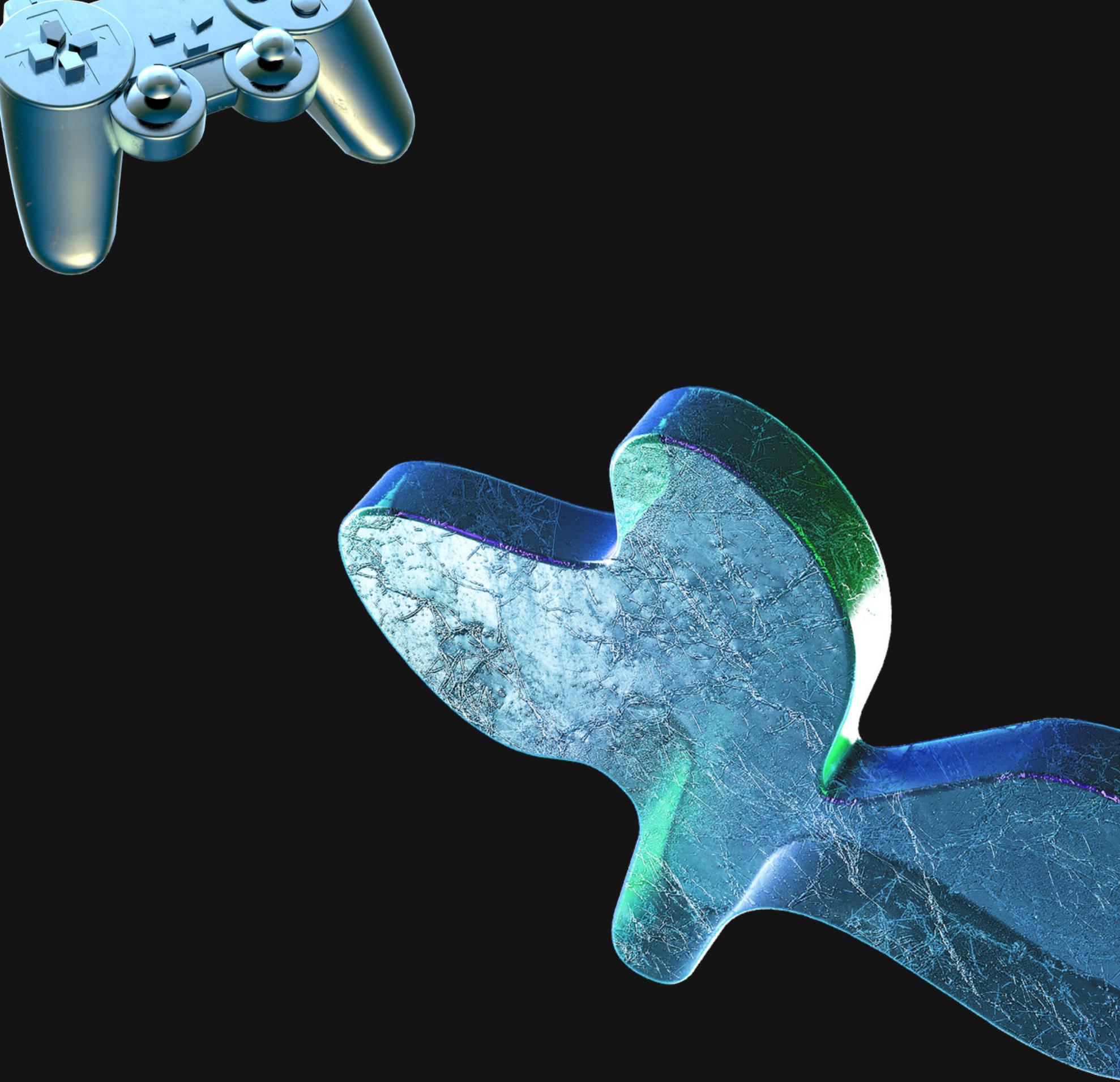


Christian Huamacto

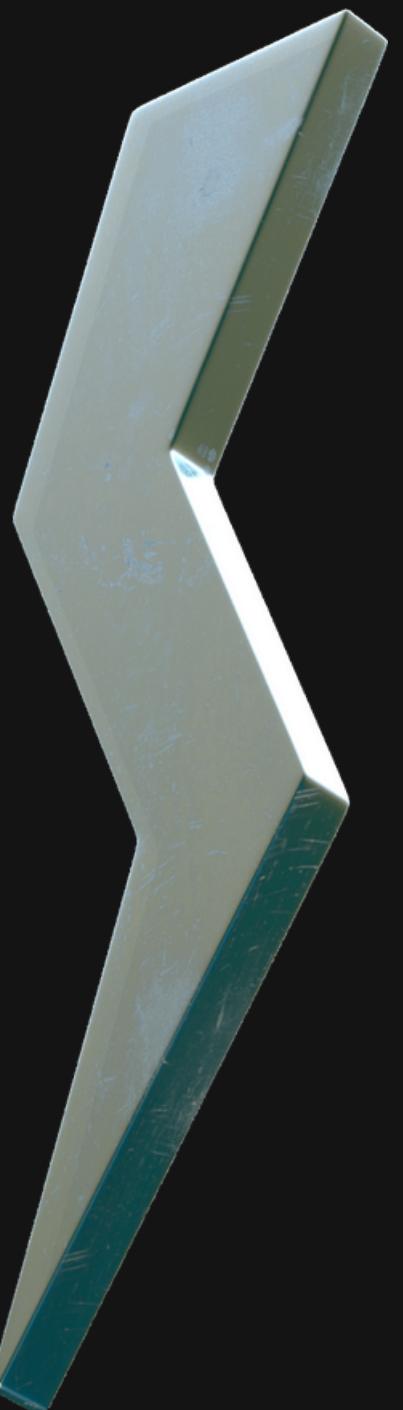
Progetto Epicode

24.11.2023



Analisi dei log

Traccia del progetto



1) AZIONI PREVENTIVE, PER UN EVENTUALE ATTACCO ALLA RETE

come possiamo difendere l'applicazione web da attacchi XSS/SQLi?

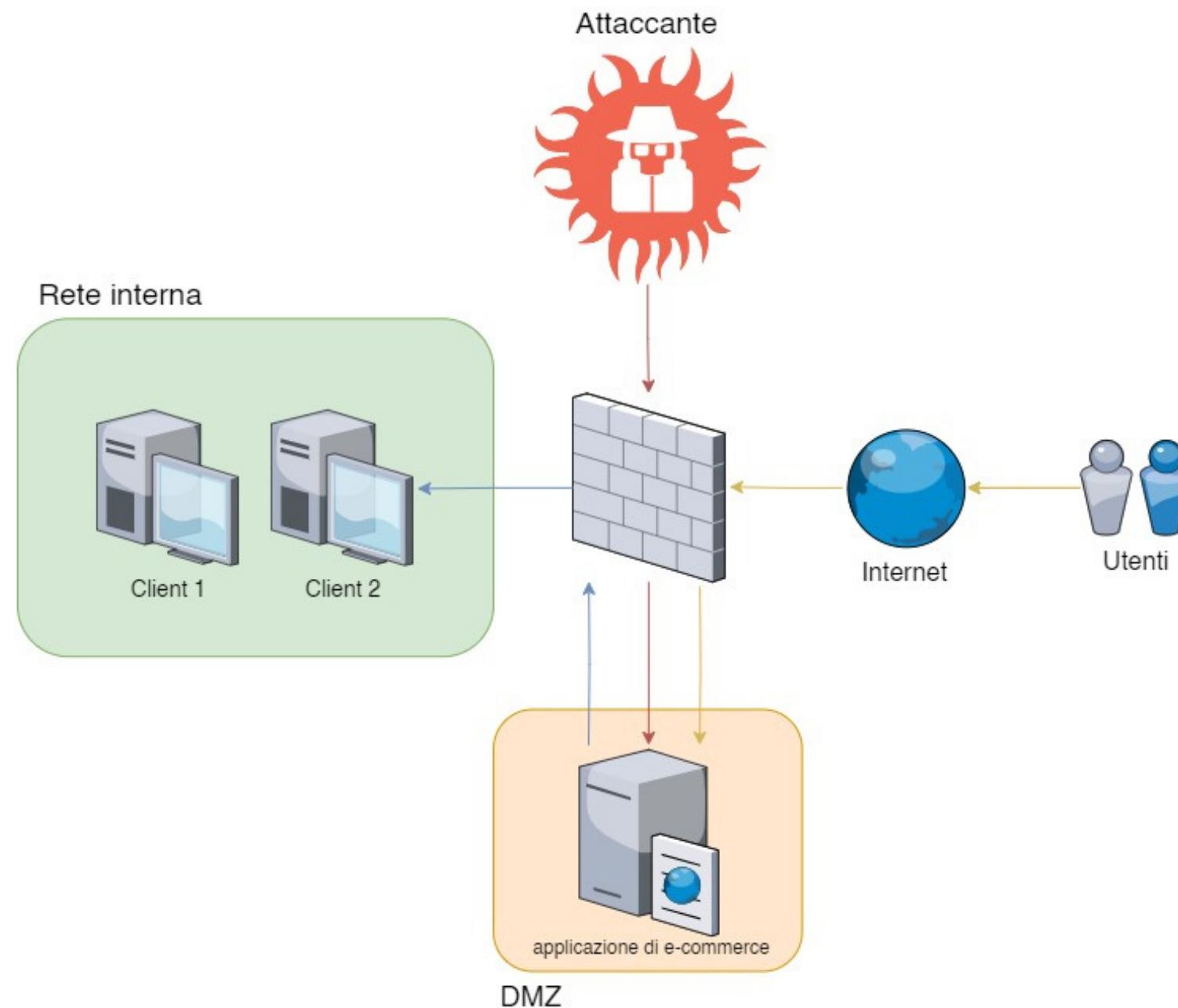
2) IMPATTO SUL BUSINESS DELL'AZIENDA TARGET

Se l'applicazione web subisse un attacco DDOS e rimanesse inattivo per 10 minuti, sapendo che ogni minuto degli utenti spendono 1500€, quale sarebbe l'impatto sul business dell'azienda

3) RESPONSE ALL'INFENZIONE DELL'APPLICAZIONE WEB DA PARTE DI UN MALWARE

Che tipologia di contenimento useremo nel caso volessimo isolare il server infetto senza rimuovere l'accesso all'attaccante

Rete compromessa



Azioni preventive per attacchi XSS e SQLi



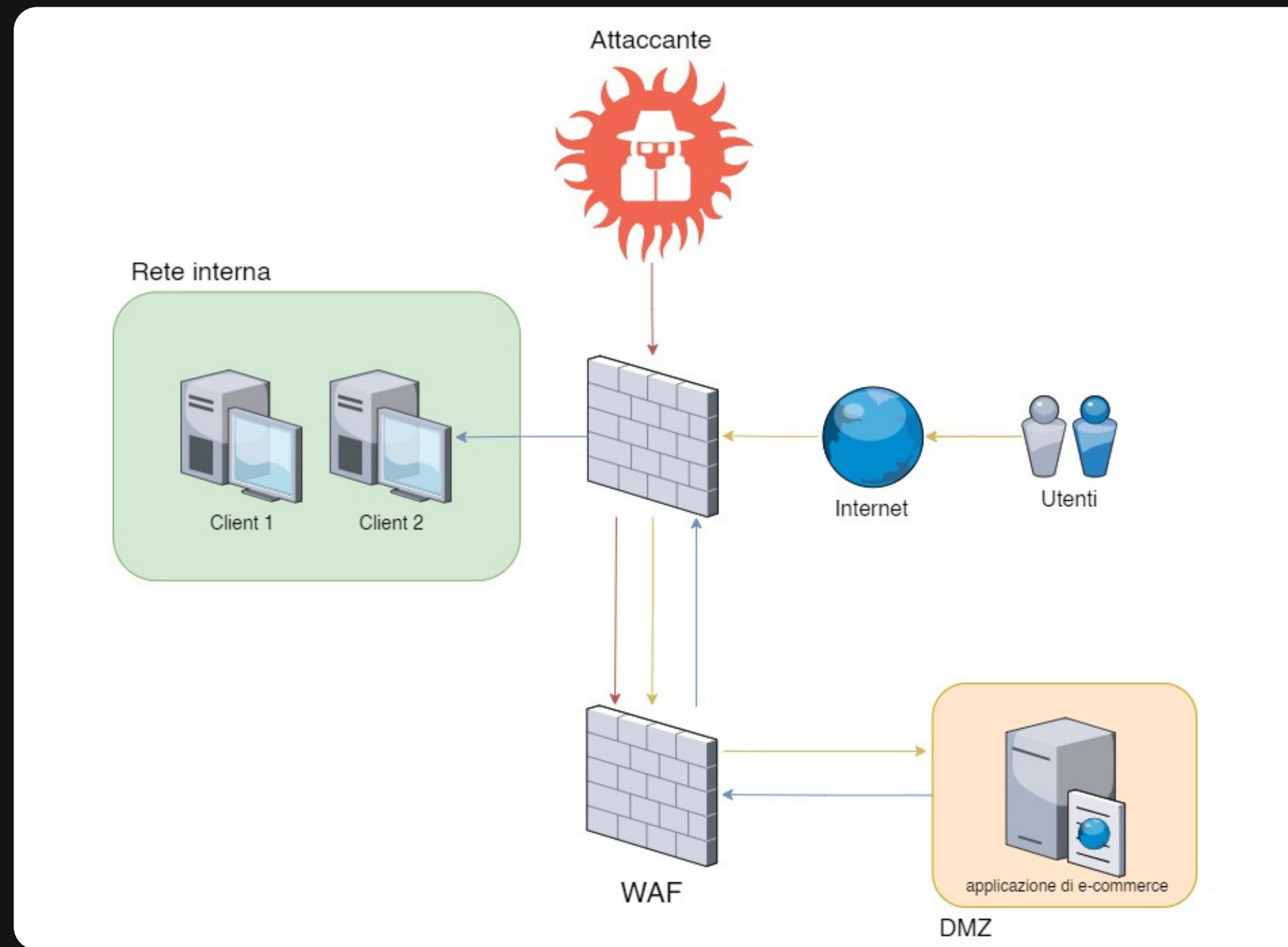
Attacchi SQLi

- Utilizzare input filtrati. Gli input degli utenti devono essere filtrati per rimuovere caratteri dannosi, come caratteri speciali, spazi vuoti ecc.
- Utilizzare una connessione sicura. Le applicazioni Web devono utilizzare una connessione sicura, come HTTPS, per proteggere i dati inviati dagli utenti.
- Eseguire regolarmente scansioni di sicurezza. Le applicazioni Web devono essere scansionate regolarmente per rilevare vulnerabilità che potrebbero essere sfruttate per attacchi SQLi.

Attacchi XSS

- Utilizzare codice HTML validato. Il codice HTML inviato dagli utenti deve essere validato per assicurarsi che non contenga codice dannoso.
- Utilizzare un filtro XSS. Un filtro XSS può essere utilizzato per rimuovere il codice dannoso dal codice HTML inviato dagli utenti.
- Eseguire regolarmente scansioni di sicurezza. Le applicazioni Web devono essere scansionate regolarmente per rilevare vulnerabilità che potrebbero essere sfruttate per attacchi XSS.

Rete per preventivare XSS e SQLi



Per preventivare gli attacchi sopracitati aggiungeremo un WAF che filtra:

- Richieste HTTP che contengono caratteri dannosi
- Richieste HTTP che contengono codice SQL o JavaScript dannoso

Oltre al WAF esistono altri dispositivi di sicurezza come IDS/IPS, non si è optato ad implementare nella rete uno dei 2 dispositivi al posto del WAF perchè, nel caso dell'IDS, non bloccherebbe l'attaccante ma invierebbero solo un'alert, oppure, nel caso dell'IPS, potrebbe generare falsi positivi e bloccare le richieste non dannose.

Impatto sul business aziendale

il nostro server, con all'interno l'applicazione e-commerce, è rimasto in down per circa 10 minuti per colpa di un attacco DDOS. Quanto è stata impattante la perdita economica in questo lasso di tempo?

Sappiamo che i nostri clienti spendono 1500€ al minuto sul nostro e-commerce

**La perdita economica
è stata di circa 15000€**



La perdita non è stata significativa perché il down del server è stato gestito in 10 minuti, però se l'attacco fosse stato più massiccio e fosse durato per ore? L'impatto economico sarebbe stato sicuramente maggiore.

Perciò sarebbe meglio eseguire delle azioni preventive per evitare un ulteriore attacco DDOS

Cos'è un attacco DDOS?

Un attacco DDoS (Distributed Denial of Service), è un attacco che mira a rendere inaccessibile un sistema informatico o un servizio. L'obiettivo di un attacco DDoS è sovraccaricare il sistema o il servizio target con un gran numero di richieste, in modo da renderlo inutilizzabile per gli utenti legittimi.

Questo tipo di attacco può essere lanciato da un singolo aggressore o da un gruppo di aggressori. Gli aggressori possono utilizzare una varietà di tecniche per lanciare un attacco DDoS, tra queste c'è la Botnet. una Botnet è un gruppo di dispositivi compromessi che sono controllati da un attaccante. Gli aggressori possono utilizzare le Botnet per inviare richieste a un sistema o servizio target e sovraccaricarlo.

Come prevenire un attacco DDoS

UTILIZZARE UN SISTEMA DI RILEVAMENTO E RISPOSTA AGLI ATTACCHI (IDS/IPS)

Un IDS/IPS può essere utilizzato per rilevare e bloccare attacchi DDoS. Gli IDS/IPS possono monitorare il traffico di rete alla ricerca di modelli anomali che potrebbero indicare un attacco DDoS.

UTILIZZARE UN SERVIZIO DI PROTEZIONE DDoS

Un servizio di protezione DDoS può fornire protezione da attacchi DDoS. I servizi di protezione DDoS utilizzano una combinazione di tecniche per mitigare gli effetti di un attacco DDoS, come il filtraggio del traffico, la ridimensionamento dinamico e la mitigazione delle vulnerabilità.

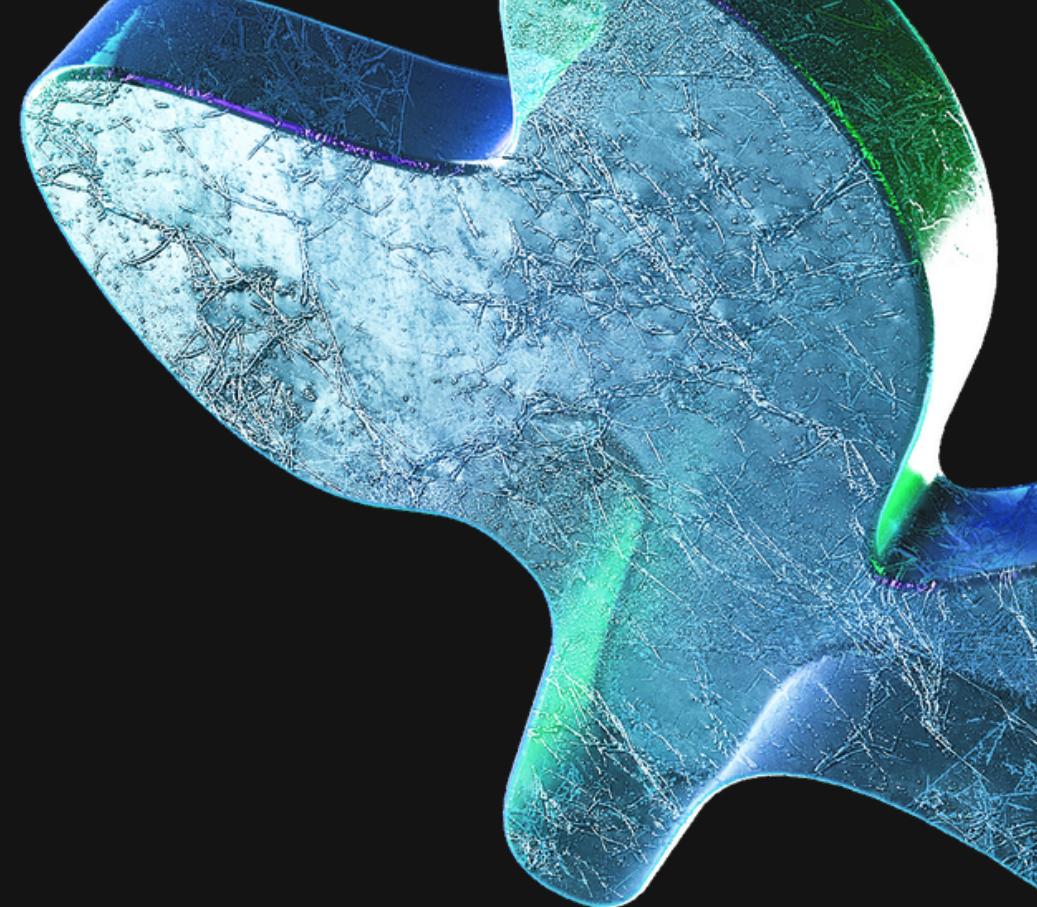
MANTENERE AGGIORNATI I SOFTWARE

I software obsoleti possono contenere vulnerabilità che possono essere sfruttate dagli aggressori per lanciare attacchi DDoS. È importante mantenere aggiornati i software di tutte le applicazioni Web e dei sistemi correlati.

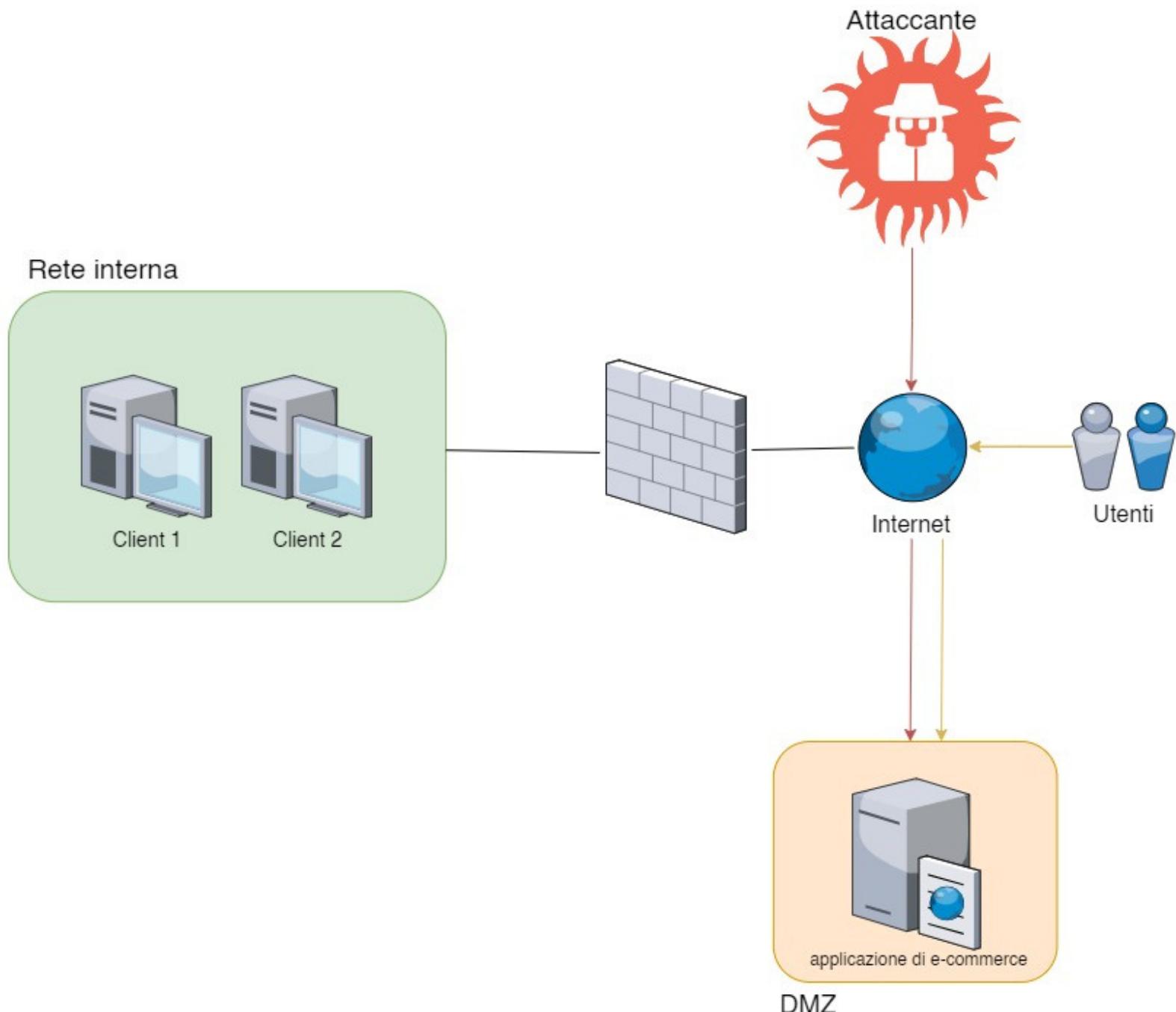
Response per servizio web infettato da un malware

Per evitare che il nostro server web infetti tutta la rete utilizzeremo il metodo dell'**isolamento**.

Quindi disconnetteremo completamente il server lasciando però l'accesso all'attaccante



Rete con metodo d'isolamento



in questo caso è stato utilizzato l'isolamento per poter lasciare un accesso al black hat mentre il server è stato completamente disconnesso dalla rete.

Non sono stati utilizzati l'Air Gap perché non avrebbe lasciato alcun accesso all'attaccante o la segmentazione perché il server infetto sarebbe rimasto all'interno della rete aziendale.

FINE

