Report Venerdì 16/09

Azioni preventive - Impatti sul business - Response

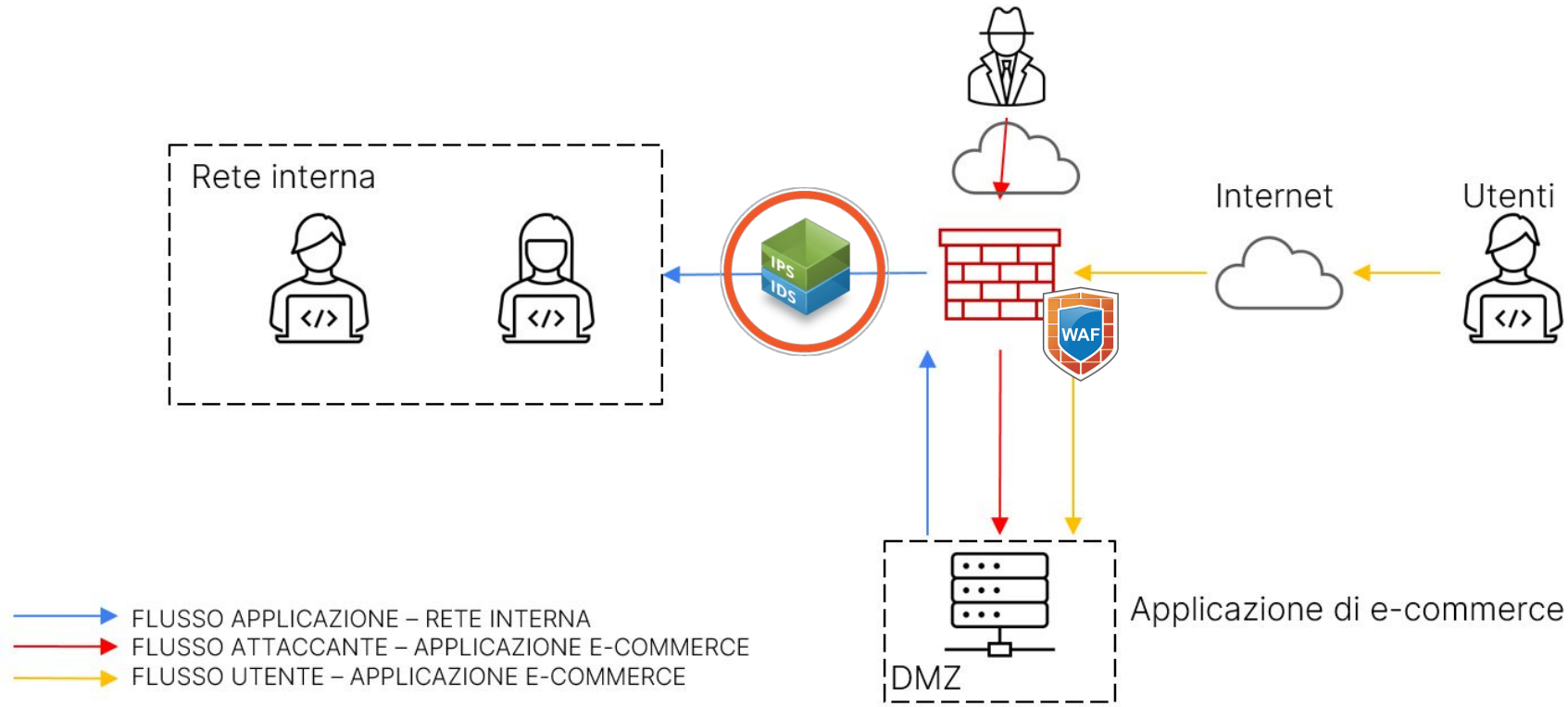
Ivona Kovacevic

Azioni preventive

Le azioni che potrebbero prevenire l'attacco da un utente malintenzionato verso la nostra web app, in particolare con la SQLi e l'XSS, sono l'inserimento di altri sistemi perimetrali di sicurezza, come i *WAF* e gli *IDS*.

IDS: l'Intrusion Detection System monitora continuamente la sicurezza della nostra rete, con lo scopo di identificare in anticipo gli attacchi alle reti informatiche ed ai computer.

WAF: il Web Application Firewall è un firewall aggiuntivo che ha il compito di aumentare la protezione delle applicazioni web aziendali. La loro specializzazione consiste nel intercettamento e realizzazione di traffico HTTP.


Rete interna
IPS
IDS
WAF
Internet
Utenti
DMZ
Applicazione di e-commerce
FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE

Impatti sul business

Se l'azienda subisce un attacco DDoS che la rende irraggiungibile per **10 minuti**, considerando che ogni minuto gli utenti spendono all'incirca **1.500 $** sull' e-commerce, l'azienda si trova in criticità '***media***' e l'impatto finanziario è pari a circa **15.000 $**.

