



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.

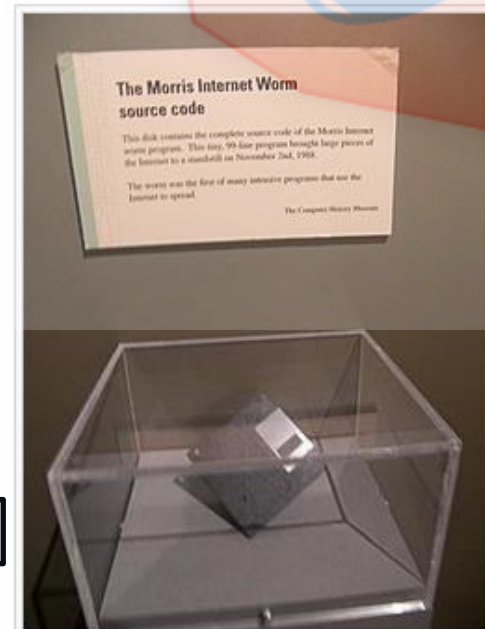
1971

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. Pittsburghu pierwszy CERT na świecie: CERT Coordination Center

TRZYDZIEŚTE
FORUM
TELEINFORMATYKI®



- 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



Wiper NotPetya: 2017



Luka w opensource -
Heartbleed: 2014



Atak na łańcuch dostaw – Sunburst:
2020

Atak ransomware – na ALAB:
2023



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



TF-CSIRT



TRZYDZIESIĄTE
e-FORUM



SHADOWSERVER


Raporty roczne

NASK CERT.PL >_

O nas | Aktualności | FAQ | Lista ostrzeżeń | Analizy | Raporty roczne | Praca | Kontakt

> Raporty roczne _

Raporty z działalności CERT Polska zawierające zebrane dane o zagrożeniach dla polskich użytkowników Internetu



Krajobraz bezpieczeństwa polskiego internetu w 2020 roku

Krajobraz bezpieczeństwa polskiego internetu w 2019 roku

Krajobraz bezpieczeństwa polskiego internetu w 2018 roku

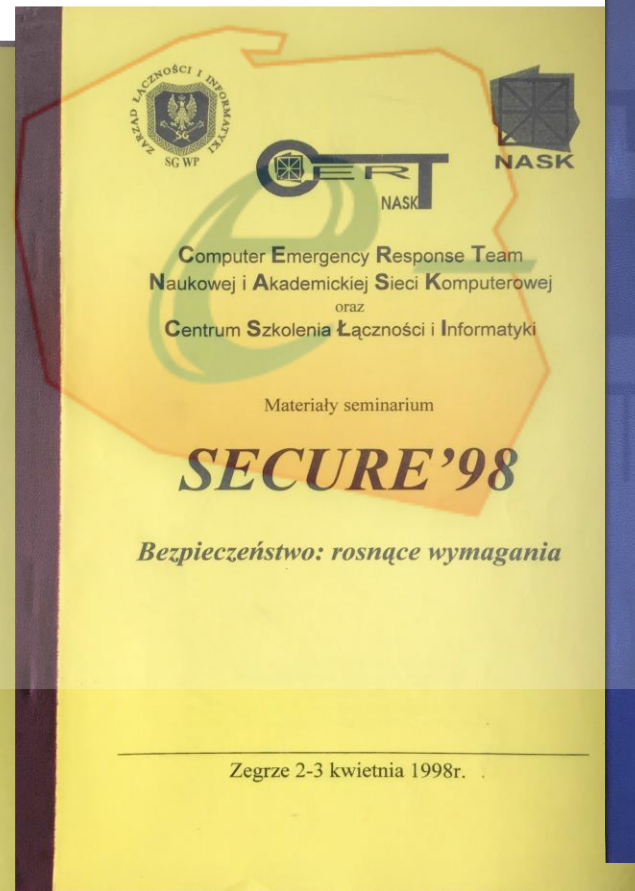
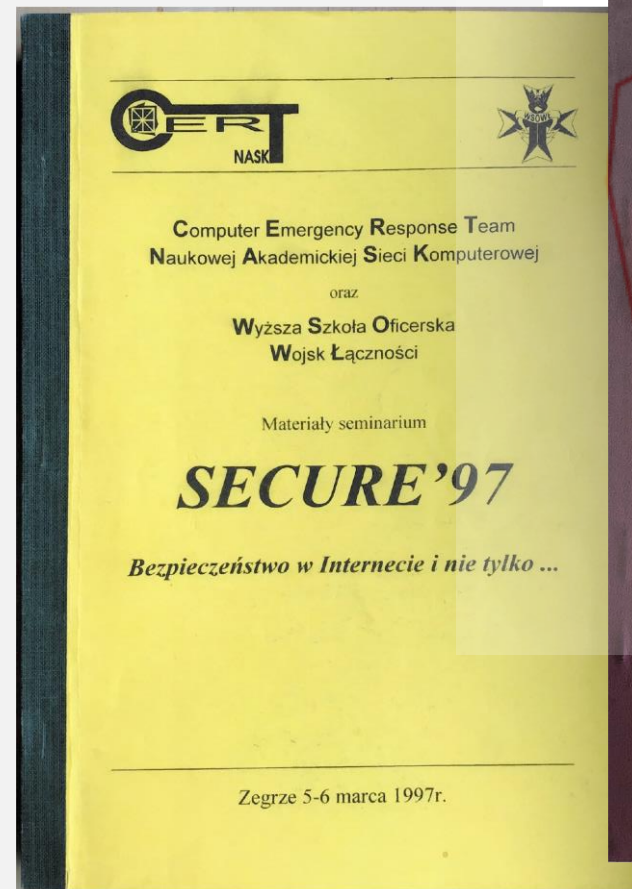
Krajobraz bezpieczeństwa polskiego internetu w 2017 roku

Krajobraz bezpieczeństwa polskiego internetu w 2016 roku

Krajobraz bezpieczeństwa polskiego internetu w 2015 roku



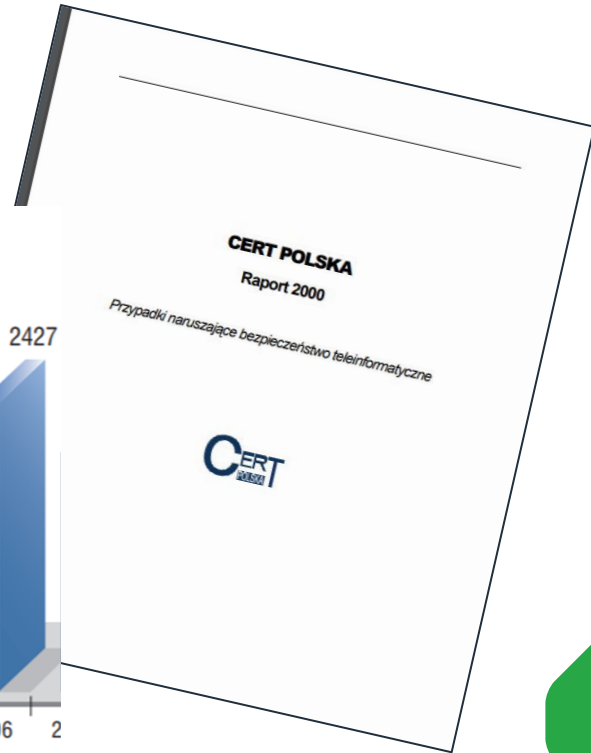
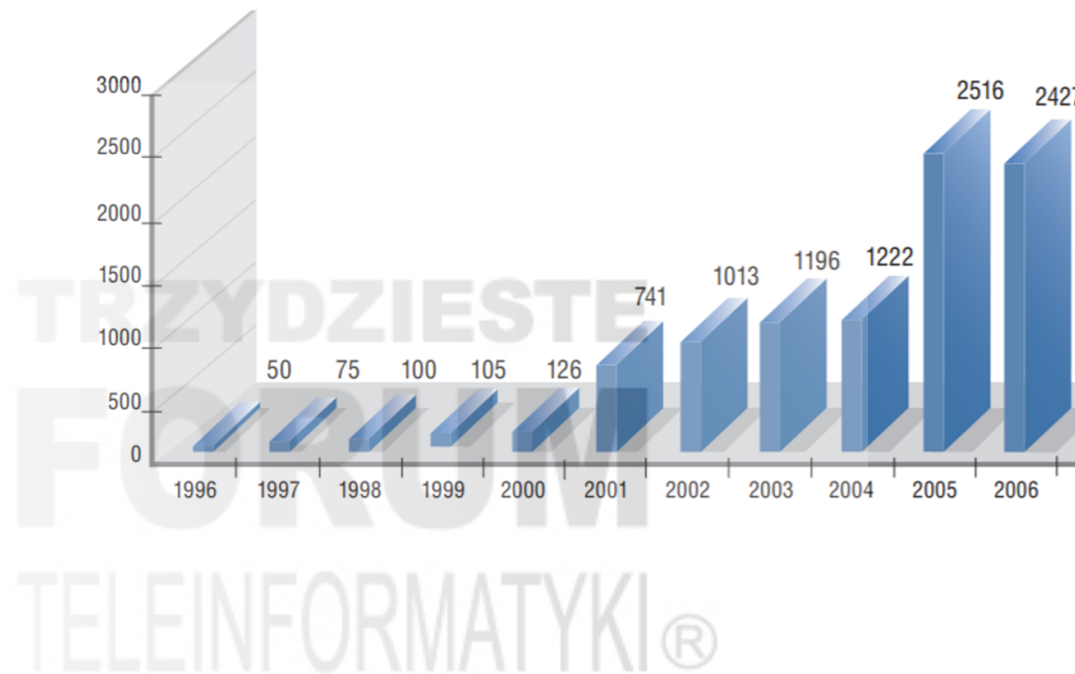
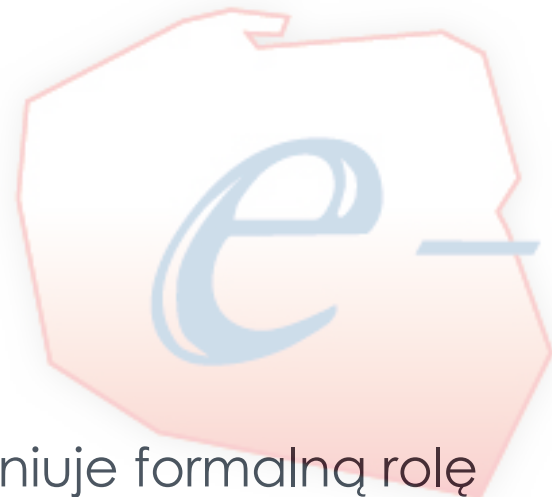
Konferencja SECURE – pierwsza w kraju konferencja poświęcona bezpieczeństwu internetu



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 – głównie dotyczące wykorzystania małoletnich w sieci
- Działa od 2004 roku, zrzeszony w INHOPE
- Jest częścią CSIRT NASK

Publikacje



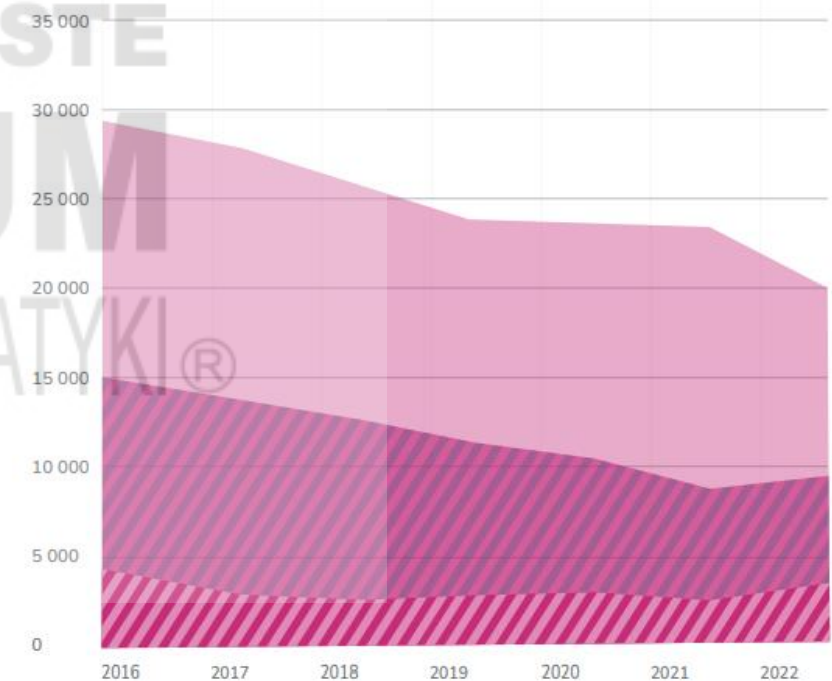
Metawersum - zagrożenia, szanse, wyzwania

2023-09-11

Metawersum to wirtualny świat, do którego dostęp możliwy jest poprzez użycie specjalnych gogli VR. Eksperti 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



OGÓLNA LICZBA PRZEANALIZOWANYCH INCYDENTÓW WSZYSTKICH KATEGORII

CSAM - OTRZYMANE ZGŁOSZENIA Z TEJ KATEGORII

CSAM - POTWIERDZONE INCYDENTY Z TEJ KATEGORII

Katalog usług cyberbezpieczeństwa opracowany przez FIRST stosowany przez zespoły CERT

 SERVICE AREA Information Security Event Management	 SERVICE AREA Information Security Incident Management	 SERVICE AREA Vulnerability Management	 SERVICE AREA Situational Awareness	 SERVICE AREA Knowledge Transfer
Monitoring and Detection <ul style="list-style-type: none">• Log and Sensor Management• Detection Use Case Management• Contextual Data Management Event Analysis <ul style="list-style-type: none">• Correlation• Qualification	Information Security Incident Report Acceptance <ul style="list-style-type: none">• Information Security Incident Report Receipt• Information Security Incident Triage and Processing Information Security Incident Analysis <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Media or Surface Analysis• Reverse Engineering• Runtime or Dynamic Analysis• Comparative Analysis Mitigation and Recovery <ul style="list-style-type: none">• Response Plan Establishment• Ad Hoc Measures and Containment• System Restoration• Other Information Security Entities Support Information Security Incident Coordination <ul style="list-style-type: none">• Communication• Notification Distribution• Relevant Information Distribution• Activities Coordination• Reporting• Media Communication Crisis Management Support <ul style="list-style-type: none">• Information Distribution to Constituents• Information Security Status Reporting• Strategic Decisions Communication	Vulnerability Discovery/Research <ul style="list-style-type: none">• Incident Response Vulnerability Discovery• Public Source Vulnerability Discovery• Vulnerability Research Vulnerability Report Intake <ul style="list-style-type: none">• Vulnerability Report Receipt• Vulnerability Report Triage and Processing Vulnerability Analysis <ul style="list-style-type: none">• Vulnerability Triage (Validation and Categorization)• Vulnerability Root Cause Analysis• Vulnerability Remediation Development Vulnerability Coordination <ul style="list-style-type: none">• Vulnerability Notification/Reporting• Vulnerability Stakeholder Coordination Vulnerability Disclosure <ul style="list-style-type: none">• Vulnerability Disclosure Policy and Infrastructure Maintenance• Vulnerability Announcement/Communication/Dissemination• Post-Vulnerability Disclosure Feedback Vulnerability Response <ul style="list-style-type: none">• Vulnerability Detection/Scanning• Vulnerability Remediation	Data Acquisition <ul style="list-style-type: none">• Policy Aggregation, Distillation, and Guidance• Asset Mapping to Functions, Roles, Actions, and Key Risks• Collection• Data Processing and Preparation Analysis and Synthesize <ul style="list-style-type: none">• Projection and Inference• Event Detection (through Alerting and/or Hunting)• Situational Impact Communication <ul style="list-style-type: none">• Internal and External Communication• Reporting and Recommendations• Implementation	Awareness Building <ul style="list-style-type: none">• Research and Information Aggregation• Report and Awareness Materials Development• Information Dissemination• Outreach Training and Education <ul style="list-style-type: none">• Knowledge, Skill, and Ability Requirements Gathering• Educational and Training Materials Development• Content Delivery• Mentoring• CSIRT Staff Professional Development Exercises <ul style="list-style-type: none">• Requirements Analysis• Format and Environment Development• Scenario Development• Exercise Execution• Exercise Outcome Review Technical and Policy Advisory <ul style="list-style-type: none">• Risk Management Support• Business Continuity and Disaster Recovery Planning Support• Policy Support• Technical Advice

Wartości

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



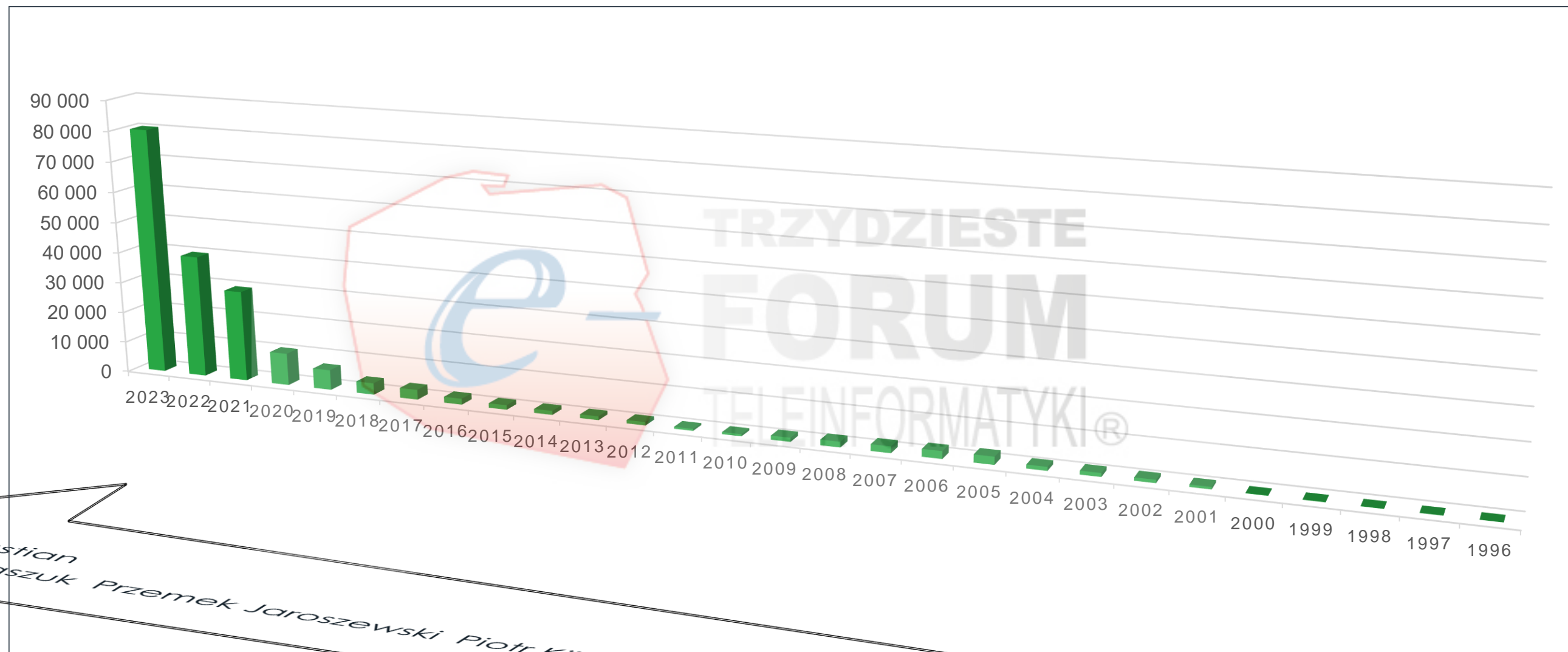
TRZYDZIESTE
FORUM
TELEINFORMATYKI®



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



Sebastian Kondraszuk

Przemek Jaroszewski

Piotr Kijewski

Miroslaw Maj

Krzysztof Silicki

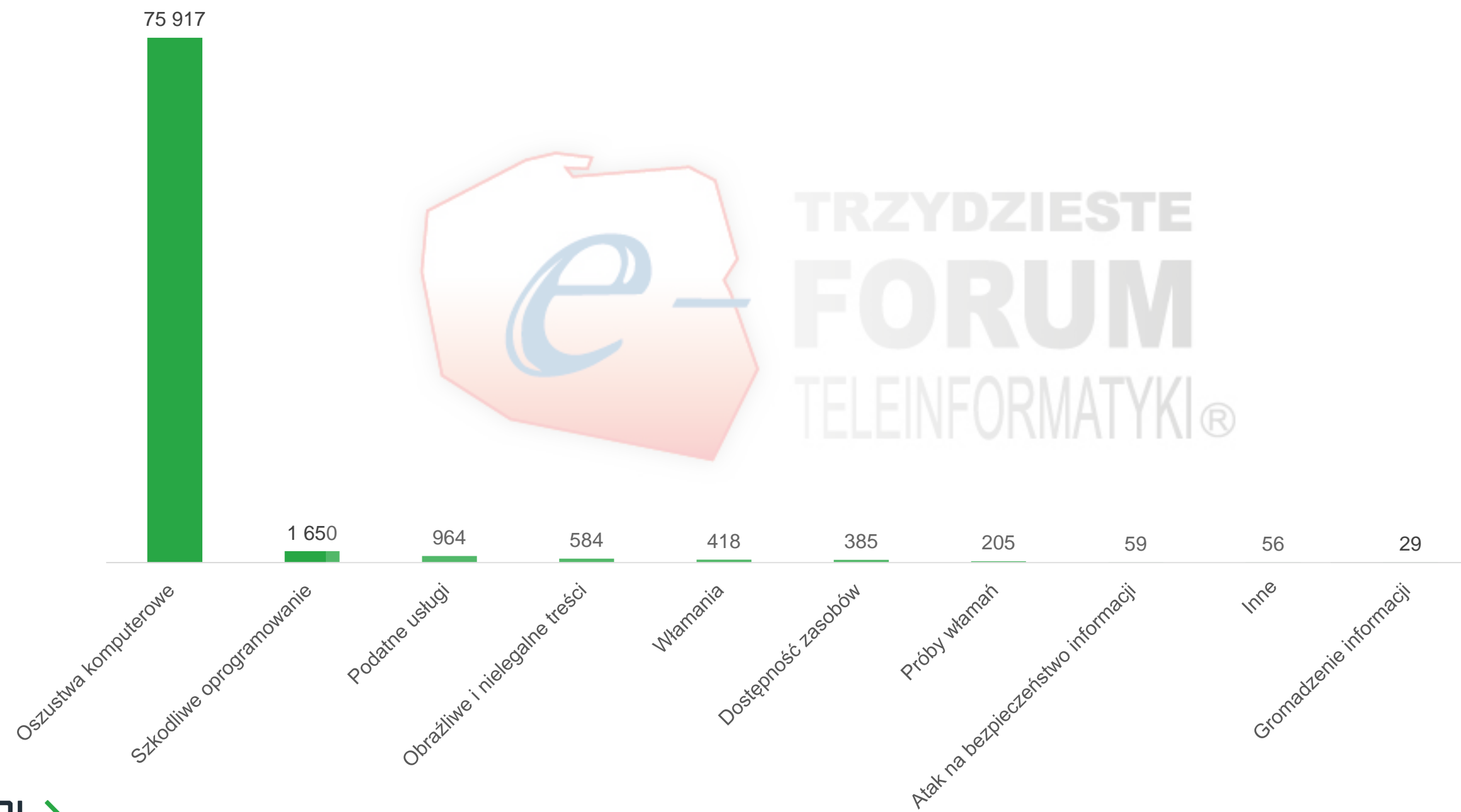
Raport CERT Polska 2023

- **371 089** zgłoszeń
- **80 267** incydentów
- **2 184** podmioty publiczne
- **95%** oszustwa komputerowe
- **40** incydentów poważnych
- **1 650** przypadków szkodliwego oprogramowania
- **79** tysięcy domen na liście ostrzeżeń
- **270k** adresów wykazujących aktywność botów



TRZYDZIESTE
FORUM
TELEINFORMATYKI®

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)

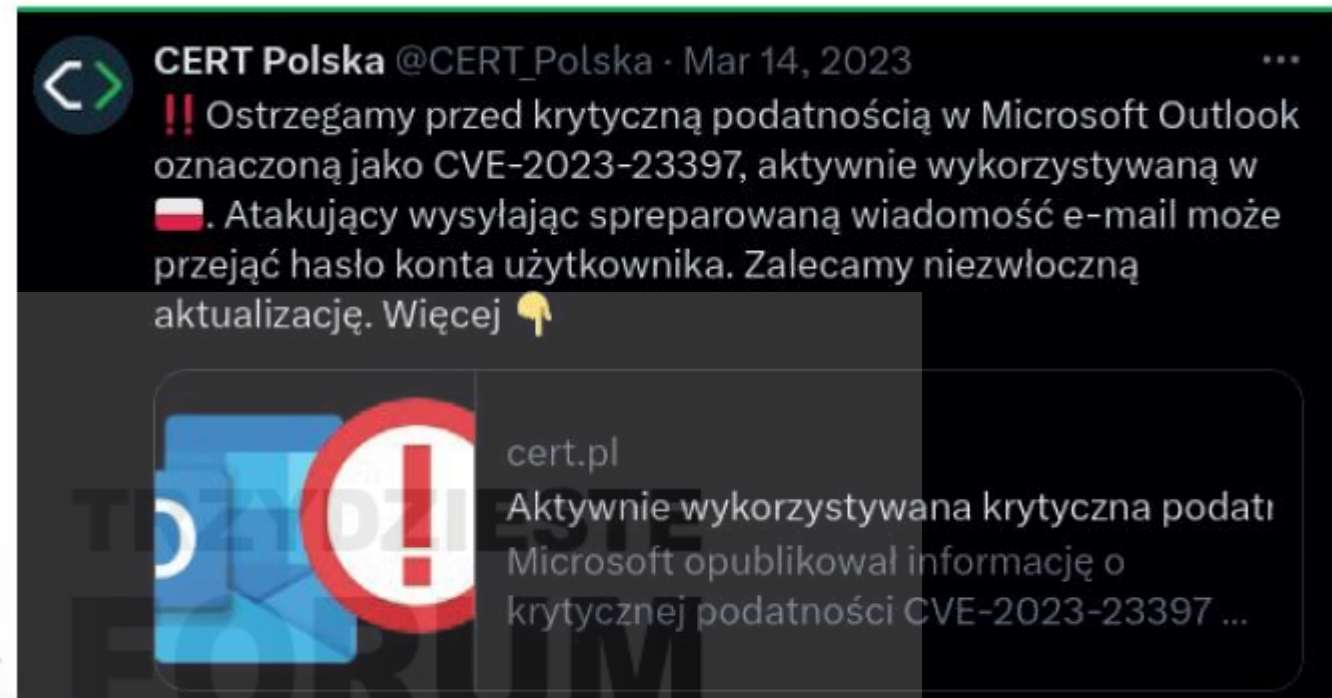
Katalog usług cyberbezpieczeństwa FIRST

SERVICE AREA Information Security Event Management	SERVICE AREA Information Security Incident Management	SERVICE AREA Vulnerability Management	SERVICE AREA Situational Awareness	SERVICE AREA Knowledge Transfer
Monitoring and Detection <ul style="list-style-type: none">Log and Sensor ManagementDetection Use Case ManagementContextual Data Management Event Analysis <ul style="list-style-type: none">CorrelationQualification	Information Security Incident Report Acceptance <ul style="list-style-type: none">Information Security Incident Report ReceiptInformation Security Incident Triage and Processing Information Security Incident Analysis <ul style="list-style-type: none">Information Security Incident Triage (Prioritization and Categorization)Information CollectionDetailed Analysis CoordinationInformation Security Incident Root Cause AnalysisCross-Incident Correlation Artifact and Forensic Evidence Analysis <ul style="list-style-type: none">Media or Surface AnalysisReverse EngineeringRuntime or Dynamic AnalysisComparative Analysis Mitigation and Recovery <ul style="list-style-type: none">Response Plan EstablishmentAd Hoc Measures and ContainmentSystem RestorationOther Information Security Entities Support Information Security Incident Coordination <ul style="list-style-type: none">CommunicationNotification DistributionRelevant Information DistributionActivities CoordinationReportingMedia Communication Crisis Management Support <ul style="list-style-type: none">Information Distribution to ConstituentsInformation Security Status ReportingStrategic Decisions Communication	Vulnerability Discovery/Research <ul style="list-style-type: none">Incident Response Vulnerability DiscoveryPublic Source Vulnerability DiscoveryVulnerability Research Vulnerability Report Intake <ul style="list-style-type: none">Vulnerability Report ReceiptVulnerability Report Triage and Processing Vulnerability Analysis <ul style="list-style-type: none">Vulnerability Triage (Validation and Categorization)Vulnerability Root Cause AnalysisVulnerability Remediation Development Vulnerability Coordination <ul style="list-style-type: none">Vulnerability Notification/ReportingVulnerability Stakeholder Coordination Vulnerability Disclosure <ul style="list-style-type: none">Vulnerability Disclosure Policy and Infrastructure MaintenanceVulnerability Announcement/Communication/DisseminationPost-Vulnerability Disclosure Feedback Vulnerability Response <ul style="list-style-type: none">Vulnerability Detection/ScanningVulnerability Remediation	Data Acquisition <ul style="list-style-type: none">Policy Aggregation, Distillation, and GuidanceAsset Mapping to Functions, Roles, Actions, and Key RisksCollectionData Processing and Preparation Analysis and Synthesize <ul style="list-style-type: none">Projection and InferenceEvent Detection (through Alerting and/or Hunting)Situational Impact Communication <ul style="list-style-type: none">Internal and External CommunicationReporting and RecommendationsImplementation	Awareness Building <ul style="list-style-type: none">Research and Information AggregationReport and Awareness Materials DevelopmentInformation DisseminationOutreach Training and Education <ul style="list-style-type: none">Knowledge, Skill, and Ability Requirements GatheringEducational and Training Materials DevelopmentContent DeliveryMentoringCSIRT Staff Professional Development Exercises <ul style="list-style-type: none">Requirements AnalysisFormat and Environment DevelopmentScenario DevelopmentExercise ExecutionExercise Outcome Review Technical and Policy Advisory <ul style="list-style-type: none">Risk Management SupportBusiness Continuity and Disaster Recovery Planning SupportPolicy SupportTechnical Advice

CERT.PL NASK https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1 14

Podatności

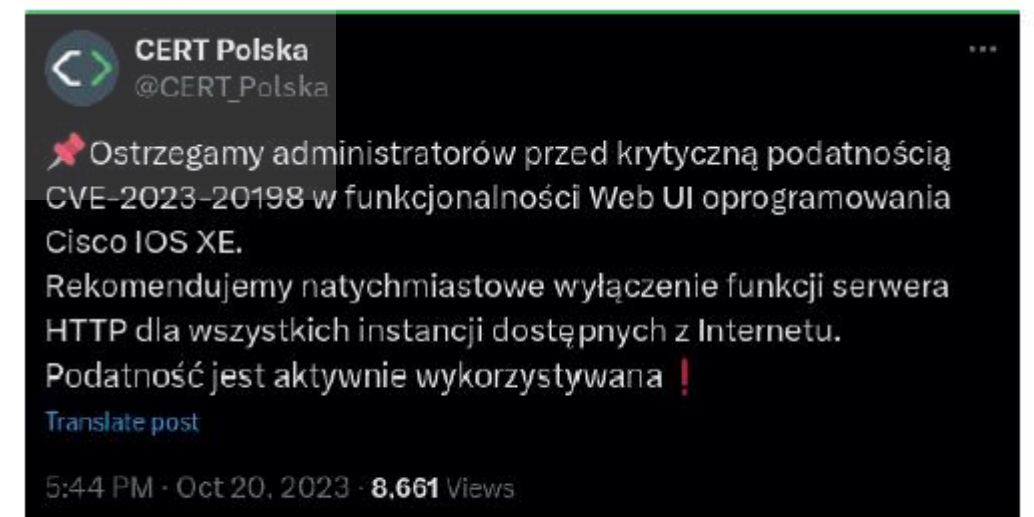
- Szerokie informowanie
- Zalecenia dla administratorów
- Próba identyfikacji obecności
- Informacje partnerskie
- Mailing, abuse, telefon, linkedin...
- Wnioskowanie wsteczne 😊



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.

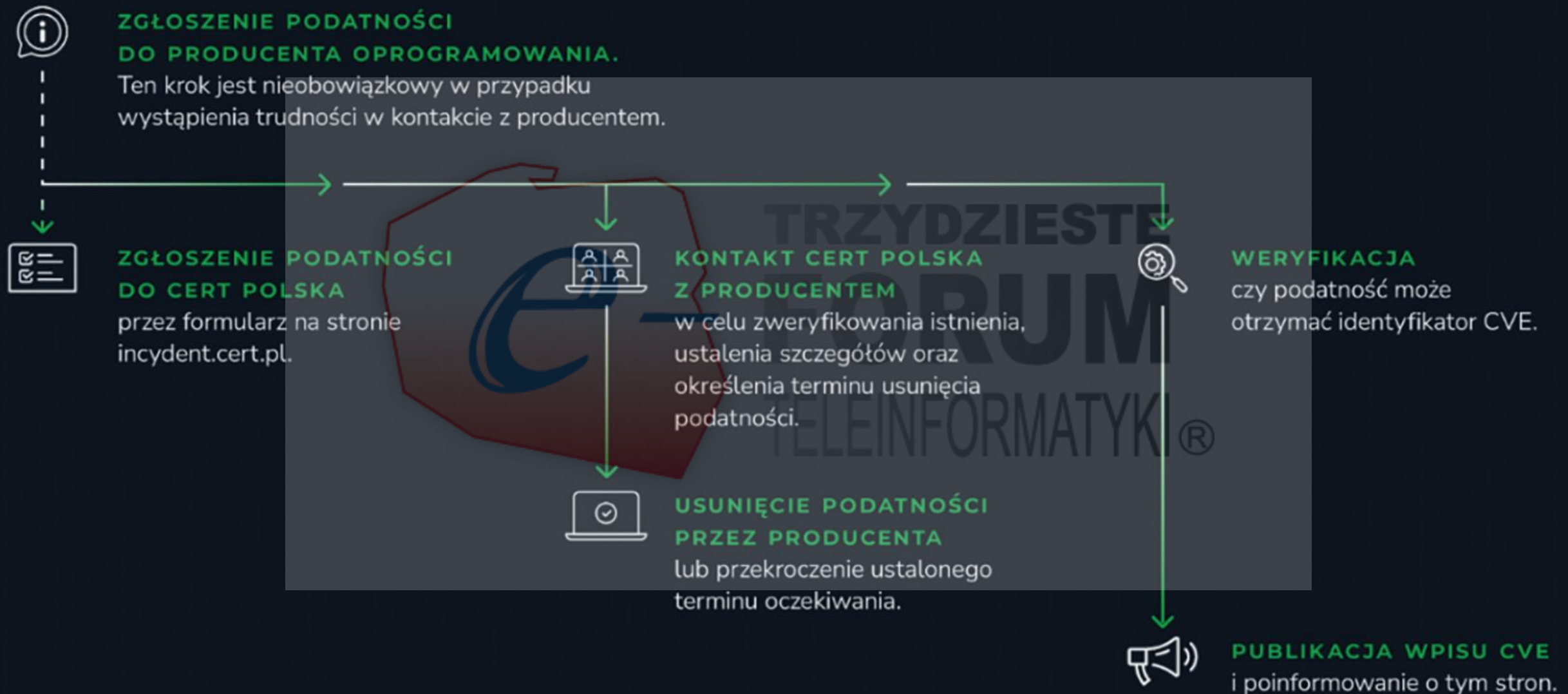
In its role as the secretariat of the EU CSIRTs network, ENISA supports CSIRTs network members in tackling vulnerabilities detected or signalled by third parties, involving clients, peers and other companies from target groups as well as those from other CSIRTs, and trusted peers from scientific and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

Proces zgłaszania podatności



Rysunek 2: Schemat procesu obsługi podatności

CVD – CERT Polska

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

CERT.PL NASK

O nas ▾ Aktualności Baza wiedzy ▾ Dla ekspertów ▾

🇬🇧 🔍 Zgłoś incydent

> Podatność w oprogramowaniu Kofax Capture

11 stycznia 2024 | CERT Polska | #podatność, #ostrzeżenie, #cve

CVE ID	CVE-2023-5118
Data publikacji	11 stycznia 2024
Producent podatnego oprogramowania	Kofax
Nazwa podatnego oprogramowania	Capture
Podatne wersje	do 11.0.0
Typ podatności (CWE)	Stored XSS (CWE-79)
Źródło zgłoszenia	Zgłoszenie do CERT Polska

Opis podatności

CERT Polska otrzymał zgłoszenie o podatności w oprogramowaniu Kofax Capture i koordynował proces ujawniania informacji. Atakujący może spreprować link, który – gdy zostanie użyty przez zalogowanego użytkownika – spowoduje wykonanie kodu JavaScript. Powodem jest niepoprawna walidacja danych przesyłanych metodą POST w końcówce `"/sofer/DocumentService.asc/SaveAnnotation"`. Podatności nadany został identyfikator CVE-2023-5118.

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 Voodoo 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



TRZYDZIESTE
FORUM
TELEINFORMATYKI®
artemis

Malware Database

MWDB



bezpiecznapoczta.cert.pl

Informacje o zagrożeniach

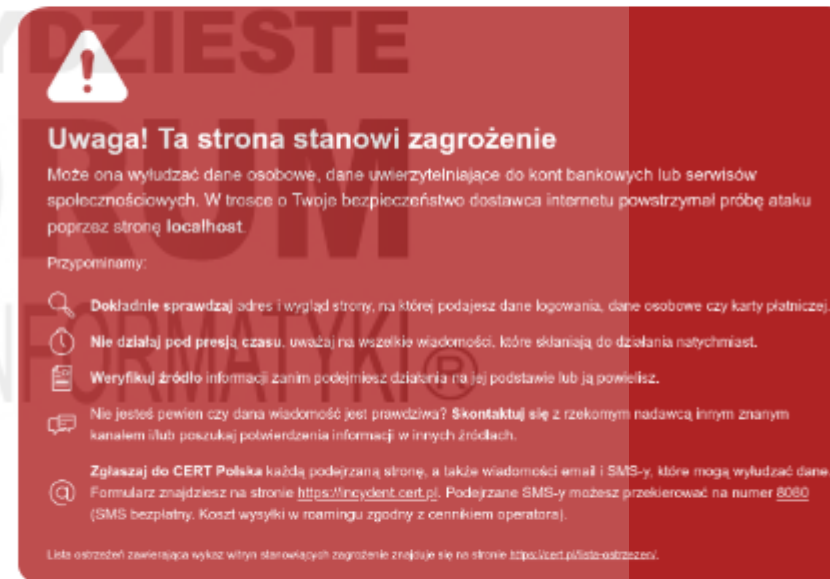


> Lista Ostrzeżeń przed niebezpiecznymi stronami _

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 wyłudniają im dane.

Strony wyłudzające dane osobowe oraz dane uwierzytelniające są obecnie zjawiskiem masowym, dotyczącym różnych grup 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.



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 powstrzymał próbę ataku poprzez stronę localhost.

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 podejmiesz działania na jej podstawie lub ją powielisz.
- Nie jesteś pewien czy dana wiadomość jest prawdziwa? Skontaktuj się z rzekomym nadawcą innym znanym kanałem lub poszukaj potwierdzenia informacji w innych źródłach.
- Zgłaszaj do CERT Polska każdą podejrzaną stronę, a także wiadomości email i SMS-y, które mogą wyłudzać dane. Formularz znajdziesz na stronie <https://incydent.cert.pl>. Podejrzane SMS-y możesz przekierować na numer 8080 (SMS bezpłatny. Koszt wysyłki w roamingu zgodny z cennikiem operatora).

Lista ostrzeżeń zawierająca wykaz witryn stanowiących zagrożenie znajduje się na stronie <https://cert.pl/lista-ostrzezen/>.

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



PRZYDZIESTE
FORUM
TELEINFORMATYKI



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 > Bezpieczna poczta

BETA Jeśli masz uwagi lub komentarze, skontaktuj się z nami pod adresem bezpiecznapoczta@cert.pl.

Bezpieczna poczta

Narzędzie 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 wysłanie testowego e-maila.

Podaj domenę




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

TRZYDZIESTE
FORUM
TELEINFORMATYKI®


cert@cert.pl

 Facebook

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

 Twitter

https://twitter.com/CERT_Polska

 GitHub

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