Report Rilevamento Attacchi

Utente: Banana

TITOLO: Zero-Day Attack

CATEGORIA: Attacchi a livello sistemico o industriale

ESITO:

Possibile attacco di tipo 'Zero-Day Attack' rilevato.

DESCRIZIONE:

Un Zero-Day Attack sfrutta vulnerabilità sconosciute o non ancora corrette in software o hardware. Poiché non esistono ancora patch ufficiali, questi attacchi sono estremamente pericolosi.nModalità di esecuzione:n- L’attaccante scopre una vulnerabilità prima che sia nota al produttore.n- Crea un exploit per colpirla prima che venga risolta.n- Può diffondersi tramite file infetti, siti web, app vulnerabili.nPossibili conseguenze:n- Compromissione completa del sistema target.n- Furto di dati, controllo remoto o sabotaggio.n- Difficoltà nell’individuazione e risposta.

LIVELLO DI RISCHIO:

alto

CONTROMISURE:

Consigli pratici per la prevenzione:n- Adottare soluzioni di sicurezza basate sul comportamento, non solo su firme.n- Tenere sempre aggiornati i sistemi.n- Limitare i privilegi degli utenti e segmentare i sistemi.n- Monitorare il traffico e i log per attività anomale.

Risposte Sì: 3 / 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: 4 / 4