WAPT

WEB APPLICATION PENETRATION TEST

L'attività, con un focus specifico sulle tecnologie web, permette di rivelare e quindi correggere problemi di sicurezza legati sia alle tecnologie utilizzate (es. linguaggio di programmazione, sistema operativo, database server, …) sia alla logica applicativa studiata per guidare l'utente nell'utilizzo dell'applicazione o del sito web.

SCOPO

Ricercare tutte le vulnerabilità esposte dell'applicazione, che possono essere sfruttate per un attacco.

COME

Viene tentata l'intrusione nei sistemi seguendo, fra le altre, le linee guida OWASP. Si tratta di un'attività manuale coadiuvata dall'utilizzo di strumenti automatizzati.

INPUT

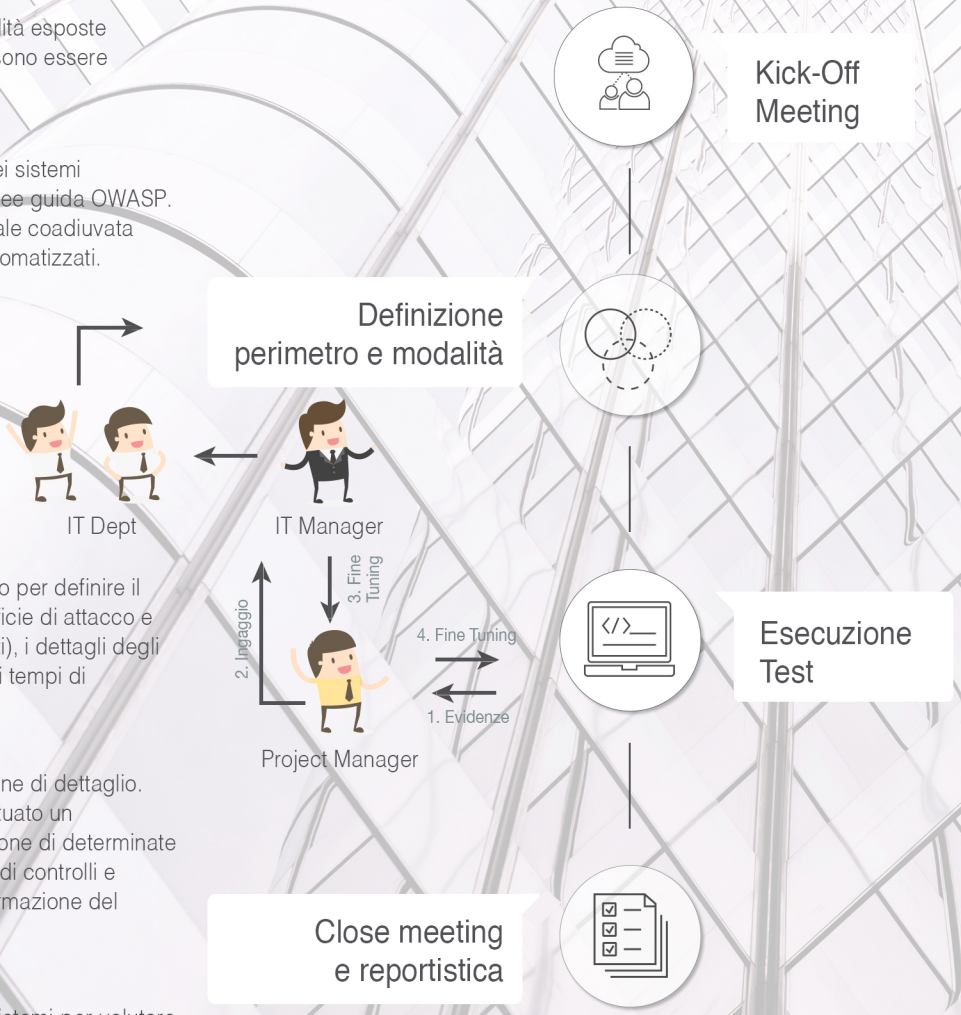
Kick-Off Meeting, necessario per definire il perimetro da testare (superficie di attacco e livelli di autorizzazione/utenti), i dettagli degli scenari di attacco, i modi e i tempi di intervento.

OUTPUT

Close-Off meeting e relazione di dettaglio. A corredo può essere effettuato un affiancamento per la soluzione di determinate criticità, l'implementazione di controlli e politiche di sicurezza, la formazione del personale.

FOLLOW UP

Si consiglia un'analisi dei sistemi per valutare l'efficacia delle contromisure adottate dall'azienda dopo 3/6 mesi dal primo WAPT. Nel caso di software di proprietà del cliente, viene proposta l'attività di Code Review.



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