Floriana Feminò

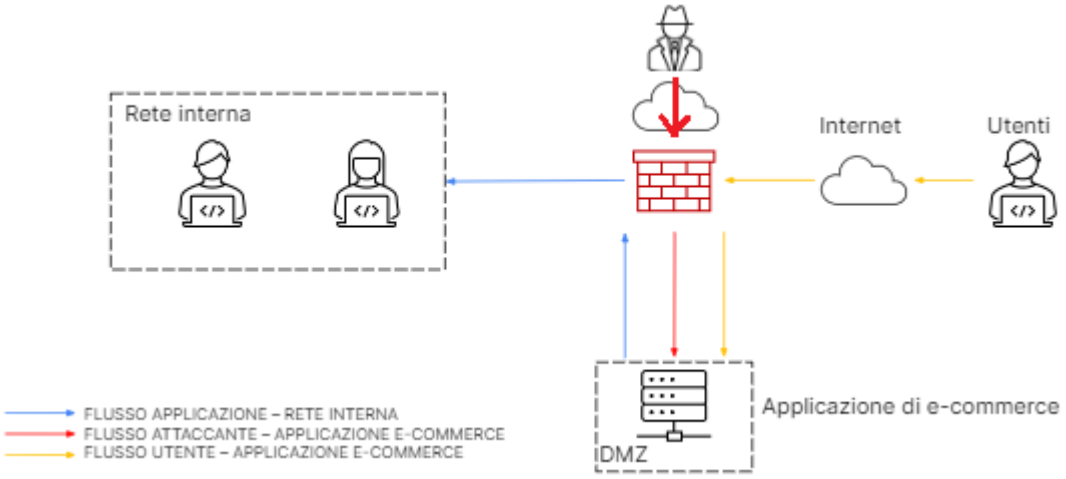
23/12/2022

SECURITY OPERATIONS

Architettura di rete di partenza:

L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet, per poter consentire loro di effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul Firewall, quindi, in caso di compromissione del server, un attaccante potrebbe raggiungere la rete interna.



Tasks:

1. **Illustrazione delle azioni preventive da portare a termine per proteggere l'applicazione web da attacchi di tipo XSS e SQLI**
2. **Calcolo dell'impatto sul business causato dalla non raggiungibilità dell'applicazione web per 10 minuti in caso di attacco DDoS**
3. **Incident response: illustrazione di un piano di contenimento del danno che impedisca ad un malware di propagarsi sulla rete senza rimuovere l'accesso alla macchina infettata da parte dell'attaccante**
4. **Illustrazione di una soluzione completa sull'infrastruttura di rete**
5. **Ulteriori modifiche suggerite all'infrastruttura di rete**

1. Illustrazione delle azioni preventive da portare a termine per proteggere l'applicazione web da attacchi di tipo XSS e SQLI

I servizi di Security Operations sono definiti secondo una logica temporale in relazione al verificarsi di una situazione particolare chiamata **incidente di sicurezza**, ossia un evento che produce un impatto negativo sulla sicurezza, l'integrità e/o la disponibilità di una data risorsa. Nello specifico, si verifica quando occorre una violazione di un sistema informativo o una minaccia imminente di violazione. Esempi di incidenti di sicurezza sono: perdita o **fuoriuscita di dati sensibili**, **intrusione** nei sistemi interni della compagnia da parte di un utente malintenzionato, **attacchi malware**.

