Progetto Settimana 9

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 .

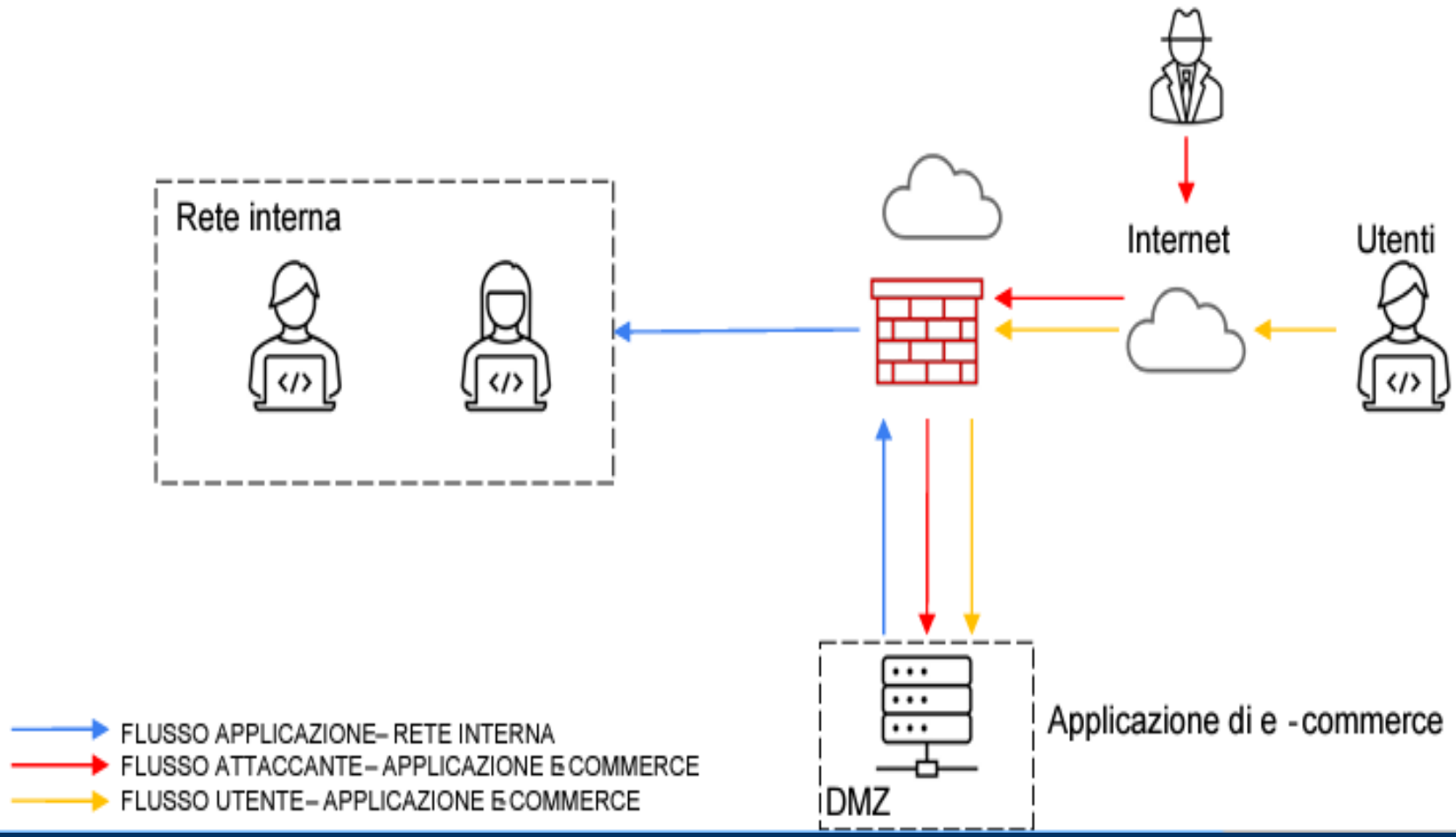
4. **Soluzione completa** : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. **Modifica «più aggressiva» dell'infrastruttura**: integrando eventuali altri elementi di sicurezza **(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.

