



MARIA HUAPAYA





ANALISI DEI LOG







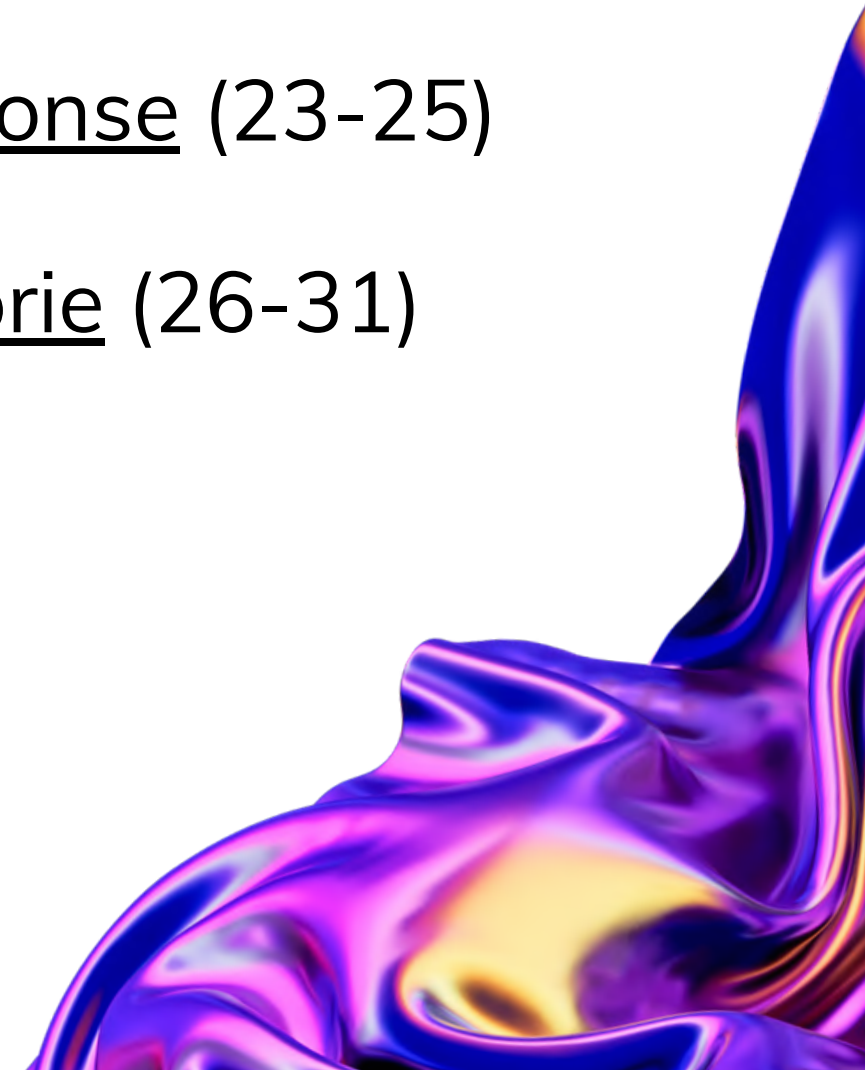
Indice

Suggerimento: utilizza i link per passare a un'altra pagina della presentazione.

Come: evidenzia il testo, clicca sul simbolo del link e seleziona la pagina della presentazione che vuoi collegare.

-  [Traccia](#)
-  [Task 1: Cenni alla teoria](#) (5-8)
-  [Task 1: Azioni preventive](#) (9-11)
-  [Task 2: Cenni alla teoria](#) (12-13)

-  [Task 2: Impatti sul business](#) (14-18)
-  [Task 3: Cenni alla teoria](#) (19-22)
-  [Task 3: Incident Response](#) (23-25)
-  [Suggerimenti e migliorie](#) (26-31)





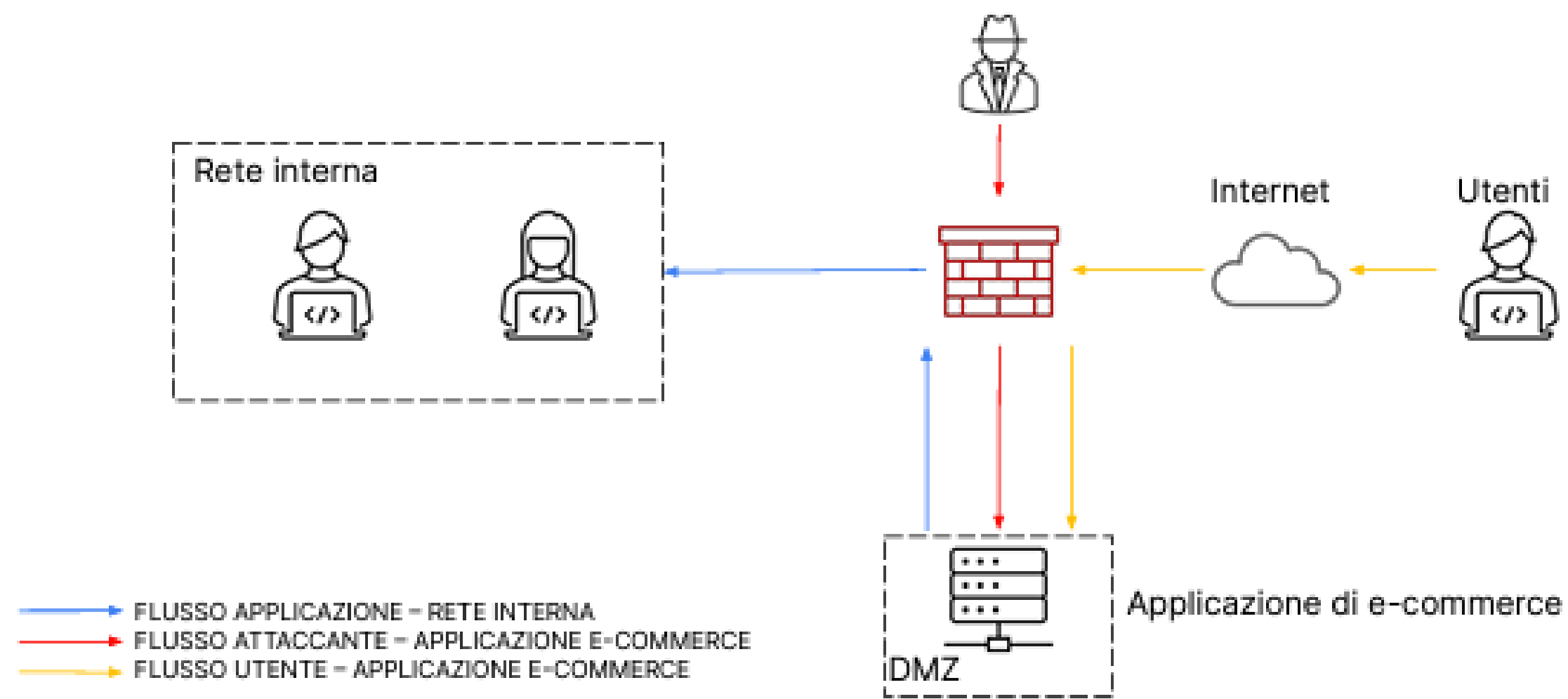
Traccia

Con riferimento alla figura in slide 4, 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 vostra 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.



[TORNA ALL'INDICE](#)

Task 1: Cenni alla teoria

Nell'ambito della gestione della sicurezza informatica, i servizi operativi di sicurezza sono strutturati seguendo un approccio metodologico che prende in considerazione il timing degli eventi critici, meglio identificati come incidenti di sicurezza. Tali incidenti sono definiti da una gamma ampia di azioni che hanno il potenziale di impattare negativamente sulla triade fondamentale della sicurezza informatica: la confidenzialità, l'integrità e la disponibilità delle risorse IT. Queste risorse comprendono dati, hardware, software, infrastrutture di rete e sistemi critici che supportano le operazioni quotidiane di un'organizzazione.

Gli incidenti di sicurezza possono manifestarsi in una varietà di scenari, inclusi ma non limitati a violazioni effettive o tentate dei sistemi di informazione, attacchi mirati a compromettere le difese informatiche o situazioni che indicano un pericolo imminente di tali violazioni. Questi eventi possono essere il risultato di azioni deliberate da parte di attori esterni o interni all'organizzazione, errori umani, fallimenti tecnologici o lacune nei processi e nelle politiche di sicurezza.

Tra gli esempi più significativi e frequentemente riscontrati di incidenti di sicurezza, meritano una menzione particolare:

- **La perdita o l'esposizione non autorizzata di dati sensibili:** questo tipo di incidente si verifica quando informazioni confidenziali, come dati personali, finanziari, o intellettuali, vengono divulgate intenzionalmente o accidentalmente a soggetti non autorizzati. Le conseguenze possono variare dalla violazione della privacy all'esposizione a rischi finanziari e reputazionali per l'individuo o l'organizzazione colpita.
- **Accessi non autorizzati ai sistemi interni:** incidenti di questa natura si verificano quando individui malintenzionati, sfruttando vulnerabilità tecniche o sotterfugi come l'ingegneria sociale, riescono a infiltrarsi nei sistemi interni di un'entità. Questo permette agli attaccanti di acquisire il controllo di risorse critiche, modificare dati, effettuare operazioni fraudolente o accedere a informazioni riservate.
- **La diffusione di software malevolo (malware):** il malware rappresenta una delle minacce più pervasive e in continua evoluzione nel panorama della sicurezza informatica. Questi software dannosi sono progettati per infiltrarsi, danneggiare o disabilitare sistemi, rubare dati sensibili, eseguire attività senza il consenso dell'utente o compromettere la sicurezza delle reti. I malware si presentano sotto diverse forme, tra cui virus, worm, trojan, ransomware, spyware, adware, e molti altri, ognuno con specifiche modalità di azione e obiettivi.

[TORNA ALL'INDICE](#)

La gestione efficace degli incidenti di sicurezza richiede un approccio olistico che include la prevenzione, il rilevamento tempestivo, la risposta coordinata e le attività di recupero. Implementare politiche di sicurezza robuste, adottare tecnologie avanzate di protezione e sensibilizzare gli utenti su pratiche sicure sono elementi fondamentali per ridurre il rischio di incidenti e mitigarne l'impatto quando si verificano.

Le strategie di intervento si differenziano a seconda del loro momento di applicazione rispetto all'incidente di sicurezza:

- **Azioni preventive** (prima dell'incidente): comprendono tutte quelle misure progettate per minimizzare la probabilità di eventi dannosi.
- **Azioni correttive e di risposta** (dopo l'incidente): si focalizzano sulla risoluzione degli incidenti e sul ripristino della funzionalità dei sistemi informativi nel più breve tempo possibile.

Nel contesto specifico della sicurezza di un'applicazione web di e-commerce, l'implementazione di misure preventive assume un'importanza cruciale. Ad esempio:

- l'adozione di un **Web Application Firewall (WAF)** si rivela essenziale per bloccare attacchi di tipo Cross-Site Scripting (XSS) e SQL Injection (SQLI), filtrando traffico web malevolo prima che possa raggiungere il server.

Riguardo alla sicurezza della rete, un attaccante può sfruttare le vulnerabilità per bypassare i firewall perimetrali e minare l'integrità della DMZ (Demilitarized Zone), che alloggia infrastrutture critiche come i server e-commerce, accessibili esternamente.

Dettagli sugli attacchi SQL Injection e XSS:

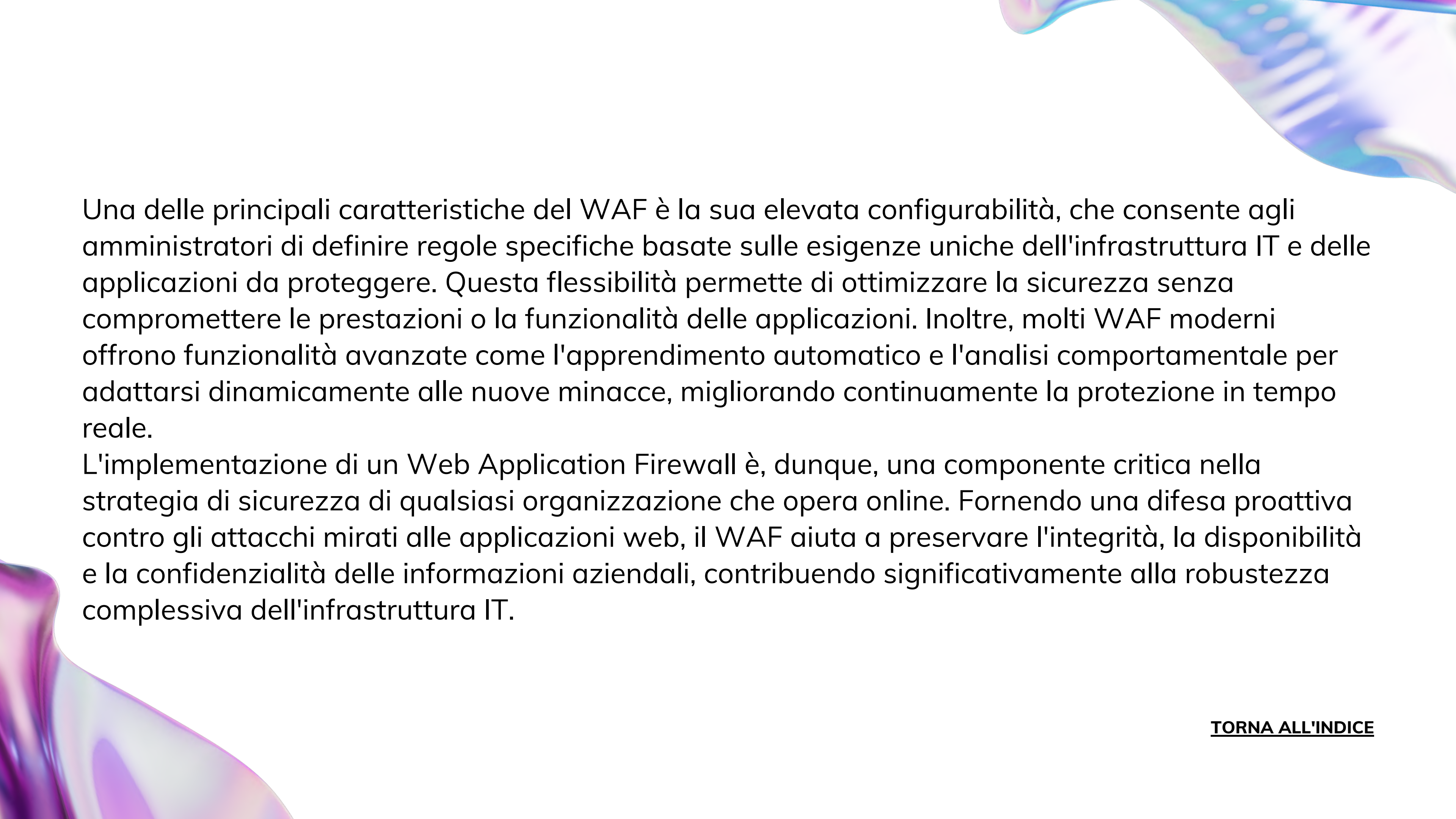
- SQL Injection:
 - SQL Injection: manipolazione di comandi SQL attraverso l'inserimento di codice malevolo negli input di un'applicazione web per rubare o corrompere dati.
 - SQL Injection Blind: una versione più sofisticata che non fornisce risposte dirette all'attaccante, il quale deve dedurre la vulnerabilità attraverso tentativi indiretti.
- Attacchi XSS:
 - XSS Riflesso: esegue script dannosi direttamente nel browser dell'utente senza permanenza sul server.
 - XSS Stored (Persistente): più insidioso, poiché lo script dannoso viene salvato sul server e può infettare più utenti che visitano il sito compromesso.

