CSAW-3 - SOCIAL ENGINEERING AWARENESS

Categoria: **Cyber Security Awareness**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
1 Giorni	Cyber Security Awareness	Docente Senior (min. 5 anni)	Utente	PCSNET

OBIETTIVI

Gli attacchi cyber-criminali assumono forme diverse e vengono perpetrati con tecniche molto sofisticate. Vanno dai ransomware, un tipo di malware che limita l'accesso del dispositivo che infetta richiedendo un riscatto (ransom in inglese) al social engineering, ossia tecniche di attacco basate sulla raccolta di informazioni mediante studio - interazione con una persona, ad altro ancora.
Tutti sfruttano i punti deboli a livello tecnico, di processo, organizzativo e anche culturale.
L'obiettivo di questi attacchi è estorcere dati ed informazioni o addirittura arrecare un danno colpendo una parte importante degli asset aziendali.
Questi attacchi impattano tutta l'azienda, sottovalutarli sarebbe molto grave, a rischio della stessa sopravvivenza dell'impresa.

Come detto per ottenere le informazioni esistono molti metodi e uno di questi è il social engineering, che si avvale non solo di tecnologie ma anche tecniche psicologiche puntando sul fattore umano, quando i sistemi aziendali non hanno criticità o falle da sfruttare.

Come identificare e proteggersi da questo tipo di attacchi?
Il percorso formativo di Social Engineering Awareness ha l'obiettivo di fornire alle persone gli strumenti per riconoscere i tentativi di attacco perpetrati dai moderni ingegneri sociali.
Partendo dalla definizione di ingegneria sociale, i partecipanti saranno introdotti ai principi psicologici normalmente abusati durante questo genere di attacchi ed alle tecniche di manipolazione impiegate per estorcere informazioni aziendali riservate.
Il docente mostrerà diversi casi di studio reali utili a comprendere il fenomeno del Social Engineering e sviluppare strategie di difesa a tali attacchi.

PREREQUISITI

Nessun prerequisito.

CONTENUTI

Modulo 1

- -Cos'è il Social Engineering
- -Cronistoria del Fenomeno dell'Ingegneria Sociale
- -Obiettivi di un Attacco di Social Engineering

Modulo 2

- -Il funzionamento del sistema operativo “uomo”
- -Principi psicologici abusati nell’Ingegneria Sociale
- -Moderni attacchi di Social Engineering

Modulo 3

- -La gestione della sicurezza “umana”
- -Incrementare il livello della human security
- -Progettare ed implementare policy di sicurezza

Modulo 4

- -Difendersi dagli attacchi di Social Engineering
- -Proteggere le “chiavi” del regno
- -Comprendere gli indicatori di un attacco
- -Come reagire ad un attacco

INFO

Materiale didattico: Materiale didattico e relativo prezzo da concordare
Costo materiale didattico: NON incluso nel prezzo del corso
Natura del corso: Dimostrativo