

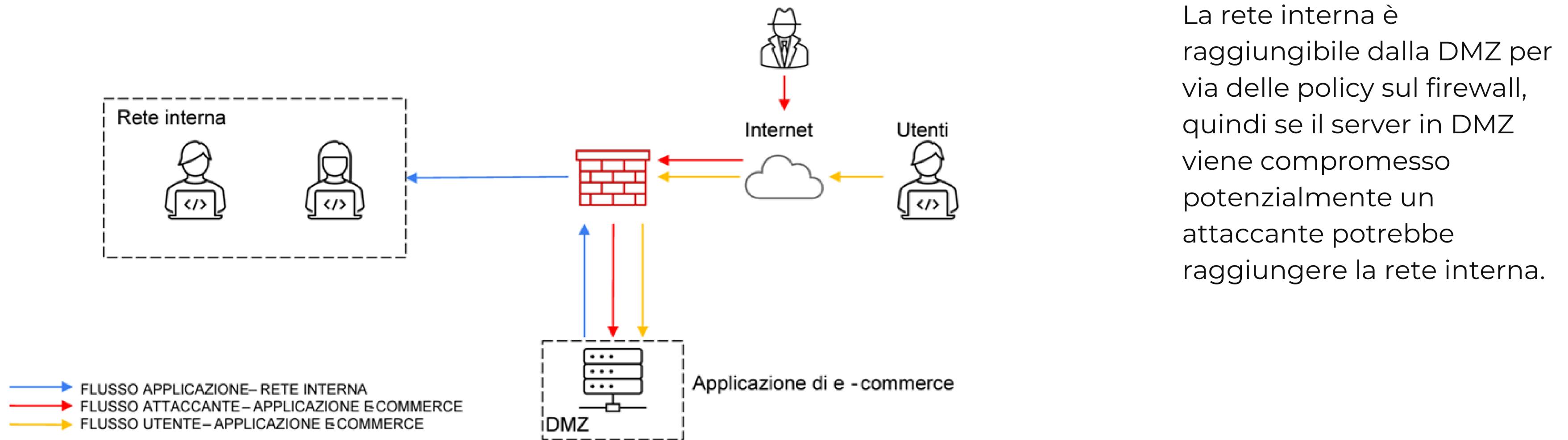
Progetto Unit 3

S9/L5

Alessio Forli

Architettura di Rete

L'applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.



Quesiti

Problem 1

Azioni Preventive

Problem 2

Impatti sul Business

Problem 3

Response

Problem 4

Soluzione Completa

Problem 5

Modifica “più aggressiva” dell’infrastruttura

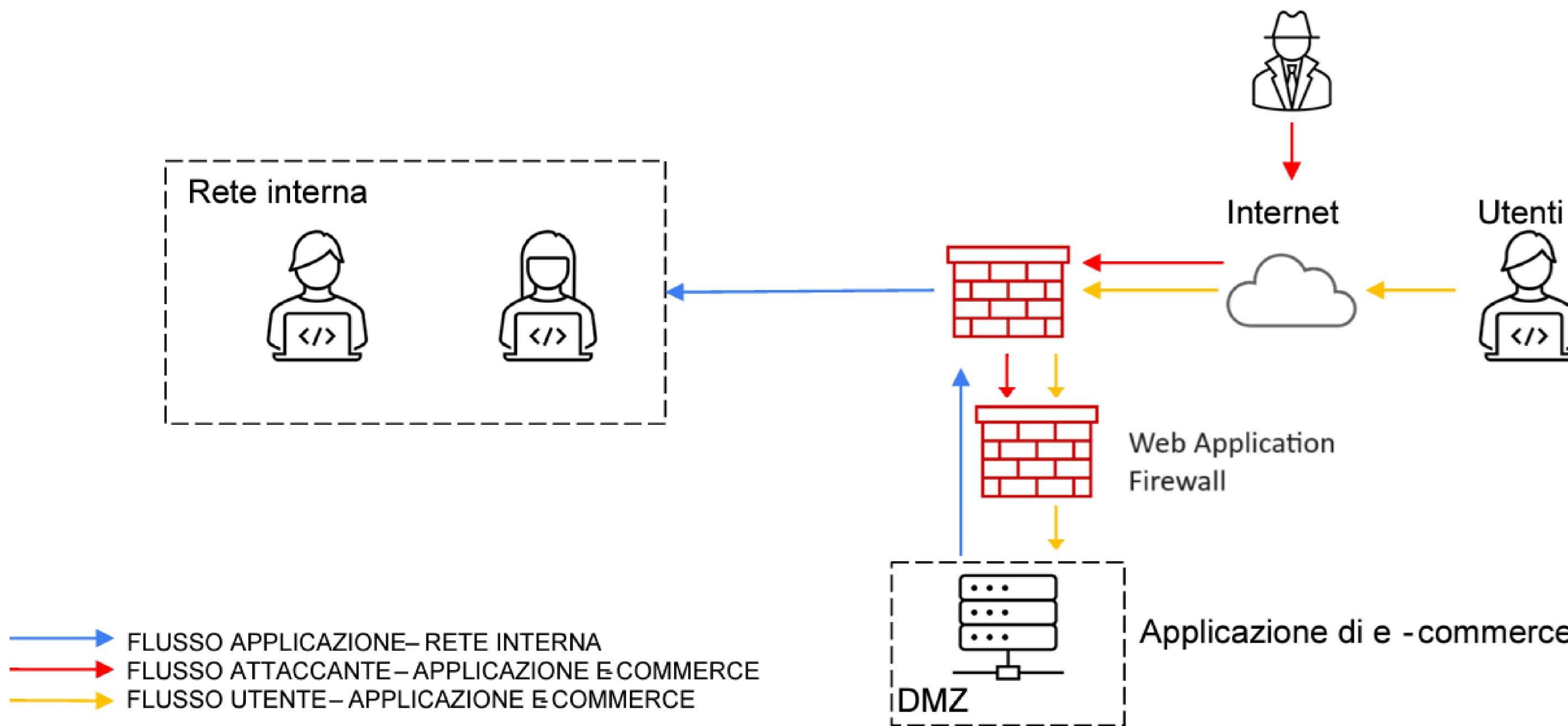
1. Azioni Preventive

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. Richiesta una sola modifica.

Per difendere l'applicazione di e-commerce da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato potremmo aggiungere un Web Application Firewall (WAF) che andrebbe ad analizzare il traffico in entrata sull' applicazione di e-commerce bloccando i potenziali attacchi che non sarebbero stati rilevati da un Firewall non specializzato per le Web Application.

1. Azioni Preventive



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 1200€ sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica.

Se l'applicazione di e-commerce subisse un attacco di tipo DDoS che renderebbe l'applicazione non raggiungibile per 10 minuti, considerando che in media gli utenti in un minuto spendono circa 1200€ sulla piattaforma, ciò causerebbe un impatto sul business di $1200\text{€} \times 10 \text{ minuti} = 12000\text{€}$.

Alcune delle azioni preventive da valutare applicabili per questa problematica sono:

- Bilanciare il carico di richieste redistribuendole su più server per evitare il sovraccarico.
- Utilizzare un sistema di rilevamento e prevenzione delle intrusioni (IDS/IPS).
- Limitare il numero di richieste che un singolo indirizzo IP può effettuare in un determinato periodo di tempo.
- Configurare una infrastruttura ridondante per garantire una continuità del servizio in caso di attacco.

3. Response

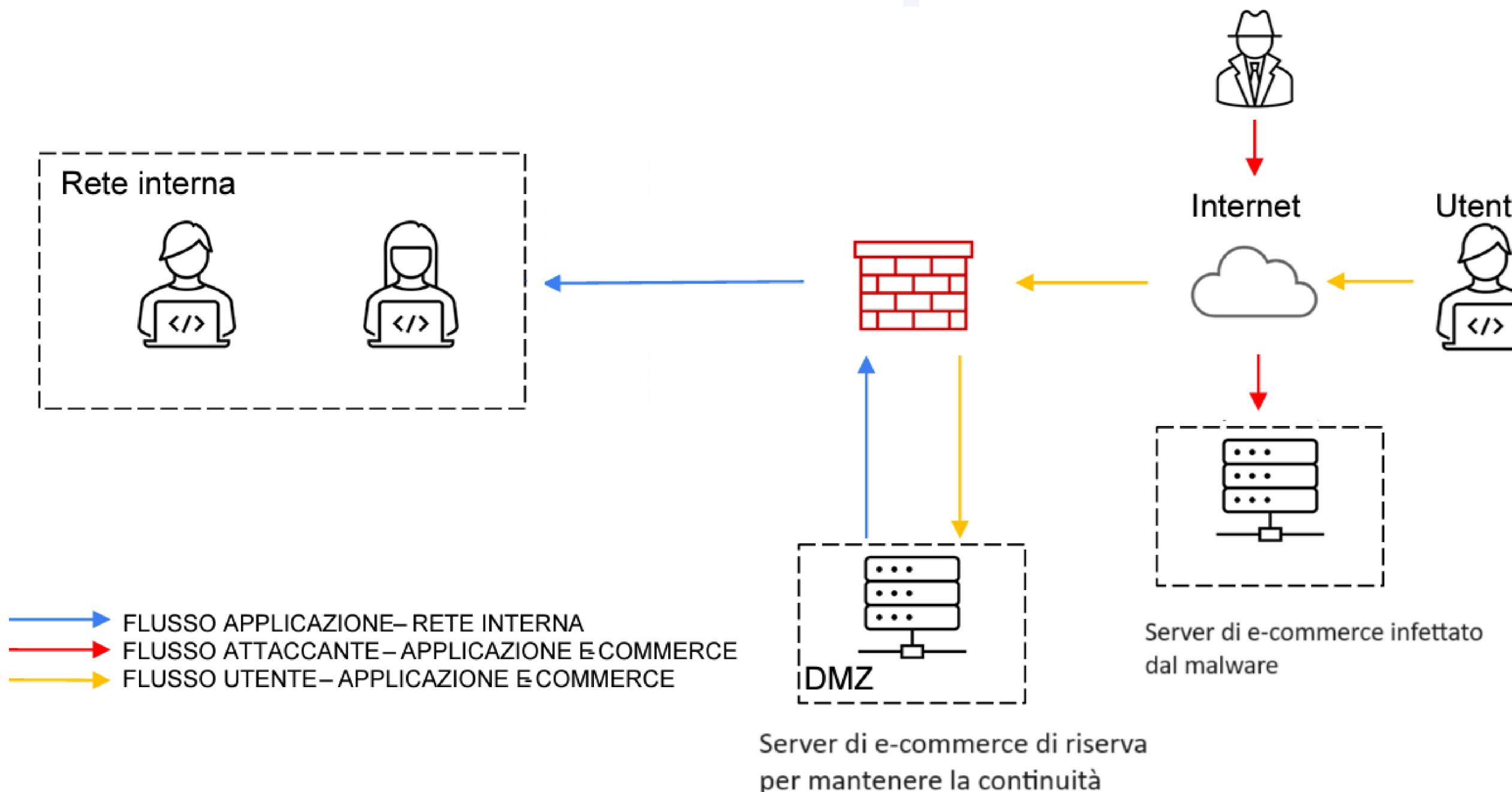
L'applicazione Web viene infettata da un malware.

La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

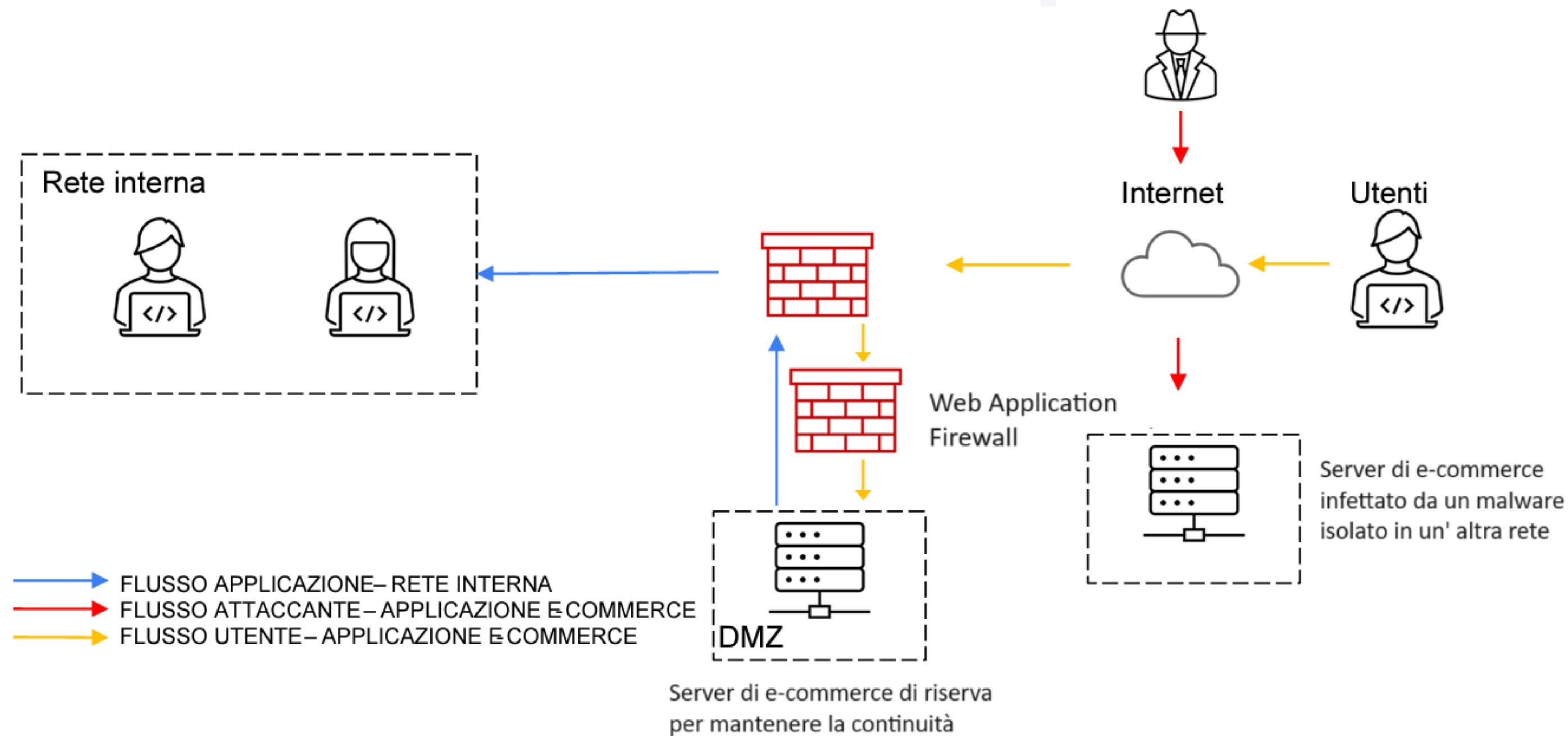
Modificare la figura con la soluzione proposta.

Se l'applicazione Web venisse infettata da un malware dovremmo evitare che il malware si propaghi nella nostra rete, se non fossimo interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata (magari per analizzare meglio l'attacco) potremmo decidere di non spegnere la macchina e di non scollegarla dalla rete; tuttavia dovremmo isolargliela in una rete diversa da quella della nostra azienda.

3. Response



4. Soluzione Completa



5. Modifica “più aggressiva”

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

Come già indicato nella risposta dell'esercizio 2 potremmo integrare altri elementi di sicurezza nella nostra architettura di rete. Calcolare il budget di 5000-10000€.

Oltre al WAF che abbiamo già integrato con il primo esercizio ed ad un IDS/IPS come suggerito nel secondo esercizio potremmo implementare dei software antivirus/antimalware, una VPN, soluzioni di Backup, piani di Disaster Recovery, formazione del personale e implementare il controllo multifattore per gli accessi.

Esercizio Bonus

The screenshot shows the AnyRun platform interface. At the top left is the logo 'ANY RUN' with the subtitle 'INTERACTIVE MALWARE ANALYSIS'. Below the logo is a blue button labeled '+ New analysis'. To the right of the button is a section titled 'Start your analysis' with the sub-instruction 'Interact with the OS directly from the browser window, and immediately see the feedback from your actions.' Below this are two main analysis options: 'Analyze URL' (Investigate phishing activity) and 'Analyze Files / Emails' (Investigate malicious activity and collect IOCs). A world map is visible in the background. On the left side, there is a sidebar with various links: 'Public reports', 'Threat Intelligence' (with a 'new' badge), 'Pricing', 'Contacts', 'FAQ', and 'Sign In'.

Analizzare le 2 segnalazioni caricate su anyrun e fare un piccolo report di ciò che si scopre relativo all'eventuale attacco spiegando ad utenti e manager la tipologia di attacco e come evitare questi attacchi in futuro.

- <https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6%20/>
- <https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2/>

Prima Segnalazione

Nella prima segnalazione possiamo notare che è stato rilevato il Phishing.

Ovvero una truffa informatica in cui un truffatore cerca di ottenere informazioni sensibili, come nomi utente, password e dettagli delle carte di credito, fingendosi un ente affidabile tramite email, messaggi o siti web falsi. L'obiettivo è ingannare le vittime per farle cliccare su link dannosi o fornire i loro dati personali.

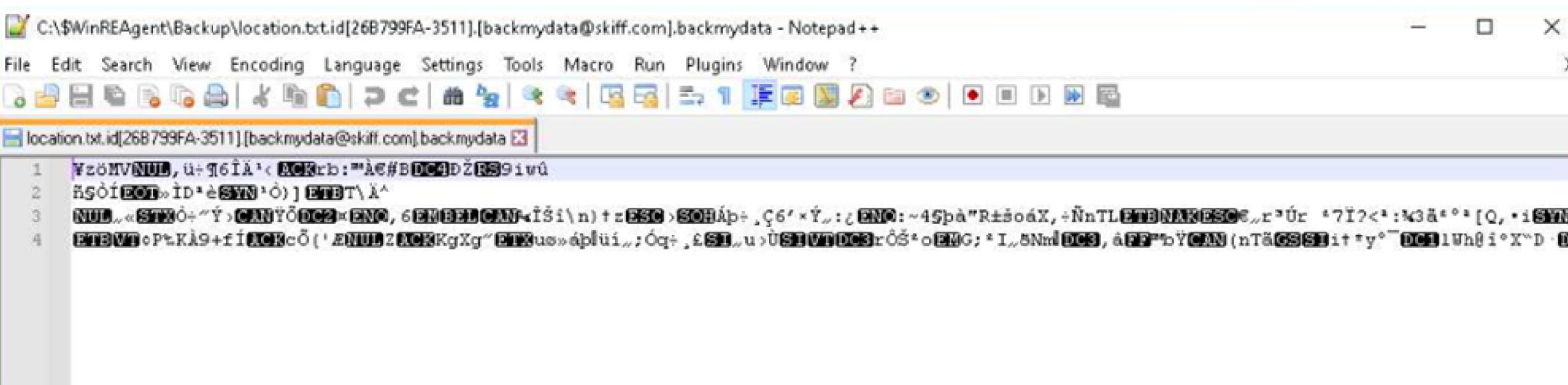


Purtroppo è una pratica molto comune e quindi è necessario formare il personale affinchè possa riconoscere queste tipo di mail, e anche con una formazione adeguata se non si sentissero sicuri di riconoscere se una mail è fraudolenta o meno evitare di aprirla/cliccare su link e contattare il dipartimento IT/Cyber Security per la conferma a se procedere o meno.

Seconda Segnalazione

Nella seconda segnalazione notiamo ancora che il programma anyrun ci segnala con certezza che si tratta di un azione malevola.

Considerando che i file sono stati criptati come vediamo in questa immagine:



The screenshot shows a Notepad++ window with the following content:

```
C:\$WinREAgent\Backup\location.txt.id[26B799FA-3511].[backmydata@skiff.com].backmydata - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
location.txt.id[26B799FA-3511].[backmydata@skiff.com].backmydata

1 VzÖMVNUL, 0+¶6ÍÀ`< ACKrb : "Àc#BDC4DZRS9ivù
2 ïgòíEOT»ID»èSYN:Ó] ETBT\À^
3 NUL,,«STXÓ+“Ý,CANYÓDC2»ENO, 6EMBELCAN<ÍSí\n)tzESC>SOHÁþ+,ç6'×Ý,:z ENO:~4Spà"R±šoáX,+ÑNTLETBNAKESCE,,r"Úr "7I?<:M3ä+“[Q,+iSYN
4 ETBVT»Pt.Kà9+fíACKcÔ('ENULZACKgXg"ETBUs»áplüi,,;Óq+,£SI,,u>ÙSIUTDC3rÔŠ»oEMG; * I,,SNm!DC3, àFP»bÝCAN(nTÄGSSEitt+y"~DC1lUh@i°X" D ·D
```

Probabilmente si è trattato di un ramsonware. Sfortunatamente recuperare i file (decriptarli) è molto difficile se non impossibile. Questi ramsonware sono stati creati per ricattare la vittima. In cambio di denaro ti promettono di darti la chiave per decriptare i dati.

Non c'è una vera e propria soluzione a questo problema, e proprio per questo motivo si raccomanda di effettuare con regolarità i backup per evitare di perdere dei dati importanti. Importante mantenere i backup non collegati alla rete, altrimenti non sarebbero al sicuro da eventuali attacchi rendendo di fatto il backup inutile.