Azioni preventive

Nell'ecosistema della sicurezza informatica, l'adozione di strategie preventive è fondamentale per contrastare proattivamente le minacce e tutelare le risorse digitali di un'organizzazione. Questo approccio mira non solo a rafforzare le difese esistenti ma anche a prevenire l'insorgere di vulnerabilità all'interno delle infrastrutture IT. Tra le tecnologie chiave impiegate per realizzare tali obiettivi, il Web Application Firewall (WAF) gioca un ruolo di primo piano nel proteggere le applicazioni web da una vasta gamma di attacchi informatici.

Web Application Firewall (WAF): Il Web Application Firewall si posiziona come uno scudo avanzato per le applicazioni web, operando direttamente al confine tra internet e le risorse digitali che si intende proteggere. Questo dispositivo specializzato è progettato per scrutare e analizzare il traffico HTTP/HTTPS in ingresso, utilizzando un insieme di regole e politiche di sicurezza per identificare e bloccare le richieste potenzialmente dannose prima che possano raggiungere il server dell'applicazione. Attraverso un processo di filtraggio accurato, il WAF è in grado di rilevare e neutralizzare tentativi di attacco come iniezioni SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), e molte altre minacce che sfruttano le vulnerabilità comuni delle applicazioni web.

[TORNA ALL'INDICE](#)



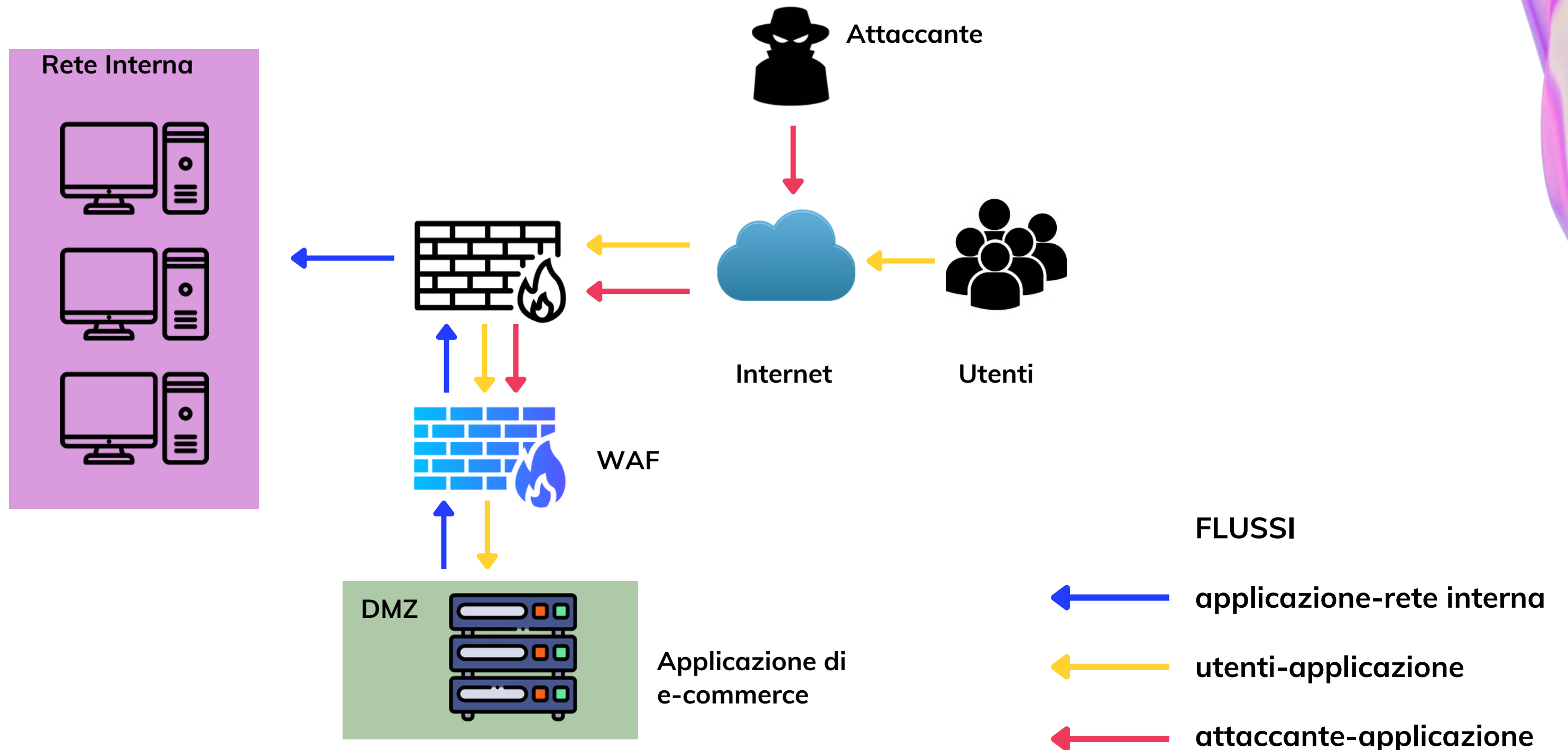
Una delle principali caratteristiche del WAF è la sua elevata configurabilità, che consente agli amministratori di definire regole specifiche basate sulle esigenze uniche dell'infrastruttura IT e delle applicazioni da proteggere. Questa flessibilità permette di ottimizzare la sicurezza senza compromettere le prestazioni o la funzionalità delle applicazioni. Inoltre, molti WAF moderni offrono funzionalità avanzate come l'apprendimento automatico e l'analisi comportamentale per adattarsi dinamicamente alle nuove minacce, migliorando continuamente la protezione in tempo reale.

