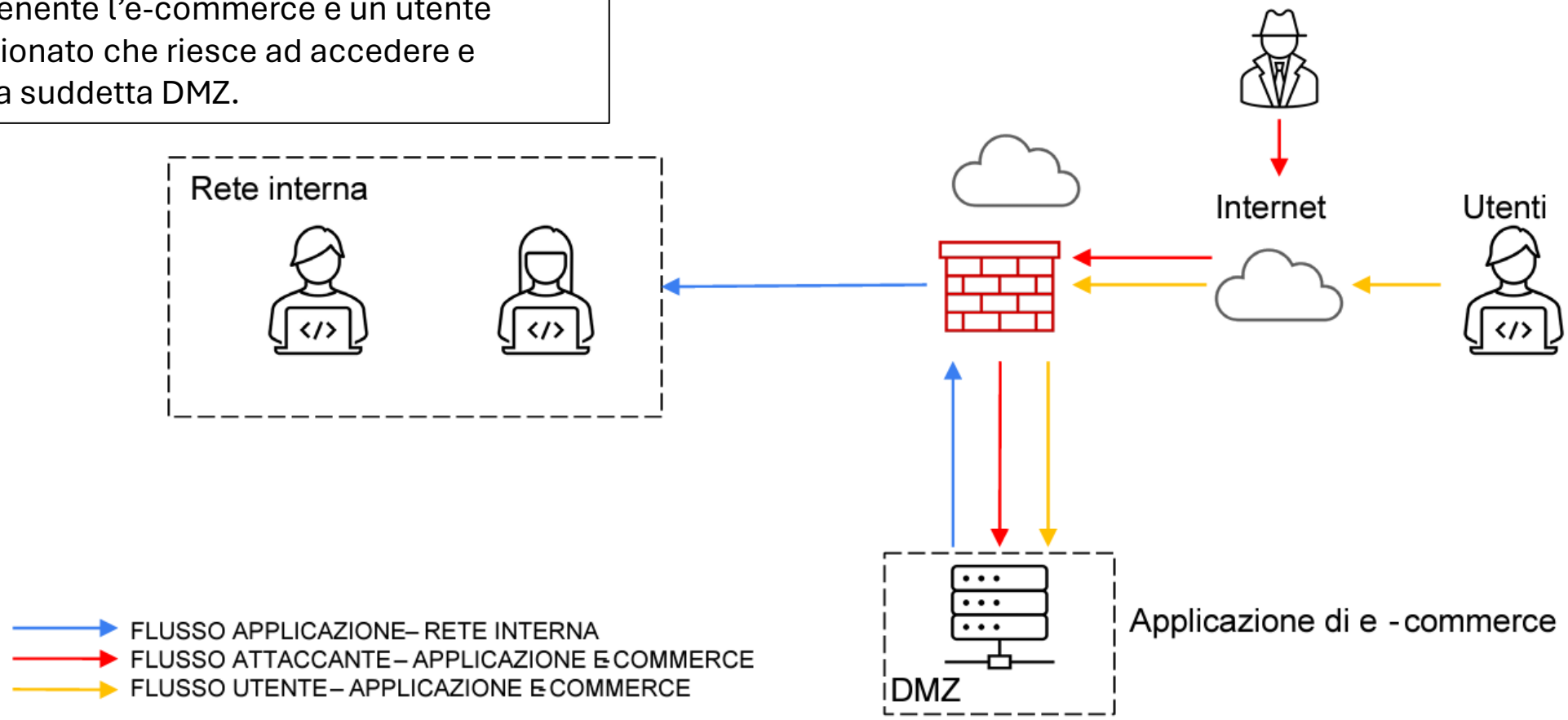
CONSEGNA SETTIMANA 9 LEZIONE 5

Threat prevention & Incident response

Supponiamo di essere stati ingaggiati per eseguire una serie di azioni per la threat prevention, l'incident response e il disaster recovery, tutte mansioni di competenza di un ipotetico team SOC (security operation center).

Prendiamo in esame la seguente situazione, che comprende una rete interna di una azienda, una DMZ contenente l'e-commerce e un utente malintenzionato che riesce ad accedere e infettare la suddetta DMZ.



