Report Finale M5 Security Operation Manini Sara

Indice generale

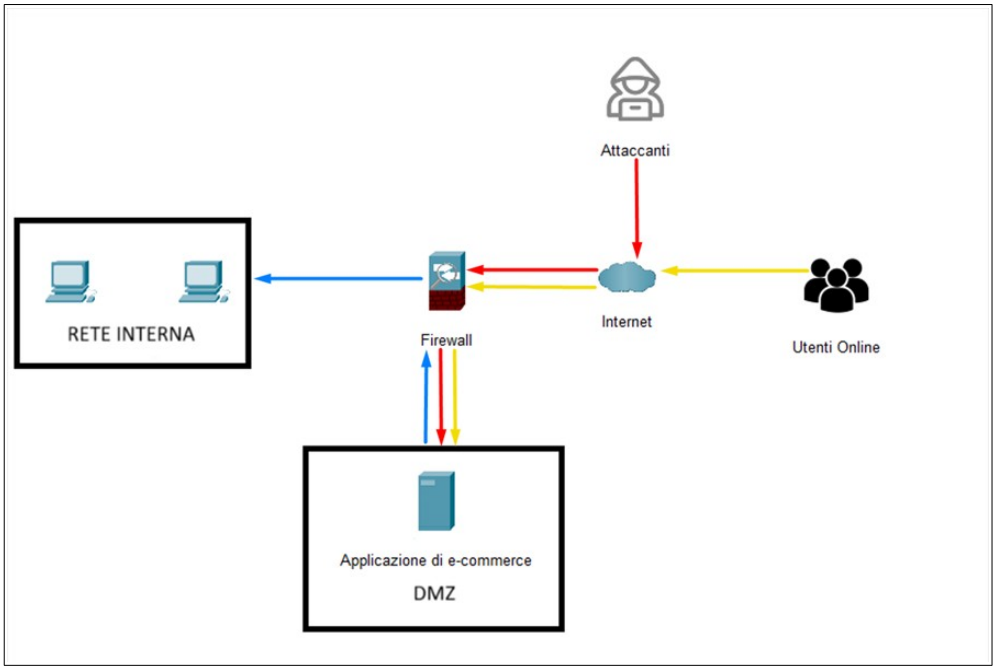
Introduzione

In questa esercitazione verranno presentati diversi scenari legati ad una struttura aziendale di tipo e-commerce, per ognuno dovremo trovare e descrivere una soluzione adatta alla problematica presentata.

Descrizione dell'ipotetica struttura aziendale

L'applicazione di e-commerce deve essere accessibile agli utenti tramite Internet per consentire gli acquisti online. Poiché le policy del firewall permettono al server situato nella DMZ di comunicare con la rete interna, un'eventuale compromissione da parte di attori malevoli di quel server potrebbe consentirgli di accedere potenzialmente anche alla rete interna.

Struttura di rete iniziale



Legenda immagine

- Freccia rossa: Flusso attaccante – applicazione e-commerce
- Freccia gialla: Flusso utente – applicazione e-commerce
- Freccia azzurra: Flusso applicazione e-commerce – rete interna

Quesito n. 1 Azioni preventive

Consegna

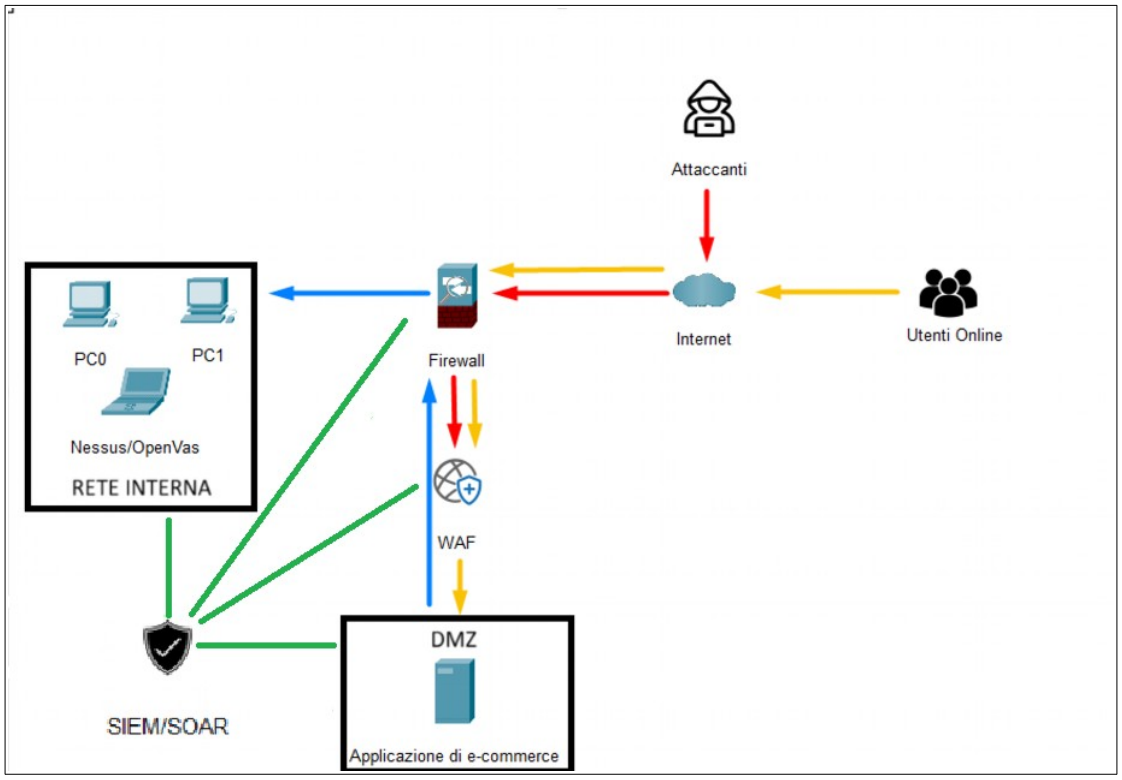
Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?
Modificate la figura in modo da evidenziare le implementazioni.

Soluzione

L'applicazione web si trova nella DMZ ed è ovviamente possibile raggiungerla tramite Internet, questo la rende vulnerabile ad attacchi da parte di potenziali attori malevoli.
Di seguito verranno illustrate le soluzioni adatte al rafforzamento della struttura iniziale:

- Implementare un WAF (Web application firewall), tra il firewall originale ed il server e-commerce. Il WAF è una barriera dedicata a proteggere gli host esposti al web da attacchi (ad esempio SQLi e XSS), filtrando e regolando il traffico HTTP.
- Schedulare scansioni regolari con software di rilevamento di vulnerabilità (come ad esempio Nessus, OpenVas) per poter verificare se il server è affetto da CVE.
- Inserire nella struttura un sistema di logging e monitoraggio del traffico tramite SIEM (Security Information and Event Management) o SOAR (Security Orchestration Automation and Response). Avendo a disposizione un sistema che centralizza i log da più fonti, è possibile avere una panoramica completa dell'andamento di eventuali attacchi ed intervenire tempestivamente per mitigare le minacce.
- Eseguire aggiornamenti di sistema e patch di sicurezza regolari, in modo da avere sempre un sistema aggiornato ed il più sicuro possibile.

Modifiche da apportare alla struttura di rete



Legenda immagine

- Freccia rossa: Flusso attaccante – applicazione e-commerce
- Freccia gialla: Flusso utente – applicazione e-commerce
- Freccia azzurra: Flusso applicazione e-commerce – rete interna
- Linea verde: Monitoraggio eventi SIEM/SOAR

Quesito n. 2 Impatti sul business

Consegna

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.
Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

Soluzione

Impatto sul business

Downtime: 10 minuti
Guadagno stimato in 1 minuto: 1.500 €
Calcolo perdita totale stimata nel downtime: 1.500 € * 10’ = 15.000 €

Azioni preventive

- Come già illustrato in precedenza implementare un WAF è la soluzione migliore per proteggere il server da attacchi come il DDoS, questo perché è possibile configurare il rate-limiting che permette di bloccare o rallentare il traffico da un determinato IP una volta superata una data soglia di richieste effettuate in poco tempo.
- Una struttura di monitoraggio dei log come citato nella soluzione del quesito n. 1, tramite quindi SIEM o SOAR, può aiutare a mitigare i rischi di un attacco DDoS intervenendo tempestivamente e bloccando il traffico anche sul firewall perimetrale.
- Avere un server secondario pronto ad entrare in azione e sostituire il server impattato, può ridurre il downtime e le perdite monetarie in attesa che si ripristini il server primario e che il team addetto alla sicurezza blocchi completamente l’attacco. Si può considerare un’opzione cloud based per i costi gestionali minori e dell’elevata disponibilità del servizio in caso di saturazione della rete.

Quesito n. 3 Response

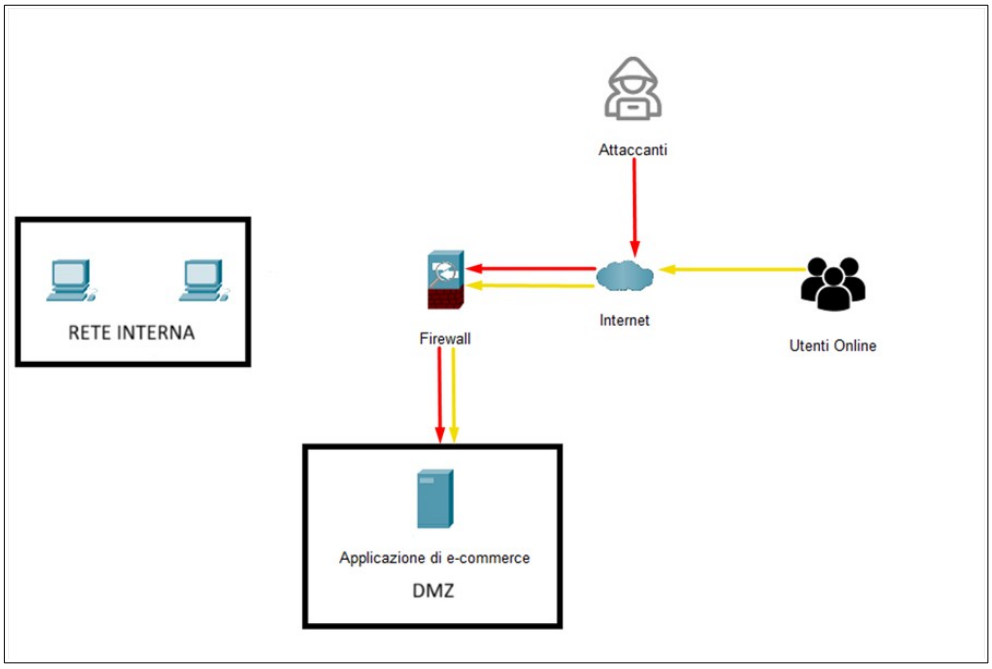
Consegna

L’applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra 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.

Soluzione

Vista la consegna, non vogliamo intervenire sulla macchina infetta per togliere l’accesso da parte dell’attore malevolo, ma solo isolarla dal resto della rete interna per evitare che il malware si propaghi.
Procederemo quindi con l’isolamento della macchina infetta su cui si trova l’applicazione web e la inseriremo in una rete di quarantena, in questo modo non taglieremo l’accesso ad Internet ma faremo in modo che la rete interna ed il web server non possano più comunicare tra loro evitando la diffusione del malware.
Indipendentemente dalla tempestività con cui abbiamo isolato la macchina infetta, dovremo comunque monitorare attentamente i log di sistema delle macchine della rete interna ed eseguire delle scansioni per verificare che il malware non abbia avuto la possibilità di diffondersi.
Come ulteriore misura di sicurezza si può pensare di blacklistare l’hash del malware sull’antivirus dei computer della rete interna.

