Progetto

L9-L5

GIULIA FIACCHI

Traccia

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

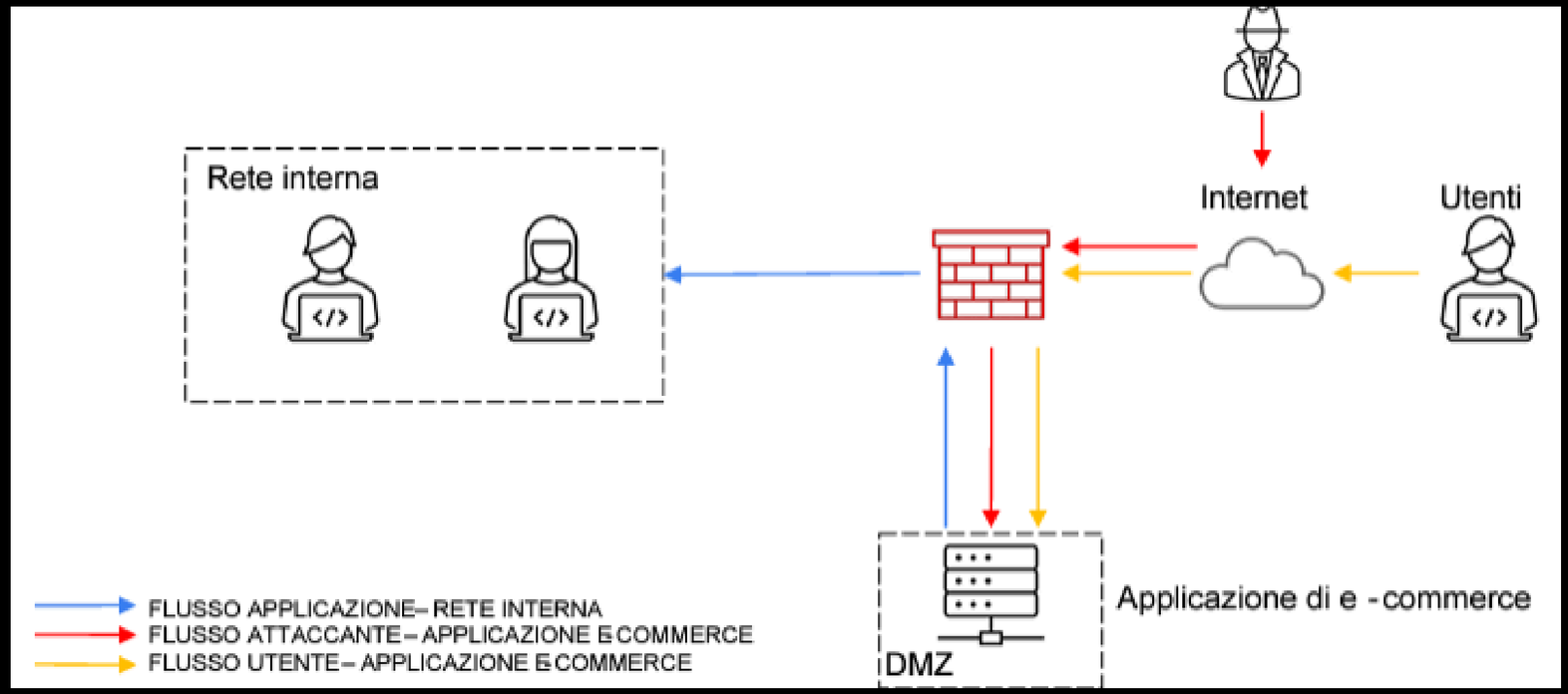
1. **Azioni preventive** : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni. È richiesta sola modifica
2. **Impatti sul business** : 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 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

Traccia

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**: anche una soluzione al punto 2) integrando eventuali altri elementi di sicurezza (integrando Budget 5000-10000 euro. Eventualmente fare più proposte di spesa

Traccia

Architettura di rete: L’applicazione di e-commerce deve essere disponibile per gli utenti tramite 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.



