PROGETTO S9L5

GIORGIO TROVESI

Introduzione:

Il progetto odierno simula alcune situazioni che un’azienda dovrebbe affrontare nel corso della sua attività, nello specifico:

- ***Azioni preventive:*** sono quelle operazioni di sicurezza che vengono adottate ed implementate anticipatamente e preventivamente per ridurre i rischi di eventi negativi;

- ***Impatti sul business (BIA):*** si tratta di uno dei principali step del Business continuity plan (BCP) e ha lo scopo di indentificare risorse critiche e principali minacce alle quali un’azienda è esposta, oltre che misurare probabilità e valore d’impatto nel caso dovessero verificarsi;

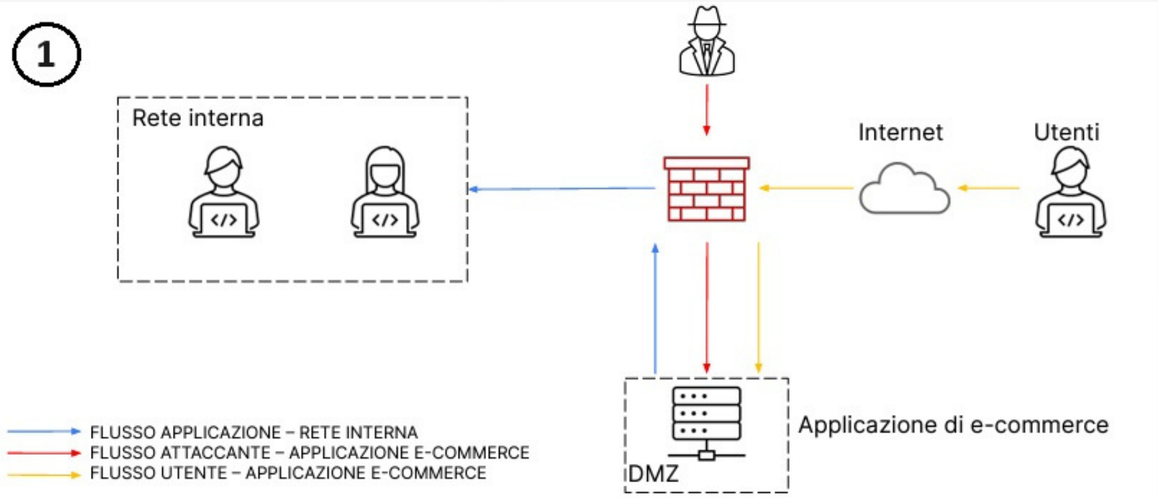
- ***Incident response:*** è un processo che l’azienda, solitamente il CSIRTs, deve attuare qualora si verificasse un incidente di sicurezza, è composto da diversi fasi e devono essere affrontate correttamente onde evitare che venga compromesso il business dell’azienda.

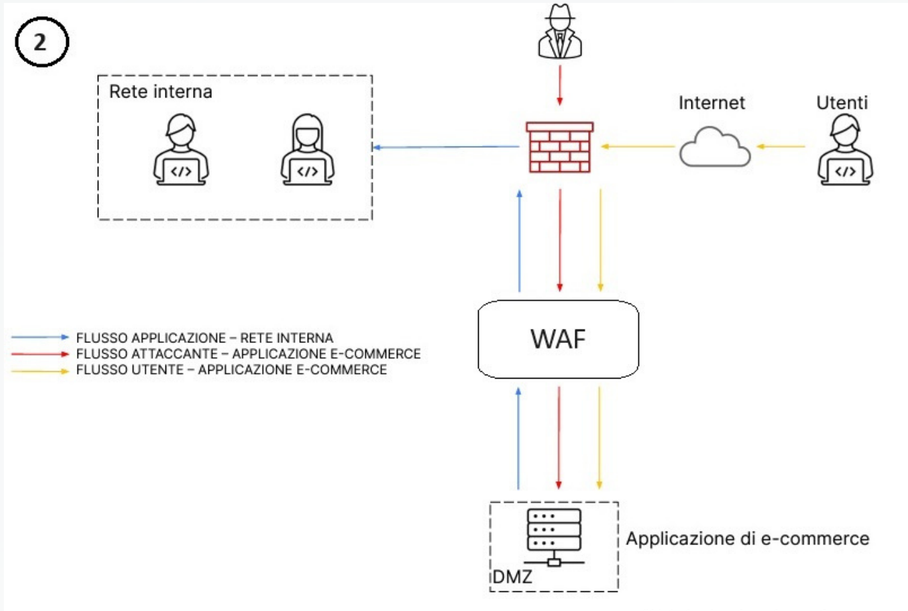
Azioni preventive:

L’azienda che dispone di un’architettura di rete come visibile nella figura 1 deve implementare delle azioni preventive affinché possa difendere l’applicazione web da attacchi SQLi oppure XSS.

Nella figura 2 è possibile constatare l’aggiunta del WAF, ovvero un Firewall per applicazioni web che consente di proteggere, in questo caso la nostra applicazione di E-commerce, da attacchi dannosi quali SQLi, XSS, DoS e traffico indisiderato quali Bot, tramite la gestione corretta delle regole e l’utilizzo di funzioni come quella di verifica Captcha.

Altre azioni che si potrebbero attuare per evitare questi attacchi consistono in un ulteriore controllo sugli input per evitare che un utente possa “iniettare” del codice malevole e il mantenere aggiornati costantemente i server e le applicazioni presenti nella DMZ.





