BLUE TEAM HACKING PEOPLE

SECURITY AWARENESS

RENDERE LE PERSONE CONSAPEVOLI ED ISTRUITE A RICONOSCERE LE ATTUALI MINACCE INFORMATICHE, FORNENDO LORO GLI STRUMENTI ADATTI PER REAGIRE, È LA SOLUZIONE PRINCIPALE AI PROBLEMI DI CYBERSECURITY.

90% **DEGLI ATTACCHI INFORMATICI INIZIANO CON UNA MAIL DI PHISHING**

74% **DEGLI INCIDENTI DI SICUREZZA SONO CAUSATI DAL FATTORE UMANO**

Dati quest'ultimi che dimostrano oggettivamente come la tecnologia non sia più sufficiente. La tutela del business aziendale e della sua reputazione comincia dalla consapevolezza e dai comportamenti responsabili del personale.

Come tutti i servizi di IMQ Intuity, anche i servizi di **Hacking People** si strutturano in **3 diverse fasi operative.**

ASSESS: fase di valutazione durante la quale IMQ Intuity fornisce una visione dettagliata dello stato di sicurezza dell'azienda, evidenziando i rischi reali ai quali è esposta, con l'obiettivo di vagliare le azioni correttive da intraprendere.

IMPROVE: fase di correzione delle vulnerabilità riscontrate nella fase di Assess riconducibili sia all'aspetto infrastrutturale che a quello comportamentale delle persone.

REINFORCE: fase di potenziamento attraverso attività continuative di rinforzo e mantenimento del livello di sicurezza e consapevolezza raggiunti.

IMQ INTUITY SRL | info@intuity.it | intuity.it/
Sede Operativa Via A. Ceron 2, 35129 | +39 049 817 0850 | **Sede Legale** via M. F. Quintiliano, 45 - 20138 Milano

LE ATTIVITA' DI SECURITY AWARENESS

ASSESS

COMPRENDERE IL LIVELLO DI CONSAPEVOLEZZA INTERNO IN MERITO ALLA CYBERSECURITY.

PHISHING ASSESSMENT: attività che prevede l'invio di una campagna di Phishing simulata, al fine di comprendere la sensibilità della propria azienda nei confronti di questo tema.

IMPERSONATION: simulazione di un furto d'identità da parte degli specialisti di IMQ Intuity per ottenere accesso fisico o virtuale a informazioni o documenti sensibili.

BAITING: distribuzione all'interno o all'esterno del perimetro aziendale, simulando uno smarrimento, di chiavi USB contenenti contenuto controllato.

DUMPSTER DIVING: recupero da documenti non opportunamente stracciati di informazioni utili per la pianificazione e la riuscita di un attacco informatico.

ANTHROPOLOGICAL WALK: raccogliere e classificare informazioni ottenute grazie ad una ricerca sul campo mediante osservazione e ascolto.

IMPROVE

ATTIVITÀ FORMATIVE SULLA CYBERSECURITY E SULLE TECNICHE PER RICONOSCERE LE MINACCE INFORMATICHE.

IN CLASS TRAINING: sessioni formative in aula con un esperto di Cybersecurity per comprendere le minacce informatiche di oggi, come riconoscerle e segnalarle.

ON JOB LEARNING: moduli formativi veicolati attraverso portale web, al quale gli utenti possono accedervi direttamente dal proprio PC per partecipare a brevi sessioni di training.

PHISHING AWARENESS: attività che combina una campagna simulata di Phishing con un training computer based. In caso di comportamento errato nei confronti di una finta mail malevola, gli utenti vengono veicolati verso piccoli tutorial di avviso e correzione.

E-LEARNING: corso multimediale sulla Cybersecurity fruibile in modalità e-learning organizzato in mini-tutorial, giochi, test e contenuti scaricabili.

REINFORCE

MANTENERE COSTANTE L'ATTENZIONE SUL TEMA DELLA CYBERSECURITY

EDUCATIONAL MATERIAL: attraverso poster, flyer, vademecum e altre tipologie di supporti visivi, promuovere internamente una Cultura della sicurezza condivisa e tenere alta l'attenzione nell'utilizzo dei propri strumenti di lavoro.

LA PIATTAFORMA DI KNOWBE4

IMQ Intuity, per l'erogazione dei propri servizi di Security Awareness, propone la piattaforma **KnowBe4**, per la formazione del personale in ambito cybersecurity e compliance, oltre che per la realizzazione di campagne di phishing simulato.

Con più di 30.000 clienti, KnowBe4 nel 2019 è stata inserita all'interno del Quadrante Magico di Gartner tra i leader di mercato, per le sue soluzioni di Security Awareness.

La partnership tra IMQ Intuity e KnowBe4 ha origine dal comune obiettivo di migliorare la linea di difesa più importante del contesto aziendale: i propri dipendenti.

Le aziende, attraverso un percorso di Security Awareness, personalizzato rispetto alle proprie necessità e vulnerabilità, sono in grado di:

- Ridurre le infezioni da malware e ransomware.
- Tutelare i dati aziendali da furti o accessi non autorizzati.
- Creare una corretta cultura sulla sicurezza delle informazioni.
- Tutelare il proprio business dalle minacce informatiche.