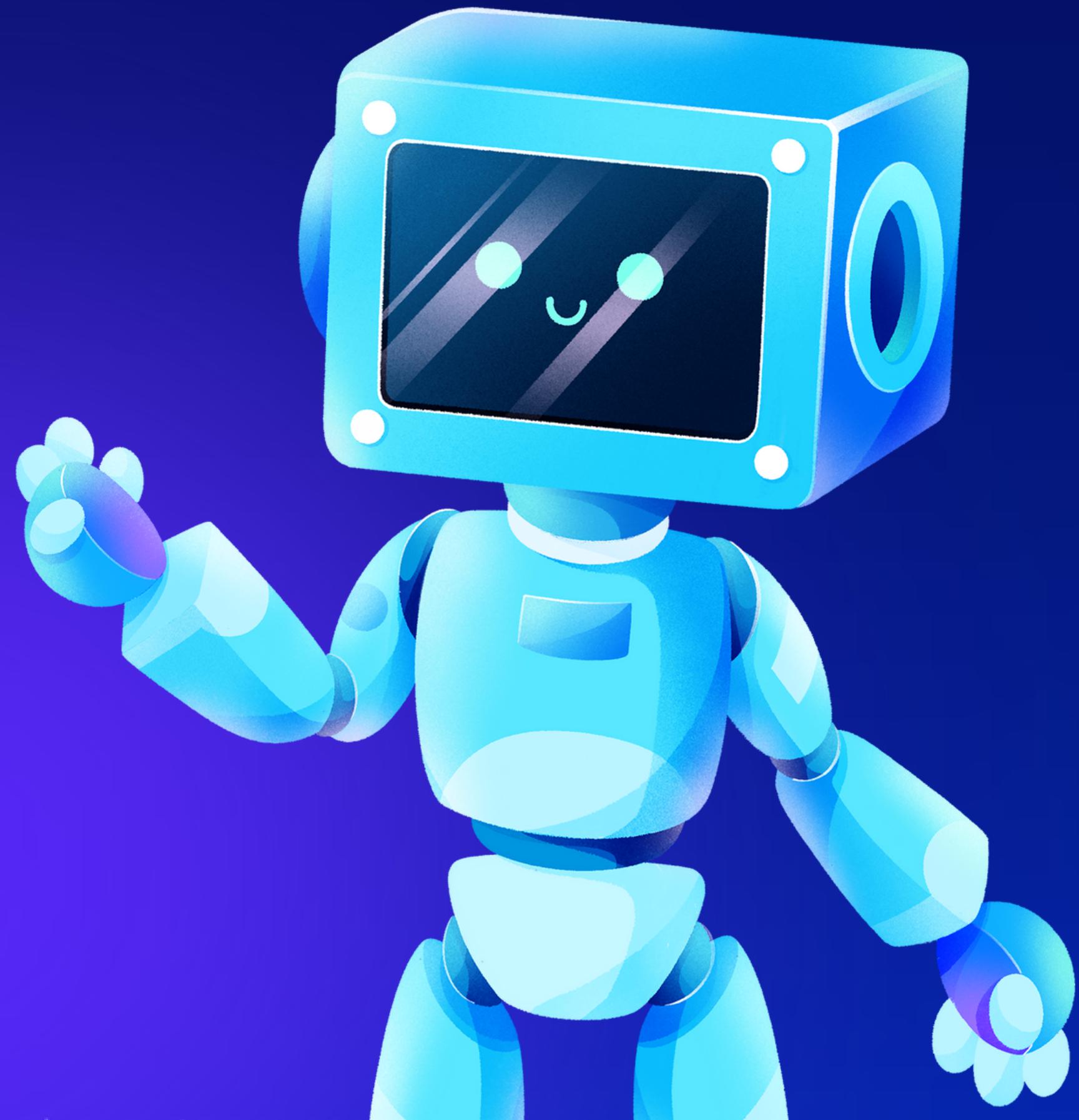


S9 / L5

WEEK-END PROJECT

Riccardo Agostino Monti





INDICE

- | | |
|------------------------|----|
| • Traccia | 01 |
| • Azioni Preventive | 02 |
| • Impatti sul Business | 03 |
| • Response | 04 |



