


PROGETTO MODULO 5

Lisa Pelagalli


 W20D4 - Pratica PDF **Esercizio**
Traccia e requisiti

Traccia:

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

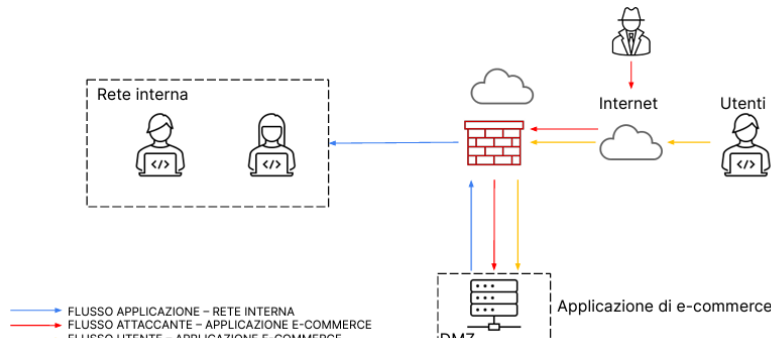
- Azioni preventive:** quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificare la figura in modo da evidenziare le implementazioni
- Impatti sul business:** l'applicazione Web subisce un 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. **Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica**
- Response:** 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. Modificare la figura in slide 2 con la soluzione proposta.
- Soluzione completa:** unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
- Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)**

2

 **Esercizio**
Traccia e requisiti

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.



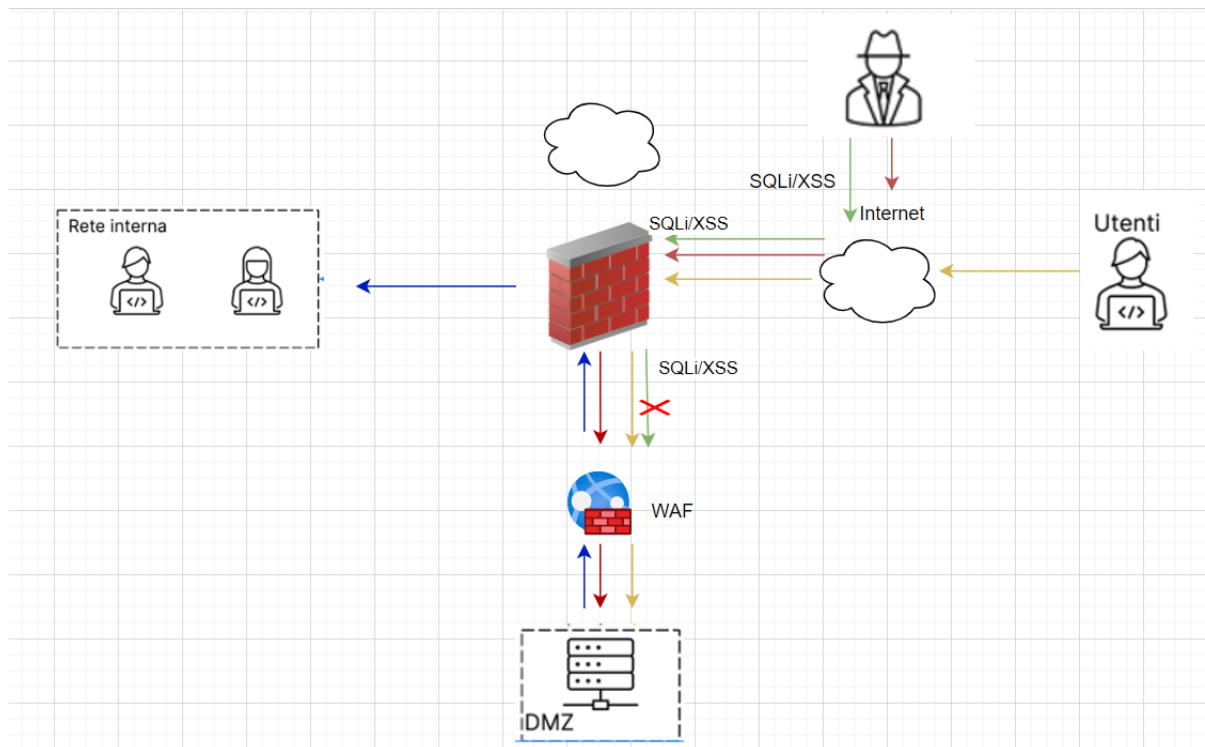
The diagram illustrates a network architecture. On the left, a dashed box labeled 'Rete interna' contains two server icons. In the center, a brick wall icon represents a firewall. To the right of the firewall is a cloud icon labeled 'Internet'. Further right is a user icon labeled 'Utenti'. Below the firewall is a dashed box labeled 'DMZ' containing a server icon labeled 'Applicazione di e-commerce'. A legend at the bottom left defines the flow types: blue arrows for 'FLUSSO APPLICAZIONE - RETE INTERNA', red arrows for 'FLUSSO ATTACCANTE - APPLICAZIONE E-COMMERCE', and yellow arrows for 'FLUSSO UTENTE - APPLICAZIONE E-COMMERCE'. The diagram shows a blue arrow from the internal network to the DMZ server, a red arrow from the Internet to the DMZ server, and a yellow arrow from the user to the DMZ server.

