Minaccia di Phishing

1. **Identificazione della Minaccia:**

È un tipo di frode ideato allo scopo di rubare l'identità di un utente della Rete; l'attaccante cerca di appropriarsi di informazioni quali numeri di carta di credito, password, informazioni relative ad account o altre informazioni personali convincendo l'utente a fornirgliele con falsi pretesti. Il phishing viene generalmente attuato tramite posta indesiderata o finestre a comparsa.

Il phishing rientra nell'ambito della frode informatica disciplinata dall'**art. 640-*ter* c.p.** che punisce l'illecito arricchimento conseguito con l'impiego fraudolento di un sistema informatico. Il raggiro al sistema informatico può configurarsi in una qualsiasi delle fasi del processo di elaborazione dei dati. Ai fini dell'applicabilità della norma è necessario che colui che agisce procuri a sé o ad altri un ingiusto profitto.
Altra norma del codice penale applicabile al phishing è sicuramente l'art. 615-quater "detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici" che punisce la detenzione non autorizzata di codici di accesso, come password, P.I.N., smart card, ecc. ed anche la loro diffusione illecita a terzi non autorizzati. Inoltre, è contemplato, quale reato, anche la diffusione di istruzioni tecniche su come eludere od ottenere i suddetti codici di accesso. Non è sufficiente la detenzione o la diffusione, illecite, di codici ma è necessario che da tale detenzione o diffusione ne derivi un profitto per sé o per altri ovvero un danno a terzi.

Il phishing può compromettere la sicurezza dell'azienda in vari modi:

- **Furto di credenziali**
- **Distribuzione di malware**

2. **Analisi del Rischio:**

Il phishing può portare a una serie di conseguenze dannose come:

- **Perdita di dati sensibili:** possono essere rubati dati aziendali critici (dati finanziari, progetti interni, informazioni dei clienti, proprietà intellettuali);
- **Interruzione operativa:** Malware possono bloccare i sistemi aziendali, ad esempio, rendendo inutilizzabili i server e i computer fino al pagamento del riscatto.
- **Danni finanziari:** Oltre al pagamento di eventuali riscatti andranno affrontati i costi relativi alla gestione dell'incidente, alla riparazione dei sistemi compromessi e alla potenziale perdita di clienti.
- **Compromissione della fiducia:** Un attacco di phishing riuscito può danneggiare la reputazione dell'azienda se vengono compromesse informazioni dei clienti, partner o dipendenti.

3. **Pianificazione della Remediation:**

Un piano di risposta efficace deve includere diverse fasi chiave per fermare la campagna di phishing.

Innanzitutto, sarà essenziale una comunicazione tempestiva ai dipendenti dell'attacco in corso, evidenziando l'importanza di non interagire con email sospette. Identificazione di un canale dedicato attraverso il quale i dipendenti stessi possano repentinamente segnalare email sospette. Essenziale, infine, sarà la formazione dei dipendenti.

Sarà poi necessario effettuare un'analisi delle email fraudolente al fine di identificarne schemi comuni e segnalarli. Si potrà poi procedere bloccando i domini sospetti e filtrando i messaggi in entrata.

Sarà poi sicuramente necessario effettuare un controllo dei sistemi aziendali al fine di verificare il livello di compromissione andando ad individuare eventuali attività sospette come accessi non autorizzati.

4. **Implementazione della Remediation:**

Formazione dei dipendenti:
Implementare la formazione del personale organizzando, ad esempio, corsi di formazione obbligatoria o eseguendo test simulati al fine di addestrare i dipendenti a riconoscere e gestire eventuali attacchi di questo tipo.

Filtri anti-phishing e soluzioni di sicurezza email:
Previsione e rafforzamento di filtri anti-phishing nel sistema di posta aziendale, utilizzando soluzioni di sicurezza che bloccano email basate su firme di phishing, tecniche di ingegneria sociale o anomalie.

5. **Mitigazione dei Rischi Residuali:**

Test di phishing simulati: Esecuzione periodica di test simulati: Organizzare regolarmente campagne di phishing simulate per valutare la prontezza e la reazione dei dipendenti.

Aggiornamenti e patching regolari: Garantire che tutti i sistemi aziendali, i software e gli strumenti siano aggiornati regolarmente con le ultime patch di sicurezza. Implementare sistemi di aggiornamento automatici per ridurre il rischio di lasciare vulnerabilità non risolte nei software.

Risposta agli incidenti:
Aggiornare e testare regolarmente il piano di risposta agli incidenti, che dovrebbe includere procedure per la gestione di attacchi phishing, il ripristino dei sistemi e la comunicazione con partner e clienti in caso di violazioni.

