CERT.PL
NASK

TRZYDZIESTE FORUM TELEINFORMATYKI®

Misja i znaczenie zespołu reagowania CERT Polska

Krzysztof Silicki, **Sebastian Kondraszuk**

Z podziękowaniami dla Przemka Jaroszewskiego za wkład w prezentację

cert.pl

NASK PIB w pigułce

- 1991 nawiązanie komunikacji IP z zagranicą
- 1992 NASK funkcjonuje przy Uniwersytecie Warszawskim
- 1993 jednostka badawczo-rozwojowa
- operator telekomunikacyjny
- rejestr domen .pl oraz gov.pl
- 1996 CERT NASK
- 2001 CERT Polska
- 2004 Dyżurnet
- 2018 CSIRT NASK

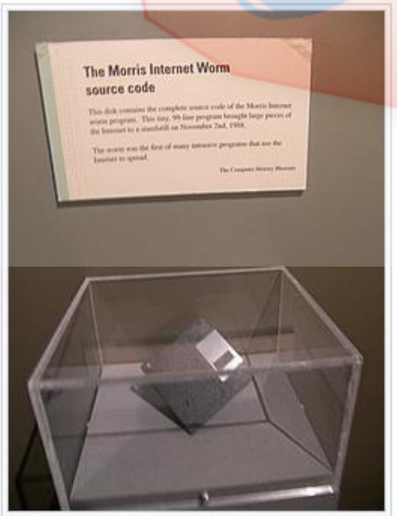
1962
The modern history of cybercrime began when Allen Scherr launched a cyber attack against the MIT computer networks, stealing passwords from their database via punch card.

1971
Researcher Bob Thomas created a computer programme called Creeper that could move across ARPANET's network, leaving a breadcrumb trail wherever it went. Ray Tomlinson, the inventor of email, wrote the programme Reaper, which chased and deleted Creeper. Reaper was the very first example of antivirus software and the first self-replicating programme, making it the first-ever computer worm.

Od kiedy zajęto się bezpieczeństwem internetu?

W roku 1988 *Morris Worm*, pierwszy sławny robak internetowy zainfekował 6 tys. komputerów (10% ówczesnego internetu)

- Dyskietka z robakiem Morrisa jako eksponat w Muzeum technologii w Bostonie



Dyskietka z *robakiem Morrisa* jako eksponat w Muzeum technologii w Bostonie.

Źródło: Wikipedia

W odpowiedzi na ten incydent powołano w 1988 r. Pitsburgu pierwszy CERT na świecie: CERT Coordination Center

- W roku 1990 powołano międzynarodowe zrzeszenie zespołów reagujących na incydenty i zagrożenia internetowe: **FIRST (Forum of Incident Response and Security Teams)**

- Obecnie FIRST zrzesza **760 CERTów ze 111 krajów na całym świecie**

Polska, rok 1994: bezpieczeństwo internetu? – kto się tym będzie zajmował?

- 30 lat temu, w pionierskich czasach budowania internetu w Polsce, NASK dostrzegł także tę ciemniejszą stronę sieci: zagrożenia, włamania do serwerów z wykorzystaniem internetu czy defacementy witryn internetowych.

- To skłoniło nas do powołania w roku 1996 zespołu reagowania na zagrożenia technologiczne – CERT a później, w roku 2004 zespołu Dyżurnet.pl przeciwdziałającemu szkodliwym treściom w sieci

- Działania na rzecz bezpieczeństwa internetu, to misja , której NASK podjął się w imię odpowiedzialności za technologie, które sam wdrażał na rzecz tworzenia powszechnego dostępu do sieci

- W ciągu 28 lat zagadnienie cyberbezpieczeństwa, z niszowego problemu stało się kluczowym czynnikiem powodzenia rozwoju cyfryzacji czy informatyzacji.

