

VA
Vulnerability Assessment

Vulnerability Assessment

Il servizio di **Vulnerability Assessment** fornito da ISGroup ha il compito di analizzare e valutare la sicurezza del sistema (o dei sistemi) al fine di rilevare eventuali vulnerabilità note.

L'attività può essere condotta **esternamente** o **internamente**. Nel caso di Vulnerability Assessment condotto esternamente, la scansione viene effettuata da un host remoto, il quale ha accesso al sistema solamente attraverso la rete **Internet**.

Nel secondo caso invece, la scansione viene effettuata dall'interno della rete privata (**Intranet**), in modo da avere maggiore visibilità sul sistema in esame.

Queste due configurazioni permettono di simulare diversi scenari di attacco: il primo **simula l'attacco da parte di un soggetto esterno** (ad esempio un concorrente aziendale sleale); il scenario invece **simula l'attacco da parte di un soggetto interno** (ad esempio un dipendente vendicativo).

In seguito allo svolgimento della fase di scansione tutte le vulnerabilità identificate vengono controllate per eliminare gli eventuali falsi positivi. Per ogni vulnerabilità effettiva viene fornita una descrizione dettagliata e soprattutto di come vi si può porre rimedio.

Dato l'alto numero di nuove vulnerabilità che vengono scoperte ogni giorno è fondamentale svolgere un Vulnerability Assessment con la **giusta frequenza** al fine di assicurarsi che le configurazioni dei sistemi siano corrette e le opportune patch di sicurezza applicate.

ISGroup fornisce soluzioni di Vulnerability Assessment adatte a qualsiasi esigenza e dimensione aziendale, garantendo un livello qualitativo elevato.

Descrizione del servizio

L'attività di **Vulnerability Assessment** inizia con **l'identificazione dei sistemi e delle risorse** (servizi, applicazioni web, etc) messe a disposizione. Successivamente tramite l'utilizzo di **tool automatici** e **manualmente** vengono identificate le problematiche di sicurezza conosciute in maniera **non invasiva**. I Vulnerability Assessment permettono di comprendere velocemente il livello di sicurezza di una rete.

L'identificazione avviene attraverso tecniche attive (ad esempio il numero di versione che il programma invia nelle risposte), passive o basate sull'inferenza (caratteristiche che un programma ha e non può nascondere). I risultati sono verificati manualmente in modo da eliminare i falsi positivi e ottenere un **Report** compatto e dettagliato, destinato sia al **Management** che allo **staff operativo** che dovrà correggere le problematiche.

Output

Il **Report** è un documento semplice e dettagliato che riassume i risultati dell'attività ed è suddiviso in tre differenti aree come precedentemente descritto:

Executive Summary

All'inizio del Report e di lunghezza non superiore ad una pagina, è il **riassunto di alto livello** destinato al Management.

Vulnerability Details

La parte tecnica che **descrive nel dettaglio le vulnerabilità** riscontrate e il loro impatto, dedicata al Security Manager.

Remediation Plan

Sezione tecnica con **istruzioni precise** su come risolvere le problematiche identificate, dedicata al System Administrator.

Richiedi servizi di Vulnerability Assessment

Lavorare con noi è molto semplice, chiamando il numero +39 045 4853232 o spedendo una mail a sales@isgroup.it potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di IT Security.