ZESZYTY NAUKOWE UNIWERSYTETU PRZYRODNICZO-HUMANISTYCZNEGO W SIEDLCACH, Nr 134
Seria: Administracja i Zarządzanie (61) 2023
pl ISSN 2082-5501

A COMPARATIVE ANALYSIS OF INFORMATION SECURITY INCIDENTS IN PUBLIC ADMINISTRATION IN SELECTED EUROPEAN UNION COUNTRIES

ANALIZA PORÓWNAWCZA INCYDENTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI W ADMINISTRACJI PUBLICZNEJ W WYBRANYCH KRAJACH UNII EUROPEJSKIEJ

https://doi.org/10.34739/zn.2023.61.03

Dominika Lisiak-Felicka

Poland, University of Łodz, Faculty of Economics and Sociology
dominika.lisiak@uni.lodz.pl, ORCID: 0000-0001-8451-4268

JEL Classification Codes: M10, M15

Abstract: The article presents the issue of information security incident management in public administration. The goal of security incident management is to minimize the negative impact of incidents and ensure the continuity of the organization's operations. It is critical to know what the threats are, including the number and types of incidents reported. The aim of the work is to compare statistical data on information security incidents in selected EU countries, according to their types, especially in the public administration sector. It outlines key incident management and legal issues related to the topic of security incidents, and the work of computer incident response teams. Examples of incidents that took place recently in public administration units in Poland are also presented. This is followed by an analysis of statistical data on reported incidents in Poland in the years 2020-2022, and the results were compared with the number of incidents reported in selected European Union countries. The results of the study show that the dominant type of incidents is fraud (mainly phishing), and public administration is one of the main targets of cybercriminals' attacks. The difficulties in conducting such a comparative analysis have also been demonstrated.
Keywords: information security management, information security incidents, cybersecurity, threats, public administration

Abstrakt: Artykuł przedstawia problematykę zarządzania incydentami związanymi z bezpieczeństwem informacji w administracji publicznej. Celem zarządzania incydentami bezpieczeństwa jest minimalizacja negatywnego wpływu incydentów oraz zapewnienie ciągłości działania organizacji. Niezwykle istotna jest wiedza o zagrożeniach, w tym o liczbie i typach zgłaszanych incydentów Celem pracy jest porównanie danych statystycznych o incydentach związanych z bezpieczeństwem informacji w wybranych krajach UE, według ich typów, szczególnie w sektorze administracji publicznej. Przedstawiono w nim kluczowe kwestie dotyczące zarządzania incydentami oraz zagadnienia prawne związane z tematyką incydentów bezpieczeństwa i pracą zespołów reagowania na incydenty komputerowe. Przedstawiono również przykłady incydentów, jakie miały miejsce ostatnio w jednostkach administracji publicznej w Polsce. Następnie przeprowadzono analizę danych statystycznych o raportowanych incydentach w Polsce w latach 2020-2022, a wyniki porównano z liczbami incydentów zgłaszanych w wybranych krajach Unii Europejskiej. Wyniki badania pokazują, że dominującym typem incydentów są oszustwa (głównie phishing), a administracja publiczna jest jednym z głównych celów ataków cyberprzestępców. Wykazano również trudności w przeprowadzaniu takich analiz porównawczych.
Słowa kluczowe: zarządzanie bezpieczeństwem informacji, incydenty związane z bezpieczeństwem informacji, cyberbezpieczeństwo, zagrożenia, administracja publiczna

Introduction

An information security incident is defined in ISO/IEC 27000, as a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (ISO/IEC 27000:2018 – 3.31). This may include unauthorized access to data, the loss or theft of information, damage to or destruction of information systems, and actions to disrupt the normal operation of information systems or services. Sometimes in the literature, the term "computer security incident" or the term "cyber incident" can be found (Kjaerland, 2006).Such incidents occur in all organizations, including public administration units. Table 1 presents some incidents

that took place recently in the public administration in Poland.

Earlier research carried out by the author of this article also confirms that local government administration units have difficulties with proper management of incidents related to information security. It has been shown, among other things, that most public administration offices do not register incidents related to information security. And those offices that keep records show very small numbers of incidents in their reports. (Lisiak-Felicka, Szmit, 2016; Lisiak-Felicka, Szmit, 2021).

