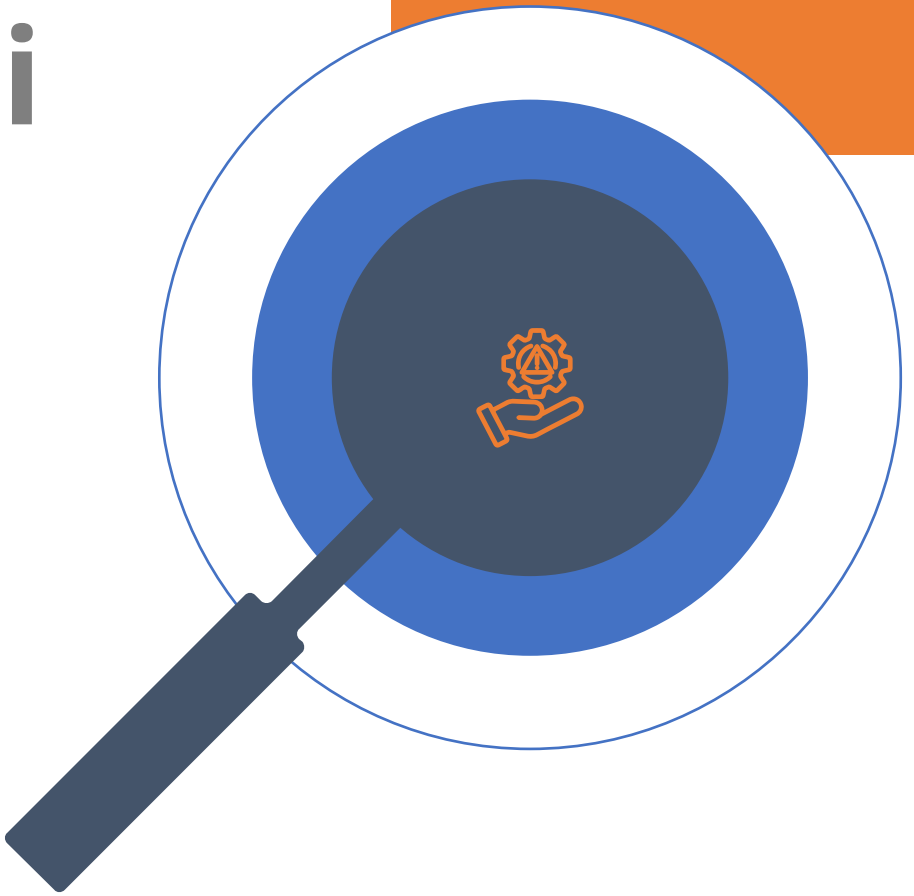
ESERCIZIO FINALE W20D4

Prevenzione Attacchi Per Applicazione E-Commerce

Progettazione sicura dell’architettura di rete per un'Applicazione E-Commerce: Strategie Preventive.



CLIENTE

DOCENTE: NIKO
ISTITUTO: EPICODE

CONSULENTE

STUDENTE:
SIMONE CISBAGLIA

TRACCIA:

ARCHITETTURA DI RETE:

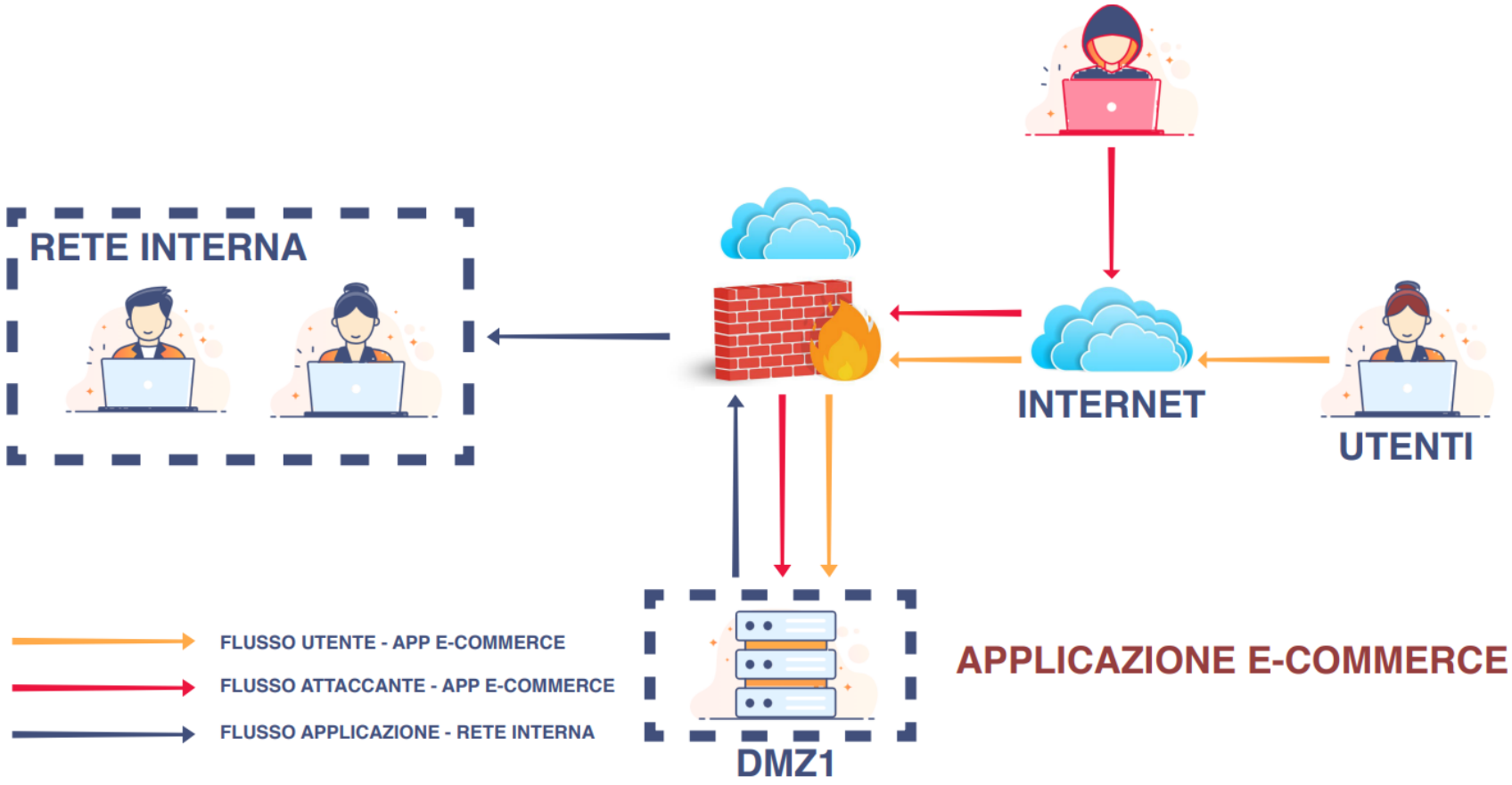
L’applicazione di e-commerce deve essere disponibile per gli utenti tramite internet per effettuare acquisti sulla piattaforma.
La rete interna è raggiungibile dalla dmz per via delle policy sul firewall, quindi se il server in dmz viene compromesso potenzialmente un attaccante potrebbe raggiungere la rete interna.

INDICE

1. SITUAZIONE INIZIALE

AMBIENTE:

QUALI AZIONI PREVENTIVE SI POTREBBERO IMPLEMENTARE PER DIFENDERE L'APPLICAZIONE WEB DA ATTACCHI DI TIPO SQLI OPPURE XSS DA PARTE DI UN UTENTE MALINTENZIONATO?



RICHIESTA

Modificate la figura in modo da evidenziare le implementazioni

2. AZIONI PREVENTIVE

Come azioni preventive in caso di una minaccia di tipo SQLi e XSS da parte di un utente malintenzionato, che può essere sia interno che esterno all'attività di e-commerce in questione, propongo una serie di opzioni che elenco di seguito:

Web Application Firewall (WAF)

Validazione e sanitizzazione degli input

HTTPS

Aggiornamenti e patch

Sensibilizzazione e formazione

Limitazione dei privilegi

Logging e monitoraggio

Vulnerability assessment

Differential backup

Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS)

Web Application Firewall (WAF): Utilizzerei un dispositivo di sicurezza dedicato specificamente a proteggere le applicazioni da attacchi come SQL Injection e Cross Site Scripting.

Validazione e sanitizzazione degli input: Mi assicurerei che tutti gli input forniti dagli utenti siano validati sia sul lato client che sul lato server, accettando solo input che soddisfano determinati criteri. Inoltre, rimuoverei o codificherei caratteri speciali che possono essere utilizzati in attacchi SQLi o XSS.

HTTPS: Utilizzerei il protocollo HTTPS per crittografare il traffico tra il client e il server, proteggendo così i dati in transito.

Aggiornamenti e patch: Mantenendo l'applicazione e il suo environment (server, database, framework, ecc.) aggiornati con le ultime patch di sicurezza, potrei prevenire attacchi che sfruttano bug noti o vulnerabilità esistenti.

Sensibilizzazione e formazione: È molto importante formare gli sviluppatori e il personale interno che ha accesso ai vari end-point alle best practice di programmazione sicura e ai rischi di sicurezza comuni e noti come SQLi e XSS.

Limitazione dei privilegi: Le connessioni al database dovrebbero utilizzare account con il minimo livello di privilegi necessario per svolgere il lavoro.

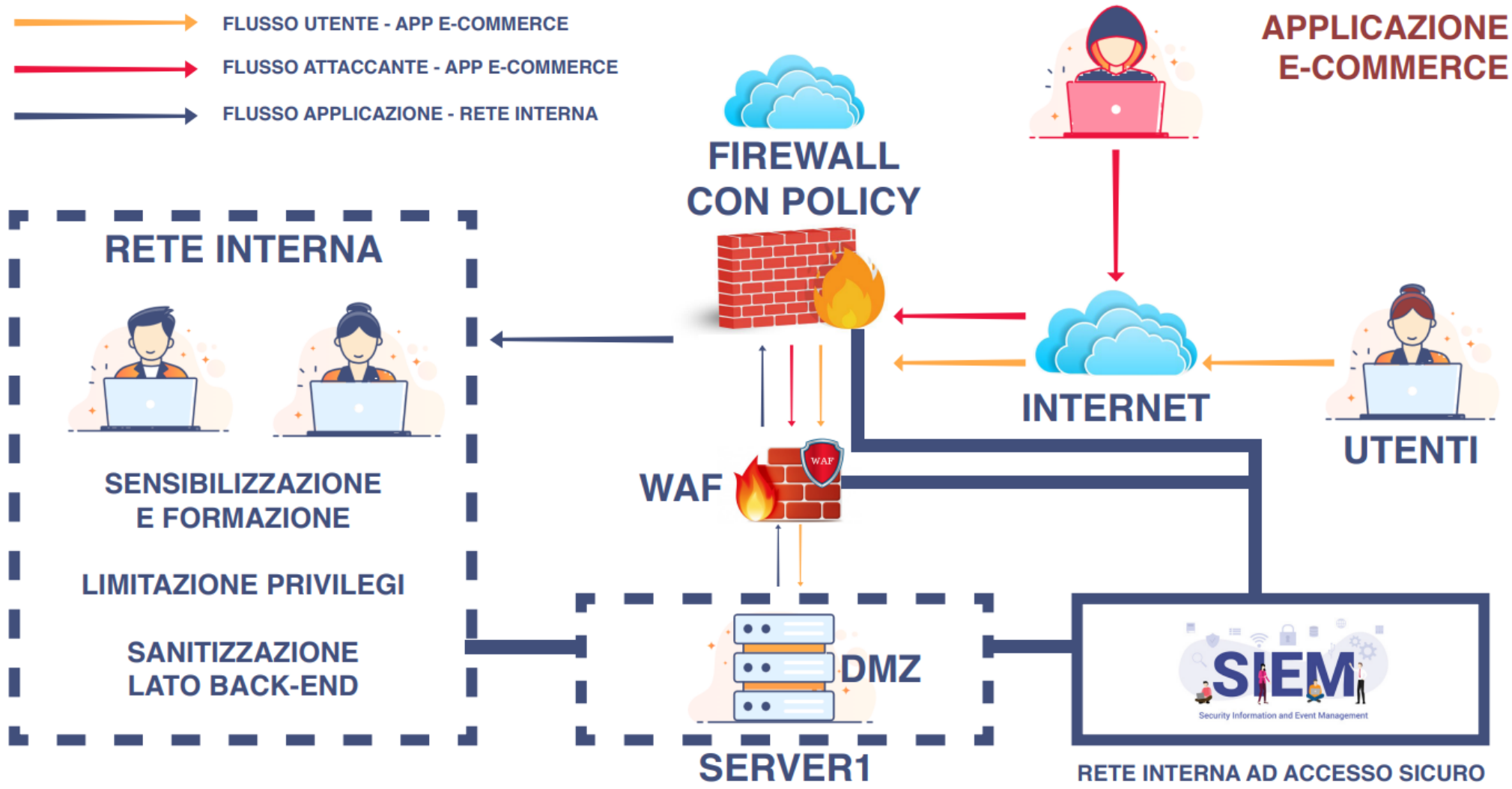
Logging e monitoraggio: Potrebbe essere utile mantenere log dettagliati delle attività per una visione centralizzata della sicurezza, magari con dei sistemi SIEM, e monitorare le app e i sistemi per individuare e reagire rapidamente a qualsiasi attività sospetta ed eventuali minacce o attacchi in corso.

Vulnerability assessment: Effettuerei continue campagne e testerei periodicamente l'applicazione con dei penetration test, un metodo utile per scoprire eventuali falle e porvi rimedio prima che possano essere sfruttate da malintenzionati.

Differential backup: Eseguirei backup regolari dei dati e del codice dell'applicazione su sistemi di storage sicuri e testerei regolarmente la procedura di ripristino. Il differential backup è una soluzione meno dispendiosa in termini di tempo, in quanto permette di implementare solo i dati che sono stati modificati dall'ultimo full backup che vengono copiati e salvati.

Sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS): Implementerei IDS/IPS per rilevare comportamenti anomali o schemi di attacco e prendere azioni automatiche per prevenire o mitigare gli attacchi.

Post-Remediation



3. IMPATTI SUL BUSINESS

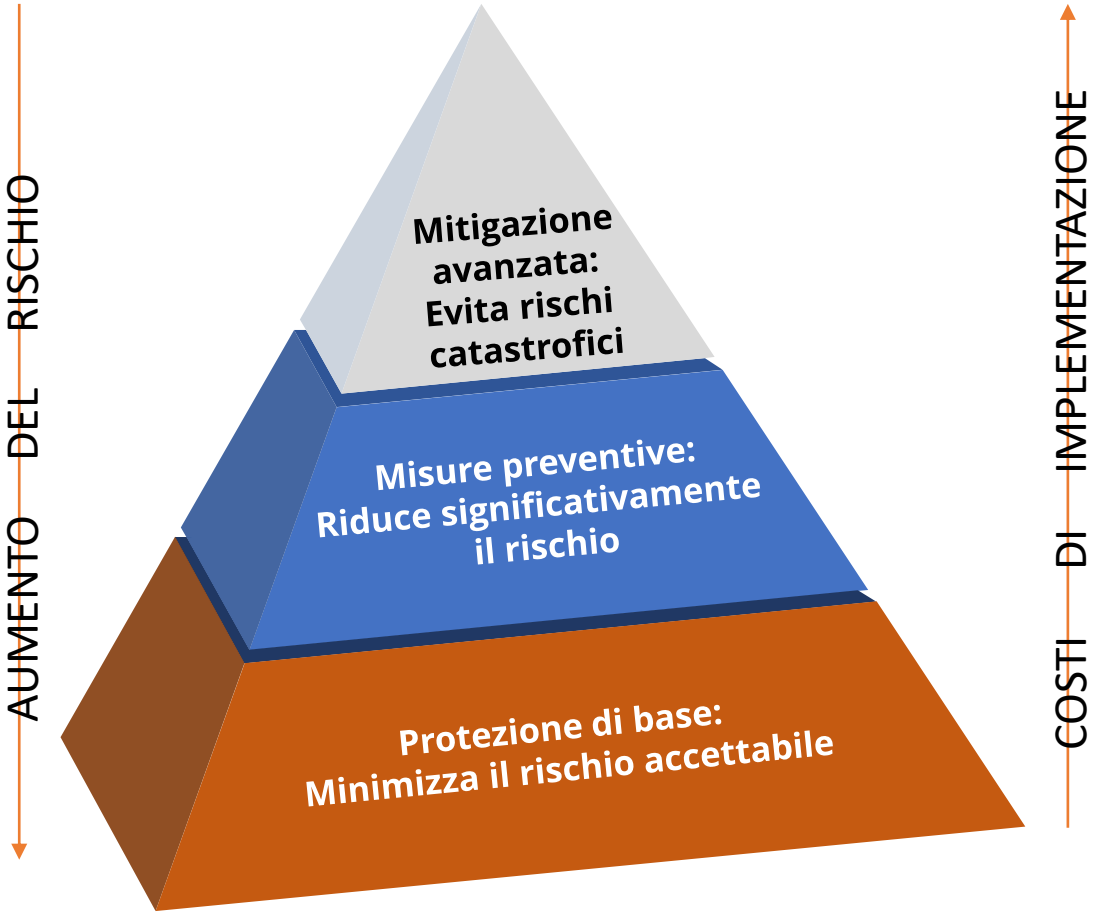
L'APPLICAZIONE WEB SUBISCE UN ATTACCO DI TIPO DDOS DALL'ESTERNO CHE RENDE L'APPLICAZIONE NON RAGGIUNGIBILE PER 10 MINUTI. CALCOLARE L'IMPATTO SUL BUSINESS DOVUTO ALLA NON RAGGIUNGIBILITÀ DEL SERVIZIO, CONSIDERANDO CHE IN MEDIA OGNI MINUTO GLI UTENTI SPENDONO 1.500 € SULLA PIATTAFORMA DI E-COMMERCE (15.000 € IN TOT.).

RICHIESTA

FARE EVENTUALI VALUTAZIONI DI AZIONI PREVENTIVE CHE SI POSSONO APPLICARE IN QUESTA PROBLEMATICA (ACCETTAZIONE DEL RISCHIO O RIDUZIONE).

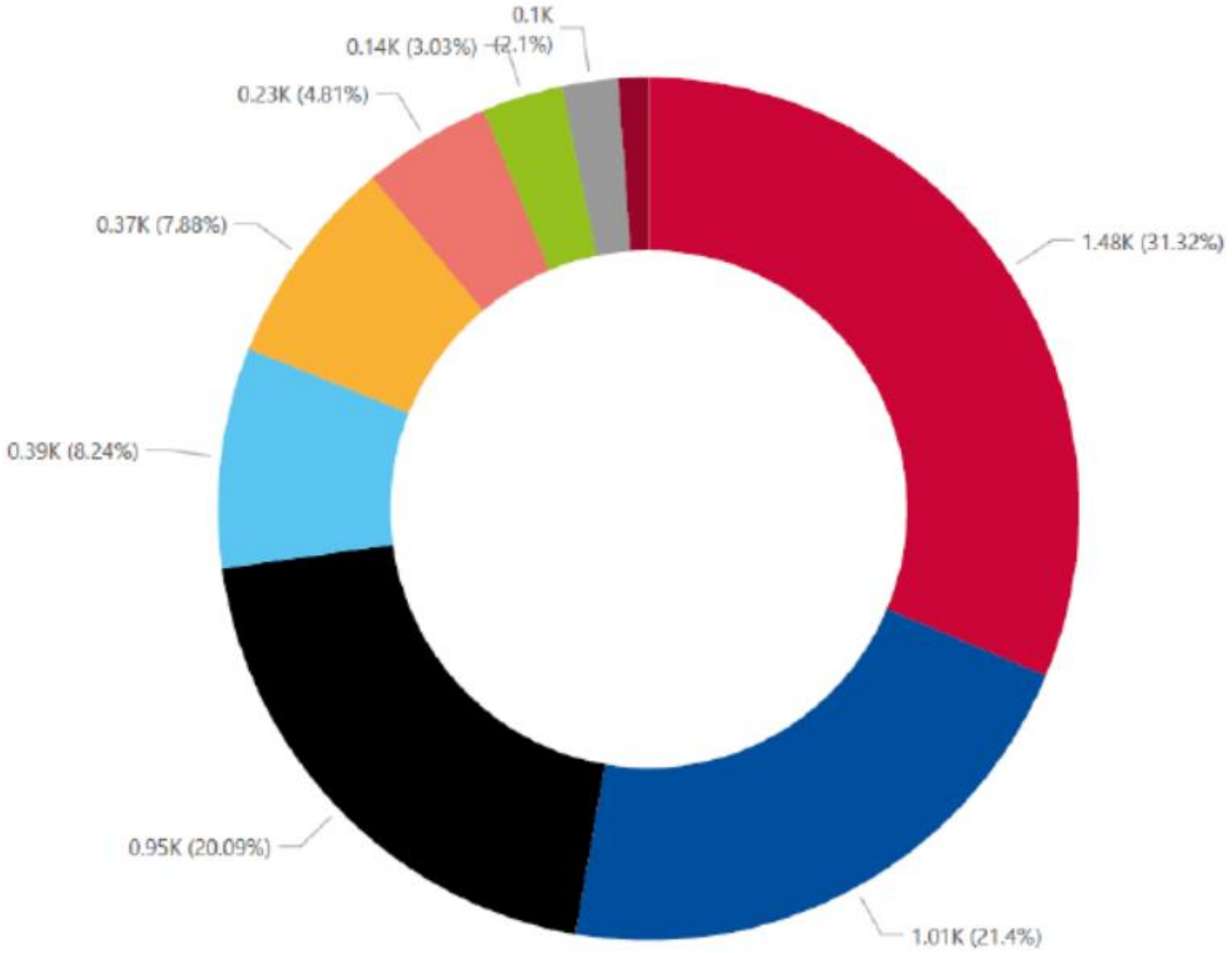
Consulenza

Considerando che non ho dettagli precisi sul settore, categoria merceologica, collocazione e situazione geopolitica, presumo che una perdita di 15.000 euro in dieci minuti indichi un'attività di media entità con un budget limitato per Security Operations e BCP. Tuttavia, è possibile trovare soluzioni efficaci contro un attacco DDoS.



Accettare il rischio non è consigliabile, visto che l'hosting deve garantire la disponibilità del servizio e rispettare la triade CIA. Vediamo quali azioni preventive adottare, poiché, secondo i report ENISA di giugno 2023, gli attacchi DDoS sono secondi solo ai ransomware in termini di frequenza.

REPORT DI ENISA



Panoramica

Gli attacchi DDoS sono diventati più complessi, coinvolgendo reti mobili e dispositivi IoT, e ora fanno parte della cyberwarfare. Secondo il report "Imperva Global DDoS Threat Landscape" del 2023, nel 2022 gli attacchi DDoS a livello di applicazione sono aumentati dell'82% rispetto al 2021, con un incremento del 121% nel settore dei servizi finanziari.

In Italia, nel primo semestre del 2023, gli attacchi DDoS sono cresciuti notevolmente, passando dal 4% del totale degli attacchi nel 2022 al 30% nel 2023, superando la media globale del 7,9%. Questo incremento è legato all'attivismo e alla guerra informatica, trasformando l'Italia in un teatro significativo per le attività hacktiviste.

Obiettivo

È chiaro che bisogna difendersi da minacce simili, anche a costo di superare i 15 mila euro di perdite in dieci minuti.

- Cambiare il DNS per distribuire il carico di traffico tra più server e utilizzare servizi di DNS secondario (o di failover) può garantire che il dominio rimanga online anche se il provider DNS primario subisce un'interruzione.
- Prevenire attacchi DDoS con strumenti di monitoraggio del traffico in tempo reale può permettere di reagire prontamente prima che l'attacco causi danni maggiori.
- Usare Cloudflare per mitigare attacchi DDoS offre protezione illimitata per siti web e una rapida risposta, utile durante un attacco.

- Mantenere log dettagliati con sistemi SIEM per monitorare le app e individuare rapidamente attività sospette.
- Implementare piattaforme di threat intelligence.
- Valutare i danni alla reputazione e gli accordi commerciali con altre aziende, limitando i rischi e minimizzando i tempi di ripristino e proteggendo l'integrità dei dati sensibili.

4. RESPONSE

TRACCIA:

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

RICHIESTA: MODIFICATE LA FIGURA IN SLIDE 2 CON LA SOLUZIONE PROPOSTA

Analisi

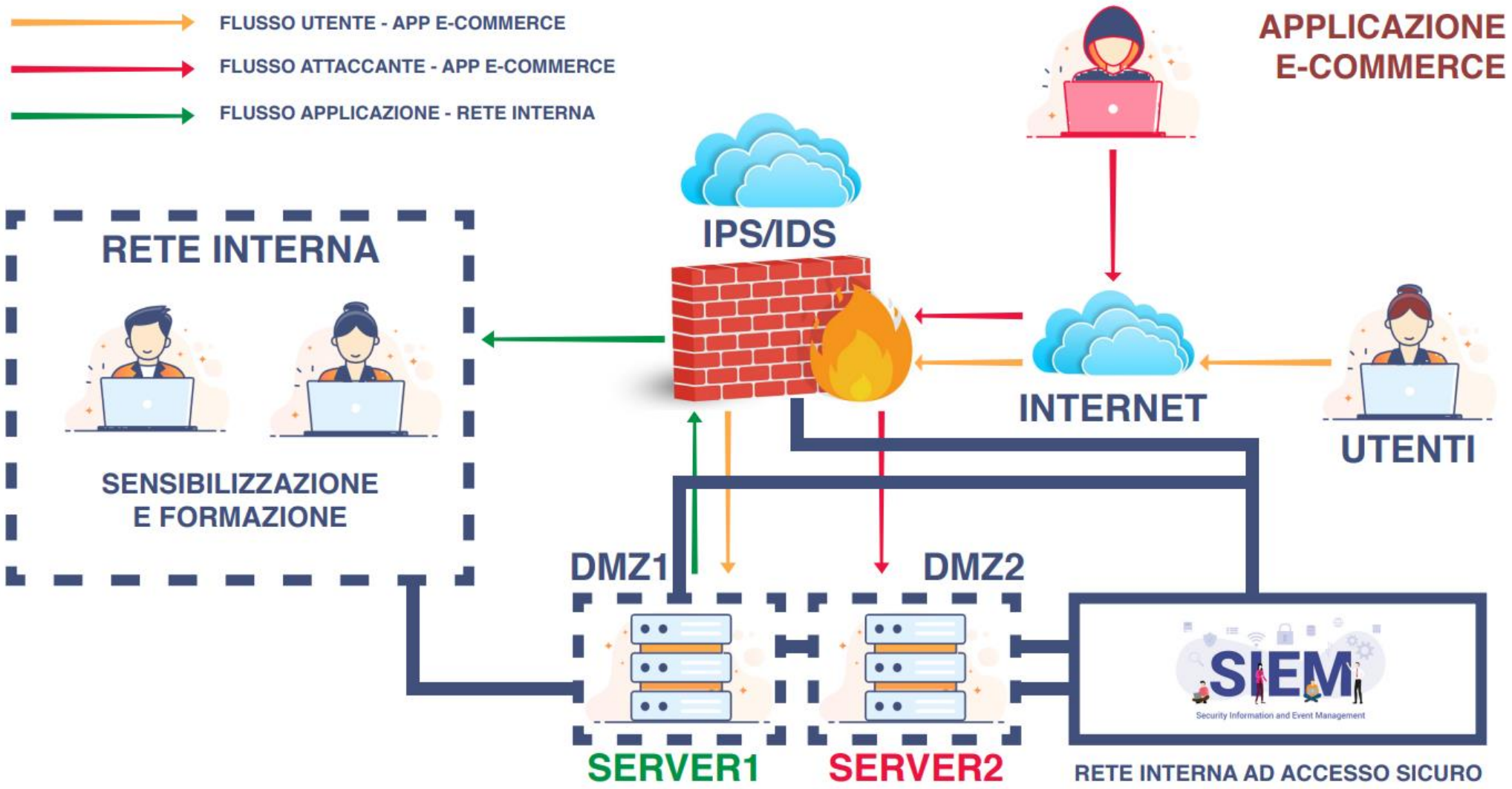
Essendo l'applicazione infettata dal malware, avendo segmentato la rete (con livelli di sicurezza differenziati come la DMZ), la cosa migliore è isolare il server infetto in una "rete di quarantena". La segmentazione permette di dividere la rete in diverse LAN o VLAN, separando il sistema infetto dagli altri, creando una rete ad hoc. Questo contiene il malware, impedendone la diffusione e permettendoci di studiarlo in seguito. Nel frattempo, possiamo switchare al server di backup per garantire la continuità operativa.

È consigliabile usare un IPS/IDS e verificare se il firewall lo supporta. Inoltre, un SIEM e un sistema di threat intelligence con sonde su server, rete ed endpoint aiuterebbero a rilevare comportamenti anomali e a prevenire o mitigare attacchi.

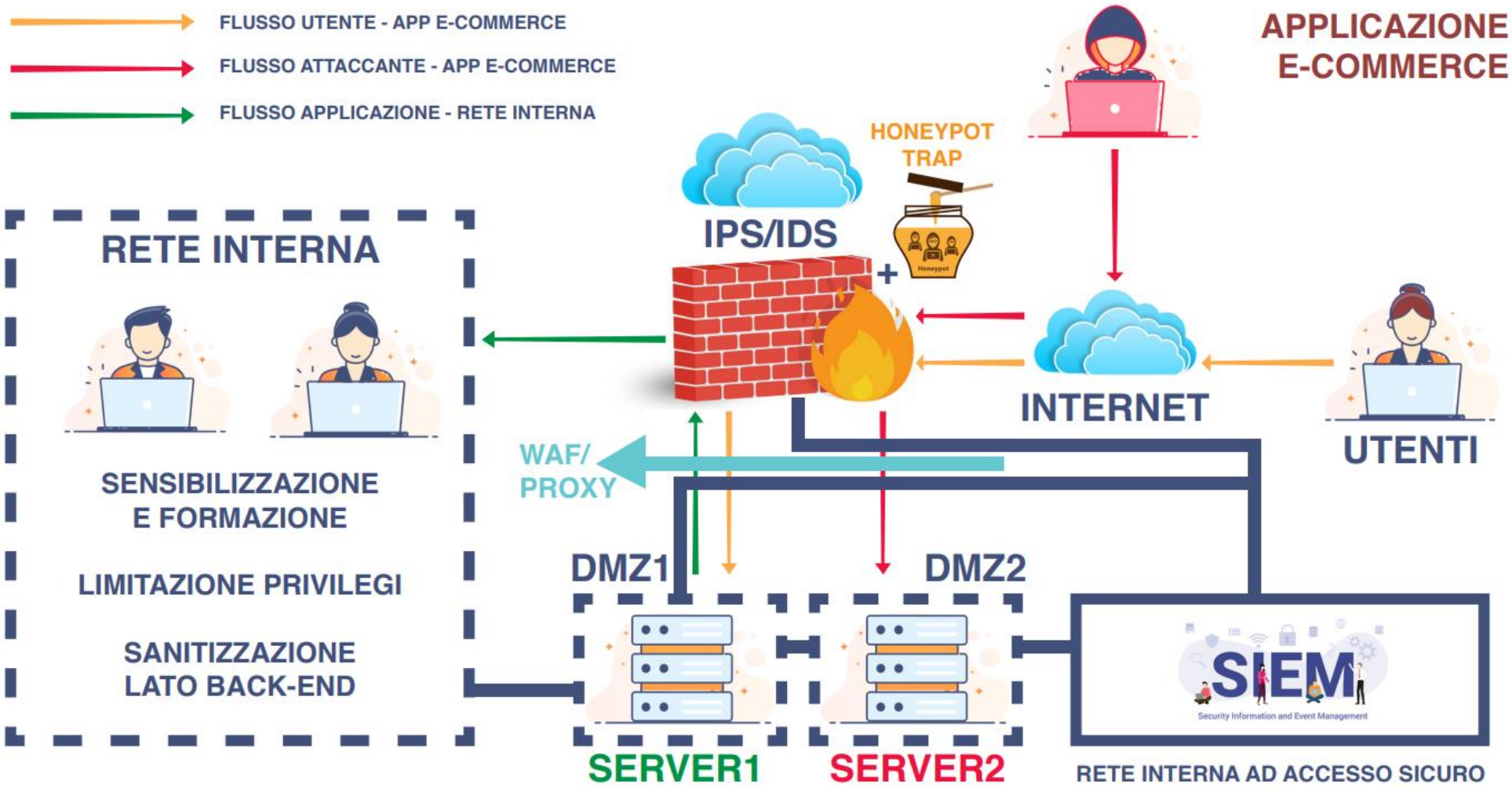
Azioni preventive utili

- **Ridondanza dei server e dei network:** Utilizzerei più server per l'hosting dell'applicazione (failover cluster) e progetterei la rete con percorsi ridondanti per evitare single point of failure. Implementando anche RAID-1 o RAID-5 per la continuità del servizio hosting.
- **Differential Backup:** Consiglio backup regolari dei dati e del codice dell'applicazione, copiando solo i dati modificati dall'ultimo full backup, e verificare regolarmente la procedura di ripristino.
- **Utilizzo di un honeypot:** Si può posizionare honeypot in aree monitorate della rete per attirare e intrappolare gli attaccanti, distogliendoli dalle risorse reali e raccogliendo informazioni sulle loro tecniche.
- **Configurare un proxy:** Usare un proxy per filtrare contenuti, nascondere l'indirizzo IP degli utenti e proteggere la rete interna da accessi diretti, analizzando e filtrando il traffico sospetto.
- **Data center geograficamente distribuiti:** Valutare la distribuzione dell'infrastruttura su più data center in diverse aree geografiche per protezione da disastri naturali o guasti di rete localizzati.
- **Software stile Darktrace:** Valutare l’utilizzo soluzioni di intelligenza artificiale e machine learning per rilevare e rispondere a minacce in tempo reale, identificando attività sospette o anomale e collaborando con altri dispositivi di sicurezza come i firewall.

Post-Remediation avanzato



5. SOLUZIONE COMPLETA



Traccia:

UNIRE I DISEGNI DELL'AZIONE PREVENTIVA E DELLA RESPONSE (UNIRE SOLUZIONE 1 E 3)

6. MODIFICA DELL'INFRASTRUTTURA

Traccia:
(SE NECESSARIO/FACOLTATIVO MAGARI INTEGRANDO LA SOLUZIONE AL PUNTO 2)

Se l'isolamento e le altre azioni preventive non bastano, potrebbe essere necessario rimuovere il sistema infetto. Questo comporta smaltire o recuperare i dischi di storage attaccati utilizzando metodi come:

- **Clear:** Rimozione dei dati tramite reset di fabbrica o sovrascrittura multipla.
- **Purge:** Rimozione fisica dei dati (es. magneti).
- **Destroy:** Distruzione totale del disco (es. alte temperature).

Per non compromettere l'attività, è essenziale avere backup e server alternativi.

DRaaS (Disaster Recovery as a Service) può essere una soluzione: i cloud provider offrono infrastrutture in cloud attivabili in caso di disastro sul sito primario. Sebbene ci siano tempi di latenza per lo switch, il servizio è conveniente perché si paga solo in caso di necessità, trasferendo così il rischio.

7. CONCLUSIONE

- In questa esercitazione, ho esaminato diverse azioni preventive per proteggere L’ applicazione e-commerce da attacchi SQLi, XSS e DDoS. Le principali misure che adotterei includono l'implementazione di un Web Application Firewall (WAF), la validazione e sanitizzazione degli input, l'uso di HTTPS, l'aggiornamento regolare del software, la formazione del personale, la limitazione dei privilegi e il logging e monitoraggio costante.
- Ho sottolineato l'importanza della ridondanza dei server e delle reti, l'uso di backup differenziali e l'implementazione di sistemi IDS/IPS. Inoltre, ho considerato l'uso di honeypot, proxy e data center distribuiti geograficamente per migliorare ulteriormente la sicurezza.
- Per la risposta agli incidenti, ho valutato l'isolamento del sistema infetto e l'uso del Disaster Recovery as a Service (DRaaS) per garantire la continuità operativa. Queste soluzioni combinate forniscono una difesa robusta e multilivello per proteggere efficacemente l’applicazione e-commerce.

GRAZIE

SIMONE CISBAGLIA