Podatności, ataki oraz incydenty były, są i będą się zdarzały…coraz częściej

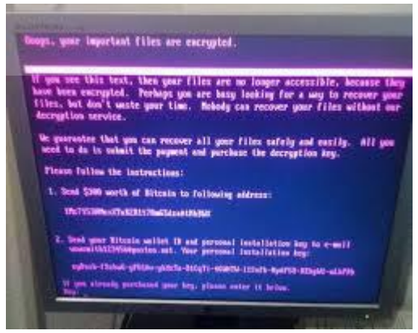
- Oraz będą coraz bardziej zaawansowane

Wirus I Love you: 2000

Stuxnet: 2007

Luka w opensource - Heartbleed: 2014

Atak ransomware – na ALAB: 2023

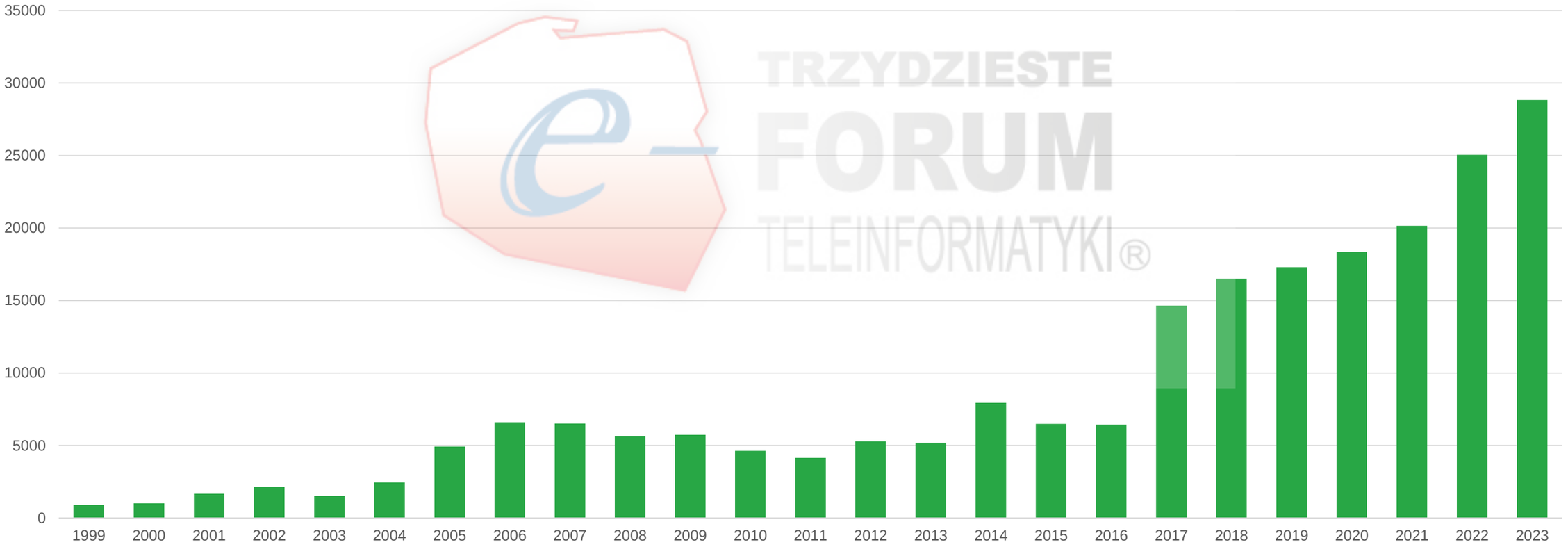


Wiper NotPetya: 2017

Atak na łańcuch dostaw – Sunburst: 2020

Krytyczna luka i atak na opr. Log4j: 2021

Nowe podatności



https://nvd.nist.gov/vuln/

Początki

1994- 1995

- Udział w internetowych konferencjach międzynarodowych gdzie temat bezpieczeństwa internetu zaczął wybrzmiewać
- Rozmowy z istniejącymi już wtedy zespołami CERT: CERT CC, DFN CERT

1996

- Decyzja Kierownictwa NASK jbr o powołaniu CERT NASK
- Pierwszy zespół reagujący w Polsce, jeden z pierwszych w Europie

1997

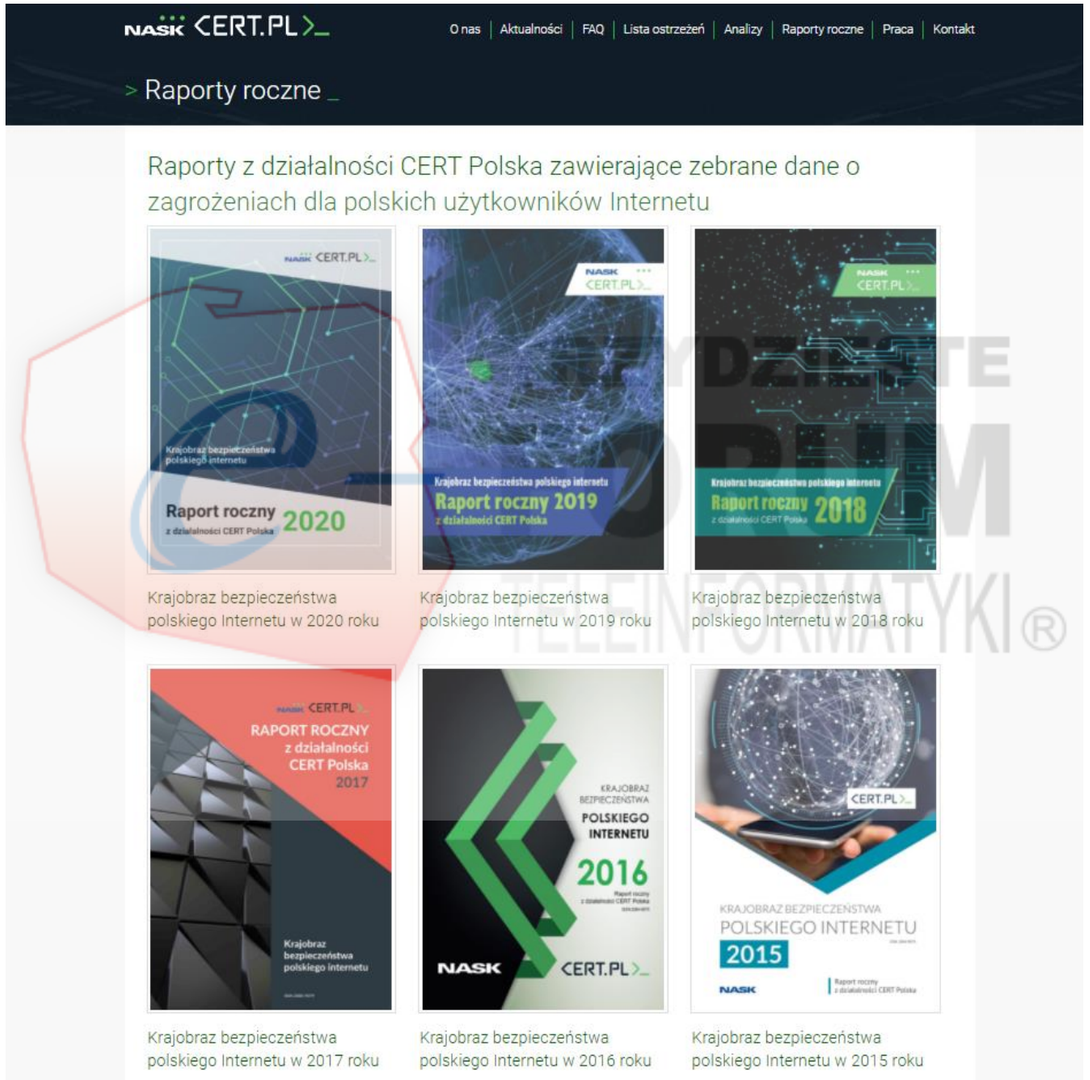
- Polski CERT staje się członkiem sieci FIRST
- Uruchomienie pierwszej edycji konferencji SECURE

Początki: od czego zacząć?

