

# Cos'è il phishing e come funziona?

Il phishing è una forma di attacco informatico in cui gli aggressori cercano di ingannare gli utenti inducendoli a fornire informazioni sensibili (es. credenziali di accesso, numeri di carte di credito) o a scaricare malware tramite email, messaggi, o siti web fraudolenti. Gli attacchi di phishing sfruttano la manipolazione psicologica e la falsificazione dell'identità per sembrare comunicazioni affidabili.

## Come può compromettere la sicurezza aziendale?

Un attacco di phishing può:

- Rubare credenziali di accesso a sistemi critici.
  - Compromettere dati aziendali sensibili, come progetti, dati finanziari o informazioni sui clienti.
  - Diffondere malware o ransomware all'interno della rete aziendale.
  - Danneggiare la reputazione aziendale se i dati dei clienti vengono violati.
- 

## Analisi del Rischio

### Impatto potenziale sull'azienda:

- **Interruzione delle attività:** Credenziali compromesse potrebbero consentire l'accesso non autorizzato a sistemi critici.
- **Perdite finanziarie:** Costi per rimediare alla violazione, multe legate alla conformità (es. GDPR), e potenziale perdita di clienti.
- **Danno reputazionale:** La compromissione dei dati dei clienti può minare la fiducia dei clienti.

### Risorse compromettibili:

- **Credenziali di accesso:** Utenti interni ed esterni.
  - **Dati sensibili:** Informazioni personali, finanziarie o commerciali.
  - **Sistemi IT:** Server, database, e dispositivi endpoint.
  - **Reputazione aziendale.**
- 

## Pianificazione della Remediation

### Piano di risposta:

- **Identificazione e blocco:**

- Configurare i filtri di sicurezza email per rilevare e bloccare email phishing conosciute.
  - Utilizzare blacklist aggiornate per domini noti di phishing.
  - **Comunicazione interna:**
    - Inviare un alert a tutti i dipendenti per informarli dell'attacco.
    - Fornire istruzioni per segnalare email sospette e i passi per proteggere i propri account.
  - **Monitoraggio:**
    - Eseguire un'analisi forense dei sistemi compromessi.
    - Monitorare l'accesso ai sistemi per rilevare attività sospette.
- 

## Mitigazione dei Rischi Residuali

### Misure preventive:

- **Test simulati:** Condurre campagne di phishing simulate per valutare il livello di consapevolezza dei dipendenti.
  - **Autenticazione forte:** Implementare l'autenticazione a due fattori (2FA) per tutti i sistemi critici.
  - **Aggiornamenti:** Garantire aggiornamenti regolari di software e sistemi operativi per ridurre vulnerabilità sfruttabili.
  - **Backup regolari:** Eseguire backup dei dati critici, assicurandosi che siano offline o in reti isolate.
- 

## Implementazione della Remediation

### Passaggi pratici:

1. **Sicurezza email:**
    - Implementare soluzioni anti-phishing (es. SPF, DKIM, DMARC).
    - Configurare sistemi di rilevamento automatico per email sospette.
  2. **Formazione del personale:**
    - Organizzare workshop per aiutare i dipendenti a riconoscere tentativi di phishing.
    - Creare una guida rapida su come comportarsi di fronte a email sospette.
  3. **Policy aziendali:**
    - Aggiornare le policy per richiedere verifiche aggiuntive (es. chiamata diretta) per richieste sensibili ricevute via email.
    - Garantire che tutti i dispositivi siano dotati di antivirus aggiornati.
-

# Cos'è un attacco DoS e come funziona

Un attacco Denial of Service (DoS) mira a rendere inaccessibili servizi o risorse di rete sovraccaricandoli di richieste. Questi attacchi sfruttano la limitata capacità di risorse di un sistema (banda, CPU, RAM) inviando un numero massivo di richieste fasulle o sfruttando vulnerabilità specifiche del software.

## Impatto sull'azienda

- **Interruzione del servizio:** Gli utenti legittimi non riescono a connettersi ai servizi critici, come portali web, e-commerce, o sistemi aziendali interni.
  - **Perdite economiche:** La mancata disponibilità può portare a perdita di clienti, mancati guadagni, e danni alla reputazione.
  - **Rischi collaterali:** Un attacco DoS potrebbe mascherare attività più gravi come un'intrusione nella rete.
- 

## Analisi del Rischio

### Impatto Potenziale sull'Azienda

- **Clienti insoddisfatti:** Perdita di fiducia da parte dei clienti.
- **Impatto operativo:** Sistemi critici (come ERP, CRM o server e-mail) inaccessibili rallentano o bloccano le operazioni quotidiane.
- **Reputazione:** Il danno all'immagine può compromettere le relazioni a lungo termine con partner e clienti.

