Report Rilevamento Attacchi

Utente: Banana

TITOLO: Phishing

CATEGORIA: Attacchi basati sull’inganno umano (Ingegneria sociale)

ESITO:

Possibile attacco di tipo 'Phishing' rilevato.

DESCRIZIONE:

Il phishing è una tecnica di ingegneria sociale utilizzata da criminali informatici per indurre gli utenti a fornire volontariamente informazioni sensibili, come credenziali di accesso, numeri di carte di credito o altri dati personali. Gli attacchi di phishing si basano sull’inganno: l’attaccante si presenta come un’entità fidata, come una banca, un servizio online noto o un collega di lavoro, per ottenere la fiducia della vittima. Modalità di esecuzione: - L’utente riceve un’email, un SMS o un messaggio istantaneo che sembra provenire da una fonte legittima. - Il messaggio contiene spesso un link a un sito contraffatto, graficamente identico a quello ufficiale. - Una volta che la vittima inserisce i propri dati, questi vengono inviati direttamente al truffatore. - Esistono anche varianti più sofisticate, come il spear phishing, mirato a persone specifiche, e il vishing, condotto per telefono. Possibili conseguenze: - Accesso illegittimo a conti bancari o profili online. - Perdita di dati personali e aziendali. - Furto d’identità e danni reputazionali. - Possibilità che l’account compromesso venga usato per ulteriori truffe.

LIVELLO DI RISCHIO:

alto

CONTROMISURE:

Consigli pratici per la prevenzione: - Diffidare di messaggi che creano urgenza (“Il tuo account sarà sospeso!”, “Hai vinto un premio!”). - Verificare sempre l’indirizzo del mittente e il dominio dei link. - Non cliccare su allegati o collegamenti sospetti. - Attivare l’autenticazione a due fattori (2FA) per i propri account. - Utilizzare software antivirus e filtri antispam aggiornati.

Risposte Sì: 2 / 4

TITOLO: Man-in-the-Middle (MitM)

CATEGORIA: Attacchi diretti agli account e all’identità

ESITO:

Possibile attacco di tipo 'Man-in-the-Middle (MitM)' rilevato.

DESCRIZIONE:

Il Man-in-the-Middle (MitM) è un attacco in cui un malintenzionato si inserisce segretamente nella comunicazione tra due parti (ad esempio tra un utente e un sito web), con l’intento di intercettare, modificare o manipolare i dati scambiati. Modalità di esecuzione: L’attacco avviene spesso su reti Wi-Fi pubbliche non protette, dove l’aggressore può facilmente intercettare il traffico. Può consistere in una falsa rete Wi-Fi (“evil twin”) che imita una rete legittima. L’attaccante osserva o modifica il traffico in transito, senza che le vittime se ne accorgano. In alcuni casi, può installare certificati falsi per “spiare” il traffico cifrato. Possibili conseguenze: Furto di credenziali, email, chat o dati bancari. Alterazione di contenuti trasmessi (es. inserimento di malware). Accesso non autorizzato a servizi online. Rischi legali e danni alla privacy personale o aziendale.

LIVELLO DI RISCHIO:

alto

CONTROMISURE:

Consigli pratici per la prevenzione: Utilizzare solo connessioni HTTPS (lucchetto nella barra del browser). Evitare di inserire dati sensibili su reti Wi-Fi pubbliche. Usare una VPN affidabile per cifrare il traffico. Tenere aggiornati browser e dispositivi per evitare vulnerabilità note.

Risposte Sì: 4 / 4

TITOLO: Brute Force Attack

CATEGORIA: Attacchi diretti agli account e all’identità

ESITO:

Possibile attacco di tipo 'Brute Force Attack' rilevato.

DESCRIZIONE:

Il Brute Force Attack è una tecnica utilizzata per ottenere accesso non autorizzato a un sistema provando tutte le combinazioni possibili di password o chiavi crittografiche. Modalità di esecuzione: - L’attaccante utilizza strumenti automatizzati per testare milioni di combinazioni di password. - Spesso è mirato a sistemi con credenziali deboli o senza limitazioni sul numero di tentativi. - Può essere usato anche per decrittare file o reti Wi-Fi. Possibili conseguenze: - Accesso non autorizzato ad account personali o aziendali. - Furto di dati sensibili. - Compromissione di sistemi o servizi con privilegi elevati.

LIVELLO DI RISCHIO:

alto

CONTROMISURE:

Consigli pratici per la prevenzione: - Utilizzare password complesse e uniche. - Implementare limiti di tentativi di login e blocchi temporanei. - Attivare l’autenticazione a due fattori (2FA). - Monitorare i log di accesso per attività sospette.

Risposte Sì: 4 / 4

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: 2 / 4