EPICODE

S9/L5

Security Operation Center: Process and procedure

Prepared for

Noemi de Martino

Table of Contents

Traccia

Con riferimento alla figura, rispondere ai seguenti quesiti:

1. Azioni preventive :
Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?
Modificate la figura in modo da evidenziare le implementazioni.

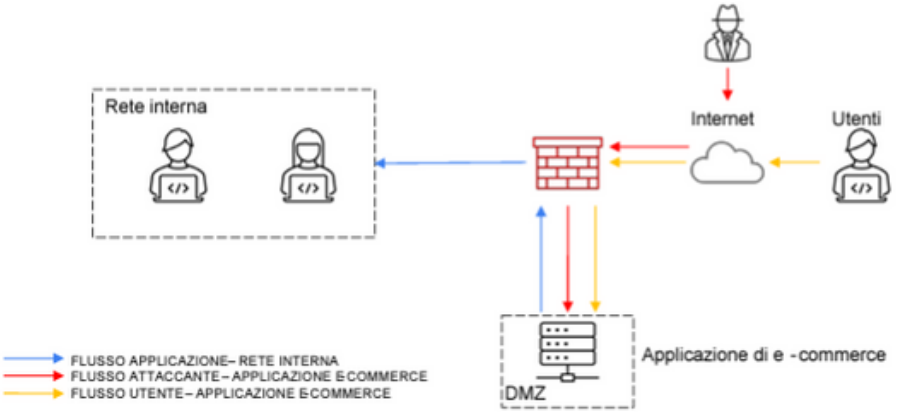
2. Impatti sul business :
L'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti . Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

3. Response :
L'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura con la soluzione proposta .

4. Soluzione completa :
Unire i disegni dell'azione preventiva e della response (unire quesito 1 e 3)

5. Modifica "più aggressiva" dell'infrastruttura:
Integrare eventuali altri elementi di sicurezza; Budget 5000-10000 euro (Eventualmente fare più proposte di spesa).

Bonus: Analizzare le seguenti segnalazioni caricate su anyrun e fare un piccolo report di ciò che si scopre relativo all'eventuale attacco spiegando ad utenti e manager la tipologia di attacco e come evitare questi attacchi in futuro.



Architettura di rete: L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

Quesito 1

Differenze XSS e SQLi

XSS

- **Tipo di vulnerabilità:**

Attacco basato **sul client** che inietta codice JavaScript maligno nelle pagine web visualizzate dagli utenti.

- **Obiettivo:**

Mirato a compromettere la sessione dell'utente, rubare cookie, manipolare il contenuto della pagina o eseguire azioni a nome dell'utente.

- **Esecuzione:**

Il codice maligno viene eseguito nel contesto del browser dell'utente. Può essere riflesso o memorizzato.

- **Tipo di Input:**

Codice JavaScript o HTML.

- **Risultati dell'attacco:**

I risultati dell'attacco sono visibili direttamente all'attaccante attraverso l'interfaccia utente del browser.

- **Comandi:**

I comandi vengono eseguiti nel browser dell'utente.

- **Impatto:**

Può colpire molti utenti, a seconda di dove è iniettato il codice maligno.

SQLi

- **Tipo di vulnerabilità:**

Attacco basato **sul server** che sfrutta le vulnerabilità del database per eseguire query SQL malevole senza ricevere un output diretto dall'applicazione.

- **Obiettivo:**

Mirato a ottenere accesso non autorizzato ai dati, manipolare il database, eseguire comandi sul server o bypassare meccanismi di autenticazione.

- **Esecuzione:**

L'attaccante invia input malevoli all'applicazione, sfruttando le risposte indirette per inferire informazioni sul database.

- **Tipo di Input:**

Codice SQL.

- **Risultati dell'attacco:**

Nessun output diretto. L'attaccante deve dedurre le informazioni basandosi su risposte sì/no o tempi di risposta.

- **Comandi:**

I comandi vengono eseguiti nel contesto del database server.

- **Impatto:**

Colpisce principalmente il database e le informazioni che contiene, con potenziali conseguenze per molti utenti.

Quesito 1

Azioni preventive

- **Parametrizzazione delle query**

Utilizzare query parametrizzate per separare il codice SQL dai dati.

- **Sanitizzazione degli input**

Convalidare e filtrare tutti gli input dell'utente, ciò impedisce l'inclusione di script dannosi o comandi SQL nelle richieste.

- **Content Security Policy (CSP)**

Implementare una CSP che limita le fonti di script eseguibili nel browser.

- **HttpOnly e Secure flags sui cookie**

Impostare i flag HttpOnly e Secure sui cookie per ridurre il rischio che vengano rubati tramite XSS.

- **Limitare i privilegi del database**

Configurare i permessi del database in modo che l'applicazione abbia accesso solo ai dati e alle operazioni necessarie.

- **Uso di Web Application Firewall (WAF)**

Un WAF può rilevare e bloccare tentativi di SQL Injection. Questo dispositivo monitora il traffico di rete e limita le richieste alle applicazioni, consentendo l'accesso solo agli utenti scelti. Esistono due tipologie di WAF, quelli basati sulla rete che vengono installati come hardware o software all'interno della rete, e quelli basati sul cloud che sono praticamente servizi in abbondamento da un provider di sicurezza.

