Scheda Tecnica

Servizio Cyber Security Awareness

SOC Cyber Defense SA, Via Cantonale 23c, CH 6928 Manno
T +41 91 611 70 00, info@soccd.swiss - www.soccd.swiss

1. *Descrizione generale*

La migliore strategia di difesa di fronte ad attacchi informatici sempre più sofisticati e mirati è sicuramente la cyber security awareness, la formazione in tema di sicurezza informatica. La maggior parte degli incidenti di sicurezza, infatti, è dovuta ad errori umani a conferma del fatto che il cosiddetto “fattore H”, il fattore umano, rimane il punto debole della cyber security in azienda.

Alcune stime parlano, addirittura, di un 80-90% di incidenti informatici riconducibili a errori umani o comportamenti errati del personale. Errori involontari, dovuti a negligenza e disattenzione del personale interno all’azienda, ma anche intenzionali compiuti da lavoratori infedeli che effettuano operazioni di sabotaggio ai danni della propria organizzazione.

Per questo motivo i nostri formatori hanno collaborato a realizzare una serie di percorsi formativi, su temi di uso quotidiano, necessari a creare la corretta consapevolezza di come, alcuni comportamenti, siano pericolosi per l’intera azienda e possano vanificare sforzi e investimenti.

Per il servizio di Cyber Security Awareness verrà chiesto al referente del cliente la lista dei nominativi che accederanno alla formazione, i dati richiesti saranno: Nome, Cognome e indirizzo eMail.

2. Descrizione prodotti e funzionalità

2.1 Formazione di Awareness continua

è un innovativo sistema di e-learning pensato specificatamente per il personale non specialistico delle organizzazioni pubbliche e private. Il primo sistema che si fonda su metodologie di formazione che tengono conto delle modalità di apprendimento digitale che risultano maggiormente efficaci. Il sistema è stato progettato per coinvolgere tutta l'organizzazione in un percorso di apprendimento educativo e stimolante, che si caratterizza per un approccio "a rilascio costante e graduale":

- la formazione impegna il partecipante per pochi minuti al mese, ma con un percorso diviso in annualità, che mantiene elevata l'attenzione del partecipante ogni qualvolta interagisce con le tecnologie digitali;
- tutte le lezioni sono disponibili in formato multimediale, con la possibilità di fruire dei contenuti sia in formato video sia in formato testuale;
- il linguaggio utilizzato risponde a un criterio divulgativo, focalizzato sul personale non specializzato sulla Cyber Security;
- ogni lezione è corredata da test di valutazione del livello di apprendimento;
- ogni modulo formativo è auto-consistente perché affronta uno specifico argomento;
- i moduli formativi sono in totale 12 per ogni anno con un incremento progressivo dei concetti e della difficoltà;
- viene fornito un attestato di partecipazione alla fine di ogni anno
- i moduli formativi vengono erogati con la frequenza predefinita (es. Mensile)

2.2 Phishing

è una soluzione innovativa di training Anti Phishing che produce risultati efficaci grazie alla sua particolare metodologia addestramento esperienziale. Basato su automazione e machine learning , la soluzione è rivolta a tutto il personale delle organizzazioni pubbliche e private, esso consente di mantenere "allenate" due importanti caratteristiche difensive umane: la prontezza e la reattività.

Questo risultato viene raggiunto mediante la simulazione di campagne di Phishing cui vengono sottoposti tutti gli utenti (con frequenza semestrale). Mail diverse verranno mandate dal sistema ai diversi utenti ed il livello di difficoltà di ogni esercitazione varierà per ogni utente sulla base delle reali prestazioni di ogni utente.

Il sistema si propone come la naturale integrazione ai programmi formativi della soluzione di Awareness, aumentando la reattività dell'individuo di fronte ad attacchi basati su tecniche di Phishing. Considerando che i maggiori pericoli per la sicurezza delle organizzazioni sono "in agguato" nelle caselle e-mail dei loro dipendenti e collaboratori, le simulazioni di attacco Phishing, messe in atto dalla soluzione, "personalizzate" sulla base delle caratteristiche peculiari di ogni singolo utente, preparano dipendenti e collaboratori a modificare i comportamenti e ad individuare con prontezza mail di phishing.