Attacco DoS (Denial of Service)

1. **Identificazione della Minaccia:**

Famiglia di attacchi informatici orientati a colpire la disponibilità di uno o più servizi inibendone l'accesso; nel caso in cui questo tipo di attacco venga eseguito mediante l'utilizzo di sorgenti multiple distribuite viene identificato come Distributed Denial of Service (DDoS).
Un attacco DDoS si basa su un semplice presupposto: saturare un server con traffico inutile in modo da rallentare, o addirittura arrestare, i siti Web che ospita.

Effetti:

- **Impossibilità di accesso ai servizi web aziendali**
- **Riduzione delle prestazioni del sistema**
- **Impatto sulla continuità operativa**

2. **Analisi del Rischio:**

Un attacco DoS può avere un impatto significativo su un'azienda comportando:

- **Perdita di ricavi:**
  Se l'azienda si affida a servizi online, come l'e-commerce, l'indisponibilità del sito può comportare una perdita immediata di ricavi.
- **Danni alla reputazione**
- **Costi di mitigazione:**
  Per far fronte all'attacco, potrebbero essere necessarie risorse specializzate, costi di consulenza o aggiornamenti di infrastrutture di rete.
- **Interruzione della produttività:**
  La produttività dell'intera azienda può essere compromessa.

3. **Pianificazione della Remediation:**

Innanzitutto sarà necessario identificare le fonti dell'attacco mediante strumenti di monitoraggio della rete, al fine di analizzare il traffico anomalo. Utilizzare soluzioni avanzate per tracciare la provenienza geografica delle richieste e identificare potenziali reti botnet o nodi malevoli.
Sarà a questo punto necessario configurare il firewall per bloccare le richieste provenienti da IP sospetti o da aree geografiche non legittime. Sarebbe ideale attivare la funzionalità di rate limiting per controllare l'afflusso di traffico.
È poi importante informare il provider di servizi Internet dell'attacco per verificare se è possibile bloccare o filtrare il traffico a monte prima che raggiunga i server aziendali.
Considerare la possibilità di distribuire il traffico su più server o implementare una Content delivery Network (CDN) per ridurre l'impatto di un traffico elevato su un singolo server.
Informare i dipendenti e i responsabili IT della situazione, fornendo aggiornamenti regolari e attivando eventuali procedure di emergenza in caso di interruzione di altri servizi critici.

Una volta che il traffico malevolo è stato mitigato, condurre un'analisi dettagliata dell'attacco per individuare eventuali vulnerabilità o debolezze nell'infrastruttura di rete che possono essere rafforzate.

4. **Implementazione della Remediation:**

Utilizzo di load balancer:
Implementare un sistema di bilanciamento del carico per distribuire il traffico in ingresso su più server, riducendo il carico su un singolo server e aumentando la resilienza contro l'attacco.
Distribuire il traffico su data center in diverse località geografiche, utilizzando il routing basato su DNS o bilanciamento a livello globale. Questo riduce la possibilità che una sola area o nodo sia sovraccaricato.

Impostare meccanismi di protezione a monte:

Integrare soluzioni di protezione che si attivano automaticamente quando viene rilevato un volume di traffico anomalo, come il DNS-based scrubbing o il Traffic engineering.

Configurazione di regole firewall per bloccare il traffico sospetto:
Configurare i firewall per bloccare il traffico proveniente da IP sospetti, da regioni non legittime o che supera un determinato limite di richieste. I firewall di nuova generazione (NGFW) possono bloccare specifici pattern di traffico utilizzati negli attacchi DoS.
Implementare rate limiting per evitare che singoli indirizzi IP possano generare troppe richieste in un breve periodo di tempo. Questo riduce l'impatto degli attacchi basati sull'invio massivo di richieste.

5. **Mitigazione dei Rischi Residuali:**

Per la mitigazione dei rischi sarà necessario lavorare a stretto contatto con il team di sicurezza aziendale per sviluppare piani di risposta agli incidenti. Ciò include la definizione di procedure operative in caso di attacco, con ruoli e responsabilità chiaramente assegnati.
Sarà necessaria l'adozione di soluzioni di sicurezza avanzate come firewall basati su cloud, protezione degli endpoint e strumenti di analisi delle minacce che possano mitigare gli attacchi prima che raggiungano l'infrastruttura critica.

Previsione di test periodici di penetrazione per valutare la resilienza dell'infrastruttura aziendale a diversi tipi di attacchi DoS. Questo aiuta a identificare debolezze nelle configurazioni di rete e nelle soluzioni di mitigazione.
Simulazioni di attacchi DoS per misurare la reattività del team IT e la capacità di mitigazione del sistema.

Sulla base dei risultati dei test valutare e aggiornare periodicamente le politiche di sicurezza e i protocolli di emergenza assicurandosi che il personale sia addestrato e pronto a rispondere.