- ...najlepiej od incydentu ☺
- w pierwszych tygodniach funkcjonowania CERT NASK DFN CERT przekazał nam bardzo duży incydent skanowania wielu sieci i instytucji w Polsce
- to pozwoliło na skontaktowanie się z dużą ilością instytucji podłączonych wtedy do internetu, zaprezentowanie się, nawiązanie kontaktu, ostrzeżenie o zagrożeniu i potencjalnym incydencie

Działanie w organizacjach i inicjatywach międzynarodowych

Raporty roczne

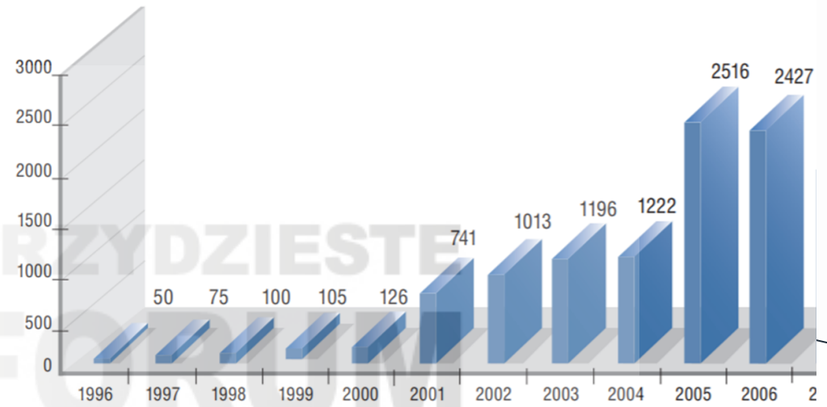


Konferencja SECURE – pierwsza w kraju konferencja poświęcona bezpieczeństwu internetu

W przyszłym roku 28 edycja konferencji !

CERT Polska – kluczowe momenty

- Dynamiczny wzrost i rozszerzenie działalności
- **rok 2001**: przekształcenie CERT NASK w CERT Polska



- **Rok 2018**: ustawa o KSC definiuje formalną rolę CERT Polska, który staje się głównym elementem krajowego zespołu reagującego **CSIRT NASK**
- BTW, częścią CSIRT NASK jest również Dyżurnet.pl

Dyżurnet.pl

- Zespół reagujący na szkodliwe i nielegalne treści – głownie dotyczące wykorzystania małoletnich w sieci
- Działa od 2004 roku, zrzeszony w INHOPE
- Jest częścią CSIRT NASK

Publikacje

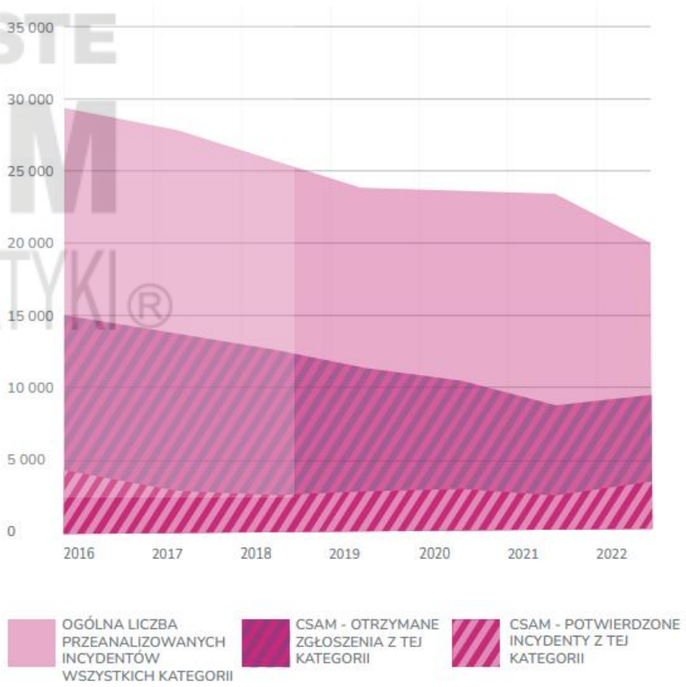
Metawersum - zagrożenia, szanse, wyzwania

2023-09-11

Metawersum to wirtualny świat, do którego dostęp możliwy jest poprzez użycie specjalnych gogli VR. Eksperci szacują, że w ciągu kilku najbliższych lat wszyscy będziemy korzystać na co dzień z tego typu rozwiązań, na wielu płaszczyznach życia codziennego. Ważnym aspektem bezpiecznego korzystania z każdej technologii, a zwłaszcza nowej, której zagrożenia nie zostały jeszcze dokładn...

ZGŁOŚ

9 | Liczba zgłoszeń dotyczących potencjalnych materiałów typu CSAM oraz potwierdzonych incydentów CSAM na tle ogólnej liczby przeanalizowanych incydentów w latach 2015-2021



Katalog usług cyberbezpieczeństwa opracowany przez FIRST stosowany przez zespoły CERT

SERVICE AREA
Information Security Event Management

Monitoring and Detection
- Log and Sensor Management
- Detection Use Case Management
- Contextual Data Management

Event Analysis
- Correlation
- Qualification

SERVICE AREA
Information Security Incident Management

Information Security Incident Report Acceptance
- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing

Information Security Incident Analysis
- Information Security Incident Triage (Prioritization and Categorization)
- Information Collection
- Detailed Analysis Coordination
- Information Security Incident Root Cause Analysis
- Cross-Incident Correlation

Artifact and Forensic Evidence Analysis
- Media or Surface Analysis
- Reverse Engineering
- Runtime or Dynamic Analysis
- Comparative Analysis

Mitigation and Recovery
- Response Plan Establishment
- Ad Hoc Measures and Containment
- System Restoration
- Other Information Security Entities Support

Information Security Incident Coordination
- Communication
- Notification Distribution
- Relevant Information Distribution
- Activities Coordination
- Reporting
- Media Communication

Crisis Management Support
- Information Distribution to Constituents
- Information Security Status Reporting
- Strategic Decisions Communication

SERVICE AREA
Vulnerability Management

Vulnerability Discovery/Research
- Incident Response Vulnerability Discovery
- Public Source Vulnerability Discovery
- Vulnerability Research

