Analysis of Cybersecurity Incidents Handled by CERT Polska (2015 - 2024)

Prepared by: Grzegorz Szydełko (www.linkedin.com/in/grzegorz-szydełko-2a981a338)

November 2025

Table of Content

1. Executive Summary

The number of incidents handled by CERT Polska has increased from ~1,400 in 2015 to over 103,000 in 2024. The dominant category is vulnerable services, which account for almost 95% of all incidents handled. Other categories of incidents, although less frequent, also require attention and monitoring because they pose a real threat. Based on conservative and polynomial forecast, the total incident volume may reach 257,000-457,000 by 2029. This indicates escalating treat levels and increasing operational load for incident response teams.

2. Dataset Description

The dataset comes from annual CERT Polska „Krajobraz bezpieczeństwa polskiego Internetu" reports (Polish Cyberspace Security Review). Cybersecurity incidents handled by CERT was grouped in 10 main categories:

- Offensive and Illegal Content,
- Malware,
- Information Gathering,
- Intrusion Attempts,
- Successful Intrusions,
- Resource Availability,
- Information Security Attacks,
- Fraudulent Activity,
- Vulnerable Services,
- Others,

This dataset contains informations how much incidents was handled by CERT Polska in each category in individual years between 2015 and 2024.

The data is the basis for analysis historical trends and gives possiblity to try forecast future volumes. It can be used to identify dominant threat types, assess year-over-year growth and support strategic planning in cybersecurity operations.

3. Methodology

- annual incident statistics were extracted from publicly available CERT Polska reports (2015–2024),
- wide format data was transformed into long format to enable easier analysis of distribution of handled incidents,
- future incident volumes (2025–2029) were estimated using polynomial regression and a conservative scenario based on historical growth rates,
- charts were created to visualize the data,
- key insights were derived by comparing incident dynamics across years and categories, with emphasis on significant growth patterns,

Used tools:

- Excel
- Google Sheets
- Polynomial regression calculator: https://stats.blue/Stats_Suite/polynomial_regression_calculator.html

4. Key Findings

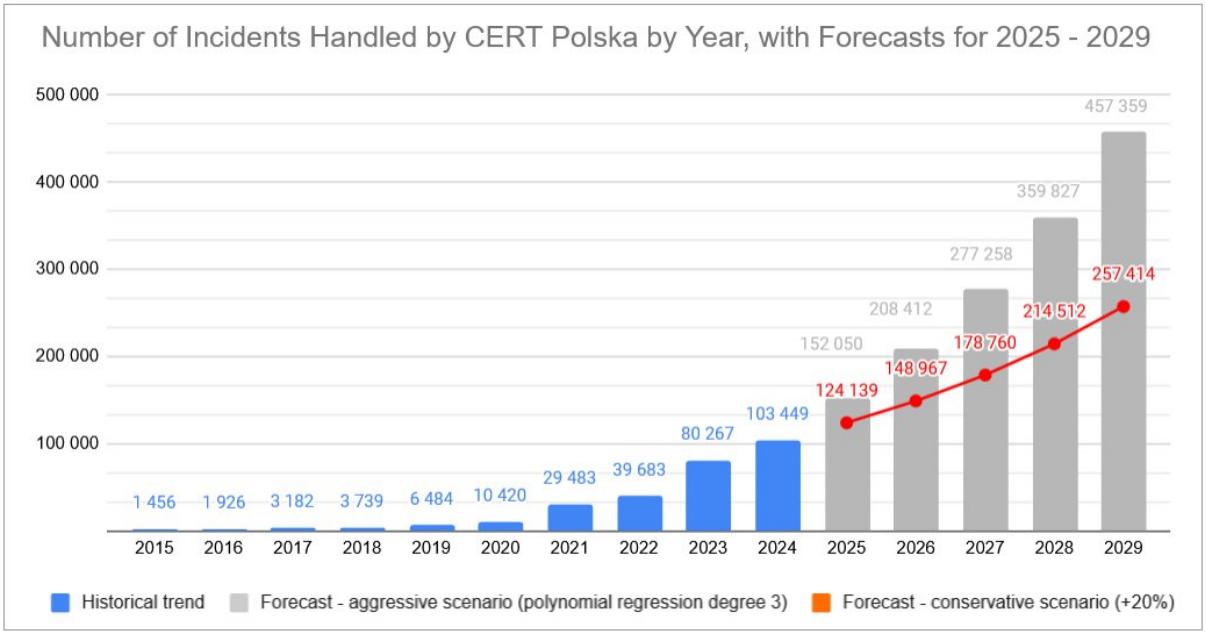

Figure 1. Number of incidents handled by CERT Polska by year, with forecast for 2025 - 2029

- Between 2015 and 2024, the number of incidents handled by CERT Polska is growing year on year. This number increased from ~1,400 in 2015 to ~103,000 in 2024.
- The two largest increases were recorded in 2021 (+183%) and 2023 (+102%). In these years, the number of fraudulent activities handled increased rapidly (see Figure 3). According to CERT Polska reports, the most common type of fraud is phishing. In 2021, the most common phishing campaigns involved stealing Facebook login creditials, while in 2023, the most common target of phishing was investment fraud.
- It should be noted that an increase in the number of incidents handled does not always mean an equal increase in the number of incidents. Public awareness is growing year on year, and security incidents are being reported more frequently.

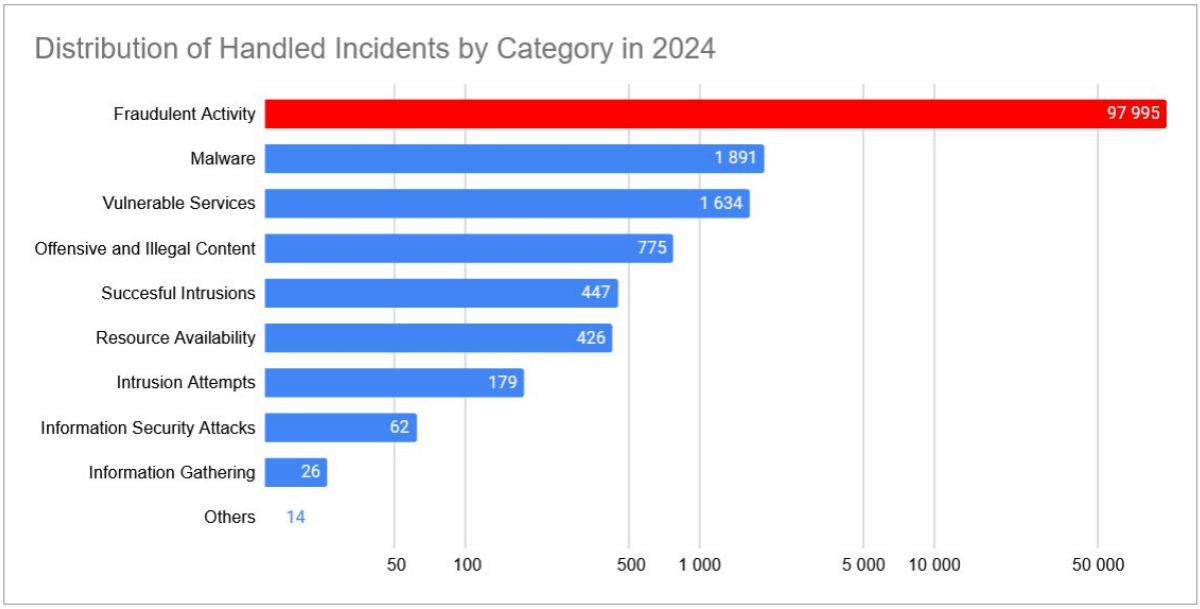

Figure 2. Distribution of handled incidents by category in 2024

- Fraudulent activity is by far the most dominant category. It accounts for almost 95% of incidents handled. All other categories (malware, vulnerable services, offensive and illegal content, successful intrusions, resource avaliabilty, intrusion attempts, information security attacks, information gathering, others) combined account for only a small percentage and have a negligible impact on the annual number of incidents handled.
- The next two common categories in 2024 were malware and vulnerable services. Malware is a major threat due to its widespread use in compromising individual users as well as corporate systems. Vulnerable services are ranked high because exposed, misconfigured or outdated systems are easy entry point for attackers.
- Information gathering was much less common than successful intrusions and intrusion attempts, even though it forms the basis of effective computer system hacking. The low number of incidents of this type is probably due to the fact that information gathering is automatically blocked by firewalls, less frequently monitored, and less frequently reported compared to successful intrusions and intrusion attempts.

5. Forecast

Two methods were used to forecast the number of handled cybersecurity incidents for the years 2025–2029. The first one is polynomial regression degree 3. This method reflects the sharp increase in incidents observed in previous years. The second method is linear growth, assuming a 20% increase over the course of a year (see figure 1).

It should be noted that NIS 2 regulations came into force in the European Union on October 17, 2024. These regulations increase the number of entities that are required to report cyber incidents. These are entities that are key for national security and additonaly others big entities, such as for example manufacturing, waste management, food sector, postal and courier services, ICT services. Work is currently underway in Poland to implement these regulations. Entities that are not required to report incidents do not always do so. Therefore, when the NIS 2 regulations come into force, a rapid increase in incidents requiring handling can be expected.

On the other hand, new security measures are likely to be developed and existing ones improved. This may slow down the increase in the number of incidents. It should also be taken into account that CERT Polska may not be ready and may not have sufficient resources to handle a large, rapidly growing number of incidents. In this situation, the number of incidents handled will be small, even if there are many more incidents requiring handling.

Based on these forecasts, it can be predicted that CERT Polska will handle between ~257,000 and ~457,000 incidents in 2029.

In both scenarios, the number of handled cyber incidents will grow fast in the future, thus increasing the demand for specialists in this field. CSIRT teams, including CERT Polska, must be properly prepared to carry out their tasks in order to ensure security in cyberspace.

6. Category Analysis

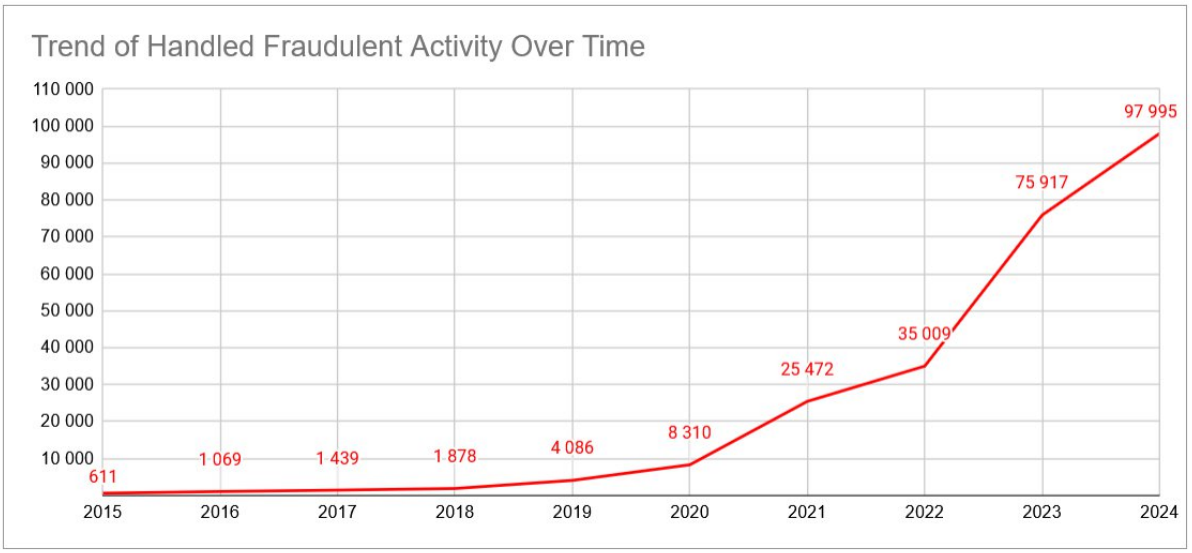

Figure 3. Trend of handled fraudulent activity over time

Fraudulent activity is the most common type of cyber incidents handled by CERT Polska each year between 2015 and 2024. This number is increasing rapidly every year, form ~600 in 2015 to ~98,000 in 2024. This category includes fraud involving the theft of login creditials, personal data or money (e.g. phishing, vishing, investment fraud, fake online stores). These attacks exploit the fact that humans are the weakest link in computer systems. Obtaining login creditials by phishing, for example, is often easier than breaking through security measures. Criminals often change their methods to trick their victims into falling for the scam. This is why there is such a high amount of fraudulent activity.

