente per la sicurezza informatica - Blog di Radware, accesso a marzo 2024
7. C. Alcaraz, J. Cumplido, A. Triviño, "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0", International Journal of Information Security, 2023, ISSN: 1615- 5262.
8. MITRA, MITRA ATT&CK, https://attack.mitre.org
9. Cifre attribuite a Vecteezy, https://www.vecteezy.com, 2024 - Grazie!

Registrazione: Come registrarsi e altre informazioni informazioni pratiche

Il processo di registrazione specifico per la formazione Cybersecurity Essentials e Management può variare a seconda dell'ente di formazione o dell'istituzione.

Tuttavia, le fasi generali sono descritte in dettaglio nella piattaforma DCM.

Connettersi con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Grazie

Se avete domande, non esitate a contattarci:

- Cristina Alcaraz
  alcaraz@uma.es
- Abdelkader Shaaban
  abdelkader.shaaban@ait.ac.at
- Stefan Schauer
  stefan.schauer@ait.ac.at
- Elias Athanasopoulos
  athanasopoulos.elias@ucy.ac.cy