Weryfikacja autentyczności stron gov.pl za pomocą aplikacji mobilnej mObywatel

Celem jest stworzenie rozwiązania, które pozwoli obywatelom na wiarygodną weryfikację stron w domenach administracji publicznej (gov.pl). W związku z rosnącą liczbą prób oszustw wykorzystujących strony stylizowane na strony rządowe i podszywanie się pod dostawów usług publicznych, potrzebna jest prosta i szybka ścieżka pozwalająca na sprawdzenie przez obywatela wiarygodności takich stron. Rozwiązanie ma umożliwić obywatelom samodzielną weryfikację stron oraz zapobieganie i zgłaszanie prób oszustw cyberprzestępców.

1. Wprowadzenie - opis organizacji, sytuacji i stanu aktualnego

Oszustwa phishingowe w Polsce coraz częściej wykorzystują strony publiczne, takie jak portale administracji rządowej, serwisy samorządowe czy platformy usług publicznych. Cyberprzestępcy tworzą fałszywe kopie tych witryn, które wyglądają niemal identycznie jak oryginały, aby wzbudzić zaufanie użytkowników. Najczęściej celem jest wyłudzenie danych logowania do usług ePUAP, Profilu Zaufanego, bankowości elektronicznej lub pozyskanie informacji osobowych, które mogą posłużyć do kradzieży tożsamości. Ataki są szczególnie skuteczne w okresach wzmożonej aktywności obywateli online, np. podczas rozliczeń podatkowych czy składania wniosków o świadczenia.

Drugim istotnym elementem jest wykorzystanie aktualnych wydarzeń i komunikatów rządowych do uwiarygodnienia oszustwa. Przykładowo, fałszywe strony mogą podszywać się pod kampanie informacyjne dotyczące dopłat, programów socjalnych czy alertów bezpieczeństwa. Cyberprzestępcy często stosują certyfikaty SSL i domeny łudząco podobne do oficjalnych, co utrudnia rozpoznanie zagrożenia. W efekcie phishing w Polsce staje się coraz bardziej zaawansowany i wymaga od użytkowników większej czujności, a od instytucji publicznych – intensyfikacji działań edukacyjnych i wdrażania mechanizmów weryfikacji autentyczności stron.

Brakuje obecnie skutecznych, powszechnie dostępnych rozwiązań, które pomagałyby obywatelom w zapobieganiu tego typu oszustwom. Choć instytucje publiczne publikują ostrzeżenia i zalecenia, są one rozproszone i często docierają do użytkowników z opóźnieniem. Nie istnieje jednolita platforma weryfikacji autentyczności stron rządowych ani proste mechanizmy, które pozwalałyby szybko sprawdzić, czy dana witryna jest oficjalna. Brak centralnych narzędzi edukacyjnych i systemów automatycznego ostrzegania sprawia, że odpowiedzialność za rozpoznanie zagrożenia spoczywa głównie na użytkowniku, który często nie posiada odpowiedniej wiedzy technicznej. To tworzy lukę, którą cyberprzestępcy wykorzystują, zwiększając skalę i skuteczność ataków phishingowych.

---

2. Wyzwanie

Stworzenie rozwiązania. Które umożliwy weryfikację autentyczności rządowych stron internetowych przy pomocy aplikacji mobilnej mObywatel. Należy zaprojektować intuicyjne narzędzie, wbudowane na stronach gov.pl w łatwo dostępnym, ale niewpływającym na użyteczność innych funkcjonalności miejscu.

Użytkownik, wykorzystując aplikację mObywatel powinien móc zweryfikować autentyczność przeglądanej strony i to, czy prezentowane informacje pochodzą z oficjalnego źródła.

3. Oczekiwany rezultat

Oczekiwanym rezultatem jest prototyp rozwiązania, pozwalający na weryfikację autentyczności strony w domenie gov.pl za pomocą aplikacji mObywatel. PRoponowany flow rozwiązania:

- Widoczny przycisk CTA do weryfikacji strony za pomocą kodu QR – w łatwo dostępnym miejscu na stronie.
- Moduł z podstawowymi informacjami weryfikującymi bezpieczeństwo serwisu
- Sprawdzenie, czy domena ma rozszerzenie .gov.
- Link do kompendium stron rządowych, zawierającego listę oficjalnych portali.
- Informacja o certyfikacie SSL (np. „Zabezpieczona połączeniem HTTPS”).
- Weryfikacja (np. jednorazowym kodem QR) poprzez zeskanowanie w aplikacji mObywatel:
- Informacja zwrotna po weryfikacji: Widoczny komunikat w aplikacji i na stronie, potwierdzający wynik weryfikacji. Scenariusz pozytywny: jasny komunikat „Strona jest zaufana” i ewentualne wskazówki do dalszego korzystania. Scenariusz negatywny: wyraźne ostrzeżenie wraz z instrukcją, co należy zrobić w przypadku potencjalnego zagrożenia

Użytkownikiem końcowym są wszyscy obywatele korzystający z aplikacji mObywatel i potrzebujący weryfikacji strony podającej się za stronę rządową.

4. Wymagania formalne

Projekt przesyłany do oceny powinien zawierać:

- szczegółowy opis i tytuł projektu,
- prezentację w formacie PDF (maksymalnie 10 slajdów),
- makiety rozwiązania, prezentujące jego użyteczność,
- film umieszczony w dostępnym, otwartym repozytorium (link), trwający maksymalnie 3 minuty i prezentujący projekt.

Dodatkowo może zawierać:

- repozytorium kodu,
- zrzuty ekranu,

- linki do demonstracji,
- materiały graficzne lub inne elementy związane z projektem.

---

5. Wymagania techniczne

- Propozycja koncepcji mechanizmu integracji
- Wykorzystanie szyfrowanej komunikacji
- Moduł powinie być lekki, niewpływający na wydajność aplikacji
- Weryfikacja QR musi generować kod jednorazowy (nonce), aby zapobiegać spoofingowi
- Rozwiązanie musi uwzględniać podstawowe zasady cyberbezpieczestwa, w tym: ograniczenie ekspozycji danych, poprawną walidacje wejścia, odporność na manipulację kodem QR oraz kluczowymi parametrami URL
- System musi identyfikować i obsługiwać przypadki błędne (np. Brak połączenia, nieprawidłowy kod QR)

6. Sposób testowania i/lub walidacji

Rozwiązanie będzie oceniane pod kątem:

- czytelności interfejsu dla użytkownika nie-technicznego,
- poprawnej integracji z aplikacją mObywatel,
- zgodności z wymogami dot. bezpieczeństwa.

W trakcie prezentacji uczestnicy powinni zaprezentować:

- scenariusz (pozytywny i negatywny) weryfikacji strony przez obywatela
- zgodność rozwiązania z
- makiety rozwiązania (lo-fi)

7. Dostępne zasoby

Uczestnicy otrzymają pakiet informacji dostępny na dedykowanym kanale discord:

- Listę oficjalnych domen i subdomen gov.pl w formacie json
- Przykładowy zbiór metadanych o certyfikatach SSL stosowanych na stronach administracji publicznej
- Sandbox z przykładowymi stronami (w tym strony symulującymi fałszywe witryny) do testów

8. Kryteria oceny

W tej części należy przedstawić kryteria oceny – powinno ich być **pięć**, z przypisanymi **wagami**, których suma wynosi 100% (nie muszą być równe).

Kryteria:

- Związek z wyzwaniem — 25%
- Wdrożeniowy potencjał rozwiązania — 25%
- Walidacja i bezpieczeństwo danych — 20%
- UX i ergonomia pracy — 15%
- Innowacyjność i prezentacja — 15%

---

9. Dodatkowe uwagi / kontekst wdrożeniowy

Najlepsze rozwiązania mogą zostać skierowane do pilotażowego wdrożenia w procesierozwoju aplikacji mObywatel. Organizator przewiduje możliwość kontynuowania prac projektowych po hackathonie.

10. Kontakt

Podczas wydarzenia dostępni będą mentorzy techniczni i merytoryczni w specjalnie oznaczonym punkcie konsultacyjnym. Dodatkowo uruchomiony zostanie kanał komunikacyjny na Discord.