Progetto S9L5: Simone Esposito

EPICODE

Esercizio
Traccia e requisiti

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. È richiesta sola modifica

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 **ogni minuto gli utenti spendono 1.200 €** sulla piattaforma di e -commerce . **Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica**

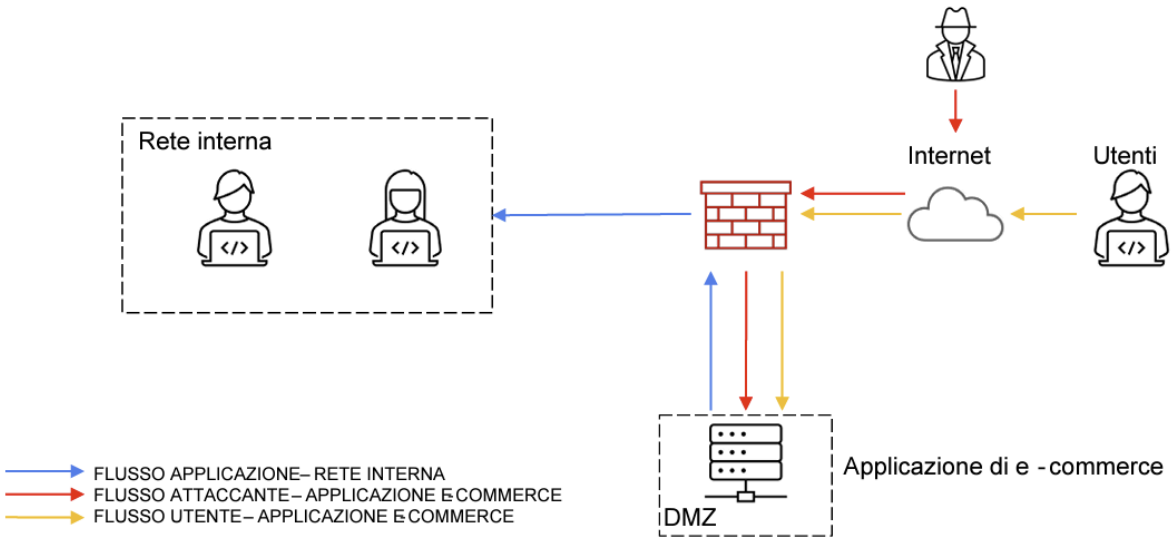
3. **Response** : l'applicazione Web viene infettata da un malware .
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta .

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

5. **Modifica «più aggressiva» dell'infrastruttura:** integrando eventuali altri elementi di sicurezza **(integrando anche una soluzione al punto 2)** Budget 5000 -10000 euro. Eventualmente fare più proposte di spesa

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.



Svolgimento punto 1:

Per difendere l’applicazione web da attacchi SQLi e XSS da parte di un utente malintenzionato, possiamo agire in questo seguente modo:

Protezione contro SQLi:

- **Prepared Statements**: query preparate, utilizzate per separare il codice SQL dai dati, le query preparate impediscono agli attaccanti di manipolare la struttura della query con input malevoli.

- **Sanitizzazione e validazione degli input**: La sanitizzazione si concentra sulla pulizia dei dati per evitare contenuti dannosi, mentre la validazione si occupa di assicurarsi che i dati siano nel formato e nel range corretto.

Rimozione di Caratteri Pericolosi: Eliminazione di caratteri speciali che possono essere utilizzati per manipolare query SQL o script.

Controllo del Formato: Verifica che i dati rispettino un formato specifico (ad esempio, numeri interi, indirizzi email).

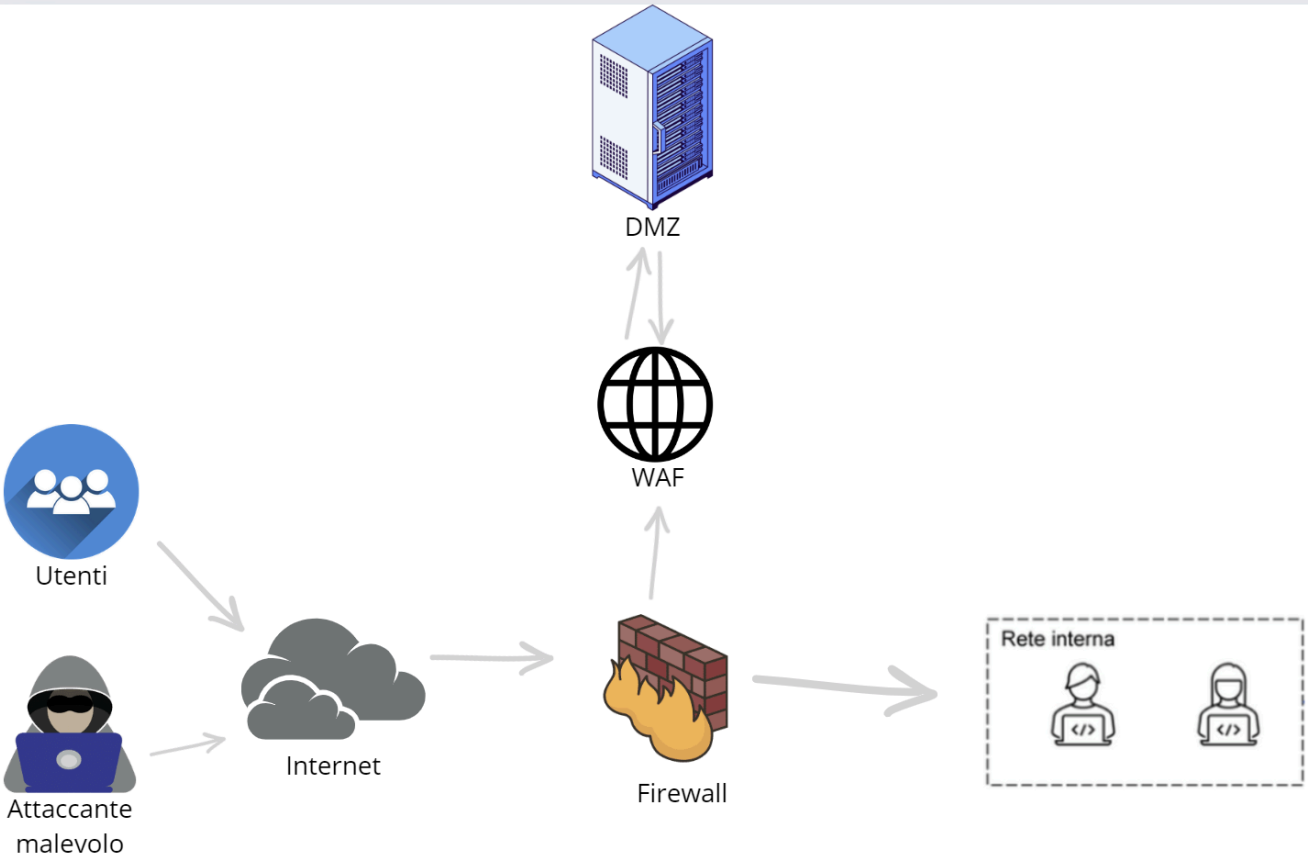
Escape per SQL: Inserimento di caratteri di escape per prevenire che i dati siano interpretati come parte della query SQL.

Protezione contro XSS:

- **Escape dei dati in output**: Quando un'applicazione web mostra dati all'utente, questi dati possono includere contenuti inseriti dagli utenti o provenienti da fonti esterne. Se questi dati non sono adeguatamente trattati, un attaccante potrebbe inserire codice HTML, JavaScript o altro codice dannoso che verrà eseguito nel contesto del browser dell'utente.

