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. Modalità di esecuzione: - L’attaccante scopre una vulnerabilità prima che sia nota al produttore. - Crea un exploit per colpirla prima che venga risolta. - Può diffondersi tramite file infetti, siti web, app vulnerabili. Possibili conseguenze: - Compromissione completa del sistema target. - Furto di dati, controllo remoto o sabotaggio. - Difficoltà nell’individuazione e risposta.

LIVELLO DI RISCHIO:

alto

CONTROMISURE:

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

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. Modalità di esecuzione: - L’attaccante può fingere di essere un collega, un tecnico IT o un’entità affidabile. - Può avvenire tramite telefono, email o interazione diretta. - Spesso è utilizzato in combinazione con altri attacchi (es. phishing). Possibili conseguenze: - Rivelazione di password o dati sensibili. - Installazione di malware da parte dell’utente stesso. - Accesso non autorizzato a reti aziendali.

LIVELLO DI RISCHIO:

medio

CONTROMISURE:

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

Risposte Sì: 2 / 4