Vulnerability Assessment e Penetration Test

protiviti®
Global Business Consulting

Uso proattivo dei risultati di Vulnerability Assessment e Penetration Test

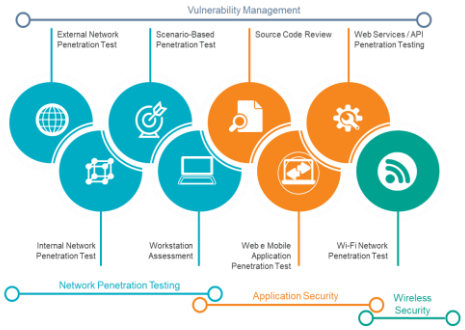
*Gli attacchi che sfruttano vulnerabilità note e debolezze delle configurazioni in apparati di rete e sistemi IT sono in forte crescita: +41% tra 2020 e 2021**

* Fonte: Rapporto Clusit 2021

La costante ricerca di vulnerabilità Zero-Day

Esiste un vero e proprio mercato nero all'interno del quale si arriva ad offrire anche 1 milione di dollari sul *dark-web* per acquistare exploit Zero-day, ovvero tecnologie utilizzate dagli hacker per attaccare i sistemi sfruttando vulnerabilità non ancora note. Ciò evidenzia quanto sia forte la motivazione degli attaccanti nel raggiungere i propri obiettivi, tipicamente di natura economica. E' quindi fondamentale effettuare Penetration Test periodici, verificando la robustezza dei propri sistemi a fronte di possibili attacchi.

I Vulnerability Assessment e Penetration Test (c.d. VA/PT) sono test mirati a **valutare il livello di rischio informatico di un'organizzazione**: il **VA** evidenzia le vulnerabilità dei sistemi informatici sotto analisi, il relativo livello di gravità e le opzioni per correggerle; il **PT** è una simulazione di un attacco *hacker* che ha lo scopo di evidenziare le debolezze più critiche del sistema e la possibilità di sfruttarle per valutarne le possibili conseguenze.



Approccio Protiviti

Set-up	Security Assessment	Manual/Auto Exploitation	Falsi Positivi	Reporting	Post Service Support
Service Fullfillment					
ATTIVITÀ					
• Identificazione e conferma target oggetto dell'attività di assessment (es. in caso di dipendenze per le attività di analisi) • Definizione modalità di comunicazione	• Rilevazione Vulnerabilità • Esecuzione verifiche sia manuali sia con strumenti automatici • Identificazione rischi per il business	• Utilizzo strumenti automatici e tecniche manuali per lo sfruttamento delle vulnerabilità identificate • Analisi risultati derivanti dall'attività di «sfruttamento» delle vulnerabilità confermate	• Analisi vulnerabilità confermate e sfruttabili • Identificazione falsi positivi e relativa eliminazione	• Analisi risultati rispetto al blueprint tecnologico • Predisposizione report tecnico con le vulnerabilità identificate • Predisposizione azioni di Remediation prioritizzate	• Meeting per discussione report • Focus sulle attività di Remediation al fine di evidenziare: - quick win puntuali vs. ambito VA-PT - azioni con benefici diffusi e a lungo termine
Linee guida di riferimento:				DELIVERABLE	• **VA-PT Report** • **Remediation Plan prioritizzato**

Valore aggiunto dei nostri servizi

Oltre ad individuare le vulnerabilità presenti sui sistemi, Protiviti si pone l'obiettivo di **comprendere le root-cause** (sistemi operativi e software obsoleti diffusi, buone pratiche di sviluppo sicuro disattese, ecc.) attraverso un'attenta analisi dei risultati delle campagne di VA e PT e valutazioni generali sul blueprint tecnologico.

Cause che, se affrontate in maniera strutturata (integrando interventi tecnologici e di processo) possono **migliorare in maniera significativa la posture di sicurezza** dell'intera organizzazione.

• Destinatari: CISO - CIO - CSO - CAE - CCO

Tipiche azioni di Remediation:

- **Revisione/integrazione del modello di governance della sicurezza** relativamente alle procedure di: gestione password, integrazione sicurezza nel ciclo di DevOps, configurazione sistemi, gestione cambiamenti e patch, programmi di sensibilizzazione e formazione
- **Sistematizzazione dei VA / PT** per verificare l'efficacia dei processi di sicurezza

www.protiviti.it enrico.ferretti@protiviti.it gianfranco.cappello@protiviti.it nicola.gobbo@protiviti.it