

**Zadanie**  
*„Model normatywny podnoszenia kompetencji cyfrowych w szkołach wyższych”  
finansowane w ramach dotacji celowej pochodzącej ze środków Ministerstwa  
Edukacji i Nauki na podstawie Umowy Nr MEiN/2023/CTC/2625*

**Konferencja naukowa**  
**„Wzmacnianie odporności szkół wyższych  
na cyberataki przez podnoszenie kompetencji cyfrowych”**

# Narzędzia techniczne wzmacniania cyberodporności uczelni

Krzysztof Zajęc, CERT Polska



# CERT Polska

- Powołany w 1996
- Część NASK PIB (instytut badawczy & rejestrator .pl)
- jeden z 3 CSIRTów poziomu krajowego
- **Constituency:** wszystko co nie u innych

# Lista ostrzeżeń

# Co to jest?

Lista niebezpiecznych stron (phishing, oszustwa inwestycyjne).

Można skonfigurować sieć, by połączenia do stron z listy były **automatycznie blokowane**.

# Jak skorzystać?

- Na stronie lista.cert.pl można sprawdzić, czy są Państwo chronieni:

Lista  
Ostrzeżeń

CERT.PL >

Twoja sieć nie jest chroniona przez Listę Ostrzeżeń CERT Polska.

Resolver IP: 195.187.239.6

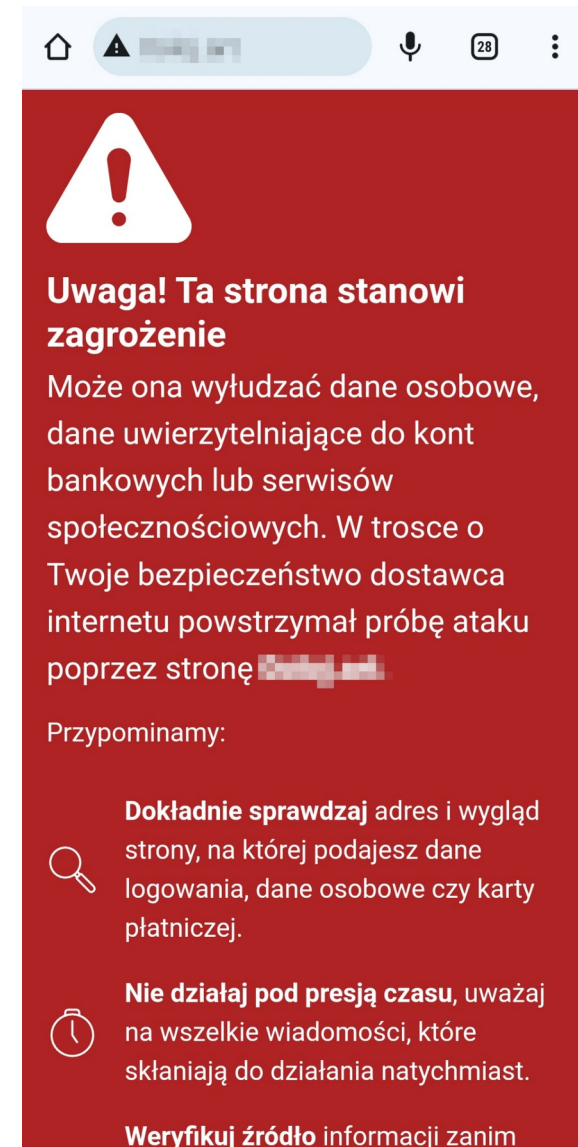
Wynik powyższego sprawdzenia może zależeć od wykorzystywanego w danym momencie sposobu połączenia z Internetem. W związku z tym, sprawdzenie należy przeprowadzić oddzielnie dla każdej wykorzystywanej sieci WiFi oraz połączenia sieci komórkowej.

CERT Polska | Więcej informacji na temat działania Listy Ostrzeżeń można znaleźć w artykule ["Lista ostrzeżeń przed niebezpiecznymi stronami"](#).

Wielu operatorów telekomunikacyjnych korzysta z listy.

# Jak skorzystać?

- Jeśli nie korzystają Państwo:  
można skonfigurować sieć, aby  
połączenia do niebezpiecznych  
stron były **blokowane**.



The screenshot shows a mobile browser interface with a red warning banner. At the top, there is a navigation bar with a home icon, a search bar containing "Biblioteka", a microphone icon, a notification icon with "28", and a menu icon. The warning banner features a white exclamation mark icon on a red background. The text in the banner reads: "Uwaga! Ta strona stanowi zagrożenie. Może ona wyłudzać dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych. W trosce o Twoje bezpieczeństwo dostawca internetu powstrzyma próbę ataku poprzez stronę [redacted]. Przypominamy: Dokładnie sprawdzaj adres i wygląd strony, na której podajesz dane logowania, dane osobowe czy karty płatniczej. Nie działaj pod presją czasu, uważaj na wszelkie wiadomości, które skłaniają do działania natychmiast. Weryfikuj źródło informacji zanim".

# Jak skorzystać?

Zachęcamy do zgłaszania:

- Podejrzanych stron pod adresem **incydent.cert.pl**,
- Podejrzanych SMSów na numer **8080**.

Ochronią Państwo w ten sposób innych!

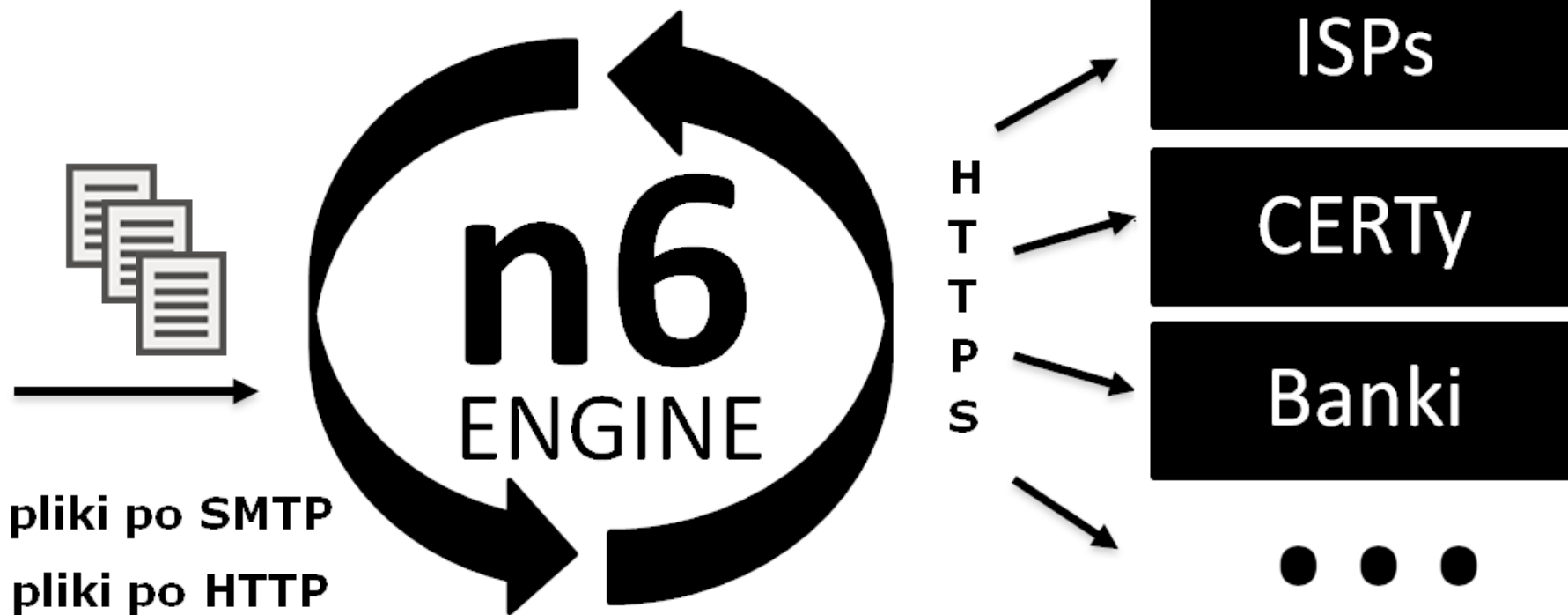
(a więc warto zachęcić rodzinę/znajomych do zgłaszania)

n6



## Security Data Providers

- URLe
- Domeny
- Adresy IP
- Malware
- Inne dane



<https://cert.pl/n6>



Zagrożenia wewnątrz sieci

Inne zagrożenia

Zdarzenia

Kolumny ▾

Eksportuj ▾

Data początkowa

10-09-2023



00:00

+ Dodaj filtr

Szukaj



| Czas zdarzenia ▲    | Kategoria ▲ | Nazwa ▲     | IP ▲           | ASN ▲  | Kraj ▲ | Domena ▲          | Źródło ▲     |
|---------------------|-------------|-------------|----------------|--------|--------|-------------------|--------------|
| 2023-09-11 10:39:15 | cnc         | lokibot     |                |        |        | kbfvzoboss.bid    | cert-pl.mwdb |
| 2023-09-11 10:39:15 | cnc         | lokibot     | 72.26.218.86   | 32475  | NL     | alphastand.win    | cert-pl.mwdb |
| 2023-09-11 10:39:15 | cnc         | lokibot     | 63.251.235.76  | 32475  | US     | alphastand.top    | cert-pl.mwdb |
| 2023-09-11 10:39:15 | cnc         | lokibot     | 141.98.6.249   | 211252 | NL     |                   | cert-pl.mwdb |
| 2023-09-11 10:39:15 | cnc         | lokibot     | 34.98.99.30    | 396982 | US     | alphastand.trade  | cert-pl.mwdb |
| 2023-09-11 10:31:43 | cnc         | smokeloader | 63.251.235.76  | 32475  | US     | somatoka51hub.net | cert-pl.mwdb |
| 2023-09-11 10:31:43 | cnc         | smokeloader | 91.195.240.101 | 47846  | DE     | sorytlic4.net     | cert-pl.mwdb |
| 2023-09-11 10:31:43 | cnc         | smokeloader |                |        |        | nuljjnuli.org     | cert-pl.mwdb |
| 2023-09-11 10:31:43 | cnc         | smokeloader | 91.195.240.101 | 47846  | DE     | bulimu55t.net     | cert-pl.mwdb |
| 2023-09-11 10:31:43 | cnc         | smokeloader |                |        |        | newzelandd66.org  | cert-pl.mwdb |
| 2023-09-11 10:31:43 | cnc         | smokeloader | 72.26.218.86   | 32475  | NL     | novanosa5org.org  | cert-pl.mwdb |
| 2023-09-11 10:31:43 | cnc         | smokeloader |                |        |        | hujukui3.net      | cert-pl.mwdb |

# Jak skorzystać z n6?

- Dostęp jest **darmowy**
- Wymóg to posiadanie fragmentu **własnej adresacji IP** - wymagany wpis we whois
- Formularz rejestracyjny: **[n6portal.cert.pl/sign-up](https://n6portal.cert.pl/sign-up)**
- Możliwość korzystania z interfejsu przeglądarkowego oraz przez API
- Open Source: **[github.com/CERT-Polska/n6](https://github.com/CERT-Polska/n6)**

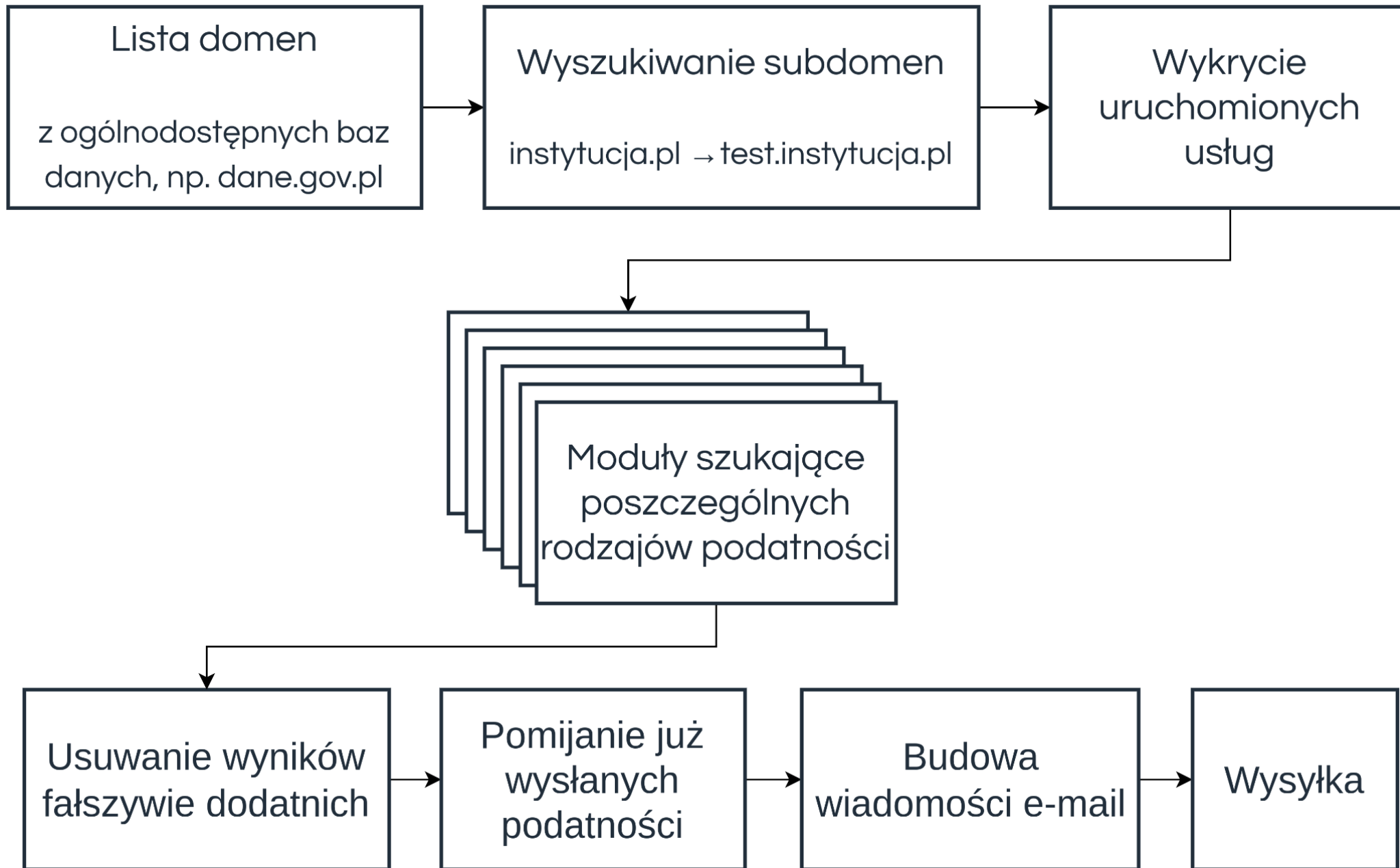
# projekt Artemis

# Projekt Artemis


Badanie bezpieczeństwa systemów m. in.:

- szkół,
- szpitali,
- instytutów badawczych,
- **uczelni**, instytucji publicznych (np. urzędów gmin),
- instytucji w domenie gov.pl.

Zwiększanie bezpieczeństwa tych systemów przez zgłaszanie administratorom znalezionych podatności.



# Kilkadziesiąt modułów

- Pełne wsparcie dla  nuclei → >10 tys. podatności i błędów konfiguracji
- Skaner portów
- Aktualność WordPressa (i wtyczek), Drupala i Joomla
- SQLi i XSS
- Certyfikaty TLS, przekierowanie na https
- SPF/DMARC
- Directory listing
- Słabe hasła
- Repozytoria (Git, SVN) i pozostawione pliki (np. wp-config.php.bak)
- ...

# Wyciek danych studentów, pracowników i współpracowników Uniwersytetu Warszawskiego

Adam Haertle dodał 18 listopada 2020 o 16:06 w kategorii [Info](#), [Prywatność](#) z tagami: [Git](#) • [MIMUW](#) • [Uniwersytet Warszawski](#) • [WPiA](#) • [wyciek](#)



# Artemis jest Open Source

**<https://github.com/CERT-Polska/Artemis/>**

**<https://github.com/CERT-Polska/Artemis-modules-extra/>**

Nie wszystkie moduły są publiczne.

Możemy je Państwu udostępnić.

# Skanowanie uczelni

Skonowanie trwa **od początku stycznia**.

Dotychczas przeskanowano **890** domen i adresów IP uczelni i dodatkowo ok. **84.4 tys.** subdomen.

# Zgłoszone podatności i błędne konfiguracje: styczeń-listopad 2023

**łącznie: ok. 160  
tys.**

**uczelnie: ok. 41 tys.**

# Statystyki

ok. 20.6 tys. przypadków korzystania z nieaktualnego oprogramowania,

ok. 9 tys. problemów z konfiguracją SSL/TLS,

ok. 4.4 tys. przypadków gdy panel logowania (bazy danych, RDP itp.) był publicznie dostępny,

ok. 3.3 tys. przypadków upublicznionych informacji: konfiguracji serwera, listy domen, indeks katalogu.

# Statystyki

ok. 1.5 tys. błędnie skonfigurowanych SPF/DMARC,

ok. 1.1 tys. konkretnych krytycznych lub poważnych podatności:

zdalne wykonanie kodu, SQL Injection itp.,

926 przypadków upublicznienia kopii zapasowych,

kodu źródłowego, zrzutów bazy danych czy logów.

# Jak skorzystać?

Zgłosić swoje domeny pod adresem:

**<https://incydent.cert.pl/skanowanie>**

Sprawdzamy główne domeny uczelni i ich subdomeny - ale może mają Państwo też inne?

Więcej informacji: [artemis@cert.pl](mailto:artemis@cert.pl)

# Formularz wyłącznie dla uczestników spotkania

Prosimy o wypełnienie poniższego formularza

Pełna nazwa instytucji

Domeny do skanowania (po jednej w każdym wierszu)

Adresy e-mail na które mają być wysłane powiadomienia (po jednym w każdym wierszu)

**[incydent.cert.pl/skanowanie](https://incydent.cert.pl/skanowanie)**

# Wnioski ze skanowania



# Wnioski ze skanowania: aktualizacje

Wykrycie nieaktualnego oprogramowania jest proste.

Istnieją gotowe exploity.

# Wnioski ze skanowania: archiwalne strony

Łatwo znaleźć archiwalne strony, które:

- korzystają z nieaktualnego oprogramowania (a więc zawierają znane podatności),
- są zbudowane bez zachowania dobrych praktyk

programistycznych:

```
query("SELECT * FROM posts WHERE id = " . $_GET["id"])
```

# Wnioski ze skanowania: **centralizacja usług**

Najważniejszy wniosek!

Jeśli na każdą konferencję jest stawiana oddzielna instancja WordPress, to:

- mniej zasobów (czas + pieniądze) można przeznaczyć na zabezpieczenia,
- łatwiej o niej zapomnieć.

# Bezpieczna Poczta

# Wiadomość

Skrzynka odbiorcza



**Powiadomienie**

2021-06-15 8:11

[ukryj](#)

od "Admin" <poczta@sej.pl>



SPF, DKIM, DMARC...

# bezpiecznapoczta.cert.pl

CERT.PL >

Bezpieczna poczta

**BETA** Jeśli masz uwagi lub komentarze, skontaktuj się z nami pod adresem [bezpiecznapoczta@cert.pl](mailto:bezpiecznapoczta@cert.pl).

## Bezpieczna poczta

Narzędzie [bezpiecznapoczta.cert.pl](https://bezpiecznapoczta.cert.pl) powstało, by chronić użytkowników poczty elektronicznej i ułatwić instytucjom sprawdzenie poprawności konfiguracji mechanizmów zapewniających jej bezpieczeństwo.

Główne funkcjonujące dziś instrumenty weryfikacji nadawcy poczty to: **SPF**, **DMARC** i **DKIM**. Jeżeli instytucja ich nie wykorzystuje, naraża się na znaczące ryzyko. Daje bowiem cyberprzestępcom możliwość wysyłania fałszywych wiadomości, w których mogą oni podszyć się pod dowolnego nadawcę z domeny tego podmiotu. Właśnie dlatego niektórzy dostawcy poczty traktują e-maile przychodzące z domen niewykorzystujących tych mechanizmów jako spam.

Chcesz sprawdzić, czy atakujący mogą łatwo podszyć się pod nadawcę w Twojej domenie? Udostępnione tu narzędzie w tym pomoże.

## Wymagania prawne

Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej nakłada na dostawców poczty elektronicznej obowiązek stosowania mechanizmów SPF, DMARC i DKIM, umożliwiających weryfikację nadawcy wiadomości e-mail. Zapisy te dotyczą dostawców poczty, którzy świadczą usługi dla:

- co najmniej 500 000 użytkowników poczty lub
- dla podmiotu publicznego.

Pełny tekst ustawy znajduje się pod adresem <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230001703/T/D20231703L.pdf>.

Chcesz sprawdzić, czy realizujesz poprawnie obowiązek ustawowy? Udostępnione tu narzędzie w tym pomoże.

## Sprawdź konfigurację wysyłając wiadomość e-mail

Gdy wyślesz testową wiadomość e-mail na specjalny adres, system zweryfikuje poprawność konfiguracji mechanizmów **SPF**, **DKIM** i **DMARC**.

**Ta ścieżka jest przez nas rekomendowana – dzięki niej będziemy w stanie wykonać dokładniejsze sprawdzenie, niż korzystając z domeny.**

Wyślij e-mail

## Sprawdź konfigurację podając domenę

Możesz skorzystać także z opcji weryfikacji konfiguracji podając domenę. W tym wypadku zostaną sprawdzone tylko mechanizmy **SPF** i **DMARC** - dla sprawdzenia DKIM konieczne jest wystanie testowego e-maila.

Podaj domenę

## Sprawdź wysyłając e-mail

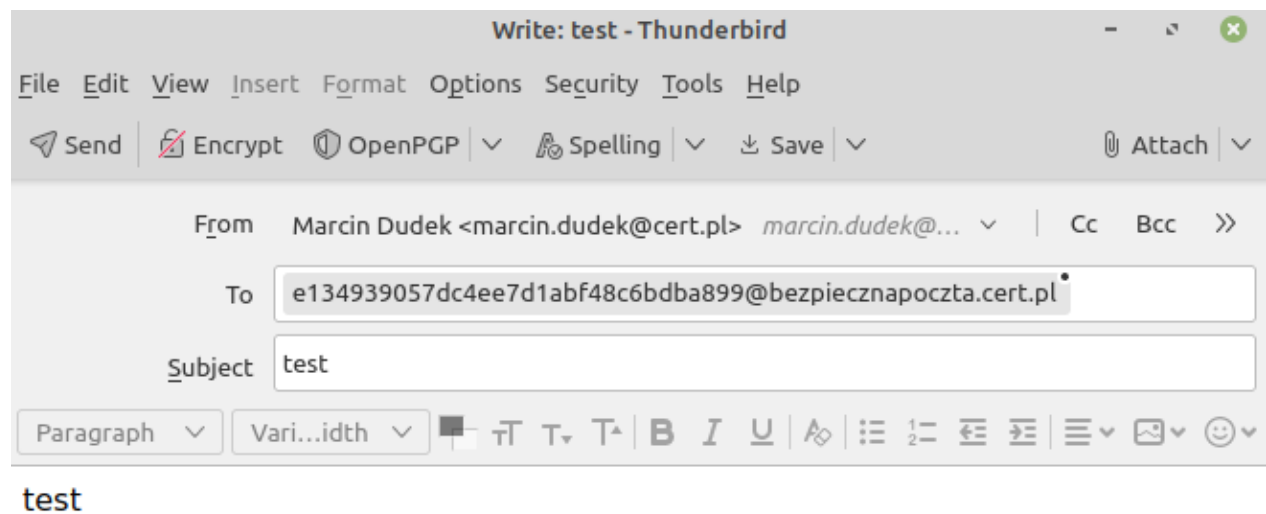
Aby zweryfikować konfigurację poczty, wyślij dowolną wiadomość e-mail na adres:

e134939057dc4ee7d1abf48c6bdba899@bezpiecznapoczta.cert.pl

Jeśli wiadomość zostanie odebrana, strona odświeży się automatycznie - zobaczysz wtedy wyniki sprawdzenia mechanizmów zabezpieczeń.

Jeśli po dłuższym czasie nie widzisz wyników, to znaczy, że nie otrzymaliśmy wiadomości. W takiej sytuacji:

- upewnij się, że wysyłasz wiadomość na poprawny adres,
- jeśli administrujesz serwerem pocztowym, sprawdź czy Twój serwer pocztowy poprawnie wysłał wiadomość,
- jeśli powyższe nie rozwiązało problemu, skontaktuj się z [bezpiecznapoczta@cert.pl](mailto:bezpiecznapoczta@cert.pl).





# domena cert.pl - wyniki testów mechanizmów zabezpieczeń poczty e-mail: SPF, DMARC i DKIM

Data sprawdzenia: 2023-09-11 11:18:15 (wiadomość e-mail z 2023-09-11 11:18:13).

Jeśli chcą Państwo udostępnić wyniki sprawdzenia, prosimy skopiować ten link:

<https://bezpiecznapoczta.cert.pl/check-results/da1162f788fe7de8e64ce242292378e342d6f909ed57145323660c860ef0e809>

✓ Podsumowanie sprawdzenia: 3 mechanizmy z 3 skonfigurowane prawidłowo.

## ✓ SPF: konfiguracja prawidłowa

|             |                                  |
|-------------|----------------------------------|
| Rekord      | v=spf1 include:_spf.cert.pl -all |
| Ostrzeżenia | brak                             |
| Błędy       | brak                             |

## ✓ DMARC: konfiguracja prawidłowa

|             |  |
|-------------|--|
| Rekord      | v=DMARC1; p=reject; rua=mailto:dmarc-cert@cert.pl; ruf=mailto:security@cert.pl; fo=s |
| Ostrzeżenia | brak   |
| Błędy       | brak   |

## ✓ DKIM: konfiguracja prawidłowa

|             |      |
|-------------|------|
| Ostrzeżenia | brak |
| Błędy       | brak |

## domena [redacted] - wyniki testów mechanizmów zabezpieczeń poczty e-mail: SPF, DMARC i DKIM

Data sprawdzenia: 2023-09-11 11:20:49 (wiadomość e-mail z 2023-09-11 11:20:48).

Jeśli chcą Państwo udostępnić wyniki sprawdzenia, prosimy skopiować ten link:

[https://bezpiecznapoczta.cert.pl/check-results/\[redacted\]](https://bezpiecznapoczta.cert.pl/check-results/[redacted])



✘ Podsumowanie sprawdzenia: 0 mechanizmów z 3 skonfigurowane prawidłowo.

### ✘ SPF: konfiguracja nieprawidłowa

Ostrzeżenia

brak

Błędy

Nie znaleziono poprawnego rekordu SPF. Rekomendujemy używanie wszystkich trzech mechanizmów: SPF, DKIM i DMARC, aby zmniejszyć szansę, że sfalszowana wiadomość zostanie zaakceptowana przez serwer odbiorcy.

### ✘ DMARC: konfiguracja nieprawidłowa

Ostrzeżenia

brak

Błędy

Nie znaleziono poprawnego rekordu DMARC. Rekomendujemy używanie wszystkich trzech mechanizmów: SPF, DKIM i DMARC, aby zmniejszyć szansę, że sfalszowana wiadomość zostanie zaakceptowana przez serwer odbiorcy.

### ✘ DKIM: konfiguracja nieprawidłowa

Ostrzeżenia

brak

Błędy

Nie znaleziono podpisu DKIM. Rekomendujemy używanie wszystkich trzech mechanizmów: SPF, DKIM i DMARC, aby zmniejszyć szansę, że sfalszowana wiadomość zostanie zaakceptowana przez serwer odbiorcy.

# Jak skorzystać?

- Wejść na stronę **bezpiecznapoczta.cert.pl**,
  - wysłać testowego maila (lub sprawdzić domenę),
  - przeanalizować wyniki, ewentualnie poprawić konfigurację.
- 
- uwagi i pytania → [bezpiecznapoczta@cert.pl](mailto:bezpiecznapoczta@cert.pl)

# Informacje o zagrożeniach i podatnościach

# Informacje o zagrożeniach i podatnościach

**<https://www.facebook.com/CERT.Polska>**

**[https://twitter.com/CERT\\_Polska](https://twitter.com/CERT_Polska)**

**<https://pl.linkedin.com/showcase/cert-polska/>**

Dziękuję za uwagę!

[info@cert.pl](mailto:info@cert.pl)