VULNERABILITY ASSESSMENT

COMPUTER DESIGN S.r.l.
Santo Stefano Ticino – Via Piave, 46 – 20010 (MI)
www.cdesign-group.com (+39) 02 97 48 21

DI CHE COSA SI TRATTA?

Nell'ambito delle tecnologie ICT, il Vulnerability Assessment (VA) è in particolare il processo di valutazione delle vulnerabilità e dei relativi rischi presenti nelle reti di computer, sistemi, hardware, applicazioni e altri enti dell'infrastruttura ICT ad ogni livello fisico e logico.

Il Vulnerability Assessment è da considerarsi una best practice fondamentale nella gestione di una rete informatica sia alla luce delle normative di conformità richieste alle organizzazioni che, ancor prima, nello svolgimento efficiente delle operazioni aziendali.

Il cuore di un VA è un'analisi che assegna un livello di rischio a ciascuna vulnerabilità in base a precisi standard come il CVSS (Common Vulnerability Scoring System).

A questa analisi possono anche essere correlati in modo personalizzato parametri di priorità, urgenza e impatto che indicano la dipendenza delle funzioni aziendali dalle risorse affette per permettere di concentrarsi dapprima su quelle vulnerabilità che, se sfruttate, potrebbero creare il maggior numero di problemi per l'organizzazione.

VANTAGGI

La valutazione delle vulnerabilità e il piano di consolidamento garantiscono a un'organizzazione i seguenti vantaggi:

- Identificazione tempestiva e coerente dei rischi e delle minacce;
- Pianificazione ed esecuzione di azioni correttive con la adeguata priorità;
- Protezione dei sistemi da accessi non autorizzati e da compromissioni dei dati;
- Ottemperanza alle esigenze di conformità sia in generale che per settori specifici (ad esempio GDPR, HIPAA e PCI DSS)

FASI DI ESECUZIONE

Assessment: Tra le metodologie per l'esecuzione delle valutazioni di vulnerabilità la più efficace in termini di tempo e costi è l'analisi tramite un software di scansione automatica corredato di un database di vulnerabilità: esso viene configurato per analizzare in modo completo ogni ente dell'infrastruttura in esame, eseguendo diversi tipi di scansioni con o senza credenziali note, dall'interno della rete e/o dall'esterno.

COMPUTER DESIGN

Il software garantisce un'elevata efficacia grazie a un frequente aggiornamento del proprio database, riduce al minimo l'evidenza di falsi positivi e falsi negativi nei rilevamenti e fornisce risultati sia fruibili senza post-processo in termini di valore CVSS che eventualmente integrabili con altre fonti dati e/o considerazioni soggettive per analisi ulteriormente personalizzate.

Remediation: L'attività di VA deve essere completata con l'esecuzione delle operazioni di consolidamento delle vulnerabilità scoperte che dipende dalla natura di ciascuna risorsa vulnerabile: ad esempio firmware di un hardware, sistema operativo di un computer, topologia della rete ecc.

DOCUMENTAZIONE

Al termine dell'attività verrà prodotta la seguente documentazione:

- Output integrale dello strumento di scansione con le note per una corretta interpretazione; Presentazione riassuntiva dei risultati ottenuti dall'analisi delle vulnerabilità con evidenza degli stati di crisi;
- Proposta Tecnico/economica per la risoluzione puntuale delle vulnerabilità evidenziate nel report;
- Proposta Tecnico/economica per un contratto di patching e update gestito. Questo servizio permette di avere costantemente aggiornata la proposta infrastruttura con le patch e le vulnerabilità riconosciute. Ad ogni ciclo di aggiornamento sarà eseguita una VA per certificare lo stato dell'infrastruttura.

IL CONSIGLIO DEGLI ESPERTI

Come avviene per tutti i processi di miglioramento della qualità, l'attività di analisi delle vulnerabilità e della loro successiva risoluzione deve essere effettuata ciclicamente essendo in continua evoluzione tecnologica sia l'infrastruttura informatica che le possibili tecniche di attacco.