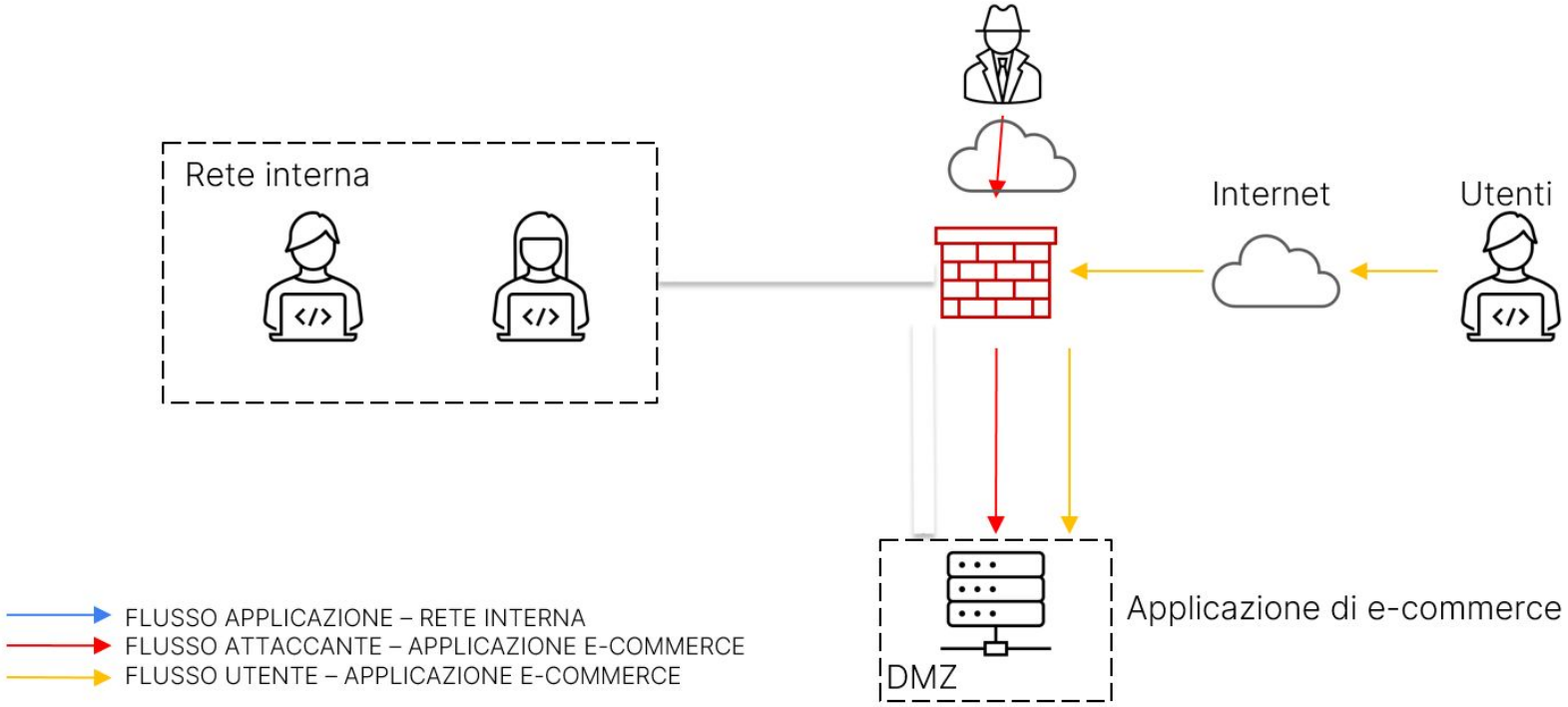
Il fatto che l'azienda si trovi nel livello medio di criticità significa che questa non può erogare alcuni dei servizi critici ad un limitato numero di utenti.

Response

La priorità, in caso di attacco da un malintenzionato verso la nostra web app, è quella di proteggere la nostra **rete interna**.

Per **interrompere la comunicazione** tra la *DMZ* e la *rete interna* dobbiamo modificare le impostazioni del firewall, perchè è il modo più probabile che il malintenzionato avrebbe usato per accedervi.

Dobbiamo interrompere lo scambio di dati tra le due parti, impostando il firewall affinché non accetti dati in entrata dalla DMZ.


Rete interna
Internet
Utenti
DMZ
Applicazione di e-commerce
FLUSSO APPLICAZIONE – RETE INTERNA
FLUSSO ATTACCANTE – APPLICAZIONE E-COMMERCE
FLUSSO UTENTE – APPLICAZIONE E-COMMERCE

Disegno completo delle modifiche fatte alla rete