Identificazione dei Caratteri Speciali: i caratteri speciali che devono essere "escapati" includono <, >, &, ", e '.

Dimostrazione grafica:



SVOLGIMENTO PUNTO 2:

L'applicazione web di e-commerce subisce un attacco DDoS (Distributed Denial of Service) che rende l'applicazione non raggiungibile per 10 minuti. Si stima che ogni minuto di downtime comporta una perdita di 1.200 €.

Perdita Finanziaria:

Se l'applicazione non è raggiungibile per 10 minuti, la perdita totale sarà:

Perdita totale =Perdita per minuto × Durata del downtime

Perdita totale = Perdita per minuto × Durata del downtime

Perdita totale = 1.200 € × 10 minuti = 12.000 €

Azioni preventive:

Web Application Firewall (WAF): Implementare un WAF che può rilevare e bloccare automaticamente il traffico sospetto. Il WAF può essere configurato per filtrare il traffico basato

su regole specifiche.

Bilanciamento del carico: è una tecnica utilizzata per distribuire il traffico di rete o le richieste di un'applicazione su più server. L'obiettivo è migliorare la capacità di gestione del traffico, aumentare la disponibilità dell'applicazione e garantire una migliore esperienza utente.

Quando un utente invia una richiesta a un'applicazione web, questa richiesta viene prima ricevuta dal bilanciatore di carico. Il bilanciatore decide quindi a quale server inoltrare la richiesta.

I bilanciatori di carico distribuiscono le richieste in base a vari algoritmi, assicurando che nessun singolo server venga sovraccaricato.

Content Delivery Network (CDN): è una rete distribuita di server che lavorano insieme per fornire contenuti web agli utenti in base alla loro posizione geografica. L'obiettivo principale di una CDN è migliorare le prestazioni e la disponibilità di un sito web, riducendo la latenza e aumentando la velocità di caricamento delle pagine.

Svolgimento punto 3:

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.

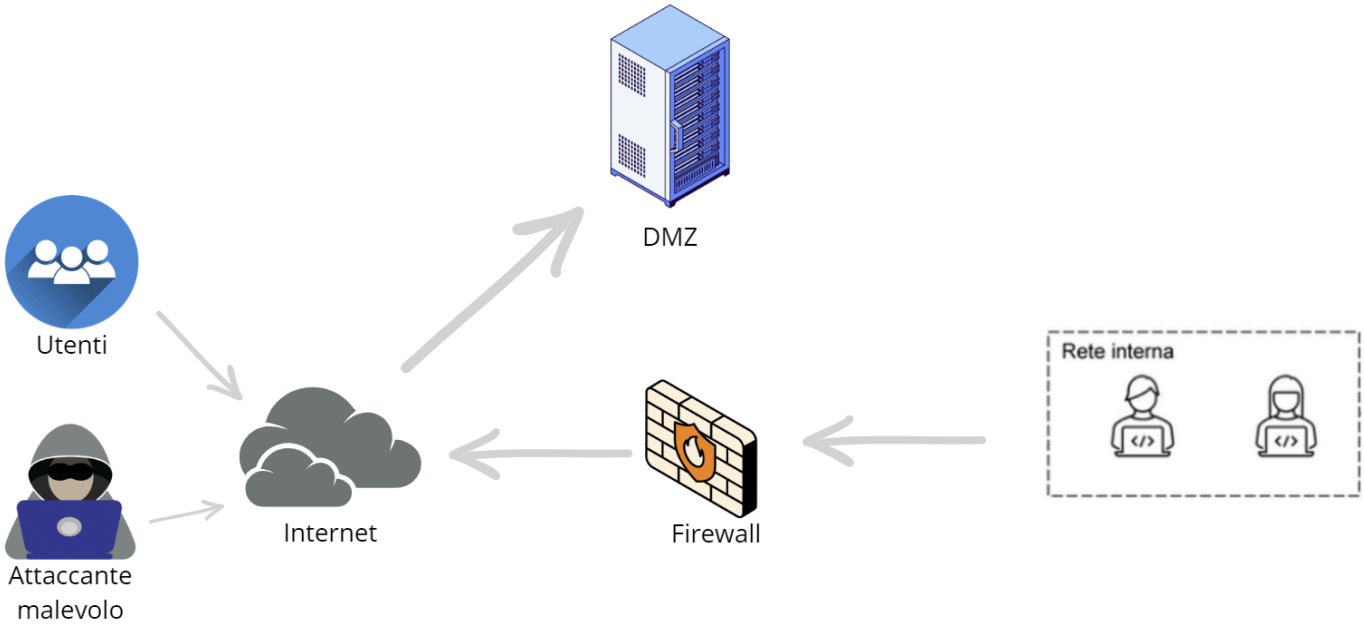
Per prevenire la propagazione del malware all'interno della rete interna, possiamo adottare le seguenti azioni:

Isolamento della DMZ: Garantire che il traffico tra la DMZ e la rete interna sia strettamente controllato attraverso regole firewall

Segmentazione della Rete: Assicurarsi che le comunicazioni tra la DMZ e la rete interna siano limitate

Firewall Avanzati: Utilizzare firewall avanzati con funzioni di ispezione approfondita dei pacchetti per monitorare e bloccare traffico sospetto.

IDS/IPS: Implementare sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS) per monitorare e bloccare traffico anomalo tra la DMZ e la rete interna.

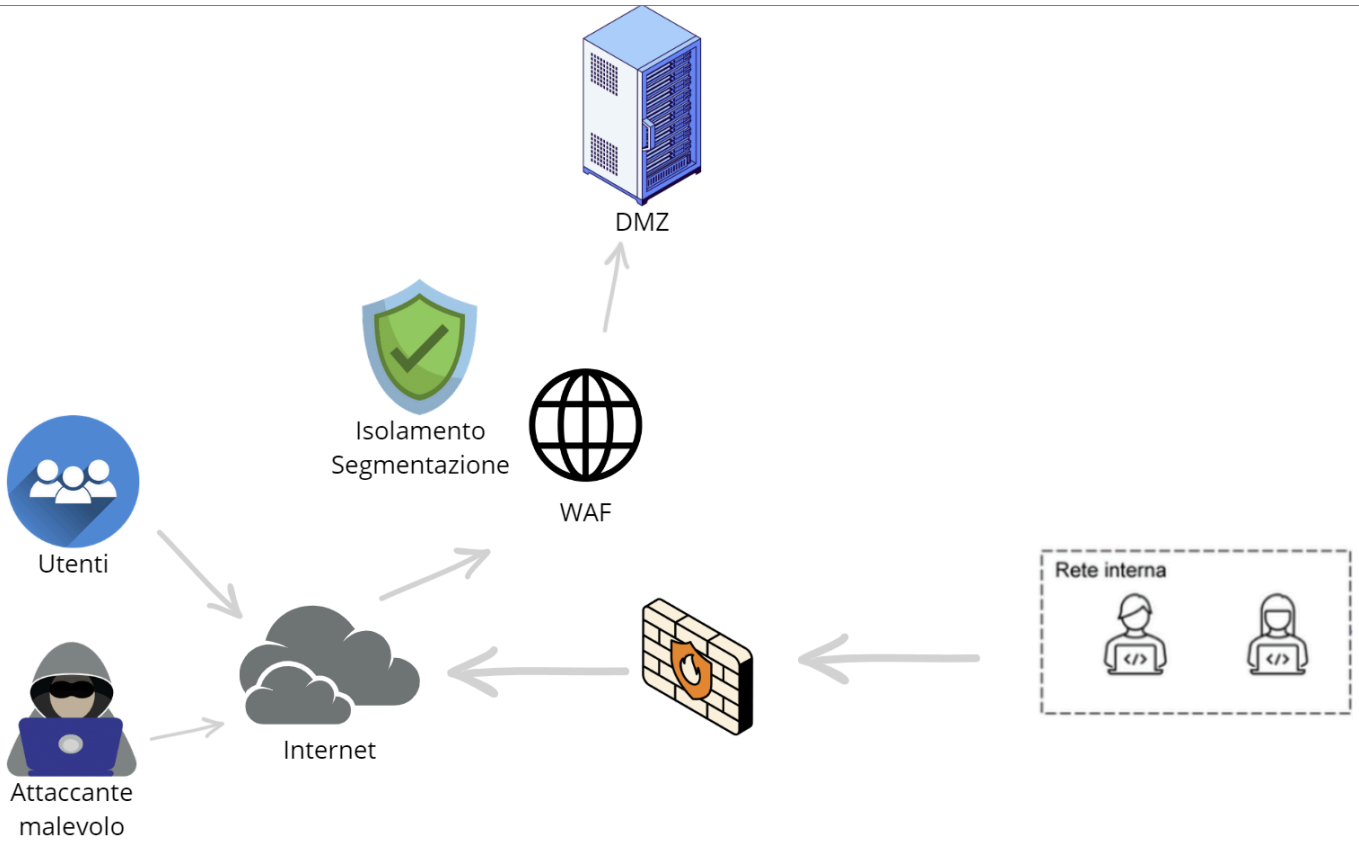


Sicurezza della DMZ: Poiché l'applicazione web è infettata, è fondamentale che la DMZ sia isolata dalla rete interna per evitare la diffusione del malware.

Contenimento del Malware: Il firewall di contenimento con implementazione IDS/IPS garantisce che anche se il malware infetta la macchina web nella DMZ, non possa propagarsi alla rete interna.

Svolgimento punto 4:

Uniamo i disegni della response e dell’azione preventiva



Svolgimento punto 5:

E' possibile implementare una serie di modifiche e aggiunte. Di seguito vengono proposte tre soluzioni con diverse opzioni di budget: una soluzione basica, una soluzione con dispositivi usati e una soluzione con dispositivi nuovi.

Soluzione Basica (Budget: 5000-7000 euro)

1. **Segmentazione della Rete:**