3

1. Azioni preventive

Per difendere l'applicazione Web da attacchi malevoli di tipo SQLi o XSS, si potrebbe in via preventiva aggiungere e configurare un WAF: Web Application Firewall.

Nella situazione proposta dalla traccia infatti, un attacco di code injection non verrebbe bloccato dal Network Firewall standard e quindi il flusso dell'attaccante arriverebbe sull'applicazione di e-commerce. Con un WAF, invece, si fa in modo di proteggere l'applicazione da questo tipo di attacco.



N.B. Siccome il flusso che dall'attaccante verso il DMZ (freccie rosse) può essere generico e non solo legato al caso specifico di un code injection, per rappresentare nel dettaglio il flusso di un attacco SQLi o XSS, sono state riportate delle frecce verdi. Dunque un attacco di questo tipo verrebbe riconosciuto e bloccato dal WAF.

Sarebbe ovviamente buona norma che il database venisse costruito in modo da avere dei buoni meccanismi di controllo degli input, sia per evitare la possibilità di fare query dinamiche, sia per evitare punti di riflessione vulnerabili a XSS. Viene così in aiuto l'attività di analisi del codice che può far rilevare bug e vulnerabilità degli input.

Come ulteriore azione preventiva, si devono attivare i log applicativi che registrano le informazioni per determinate applicazioni web, come per esempio accesso a database, modifiche a determinate table e si devono attivare anche i log dei Firewall, in modo da conoscere il traffico che li attraversa, indirizzi IP e porte sorgenti e di destinazione, policy adoperate... Tutto ciò permette di monitorare la situazione e capire se ci sono eventi anomali. Per aumentare i livelli di automatismo, spesso si implementano delle policy di sicurezza che in presenza di determinati eventi anomali fanno scattare degli alert di sicurezza.

Quindi si possono inviare i log ricavati, ad un SIEM (Security Information Event Management) che fa da collettore dei vari log ottenuti e mette insieme le informazioni per il monitoraggio automatico degli eventi.

Sempre nell'ottica di un monitoraggio preventivo, è bene che chi lavora su questi sistemi conosca correttamente il comportamento che deve avere la web application nel suo normale funzionamento, in modo da allarmarsi se inizia a comportarsi in modo inusuale. Ad esempio, se vittima di una SQL injection, l'applicazione potrebbe iniziare a mostrare in output nome degli utenti e password. Quindi non è banale pianificare anche delle sessioni di formazione e aggiornamento del personale.

Sarebbe inoltre utile avere stabilito un piano strategico di backup per il recupero eventuale dei dati persi a fronte di un evento malevolo.

Anche un sistema di autenticazione per l'accesso alla Web Application è un'azione preventiva altamente consigliata.

Ulteriore azione preventiva è quella di stabilire, magari con cadenza annuale, una attività di Penetration Testing sull'applicazione e anche di Vulnerability Assessment, per valutare lo stato di sicurezza e coprire eventualmente le scoperture, implementando le azioni di rimedio.