TRACCIA

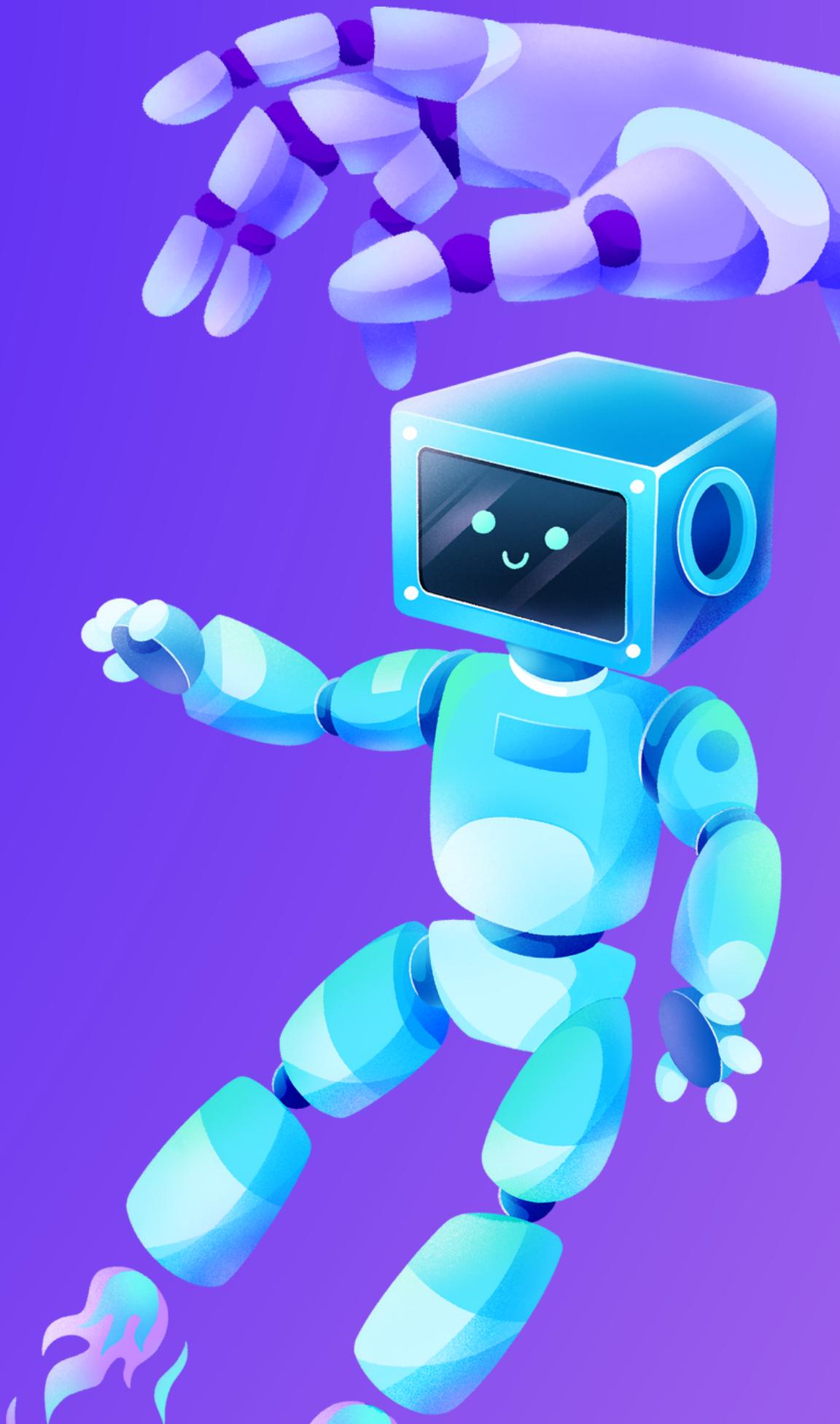


Con riferimento alla figura nella slide successiva, rispondere ai seguenti quesiti.

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.

