

Difendersi da Ingegneria Sociale e Spionaggio Industriale

Sembra essere una verità assoluta che molte persone non credono che l'Ingegneria Sociale (ottenere informazioni con l'inganno) possa essere così facile. "Nessuno può essere così stupido" è una frase comune che si può udire da chi sente per la prima volta parlare di come funziona questo genere di attacchi. Comunque, una volta dimostrato (specialmente con alcune informazioni personali su di loro), questi diventano improvvisamente dei fermi credenti. Solo vederlo in azione con i propri occhi fa capire come queste informazioni possano trapelare da praticamente qualunque impiegato e che è necessario essere sempre in guardia. Attraverso un addestramento di due giorni, Selenu vi porterà attraverso la casistica, esempi, e metodi di ingegneria sociale. Esaminando come gli attaccanti raccolgono le informazioni personali, abusano della fiducia, e scelgono i loro obiettivi, si può essere più preparati nel prevenire questi incidenti. Ponendo l'attenzione sui fattori umani coinvolti con la sicurezza dell'informazione, Selenu spiega perché tutti i firewall ed i protocolli di criptazione al mondo non saranno mai abbastanza per fermare un malintenzionato con le giuste conoscenze che vuole ottenere un database aziendale o un impiegato arrabbiato determinato a danneggiare un sistema. Anche con l'aiuto di affascinanti storie di REALI attacchi di successo a scapito di attività commerciali e governative, illustra quanto anche il sistema informativo più protetto sia suscettibile ad un furbo truffatore che impersona un impiegato del fisco. Raccontando dal punto di vista di attaccanti e vittime, spiega perché quell'attacco è stato così di successo e come si sarebbe potuto prevenire in un'esposizione elegante ed analitica. Richiedi il programma del corso e vedi come possiamo aiutarVi nei confronti della politica aziendale, della sicurezza, e nell'addestrare un personale informato capace di fornire una protezione contro i futuri attacchi alla tua azienda.