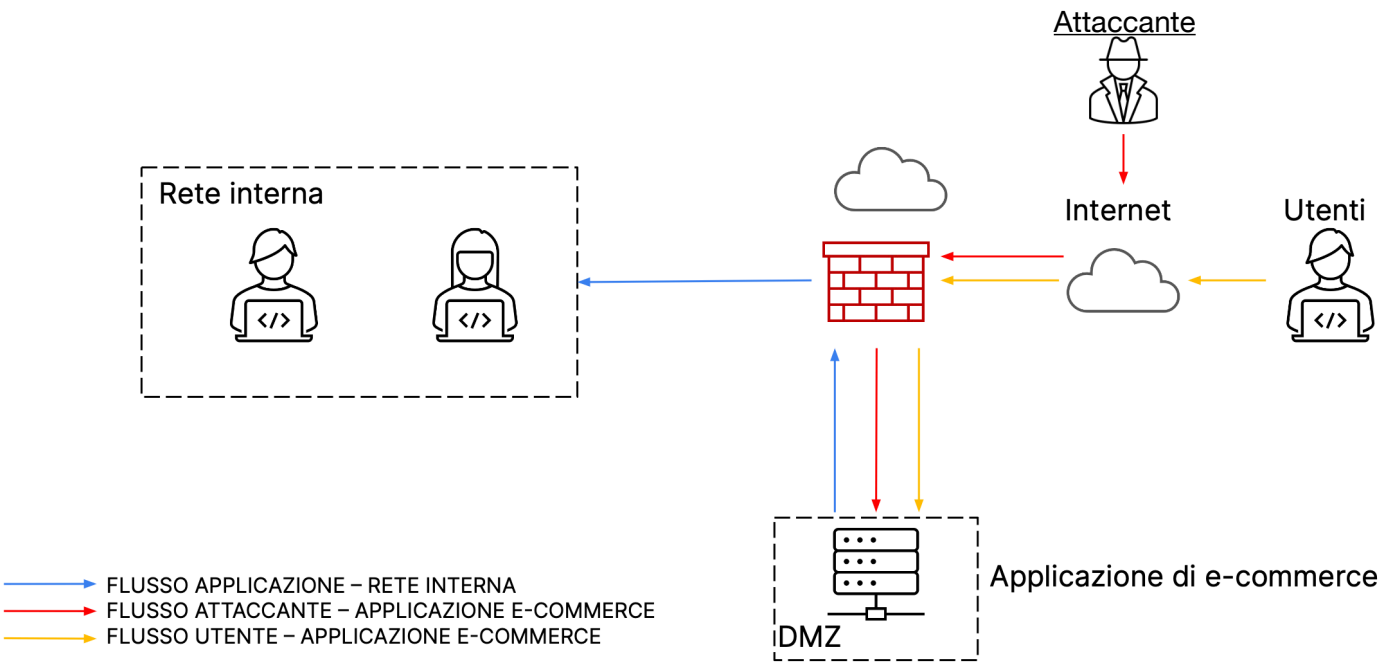


Report di fine mese numero 5 Christian Brenci

1) Azioni preventive

Proteggere il proprio sito da persone malintenzionate o da virus è fondamentale sia per l'esercente che per il cliente, tuttavia non sempre si pensa a come prevenire quest'ultimi per poi pagarne le conseguenze. Oggi vedremo come prevenire o rimediare ad eventuali danni provocati da essi.
La prima cosa da fare per evitare che un malintenzionate possa iniettare del codice malevolo o recuperare informazioni dal nostro sito o server che sia, è implementare una sicurezza perimetrale conosciuta come WAF.
WAF sta per Web application firewall, una tecnologia firewall creata apposta per le web app dove, in quest'ultima, possiamo decidere e controllare le richieste del firewall per vedere chi sta cercando di entrare nel nostro server e con quali mezzi.

Ma da cosa ci protegge?

Da tutte quelle azioni che iniziano un attacco verso di noi come: traffico Internet indesiderato, bot, sql injection(SQLi), denial of service (DoS) a livello applicativo e attacchi XSS. Questa misura di sicurezza non è importante solo per noi ma anche per evitare di rilasciare un malware all'utente o diffonderlo su internet, a 360° è il metodo più sicuro ed efficiente per prevenire attacchi di vario tipo indirizzato da ambedue le parti.

2) Impatti sul business

Nel caso non fosse installata nessuna sicurezza perimetrale o che in qualche modo un utente malevolo fosse riuscito a raggirarla, sarebbe in grado di

recarci un danno, e se quest'ultimo è un attacco di tipo DDOS sarebbe in grado di inviarci un numero ingente di pacchetti da più pc infettati.

Ma come è possibile?

Come già detto, gli attacchi di tipo DOS si presentano inviando ingenti pacchetti verso la vittima, facendo così saturare la nostra CPU, e una volta che quest'ultima sarà al 100% del suo utilizzo non sarà in grado di processare altre richieste, peggio ancora sono gli attacchi DDOS i quali hanno lo stesso identico funzionamento ma con più macchine coinvolte contemporaneamente verso la vittima.
Cosa puo' succedere?
Il tutto dipende da vari fattori ma possiamo riassumerli dicendo:

- Riusciamo ad intercettare l'attacco e fermarlo, oppure spostiamo momentaneamente il problema usufruendo di mezzi a nostra disposizione come un secondo server attivo.
- Non riusciamo ad intervenire in tempo e subiamo il danno.

Prendiamo il secondo caso e analizziamolo, la nostra web app di e-commerce viene attaccata per **10 minuti,** sappiamo che in media in questo lasso di tempo, il guadagno stimato è di 1.500€ al minuto per un totale di 15.000€ circa, ma dobbiamo calcolare anche le spese di eventuali danni portati a componenti hardware nel caso di malfunzionamento o sovraccarico di quest'ultimi e nelle peggiori delle ipotesi anche un rimborso ai clienti di eventuali transazioni non andate a buon fine durante l'attacco. Possiamo dedurre quindi che la spesa per il danno recatoci supera ben oltre le eventuali spese per mettere in sicurezza il nostro server da questo tipo di attacchi.

Quindi cosa fare?

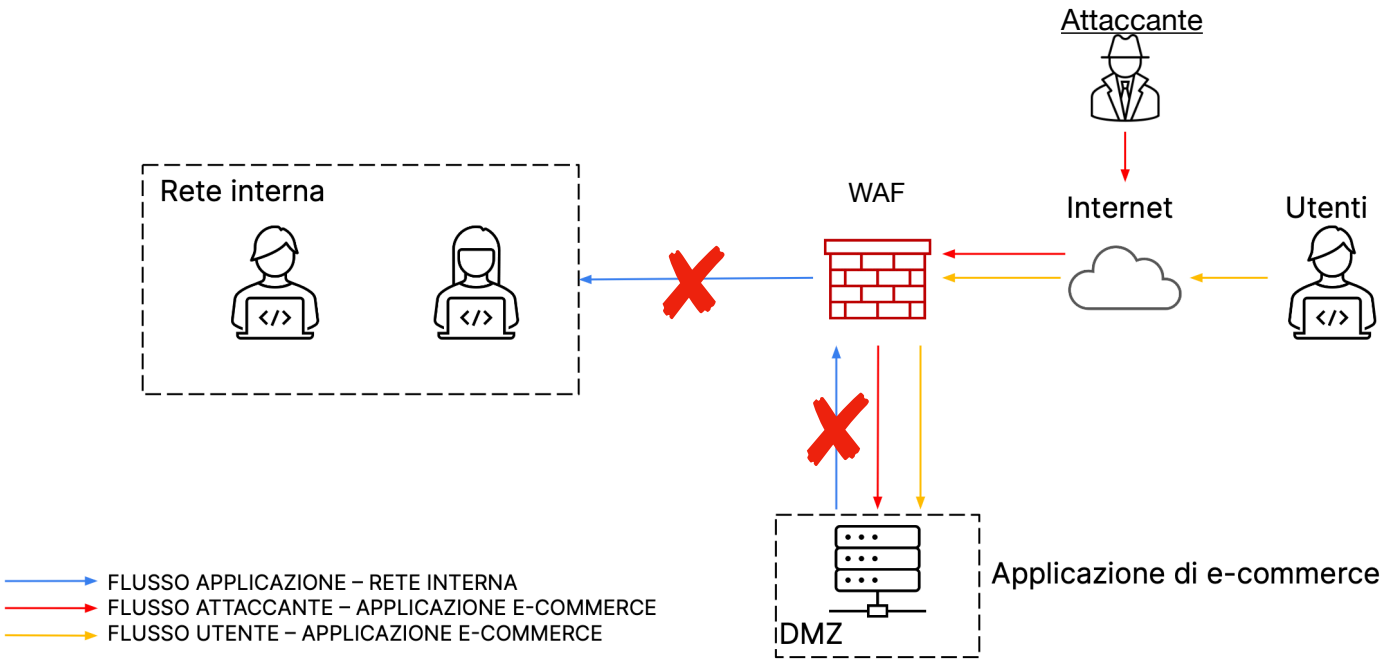
Ci sono molteplici soluzioni ognuna valida al fine di proteggere il nostro sito. La prima cosa da fare come detto precedentemente è installare un firewall WAF per le web Application, questo ci permette di creare una prima protezione da eventuali attacchi esterni, ma se questo non dovesse bastare possiamo inoltre implementare uno o più server CDN (Content Delivery Network) consistono in un gruppo di server situati in diverse localizzazioni nel mondo, chiamate Point of Presence (PoP). Questi punti ridistribuiscono localmente i contenuti dei server memorizzando nella cache i file che non richiedono aggiornamenti regolari, in questo modo anche se siamo vittima di un attacco il nostro sito sarà in grado di continuare a svolgere regolarmente le proprie funzioni senza perdere nemmeno un centesimo. Se prima abbiamo detto che la perdita per soli 10 minuti di un attacco è uguale o superiore ad 15.000 euro, a confronto le spese annuali per proteggere il nostro sito sono nulla a confronto.