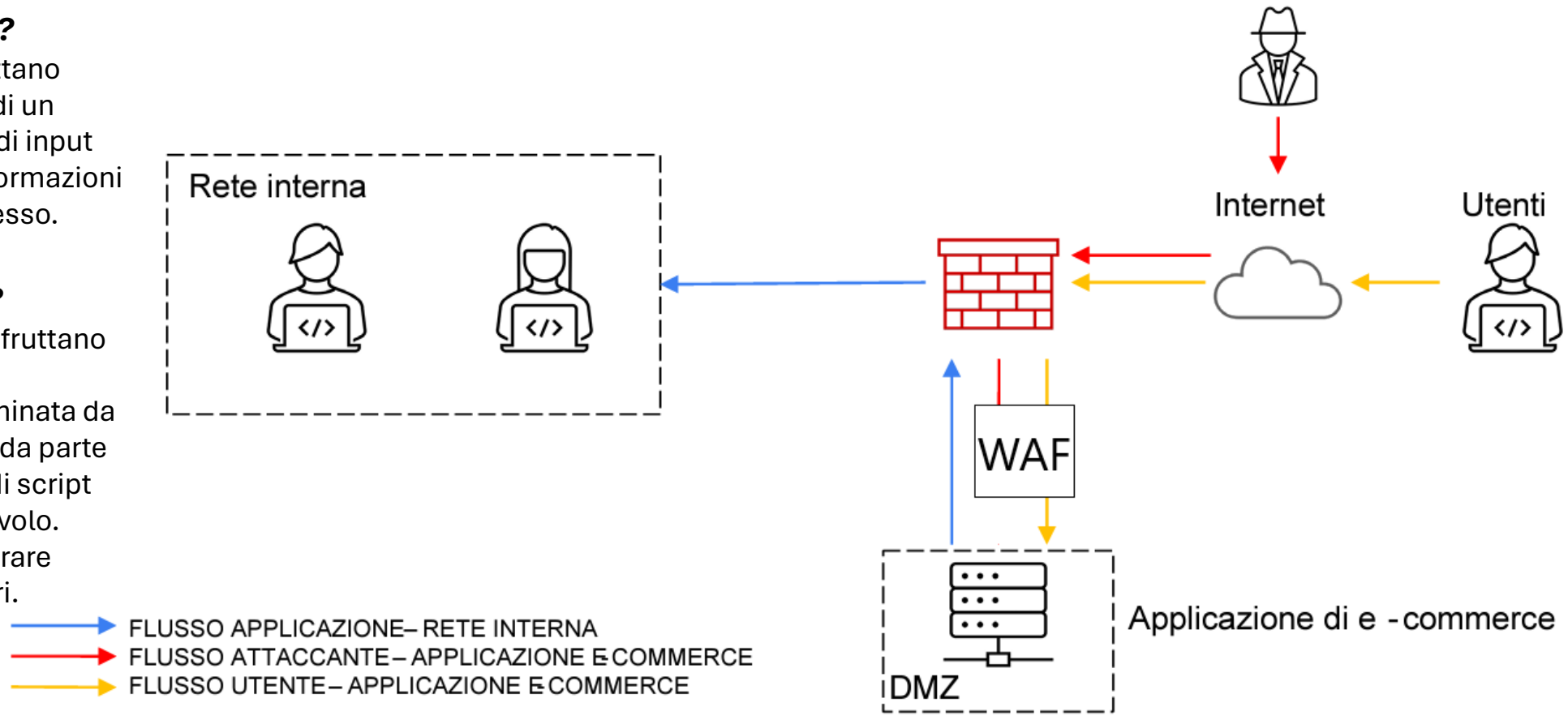
CONSEGNA SETTIMANA 9 LEZIONE 5
.1 - AZIONI PREVENTIVE

Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?

La principale soluzione per difendere applicazioni Web da attacchi di tipo SQLi e XSS è il **WAF** (**web application firewall**) che permette di filtrare le connessioni in ingresso, inserendo un secondo layer di protezione, difendendo nel nostro caso l'e-commerce da malintenzionati lasciando libero accesso agli utenti legittimi.

Cosa sono gli attacchi SQLi?
Gli attacchi sequel injection sfruttano vulnerabilità presenti all'interno di un database tramite l'uso malevolo di input SQL, con lo scopo di ottenere informazioni riservate salvate nel database stesso.

Cosa sono gli attacchi XSS?
Gli attacchi Cross-site scripting sfruttano una vulnerabilità presente nella applicazione Web, spesso determinata da una mancanza di configurazione da parte dello sviluppatore, tramite l'uso di script per poter immettere codice malevolo. Spesso vengono usati per recuperare cookie di sessione da utenti ignari.



CONSEGNA SETTIMANA 9 LEZIONE 5
.2 – IMPATTI SUL BUSINESS

L'applicazione Web subisce un attacco DDoS dall'esterno che rende irraggiungibile l'applicazione per 10 minuti. Calcolare l'impatto sul business considerando che ogni minuto vengono spesi circa 1500€. Implementare eventuali azioni preventive che si possono applicare in questa problematica.

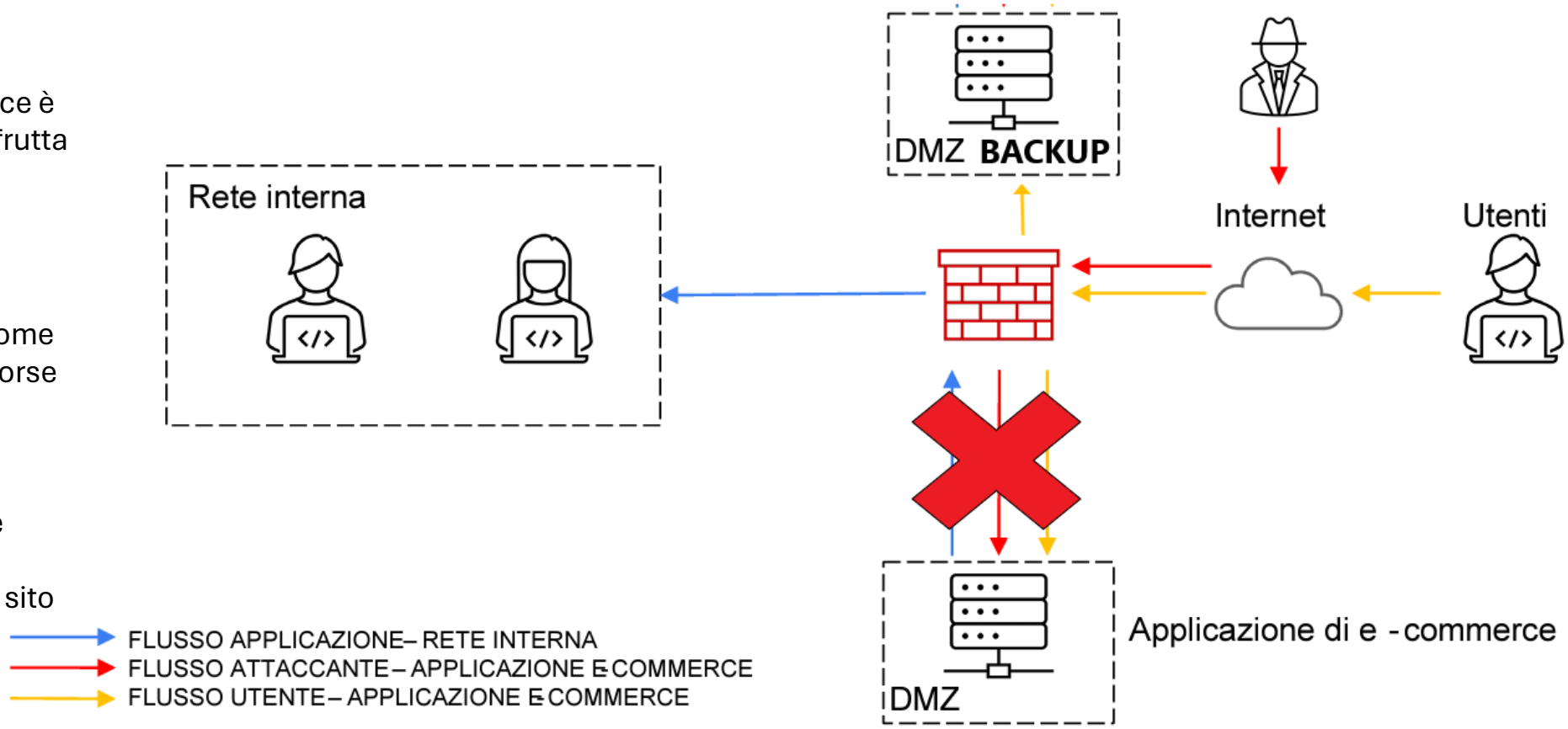
Possiamo calcolare l'impatto che questo attacco DDoS ha avuto sul business semplicemente moltiplicando l'ipotetico ingresso economico per il tempo in cui l'applicazione web rimane irraggiungibile (1.500 € x 10 min = 15.000 €). Una possibile prevenzione comprende l'implementazione di un **server clone di backup**, da mettere in funzione quando l'originale non è raggiungibile.

