REPORT 23/12/2022 LORENZO SCORBAIOLI

TASK:

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

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 1.500 €** sulla piattaforma di e-commerce.

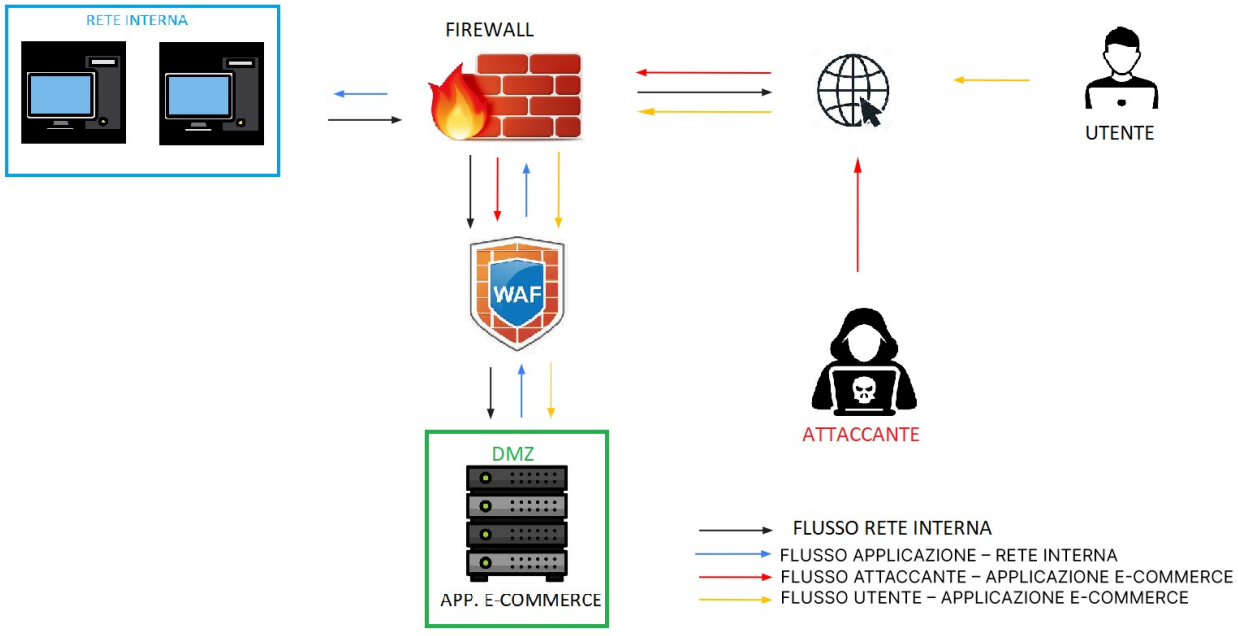
3. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response

5. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo)**

PUNTO 1:

Dalle nostre conoscenze teoriche sappiamo che un ottimo metodo per impedire a un malintenzionato di attuare un attacco SQLi e XSS è quello di installare un Web Application Firewall. Essi aiutano a proteggere le applicazioni distribuite nel cloud pubblico, on premise e in ambienti multicloud con controlli dell'accesso basati sui dati di geolocalizzazione, sulla lista di inclusione e sugli indirizzi IP in backlist, sull'URL HTTP (Hypertext Transfer Protocol Uniform Resource Locater) e sull'intestazione HTTP. Inoltre filtra le richieste dannose a un'applicazione Web o a un'API. Offre altresì maggiore visibilità sulla provenienza del traffico, consentendo di ottenere maggiore disponibilità delle applicazioni e applicare così al meglio i requisiti di conformità[1]. Qui sotto si può vedere l'immagine in cui sono contenute le modifiche ed implementazioni in modo da migliorare la rete come azione preventiva:



1 https://www.oracle.com/it/security/cloud-security/what-is-waf/

PUNTO 2:

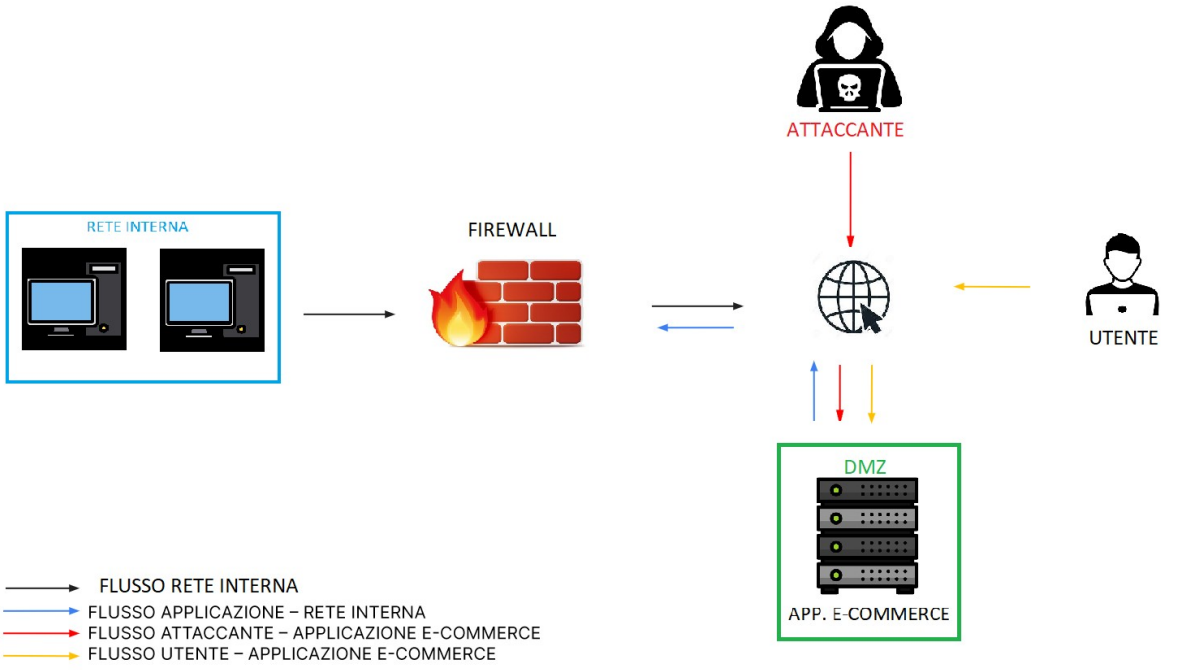
Sappiamo che l'azienda per cui lavoriamo sta subendo un attacco Ddos, cioè un Distributed Denial of Service. La differenze con l'attacco Dos, in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client, è che il traffico dei dati in entrata che inonda la vittima proviene da molte fonti diverse. Sappiamo che ogni minuto gli utenti che accedono all'applicazione Web spendono 1500 Euro. Sappiamo inoltre che a causa dell'attacco DDoS la nostra Web application non è stata raggiungibile per 10 minuti. Quindi l'impatto che l'attacco ha avuto sul nostro business a livello quantitativo è dato da:

1500 €/m * 10 m = 15000 €

Qundi l'impatto dal punto di vista finanziario dell'attacco DDoS sulla nostra azienda equivale a un danno di 15000 €. Mentre l'impatto dal punto di vista funzionale sui servizi ha impedito alla compagnia di erogare parte dei suoi servizi ad un sottoinsieme limitato di utenti. Ciò lo fa rientrare nella categoria di incidenti di criticità media.