Una piccola media impresa all'anno spende circa 5.000 euro per l'installazione e il servizio di una WAF, mentre per quanto riguarda l'installazione di una CDN varia in base alle proprie esigenze, ma comunque facendo una stima si spende annualmente dai 1.000 ai 5.000 euro.
Sappiamo bene che in un anno potremmo essere vittima di piu' attacchi e quindi, per soli 10 minuti, perdere centinaia di migliaia di euro, saremmo anche soggetti alla sfiducia da parte dei clienti e partner, cattiva pubblicità e molto altro.
La scelta migliore è applicare le procedure di sicurezza precedentemente elencate.

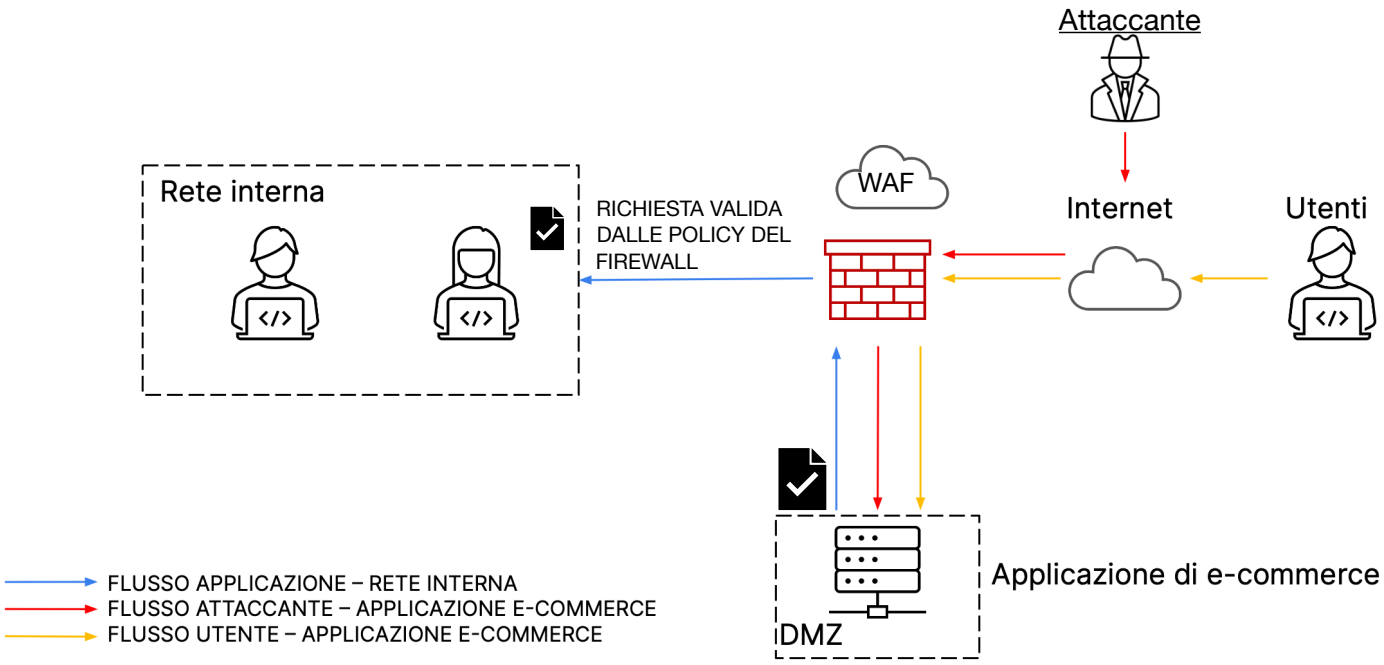
3) Response

Sappiamo che un malware ha infettato la nostra web app, la nostra priorità è quella di non permettere al malware di propagarsi nella nostra rete, e non è nei nostri interessi togliere l'accesso dell'attaccante sulla nostra macchina infettata.
Dobbiamo aggiornare le policy del firewall in modo tale da bloccare l'accesso tra la rete interna e il DMZ.

Questo è lo schema del *terzo* quesito.



Questo è lo schema del *primo* quesito.



Questo è lo schema del *quarto* e del *quinto* quesito.