Progetto S9-L5

log analysis & response

INDICE

Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

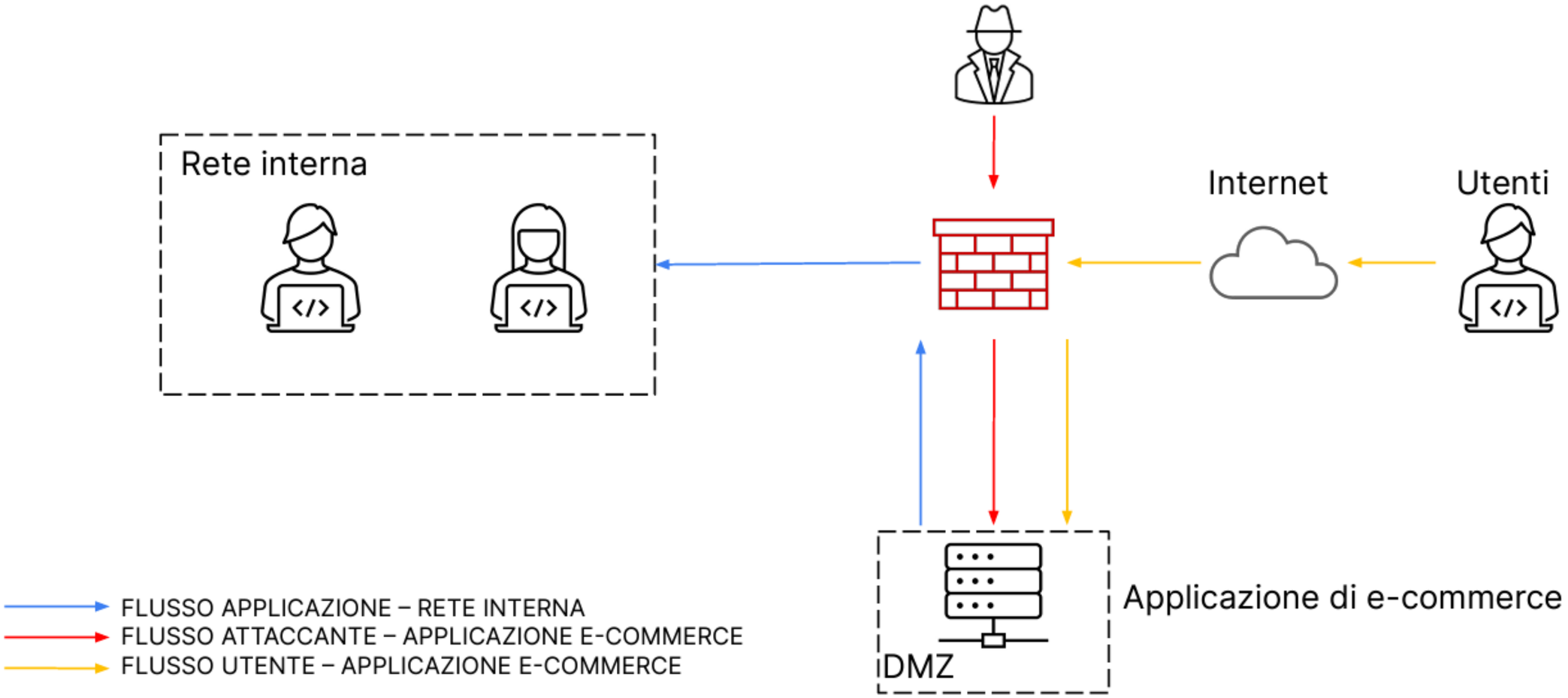
1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

1. **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 **ogni minuto gli utenti spendono 1.500 €** sulla piattaforma di e-commerce.

1. **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 in slide 2 con la soluzione proposta.

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.



AZIONE PREVENTIVA

prima di tutto capiamo con che tipo di vulnerabilita’ andiamo a che fare, nel nostro caso xss ed sqlinjection.

