Strategie di Remediation e Mitigazione contro Phishing e Attacchi DoS

1. Introduzione

Il presente documento fornisce una panoramica dettagliata delle misure di **remediation** e **mitigazione** da adottare per fronteggiare due tra le principali minacce informatiche che affliggono le organizzazioni moderne: il **phishing** e gli attacchi **Denial of Service (DoS)**.

Nell'ambito della sicurezza informatica, la gestione efficace delle minacce si basa su due approcci complementari:

- **Remediation**, ovvero l'eliminazione delle vulnerabilità esistenti mediante azioni risolutive;
- **Mitigazione**, finalizzata a contenere l'impatto di un attacco fino all'attuazione di contromisure definitive.

2. Minaccia di Phishing

2.1 Definizione e modalità di attacco

Il phishing è una tecnica di attacco che sfrutta la manipolazione psicologica (social engineering) per indurre gli utenti a fornire informazioni sensibili o ad eseguire azioni compromettenti. Gli attori malevoli si avvalgono principalmente di:

- Email contraffatte,
- Pagine web falsificate,
- Comunicazioni ingannevoli apparentemente provenienti da fonti affidabili.

2.2 Valutazione del rischio

Il phishing può comportare gravi conseguenze per un'organizzazione, tra cui:

- **Compromissione di account** e accesso non autorizzato a sistemi aziendali;
- **Diffusione di malware** (es. ransomware, spyware);
- **Danni reputazionali** con impatti sulla fiducia di clienti e partner.

Le risorse particolarmente vulnerabili includono: account email, database sensibili e credenziali di accesso a sistemi gestionali e finanziari.

2.3 Strategia di remediation

a) Filtraggio e blocco proattivo

- Implementazione di filtri anti-phishing mediante soluzioni come *Microsoft Defender for Office 365* o *Proofpoint*.
- Configurazione dei protocolli **SPF**, **DKIM** e **DMARC** per la validazione delle email in entrata.
- Definizione di regole personalizzate per l'identificazione di pattern tipici delle email fraudolente.

b) Formazione e sensibilizzazione del personale

- Organizzazione di sessioni formative periodiche per incrementare la consapevolezza degli utenti.
- Diffusione di linee guida operative per la segnalazione tempestiva dei tentativi di phishing.
- Simulazioni regolari per testare la prontezza dei dipendenti.

c) Monitoraggio e risposta

- Integrazione di un sistema SIEM per la raccolta e l'analisi dei log di accesso.
- Impiego di soluzioni EDR come *CrowdStrike* o *Carbon Black* per il rilevamento di attività sospette in tempo reale.

d) Recupero e bonifica

- Revoca delle credenziali compromesse.
- Esecuzione di scansioni di sicurezza su endpoint e server.

- Applicazione delle patch ai sistemi affetti da vulnerabilità note.

2.4 Misure di mitigazione

- Abilitazione dell'autenticazione a due fattori (2FA) per gli account critici.
- Backup crittografati e conservati offline per i dati sensibili.
- Test ciclici di simulazione phishing per mantenere alto il livello di preparazione del personale.

---

3. Attacco DoS (Denial of Service)

3.1 Caratteristiche dell'attacco

Gli attacchi DoS (e la variante DDoS, Distributed Denial of Service) mirano a **rendere indisponibili servizi o risorse** aziendali, sovraccaricando infrastrutture IT con traffico anomalo e intenzionalmente eccessivo. Le tecniche più comuni includono:

- Saturazione della banda disponibile,
- Sovraccarico di CPU e RAM,
- Exploit di vulnerabilità in servizi esposti.

3.2 Valutazione del rischio

Un attacco DoS può causare:

- **Interruzione di servizi critici** (es. siti web, sistemi di pagamento),
- **Perdite economiche** dirette e costi di ripristino elevati,
- **Deterioramento della reputazione** aziendale.

Tra i servizi maggiormente esposti figurano: web server, applicazioni aziendali, database centrali e infrastrutture di rete.

3.3 Strategia di remediation

a) Individuazione e contenimento

- Analisi dei log di rete con strumenti come *Wireshark* o *Zeek*.
- Isolamento e blocco degli indirizzi IP responsabili tramite firewall dinamici.
- Supporto da parte dell'ISP per mitigare il traffico in entrata.

b) Filtraggio e protezione

- Configurazione di un **Web Application Firewall (WAF)** per il filtraggio avanzato.
- Integrazione di servizi anti-DDoS quali *Cloudflare*, *Akamai* o *AWS Shield*.
- Impiego del *blackhole routing* per neutralizzare flussi malevoli.

c) Resilienza e distribuzione

- Utilizzo di **load balancer** (es. *HAProxy*) per bilanciare il traffico.
- Integrazione di una **Content Delivery Network (CDN)** per alleggerire il carico diretto sui server.
- Aumento della capacità delle risorse hardware per assorbire picchi improvvisi.

d) Ripristino e consolidamento

- Ripristino dei servizi tramite backup aggiornati.
- Revisione delle policy di sicurezza di rete.
- Conduzione di una **post-mortem analysis** per identificare lacune nella protezione.

3.4 Misure di mitigazione

- Monitoraggio continuo del traffico di rete tramite soluzioni di Network Behavior Analysis.
- Test di stress e simulazioni periodiche per verificare la tenuta delle difese.
- Redazione di **piani di business continuity** e disaster recovery strutturati.

---

4. Conclusioni

Le minacce informatiche come il phishing e gli attacchi DoS richiedono un approccio integrato che combini:

- **Tecnologie avanzate di prevenzione e rilevamento**,
- **Processi formativi mirati per il personale**,
- **Procedure strutturate di risposta e recupero**.

Sintesi operativa

Minaccia	Prevenzione	Remediation	Mitigazione
Phishing	Formazione, SPF/DKIM/DMARC, filtri	Revoca credenziali, scansioni, patch	2FA, backup sicuri, simulazioni
DoS/DDoS	Firewall, CDN, bilanciamento del carico	Analisi traffico, WAF, blackhole	Monitoraggio, test stress, piani BCP

L’adozione sistematica di queste pratiche consente di rafforzare la postura di sicurezza aziendale e di rispondere efficacemente alle minacce presenti e future.