L'implementazione di un Web Application Firewall è, dunque, una componente critica nella strategia di sicurezza di qualsiasi organizzazione che opera online. Fornendo una difesa proattiva contro gli attacchi mirati alle applicazioni web, il WAF aiuta a preservare l'integrità, la disponibilità e la confidenzialità delle informazioni aziendali, contribuendo significativamente alla robustezza complessiva dell'infrastruttura IT.

[TORNA ALL'INDICE](#)

[TORNA ALL'INDICE](#)

Schema di rete: modificato



Task 2: Cenni alla teoria

- **Definizione degli Attacchi DDoS e DoS:**
 - Attacchi DoS (Denial of Service): mirano a rendere una risorsa di rete (ad esempio, un sito web) inaccessibile agli utenti legittimi. Questo viene realizzato inondando il server target con una quantità eccessiva di richieste, superando la capacità del server di gestirle, il che porta a una saturazione delle risorse (come la CPU), rendendo il server incapace di rispondere a ulteriori richieste legittime.
 - Attacchi DDoS (Distributed Denial of Service): rappresentano una forma avanzata e più pericolosa degli attacchi DoS. A differenza dei tradizionali attacchi DoS, i DDoS provengono da molteplici fonti distribuite (spesso una botnet), rendendo molto più difficile per le vittime mitigare l'attacco e identificare gli aggressori.

- **Importanza della Business Continuity e del Disaster Recovery:**
 - Business Continuity Planning (BCP) e Disaster Recovery Planning (DRP) sono processi che aiutano le organizzazioni a prepararsi e rispondere a eventi critici, come gli attacchi DDoS, per assicurare la continuità operativa e la rapida ripresa delle attività.
 - Intersezione con Incident Response Planning (IRP): Il calcolo dell'impatto economico e la gestione degli attacchi DDoS rappresentano punti di convergenza tra BCP, DRP e IRP, enfatizzando l'importanza di una strategia integrata per la gestione dei rischi e degli incidenti.

Task 2: Impatti sul business

Valutazione dell'Impatto Economico di un Attacco DDoS sull'E-Commerce

Nel contesto digitale odierno, gli attacchi informatici rappresentano una minaccia costante per le aziende che operano online. Uno degli attacchi più dannosi è l'attacco Distributed Denial of Service (DDoS), il cui impatto può essere devastante per le attività commerciali, specialmente per quelle che dipendono fortemente dalla loro presenza online, come le piattaforme di e-commerce. Di seguito, esamineremo in dettaglio come calcolare l'impatto economico di un attacco DDoS, usando come esempio un'indisponibilità di 10 minuti di un'applicazione web di e-commerce.

[TORNA ALL'INDICE](#)

- **Calcolo dell'Impatto Economico:**
 - **Formula di Calcolo:** l'impatto economico dell'indisponibilità del servizio può essere calcolato come il prodotto del tempo di interruzione per la perdita monetaria per minuto.
 - **Applicazione della Formula:**
 - **Tempo di Interruzione:** 10 minuti.
 - **Perdita Monetaria per Minuto:** 1.500 €.
 - **Danno Economico Totale:** $10 \text{ minuti} \times 1.500 \text{ €/minuto} = 15.000 \text{ €}$.

L'indisponibilità del sito web per 10 minuti, a causa dell'attacco DDoS, può costare all'azienda proprietaria fino a 15.000 € in termini di perdite di vendite.

- **Ruolo del CSIRT (Computer Security Incident Response Team):**
 - Il CSIRT è il team dedicato alla gestione degli incidenti di sicurezza informatica. La sua funzione è cruciale per valutare e rispondere efficacemente agli attacchi, come quello DDoS in esame.
 - **Classificazione degli Incidenti:** Il CSIRT classifica gli incidenti in base a vari fattori, tra cui il tipo e la criticità dell'incidente, per determinare la risposta più appropriata e mitigare l'impatto negativo sugli asset aziendali.

[TORNA ALL'INDICE](#)

MEDIA

- +La compagnia non riesce ad erogare alcuni dei servizi critici
- +Servizi critici non erogati a un sottinsieme limitato di utenti
- +Impatto economico non indifferente(es. 10.000 / 500.000€)

La classificazione dell'incidente come "criticità media" da parte del CSIRT (Computer Security Incident Response Team) implica che l'incidente ha causato un'interruzione parziale dei servizi critici dell'azienda e che l'impatto economico è significativo, ma non catastrofico. Quando si considera la perdita di 15.000 euro in 10 minuti a causa di un attacco DDoS, il CSIRT tiene conto di diversi fattori per valutare l'incidente e pianificare la risposta:

1. Valutazione dell'impatto funzionale:

- **Servizi Critici Interrotti:** determinare quali servizi critici sono stati interrotti e per quanto tempo.
- **Utenti Affetti:** identificare la portata dell'interruzione in termini di numero di utenti o clienti influenzati.
- **Ripristino dei Servizi:** stimare quanto velocemente i servizi possono essere ripristinati alla normalità.

2. Valutazione dell'impatto economico:

- **Perdite Dirette:** calcolare le perdite dirette basate sul fatturato medio per minuto (in questo caso 1.500 euro al minuto).
- **Perdite Indirette:** stima delle perdite indirette, come il danno alla reputazione e la potenziale perdita di clienti futuri.

3. Risposta e Mitigazione:

- **Analisi dell'Incidente:** determinare la causa dell'attacco DDoS e se poteva essere previsto o mitigato.
- **Misure di Mitigazione:** attuare misure di sicurezza per prevenire o limitare il danno di futuri attacchi DDoS.
- **Comunicazione con gli Stakeholder:** informare gli stakeholder interni ed esterni sull'incidente e sulle azioni intraprese.

4. Recupero e Business Continuity:

- **Disaster Recovery Plan (DRP):** attivare il piano di recupero dai disastri per ripristinare i servizi.
- **Business Continuity Plan (BCP):** assicurare che le operazioni aziendali possano continuare o riprendere rapidamente dopo l'interruzione.



5. Revisione e Preparazione:

- **Debriefing:** dopo la risoluzione dell'incidente, eseguire una revisione post-mortem per comprendere cosa ha funzionato e cosa no.
- **Aggiornamento dei Piani di Sicurezza:** basandosi sulle lezioni apprese, aggiornare i piani di risposta agli incidenti e le strategie di sicurezza.

6. Considerazioni Legali e Normative:

- **Conformità alle Norme:** verificare che l'incidente sia stato gestito in conformità con tutte le leggi e normative pertinenti, inclusa la notifica agli enti regolatori se necessario.

La classificazione di "criticità media" riflette quindi una situazione che richiede un'azione immediata per contenere e mitigare gli effetti dell'incidente, ma che allo stesso tempo non compromette l'intera capacità operativa dell'azienda. Il CSIRT dovrà lavorare in modo proattivo per analizzare l'incidente, coordinare la risposta e attuare le strategie di mitigazione per prevenire future interruzioni e perdite finanziarie.

Task 3: Cenni di teoria

Analizziamo un caso in cui un attaccante sia riuscito a compromettere un'applicazione web attraverso l'uso di malware. Questi software dannosi, noti come "Malicious Software", rappresentano una minaccia significativa per la sicurezza dei sistemi informatici. Possono avere diverse finalità nocive, tra cui:

- Causare un'interruzione del servizio (Denial of Service), che rende le risorse di rete inaccessibili agli utenti legittimi.
- Spiare le attività degli utenti, raccogliendo dati sensibili senza il loro consenso.
- Ottenere il controllo non autorizzato su dati e sistemi, permettendo agli attaccanti di manipolare o rubare informazioni riservate.

I malware rappresentano una delle minacce più pervasive e dannose nel panorama della sicurezza informatica. Essi sono progettati con l'intento specifico di causare danno, disturbo o furto all'interno dei sistemi informatici a cui riescono ad avere accesso. La categoria "malware" comprende una vasta gamma di tipologie di software nocivo, ognuna delle quali possiede caratteristiche e modalità operative distinte.



Principali tipologie di malware e le loro peculiarità:

1. Virus

Un virus informatico è un tipo di malware che si replica attaccandosi a file o programmi. Quando il file infetto viene eseguito, il virus si attiva, potendo causare danni vari, dalla corruzione di dati alla cancellazione di file. I virus richiedono l'intervento dell'utente per diffondersi, ad esempio tramite l'apertura di un allegato email infetto o il download di software da fonti non sicure.

2. Worm

I worm sono simili ai virus nella loro capacità di replicarsi, ma possono diffondersi autonomamente attraverso reti senza la necessità di un file ospite. Questi malware sfruttano vulnerabilità nei sistemi operativi o in altre applicazioni per replicarsi e diffondersi a nuovi computer, spesso causando danni significativi a livello di rete.

3. Trojan

I trojan, o cavalli di Troia, sono malware che si mascherano da software legittimi per ingannare gli utenti e indurli ad installarli. Una volta attivati, possono svolgere diverse funzioni dannose, come aprire una backdoor per permettere ad attaccanti di accedere al sistema, rubare dati o installare ulteriori malware.



[TORNA ALL'INDICE](#)

4. Spyware

Gli spyware sono progettati per spiare le attività degli utenti su un computer, raccogliendo informazioni senza il consenso dell'utente. Possono monitorare le abitudini di navigazione, raccogliere dati personali e sensibili come password e dettagli bancari, o registrare battiture sulla tastiera (keylogging).

5. Adware

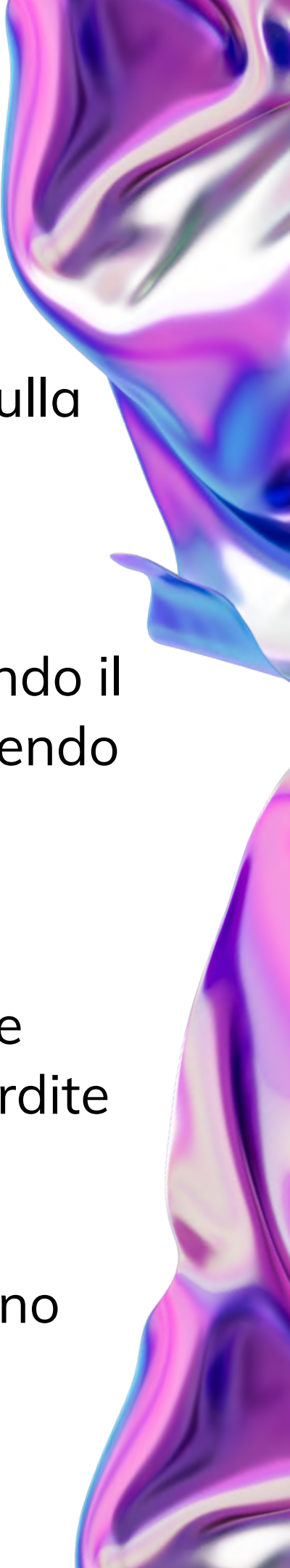
L'adware, sebbene non sempre considerato malware nel senso tradizionale, può diventare malevolo quando compromette la privacy dell'utente mostrando annunci invasivi o reindirizzando il browser a siti web dannosi. Spesso, l'adware viene installato insieme a software gratuito, offrendo pubblicità non desiderate.


6. Ransomware

Il ransomware è una forma particolarmente dannosa di malware che cripta i file dell'utente, rendendoli inaccessibili, e richiede un riscatto per la loro decrittazione. Gli attacchi ransomware possono colpire sia utenti individuali che reti aziendali, causando interruzioni significative e perdite finanziarie.

7. Rootkit

I rootkit consentono accesso remoto al sistema infetto mantenendo nascoste le loro tracce. Sono particolarmente insidiosi poiché possono eludere il rilevamento da parte di software antivirus, permettendo agli attaccanti di manipolare il sistema a loro piacimento.





Per fronteggiare efficacemente un incidente di sicurezza, è fondamentale attuare un piano di risposta agli incidenti strutturato in fasi. La terza fase, il contenimento, mira a limitare il danno causato dall'incidente il più rapidamente possibile, per prevenire la diffusione della minaccia ad altri sistemi, applicazioni e asset aziendali.

L'obiettivo è isolare l'incidente per evitare ulteriori danneggiamenti alle reti e ai sistemi, riducendo l'impatto dell'attacco. Le principali tecniche impiegate a questo scopo includono:

- **Segmentazione:** divisione della rete in diverse sotto-reti (LAN o VLAN) attraverso il subnetting, per limitare la diffusione del malware.
- **Isolamento:** disconnessione completa del sistema infettato dalla rete interna, per restringere ulteriormente l'accesso all'attaccante.
- **Rimozione:** eliminazione del malware dal sistema compromesso per ripristinare la sicurezza.

Task 3: Incident Response

Nel caso specifico che stiamo esaminando, si è scelto di adottare l'isolamento come tecnica di contenimento. Questa decisione è stata presa per prevenire la diffusione del malware senza tuttavia eliminare l'accesso al sistema infettato da parte dell'attaccante. L'isolamento si rivela particolarmente efficace nei casi in cui la semplice segmentazione della rete non offra garanzie sufficienti di sicurezza. Attraverso l'isolamento, il sistema infetto viene completamente scollegato dalla rete interna, limitando drasticamente le possibilità di accesso da parte dell'attaccante.

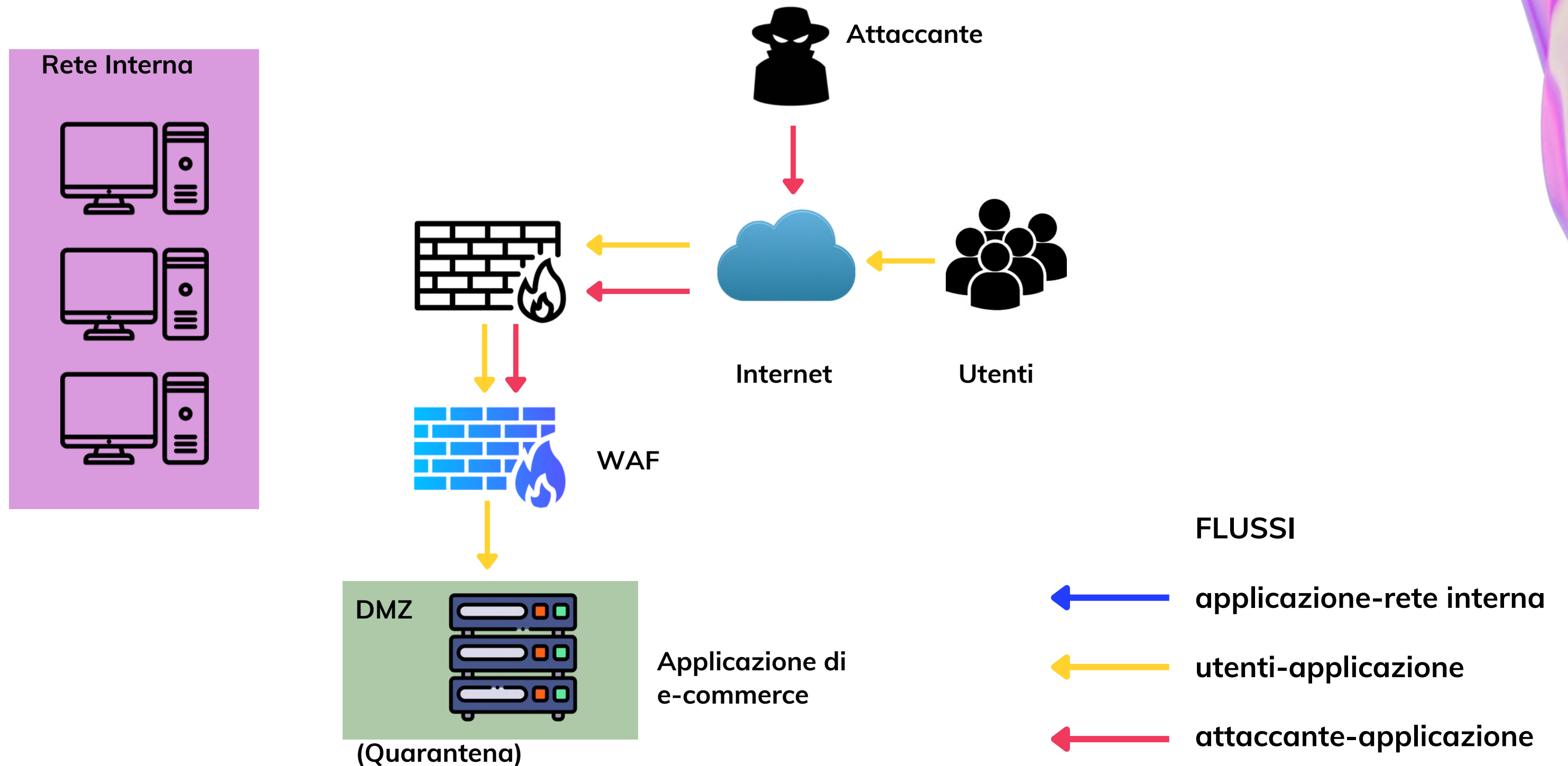
L'isolamento può essere attuato in due modi:

- **Isolamento fisico:** comporta la separazione fisica del sistema compromesso dalla rete, ad esempio scollegando i cavi di rete o disattivando l'alimentazione elettrica.
- **Isolamento logico:** si interrompe la comunicazione di rete tra il sistema compromesso e il resto della rete interna, ad esempio modificando le configurazioni di rete o implementando politiche sui firewall e altri dispositivi di rete per bloccare le connessioni in entrata e in uscita dal sistema interessato.

[TORNA ALL'INDICE](#)

[TORNA ALL'INDICE](#)

Isolamento macchina infetta



Efficacia dell'isolamento

Come emerge dall'analisi dello schema di rete modificato la zona demilitarizzata (DMZ) rimane accessibile da Internet, il che significa che anche l'attaccante può raggiungerla, tuttavia, è stata strategicamente isolata dalla rete interna dell'organizzazione.

Questa configurazione svolge un ruolo cruciale nella gestione della sicurezza informatica, poiché permette agli amministratori di rete e ai team di sicurezza di mantenere un controllo mirato sul traffico in ingresso e in uscita dalla DMZ, senza compromettere l'integrità e la sicurezza delle risorse interne.

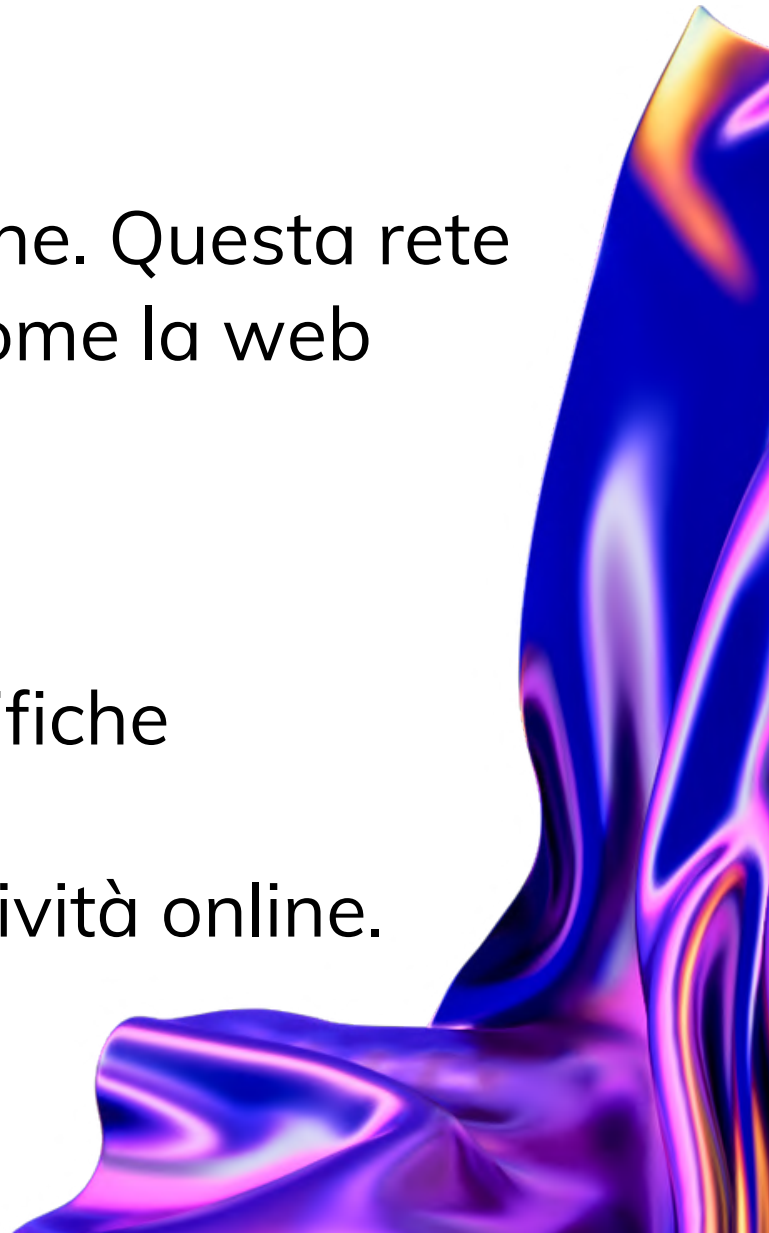
L'isolamento della DMZ dalla rete interna è una misura precauzionale che impedisce al malware o agli attacchi provenienti da Internet di infiltrarsi ulteriormente nei sistemi aziendali critici. Questo approccio non solo limita il raggio d'azione dell'attaccante ma offre anche ai responsabili della sicurezza informatica un'opportunità preziosa per monitorare attentamente e analizzare il traffico malevolo. Attraverso l'esame dettagliato di queste attività dannose, è possibile identificare le tecniche, gli strumenti e le procedure utilizzate dagli aggressori, fornendo così dati vitali per rafforzare le difese contro future intrusioni.

Suggerimenti e migliorie

L'architettura di rete di un'organizzazione è fondamentale per garantire la sicurezza delle informazioni e la continuità delle operazioni aziendali. Una configurazione ottimale deve bilanciare l'accessibilità e la funzionalità con la protezione contro le minacce informatiche.

Componenti chiave di un'architettura di rete robusta

Rete Interna

- Definizione: Una rete dedicata all'uso esclusivo dei dipendenti dell'organizzazione. Questa rete consente una comunicazione sicura e controllata sia con applicazioni interne, come la web application aziendale, sia con l'Internet più ampio.
 - Funzioni principali:
 - Condivisione di risorse interne come file server e stampanti.
 - Accesso a sistemi di gestione database interni e applicazioni software specifiche dell'azienda.
 - Connessione sicura a Internet per ricerche, comunicazioni esterne e altre attività online.
- 

DMZ (Demilitarized Zone)

- Porzione di rete posizionata tra la rete interna sicura dell'organizzazione e una rete esterna non affidabile, tipicamente Internet. La DMZ ospita servizi esposti a Internet, come web server o server di posta, minimizzando il rischio di attacchi diretti ai sistemi interni.

Web Application Firewall (WAF) e Next Generation Firewall (NGFW);

- WAF si concentra sulla sicurezza delle applicazioni web filtrando e monitorando il traffico HTTP/HTTPS
- NGFW offre una protezione più ampia. Ad esempio analizza il traffico alla ricerca di segnali di possibili intrusioni o attacchi (IDS) e permette di applicare politiche di sicurezza specifiche.



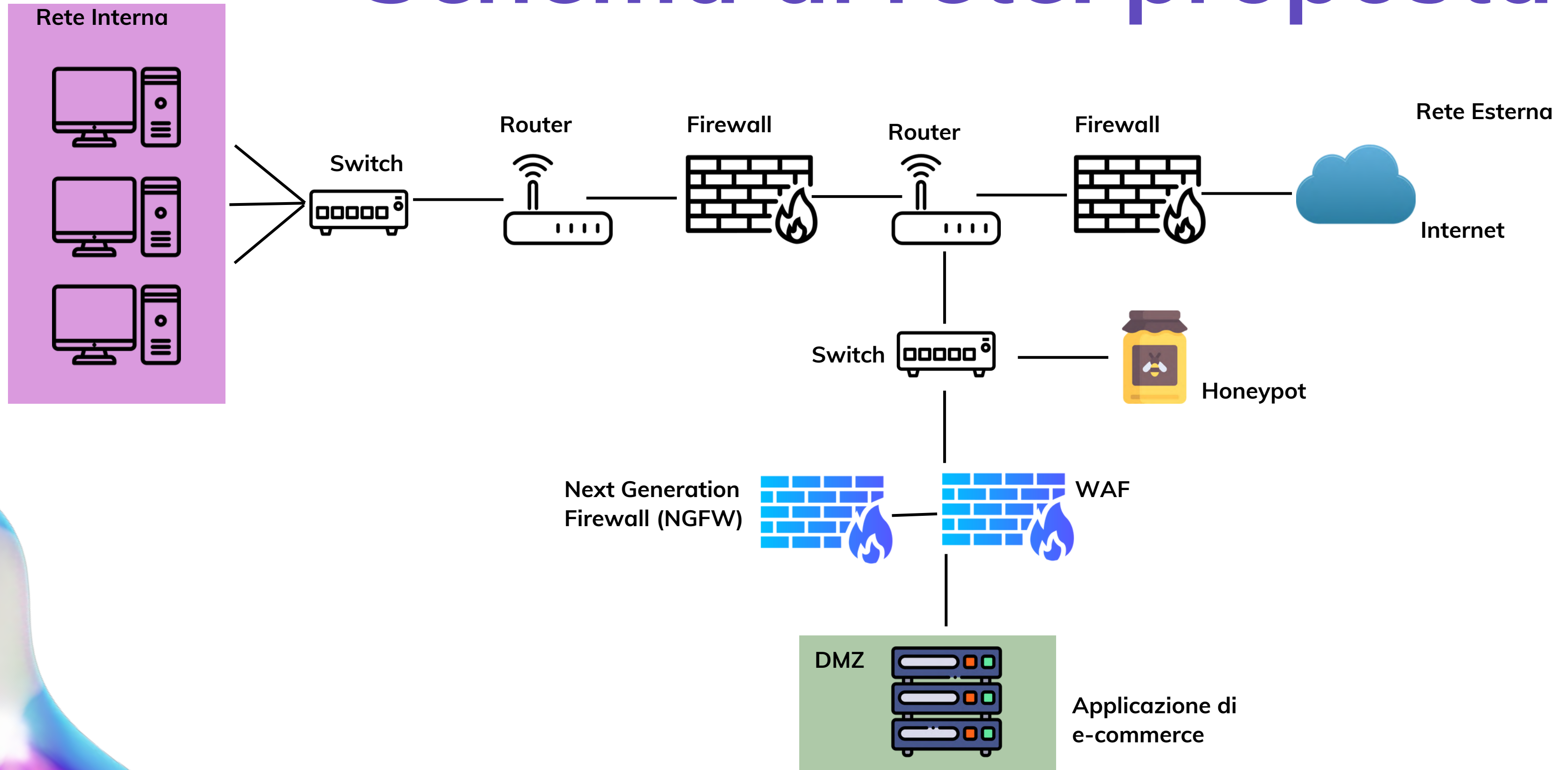
Honeypot

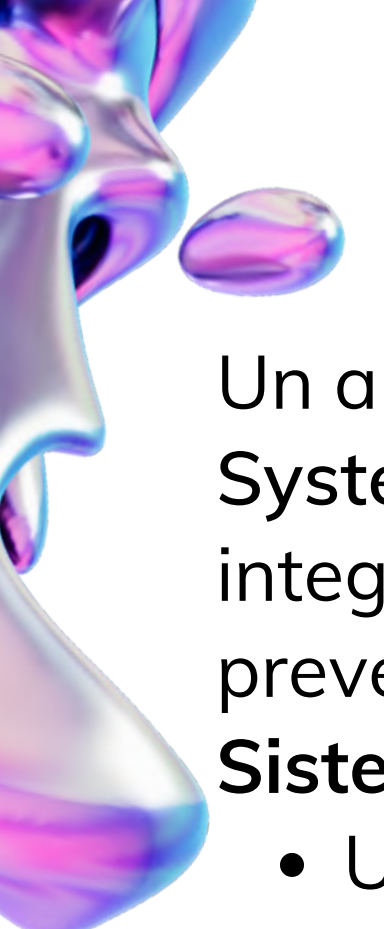
- Un sistema o rete progettato per apparire vulnerabile e attraente per gli attaccanti. L'obiettivo di un honeypot è di distogliere gli attacchi dai sistemi critici, raccogliere informazioni sugli attaccanti e sui loro metodi, e aiutare a migliorare le strategie di sicurezza. Gli honeypot possono essere:
 - **A bassa interazione:** Simulano solo i servizi più comunemente attaccati per attirare attività malevole.
 - **Ad alta interazione:** Forniscono un ambiente completo che può registrare attività avanzate e sofisticate da parte degli attaccanti.

Rete Esterna

- Comprende gli utenti esterni che accedono ai servizi online dell'organizzazione.

Schema di rete: proposta





Un altro elemento cruciale è il Sistema di Prevenzione delle Intrusioni (IPS, Intrusion Prevention System). L'IPS gioca un ruolo fondamentale nel rafforzare le difese contro le minacce informatiche, integrando le capacità di rilevamento degli Intrusion Detection Systems (IDS) con la capacità di prevenire attivamente le intrusioni.

Sistema di Prevenzione delle Intrusioni (IPS)

- Un IPS è un dispositivo di sicurezza di rete che esamina il traffico di rete per rilevare e prevenire attività malevole. A differenza dell'IDS, che si limita a rilevare e segnalare le intrusioni, l'IPS ha la capacità di bloccare tali attività prima che raggiungano i sistemi target.
- L'IPS monitora il traffico di rete in tempo reale, utilizzando una serie di firme di attacchi conosciuti, anomalie di traffico e politiche di sicurezza per identificare comportamenti sospetti. Quando rileva un'attività potenzialmente dannosa, l'IPS può prendere misure preventive per bloccarla, come:
 - Rifiuto del pacchetto di dati incriminato.
 - Terminazione della connessione TCP che trasporta il traffico malevolo.
 - Riconfigurazione dinamica del firewall o di altri dispositivi di sicurezza per prevenire attacchi simili in futuro.

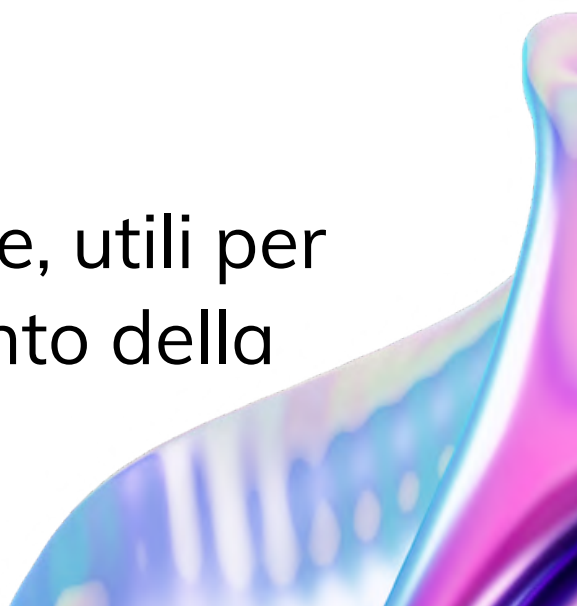
[TORNA ALL'INDICE](#)



L'IPS si integra nell'architettura di rete dell'organizzazione come segue:

- **Collocazione Strategica:** l'IPS è tipicamente posizionato dietro al firewall (e al NGFW) per ispezionare il traffico che è già stato filtrato dai firewall. Questo posizionamento consente di ridurre il volume di traffico che l'IPS deve analizzare, permettendogli di concentrarsi sui flussi di dati più rilevanti per la sicurezza.
- **Protezione della DMZ e della Rete Interna:** mentre il NGFW e il WAF proteggono specificamente il web server nella DMZ, l'IPS estende questa protezione monitorando il traffico verso tutti i dispositivi all'interno della DMZ e verso la rete interna, offrendo un ulteriore strato di difesa contro le intrusioni.
- **Prevenzione di Attacchi Esterni e Interni:** oltre a bloccare gli attacchi provenienti da Internet, l'IPS può anche identificare e prevenire attività sospette o malevole all'interno della rete interna, come il movimento laterale di malware o tentativi di accesso non autorizzati a risorse riservate.

Vantaggi Aggiuntivi

- **Riduzione dei Falsi Positivi:** gli IPS moderni sono progettati per minimizzare i falsi positivi, utilizzando tecniche avanzate di analisi e apprendimento automatico per distinguere accuratamente il traffico legittimo dalle minacce reali.
 - **Compliance e Reportistica:** forniscono funzionalità di logging e reportistica dettagliate, utili per le analisi forensi, il miglioramento continuo delle politiche di sicurezza e il mantenimento della conformità con le normative sulla protezione dei dati.
- 



Grazie!

[TORNA ALL'INDICE](#)