XSS & SQLinjection cosa sono

XSS: Cross-Site Scripting, è una vulnerabilità di sicurezza comune che colpisce le applicazioni web. Si tratta di un attacco in cui un aggressore inserisce script dannosi (solitamente codice JavaScript) all'interno dei dati che vengono visualizzati da altri utenti. Questi script consentono all'attaccante di rubare informazioni sensibili, manipolare l'aspetto della pagina web, reindirizzare l'utente su pagine dannose o eseguire azioni dannose a nome dell'utente.
Esistono principalmente tre tipi di XSS:

- **Stored XSS: L'input contenente lo script dannoso viene archiviato nel server e successivamente restituito a tutti gli utenti che visualizzano la pagina.**

- **Reflected XSS: Lo script dannoso viene incorporato direttamente nell'URL e viene riflesso sulla pagina web. Questo tipo di XSS è spesso legato all'invio di link malevoli che inducono gli utenti a eseguire lo script.**

- **DOM-based XSS: La vulnerabilità si verifica nel Document Object Model (DOM), manipola il DOM in modo imprevisto e dannoso.**

SQL Injection: è una vulnerabilità di sicurezza che si verifica quando un'applicazione web non filtra correttamente l'input dell'utente inserito in campi di input che vengono utilizzati nelle query SQL. Gli attaccanti sfruttano questa debolezza inserendo input malevoli che possono alterare il comportamento delle query SQL eseguite dal sistema.Ciò può consentire all'attaccante di manipolare, visualizzare o eliminare dati nel database, compromettendo la sicurezza e l'integrità delle informazioni. esistono vari tipi di SQLI due delle piu' famose sono:

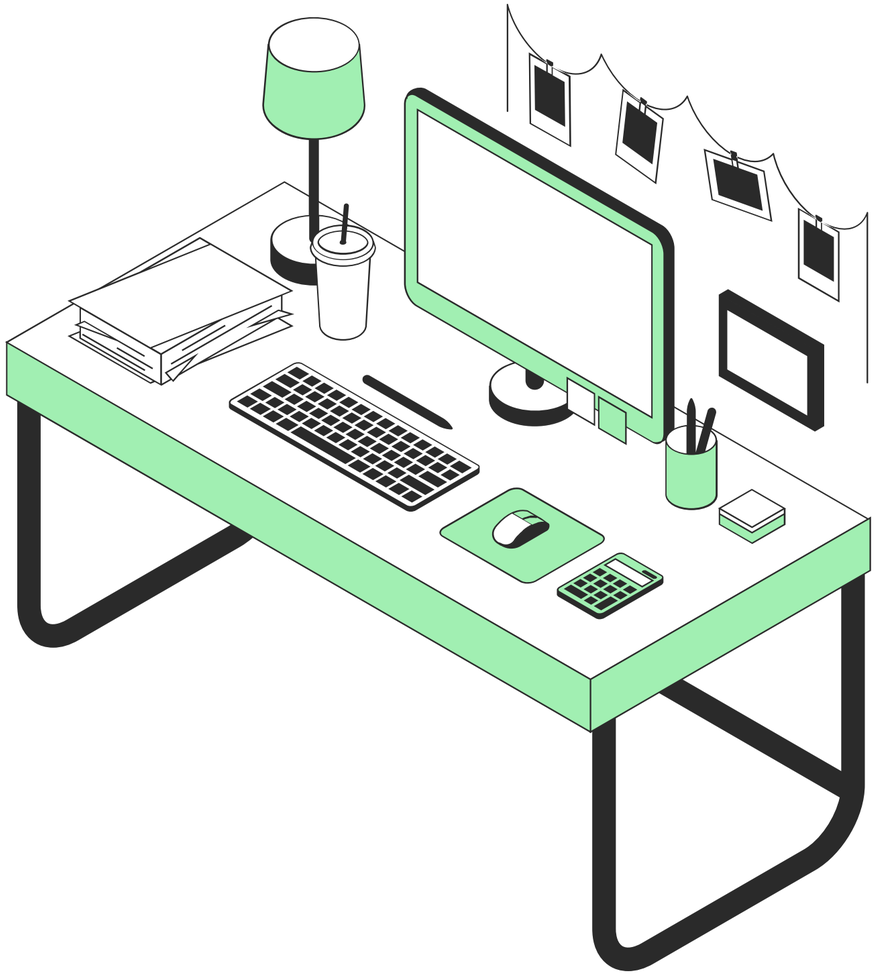
- **SQL Injection classica:**
  - **Descrizione: In questo tipo di SQL Injection, un attaccante inserisce input malevoli nelle caselle di input dell'applicazione web.**
  - **Come funziona: L'input malevolo altera la struttura della query SQL, permettendo all'attaccante di eseguire comandi non autorizzati sul database.**
- **Blind SQL Injection:**
  - **Descrizione: Questa variante non restituisce direttamente i risultati dell'attacco all'attaccante, ma li puo' ottenere tramite domande binarie (vero / falso)**
  - **Come funziona: L'attaccante sfrutta le condizioni booleane nelle query per ottenere informazioni sensibili senza visualizzare direttamente i dati.**