- **Autenticazione Multifattoriale (MFA)**

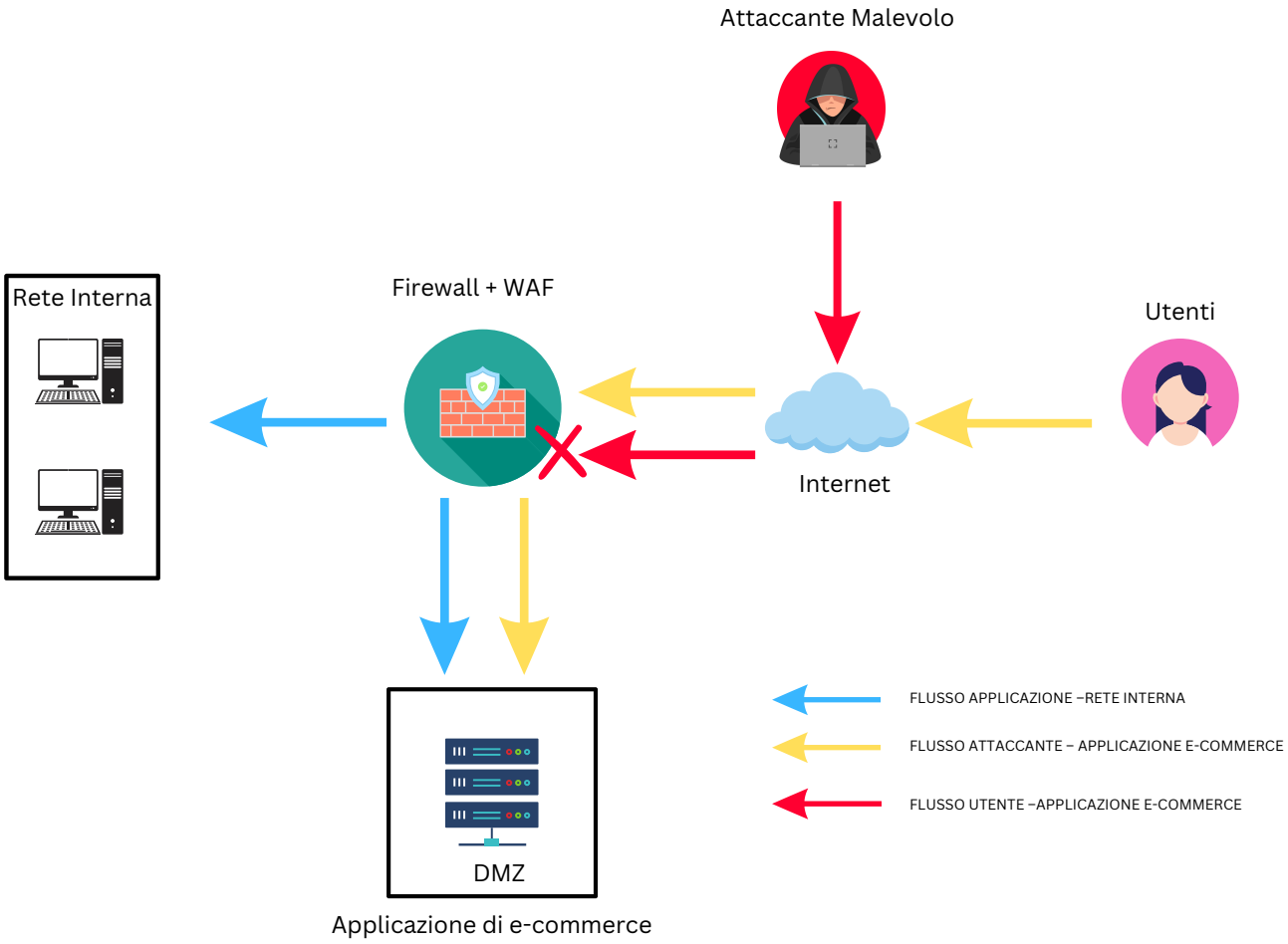
Migliorare i controlli di accesso tramite un autenticazione multifattore.

- **Aggiornamenti costanti:**

Mantenere costantemente aggiornato il software.

Quesito 1

Disegno di rete



Quesito 2

Impatto sul business

Per calcolare l'impatto economico di un attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti, possiamo utilizzare la seguente formula:

Impatto economico = Perdita media al minuto × Durata dell'interruzione

→ Perdita media al minuto	**1.200 €**
→ Durata interruzione	**10 minuti**
→ Impatto economico	**12.000€**

