
GESTIONE DELLE MINACCE DI PHISHING E ATTACCHI DOS

Mattia Montis





Anteprima

Questa presentazione illustra le misure per identificare, analizzare, e mitigare due delle più comuni minacce alla sicurezza informatica aziendale: Phishing e DoS (Denial of Service). Attraverso strategie pratiche e tecniche di remediation, si propone un piano strutturato per rafforzare la resilienza dell'organizzazione contro tali minacce.

INDICE



1

INTRODUZIONE ALLE MINACCE

- 1.1 PHISHING
- 1.2 ATTACCO DOS

2

ANALISI DEL RISCHIO

- 2.1 IMPATTI POTENZIALI
- 2.2 SERVIZI CRITICI COMPROMESSI

3

TECNICHE DI ATTACCO

- 3.1 TECNICHE DI PHISHING
- 3.2 TECNICHE DI DOS

4

PIANO DI REMEDIATION

- 4.1 MISURE CONTRO IL PHISHING
- 4.2 MISURE CONTRO L'ATTACCO DOS

5

MITIGAZIONE DEI RISCHI RESIDUALI

- 4.1 PER IL PHISHING
- 4.2 PER IL DOS

6

DOCUMENTAZIONE FINALE



INTRODUZIONE ALLE MINACCE

1

Phishing

- **Definizione:** Il phishing è un attacco che utilizza email fraudolente per ingannare i destinatari al fine di rubare credenziali o dati sensibili.
- **Meccanismo:**
 - I truffatori inviano email che imitano organizzazioni fidate.
 - Gli utenti cliccano link o aprono allegati dannosi.
- **Obiettivi:**
 - Compromissione di credenziali aziendali.
 - Furto di dati sensibili.

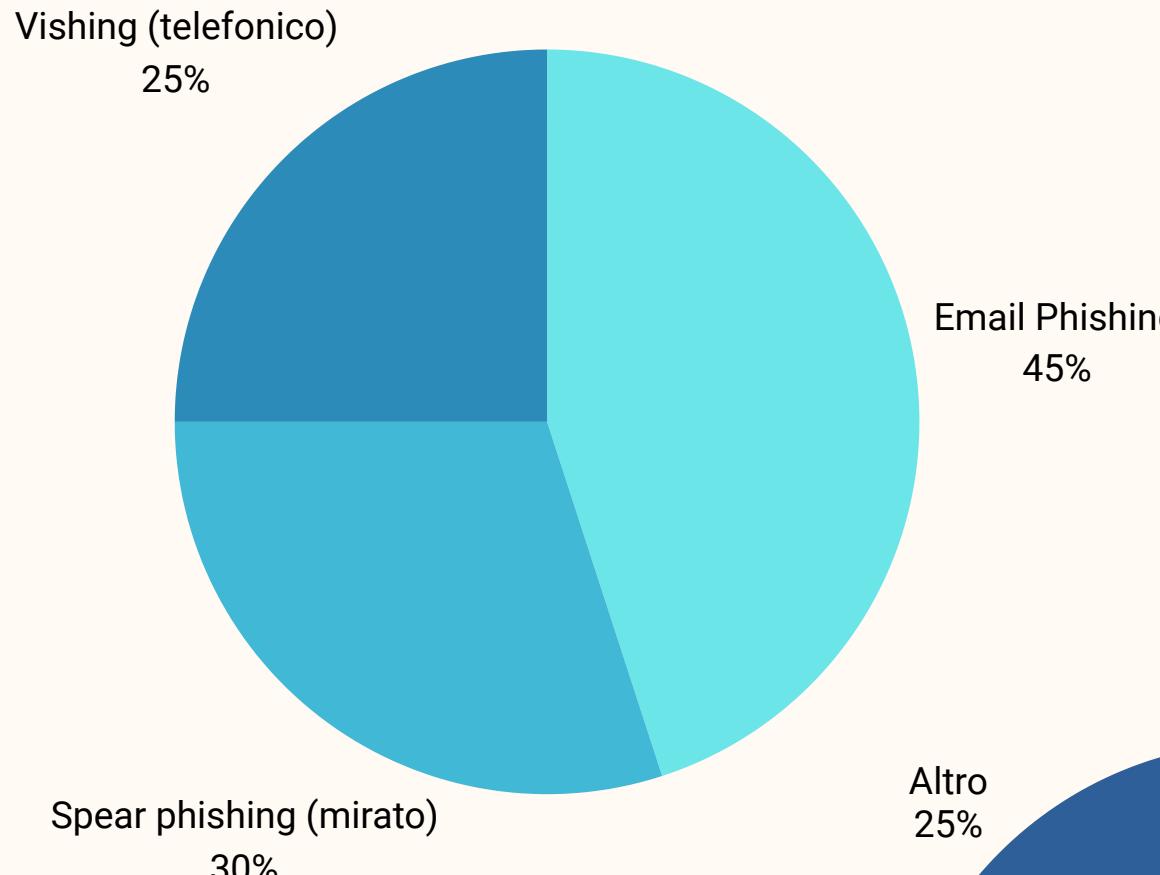
Attacco DoS

- **Definizione:** Un attacco DoS mira a rendere inaccessibili i servizi aziendali sovraccaricando i server con richieste eccessive.
- **Meccanismo:**
 - Richieste inviate da fonti singole o multiple.
 - I server diventano incapaci di rispondere ai legittimi utenti.
- **Obiettivi:**
 - Interruzione delle operazioni aziendali.
 - Perdita di clienti e danni reputazionali