Cosa sono gli attacchi DDoS?

Gli attacchi distributed denial of service è una variante degli attacchi DoS che sfrutta molteplici fonti malevole, come ad esempio una botnet.

Cosa sono gli attacchi DoS?

Gli attacchi denial of service hanno come obbiettivo rendere inaccessibile le risorse di un determinato Sistema o sito web. Per fare ciò gli attaccanti creano un sovraccarico sul sistema (o sito web) inviando costantemente richieste che vengono accettate, consumando di conseguenza risorse e, nel caso di un sito web, larghezza di banda.



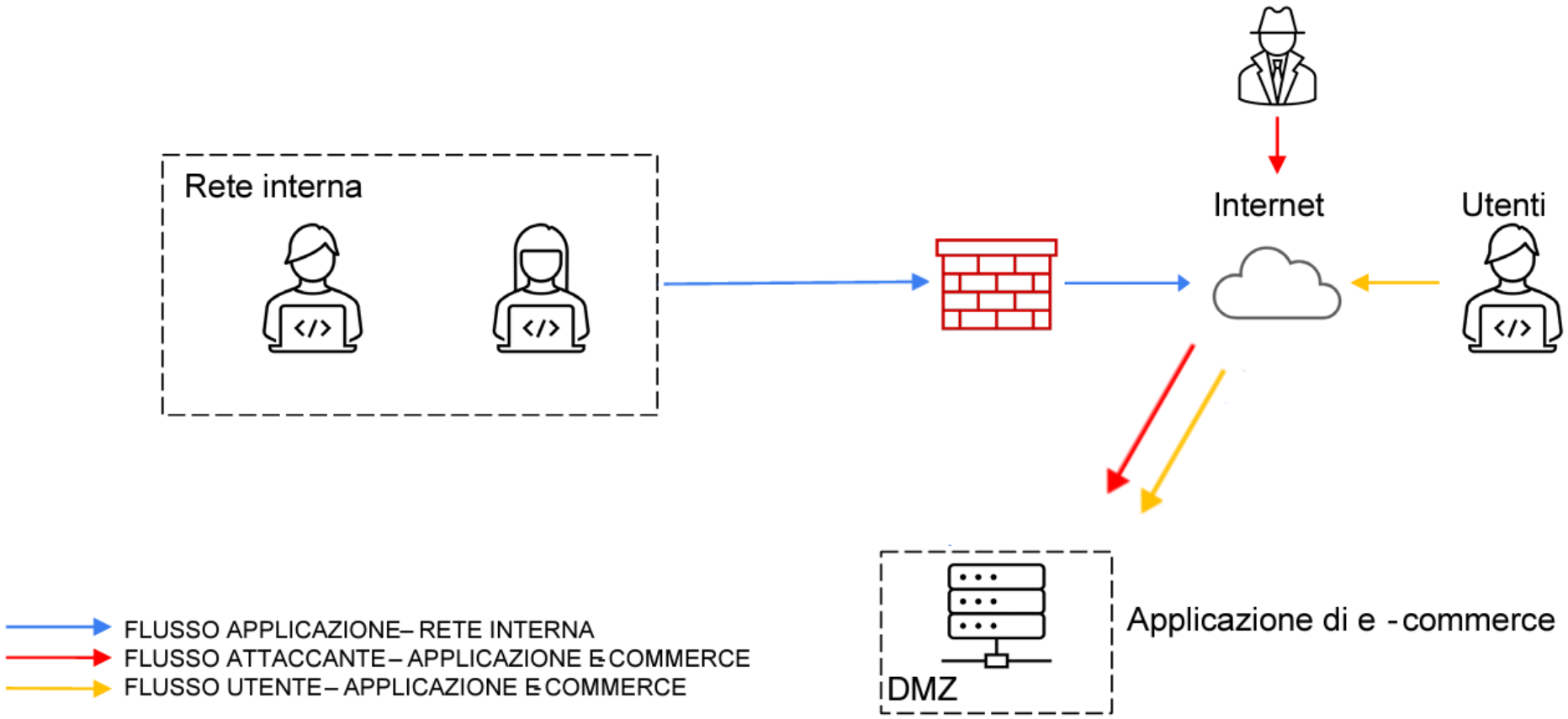
CONSEGNA SETTIMANA 9 LEZIONE 5
.3 - RESPONSE

