



BUILD  
WEEK



Net Rebels

# DESIGN DI RETE

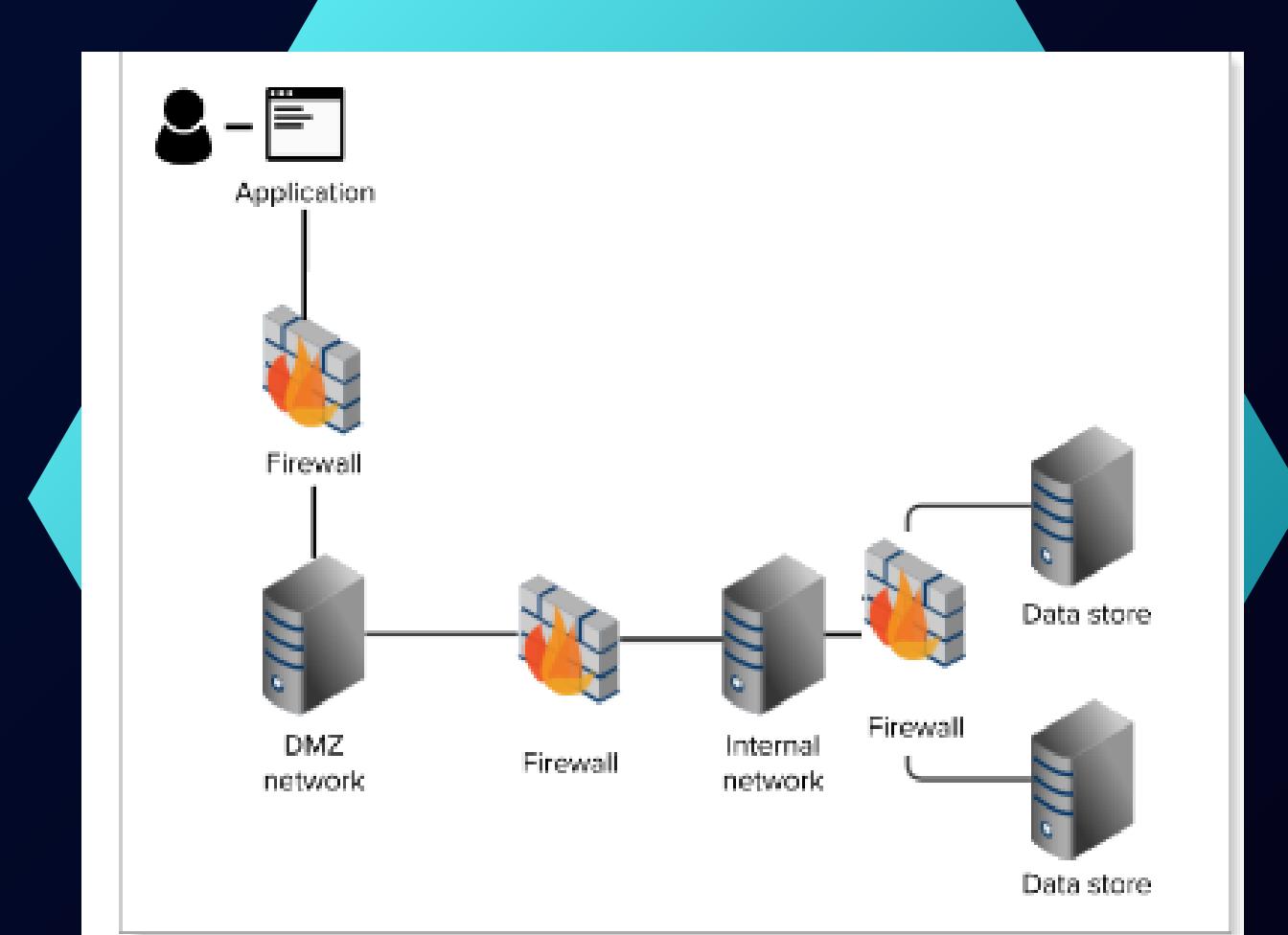
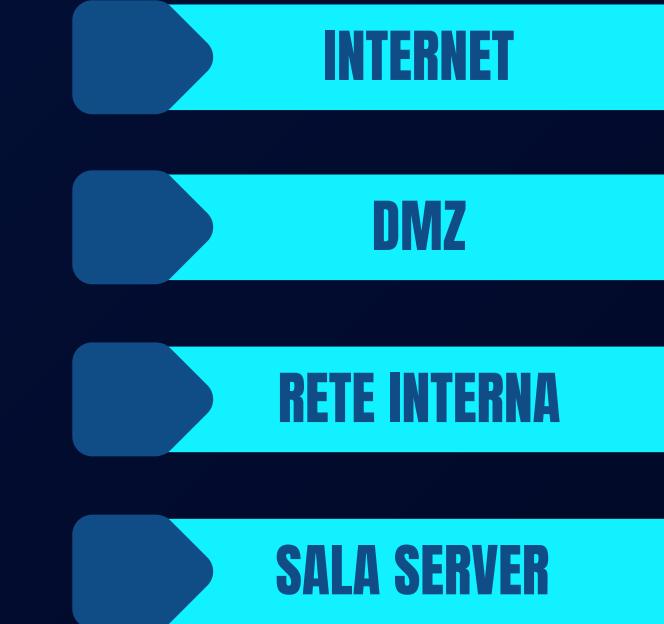


Per il design di rete si è optato per la tecnica della segmentazione che divide una rete locale in parti più piccole allo scopo di migliorarne prestazioni e sicurezza.

## VANTAGGI:

- efficientare il monitoraggio
- aumentare le prestazioni
- localizzare problemi tecnici

Le minacce Cyber arrivano da internet e soprattutto dall'interno. Motivo per il quale, è necessario che l'azienda adoperi una struttura di rete come quella della multi-tier DMZ, nel quale oltre ad esserci la divisione in zone di rete in base alla criticità degli asset sui segmenti di rete, si aggiungono più livelli di sicurezza.



# FIREWALL

Si è applicato un *firewall perimetrale*, utile per definire la sicurezza della rete e per controllare il traffico in entrata e in uscita.

Mentre il secondo firewall è stato messo a protezione della rete interna negando ogni accesso.

In questo modo possiamo monitorare le informazioni filtrandole nel caso le ritenga non affidabili e bloccandole se necessario. Tipicamente un firewall definisce ciò che può entrare o uscire dal sistema, utilizzando dei criteri.

Il terzo firewall è stato messo a protezione della sala server, come ulteriore strumento di sicurezza. (Il modello di firewall scelto, che vedremo in seguito, ci darà la possibilità di attivare anche un *revers proxy*)

---

Nel nostro caso andremo anche a disabilitare tutti i protocolli verso la rete interna lasciando attivi solo **http/https** verso la rete DMZ. In più verrà creata una black list con all'interno una lista di ip malevoli e richieste Http (con log injection) già conosciute in rete, quest'ultima verrà poi tenuta costantemente aggiornata grazie al monitoring dell'analista aiutato anche dallo strumento SOAR (che illustreremo in seguito).



Queste tecnologie vengono configurate seguendo determinati parametri e regole che se risultano troppo permissive, possono presentare delle falle ed esporre il sistema informatico al pericolo di essere attaccato.

Per il design della rete riteniamo quindi utile applicare:

# FIREWALL FORTIGATE 100F

dell'azienda statunitense Fortinet



## Caratteristiche tecniche:

- Identifica migliaia di applicazioni all'interno del traffico di rete grazie ad un'ispezione approfondita e profonda
- Protegge da malware, exploit e siti Web dannosi in traffico crittografato e non crittografato
- Previene e rileva da attacchi noti e sconosciuti
- Traffico crittografato
- Funzionalità di rete avanzate, ad alte prestazioni e capacità VPN IPsec scalabili per consolidare la rete
- Console centralizzata con interfaccia grafica, semplice da utilizzare
- Monitoraggio in tempo reale delle sonde IPS/IDS

In questo modello di firewall è previsto anche il **WAF (web application firewall)** che consente di proteggere le applicazioni Web da attacchi dannosi e traffico Internet indesiderato, inclusi bot, injection e denial of service (DoS) a livello di applicazione.

Inoltre, consigliamo l'attivazione del **reverse proxy** che è un server che si trova tra i client e un gruppo di server backend, inoltrando le richieste dei client ai server appropriati e rispondendo ai client per conto di quei server. Questo tipo di configurazione offre numerosi vantaggi in termini di sicurezza, prestazioni e gestione del traffico.