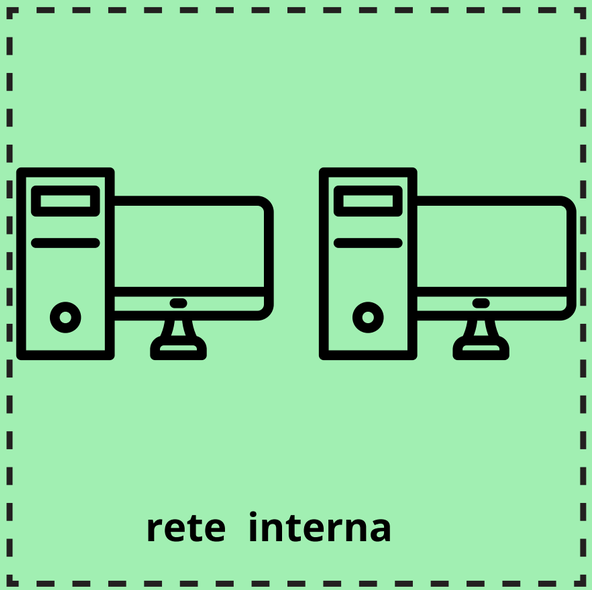
AZIONI PREVENTIVE NELLO SPECIFICO

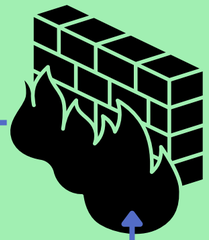
Per prevenire le SQL Injection, è fondamentale utilizzare parametri nelle query SQL. Inoltre, è importante effettuare la validazione e la sanitizzazione dell'input dell'utente, evitando di incorporare direttamente dati inseriti dagli utenti nelle query SQL senza una corretta manipolazione.

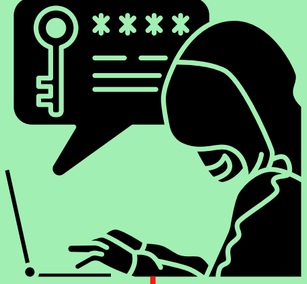
Per prevenire attacchi XSS, gli sviluppatori web dovrebbero adottare buone pratiche di sicurezza come la validazione dell'input e l'uso di funzioni di escape nei linguaggi lato server, Inoltre, l'implementazione di meccanismi di Content Security Policy (CSP) può aiutare a mitigare gli attacchi XSS limitando le risorse che possono essere caricate ed eseguite all'interno di una pagina web.

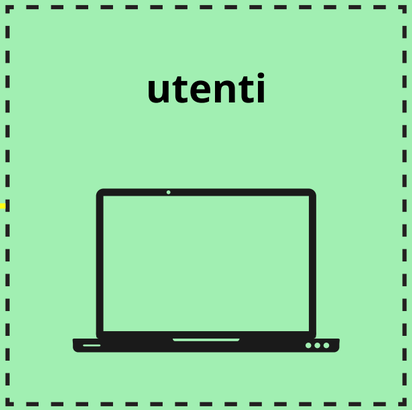
infine si puo' inplementare un WAF.
WAF, o Web Application Firewall, è un sistema di sicurezza progettato per proteggere le applicazioni web da una varietà di attacchi online, tra cui SQL injection e cross-site scripting (XSS).Il ruolo principale di un WAF è quello di filtrare e monitorare il traffico HTTP tra un'applicazione web e l'Internet per impedire che attacchi dannosi raggiungano l'applicazione.











WAF

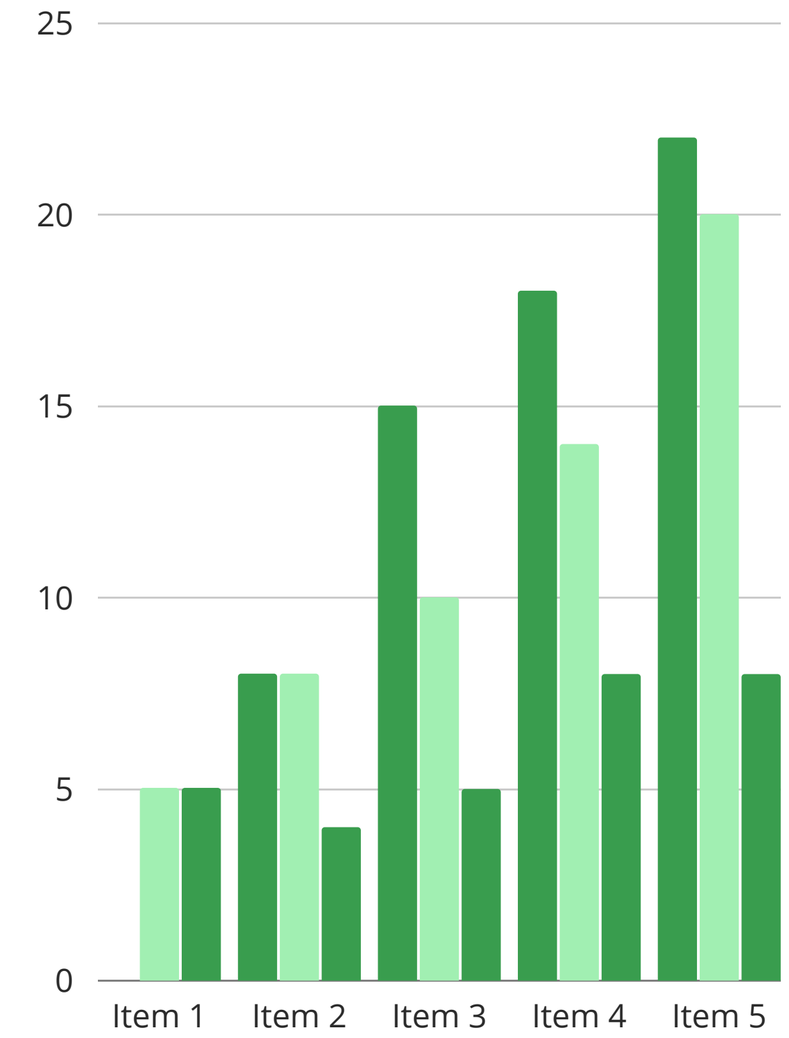
DMZ

nella nuova architettura di rete viene implementato un WAF (web aapplication firewall) che quindi dona una sicurezza aggiuntiva nei confronti di attachi specifici rivolti alle web app come XSS ed SQLI, se invece immaginiamo una situazione in cui viene investito un capitale maggiore si potrebbe pensare all'aggiunta di un NGFW (next generation firewall) in quanto e' comprensivo di difese come IDS ed IPS le quali aiutano nell'intercettazione di traffico malevolo

impatti sul business

al secondo punto della traccia ci viene detto che la piattaforma subisce un attacco DDOS della durata di 10 minuti, la domanda dunque e' la seguente: quant' e' la perdita totale dell'azienda sapendo che il guadagno e' di circa 1500$ al minuto?

