EPICODE

Andrea Rocca
CSPT0323

Cybersecurity Analyst

Week 20 - W20D4

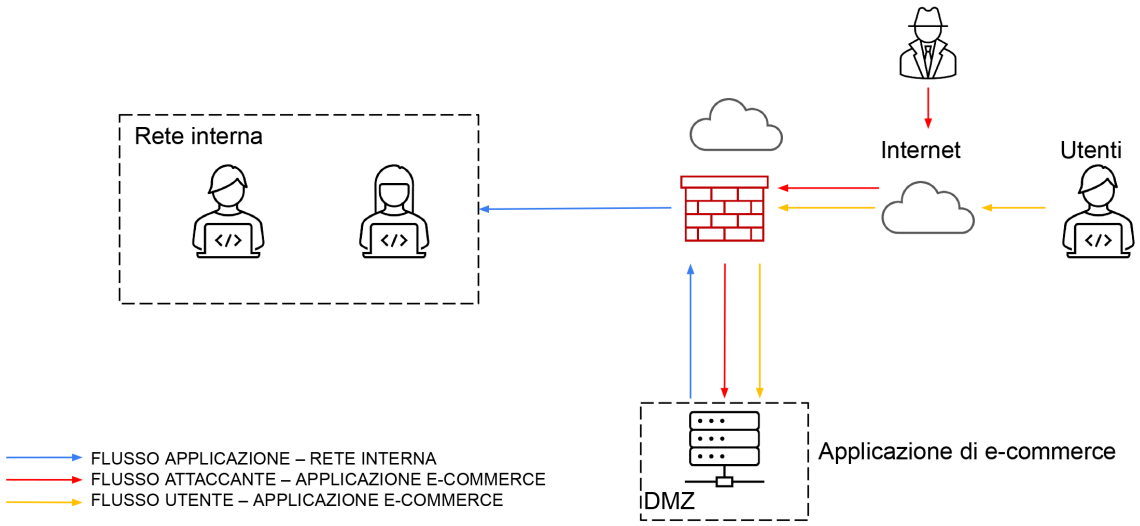
M5: Security Operation & Threat Intelligence

Progetto

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.



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 relativa all'architettura di rete in modo da evidenziare le implementazioni.

Per difendere l'applicazione web da eventuali attacchi SQLi e XSS si potrebbero implementare le seguenti diverse misure:

A) Web Application Firewall (WAF)

Mediante l'integrazione di un WAF, sarebbe possibile ispezionare il traffico in arrivo per bloccare le richieste malevole prima che raggiungano l'e-commerce. Questa soluzione di sicurezza farebbe si, infatti, che ci sarebbe una sorta di "barriera protettiva" tra il traffico Internet in entrata e l'applicazione web, facendo in modo che attraverso un insieme di regole, il WAF sarebbe in grado d'identificare e bloccare tentativi di attacchi comuni, inclusi SQLi e XSS.

I vantaggi relativamente all'uso di un WAF sarebbero inoltre la possibilità di poter essere aggiornato in modo rapido introducendo nuove regole contro vulnerabilità non ancora note (zero day) e la capacità di report dettagliato su eventuali attività sospette.

B) Sanificazione del codice

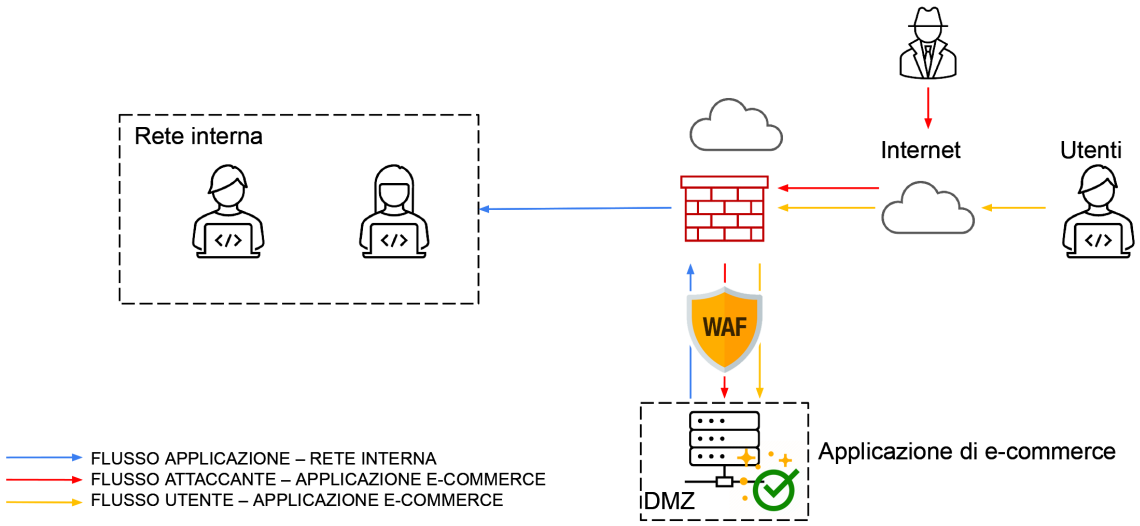
Una seconda eventuale implementazione preventiva potrebbe essere la sanificazione del codice, il processo cioè di pulizia degli input ricevuti dagli utenti per assicurarsi che siano sicuri prima di elaborarli o inserirli nei database dell'e-commerce per prevenire attacchi come SQLi e XSS, dove gli aggressori cercano di iniettare codice malevolo nell'applicazione.

Analisi finali "azioni preventive":

La combinazione di un WAF e di pratiche di sanificazione del codice offrirebbe un approccio di difesa in profondità, proteggendo le applicazioni web da una vasta gamma di attacchi, compresi quelli presi in esame (SQLi e XSS). Mentre il WAF fornirebbe una barriera esterna per filtrare le minacce prima che raggiungano l'applicazione, la sanificazione del codice assicurerebbe che l'applicazione stessa gestisca gli input in modo sicuro, riducendo il rischio di exploit da parte di un utente malintenzionato.

1. Azioni preventive

Architettura di rete



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

Se l'applicazione non è raggiungibile per 10 minuti e ogni minuto in media si generano entrate pari a 1500€, l'impatto economico stimato sarebbe di 15000€.
A considerazione di ciò, si potrebbero attuare diverse soluzioni per evitare di subire un attacco di tipo DDoS o quantomeno cercare di limitarlo:

A) Uso di servizi CDN

L’utilizzo di un servizio CDN come ad esempio Cloudflare, potrebbe essere utile sia a distribuire il carico, sia a mitigare gli attacchi DDoS.
Una CDN funziona appunto ripartendo il traffico tra diversi data center dislocati in tutto il mondo, riducendo il carico su un singolo punto e migliorando la disponibilità di accesso ai contenuti. Inoltre, nel nostro caso, Cloudflare servirebbe soprattutto ad analizzare il traffico verso il nostro e-commerce per identificare e bloccare il traffico sospetto prima che raggiunga l'infrastruttura presa in esame, offrendo per l’appunto protezione contro gli attacchi DDoS, sfruttando la sua vasta rete per assorbire e disperdere gli attacchi.

B) Aumento della banda

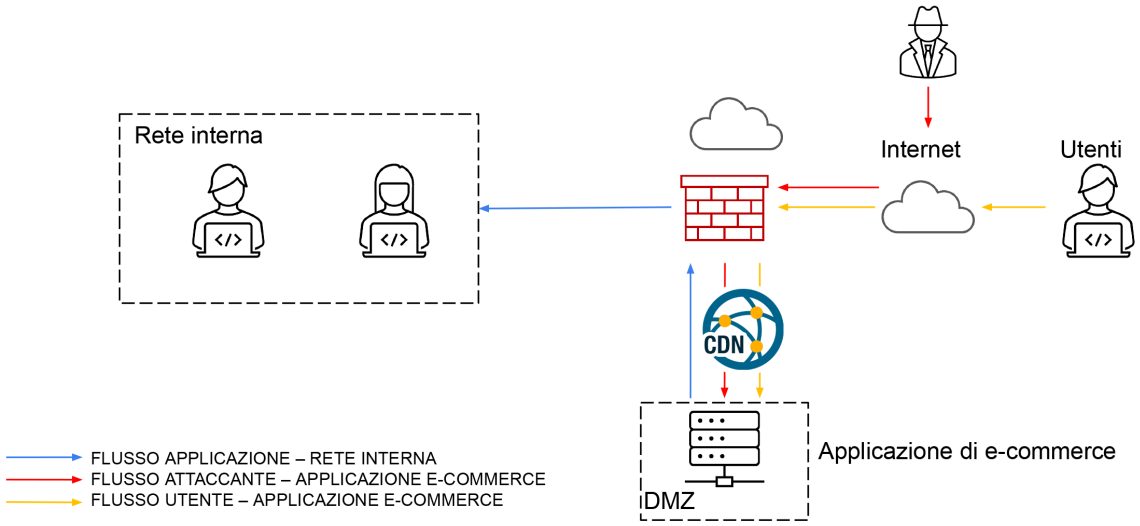
Una supplementare strategia per mitigare gli attacchi DDoS potrebbe essere quella di aumentare la capacità di banda. Avere a disposizione più banda di quanto normalmente necessario offrirebbe una sorta di “ammortizzatore” contro l'aumento improvviso del traffico causato da un DDoS, facendo in modo che l’infrastruttura da proteggere sia in grado di assorbire una quantità maggiore di traffico malevolo prima che gli effetti dell'attacco diventino critici.

Analisi finali “Impatti sul business”:

Bisogna considerare che, sebbene l'aumento della banda possa fornire un “cuscinetto” contro gli attacchi DDoS, non sarebbe una soluzione completa di sicurezza ma eventualmente piuttosto una strategia da integrare con altre misure come l’implementazione di servizi CDN (dettagliati nel punto A) per una protezione complessiva più efficace.

2. Impatti sul business

Architettura di rete



3. 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.
Modificate la figura relativa all’architettura di rete con la soluzione proposta.

In uno scenario di questo tipo sarebbe possibile esaminare due approcci per gestire la situazione mantenendo l'obiettivo di non rimuovere l’accesso all'attaccante:

A) Isolamento della macchina infettata

In questo caso l'obiettivo sarebbe isolare la macchina infettata dal resto della rete senza interrompere la connessione all'attaccante. Questo approccio consisterebbe nel separare il sistema infetto creando una rete ad hoc (chiamata generalmente “rete di quarantena”). Con le dovute configurazioni a livello network, il malware risulterebbe così separato dal resto della rete ed incapace di riprodursi, lasciando però intatta la connessione internet in modo che l'attaccante non si renda conto dell'isolamento e affinché si possa, implementando strumenti di monitoraggio, registrare tutte le sue azioni per studiarne il comportamento e valutare azioni contro eventuali future minacce.

