Vulnerability Assessment

Procedura di verifica della sicurezza dei sistemi informatici di una rete

Il **Network Vulnerability Assessment** è parte di quelle procedure per la sicurezza informatica diventate fondamentali sia per le aziende private, sia per gli enti pubblici. Ricordiamo che la maggior parte delle intrusioni ai server avviene sfruttando vulnerabilità conosciute che potrebbero essere corrette con semplicità, per esempio eliminando errori di programmazione o errate configurazioni dell'infrastruttura.

Il **Vulnerability Assessment** è di fatto il check-up dei sistemi informatici di una rete, eseguito per accertarne il livello di sicurezza, rilevare la presenza di eventuali punti deboli ed eliminarli in modo da bloccare le possibili intrusioni e proteggere i dati aziendali e quelli dei clienti. Purtroppo, troppo spesso l'importanza di questa procedura viene sottostimata. Consideriamo che la valutazione andrebbe eseguita almeno una volta ogni sei mesi o ogni qualvolta si applicano modifiche alla struttura della rete. Se per le aziende private queste procedure sono importantissime, per gli enti pubblici diventano essenziali, in quanto le amministrazioni dovrebbero seguire le regole imposte da **AGID** (Agenzia per l'Italia digitale) che sollecita la verifica periodica della rete e dei servizi ad essa collegati.

PROCEDURA SICURA E NON INVASIVA

Di fatto il **Vulnerability Assessment** è una procedura non invasiva che non rallenta il funzionamento dell'infrastruttura ed è eseguita in varie fasi partendo dalla modalità **Black-box**, in cui il team di **HyperGrid** esegue l'analisi senza conoscere i dettagli della rete. A questa segue la valutazione in modalità **White-box**, dove l'azienda condivide con **HyperGrid** le informazioni relative alle risorse di rete da analizzare. Al termine della procedura viene fornito un dettagliato report con la descrizione di ogni vulnerabilità individuata e naturalmente le soluzioni per porvi rimedio. A ogni vulnerabilità viene attribuita una classificazione in base al suo grado di minaccia che può essere: **Bassa, Moderata, Alta** o **Critica**.

FASI DEL CONTROLLO DELLA SICUREZZA

Analisi di sicurezza: le vulnerabilità vengono analizzate tramite l'uso dei migliori strumenti software open source e proprietari in modo da non generare nessun impatto o rallentamento al funzionamento dell'infrastruttura.

Black-box: il team di **HyperGrid** esegue l'analisi sulle eventuali vulnerabilità in autonomia, senza essere a conoscenza dei dettagli relativi all'infrastruttura da analizzare.

White-box: il cliente condivide con **HyperGrid** informazioni relative alle sole risorse della rete da analizzare per poter eseguire test più approfonditi.

Valutazione dei rischi: le vulnerabilità rilevate vengono controllate per eliminare eventuali falsi positivi. Viene fornita una descrizione di ogni vulnerabilità e le procedure per eliminarle.

Misure correttive: vengono eseguite le azioni per rimuovere le vulnerabilità rilevate.

Controllo: si effettua una seconda scansione per verificare che le vulnerabilità siano state corrette.

PENETRATION TEST

Il **Penetration Test** o **Pen Test** è la verifica finale per dimostrare che l'infrastruttura non presenti più criticità. Diversamente dal **Vulnerability Assessment** (il cui scopo è di identificare le falle di sicurezza) è un'azione invasiva in cui viene simulato un attacco informatico verso un determinato obiettivo per testarne le difese e verificare che le operazioni di correzione delle criticità abbiano avuto successo. Il test è condotto su più fasi e si concentra sulle problematiche rilevate dal Vulnerability Assessment, in modo da verificare che le difese del sistema sono sicure. Viene anche verificata la tenuta generale delle difese interne ed esterne del sistema.

REPORT FINALE

Al termine dell'attività **HyperGrid** procede alla stesura della reportistica che costituisce la documentazione formale dei test eseguiti, contenente i risultati delle scansioni e dei test eseguiti durante le varie fasi della procedura.

Ricordiamo che è altamente consigliato svolgere la procedura di Vulnerability Assessment con la giusta frequenza al fine di assicurarsi che le configurazioni dei sistemi restino corrette e sicure durante il loro ciclo di vita, in particolare quando si eseguono modifiche alla rete.

Per richiedere ulteriori informazioni o un preventivo:

www.hypergrid.it - info@hypergrid.it - Tel. 0382 528875