



**DARIO
SANTIGLIANO**

S9L5

PROJECT

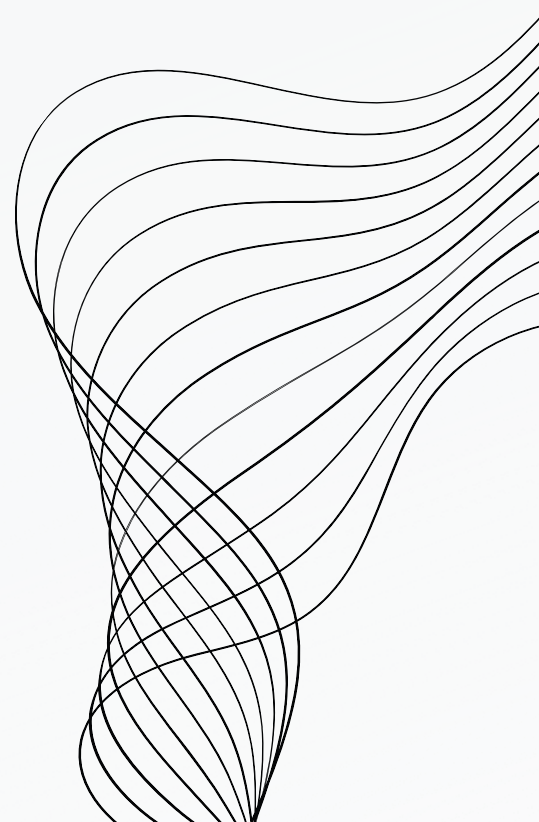


INDICE RELAZIONE

- 01** TRACCIA ESERCIZIO
- 02** ARCHITETTURA DI RETE
- 03** AZIONI PREVENTIVE
- 04** IMPATTI SUL BUSINESS
- 05** RESPONSE

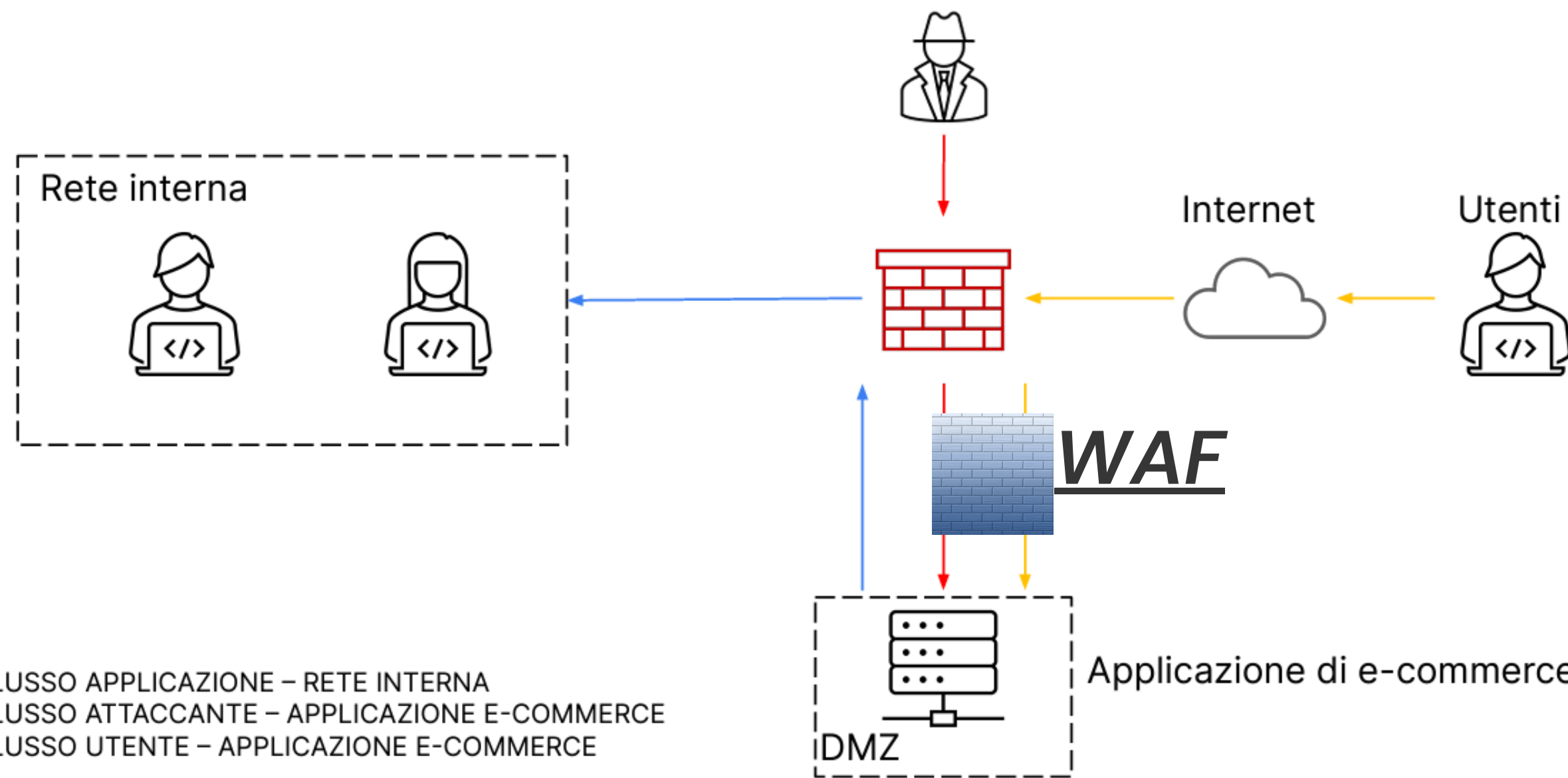
TRACCIA ESERCIZIO

TRACCIA: CON RIFERIMENTO ALLA FIGURA IN SLIDE 2, 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

IN QUESTA SITUAZIONE POSSIAMO RICORRERE ALL'USO DEL WAF PER PROTEGGERE IL WEB SERVER. CI SONO TUTTAVIA DEGLI ACCORGIMENTI DA PRENDERE PER AUMENTARE LA PROTEZIONE DAGLI ATTACCHI COME LA SANIFICAZIONE DEGLI INPUT DELL'APPLICAZIONE IN MODO CHE ACCETTINO SOLO I VALORI CHE SI ASPETTANO.



WAF

ANDIAMO A VEDERE NELLO SPECIFICO COS'È UN WAF.

**È L'ACRONIMO DI WEB APPLICATION FIREWALL E IL SUO SIGNIFICATO STA
A INDICARE UNA TECNOLOGIA CHE AUMENTA LA PROTEZIONE DELLE
APPLICAZIONI WEB AZIENDALI E AIUTA LE ORGANIZZAZIONI A DIFENDERSI
ADEGUATAMENTE DA DIVERSI TIPI DI ATTACCHI INFORMATICI,
PROTEGGENDO IN MANIERA SICURA I DATI.**

PERCHÉ LA SICUREZZA WAF È IMPORTANTE?

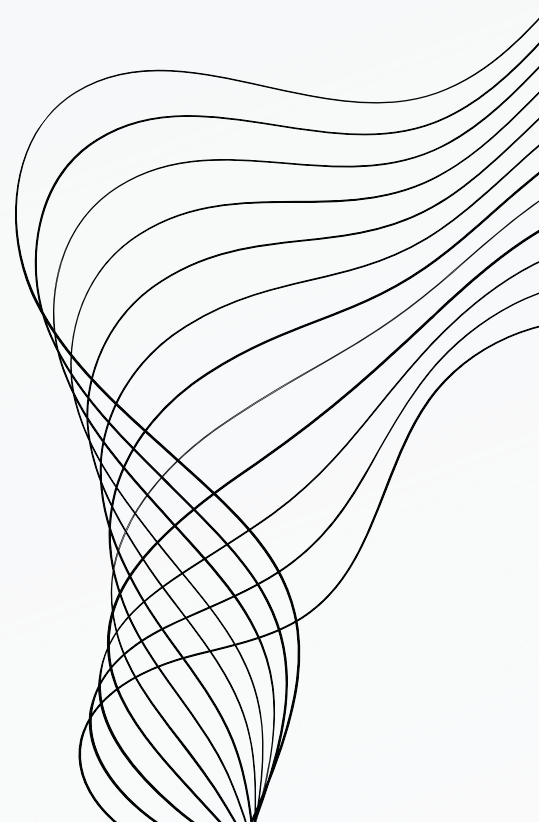
**I FIREWALL DELLE APPLICAZIONI WEB AIUTANO A PROTEGGERE LE
APPLICAZIONI DISTRIBUITE NEL CLOUD PUBBLICO, ON PREMISE E IN
AMBIENTI MULTICLOUD CON CONTROLLI DELL'ACCESSO BASATI SUI DATI
DI GEOLOCALIZZAZIONE, SULLA LISTA DI INCLUSIONE E SUGLI INDIRIZZI IP
IN BACKLIST, SULL'URL HTTP (HYPERTEXT TRANSFER PROTOCOL UNIFORM
RESOURCE LOCATER) E SULL'INTESTAZIONE HTTP.**

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.

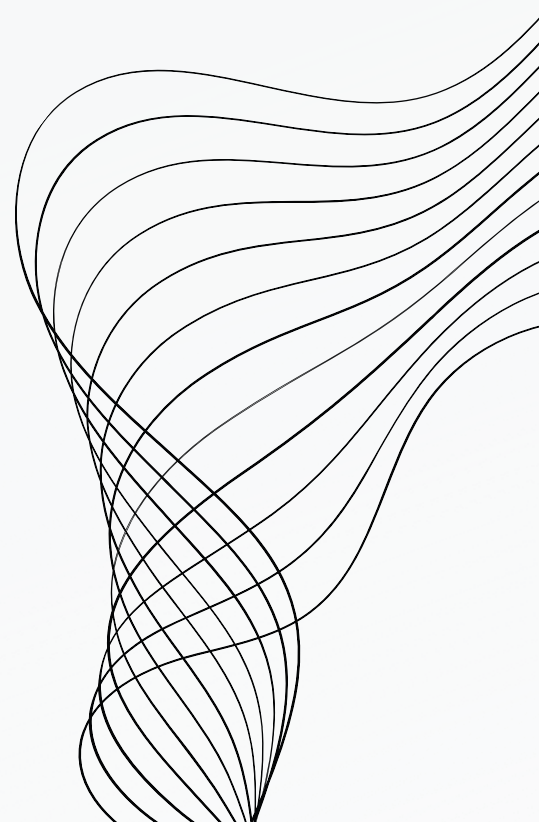
STIMA DEI DANNI


CONSIDERANDO CHE OGNI MINUTO L'AZIENDA GUADAGNA 1.500€ ALL'ORA PER 10 MINUTI DI IRRAGGIUNGIBILITÀ L'AZIENDA PERDERÀ 15.000 €.



RESPONSE

***VISTA LA PRIORITÀ È POSSIBILE IMPLEMENTARE UNA STRATEGIA BASATA
SULL'ISOLAMENTO DELLA MACCHINA INFETTA. IN QUESTO MODO LA
MACCHINA SARÀ CONNESSA AD INTERNET ED ACCESSIBILE
ALL'ATTACCANTE MA NON AVRÀ MODO DI ACCEDERE ALLA RETE INTERNA***



02. 

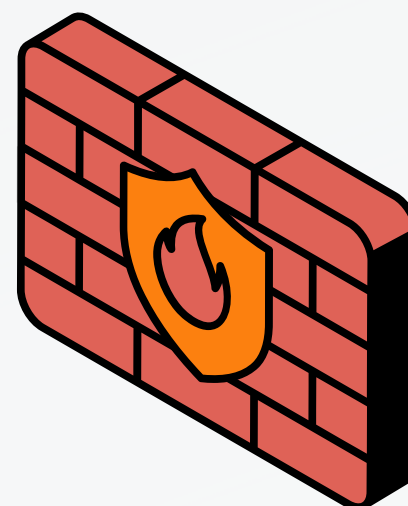
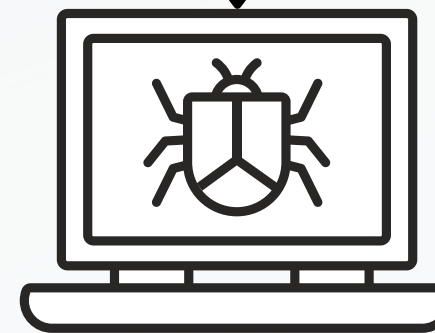
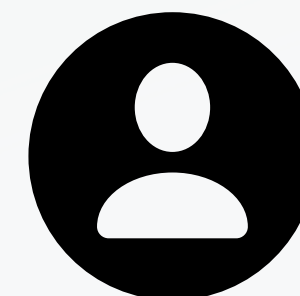
RESPONSE

ATTACCANTE



INTERNET

USER



DMZ

RETE INTERNA