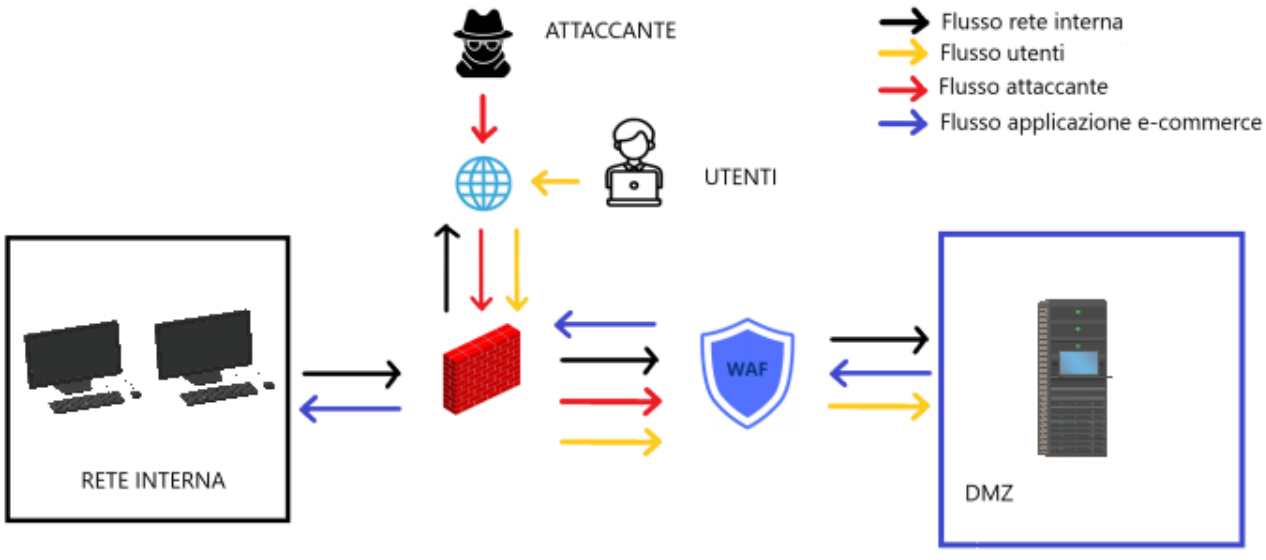
Possiamo distinguere più classi di azioni **a seconda del posizionamento temporale** rispetto all'incidente di sicurezza:

Azioni preventive (= prima dell'incidente): includono azioni di sicurezza adottate per ridurre i rischi di eventi negativi

Azioni correttive e di risposta agli incidenti (= dopo l'incidente): azioni di **rimedio** per risolvere gli incidenti e ripristinare il corretto funzionamento dei sistemi informativi il prima possibile

Le azioni preventive da portare a termine per proteggere l'applicazione web di e-commerce oggetto di analisi odierna consistono nell'implementazione di un **Web Application Firewall** (**WAF**), ossia di un Firewall specifico per applicazioni web che si rivela di fondamentale importanza per **prevenire attacchi di tipo XSS e SQLI**. In caso di tentativi di attacco di tipo Cross-site Scripting Riflesso, ad esempio, il WAF è in grado di rilevare immediatamente la presenza di un payload malevolo in una GET request inviata al web Server.

L'implementazione di un WAF nell'architettura di rete può essere effettuata mel modo seguente:



Come si vede, configurando le policy adeguate il WAF filtra il traffico malevolo (eventuali attacchi di tipo XSS e/o SQLI) di un potenziale attaccante rivolto alla **DMZ** (*Zona Demilitarizzata* che espone servizi accessibili dall'esterno) senza intaccare il normale traffico di rete proveniente dagli utenti della rete interna aziendale e della rete esterna (ossia i clienti della piattaforma di e-commerce).

2. Calcolo dell'impatto sul business causato dalla non raggiungibilità dell'applicazione web per 10 minuti in caso di attacco DDoS

Gli attacchi di tipo **Denial of Service (DoS)** hanno lo scopo di mettere fuori uso un servizio in esecuzione su un sistema, ad esempio un'applicazione web, mediante la trasmissione di un ingente numero di pacchetti ad un server finalizzato a saturare l'utilizzo della CPU e renderla incapace di processare altre richieste. La metodologia più comune di attacco DoS è costituita dal **Distributed DoS** (**DDoS**), che consiste in un attacco DoS inviato verso un target da sorgenti multiple (= una botnet).

Oggetto di esame odierno è il calcolo dell'impatto di un eventuale attacco **DDoS** sul business dell'azienda proprietaria di un'applicazione di e-commerce, considerando una casistica in cui tale attacco provochi l'indisponibilità della piattaforma per 10 minuti e partendo dal presupposto che gli utenti clienti della piattaforma commerciale spendono in media 1500€ al minuto.

