Cos’è il phishing?

Il phishing è una tipologia di truffa informatica e di ingegneria sociale che consiste nel convincere la vittima a rivelare informazioni personali, fingendosi un mittente fidato o affidabile. Un esempio comune è ricevere un'email apparentemente inviata dalla propria banca, che segnala un accesso sospetto all'account e invita a cliccare su un link per reimpostare le credenziali.

Come un attacco di phishing può compromettere la sicurezza aziendale?

Un attacco di phishing può compromettere la sicurezza aziendale in diversi modi. Le credenziali rubate possono essere utilizzate per accedere a dati sensibili. Inoltre, il link presente nell'email di phishing potrebbe condurre al download di un malware, che a sua volta può permettere l'accesso non autorizzato ai sistemi aziendali o risultare in un attacco ransomware, "prendendo in ostaggio" i dati aziendali. Se l'attacco di phishing provoca il furto di dati, l'azienda potrebbe subire una perdita di fiducia da parte dei clienti.

Analisi del rischio:

Un attacco phishing potrebbe interrompere la normale operatività aziendale durante le attività di bonifica. Inoltre, potrebbe causare danni finanziari. In caso di attacco ransomware, l'azienda potrebbe essere costretta a pagare per "liberare" i dati e sostenere i costi di ripristino del sistema, oltre a dover affrontare eventuali conseguenze legali nel caso di furto di dati sensibili dei clienti. Le risorse compromesse potrebbero includere credenziali di accesso ai sistemi aziendali, proprietà intellettuali (come brevetti o progetti), dati personali e finanziari di clienti o dipendenti, oppure i sistemi stessi.

Pianificazione della remediation:

Per ridurre al minimo le possibilità di un attacco di phishing, è necessaria l’implementazione di filtri per le email sospette, capaci di identificare messaggi potenzialmente pericolosi. La formazione dei dipendenti è fondamentale per prevenire il successo di tali attacchi. Implementare procedure di monitoraggio e auditing di sicurezza può essere utile per individuare tempestivamente eventuali anomalie. La segmentazione della rete aziendale è un metodo efficace per limitare il danno in caso di compromissione, confinandolo a specifiche aree. Limitare i privilegi dei dipendenti ai soli necessari riduce l'impatto di un eventuale furto di credenziali. Infine, una comunicazione rapida alle aziende partner riguardo ad attacchi andati a segno può impedire la diffusione del problema.

Implementazione della remediation:

Esistono filtri antiphishing che possono mettere in quarantena le email sospette o avvisare l'utente della natura sospetta del mittente. È possibile disabilitare link e immagini provenienti da fonti non affidabili, e aggiungere una notifica che segnala la ricezione di email da indirizzi esterni al sistema aziendale. La formazione del personale è essenziale per insegnare come riconoscere le email sospette e quali misure adottare. I dipendenti dovrebbero essere incoraggiati a controllare l'indirizzo email del mittente e segnalare tempestivamente eventuali email sospette alla persona incaricata della gestione della sicurezza. Bloccare automaticamente i domini noti per essere utilizzati in attacchi di phishing potrebbe aumentare ulteriormente la sicurezza.

Mitigazione dei rischi residui:

Effettuare test periodici per verificare se i dipendenti sono in grado di riconoscere le email di phishing è una buona prassi, in modo da poter correggere comportamenti rischiosi o implementare misure più stringenti. L'adozione dell'autenticazione a due fattori fornisce un ulteriore livello di sicurezza: anche in caso di furto di credenziali, queste non sarebbero sufficienti per accedere ai sistemi. Gli aggiornamenti regolari dei sistemi aiutano a ridurre le vulnerabilità. Per evitare lo spoofing, è possibile implementare i protocolli SPF (Sender Policy Framework), che verifica se il server è autorizzato a inviare email per conto di un determinato dominio, DKIM (DomainKeys Identified Mail), che garantisce che il contenuto della mail non sia stato alterato, e DMARC (Domain-based Message Authentication, Reporting & Conformance), che coordina i due protocolli e fornisce istruzioni su come gestire le email che non superano questi controlli. Infine, è importante verificare la sicurezza delle VPN aziendali e, se necessario, rafforzarne le misure di sicurezza.