mWitryna

Proszę zapoznać się z instrukcją instalacji rozszerzenia - jest krótka i zawiera również najprostszy scenariusz, w którym chroni użytkownika!

Przedstawione **działające rozwiązanie** to oparte na systemie mObywatel rozszerzenie do przeglądarek internetowych. Jest to dodatkowa warstwa zabezpieczeń przed phishingiem, tzn. podszywaniem się pod witryny rządowe.

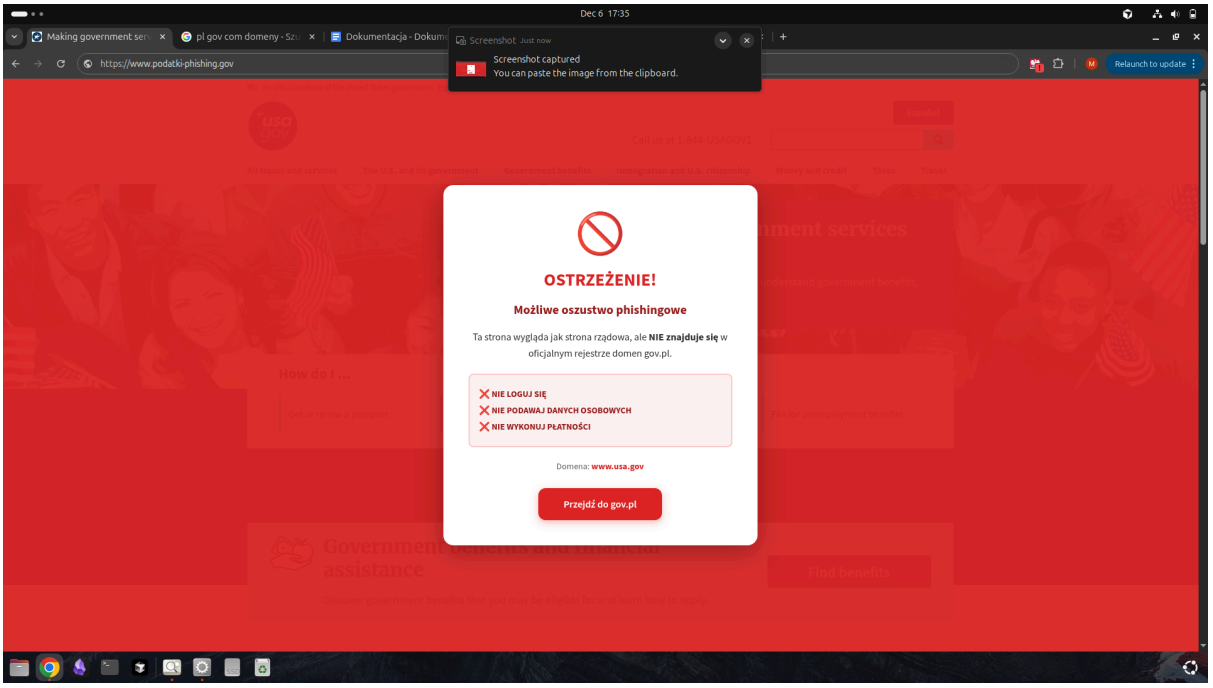
Tylko zweryfikowane domeny pokazują "zieloną ikonę" symbolizującą, że użytkownik jest na autoryzowanej witrynie.

Niebezpieczne strony pokazują bardzo widoczny dla użytkownika komunikat.

Istotną zaletą jest fakt, że nowe strony phishingowe mogą zostać dodane do rejestru i być natychmiastowo oznaczone jako niebezpieczne na komputerach lub telefonach użytkowników, gdy spróbują się z tą witryną połączyć.

Rozwiązanie weryfikuje więc bezpieczeństwo na wielu poziomach:
- certyfikat SSL
- domena jest z bezpiecznej listy - lista dostarczona przez mObywatel
- domena nie jest na liście stron niebezpiecznych

Użytkownik dostaje informację zwrotną od razu po załadowaniu się strony.
W przypadku pozytywnej weryfikacji na ikonce rozszerzenia, tzn. na Godle Polskim, pokazuje się zielony znaczek potwierdzający bezpieczeństwo.
Jeśli wykryta zostanie strona phishingowa, użytkownik powiadamiany jest widocznym komunikatem:



Mechanizm Integracji

Rozszerzenie jest gotowe do pobrania i zainstalowania. Wiekszość użytkowników czerpałaby z aplikacji korzyści już dziś.
Jest jednak kilka rzeczy, które znacząco poprawiłyby bezpieczeństwo obecnego prototypu. Umożliwiłyby one też korzystanie z aplikacji większej ilości użytkowników.

Przede wszystkim są to:
- **większa integracja z mObywatel**: pobieranie listy stron bezpiecznych z API mObywatel. Obecnie lista jest zapisana na komputerze użytkownika. Jest to rozwiązanie niebezpieczne, ponieważ taką listę można sfalsyfikować.
- **stworzenie rejestru stron niebezpiecznych.** Taki zbiór też powinien zostać udostępniony przez mObywatel. To rozwiązanie ma ogromny potencjał, bo po wykryciu strony phishingowej i dodaniu jej do rejestru, każdy użytkownik od razu byłby ostrzegany po wejściu na tę stronę.
- **rozwiązanie należy przetestować.** Testy powinny obejmować wszystkie kombinacje przeglądarek, witryn i systemów operacyjnych. Obecnie aplikacja przetestowana jest tylko na komputerach z systemem Windows oraz na MacBookach używających przeglądarki Google Chrome.
- **stworzenie rejestru zagranicznych stron rządowych** i udostępnienie go w API mObywatela. To też ma ogromny potencjał - rozwiązanie mogłoby być umożliwić bezpieczeństwo nie tylko na państwowym poziomie, ale też na poziomie np. Unii Europejskiej - sprawdzałoby wtedy oryginalność systemów innych państw członkowskich
- **instrukcję dla użytkownika**, np. przypominającą o “przypięciu” rozszerzenie w przeglądarce. Bez tego aplikacja również działa, ale nie dostarcza tak szybkiej wizualnej informacji zwrotnej. Proces instalacji jest bardzo prosty.
- **wyszarzenie ikonki**, gdy strona nie jest związana z polskimi systemami rządowymi. Dla wielu ludzi, szczególnie osób mniej na bieżąco z technologią (np. osoby starsze), czerwone godło, nawet bez zielonej ikonki, może dawać złudne poczucie bezpieczeństwa.
- **informacja o braku połączenia**: w przypadku niedostępności Internetu na ikonce widoczna powinna być szara ikona ładowania, pokazująca jasno, że mWitryna nie działa.
- **implementacja rozszerzenia dla użytkowników mobilnych**. Implementacja na urządzeniach mobilnych wychodzi naszym zdaniem poza założenia naszego projektu, ponieważ na telefonie najbezpieczniejszym sposobem jest używanie istniejącej aplikacji mObywatel. Ponadto, weryfikacja kodem QR strony mobilnej jest trudna, bo wymaga posiadania drugiego urządzenia do zeskanowania kodu.
- **weryfikacja oryginalności rozszerzenia**: pod aplikacje teoretycznie można byłoby się podszyć, umieszczając fałszywą wersję np. w Chrome Web Store. Istnieje możliwość certyfikacji rozszerzeń. Analogicznie ktoś mógłby wstawić na Sklep Play lub Apple Store fałszywą wersję aplikacji mobilnej mObywatel.
- **formularz do zgłaszania potencjalnych oszustw**: rozszerzenie po kliknięciu na ikonkę wyświetla kod QR, który użytkownik mógłby zeskanować i zgłosić do systemów powiązanych z mObywatel.

Podsumowując i technicznie mówiąc, obecne API systemu mObywatel powinno dostarczać dodatkowo:
- endpoint zwracający listę rządowych stron bezpiecznych
- endpoint zwracający rejestr stron phishingowych
- endpoint zwracający listę zagranicznych stron rządowych z domeną ".gov"., np. "www.usa.gov"
- opcjonalnie: formularz w aplikacji mObywatel, gdzie możnaby było zgłosić potencjalne oszustwo. Do tego odsyłałby kod QR widoczny po kliknięciu na ikonkę rozszerzenia na komputerze użytkownilka.

Rozwiązanie działa jednak też w obecnym stanie.

Użycie i przetestowanie aplikacji

Żeby przetestować aplikację, należy zainstalować rozszerzenie według dołączonej instrukcji.

Następnie wejść na stronę bezpieczną, np.
www.gov.pl
Na ikonce (Godle Polskim) pojawi się wtedy "zielony ptaszek" symbolizujący bezpieczeństwo.
Następnie wejść należy na stronę potencjalnie niebezpieczną. Może to być np. rządowa strona obcego państwa, np:
www.usa.gov
Strony rządowe innych krajów to obecnie wyniki fałszywie oznaczone jako niebezpieczne. Problem oznaczania zagranicznych stron rządowych jako niebezpieczne zniknąłby po zrealizowaniu planu w podpunkcie mechanizm integracji.
Nie wszystkie strony bezpieczne zostały dodane na listę na potrzeby konkursu. Np. domenę mObywatel rozszerzenie obecnie oznaczyłoby jako niebezpieczną, bo nie ma jej na konkursowej liście. Jest to więc obecnie wynik fałszywie dodatni. Ten problem zniknąłby po implementacji propozycji z rozdziału o mechanizmie integracji.

Docelowo instalacja będzie znacznie prostsza, tzn. prostsza niż zainstalowanie aplikacji mobilnej mObywatel na telefonie.

Spełnienie kryteriów:

Tworząc ten system, staraliśmy się, żeby spełnić wszystkie wymagania projektowe. Przygotowaliśmy więc listę tych wymagań z naszym komentarzem, żeby zaznaczyć, że przemyśleliśmy rozwiązanie pod każdym aspektem.

Związek z wyzwaniem

Rozszerzenie jest ściśle związane z problematyką opisaną w dostępnym PDFie. Już na tym poziomie uchroniłoby wielu użytkowników.

Zdajemy sobie sprawę z tego, że proponowane było rozwiązanie oparte na kodzie QR. Początkowo zaimplentowaliśmy to korzystając z tej propozycji. Weryfikacja kodem QR ma jednak kilka bardzo trudnych do obejścia problemów z cyberbezpieczeństwem, którym trudno zapobie:

- strona phishingująca może wyświetlić zapytanie do API mObywatela i wysłać prawidłową domenę. Przykładowo wchodząc na witrynę "phishing-podatki.gov" można byłoby przesłać do mObywatela fałszywą informację, że użytkownik znajduje się na domenie "podatki.gov".
- rozszerzenie nie może odczytać detali certyfikatu SSL. Tzn. Pierwszy problem dałoby się zlikwidować, gdyby kod QR tworzyć na podstawie i domeny, i certyfikatu SSL. Jest to jednak niemożliwe, ponieważ przeglądarka nie umożliwia odczytywania certyfikatu SSL z poziomu rozszerzenia. Sprawdzić można więć tylko to, że certyfikat jest - co jest już zaimplementowane.

Proponowane przez nas rozwiązanie jest prostsze niż takie oparte na kodzie QR. Jest dzięki temu prostsze i łatwiejsze do wprowadzenia.

Na kodzie QR oparliśmy funkcjonalność zgłaszania oszustw. Użytkownik musiałby tylko kliknąć na ikonkę rozszerzenia i zeskanować kod QR aplikacją mObywatel.

Wdrożeniowy potencjał rozwiązania

Wdrożeniowy potencjał rozwiązania jest ogromny, a pełna implementacja byłaby relatywnie bardzo łatwa. Wszystkie kroki zostały opisane w podpunkcie o mechanizmie integracji.

Walidacja i bezpieczeństwo danych

Rozwiązanie nie zakłada potrzeby dostępu do danych osobowych ani jakichkolwiek danych wrażliwych. Jest z tego powodu pod tym kątem bardzo bezpieczna.

Walidacja danych polegałaby na tym, że rozszerzenie powinno być możliwe do pobrania tylko z serwerów mObywatel. Udostępniony powinno zostać narzędzie do sprawdzania oryginalności kodu źródłowego.

Nic nie stoi na przeszkodzie, żeby rozwiązanie było open-source, tzn. żeby kod źródłowy był publicznie dostępny. Dzięki temu każdy zainteresowany ekspert mógłby ocenić bezpieczeństwo projektu.

Ux i ergonomia pracy

Proponowane rozwiązanie nie wymaga żadnych akcji od użytkownika poza instalacją. Podejście oparte na rozszerzeniu przeglądarki daje możliwość dostarczenia szybkiej informacji zwrotnej, czy strona jest bezpieczna.

Potencjalnym problem to wyniki fałszywie pozytywne. Jeśli użytkownik byłby całkowicie pewny, że witryna jest bezpieczna, powinien móc skorzystać z opcji zignorowania ostrzeżenia. Tak działają podobne, wdrożone już systemy, np. system ostrzegania w przeglądarce Google Chrome.

Innowacyjność i prezentacja

Zdajemy sobie sprawę, że rozwiązanie należy pod każdym kątem przeanalizować i przetestować. Dogłębna analiza wymaga dyskusji, więc jesteśmy w każdej chwili trwania konkursu gotowi na rozwianie wszelkich wątpliwości.

Kontakt:
+ 48 503 657 782
michal.kus0@gmail.com
mrszosiaes@gmail.com