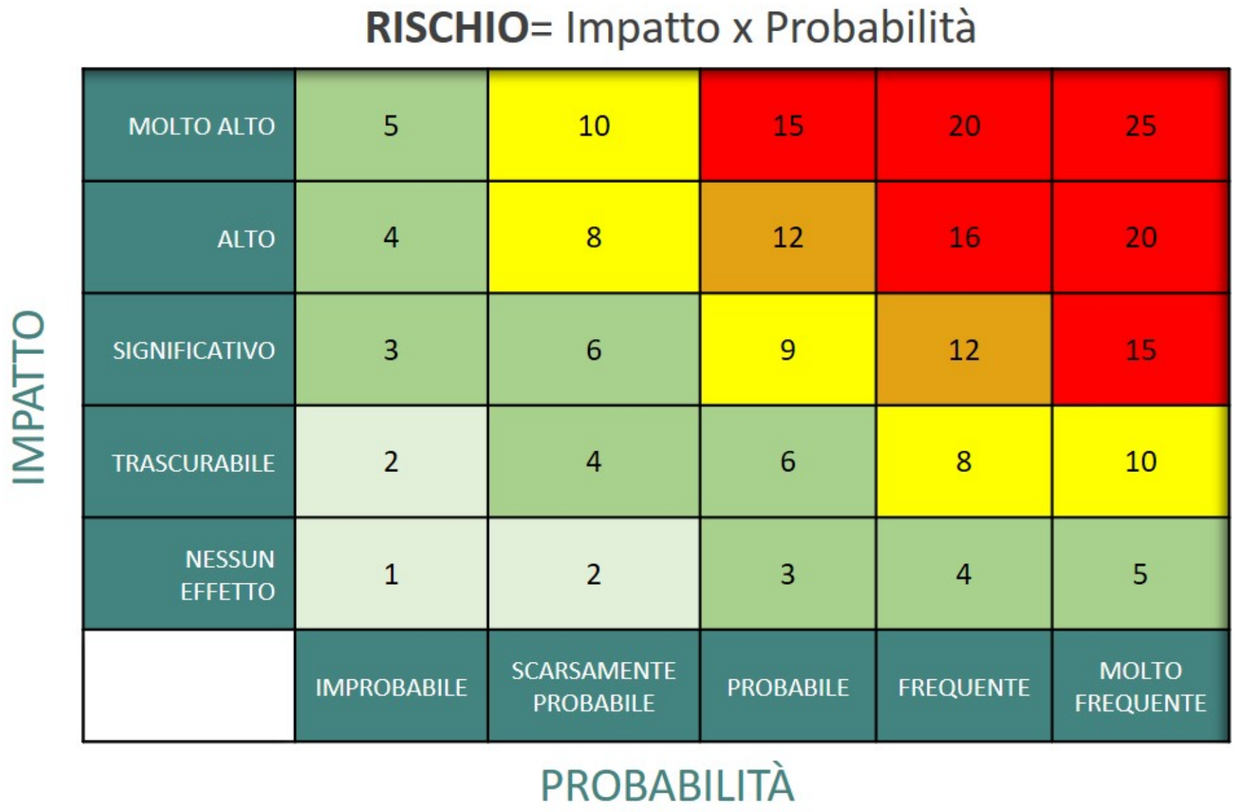
Build Week – 1

REPORT FINALE

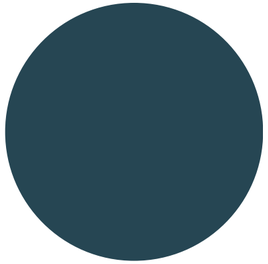
BRUTE FORCE

Per difendersi dagli attacchi di forza bruta, è essenziale implementare misure di sicurezza robuste. In primo luogo, l'uso di password complesse, combinate con politiche di aggiornamento regolare, rende più difficile indovinare le credenziali. Inoltre, l'implementazione di blocchi temporanei dopo un numero specifico di tentativi falliti protegge dall'accesso non autorizzato. L'autenticazione a due fattori aggiunge un ulteriore strato di sicurezza, richiedendo un secondo metodo di verifica oltre alla password. Andando avanti con le Slide troveremo alcuni metodi e andremmo a spiegare nel dettaglio il loro funzionamento