Modifiche da apportare alla struttura di rete



Legenda immagine

- Freccia rossa: Flusso attaccante – applicazione e-commerce
- Freccia gialla: Flusso utente – applicazione e-commerce

Quesito n. 4 Soluzione completa

Consegna

Unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3).

Soluzione

Tabella riassuntiva delle soluzioni di sicurezza quesito n. 1 e 3

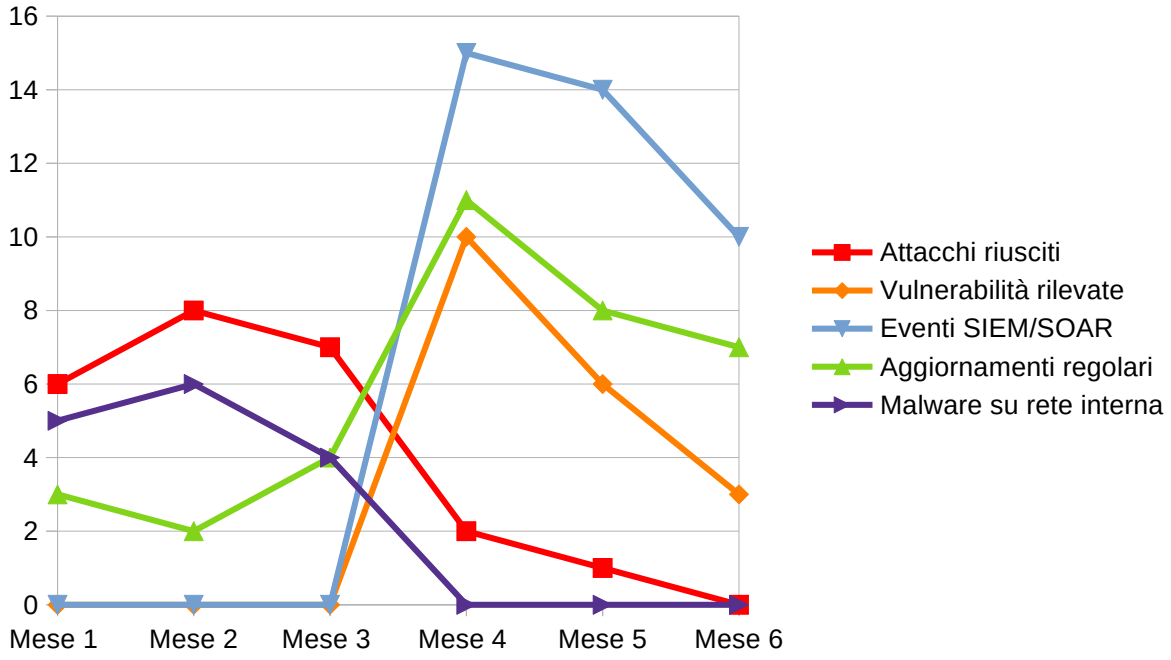
In queste tabelle riassuntive sono illustrate le soluzioni citate in precedenza, con relativo grado di efficacia.

Quesito n. 1			
Soluzione	Scopo	Risultato	Efficacia
WAF	Protezione dagli attacchi alle web app.	Protezione contro vulnerabilità comuni come SQLi, XSS, DDoS.	Alta (se ben configurato)
Scansioni di vulnerabilità	Rilevamento vulnerabilità note.	Conoscendo le vulnerabilità da cui è affetto il sistema si può intervenire rapidamente.	Medio/alta
SIEM/SOAR	Monitoraggio accurato dei log di sistema.	Monitorando i log si possono scoprire e sanare le anomalie.	Alta (eliminando eventi falsi positivi e monitorando a dovere)
Aggiornamenti regolari	Avere delle macchine più sicure.	Gli aggiornamenti e le patch riducono il rischio di compromissione.	Media

Quesito n. 3			
Soluzione	Scopo	Risultato	Score
Isolamento della macchina infetta	Proteggere il resto della rete dalla propagazione dei malware.	L'attaccante non ha accesso al resto della rete (necessari accertamenti).	Medio/alta

Grafico degli eventi

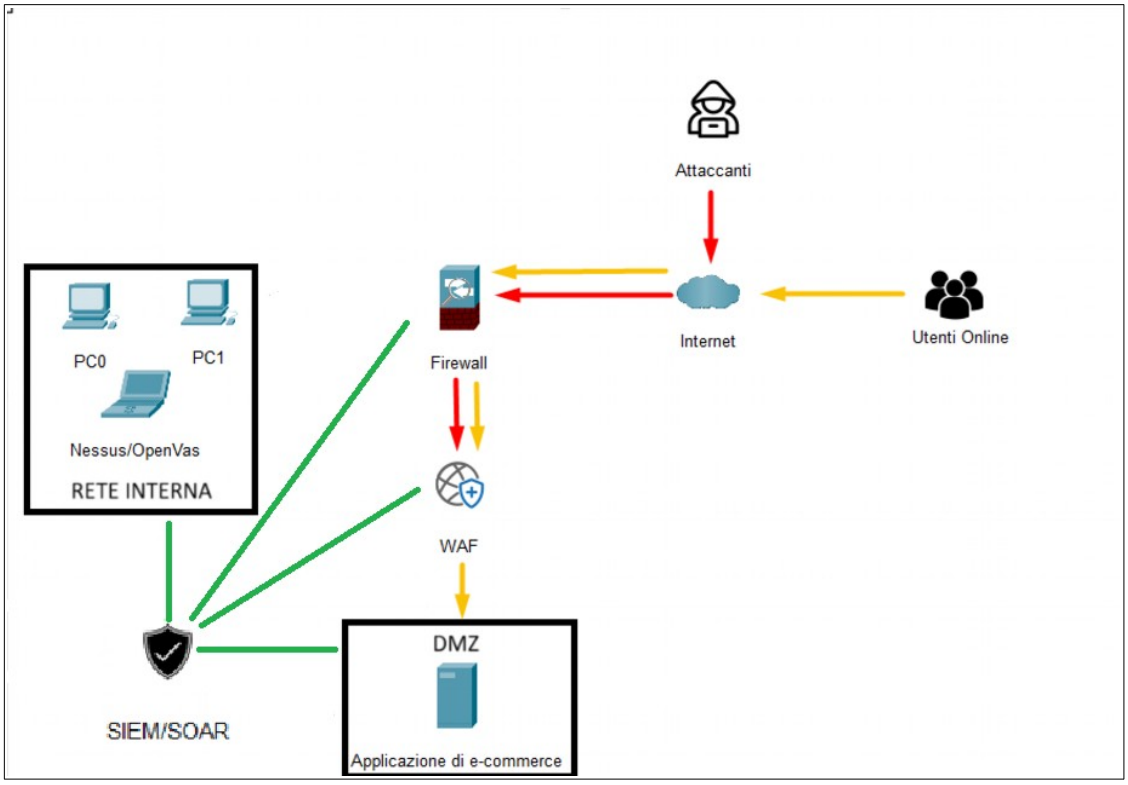
Per mostrare meglio gli effetti delle modifiche alla sicurezza, è stato prodotto un grafico degli eventi che ipotizza gli attacchi subiti dall'azienda prima e dopo l'implementazione delle misure consigliate.
Dal mese 1 al mese 3 è mostrata la situazione di partenza senza nessuna misura aggiuntiva implementata, dal mese 4 al mese 6 invece viene mostrato il quadro degli eventi dopo aver adottato tutte le misure descritte nel quesito n. 1.
Allo stesso modo è stato mostrato l'andamento potenziale dei malware che potrebbero infettare la rete interna prima e dopo l'implementazione della policy di isolamento del server su cui si trova l'applicazione web.



Legenda del grafico

- Attacchi riusciti: Mostra l'efficacia del WAF nel bloccare gli attacchi;
- Vulnerabilità rilevate: Tramite scanner di vulnerabilità è possibile ridurre nel tempo il numero di esposizioni delle macchine;
- Eventi SIEM/SOAR: Avendo a disposizione un SIEM/SOAR è possibile raccogliere log da più fonti per avere una visione completa del quadro degli eventi ed eseguire automatismi sulle criticità (blocco IP malevoli, aprire incident di sicurezza).
  Con il tempo il numero di eventi diminuisce perché vengono implementate regole ad hoc, riducendo i falsi positivi;
- Aggiornamenti regolari: Eseguendo aggiornamenti ed implementando patch di sicurezza, il sistema sarà di conseguenza meno soggetto ad exploit;
- Malware su rete interna: Isolando il web server dalla rete interna qualora venisse riscontrato un malware su di esso, si elimina il rischio di propagazione dell'infezione sulle maccchine della rete interna.

Modifiche da apportare alla struttura di rete



Legenda immagine

- Freccia rossa: Flusso attaccante – applicazione e-commerce
- Freccia gialla: Flusso utente – applicazione e-commerce
- Linea verde: Monitoraggio eventi SIEM/SOAR

Quesito n. 5 Modifica aggressiva

Consegna

Modifica “più aggressiva” dell’infrastuttura (se necessario/facoltativo magari integrando la soluzione al punto 2).
Il budget per le potenziali migliorie da apportare è di 20.000/30.000 €.

Soluzione

I prezzi e le soluzioni sono stati pensati per un’ipotetica piccola/media impresa di circa 100 dipendenti (alcuni prezzi sono stati convertiti da altre valute e quindi possono variare leggermente) .

Soluzioni essenziali per la protezione della struttura

Tipo di soluzione	Software consigliato	Costo annuo
WAF	Cloudflare	2.200 € per la versione Business
SIEM/SOAR	Microsoft Sentinel	5.200 € per la versione pay-as-you-go (considerando 100 devices e 100 utenti)
EDR	Microsoft Defender for Endpoint	5.100 € per il piano P2 (considerando 100 devices e 100 utenti)
Scansione dei sistemi	OpenVas	Gratuito, si applica il costo del device dove è installato (costo una tantum 600 € per un laptop dedicato)
Server cloud di fail-over	AWS (Amazon Web Services)	230 € per T3 Medium
Segmentazione della rete tramite VLAN	Switch CISCO	1.500 € per Catalyst 9200 (costo una tantum)

Costo (stimato) delle soluzioni di cui sopra: 14.830 €

Soluzioni extra per la protezione della struttura

Tipo di soluzione	Software consigliato	Costo annuo
Server honeypot on premises	Thinkst Canary	5.000 € per due canaries (costo una tantum circa 1.200 € per un server dedicato)
Corsi di formazione per il personale IT	Linkedin Learning	325 € per licenza (ipotizzando 5 persone) = 1.625 €
Nuovo Firewall perimetrale	Fortinet	800 € per Fortigate 60F più 700 € per licenza UTP