This article aims to compare the data about information security incidents in selected EU countries, especially by numbers, types and in the public administration sector. To achieve the aim of the research, the following research questions were formulated:

- Q1: How many incidents have been reported to computer security incident response teams of selected EU countries in years 2020-2022?
- Q2: What were the dominant types of incidents reported?
- Q3: Is local government administration one of the main targets of cybercriminal attacks?

The theoretical part focuses on managing incidents related to information security and legal issues. The practical part includes an analysis of statistical data in six selected EU countries in the years 2020-2022, other researchers' results were referred to in the discussion. Finally, the most important conclusions, limitations, and directions for further research were also indicated.

Table 1. Samples of recent information security incidents in public administration in Poland

Date	Description of incidents
2022-08-15	Hacking into the servers of the Pawłowice Municipality Office and encrypting the databases using ransomware software (Urząd Gminy Pawłowice, 2023).
2022-09-20	A cybercriminal took over the account of one of the employees and published (replaced) information on the eFaktura.gov.pl portal. The government website was supposedly hacked by an Indonesian group. In addition, for a long time, obscene content appeared on the platform, which was indexed in Google's search engine (Palczewski, 2022).
2022-11-07	A DDoS attack from external servers on the infrastructure of the eZamowienia platform (*Busines Insider*, 2022).
2022-12-05	A ransomware attack on Marshall Office of Mazovian Voivodeship (Biuletyn Informacji Publicznej Samorządu Województwa Mazowieckiego, 2022).
2023-02-28	The government website of the podatki.gov.pl portal was unavailable. After a long time spent logging in to the domain, the message "This site is unreachable" appeared. The government domain was unavailable due to a Russian DDoS cyberattack (Florek, 2023).
2023-04-19	Hacker attack on city office. About 30,000 phone numbers of residents were leaked. Unauthorized persons gained access to telephone numbers and the content of messages from the Poznań City Office (ePoznan.pl, 2023).
2023-06-13	A DDoS attack on the ePUAP platform. Services were available, but there were disruptions (Serwis samorządowy PAP, 2023).
2023-06-24	A hacker attack on the IT systems of the municipal unit of ZDZiT in Olsztyn. As a result of the hacker attack, there were inoperative traffic control systems, inoperative ticket machines and limited access to the passenger information system. (Urząd Miasta Olsztyn, 2023).

Source: own elaboration based on information about cyber-attacks.

Literature review and theoretical basis

In the Scopus database between 2003 and 2023, there were 300 articles with the keyword "information security incidents", the vast majority were related to computer science aspects. Only 22 included the keyword "incident management" and none of the documents connected with "public administration" were found. Similarly, for the keyword "cybersecurity incidents" there were 297 documents found, 9 with the "incident management" and one containing the "public administra-tion" keyword. Many publications with information security management issues concern reviews and surveys in the field of information security in public administration units in individual countries, but there are no comparative analyses (Banciu et al., 2020; Nagy-Takács, Berényi, 2022; Rehbohm et al., 2019; Ubowska, Królikowski, 2022; Baničević, 2018).

Information security incidents can result from a variety of factors, such as a cyber-attack, human error, faulty software, hardware failures, external or internal actions, and many others. They are unpredictable and can affect organizations, businesses, institutions, or individuals. They can lead to a variety of consequences, such as a loss of data confidentiality, reputational damage, financial losses, loss of customer confidence, legal or regulatory sanctions, and disruption of normal business operations. To minimize the risk of information security incidents, organizations implement various security measures, such as securing information systems, applying security policies, training personnel, monitoring network activity, encrypting data, and many others (Tøndel, 2014; Patterson et al., 2023).

Information security incident management refers to all processes and procedures that should be used by organizations to effectively respond to and mitigate any potential or actual security breaches, cyber-attacks or other incidents that could threaten the confidentiality, integrity, or availability of information. It is defined as "a set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents" (ISO/IEC 27000:2018 – 3.32). Incident management is a key aspect of maintaining the security of data and systems in cyberspace. The general steps in this process are "plan and prepare", "detect and report", "assess and decide", "respond" and "learn lessons". Incident management is a continuous and dynamic process (ISO/IEC 27035-1:2023).

In addition to management issues, legal aspects are also important. In Poland, there are several legal acts related to cybersecurity incidents, which define the obligations, procedures and sanctions related to the protection of critical infrastructure and response to cyber-attacks. Detailed issues regarding the handling of incidents are discussed in the Act of 5 July 2018 on the national cybersecurity system and related implementing acts. They define the organization of the national cybersecurity system as well as the tasks and responsibilities of the entities comprising this system, the manner of supervision and control in the application of the provisions of the Act and the scope of the Cybersecurity Strategy of the Republic of Poland for 2019-2024. The aim of the national cybersecurity system is to ensure cybersecurity at the national level, including the uninterrupted provision of key services and digital services, by achieving an appropriate level of security for information systems used to provide these services and ensuring incident handling. In the context of EU law, need to be considered, in the field of cybersecurity, especially the new Network and Information Systems Directive 2 (NIS2).

The above-mentioned legal acts constitute the legal basis for activities related to cybersecurity and response to cyber incidents in Poland. It is important that both public and private entities comply with these regulations and take appropriate measures to protect their IT systems and data.

Research method

The research methods used are a literature review and a quantitative analysis of information security incidents in selected six European Union countries (mentioned below).

As a part of the research work, a literature review and an analysis of the source documents were conducted. Statistical data was collected based on reports on the activities of nationality and government computer security incident response teams from selected countries:

1. Poland: CERT.PL and CSIRT.GOV.PL,
2. Portugal: CERT.PT,
3. Croatia: CERT.HR,
4. Slovenia: SI-CERT,
5. Czech Republic: CSIRT.CZ and GovCERT.CZ,
6. Italy: CSIRT.IT.

The choice of the above countries was determined by two factors: the availability of statistical data on incidents in the reports and the score of the cyber security index. One country with a similar value of the index as Poland, two countries with a significantly lower index and two countries with a very high index were selected for the analysis. The values of the indexes are presented in Table 2. The surveyed teams are ENISA CSIRTS network members. Microsoft Excel and Microsoft Power BI software were used to prepare tables and visualizations.

Table 2. Cyber security indexes for surveyed countries

Country	Cyber Security Index 2020
Poland	93.86
Portugal	97.32
Croatia	92.53
Slovenia	74.93
Czech Republic	74.37
Italy	96.13

Source: own elaboration based on Cyber Security Index 2020 report (ITU, 2020).

Results and discussion

To achieve the goal related to good incident management, the information about numbers and types of them should be known.

Poland

In Poland, there are three groups responsible for reporting incidents. Every year two of them prepare annual reports including information about the number of reported incidents. These are the CERT.PL and CSIRT.GOV.PL organizations. Numbers of reported incidents are shown in Figure 1. Based on the received notifications (number of requests), CERT.PL performs careful classification, based on which it selects a certain number of notifications (number of selected requests), from which it, in turn, registers cybersecurity incidents (number of incidents).

In 2021, CERT.PL recorded an increase in incidents handled at the level of 182% compared to the 2020 year. In 2022, the team observed an over 34% increase in registered cybersecurity incidents compared to the previous year. The increase in reports and cybersecurity incidents is certainly due to the growing awareness of the team. In 2022, a social campaign was launched on media that informed about the threats and how to report them. The most frequently reported type of incidents registered in the analyzed period were computer frauds, in particular phishing. Another type of incident that was frequently reported in the analyzed years was malware. The third type of incidents that occurred most often was abusive content (in 2020 and 2021), and intrusions (in 2022), e.g., burglaries to IT systems and e-mail accounts (Fig. 2). Table 3 presents data about information security incidents in the public administration in Poland in the surveyed years. The number of incidents in this sector has not exceeded 4%.

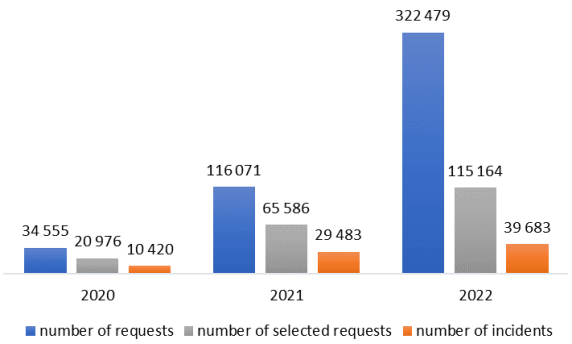

Figure 1. Numbers of requests, selected requests and incidents reported by CERT.PL

Source: own elaboration based on Cert.pl reports.

Type	2020	2021	2022
Fraud	8 310	25 472	35 009
Malicious code	746	2 847	3 409
Intrusions	317	247	354
Abusive Content	371	311	308
Vulnerable services	211	216	188
Availability	121	148	175
Intrusion attempts	174	127	121
Other	42	33	49
Information content security	68	55	39
Information gathering	60	27	31

Figure 2. Types of incidents reported by CERT.PL

Source: own elaboration based on Cert.pl reports.