B) Disconnessione della rete interna

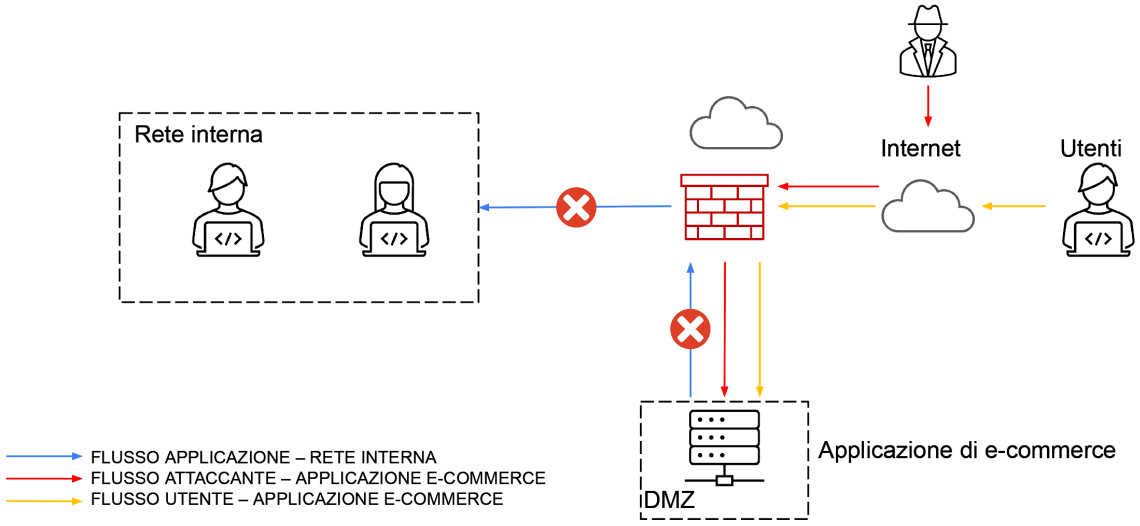
Questo approccio prevederebbe di mantenere attiva la connessione internet della macchina infettata ma di eliminare semplicemente la connessione verso la rete interna. Anche in questo caso l'obiettivo sarebbe di prevenire la diffusione del malware e allo stesso tempo di conservare la possibilità di monitorare l'attaccante e i suoi comportamenti attraverso sistemi di rilevamento e analisi del traffico, mantenendo la macchina infettata sotto stretta osservazione.

Analisi finali “Response”:

La scelta tra i due approcci dipende principalmente dalle esigenze dell’azienda; se quest’ultima dispone delle risorse necessarie (tempo e possibilità di installare nuove infrastrutture), isolare la macchina colpita in una nuova rete “di quarantena” potrebbe essere la scelta migliore. Tuttavia, se l'impatto dev’essere minimizzato in breve tempo senza grande dispendio di risorse, la disconnessione dalla rete interna potrebbe essere sufficiente per gestire la situazione in modo efficace.

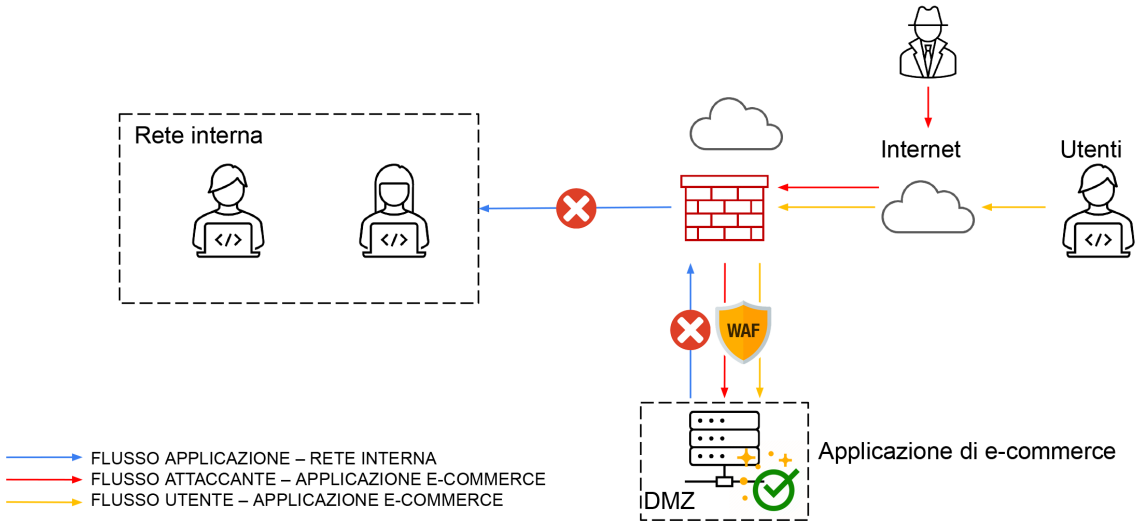
3. Response

Architettura di rete approccio B



4. Soluzione completa

Unire i disegni dell'Azione preventiva e della Response (soluzioni 1 e 3).



5. Modifica «più aggressiva» dell'infrastruttura