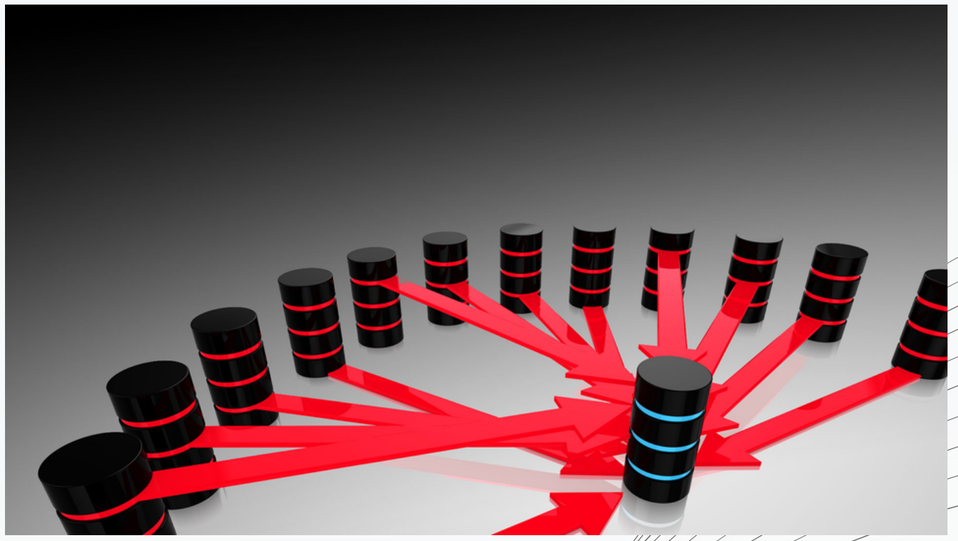
Impatti sul Business:

Si presuppone che l’applicazione web subisca un attacco DDOS dall’esterno che rende l’applicazione non raggiungibile per 10 minuti.

Considerando che gli utenti di media per ogni minuto spendono sulla piattaforma 1500€, il valore d’impatto sul business di quest’attacco è di 15000€.

Considerando che in base a un report report trimestrale di Kaspersky sono stati segnalati quasi 57mila attacchi DDOS e Cloudfare ha constatato un aumento del 67% rispetto al 2022, consigliamo all’azienda di prendere provvedimenti a riguardo quali possono essere:

- l’utilizzo di Firewall, WAF, NGWF;
- configurare dei limiti sulle connessioni;
- distribuire il carico del traffico;
- effettuare dei test sulla sicurezza;
- mantenere aggiornati i software.

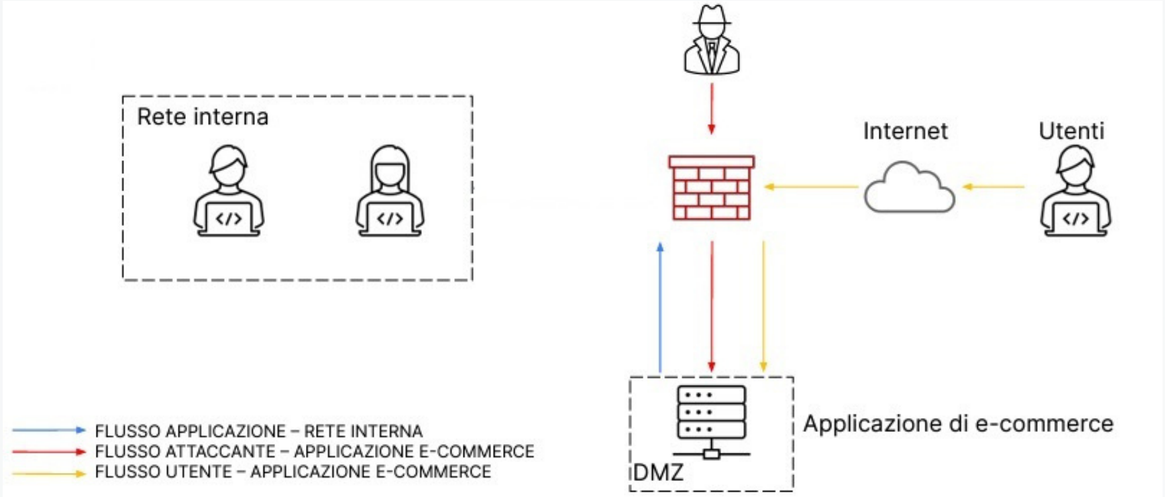


Incident response:

L’applicazione web è stata infettata da un malware, la nostra priorità è che il malware non si propaghi sulla nostra rete interna mentre non siamo interessati a rimuovere l’accesso da parte dell’attaccante alla macchina infetta, modificare l’architettura come richiesto.

Come si evince dalla figura sottostante per ridurre gli impatti del codice malevolo è stata effettuata un’operazione di isolamento mantenendo l’applicazione web connessa a internet.

Questa pratica però è sconsigliabile perché mette a serio rischio i nostri clienti che continueranno ad utilizzare l’e-commerce e piuttosto sarebbe stato utile prevedere questo rischio utilizzando dei sistemi di sicurezza quali Firewall, IPS, software anti-malware aggiornati e predisponendo una tecnica di ridondanza per un secondo server di e-commerce che sarebbe diventato operativo permettendo la rimozione di quello infetto.



CONCLUSIONI:

Come abbiamo visto oggi è importantissimo che un’azienda attivi delle azioni preventive e predisponga un solido piano per la continuità del proprio Business, per ridurre il più possibile i rischi e il relativo impatto in caso di eventi negativi.
E’ altrettanto importante che qualora si verificassero l’azienda si faccia trovare pronta e organizzata.