Report Rilevamento Attacchi

Utente: Banana

TITOLO: Supply Chain Attack

CATEGORIA: Attacchi a livello sistemico o industriale

ESITO:

Possibile attacco di tipo 'Supply Chain Attack' rilevato.

DESCRIZIONE:

Un Supply Chain Attack (attacco alla catena di fornitura) colpisce indirettamente un’organizzazione compromettendo fornitori o partner terzi. L’attaccante inserisce codice malevolo o sfrutta vulnerabilità nei software o hardware forniti da terzi. Modalità di esecuzione: - Compromissione di aggiornamenti software distribuiti da vendor legittimi. - Infiltrazione nei sistemi di un fornitore con accesso alla rete target. - Distribuzione di componenti hardware alterati. Possibili conseguenze: - Infezione di numerosi sistemi con un solo attacco. - Diffusione silenziosa e difficilmente rilevabile. - Impatto esteso a tutta l’infrastruttura aziendale o nazionale.

LIVELLO DI RISCHIO:

alto

CONTROMISURE:

Consigli pratici per la prevenzione: - Monitorare e valutare periodicamente i fornitori di software e hardware. - Applicare controlli di integrità e firma digitale sui pacchetti installati. - Segmentare la rete per limitare gli accessi da terze parti. - Effettuare audit di sicurezza su fornitori critici.

Risposte Sì: 4 / 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: 3 / 4