2 ANALISI DEL RISCHIO

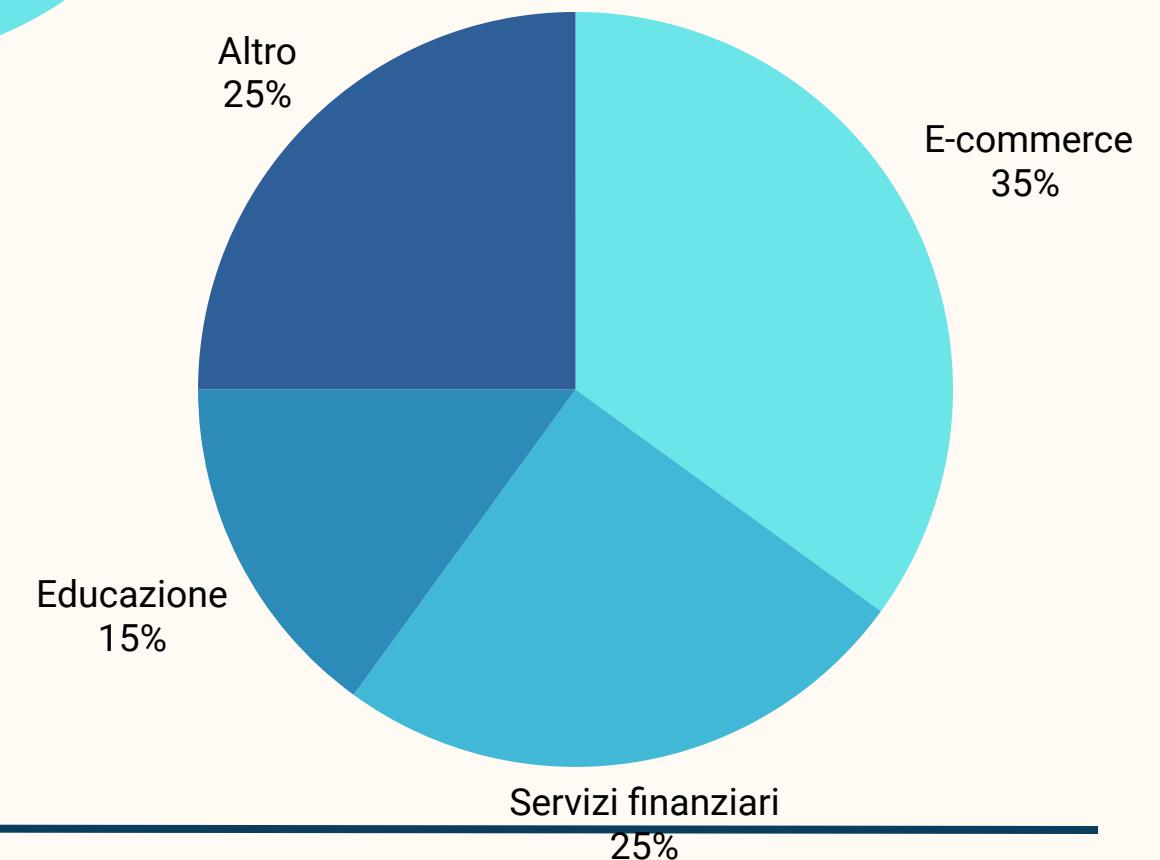
PHISHING

- IMPATTO POTENZIALE:
 - ESPOSIZIONE DI CREDENZIALI E DATI SENSIBILI.
 - COMPROMISSIONE DI SISTEMI CRITICI AZIENDALI.
- SERVIZI CRITICI COMPROMESSI:
 - ACCOUNT EMAIL AZIENDALI.
 - APPLICAZIONI CLOUD E DATABASE.



DOS

- IMPATTO POTENZIALE:
 - INTERRUZIONE DI SERVIZI WEB E APPLICAZIONI.
 - DANNI ECONOMICI DOVUTI A PERDITA DI ACCESSO AI SISTEMI.
- SERVIZI CRITICI COMPROMESSI:
 - SERVER WEB E APPLICAZIONI AZIENDALI.
 - SISTEMI DI PAGAMENTO ONLINE O PIATTAFORME E-COMMERCE.



3 TECNICHE DI ATTACCO

Tecniche di Phishing

Il phishing può essere realizzato attraverso diverse tecniche, tra cui:

- Phishing Tradizionale:
 - Email fraudolente inviate a un ampio numero di destinatari, spesso con link che conducono a siti web falsi dove l'utente è invitato a inserire informazioni sensibili.
- Spear Phishing:
 - Attacco mirato, in cui gli aggressori personalizzano l'email, rendendola più credibile per il destinatario. Spesso queste email sono indirizzate a specifici dipendenti o dirigenti aziendali.
- Vishing (Phishing Telefonico):
 - Gli hacker si fingono rappresentanti di una banca o di una compagnia telefonica e cercano di ottenere informazioni personali via telefono.
- Smishing (Phishing via SMS):
 - Utilizzo di messaggi di testo fraudolenti che inducono l'utente a cliccare su link dannosi o a rivelare informazioni riservate.

