POLSKA OBYWATELSKA
CYBEROBRONA

RAPORT

Stan bezpieczeństwa stron internetowych

Posłów Rzeczypospolitej Polskiej

Czerwiec 2020

Spis treści

Informacje o Polskiej Obywatelskiej Cyberobronie

Polska Obywatelska Cyberobrona jest społeczną inicjatywą wspierającą cyberbezpieczeństwo Rzeczypospolitej Polskiej. Zrzesza pasjonatów i ekspertów tematyki cyberbezpieczeństwa o motywacjach patriotycznych, którzy swoją wolontariacką pracą chcą się przyczynić do poprawy bezpieczeństwa Rzeczypospolitej Polskiej. Niniejszy raport jest jednym z przejawów działalności członków Stowarzyszenia.

Nazwa stowarzyszenia: Polska Obywatelska Cyberobrona

Opis stowarzyszenia: Polska Obywatelska Cyberobrona (POC) jest stowarzyszeniem powołanym w 2015 roku z inicjatywy Fundacji Bezpieczna Cyberprzestrzeń. Głównym celem Stowarzyszenia jest „podejmowanie działań na rzecz umacniania cyberbezpieczeństwa Polski, w tym utworzenie i systematyczne doskonalenie zespołu ekspertów z zakresu cyberbezpieczeństwa, gotowych służyć swoją wiedzą i umiejętnościami w sytuacji zagrożenia bezpieczeństwa cyberprzestrzeni RP, przede wszystkim na potrzeby obronności państwa”.

Dane rejestrowe: Sąd Rejonowy dla m. st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego KRS: 0000786384, NIP: 7010929391, REGON: 383563539

Adres: ul. Branickiego 13, 02-792 Warszawa

WWW: poc.org.pl

Email: team@poc.org.pl

Opis projektu

Projekt skupia się na badaniu bezpieczeństwa stron internetowych posłów Rzeczypospolitej Polskiej w dobie rosnącego znaczenia tego typu kanału komunikacji z obywatelami. Strony internetowe stanowią jeden z pierwszych wektorów ataku m.in. ze względu na ich dostępność 24 godziny na dobę, 7 dni w tygodniu. W trakcie badania skupiono się na wykryciu podatności oraz błędów konfiguracyjnych, które mogłyby zostać wykorzystane przez potencjalnych atakujących. Celem takich ataków najczęściej jest uzyskanie korzyści finansowych przez dostęp i manipulację poufnymi danymi oraz, co w przypadku badanych stron jest podstawowym zagrożeniem, publikowanie nieautoryzowanych treści, które mogą wywołać niekorzystne skutki w zakresie informowania obywateli oraz negatywnie wpływać na reputację posłów. Konkretne i najbardziej istotne scenariusze ataków przedstawione zostały w rozdziale „Potencjalne scenariusze zagrożeń".

Celem projektu jest uzyskanie informacji o poziomie bezpieczeństwa stron posłów Rzeczypospolitej Polskiej, przekazanie właścicielom stron informacji o wykrytych problemach wraz z rekomendacjami dotyczącymi możliwości poprawy stanu ich bezpieczeństwa, usunięcie wykrytych błędów oraz poinformowanie obywateli o rezultatach badania.

Inspiracją do przeprowadzenia opisanego badania była analiza bezpieczeństwa 25 stron internetowych lokalnych polityków rejonu Canberra w Australii[1] przeprowadzona w 2017 roku. W wyniku tej analizy odkryto, że ponad połowa z nich oparta była o przestarzałe oprogramowanie posiadające błędy bezpieczeństwa.

Realizacja projektu odbyła się w dwóch fazach, z których pierwsza miała miejsce przed wyborami parlamentarnymi w 2019 roku, zaś druga była uzupełnieniem badania o strony nowych posłów, którzy znaleźli się w Sejmie RP po wspomnianych wyborach. Poniższy dokument stanowi podsumowanie drugiej fazy opisanego projektu.

[1] https://www.sam.today/blog/local-politicians-meet-infosec-a-wordpress-disaster

Metodyka i zakres badań

Badanie zostało podzielone na sześć etapów, z czego większość została zrealizowana w sposób automatyczny, a wyniki zostały zweryfikowane manualnie. Polska Obywatelska Cyberobrona zdecydowała się na analizę automatyczną ze względu konieczność przebadania bardzo wielu stron. Ta metodyka zapewnia jednocześnie możliwość realizacji najbardziej efektywnej czasowo, przy zachowaniu możliwości identyfikacji najpoważniejszych zagrożeń.

Etap I – Identyfikacja stron www posłów

Pierwszy etap zakładał identyfikację adresów stron internetowych posłów z wykorzystaniem wyszukiwarki Google oraz skryptu automatyzującego wyszukiwanie. W wyniku tego etapu zostało odnalezionych 148 adresów URL, z czego jeden okazał się adresem do nieaktualnej strony jednego z posłów. Adres ten został wykryty na ostatnim etapie badania i z tego względu został on również poddany dalszej analizie. Jednak wyniki dotyczące tego adresu zostały wyłączone z niniejszego raportu.

Etap II – Wstępne skanowanie

Adresy stron internetowych zidentyfikowane podczas I etapu zostały poddane skanowaniu wstępnemu, którego celem było wykrycie rodzajów i wersji użytego oprogramowania. Na tym etapie został wykorzystany program *whatweb*[2] w wersji 0.4.9 oraz autorskie oprogramowanie agregujące wyniki. Strony zostały również poddane weryfikacji wykorzystywanego protokołu komunikacji, w tym sprawdzone zostało występowanie typowych problemów z certyfikatami TLS tj. nieprawidłowy certyfikat czy certyfikaty z własnym podpisem.

Etap III – Szczegółowe skanowanie

Etap III skupiał się na stronach internetowych opartych o system do zarządzania treścią WordPress jako najczęściej wykorzystywany CMS (Content Management System) wśród przeskanowanych stron[3]. Na tym etapie strony oparte o CMS WordPress zostały przeskanowane narzędziem *wpscan*[4] w wersji 2.9.3 w celu wyszukania błędów konfiguracyjnych oraz błędów bezpieczeństwa. Autorskie oprogramowanie zostało użyte do równoległego przeprowadzenia skanów oraz zagregowania

[2] https://github.com/urbanadventurer/WhatWeb
[3] 79 na 148 stron opartych o CMS WordPress
[4] https://github.com/wpscanteam/wpscan

wyników. Badanie, podobnie jak wszystkie inne, zostało przeprowadzone w sposób nieinwazyjny oraz niezakłócający normalnej pracy badanych stron internetowych. Samo badanie nie stanowiło żadnego zagrożenia dla bezpieczeństwa badanych stron i nie stanowiło naruszenia jakiejkolwiek z cech ich bezpieczeństwa, tj. dostępności, integralności czy poufności.

Etap IV – Weryfikacja wyników

Na tym etapie została przeprowadzona weryfikacja uzyskanych wyników wszystkich skanów i w efekcie jej przeprowadzenia zostały usunięte duplikaty oraz zidentyfikowane fałszywe wyniki.

Etap V – Przygotowanie szczegółowych raportów

Informacje o wykrytych błędach bezpieczeństwa dla każdej ze stron internetowych zostały zamieszczone w 148 indywidualnych raportach oraz jednym raporcie zbiorczym. Raporty zostały wysłane do zespołu CSIRT NASK (CERT Polska) w lutym 2020 roku, a informacja o wysłaniu raportów została przekazana do Kancelarii Sejmu. Informacja o przygotowywaniu raportu publicznego została przekazana do CERT Polska.

Etap VI – Przygotowanie publicznego raportu

Opis, przebieg i wyniki badania zostały umieszczone w niniejszym raporcie.

Klasyfikacja krytyczności

W celu określenia krytyczności zostały wydzielone kategorie błędów grupujące podatności o podobnym poziomie zagrożenia. Kategorie zostały określone na podstawie nazw podatności, które określały jednocześnie ich charakter. Podatności, których nazwa odpowiadała ogólnemu charakterowi [5] danej kategorii do niej trafiała. Podatności, których nazwy nie wskazywały na żadną z istniejących kategorii, trafiły do grupy „Inne niesklasyfikowane”. Następnie dla każdej z wydzielonych kategorii został określony poziom zagrożenia w sposób przedstawiony poniżej:

- Krytyczny
    - Zdalne wykonanie kodu
    - Możliwość wgrania oprogramowania typu backdoor[6]

[5] Nazwa podatności odpowiadała wyrażeniu regularnemu danej kategorii, np. *Authenticated.*?XSS*
[6] Tego typu oprogramowanie pozwala na zdalny, nieuprawniony i trudny do identyfikacji dostęp do strony przez atakującego

    - Wstrzyknięcie obiektu, które może prowadzić do nieuprawnionych działań na stronie internetowej
    - Nieprawidłowa deserializacja, która może prowadzić do nieuprawnionego uruchomienia programu na serwerze, na której znajduje się strona internetowa
- Wysoki
    - Możliwość nieuprawnionego przesłania plików na serwer
    - SQL Injection nie wymagający uwierzytelnienia, prowadzący do nieuprawnionego dostępu do bazy danych
    - Stored Cross-Site Scripting (XSS) nie wymagający uwierzytelnienia i prowadzący do naruszenia integralności wyświetlanej strony
    - Path Traversal, prowadzący do potencjalnego dostępu do danych znajdujących się na serwerze
    - Kilka zgrupowanych podatności
- Średni
    - Eskalacja uprawnień
    - SQL Injection wymagający uwierzytelniania
    - XSS (Cross-Site Scripting) wymagający uwierzytelnienia
    - Publiczne pliki kopii zapasowych
    - CSRF (Cross-Site Request Forgery), prowadzący do naruszenia integralności wyświetlanej strony
- Niski
    - Brak przekierowania na protokół szyfrowany (z HTTP na HTTPS), co narusza dobrą praktykę w zakresie bezpieczeństwa serwisu
    - Nazwa właściwa certyfikatu nie odpowiada nazwie domeny
    - Certyfikat przedawniony
    - Niezaufany łańcuch certyfikatów
    - Ujawnienie informacji
    - Możliwość ominięcia mechanizmu Captcha
- Niesklasyfikowany
    - Inne

Błędy, których nie można było przydzielić do żadnej z kategorii, zostały określone jako niesklasyfikowane.

Zakres badań

W ramach projektu zidentyfikowanych i przeskanowanych zostało 148 stron internetowych posłów na Sejm IX kadencji. Ta liczba odbiega od liczby posłów na Sejm RP, dlatego że część posłów nie posiada strony internetowej lub adresy ich stron nie zostały zidentyfikowane przez wykorzystane w badaniu narzędzia.

W trakcie tego badania wykrytych zostało ponad 165 unikalnych problemów bezpieczeństwa. Wiele z wykrytych błędów stanowi poważne zagrożenie dla bezpieczeństwa strony internetowej, a zarazem jej właściciela i użytkowników. Potencjalny atakujący jest w stanie w prosty sposób wykorzystać istniejące luki w oprogramowaniu, dokonać różnych zniszczeń oraz wykraść informacje nieprzeznaczone dla opinii publicznej.

Wszystkie zidentyfikowane strony www zostały poddane badaniu podstawowemu. Bardziej szczegółowej analizie zostały poddane strony internetowe oparte o system zarządzania treścią Wordpress jako najbardziej popularny CMS (Content Management System).

Spośród 148 stron przeskanowanych stron internetowych aż 96 z nich zostało zidentyfikowanych jako strony oparte o CMS.

Liczbę wykrytych systemów zarządzania treścią prezentuje poniższa tabela:

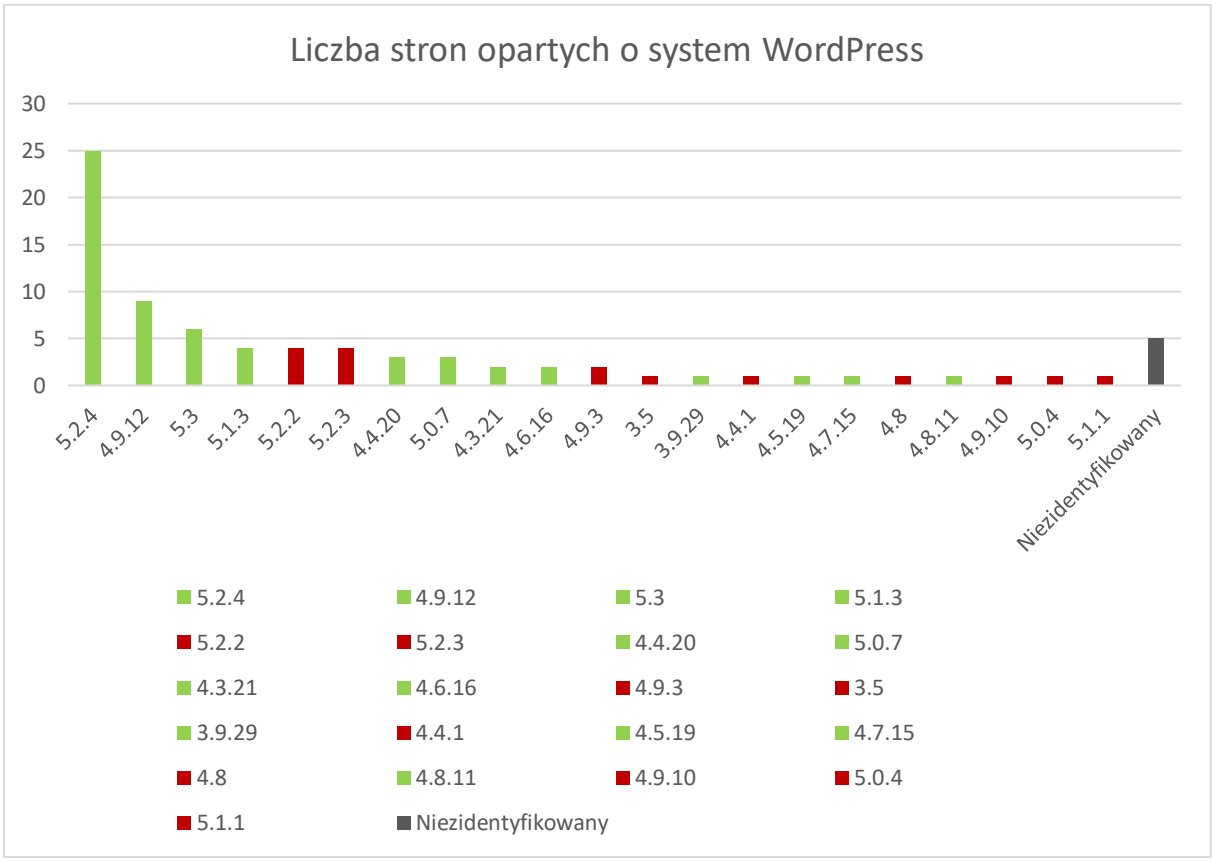
Tabela 1 Liczba stron opartych o poszczególne systemy do zarządzania treścią

Nazwa CMS	Liczba stron opartych o CMS
WordPress	79
Joomla!	10
Wix	3
Drupal	2
ProcessWire	1
Quick.Cms.Ext	1

Aktualne wersje WordPressa na dzień 3 grudnia 2019 roku wykorzystywane na analizowanych stronach:

- 5.3
- 5.2.4
- 5.1.3
- 5.0.7
- 4.9.12
- 4.8.11
- 4.7.15
- 4.6.16
- 4.5.19
- 4.4.20
- 4.3.21
- 4.2.25
- 4.1.28
- 4.0.28
- 3.9.29
- 3.8.31
- 3.7.31

Poniższy wykres prezentuje rozkład wykorzystywanych wersji systemu WordPress. Kolorem zielonym zostały oznaczone aktualne na dzień wykonania skanów wersje oprogramowania CMS, a kolorem czerwonym wersje nieaktualne. Spośród 79 stron internetowych opartych o system WordPress 16 (20%) działała na nieaktualnej wersji.



Wykres 1 Rozkład wykorzystywanych wersji systemu WordPress

Powyższy wykres może sugerować, że większość wykrytych podatności dotyczy nieaktualnych wersji wtyczek wykorzystywanych na badanych stronach internetowych.

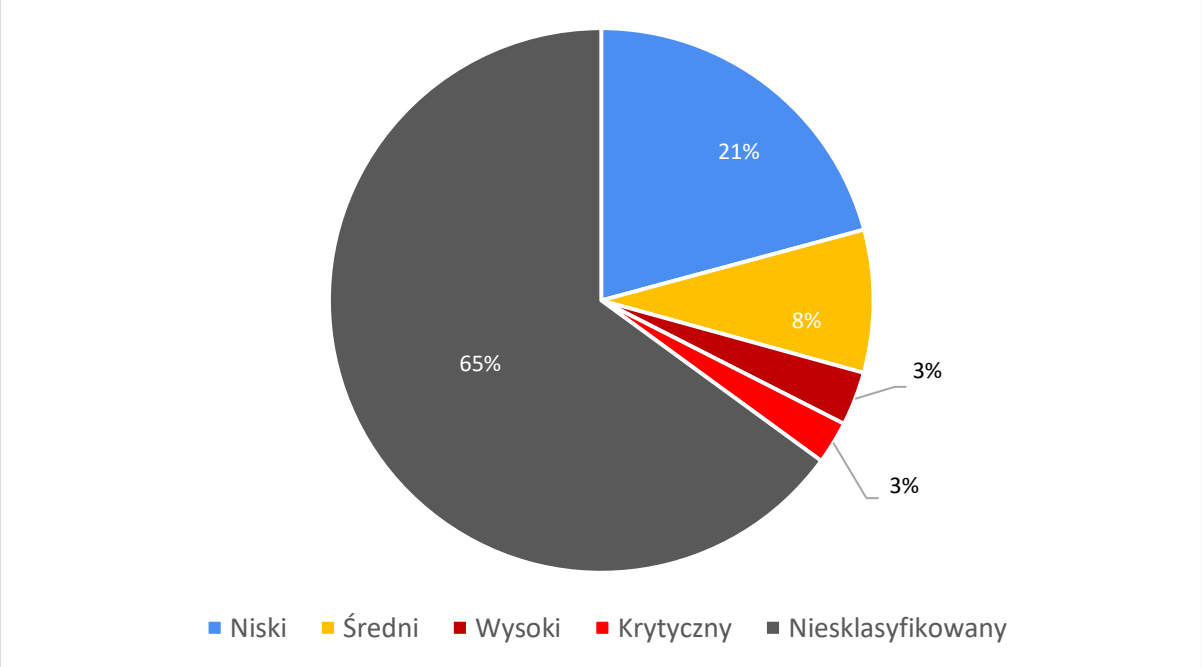
Rezultaty

W wyniku przeprowadzonego badania otrzymano wykaz błędów bezpieczeństwa znalezionych na badanych stronach internetowych. Każda z przeanalizowanych stron obarczona była przynajmniej jednym problemem dotyczącym bezpieczeństwa. Podsumowanie poziomu zagrożenia znalezionych błędów bezpieczeństwa przedstawiono na wykresie nr 2 oraz nr 3.

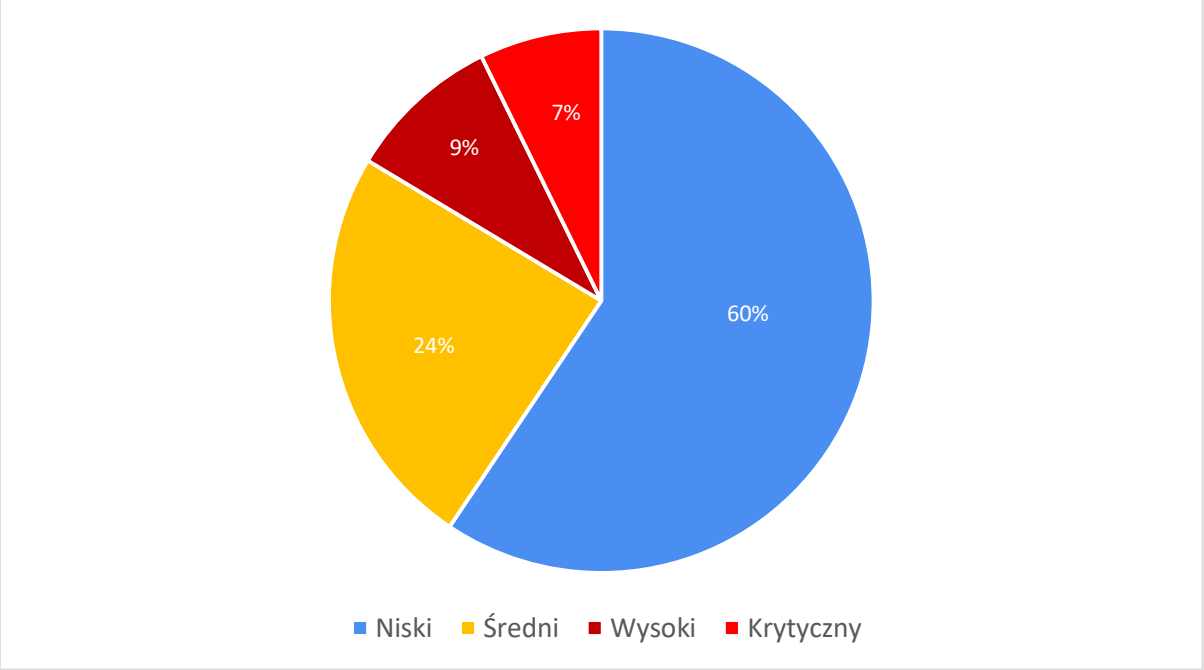
Najczęściej występujące problemy bezpieczeństwa:

- brak wymuszania komunikacji szyfrowanej z wykorzystaniem protokołu HTTPS;
- brak przekierowywania z komunikacji protokołem HTTP na komunikację szyfrowaną z wykorzystaniem protokołu HTTPS;
- brak nagłówka X-Frame-Options;
- problemy z certyfikatem SSL/TLS, w tym brak zgodności CN z nazwą hosta oraz brak zaufanego łańcucha bezpieczeństwa.

Szczegółowe zestawienie zidentyfikowanych błędów bezpieczeństwa znajduje się w załączniku do tego raportu.



Wykres 2 Podział zagrożeń pod względem poziomu krytyczności znalezionych błędów bezpieczeństwa z uwzględnieniem błędów niesklasyfikowanych



Wykres 3 Podział zagrożeń pod względem poziomu krytyczności znalezionych sklasyfikowanych błędów bezpieczeństwa

Tabela 2 Podsumowanie ilościowe znalezionych błędów w zależności od kategorii

Nazwa kategorii błędu bezpieczeństwa	Poziom zagrożenia	Liczba wystąpień błędu z kategorii
Brak przekierowania na protokół szyfrowany (z HTTP na HTTPS)	Niski	111
Nazwa właściwa certyfikatu nie odpowiada nazwie domeny	Niski	68
XSS (Cross-Site Scripting) wymagający uwierzytelnienia	Średni	46
Niezaufany łańcuch certyfikatów	Niski	29
CSRF (Cross-Site Request Forgery)	Średni	24
Możliwość przesłania złośliwych plików na serwer	Wysoki	17
Zdalne wykonanie kodu	Krytyczny	13
Wstrzyknięcie obiektu	Krytyczny	11
Path Traversal	Wysoki	11
Eskalacja uprawnień	Średni	10
SQL Injection wymagający uwierzytelniania	Średni	9
Ujawnienie informacji	Niski	6
Certyfikat przedawniony	Niski	6
SQL Injection niewymagający uwierzytelnienia	Wysoki	3
Możliwość wgrania pliku typu backdoor	Krytyczny	2
Wiele niesklasyfikowanych podatności	Wysoki	2
Nieprawidłowa deserializacja	Krytyczny	1
Stored Cross-Site Scripting (XSS) nie wymagający uwierzytelnienia	Wysoki	1
Publicznie dostępne pliki kopii zapasowych	Średni	1
Możliwość ominięcia mechanizmu Captcha	Niski	1
Inne	Niesklasyfikowany	690

Tylko jedna strona internetowa ze wszystkich przeskanowanych stron internetowych posłów posiadała nagłówek HSTS (HTTP Strict Transport Security) wymuszający łączenie się ze stroną protokołem szyfrowanym.

Podsumowanie

W wyniku przeprowadzonej analizy ustalono, że wszystkie badane strony internetowe posiadały co najmniej jeden problem dotyczący bezpieczeństwa. Spośród sklasyfikowanych błędów bezpieczeństwa 16% to błędy o wysokim lub krytycznym poziomie zagrożenia.

W procesie informowania właścicieli stron internetowych o zagrożeniu Stowarzyszenie działało zgodnie z zapisami ustawy o krajowym systemie cyberbezpieczeństwa oraz dobrymi praktykami stosowanymi przez ośrodki zajmujące się cyberbezpieczeństwem. Z informacji, jaką posiadamy, poszczególne kluby poselskie otrzymały przygotowane przez Polską Obywatelską Cyberobronę indywidualne raporty bezpieczeństwa stron internetowych posłów za pośrednictwem dedykowanego do przekazywania takich informacji zespołu CSIRT NASK. Niestety żaden z klubów poselskich nie przekazał potwierdzenia otrzymania raportów ani informacji o podjętych działaniach[7].

Występowanie błędów bezpieczeństwa na stronach osób publicznych, związanych z zarządzaniem państwem stanowi zagrożenie w postaci nieodpowiedniego dostępu i manipulacji poufnymi informacjami. Z tego powodu planowane są ponowne testy w celu weryfikacji, w jakim stopniu przeprowadzony projekt przyczynił się do poprawy bezpieczeństwa stron internetowych posłów na Sejm IX kadencji. Liczymy na to, że raport Polskiej Obywatelskiej Cyberobrony, a w szczególności informacje dotyczące natury podatności, w tym te zawarte w indywidualnych raportach, przyczynią się do poprawy sytuacji w tym ważnym aspekcie cyberbezpieczeństwa Kraju.

Potencjalne scenariusze zagrożeń

Scenariusz 1: Całkowite przejęcie kontroli nad stroną internetową

Liczba stron internetowych objętych niniejszym badaniem, w których opisany poniżej scenariusz jest możliwy: 12 (8%)

Jest to najpoważniejszy scenariusz skutkujący przejęciem kontroli nad stroną internetową, prezentowanymi treściami, bazą danych oraz systemem operacyjnym. Dzięki temu potencjalny atakujący może realizować dalsze ataki na administratorów, odwiedzających oraz infrastrukturę strony internetowej. Może on zablokować dostęp do strony internetowej, podmieniać treści czy uzyskać informację o hasłach administratorów strony internetowej.

Każdy z niżej opisanych scenariuszy jest możliwy w przypadku przejęcia kontroli nad stroną internetową.

[7] Stan na dzień publikacji raportu

Scenariusz 2: Kradzież danych

Liczba stron internetowych objętych niniejszym badaniem, w których opisany poniżej scenariusz jest możliwy: 19 (13%)

Potencjalny atakujący uzyskuje dostęp do wrażliwych informacji przechowywanych na serwerze strony internetowej. Wrażliwe informacje mogą obejmować dane osobowe odwiedzających osób kontaktujących się z posłami wraz z treścią komunikacji, przechowywane przez posła dokumenty lub także treść jeszcze nieopublikowanych komunikatów do odwiedzających strony internetowe.

Scenariusz 3: Podmiana prezentowanych treści na stronie internetowej

Liczba stron internetowych objętych niniejszym badaniem, w których opisany poniżej scenariusz jest możliwy: 34 (23%)

W tym scenariuszu potencjalny atakujący może dowolnie modyfikować, tworzyć oraz usuwać treści na stronie internetowej. Przykładem wykorzystania takich możliwości jest prezentacja poglądów politycznych włamywacza, które zostaną odebrane przez odwiedzających jako poglądy posła. Może to prowadzić do utraty dobrego imienia lub nawet utraty mandatu poselskiego, jeśli będą one obraźliwe lub będą naruszać obowiązujące regulacje prawne. Może to również prowadzić do nieporozumień, jeśli poglądy włamywacza będą uznane przez innych posłów i obywateli za poglądy tego posła.

Scenariusz 4: Infekowanie odwiedzających złośliwym oprogramowaniem

Liczba stron internetowych objętych niniejszym badaniem, w których opisany poniżej scenariusz jest możliwy: 34 (23%)

Posiadając kontrolę nad treścią strony Internetowej, potencjalny atakujący może zachęcać odwiedzających stronę internetową (w tym samego posła i osoby zarządzające stroną) do instalacji złośliwego oprogramowania. To oprogramowanie może pełnić wiele różnych funkcji, w tym między innymi:

- przejmowanie kontroli nad komputerem;
- wykradanie informacji i danych;
- szyfrowanie plików na komputerze potencjalnej ofiary i żądanie okupu za ich przywrócenie.

Załączniki

1. Lista adresów stron internetowych objętych badaniem

- adamgaweda.pl
- amularczyk.pl
- andrzejgawron.pl
- arent.olsztyn.pl
- arkadiuszmarchewka.pl
- aziewicz.pl
- bartlomiejwroblewski.pl
- baszko.pl
- dariuszwieczorek.pl
- dworczyk.pl
- ewakolodziej.pl
- gabrielalenartowicz.pl
- gadowski.pl
- gawkowski.pl
- gembickaanna.pl
- glencteresa.pl
- grabczuk.pl
- grzegorzmatusiak.pl
- grzegorzpiechowiak.pl
- ireneuszras.pl
- ireneusz-zyska.pl
- januszkowalski.pl
- jaroslaw-gonciarz.pl
- jaroslawwalesa.pl
- jaroslawzielinski.pl
- jerzymalecki.pl
- jerzypolaczek.pl
- jerzywilk.pl
- joannaborowiak.pl
- joannafabisiak.pl
- kacperplazynski.pl
- katarzynaczochara.pl
- kidawa-blonska.pl
- konradberkowicz.pl
- korwin-mikke.pl
- krystynasibinska.pl
- krzysztofkubow.pl
- kulesza.pl
- lenzgo.pl
- lisieckipawel.pl
- magdalenasroka.pl
- malgorzatachmiel.pl
- marcingwozdz.pl
- marczulajtiswalczak.pl
- marekast.pl
- marekwesoly.pl
- mariakurowska.pl
- martawcislo.pl
- mateusiak-pielucha.pl
- michaljaros.pl
- michalkrawczyk.pl
- michalwypij.pl
- mieczyslawkasprzyk.pl
- miszalski.pl
- monika-rosa.pl
- monikawielichowska.pl
- mrzyglocka.pl
- mwassermann.pl
- norbertkaczmarczyk.pl
- paslawska.pl
- paszyk.pl
- pawelpapke.pl
- pawelrychlik.pl
- pawelszramka.pl
- piotrmuller.pl
- piotruruski.pl
- plocke.pl
- robertobaz.pl
- roberttyszkiewicz.pl
- ryszard-galla.pl
- slawomirpiechota.pl
- slawomirzawislak.pl
- stanislawszwed.pl
- stanislawtyszka.pl
- szczurek-zelazko.pl
- szumilas.pl
- szymongizynski.pl
- tadeuszchrzan.pl
- telusrobert.pl
- urszula-augustyn.pl
- urszularusecka.pl
- urszula-zielinska.pl
- uscinski.pl
- wargockateresa.pl
- wojciechzubowski.pl
- www.andrzejadamczyk.pl
- www.babalski.pl
- www.boguslawsonik.pl
- www.czartoryski.pl
- www.czeslawmroczek.pl
- www.danielmilewski.pl
- www.dziedziczak.pl
- www.edwardsiarka.pl
- www.elzbietaduda.pl
- www.glogowski.pl
- www.grzegorzbraun.pl
- www.grzegorznapieralski.pl
- www.grzegorzwozniak.pl
- www.hanajczyk.pl
- www.iwonamichalek.pl
- www.jacekprotas.pl
- www.jacektomczak.pl
- www.janczyk.pl
- www.kazimierzgolojuch.pl
- www.kazimierz-moskal.pl
- www.kazimierzsmolinski.pl
- www.koperski.pl
- www.kostus.pl
- www.krzakala.pl
- www.krzysztof-lipiec.pl
- www.leonardkrasulski.pl
- www.lidiaburzynska.pl
- www.maciejmalecki.pl
- www.malgorzatagosiewska.pl
- www.marcinkulasek.pl
- www.marekbiernacki.pl
- www.karekkuchcinski.pl
- www.marekopiola.pl
- www.marekrzasa.pl
- www.marekwojcik.pl
- www.marzenamachalek.pl
- www.maslowska.pl
- www.miroslawanykiel.pl
- www.miroslawmaliszewski.pl
- www.mjanyska.pl
- www.pawelolszewski.pl

- www.piotrbabinetz.pl
- www.piotrpolak.pl
- www.pomaska.pl
- www.przemyslawdrabek.pl
- www.rosati.pl
- www.sachajko.pl
- www.sekula-szmajdzinska.pl
- www.sellin.pl
- www.siekierski.pl
- www.skowronska.info.pl
- www.tadeusztomaszewski.pl
- www.tomaszanisko.pl
- www.tomasz-nowak.pl
- www.tomaszszymanski.pl
- www.tulajew.pl
- www.tzwiefka.pl
- www.waldemarslugocki.pl
- www.wkrajewski.pl
- www.wojciech-krol.pl
- www.zientarski.pl
- zbigniewchmielowiec.pl

Ponadto, jedna z wykrytych i przeanalizowanych stron – zyw2ea.webwavecms.com – została poddana badaniu, jednak na ostatnim etapie została uznana za nieaktualną stronę posła. Wyniki dotyczące tej strony zostały wyłączone z niniejszego raportu.