   - Creazione di VLAN separate per la DMZ, la rete interna e la rete amministrativa.
   - Configurazione delle regole del firewall per limitare rigorosamente il traffico tra queste VLAN.
2. **Firewall Aggiornato:**
   - Installazione di un firewall avanzato con funzioni di ispezione approfondita dei pacchetti (DPI) e rilevamento delle intrusioni (IDS).
3. **Intrusion Detection System (IDS):**
   - Implementazione di un sistema IDS per monitorare il traffico della rete e rilevare comportamenti sospetti.
4. **Aggiornamenti di Sicurezza e Patch:**
   - Assicurarsi che tutti i server e dispositivi siano aggiornati con le ultime patch di sicurezza.

Soluzione con Dispositivi Usati (Budget: 7000-9000 euro)

1. **Segmentazione della Rete:**
   - Come nella soluzione basica.

2. **Firewall di Next-Generation (NGFW):**
   - Acquisto di un firewall di prossima generazione usato, come un Palo Alto Networks PA-3020 o un Fortinet FortiGate 100E.
   - Configurazione per un'ispezione avanzata dei pacchetti e funzioni di prevenzione delle intrusioni (IPS).
3. **Intrusion Prevention System (IPS):**
   - Implementazione di un IPS usato per prevenire attacchi sulla rete.
4. **Network Access Control (NAC):**
   - Acquisto di un dispositivo NAC usato per controllare l'accesso alla rete interna.
5. **Virtual Private Network (VPN):**
   - Implementazione di una VPN per consentire accessi sicuri ai dipendenti remoti.