L'applicazione Web viene infettata da un malware, come possiamo agire per evitare che si propaghi sulla rete interna?

Una prima soluzione per evitare che un malware presente in un sistema (nel nostro caso l'applicazione Web) infetto possa propagarsi all interno della rete locale è l '**isolamento**. In questo caso creeremo una **rete di quarantena** contenente solo la DMZ infetta ma mantenendo l'accesso alla rete internet. In questo modo non sarà possibile per l'attaccante poter infettare il resto della rete interna.

Cos'è un malware?

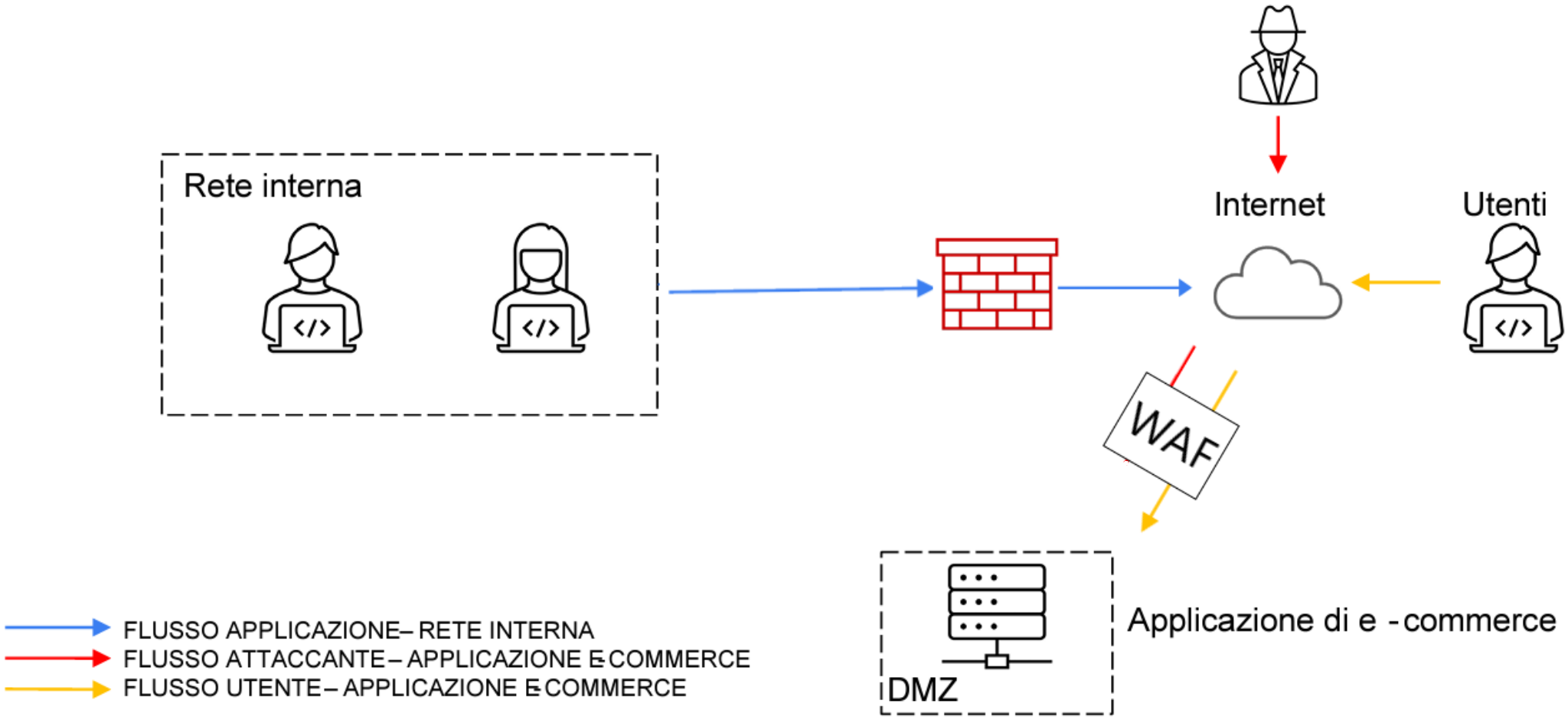
Con malware (abbreviazione di malicious software) facciamo riferimento ad un qualsiasi codice o programma ideato appositamente per danneggiare un sistema informatico. A differenza di un exploit, un malware crea lui stesso una vulnerabilità non presente in un sistema per poi sfruttarla. Delle varie sottocategorie dei malware ricordiamo i ransomware, gli adware e i più noti virus. Tra I vari obbiettivi dei malware ci sono ottenere accesso non autorizzato a dati sensibili, recuperare credenziali di Accesso e interrompere il corretto funzionamento dei servizi su un sistema.



