VA

VULNERABILITY ASSESSMENT

Il servizio offre un'analisi avanzata dell'infrastruttura, con l'obiettivo di fornire una visione chiara e dettagliata delle vulnerabilità presenti sui sistemi e nei servizi, calcolandone il livello di impatto, valutandone il rischio correlato al business e suggerendo azioni correttive.

SCOPO

Identificare, classificare e descrivere le vulnerabilità presenti che, se utilizzate, possono portare a compromissioni volontarie o involontarie del sistema in esame.

COME

Attraverso una scansione automatica coadiuvata dalla verifica manuale delle evidenze.

INPUT

Kick-Off Meeting, per permettere l'identificazione del raggio d'azione dell'attività: interno, esterno, wifi, vpn, applicativo.

OUTPUT

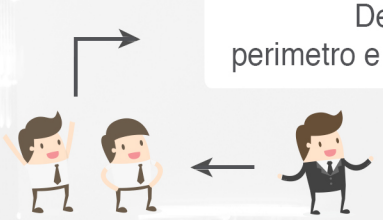
Documentazione tecnica e amministrativa dettagliata per evidenziare il livello di rischio, consegnata durante il Close-Off Meeting.

FOLLOW UP

A conclusione del Vulnerability Assessment si propone l'attività di Penetration Test e/o una serie di VA trimestrali. È comunque sempre consigliato un VA a seguito di ogni cambiamento significativo del sistema in esame.

Kick-Off Meeting

Definizione perimetro e modalità



Esecuzione Assessment

Close meeting e reportistica

Il potenziale impatto finanziario degli attacchi sulle aziende, dalle grandi alle piccole e medie imprese, è enorme. Oltre il 50% delle aziende analizzate nell'Annual Cybersecurity Report 2017 di Cisco ha dovuto affrontare severi controlli a seguito di una violazione.
I sistemi più colpiti sono quelli dei dipartimenti Operation & Finance, seguiti dalla perdita di reputazione del marchio e della fidelizzazione dei clienti. Per le aziende che hanno subito un attacco, l'effetto è stato notevole ed è preoccupante che i tempi medi impiegati per rilevare la minaccia si aggirino intorno ai 200 giorni.
- Il 22% delle aziende ha perso clienti - il 40% ha perso oltre il 20% della propria base di clienti.
- Il 29% ha perso fatturato - il 38% ha subito perdite per oltre il 20%delle entrate.
- Il 23% ha perso delle opportunità di business – il 42% ha preso oltre 20%.

Effettuare con regolarità attività di Ethical Hacking come Vulnerability Assessment e Penetration Test, abbatte i rischi di intrusione e perdita di dati sensibili dell'azienda. Non aspettare di avere subito un data breach!

NETMIND
SYSTEM INTEGRATOR