### Servizi Critici Coinvolti

- **Server web aziendali:** Accesso al sito web e servizi online.
  - **Sistemi di e-commerce:** Perdite dirette nelle vendite.
  - **Applicazioni aziendali:** Sistemi interni come ERP, gestione documentale, o comunicazione.
  - **Infrastruttura di rete:** Router, firewall, o VPN potrebbero subire rallentamenti significativi.
- 

## Pianificazione della Remediation

### Passaggi per Rispondere all'Attacco DoS

1. **Identificazione delle fonti dell'attacco**

- Monitoraggio del traffico con strumenti come **Wireshark**, **Splunk**, o firewall aziendali per identificare gli IP sorgenti e il tipo di richieste.
  - Verifica dei log per individuare picchi anomali di traffico o pattern di attacco.
  - 2. **Mitigazione del traffico malevolo**
    - **Blackholing o Sinkholing**: Reindirizzare il traffico sospetto verso un "buco nero" per evitare che raggiunga il server.
    - **Blocchi IP**: Configurare regole temporanee nei firewall per bloccare gli IP di origine identificati.
    - **Rate limiting**: Configurare limiti di richieste per IP sui server tramite strumenti come Nginx o Apache.
    - **Content Delivery Network (CDN)**: Utilizzare soluzioni come Cloudflare o Akamai per distribuire il carico e filtrare il traffico malevolo.
  - 3. **Piano di prevenzione a lungo termine**
    - **Implementare soluzioni di mitigazione DoS**: Sistemi come AWS Shield o Arbor Networks proteggono il traffico in entrata.
    - **Load balancing**: Distribuire il carico su più server per evitare singoli punti di guasto.
    - **Test periodici**: Condurre simulazioni di attacchi DoS per identificare punti deboli nell'infrastruttura.
    - **Training del personale**: Formare il team IT per rispondere rapidamente a situazioni simili.
- 

## Azioni Immediati

- Contatta il tuo provider Internet per supporto nel bloccare traffico malevolo upstream.
- Attiva servizi di protezione DDoS se disponibili.
- Informa gli stakeholder e i dipendenti dell'azienda sull'interruzione temporanea dei servizi e sui piani di risposta in corso.

## Implementazione della Remediation

### Bilanciamento del carico

- **Installazione di un Load Balancer**:
  - Configuro un bilanciatore di carico (es. HAProxy, NGINX, AWS Elastic Load Balancer) per distribuire il traffico su più server.
  - Implementare meccanismi di failover per garantire la continuità del servizio anche in caso di sovraccarico di alcuni nodi.
- **Configurazione di server scalabili**:
  - Uso tecnologie di cloud computing per scalare i server in modo elastico (es. scalabilità orizzontale o verticale).

## Mitigazione tramite terze parti

- **Servizi Anti-DDoS:**
  - Integro servizi di protezione da DoS/DDoS come Cloudflare, Akamai o AWS Shield.
  - Configurare filtri per il traffico sospetto, come limitare le richieste da regioni geografiche insolite o bloccare bot noti.
- **Content Delivery Network (CDN):**
  - Uso un CDN per distribuire il carico di contenuti statici e ridurre la pressione sul server principale.

## Regole Firewall

- **Filtri avanzati:**
    - Configurare il firewall per limitare le connessioni simultanee per IP.
    - Implementare regole basate su rate limiting per impedire traffico eccessivo da fonti singole o insiemi di IP sospetti.
  - **Access Control List (ACL):**
    - Uso ACL nei router e nei switch per filtrare i pacchetti a livello di rete.
- 

## Mitigazione dei Rischi Residuali

### Monitoraggio Continuo

- **Strumenti di monitoraggio:**
  - Implementare sistemi SIEM (es. Splunk, Elastic Stack) per analizzare il traffico e generare alert su comportamenti anomali.
  - Monitoro metriche chiave come latenza, utilizzo della banda e numero di connessioni attive.
- **Automazione della risposta:**
  - Integro script o soluzioni automatizzate per attivare regole di mitigazione al rilevamento di schemi di attacco.

### Collaborazione con il team di sicurezza

- **Revisione delle politiche di sicurezza:**
  - Lavoro con il team di sicurezza per rafforzare il piano di risposta agli incidenti.
- **Partnership con ISP:**
  - Collaboro con il fornitore di servizi Internet per filtrare il traffico a monte.

### Test Periodici di Resilienza

- **Simulazioni di attacco:**

- Organizzo test di penetrazione mirati a verificare la resilienza del sistema contro DoS/DDoS.
- **Aggiornamento continuo:**
  - Valuto regolarmente le nuove tecnologie di mitigazione e aggiornamento di sistemi in base alle migliori pratiche.

Diego Petronaci