CONSEGNA SETTIMANA 9 LEZIONE 5
.4 SOLUZIONE COMPLETA

Unire le soluzione del punto 1 e del punto 3 per una soluzione completa.

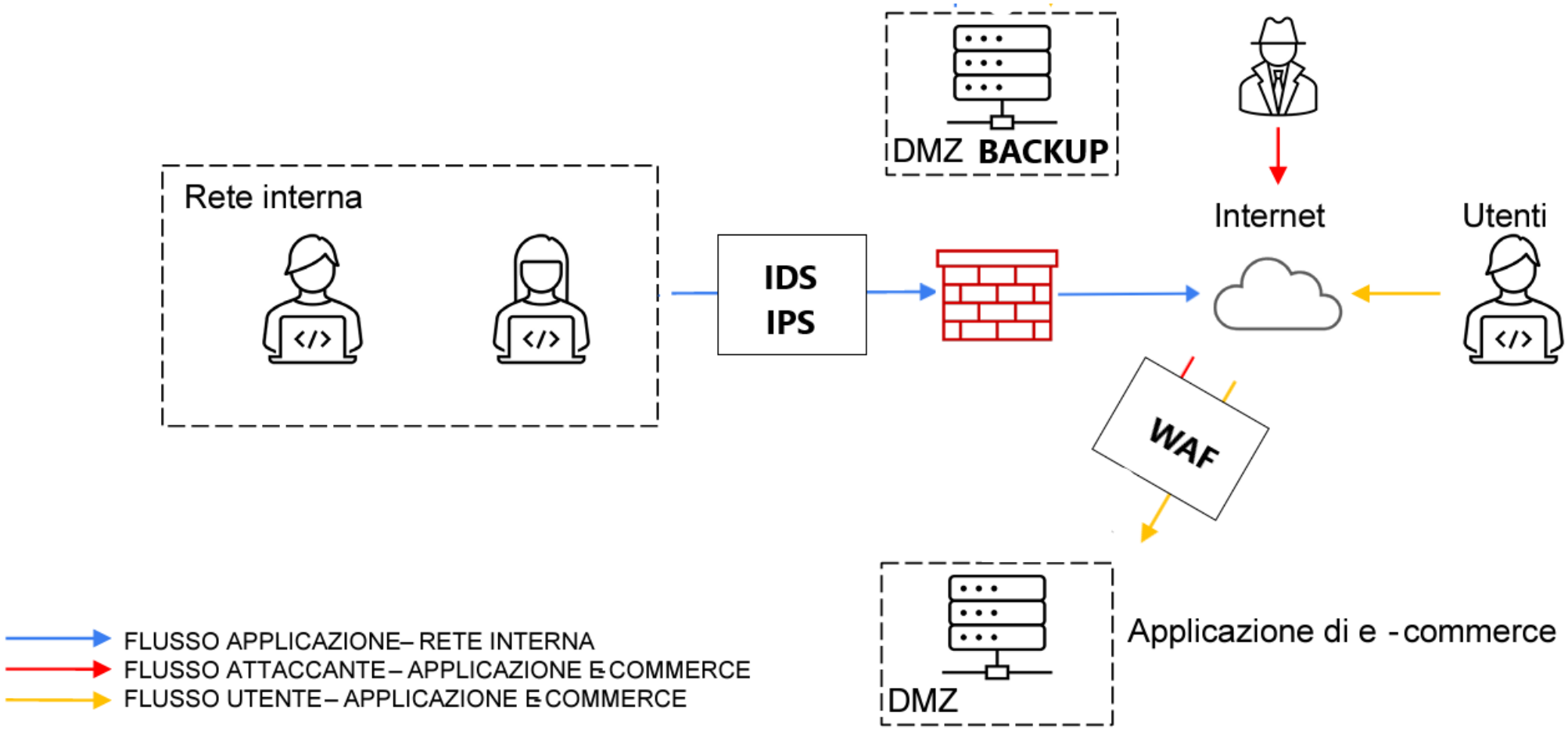
Unendo le soluzioni implementate nelle task precedenti (1 e 3) possiamo ricreare la rete in questo modo. La DMZ si troverà su una rete di quarantena, non consentendo la propagazione di eventuali malware sulla rete interna, e allo stesso tempo verrà difesa da un WAF, limitando i possibili attacchi SQLi e XSS.