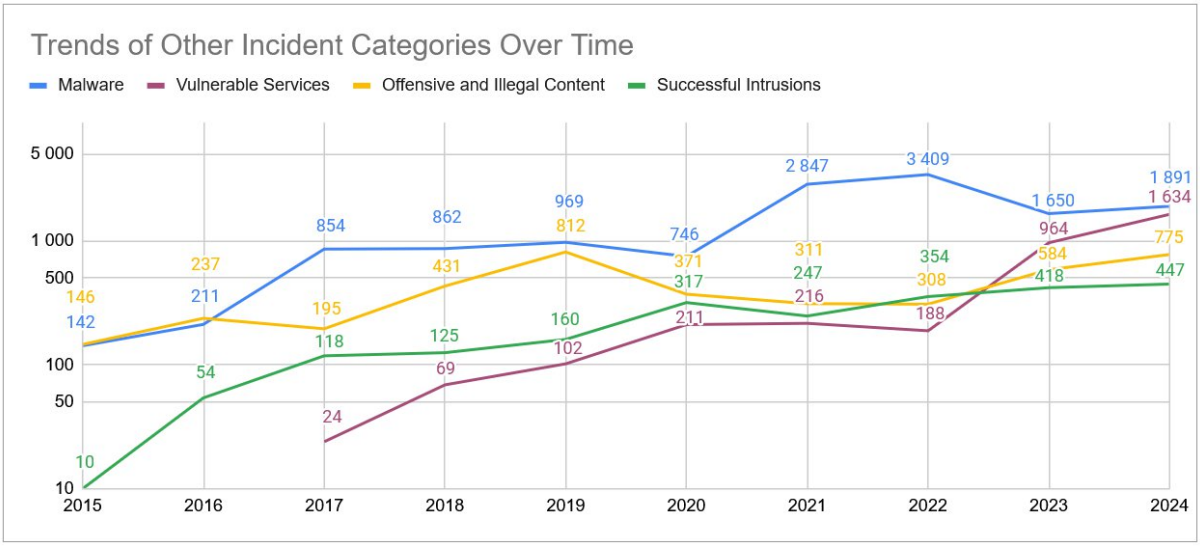

Figure 4. Trends of other incident categories over time

Malware ranks second among the most frequently handled incidents. The two largest increases occurred in 2017 and 2021. In 2017, a series of cyberattacks using the Wanna Cry and NotPetya ransomware appeared worldwide. The increase in 2021 may be related to the fact that remote and hybrid work was popular in Poland between 2020 and 2022 due to the coronavirus pandemic.

In 2017 CERT Polska separated vulnerable services into a separate category. The number of incidents handled in this category remained low until 2023, when it began to rise sharply. This may be due to the large number of services and perhaps their insufficient security, as well as the recent popularity of cloud services.

The handled offensive and illegal content category remains relatively stable over time, with small fluctuations. This may indicate that the number of actual occurrences of this type of incident in Poland also remains stable.

Succesful intrusions number is growing slowly and ranks fifth in terms of the numbers of incidents handled. In 2024, 447 incidents of this category were handled.

The remaining categories (resources avaliability, intrusion attempts, information security attacks, information gathering, others) are handled even less frequently, which means that they rarely occur in Polish cyberspace, are difficult to detect, or simply are not reported.

7. Conclusions

- The number of incidents handled by CERT Polska in 2015-2024 grew rapidly and is likely to continue growing in the future. This growth will result from a real increase in the number of incidents, growing public awareness, and a broader reporting obligation introduced by NIS 2.
- It is worth investing in training to raise awareness and security measures, filters to protect against fraudulent activity, which is the most common threat in cyberspace.
- Although fraudulent activity dominates other categories of threats, we should not forget about the others. Their number is growing every year and they pose a real threat to the security of computer systems.
- It is necessary to keep the operating system and software up to date. This is confirmed by the rapidly growing number of handled incidents in 2023 and 2024, related to vulnerable services.

8. Appendix

a. Table of Figures

b. Data Sources

- CERT Polska (2016), Krajobraz bezpieczeństwa polskiego Internetu w 2015 roku
- CERT Polska (2017), Krajobraz bezpieczeństwa polskiego Internetu w 2016 roku
- CERT Polska (2018), Krajobraz bezpieczeństwa polskiego Internetu w 2017 roku
- CERT Polska (2019), Krajobraz bezpieczeństwa polskiego Internetu w 2018 roku
- CERT Polska (2020), Krajobraz bezpieczeństwa polskiego Internetu w 2019 roku
- CERT Polska (2021), Krajobraz bezpieczeństwa polskiego Internetu w 2020 roku
- CERT Polska (2022), Krajobraz bezpieczeństwa polskiego Internetu w 2021 roku
- CERT Polska (2023), Krajobraz bezpieczeństwa polskiego Internetu w 2022 roku
- CERT Polska (2024), Krajobraz bezpieczeństwa polskiego Internetu w 2023 roku
- CERT Polska (2025), Krajobraz bezpieczeństwa polskiego Internetuw 2024 roku

Retrieved from: https://cert.pl/publikacje/#raport

c. Forecast Formula

$y = 206{,}7018x^3 - 1199{,}7127x^2 + 1895{,}2976x + 1246{,}4$

(polynomial regression degree 3)