Vulnerability Assessment
Cos'è e come funziona

Con procedura di **Vulnerability Assessment**, si intende il complesso di operazioni svolte al fine di individuare tutte, o il maggior numero possibile, di vulnerabilità che affliggono un sistema informatico o una singola applicazione. Nel mondo digitale moderno, le aziende dipendono fortemente dalla tecnologia dell'informazione e della comunicazione, e una delle maggiori minacce è costituita dal potenziale sfruttamento da parte di criminali e malintenzionati di vulnerabilità e punti deboli dell'infrastruttura informatica o delle applicazioni, per poter interrompere servizi o rubare informazioni.

Le vulnerabilità dipendono da imperfezioni del software a vari livelli, dal firmware fino all'applicativo utente, e sono generalmente legate a mancati aggiornamenti o a carenze nell'implementazione delle patch e nei controlli di routine.
Un **vulnerability assessment** serve inoltre per compiere una revisione, classificazione e assegnazione di priorità alle vulnerabilità rilevate, in modo tale da essere risolte tempestivamente prima che possano essere da reali malintenzionati.

Le procedure da utilizzare per identificare le minacce si differenziano in relazione all'oggetto preso in esame, infatti qualunque device digitale dotato di sistema operativo, esposto in internet o connesso ad una rete locale, può venire sottoposto ad una **VA**. Gli esempi sono vasti, da un'applicazione per smartphone fino ad un macchinario industriale intelligente. Normalmente l'attività di **VA** viene svolta dall'interno dell'azienda, ma negli ultimi tempi si è diffuso il metodo di effettuarla "dal punto di vista di un hacker", che consente di simulare diversi scenari di attacco e appunto verificare il grado di **capacità di reazione dell'azienda**.

Bisogna specificare che la miglior pratica è quella di condurre periodicamente delle scansioni delle reti, dispositivi e applicazioni, in modo da rimanere sempre aggiornati sui nuovi aggiornamenti rilasciati e non trovarsi mai impreparati contro un attacco. La maggior parte degli attacchi informatici sfrutta vulnerabilità note e già risolvibili, e la periodica verifica consente di mapparle secondo un piano di priorità, definito attraverso la **CVSS** (**C**ommon **V**ulnerability **S**coring **S**ystem) e la criticità del sistema informatico interessato (legata all'importanza per il business dell'azienda, al tipo di dati trattati ecc.).

Il **vulnerability assessment**, in quanto test passivo, ha il vantaggio di non creare problemi sui sistemi informatici, e di poter quindi essere ripetuto frequentemente (mensilmente, o anche settimanalmente). Può anche essere condotto "a tappeto" su tutte le reti, dispositivi e applicazioni, consentendo di individuare tutte le vulnerabilità note e più "semplici" magari sfuggite a controlli più grossolani precedenti.

Sul mercato esistono diversi **vulnerability scanner**, sia realizzati come open source, che a pagamento (ad esempio il Nessus, prodotto da Tenable, disponibile sia in versione community che professional). Per effettuare queste analisi di solito si considerano metodologie standard, come **OWASP** o **OSSTMM** (**O**pen **S**ource **S**ecurity **T**esting **M**ethodology **M**anual), che permettono di seguire metodologie condivise, consolidate e interpretabili dalla comunità informatica di cybersicurezza.
Il tecnico può svolgere una **VA** come se non avesse alcuna informazione sul sistema (metodo **black box**) oppure come se conoscesse l'intero sistema prima dell'avvio delle attività (metodo **white box**). Tramite questi due metodi è possibile effettuare delle **VA** che richiedono specificatamente l'uso di un determinato standard per essere compiacenti delle normative vigenti. Esiste anche un terzo metodo, intermedio tra i due, chiamato **"grey box"**.

Per approfondire l'utilizzabilità di una vulnerabilità scoperta, si può ricorrere anche ad un **Penetration Test**, che prevede la simulazione di attacchi reali per valutare i rischi riscontrati. Questa procedura è complementare al **Vulnerability Assessment**, estendendo le differenze tra le diverse procedure effettuabili:

- **VA e PT infrastrutturali**: si verificano le vulnerabilità delle reti cablate, sia server che client

- **VA e PT applicativi**: si verificano i "punti esposti" online e le pagine di login, amministrazione e utente di diversi tipi di applicazioni mobili, software, portali web, CRM ecc.

- **VA e PT a infrastruttura wireless**: è una procedura specifica per la verifica delle reti senza fili, spesso lasciate senza adeguata manutenzione o sistemi di sicurezza.

I **Penetration Test** consentono ai team di sicurezza di capire in modo preciso le modalità con cui i criminali potrebbero accedere e danneggiare il

sistema e quindi correggere, o potenziare, i controlli di sicurezza per evitare che accada.

Al termine delle procedure viene fornito un report dettagliato sulle vulnerabilità riscontrate, la lista delle violazioni effettuabili con relativa modalità, la valutazione del livello di rischio per ognuna e le indicazioni per correggerle.

Da citare il **CVE** (**C**ommon **V**ulnerabilities and **E**xposures), uno standard utilizzato in cybersicurezza per identificare e riferire vulnerabilità informatiche o esposizioni comuni. Il suo obiettivo è quello di fornire un sistema di nomenclatura unificato per rendere più facile l'individuazione, il monitoraggio e la gestione delle vulnerabilità nei sistemi informatici e nei software.
Le caratteristiche chiave del CVE sono:

- **Numerazione univoca**: ad ogni vulnerabilità rilevata viene assegnato un numero di identificazione univoco, noto come "CVE ID", nel formato "CVE-anno-numero".

- **Dettagli descrittivi**: ogni CVE ID è associato a una descrizione dettagliata della vulnerabilità, che spiega cosa è, come può essere sfruttato e quali sono le potenziali conseguenze.

- **Aggiornamenti e Monitoraggio**: i CVE sono aggiornati e monitorati costantemente. Questa pratica consente agli amministratori di sicurezza e ai professionisti di rimanere aggiornati sulle nuove vulnerabilità e prendere misure per mitigarle e correggerle.

- **Referenziamento incrociato**: ogni CDE ID è collegato a fonti attendibile e affidabili, come avvisi di sicurezza, correzioni e patch rilasciate dagli sviluppatori software o dagli enti responsabili della sicurezza.

- **Standardizzazione**: il sistema CVE è un importante standard di riferimento nel settore, e viene utilizzato in tutto il mondo. Aiuta a eliminare la confusione nei riferimenti alla vulnerabilità e permette la collaborazione e lo scambio di informazioni tra esperti di sicurezza.

Quando una nuova vulnerabilità viene identificata e riceve un CVE ID, è più facile per il tecnico che effettua un vulnerability assessment studiarla e sviluppare soluzioni per risolvere il problema.

Fonti:
https://www.agendadigitale.eu/sicurezza/vulnerability-assessment-e-penetration-test-cosa-sono-e-in-cosa-sono-diversi/

https://www.defensis.it/servizi/procedura_vulnerability_assessment.htm

https://www.cybersecurity360.it/soluzioni-aziendali/vulnerability-assessment-cose-e-come-farlo-per-mettere-al-sicuro-i-dati-aziendali/