Soluzione con Dispositivi Nuovi (Budget: 9000-10000 euro)

1. **Segmentazione della Rete:**
   - Come nelle soluzioni precedenti.
2. **Firewall di Next-Generation (NGFW):**
   - Acquisto di un firewall di prossima generazione nuovo, come un Palo Alto Networks PA-220 o un Fortinet FortiGate 60F.
   - Configurazione per un'ispezione avanzata dei pacchetti e funzioni di prevenzione delle intrusioni (IPS).
3. **Intrusion Prevention System (IPS):**
   - Implementazione di un IPS nuovo per prevenire attacchi sulla rete.
4. **Network Access Control (NAC):**
   - Acquisto di un dispositivo NAC nuovo per controllare l'accesso alla rete interna.
5. **Security Information and Event Management (SIEM):**
   - Implementazione di una soluzione SIEM per monitorare e analizzare in tempo reale i log di sicurezza e gli eventi della rete.

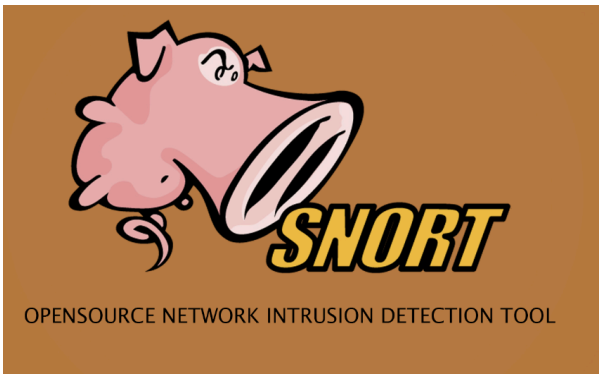
Esempi di Prodotti e Costi

Firewall di Next-Generation (NGFW)

- Palo Alto Networks PA-220: circa 5000-6000 euro nuovo.
- Fortinet FortiGate 60F: circa 6000-7000 euro nuovo.

Intrusion Prevention System (IPS)

- Snort: soluzione open-source, costo di implementazione circa 1000-2000 euro per hardware e configurazione.



Network Access Control (NAC)

- Cisco Identity Services Engine (ISE): circa 3000-4000 euro nuovo.
- Aruba ClearPass: circa 4000-5000 euro nuovo.

Security Information and Event Management (SIEM)

- Splunk: licenza base a partire da 2000-3000 euro.
- ELK Stack (Elasticsearch, Logstash, Kibana): soluzione open-source, costo di implementazione circa 2000-3000 euro per hardware e configurazione.

splunk>enterprise

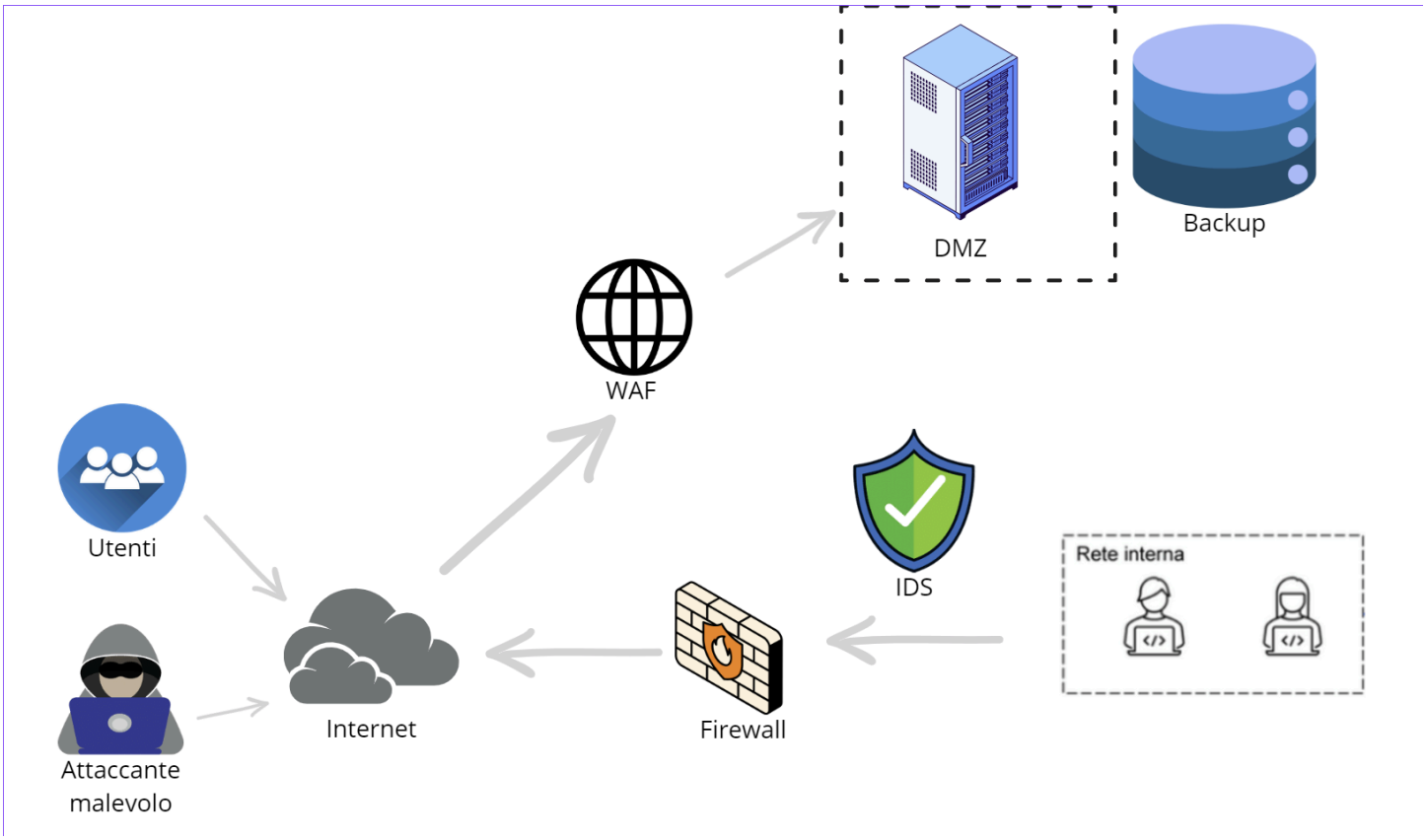
Splunk Enterprise software pricing is based on how much data you send into your Splunk installation each day.

Index Volume/Day	Annual License	Perpetual License
15 GB / Day	$1,150/GB	$2,875/GB
Annual Support	Included	$575/GB
Total	$1,150/GB	$3,450/GB

Not quite what you need? You can buy any index volume

Implementazione e Manutenzione

1. **Formazione del Personale:**
   - Organizzazione di corsi di formazione per il personale IT su nuove tecnologie e best practices di sicurezza.
2. **Monitoraggio Continuo:**
   - Implementazione di monitoraggio continuo e aggiornamenti regolari delle politiche di sicurezza.
3. **Backup e Ripristino:**
   - Configurazione di soluzioni di backup e ripristino per garantire la continuità operativa in caso di incidente.



ESERCIZIO BONUS 1:

Cliccando sul link ed aprendo il file possiamo notare un documento di DocuSign, chiedendo all'utente di cliccare su un link per visualizzare o scaricare un documento firmato. Questa è una tecnica comune utilizzata nei tentativi di phishing.

- Una finestra di dialogo di sicurezza che chiede all'utente se consentire o bloccare la connessione al sito clickme.thvy.com. Questo suggerisce che il PDF contiene un link malevolo che tenta di connettersi a un server esterno.
- Diversi processi Adobe Acrobat (Acrobat.exe, AcroCEF.exe) attivati, con numerosi tentativi di connessione a URL esterni.
- Numerose richieste a URL che restituiscono errori 404: Not Found, insieme ad alcune risposte 200: OK. Ciò indica che il file sta tentando di contattare vari server, probabilmente per scaricare ulteriori componenti malevoli o per esfiltrare dati.

Tipologia di Attacco

L'attacco è un tipico caso di **phishing** tramite un file PDF malevolo. Il file si presenta come un documento legittimo (DocuSign in questo caso) per ingannare l'utente e convincerlo a cliccare su un link o consentire una connessione a un sito malevolo.

Funzionamento dell’attacco

1. **Email di Phishing**: L'utente riceve un'email che sembra provenire da una fonte legittima (ad esempio, DocuSign).
2. **File Allegato**: L'email contiene un allegato PDF che sembra contenere informazioni importanti o urgenti.
3. **Apertura del PDF**: Quando l'utente apre il file PDF, viene visualizzato un messaggio che richiede di consentire una connessione a un sito esterno.
4. **Connessione al Sito Malevolo**: Se l'utente consente la connessione, il PDF tenta di collegarsi a un server controllato dall'attaccante. Questo server può:
    - Scaricare ulteriori malware sul sistema dell'utente.
    - Esfiltrare dati sensibili.
    - Compromettere ulteriormente la rete aziendale.

Possibili conseguenze

- **Furto di Dati**: Informazioni sensibili potrebbero essere rubate.
- **Infezione da Malware**: Il sistema dell'utente potrebbe essere infettato con malware aggiuntivo, inclusi trojan o ransomware.

- **Compromissione della Rete**: L'attacco potrebbe propagarsi all'interno della rete aziendale, compromettendo ulteriormente i sistemi.

Mitigare l’attacco

1. **Formazione del Personale**:
   - Educare i dipendenti su come riconoscere email di phishing e allegati sospetti.
   - Implementare simulazioni di phishing per migliorare la consapevolezza.
2. **Soluzioni di Sicurezza**:
   - Utilizzare software antivirus e antimalware aggiornati.
   - Implementare un sistema di filtraggio delle email per bloccare allegati sospetti.
   - Configurare firewall e sistemi di prevenzione delle intrusioni (IPS).

ESERCIZIO BONUS 2:

Dal link ricevuto possiamo osservare che sono stati avviati diversi processi come **cmd.exe**, e ha eseguito comandi specifici per modificare le impostazioni di sistema e cancellare backup.

Sono state effettuate connessioni a server esterni, principalmente per verificare certificati tramite **digicert.com**.

Il file ha scritto dati su **desktop.ini**, che potrebbe essere usato per nascondere cartelle. Ha inoltre creato un file di backup **(backmydata)** con dati cifrati, indicando **attività di ransomware.**

L'attacco è un tipico caso di **ransomware**, specificamente identificato come **Phobos**, accompagnato da funzionalità di **stealer** (furto di dati). Il ransomware cifra i file dell'utente e richiede un riscatto per decriptarli.

Funzionamento

Il malware può essere distribuito tramite email di phishing, allegati malevoli, exploit kit o siti web compromessi.

Una volta eseguito, il ransomware avvia processi e comandi per alterare il sistema operativo, disabilitare funzionalità di sicurezza e cancellare backup.

Cifra i file dell'utente, rendendoli inaccessibili, e crea un file di backup con i dati cifrati.

Mostra un messaggio all'utente, chiedendo un riscatto in criptovaluta in cambio della chiave di decrittazione.

Possibili Conseguenze

Senza un backup adeguato, i dati cifrati potrebbero essere persi definitivamente.

L'accesso ai file critici viene negato, interrompendo le operazioni aziendali.

L'azienda potrebbe essere costretta a pagare un riscatto significativo per recuperare i dati.