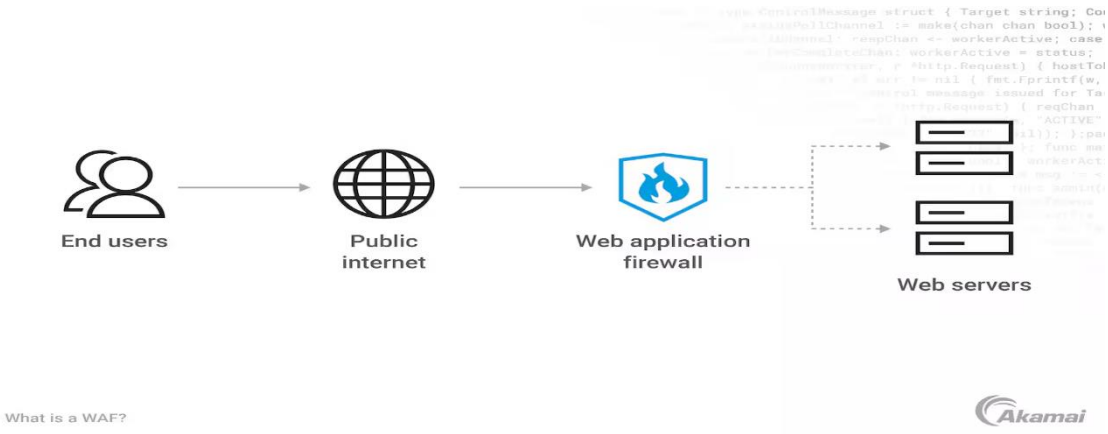
W20D4

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 in modo da evidenziare le implementazioni

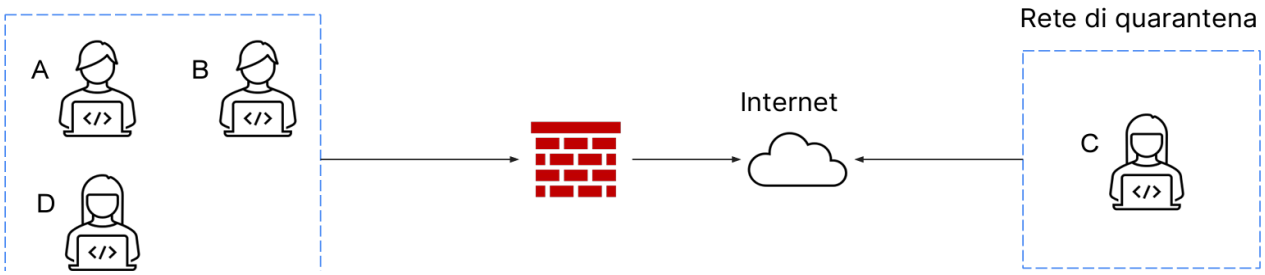
    1. Aggiornamento del software : aggiornare il software di gestione del servizio puo aiutare a prevenire attacchi SQLI E XSS
    2. Validazione dell input: l input dell utente dovrebbe essere sempre validato prima di essere utilizzato. Questo può aiutare a prevenire attacchi SQLi in cui un utente malintenzionato cerca di manipolare le query SQL.
    3. Codifica dell ouput **:** Questo può aiutare a prevenire attacchi XSS in quanto rende inoffensivi i caratteri speciali che potrebbero essere utilizzati per iniettare codice maligno.
    4. Utilizzo di HTTPOnly e flag Secure per i cookie: Questo puo aiutare a prevenire attacchi XSS rubando i cookie di sessione.
    5. Implementazione di Content Security Policy (CSP): Questo aiuta a prevenire attacchi XSS limitando le risorse che possono essere caricate dalla pagina.
    6. Utilizzo di prepared statements o parametrizzazione delle query: Questo può aiutare a prevenire attacchi SQLi in quanto i valori dell'input dell'utente vengono gestiti come stringhe letterali e non come parte della query SQL
    7. Web Application Firewall (WAF) : dei dispositive di sicurezza dedicati per proteggere le applicazioni da attacchi quali SQLi e XSS



come vediamo nella figura il dispositivo di protezione filtra il traffico dati compreso di input utente , prima che raggiungano i web server e/o la rete interna aziendale .