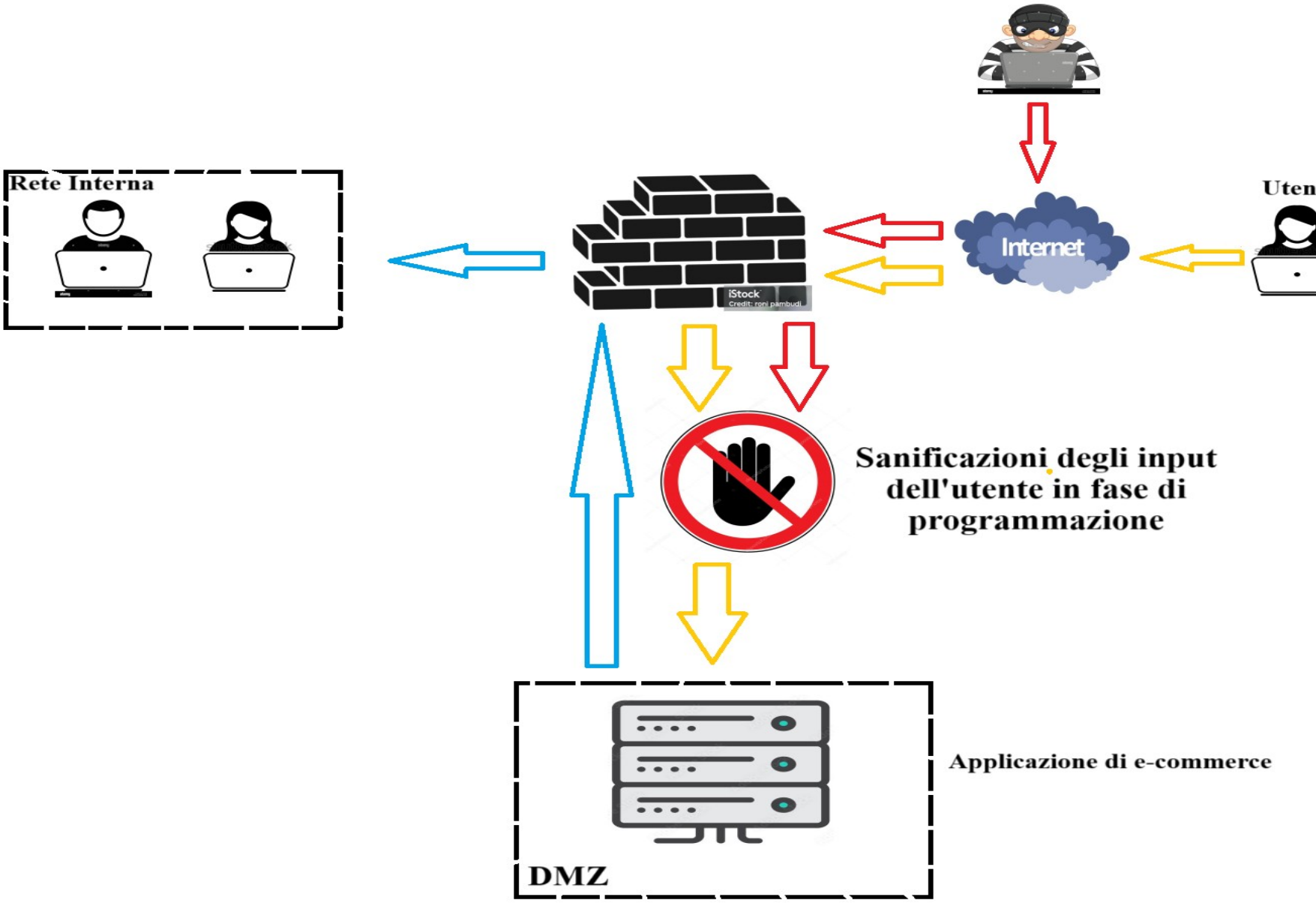
La rete interna è raggiungibile dalla DMZ per via delle policy sul firewall, quindi se il server in DMZ viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.



Azioni Preventive 1

- In questo caso per scongiurare eventuali attacchi di tipo SQLi e XSS, in fase di programmazione, andiamo a sanare gli input da parte dell'utente. In questo modo renderemo vani i tentativi di inserimento di script malevoli sulla pagina di e-commerce dell'azienda.

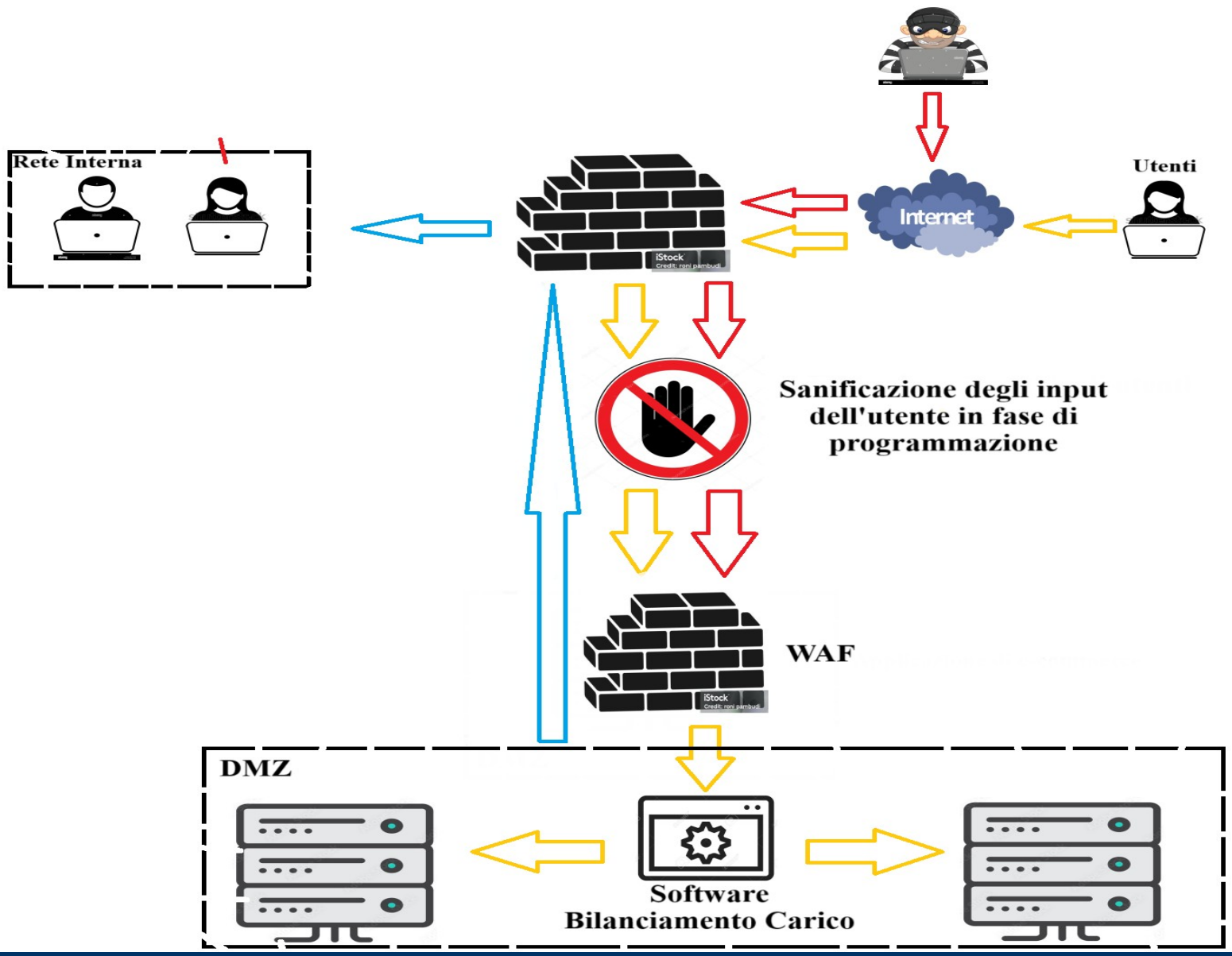
Azioni Preventive 1



Impatti sul Business 2

- Valutando il possibile evento del punto 2, la web server irraggiungibile per 10 minuti, calcolando una possibile perdita di €15.000,00.
- Per scongiurare un futuro attacco DDOs consiglio l'installazione di un sistema WAF che va a frapporsi tra il web server e gli utenti, combinato ad un software di bilanciamento del carico. Il WAF o firewall per applicazioni web è una delle migliori difese contro gli attacchi DDoS. Si frappone tra il tuo sito web e le richieste e filtra il traffico di rete per escludere gli accessi dannosi. Questo non solo aiuta a proteggere dagli attacchi, ma può anche contenere gli attacchi DDoS limitando le richieste. Integrando un server in più e un software che va a bilanciare le richieste rendiamo la possibilità di ricevere attacchi DDOS molto più esigua.

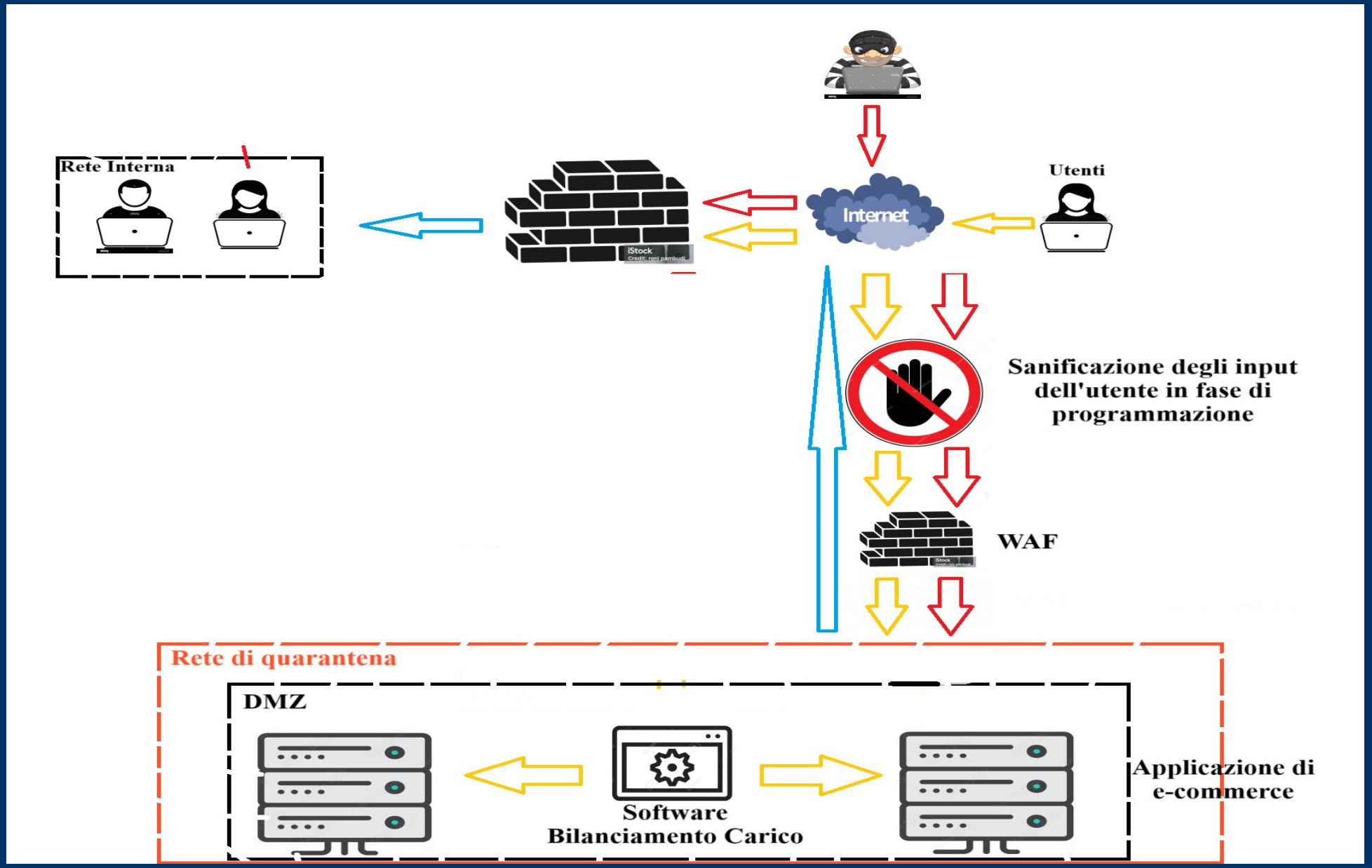
Impatti sul Business 2



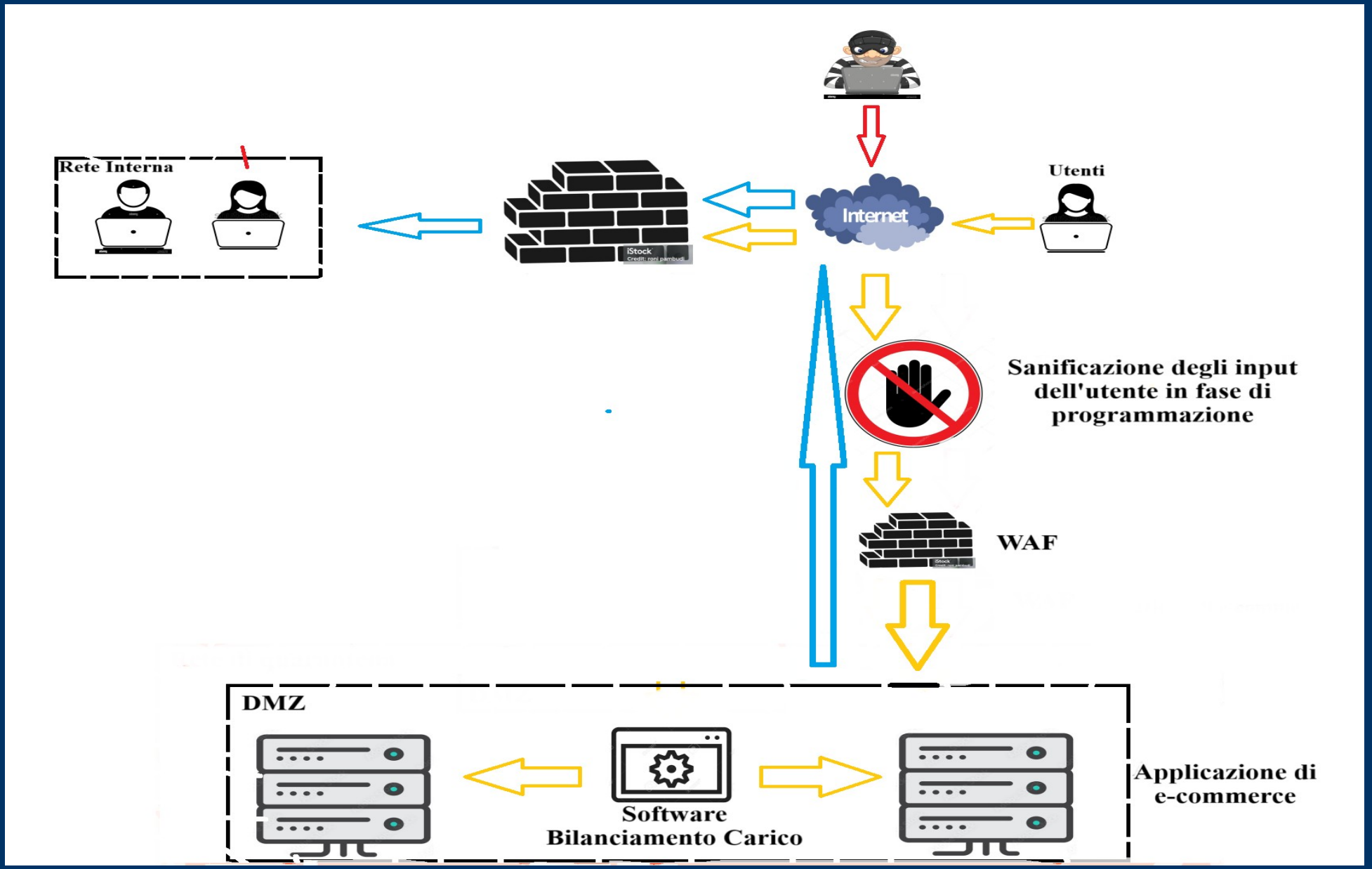
Response 3

- Nel cosa in cui la nostra applicazione Web venga infettata da un malware e la nostra priorità è che il malware non si propaghi sulla vostre rete, ho pensato di utilizzare la tecnica dell'isolamento.
- L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere l'accesso alla rete interna da parte dell'attaccante. In questo scenario l'attaccante hanno ancora accesso al server tramite internet.

Response 3


Rete Interna
Internet
Utenti
Sanificazione degli input dell'utente in fase di programmazione
WAF
Rete di quarantena
DMZ
Software
Bilanciamento Carico
Applicazione di e-commerce

Soluzione completa 4



Modifica dell'infrastruttura 5

- Oltre alle modifiche evidenziate in precedenza ho pensato di inserire altri due sistemi di sicurezza, l'IDS e l'IPS. Soluzioni che possono integrare software e hardware per garantire il massimo livello possibile di protezione da attacchi digitali di vario genere.
- L'IDS (Intrusion Detection System) è un sistema di sicurezza che individua e riporta attività sospette o potenzialmente dannose in una rete.
- L'IPS (Intrusion Prevention System) è un sistema di sicurezza che, a differenza dell'IDS, non solo rileva le attività dannose, ma intraprende anche azioni attive per prevenirle o bloccarle

Modifica dell'infrastruttura 5