Quesito 2

Azioni preventive

- **Utilizzo di un servizio di protezione DDoS:**

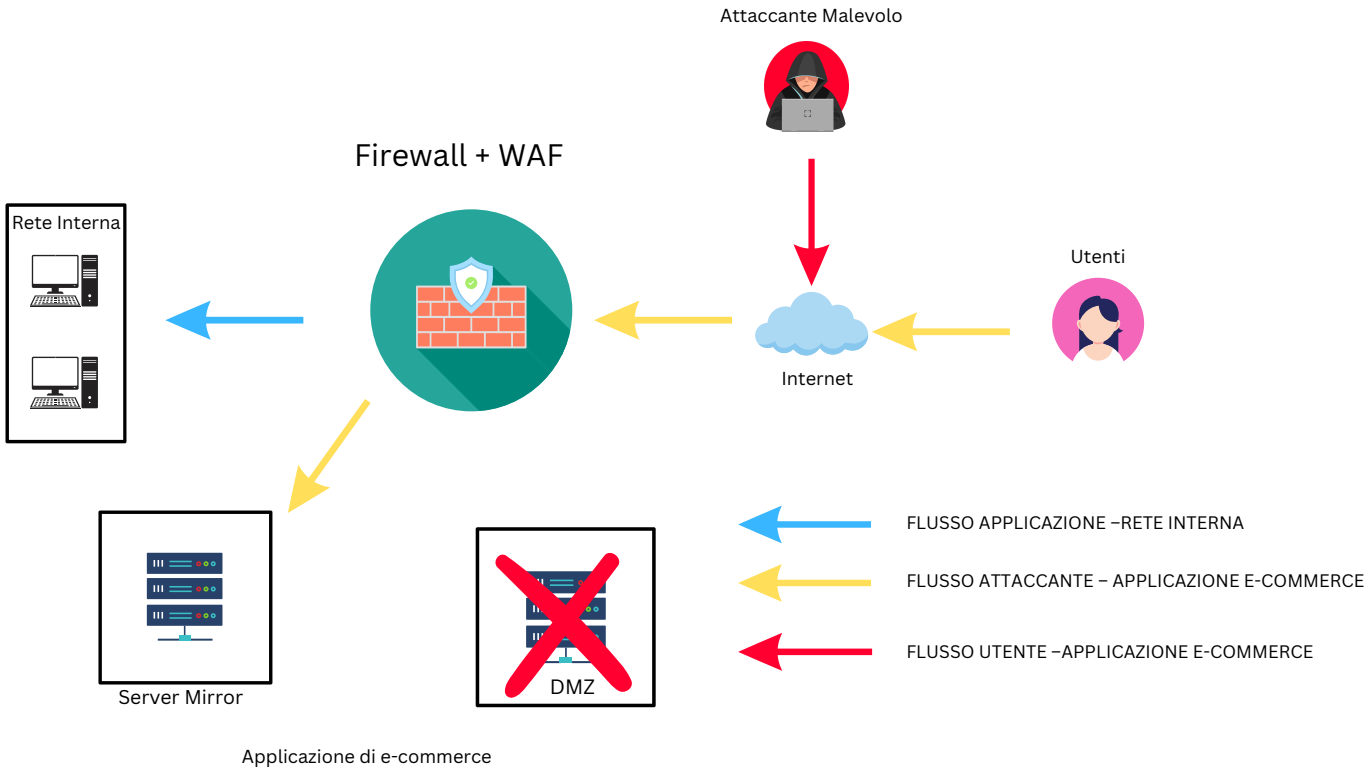
Implementare servizi che possono rilevare attacchi DDoS in tempo reale come **Cloudflare**, **Akamai** che offrono protezione DDoS integrata oppure servizi specifici come **Google Cloud Armor.**
Si potrebbe anche utilizzare una **CND(Content Delivery Network)** per distribuire il contenuto su server globali, riducendo il carico sui principali server e quindi migliorando la resistenza in un possibile attacco.

- **Firewall e filtri**

Implementare un **WAF** per filtrare il traffico malevolo prima che raggiunga l'applicazione e configurare regole di firewall personalizzate per bloccare **indirizzi IP** o range di **IP sospetti**.
Inoltre per garantire la **business continuity**, si può anche far uso di un **server mirror** che sostiuisca il server principale in caso di attacco.

- **Configurazione di Rate limiting**

Implementare meccanismi di rate limiting per limitare il numero di richieste che un singolo IP può fare in un dato periodo di tempo, il processo si basa sul monitoraggio degli indirizzi IP da cui provengono le richieste e di quanto tempo passa fra una richiesta e l'altra.