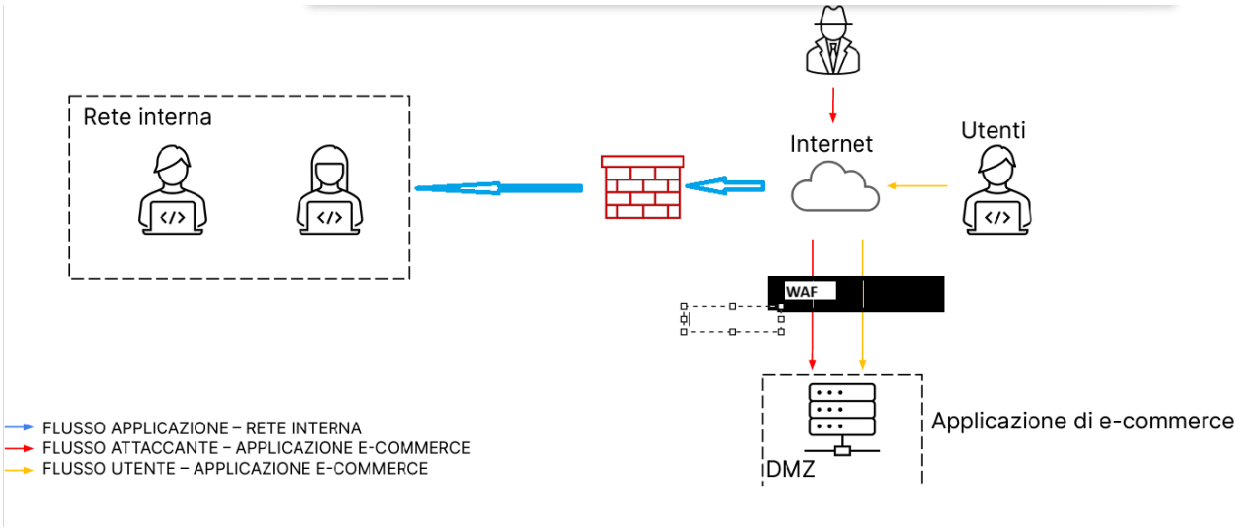
2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica
   Impatto = 1500 € x 10 min = 15000 € di perdita
   Come azione preventiva oltre al Firewall (che puo essere settato sulla quantita di pacchetti X sec. da far passare) , si puo applicare il concetto di rindondanza o per meglio dire «failover cluster»
   Il «failover cluster» include due o più server e permette l'operatività dell'intero sistema anche a fronte di un errore su uno dei due server. Quando il server attivo smette di funzionare, il secondo server prende il suo posto come server attivo tramite un processo che viene chiamato appunto «failover».

3. Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

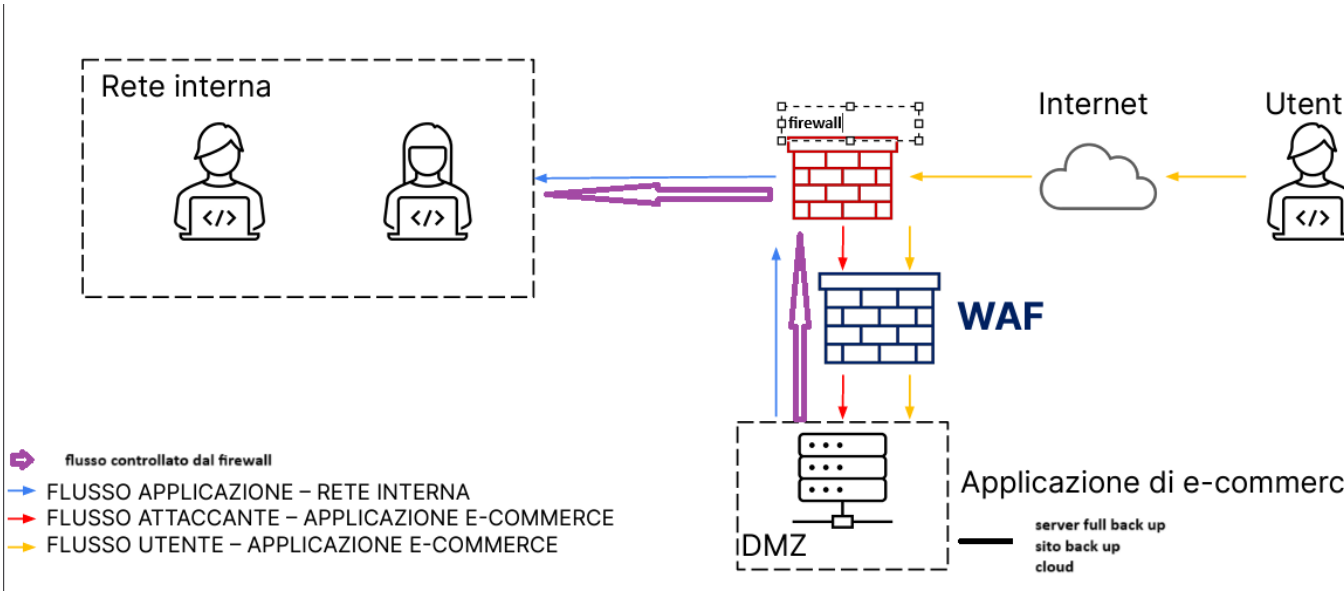


   In questo caso si utilizza l isolamento . Questa tecnica consiste nella totale separazione del sistema infetto dalla rete interna . In questo modo evitiamo uno spostamento verticale da parte dell attaccante dal sistema infetto verso altri sistemi presenti sulla rete interna, nonostante questo l attaccante ha ancora accesso sul sistema infetto .

4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)


Rete interna
Internet
Utenti
WAF
DMZ
Applicazione di e-commerce
FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE

5.


Rete interna
firewall
Internet
Utent
WAF
DMZ
Applicazione di e-commerc
flusso controllato dal firewall
FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE
server full back up
sito back up
cloud