W20D4
PROGETTO FINE MODULO

Calogero Schembri

TRACCIA

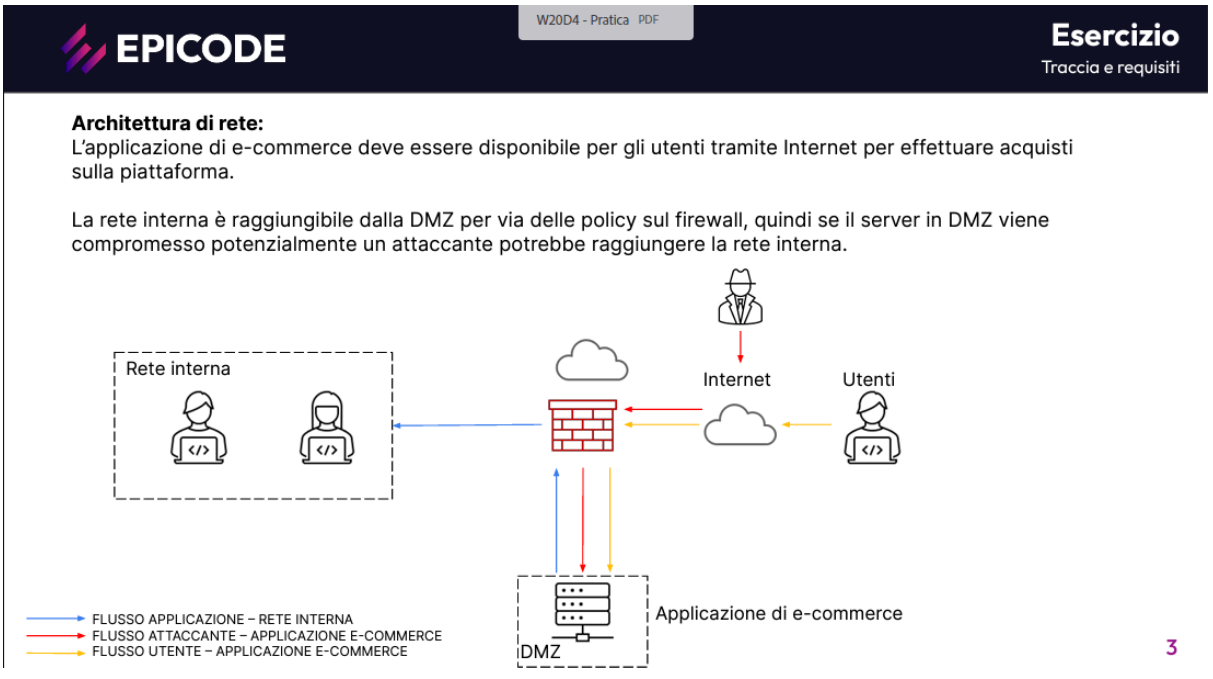
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