Per migliorare ancora di più la vostra sicurezza di rete consigliamo l'implementazione di sistemi di gestione centralizzata e strumenti di monitoraggio:

## 1 SIEM

(Security information and event management) in italiano, raccoglie dati da varie fonti, come server e applicazioni per identificare attività dannose, inoltre fornisce informazioni sulle minacce correlando dati provenienti da diverse fonti e creando una dashboard di facile consultazione

## 2 SOAR

(Security Orchestration, Automation and Response), in italiano, l'orchestrazione, l'automazione e la risposta alla sicurezza, è una soluzione software che consente ai team di integrare e coordinare strumenti di sicurezza separati, automatizzare le attività ripetitive e semplificare i workflow di risposta agli incidenti e alle minacce

### Abbiamo optato per un “*Splunk Enterprise*” prodotto da CISCO

“ Pertanto l'implementazione di entrambi gli strumenti porterebbe un grande vantaggio all'azienda in termini di sicurezza e risposta agli incidenti in quanto, possono creare una soluzione di sicurezza più completa e reattiva.



# 1 SIEM

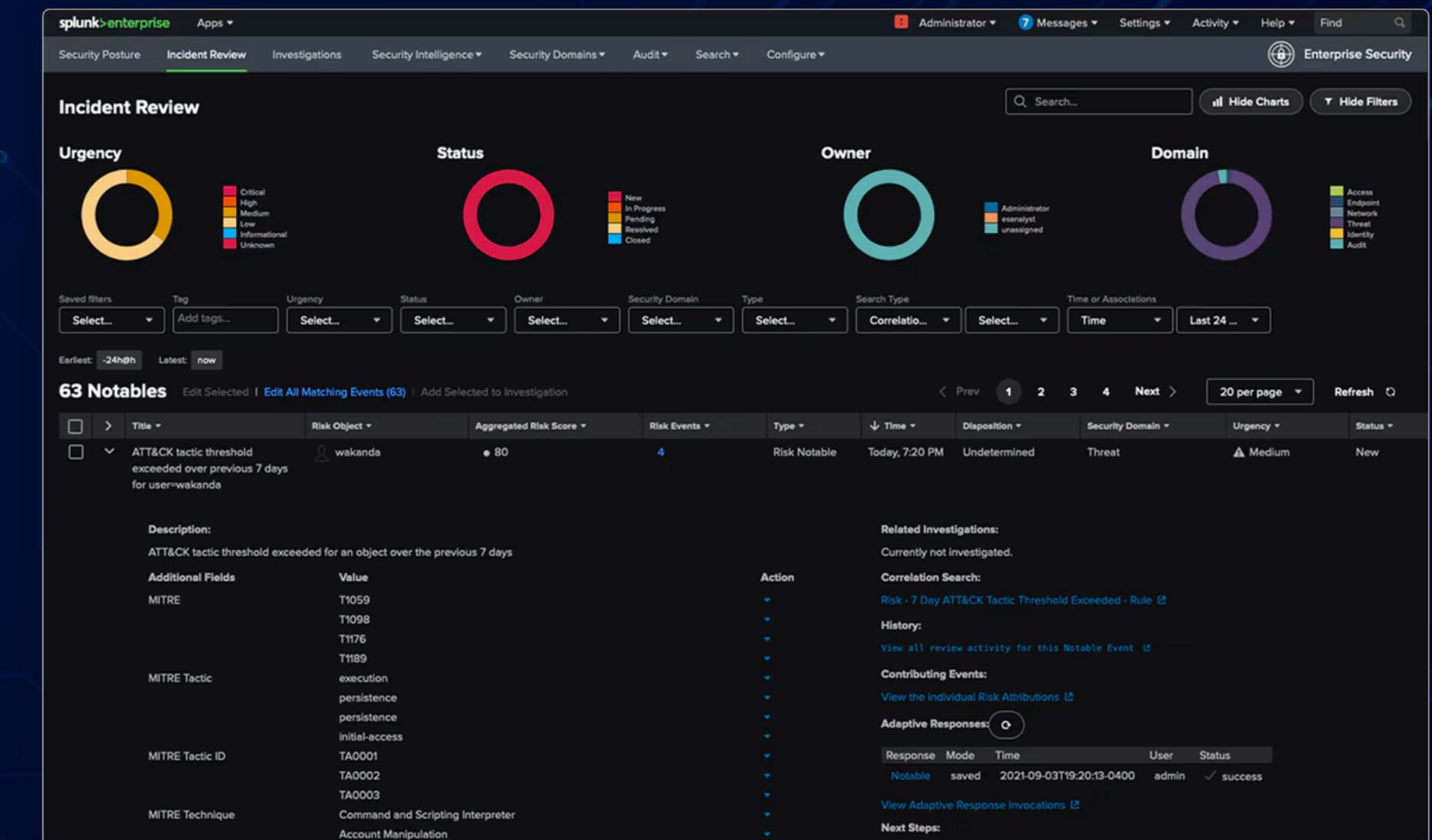
I componenti di un SIEM sono:

- La raccolta dei dati
- Categorizzazione
- Correlazione
- Monitoraggio costante di anomalie
- Report e Analisi



## VANTAGGI:

- Riconoscimento delle minacce in tempo reale
- Migliorare efficienza organizzativa
- Rilevamento di minacce avanzate e sconosciute



Le soluzioni SIEM viene usato per semplificare la gestione della sicurezza su reti grandi e disperse.

Aiuta a mantenere un registro rigoroso delle attività degli utenti.

Fornisce informazioni dettagliate su chi ha avuto accesso a quali risorse e quando, aiutando a rilevare e prevenire attività non autorizzate. Archiviando e analizzando i dati di registro relativi alle attività degli utenti è quindi possibile effettuare indagini sugli incidenti.



# SOAR



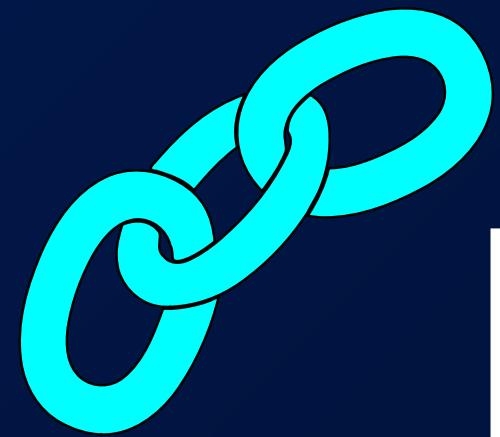
Per **orchestrazione della sicurezza** si intende il modo in cui le piattaforme SOAR si connettono e coordinano l'hardware e gli strumenti software nel sistema di sicurezza di un'azienda.

La soluzione di sicurezza SOAR utilizza l'intelligenza artificiale basata sull'apprendimento automatico per dare priorità agli avvisi sugli incidenti e alle azioni di risposta. Aiuta ad analizzare e correlare grandi quantità di dati. Sfruttando le sue capacità aiuta a distinguere tra falsi positivi e minacce reali. Analizza i dati storici e identifica modelli ripetibili di comportamenti noti buoni e cattivi. Questo riconoscimento aiuta a ridurre i falsi allarmi. E' possibile creare procedure di risposta predefinite per mitigare l'impatto di un incidente di sicurezza.

Queste procedure possono includere:

- Isolamento e messa in quarantena dei sistemi interessati.
- Identificare la fonte della minaccia.
- Determinare la gravità della minaccia e avviare una serie di azioni di risposta automatizzate in base a tale gravità.

Integrando SIEM con una piattaforma SOAR, possiamo sfruttare le funzionalità di monitoraggio e correlazione degli eventi in tempo reale di SIEM e automatizzare le risposte agli incidenti tramite SOAR.



## **SIEM**

Raccolta, analisi e monitoraggio dei log e degli eventi di sicurezza in tempo reale.

Correlazione degli eventi, rilevamento delle minacce, gestione degli incidenti e conformità

## **SOAR**

Automazione e orchestrazione delle operazioni di sicurezza, inclusa la gestione degli incidenti e la risposta alle minacce

Automazione delle risposte agli incidenti, orchestrazione tra diversi strumenti di sicurezza, gestione dei casi

Oltre all'applicazione di questi strumenti è necessario assicurarsi che i server e tutte le applicazioni siano aggiornati con le ultime patch di sicurezza quindi è altamente consigliato consultare il sito NIST ( National Institute of Standards and Technology )

# PRINCIPIO DEL PRIVILEGIO MINIMO

è uno dei principi fondamentali nella protezione degli ambienti IT

## Proponiamo il software della **STRONG DM**

Limitare le autorizzazioni di ciascun utente solo a ciò che è strettamente necessario, riduce la superficie di attacco dei sistemi critici. In particolare, POLP riduce il rischio di utilizzo sia involontario che dannoso di dati e applicazioni, indipendentemente dal fatto che tali azioni provengano dagli utenti stessi o da aggressori esterni che ne hanno compromesso le credenziali.

Ad esempio, POLP riduce il rischio di infezione da ransomware, poiché la maggior parte degli account utente non avrà i privilegi amministrativi necessari per installare il malware. E anche se viene eseguito, sarà in grado di crittografare solo i dati a cui ha accesso l'account utente, quindi lo strumento POLP riduce il danno che può essere inflitto.

Ma nei peggiori dei casi vi sono solidi piani di risposta e ripristino agli incidenti.



**strongdm**

## FORMAZIONE DEL PERSONALE NON TECNICO

Ancora, riteniamo necessario prevedere un corso di formazione del personale non tecnico per rendere la loro esperienza nella rete più consapevole e sicura.

Iniziando con sondaggi e questionari per capire il livello delle competenze dei dipendenti e fissare dei meeting online o in azienda per introdurre concetti di base sulle minacce comuni (phishing, malware, ransomware) e far capire l'importanza di utilizzare credenziali (password) forti e uniche.

## PERSONALE IT

Incentivare il personale IT a ottenere certificazioni riconosciute e fare corsi di aggiornamento per rimanere sempre al passo con le nuove tecnologie e minacce.



# BACKUP E AI PIANI DI RIPRISTINO

fondamentali per garantire la continuità operativa e la protezione dei dati aziendali in caso di guasti, attacchi informatici, disastri naturali o altri eventi imprevisti.

Il modello che consigliamo è **Acronis Cyber Backup Advanced for Server**

## Caratteristiche

- **Backup Completo:** Protegge server fisici, virtuali, endpoint e dati cloud.
- **Cyber Protection:** Include funzionalità di protezione contro ransomware.
- **Ripristino Rapido:** Ripristino rapido dei dati e delle applicazioni critiche.
- **Gestione Centralizzata:** Console di gestione centralizzata per la gestione dei backup.



PRO	CONTRO
Protezione integrata contro ransomware	Prezzi variabili a seconda delle funzionalità richieste
Facilità d'uso e di implementazione	Potrebbe avere funzionalità avanzate limitate rispetto ad altri strumenti
Ottimo supporto per ambienti ibridi	

# AUTENTICAZIONE A DUE FATTORI (2FA)

Rappresenta un'ulteriore sicurezza per la protezione delle password, è indispensabile prevedere oltre alla password un altro fattore di autenticazione e consigliamo di utilizzare dei soft token che generano un OTP (one time password), codice a 6 cifre, associato ad uno specifico account.

In particolare potrete scegliere di optare per [Google authenticator](#), selezionando l'account di interesse permette di creare un codice temporaneo che si potrà utilizzare per l'autenticazione (di solito valido per 30s). Può essere utilizzato anche in modalità offline, configurare più account nell'app, compatibile sia per android che iOS ed è gratuito.

## Vantaggi

- Sicurezza Migliorata: Aggiunge un ulteriore livello di protezione ai tuoi account, riducendo il rischio di accessi non autorizzati.
- Facilità d'Uso: L'app è intuitiva e semplice da usare, con un'interfaccia user-friendly.
- Compatibilità: Supporta una vasta gamma di servizi online, non solo quelli di Google.



# FATTURA



NetRebels S.r.l.

Via ribelli del Web, 456  
18467953180

Unicredit  
SWIFT/BIC: UNICRTMM  
Numero del conto corrente:  
IT60X 0542811101000000123456

## Preventivo

Theta S.r.l  
Via Roma, 10

Data fattura:  
18/06/2024  
Data di scadenza:  
03/07/2024

Quantità	Descrizione	Prezzo	Iva	Subtotale
3	Fortinet Fortigate 100F Firewall - 1 Anno	€ 11.616,00	€ 2.555,52	€ 9.060,48
1	Siem Splunk Enterprise – 1 Anno	€ 2.500,00	€ 550,00	€ 1.950,00
1	Soar Splunk Enterprise – 1 Anno	€ 7.500,00	€ 1.650,00	€ 5.850,00
1	Acronis cyber backup (server)-3 Anni	€ 1.184,07	€ 260,48	€ 923,52
1	Consulenza sulla sicurezza informatica (Da definire la grandezza della Infrastruttura interna)	€ 3.500,00	€ 770,00	€ 2.730,00
1	Strong DM	€ 4.800,00	€ 1.056,00	€ 3.744,00

SUBTOTALE € 24.258,00  
IVA € 6.842,00

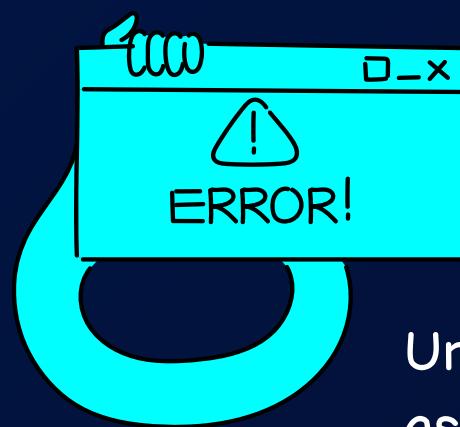
**TOTALE € 31.100,07**

# CONCLUSIONE

Implementare queste misure di sicurezza aiuterà a proteggere sia il web server esposto pubblicamente che il server applicativo accessibile solo internamente. Questo approccio multilivello garantisce che la sicurezza sia integrata in tutti gli aspetti dell'infrastruttura, riducendo i rischi e migliorando la resilienza contro le minacce.

# SQL INJECTION

Gli attacchi SQL injection sono un tipo di attacco informatico in cui gli hacker mirano a iniettare, o inserire, il proprio codice in un sito web, in un'app o addirittura in un programma. Per cui, quando i criminali informatici trovano piccoli errori di script o imprecisioni nel codice sorgente dei sistemi di database basati su SQL, è come se trovassero una porta aperta perché sono in grado di scoprire vulnerabilità e di iniettare il proprio codice.



Un attacco SQL injection andato a buon fine potrebbe risultare asintomatico. Tuttavia, talvolta questi attacchi sono segnalati da indicatori come:

- Numero eccessivo di richieste in breve tempo. Potresti ad esempio ricevere numerose e-mail provenienti dal modulo di contatto della tua pagina Web.
- Annunci che reindirizzano a siti Web sospetti.
- Strani messaggi pop-up e di errore.

## Impatto degli attacchi SQL injection

Un attacco SQL injection andato a buon fine può avere gravi conseguenze per un'azienda. Questo avviene perché un attacco SQL injection può:

- Esporre dati sensibili
- Compromettere l'integrità dei dati
- Compromettere la privacy degli utenti
- Concedere all'autore di un attacco l'accesso al sistema come amministratore
- Concedere a un aggressore l'accesso generale al sistema

Il costo di un attacco SQL injection non è solo finanziario, può anche comportare la perdita di fiducia dei clienti

## Escape

Un modo diretto, anche se soggetto ad errori per prevenire attacchi di SQLI è quello di evitare caratteri che hanno un significato speciale in SQL.

# STEGANOGRAFIA

La steganografia è un'arte che permette di nascondere messaggi segreti all'interno di contenitori innocui, tecnica conosciuta già nell'antica Grecia. Il messaggio nascosto rimane invisibile all'occhio umano e può essere estratto solo da chi possiede le informazioni necessarie.

## Tecniche

### steganografia iniettiva

la più comune identificata anche come LSB (least significant Bit) , e si basa sulla modifica del bit meno significativo. Consiste nell'inserire (iniettare) il messaggio segreto all'interno di un altro messaggio che funge da contenitore, in modo tale da costruire un messaggio contenitore (a volte detto steganogramma) praticamente indistinguibile dall'originale

### steganografia generativa

consiste nel prendere il messaggio segreto e costruirgli un opportuno contenitore in modo tale da nascondere il messaggio nel miglior modo possibile.

## Come funziona:

La steganografia sfrutta la ridondanza presente nei file digitali per nascondere il messaggio segreto. Ad esempio, in un'immagine. I tools steganografici possono "rompere" pixel poco significativi e celare un'informazione al loro interno, ma la differenza è così piccola che sarà impercettibile per l'occhio umano notare cambiamenti, ma qualsiasi modifica effettuata dopo l'inserimento del messaggio ne comporterà la perdita.

**La steganografia è uno strumento potente che può essere utilizzato per nascondere messaggi segreti in modo sicuro e discreto. Tuttavia, è importante essere consapevoli dei suoi limiti e utilizzarlo in modo responsabile**

4

THANKS

YOU

4

4