REPORT DI SICUREZZA: TEST DI INGEGNERIA SOCIALE (PHISHING)

Obiettivo del Report

Questo documento non serve solo a fare un elenco di problemi, ma a far capire cosa rischia l'azienda. L'obiettivo è spiegare in modo semplice i pericoli informatici così che chi deve decidere possa capire perché è importante intervenire e quanto potrebbe costare non fare nulla.

Il report è scritto per essere compreso da:

- Dirigenti: Persone che vogliono solo i risultati finali, senza parole tecniche complicate.
- Responsabili dell'ufficio: Persone che devono capire come agire praticamente.
- Tecnici: Persone che hanno bisogno di dettagli precisi per sistemare i computer.

Sintesi per i Dirigenti (Executive Summary)

È stata condotta una simulazione di phishing per valutare l'affidabilità del personale amministrativo.

Punteggio di Sicurezza Generale: Critico.

Rischio Identificato: Elevata vulnerabilità al furto di credenziali.

Raccomandazione Chiave: Implementazione immediata dell'autenticazione a più fattori (MFA) e sessioni di formazione mirate per i dipendenti.

Metodologia

Spiegazione del lavoro che è stato eseguito

Strumenti: è stata utilizzata l'intelligenza artificiale per la creazione un testo molto credibile e il sito gophish per registrare i dati inseriti dai dipendenti.

Perimetro analizzato: Reparto Amministrazione e Dipendenti con accesso ai sistemi di rimborso spese e contabilità.

Data della simulazione: Il test è stato effettuato in data odierna 9/01/2026

Risultati del test

Descrizione:

Vulnerabilità di Ingegneria Sociale che permette ad un attaccante di impersonare un collega dell'Ufficio Contabilità per richiedere l'accesso a un portale falso.

Impatto:

Lo sfruttamento del problema consente all'Attaccante una possibile lettura di database aziendali, accesso a informazioni finanziarie riservate e lettura di dati sensibili.

Evidenza:

Di seguito la copia dell'email inviata, nella quale sono presenti possibili campanelli di allarme di una mail fittizia come il protocollo http invece di https , errori di battitura in una comunicazione ufficiale come steessso, oppure richieste urgenti.

Oggetto: URGENTE: Errore dati per Rimborso Spese - Azione richiesta entro oggi

Ciao, ti scrivo dall'Ufficio Contabilità perché è emerso un errore nei dati del tuo rimborso spese relativo all'ultima nota inviata. Se non viene corretto entro oggi, il pagamento potrebbe subire un ritardo nel prossimo ciclo.

Per verificare e aggiornare i dati mancanti, ti chiedo di accedere il prima possibile al portale tramite il link qui sotto: **http://portale-amministrazione-check.com**

L'operazione richiede solo pochi minuti, ma è importante farla oggi stessso per evitare blocchi amministrativi.

Grazie per la collaborazione,

Francesco - Ufficio Contabilità

La mail sembra legittima e ingannevole perché oltre ad apparire lecita a chi la legge punta all’avidità delle persone offrendo un possibile rimborso. Questo tipo di mail insieme a quelle di fittizio accesso all’account da parte di un’altro utente sono considerate tra le più ingannevoli.

Raccomandazioni e piano d’azione

Soluzione immediata:

Bloccare subito l'indirizzo internet finto usato nella mail a livello firewall aziendale e procedere al reset delle password degli utenti che hanno interagito con il link della mail.

Soluzione per il futuro:

Implementare l'autenticazione MFA(autenticazione a più fattori) e avviare un programma di Security Awareness Training incentrato sul riconoscimento dei link sospetti.