Table 3. Security incidents in the public administration in Poland

Year	Number of incidents	Number of incidents [%]
2020	388	3.72
2021	429	1.46
2022	757	1.91

Source: own elaboration based on Cert.pl reports.

On the other hand, the CSIRT.GOV.PL team registered 1,234,040 requests of a potential incident in 2022. The recorded number of notifications is an increase compared to the previous year, in which 762,175 notifications were registered. The number of notifications translated into 21,563 events classified and registered as information security incidents in 2022 (Fig. 3). Among the registered incidents in 2022, the largest part was reported from the ARAKIS GOV early warning system (16,604). The remaining 4,959 were incidents from reports submitted to the CSIRT.GOV.PL by entities of the national cybersecurity system. Tab. 4 presents incident statistics by selected entities and Fig. 4 – incidents by type.

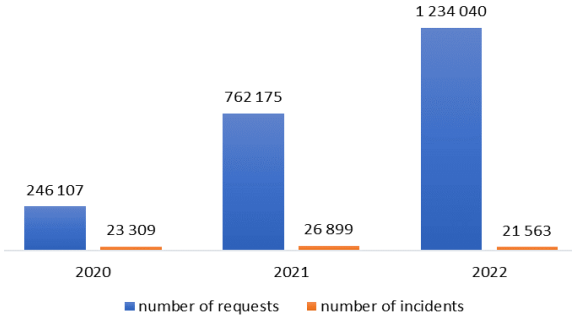

Figure 3. Numbers of requests and incidents reported by CSIRT.GOV.PL

Source: own elaboration based on Cert.pl reports.

Table 4. Incident statistics by type of entities

Entity	2020	2021	2022 reports	2022 ARAKIS system	2022 total
office	8,356	5,563	809	2,301	3,110
others	4,714	644	650	2,189	2,839
critical infrastructure	2,626	9,196	1,798	5,547	7,345
institution	2,518	7,203	400	2,758	3,158
public administration	2,039	0	0	0	0
ministry	1,656	3,056	503	2,197	2,700
services and the army	1,400	1,237	0	0	0
state authority*	0	0	599	1,262	1,861
services*	0	0	200	350	550
total	23,309	26,899	4,959	16,604	21,563

Source: own elaboration based on Csirt.gov.pl reports. Note: * – since 2022.

Type	2020	2021	2022
vulnerability	1 366	1 148	2 187
social engineering	0	904	1 053
unavailability	254	310	826
publication	11	158	316
content	0	0	191
attack	96	74	174
scanning	2 604	118	151
virus	16 777	24 171	61
botnet	36	16	0
burglary	8	0	0
discredit	66	0	0
leak	230	0	0
phishing	1 396	0	0
spam	311	0	0
spoofing	72	0	0
swap	13	0	0
wrong configuration	69	0	0

Figure 4. Types of incidents reported by CSIRT.GOV.PL

Source: own elaboration based on Csirt.gov.pl reports.
Note: the year 2022 does not include incidents reported by the ARAKIS system.

Portugal

CERT.PT recorded a 26% increase in the number of cybersecurity incidents in 2021 compared to the previous year, exceeding from 1,418 events recorded in 2020 to 1,781 in 2021. Types of incidents are presented in Figure 5. In 2021, 33% of incidents were registered in public entities, which is a difference of 2 percentage points (pp) compared to the previous year, when 31% of incidents were recorded in public entities. The data from 2022 is unavailable.

Type	2020	2021
Phishing	613	715
Social engineering	0	246
Distribution of malware	119	226
Commitment of non-privileged account	111	114
Illegitimate use of third party name	32	80
Undetermined (other)	28	50
Infected system (malware)	169	46
Vulnerable system (vulnerability)	41	44
Unauthorized modification (ransomware)	0	38
Vulnerability exploitation (intrusion)	0	37
Commitment of application	55	0
Login attempt	26	0
Unauthorized access	58	0

Figure 5. Types of incidents reported by CERT.PT

Source: own elaboration based on Cert.pt reports.

The distribution of cybersecurity incidents by sector and government area shows an increase in the government area from eighth position in 2020 to third position the following year (9% in 2021). The area of internal administration also saw a sharp relative increase in the number of incidents, ranking in sixth place (6% in 2021), while local administration saw a decrease by one place and is in 8th place in 2021 (4%).