2. Impatti sul business

Se l'applicazione Web subisce un attacco DDoS che rende inutilizzabile i servizi per 10 minuti, stimando che in media ogni minuto gli utenti spendono 1500 € sulla piattaforma, si può dire che l'impatto complessivo sul business per l'irraggiungibilità del servizio è:

$$1500 \text{ €/min} * 10 \text{ min} = 15000 \text{ €}$$

In tal caso, è stata intaccata la "Availability" dei dati e dei servizi, uno dei principi cardine della triade CIA (Confidentiality, Integrity, Availability).

Per ovviare in via preventiva a tale problematica, si può pensare di implementare meccanismi anti-Denial of Service (investendo in tecnologie e servizi che possano rilevare e mitigare gli attacchi DDoS prima che raggiungano l'applicazione Web), strategie di back up e recupero dei dati, meccanismi di ridondanza dell'infrastruttura e gestione degli errori.

Un esempio di tecnologia anti DDoS è il servizio Cloudflare, che l'azienda può valutare di acquistare nelle varie modalità offerte, se ritiene che il costo sia affrontabile e vantaggioso.

Come sistema di ridondanza si potrebbe pensare ad un meccanismo di *failover cluster*: include due o più server e permette l'operatività dell'intero sistema anche a fronte di un errore su uno dei due server. Quando il server attivo smette di funzionare, il secondo server prende il suo posto come server attivo tramite un processo che viene chiamato appunto *failover*.

Inoltre si potrebbe implementare un sistema di monitoraggio continuo per rilevare tempestivamente eventuali anomalie nel traffico e nelle prestazioni del sistema, permettendo di rispondere prontamente agli attacchi.

Anche il personale deve essere formato su questo tipo di minaccia, in modo da saper riconoscere subito gli indizi di un attacco DDoS in corso, segnalando e rispondendo repentinamente all'incidente di sicurezza.

Queste azioni preventive, portano con sé sicuramente dei costi in termini di risorse hardware, software e capitale umano per cui è importante considerare alcuni degli scenari possibili:

1. I costi delle azioni preventive risultano superiori a 15000 €: in questo caso, l'azienda potrebbe valutare che, se la probabilità di accadimento dell'evento nell'arco temporale di un anno (ARO) è bassa, la spesa da sostenere sia eccessiva rispetto all'accettazione del rischio, che dunque viene accettato;
2. I costi delle azioni preventive risultano inferiori a 15000 € e dunque può risultare vantaggioso intraprenderle, per ridurre un rischio magari elevato di accadimento dell'evento. Si parla in questo caso di riduzione del rischio;
3. Possono inoltre esserci scenari intermedi, nei quali l'azienda deciderà la soluzione migliore da intraprendere per il bene della compagnia.

In generale, un'azienda deve applicare una valutazione del rischio e cercare di migliorare la sicurezza informatica, servendosi dei principi ufficiali offerti dal NIST Cybersecurity Framework, sviluppato dal National Institute of Standards and Technology degli Stati Uniti.

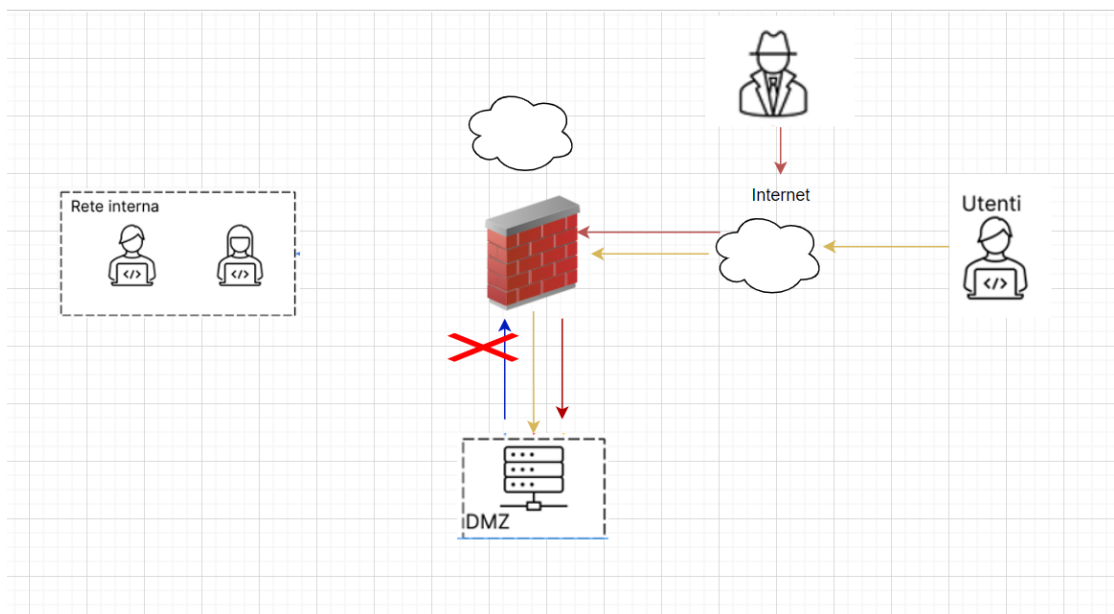
Il framework si basa su un approccio volontario, flessibile e adattabile alle specifiche esigenze di ogni organizzazione. Fin dalla sua prima pubblicazione nel 2014, il NIST Cybersecurity Framework è stato ampiamente riconosciuto per il suo valore in termini di riduzione della vulnerabilità alle minacce informatiche, miglioramento della risposta agli incidenti e promozione di una cultura della sicurezza informatica.

Dalla valutazione dei rischi e degli impatti economici sul business, l'azienda può decidere se intraprendere un'azione di riduzione del rischio, accettazione o nei casi proprio inaccettabili si ricorre alla rimozione dell'asset soggetto ad un elevato rischio.

Response

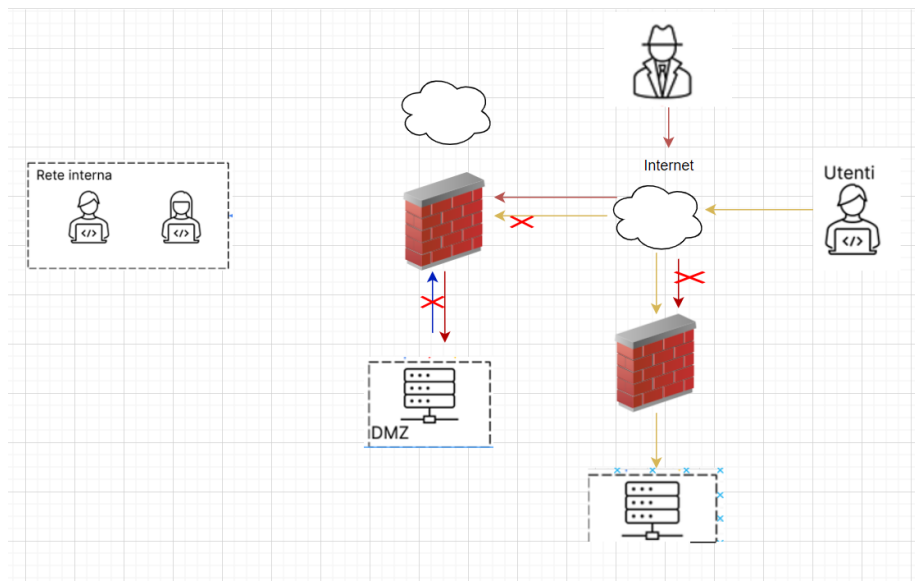
Se l'applicazione viene infettata da un malware, poiché la priorità è che questo non infetti la rete interna, senza preoccuparsi che l'attaccante continui ad avere accesso alla macchina infetta, si procede alla tecnica dell'isolamento, essendo già in passato stata applicata la segmentazione della rete DMZ rispetto alla rete interna.

Esso consiste nella disconnessione del sistema infetto dalla rete interna, facendo sì che con policy Firewall più restrittive rispetto a quelle iniziali, il flusso proveniente dalla DMZ non raggiunga la rete interna, per restringere ancora maggiormente l'accesso da parte dell'attaccante, che avrà però ancora accesso alla macchina infetta:

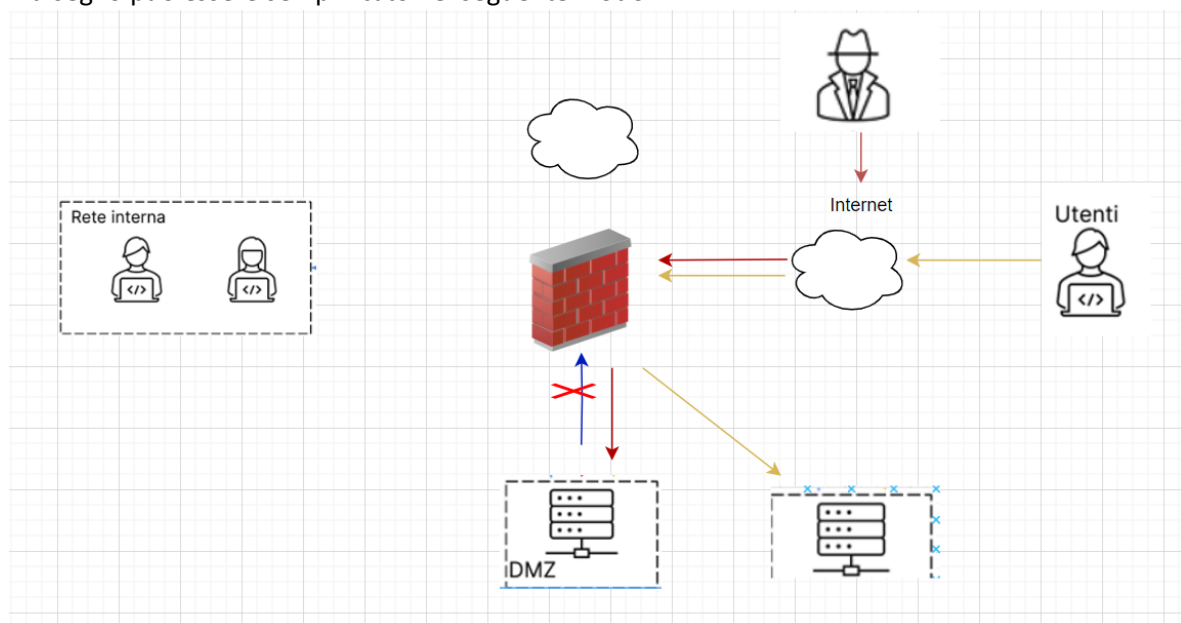


Occorre però andare a eliminare anche il flusso dei dati che dall'utente vanno verso l'applicazione di e-commerce che è stata infettata, restringendo ancora di più le policy del Firewall.

Per garantire la continuità nei servizi e quindi la Business Continuity, si potrebbe adoperare un server secondario da attivare al bisogno, in modo che il server nella rete DMZ infetto, sia completamente isolato. Si applicano politiche nel Firewall in modo da impedire il flusso di richieste dall'indirizzo dell'attaccante:



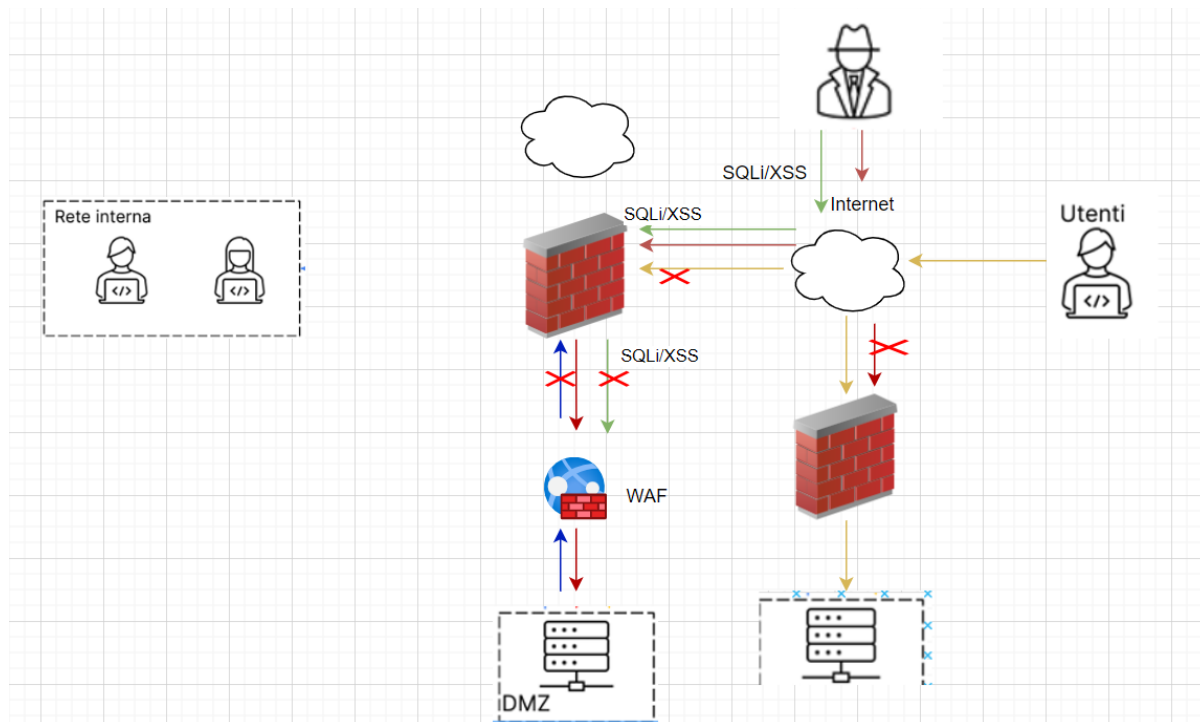
Il disegno può essere semplificato nel seguente modo:



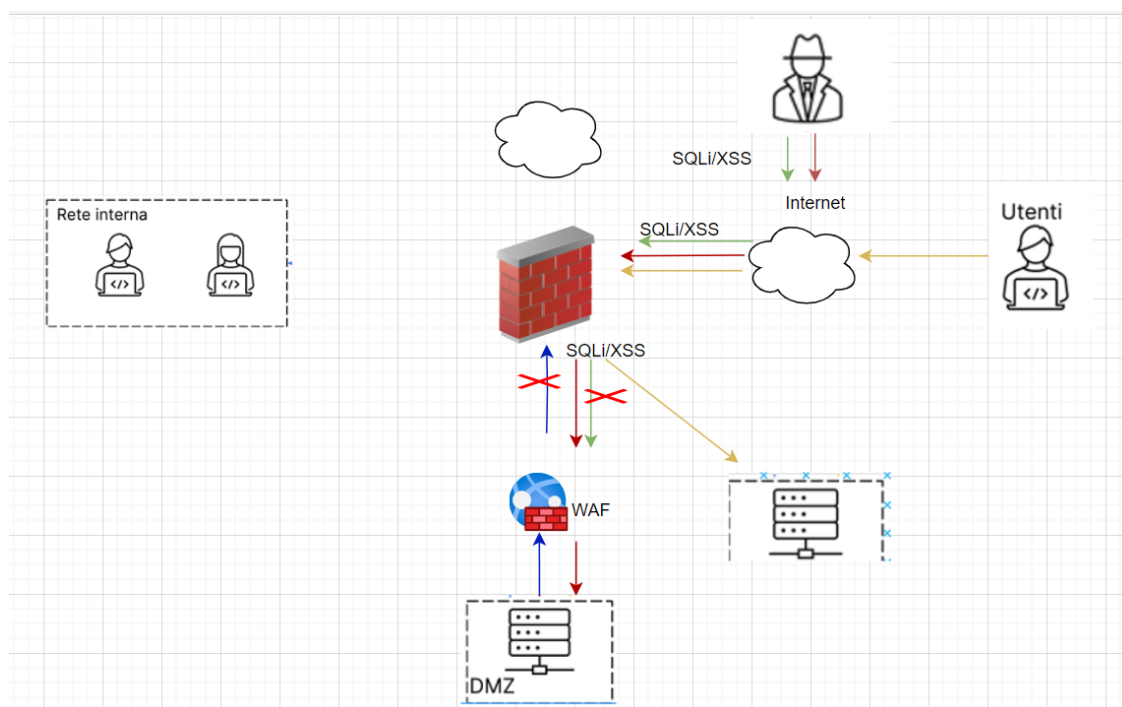
Sull'applicazione infetta passerà solo il flusso dell'attaccante, in modo tale da farne un'analisi comportamentale e scoprire eventuali nuove vulnerabilità. Invece il flusso che dal DMZ prima passava e andava verso la rete interna, è ora bloccato. Il flusso lato utente viene instradato verso il server secondario.

