ditech
Improve your performance

SICUREZZA DELLE INFORMAZIONI

PENETRATION TEST

È il servizio Di.Tech che permette di verificare l'esposizione al rischio di cybercrime da parte di soggetti esterni, come hacker o organizzazioni criminali, o di soggetti interni.

- **Vulnerability Assessment interno** è un servizio di simulazione comportamentale che serve a verificare la presenza di vulnerabilità che il personale interno all'azienda potrebbe sfruttare per avere accesso a dati e informazioni riservate.
- **Vulnerability Assessment esterno** è un servizio di simulazione di accesso dall'esterno che ha l'obiettivo di verificare la robustezza del sistema e la presenza di vulnerabilità sfruttabili da chi intende accedere a dati, sistemi e applicazioni protette.

Queste due tipologie di simulazione sono da considerasi più efficaci se svolte in maniera **integrata**.

A COSA SERVE

Oggi la società globalizzata ha portato il cybercrime a crescere in maniera esponenziale: si è passati dall'hacking come forma di sfida ideologica ad attività organizzate di stampo malavitoso. Termini come **hacker**, **cybercrime**, **phishing**, **smishing** o **malware** sono diventati di uso comune perché hanno un impatto sul business delle aziende, mettendone a repentaglio la sicurezza.
In questo contesto non sono però da sottovalutare le **minacce alla sicurezza che arrivano dall'interno**: dipendenti infedeli, personale di terze parti che opera all'interno dell'azienda (consulenti, progettisti ecc.) e semplici visitatori.
L'insider rappresenta un problema di sicurezza a causa della conoscenza che ha dei processi aziendali e dei relativi sistemi informativi.
Le aziende hanno bisogno di proteggere le proprie informazioni, prevenendo eventuali azioni da parte di organizzazioni esterne o personale interno che possano danneggiare la produttività dell'azienda o rendere pubblico il patrimonio informativo riservato.
Hanno, quindi, bisogno di **conoscere i rischi** a cui sono esposti e di proteggersi da tutte le minacce alla sicurezza che comportano danni economici e all'immagine aziendale. Acquisire la consapevolezza dei rischi è indispensabile per individuare e implementare azioni correttive.

A CHI SERVE

Tutti i retailer.

ditech
Improve your performance

BENEFICI

Miglioramento della profilazione e dell'organizzazione: aiuta a focalizzare meglio i ruoli aziendali, a gestire la definizione dei compiti e la segregazione delle funzioni. Contribuisce inoltre alla revisione e al miglioramento di processi e procedure di sicurezza.
Compliance: alcuni controlli compresi nel servizio possono far parte di un'analisi più ampia sulla conformità a norme cogenti, best practices, norme di settore ecc. (es: privacy, ISO 27000).
Consapevolezza: crea consapevolezza del livello di sicurezza con il quale vengono gestite le informazioni (evidenze dell'esposizione al rischio in termini di confidenzialità, l'integrità e le disponibilità) e supporta le decisioni sulle strategie.

COME FUNZIONA

Il servizio è finalizzato alla **valutazione del grado di sicurezza** di reti, sistemi, applicazioni e informazioni e prende in considerazione i tre aspetti fondamentali per la gestione della sicurezza delle informazioni: **Confidenzialità**, **Integrità** e **Disponibilità**.

Le attività vengono svolte con strumenti automatici e in modalità **Ethical Hacking**, effettuando anche attività mirate di tipo manuale.

CARATTERISTICHE

Il servizio può essere erogato con diverse modalità, in funzione degli obiettivi che il cliente si pone.

- "**Black Box**": un hacker effettua tutti i tentativi per accedere alle informazioni critiche dell'azienda pur non avendone diritti e privilegi (test pre-autenticazione). Il servizio impone, per essere efficace, che non vi sia alcuna conoscenza pregressa dell'architettura dell'azienda.
- "**Grey Box**": un utente con accesso limitato o il diritto di utilizzare alcune applicazioni (utente home banking, e-commerce o l'accesso di un fornitore o di un partner B2B) effettua tentativi di accesso a informazioni critiche e a dati riservati, che dovrebbero essergli preclusi, anche attraverso una escalation di privilegi (test post autenticazione).
- "**White Box**": (previsto solo nel servizio Vulnerability Assessment Interno), in questo caso lo specialista accede all'architettura con privilegi di amministrazione e ha a disposizione tutte le informazioni disponibili relativamente a HW, SW, configurazioni ecc.