REPORT ESERCIZIO PRATICO

In questo report verranno illustrate le seguenti soluzioni ai seguenti 3 problemi

1. Azioni preventive agli attacchi sql injection e xss cross site scripting a una webapp
2. Calcolo impatto economico sulla non raggiungibilità di un servizio e-commerce per via di un attacco DDOS
3. Remediation di una web app infettata da malware.

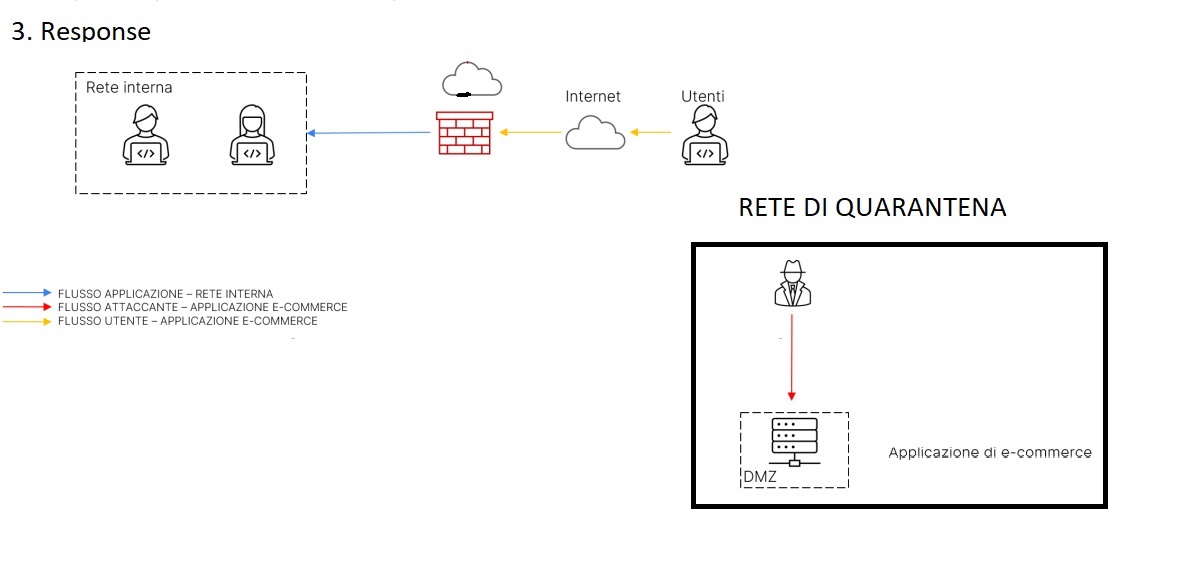
1.Come azione preventiva da attacchi Sqli e Xss è consigliabile aggiornare il javascript all’ultima versione inserendo misure di sicurezza essenziali come i flag http only che non permette di accedere ai cookie tramite script lato client, impedendo di rivelare il cookie di sessione a un utente non autorizzato.

il flag SameSite che impedisce gli attacchi di tipo Cross site per prevenire altre attività ingannevoli con lo scopo di usare il browser stesso dell’utente senza bisogno di rubare il cookie di sessione.

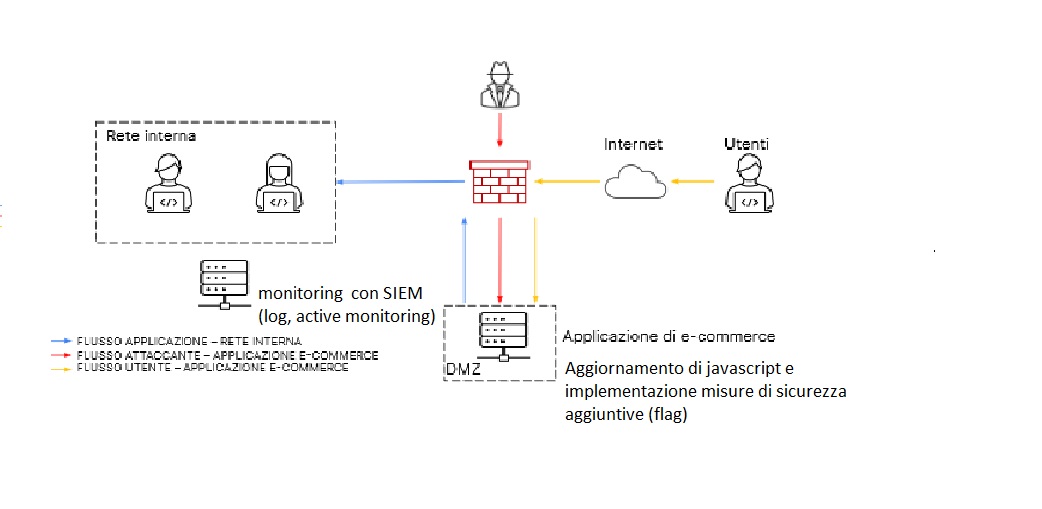
Infine l’attributo secure, che forza i browser web a forzare l’uso del protocollo https, che rendono i cookie illegibili dall’attaccante.

2.L’impatto economico nella non raggiungibilità dell’ e-commerce ammonta ai 15.000 euro totali per 10 minuti, ricavati facendo il seguente calcolo: 1.500 euro al minuto persi per un’interruzione di 10 minuti dell’applicazione e-commerce ovvero 1.500x 0,1= 15.000 euro di perdite per 10 minuti di inattività.

3.La soluzione per evitare che il malware si propaghi nella rete è di isolare server web e l’attaccante dalla rete limitandoli in una rete di quarantena.

1. Figure azioni preventiva e response

Nella seguente figura sono stati collocati l’attaccante e l’applicazione e-commerce in una rete di quarantena in modo da poter analizzare la metodologia di attacco dell’attaccante e la successiva rimozione del malware.



In questa figura invece, vengono illustrati le azioni di prevenzione di attacco tramite sqli\xss.