Parte 1

Azioni preventive

Per proteggere un'applicazione web dagli attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), è fondamentale implementare alcune misure di sicurezza come:

- l’implementazione di un **WAF** (Web Application Firewall)

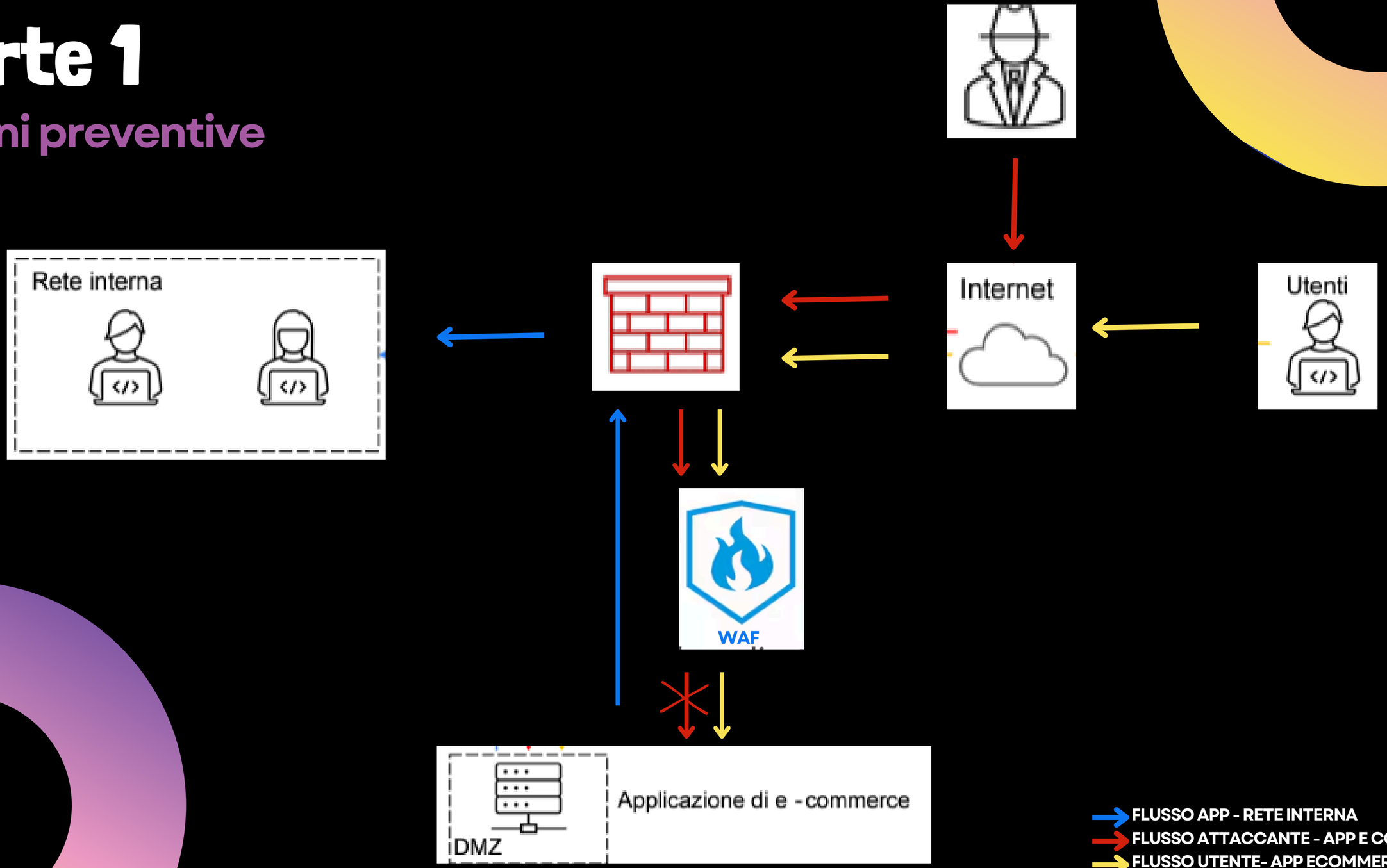
E’ un dispositivo o servizio di sicurezza che protegge le applicazioni web monitorando e filtrando il traffico HTTP tra un'applicazione web e Internet.

Vantaggi

- **Protezione contro SQLi e XSS**
- **Difesa contro altre minacce**
- **Filtraggio e monitoraggio del traffico HTTP/HTTPS:** per identificare e bloccare richieste sospette o malevoli.
- **Facilità di implementazione**
- **Logging e monitoraggio**
- **Regole personalizzabili**
- **Aggiornamenti frequenti**

Parte 1

Azioni preventive



Parte 2

Impatti sul business

- **app non raggiungibile per 10 minuti**
- **ogni minuto gli utenti spendono 1.200 € sulla piattaforma di e-commerce**

Calcolo dell'Impatto

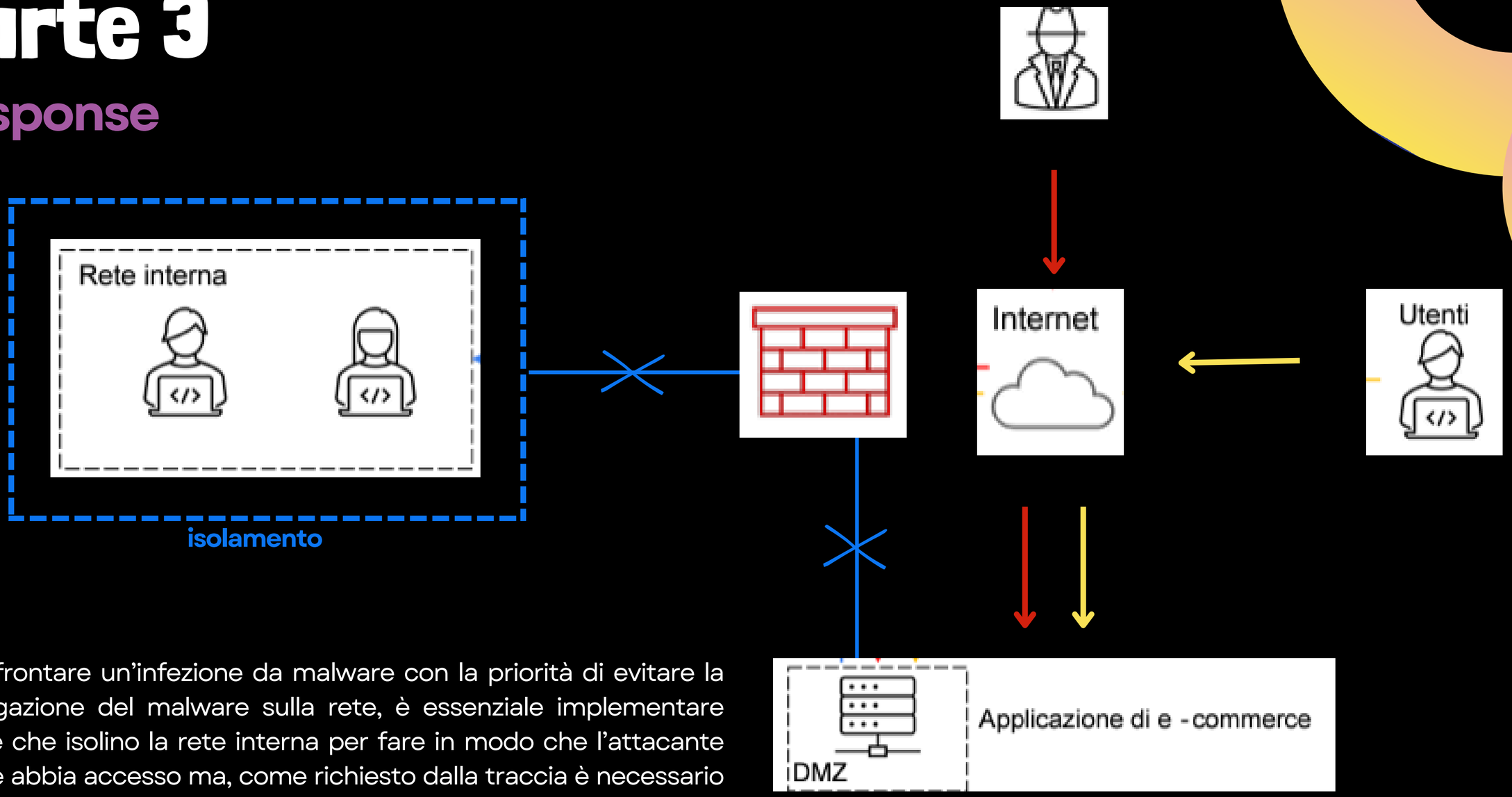
Impatto Economico = Durata dell'Indisponibilita` x Entrate per Minuto

10 x 1.200 = 12.000 €

Implementare misure preventive può aiutare a mitigare il rischio e ridurre l'impatto economico di tali attacchi come ad esempio: **Web Application Firewall (WAF), un servizio di protezione DDoS, Servizi Cloud, Load Balancing, Monitoraggio del Traffico, Failover** (quest'ultimo implica il passaggio automatico o manuale da un componente o sistema guasto a uno di riserva per mantenere la disponibilità e l'affidabilità del servizio) .

Parte 3

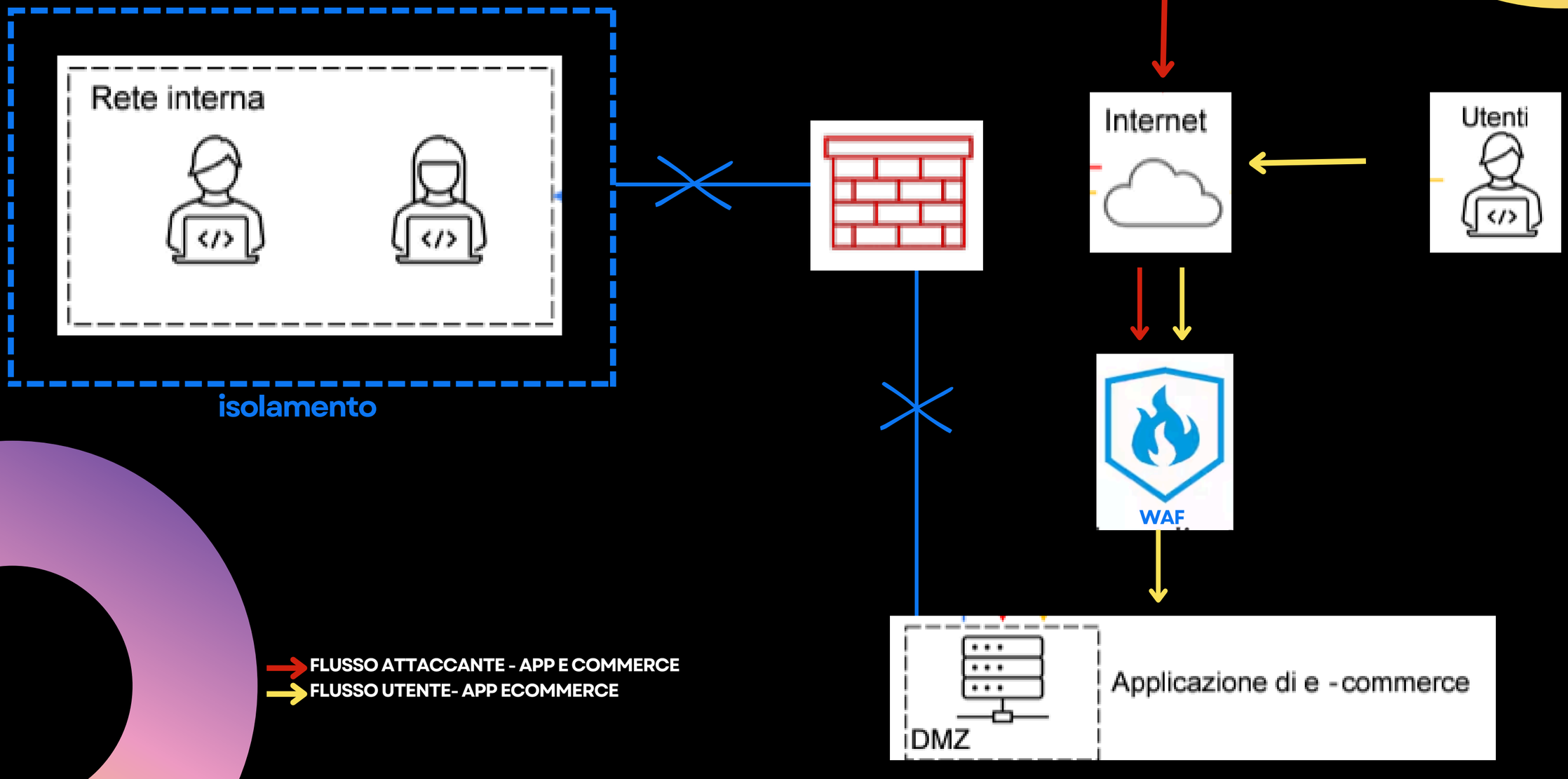
Response



Per affrontare un'infezione da malware con la priorità di evitare la propagazione del malware sulla rete, è essenziale implementare misure che isolino la rete interna per fare in modo che l'attacante non ne abbia accesso ma, come richiesto dalla traccia è necessario collegare la web app direttamente ad internet per permetterne comunque all'attacante l'accesso.

Parte 4

Soluzione completa - disegno



Parte 5

Modifica «più aggressiva» dell'infrastruttura

Avendo a disposizione un budget che varia dai 5.000 ai 10.000 € proponiamo l'implementazione di ulteriori misure di sicurezza, anche in risposta agli eventuali attacchi Ddos (parte2):

Proposta 1

- **WAF - WEB APPLICATION FIREWALL**

Protegge le applicazioni web da attacchi comuni come SQL injection, cross-site scripting (XSS), e altre minacce basate su applicazioni, permette di adattare le regole di sicurezza alle esigenze specifiche dell'applicazione. In particolare consigliato il **MODELLO FORTINET FORTIGATE 100F** che, di base nasce come Firewall tradizionale ma comprende anche funzioni di protezione su web-app e inoltre include IDS/IPS per il rilevamento e la prevenzione delle intrusioni a livello di rete e di host.

- **REPLICA DATABASE E FAILOVER**

Replica database implica avere una copia del database primario che può essere utilizzata se il database principale fallisce, il failover consente al sistema di passare automaticamente alla replica del database in caso di guasto del primo. Sono fondamentali per garantire la disponibilità, la scalabilità e la resilienza dei sistemi informativi.

Parte 5

Modifica «più aggressiva» dell'infrastruttura

- **BACKUP E MONITORAGGIO AGGIUNTIVO**

Backup include soluzioni per eseguire regolarmente copie di sicurezza dei dati, permettendo di ripristinarli in caso di perdita o corruzione. Monitoraggio si riferisce a strumenti e servizi che controllano continuamente l'infrastruttura IT per rilevare e rispondere a eventuali problemi.

tabella costi

WAF	4.000- 4.500 €
REPLICA DATABASE E FAILOVER	1.500 - 3.000 €
BACKUP E MONITORAGGIO AGGIUNTIVO	500 - 1.000 €
TOTALE	6.000 - 8.500 €

Parte 5

Modifica «più aggressiva» dell'infrastruttura

Avendo a disposizione un budget che varia dai 5.000 ai 10.000 € proponiamo l'implementazione di ulteriori misure di sicurezza, anche in risposta agli eventuali attacchi Ddos (parte2):

