Benchmark W20D4 Zanini Riccardo

Traccia:

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**
2. **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**
3. **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.**
4. **4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)**
5. **5. Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)**

1.1) Azioni preventive SQL

- Per poter prevenire attacchi SQL è essere sempre aggiornati su i tipi di vulnerabilità esistenti. E' quindi importante mantenere un database interno sulle vulnerabilità rilevate ad oggi. E' possibile inoltre appoggiarsi a siti terzi in grado di raccogliere informazioni a livello mondiale e di condividerli con gli utenti fruitori del servizio.
- Limitare i privilegi ai database può aiutare a prevenire l'accesso a persone malintenzionate
- Utilizzare un firewall in modo da filtrare e monitorare il trafico HTTP in entrata.
- Parametrizzare il database in modo che i valori in entrata e uscita vengano trattati come dati e non come codice, viene evitato in questo modo l'esecuzione di codice arbitrario.
- Utilizzare delle librerie di comparazione in modo da verificare che i dati immessi dall'utente siano coonformi al formato atteso

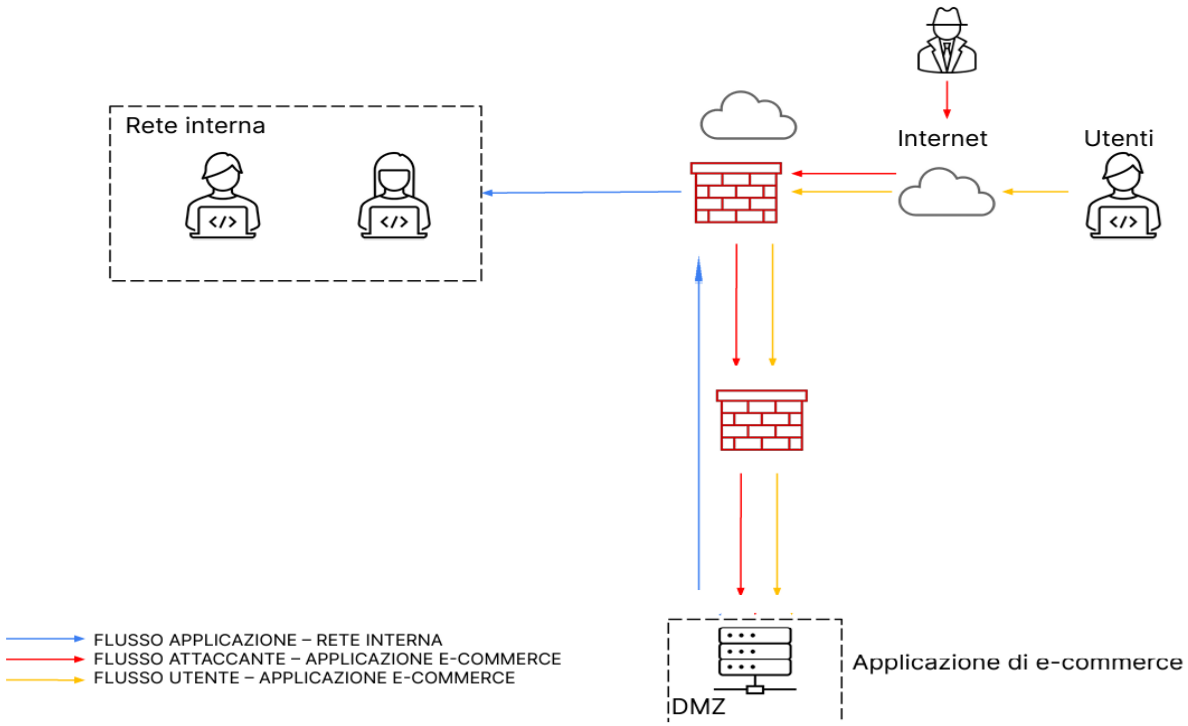
1.2) Azioni preventive XSS

- Utilizzare una Content Security Policy in modo da specificare a monte le origini autorizzate a fornire dati al nostro server
- Codificare sempre i dati che vengono inseriti nel codice HTML utilizzando funzioni apposite per evitare l'esecuzione di script dannosi.

Per evitare entrambi i tipi di attacco è bene:

- Crittografare i dati sensibili, come le password, utilizzando algoritmi robusti.
- Esecuzione di backup regolari in modo da poter riprestinare il server nel più breve tempo possibile

Nella soluzione proposta di seguito nell'architettura di rete è stato implementato un firewall utile a controllare il traffico in entrata nella nostra applicazione web.



