ORDINE DEGLI INGEGNERI
PROVINCIA DI TRIESTE

CYBERSECURITY

Aspetti tecnici, gestionali e giuridici

ciclo di seminari in videoconferenza

con piattaforma Microsoft Teams

Mercoledì 22 novembre 2023 dalle 15:00 alle 19:00

Mercoledì 29 novembre 2023 dalle 15:00 alle 19:00

Lunedì 4 dicembre 2023 dalle 9:00 alle 13:00

Martedì 12 dicembre 2023 dalle 9:00 alle 13:00

Lunedì 18 dicembre 2023 dalle 9:00 alle 13:00

CREDITI FORMATIVI:

4 CFP per ingegneri per singolo seminario

20 CFP per ingegneri per il ciclo intero

CFP per le altre categorie professionali
secondo i rispettivi Regolamenti

DOCENTI

ing. Giuseppe Panarello

Centro Operativo per la Sicurezza Cibernetica
Polizia Postale e delle Comunicazioni FVG

ing. Diego Chiozzi
dott. Cristian Roner
dott. Matteo Rizzi
avv. Federico Fedrizzi

consulenti di Techneos
società che lavora nella trasformazione digitale

OBIETTIVI FORMATIVI

Spesso, quando si parla di sicurezza informatica, si pensa che sia un tema squisitamente tecnico.

Valutare una vulnerabilità informatica in relazione alla possibilità di intrusione da parte di un malintenzionato è riduttivo: la medesima vulnerabilità ha impatti diversi se collocata in punti diversi dell'organizzazione.

Dall'altra parte è impensabile annullare con un unico intervento istantaneo tutte le vulnerabilità all'interno di un'azienda, a maggior ragione con costi ben definiti e accettabili per l'azienda.

Per questo motivo, la gestione consapevole della sicurezza deve seguire un approccio basato sul rischio e considerare, assieme agli aspetti tecnici della vulnerabilità, anche l'impatto organizzativo, finanziario e giuridico delle conseguenze di un potenziale attacco.

Il percorso, nel suo complesso, punta a fornire una prima formazione completa e funzionale all'implementazione di un approccio di gestione della cybersicurezza risk-based.

PROGRAMMA DEI SEMINARI

Si veda dettaglio nella pagina successiva

ISCRIZIONE

Le iscrizioni vanno effettuate **esclusivamente** on-line

http://ordineingegneri.ts.it/cybersecurity2023/

Il ciclo di seminari verrà attivato al raggiungimento di un minimo di 20 iscrizioni alla data del 15 novembre 2023. Sarà comunque possibile iscriversi e partecipare anche successivamente a tale data (salvo il raggiungimento del numero minimo di iscrizioni).

Quota di iscrizione (singolo seminario):
40,00 euro (IVA compresa)

Quota di iscrizione (ciclo di seminari completo):
160,00 euro (IVA compresa)

ORDINE DEGLI INGEGNERI
PROVINCIA DI TRIESTE

IL CYBERCRIME IN ITALIA

Mercoledì 22 novembre 2023 dalle 15:00 alle 19:00

ing. Giuseppe Panarello

Attacchi informatici: panoramica e distribuzione

I nuovi trend del Cybercrime: il CaaS

Fenomenologia, case study e reati informatici associati:

- Phishing,
- Ransomware,
- Data Exfiltration,
- BEC/Man in the Middle,
- CEO Fraud,
- Sim Swap

Cybersecurity: cenni. Il fattore tecnico ed il fattore umano

ASPETTI TECNICI E DI VALUTAZIONE DEL RISCHIO

Mercoledì 29 novembre 2023 dalle 15:00 alle 19:00

ing. Diego Chiozzi, dott. Cristian Roner

Introduzione ed evoluzione della sicurezza digitale

La Cyber Killchain

- Ricognizione
- Intrusione
- Diffusione
- Sabotaggio

Analisi della superficie d'attacco

- Analisi della vulnerabilità alle tecniche di ingegneria sociale
- Il Penetration testing

Controllo del Rischio e Security by Design

Tecniche di mitigazione e controlli

Framework Nazionale per la Cybersecurity e Data Protection

Business impact analysis

ASPETTI GESTIONALI E DI VALUTAZIONE DEL RISCHIO

Lunedì 4 dicembre 2023 dalle 9:00 alle 13:00

ing. Diego Chiozzi, dott. Cristian Roner

Risk assessment - awareness su rischio cyber e rischio d'impresa

Il metodo CRUSE (impostazione)

- Rilevazione delle vulnerabilità
- Analisi delle vulnerabilità
- Valutazione dell'entità economico-finanziaria del rischio
- Gestione del rischio
- Tecniche di mitigazione

Le tecniche operative

- Modelli organizzativi per la gestione della sicurezza
- Identificazione e analisi delle vulnerabilità del sistema di gestione della sicurezza
- Framework Nazionale per la Cybersecurity e Data Protection
- Rischio cyber e rischio d'impresa
- Struttura dei costi per la compensazione di un attacco hacker
- Modelli organizzativi per la gestione della sicurezza
- La valutazione quantitativa del rischio
- Struttura dei costi per la compensazione di un attacco hacker
- Valutazione degli impatti economico-finanziari

Casi studio

ORDINE DEGLI INGEGNERI
PROVINCIA DI TRIESTE

SICUREZZA DI PRODOTTO

Martedì 12 dicembre 2023 dalle 9:00 alle 13:00

dott. Matteo Rizzi

Importanza della Cybersecurity per i prodotti

Cosa è inerente alla sicurezza del prodotto?

- Ruolo fondamentale della cybersecurity nei prodotti
- Casi d'Uso di Prodotti e Vulnerabilità
- Veloci richiami dei concetti importanti visti nei moduli precedenti

Security by Design in IoT

- MQTT
- TLS e Certificati
- API Calls
- Device Interconnessi e Autenticazione
- Considerazioni sulla sicurezza nella progettazione

Sicurezza Fisica

- Attacchi a oggetti offline (Chiavi COGES, Badge NFC, Sbarre automatiche)
- Differenza tra Trusted Execution Environment, Secure Area, Secure Element e Hardware Security Module

Preparazione del Device con Microkernel

- Sicurezza nei sistemi operativi "pocket"
- Mettere in sicurezza dispositivi con sistemi operativi minimi

Cenni di AI e sicurezza di prodotto

ASPETTI GIURIDICI

Lunedì 18 dicembre 2023 dalle 9:00 alle 13:00

avv. Federico Fedrizzi

Privacy e protezione delle informazioni, GDPR

- Protezione dati e libertà dell'individuo
- Principi fondamentali
- Data leak
- Data breach (Linee Guida 01/2021 dell'EDPB)
- Sicurezza e privacy by design
- Sistema di Gestione della protezione dati

Aspetti giuridici della sicurezza informatica:

- la direttiva NIS, la proposta di direttiva NIS 2 ed il loro recepimento in Italia
- il Regolamento (UE) 2019/881
- la tutela penale della sicurezza informatica
- la sicurezza informatica ed il d.lgs. 231/2001
- sicurezza informatica e responsabilità civile