Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

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. **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**

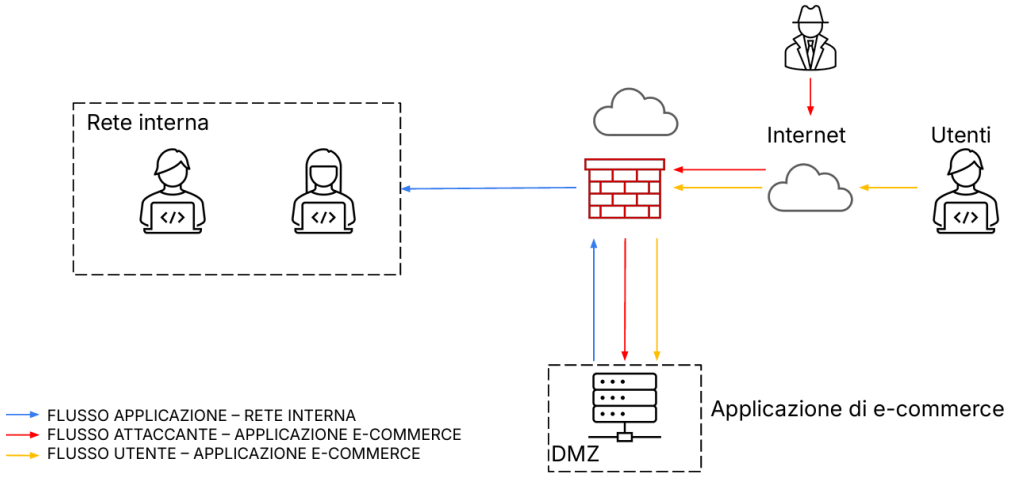
1. **Response**: l'applicazione Web viene infettata da un malware.
   La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.

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

1. **Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)**

Architettura di rete:
L'applicazione di e-commerce deve essere disponibile per gli utenti tramite Internet per effettuare acquisti sulla piattaforma.

La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

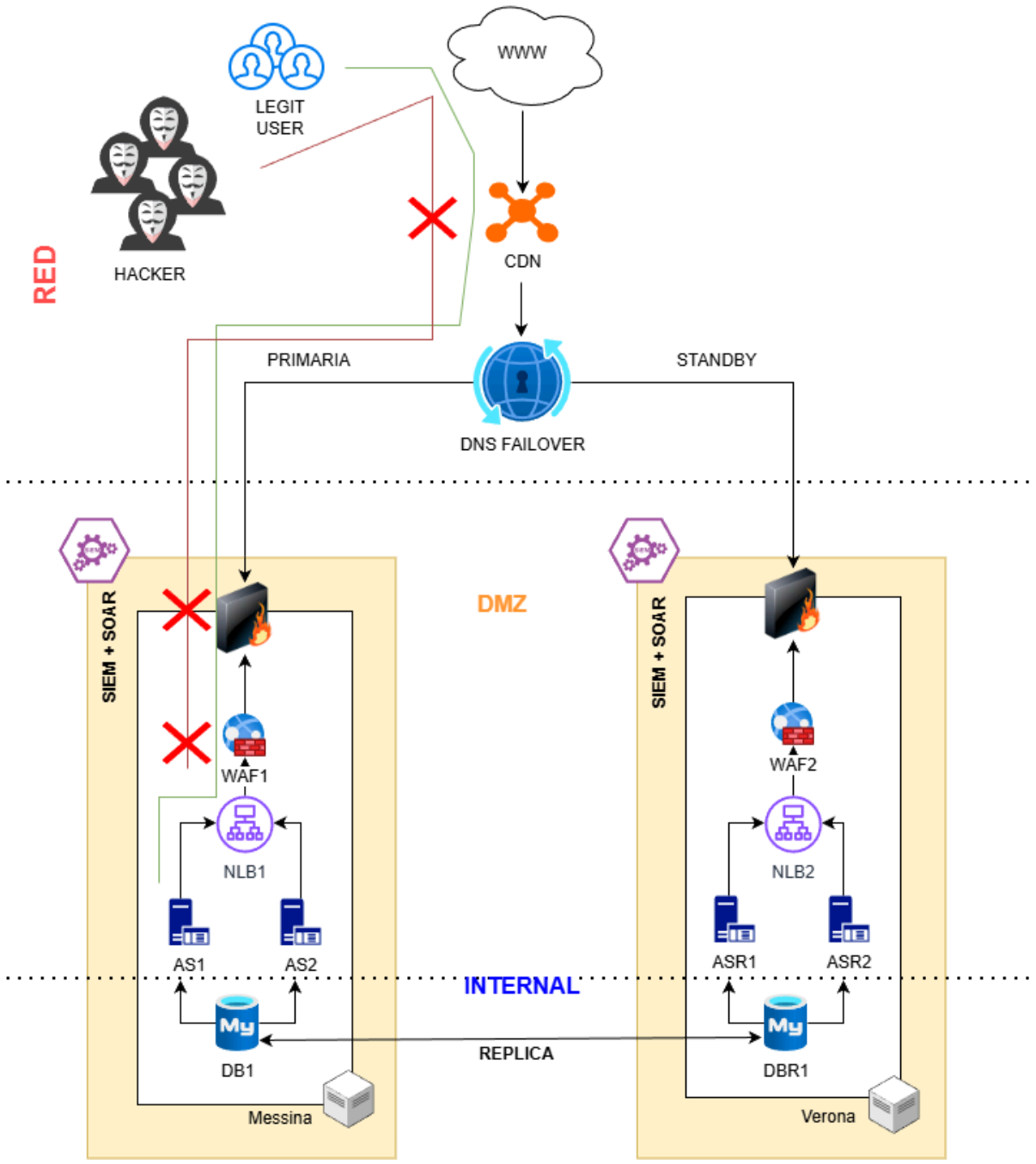


SVOLGIMENTO:

1. **Azioni preventive:** per difendere l'applicazione web da attacchi di tipo SQL oppure XSS

come prima cosa si potrebbe dotare la rete di un WAF (web application firewall) che a differenza degli altri firewall standard proteggono le applicazioni web da attacchi di tipo SQLi e XSS poiché monitorano e filtrano il traffico HTTP tra un'applicazione e internet, ispeziona le richieste analizzando le stesse per contenuto dannoso come script o comandi, utilizza dei filtri e delle regole blacklist e whitelist per decidere cosa bloccare o cosa consentire, protezione da attacchi come XSS o SQL injection, protezione dai bot identificando e bloccando un ipotetico traffico automatizzato malevolo.
A seconda dell'attività di e-commerce si possono utilizzare diverse soluzioni come quella di crowdsec WAF con un reverse proxy Nginx con la possibilità del reverse proxy aumentando così la sicurezza e anche le prestazioni.

Per completare si può inserire un SIEM/SOAR che riceva informazioni dalla rete interna e dal WAF e dalla DMZ così da raccogliere informazioni per identificare minacce (SIEM) e di automatizzare la risposta di tali minacce (SOAR) qualora siano rilevate dal SIEM.



SPIEGAZIONE SCHEMA:
Piuttosto che modificare lo schema delle slide ho preferito fare un altro schema, lo schema mostra tutta l'architettura di rete con i due flussi uno legittimo e uno malevolo, il flusso legittimo riesce ad arrivare ai nostri application server e ad usufruire del servizio al contrario il flusso malevolo può interrompersi già al servizio di cdn (content delivery network) questo servizio non è altro che una rete di server distribuita geograficamente che velocizza la

distribuzione di contenuti web grazie alla cache dei contenuti statici come immagini script video ecc.. ma al contempo stesso offre servizi di sicurezza come protezione contro gli attacchi DDoS, clouflare offre un servizio ad esempio di CDN, poi ho messo un DNS failover per far si che qualora il servizio sulla prima sede smette di funzionare ad esempio guasto elettrico, mancanza di rete o eventuale attacco è possibile reindirizzare il servizio sull'altra sede di standby sull'altra sede è prevista una replica asincrona per mitigare eventuali danneggiamenti ai database in caso di attacco
Poi il traffico passa attraverso il firewall perimetrale e qualora non venisse bloccato un ipotetico attacco alle applicazioni web è previsto un WAF dedicato.
Chiaramente entrambe le sedi sono monitorate mediante l'utilizzo di un SIEM con funzionalità SOAR.
Per ottimizzare ho inserito un network load balancer (NLB) per distribuire il carico delle richieste (a questo punto legittime) e per mitigare un eventuale rottura di un application server.

2. **Impatti sul business:** l'applicazione web subisce un DDoS che non rende raggiungibile il server per 10 minuti, ogni minuto si stima che gli utenti spendono sulla piattaforma di e-commerce 1.500 euro.

Calcolare i danni e fare eventuali valutazioni di azioni preventive che si possono applicare a questa problematica.

calcoli della perdita: 1.500 euro spesi ogni minuto, 10 minuti di disservizio
il calcolo prevede moltiplicare la spesa degli utenti per un minuto moltiplicato i minuti del disservizio

1.500 x 10 = 15.000 euro

per 10 minuti a causa del disservizio creato dall'attacco l'azienda ha una perdita di 15.000 euro di potenziali acquisti.

azioni preventive che si possono applicare a questa problematica:

bilanciamento del carico: un'azione che si potrebbe fare è un bilanciamento del carico, considerando che gli attacchi DDoS mirano a sovraccaricare un sistema rendendolo non disponibile, distribuire il traffico di rete su più server può aiutare a gestire picchi di richieste e rendere più difficile un attacco di questo tipo.
servizi di mitigazione CDN: esistono dei servizi specializzati di content delivery network, questi servizi utilizzano una rete globale per distribuire il traffico e sono in grado di assorbire e filtrare automaticamente il traffico dannoso servizi come cloudfare offrono un servizio business al mese che comunque non arrivano alle perdite stimate di un potenziale attacco quindi la spesa sarebbe ampiamente giustificata.
formazione del personale: formare il personale per riconoscere e gestire le minacce informatiche attività di cruciale importanza considerando che molti attacchi arrivano proprio da sistemi interni (chiavette infette,scaricare allegati malevoli ecc..)

3. **Response:** l’applicazione web viene infettata da un malware, la priorità è che il malware non si propaghi sulla vostra rete non siete interessati a rimuovere l’accesso da parte dell’attaccante alla macchina infetta.

In questo caso la soluzione in linea con la richiesta è quella di prevedere un’ azione automatica di isolamento tramite il SOAR della macchina infetta. Così facendo si continuerà ad erogare il servizio con gli altri application server e si potrà effettuare l’analisi in un secondo momento con la macchina “blindata”. In aggiunta, qualora il SIEM non individui subito l’attività malevola e questa si sia propagata nella struttura, rendendo di conseguenza inutilizzabile la sede primaria, si potrà effettuare in failover verso la sede di standby con una perdita di dati minima, e conseguente costo del danno limitato.
Anche in questo caso, potendo ricominciare a fornire il servizio in breve tempo, sarà possibile effettuare analisi e ripristino della sede primaria in un secondo momento.