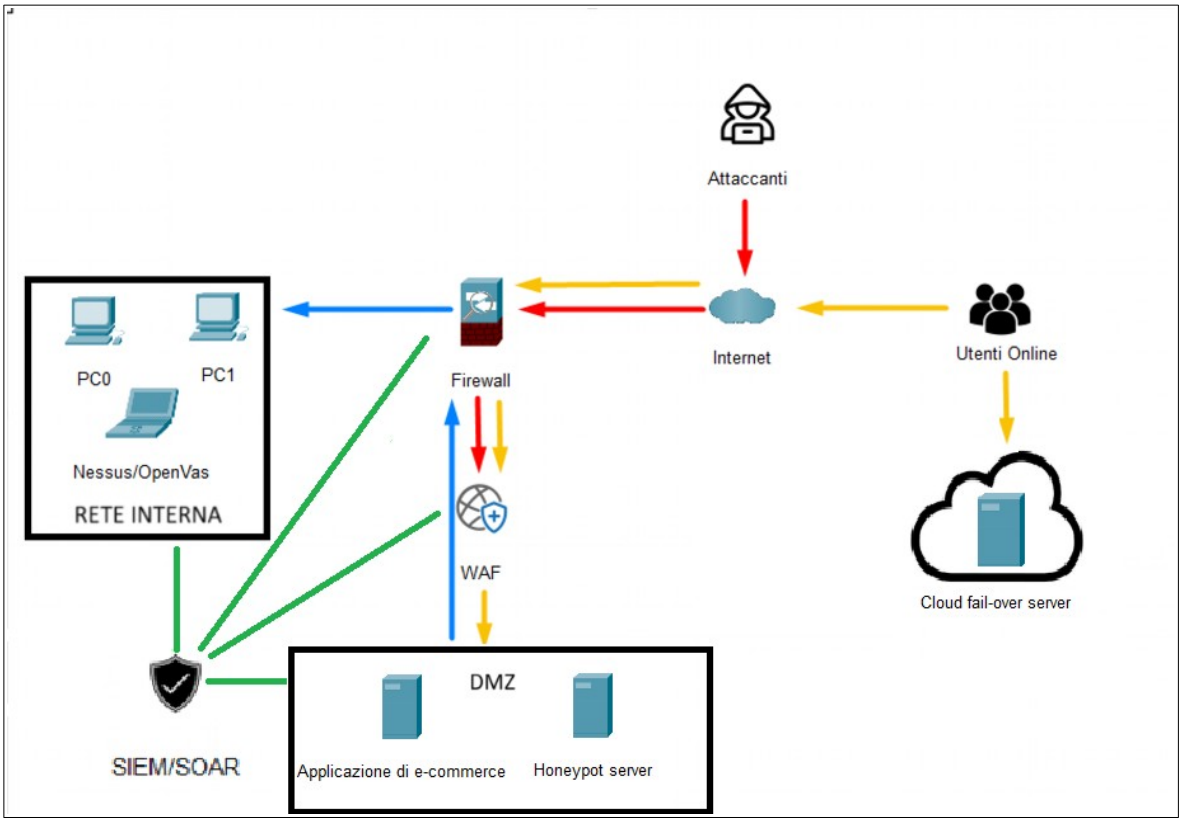
Costo (stimato) delle soluzioni di cui sopra: 9.325 €

Costo totale (stimato) delle soluzioni essenziali ed extra: 24.155 €

Possiamo anche aggiungere alcuni accorgimenti senza ulteriori costi per l’azienda:

- Assicurarsi che il traffico web passi per la porta 443 HTTPS (traffico criptato) e che la porta 80 HTTP, così come altre porte critiche non siano esposte o prive di autenticazione.
- Usare politiche zero trust per quanto riguarda la DMZ, in questo modo non si avrà nessun accesso diretto alla rete interna.
- Applicare politiche di password sicure e MFA (Multi Factor Authentication) per gli accessi al server web.

Modifiche da apportare alla struttura di rete



Legenda immagine

- Freccia rossa: Flusso attaccante – applicazione e-commerce
- Freccia gialla: Flusso utente – applicazione e-commerce
- Linea verde: Monitoraggio eventi SIEM/SOAR
- Freccia azzurra: Flusso applicazione e-commerce – rete interna