2.1) Stima sulle perdite attacco DdoS

Con i dati forniti è facile calclare la perdita economica immediata ai danni dell'azienda:
10 minuti * 1.500 €/minuto = 15.000 €

E' bene però tenere in considerazione altri tipi di perdite non rilevabili con il semplice calcolo matematico:

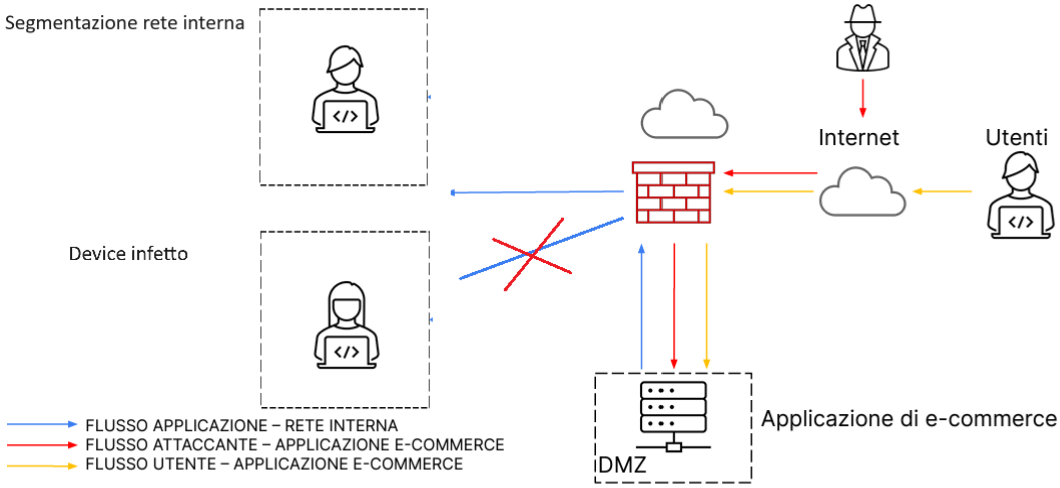
- Clienti potenzialmente persi a causa della cattiva esperienza.
- Danno reputazionale nei confronti di clienti già fruitori del servizio o di nuovi clienti
- Costi legati alla risoluzione del problema, personale IT, Cybersecurity analist,

2.2) Azioni prevntive DdoS

- Bloccare il traffico proveniente da determinate regioni geografiche.
- Impostare limiti alla quantità di traffico che può essere gestito contemporaneamente.
- Utilizzare Firewall specifici in grado di identificare e bloccare il traffico proveniente da botnet
- Utilizzare un accesso con CAPTCHA
- Limitare il numero di richiesta che un utente può effettuare in un determinato lasso di tempo

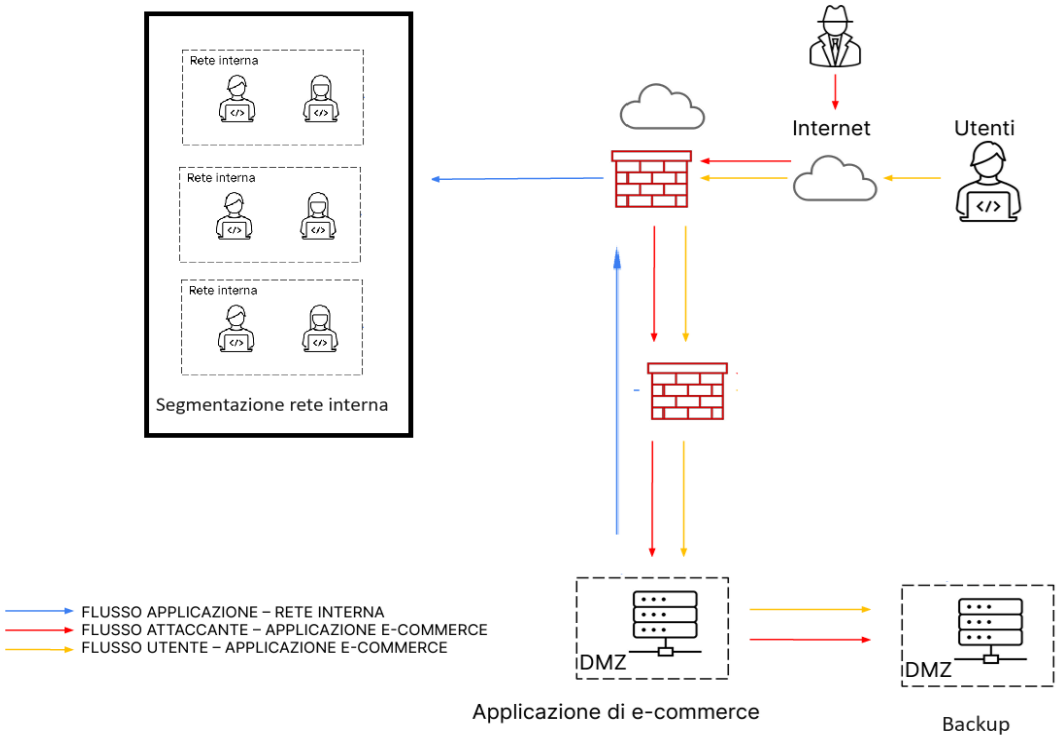
3) Isola la macchina infettata evitando che il malware si propaghi sulla rete

Per evitare che un malware si propaghi nella rete è necessario segmentare ed isolare il device infetto.
Questa nuova rete viene chiamata “rete di quarantena”, talvolta come soluzione non risulta sufficiente ed è necessario il completo isolamento, disconettendo completamente il device infetto dalla rete.



4)Unire architettura di rete dei punti 1 e 3

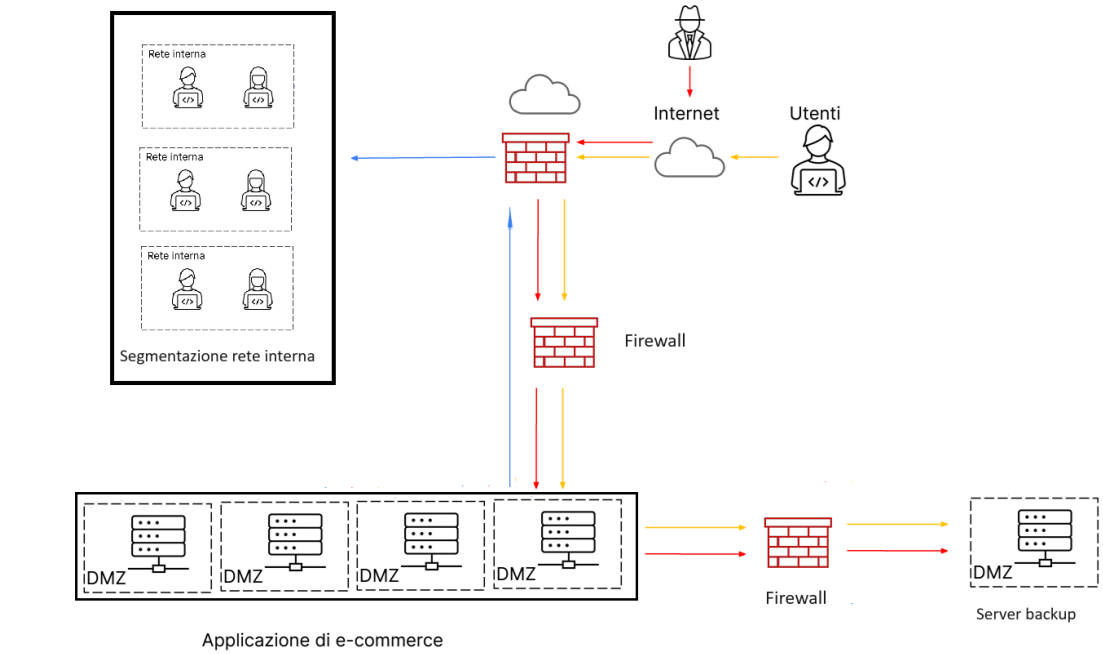
Oltre ad unire le soluzioni ai punti 1 e 3 è stato implementato un ulteriore server di backup, utile a recuperare i dati in caso di attacco



5) Modifica «più aggressiva» dell'infrastruttura

In quest'ultima soluzione oltre a quanto già visto, segmentazione della rete e firewall aggiuntivo sono state implementate:

1. suddivisione del traffico tra più server, al fine di evitare sovraccarichi dovuti ad attacchi DdoS
2. Ulteriore firewall tra applicazione web e server di backup



FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE