Report Rilevamento Attacchi

Utente: Banana

TITOLO: Drive-by Download

CATEGORIA: Attacchi alle applicazioni web e ai database

ESITO:

Possibile attacco di tipo 'Drive-by Download' rilevato.

DESCRIZIONE:

Il Drive-by Download è un attacco che scarica ed esegue automaticamente codice dannoso sul dispositivo dell’utente quando visita un sito web compromesso, senza richiedere alcuna azione.nModalità di esecuzione:n- Il sito web è stato infettato con codice malevolo che sfrutta vulnerabilità del browser o plugin.n- L’utente visita inconsapevolmente il sito e il malware viene installato.n- L’attacco può avvenire anche tramite pubblicità (malvertising).nPossibili conseguenze:n- Installazione di malware, ransomware o spyware.n- Compromissione della sicurezza del dispositivo.n- Accesso remoto non autorizzato.

LIVELLO DI RISCHIO:

medio

CONTROMISURE:

Consigli pratici per la prevenzione:n- Mantenere aggiornati browser, plugin e sistemi operativi.n- Usare estensioni di sicurezza per il browser.n- Navigare su siti affidabili e dotati di certificati HTTPS.n- Utilizzare antivirus con protezione web attiva.

Risposte Sì: 2 / 4

TITOLO: Social Engineering

CATEGORIA: Tecniche di intrusione e manipolazione avanzata

ESITO:

Possibile attacco di tipo 'Social Engineering' rilevato.

DESCRIZIONE:

Il Social Engineering è una tecnica di manipolazione psicologica che sfrutta la fiducia dell’utente per ottenere informazioni riservate o indurlo a compiere azioni dannose.nModalità di esecuzione:n- L’attaccante può fingere di essere un collega, un tecnico IT o un’entità affidabile.n- Può avvenire tramite telefono, email o interazione diretta.n- Spesso è utilizzato in combinazione con altri attacchi (es. phishing).nPossibili conseguenze:n- Rivelazione di password o dati sensibili.n- Installazione di malware da parte dell’utente stesso.n- Accesso non autorizzato a reti aziendali.

LIVELLO DI RISCHIO:

medio

CONTROMISURE:

Consigli pratici per la prevenzione:n- Formare il personale a riconoscere tentativi di ingegneria sociale.n- Verificare sempre l’identità di chi richiede accesso o informazioni.n- Stabilire procedure di sicurezza per richieste sensibili.n- Simulare periodicamente attacchi per testare la consapevolezza.

Risposte Sì: 3 / 4