Vulnerability Assessment

Cos'è il Vulnerability Assessment

Il servizio di VA è un'analisi di sicurezza che ha l'obiettivo di identificare, classificare e misurare tutte i rischi e le vulnerabilità dei sistemi informativi aziendali. In pratica si tratta di realizzare una fotografia dei sistemi informatici mirata a verificare quanto un'azienda è esposta e quali rischi corre nel caso in cui le protezioni di cui si è dotata dovessero venire bypassate.
Con la valutazione del livello di sicurezza si ha una visione dello stato e permette di identificare tutti quei contesti da migliorare al fine di ridurre eventuali attacchi esterni ed interni e tutelare i propri dati aziendali.
Al termine della valutazione del VA viene fornito un report dettagliato contenente i risultati dell'analisi svolta e le indicazioni sulle eventuali contromisure da adottare per risolvere le problematiche di sicurezza rilevate.

Perché fare una scansione delle vulnerabilità?

Uno degli errori in cui più frequentemente incorrono le aziende è la convinzione di sentirsi invulnerabili.
Esistono infatti due miti molto diffusi tra gli imprenditori:

- La convinzione che basti un antivirus per proteggere la rete
- La convinzione che la propria azienda non sia un bersaglio

Cos'è vulnerabile e cosa è necessario controllare?

Sfortunatamente, quando si parla di sicurezza della rete aziendale, la maggior parte delle organizzazioni si ferma alla sicurezza perimetrale, al software antivirus o al massimo alla gestione delle patch.
Ecco invece una lista di elementi potenzialmente vulnerabili ai quali non si presta mai sufficiente attenzione:

- Cartelle condivise non protette
- Sistemi lasciati con impostazioni di fabbrica
- Dispositivi esterni non autorizzati collegati alla rete aziendale
- Dispositivi o applicazioni dati in gestione a terzi
- Account utente di default non necessari attivi
- Porte TCP aperte non necessarie
- Esecuzione di servizi Web che contengono vulnerabilità note

Quali sono i vantaggi del Vulnerability Assessment

Lo scopo del VA è quello di fornire una valutazione complessiva del livello di sicurezza del sistema informativo aziendale per poter poi intraprendere le opportune contromisure. Il primo vantaggio è certamente la consapevolezza del livello di sicurezza dei propri sistemi e la conseguente opportunità di abbassare il livello di rischio verso lo zero. Con una protezione alta, quindi con una politica di prevenzione degli attacchi, la continuità operativa dell'azienda è garantita e il pericolo di perdite economiche ridotto. C'è però un altro fattore essenziale connesso alla sicurezza: quello della reputation. Non c'è perdita peggiore, per un'azienda, di quella della reputazione.

La nostra proposta di consulenza come si articola!

STEP1 - Setup ed acquisizione delle informazioni

– Verifica della infrastruttura tecnica.
– Inventory Hardware e Software.
– Scelta degli strumenti.
– Rilascio dell'informativa comprensiva degli obblighi di riservatezza.
– Lista in dettaglio degli indirizzi IP o subnet per i quali si desidera il servizio.
– Fornitura di eventuali username (non le password).
– Pianificazione dei giorni ed orari durante i quali eseguire i test.

STEP2 – Valutazione Preliminare

– Esecuzione di un pre Security Assessment.
– Lettura dei indici BRD (Business Risk profiles) e DiDi (Defense in Depth Index)
– Lettura ed individuazioni degli ambiti di maggior rischiosità sui quali approfondire l'indagine.

STEP3 – Esecuzione e Verifica

– Esecuzione delle scansioni e collezione delle vulnerabilità.
– Valutazione delle vulnerabilità e verifica dei falsi positivi.
– Definizione degli scenari di attacco.
– Validazione degli scenari.
– Definizione del livello di sicurezza corrente.
– Consegna del primo report.
– Determinazione e spiegazione dell'eventuale impatto di ogni exploit/vulnerabilità.
– Definizione delle contromisure al fine di eliminare o impedire che le vulnerabilità vengano sfruttate.
– Organizzazione per priorità delle eventuali remediation.
– Attesa per un tempo congruo da parte del cliente al fine di applicare le remediation.
– Nuova esecuzione dei test in oggetto dopo le remediation.

STEP4 – Produzione della documentazione e chiusura

– Stesura del report finale.
– Chiusura con briefing con committente.
– Facilitare il recepimento delle raccomandazioni e azioni di rimedio.
– Rientro degli eventuali apparati concessi in comodato.

Sede Legale: 70125 - Bari, Via Pasubio, 35 Tel +39.0805427549, Fax +39.0805427549, e-mail info@pcsoftware.it, URL *www.pcsoftware.it*
CCIAA BARI N° 406755 - P.IVA 05235280723