Relazione Attacco Phishing e Attacco DoS

(Mitigation & Remediation)

Report e relazione di un ATTACCO PHISHING

Identificare l'ATTACCO PHISHING

il **PHISHING** è un attacco informatico con cui l'attaccante tramite l'invio di e-mail ingannevoli che sembrano provenire da fonti affidabili e quindi possano sembrare veritiere, invoglia la/le vittima/e alla divulgazione delle proprie informazioni sensibili o a cliccare su eventuali link, presenti nella e-mail (**malevola**) così da dare un input e far partire il download e di conseguenza l'avvio dell'attacco.

Analizzare il rischio (ATTACCO PHISHING)

l'attacco informatico **PHISHING** può portare alla compromissione dei dati personali, come, credenziali per la fase di Login, ad account personali, del privato cittadino, account aziendali, del dipendente accesso, rivelare informazioni sensibili e quindi dare accesso all'attacco e portare a una compromissione più ampia.

Fase di MITIGAZIONE sull'ATTACCO PHISHING

simulazioni di attacchi **PHISHING** per la valutazione e per acquisire consapevolezza sulle misure da intraprendere per mitigare l'attacco.

Misure di sicurezza per prevenire un attacco PHISHING

2FA – 2 FACTOR AUTHENTICATION:

implementazione di due fasi per effettuare l'accesso (Login), per evitare o comunque diminuire le probabilità di furto delle credenziali:

ELENCO DELLE RISORSE POTENZIALMENTE COMPROMESSE

credenziali privato cittadino e/o dipendente aziendale

dati personali del cliente, dati aziendali del dipendente, dati documenti finanziari

mantenere sempre aggiornati i sistemi operativi privati/aziendali

Fase di REMEDIATION sull'ATTACCO PHISHING

ANTI PHISHING:

configurazione di filtri avanzati sul servizio di posta elettronica (**outlook, gmail, libero, tiscali ecc..**) ed implementazione di soluzioni di sicurezza.

ATTUARE LA FASE DI REMEDIATION sull'ATTACCO PHISHING

implementazione **ANTI PHISHING**, implementazione dei sistemi di rilevamento per identificare eventuali e-mail ingannevoli con l'utilizzo di identificazione dei sistemi di posta elettronica.

utilizzare tecnologie come SPF (**Sender Policy Framework**), DKIM (**DomainKeys Identified Mail**) ed infine DMARC (**Domain-based Message Authentication, Reporting, and Conformance**) per l'autenticazione di email legittime e per intervenire nel bloccare e-mail, ingannevoli.

Report e relazione di un ATTACCO DOS (Denial of Service)

Identificare l'ATTACCO DoS (Denial of Service)

l'attacco DoS (**Denial of Service**) ha l'obiettivi di lanciare un numero non definito di pacchetti dati, in grado di mettere fuori uso, mettere fuori servizio un sito e/o servizi aziendali, sovraccaricando i Server.

Analizzare il rischio (ATTACCO DoS)

Un attacco DoS è in grado di mettere fuori uso l'accesso ai siti web ed ai server web dell'azienda che si trova sotto attacco e alle applicazioni critiche dell'azienda, causando interruzioni dei servizi, perdite di ricavi e danni reputazionali.

Fase di MITIGAZIONE sull'ATTACCO DoS

implementazione di sistemi di filtraggio e di bilanciamento del carico (**pacchetti dati**) per distribuire il traffico.

configurazione **Firewall** per bloccare il flusso del traffico malevolo, provenienti da indirizzi IP

monitoraggio continuo del traffico di rete per identificare nuovi attacchi e rispondere rapidamente.

collaborazione con il Security Team per il miglioramento delle difese dell'OS da attacchi DoS

effettuare periodicamente test (**DoS simulati in ambiente sicuro**) di carico per valutare l'efficienza delle misure di mitigazione e la capacità dell'infrastruttura sulla gestione carichi elevati.

ELENCO DELLE RISORSE POTENZIALMENTE COMPROMESSE

Server web aziendali.

Sistemi di e-commerce.

CRM - Customer Relationship Management e ERP - Enterprise Resource Planning

Fase di REMEDIATION sull'ATTACCO DoS

identificare la fonte o le fonti, di provenienza da cui è partito l'**ATTACCO DOS**

utilizzare Tools per il monitoraggio della rete ed identificare le fonti del flusso di traffico di rete (**pacchetti dati**), analisi dei log per il tracciamento e successivo blocco degli indirizzi IP sospetti.

ATTUARE LA FASE DI REMEDIATION sull'ATTACCO DoS

implementazione delle varie soluzioni di bilanciamento del carico del flusso dei pacchetti dati per una distribuzione su più Server e ridurre la possibilità di sovraccarico.

utilizzo di software come **Cloudflare**, in grado di mitigare attacchi DoS, e filtrare il traffico malevolo e prevenire che i Server aziendali, vengano attaccati.

utilizzo e configurazione di **Firewall** e **IDS** per bloccare il traffico malevolo ed identificare eventuali intrusioni nell'OS e Server aziendali.

ANALISI FINALE SULL'ATTACCO DOS

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-07-19 06:51:17.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
2	2024-07-19 06:51:18.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
3	2024-07-19 06:51:19.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
4	2024-07-19 06:51:20.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
5	2024-07-19 06:51:21.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
6	2024-07-19 06:51:22.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
7	2024-07-19 06:51:23.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
8	2024-07-19 06:51:24.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
9	2024-07-19 06:51:25.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
10	2024-07-19 06:51:26.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet

Macchina attaccante: **192.168.1.1 e 192.168.1.2**

Server aziendale: 10.0.0.1

Dall'immagine sopra riportata si evidenzia un attacco DoS, rilevato e catturato con il tool Wireshark, possiamo vedere come ci sia una serie di pacchetti dati (**anomali**) con protocollo TCP (**Transmission Control Protocol**) di 60 byte con provenienza dall'indirizzo IP **192.168.1.1** e **192.168.1.2** verso la vittima, in questo caso un Server, identificato con l'indirizzo IP **10.0.0.1**

In conclusione, il flusso di pacchetti, con protocollo TCP, sono in costante invio verso il Server 10.0.0.1 e di conseguenza, ci sarà un sovraccarico del Server aziendale e tutti i servizi sarano messi fuori uso.

Come prevenire le minacce informatiche

- ***FORMAZIONE PERIODICA CON CORSI DI FORMAZIONE AI DIPENDENTI***

- ***AGGIORNAMENTI PERIODICI E PATCHING DI SICUREZZA***

- ***UTILIZZO DELLE POLICY DI SICUREZZA***

21/10/2021 **Christian Vagnoni**