Report 16 Settembre 2022

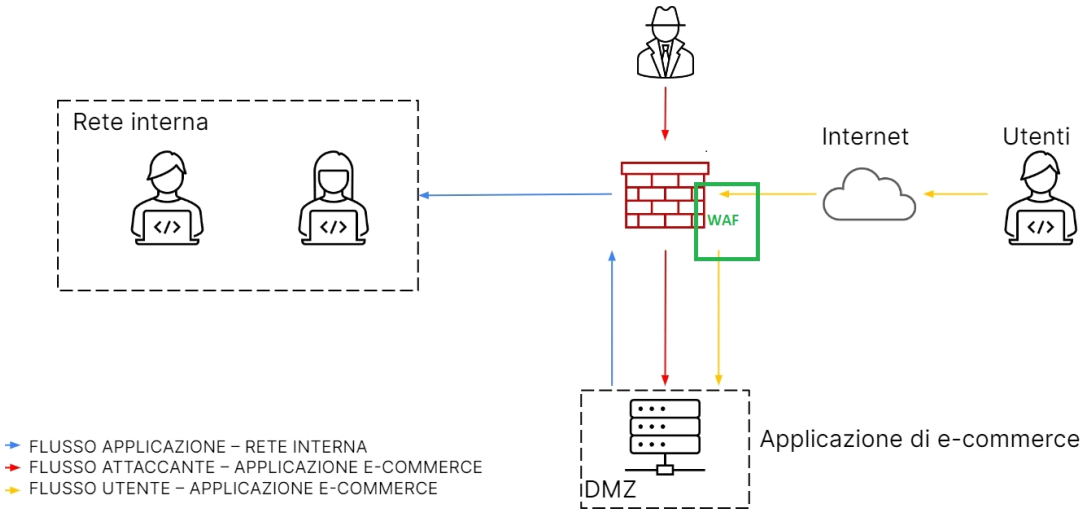
Azioni preventive:

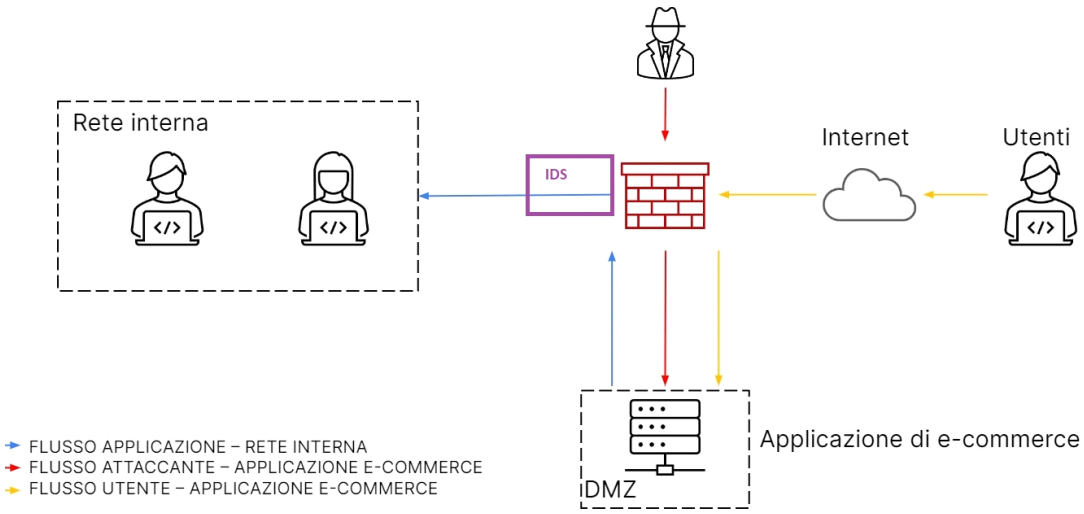
Un azione che potrebbe prevenire un attacco (in particolare SQLi e XSS)sulla nostra web app da un utente malintenzionato, sarebbe quella di inserire ulteriori sistemi perimetrali di sicurezza, come gli IDS e i WAF.

IDS: (Intrusion Detection System) controlla continuamente la sicurezza della rete, identificando in anticipo gli attacchi ai computer e alle reti informatiche.

WAF: (Web Application Firewall) si tratta di un firewall aggiuntivo che si occupa di aumentare la protezione delle applicazioni web aziendali. Si occupano principalmente di intercettare e realizzare il traffico HTTP.

Nelle immagini sottostante, abbiamo inserito il **WAF** tra il applicazione e-commerce e l'utente e l'IDS tra la rete interna e il firewall così da garantire una protezione.





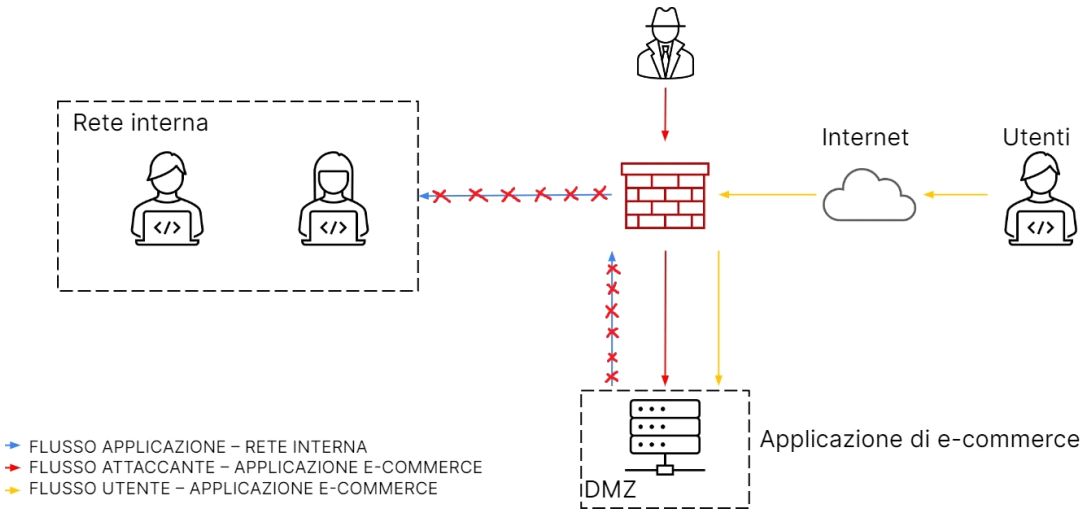
Impatti sul buisness:

Dal momento in cui l'azienda guadagna 1.500€ al minuto e l'applicazione non è raggiungibile per 10 minuti, l'azienda andrà a perdere 15.000€ (1.500x10=15.000).

Quindi, dopo aver fatto questo calcolo , possiamo dedurre che la criticità sia media, ovvero che la compagnia non riesce ad erogare alcuni dei servizi critici, oppure solo una parte, ma non a tutti gli utenti.

Response:

Dobbiamo settare in modo differente il firewall così che la DMZ e la rete interna non comunichino tra loro così da poter evitare un eventuale attacco di questo tipo



Disegno finale della rete: