Piano di Risposta Integrato a un Attacco di Sicurezza Informatica

Un attacco informatico ha compromesso un server cloud aziendale non aggiornato, probabilmente proveniente da attori esterni (Iran, Corea del Nord, o Russia), con l’obiettivo di rubare dati sensibili dei clienti, possibili prede per un attacco ransomware. Di seguito le principali azioni per ciascun dipartimento coinvolto:

1. Responsabile Cyber Security

Obiettivi: Analizzare la natura e la portata dell’attacco, verificare il furto di dati.

Azioni immediate: Analisi dei log di accesso, controllo degli hash dei file, tracciamento dell’IP sospetto. Isolamento del server compromesso e disattivazione delle credenziali sospette.

Proposte operative: Aggiornamento dei server, hardening della sicurezza, introduzione di sistemi di analisi comportamentale basati su AI.

2. Responsabile Tecnico

Visione del problema: L'attacco ha mirato a rubare dati sensibili per un possibile attacco ransomware. Il server compromesso non è stato aggiornato da oltre tre mesi.

Azioni: Ripristino e aggiornamento del server compromesso, correzione delle vulnerabilità sfruttate.

3. Responsabile Legale/Privacy

Obblighi legali: Notifica al Garante entro 72 ore, comunicazione agli interessati solo se il rischio è elevato.

Azioni: Coordinamento con il team Cyber Security per identificare i dati compromessi, preparazione della notifica al Garante, comunicazione ai clienti coinvolti.

4. Responsabile Marketing

Comunicazione iniziale: Dichiarazione tempestiva dell'incidente, ammettendo il problema senza minimizzarlo.

Azioni successive: Aggiornamenti regolari attraverso canali ufficiali (social, newsletter). Monitoraggio delle conversazioni sui social media e supporto diretto ai clienti.

Post-incidente: Comunicazione delle misure preventive adottate per evitare future violazioni.

Conclusione:

La gestione dell’incidente richiede una collaborazione tra i dipartimenti per contenere l'attacco, garantire la conformità alle normative, mantenere la fiducia dei clienti e prevenire futuri incidenti. Una risposta coordinata e tempestiva è essenziale per ridurre i danni a breve e lungo termine.