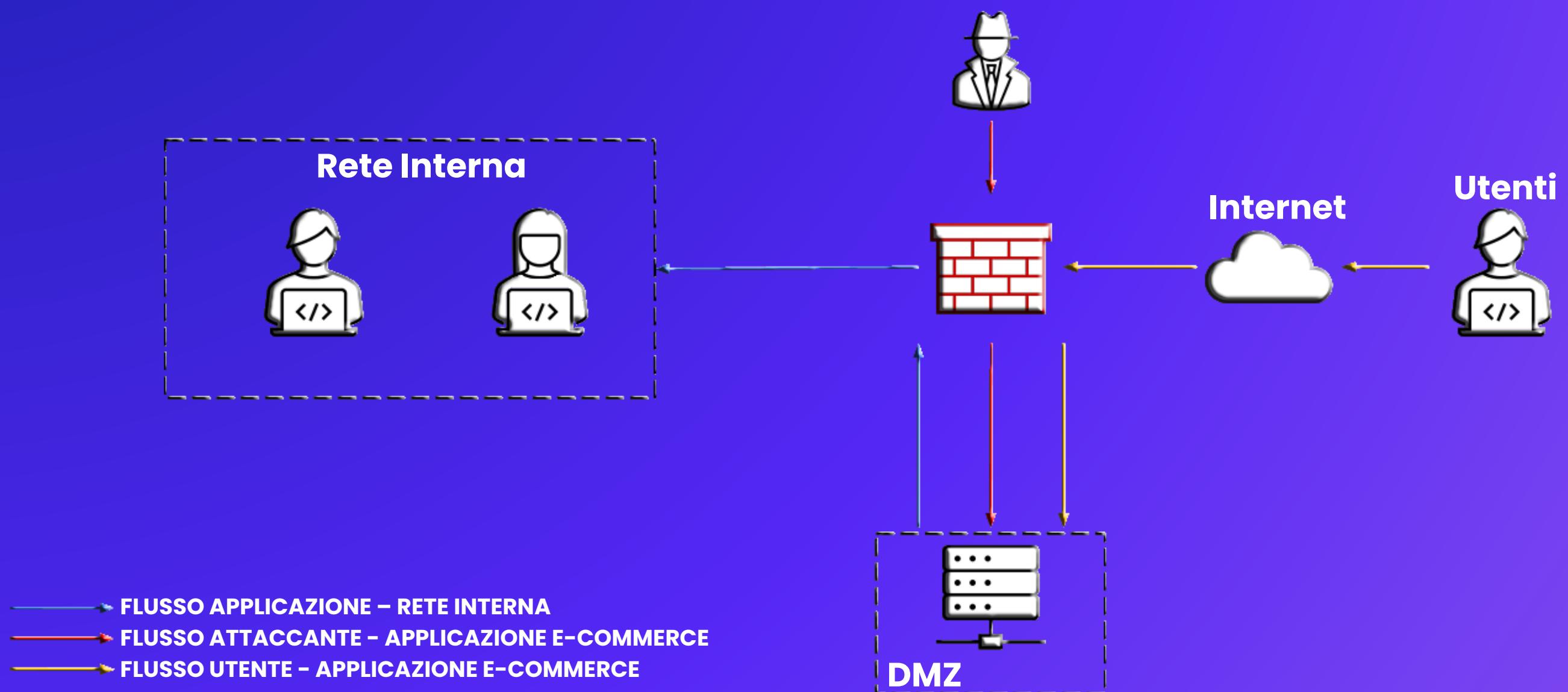
3. **Response:** l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.



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.



DMZ

La DMZ, acronimo di "Demilitarized Zone", (Zona Demilitarizzata) è una rete perimetrale che protegge la rete locale (LAN) interna di un'organizzazione dal traffico non attendibile. Essa indica comunemente una sottorete che si trova tra la rete Internet pubblica e le reti Private.

Le organizzazioni in genere archiviano nella DMZ servizi e risorse rivolti all'esterno, nonché server DNS, FTP, posta, proxy, VoIP e server Web. Questi server e risorse sono isolati e dispongono di un accesso limitato alla rete LAN, per garantire che sia possibile accedervi tramite Internet ma tenendo la rete LAN interna in sicurezza.

In pratica, un approccio con la DMZ rende più difficile per un hacker ottenere l'accesso diretto ai dati e ai server interni di un'organizzazione tramite internet.

Rete Interna

Una rete interna aziendale, nota anche come Intranet, è una rete aziendale che è completamente isolata dalla rete esterna (Internet) a livello di servizi offerti. Questa rete rimane solo a uso interno, comunicando eventualmente con la rete esterna e altre reti attraverso opportuni sistemi di sicurezza, come firewall o proxy server. In sintesi, una rete interna è un sistema di comunicazione sicuro e isolato utilizzato per lo scambio di informazioni all'interno di un'organizzazione. Questa rete può essere estesa per includere utenti attraverso l'uso di VPN o Extranet, garantendo al contempo la sicurezza dei dati e delle informazioni.

Firewall

All'interno della rete è presente un Firewall, un sistema di sicurezza della rete informatica che limita il traffico Internet in entrata, in uscita o all'interno di una rete privata. Questo software o unità hardware-software dedicata, funziona bloccando o consentendo in maniera selettiva i pacchetti di dati.

