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 Zając, 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

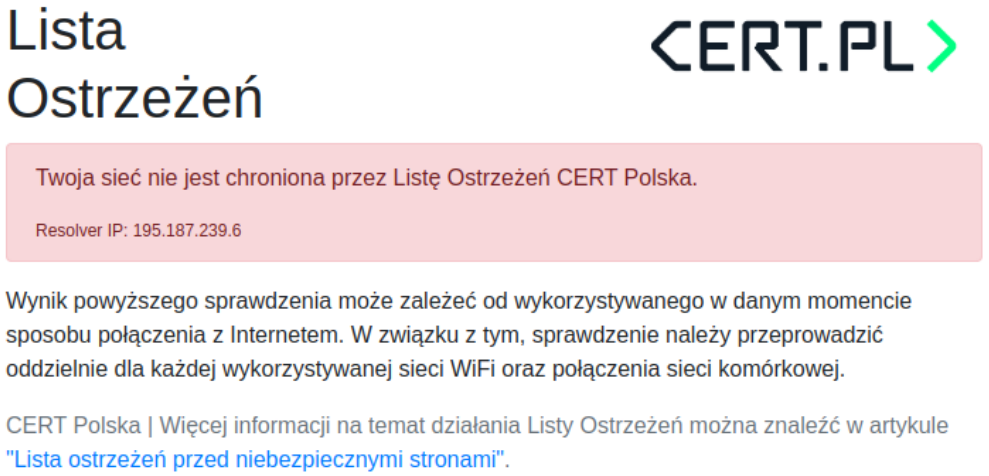
Co to jest?

Lista niebezpiecznych stron (phishing, oszustwa inwestycyjne).

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

Jak skorzystać?

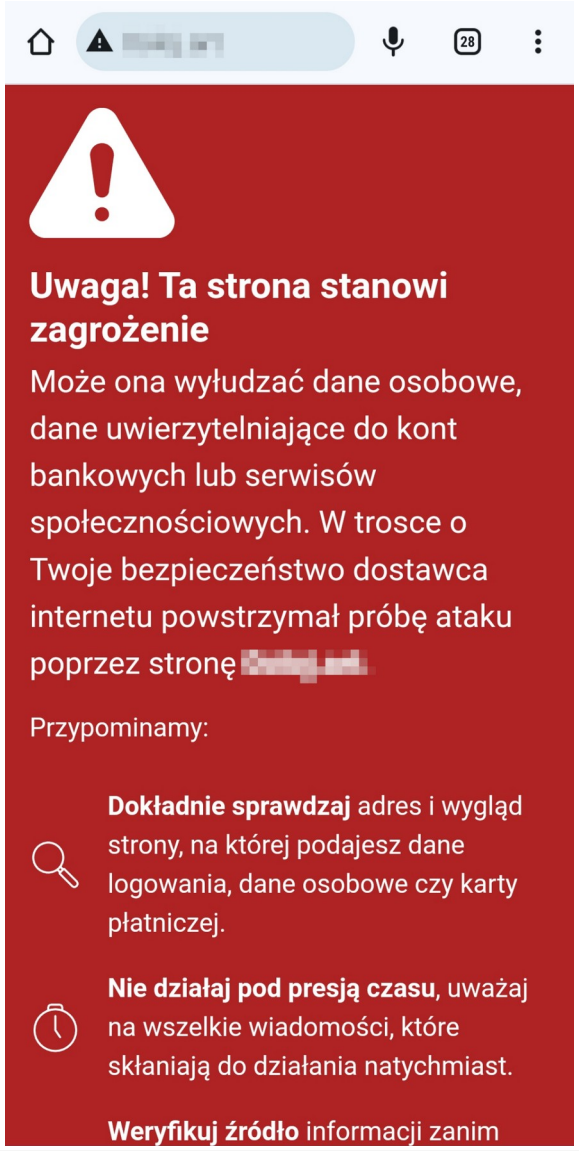
- Na stronie lista.cert.pl można sprawdzić, czy są Państwo chronieni:



Wielu operatorów telekomunikacyjnych korzysta z listy.

Jak skorzystać?

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



Jak skorzystać?

