Benchmark W20D4 EPICODE

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

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.

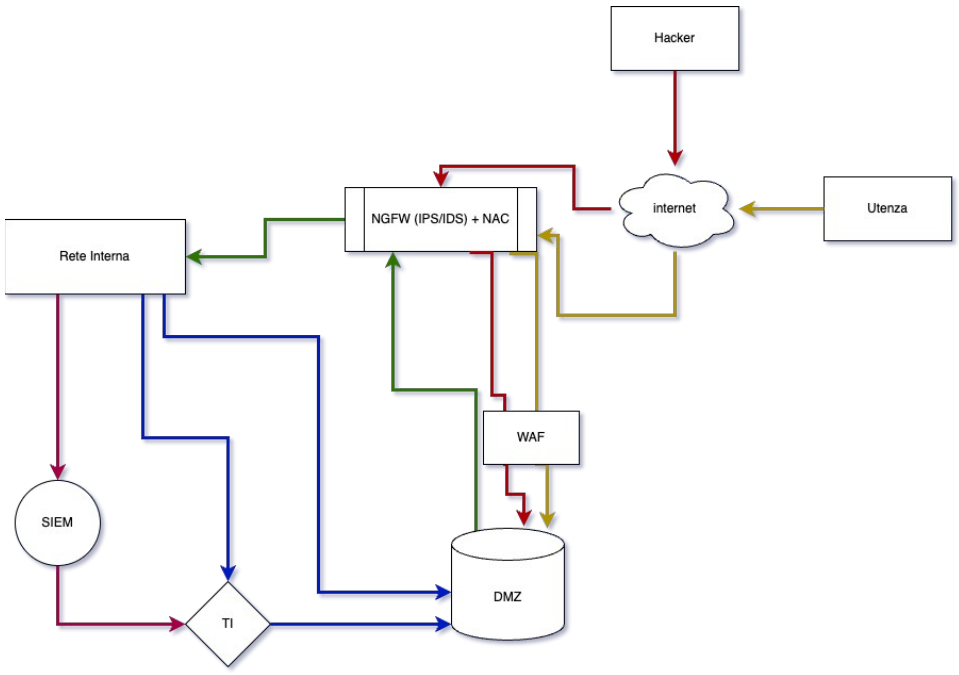
4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

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

Risoluzione:

Punto 1 Azioni Preventive:

Alcune azioni preventive possono essere: il NAC (Network Access Control), il SIEM (Security Information Event Management), fare un upgrade al firewall con uno piu performante ma piu costoso (Netx Generation Firewall) che ha integrato un sistema IPS/IDS, Patching dei sistemi, la piattaforma di TI (Threat Intelligence), validazione e sanificazione degli input.