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

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



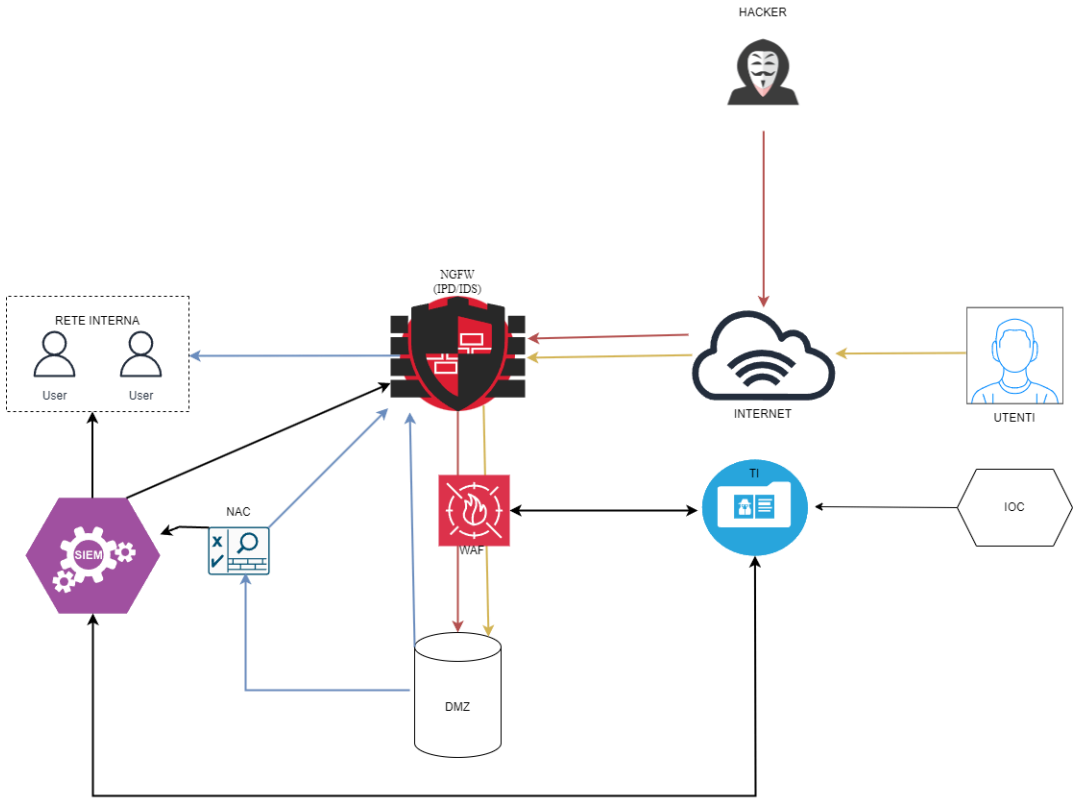
Azioni Preventive

Prima di affrontare le azioni preventive
E' importante seguire le best practice di incident response che sono fondamentali per la gestione efficace delle minacce alla sicurezza informatica
Alcune best practice includono:

- Vulnerability Assessment
- Penetration Test
- Threat Analysis

Azioni preventive per difendere un'applicazione web da attacchi SQLi e XSS
Riconoscere che la sicurezza informatica è un processo continuo e multifase
Implementare soluzioni di sicurezza aggiuntive per ridurre il rischio di attacchi informatici
Alcune soluzioni di sicurezza includono:

- Network Access Control (NAC)
- Next Generation Firewall (NGFW)
- Web Application Firewall (WAF)
- Security Information and Event Management (SIEM)
- Aggiornamento regolare del software



Impatti sul business

Calcolo del danno:

Tempo di non raggiungibilità: 10 minuti
Spesa media al minuto: €1.500
Danno economico totale: 10 minuti * €1.500/minuto = €15.000
Danno all'immagine e alla reputazione del brand: Un attacco DDoS può danneggiare la fiducia dei clienti e la reputazione del brand.
Perdita di clienti: I clienti potrebbero rivolgersi a competitor se non riescono ad accedere al servizio.
Costi di ripristino: Potrebbero esserci costi per ripristinare il servizio e per mitigare gli effetti dell'attacco.

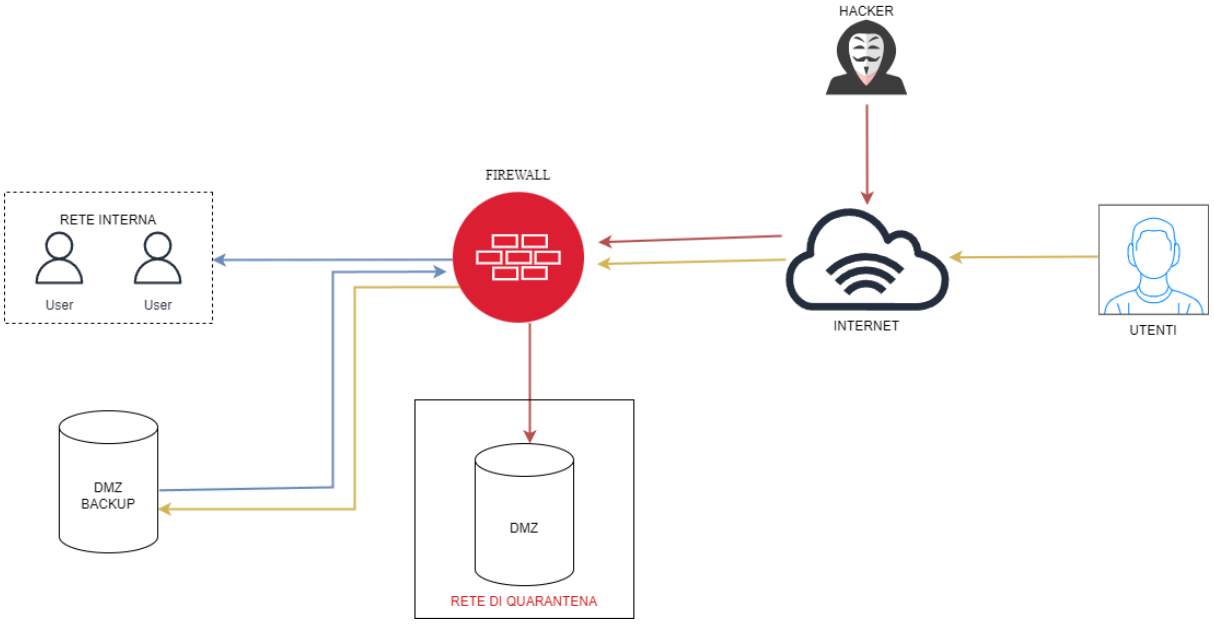
Azioni preventive contro gli attacchi DDoS:

- È importante avere un piano di disaster recovery in caso di attacco DDoS o di altri eventi che causano la non raggiungibilità del servizio.
- Il personale IT dovrebbe essere formato su come identificare e rispondere agli attacchi DDoS.
- È importante monitorare continuamente la rete e il servizio per identificare eventuali minacce.

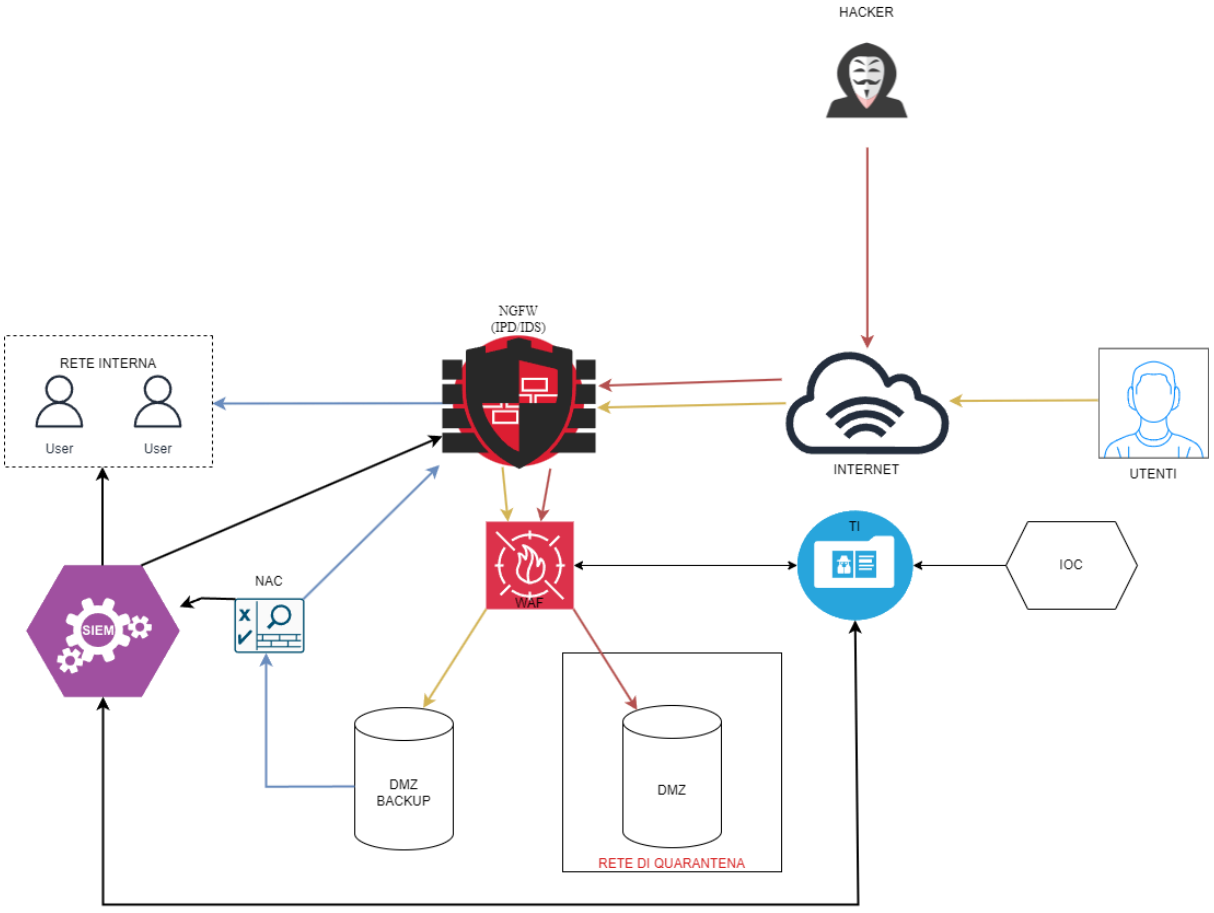
Response

Supponendo l'esistenza di un backup dell'applicazione web procediamo con indirizzare il traffico dell'attaccante sulla DMZ già infettata. Sul DMZ di backup avverranno le connessioni della rete interna e degli utenti che devono utilizzare i servizi dell'e-commerce.
Quindi dobbiamo impostare una regola firewall che dividerà in modo automatico le connessioni:

- la connessione verso il DMZ infetto per gli utenti malevoli
- verso il DMZ backup per gli utenti autorizzati



Soluzione completa



Modifica «più aggressiva» dell'infrastruttura

L’alternativa sarebbe di isolare completamente la rete, bloccando quindi qualsiasi tipo di connessione, anche se inibisce l’utilizzo sia ai dipendenti che agli utenti.