Il team responsabile di attuare il piano di risposta agli incidenti di sicurezza è il **CSIRT** (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam). Ad ogni occorrenza di un incidente, il CSIRT deve fornire una **classificazione dell'incidente** basata su diversi fattori, come il **tipo di incidente** e la **criticità**. Mediante quest'ultimo criterio, nello specifico, si intende misurare l'impatto negativo sugli asset della compagnia in termini funzionali e monetari causato da un determinato incidente.

In questo caso, è sufficiente moltiplicare i guadagni percepiti dalla piattaforma di e-commerce al minuto per gli eventuali minuti di inattività:

1500€ * 10 minuti di inattività = **15000€**

Possiamo dedurre quindi che sarebbero sufficienti 10 minuti di inattività del sito web sopracitato per far perdere all'azienda proprietaria dello stesso 15000€ di possibili guadagni. Considerando la figura sottostante, si tratta di un impatto finanziario di criticità media:

CRITICITÀ	IMPATTO SUI SERVIZI (FUNZIONALE)	IMPATTO FINANZIARIO
NESSUNA	Nessun impatto sui servizi e sugli utenti. La compagnia riesce a fornisce tutti i servizi a tutti gli utenti	La compagnia non si aspetta nessuna perdita economica
BASSA	Minimo impatti su servizi ed utenti. Tutti i servizi critici erogati dalla compagnia sono attivi	La compagnia si aspetta un impatto economico limitato (e.g. 10.000€)
MEDIA	La compagnia non riesce ad erogare alcuni dei servizi critici o parte di essi ad un sottoinsieme limitato di utenti	La compagnia si aspetta un impatto economico non indifferente (e.g. 10.000 / 500.000€)
ALTA	La compagnia non riesce ad erogare servizi critici per tutti gli utenti	La compagnia si aspetta un grosso impatto economico (e.g. >500.000€)

3. Incident response: illustrazione di un piano di contenimento del danno che impedisca ad un malware di propagarsi sulla rete senza rimuovere l'accesso alla macchina infettata da parte dell'attaccante

Il processo di **incident response** (= risposta agli incidenti di sicurezza) di articola in diverse fasi:

1) Preparazione
2) Rilevamento ed analisi
3) Contenimento, eliminazione e recupero
4) Attività post-incidente

In questa attività, ci focalizzeremo sulla **terza fase** del processo di incident response e prenderemo in analisi una casistica in cui un attaccante sia riuscito ad infettare la web application tramite malware.

Il primo step della terza fase di un piano di incident response è il **contenimento del danno** causato dall'incidente di sicurezza, da effettuarsi nel minor tempo possibile onde evitare il propagarsi della minaccia su ulteriori sistemi, applicazioni e asset aziendali oltre quello/i già colpiti. La finalità di tale processo è isolare l'incidente – in modo da non creare ulteriori danni a reti/sistemi – riducendo dunque l'impatto causato dall'incidente. Le tecniche utilizzate a tale scopo sono:

- Segmentazione
- Isolamento
- Rimozione

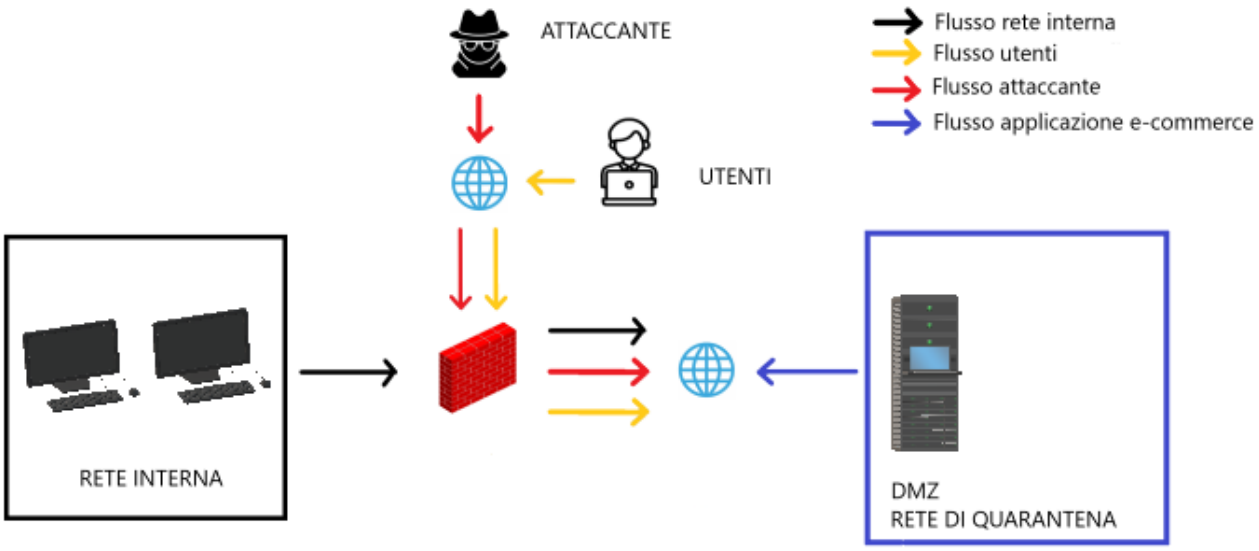
Vogliamo adottare una tecnica di contenimento che impedisca al malware in oggetto di propagarsi sulla rete, ma senza rimuovere l'accesso alla macchina infettata da parte dell'attaccante, pertanto sceglieremo la tecnica di isolamento.

Tecnica di isolamento

Si tratta di una tecnica adottata in quei casi in cui una semplice **segmentazione** della rete (= suddivisione della stessa in diverse sottoreti LAN o VLAN tramite subnetting) non sia abbastanza sicura da far considerare conclusa la fase di contenimento. Quando è necessario un contenimento maggiore, si ricorre alla tecnica dell'**isolamento**: si effettua la **completa disconnessione** del sistema infetto dalla rete interna, allo scopo di restringere ancor più l'accesso alla suddetta rete da parte dell'attaccante. In questo scenario, l'attaccante **ha ancora accesso al sistema infetto tramite la rete Internet**: infatti, l'isolamento costituisce una tecnica spesso utilizzata per raccogliere più informazioni possibili circa l'attacco in corso (ad esempio tramite operazioni di monitoraggio del

traffico di rete) e l'attaccante in questione senza mettere a repentaglio gli asset dell'intera compagnia.

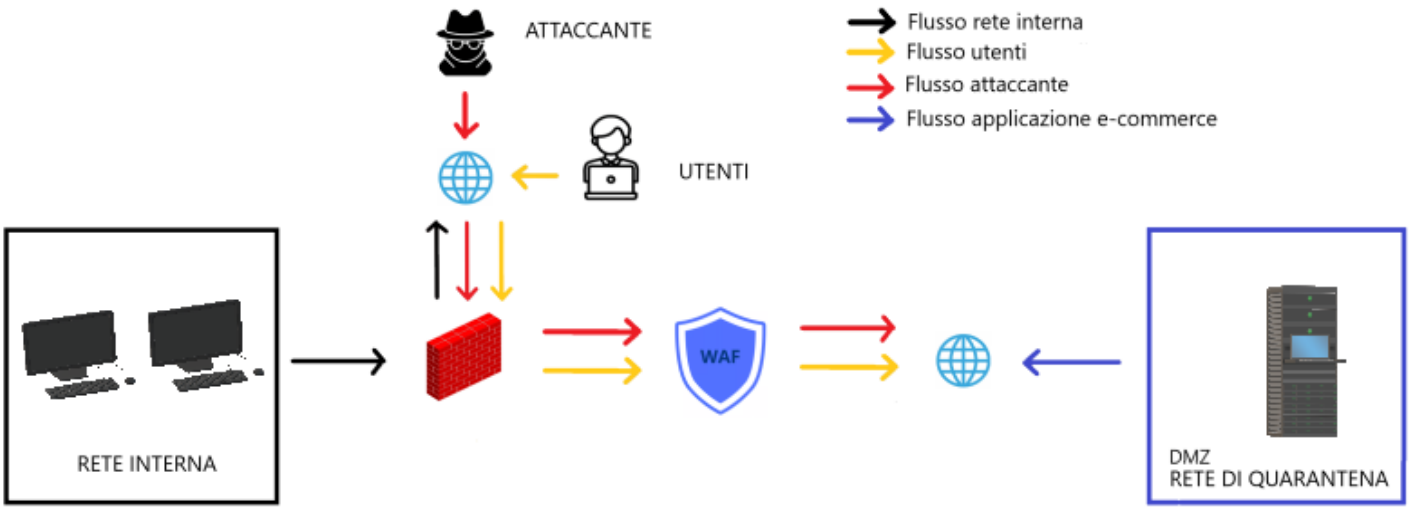
Si può procedere all'implementazione della tecnica appena descritta nel modo seguente:



Come si può notare, la DMZ è **ancora connessa ad internet**, ma non è più in comunicazione con la rete interna. Questo ci darà l'occasione di poter effettuare tutte le analisi del caso sul traffico malevolo in arrivo sulla web application infetta.

4. Illustrazione di una soluzione completa sull'infrastruttura di rete

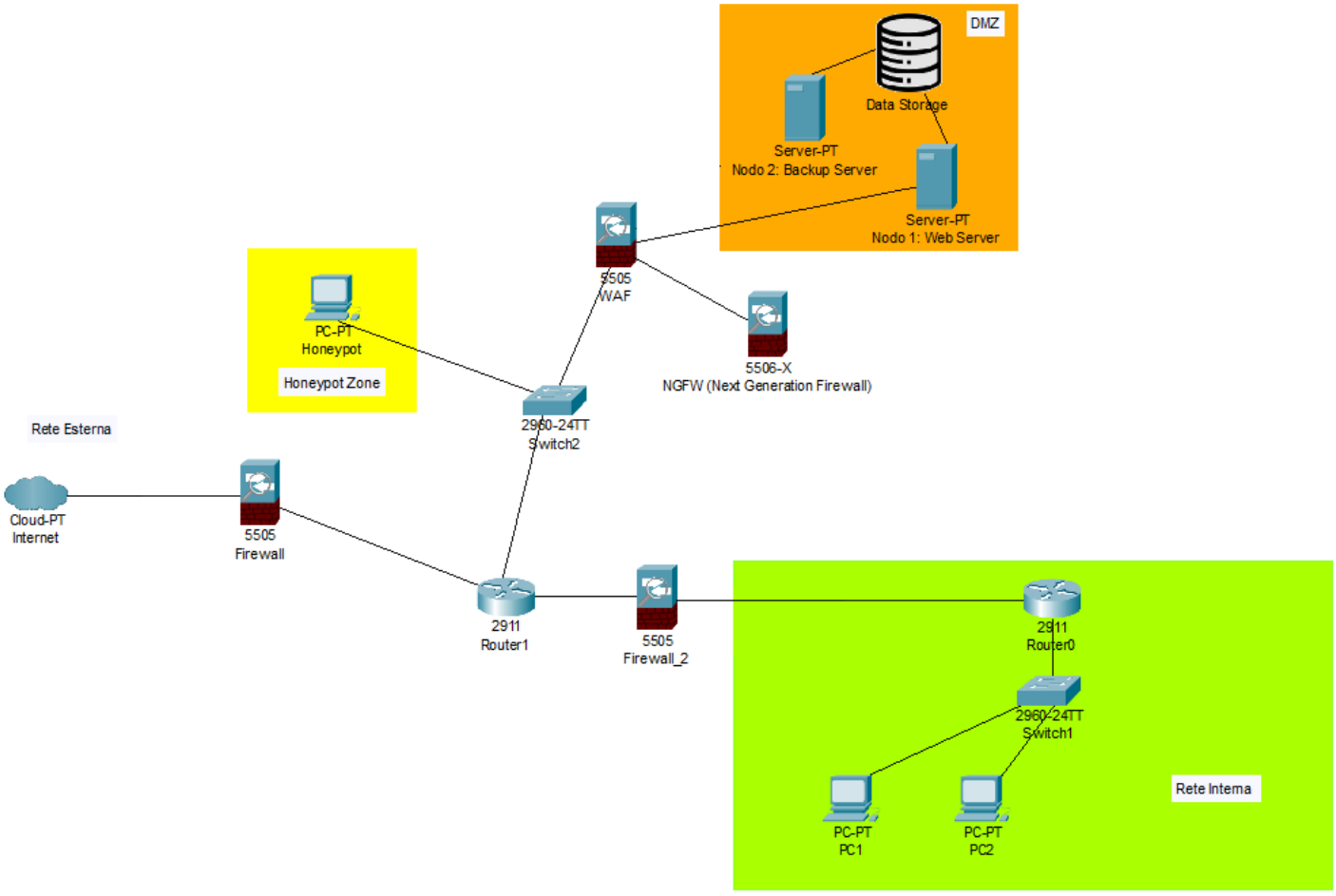
Per una gestione ottimale degli incidenti di sicurezza, può essere utile adottare una soluzione completa che include le tecniche e gli strumenti difensivi adottati finora, come quella proposta nella figura sottostante:



Come è possibile notare, è stato implementato un WAF (già incluso nella prima soluzione proposta) per preservare l'applicazione web da XSS e SQLI, mantenendo la scelta di isolare la DMZ dalla rete interna, ponendola su una rete di quarantena; sia la rete interna che la DMZ hanno accesso ad Internet.

5. Ulteriori modifiche suggerite all'infrastruttura di rete

Infine, si suggerisce l'adozione di un'infrastruttura di rete adeguatamente fornita di ulteriori appropriati elementi difensivi, come proposto nella figura sottostante:



Composizione dell'architettura di rete

Rete Interna – network ad uso esclusivo dei dipendenti, in grado di comunicare sia con la web application che con la rete Internet.

DMZ (Demilitarized Zone) – ospita al suo interno il **Web Server** principale ed un **Backup Server** per assicurare la **ridondanza** e la resilienza dell'infrastruttura. I due Server costituiscono i nodi all'interno di un meccanismo di **failover cluster**: si tratta di una struttura che include due o più Server che condividono un sistema di **data storage**. Questa strategia permette l'operatività dell'intero sistema anche a fronte di un errore su uno dei due Server: qualora il Web Server principale smettesse di funzionare (ad esempio in caso di attacco DDoS), il secondo Server (indicato come "Nodo 2" del cluster) verrebbe promosso a nodo attivo, ossia prenderebbe il suo posto come server principale tramite un processo automatico chiamato, appunto, *failover*.

Il traffico di rete verso il Web Server viene processato da un **Web Application Firewall** (**WAF**) e da un **Next Generation Firewall** (**NGFW**) in parallelo, il quale include al suo interno un sistema **IDS** (*Intrusion Detection System*) che analizza il traffico di rete alla ricerca di eventuali intrusioni malevole. I NGFW includono più funzionalità di analisi rispetto ai comuni Firewall: permettono ad esempio il controllo dei flussi basati sull'utente che effettua la connessione, sull'applicativo utilizzato ed altro ancora.

Rete Esterna – composta da utenti esterni che accedono alla piattaforma e-commerce del Web Server. Il traffico proveniente da client esterni verrà inizialmente analizzato e gestito da un Firewall e, prima di poter raggiungere il Web Server, sarà ulteriormente oggetto di controlli da parte dai dispositivi di sicurezza già menzionati.

Honeypot – dispositivo "esca" le cui vulnerabilità sono deliberatamente esposte allo scopo di indurre attacchi da parte di ipotetici attaccanti, per carpire informazioni riguardo i suddetti e studiarne il modus operandi.