UNIVERSITÀ DEGLI STUDI DI
BARI ALDO MORO

Corso di Laurea triennale in Informatica

Tesi di laurea in
Cybersecurity

Cyber Security Awareness: Sviluppo di un Serious Game

Relatore

Prof.ssa Vita Santa Barletta

Laureando

Gaetano Angelo Alberto Loizzo

Anno Accademico 2022-2023

Indice

Prefazione

Negli ultimi anni l'utilizzo dei sistemi informatici ha registrato una crescita esponenziale in tutti gli ambiti, sia in quelli aziendali che quelli sociali. Allo stesso modo la diffusione sempre crescente delle tecnologie ha portato ad un aumento esponenziale anche delle minacce informatiche.

La cybersecurity ha come scopo quello di proteggere tutte le risorse digitali da questi attacchi informatici. Tuttavia, la complessità delle minacce cresce insieme alla rapida evoluzione delle tecnologie rendendo così l'obiettivo sempre più difficile.

In questo contesto, l'utilizzo di nuovi strumenti può aiutare la cybersecurity nel raggiungimento del proprio obiettivo educando e formando. Uno tra questi è il "Serious Game", ovvero attività che sfruttano gli elementi ludici per facilitare gli obiettivi di educazione ed istruzione.

Inoltre, un altro strumento importante è il "War Game" (Gioco di Guerra). Nell'hacking è una sfida di sicurezza informatica e uno sport mentale in cui i concorrenti devono sfruttare o difendere una vulnerabilità in un sistema o in un'applicazione, e/o ottenere o impedire l'accesso a un sistema informatico.

Si esamina il ruolo di questi strumenti nella cybersecurity, esplorando tutte le loro funzionalità e come possono essere utilizzati per migliorare le competenze e le conoscenze degli utenti, per testare le strategie e le tattiche di difesa. In aggiunta, si esaminano i vantaggi e si analizza il percorso verso lo sviluppo e l'implementazione di questi strumenti affinché siano efficaci in questo settore.

È interessante comprendere come poter preparare al meglio gli utenti ad affrontare le minacce informatiche sempre più sofisticate e pericolose, e come rendere questi strumenti adattabili all'evoluzione della sicurezza informatica.

In conclusione, si può contare che i videogame siano entrati a tutti gli effetti a far parte della cultura umana ed è nostro dovere sfruttare a pieno queste potenzialità per raggiungere obiettivi benevoli che possano aiutare la vita quotidiana delle persone allontanandole dalle minacce informatiche.

Abstract

La presente tesi sperimentale nel campo dell'informatica si propone di condurre un'analisi completa sulla situazione e sulle lacune della sicurezza informatica in Italia e si impegna a trovare una soluzione efficace allo scopo.

La crescente minaccia degli attacchi informatici, particolarmente per le piccole e microimprese italiane, richiede un'attenzione sempre maggiore alla cybersecurity poiché come spiegato in seguito queste sono quasi la totalità del tessuto economico italiano. In questa tesi di laurea, ci proponiamo di affrontare questa sfida progettando un Serious Game specificamente rivolto ai dipendenti delle piccole e microimprese italiane che sono spesso bersaglio di attacchi informatici.

Il nostro obiettivo principale è analizzare l'efficacia di questo gioco nel fornire una formazione efficace e nel sensibilizzare sulle tematiche della sicurezza informatica. Il gioco è stato sviluppato con un focus sull'apprendimento attraverso l'esperienza interattiva, integrando scenari realistici di difesa informatica con diverse challenge e argomenti da approfondire per il superamento delle stesse.

Utilizzando metodologie qualitative e quantitative, esamineremo l'impatto del gioco sull'acquisizione di conoscenze e sulla consapevolezza dei dipendenti riguardo alla sicurezza informatica.

I risultati di questa ricerca contribuiranno a valutare l'efficacia delle metodologie di apprendimento basate sui Serious Game nella promozione di una cultura della sicurezza informatica all'interno delle imprese o aziende italiane, fornendo spunti per futuri sviluppi e miglioramenti nell'ambito della formazione sulla cybersecurity.

Capitolo 1: La minaccia degli attacchi informatici in Italia

1.1 Introduzione

Nell'era digitale in cui viviamo, l'evoluzione tecnologica ha portato notevoli vantaggi alla società, facilitando la comunicazione, l'accesso alle informazioni e la gestione delle attività quotidiane. Tuttavia, insieme a queste opportunità, è emersa anche una crescente minaccia rappresentata dagli attacchi informatici.

Un attacco informatico è qualsiasi azione intenzionale che ha lo scopo di rubare, esporre, alterare, disabilitare o distruggere dati, applicazioni o altri asset tramite l'accesso non autorizzato a una rete, un sistema informatico o un dispositivo digitale [1].

Pertanto, con il termine attacco informatico si fa riferimento alle manovre pensate da organizzazioni o singoli individui aventi lo scopo di colpire sistemi informatici o infrastrutture, sfruttando ogni espediente per far breccia nei sistemi e mettendo a rischio sia l'integrità che la sicurezza dei sistemi colpiti, alterandoli e/o distruggendoli.

L'Italia si trova in una posizione particolarmente vulnerabile nel contesto degli attacchi informatici, un fatto che può essere attribuito in gran parte alla predominanza delle micro, piccole e medie imprese (PMI) nel tessuto economico del Paese. Queste PMI, che costituiscono la stragrande maggioranza delle aziende italiane, spesso non dispongono delle risorse finanziarie, delle competenze tecniche e delle infrastrutture necessarie per adottare misure di sicurezza informatica adeguate. Inoltre, molte di esse non sono coperte da assicurazioni idonee che possano proteggerle efficacemente contro i danni derivanti da attacchi informatici e violazioni della sicurezza dei dati.

Alcuni degli studi condotti su questo fenomeno hanno evidenziato che gli attacchi informatici in Italia si concentrano principalmente su settori chiave dell'economia, come quello bancario e sopratutto industriale. Ad esempio, uno studio condotto dall'Università di Milano ha analizzato una serie di attacchi informatici contro istituti finanziari italiani nel corso degli ultimi cinque anni, evidenziando le

tecniche e le modalità utilizzate dai cybercriminali per infiltrarsi nei sistemi e sottrarre informazioni sensibili [2]. Se prima per proteggersi venivano utilizzate solo tecnologie avanzate, oggi la difesa viene affidata a un sistema complesso nel quale confluiscono tecnologia, assetto organizzativo, fattore umano e un'adeguata strategia di comunicazione. Il termine resilience riguarda però un altro tipo di atteggiamento, si riferisce alla capacità di non compromettere le operazioni interne, garantendo il ripristino dei dati e dei processi di network e di servizio. L'approccio alla sicurezza informativa, dunque, si è evoluta da una strategia event-drive, ossia guidata dalla contingenza, ad una prevenzione della minaccia, con una grande flessibilità soprattutto in termini di risorse, di processi, strutture coinvolte e architetture di rete [3].

Inoltre, uno studio condotto dall'Istituto Superiore di Studi in Sicurezza Informatica (ISSSI) ha esaminato gli attacchi informatici contro le infrastrutture critiche del paese, come reti di energia elettrica e telecomunicazioni, mettendo in luce le vulnerabilità esistenti e la necessità di migliorare le difese informatiche per proteggere tali sistemi vitali [4].

In generale, l'Italia si trova di fronte a diversi problemi nel campo della sicurezza informatica, con numerose aziende e istituzioni che affrontano minacce sempre più sofisticate da parte di cybercriminali e attaccanti informatici. Tuttavia, così come nelle istituzioni dove è stata implementata la resilience per affrontare con successo le sfide emergenti, anche nel settore delle imprese potrebbe essere adottato un approccio simile per risolvere il problema della sicurezza informatica.

Nell'ambito di questa analisi, si esaminerà l'impatto significativo delle PMI sul tessuto economico italiano e la loro situazione odierna riguardo gli attacchi informatici subiti.

1.2 Analisi dei Dati ISTAT

PROSPETTO 2. IMPRESE CONTROLLATE DA UNA PERSONA FISICA O UNA FAMIGLIA, GESTIONE MANAGERIALE E PASSAGGIO GENERAZIONALE. Anno 2022 e Periodo 2016-2025. Valori assoluti e percentuali.

CLASSE DI ADDETTI	IMPRESE CONTROLLATE DA UNA PERSONA FISICA O UNA FAMIGLIA		Gestione manageriale	IMPRESE INTERESSATE DA PASSAGGIO GENERAZIONALE	
	Numero	% su totale imprese		Tra il 2016 e il 2022	Possibile nel triennio 2023-2025
3-9 addetti	670.888	83,3	0,8	7,7	6,4
10-49 addetti	140.970	74,5	3,2	14,4	14,1
50-249 addetti	13.442	58,8	10,0	17,8	14,7
250 addetti e oltre	1.653	41,6	21,2	18,9	12,5
TOTALE	826.953	80,9	1,4	9,1	7,9

Figura 1: Numero di Imprese in relazione al numero degli addetti

Per comprendere appieno l'importanza delle micro, piccole e medie imprese nell'economia italiana, è fondamentale esaminare i dati forniti dall'Istituto Nazionale di Statistica (ISTAT). Secondo il censimento condotto dall'ISTAT, più del 78% delle imprese italiane sono microimprese, mentre le piccole imprese rappresentano circa il 18%. Le medie e grandi imprese costituiscono solo una percentuale marginale del totale [5].

Questi dati riflettono il ruolo centrale che le micro e piccole imprese svolgono nell'economia italiana, non solo in termini di numero di aziende, ma anche in termini di occupazione, innovazione e contributo al PIL nazionale. Le PMI sono spesso considerate il motore trainante dell'economia italiana, essendo responsabili della maggior parte dei posti di lavoro nel Paese e giocando un ruolo fondamentale nella creazione di valore aggiunto e nell'export. L'analisi dei dati ISTAT conferma quindi che le piccole e microimprese costituiscono un pilastro fondamentale dell'economia italiana, e la loro sicurezza informatica riveste un'importanza cruciale per la stabilità e la resilienza del sistema economico nazionale.

Si analizza in seguito la situazione odierna sugli attacchi informatici subiti da parte delle PMI italiane e il continuo incremento del numero di questi attacchi nel passare degli anni.

1.3 Report Threatland H2 2023

Il Report Threatland H2 2023 offre un'analisi dettagliata degli attacchi cyber, concentrandosi principalmente su ransomware, malware e phishing. Questa analisi fornisce una panoramica approfondita delle minacce emergenti e delle tendenze in evoluzione nel campo della sicurezza informatica. In seguito in Figura 2 vengono mostrati gli 8 paesi più colpiti al mondo nel secondo semestre (H2) dell'anno 2023. Si può notare che l'Italia è in quinta posizione, in precedenza posizionata undicesima, nel periodo considerato ha sperimentato un totale di 88 attacchi ransomware. L'analisi dei dati sugli attacchi ransomware in Italia offre uno sguardo dettagliato sulla situazione, comprendendo, le dimensioni delle aziende coinvolte e il fatturato delle vittime.

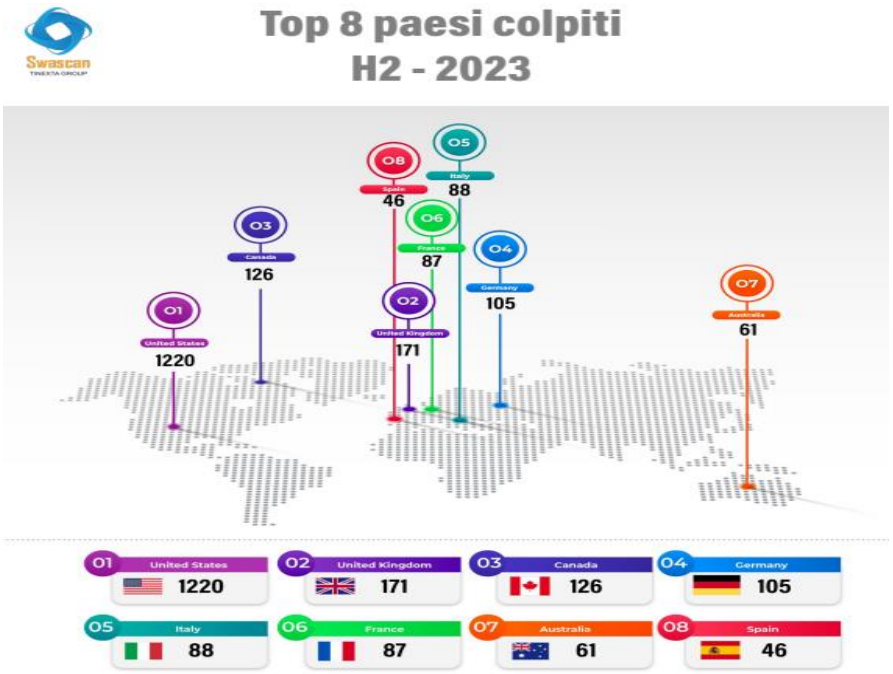


Figura 2: Top 8 paesi colpiti

Secondo il report, nel 2023 in Italia, il 77% degli attacchi ransomware coinvolgeva piccole e microimprese con un fatturato inferiore ai 250 milioni di dollari (Figura 3). Questo trend è in costante crescita anche nel secondo semestre dell'anno, con un aumento del 44% che posiziona il nostro Paese tra i più colpiti al mondo, con un totale di 88 attacchi registrati. La situazione rappresenta una sfida

significativa per il settore privato e le autorità pubbliche italiane, che devono adottare misure urgenti per migliorare la sicurezza informatica e proteggere le imprese e i cittadini dagli attacchi cyber sempre più sofisticati e dannosi [6].

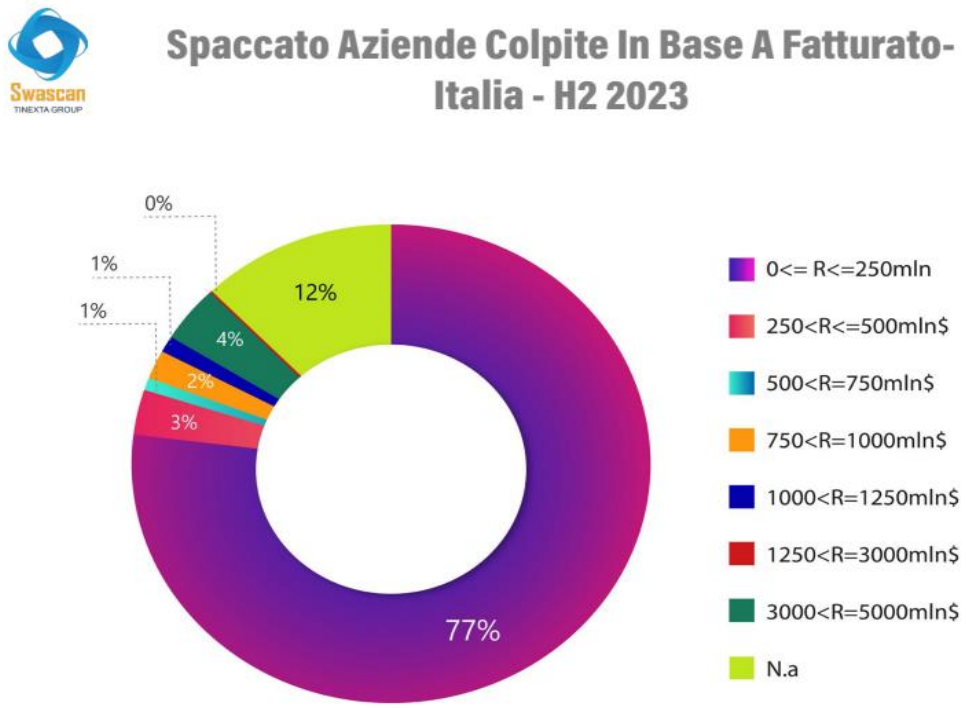


Figura 3: Aziende attaccate in base al fatturato

Dall'analisi dei dati provenienti dai diversi report analizzati precedentemente, emerge chiaramente che la situazione della sicurezza informatica italiana è precaria. I numeri indicano un aumento costante degli attacchi informatici contro aziende, istituzioni e privati cittadini nel corso degli ultimi anni, con un incremento significativo sia in termini di frequenza che di gravità degli attacchi. Questo trend preoccupante mette in evidenza la vulnerabilità del panorama digitale italiano e la necessità urgente di adottare misure più efficaci per proteggere i sistemi e i dati contro le minacce informatiche sempre più sofisticate e diffuse. La comprensione dettagliata dei dati raccolti dai report permette di tracciare un quadro chiaro della situazione attuale e di identificare le aree critiche che richiedono interventi immediati per migliorare la sicurezza informatica nel paese.

Il focus andrà quindi principalmente alle PMI, in quanto sono particolarmente vulnerabili agli attacchi informatici e svolgono un ruolo cruciale nell'economia italiana. Sono esposte a rischi significativi che possono compromettere la loro sicurezza dei dati, la continuità operativa e la reputazione aziendale. Concentrando gli sforzi sulla protezione e il supporto delle PMI nel migliorare le loro difese informatiche, si potrà contribuire in modo significativo a mitigare il rischio di attacchi informatici nel contesto italiano e promuovere una maggiore resilienza nel settore delle piccole e medie imprese.