3. Soluzione completa

Si uniscono le due soluzioni del punto 1 e 3 nell'ottica di isolare il sistema affetto da malware e evitare SQL injection o attacchi XSS da parte dell'attaccante che continua ad essere collegato al server infetto. Si continua a garantire l'operatività del sistema:



Semplificando:



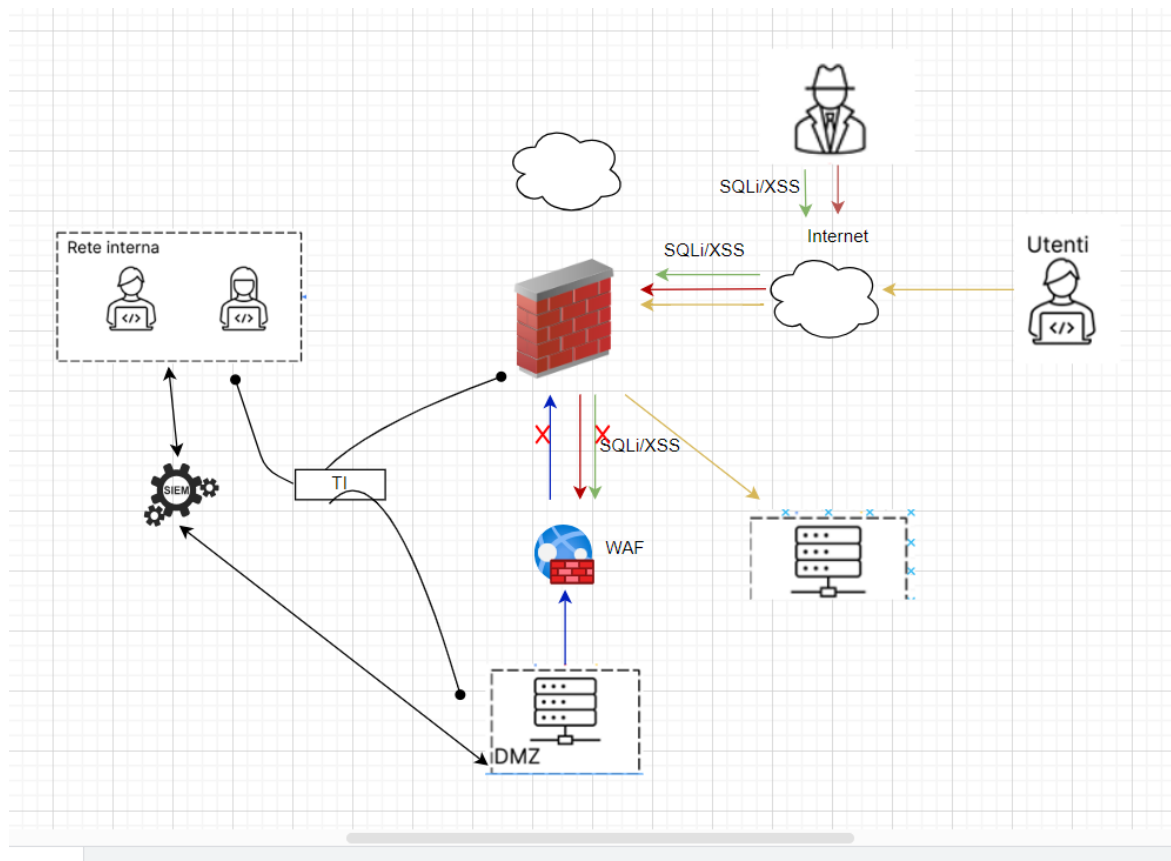
L'applicazione è dunque isolata dalla rete interna, è protetta da attacchi di tipo SQLi o XSS e il flusso delle richieste utenti è spostato su un secondo sito attivato al bisogno, per garantire continuità di servizio. Ovviamente, se il secondo sito è disponibile secondo una modalità *cold site*, oppure *warm site*, allora c'è da attendere il tempo necessario per il recupero e allineamento dei dati.