Croatia

In 2020, the national CERT.HR handled a total of 1,710 computer security incidents. The leading types of incidents were phishing URL, phishing and password guessing. In 2021, 1,211 incidents were registered. The leading types were phishing URL,

phishing, and malware URL. During 2022, a total of 1,296 incidents were registered and the leading types of incidents were phishing, scam, and phishing URL. Figure 6 presents types of incidents reported by CERT.HR. Unfortunately, CERT.HR does not publish data on incidents by sector of the economy.

Type	2020	2021	2022
Phishing	277	166	371
Scam	45	25	191
Phishing URL	446	353	186
Guessing passwords	205	111	130
Web defacement	188	112	71
Malware URL	132	139	67
System infected with malicious code	83	96	54
Attempt to exploit a vulnerability	59	57	48
Spam url	21	0	48
Shakedown	0	0	34
Spam	35	20	27
Business fraud	0	0	19
DoS - volumetric attack	27	39	17
User account	29	20	11
C&C (command and control)	12	3	7
Scanning	12	3	5
Outage	5	6	4
DoS - attack on the application layer	1	11	2
Malicious web site	0	0	2
Other	2	17	2
Hoax	116	15	1
Malicious cryptocurrency mining	0	0	1
Availability	1	0	0
Collecting information	0	1	0
Cryptojacking	1	0	0
Scams	13	17	0

Figure 6. Types of incidents reported by CERT.HR

Source: own elaboration based on Cert.hr reports. Note: in 2022 there is a mistake in data. Total number of incidents is 1 298, while in Report 1, 296 incidents were noted.

Slovenia

SI-CERT recorded 4,123 cyber incidents in 2022. It represents a 30% increase compared to 2021 (3,177). In 2020, there were 2,775 incidents. Once again, phishing attacks lead the way. In 2022, the SI-CERT dealt with 1,432 phishing incidents, and in 2021 – 950, which means that the greatest growth was again recorded in this category. Figure 7 presents the types of incidents reported by the Slovenian team. Among all sectors of the economy, there were 39 phishing incidents in the public administration sector, making this sector the 5th most frequently attacked sector in 2022.

Type	2020	2021	2022
Fraud	1 848	2 094	2 900
Malicious code	295	306	375
Other	279	310	321
Intrusions	93	116	118
Unclassified	9	8	112
Abusive content	97	133	107
Vulnerable	36	57	72
Information gathering	31	42	45
Information Content Security	26	40	28
Availability	40	37	23
Intrusion attempts	20	33	21
Test	1	1	1

Figure 7. Types of incidents reported by SI-CERT

Source: own elaboration based on Cert.si reports.

Czech Republic

GovCERT.CZ reported 146 cyber security incidents in 2022. Despite a significant increase in reports, there was a slight year-on-year decrease in recorded incidents in 2022. In 2021, there were 157 incidents. In 2020, there were 99 incidents. The public sector is traditionally one of the most affected sectors, with 2022 being no different. A total of 51 cyber incidents were registered in this sector, which makes up more than a third of their total number. Compared to last year, however, the nominal representation of incidents decreased slightly (62 in 2021). In 2020, there were 52 incidents. The largest number of cyber-attacks focused on data availability (Figure 8a).

In turn, in 2020, the CSIRT.CZ reported 1,267 incidents. In 2021, the number was increased to 1,725 and 2,067 in 2022. The statistics of incidents by type reported by CSIRT.CZ are shown in Figure 8b.

(a)

Type	2020	2021	2022
Availability	29%	34%	58%
Penetration	9%	22%	12%
Fraud	15%	10%	11%
Information security	4%	8%	10%
Malicious code	36%	25%	8%
Inne	0%	0%	3%
Abusive content	0%	0%	0%
Collection of information	2%	0%	0%
Penetration attempt	4%	1%	0%

b)

Type	2020	2021	2022
Phishing	738	1 297	1 485
Malware	111	153	228
Spam	216	163	220
Information gathering	97	74	71
Intrusions	3	1	39
Other	86	26	24
DoS	16	11	0

Figure 8. Types of incidents reported by GovCERT.CZ (a) and CSIRT.CZ (b)

Source: own elaboration based on govcert.cz and csirt.cz reports. Note: GovCsirt.cz gives numbers of incidents in percentage.

As can be seen from Figure 8b, in 2022, there was an increase in phishing, malware, spam and intrusion. In 2021, just like in the previous year, there was a fundamental increase in phishing. In addition, there was an increase in the number of incidents in the category of malware. In all other categories, there was a decrease in the number of incidents.

Italy

In 2021, from the CSIRT.IT analysis and subsequent classification of the events detected between September and December of 2021; the following 5 most frequent types emerge: Spread of malware: 151 occurrences; Brand abuse: 59 occurrences; Vulnerability exploitation: 47 occurrences; Phishing: 45 occurrences; Ransomware: 39 occurrences.

In 2022, CSIRT.IT dealt with 1,094 cyber incidents. From the analysis and subsequent classification of the 1,094 cyber events, it was possible to identify the types shown in Figure 9. By classifying the ransomware victims according to economic activity sectors, it emerges that the second most affected in 2021 was public administration. In 2022, the share of ransomware attacks on state administration bodies decreased.

Type	2022
spreading malware via email	517
brand abuse	204
phishing	203
ransomware	130
vulnerability exploitation	126
information disclosure	103
exploit vulnerability towards web server	87
scans	74
data exposure	67
credential intrusion attempts	64

Figure 9. Types of incidents reported by CSIRT.IT (top ten)

Source: own elaboration based on Csirt.it reports. Note that each of the incidents may have been associated with one or more types. Previous data is unavailable.

For the collected data, an analysis of the changes in the number of incidents was performed (Table 5). Measures of dynamics were calculated, which indicate the percentage of changes in the phenomenon in the analysed period in relation to the previous one (relative change) according to the formula:

$$Relative\ change(v_{ref}, v) = \frac{Actual\ change}{v_{ref}} \times 100\% = \frac{v - v_{ref}}{v_{ref}} \times 100\%$$

Table 5. Relative changes in numbers of incidents in selected computer security incident response teams between years 2020-2021 and 2021-2022

Team	2020-2021	2021-2022
CERT.PL	183%	35%
CSIRT.GOV.PL	15%	-20%
CERT.PT	26%	N/A
CERT.HR	-29%	7%
SI-CERT	14%	30%
GovCERT.CZ	59%	-7%
CSIRT.CZ	36%	20%

Source: own elaboration based on obtained data.

Most teams have seen an increase in incidents year over year. Decreases were recorded only in CERT.HR (2020-2021) and CSIRT.GOV.PL and Gov.CERT.CZ (2021-2022).

In comparison to the results, Poland registered the biggest number of incidents. Other countries report several thousand incidents each year, while Poland reports tens of thousands of such incidents. Poland is the second largest country by population in this group and the disproportion could be a result of the automatic system used to report incidents (e.g., ARAKIS) and including data from these systems in reports. The dominant type of incidents in surveyed countries is fraud (especially phishing). This is the first place in Poland, Portugal, Croatia, and Slovenia. The malicious code (Poland, Slovenia) and spreading malware via e-mail (Italy) are also popular. Incidents such as social engineering, scams, spam, attacks on availability, and using vulnerability are quite a large group. The public administration is not the most important target for cybercriminals, but it is at the forefront of the attacked sectors. The results are like the results from the ENISA report, where during the reporting period (July 2021 – June 2022), many incidents targeting public administration and government can be observed – 24.21 % of all incidents. (ENISA, 2022). The conducted analysis enabled finding answers to the research questions.

As can be seen from the above data and examples, comparative analysis is difficult to perform as there are no uniform report templates published by computer security incident response teams. Not all countries provide data for individual economic sectors (e.g., Croatia). Some characterize the public administration sector in terms of a specific group of incidents (e.g., phishing – Slovenia, ransomware – Italy). The lack of a unified classification of incidents also makes statistical analysis even more difficult.

The above results were consistent with the results of other scientists and companies preparing reports on IT threats. Malware is the top security threat in the Romanian landscape (Cristea, 2020). Polish scientists (Ubowska, Królikowski, 2022) also declared that many cases related to data destruction or corruption (e.g., due to malware infection) or disclosed confidential data (e.g., due to hacking, pharming, phishing). On the other hand, Insights for Professionals (IFP, 2022) lists, apart from malware, and phishing, also attacks against cloud security. Forrester expects the top five cybersecurity threats: generative AI tools, geopolitical threats, cloud complexity, ransomware, and social engineering, that organizations will face in future (Forrester, 2023).

A good solution to compare the numbers of incidents is CIRAS – the Cybersecurity Incident Reporting, and Analysis System, maintained by ENISA (The European Union Agency for Cybersecurity). It supports the member states in submitting incident reports (ENISA, 2023). The aim of the online tool is to facilitate the gathering of the incident details per sector, per country. However, when analysing the number of incidents (e.g., 1 083 reported incidents in 2022), it can be concluded that not all countries participated in this project. The situation may be improved by the NIS2 directive implemented in 2023, which updates and harmonises EU cybersecurity regulations (Kabelka, 2022).

Conclusions

Knowledge of the numbers and types of incidents in individual EU countries, considering economic sectors, would contribute to better information security management. Information of the threats and attacks to which public administration units are currently exposed could be the basis for even better identification of risk sources and would also contribute to proper security planning. The system implemented by ENISA would be a good solution for introducing reported incidents, under the cognition that data from all member states will be available, considering the dates of occurrence, types of incidents, sectors of the economy. This would facilitate the comparative analysis of incident data and help authorities recognize and respond to current trends and vulnerabilities.

It should be noted that the noticeable significant increase in the number of incidents in selected reports is also the result of the automation introduced in the attack detection systems. Computer security incident response teams are developing their detection systems, which translates into an increased number of registered incidents.

Limitations and future research directions

There are two main limitations of this research. Firstly, the national CSIRTs reports are prepared according to their templates. They are significantly different. Not all data is presented in them, which makes it difficult to conduct advanced analyses. Secondly, not all cases are reported to the national CSIRTs, so these teams do not have comprehensive information about all incidents that have occurred.

As part of further work, the scope of the research could be extended to other countries of the European Union. It would be worth trying to conduct a questionnaire survey among these teams. The obtained data would be a good source for conducting advanced statistical analyses.

References

Act of 5 July 2018 on the national cybersecurity system. Journal of Laws 2018, item 1560. [Act of July 5, 2018. National cybersecurity system].

Banciu, D., Rădoi, M., Belloiu, S. (2020). Information security awareness in Romanian public administration: An exploratory case study. *Studies in Informatics and Control*, (291), 121–129. DOI: 10.24846/v29i1y202012.

Baničević, P. (2018). Cyber Security and Public Administration in Croatia. Retrieved from https://commons.lib.jmu.edu/cgi/viewcontent.cgi?article=1003&context=ese.

Biuletyn Informacji Publicznej Samorządu Województwa Mazowieckiego (2022). *Incydent cyberbezpieczeństwa*. [Cybersecurity incident]. Retrieved from https://mazovia.pl/pl/bip/komunikaty/incydent-cyberbezpieczenstwa-1.html.

Business Insider (2022). Hakerzy zaatakowali rządową stronę. [Hackers attacked government website]. Retrieved from https://businessinsider.com.pl/wiadomosci/hakerzy-zaatakowali-rzadowa-strone-atak-z-serwerow-poza-granicami-kraju/5c8kr1c.

Cert.hr (2023). Godišnji izvještaj. [Annual reports]. Retrieved from https://www.cert.hr.

Cert.pl (2023). Raporty roczne z działalności zespołu CERT Polska. [Annual reports on the activities of the CERT Polska team]. Retrieved from https://cert.pl.

Cert.pt (2023). Riscos & Conflitos 3a edição. [Risks and Conflicts, 3rd Edition]. Retrieved from https://www.cncs.gov.pt.

Cert.si (2023). Poročilo o kibernetski varnosti za leto 2022. [2022 Cyber Security Report]. Retrieved from https://www.cert.si.

Csirt.cz (2023). Zpráva o činnosti csirt.cz. [Report on the activity of csirt.cz]. Retrieved from https://csirt.cz/.

Csirt.gov.pl (2023). Raporty o stanie bezpieczeństwa cyberprzestrzeni RP. [Reports on the state of Poland's cybersecurity]. Retrieved from https://csirt.gov.pl.

Csirt.it (2023). 2022 Relazione annuale al parlamento. [2022 Annual report to parliament]. Retrieved from: https://www.acn.gov.it/.

Cristea. L.M. (2020). Current security threats in the national and international context. *Accounting and Management Information Systems*, 19(1): 351-378. DOI: http://dx.doi.org/10.24818/jamis.2020.02007.

ENISA (2023). CIRAS – the Cybersecurity Incident Reporting and Analysis System. Retrieved from https://ciras.enisa.europa.eu/.

ENISA (2022). ENISA THREAT LANDSCAPE 2022. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

Epoznan.pl (2023). Poznański magistrat rozsyła wiadomość do mieszkańców: doszło do ataku hakerskiego. [Poznan municipality sends message to residents: there was a hacking attack]. Retrieved from https://epoznan.pl/news-news-138924-poznanski_magistrat_rozsyla_wiadomosc_do_mieszkancow_doszlo_do_ataku_hakerskiego_naruszenie_bezpieczenstwa_u_naszego_dostawcy_uslug_sms.