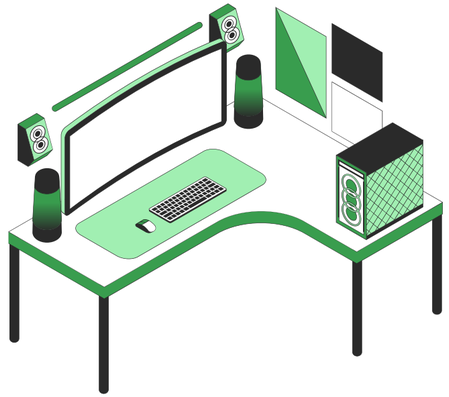
se facciamo un rapido calcolo possiamo stimare in maniera molto basilare e superficiale la perdita potenziale dell'azienda per fare cio' ci basta eseguire il calcolo:
1500 ($ al minuto) x 10 (minuti dell'attacco)= 15.000$
C'e' da ricordare pero' che in una situazione realistica ci sono molti piu' fattori che influenzano tale dato come l'area geocrafica ed il tempo del giorno in quanto i guadagni variano da zona a zona sia temporale ,che geografica si intende

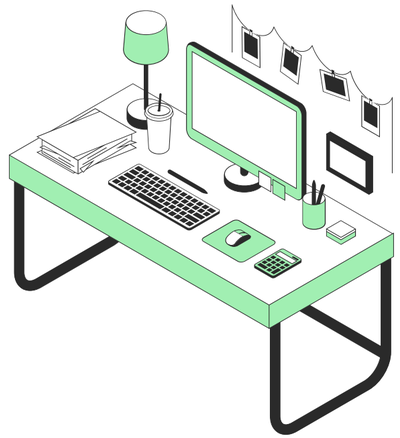


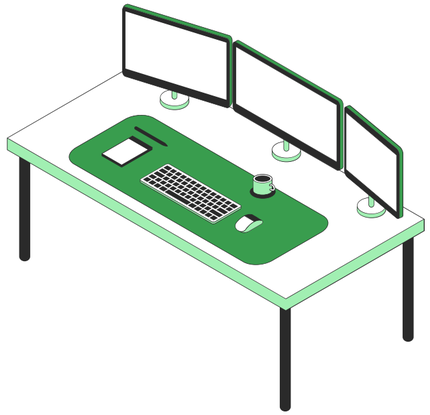
COS’ E’ UN DDOS

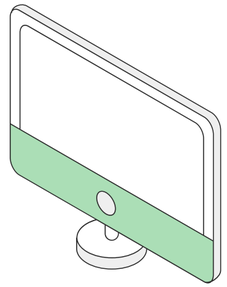
Un attacco DDOS, acronimo di Distributed Denial of Service, è un tipo di attacco informatico in cui un gran numero di dispositivi, spesso costituiti da una rete di computer compromessi (botnet), invia un volume massiccio di richieste di traffico a un singolo servizio o server, sovraccaricandolo e impedendo agli utenti legittimi di accedervi. L'obiettivo principale di un attacco DDOS è rendere il servizio o il sito web inaccessibile o rallentato, causando un "denial of service" per gli utenti legittimi.

La prevenzione degli attacchi DDOS spesso coinvolgono l'uso di servizi di mitigazione DDOS dedicati, la configurazione di firewall avanzati, la distribuzione di sistemi di rilevamento degli attacchi, e la cooperazione con i fornitori di servizi Internet per filtrare il traffico dannoso.