Vulnerability Report Intake
- Vulnerability Report Receipt
- Vulnerability Report Triage and Processing

Vulnerability Analysis
- Vulnerability Triage (Validation and Categorization)
- Vulnerability Root Cause Analysis
- Vulnerability Remediation Development

Vulnerability Coordination
- Vulnerability Notification/Reporting
- Vulnerability Stakeholder Coordination

Vulnerability Disclosure
- Vulnerability Disclosure Policy and Infrastructure Maintenance
- Vulnerability Announcement/ Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

Vulnerability Response
- Vulnerability Detection/Scanning
- Vulnerability Remediation

SERVICE AREA
Situational Awareness

Data Acquisition
- Policy Aggregation, Distillation, and Guidance
- Asset Mapping to Functions, Roles, Actions, and Key Risks
- Collection
- Data Processing and Preparation

Analysis and Synthesize
- Projection and Inference
- Event Detection (through Alerting and/or Hunting)
- Situational Impact

Communication
- Internal and External Communication
- Reporting and Recommendations
- Implementation

SERVICE AREA
Knowledge Transfer

Awareness Building
- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

Training and Education
- Knowledge, Skill, and Ability Requirements Gathering
- Educational and Training Materials Development
- Content Delivery
- Mentoring
- CSIRT Staff Professional Development

Exercises
- Requirements Analysis
- Format and Environment Development
- Scenario Development
- Exercise Execution
- Exercise Outcome Review

Technical and Policy Advisory
- Risk Management Support
- Business Continuity and Disaster Recovery Planning Support
- Policy Support
- Technical Advice

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

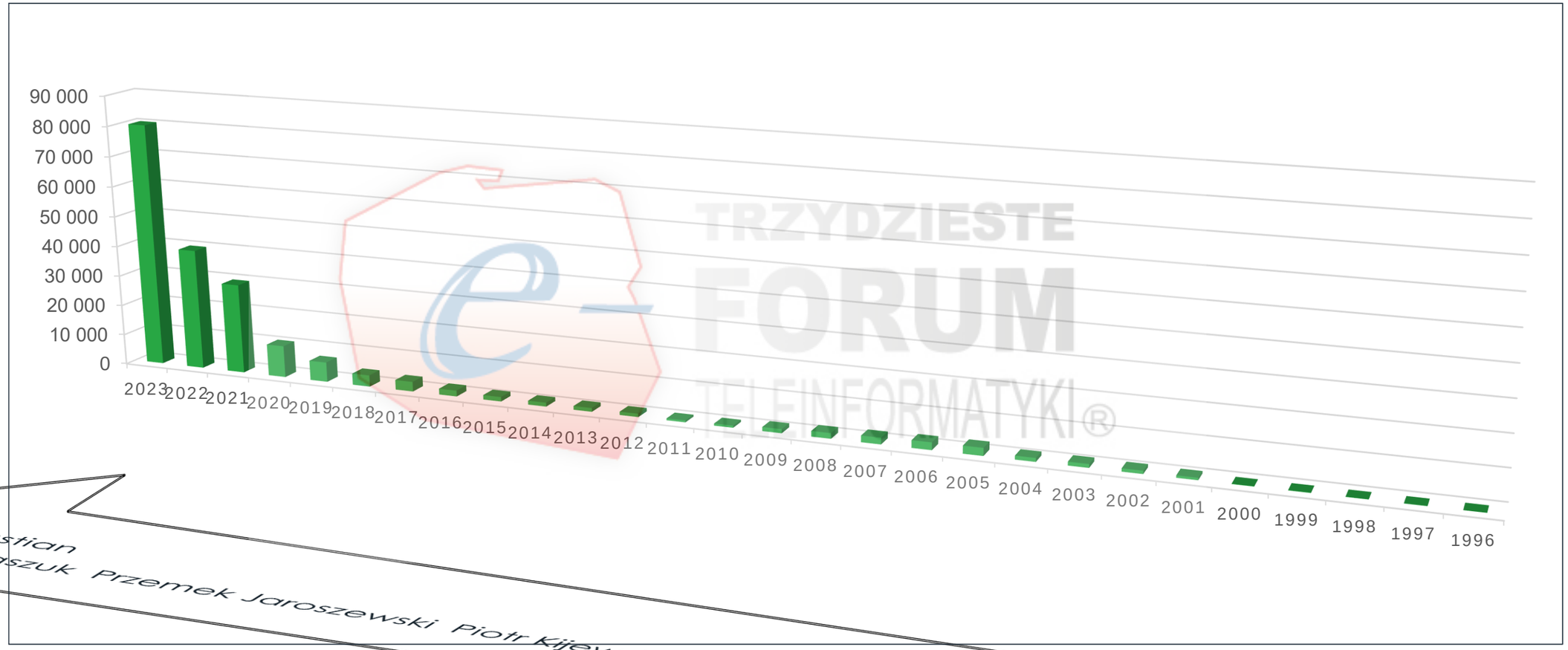
Wartości

- Kompetencje
- Poczucie misji
- Odpowiedzialność
- Wysokie standardy etyczne
- Chęć dzielenia się wiedzą i efektami działań

Dzięki temu…

- Świetni ludzie, świetne pomysły
- Realny wpływ na to, co się dzieje
- Okazja do realizacji własnych pomysłów badawczych i implementacyjnych
- Stała możliwość rozwoju i doskonalenia się

Od historii do teraźniejszości



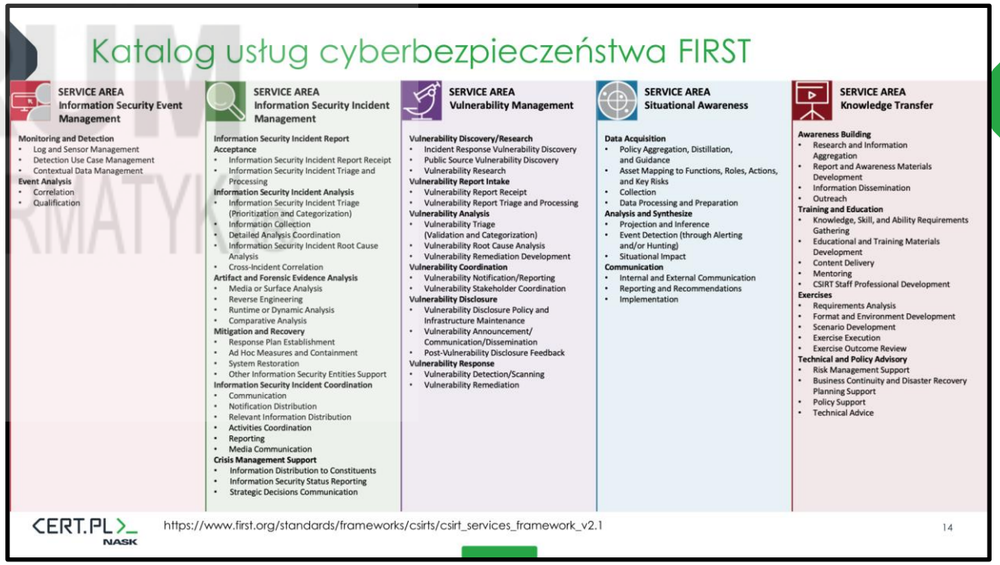
Raport CERT Polska 2023

- **371 089** zgłoszeń
- **80 267** incydentów
- **2 184** podmioty publiczne
- **95%** oszustwa komputerowe
- **40** incydentów poważnych
- **1650** przypadków szkodliwego oprogramowania
- **79** tysięcy domen na liście ostrzeżeń
- **270k** adresów wykazujących aktywność botów

2023: Incydenty według kategorii

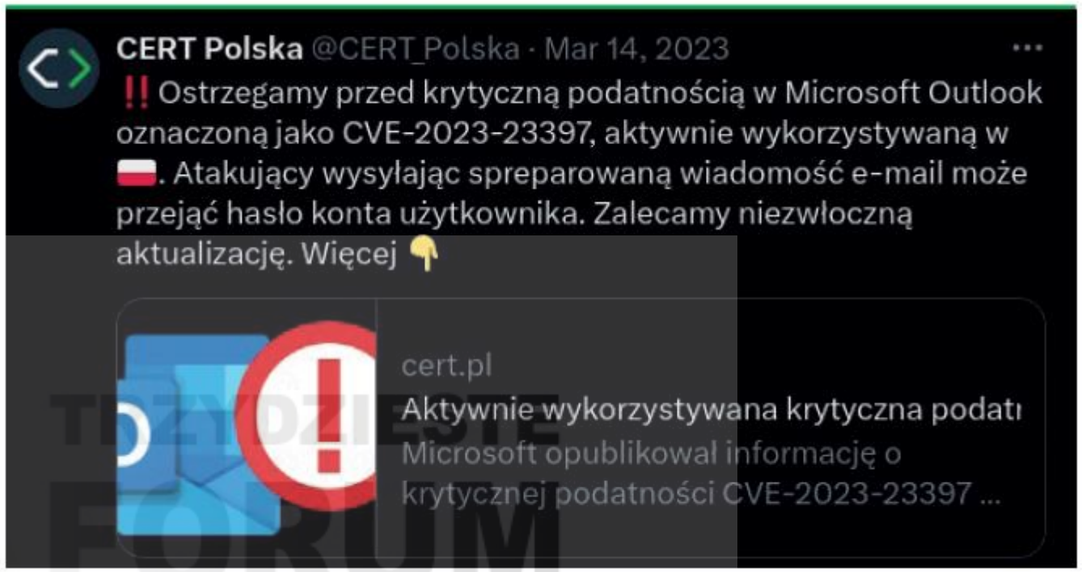
Działalność CERT Polska - poza obsługą i koordynacją incydentów

- Większość usług z katalogu FIRST, w tym:
- Informowanie o zagrożeniach i alertowanie constituency
- Budowanie eksploatacja innowacyjnych narzędzi i usług
- Wiele działań nakierowanych na budowanie świadomości
- Obserwacja i analizy związane z grupami APT
- Współpraca krajowa i zagraniczna
- Pomoc zaatakowanym podmiotom
- Współpraca z organami ścigania
- Praca na rzecz skoordynowanego ujawniania podatności (CVD)

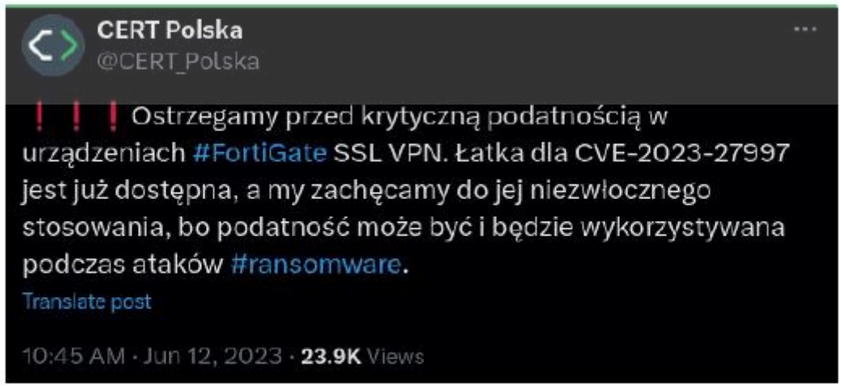


Podatności

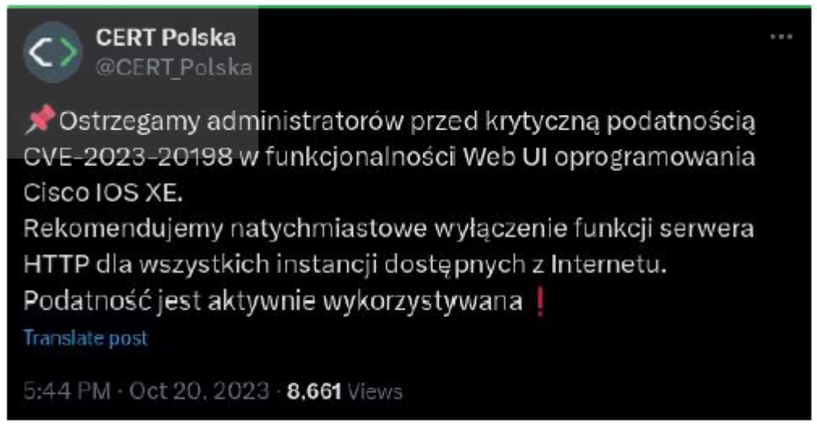
- Szerokie informowanie
- Zalecenia dla administratorów
- Próba identyfikacji obecności
- Informacje partnerskie
- Mailing, abuse, telefon, linkedin…
- Wnioskowanie wsteczne ☺