In alternativa, si potrebbe usare un approccio *hot site*, con il quale il secondo sito è sempre attivo e disponibile all'utilizzo, con costi di gestione sicuramente più alti.

Ulteriore possibilità è quella di adoperare una piattaforma cloud da attivare al bisogno (Disaster Recovery As a Service).

In aggiunta, in questo sistema si potrebbe anche inserire un sistema di Threat Intelligence con delle sonde che eseguano un monitoraggio continuo della rete, al fine di individuare ulteriori anomalie e evitare che problematiche del genere possano riaccadere.

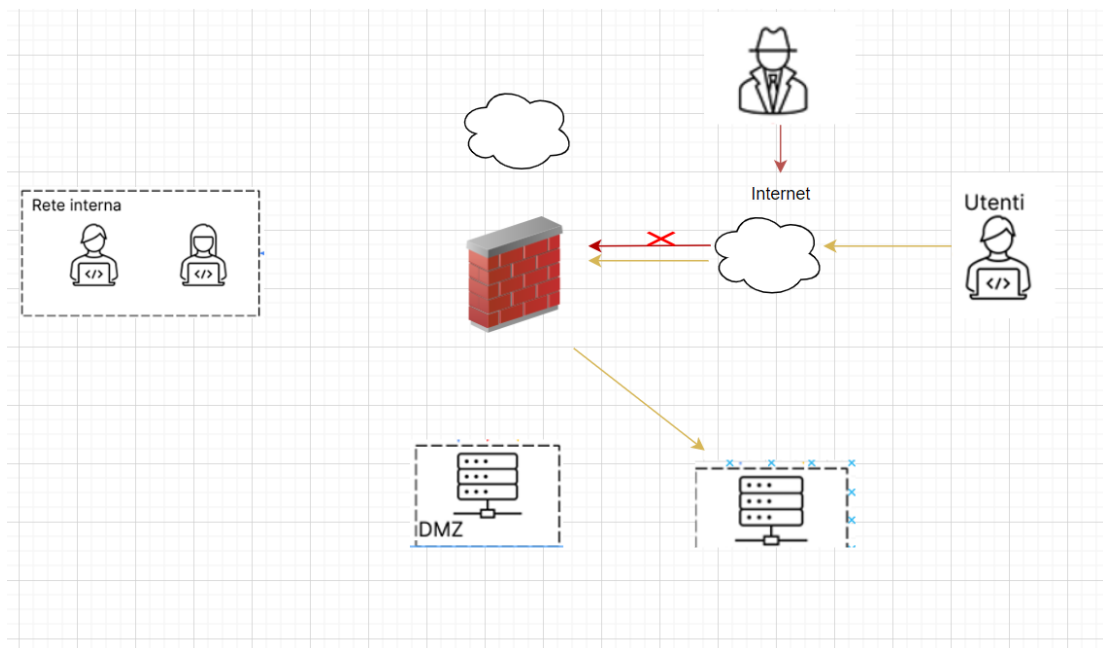
Con un SIEM, si possono collezionare i log applicativi che registrano i vari eventi, in modo da individuare qualcosa di sospetto e correlarli tra di loro.



4. Modifica più aggressiva dell'infrastruttura

In maniera ancora più aggressiva, si potrebbe togliere l'accesso ad Internet della rete DMZ, rimuovendo completamente l'elemento affetto dal malware. Questa soluzione è detta *rimozione*.

Di sicuro in questo modo l'attaccante non avrà più accesso a nulla ma è una soluzione molto drastica, da valutare attentamente:



Ancora più drasticamente, si può pensare alla distruzione dei dischi di storage del database su cui si basa l'applicazione. Le tecniche possibili sono:

- **Clear:** i dischi vengono completamente ripuliti dal loro contenuto con tecniche logiche. Si utilizza un approccio di tipo read and write dove il contenuto viene sovrascritto più volte o si utilizza la funzione di factory reset per riportare i dispositivi nello stato iniziale;
- **Purge:** si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili sui dischi;
- **Destroy:** è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.