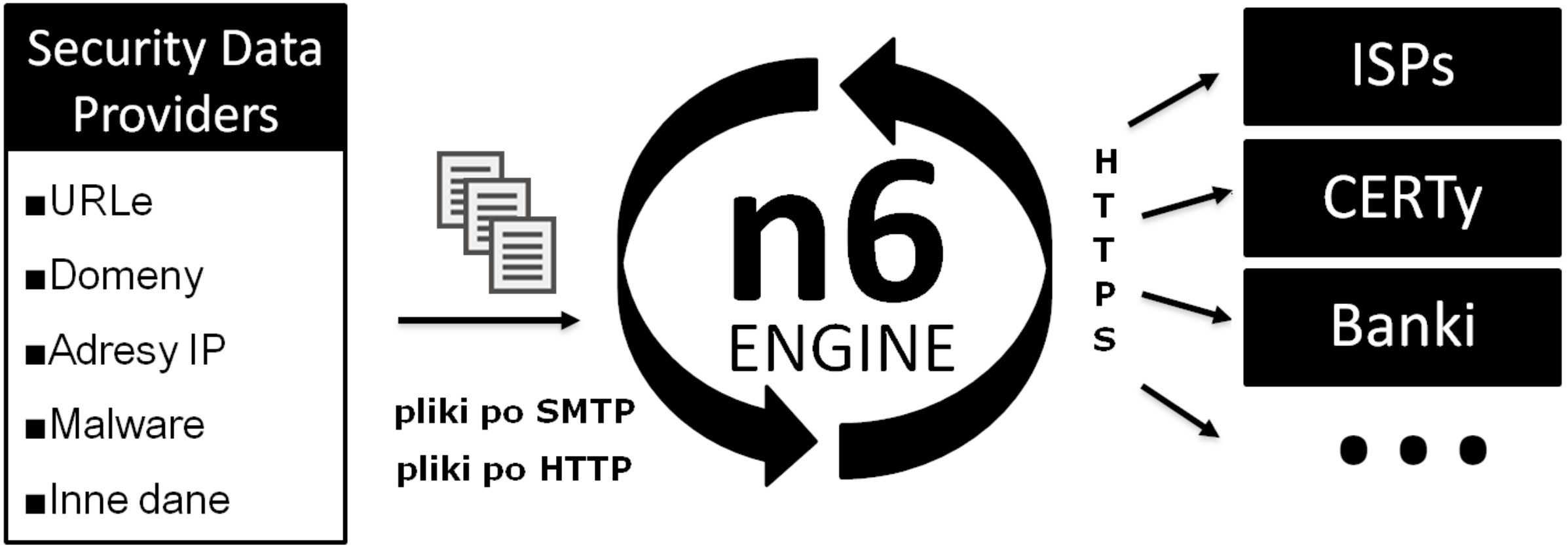
Zachęcamy do zgłaszania:

- 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



https://cert.pl/n6

Portal

Organizacja Incydenty Baza wiedzy

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	soryytlic4.net	cert-pl.mwdb
2023-09-11 10:31:43	cnc	smokeloader				nuljjjnuli.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				newzelannd66.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**
- Możliwość korzystania z interfejsu przeglądarkowego oraz przez API
- Open Source: **github.com/CERT-Polska/n6**