Proposta 2

- **SIEM**

raccoglie dati da varie fonti, com e server e applicazioni per identificare attività dannose, inoltre fornisce informazioni sulle minacce correlando dati provenienti da diverse fonti e creando una dashboard di facile consultazione. Aiuta a m antenere un registro rigoroso delle attività degli utenti.
Fornisce inform azioni dettagliate su chi ha avuto accesso a quali risorse e quando, aiutando a rilevare e prevenire attività non autorizzate. Archiviando e analizzando i dati di registro relativi alle attività degli utenti è quindi possibile effettaure indagini sugli incidenti.

- **SOAR**

l'orchestrazione, l'automazione e la risposta alla sicurezza, è una soluzione software che consente ai team di integrare e coordinare strumenti di sicurezza separati, automatizzare le attività ripetitive semplificare i workflow di risposta agli incidenti e alle minacce.

Parte 5

Modifica «più aggressiva» dell'infrastruttura

- **Firewall Ridondanti**

assicurano che il traffico di rete sia protetto anche se un firewall fallisce. Questo può includere l'uso di due firewall in configurazione attiva-passiva o attiva-attiva

- **Load Balancer**

distribuiscono il traffico tra più server per assicurare che nessun singolo server venga sovraccaricato e che il servizio rimanga disponibile anche se uno dei server fallisce. Possono essere hardware dedicati, software o servizi cloud.

tabella costi

SIEM	**2.500 - 3.000 €**
SOAR	**7.500 €**
FIREWALL RIDONDANTI	**1.000 - 2.000 €**
LOAD BALANCER	**1.500 -3000 €**
TOTALE	**12.500 - 15.500€**

Bonus

https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6 /

Analizzando il primo link possiamo notare che si tratta di un attacco di **phishing**.
Il messaggio di phishing spesso include un avviso urgente, una richiesta di verifica delle credenziali o un'offerta imperdibile, con lo scopo di suscitare una risposta immediata.
In questo caso apre un documento su Acrobat in cui afferma che sia necessaria la firma dell'utente su quel documento di sicurezza e che lo dovrà fare entro 2 giorni altrimenti si riterrà risolta, ancora afferma che che è possibile scaricare una copia per tenerne lo storico e come è possibile vedere dalla scansione cerca di connettersi ad un sito sospetto e non fidato probabilmente per ottenere un accesso o sniffare dati.

In questi casi è quindi necessario :

- Non cliccare su link o aprire allegati provenienti da email sospette o non verificate
- Controllare gli URL
- Mantenere aggiornati antivirus e software di sicurezza
- Contatta direttamente l'entità da cui sembra provenire la comunicazione per confermare la sua autenticità se si hanno dei dubbi
- Effettuare una scansione

Bonus

https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6 /

Analizzando il secondo link possiamo notare che si tratta di un **ransomware Phobos**.
E' una variante di malware che combina caratteristiche di ransomware e di stealer (software progettato per rubare informazioni). Questo tipo di minaccia ha come obiettivo principale quello di bloccare l'accesso ai dati dell'utente o dell'organizzazione e, allo stesso tempo, rubare informazioni sensibili.

In questo caso possiamo osservare come sia stato installato, entrando nel Disco locale e poi va in program files e poi in program data e infine clicca su $WinREAgent, nella cartella backup possiamo vedere un file che poi viene aperto e che contiene dati criptati e che non sono leggibili (probabilmente per recuperare i dati in chiaro sarà stato richiesto un riscatto).

Per evitare questo è necessario:

- effetturare dei continui backup per un recupero dei dati veloce ed efficacie
- utilizzare software di sicurezza (aggiornare antivirus)
- evitare download da fonti non affidabili
- monitoraggio continuo delle attività

Risposta a un'Infezione da Software Stealer

1. Isolamento:
2. Analisi e Rimozione
3. Cambio delle Credenziali:
4. Segnalazione
5. Recupero e Ripristino