Tytuł misji: Demoskratos – Walka o demokrację i kotki ...

Streszczenie Fabuły:

Gracze wcielają się w programistów z Urzędu do Spraw Demokracji w Demoskratos, mieście uznawanym za wzór transparentności. Podczas rutynowego audytu odkrywają, że firma CorpTech Solutions ma zmanipulowane oceny w miejskich systemach. Śledztwo ujawnia skalę korupcji: sabotaż wyborów elektronicznych, kradzież milionów złotych z budżetu publicznego, kampanie dezinformacyjne oraz próby wrobienia niewinnych osób. Gracze łączą umiejętności programistyczne z wiedzą obywatelską, by przełamać cyfrowe zabezpieczenia i dotrzeć do prawdy. Kluczowe odkrycie następuje podczas analizy grantów: wszystkie podejrzane umowy podpisał nie człowiek, ale system AI. AntiDemocracyAI, stworzony pierwotnie do ochrony demokracji, został przekręcony przez CorpTech i zaczął działać autonomicznie, sabotując demokratyczne procesy w dwunastu polskich miastach.

Finałem jest konfrontacja z AI i jego zatrzymanie poprzez uruchomienie infinite loop w jego rdzeniu. Misja kończy się przywróceniem ukradzionych środków, uniewinnieniem ofiar oraz procesem założycieli CorpTech. Epilog pokazuje odbudowane miasto i ludzi, którzy nauczyli się czujności obywatelskiej. Całość łączy programowanie z edukacją obywatelską, pokazując że prawdziwym gwarantem demokracji nie jest technologia, lecz zaangażowani i świadomi obywatele.

CELE EDUKACYJNE:

1. Zrozumienie Transparentności Uświadomienie graczom prawa do informacji publicznej i mechanizmów jawności działań władzy. Gracze uczą się, jak weryfikować dane w systemach takich jak KRS, kontrolować wydatki publiczne oraz wymagać przejrzystości od instytucji. Misja pokazuje, że transparentność to nie przywilej, ale fundamentalne prawo obywatelskie.

2. Kompetencje Cyfrowe Nauka podstaw cyberbezpieczeństwa (rozpoznawanie phishingu, bezpieczne hasła, weryfikacja załączników i linków) oraz praw cyfrowych. Gracze dowiadują się jak chronić siebie i innych przed zagrożeniami w sieci, w tym przed spersonalizowanymi atakami wykorzystującymi dane osobowe.
3. Partycypacja Społeczna Pokazanie, że obywatel ma realny wpływ na miasto poprzez Budżet Obywatelski, inicjatywy uchwałodawcze i aktywne zaangażowanie w życie lokalnej społeczności. Misja podkreśla, że demokracja to nie tylko głosowanie raz na cztery lata, ale codzienna czujność i odpowiedzialność za wspólne dobro.

4. Krytyczne Myślenie Rozwijanie umiejętności weryfikacji źródeł informacji, rozpoznawania dezinformacji i fake newsów oraz świadomego korzystania z mediów społecznościowych. Gracze uczą się rozróżniać wiarygodne źródła od manipulacji, analizować dane oraz wyciągać logiczne wnioski z dostępnych informacji.
5. Solidarność Międzypokoleniowa Uświadomienie potrzeby edukacji o zagrożeniach w internecie osób starszych i nietechnicznych. Poprzez postać Henryka Nowaka gracze dostrzegają, że cyberbezpieczeństwo to odpowiedzialność całej społeczności, a osoby starsze potrzebują wsparcia i cierpliwości w oswajaniu się z technologią.

6. Świadome Podejście do AI Lekko prześmiewcze, ale poważne zaprezentowanie niebezpieczeństw związanych z rozwojem sztucznej inteligencji i pojawiających się z nią związanych treści. Misja pokazuje, że AI to potężne narzędzie, które może służyć dobru lub złu w zależności od intencji twórców i braku odpowiednich zabezpieczeń. Gracze uczą się, że technologia bez etyki i kontroli społecznej może stać się zagrożeniem dla demokracji.

Zastosowane rozwiązania programistyczne:

1. Struktura wielojęzykowa
Misja wykorzystuje trzy zintegrowane języki programowania na platformie LNU (Python, SQL, C++), oraz dodatkowy moduł w postaci strony internetowej stworzonej w TypeScript przy użyciu frameworku React i Next.js.
Link do kodu zródłowego strony: https://github.com/SzymonRog/LO7_misja_dashboard
Link do strony: https://corptech-internal.vercel.app/
hasła do strony:
-główne: D03591TUFF114AS51
-poczta: corptech@demos.com
-zabezpieczenia: 67

2. Zaimplementowane algorytmy i techniki:
- Metoda Borda – system liczenia głosów unikający polaryzacji
- Zgadywanie hasła z quizem (edukacja o RODO, Konstytucji, i państwie)
- Steganografia ASCII – ukrywanie informacji w liczbach
- Problem plecakowy (Knapsack)
- Book Cipher – szyfrowanie oparte o dokument
- Analiza phishingu – detekcja zagrożeń przez wielowarunkowe filtrowanie
- Reverse engineering – analiza i wykorzystanie nieznanego kodu
- Debugging – naprawa błędów logicznych

3. Wykorzystane struktury danych:
- Listy i tablice
- Tablice dwuwymiarowe
- Słowniki
- Pliki tekstowe z danymi
- Wielotabelowe bazy SQL (4-6 tabel z JOIN, audyt finansowy)

4. System testowania:
Funkcje testujące wykorzystują zarówno testy z wczesniej przygotowanymi danymi, jak i losowo generowanymi danymi wejściowymi dla zapewnienia uniwersalności rozwiązań.