CONSEGNA SETTIMANA 9 LEZIONE 5
.5 – MODIFICHE AGGRESSIVE

Come possiamo implementare una modifica più aggressiva, integrando altri elementi di sicurezza?

Una possibile implementazione per aumentare la sicurezza della rete comprende, dopo aver isolato preventivamente la DMZ principale e implementato il WAF, una DMZ clone secondaria in caso di attacchi DDoS per garantire la continiutà del servizio di e-commerce e un IPS/IDS per la rete interna.

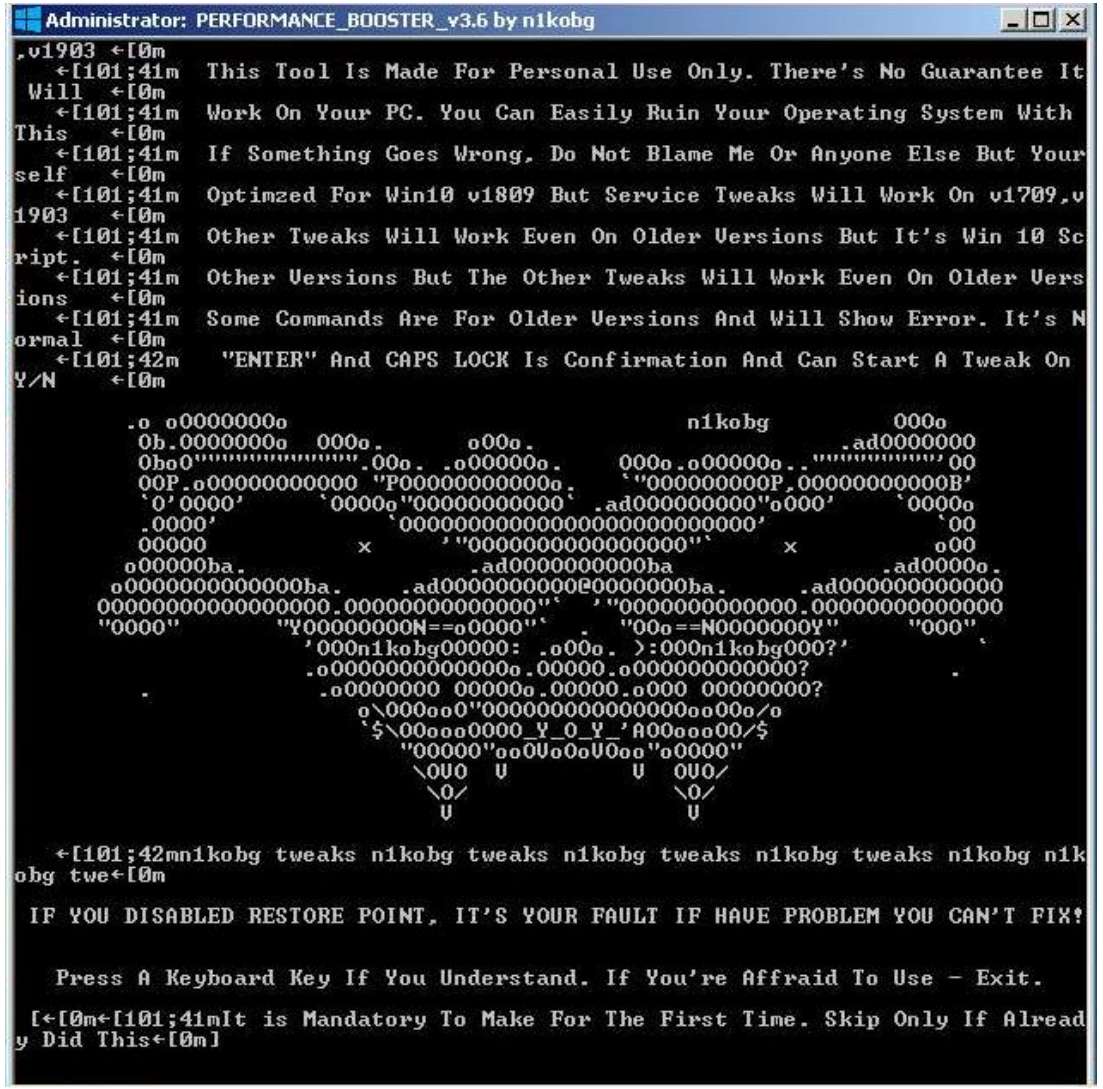


CONSEGNA SETTIMANA 9 LEZIONE 5
BONUS – ANALISI I

Analizziamo due segnalazioni caricate su Anyrun, come avviene l'attacco? Come si possono evitare simili minacce?

La prima segnalazione fa riferimento ad un software nominato **PERFORMANCE_BOOSTER.**

Come avviene l'attacco?
Questa applicazione potenzialmente malevola effettua il suo attacco richiamando inizialmente il prompt dei comandi come amministratore.
Modifica le policy per l'esecuzione di windows Powershell, per poi modificare i permessi di file e cartelle (comprese le nascoste) all'interno del sistema.
Tramite poi il registro di sistema effettua una ricerca per eventuali software installati, il path di installazione di Microsoft Outlook, la presenza del framework .NET e eventuali connessioni RDP passate.
Tutte queste attività malevole non vengono eseguite in autonomia dal software, ma richiede un input iniziale consapevole da parte dell'utente.
Considerando la falsa natura del software, che ipotizzo finga di poter migliorare le prestazioni del computer, è logico pensare che un ignaro utente abbia scaricato ed avviato il software proprio per questo motivo, inconsapevole delle possibili minacce contenute all interno.



Come si possono evitare tali minacce?
Partendo dal presupposto che software che garantiscono di migliorare le prestazioni del sistema spesso nascondono al loro interno qualche scopo malevolo è consigliabile verificare la fonte del software che si intende scaricare prima di eseguire il download.

CONSEGNA SETTIMANA 9 LEZIONE 5
BONUS – ANALISI II

Analizziamo due segnalazioni caricate su Anyrun, come avviene l'attacco? Come si possono evitare simili minacce?

La seconda segnalazione fa riferimento ad un software nominato **Microsoft edge update.**

Analizzando la seconda segnalazione presente su Anyrun, ad una prima occhiata potrebbe sembrare che il software durante l'installazione ottenga l'accesso non consentito ad eventuali file e cartelle inusuali.
Ma ricontrollando la fonte del file scaricato si può evincere che è una fonte sicura, ovvero **microsoft**, con un **endpoint per il download verificato**.
Pertanto non vedo altri possibili parametri che possano ricondurre il file scaricato ad una attività malevola.