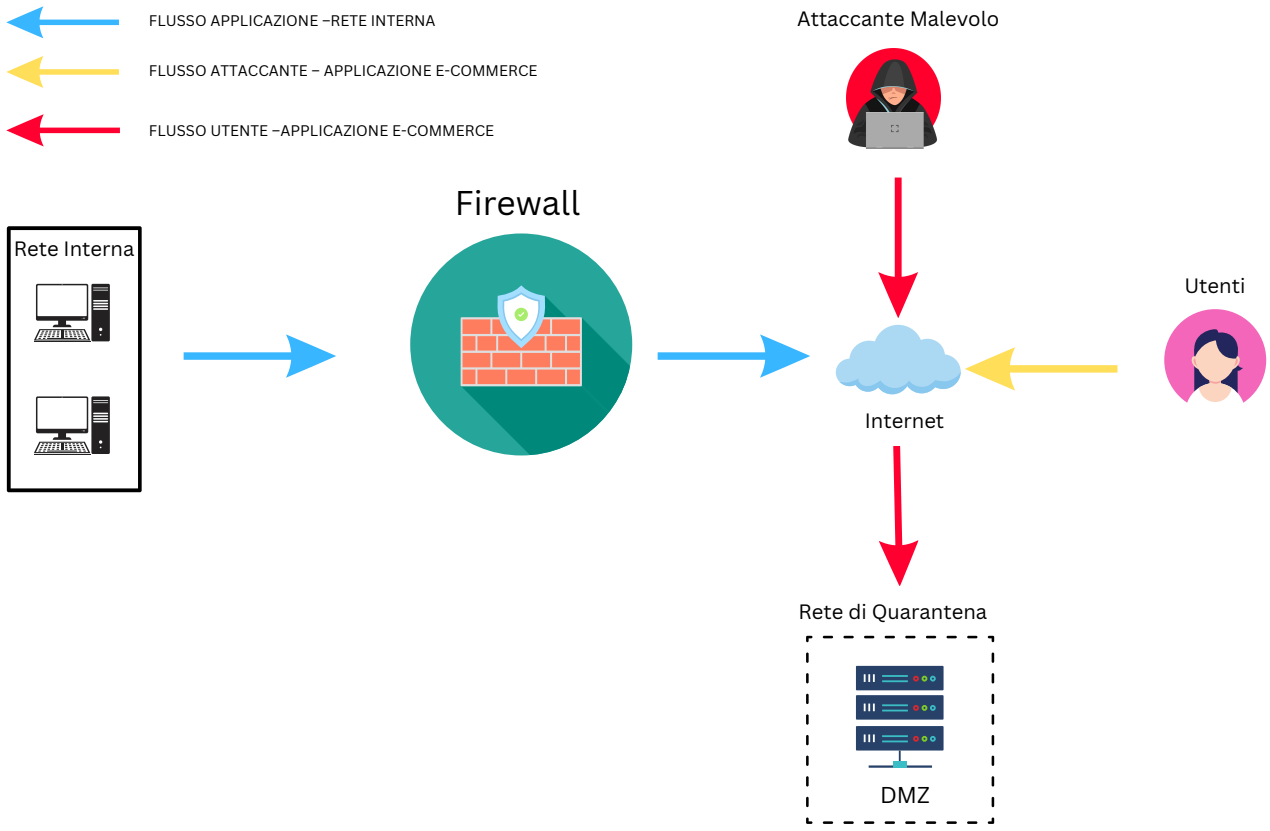


Quesito 3

Response

Se l'applicazione Web viene infettata da un malware, e non ci interessa rimuovere l'accesso da parte dell'attaccante alla macchina infettata possiamo creare una **Rete di Quarantena.**

La **Rete di Quarantena,** isola il server infetto in una VLAN dedicata ed impedisce al malware di propagarsi ad altri dispositivi sulla rete, ci permette inoltre di monitorare il server infetto e ci facilità l'analisi del malware e delle sue attivita.
Inoltre isolare il server ci aiuta a gestire più facilmente l'emergenza senza doverci preoccupare dell'impatto sugli altri server, e sicuramente gli interventi di sanificazione potranno avvenire senza impattare troppo il normale funzionamento della rete aziendale.



Quesito 4

Soluzione completa

Le soluzioni proposte per prevenire l'attacco sono:

- **Uso di Web Application Firewall (WAF)**

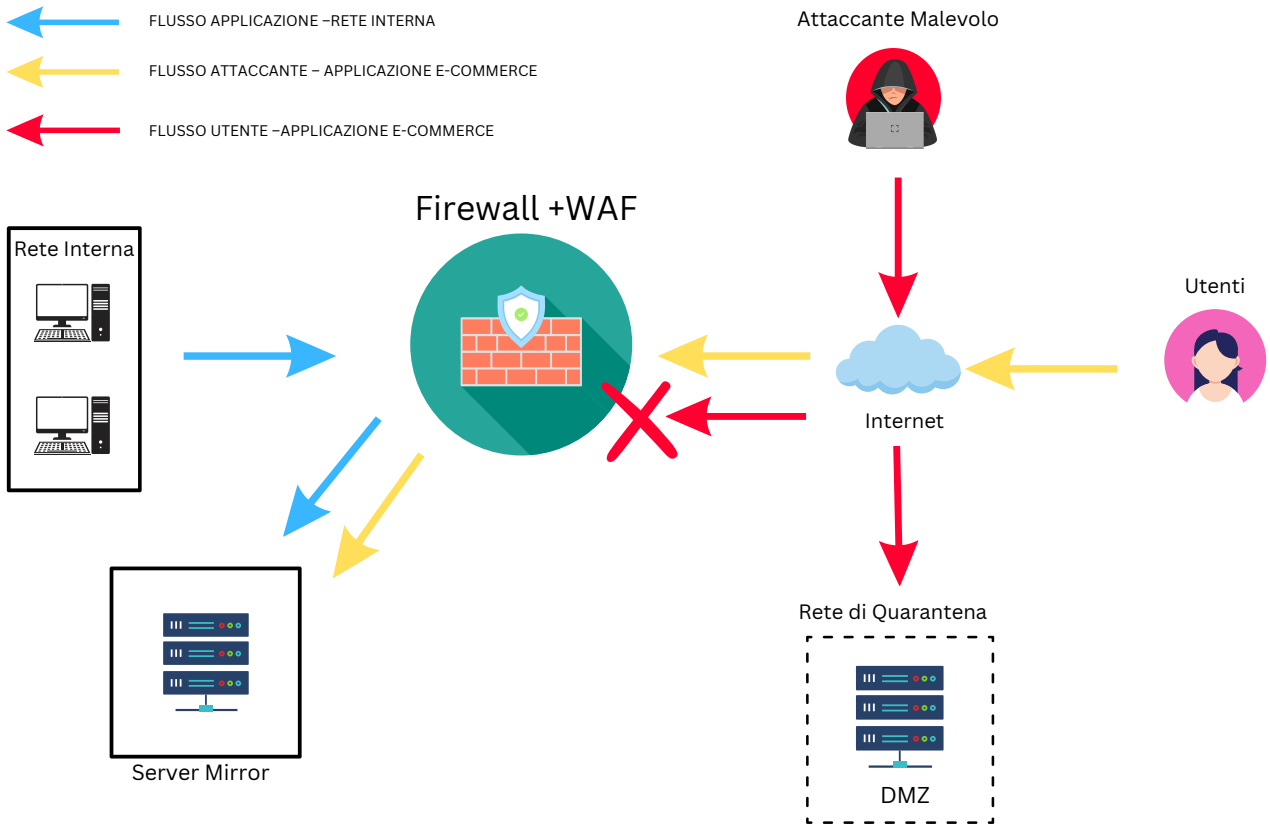
mplementare un WAF per filtrare il traffico malevolo prima che raggiunga l'applicazione e configurare regole di firewall personalizzate per bloccare indirizzi IP o range di IP sospetti.