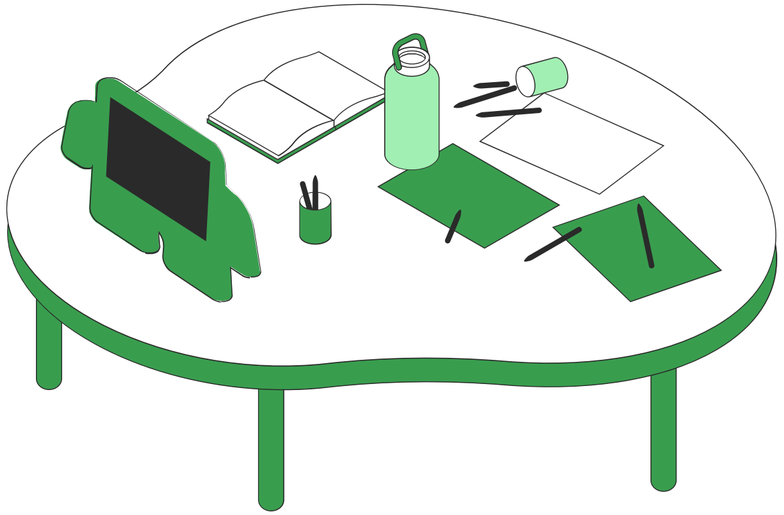


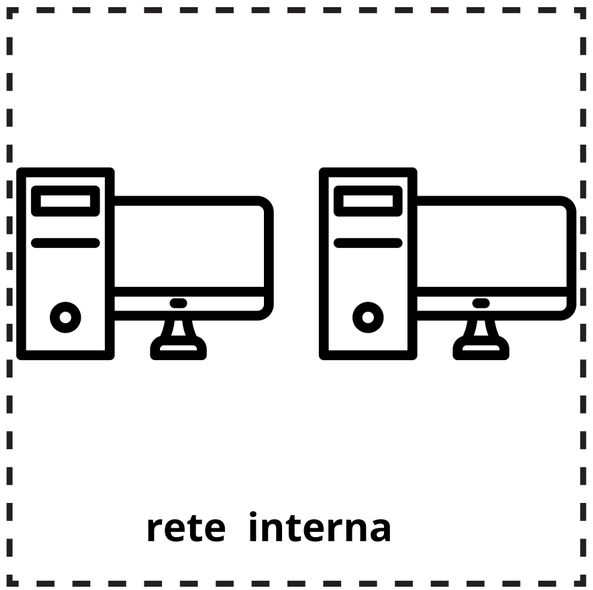
RESPONSE

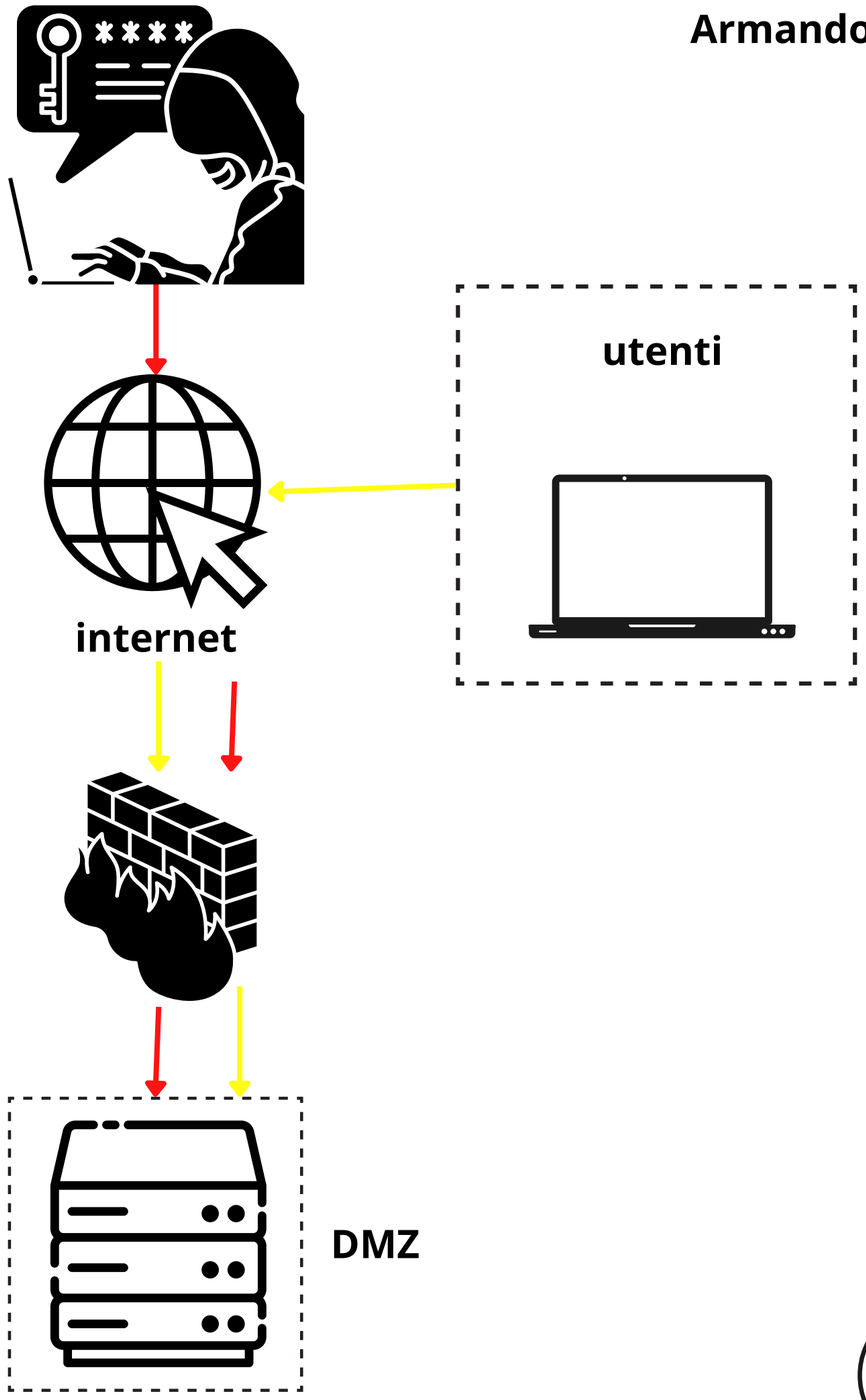
nella terza parte dell’ esercizio ci viene richiesto di adottare misure nei confronti di un malware ma allo stesso tempo di non escludere l’acesso al cybercriminale, per fare cio’ useremo la tecnica vista in queste setttimane dell’isolamento in quanto ci permette di evitare che il malware si propaghi e allo stesso tempo di studiare l’attacco in corso. Cio’ puo’ essere utile in quanto ci permette di capire come e’ avvenuto l’attacco e cosa potremmo fare noi, cosi’ come l’azieda, per difebderci, prevenire o, addirittura, evitare una futura situazione simile. Nella slide successiva avremo una dimostrazione visiva di cio’ che avviene in un isolamento

COS’ E’ UN MALWERE

Il malware(o malicious software) è un termine generico che si riferisce a software dannoso progettato per danneggiare, infiltrarsi o compromettere un sistema informatico senza il consenso dell'utente. Questi programmi dannosi possono assumere varie forme, come virus, worm, trojan, spyware o ransomware, e sono spesso creati con l'intento di danneggiare dati, rubare informazioni personali, compromettere la sicurezza del sistema o eseguire azioni dannose senza il consenso dell'utente







Come si puo' notare consiste, semplicemente, nel'estromettere la rete interna dal server infetto, cosi' da evitare una possibbile propagazione del malware