Rysunek 26: Ostrzeżenie przed podatnością CVE-2023-23397



Rysunek 27: Ostrzeżenie przed podatnością CVE-2023-27997



Rysunek 28: Ostrzeżenie przed podatnością CVE-2023-20198

https://nvd.nist.gov/vuln/

CVD

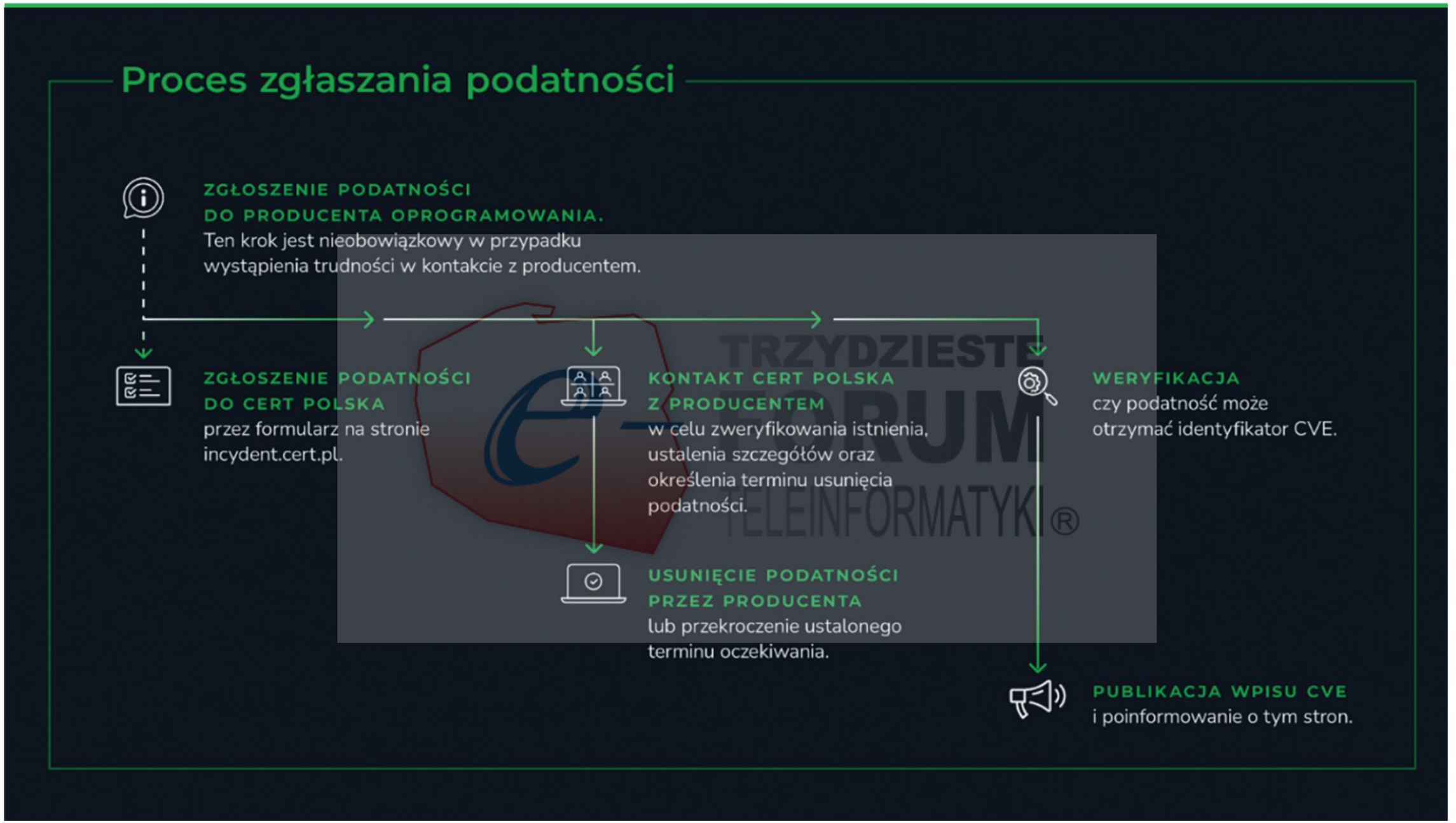
Coordinated Vulnerability Disclosure Policy

EU CSIRTs network members and ENISA advise parties to process signalled vulnerabilities and incidents with affected vendors or manufacturers (i.e., vulnerability owners) in a cooperative and coordinated manner under the principles of Responsible / Coordinated Vulnerability Disclosure.

In its role as the secretariat of the EU CSIRTs network, ENISA supports CSIRTs network members in tackling vulnerabilities detected or signalled by third parties, involving clients, peers and other companies from target groups as well as those from other CSIRTs, and trusted peers from scientific and research branches.

As such, ENISA may register vulnerabilities and support vulnerability disclosure in relation to
- vulnerabilities in IT products discovered by EU CSIRTs themselves and
- vulnerabilities reported to EU CSIRTs for coordinated disclosure, which are not already in another CNA's scope.