- **Rete di Quarantena:**

Una rete di quarantena per isolare i server infetti è una pratica di sicurezza efficace che protegge la rete aziendale dalla diffusione del malware, migliora il monitoraggio e facilita la gestione delle infezioni, minimizzando l'impatto sul business.

- **Server Mirror:**

IPer garantire la business continuity, si può anche far uso di un server mirror che sostiuisca il server principale in caso di attacco.



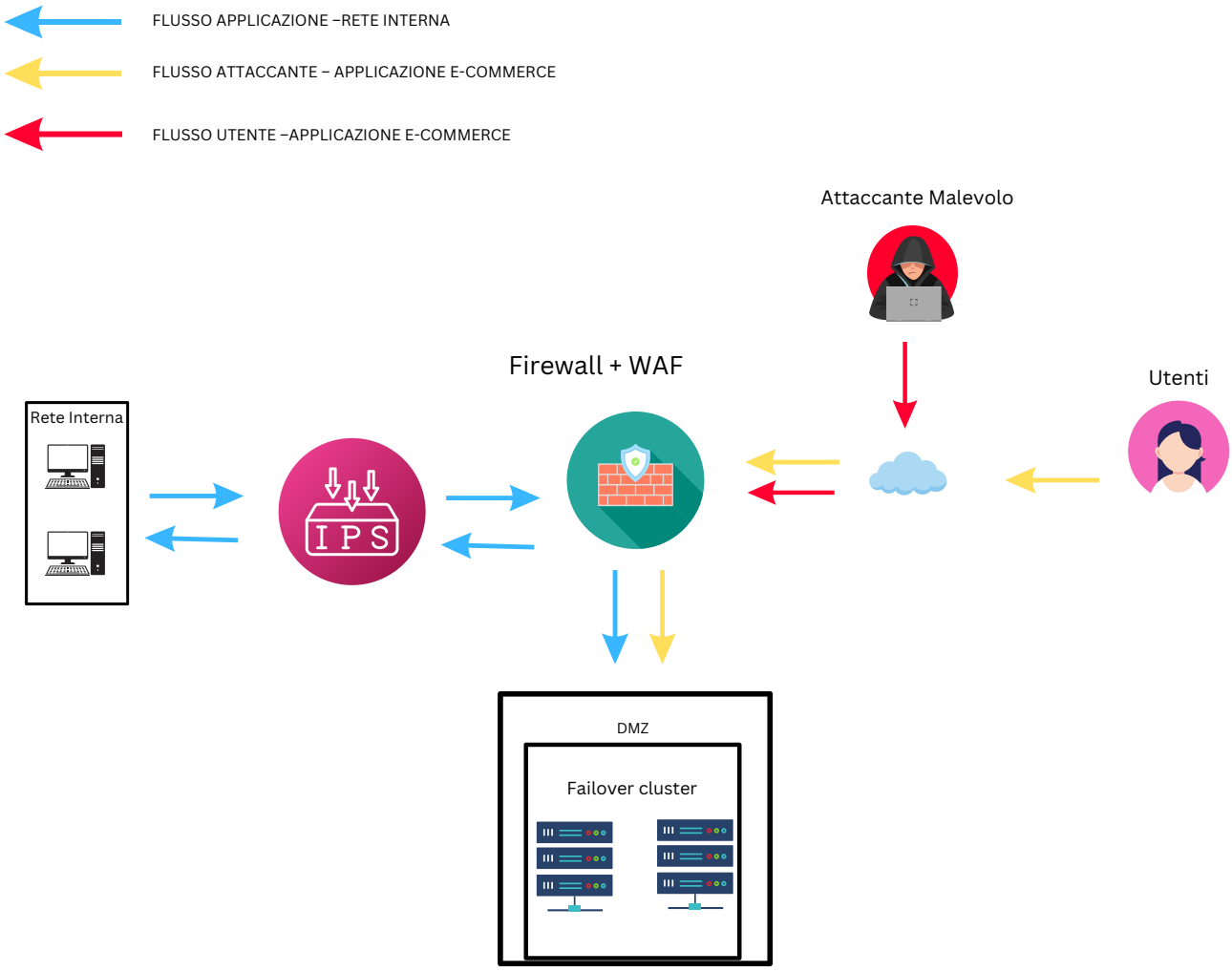
Quesito 5

Infrastruttura modificata Proposta 1

La prima proposta di rete prevede:

- **Rete Interna:** Collega i dispositivi interni all'IPS.
- **IPS (Intrusion Prevention System):** Monitora e protegge la rete interna da attacchi.
- **Firewall/WAF (Web Application Firewall):** Ulteriore livello di sicurezza che protegge le applicazioni web.
- **DMZ (Demilitarized Zone):** Contiene un cluster failover, un gruppo di server configurati per lavorare insieme in modo da garantire la continuità operativa di un servizio o di un'applicazione. Se uno dei server nel cluster diventa inoperativo, un altro server nel cluster prende automaticamente il suo posto, minimizzando l'interruzione del servizio.