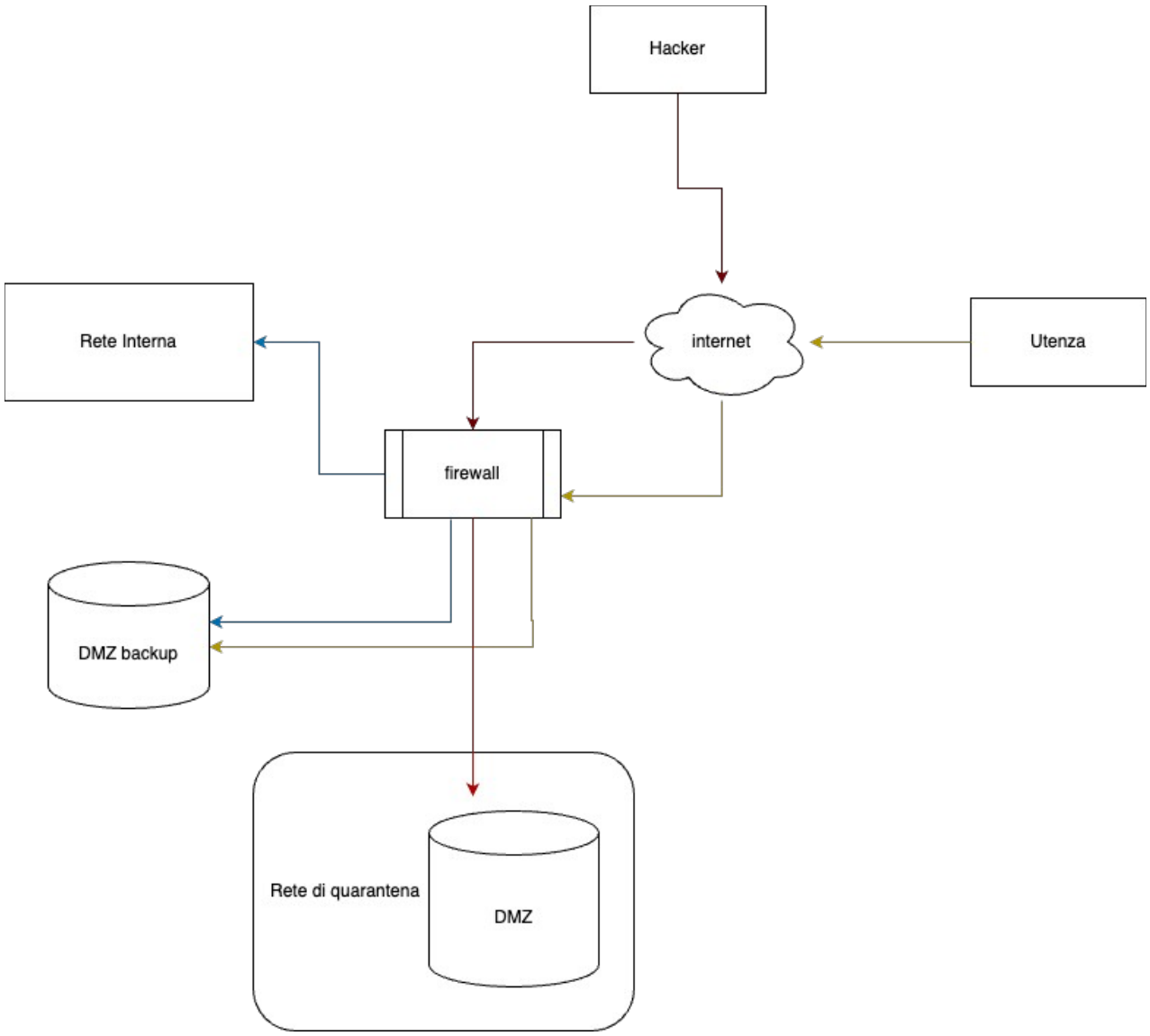


Punto 2 Impatti sul business:

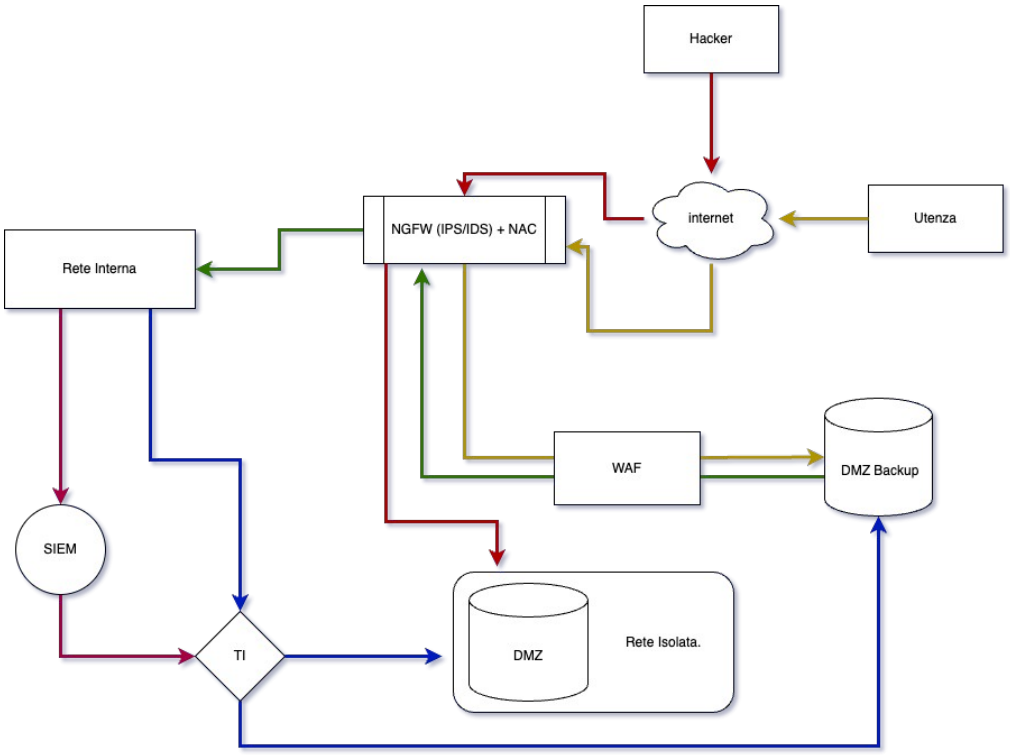
Se dopo un DDoS rende l'applicazione non raggiungibile per 10 minuti e per ogni minuto in media gli utenti spendono 1500 Euro sulla piattaforma di e-commerce. La perdita sarà di 15.000 Euro ogni 10 minuti. Come azione preventiva si potrebbe optare di utilizzare un sistema anti-DDoS.

Punto 3 Response:

Per evitare che il malware si propaghi alla rete interna il modo migliore è create una rete di quarantena e isolare l'asset infetto ma lasciandogli l'accesso ad internet, così sarà possibile studiare il metodo e il tipo di malware in questione. Dopodichè sarebbe oppurtuno utilizzare un sito di backup cosi da garantire la continuità delle operazioni.



Punto 4 Soluzione Completa:



Punto 5 Modifica più <<aggressiva>>:

Isolare totalmente l’asset anche da internet