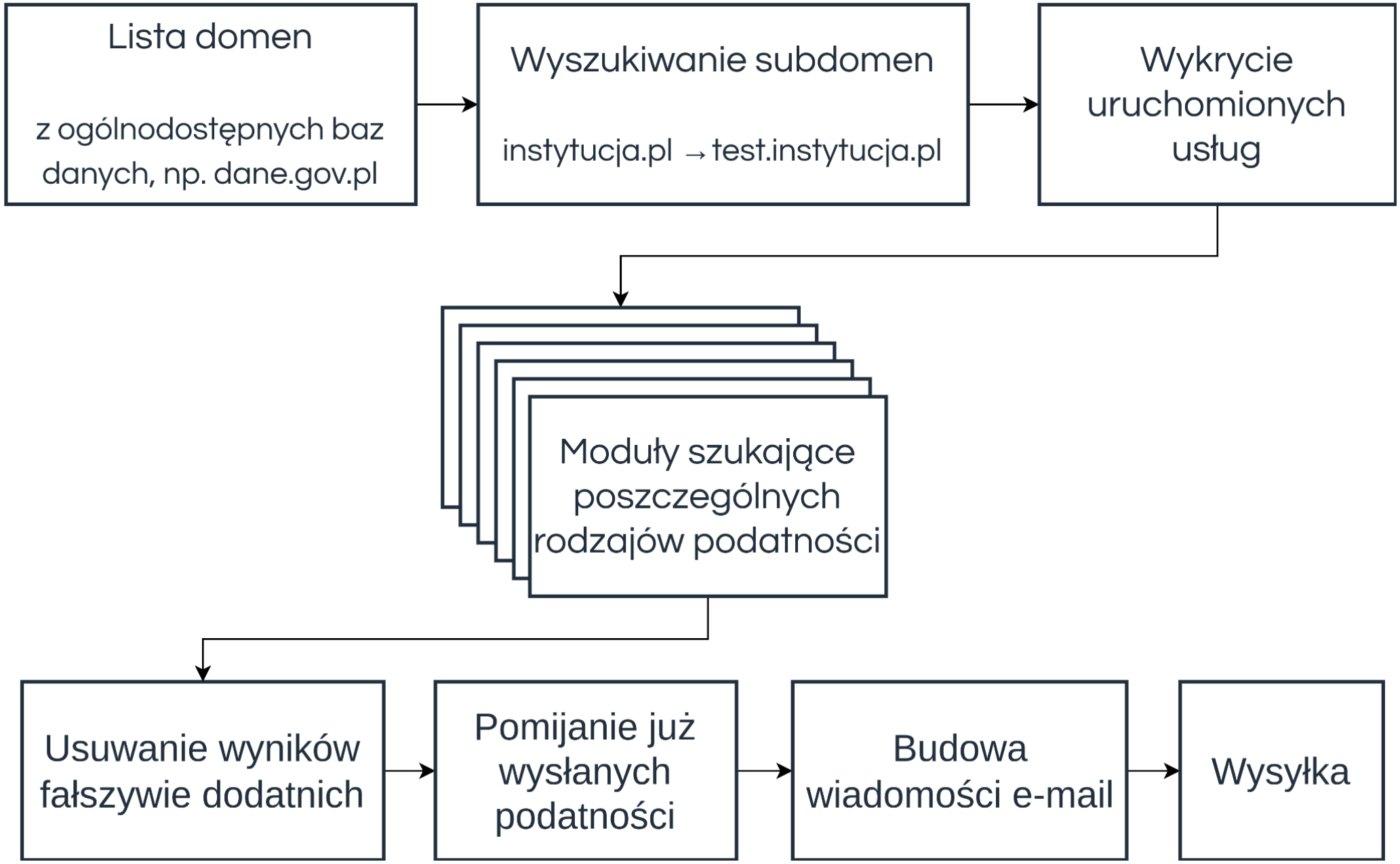
projekt Artemis

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.


Lista domen
z ogólnodostępnych baz danych, np. dane.gov.pl
Wyszukiwanie subdomen
instytucja.pl → test.instytucja.pl
Wykrycie uruchomionych usług
Moduły szukające poszczególnych rodzajów podatności
Usuwanie wyników fałszywie dodatnich
Pomijanie już wysłanych podatności
Budowa wiadomości e-mail
Wysyłka

Kilkadziesiąt modułów

- Pełne wsparcie dla 

>10 tys. podatności i błędów konfiguracji
- Skaner portów
- Aktualność WordPressa (i wtyczek), Drupala i Joomli
- 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

Skanowanie 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?

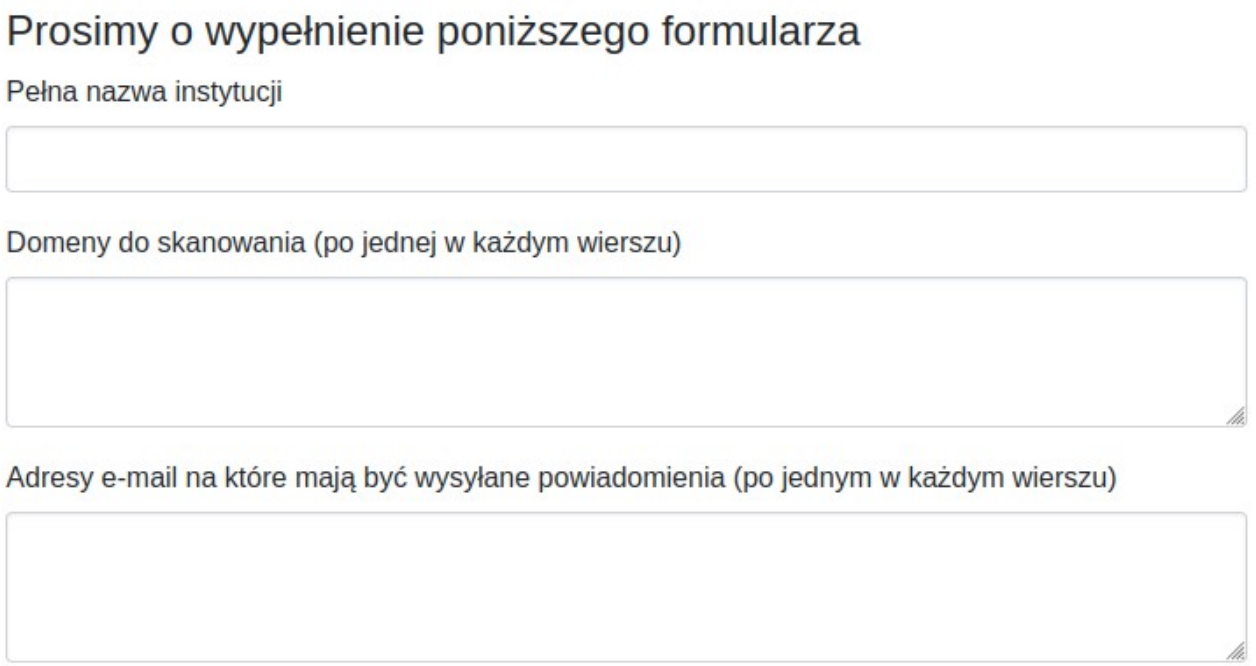
Zgłosić swoje domeny pod adresem:

https://incydent.cert.pl/skanowanie

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

Więcej informacji: artemis@cert.pl

Formularz wyłącznie dla uczestników spotkania



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:

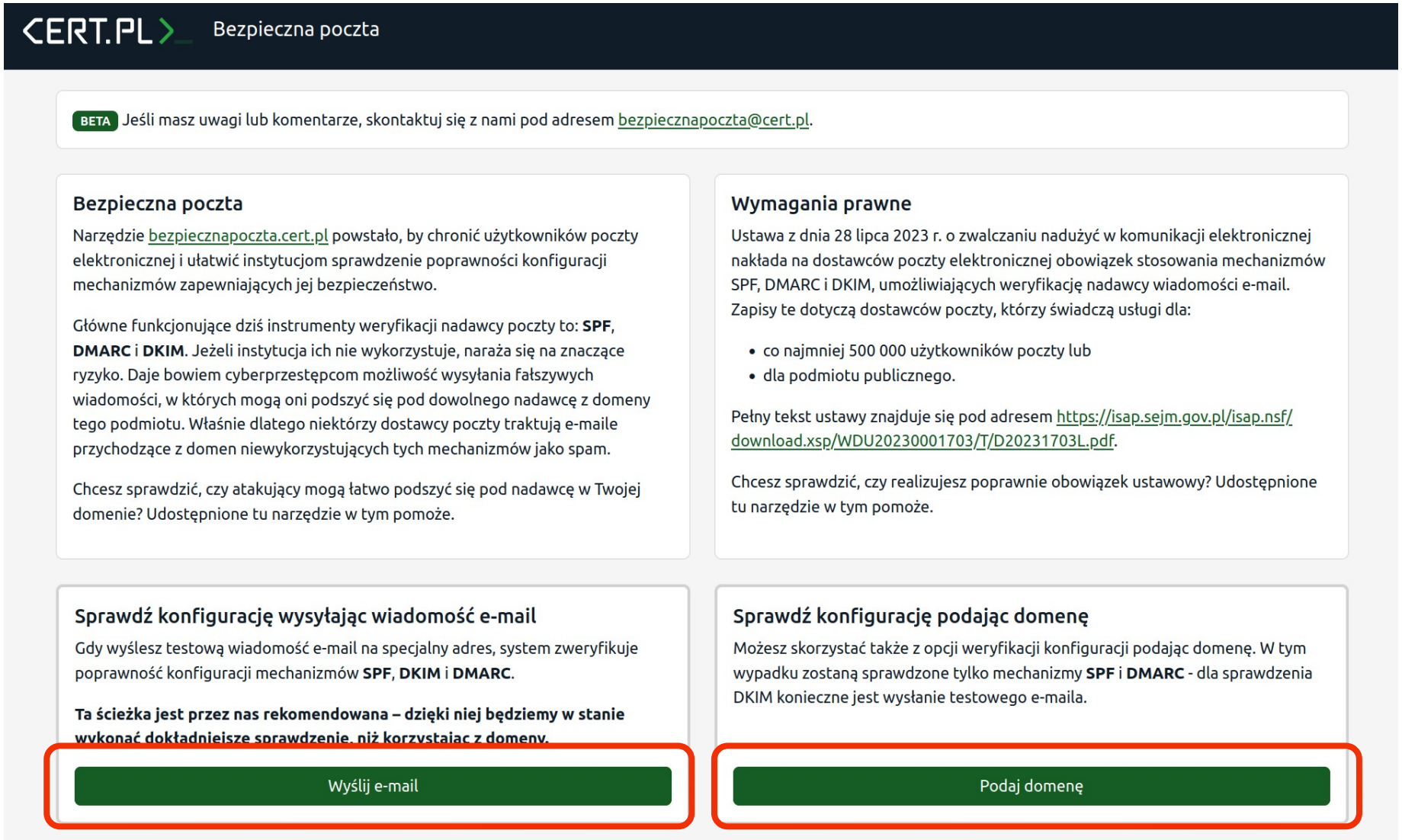
- mniej zasobów (czas + pieniądze) można przeznaczyć na zabezpieczenia,
- łatwiej o niej zapomnieć.

Bezpieczna Poczta


Wiadomość
Skrzynka odbiorcza
Powiadomienie
2021-06-15 8:11
ukryj
od "Admin" <poczta@sej.pl>

SPF, DKIM, DMARC…

bezpiecznapoczta.cert.pl



Sprawdź wysyłając e-mail

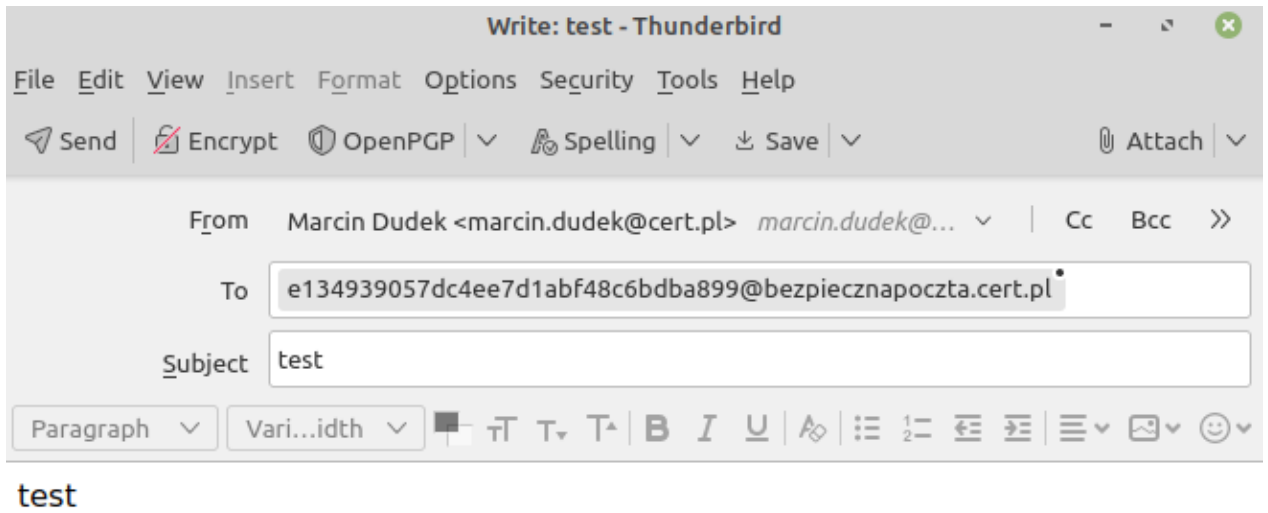
Aby zweryfikować konfigurację poczty, wyślij dowolną wiadomość e-mail na adres:

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.



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]

❌ 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 sfałszowana 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 sfałszowana 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 sfałszowana 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

Informacje o zagrożeniach i podatnościach

Informacje o zagrożeniach i podatnościach

https://www.facebook.com/CERT.Polska

https://twitter.com/CERT_Polska

https://pl.linkedin.com/showcase/cert-polska/

Dziękuję za uwagę!

info@cert.pl