Un Firewall decide quale traffico di rete può passare e quale è pericoloso, separando l'attendibile dal non attendibile. I Firewall sono pensati per garantire la sicurezza delle reti private e dei dispositivi endpoint al loro interno, detti host di rete. Ne esistono di vari tipi, come quello con filtro di pacchetti, con analisi dello stato della connessione a livello di applicazioni. Nel nostro caso non ci è dato sapere che tipo di Firewall è utilizzato.

AZIONI PREVENTIVE





Per salvaguardare le applicazioni web da potenziali minacce come gli attacchi XSS (Cross-Site Scripting) e SQLi (SQL Injection), è possibile adottare preventivamente una soluzione basata su un Web Application Firewall (WAF). Questo strumento, a differenza dei firewall tradizionali, è specificamente progettato per proteggere le applicazioni web da tali tipi di attacchi. Se immaginiamo la nostra rete, l'aggiunta di un WAF modificherebbe la configurazione iniziale. Ad esempio, se consideriamo la rete presentata nelle slide precedenti, il WAF sarebbe posizionato in modo da proteggere il traffico in entrata sulla Web App proveniente da Internet.

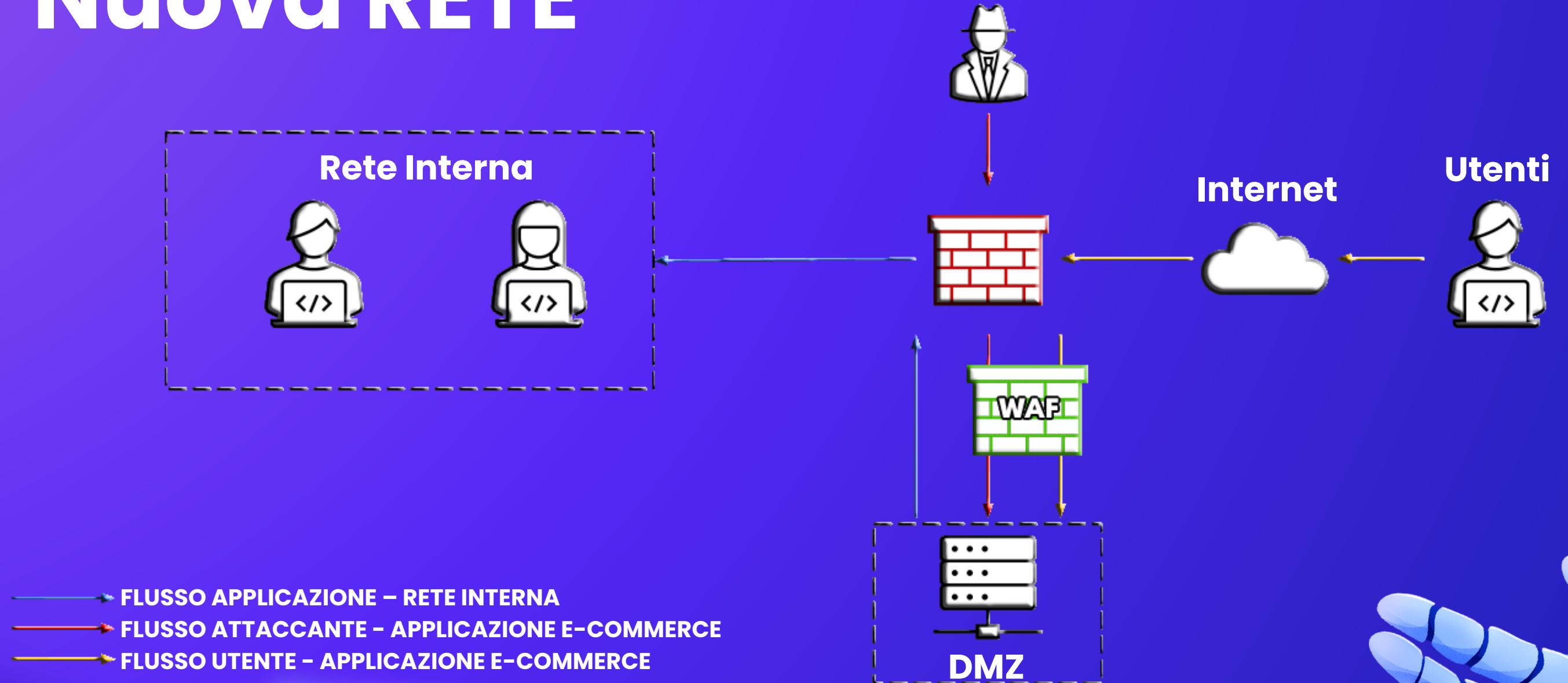
WAF

Nel contesto di una rete aziendale, il WAF agisce come un baluardo tra l'applicazione web e il traffico Internet in entrata, che può includere sia utenti legittimi che potenziali aggressori. Questo significa che tutte le richieste web dirette all'applicazione passano prima attraverso il WAF, che esamina ogni richiesta alla ricerca di possibili segnali di attività sospetta o malevola. Operando quindi al settimo livello della pila ISO/OSI (Application Server).

In questo modo, il WAF fornisce un ulteriore livello di sicurezza, filtrando attivamente il traffico web per identificare e bloccare gli attacchi prima che possano raggiungere l'applicazione web. Questo non solo aiuta a proteggere l'applicazione stessa, ma anche i dati sensibili che potrebbero essere esposti in caso di una violazione della sicurezza.

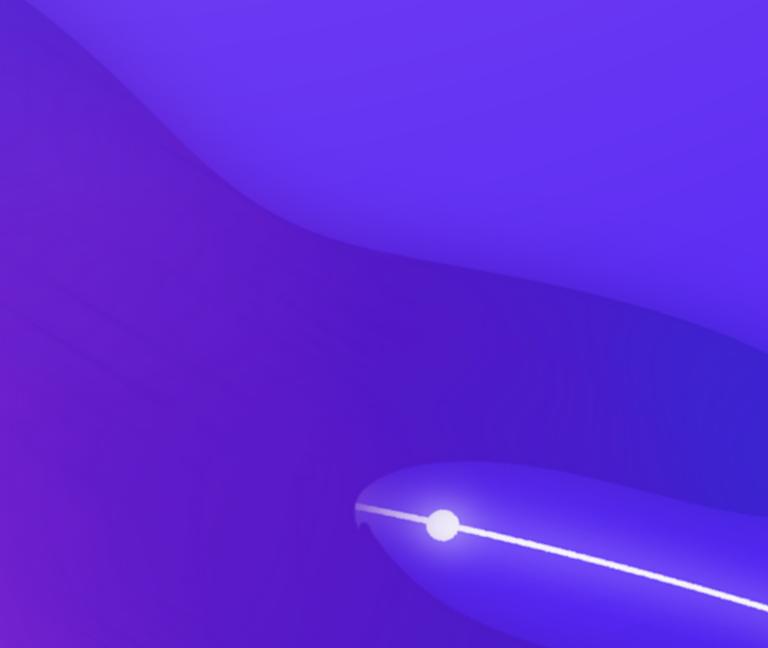
Inoltre, l'uso di un WAF può aiutare a garantire la conformità con vari standard e regolamenti di sicurezza informatica, fornendo un registro dettagliato di tutte le attività di rete.

Nuova RETE



IMPATTI SUL BUSINESS





Un attacco DDoS ha reso inaccessibile una piattaforma di e-commerce per un periodo di 10 minuti. Se consideriamo che gli utenti normalmente spendono all'incirca 1.500€ ogni minuto, possiamo calcolare l'impatto economico di questo downtime. Moltiplicando la spesa media al minuto degli utenti (1.500€) per la durata dell'interruzione del servizio (10 minuti), otteniamo un valore di 15.000€. Questo significa che, a causa di questi 10 minuti di inattività, l'azienda ha perso la possibilità di guadagnare 15.000€ dalle potenziali vendite.

Tuttavia, è importante notare che questo è solo l'impatto immediato. Gli attacchi DDoS possono anche avere effetti a lungo termine, come la perdita di fiducia dei clienti e danni alla reputazione dell'azienda, che possono essere molto più costosi nel lungo periodo.

DDoS

Un attacco DDoS, o Distributed Denial of Service, è una forma di attacco informatico che ha l'obiettivo di rendere un servizio online, come un sito web, inutilizzabile inondandolo con un volume di traffico di rete eccessivo.

Durante un attacco DDoS, l'attaccante sfrutta una rete di computer, spesso denominata "botnet", per inviare un gran numero di richieste al sistema bersaglio. Queste richieste possono superare la capacità del sistema di gestirle, provocando rallentamenti o addirittura un'interruzione totale del servizio.

Gli attacchi DDoS possono essere diretti contro vari tipi di servizi online, tra cui siti di e-commerce, casinò online e qualsiasi altra azienda o organizzazione che offre servizi online. L'obiettivo finale di un attacco DDoS è di interrompere il normale funzionamento del servizio web, causando un "rifiuto del servizio".

RESPONSE



Tenendo conto dell'urgenza, è possibile implementare un approccio che prevede l'isolamento del computer infetto. In questa situazione, la DMZ sarà connessa direttamente a internet, accessibile all'aggressore, ma non sarà più collegato alla rete interna. L'immagine nella slide successiva illustra la soluzione che impiega la tattica dell'isolamento del server infetto. Si può notare che non c'è più alcuna comunicazione tra l'applicazione web e la rete interna.

Isolamento

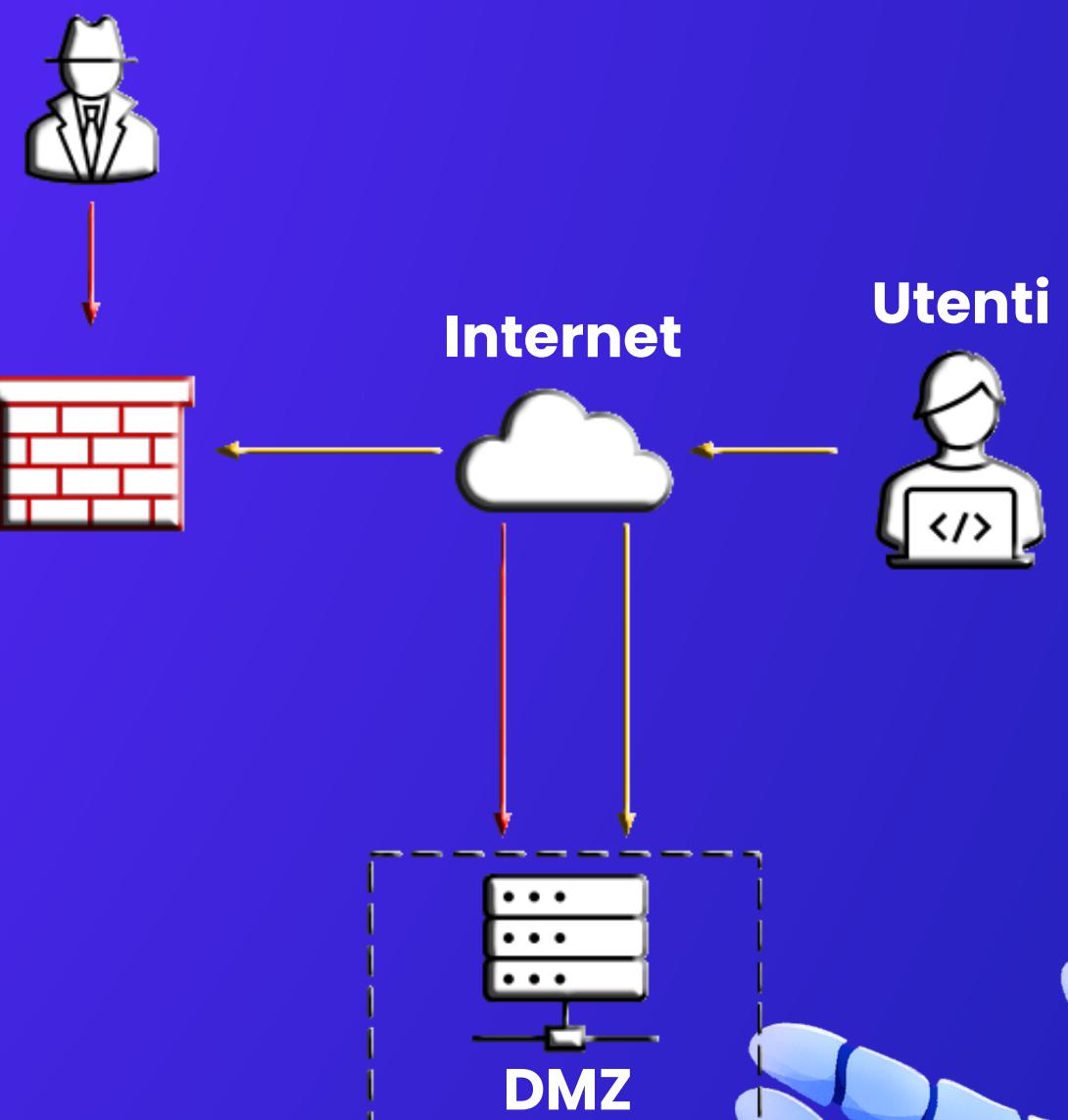
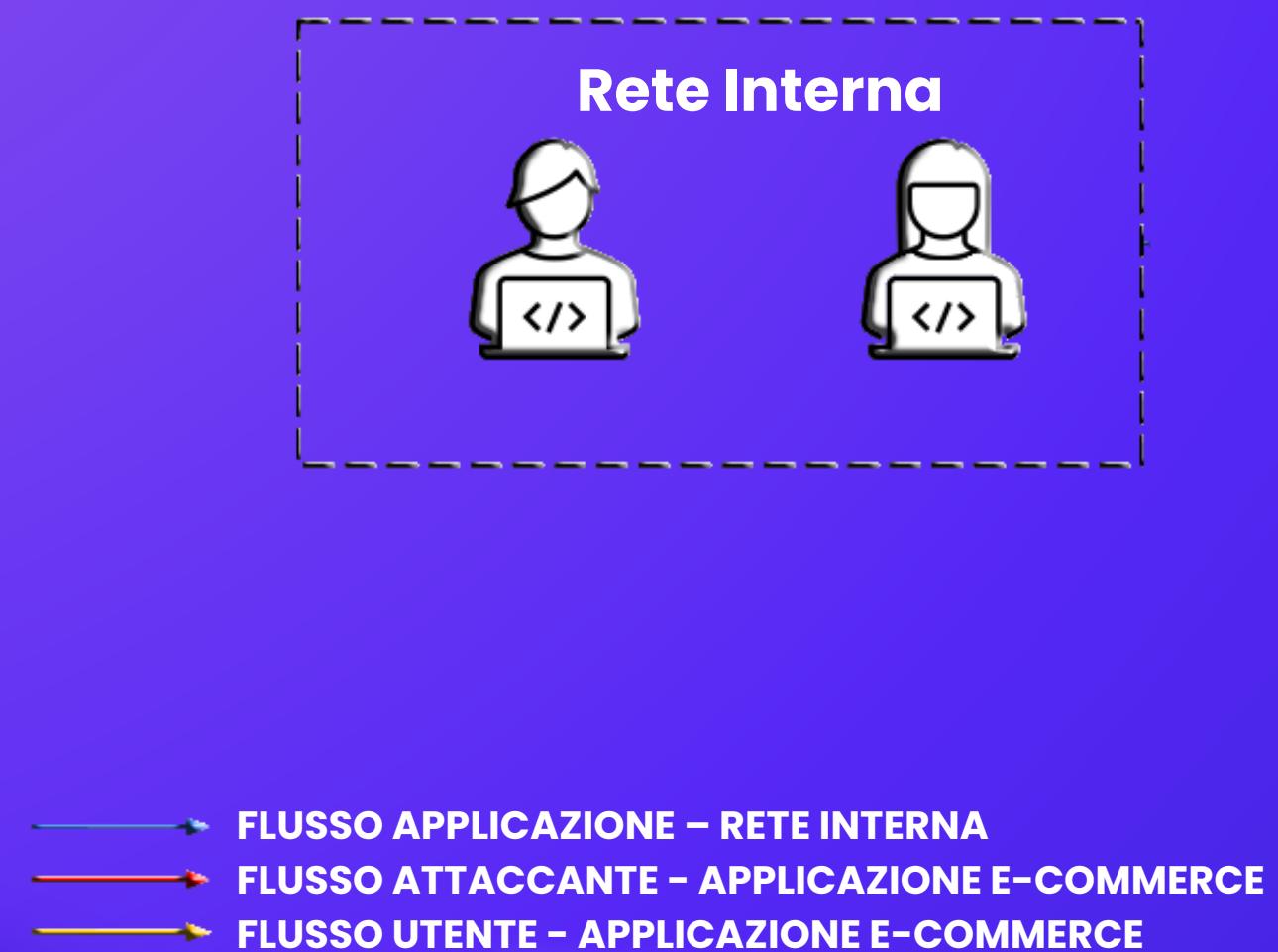
Quando si parla di isolamento di una macchina infetta, ci si riferisce a un approccio di sicurezza informatica che prevede la disconnessione del computer infetto dalla rete interna e la sua connessione diretta a internet. Questo è fatto per prevenire la diffusione dell'infezione ad altre macchine sulla rete interna.

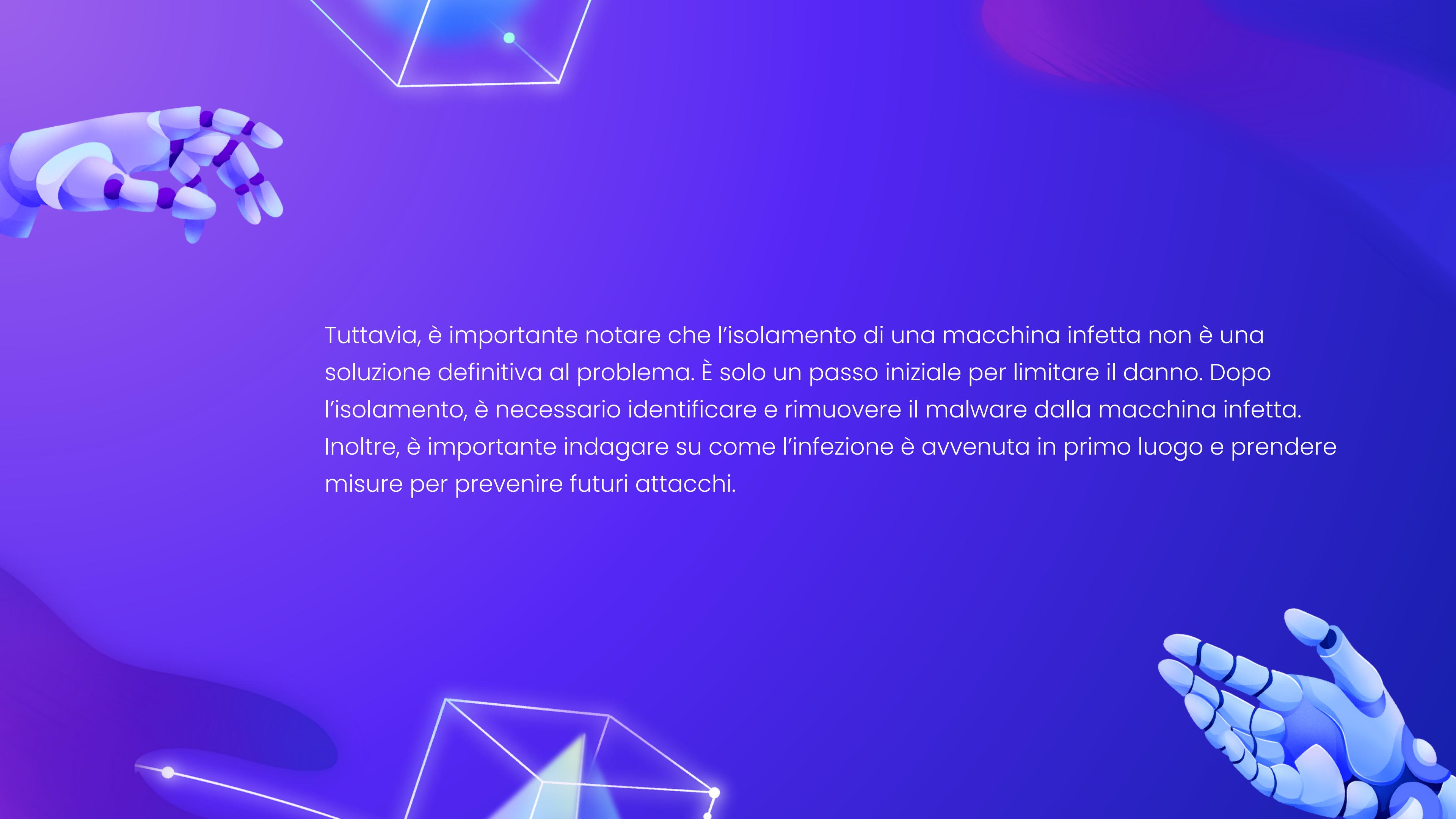
L'isolamento della macchina infetta è una strategia efficace per limitare il danno causato da un attacco informatico. Una volta che la macchina è isolata, l'attaccante può ancora accedervi, ma non può più raggiungere o infettare altre macchine sulla rete interna.

La figura nella prossima slide illustra questa strategia. Si può notare che non c'è più alcuna comunicazione tra l'applicazione web sulla macchina infetta e la rete interna.

Questo significa che l'applicazione web non può più essere utilizzata come un veicolo per diffondere l'infezione.

Nuova RETE





Tuttavia, è importante notare che l'isolamento di una macchina infetta non è una soluzione definitiva al problema. È solo un passo iniziale per limitare il danno. Dopo l'isolamento, è necessario identificare e rimuovere il malware dalla macchina infetta. Inoltre, è importante indagare su come l'infezione è avvenuta in primo luogo e prendere misure per prevenire futuri attacchi.