.

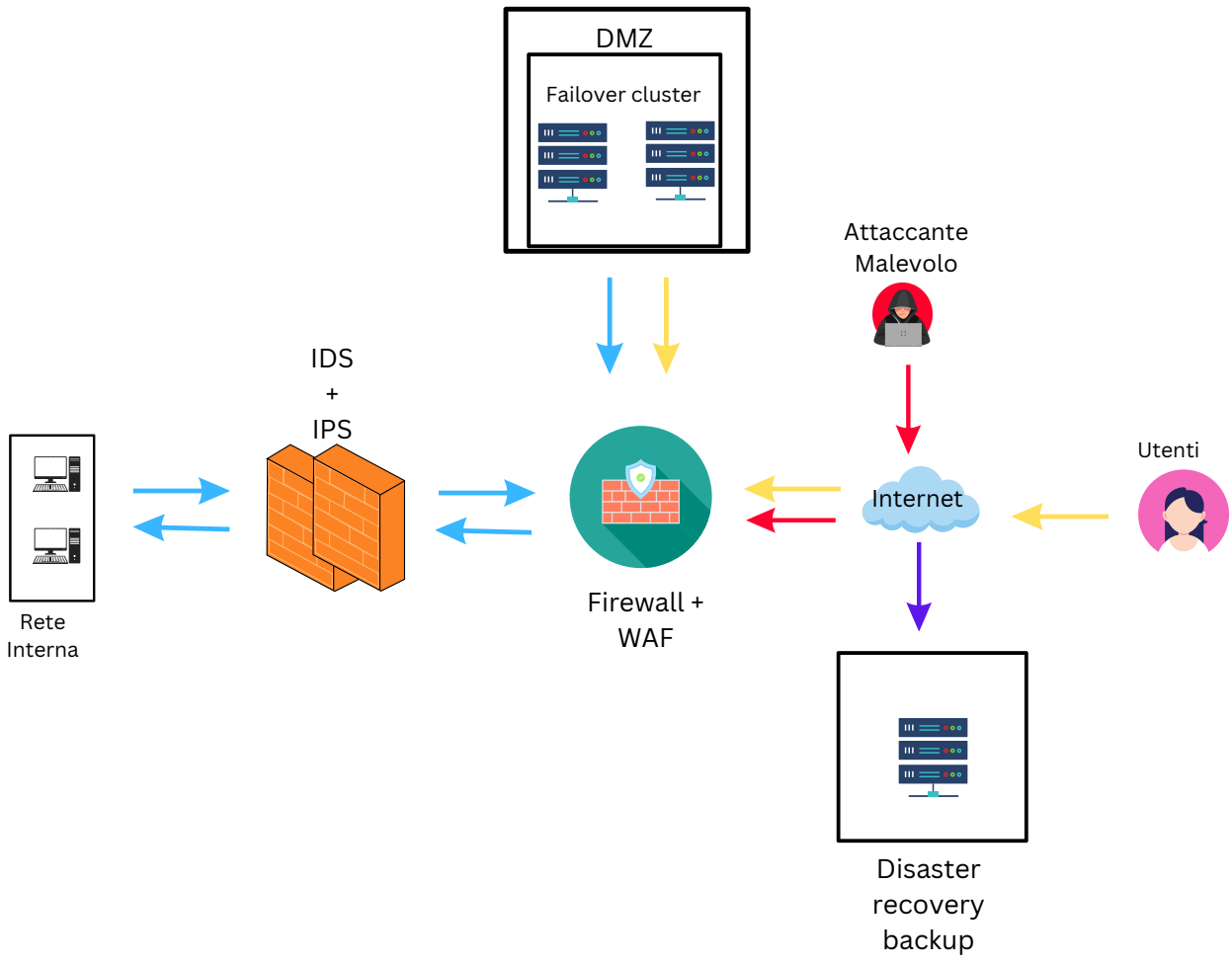


Quesito 5

Infrastruttura modificata Proposta 2

La seconda proposta di rete prevede:

- **Rete Interna:** Collega i dispositivi interni all'IPS.
- **IPS (Intrusion Prevention System):** Monitora il traffico di rete in tempo reale e blocca automaticamente le attività sospette o malevole.
- **IDS (Intrusion Detection System):** Monitora il traffico di rete per rilevare attività sospette o malevole.
- **Firewall/WAF (Web Application Firewall):** Ulteriore livello di sicurezza che protegge le applicazioni web.
- **Disaster recovery backup:** un sistema di backup progettato per proteggere e recuperare i dati e le applicazioni critiche in caso di disastro, come guasti hardware, attacchi informatici o disastri naturali. I vantaggi sono sicuramente la **possibilità di continuare a svolgere operazioni aziendali** senza interruzioni troppo importanti, **la protezione dei dati** e quindi di conseguenza anche il **ripristino veloce** dei sistemi e dei dati persi.



Bonus

ANY.RUN

ANYRUN è una piattaforma di analisi malware interattiva e basata sul cloud, progettata per eseguire e analizzare file sospetti in un ambiene sicuro e controllato.

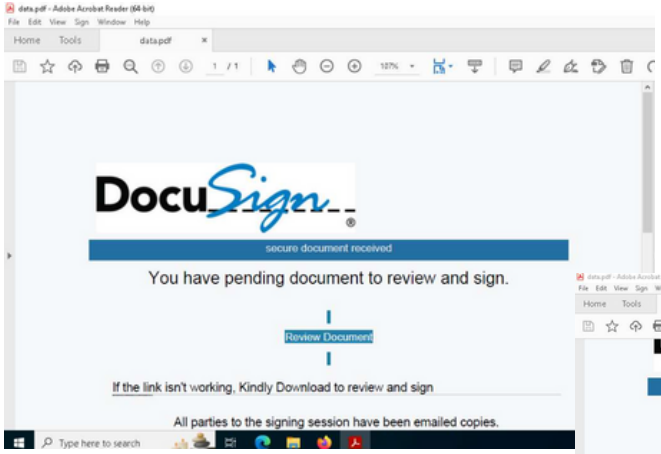
Le caratteristiche principali di ANYRUN sono:

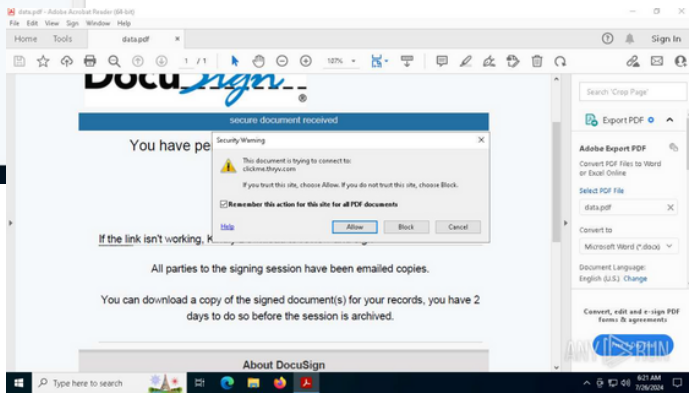
- **Interazione in tempo reale**: Gli utenti possono interagire direttamente con la sandbox durante l'analisi.
- **Monitoraggio delle attività**: La piattaforma traccia molteplici aspetti dell'analisi, tra cui la creazione di nuovi processi, file sospetti, attività di rete, modifiche al registro
- **Database di threat intelligence**
- **Mappe interattive dei processi:** Gli attacchi vengono visualizzati in una struttura ad albero interattiva

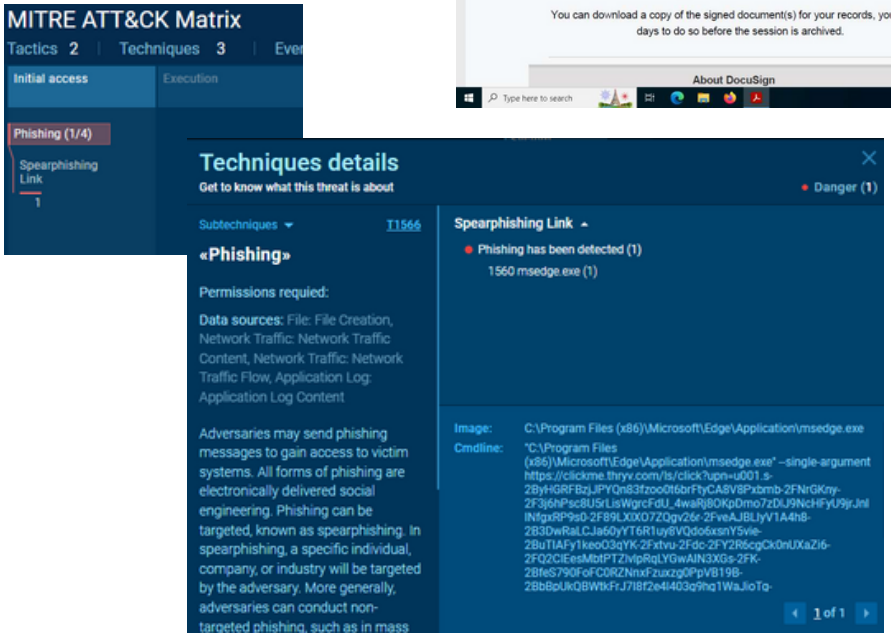
---

Bonus

Attacco 1



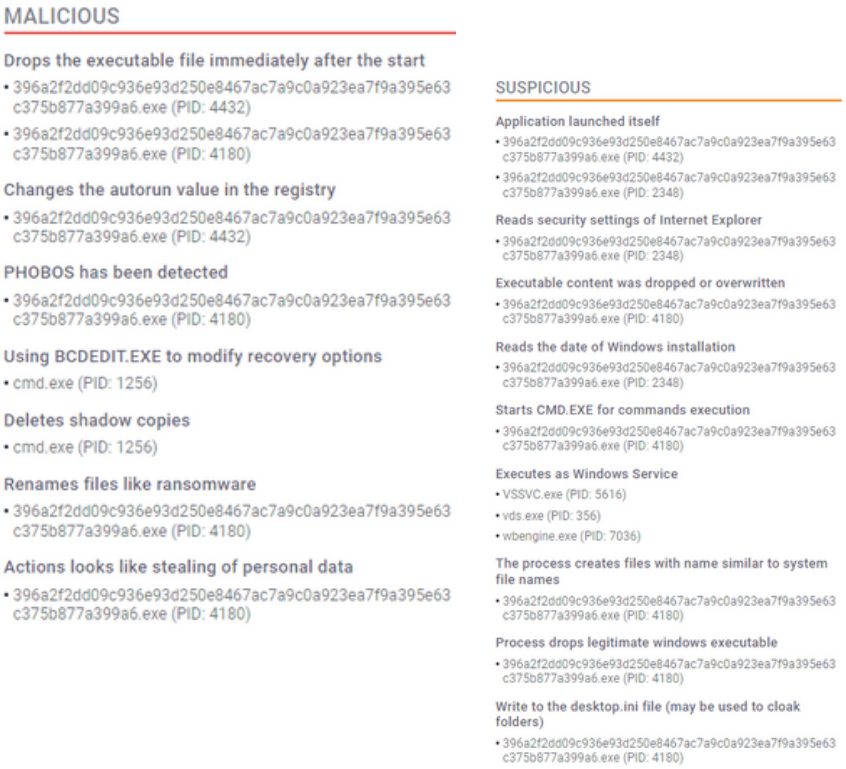




Il file **data.pdf** analizzato su **Windows 10 Professional (build: 19045, 64 bit).** contiene **exploit** progettati per sfruttare vulnerabilità nei lettori PDF e eseguire codice malevolo sul sistema della vittima, questo codice può portare ad operazioni dannose come l'installazione di malware aggiuntivi, l'esecuzione di comandi o altre attività pericolose per l'azienda.

Bonus

Attacco 2



MALICIOUS

Drops the executable file immediately after the start
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Changes the autorun value in the registry
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)

PHOBOS has been detected
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Using BCDEDIT.EXE to modify recovery options
- cmd.exe (PID: 1256)

Deletes shadow copies
- cmd.exe (PID: 1256)

Renames files like ransomware
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Actions looks like stealing of personal data
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

SUSPICIOUS

Application launched itself
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)

Reads security settings of Internet Explorer
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)

Executable content was dropped or overwritten
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Reads the date of Windows installation
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)

Starts CMD.EXE for commands execution
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Executes as Windows Service
- VSSVC.exe (PID: 5616)
- vds.exe (PID: 356)
- wbengine.exe (PID: 7036)

The process creates files with name similar to system file names
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Process drops legitimate windows executable
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Write to the desktop.ini file (may be used to cloak folders)
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Il file eseguibile,
396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe
analizzato su **Windows 10 Professional (build: 19045, 64 bit)**
è un tipo di malware di cui le principale attività malevole svolte sono state:

- **Installazione e Esecuzione:** Il file si avvia immediatamente dopo essere stato eseguito e modifica le impostazioni del registro di sistema per assicurarsi che venga eseguito automaticamente ogni volta che il sistema viene riavviato.
- **Modifica del Registro di Sistema:** Cambia il valore di autorun nel registro, che consente al malware di avviarsi automaticamente.
- **Utilizzo di BCDEDIT.EXE:** Modifica le opzioni di recupero del sistema, che potrebbe impedire la possibilità di ripristinare il sistema da una situazione compromessa.
- **Eliminazione delle Copie Shadow:** Rimuove le copie shadow dei file, che sono utilizzate per il ripristino in caso di attacco ransomware.
- **Rinominazione dei File:** Cambia i nomi dei file in modo da impedire l'accesso ai dati o per criptarli.
- **Creazione di File e Cartelle:** Crea file e cartelle con nomi simili a quelli di sistema per confondere l'utente e nascondere la propria presenza.
- **Scrittura su Desktop.ini:** Modifica il file desktop.ini, che potrebbe essere utilizzato per nascondere cartelle o file.
- **Esecuzione di Comandi:** Usa cmd.exe per eseguire comandi e potrebbe alterare altre impostazioni di sistema.
- **Controllo delle Impostazioni di Sistema:** Legge e potrebbe modificare le impostazioni di sicurezza e configurazione del sistema, come le impostazioni di Internet Explorer e la posizione del computer.

Bonus

Consigli per i manager

Formazione personale

Organizzare sessioni di formazione regolari sulle tematiche come il riconoscimento di email di phishing, la gestione delle password e le best pratice per la sicurezza informatica. Potrebbe essere anche utile condurre esercitazioni periodiche con tentativi di phishing simulato.

Aggiornamenti

Aggiornamenti precisi e puntuali per mantenere il software e i sitemi operativi aggiornati.
Sopratutto è importante implementare un sistema di gestione delle patch per assicurarsi che tutte le vulnerabilità conosciute siano corrette.

Backup Periodici

Per garantire che i dati aziendali possano essere recuperati è importante che vengano fatti backup regolari dei dati più importanti, inclusi file, database e configurazioni di sistema.