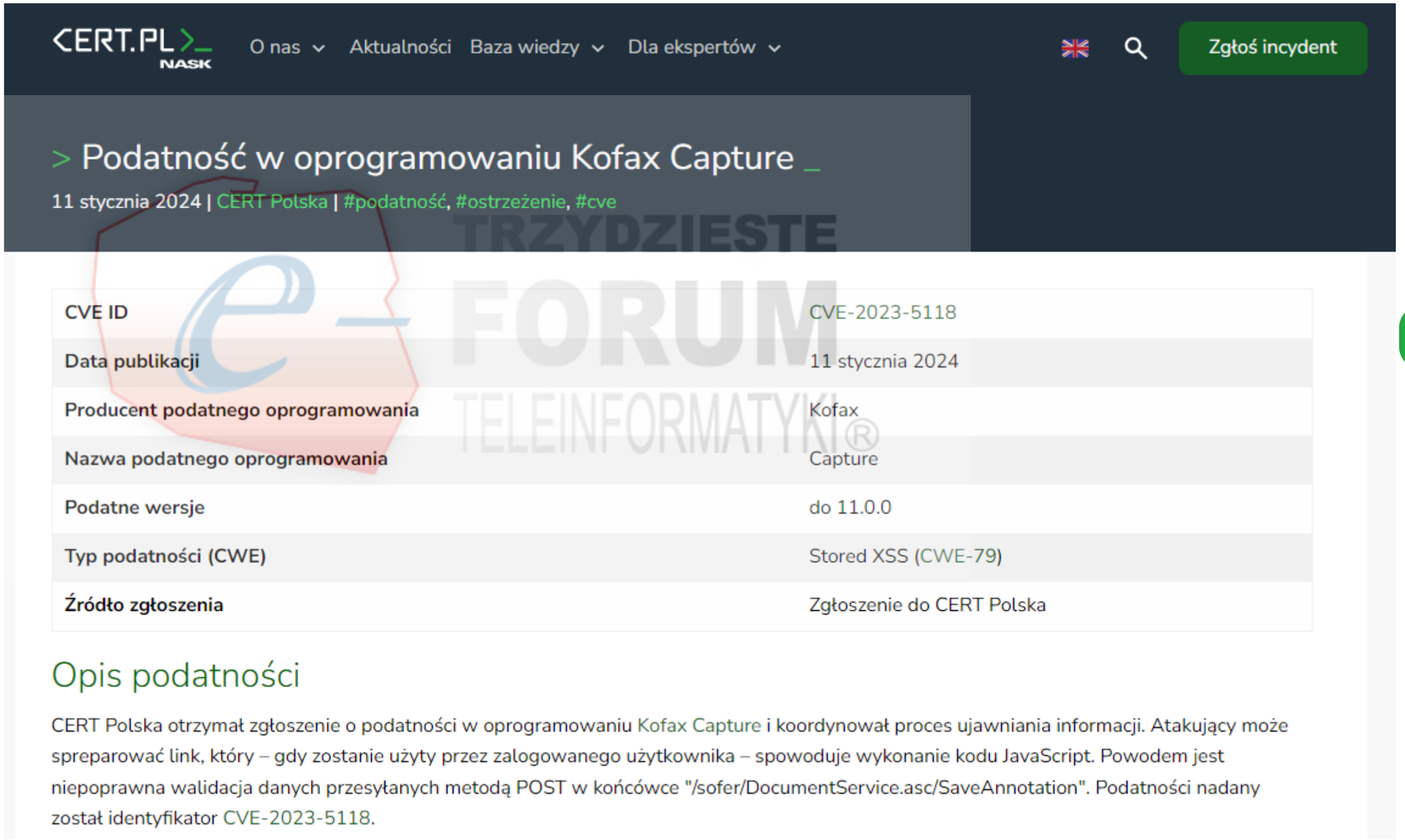
https://csirtsnetwork.eu/homepage?tab=cvd



Rysunek 2: Schemat procesu obsługi podatności

CVD – CERT Polska

- https://cert.pl/cvd/
- https://incydent.cert.pl/
- https://cert.pl/cve/



CERT.PL NASK

APT

	Styczeń	Luty	Marzec	Kwiecień	Maj	Czerwiec	Lipiec	Sierpień	Wrzesień	Październik	Listopad	Grudzień
UNC1151 | Ghostwriter (Rosja/Białoruś)	X	X	X	X	X	X		X	X	X	X	
APT28 | Fancy Bear | Forest Blizzard (Rosja)			X		X		X		X	X	X	X
APT29 | Cozy Bear | Midnight Blizzard (Rosja)	X	X	X	X	X	X	X				X	X
Callisto | Star Blizzard | Coldriver (Rosja)						X		X	X	X		
Sandworm | Voodo Bear | Seashell Blizzard (Rosja)		X										
Gamaredon | Primitive Bear | Aqua Blizzard (Rosja)	X	X										
Turla | Venomous Bear | Secret Blizzard (Rosja)		X	X									X
Winter Vivern (Rosja)		X								X		
Mustang Panda (Chiny)	X	X										
APT-UNK1		X						X				
APT-UNK2									X	X		

Tabela 1: Aktywność grup APT obserwowanych przez CERT Polska/CSIRT NASK w 2023 r

Systemy budowane przez CP & serwisy oferowane

lista.cert.pl

Lista Ostrzeżeń

artemis

Malware Database

MWDB

bezpiecznapoczta.cert.pl

Informacje o zagrożeniach

> Lista Ostrzeżeń przed niebezpiecznymi stronami _

Nieprzerwanie od marca 2020 roku prowadzimy Listę Ostrzeżeń przed niebezpiecznymi stronami. 24 godziny na dobę, 7 dni w tygodniu wpisujemy na listę domeny, które wprowadzają użytkowników w błąd i wyłudzają od nich dane.

Strony wyłudzające dane osobowe oraz dane uwierzytelniające są obecnie zjawiskiem masowym, dotykającym różne grupy użytkowników Internetu w Polsce. Linki do nich przesyłane są różnymi kanałami: przez SMS, e-mail lub media społecznościowe. Strony te są rejestrowane w dużych ilościach i wykorzystywane w dość krótkim czasie od rejestracji, po czym są porzucane na rzecz nowych adresów. Z tego powodu bardzo ważne jest szybkie rozpoznawanie zagrożeń i dzielenie się informacjami z dotkniętymi organizacjami i administratorami sieci.

Lista Ostrzeżeń jest wykorzystywana przez operatorów telekomunikacyjnych, firmy, organizacje i samych użytkowników do automatycznego blokowania dostępu do złośliwych stron i tym samym ograniczania skutków ataków phishingowych i innych kampanii wymierzonych w obywateli Polski.

Plansza hole.cert.pl wyświetlania przy wejściu na zablokowaną stronę

cert.pl/skanowanie

2023:
sprawdziliśmy 50.6 tys. domen (251.7 tys. subdomen)

- szkoły i placówki oświatowe
- JST
- *.gov.pl
- zdrowie
- banki
- komitety wyborcze

artemis

Co znaleźliśmy

styczeń-wrzesień 2023:
184.8 tys. błędów i podatności (11.6 tys. z wysoką oceną)

- 78.7 tys. nieaktualne oprogramowanie
- 44.2 tys. – problemy z konfiguracją SSL/TLS
- 27 tys. – SPF, DKIM, DMARC
- **4.5 tys. – krytycznych podatności** umożliwiających np. przejęcie strony lub pobranie bazy danych
- 3.4 tys. – publicznie dostępne kopie zapasowe, kod źródłowy, itd.

Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej

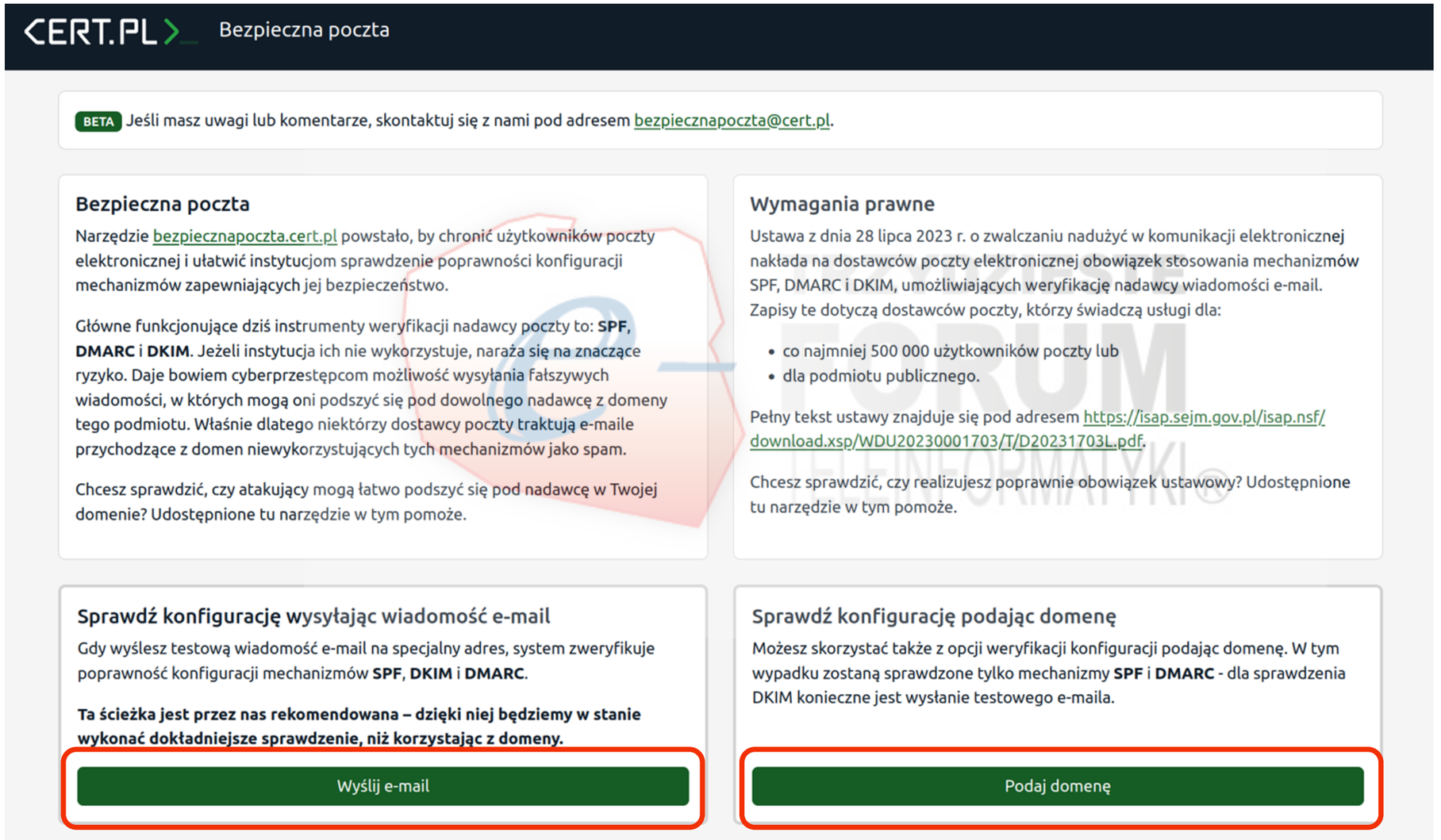
➔ Opublikowana 25 sierpnia.

Obowiązek stosowania mechanizmów SPF, DKIM i DMARC

dla:

- dostawców poczty dla co najmniej 500 tys. użytkowników
- **podmiotów publicznych**

bezpiecznapoczta.cert.pl



CERT.PL NASK

European Cyber Security Contest

- CERT Polska organizuje od 2018 r. eliminacje krajowe do zawodów ECSC organizowanych przez ENISA.

- Zadania publikowane na platformie hack.cert.pl
- Warsztaty dla wyłonionej reprezentacji
- Wyjazd na finały pod okiem trenerów

- W 2021 Polska zajęła najlepsze w historii II miejsce.
- W 2025 roku Polska będzie organizatorem finałów ECSC

CERT.PL
NASK

cert@cert.pl

Facebook	https://www.facebook.com/CERT.Polska/
Twitter	https://twitter.com/CERT_Polska
GitHub	https://github.com/CERT-Polska