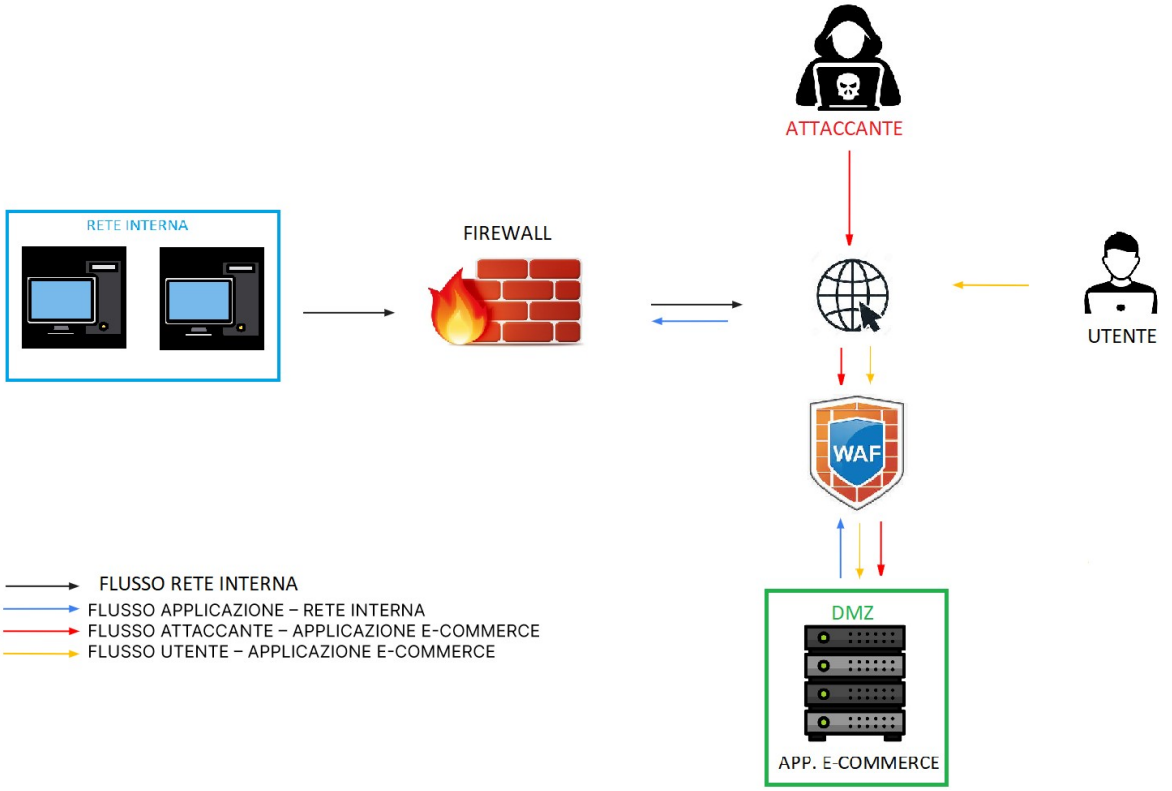
PUNTO 3:

Sappiamo che la nostra applicazione web è stata infettata da un malware. Data come priorità che la diffusione di questo malware non avvenga nella rete interna, senza essere interessati al rimuovere l'accesso dell'attaccante alla macchina infetta, ho deciso di adottare la tattica dell'isolamento ai fini della fase di contenimento, così da ridurre l'impatto del malware:



Nell'immagine qui sopra possiamo vedere come la nostra Web application, inserita all'interno della DMZ, è sempre connessa a internet e quindi l'attaccante può continuare ad averne l'accesso. Tuttavia il firewall viene aggiornato con nuove policy in modo tale che esso non permetta più la comunicazione tra la rete interna e la web application infetta.

PUNTO 4:



Nell'immagine qui sopra possiamo vedere come il Web application server sia stato posto in isolamento in quanto, nonostante la protezione del Web Application Firewall da attacchi SQLi e XSS, sia stato colpito da un malware. L' attaccante continua ad avere l'accesso al server ma il server viene fermato dal Firewall perimetrale impedendogli di comunicare con la rete interna dell'azienda.

PUNTO 5: