Rekomendacje dotyczące bezpieczeństwa stron WWW jednostek samorządu terytorialnego

Przemek Jaroszewski, CERT Polska/NASK

Miasta w Internecie. Online, 19 listopada 2020 r.

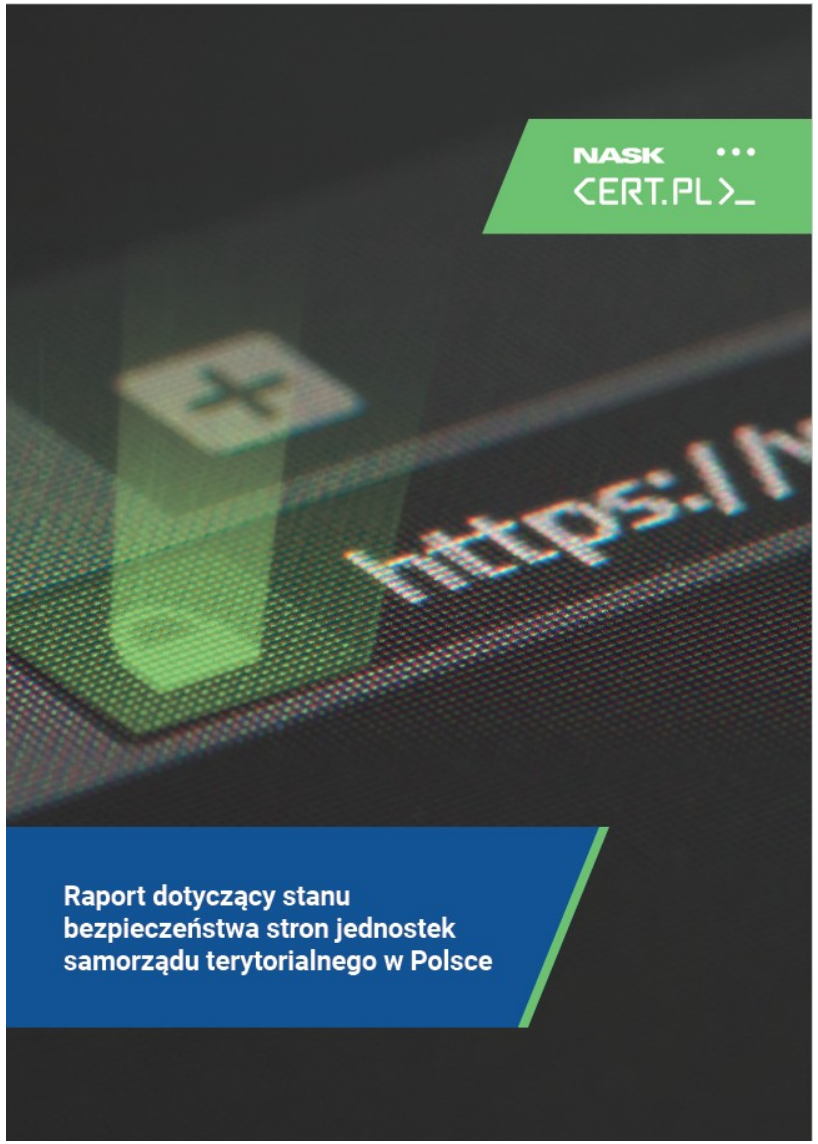
NASK CERT.PL

Kontekst

- Badanie wykonane przez CERT Polska*)

  w lutym 2020
- 2806 adresów stron internetowych z bazy

  teleadresowej JST



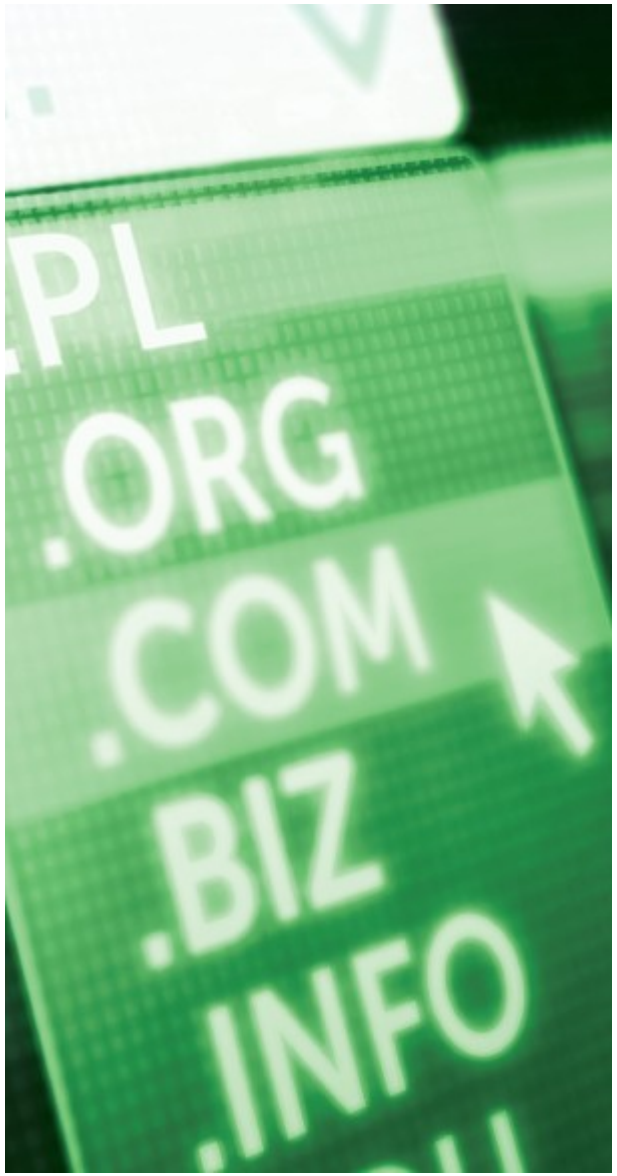
*) Badanie sfinansowane częściowo w ramach dotacji podmiotowej z części budżetu państwa, której dysponentem jest minister właściwy do spraw informatyzacji na podstawie art. 26 ust. 9 ustawy o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560)

Domeny

Administrator domeny może przekierować usługi (www, poczta) na dowolny serwer.

Niewłaściwe, nieprecyzyjne dane w rejestrze opóźniają reakcję w razie wykrytych problemów

Przejęcie domeny (np. nieprzedłużonej) prowadzi do dużych strat wizerunkowych i finansowych.



- 94,5% stron w domenie .pl, ale także:

  .eu, .com, .net, .info, .org, .cc, .biz, .tv
- **7,5%** domen nie jest zarejestrowana na urząd
- **2,5%** domen zarejestrowana na osobę prywatną

Szyfrowanie

Szyfrowanie jest wymagane gdy przetwarzane są informacje wrażliwe, np. dane osobowe, ale jest także dobrą praktyką.

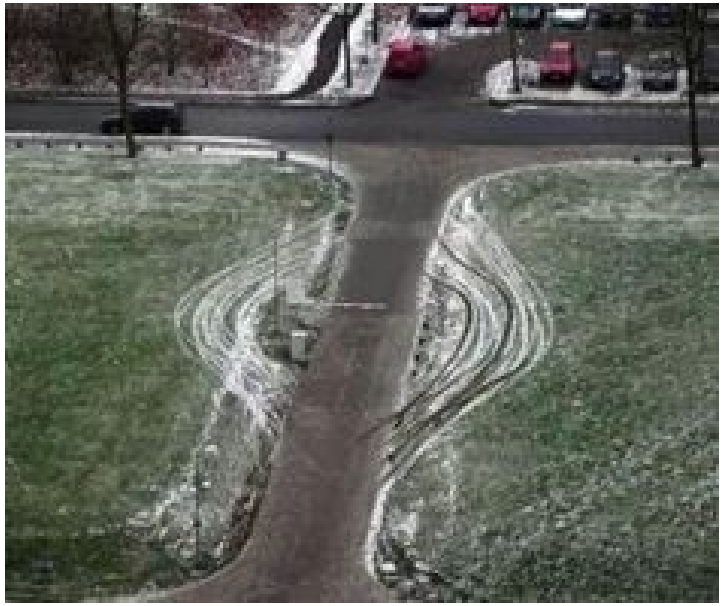
Strony niewspierające HTTPS są traktowane jako mniej zaufane i gorzej się pozycjonują.

Należy wymuszać połączenie szyfrowane przez przekierowanie użytkownika wchodzącego na stronę bez szyfrowania.

- **4,8%** stron nie używa w ogóle certyfikatów TLS
- **68%** stron używa nieprawidłowych certyfikatów TLS (przeterminowanych, wystawionych na inny podmiot, niezaufanych)
- **63%** stron wspierających szyfrowanie nie wymusza go

Separacja usług

Łączenie wielu usług (poczta, baza danych, serwer plików, RDP) na jednym serwerze ze stroną WWW znacząco zwiększa *powierzchnię ataku*. Dostęp do paneli logowania warto ograniczać do konkretnych sieci, ew. z VPN



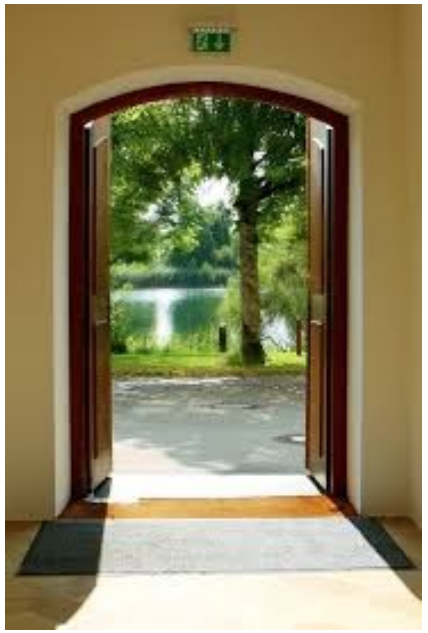
- **39%** serwerów było jednocześnie używanych do obsługi poczty
- **35%** serwerów miało udostępnioną publicznie usługę bazy danych
- **15%** serwerów udostępniało usługę SVN
- **12%** publicznie udostępnia logowanie SSH
- Niemal wszystkie strony miały publicznie dostępny panel logowania do CMS i/lub bazy danych

Aktualność oprogramowania

Oprogramowanie tworzące stronę WWW zawiera standardowe elementy (OS, serwer, często CMS). Ich podatności wykorzystywane są w atakach. Przebadaliśmy zakres wykorzystania i aktualność popularnych CMS, przede wszystkim **Joomla** i **Wordpress**.

- **33,4%** stron używa standardowego oprogramowania CMS.
- **55,7%** stron wykorzystujących Joomla lub Wordpress nie jest aktualizowana na bieżąco
- **22%** stron wykorzystających Joomla lub Wordpress posiadało błędy o średniej lub wysokiej krytyczności

Publicznie dostępne pliki

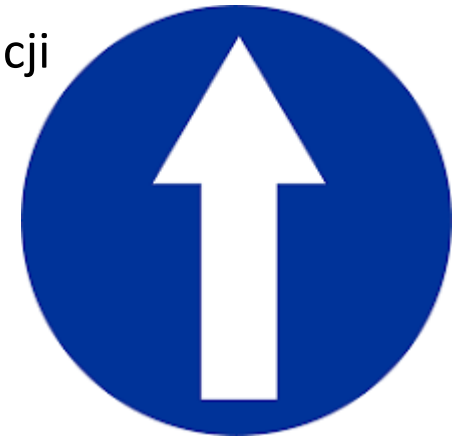


W wyniku błędnej konfiguracji część zawartości serwera bywa dostępna publicznie, bez konieczności uwierzytelnienia.

W niektórych przypadkach dostępny był anonimowy serwer plików FTP.

- 88 stron umożliwiało wyświetlenie zawartości katalogu
- **796** anonimowych serwerów FTP
- **120** publicznych plików logów
- **10** publicznych plików konfiguracyjnych z hasłami lub skrótami haseł administracyjnych
- **1** publiczne „prywatne” repozytorium git

Zalecenia



- Zidentyfikuj lub stwórz procesy dotyczące odnawiania domeny, certyfikatu, aktualizacji oprogramowania
- Zidentyfikuj osoby odpowiedzialne za te procesy
- Sprawdź poprawność danych w rejestrze
- Sprawdzaj aktualność oprogramowania, w tym systemu CMS
- Zadbaj o wsparcie dla szyfrowania – aktualny, poprawny certyfikat i brak ostrzeżeń w przeglądarce
- Przeprowadzaj okresowe testy bezpieczeństwa strony
- Dopilnuj by serwer nie udostępniał nadmiarowych usług
- Zapewnij stosowanie silnych haseł (silnego uwierzytelnienia) przez wszystkie osoby, które zarządzają stroną – polityka i jej egzekwowanie!

Pokłosie

- Tylko 4 obsłużone zgłoszenia *abuse* dotyczące skanowań.
- Raport został przekazany Ministrowi Cyfryzacji oraz pozostałym CSIRTom krajowym.
- Zidentyfikowano **23 poważne błędy**.
- Administratorów stron poinformowano także o pozostałych znalezionych podatnościach i błędach komunikacji. Większość z nich została poprawiona przed publikacją raportu.
- Wysłano łącznie **1583 maile** z informacjami i zaleceniami.

Dziękuję za uwagę!

Przemyslaw.Jaroszewski@cert.pl

info@cert.pl