L'Ordine degli Ingegneri della Provincia di Forlì-Cesena
organizza:

Il SEMINARIO

presso SCUOLA EDILE ARTIGIANA ROMAGNA, VIA MAESTRI DEL LAVORO D'ITALIA 129, FORLIMPOPOLI

QUANDO

MARTEDI' 03 OTTOBRE 2023 ore 14.30 -18.30

MERCOLEDI' 11 OTTOBRE 2023 ore 14.30 – 18.30

Finalità del seminario

In questo seminario verranno trattati argomenti di Sicurezza Informatica, per utenti evoluti.
Nessuno oggi può prescindere dal considerare la Cyber Security come elemento strategico per la difesa dei dati della propria azienda o del proprio studio professionale. Perché se un'azienda perde i propri dati non è più nulla.
L'evoluzione del cybercrime ha sostituito l'hacker con vere e proprie organizzazioni criminali dotate di grandi mezzi ed in grado di portare attacchi a chiunque. Non è un problema di sapere "se verremo attaccati" ma solo "quando saremo attaccati". Non importa se siamo grandi o piccoli: prima o poi ci attaccheranno.
I mezzi per difenderci già esistono: quello che manca è la consapevolezza del problema e la conoscenza degli strumenti più idonei da adottare per proteggerci.

PROGRAMMA DI MARTEDI' 03 OTTOBRE 2023

14.15: Registrazione dei partecipanti

14:30 Inizio momento formativo:

Come è cambiato il Cybercrime negli ultimi anni

- I dati del crimine informatico nell'Italia e nel mondo: il rapporto CLUSIT
- Il rapporto DESI (Digital Economy and Society Index): la criticità del fattore umano
- Cyberwarfare, la guerra cibernetica: il caso Russiagate e Stuxnet
- Il Deep Web, il Dark Web e la rete TOR

Panoramica sulle principali tecniche di cyber attacco

- Le tipologie degli attacchi
- APT (Advanced Persistent Threat): le fasi dell'attacco
- Le tecniche di OSINT (Open Source INTelligence)
- Hackers ed Hackers "state sponsored"
- Vulnerabilità, 0-Day ed Exploit: cosa sono e dove trovarli

Social Engineering e Phishing

- Cos'è il Social Engineering.
- Le varianti del Phishing: whaling, smishing, vishing e QRishing
- Phishing, Spear Phishing e Watering Hole: le tecniche d'attacco
- Casi pratici e come riconoscerli
- Riconoscere i siti di phishing: il typosquatting

I Ransomware: la minaccia oggi più temuta

- I Ransomware: cosa sono
- Come ci attaccano: i vettori d'infezione
- Alcuni attacchi famosi: da WannaCry a NotPetya
- Come difendersi dai Ransomware: le misure di prevenzione
- Sono stato colpito da un Ransomware: cosa fare ora? Quali sono le possibili opzioni
- Implicazioni giuridiche per le vittime dei ransomware: profili di responsabilità derivanti dal pagamento di riscatti

18:30 Conclusione dei lavori

PROGRAMMA DI MERCOLEDI' 11 OTTOBRE 2023

14.15: Registrazione dei partecipanti

14:30 Inizio momento formativo:

L'Email non è uno strumento sicuro

- Gli attacchi attraverso la posta elettronica
- Business Email Compromise (BEC): che cosa è e quanti danni sta causando nelle aziende
- Le truffe "The Man in the Mail" e "CEO fraud"
- L'email non è uno strumento sicuro: lo spoofing
- L'importanza dell'Antispam e dei protocolli di setup
- PEC e posta crittografata: caratteristiche, utilizzi e differenze
- La crittografia dell'email: che cosa è la PGP (Pretty Good Privacy) e come si usa

L'importanza delle Password

- Come gli hacker riescono a violare i nostri account (più facilmente di quello che crediamo)
- Le tecniche di Password Cracking
- La corretta gestione delle Password sicura e gli errori da evitare
- I Password Manager: quali scegliere e come usarli
- L'autenticazione forte (MFA): una protezione ulteriore

I rischi aziendali

- La "deperimetralizzazione": il Teorema del Fortino
- In azienda il pericolo arriva (anche) dall'interno: malicious insider, utenti compromessi ed accidentali.
- Il principio del Minimo Privilegio ed il modello "Zero Trust Architecture (ZTA)"
- Cosa è lo "Shadow IT"

Le misure di cybersecurity in ambito aziendale

- Pensa come pensa l'attaccante
- Implementare una "layered security": la difesa a strati
- Come gestire correttamente il Backup: la regola 3-2-1
- NAS e sistemi RAID: cosa sono e come usarli per conservare in sicurezza i nostri dati
- I sistemi di protezione avanzata: IDS, IPS, EDR, XDR e User Behavior Analytics (UBA)
- SIEM e SOC: cosa sono e perché utilizzarli
- Il fattore umano è l'anello debole della sicurezza: acquisire consapevolezza. L'importanza della formazione e delle policy di sicurezza

18:30 Conclusione dei lavori

DOCENTE:

Giorgio Sbaraglia, ingegnere, è Information & Cyber Security Advisor e DPO (Data Protection Officer).
Svolge attività di consulenza e formazione per la sicurezza informatica e per il GDPR. Tiene corsi su questi temi per molte importanti società italiane, tra le quali la 24Ore Business School (https://www.24orebs.com/docenti/giorgio-sbaraglia).

Coordinatore scientifico del Master "Cybersecurity e Data Protection" della 24Ore Business School: https://bit.ly/master24OreBS

È membro del Comitato Direttivo CLUSIT (Associazione Italiana per la Sicurezza Informatica) e certificato "Innovation Manager" da RINA.

Ha pubblicato per GoWare i libri:

- "GDPR kit di sopravvivenza",
- "Cybersecurity kit di sopravvivenza. Il web è un luogo pericoloso. Dobbiamo difenderci!" (2ª edizione 2022),
- "iPhone. Come usarlo al meglio. Scopriamo insieme tutte le funzioni e le app migliori".

Collabora con CYBERSECURITY360 https://www.cybersecurity360.it/about testata specialistica del gruppo Digital360 per la sicurezza informatica.

Scrive anche per la testata ICT Security Magazine https://www.ictsecuritymagazine.com e per www.agendadigitale.eu/ e per la rivista CLASS.

L'Ordine Ingegneri della Provincia di Forlì-Cesena riconoscerà ai partecipanti n. 4 CFP per ciascun evento per un totale di 8 CFP se si partecipa ad entrambi.
Si può partecipare anche ad un singolo seminario.
QUOTA DI ISCRIZIONE € 20,00 PER OGNI SINGOLA GIORNATA FORMATIVA (ESENTE IVA EX ART 10, COMMA 1, NUMERO 20 DEL DPR N. 633/1972).
ISCRIZIONI SUL PORTALE:WWW.ISIFORMAZIONE.IT