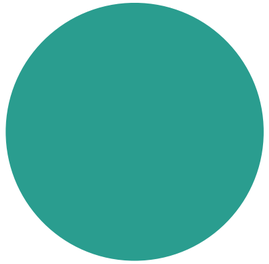
Formula del rischio



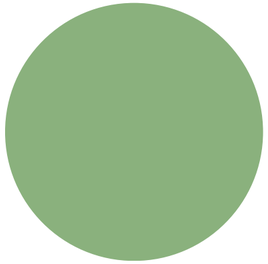
La formula del rischio in sicurezza informatica si basa sull'idea che il rischio è il risultato dell'impatto delle possibili vulnerabilità moltiplicato per la probabilità che queste vulnerabilità vengano sfruttate. In altre parole, quanto gravi possono essere le conseguenze di una minaccia (impatto) e quanto è probabile che tale minaccia si verifichi (probabilità). Questa formula aiuta a valutare e gestire meglio i rischi informatici, focalizzando le risorse sulle aree con il potenziale maggiore impatto e probabilità.



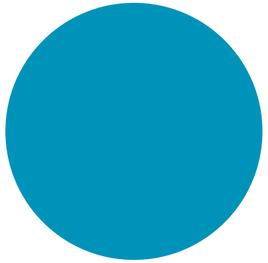
PROTOCOLLO HTTPS



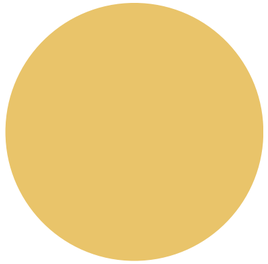
PASSWORD ROBUSTE



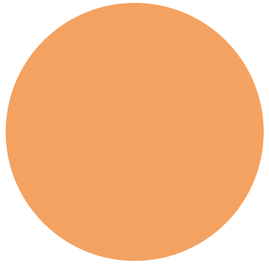
AUTENTICAZIONE 2FA



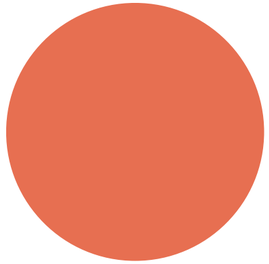
CRYPTOGRAFARE CREDENZIALI



JWT - TOKEN



FIREWALL - BLACK LIST



PERSONALE FORMATO

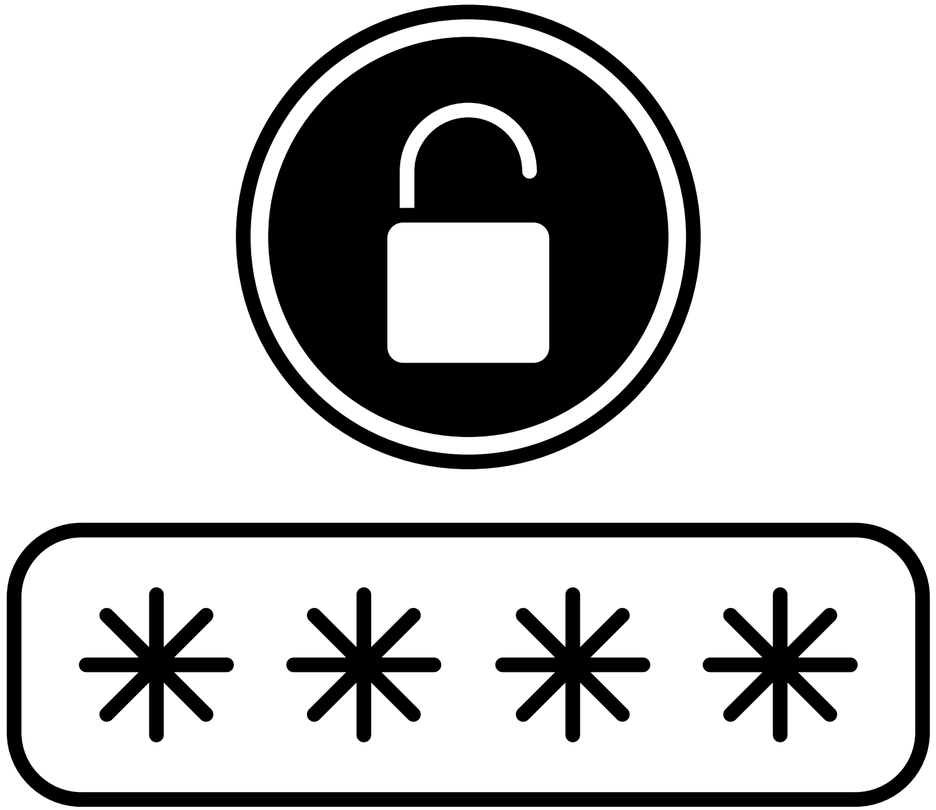
TIMESLEP - TENTATIVI

PROTOCOLLO HTTPS

Il protocollo HTTP attualmente usato e mo lto vulnerabile ad avere il traffico tra nostro web server e clienti intercettato per utenti esterni, ed avere la informazione sensibile ispezionata. Il metodo HTTP aggiunge i protocolli di criptazione SSL/TLS che permetteranno un tunnel di comunicazione sicura.

PASSWORD ROBUSTE

Esistono tre principali tipi di attacchi per violare una password: attacco a dizionario, password profiling e brute force attack. Per difendersi, è consigliabile adottare password robuste di almeno 8 caratteri, evitando informazioni prevedibili facilmente rintracciabili. La sostituzione di lettere con caratteri speciali non è sufficiente; è preferibile usare combinazioni di numeri, lettere e caratteri speciali. È importante utilizzare password diverse per ogni account e, se possibile, cambiarle regolarmente, specialmente su piattaforme frequentemente bersagliate da hacker. La protezione delle password è cruciale per la tutela dei dati aziendali e la continuità operativa.



Esempio di password robusta: **&9Kp#2qZw!**

AUTENTICAZIONE 2FA

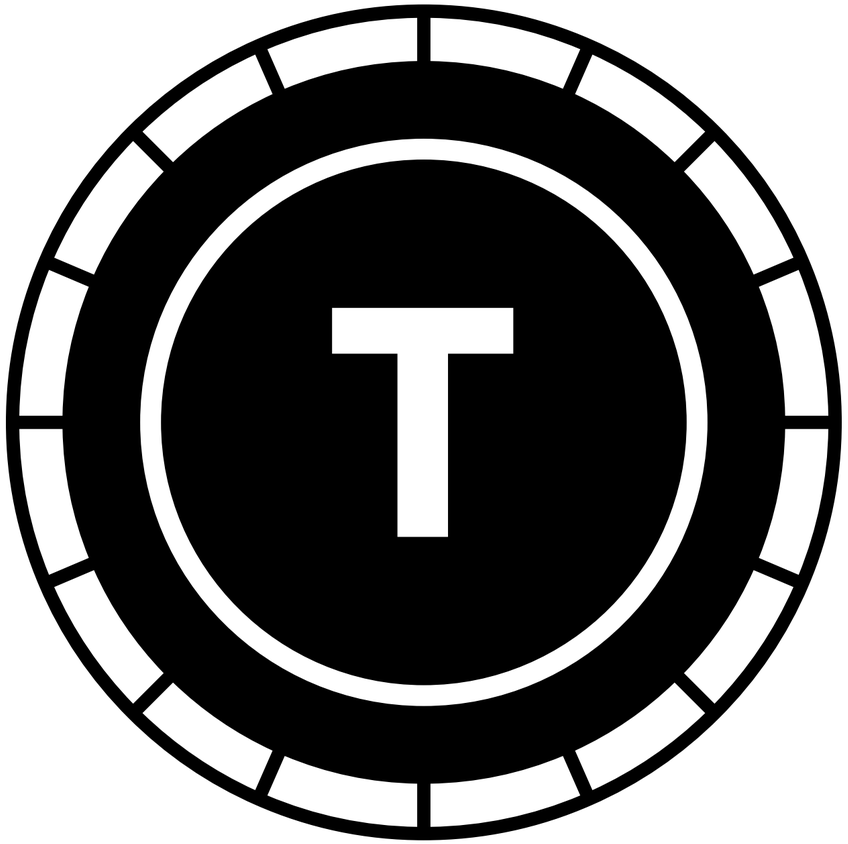
2FA, o autenticazione a due fattori, è un metodo di verifica dell'identità che richiede che un utente fornisca un secondo fattore di autenticazione in aggiunta alla password per poter accedere a un sito Web.
Poiché è più complesso violare un secondo fattore di autenticazione e poiché altri tipi di fattori sono più difficili da rubare o falsificare, 2FA migliora la sicurezza dell'account e protegge in modo più efficace un'organizzazione e i suoi utenti dall'accesso non autorizzato.

Per l'autenticazione ai servizi digitali sono ipotizzabili tre metodi basati su:
1.**UNA COSA CHE CONOSCI:** la password o un PIN
2.**UNA COSA CHE HAI:** lo smartphone o un token fisico
3.**UNA COSA CHE SEI:** alcune tue caratteristiche fisiche l'impronta digitale, la scansione dell'iride

CRYPTOGRAFIA CREDENZIALI

A7B8M3L6790JYTVN124
NTCY42U565N23B7N9A7
V87DVI62S8S768IQRKUI
NY1QJHBUO8I1GUICHVI1
23089BWRIYUO98J1

La crittografia delle credenziali è un modo per proteggere i dati sensibili durante la loro trasmissione o archiviazione. Utilizzando il metodo hashing si trasformeranno questi dati sensibili in una stringa esadecimale computazionalmente infattibile da decrittare senza la chiave segreta.



JWT TOKEN

JWT, acronimo di JSON Web Token, è un sistema di cifratura e di contatto in formato JSON per lo scambio di informazioni tra i vari servizi di un server.
Il client invia una richiesta al server e questo genera un token di autenticazione che il client utilizzerà tutte le volte che andrà a collegarsi allo stesso nodo.

STRUTTURA: HEADER.PAYLOAD.SIGNATURE

SIGNATURE, fase di cifrature delle due parti:
Payload e Header del token, vengono dapprima unite e successivamente sottoposte ad un operazione di crittografia, alla fine viene generata una chiave che darà luogo al token stesso.

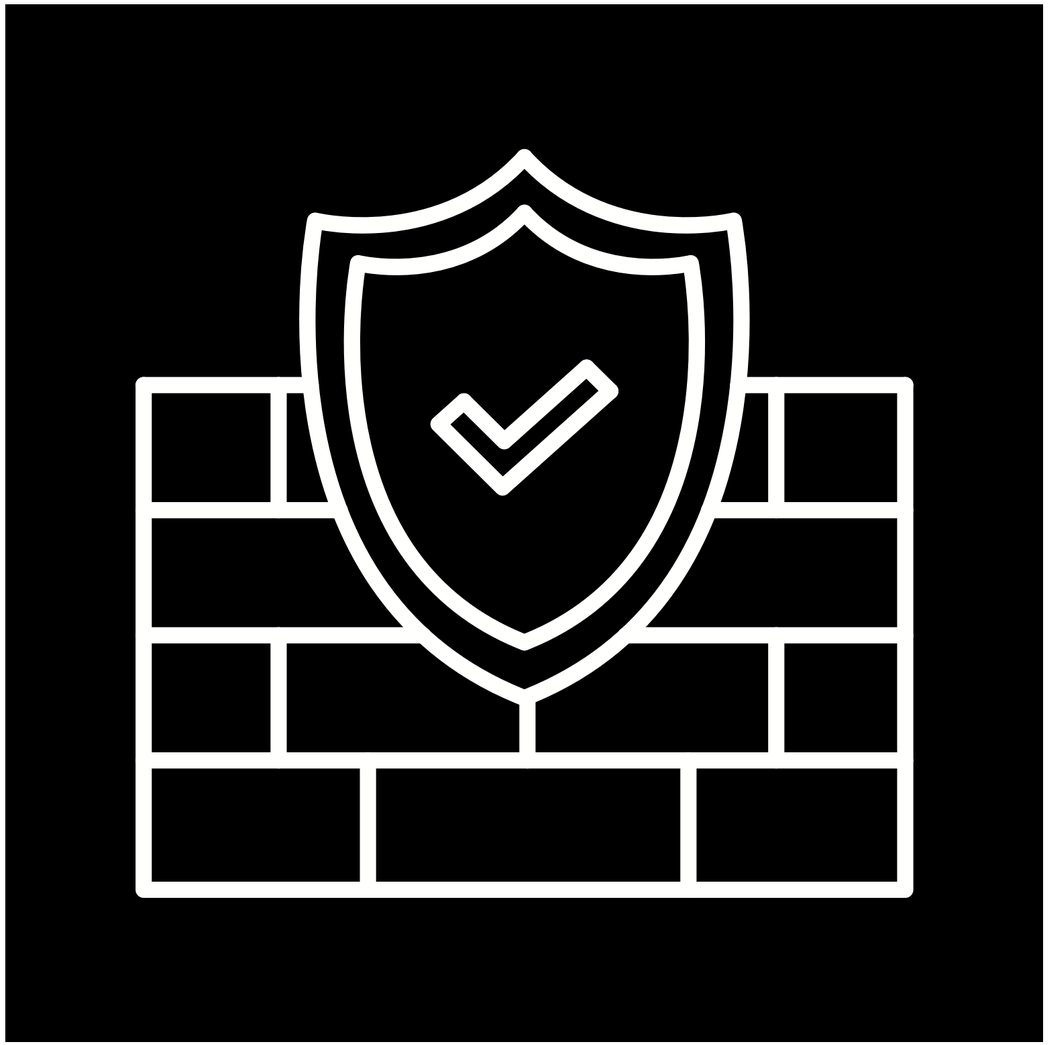
la stringa che viene creata può essere letta dal solo server che è in possesso della chiave segreta che ha generato.
Il token che viene rilasciato allo user è quindi una sequenza alfanumerica che racchiude dei dati ma non permette l'accesso al server, che si preoccupa di verificare solo la veridicità dell'hash

FIREWALL - BLACK LIST

La black list è un metodo utilizzato dai firewall per bloccare l'acceso di gli indirizzi IP specificati, impedendo che potenziale minace possano entrare alla rete. Sono degli elenchi contenenti regole, intervalli o singoli indirizzi IP che desideri bloccare.

FIREWALL - WHITE LIST

La white list, al contrario, viene utilizzata per garantire l'accesso degli indirizzi IP specificati, questo potrebbe venire usato per garantire l'accesso al vostro server E-commerce solo a gli impiegati di Theta.



PERSONALE FORMATO

Per proteggere l'azienda dagli attacchi hacker i dipendenti devono seguire dei protocolli come: corsi sulla sicurezza informatica; imparare a riconoscere le e-mail phishing e social engineering; non condividere i dati sensibili e utilizzare il pc aziendale solo per lavoro e ricordarsi di non lasciarlo incustodito.
Mantenere una formazione costantemente allineata alle nuove minacce.

TIMESLEEP - MAX TENTATIVI

Per aumentare la sicurezza si consiglia l'implementazione del codice "timesleep", nella parte back-end, il quale va ad interagire con un determinato thread in modo da metterlo in pausa per un periodo definito di tempo così da prevenire un tentativo continuo di invio di credenziali. In aggiunta a ciò si consiglia, in oltre, di inserire un numero massimo di tentativi facendo in modo di bloccare il dispositivo una volta superato tale numero, prevenendo così diversi tipi di attacchi come ad esempio il brute force o l'intrusione tramite social engineering.