



L'importanza della cyber security in azienda

VULNERABILITY ASSESSMENT



Vulnerability Assessment

M2
INFORMATICA

La valutazione di vulnerabilità (VA - Vulnerability Assessment) consiste in una scansione della rete aziendale interna ed esterna alla ricerca di falle: si tratta di una verifica oggettiva, svolta da un software e accompagnata da una relazione finale di conformità dell'infrastruttura. Una VA può essere richiesta sia da parte dell'autorità, in caso di ispezione o di data breach, sia da parte dei vostri stessi clienti, a dimostrazione del livello di accuratezza con cui avete valutato i rischi del vostro sistema informatico: essa certifica in maniera oggettiva quanto abbiate messo in essere per prevenire e minimizzare i rischi di data breach e i risultati ottenuti.

Una VA si svolge in più step:

- **attività preparatoria:** prevede un aggiornamento preventivo del sistema, aggiornando un Bios delle macchine (in particolare tutti i server e almeno un PC come campione, a simboleggiare la media dei PC presenti in azienda), in modo che il primo passaggio non evidenzi criticità evitabili;
- **testing:** si effettua una scansione che rileva tutti i rischi, sia per l'accesso indesiderato dall'esterno che dall'interno dell'infrastruttura.;
- **reporting:** viene generata una reportistica sullo stato dell'arte delle vulnerabilità del sistema, in base alla quale devono essere messe in atto eventuali rimedi.

01 ATTIVITÀ PREPARATORIA

Prevede, da parte dell'azienda, la verifica dello stato Windows Update e stato antivirus su tutti i client e la verifica/aggiornamento di server e PC. Solitamente una buona attività preparatoria volta a minimizzare le segnalazioni di sicurezza prevede le seguenti attività:

- aggiornamento degli apparati di rete quali firewall, switch access point e stampanti alle ultime versioni firmware o con le relative patch di sicurezza;
- aggiornamento dei sistemi operativi client mediante MS Windows Update o installazione delle ultime patch di sicurezza per sistemi OSX o Linux;
- aggiornamento dei sistemi operativi server e dei relativi pacchetti software installati che espongono servizi verso i client (inclusi NAS di backup);
- revisione dei criteri di accesso alla rete dall'esterno eliminando i servizi non utilizzati o superflui;
- aggiornamento alle ultime versioni di sicurezza dei servizi esposti all'esterno con particolare attenzione ai server WEB;
- aggiornamento su tutti i sistemi che lo prevedono degli antivirus installati.

Per ottenere un risultato più attendibile eventuali servizi sul firewall o sulle macchine che prevedono la quarantena o il blocco degli IP che eseguono scansione delle porte o degli IP vanno disattivati.

02 TESTING

A chiusura del primo step viene eseguita la scansione con lo strumento di Vulnerability Assessment sulla subnet della rete interna e sulla subnet della rete esterna.

Durata e complessità di questa fase derivano in gran parte dalla bontà di quanto messo in essere durante l'attività preparatoria

03 REPORTING

La reportistica al termine delle attività consiste in due documenti distinti, una relazione e un report:

- la relazione tecnica è di facile comprensione ed è da esibire in caso di verifiche o da presentare a clienti e fornitori per dimostrare lo stato di protezione del sistema;
- il report, estremamente tecnico e dettagliato, generato dallo strumento di VA, è un documento complesso e articolato, completo di tutte le vulnerabilità rilevate con i relativi punteggi secondo standard CVSS 2.0. Contiene informazioni confidenziali sul sistema che non devono essere conosciute da soggetti terzi. Nel caso, il report potrà essere presentato dietro specifica richiesta al Garante Privacy o alle autorità preposte.