Florek, D. (2023). Cyberatak na stronę podatki.gov.pl. [Cyber-attack on podatki.gov.pl website]. Retrieved from https://www.bankier.pl/wiadomosc/Cyberatak-na-strone-podatki-gov-pl-8496933.html.

Forrester (2023). Top Cybersecurity Threats in 2023. Retrieved from https://www.forrester.com/report/top-cybersecurity-threats-in-2023/RES179154.

Govcert.cz (2023). Zpráva o stavu kybernetické bezpečnosti České republiky. [Reports on the state of cybersecurity in the Czech Republic for the year 2022]. Retrieved from https://www.nukib.cz/.

IFP (2022). 10 Types of Security Threat and How to Protect Against Them. Retrieved from https://www.insightsforprofessionals.com/it/security/types-of-security-threat.

ITU (2020). Global Cybersecurity Index 2020. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

Kabelka, L. (2022). EU's cyber incident reporting mechanism does not work, agency chief warns. Retrieved from https://www.euractiv.com/section/cybersecurity/news/eus-cyber-incident-reporting-mechanism-does-not-work-agency-chief-warns/.

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, 25(7): 522–538. DOI: 10.1016/j.cose.2006.08.004.

Lisiak-Felicka, D., Szmit, M. (2016). *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia* [Cyber security of public administration in Poland. Selected issues]. Kraków: European Association for Security.

Lisiak-Felicka, D., Szmit, M. (2021). Zarządzanie bezpieczeństwem informacji w urzędach administracji samorządowej. Główne problemy [Information security management in local government offices. Main problems], in: J. Grubicka, A. Kamińska-Nawrot (Eds.), *Współczesny człowiek wobec wyzwań: szans i zagrożeń w cyberprzestrzeni* (pp. 101-115). [Modern man facing challenges: opportunities and threats in cyberspace]. Słupsk: Akademia Pomorska w Słupsku.

Nagy-Takács, V., Berényi, L. (2022). *Information Security Management System Standards in Hungarian Public Administration.* ACM International Conference Proceeding Series, 112-117, DOI: 10.1145/3551504.3551554.

Palczewski, S. (2022). Zhakowano rządowy serwis. Pomimo obowiązywania CHARLIE-CRP. [A government service was hacked. Despite the validity of CHARLIE-CRP]. Retrieved from https://cyberdefence24.pl/cyberbezpieczenstwo/zhakowano-rzadowy-serwis-pomimo-obowiazywania-charlie-crp.

Patterson, C.M., Nurse J.R.C., Virginia N.L. Franqueira, V.N.L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers &* Security, 132, 1-16. DOI: 10.1016/j.cose.2023.103309.

Rehbohm, T., Sandkuhl, K., Kemmerich, T. (2019). On challenges of cyber and information security management in federal structures – The example of German public administration (Conference Paper). *CEUR Workshop Proceedings*, Volume 2443, 1-13.

Serwis samorządowy PAP (2023). Minister Cyfryzacji: cyberatak na ePUAP. [Minister of Digitization: cyber-attack on ePUAP]. Retrieved from https://samorzad.pap.pl/kategoria/e-urzad/minister-cyfryzacji-cyberatak-na-epuap.

Tøndel, I.A., Line, M.B., Jaatun, M.G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, 45, 42–57. DOI: 10.1016/j.cose.2014.05.003.

Ubowska, A., Królikowski, T. (2022). Building a cybersecurity culture of public administration system in Poland. *Procedia Computer Science*, 207, 1242–1250. DOI: 10.1016/j.procs.2022.09.180.

Urząd Gminy Pawłowice (2022). Cyberatak na Urząd Gminy Pawłowice. [Cyber-attack on Pawlowice Municipality Office]. Retrieved from https://www.pawlowice.pl/aktualnosci/artykul/news/cyberatak-na-urzad-gminy-pawlowice/.

Urząd Miasta Olsztyn (2023). Atak hakerski na systemy informatyczne ZDZiT w Olsztynie. [Hacking attack on IT systems of ZDZiT in Olsztyn]. Retrieved from https://olsztyn.eu/o-olsztynie/aktualnosci/article/zdzit-bezpieczestwo-15485.html.