Tecniche di Attacco 3

Tecniche di DoS

Gli attacchi DoS possono essere realizzati utilizzando diverse tecniche, tra cui:

- **Flooding:**
 - L'invio di un numero eccessivo di richieste da una sola macchina (**DoS**) o da più macchine coordinate (**DDoS**). I server vengono sovraccaricati, causando un'interruzione del servizio.
- **SYN Flood:**
 - Un tipo di attacco che sfrutta il processo di handshake TCP, inviando richieste SYN in modo massivo senza completare la connessione. Questo impedisce ai server di gestire altre connessioni legittime.
- **Amplification Attacks:**
 - Gli attaccanti inviano richieste a server vulnerabili (es. DNS), i quali rispondono con una quantità molto maggiore di dati verso la vittima, amplificando l'attacco.
- **Application Layer Attacks:**
 - Attacchi più sofisticati che mirano a sovraccaricare le risorse applicative (ad esempio, iniettando richieste molto specifiche a un server web).

PIANO DI REMEDIATION



PHISHING

Identificazione e Blocco:

- Configurare filtri anti-phishing nei sistemi email (es. Microsoft Defender, Google Workspace Security).
- Monitorare i log dei server per individuare attività sospette.

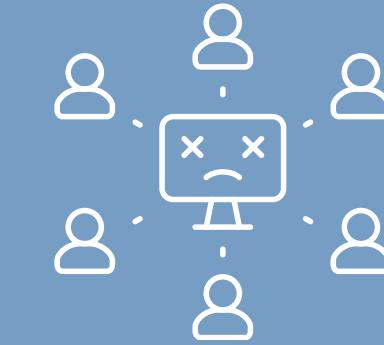
Comunicazione Interna:

- Informare i dipendenti sugli indicatori di email fraudolente.
- Predisporre un canale di segnalazione interna per email sospette.

Verifica dei Sistemi:

- Effettuare scansioni antivirus su tutti i dispositivi aziendali.
- Controllare i log delle applicazioni per individuare accessi non autorizzati

DOS



Identificazione delle Fonti:

- Analizzare il traffico di rete con strumenti come Wireshark o Splunk.
- Correlare eventi utilizzando i log dei firewall.

Mitigazione del Traffico:

- Configurare regole firewall per bloccare IP sospetti.
- Implementare bilanciatori di carico per distribuire il traffico legittimo.
- Utilizzare servizi di mitigazione DoS (es. Cloudflare, AWS Shield).

Cooperazione con il Provider:

- Contattare l'ISP per filtrare il traffico in entrata a monte.

Phishing

- Test di Phishing Simulati:
 - Creare campagne simulate per testare la reattività dei dipendenti.
- Autenticazione a Due Fattori (2FA):
 - Obbligare l'uso di 2FA su tutti i sistemi aziendali.
- Aggiornamenti e Patch:
 - Mantenere aggiornati sistemi operativi e software.

DoS

- Monitoraggio Continuo:
 - Configurare IDS/IPS per analizzare continuamente il traffico.
- Simulazioni di Attacchi:
 - Condurre test regolari di resilienza contro attacchi DoS.
- Policy di Sicurezza Aggiornate:
 - Rafforzare le regole di firewall e implementare piani di continuità operativa.

MITIGAZIONE DEI RISCHI RESIDUALI

DOCUMENTAZIONE FINALE

PHISHING

- DESCRIZIONE: MINACCIA CHE SFRUTTA EMAIL FRAUDOLENTE PER RUBARE DATI.
- REMEDIATION: CONFIGURARE FILTRI EMAIL, FORMARE I DIPENDENTI, IMPLEMENTARE 2FA.
- RISCHI RESIDUALI: SIMULAZIONI E MONITORAGGIO CONTINUO.

DOS

- DESCRIZIONE: SOVRACCARICO DI RICHIESTE CHE RENDE INACCESSIBILI I SERVER.
- REMEDIATION: BILANCIATORI DI CARICO, SERVIZI DI MITIGAZIONE, REGOLE FIREWALL.
- RISCHI RESIDUALI: MONITORAGGIO, TEST DI RESILIENZA, COLLABORAZIONE CON ISP.

CONCLUSIONI

UN APPROCCIO STRUTTURATO, CHE COMBINA TECNOLOGIA E FORMAZIONE DEL PERSONALE, È ESSENZIALE PER PROTEGGERE L'AZIENDA DA MINACCE COME PHISHING E DOS. IMPLEMENTARE SOLUZIONI PROATTIVE E MANTENERE AGGIORNATE LE DIFESE GARANTIRÀ UNA MAGGIORE RESILIENZA CONTRO ATTACCHI FUTURI.



GRAZIE

Mattia Montis