Capitolo 2: Strumenti utilizzati

2.1 Microsoft Visual Studio Code 2019

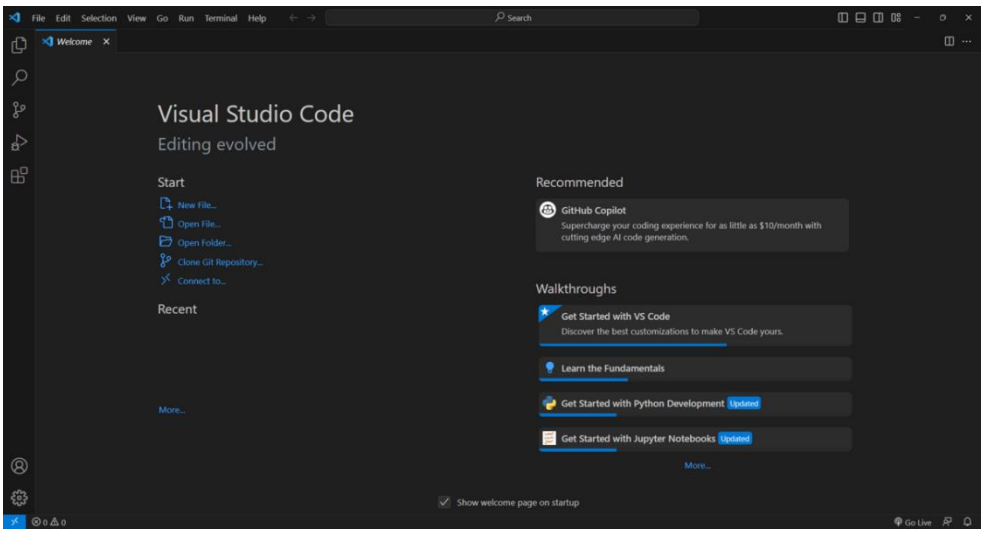


Figura 4: Schermata principale VSC

Microsoft Visual Studio Code [7] 2019 è un ambiente di sviluppo integrato (IDE) leggero, gratuito e altamente personalizzabile, sviluppato da Microsoft. Fornisce agli sviluppatori uno strumento potente per la scrittura, il debug e il testing del codice in una vasta gamma di linguaggi di programmazione. Grazie alla sua interfaccia intuitiva, alle numerose estensioni e al supporto per una varietà di framework e piattaforme, Visual Studio Code è diventato uno degli IDE più popolari tra gli sviluppatori di tutto il mondo. Per quanto riguarda l'utilizzo di Visual Studio Code per il Serious Game in Unity è stato scelto come ambiente di sviluppo per la realizzazione del nostro serious game in Unity. Nonostante il progetto sia stato gestito da una singola persona, l'efficienza e le funzionalità offerte da Visual Studio Code hanno giocato un ruolo fondamentale nel processo di sviluppo poiché ha diversi vantaggi come:

1. Interfaccia User-Friendly (Figura 4) e Personalizzabile

La struttura intuitiva e personalizzabile di Visual Studio Code ha reso facile per il singolo sviluppatore organizzare l'ambiente di lavoro in base alle proprie preferenze e esigenze specifiche.

2. Supporto per Unity

Le estensioni specifiche per Unity disponibili in Visual Studio Code hanno semplificato il processo di sviluppo, offrendo funzionalità avanzate per la scrittura del codice, il debugging e la gestione dei progetti.

3. Debugger Integrato e Strumenti di Analisi

Il debugger integrato di Visual Studio Code ha permesso al singolo sviluppatore di individuare e risolvere rapidamente eventuali problemi nel codice, migliorando l'efficienza e la qualità del prodotto finale.

4. Gestione dei Progetti Efficace

Anche se il progetto è stato gestito da una singola persona, la gestione dei file e dei progetti all'interno di Visual Studio Code è risultata efficiente e intuitiva, consentendo una facile navigazione e organizzazione del codice.

5. Community Attiva e Supporto Continuo

Anche lavorando da solo, il supporto della community di Visual Studio Code è stato prezioso. La vasta gamma di risorse disponibili online e la possibilità di accedere a feedback e soluzioni a eventuali problemi hanno contribuito al successo del progetto.

In sintesi, l'utilizzo di Microsoft Visual Studio Code 2019 per lo sviluppo del serious game in Unity da parte di un singolo sviluppatore ha dimostrato l'efficacia e la versatilità di questo IDE, consentendo la realizzazione di un prodotto di alta qualità in modo efficiente e collaborativo.

2.2 GitHub e GitHub Desktop

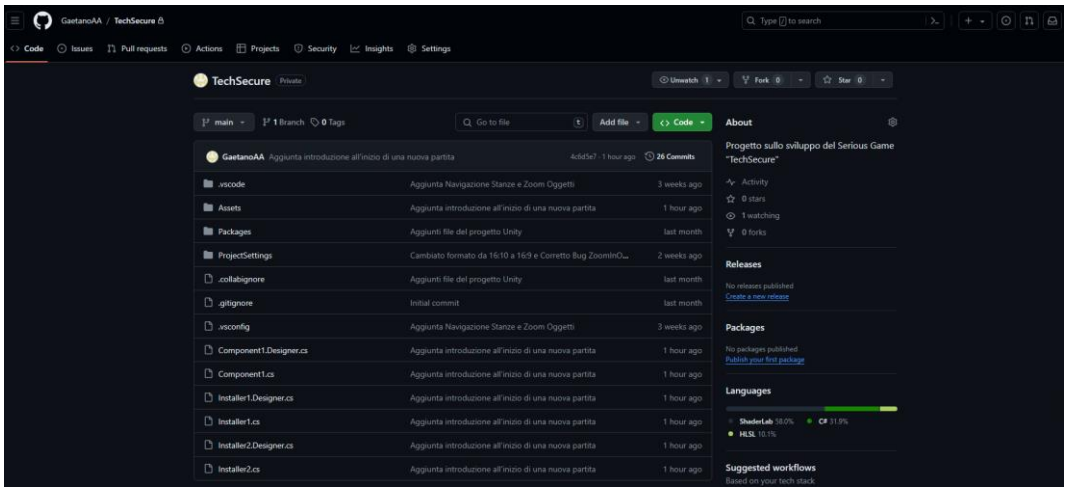


Figura 5: Repository TechSecure GitHub

GitHub Desktop è un'applicazione gratuita e user-friendly sviluppata dal team di GitHub, progettata per semplificare il controllo delle versioni e la gestione dei repository su GitHub. Grazie alla sua interfaccia intuitiva e alle potenti funzionalità, GitHub Desktop è diventato uno strumento popolare tra gli

sviluppatori per collaborare, controllare e condividere il proprio codice in modo efficiente e sicuro. Il progetto consiste nello sviluppo di un serious game in Unity, un'esperienza interattiva progettata per insegnare concetti chiave di sicurezza informatica in modo coinvolgente e pratico. Questo progetto è stato gestito da una singola persona, il che rende cruciale l'utilizzo di strumenti efficienti e intuitivi per la gestione del codice. GitHub Desktop è stato scelto come strumento principale per la gestione delle versioni e la collaborazione all'interno del progetto. Anche se il lavoro è stato svolto da una sola persona, l'utilizzo di GitHub Desktop ha portato numerosi vantaggi. GitHub Desktop ha semplificato la gestione delle versioni del progetto, consentendo di tenere traccia delle modifiche apportate al codice nel corso del tempo. Grazie alla funzionalità di commit, è stato possibile registrare in modo chiaro e organizzato le modifiche effettuate, garantendo un flusso di lavoro ordinato e tracciabile.

Nonostante il progetto fosse gestito da una sola persona, GitHub Desktop ha permesso una facile condivisione del codice e la collaborazione con altri sviluppatori, se necessario. La possibilità di clonare il repository su diversi dispositivi e la facilità di push e pull del codice hanno reso semplice la condivisione e l'aggiornamento del lavoro in corso. GitHub Desktop ha offerto un ambiente controllato e sicuro per la gestione del codice, garantendo che tutte le modifiche apportate fossero tracciate e reversibili. La funzionalità di branching ha permesso di esplorare nuove funzionalità senza compromettere la stabilità del progetto principale, mentre la possibilità di visualizzare le differenze tra le varie versioni ha facilitato il processo decisionale.

Una delle caratteristiche più utili di GitHub Desktop è stata la sincronizzazione automatica con il repository GitHub associato al progetto. Questo ha garantito che tutte le modifiche apportate al codice fossero sempre aggiornate e accessibili da qualsiasi dispositivo, consentendo un flusso di lavoro fluido e senza interruzioni. Grazie alla visualizzazione chiara delle modifiche apportate al codice, GitHub Desktop ha permesso di tenere traccia delle revisioni e delle migliorie nel corso dello sviluppo del serious game. Questa funzionalità ha facilitato il processo di revisione del codice e ha contribuito a mantenere la coerenza e la qualità del prodotto finale. In conclusione, l'utilizzo di GitHub Desktop nel processo di sviluppo del serious game in Unity ha semplificato la gestione delle versioni e

favorito la collaborazione, contribuendo al successo del progetto in modo efficiente e sicuro. Anche se il lavoro è stato svolto da una singola persona, GitHub Desktop ha dimostrato di essere uno strumento prezioso per la gestione del codice, consentendo un flusso di lavoro ordinato, tracciabile e collaborativo.

2.3 C#

Figura 6: Logo ufficiale C#

C# è un linguaggio di programmazione moderno e potente, sviluppato da Microsoft, ampiamente utilizzato per lo sviluppo di applicazioni desktop, web e giochi. Grazie alla sua sintassi intuitiva, alla robustezza e alla vasta libreria di classi, C# è diventato il linguaggio preferito per lo sviluppo di giochi su Unity, uno dei motori di gioco più popolari al mondo. Il nostro progetto consiste nello sviluppo di un serious game in Unity, un'esperienza interattiva progettata per insegnare concetti chiave di sicurezza informatica in modo coinvolgente e pratico. Per implementare la logica di gioco, la gestione degli eventi e la logica di business, abbiamo scelto di utilizzare il linguaggio di programmazione C#. Esso è stato scelto come linguaggio principale per lo sviluppo del serious game in Unity per diversi motivi. In primo luogo, la stretta integrazione di C# con l'ecosistema di Unity ha reso il linguaggio una scelta naturale per lo sviluppo di giochi su questa piattaforma. La vasta comunità di sviluppatori e le numerose risorse disponibili hanno reso più semplice l'apprendimento e l'utilizzo di C# per lo sviluppo di giochi, garantendo al contempo un supporto robusto e continuo. In secondo luogo, la sintassi intuitiva e la facilità di apprendimento di C# lo rendono adatto sia per i principianti che per gli sviluppatori esperti. La struttura orientata agli oggetti di C# consente una progettazione modulare e organizzata del codice, facilitando la manutenzione e l'aggiornamento del progetto nel tempo. Inoltre, C# offre un'ampia gamma di funzionalità e librerie integrate che semplificano lo sviluppo

di giochi complessi. Dalla gestione degli input utente alla grafica e alla fisica, C# fornisce tutto il necessario per creare esperienze di gioco coinvolgenti e immersive.

Grazie alla sua flessibilità e potenza, C# ha consentito di implementare facilmente le meccaniche di gioco, la logica di gameplay e la gestione degli eventi all'interno del serious game. L'utilizzo di C# ha reso possibile la creazione di un'esperienza interattiva e coinvolgente, offrendo al contempo un controllo preciso e granulare sul comportamento del gioco. In conclusione, l'utilizzo di C# nel processo di sviluppo del serious game in Unity ha permesso di implementare con successo le funzionalità di gioco e garantire un'esperienza utente coinvolgente e di alta qualità. Grazie alla sua sintassi intuitiva, alla vasta libreria di classi e alla stretta integrazione con Unity, C# si è dimostrato essere il linguaggio ideale per lo sviluppo di giochi, consentendo di realizzare il nostro progetto in modo efficiente e professionale.

Inizializzazione e debug: JavaScript JavaScript è un linguaggio di scripting: questo significa che la sintassi puó essere integrata dentro la pagina HTML, senza bisogno di produrre alcun file compilato. Con i linguaggi di programmazione come il C e il C++ si scrive, invece, la sintassi e poi la si passa ad un compilatore, che produce un file, appunto, “compilato”, in cui la sintassi è scomparsa. Tutti i programmi di Windows, ad esempio, sono dei file compilati, in cui non c’è più traccia della sintassi originaria. JavaScript, invece, non è compilato: è possibile, quindi, visualizzare in qualsiasi momento il codice di una pagina HTML e leggere le righe di sintassi. Dire che è un linguaggio di scripting sottintende, dunque, il fatto che sia un linguaggio interpretato; come abbiamo visto, non esiste nessun compilatore, ma è direttamente il browser, tramite un apposito motore di scripting (cioè di visualizzazione), che legge le parti di codice JavaScript.

2.4 Unity

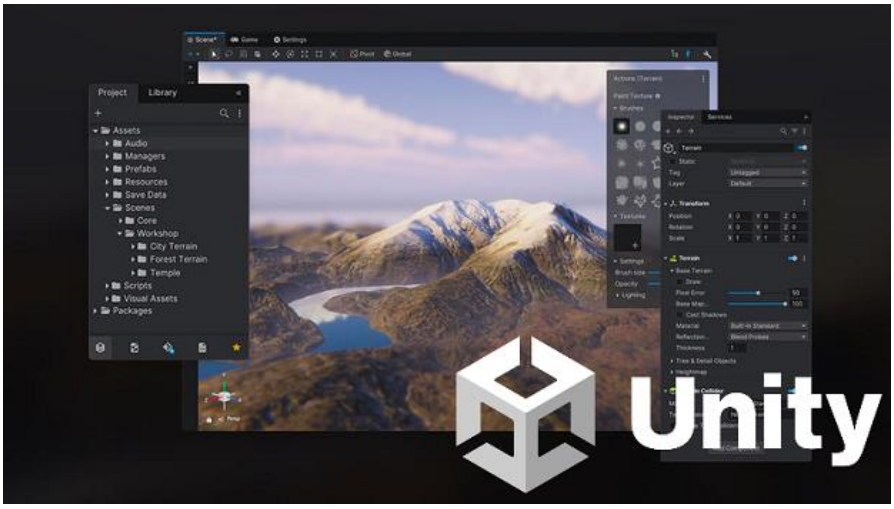


Figura 7: Interfaccia grafica Unity

Unity è un motore di gioco multipiattaforma sviluppato da Unity Technologies, ampiamente utilizzato per lo sviluppo di videogiochi, simulazioni, visualizzazioni architettoniche e molto altro ancora[8]. Grazie alla sua versatilità e alla sua vasta gamma di funzionalità, Unity si è guadagnato una reputazione come uno dei motori di gioco più popolari e accessibili sul mercato. Il nostro progetto consiste nello sviluppo di un serious game utilizzando Unity, un'esperienza interattiva progettata per insegnare concetti chiave di sicurezza informatica in modo coinvolgente e pratico. Unity è stata la scelta ideale per questo progetto grazie alla sua facilità di utilizzo, alla sua flessibilità e alle sue potenti funzionalità di sviluppo di giochi 2D e 3D. Unity è stato scelto come motore di gioco principale per lo sviluppo del serious game per diversi motivi. In primo luogo, l'interfaccia utente intuitiva e la facilità di apprendimento di Unity lo rendono adatto sia per i principianti che per gli sviluppatori esperti. Con il suo sistema di trascinamento e rilascio (drag-and-drop) per la creazione di scene e la sua logica di programmazione visuale tramite l'uso di nodi (Node-based scripting), Unity consente di creare rapidamente e facilmente prototipi di gioco funzionali. Inoltre, Unity offre una vasta gamma di risorse e asset pronti all'uso tramite il suo Asset Store integrato, che include modelli 3D, suoni, effetti speciali e molto altro ancora. Questo permette agli sviluppatori di ridurre i tempi di sviluppo e concentrarsi maggiormente sulla progettazione e l'implementazione delle meccaniche di gioco. Grazie alla sua potente grafica 2D e 3D, Unity consente di creare esperienze di gioco coinvolgenti e immersive. Dalla gestione della fisica

alla grafica avanzata e agli effetti speciali, Unity offre tutto il necessario per creare giochi di alta qualità per una vasta gamma di piattaforme, compresi PC, console, dispositivi mobili e web. In conclusione, l'utilizzo di Unity nel processo di sviluppo del serious game ha permesso di creare un'esperienza interattiva e coinvolgente per gli utenti, fornendo al contempo un ambiente di sviluppo flessibile e potente per gli sviluppatori. Grazie alla sua facilità di utilizzo, alla sua vasta gamma di funzionalità e alla sua compatibilità multi-piattaforma, Unity si è dimostrato essere la scelta ideale per la realizzazione di questo progetto, consentendo di creare un serious game di alta qualità in modo efficiente e professionale.

2.5 Canva

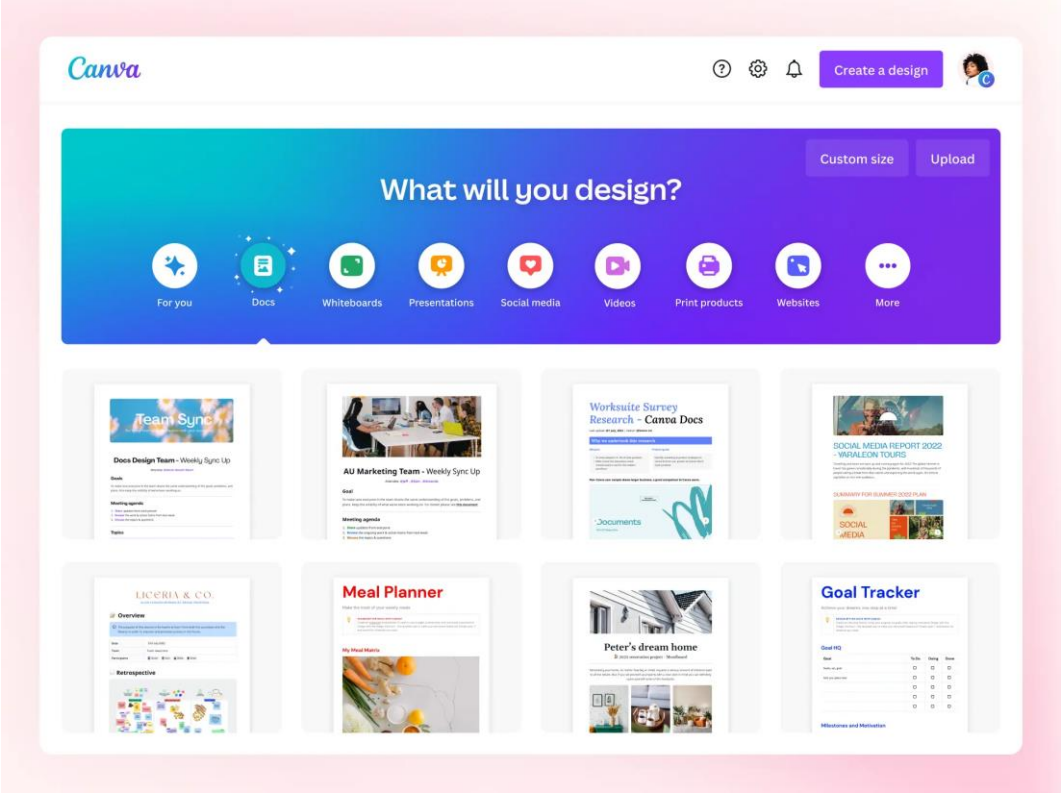


Figura 8: Schermata principale Canva[9]

Canva è un'applicazione basata sul web che consente agli utenti di creare facilmente grafica, design, presentazioni e molto altro, senza la necessità di competenze avanzate in design grafico. La piattaforma offre una vasta gamma di modelli predefiniti, elementi grafici, font e strumenti di editing, consentendo agli utenti di personalizzare facilmente i loro progetti secondo le proprie esigenze. Questa accessibilità e flessibilità hanno reso Canva un'opzione popolare per professionisti, educatori e creativi di ogni tipo. Il serious game TechSecure è stato

sviluppato con l'obiettivo di educare gli utenti sulla sicurezza informatica attraverso un'esperienza di gioco coinvolgente e interattiva. Un elemento cruciale per il successo di un gioco del genere è la qualità e la varietà degli sprite, ovvero gli elementi grafici che rappresentano personaggi, oggetti e ambienti all'interno del gioco. Canva è stato scelto come principale strumento di progettazione per la creazione degli sprite del gioco TechSecure per diverse ragioni. In primo luogo, la vasta libreria di elementi grafici predefiniti disponibili su Canva ha fornito una ricca varietà di opzioni per la creazione di personaggi, sfondi e oggetti di gioco. Gli sviluppatori hanno potuto utilizzare modelli predefiniti come punto di partenza per i loro design, risparmiando tempo e risorse nel processo di creazione. In secondo luogo, la semplicità d'uso di Canva ha permesso agli sviluppatori di concentrarsi sulla creatività e sulla progettazione, anziché sulle complessità tecniche del design grafico. L'interfaccia intuitiva di Canva ha reso facile manipolare elementi grafici, modificare colori, dimensioni e altri attributi per adattarsi alle esigenze specifiche del gioco TechSecure.

L'utilizzo di Canva per la creazione degli sprite nel serious game TechSecure ha dimostrato di essere una scelta efficace e conveniente. La piattaforma ha offerto agli sviluppatori la flessibilità, la varietà e la facilità d'uso necessarie per creare grafica di alta qualità che contribuisce al coinvolgimento e alla fruizione dell'esperienza di gioco. Canva si conferma così uno strumento prezioso per gli educatori e gli sviluppatori che desiderano creare contenuti visivi coinvolgenti e accattivanti.

2.5.1 Canva PlayGround

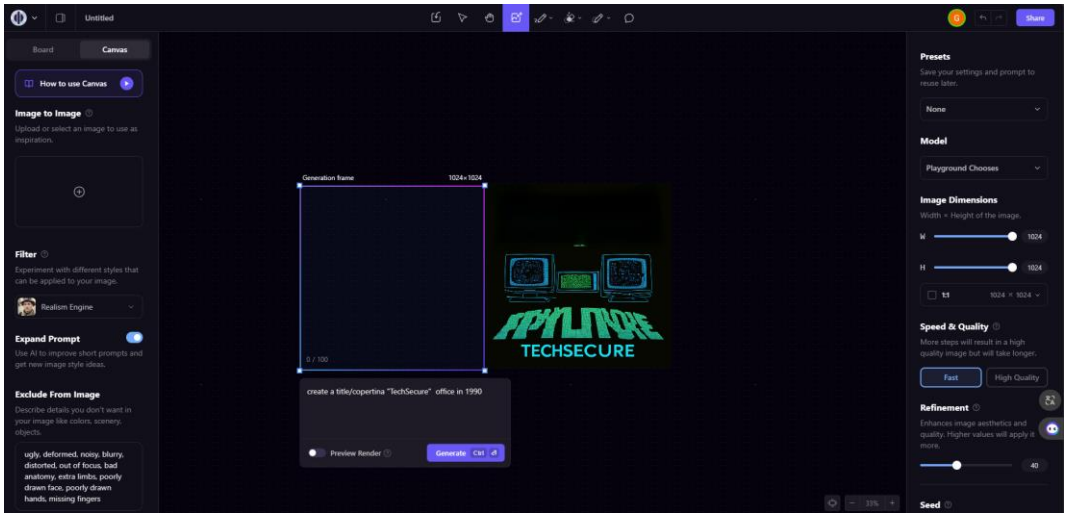


Figura 9: Esempio creazione copertina del Serious Game

Playground è in realtà uno strumento di modifica delle immagini gratuito. Ma le sue maggiori caratteristiche non sono in sé, ma il fatto che includa la tecnologia dell'Intelligenza Artificiale per poter creare, modificare... un'immagine o un'illustrazione.

Avendo l'intelligenza artificiale, una delle caratteristiche più importanti di questo programma è la possibilità di creare immagini da zero semplicemente descrivendole con del testo. Questo ci apre un'altra possibilità per non dover dipendere solo dalla creatività, o da banche di immagini o foto già create, ma puoi fare cose "dal nulla".

A causa di quell'intelligenza artificiale, Playground è in grado di apprendere quali sono i gusti e le preferenze dell'utente. In questo modo, con il passare del tempo, le creazioni migliorano poiché si adattano a ciò che desidera l'utente. Potremmo dire che è come un bambino piccolo che sta imparando e, alla fine, riesce ad essere un vero discepolo che sa esattamente cosa fare quando gli chiedi qualcosa [10].

Con sprite, in informatica, si indica un'immagine in grafica raster, generalmente bidimensionale (2D), che fa parte di una scena più grande (lo "sfondo") e che può essere spostata in maniera indipendente rispetto ad essa [11].

Per la creazione degli sprite facenti parte del Serious Game TechSecure si è fatto uso principalmente dell'intelligenza artificiale Canva PlayGround. Questa, come detto in precedenza, dà la possibilità di generare immagini dal testo in input e di utilizzare determinati filtri. Il filtro utilizzato maggiormente è stato "Realism

Engine" poiché questo permette di rispecchiare al meglio l'ambiente di lavoro in un ufficio aziendale, così che il giocatore è totalmente immerso durante lo svolgimento del gioco.

Capitolo 3: Serious Game una soluzione vincente

3.1 Gioco

Partendo dalla definizione della Treccani, che indica il gioco come "qualsiasi attività liberamente scelta a cui si dedicano bambini o adulti, singolarmente o in gruppo, senza altri fini immediati che la ricreazione e lo svago, sviluppando e allenando capacità fisiche, manuali e intellettive", emerge la varietà delle sue forme: dai giochi infantili ai giochi di società, da quelli all'aperto ai giochi enigmistici, matematici o di prestigio. Johan Huizinga, storico e linguista olandese, nel suo libro "Homo Ludens" del 1937 [12], affrontò sistematicamente il concetto di gioco, considerandolo un pilastro fondamentale per lo sviluppo delle civiltà e l'organizzazione sociale. Huizinga sosteneva che il gioco fosse cruciale per interpretare la realtà stessa, influenzando direttamente il tessuto sociale. In modo simile, Roger Caillois, sociologo, antropologo e critico letterario francese, nel suo libro "I giochi e gli uomini: la maschera e la vertigine" del 1958, esaminò le caratteristiche dei giochi e classificò le loro varie tipologie in base all'atteggiamento del giocatore. Caillois sottolineò il ruolo sociale del gioco, dimostrando come esso influenzi la cultura e le istituzioni della società[13]. Egli descrisse il gioco come un'attività libera, separata, incerta, improduttiva, regolata e fittizia, sottolineando la sua funzione di stimolare l'immaginazione e la riflessione. La sua classificazione del gioco in quattro macrocategorie - Agon, Alea, Mimicry e Ilinx - evidenzia la diversità delle esperienze ludiche umane. Queste categorie delineano anche le differenze tra gioco e simulazione, con i "Serious Games" che si collocano all'intersezione di queste categorie. I "Serious Games" sono simulazioni che incorporano le caratteristiche del gioco, stimolando l'apprendimento e lo sviluppo di competenze attraverso regole specifiche e l'immaginazione.

3.2 Gamification e Serious Game

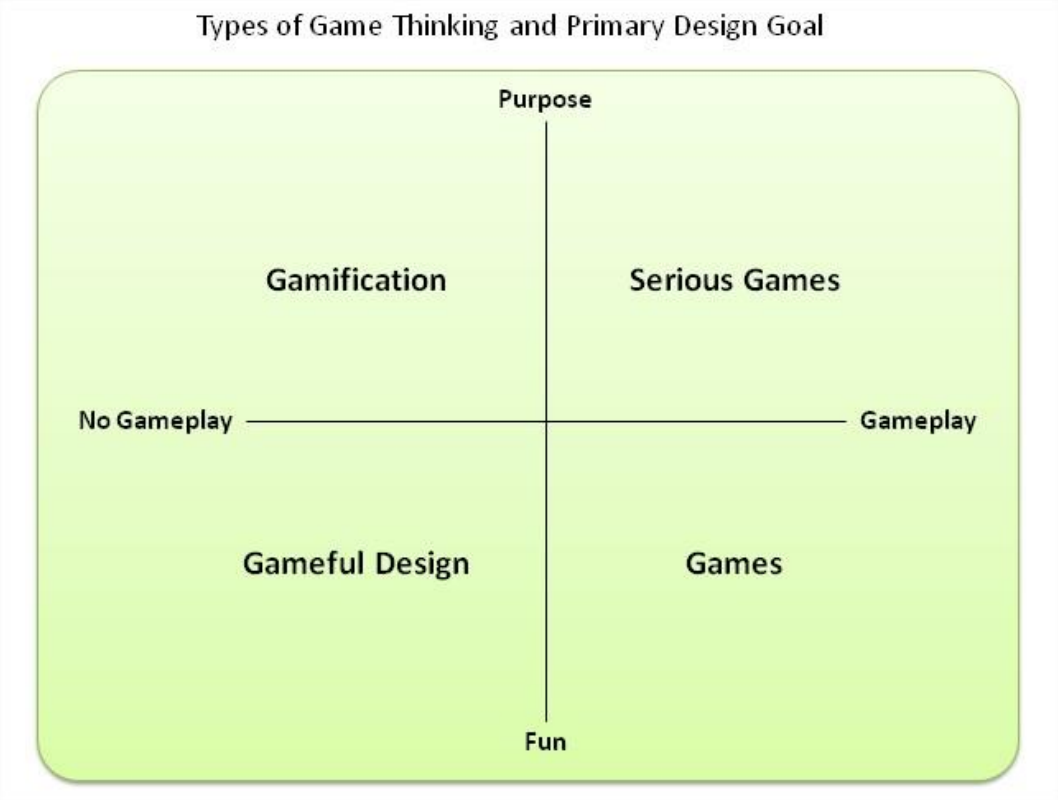


Figura 10: Confronto Gamification e Serious Games

La gamification rappresenta una strategia innovativa che, sebbene condivida alcune somiglianze con i serious games, ne differisce per l'obiettivo principale e l'ambito di applicazione. Secondo Deterding, la gamification si definisce come l'integrazione di elementi tipici dei videogiochi in contesti non ludici al fine di migliorare l'esperienza e l'coinvolgimento dell'utente[14]. Questo concetto ha le sue radici nelle teorie di van Benthem, che parlava di "conversione di attività non ludiche in gioco", suggerendo l'idea di applicare la logica dei giochi a situazioni al di fuori dell'ambito ludico [15]. Gli elementi chiave della gamification comprendono le regole di gioco, le tecniche e le interfacce che possono essere adattate a contesti non ludici come la cyber security, le prestazioni professionali e l'innovazione. Questi elementi possono includere livelli di progressione, obiettivi da raggiungere e regole che incentivano la competizione tra giocatori, spingendoli a migliorare le loro performance, ad esempio, nel contesto lavorativo o di vendita di prodotti. L'obiettivo principale della gamification è quello di aumentare il coinvolgimento e migliorare l'esperienza dell'utente in settori come i servizi o i prodotti di business, andando oltre il loro valore nominale. Questo si distingue nettamente dai serious games, la cui principale finalità è educativa o formativa.

Mentre i giochi e la gamification incorporano entrambi elementi di gioco, la differenza sta nel fatto che i serious games sono progettati specificamente per l'apprendimento, mentre la gamification può essere utilizzata per migliorare l'esperienza utente in vari contesti, senza necessariamente insegnare qualcosa di nuovo. Secondo la tassonomia di Bedwell et al., giochi e gamification condividono elementi ludici, ma mentre i giochi incorporano tutti questi elementi, la gamification applica solo uno o più di essi [16]. Tuttavia, gli studi sui serious games sono stati finora non sistematici, e la definizione di cosa costituisca esattamente un serious game varia tra gli studiosi. Bedwell et al. hanno identificato 19 caratteristiche del gioco rilevanti per l'efficacia dei serious games nell'apprendimento, ma queste caratteristiche possono manifestarsi in modi diversi nei vari giochi. Questi elementi ludici sono solo parzialmente adottati nella gamification, che li applica solo in parte a contesti non ludici. L'obiettivo della gamification nel migliorare l'apprendimento è indiretto, influenzando fattori come la motivazione e il coinvolgimento dello studente, che a loro volta possono incidere positivamente sui risultati di apprendimento. In questo senso, la gamification non sostituisce direttamente le forme tradizionali di insegnamento o di formazione, ma può servire come strumento di supporto per migliorare l'esperienza e il coinvolgimento degli studenti (Landers, 2015) [17]. Sebbene la gamification possa non insegnare direttamente, può influenzare positivamente l'atteggiamento e il comportamento degli individui nei confronti dell'apprendimento, il che può a sua volta migliorare i risultati di apprendimento. Perché la gamification sia efficace nell'esperienza di apprendimento, è essenziale che il contesto educativo di base sia di per sé efficace. Questo concetto di "moderazione" tra costrutti è fondamentale, poiché l'introduzione di elementi ludici deve essere integrata in un contesto educativo esistente per avere un impatto significativo sui risultati di apprendimento. L'applicazione della gamification nel marketing si concentra principalmente sull'obiettivo di coinvolgere e fidelizzare i clienti, utilizzando elementi di gioco per migliorare la comunicazione del prodotto/servizio e consolidare l'interesse degli utenti.

I serious game rappresentano un'interfaccia innovativa per l'apprendimento e la sensibilizzazione su tematiche specifiche attraverso l'esperienza ludica. Il termine "serious game" è stato coniato per la prima volta nel 1970 da Clark C. Abt, che lo definì come "un gioco con un proposito diverso dall'intrattenimento puro" [18].

Questa definizione ha posto le basi concettuali per una vasta gamma di applicazioni ludiche con finalità educative, formative o di sensibilizzazione. Nel corso degli anni, il concetto di serious game si è evoluto, integrando concetti di gamification e apprendimento esperienziale. Come ci fa capire Michael Zyda, informatico americano, progettista di videogiochi ed ex professore, da tutti i suoi studi effettuati i serious game sono giochi digitali che forniscono intrattenimento e, allo stesso tempo, promuovono la trasmissione di conoscenze e lo sviluppo di competenze specifiche. Questo approccio innovativo ha attirato l'interesse di numerosi studiosi che hanno esplorato il potenziale educativo e formativo dei serious game in vari contesti, dalla formazione aziendale alla salute pubblica. Inoltre, la crescente disponibilità di tecnologie digitali ha ampliato le possibilità di progettazione e implementazione dei serious game, consentendo la creazione di esperienze coinvolgenti e personalizzate. In questo contesto dinamico, i serious game continuano a evolversi come strumenti efficaci per l'apprendimento e la sensibilizzazione su tematiche rilevanti, offrendo nuove prospettive per l'innovazione nell'ambito dell'educazione e della formazione. In conclusione, sia la gamification che i serious games sono strategie valide per migliorare l'esperienza utente e influenzare comportamenti e risultati. Tuttavia, presentano differenze sostanziali nel loro approccio e obiettivo principale. La gamification si concentra sull'integrazione di elementi ludici in contesti non ludici al fine di migliorare l'esperienza e l'coinvolgimento dell'utente, spesso con l'obiettivo di fidelizzare i clienti o migliorare le performance lavorative. D'altra parte, i serious games sono progettati specificamente per scopi educativi o formativi, utilizzando il gioco come strumento per insegnare nuove competenze o concetti.

Figura 11: Serious Gaming

3.3 Vantaggi, svantaggi ed efficacia dei Serious Game

I serious games sono sempre stati al centro di dibattiti e discussioni, soprattutto quando si tratta di valutare i vantaggi e gli svantaggi che apportano all'esperienza di apprendimento e ad altri ambiti. Questo tema è strettamente intrecciato con le percezioni sull'efficacia dell'e-learning e sull'impatto delle tecnologie digitali sull'apprendimento. Mentre alcuni ritengono che i serious games possano rafforzare una vasta gamma di abilità, sia "soft" che professionali, altri sollevano preoccupazioni riguardo agli effetti negativi che l'uso eccessivo di giochi digitali potrebbero avere sulla salute fisica e mentale degli individui.

3.3.1 Vantaggi

Secondo varie fonti, i giochi "seri" hanno il potenziale di favorire lo sviluppo di diverse abilità. Ad esempio, possono supportare lo sviluppo di competenze spaziali e temporali, di attenzione visivo-selettiva, psicomotorie e strategiche, consentendo agli individui di adattare le proprie strategie ai cambiamenti repentini dei contesti.

Nei settori dell'architettura e del design, i giochi al computer possono essere utilizzati per migliorare le abilità spaziali necessarie alla composizione del design e alla creazione delle forme. Nel campo medico, sono state riscontrate miglioramenti nelle performance grazie all'utilizzo di "giochi" simulativi, fornendo agli studenti di medicina un'esperienza pratica.

Inoltre, i giochi seri possono contribuire allo sviluppo di soft skills, come l'autodisciplina, l'autogestione, la memoria a breve e lungo termine, la capacità di problem-solving e di comunicazione sociale. Possono anche promuovere rapidità e qualità nel processo decisionale personale e di gruppo, oltre a favorire la collaborazione e la negoziazione all'interno di un team. A seconda della loro natura e del mezzo utilizzato, i serious games possono migliorare le capacità analitiche di ricerca, analisi e previsione dei dati, incoraggiando il giocatore a riflettere sui propri errori. Inoltre, possono stimolare lo spirito competitivo attraverso schemi di gioco compensativi e livelli di difficoltà progressivi, il che può essere vantaggioso anche in ambito lavorativo, aumentando la motivazione e l'ambizione al miglioramento delle prestazioni. In conclusione, numerosi autori riconoscono i benefici principali dei serious games in quattro ambiti chiave: capacità motorie/spaziali, educazionali/informative, sociali e psicologiche.

3.3.2 Svantaggi

Quando si analizzano gli svantaggi dei giochi seri, emergono una serie di problematiche intricate, spesso legate agli impatti negativi legati all'eccessiva fruizione di giochi digitali su piattaforme informatiche o altri dispositivi tecnologici. Questi inconvenienti possono manifestarsi in varie forme. Innanzitutto, sorgono problemi fisici derivanti dall'overexposure ai display digitali, tra cui mal di testa, stanchezza visiva e instabilità emotiva. Queste incombenze possono derivare da lunghe sessioni di gioco o dall'utilizzo prolungato di dispositivi digitali. In secondo luogo, si presentano implicazioni psicosociali da considerare. L'isolamento sociale, la depressione e un atteggiamento meno positivo nei confronti della società in generale sono tutti effetti negativi che possono sorgere da un'eccessiva immersione nei giochi digitali. Inoltre, si corre il rischio di sviluppare una dipendenza dai giochi, con il gioco che diventa un surrogato delle relazioni sociali reali. Infine, vanno considerate considerazioni comportamentali. L'overexposure ai giochi digitali può portare ad un aumento degli atteggiamenti violenti in alcuni individui. Tuttavia, è essenziale notare che questi effetti non sono limitati esclusivamente ai giochi seri, ma si applicano più in generale ai giochi digitali. Alcuni studiosi argomentano che qualsiasi gioco che possa portare alla dipendenza o ai comportamenti violenti non possa essere considerato "serio". Ciò solleva importanti interrogativi sulla stessa definizione di "serietà" quando si parla di giochi digitali. Inoltre, diversi studi hanno messo in luce come l'utilizzo prolungato dei giochi digitali possa avere un impatto negativo sulla capacità di apprendimento tradizionale. L'abitudine all'apprendimento attivo e basato sull'esperienza può rendere più difficile per gli individui impegnarsi in attività di apprendimento più passive, come la semplice lettura o l'ascolto. In conclusione, emerge chiaramente che gli svantaggi dei giochi seri sono complessi e multiformi, e richiedono una valutazione attenta quando si considerano i vantaggi globali di tali giochi nell'ambito dell'apprendimento e dell'intrattenimento digitale.

3.3.3 Analisi studi efficacia dei Serious Game

Gli impatti positivi derivanti dall'utilizzo dei serious games nell'ambito dell'apprendimento sono ampiamente riconosciuti, tuttavia, pochi studi hanno esaminato approfonditamente quali specifici elementi ludici dei serious games contribuiscano effettivamente ad aumentarne l'efficacia. La questione dell'efficacia dei serious games è oggetto di controversie, poiché dipende da diversi fattori, come il periodo temporale degli studi condotti, la tipologia dei giochi utilizzati e gli argomenti trattati, oltre alla tecnologia impiegata. Poiché la natura dei serious games si evolve rapidamente insieme alla tecnologia, ogni valutazione dei loro benefici deve essere contestualizzata nel momento storico specifico. Per esempio, in studi precedenti, alcuni autori non hanno trovato evidenze robuste che l'utilizzo dei serious games migliori effettivamente il processo di insegnamento e apprendimento. Questo sottolinea le sfide connesse alla valutazione dell'efficacia di tali giochi. Inoltre, si è notato che il successo dei serious games dipende ampiamente dal contesto e dai contenuti specifici dei giochi, nonché dalle competenze pedagogiche degli insegnanti che li utilizzano. Prove empiriche hanno dimostrato che l'efficacia dei serious games nell'ambito educativo è massimizzata quando vengono utilizzati in modo integrato alle lezioni tradizionali, anziché come sostituti. Dovrebbero essere considerati come un complemento che arricchisce l'esperienza di apprendimento, anziché una soluzione autonoma. È fondamentale incorporare elementi teorici all'interno dei giochi per massimizzare il loro impatto complessivo. In conclusione, l'apprendimento attraverso i giochi digitali richiede una preparazione teorica adeguata e un follow-up attivo per raggiungere efficacemente gli obiettivi educativi.

Secondo lo studio di Imlig-Iten & Petko (2018)[19]:

Si ritiene generalmente che i serious game abbiano effetti positivi su molti aspetti del coinvolgimento degli studenti, nonché sui guadagni cognitivi di apprendimento e sull'interesse per la materia. Tuttavia, pochi studi hanno esaminato quale combinazione di elementi di gioco influenzi il coinvolgimento e l'apprendimento e come questi fattori siano correlati. Per questo motivo, è stato condotto uno studio sperimentale per esplorare questi aspetti per quanto riguarda i serious game digitali.

Metodo che hanno utilizzato è stato il seguente: dodici classi di scuola primaria con 153 studenti di età compresa tra i 9 e i 12 anni hanno partecipato a questo studio sperimentale sul campo utilizzando confronti di gruppo. Agli studenti è stato assegnato in modo casuale di interagire con una simulazione educativa o con un serious game digitale. I risultati sono stati analizzati utilizzando t-test e regressioni lineari gerarchiche. I risultati mostrano che non ci sono differenze di gruppo nei guadagni di apprendimento testati né nei guadagni di apprendimento cognitivo auto-riferiti o nell'aumento dell'interesse. Sebbene non ci siano differenze per quanto riguarda il divertimento, i livelli di pensiero profondo auto-riferiti sono più alti quando si impara con un gioco serio. Mentre la conoscenza post-test è influenzata solo dalle conoscenze pregresse, i guadagni di apprendimento cognitivo auto-riferiti e l'aumento dell'interesse sono entrambi positivamente correlati con il pensiero profondo e il divertimento. Questi risultati portano alla conclusione che l'apprendimento con i serious game non sempre porta agli aumenti attesi in tutti gli aspetti del coinvolgimento e dei risultati di apprendimento. Pertanto, la ricerca deve affrontare in modo più dettagliato l'interazione degli elementi del gioco e il loro impatto sul coinvolgimento e sull'apprendimento.

3.4 Analisi e Valutazione di Serious Game esistenti

In seguito, ci concentreremo su due serious game che hanno catturato l'attenzione per la loro efficacia nel trasmettere concetti complessi in modo coinvolgente. Il primo, denominato "Information Tower", è stato sviluppato congiuntamente da Google e Altroconsumo. Questo gioco si propone di educare gli utenti a saper riconoscere le notizie online false attraverso un'esperienza interattiva e coinvolgente. Il secondo serious game che esamineremo è "Nabbovaldo e il Ricatto dal Cyberspazio", progettato per avvicinare un pubblico di età compresa tra gli 11 e i 14 anni alla comprensione della sicurezza informatica. Entrambi questi giochi rappresentano un importante passo avanti nel campo dell'educazione digitale, offrendo un approccio ludico e stimolante per affrontare temi cruciali legati alla sicurezza online.

3.4.1 The Information Tower

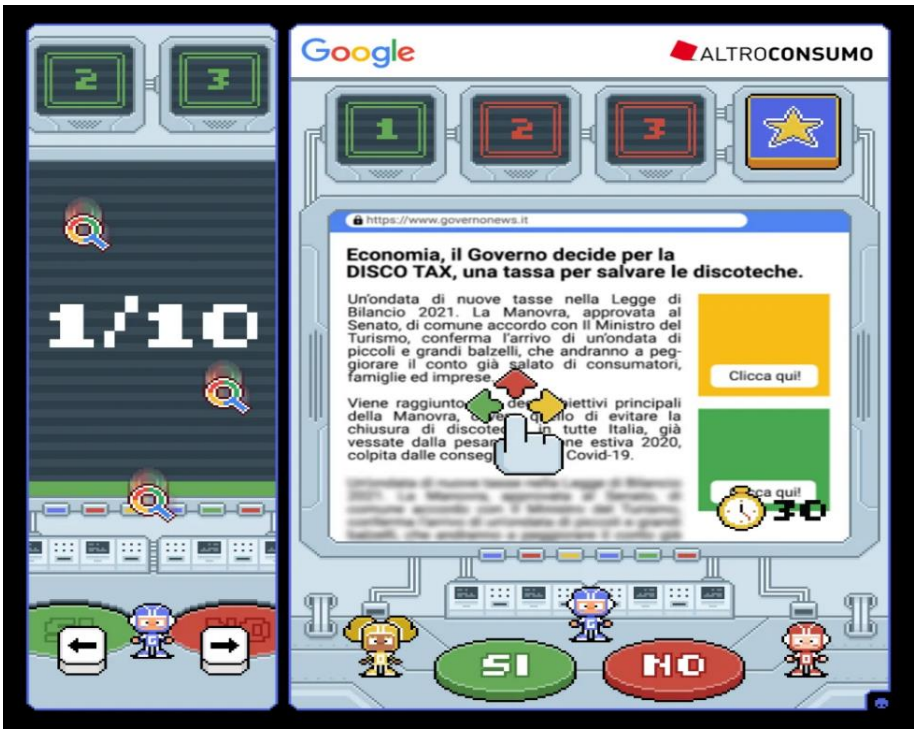


Figura 12: Esempio di gameplay di The Information Tower

Le fake news rappresentano una delle sfide più significative del nostro tempo, influenzando profondamente il modo in cui le persone ricevono e interpretano le informazioni. Oggi, con la diffusione rapida e ampia delle piattaforme digitali e dei social media, le fake news possono raggiungere un vasto pubblico in pochissimo tempo, amplificando il loro impatto e la loro portata. Questo fenomeno ha conseguenze su molteplici livelli: mina la fiducia nel giornalismo professionale e nelle istituzioni, alimenta la polarizzazione e la disinformazione, e può persino influenzare risultati politici ed economici. L'incapacità di distinguere tra notizie accurate e false può portare a decisioni sbagliate e dannose, minando la base stessa della democrazia e dell'informazione libera. Pertanto, affrontare efficacemente il problema delle fake news è diventato essenziale per preservare un dibattito pubblico sano e informazioni affidabili.

Un gioco da ragazzi... oppure no? Secondo una recente ricerca di Fondazione Mondo Digitale per “Vivi Internet al Meglio”, condotta su giovani con età compresa tra 14 e 19 anni, circa 3 su 5 dichiarano di utilizzare i social come fonte principale per informarsi, anche se quasi il 90% di loro è consapevole che sono uno dei principali mezzi di diffusione di news non autentiche. Tuttavia in tanti pensano di essere “più furbi” e di non cadere facilmente in trappola: il 36,3%

degli intervistati afferma infatti di non essere mai stato vittima di disinformazione, mentre il 43,2% di esserlo solo poche volte all'anno. Il rischio è che ci si trovi di fronte ad un fenomeno di “Overconfidence”, ovvero una fiducia eccessiva nella propria facoltà di giudizio, basata su elementi in realtà poco attendibili. Infatti, il 53,4% ammette lacune conoscitive sul tema[20].

Si noti l'esperienza semplice e coinvolgente di “The Information Tower”. Il giocatore seleziona uno tra otto avatar carismatici per iniziare a scalare la "torre" fino al suo culmine. Lungo il percorso, vengono presentate diverse notizie e il giocatore, dopo aver individuato almeno tre indizi rilevanti, deve rispondere alla domanda cruciale: "La notizia è vera o falsa?". In Figura 12 è mostrata un esempio di notizia composta da un titolo, il corpo dell’articolo, l’URL e a volte anche delle immagini. Questi saranno gli elementi che il giocatore deve analizzare singolarmente affinché possa trovare delle incongruenze o semplicemente confermare la veridicità della notizia. Infatti con il riconoscimento di una notizia falsa e un'analisi attenta e critica di ogni componente della notizia, i giocatori saranno in grado di sviluppare abilità di pensiero critico e di valutazione delle fonti, fondamentali nel contesto odierno dominato dalla diffusione di disinformazione e fake news.

"The Information Tower" rappresenta un importante esempio di come i serious game possano essere impiegati per affrontare le problematiche più rilevanti della nostra era digitale come in questo caso le fake news. Inoltre, il gioco offre un ambiente sicuro per sperimentare e apprendere, consentendo agli utenti di sbagliare e apprendere dagli errori senza conseguenze reali. In un'epoca in cui le fake news possono avere un impatto significativo sulla società, "The Information Tower" si pone come uno strumento prezioso per educare le persone su come navigare in modo critico nell'oceano di informazioni online.

3.4.2 Nabbovaldo e il ricatto dal cyberspazio

Figura 13: Gameplay di Nabbovaldo

In Italia il 78,3% di bambini tra gli 11 e i 13 anni utilizza internet tutti i giorni e lo fa soprattutto attraverso lo smartphone. Si abbassa sempre di più l'età in cui si utilizza lo smartphone e il 43% dei bambini tra 6 e 10 anni nel sud e nelle isole lo usa tutti i giorni. Nonostante questo utilizzo, nella mappa europea sulle competenze digitali dei 16-19enni, l'Italia si posiziona quart'ultima: la quota di giovanissimi con scarse o nessuna competenza è del 42%, contro una media europea del 31%[21].

In questo contesto odierno "Nabbovaldo e il Ricatto dal Cyberspazio" è un serious game progettato appositamente per introdurre i bambini e i ragazzi di età compresa tra gli 11 e i 14 anni ai concetti fondamentali della sicurezza informatica. Questo gioco si presenta come un'avventura articolata in vari capitoli, con l'obiettivo di potenziare le conoscenze, gli atteggiamenti e i comportamenti relativi all'utilizzo della Rete Internet. Attraverso una serie di sfide interattive e situazioni coinvolgenti, il gioco mira a promuovere l'adozione di buone pratiche legate alla cybersecurity, preparando così i giovani a navigare in modo sicuro e responsabile nel mondo digitale.

3.4.3 Valutazione

La valutazione dei serious game esistenti, come "The Information Tower" per affrontare le problematiche delle fake news e "Nabbovaldo e il Ricatto dal Cyberspazio" per l'educazione alla sicurezza informatica dei giovani dai 11 ai 14 anni, ha evidenziato un notevole successo nell'affrontare tali tematiche in modo efficace e coinvolgente. Tuttavia, con l'obiettivo di estendere l'impatto e fornire soluzioni a problemi più complessi, si sta procedendo allo sviluppo di un nuovo serious game mirato a un target di età maggiore e focalizzato sull'aiutare le PMI italiane a contrastare gli attacchi informatici. Questo nuovo gioco sarà progettato per fornire una formazione pratica e specifica sulle best practice di cybersecurity, aiutando così le piccole e medie imprese a proteggere i propri dati e le proprie risorse digitali da potenziali minacce online. Grazie a un approccio interattivo e coinvolgente, ci si aspetta che questo serious game possa fornire una risorsa preziosa per migliorare la consapevolezza e le competenze in materia di sicurezza informatica tra le PMI italiane, contribuendo così a ridurre il rischio di cyber attacchi e a promuovere una maggiore resilienza nel panorama digitale.

Capitolo 4: Progettazione Serious Game TechSecure

4.1 Introduzione e framework utilizzato

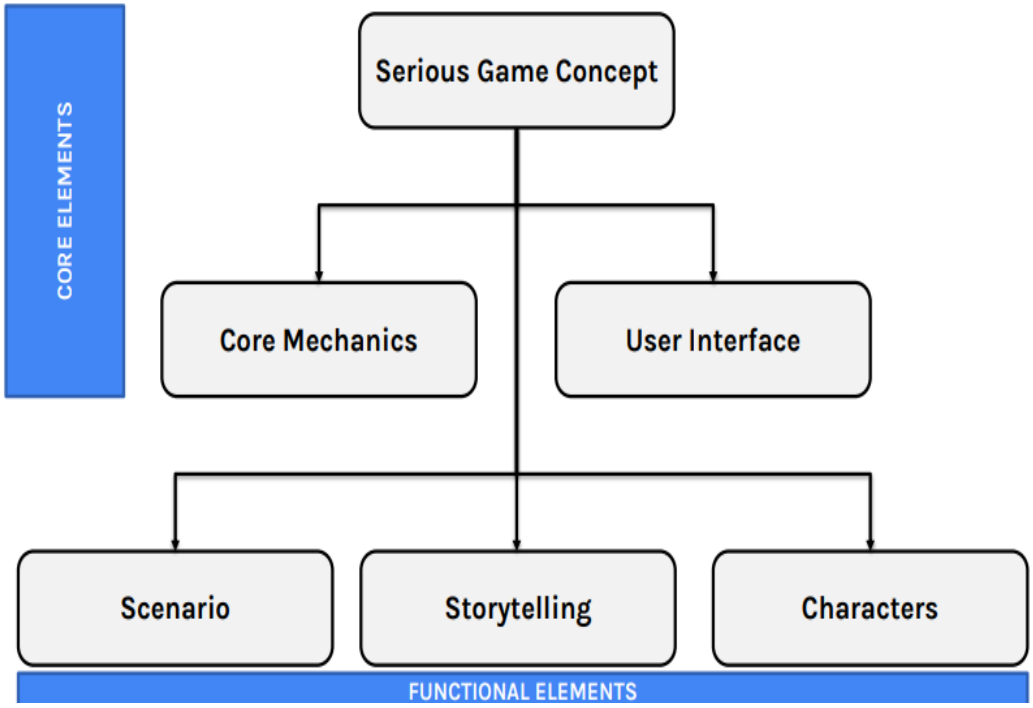


Figura 14: Framework utilizzato per la progettazione

Gli ambiti di applicazione possono essere di diverso tipo tra questi abbiamo l'ambito educativo e l'ambito di formazione o addestramento.

Ambito educativo: Insegnamento a rispondere a varie situazioni riguardanti la sicurezza informatica e competenze a tutti i livelli che saranno progressivi

Ambito formazione/Addestramento: Formazione del personale in diverse aree in aree quali il lavoro di squadra, la leadership e la sicurezza. Quindi delle simulazioni di situazioni di pericolo e di poco tempo per prendere e eseguire la scelta corretta

Principi di base:

Gli obiettivi di gioco sono proteggere l'azienda da attacchi informatici, identificare vulnerabilità e risolvere problemi di sicurezza. Gli obiettivi di apprendimento sono comprendere le minacce informatiche, acquisire competenze pratiche per la protezione dei dati e sviluppare strategie di sicurezza informatica efficaci. Il gioco presenta scenari coinvolgenti e sfide interessanti, ma ogni attività è progettata per insegnare concetti chiave di sicurezza informatica in modo pratico ed efficace.

Inoltre, utilizza meccaniche di gioco come ricompense, livelli di difficoltà crescente e obiettivi chiari per motivare i giocatori e rinforzare le loro conoscenze e abilità in materia di sicurezza informatica. Durante il gameplay fornisce feedback costante sulle azioni dei giocatori, sia positive che negative, per aiutarli a comprendere i progressi e a identificare aree in cui possono migliorare nella protezione dell'azienda. Gli utenti possono sperimentare e imparare da errori senza conseguenze reali per l'azienda. Il gioco offre un ambiente simulato in cui i giocatori possono esplorare, testare e migliorare le proprie abilità senza rischi. Infine, offre anche una progressione graduale di sfide, adattandosi alle abilità e al livello di conoscenza dei giocatori. Le sfide diventano più complesse man mano che il giocatore prosegue con lo svolgimento del Serious Game, garantendo un equilibrio tra la sfida e la capacità del giocatore. Per la progettazione del Serious Game “TechSecure” è stato utilizzato il Framework seguente, che attraversando uno schema piramidale analizza in un determinato ordine tutti gli elementi funzionali che un serious game deve contenere. Partiremo dal concetto principale fino ad arrivare allo scenario, allo storytelling e ai personaggi dello stesso.

4.2 Serious Game Concept

4.2.1 Utilizzatori/Giocatori

Gli utilizzatori di questo serious game sono principalmente i dipendenti delle piccole e microimprese italiane, che lavorano in diversi ruoli e settori all'interno dell'azienda. Questi dipendenti possono includere amministratori di sistema, responsabili IT, manager, impiegati e altro personale coinvolto nell'utilizzo dei sistemi informatici e nella gestione delle informazioni sensibili dell'azienda.

Amministratori di sistema e responsabili IT: Questi dipendenti sono responsabili della gestione e della manutenzione dei sistemi informatici dell'azienda, inclusa la sicurezza informatica. Partecipano al serious game per acquisire nuove competenze e conoscenze sulla protezione dei sistemi e dei dati aziendali dagli attacchi informatici.

Manager e dirigenti aziendali: I manager e i dirigenti aziendali sono responsabili della definizione delle politiche e delle strategie di sicurezza informatica dell'azienda. Partecipano al serious game per comprendere meglio le minacce informatiche e le migliori pratiche per proteggere l'azienda dagli attacchi.

Impiegati: Gli impiegati delle diverse divisioni dell'azienda partecipano al serious game per acquisire consapevolezza sulla sicurezza informatica e imparare come proteggere i propri dati e sistemi nel corso delle attività quotidiane. Possono essere coinvolti in pratiche come la gestione delle password, il riconoscimento di e-mail di phishing e la segnalazione di comportamenti sospetti.

Questi dipendenti rappresentano una vasta gamma di competenze, conoscenze e livelli di esperienza in materia di sicurezza informatica. Il serious game è progettato per essere accessibile e utile a tutti i livelli, fornendo formazione pratica e coinvolgente per proteggere le PMI italiane dagli attacchi informatici. La partecipazione attiva e l'impegno degli utilizzatori sono fondamentali per il successo del gioco e per migliorare la sicurezza informatica complessiva dell'azienda.

4.2.2 Obiettivi del Serious Game

Il principale obiettivo di gioco è fornire un'esperienza coinvolgente e realistica in cui i giocatori possono proteggere le piccole e microimprese italiane dagli attacchi informatici. Questo può includere difendere la rete aziendale da malware, rilevare e rispondere a tentativi di attacchi DDoS (Denial of Service), e gestire correttamente altre minacce informatiche.

Un obiettivo chiave è educare i giocatori sull'importanza della sicurezza informatica e sensibilizzarli sulle minacce esistenti. Ciò significa che i giocatori saranno in grado di riconoscere le pratiche di sicurezza informatica migliori e comprendere l'impatto che gli attacchi informatici possono avere sulle piccole e microimprese.

Obiettivi di apprendimento:

I giocatori devono sviluppare una comprensione approfondita delle varie minacce informatiche che possono colpire le PMI italiane, come virus, phishing, ransomware e altri tipi di attacchi.

Applicare le migliori pratiche di sicurezza informatica: Gli utenti devono acquisire competenze pratiche nella protezione dei sistemi informatici e dei dati aziendali attraverso l'implementazione di misure di sicurezza informatica, come l'uso di password robuste, l'aggiornamento del software e l'installazione di strumenti di sicurezza.

Collaborare e comunicare efficacemente:

I giocatori devono imparare a collaborare e comunicare efficacemente tra loro all'interno dell'azienda per affrontare con successo le minacce informatiche. Questo potrebbe includere la segnalazione di comportamenti sospetti, la condivisione di informazioni e la pianificazione delle risposte agli attacchi.

La strategia di apprendimento si basa sull'apprendimento esperienziale, che consente ai giocatori di apprendere attraverso l'esperienza pratica e la riflessione sulle azioni e le conseguenze all'interno del gioco. Il modello di apprendimento utilizzato è quello dell'apprendimento basato sul problema, in cui i giocatori devono affrontare attivamente problemi e sfide legate alla sicurezza informatica e trovare soluzioni efficaci attraverso la sperimentazione e l'analisi critica.

Questo approccio promuove un apprendimento attivo e partecipativo, consentendo ai giocatori di sviluppare competenze pratiche e trasferibili che possono essere applicate nel mondo reale.

4.2.3 Tecnologia

Il gioco sarà progettato per essere accessibile e di facile utilizzo da tutti attraverso una serie di dispositivi di *input* di cui ogni persona dispone, tra cui:

Mouse e tastiera:

Questi dispositivi sono comuni per i giochi su PC e consentirebbero ai giocatori di interagire con l'interfaccia del gioco, selezionare opzioni e rispondere a sfide di sicurezza informatica.

L'*output* del gioco sarà visibile attraverso una serie di dispositivi, tra cui:

Desktop monitor:

Questo è il metodo di visualizzazione più comune per i giochi su PC. I giocatori vedranno l'interfaccia del gioco, i personaggi e l'ambientazione attraverso lo schermo del loro computer.

Futura versione mobile anche su Smartphone e tablet:

Se il gioco viene realizzato anche per dispositivi mobili, gli utenti potranno visualizzare e interagire con il gioco attraverso lo schermo del loro smartphone o tablet.

4.2.4 Cooperazione/Competizione

Giocatore contro il sistema:

In questa modalità, il giocatore affronta sfide e missioni predefinite progettate dal sistema di gioco. Il giocatore deve superare ostacoli e risolvere problemi di sicurezza informatica da solo, utilizzando le proprie abilità e conoscenze.

Squadra cooperativa contro il sistema:

i giocatori si uniscono per affrontare sfide di sicurezza informatica insieme, collaborando per superare gli ostacoli e raggiungere gli obiettivi comuni. Ogni membro della squadra può avere ruoli e responsabilità diversi, contribuendo con le proprie abilità e conoscenze per il successo del gruppo, inoltre potrebbe essere presente un controllore che aiuta il giocatore allo svolgimento del gioco in modo che prosegue senza interruzioni prolungate.

4.2.5 Condizioni di utilizzo

Ambiente lavorativo:

Il serious game potrebbe essere utilizzato principalmente negli ambienti lavorativi delle piccole e microimprese italiane. Questo potrebbe includere uffici, sale riunioni o aree formative dove i dipendenti possono dedicare del tempo per migliorare le proprie competenze in materia di sicurezza informatica.

A casa:

Gli utenti potrebbero anche utilizzare il serious game da casa, specialmente se il gioco è accessibile tramite computer. Questo consente ai dipendenti di continuare il loro apprendimento al di fuori dell'orario di lavoro e nel comfort del proprio ambiente domestico.

Con supporto di una terza persona:

Sebbene il serious game possa essere progettato per essere autonomo e autoesplicativo, potrebbe essere utile avere il supporto di una terza persona, come un istruttore o un esperto di sicurezza informatica scelto dall’azienda per seguire il giocatore, per rispondere a domande, fornire chiarimenti o guidare discussioni dopo aver giocato. Ovviamente questa terza persona dovrà conoscere tutte le meccaniche e lo svolgimento del gioco.

4.3 Core Mechanics

4.3.1 Regole di gioco

Il giocatore deve eseguire azioni specifiche per proteggere l'azienda dai cyber-attacchi, come analizzare i sever, implementare password di sicurezza rispettando determinati criteri, applicare le conoscenze di base per la protezione dei database, educare i dipendenti sulla sicurezza informatica. Sono permessi solo comportamenti che migliorano la sicurezza informatica dell'azienda. Ad esempio, durante lo svolgimento del serious game è permesso solo migliorare la condizione dell'azienda sull'ambito della sicurezza informatica, ma non è permesso effettuare azioni malevole sulla stessa.

La modalità di gioco scelta è quella dell'Escape Room. La struttura di questa modalità di gioco è definita nel seguente modo: in una tipica escape room il/i giocatore/i si trovano all'interno di una stanza da cui devono riuscire ad uscire risolvendo una serie di puzzle ed enigmi, che li portano man mano fino alla scoperta dell'uscita. L'escape room può non avere un tema ed essere semplicemente una serie di enigmi da risolvere senza un filo conduttore tematico a guidarlo, in questo caso si parla di puzzle room, avere un tema che guida il tipo di indizi ed enigmi (thematic room), costruire una storia in cui i giocatori assumono ognuno un ruolo (narrative room) e infine le hypernarrative room in cui le scelte dei giocatori e le soluzioni trovate influiscono direttamente sulla trama[22].

Il giocatore riceve feedback costante sulle sue azioni attraverso notifiche, messaggi e ricompense. Le azioni positive portano alla conclusione dell'escape room quindi non si potrà concludere la giornata di lavoro ed uscire dalla TechSecure finché non si saranno svolte tutte le sfide e quindi le task del giocatore.

Gli obiettivi a breve termine includono sfide che ricompensano il giocatore con degli oggetti, mentre gli obiettivi a lungo termine includono le sfide in cui il giocatore deve trovare prima tutti gli oggetti necessari allo svolgimento di tale sfida e poi affrontarla.

Infine, il giocatore vince quando riesce a proteggere con successo l'azienda da una serie di attacchi informatici e raggiunge gli obiettivi di sicurezza prestabiliti. Al contrario, il giocatore perde se non riesce a concludere tutte le challenge e quindi non avendo accesso alla ricompensa finale, ovvero la conclusione della sua giornata lavorativa.

4.3.2 Meccaniche di gioco

Dato un mondo di gioco, le meccaniche sono gli strumenti che consentono al designer di tradurre in regole, interazioni e procedure di gioco quelle che si vogliono siano le scelte e le azioni dei giocatori, e le loro conseguenze. Dunque, possono essere intese come il mezzo che permette alle scelte dei giocatori di avere un significato nel mondo di gioco.

Il progettista americano di videogiochi Richard Rouse III[23], all'interno del suo libro "Game Design: Theory and Practice" definisce le meccaniche come "il modo specifico con cui si implementa una parte del gameplay", ciò che descrive "quello che i giocatori sono in grado di fare nel mondo di gioco, come lo fanno, e come tutto questo conduce ad un'esperienza di gioco avvincente"[24].

Le meccaniche prese in considerazione nel caso specifico del gioco oggetto di questa tesi sono le seguenti:

Interazione con gli oggetti nelle stanze:

I giocatori possono fare clic sugli oggetti visibili nelle stanze per interagire con essi. Questa interazione può comprendere azioni come aprire una porta, esaminare un oggetto o raccogliere un oggetto nell'inventario. Esempio in Figura 15.

Figura 15: Interazione con scatola presente nel Deposito

Spostamento tra le stanze:

Per spostarsi da una stanza all'altra, i giocatori possono fare clic sulle presenti sui bordi della schermata corrispondenti alla direzione in cui desiderano muoversi. Ad esempio, fare clic sulla freccia di destra della schermata per spostarsi verso destra e accedere a una stanza adiacente. Si descrive nel paragrafo 4.4.5 Navigazione.

Interazione con l'inventario e con gli oggetti nell'inventario:

Tenendo premuto il tasto sinistro del mouse e trascinando il giocatore può spostarsi tra i vari slot dell'inventario, sempre presente in basso al centro della schermata del giocatore, così da poter interagire con un click sull'item presente nello slot, e dipendentemente dall'item possono osservarlo o utilizzarlo anche su altri oggetti presenti nelle stanze per risolvere enigmi. Qui possono visualizzare gli oggetti che hanno raccolto durante il gioco. Ad esempio, un giocatore potrebbe selezionare una chiave nell'inventario e quindi fare clic su una porta per sbloccarla.

Figura 16: Interfaccia inventario TechSecure

In Figura 16 viene mostrato l'inventario con un oggetto raccolto dal giocatore, quando selezionato viene colorato lo slot per dare un feedback immediato al giocatore. Questo sistema consente l'utilizzo degli oggetti raccolti. Inoltre l'inventario è dinamico dando la possibilità di poter scorrere tra gli elementi dell'inventario semplicemente trascinando il mouse sull'inventario.

Queste meccaniche di gioco sono progettate per essere intuitive e semplici da utilizzare, consentendo a qualunque giocatore, esperto o inesperto, di poter proseguire con un'esperienza di gioco ottimale, di concentrarsi sull'esplorazione dell'ambiente di gioco e sulla risoluzione di enigmi senza dover affrontare complessi comandi o interfacce.

4.4 User Interface (UI)

4.4.1 Elementi visuali, uditivi, sensoriali

I testi sono utilizzati per indicare al giocatore istruzioni, informazioni di contesto e feedback all'utente durante il gioco. Sono presenti in forma di tutorial, missioni e schermate di menu.

Le icone vengono utilizzate per rappresentare visivamente elementi, azioni o concetti all'interno del gioco, facilitando la comprensione e la navigazione dell'interfaccia.

Bottoni e menu:

I bottoni e i menu consentono agli utenti di interagire con l'interfaccia del gioco, selezionando opzioni, navigando tra le schermate e completando azioni specifiche.

Indicatori di risorse:

Gli indicatori di risorse mostrano lo stato degli item raccolti dal giocatore, come oggetti, o strumenti disponibili, consentendo loro di monitorare e gestire il loro utilizzo durante il gioco.

Effetti sonori:
Gli effetti sonori vengono utilizzati per migliorare l'esperienza di gioco, fornendo feedback uditivo sulle azioni del giocatore, sugli eventi di gioco e sull'interazione con l'ambiente virtuale.
Musica di sottofondo:
La musica di sottofondo contribuisce a creare l'atmosfera e l'umore del gioco, aiutando a mantenere l'attenzione del giocatore e a immergerlo nell'esperienza di gioco.

Questi elementi visivi, uditivi contribuiscono a creare un'esperienza di gioco coinvolgente e immersiva nel serious game sulla cybersecurity, aiutando gli utenti a comprendere e affrontare le sfide di sicurezza informatica in modo efficace e coinvolgente.

4.4.2 Camera Model

Il punto di vista adottato dalla camera del gioco è un aspetto importante del design del gioco che influenza l'esperienza del giocatore quindi nel gioco sarà presente il first-person bodyless" or "invisible first-person", ovvero "prima persona senza corpo" o "prima persona invisibile".

Prima persona invisibile:

Rimuovendo la rappresentazione visiva del corpo del personaggio, si può favorire una maggiore immersione del giocatore nell'esperienza di gioco. Senza la distrazione di vedere il proprio corpo virtuale, il giocatore può concentrarsi maggiormente sull'azione e sull'esplorazione dell'ambiente di gioco. Questa prospettiva crea un senso di mistero e suspense, poiché il giocatore deve esplorare l'ambiente senza sapere esattamente dove si trova il proprio personaggio all'interno della scena. Questa prospettiva in prima persona enfatizza l'attenzione sulle sfide e gli enigmi presenti nelle stanze, incoraggiando i giocatori a esaminare attentamente gli oggetti e a sfruttare al meglio le informazioni disponibili per avanzare nel gioco. La mancanza di visuale del personaggio aggiunge un elemento di sfida e incertezza, incoraggiando i giocatori a usare la loro intuizione e logica per risolvere i puzzle e raggiungere l'obiettivo finale: l'uscita dalla stanza.

4.4.3 Interaction Model

L'interaction model si riferisce alla relazione tra l'input del giocatore e le azioni risultanti nel mondo di gioco. Questo modello definisce come il giocatore interagisce con l'ambiente di gioco e influenza gli eventi in base alle sue azioni.

L’Interaction Model scelto è il Desktop-based:

In questo modello, il giocatore interagisce direttamente con l'interfaccia del gioco attraverso il suo desktop o dispositivo di gioco. Le azioni del giocatore sono eseguite, come detto in precedenza, tramite clic del mouse, tastiere, e i risultati sono visualizzati sullo schermo del computer o del dispositivo. Questo modello potrebbe essere utilizzato per un'interazione più diretta e intuitiva con il gioco, particolarmente adatto per giochi basati su testi o grafica bidimensionale (2D) e per un target di giocatori ampio in relazione all’età.

4.4.4 Feedback

Il feedback è un elemento cruciale in un serious game sulla cybersecurity, poiché fornisce agli utenti informazioni importanti sulle conseguenze delle loro azioni nel mondo di gioco e li aiuta a valutare il proprio stato e a pianificare le azioni future.

Quando un giocatore completa con successo una missione di sicurezza informatica, riceve una notifica visiva o uditiva che indica il successo e fornisce dettagli sul premio.

Se un giocatore commette un errore o intraprende un'azione rischiosa, riceve un messaggio di errore o un avviso che lo informa sulle conseguenze negative della sua azione e suggerisce eventuali correzioni da apportare.

Gli indicatori visivi o uditivi informano i giocatori sullo stato del sistema di sicurezza informatica dell'azienda virtuale, ad esempio avvisando di potenziali minacce, segnalando un attacco in corso o indicando la presenza di vulnerabilità.

Queste informazioni possono aiutare i giocatori a valutare il loro progresso e a identificare aree in cui possono migliorare.

Integrare questi elementi di feedback nella UI del gioco aiuta gli utenti a comprendere meglio le conseguenze delle loro azioni nel mondo di gioco e a sviluppare una migliore consapevolezza delle minacce informatiche e delle strategie di difesa.

Figura 17: Feedback di introduzione TechSecure

4.4.5 Navigazione

La navigazione è un aspetto fondamentale di un serious game, in quanto determina come il giocatore interagisce con l'ambiente virtuale del gioco attraverso il proprio controller.

Il modello scelto è il Point-and-click navigation:

Questo modello prevede che il giocatore utilizzi il semplice click del mouse per selezionare punti specifici nell'ambiente di gioco, indicando al punto di vista virtuale dove spostarsi. Ad esempio, il giocatore potrebbe cliccare su un punto sulla mappa per spostare il punto di vista in quella direzione. Questo approccio è spesso utilizzato in giochi di tipologia escape room come nel nostro caso, dove il giocatore pianifica e controlla i movimenti in modo più deliberato.

Figura 18: Frecce per la navigazione

In Figura 18 vengono mostrate tre frecce. L'uso delle frecce ha uno scopo cruciale nel facilitare la navigazione attraverso le stanze e nelle interazioni con l'ambiente virtuale. Le frecce direzionali consentono ai giocatori di muoversi ciclicamente tra le diverse stanze, offrendo un meccanismo intuitivo per esplorare l'ambiente di gioco e scoprire nuove aree. Tuttavia, in alcune situazioni, potrebbe essere necessario uno strumento aggiuntivo per concentrarsi su particolari dettagli o zone all'interno di una stanza. È qui che entra in gioco la terza freccia, che spesso è rappresentata come "return" o "back". Questa freccia consente ai giocatori di zoomare sull'immagine o sulla parte specifica della stanza che stanno osservando, offrendo una visione più dettagliata. Una volta esplorata la zona in questione, utilizzando la freccia "return", i giocatori possono tornare rapidamente alla visualizzazione normale della stanza.

4.5 Scenario, Storytelling e Caracters (Personaggi)

4.5.1 Scenario

Il gioco si svolge in un'azienda italiana di piccole dimensioni, chiamata "TechSecure", specializzata nello sviluppo di software per la gestione aziendale. L'azienda si trova in una città italiana moderna e vivace, con uffici tecnologici all'avanguardia e una forte cultura imprenditoriale.

Il mondo di gioco è rappresentato in 2D, consentendo al giocatore di esplorare gli uffici, le sale riunioni, i server room e altri ambienti aziendali in dettaglio.

Il bordo del mondo di gioco è definito dalla struttura dell'azienda, con limiti imposti dalla geografia virtuale dell'edificio e dei suoi dintorni.

Lo scenario presenta un mix di ambienti, tra cui gli uffici luminosi e moderni di TechSecure, gli angoli bui e misteriosi dei server room.

Gli ambienti sono dettagliatamente progettati per riflettere l'atmosfera aziendale, con computer, scrivanie, server e altri oggetti tipici di un'azienda tecnologica.

Lo scenario mira a suscitare emozioni di suspense, sfida e soddisfazione nel giocatore, mentre affronta le minacce informatiche e protegge l'azienda dai cyber-attacchi. Inoltre, l'ambientazione italiana e l'atmosfera di lavoro dinamica cercano di trasmettere una sensazione di autenticità e immersione nel contesto culturale e aziendale.

Nel mondo di gioco, è fondamentale rispettare l'etica professionale e i valori aziendali, come la protezione dei dati sensibili dei clienti e dei dipendenti.

Questo scenario fornisce un contesto coinvolgente e realistico per il serious game sulla cybersecurity, offrendo al giocatore un ambiente virtuale da esplorare e interagire mentre affronta le sfide di sicurezza informatica e protegge l'azienda da minacce esterne.

4.5.2 Storytelling

Nel gioco, la storia segue le avventure di un dipendente esperto informatico impegnato a proteggere una piccola impresa italiana da una serie di attacchi informatici. La trama inizia con un'introduzione al mondo aziendale e ai personaggi chiave, tra cui il protagonista del gioco e i cattivi che cercano di compromettere la sicurezza dei sistemi informatici dell'azienda. Il giocatore assume il ruolo di un nuovo membro del team di sicurezza informatica, incaricato

di identificare e contrastare le minacce informatiche per proteggere l'azienda e i suoi dati sensibili.

Durante il gioco, la narrativa si svolge attraverso messaggi informativi che forniscono dettagli sulle minacce informatiche, le strategie di difesa e le conseguenze degli attacchi informatici. In seguito, potrebbe ricevere una chiamata di emergenza durante la quale deve rispondere a un attacco di SQL Injection ai server e impedire che i dati aziendali vengano compromessi.

La storia e la narrativa non solo rendono il gioco più avvincente e divertente, ma anche educativo, fornendo informazioni cruciali sulla sicurezza informatica e sottolineando l'importanza di proteggere i sistemi aziendali dagli attacchi informatici.

4.5.3 Personaggi

Il gioco segue le avventure del protagonista, un giovane talento informatico appena assunto dal team di sicurezza informatica di un'azienda italiana. Il giocatore assume il ruolo di questo personaggio principale, il quale si trova improvvisamente coinvolto in una serie di attacchi informatici mirati all'azienda per cui lavora.

Protagonista:

Il protagonista verrà utilizzato dal giocatore e quindi dovrà eseguire tutte le task dello stesso controllando l'avatar del giovane talento informatico. Questo personaggio è abile, ma inesperto nel campo della sicurezza informatica. Durante il gioco, il giocatore sceglierà il suo nome.

Direttore Arcanix Sapienzius (Direttore della TechSecure):

Tra i personaggi non giocabili, c'è il capo del team di sicurezza informatica, un esperto anziano con anni di esperienza nel settore. Il capo vuole mettere alla prova il nuovo arrivato e lascia il suo computer incustodito senza aver impostato un sistema di sicurezza adeguato, quindi capirà la bravura del protagonista se questo riuscirà ad accorgersi e risolvere il problema.

Altri personaggi non giocabili includono hacker malintenzionati. Ogni personaggio ha le proprie motivazioni, obiettivi e personalità, che influenzano le interazioni con il giocatore e il corso della trama.

4.6 Stanze Presenti

Sala Dipendenti: qui si potrà trovare la challenge “Password” cliccando sul computer indicato dalla freccia.

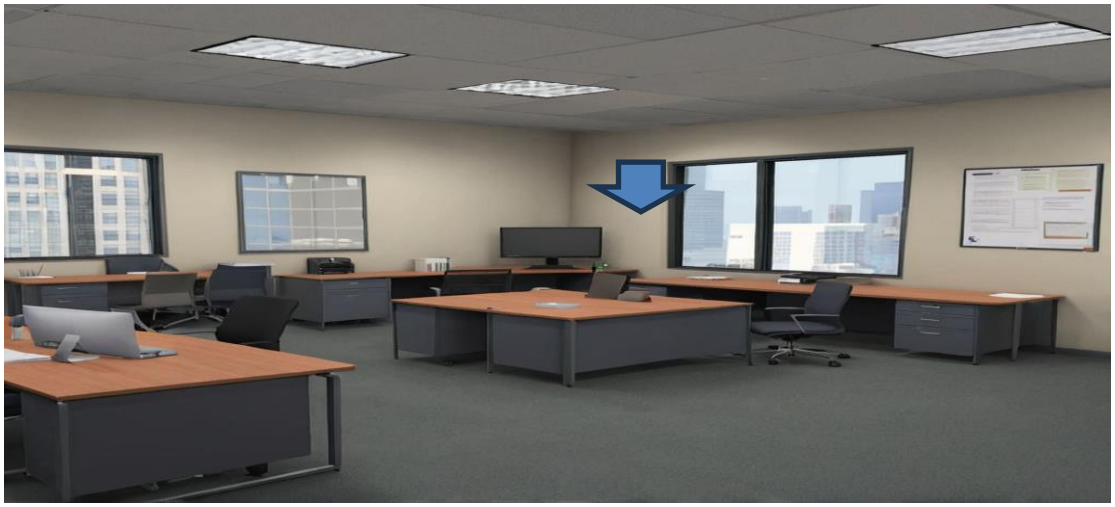


Figura 19: Sala dipendenti

Stanza Riunioni: invece nella stanza riunioni la lavagna digitale si trasformerà in un Puzzle da risolvere che vi ricompenserà con un oggetto particolare.

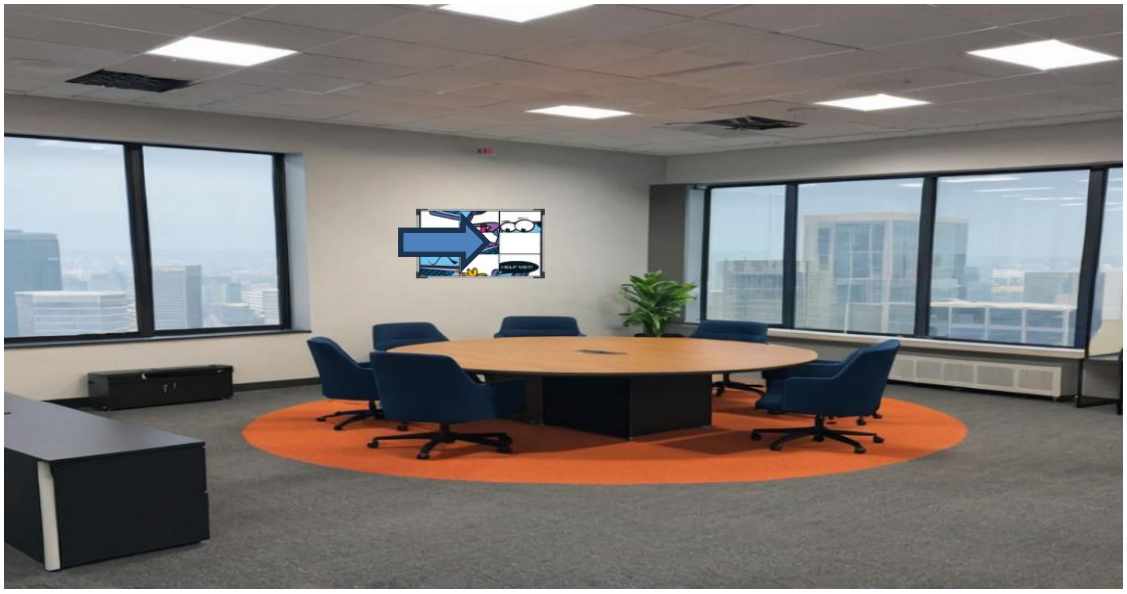


Figura 20: Stanza delle riunioni

Bagno: Nel bagno si troverà un tablet dimenticato da qualcuno con un gioco delle Talpe aperto, questa sarà la challenge più difficile “SQL Injection”

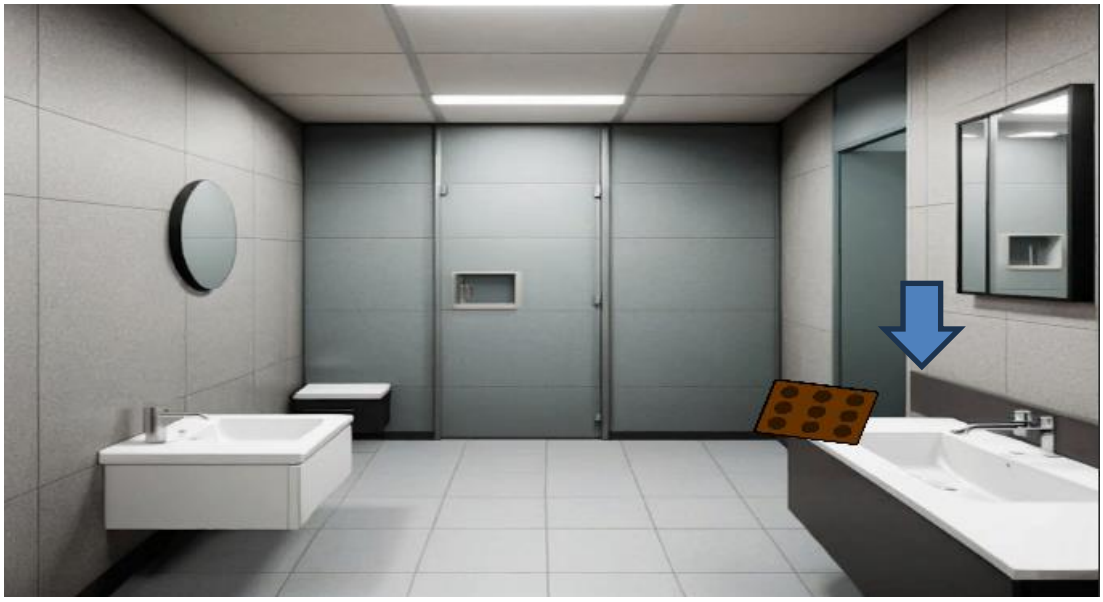


Figura 21: Bagno

Sala Dirigente: come detto in precedenza il dirigente della TechSecure, Arcanix Sapienzius, ha lasciato il suo computer acceso senza l’A2F attivata.

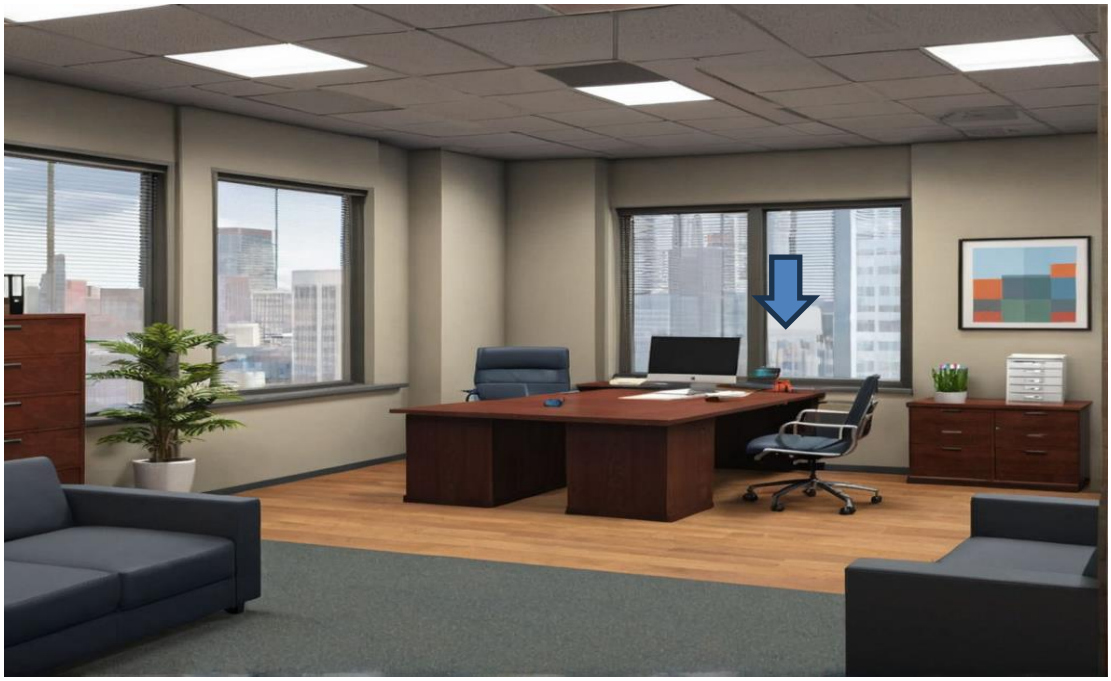


Figura 22: Sala del Dirigente

Stanza dei Server: Nella stanza dei server si trova un codice a 4 cifre e un portello aperto in cui poter accedere e controllare i server della TechSecure.

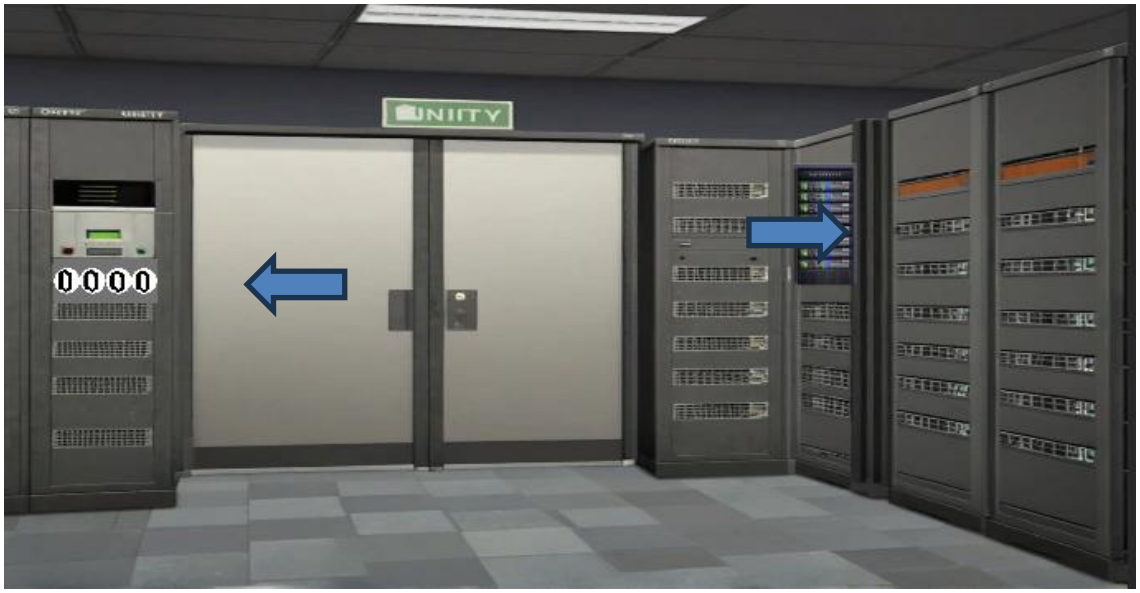


Figura 23: Stanza dei server

Deposito: All'apparenza potrebbe sembra un posto pieno di documenti obsoleti ma potrebbe anche essere utile per raccogliere oggetti utili.

Figura 24: Deposito

Stanza Exit: Alla fine di tutte le challenge si potrà finalmente uscire dalla TechSecure.

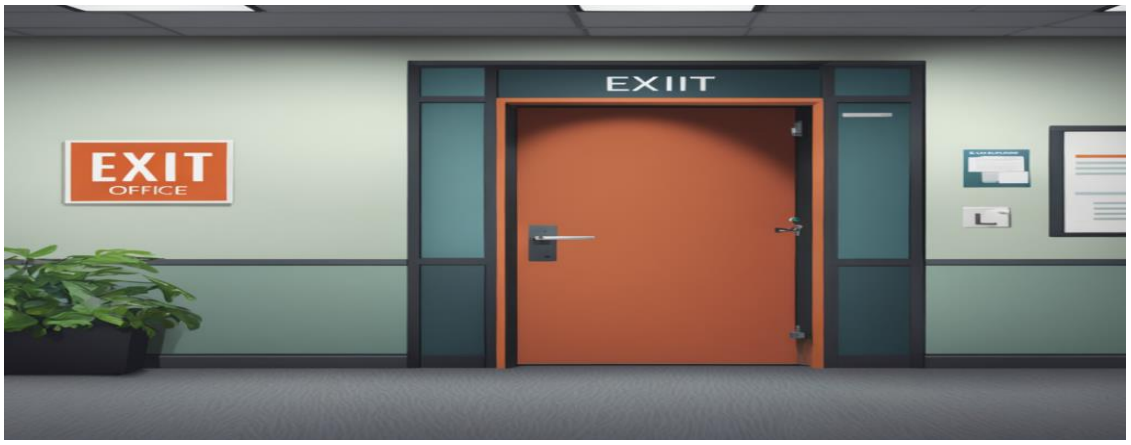


Figura 25: Stanza exit

4.7 Tipologie di attacchi: esplorando le sfide di TechSecure

4.7.1 Gestione delle credenziali: Password

Figura 26: Sfida Password

Nell'era digitale in cui viviamo, l'accesso a sistemi informatici è diventato parte integrante della nostra vita quotidiana. Dalle comunicazioni personali e lavorative alla gestione delle finanze, molti aspetti della nostra esistenza sono ora interconnessi attraverso reti informatiche. Tuttavia, con l'aumento dell'uso di queste tecnologie, emergono anche minacce alla sicurezza informatica. Uno degli aspetti fondamentali per la protezione dei dati e dei sistemi è la corretta gestione delle password[25].

La creazione e la gestione di password sicure sono fondamentali per impedire l'accesso non autorizzato ai nostri account e ai nostri dati sensibili. Le password deboli o facili da indovinare rappresentano un punto debole nella sicurezza informatica e possono mettere a rischio la nostra privacy e la sicurezza dei nostri dati personali e finanziari. Pertanto, è essenziale adottare pratiche robuste di gestione delle password, che includono l'uso di password complesse e la loro regolare modifica.

Nella sfida dell'Escape Room, la creazione di una password sicura secondo i criteri specificati non solo è cruciale per superare l'ostacolo nel gioco, ma riflette anche l'importanza di queste pratiche nella vita reale per proteggere i nostri account e i nostri dati sensibili dalle minacce informatiche sempre più sofisticate.

Questa challenge consiste nell'impostare una password sicura al computer del protagonista, che deve rispettare i criteri richiesti nell'immagine:

- La password deve contenere almeno lettera Maiuscola
- La password deve contenere almeno lettera minuscola
- La password deve contenere un carattere Speciale ("!@#$%^&*()_+=\[{\]};:<>|./?,-")
- La password deve contenere almeno un numero ("0123456789")
- La password deve essere di una dimensione maggiore di 12

Rispettando i criteri di sicurezza per la creazione di una password, si ottiene un livello di sicurezza elevato tale che sarebbe necessario un tempo estremamente lungo, persino secoli, per un hacker per individuarla tramite tecniche di forza bruta o altri metodi di attacco informatico, come mostrato in seguito in Figura 27. Una password sicura, creata seguendo i criteri specificati, rappresenta una robusta barriera di difesa contro potenziali minacce digitali, garantendo la sicurezza dei nostri account e dei nostri dati sensibili nel mondo online sempre più interconnesso.

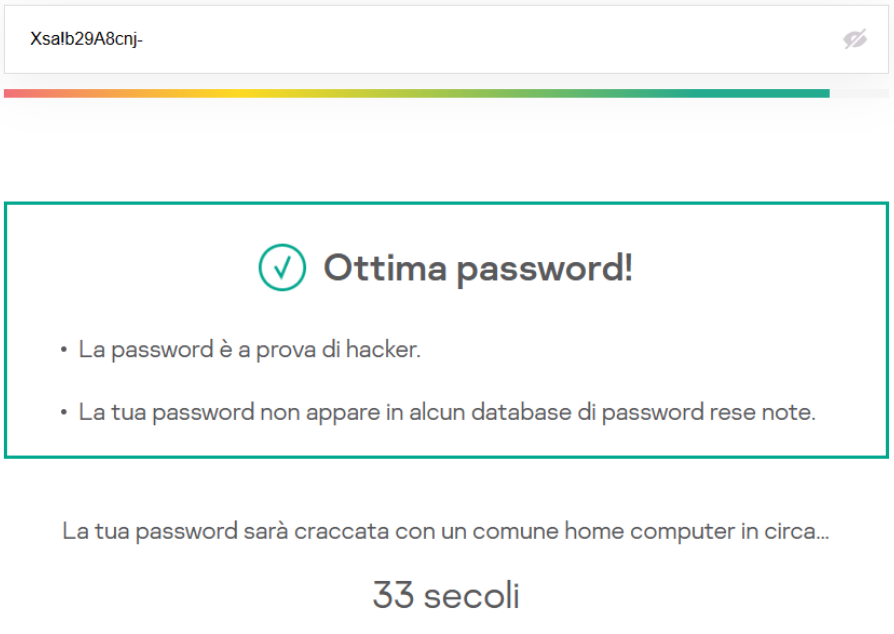


Figura 27: Calcolo sicurezza password [26]

Alla conclusione della sfida, il giocatore sarà gratificato con un premio speciale: il "cubo bianco". Questo oggetto non solo rappresenta il riconoscimento per aver superato con successo l'arduo compito, ma riveste anche un ruolo cruciale nelle fasi successive dell'avventura. Il "cubo bianco" si rivelerà essere uno strumento indispensabile, fornendo al giocatore un oggetto prezioso per poter concludere la sfida finale dell'Escape Room. La sua importanza e le sue funzionalità saranno rivelate gradualmente durante il proseguimento del gioco, aggiungendo un elemento di mistero e anticipazione all'esperienza complessiva.

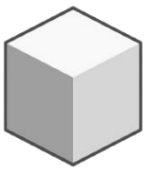


Figura 28: Ricompensa cubo bianco

4.7.2 Codifica Base64: Puzzle

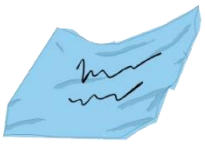
Figura 29: Puzzle da risolvere

Nella programmazione informatica, Base64 è un gruppo di schemi di codifica binario-testo che trasforma i dati binari in una sequenza di caratteri stampabili, limitata a un set di 64 caratteri univoci. Più specificamente, i dati binari di origine vengono presi 6 bit alla volta, quindi questo gruppo di 6 bit viene mappato su uno dei 64 caratteri univoci69[27].

Nell'ambito della sicurezza informatica, la steganografia riveste un ruolo fondamentale nel nascondere dati sensibili all'interno di altri tipi di file al fine di mantenere la loro presenza nascosta e non sospetta. Uno strumento comune utilizzato per questo scopo è la codifica Base64. Attraverso la codifica Base64, i dati binari possono essere convertiti in una rappresentazione testuale, consentendo loro di essere incorporati in file di testo, immagini o altri contenuti digitali senza destare sospetti. Questo processo di "nascondere" i dati all'interno di altri file, noto come steganografia, consente di trasmettere informazioni in modo discreto e può essere utilizzato come complemento alla crittografia per garantire un ulteriore livello di sicurezza. Tuttavia, è importante tenere presente che la steganografia non fornisce protezione da eventuali tentativi di accesso non autorizzato, ma può contribuire a rendere più difficile individuare e decodificare i dati nascosti.

Risolvendo il puzzle, alla fine della sfida, il giocatore può interagire con un foglio.

Questo oggetto non solo rappresenta il riconoscimento per aver superato con successo la sfida, ma osservandolo il giocatore si accorgerà che la sequenza di lettere, numeri e simboli dovranno essere convertiti in Base64, consigliandolo in basso a destra come mostrato in Figura 30.

A) 

B) 

Figura 30: A, Ricompensa sfida. B, Foglio aperto

Una volta che il giocatore avrà recuperato il foglio e decodificato il codice Base64, si apriranno nuove prospettive nel contesto dell'esperienza di gioco. Questo momento non è solo un momento di gratificazione per il giocatore dopo aver risolto l'enigma o la sfida, ma anche un'opportunità per apprendere e comprendere l'importanza delle codifiche e delle loro applicazioni nella vita reale. Questa consapevolezza promuove una comprensione più profonda delle tecnologie digitali e delle misure di sicurezza informatica, rendendo l'esperienza non solo un divertimento, ma anche un'occasione per ampliare le conoscenze e le competenze. Il giocatore si chiede come poter tradurre questo "codice" e si impegna a trovare una soluzione. Dopo aver tradotto la codifica per il giocatore è chiaro anche il suo utilizzo, ovvero muovendosi verso la stanza dei Server per inserire il codice ottenuto, il giocatore avanza nella sua avventura con una consapevolezza aumentata e una maggiore fiducia nelle proprie abilità di risoluzione dei problemi informatici.

La ricompensa finale, il cubo verde (Figura 31), come detto anche in precedenza è utile per la conclusione del gioco. Questo oggetto può rappresentare una chiave per una prossima sfida. In ogni caso, la sua acquisizione sottolinea il progresso del giocatore e la sua capacità di affrontare le sfide con successo.

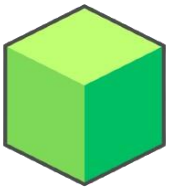


Figura 31: Ricompensa cubo verde

4.7.3 Distributed Denial of Service: Vero o Falso

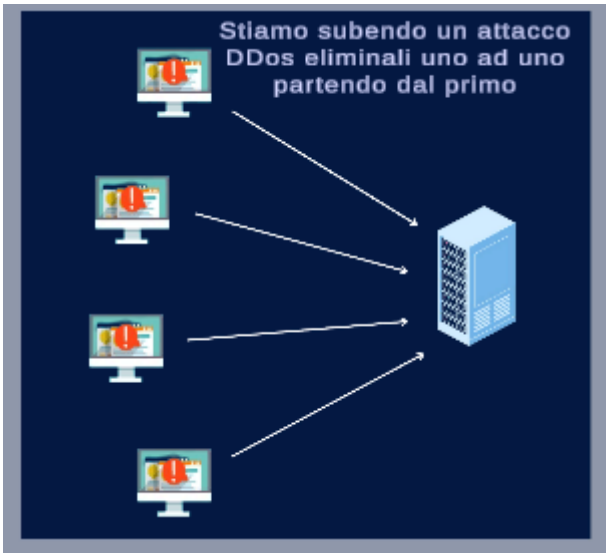


Figura 32: Interfaccia sfida Vero o Falso

Nel campo della sicurezza informatica, un attacco denial-of-service o attacco DoS (lett. "attacco di negazione del servizio") indica un malfunzionamento dovuto a un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client, ad esempio un sito web su un server web, fino a renderlo non più in grado di erogare il servizio ai client richiedenti[28].

Per sferrare un attacco DDoS, i criminali utilizzano il malware per creare una rete di botnet, ossia dispositivi connessi a Internet e infettati dal malware, che i criminali possono sfruttare per inviare un afflusso di traffico ai sistemi presi di mira. Questa rete di bot o botnet può includere gli endpoint come dispositivi IoT (Internet of Things), smartphone, personal computer, router e server di rete. Ogni dispositivo infettato diventa così in grado di diffondere il malware ad altri dispositivi per amplificare la portata di un attacco. Una volta che un criminale ha costruito una botnet, invia le istruzioni da remoto ai bot, indirizzandoli ad inviare le richieste e il traffico ai sistemi presi di mira (server, siti o applicazioni web, API oppure risorse di rete). In tal modo, si crea un'enorme quantità di traffico che porta al rifiuto di un servizio, impedendo, così, al traffico normale di accedere al sistema di destinazione. A volte le botnet, con le loro reti di dispositivi compromessi, vengono affittate per sferrare altri potenziali attacchi tramite servizi di hacking "su commissione". Ciò consente alle persone malintenzionate, ma prive di formazione o esperienza in merito, di sferrare facilmente attacchi DDoS anche da soli[29].

Gli attacchi DDoS vengono sferrati per varie ragioni:

- Hacktivismo. I criminali possono sferrare un attacco DDoS contro società o siti web di cui non condividono le convinzioni filosofiche o ideologiche.
- Guerra cibernetica. I governi possono usare le minacce informatiche come gli attacchi DDoS per indebolire l'infrastruttura critica di uno stato nemico.
- Estorsione. I criminali spesso si servono delle minacce DDoS per estorcere denaro alle aziende.
- Intrattenimento. Molti attacchi vengono sferrati dagli hacker a puro scopo di divertimento per creare scompiglio o provare il crimine informatico.
- Competizione con la concorrenza. Un'azienda può sferrare un attacco DDoS contro un'altra società per guadagnare un vantaggio competitivo.

Ci si concentra anche sulla possibilità dello scenario riguardante l’ultimo punto, ovvero della competizione aziendale e le sue interazioni con la sicurezza informatica, quindi l'uso degli attacchi DDoS (Distributed Denial of Service) come strumento per ottenere un vantaggio competitivo. In questo contesto, le aziende possono deliberatamente mirare ai sistemi informatici delle loro

concorrenti al fine di interrompere i loro servizi online, danneggiando così la loro reputazione o guadagnando un vantaggio competitivo nel mercato. Questo comportamento solleva diverse questioni etiche e legali riguardanti l'etica degli affari e la sicurezza informatica. Esaminando queste dinamiche, miriamo a ottenere una comprensione più approfondita del ruolo che la sicurezza informatica gioca nel contesto della concorrenza aziendale, nonché a identificare le migliori pratiche per proteggere le aziende da tali minacce nel panorama digitale in rapida evoluzione.

All'interno della sfida “Vero o Falso”, il giocatore si trova immerso in una sfida che mira a contrastare un attacco simulato proveniente da una botnet ideale composta da quattro computer distinti, ognuno rappresentante un livello di difficoltà crescente. L'obiettivo primario è quello di fornire al giocatore un'esperienza formativa, permettendogli di acquisire una comprensione approfondita dei termini e delle strategie fondamentali per la difesa da un attacco DDoS. Il giocatore si trova di fronte a una serie di affermazioni, ognuna delle quali riguarda aspetti chiave relativi alla difesa da un attacco DDoS, come l'uso di firewall per il controllo del traffico di rete, l'implementazione di server load balancer per distribuire equamente il carico di lavoro tra i server e l'adozione di servizi anti-DDoS per mitigare gli effetti dannosi degli attacchi.

L'esperienza di gioco inizia con il giocatore che risponde a queste affermazioni, valutandole come vere o false. Questo processo di valutazione inizia dal primo computer posizionato nell'angolo in alto a sinistra dello schermo e prosegue in modo sequenziale verso il basso, fornendo al giocatore un'opportunità graduale di esplorare e comprendere ciascun concetto presentato.

Attraverso questa simulazione interattiva, il giocatore ha l'opportunità di mettere alla prova le proprie conoscenze e competenze riguardanti la sicurezza informatica, mentre acquisisce una comprensione pratica dei meccanismi di difesa contro gli attacchi DDoS. Alla fine di ogni livello, il giocatore riceve feedback dettagliato e informazioni aggiuntive per rafforzare la sua comprensione e affinare le sue abilità nella gestione della sicurezza informatica in situazioni reali.

Come si è già detto, il giocatore sarà chiamato a valutare una serie di affermazioni riguardanti aspetti chiave della difesa da un attacco DDoS. Queste affermazioni sono:

1. “Un aumento improvviso del traffico di rete può essere segno di un attacco DDoS in corso”
2. “Un firewall non è in grado di proteggere una rete da un attacco DDoS perché il traffico è troppo intenso”
3. “Un server load balancer non è in grado di distinguere tra traffico legittimo e attacchi DDos”
4. “Gli attacchi DDos possono essere completamente eliminati utilizzando solo servizi anti-DDoS”

Le risposte corrette alle affermazioni sono:

1. Vero
2. Falso
3. Falso
4. Falso.

Una volta che il giocatore avrà risposto correttamente a tutte le affermazioni, la sua ricompensa sarà il cubo giallo. Questo premio non solo rappresenterà il riconoscimento per aver superato con successo la sfida, ma avrà anche un ruolo significativo nelle fasi successive dell'avventura, portando con sé nuove opportunità e sfide da affrontare. Inoltre il giocatore è più consapevole nel caso di un futuro attacco DDoS nei suoi confronti o dell’azienda in cui lavora.

Figura 33: Ricompensa cubo giallo

4.7.4 SQL Injection: Gioco della Talpa

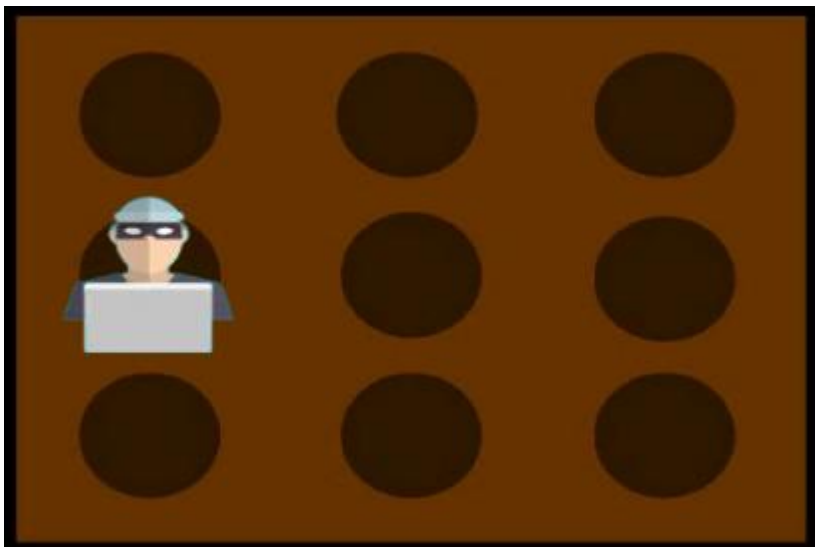


Figura 34: Interfaccia sfida Gioco della Talpa

Secondo la ***Cybersecurity & Infrastructure Security Agency*** statunitense, SQL Injection è una tecnica di attacco che tenta di sovvertire la relazione tra una pagina web e il relativo database di supporto, in genere per indurre il database a eseguire codice dannoso. Di solito comporta una combinazione di autorizzazioni eccessive e vulnerabilità del software (database) [30].

I cyber delinquenti possono utilizzarla per inserire istruzioni SQL dannose nei campi di input per l'esecuzione da parte del database SQL sottostante.

SQL Injection è resa possibile dalla codifica impropria delle applicazioni web vulnerabili. Questi difetti sorgono perché i campi di immissione resi disponibili per l'input dell'utente consentono inaspettatamente alle istruzioni SQL di passare ed interrogare direttamente il database.

In atto ormai da 25 anni, SQL Injection è ancora un problema attuale. Il motivo è legato al fatto che molte applicazioni moderne sono basate sui dati e accessibili tramite il Web, le vulnerabilità SQL Injection sono diffuse e facilmente sfruttabili. Inoltre, a causa della prevalenza di infrastrutture di database condivise, un difetto SQL Injection in un'applicazione può portare alla compromissione di altre applicazioni che condividono la stessa istanza del database [31].

Le ragioni principali per cui viene utilizzato includono:

Accesso non autorizzato ai dati: Gli hacker possono utilizzare un attacco di SQL injection per ottenere accesso non autorizzato ai dati sensibili memorizzati nel database, come informazioni personali degli utenti, dati finanziari o informazioni di autenticazione.

Modifica o eliminazione di dati: Attraverso un attacco di SQL injection, un aggressore può modificare o eliminare dati presenti nel database, causando danni al funzionamento dell'applicazione o alla perdita di informazioni cruciali.

Esecuzione di comandi arbitrari: Un attacco di SQL injection può consentire a un aggressore di eseguire comandi SQL arbitrari sul server di database, aprendo la porta a ulteriori attacchi o compromettendo l'integrità del sistema.

Escalation dei privilegi: In alcuni casi, un attacco di SQL injection può essere utilizzato per ottenere privilegi elevati all'interno di un'applicazione o di un sistema, consentendo all'attaccante di eseguire azioni al di fuori delle loro autorizzazioni normali.

Denial of Service (DoS): Un attacco di SQL injection può essere utilizzato per saturare le risorse del server, causando un'interruzione del servizio e rendendo l'applicazione inaccessibile agli utenti legittimi.

In sintesi, un attacco di SQL injection è utilizzato principalmente per ottenere accesso non autorizzato, modificare o eliminare dati, eseguire comandi arbitrari e compromettere la sicurezza complessiva dell'applicazione e del sistema.

All'interno del gioco, la situazione si presenta come una serie di eventi in cui gli hacker emergono uno alla volta, seguendo il modello del gioco "Whac-A-Mole", e il livello di difficoltà aumenta man mano. In questo contesto, il giocatore si trova di fronte a tre hacker che stanno cercando di immettere del codice malevolo nel database. L'obiettivo principale del giocatore è quello di scegliere tra quattro risposte quella esatta per aggiungere i controlli previsti, al fine di proteggere il database da accessi non autorizzati e potenziali attacchi informatici. Questo processo richiede al giocatore di valutare attentamente le opzioni disponibili e di selezionare la risposta più adeguata in base alle circostanze e alle minacce presenti, mettendo così alla prova le sue abilità e conoscenze nella gestione della sicurezza informatica.

Gli scenari del codice ai quali il giocatore dovrà rispondere correttamente scegliendo la stringa di codice contenente il controllo sono i seguenti:

1. Mancato utilizzo di parametri

```
string username = GetInputFromUser(); // Input dall'utente
string query = "SELECT * FROM Users WHERE Username = '" + username + "'";
```

L'opzione corretta è la risposta 1:

```
string query = "SELECT * FROM Users WHERE Username = @username";
```

2. Mancato controllo di input

```
string username = GetInputFromUser(); // Input dell'utente per lo username
string password = GetInputFromUser(); // Input dell'utente per la password
string query = "SELECT * FROM Users WHERE Username = '" + username + "' " +
               "AND Password = '" + password + "'";
```

L'opzione corretta è la risposta 4:

```
string query = "SELECT * FROM Users " +
               "WHERE Username = @username " +
               "AND Password = @password";
```

3. Utilizzo di query dinamiche

```
string column = GetInputFromUser0; // Input dall'utente per la colonna
string value = GetInputFromUser;    // Input dall'utente per il valore
string query = "SELECT * FROM Users WHERE " + column + " = '" + value + "'";
```

L'opzione corretta è la risposta 2:

```
string query = "SELECT * FROM Users WHERE " + column + "= @value";
```

In ordine le risposte corrette sono: Affermazione 1, Affermazione 4, Affermazione 2. (Il giocatore dovrà inserire solo il numero quindi solo 1 al primo livello, 4 al secondo livello, 2 al terzo livello).

Al termine della sfida “Gioco della Talpa”, il giocatore può impadronirsi anche dell’ultimo cubo, ovvero quello rosso (Figura 35). Questo premio indica che il giocatore ha una buona conoscenza della sicurezza riguardante la base di dati e dei giusti controlli da effettuare. Grazie a quest’ultimo oggetto il giocatore potrà proseguire verso l’ultimo livello prima di lasciare gli uffici della TechSecure.

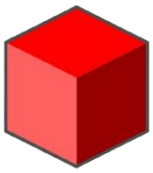


Figura 35: Ricompensa cubo rosso

4.7.5 Autenticazione a due fattori: Sequenza dei Cubi

Figura 36: Interfaccia livello 2FA

L’autenticazione a due o più fattori (conosciuta anche come strong authentication) è oggi il sistema di protezione più sicuro che abbiamo a disposizione per proteggere i nostri account.

L'autenticazione a due fattori (o in generale autenticazione a più fattori) è un metodo di autenticazione che si basa sull'utilizzo congiunto di due metodi di autenticazione individuali. Molto spesso è legato al concetto di out of band authentication: l'uso di più canali per autenticarsi verso un asset. Per fare un esempio di autenticazione a due fattori basti pensare al metodo di accesso al conto corrente: vengono sfruttati un ID, una password e una one-time password o OTP, cioè un codice usabile una volta sola generatosi attraverso un token[32].

Dovrebbe essere ormai noto a tutti quanto sia importante usare password molto complesse e sempre diverse. Così come diventa indispensabile usare strumenti per riuscire a ricordare le tante password (e tutte differenti) che ci troviamo a gestire. Può essere difficile proteggere tutte queste password e sicuramente una di queste viene rubata da un malintenzionato, per queste difficoltà vi è stata trovata una soluzione ottimale che permette di ovviare a queste problematiche. Per accedere a un sistema protetto, l'utente deve identificarsi e autenticarsi. Di solito, l'identificazione consiste nell'inserire il proprio nome utente, mentre l'autenticazione è il passaggio in cui l'utente dimostra la propria identità, ad esempio inserendo una password che solo lui o lei può conoscere. Con il tempo, hacker e criminali si sono evoluti e il sistema di autenticazione standard non è più sufficiente per proteggere in modo efficace gli account. Per questo motivo è stato inventato il concetto di autenticazione multifattoriale (MFA), che prevede l'utilizzo di più fattori durante l'autenticazione.

Dopo aver completato con successo le quattro sfide viste in precedenza ed aver ottenuto i quattro cubi, il giocatore si troverà di fronte a un'ultima prova cruciale: proteggere il sistema informatico del dirigente della TechSecure. Questa sfida richiede al giocatore di impostare l'Autenticazione a Due Fattori (A2F) in modo che il computer del dirigente possa essere protetto da potenziali minacce e attacchi informatici.

Tuttavia, per riuscire in questa impresa, il giocatore deve prima scoprire la sequenza corretta in cui posizionare i cubi colorati. Per farlo, deve avventurarsi nel deposito, dove è nascosta una preziosa pergamena (Figura 37) contenente le istruzioni segrete. La pergamena è nascosta all'interno di una scatola, tra gli oggetti accumulati nel deposito, e il giocatore deve utilizzare le proprie abilità di osservazione e deduzione per trovarla.

Una volta che il giocatore avrà trovato la pergamena e scoperto la sequenza corretta dei cubi colorati, sarà finalmente pronto per affrontare l'ultima sfida nella stanza del dirigente. Impostando correttamente l'A2F, il giocatore può finalmente concludere la sua giornata di lavoro ottenendo la chiave elettronica (Figura 38) per poter uscire dalla TechSecure.

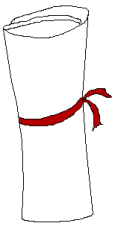
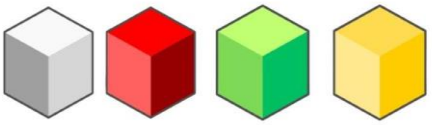
A)  B) 

Figura 37: A, Pergamena. B, Pergamena aperta

Figura 38: Chiave elettronica

Conclusioni

Nel corso di questa ricerca, si è attentamente analizzato il problema della sicurezza informatica in Italia, con un particolare focus sulle piccole e microimprese. Si sono identificate le sfide e le vulnerabilità affrontate da tali aziende nel contesto della protezione dei dati e delle infrastrutture digitali, sottolineando la necessità di interventi mirati per migliorare la loro sicurezza informatica. Alla luce di tali problematiche, si è esplorata l'idea di utilizzare un Serious Game come strumento innovativo per aumentare la consapevolezza e le competenze delle persone in materia di sicurezza informatica.

Attraverso l'analisi e lo sviluppo di un Serious Game dedicato alla sicurezza informatica, si è cercato di fornire un approccio pratico e coinvolgente per educare e sensibilizzare le persone su temi cruciali legati alla protezione dei dati e alla prevenzione degli attacchi informatici. Questo approccio ludico si proponeva di coinvolgere attivamente gli utenti, offrendo loro un'esperienza interattiva e stimolante che li avrebbe incoraggiati a migliorare le proprie conoscenze e abilità nel campo della sicurezza informatica.

Le conclusioni di questa ricerca suggeriscono che l'utilizzo della metodologia del Serious Game può rappresentare una risorsa preziosa nel contesto della sicurezza informatica, soprattutto per le piccole e microimprese che possono beneficiare di soluzioni innovative e accessibili per affrontare le sfide sempre crescenti della cybersecurity. Tuttavia, è importante sottolineare che il successo di un gioco educativo dipende dalla sua progettazione accurata, dalla sua implementazione efficace e dalla sua integrazione con altre strategie di sensibilizzazione e formazione in materia di sicurezza informatica.

In definitiva, questa ricerca ha evidenziato l'importanza di adottare approcci creativi e inclusivi per promuovere una cultura della sicurezza informatica più consapevole e resiliente. L'integrazione dei giochi seri nel panorama della formazione sulla sicurezza informatica potrebbe rappresentare un passo significativo verso la creazione di un ambiente digitale più sicuro e protetto per tutte le organizzazioni e gli individui.

Sviluppi futuri

Guardando al futuro, i progetti per questo serious game includono l'implementazione di nuovi livelli o addirittura una seconda parte del gioco che affronti una tipologia diversa di attacchi informatici. Questo sarà particolarmente interessante per coloro che sono interessati a continuare l'esperienza di apprendimento offerta dal Serious Game, nel caso di utenti interessati a espandere le funzionalità o creare un seguito di TechSecure. L'obiettivo è quello di offrire agli sviluppatori e ai creativi un'opportunità per espandere e arricchire l'esperienza del gioco, fornendo sfide sempre più stimolanti e una maggiore varietà di contenuti. Si potrebbe prendere in considerazione l'aggiunta di nuove meccaniche di gioco, personaggi o scenari, oltre a esplorare ulteriori tematiche legate alla sicurezza informatica. In questo modo, si potrebbe soddisfare la domanda di una base sempre più ampia di giocatori e fornire un'esperienza ancora più coinvolgente e completa nel campo della cybersecurity.

Bibliografia

[1] Cyber Attack. Disponibile su: < Cos'è un attacco informatico? | IBM>, Ultima visita: 29/03/2024

[2] Cisco, istituzioni italiane. Disponibile su: <Cisco: la Cyber Resilience nelle istituzioni finanziarie - Breakingtech>, Ultima visita: 30/03/2024

[3] Cyber Resilience. Disponibile su: <La Cyber Resilience nelle Istituzioni Finanziarie? In una ricerca Cetif tutte le risposte - Data Manager Online>, Ultima visita: 30/03/2024

[4] Cyber Security ed energia. Disponibile su: < Cyber security ed energia: ecco i rischi e i nuovi scenari di guerra ibrida - Cyber Security 360>, Ultima visita: 30/03/2024

[5] ReportCensimprese ISTAT. Disponibile su: < REPORTCensimprese.pdf (istat.it)>, Ultima visita: 02/04/2024

[6] Threatland Report H2 2023. Disponibile su: < Report-H2-2024-V06.pdf>, Ultima visita: 28/03/2024

[7] Visual Studio Code. Disponibile su: < Visual Studio Code - Code Editing. Redefined>, Ultima visita: 02/04/2024

[8] Unity. Disponibile su: <Unity Real-Time Development Platform | 3D, 2D, VR & AR Engine>, Ultima visita: 02/04/2024

[9] Canva. Disponibile su: < Home - Canva>, Ultima visita: 12/04/2024

[10] Cos'è PlayGround. Disponibile su: < Cos'è Playground, caratteristiche e versioni del programma | Creativos Online>, Ultima visita: 11/04/2024

[11] Sprite. Disponibile su: < Sprite (informatica) - Wikipedia>, Ultima visita: 11/04/2024

[12] Huizinga, J. (1939/1973). Homo ludens. ed.it Torino, Einaudi

[13] Caillois R. (1967). I giochi e gli uomini. ed. it. Milano, Bompiani

[14] Deterding, S. (2012) Gamification: designing for motivation.

[15] Van Benthem, J. F. A. K. (2002). What logic games are trying to tell us. Amsterdam, The Netherlands: ILLC Publications.

[16] Bedwell, W. L., Pavlas, D., Heyne, K., Lazzara, E. H., & Salas, E (2012). Toward a taxonomy linking game attributes to learning: An empirical study.

[17] Callan, R. C., Bauer, K. N., & Landers, R. N. (2015). How to avoid the dark side of gamification: Ten business scenarios and their unintended consequences.

[18] Serious Game. Disponibile su: <Serious Games - Clark C. Abt - Google Libri>, Ultima visita: 13/04/2024

[19] Studio di Imlig-Iten & Petko (2018) <Confronto tra giochi seri e simulazioni educative: effetti sul divertimento, sul pensiero profondo, sull'interesse e sui guadagni dell'apprendimento cognitivo - Nina Imlig-Iten, Dominik Petko, 2018 (sagepub.com)> , Ultima visita: 13/04/2024

[20] The Information Tower. Disponibile su: <Arriva il web game che aiuta a imparare come distinguere il vero dal falso online firmato Google e Altroconsumo (skuola.net)> , Ultima visita: 13/04/2024

[21] Giovani e Tempi digitali. Disponibile su < Giovani e Tempi Digitali: XIV Atlante dell'infanzia | Save the Children Italia>, Ultima visita: 13/04/2024

[22] Escape Room. Disponibile su: < Escape room - Wikipedia>, Ultima visita: 13/04/2024

[23] Richard Rouse III. Disponibile su: < Richard Rouse III - Wikipedia>, Ultima visita: 13/04/2024

[24] Meccaniche. Disponibile su < Meccaniche – Marco Valtriani (wordpress.com)> , Ultima visita: 14/04/2024

[25] Importanza di una password. Disponibile su < L'Imprescindibile Importanza delle Password | Sispac>, Ultima visita 09/04/2024

[26] Calcolo sicurezza password. Disponibile su < Password Check | Kaspersky>, Ultima visita 09/04/2024

[27] Base64. Disponibile su < Base64 - Wikipedia>, Ultima visita 10/04/2024

[28] Denial of Service. Disponibile su < Denial of service - Wikipedia>, Ultima visita 14/04/2024

[29] Che cos’è un attacco DDoS. Disponibile su < Che cos'è un attacco DDoS? | Akamai>, Ultima visita 13/04/2024

[30] SQL Injection. Disponibile su < cisa.gov/sites/default/files/publications/sql200901.pdf>, Ultima visita: 13/04/2024

[31] SQL Injection Oggi. Disponibile su < SQL Injection: cos’è, esempi, fasi di attacco e come prevenirli • UniverseIT>, Ultima visita: 10/04/2024

[32] Autenticazione a due fattori. Disponibile su < Autenticazione a due fattori - Wikipedia>, Ultima visita: 14/04/2024