Systemy Logistyczne Wojsk
Zeszyt 61 (2024)
ISSN 1508-5430, s. 193-210
DOI: 10.37055/slw/203443

Instytut Logistyki
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Military Logistics Systems
Volume 61 (2024)
ISSN 1508-5430, pp. 193-210
DOI: 10.37055/slw/203443

Institute of Logistics
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Trends in the occurrence of ICT incidents in terms of cybersecurity

Tendencje w występowaniu incydentów ICT w aspekcie cyberbezpieczeństwa

Rafał Parczewski
borys174@wp.pl; ORCID: 0000-0002-2603-0596
Faculty of Security, Logistics and Management, Military University of Technology, Poland

Patrycja Guzanek
patrycja.guzanek@student.wat.edu.pl; ORCID: 0000-0001-6650-7187
Faculty of Security, Logistics and Management, Military University of Technology, Poland

Robert Szczur
robert.szczur@wat.edu.pl; ORCID: 0009-0000-7210-814X
Military University of Technology, Poland

Łukasz Ilczuk
lukasz.ilczuk@wat.edu.pl; ORCID: 0009-0003-5636-6992
Military Training College, Military University of Technology, Poland

Przemysław Jabłoński
przemek.jablonski.9@gmail.com; ORCID: 0009-0003-7376-9486
41st Training Aviation Base, Poland

Ewa Jankiewicz
ewa.jankiewicz@wat.edu.pl; ORCID: 000-0003-1689-0733
Military University of Technology, Poland

Abstract. Quick and unhindered access to information is a feature of social and economic development, and the functioning of the entire state depends on the efficiency and stability of ICT systems. A breakdown in digital security brings with it the risk of citizens' safety being compromised, the interception of sensitive data, including personal data, invasion of privacy, loss of money and often health. Effective countermeasures require the continuous establishment and development of a cybersecurity system. The purpose of this article is to analyze and assess the scale and type of emerging incidents. It was assumed (research hypothesis) in ICT systems, including those related to the critical infrastructure of the state, there is an increasing number of incidents involving malicious software and events involving illegal collection of information. The study was based on data on incidents coordinated by the GOV CSIRT (Governmental Computer Security Incident Response Team). The information was obtained from the reports of the CSIRT GOV team for the years 2010-2022. The number of reports and actual incidents was analysed on a quarterly and annual basis, as well as their classification in various categories, using primarily the method of scientific observation, document examination, mathematical analysis and inference. Groups of threats were identified that are characterised by a clear increase in the number of incidents in recent years and against which an intensification of preventive measures is required. The results of the study are in line with the trend observed worldwide. The study clearly shows that malware incidents or information-gathering incidents are becoming more frequent in the virtual world.

Keywords: ICT (information and communication technologies) security, risk assessment, incidents, National Cybersecurity System

Abstrakt: Szybki i nieskrępowany dostęp do informacji jest atrybutem rozwoju społecznego i gospodarczego, a od sprawności i stabilności systemów teleinformatycznych zależy funkcjonowanie całego państwa. Zachwianie bezpieczeństwa cyfrowego wiąże się z ryzykiem naruszenia bezpieczeństwa obywateli, przejęciem wrażliwych danych, w tym osobowych, naruszenia prywatności, utraty pieniędzy, a nierzadko też zdrowia. Skuteczne przeciwdziałanie wymaga permanentnej budowy i rozwoju systemu cyberbezpieczeństwa. Celem artykułu jest analiza i ocena skali oraz rodzaju pojawiających się incydentów. Założono, (hipoteza badawcza) że w systemach teleinformatycznych, w tym związanych z infrastrukturą krytyczną państwa, coraz częściej dochodzi do incydentów z udziałem złośliwego oprogramowania oraz zdarzeń polegających na nielegalnym pozyskiwaniu informacji. Podstawą badania były dane dotyczące incydentów koordynowanych przez zespół CSIRT GOV (Governmental Computer Security Incident Response Team). Informacje zostały pozyskane z raportów zespołu CSIRT GOV z lat 2010-2022. Analizowano liczbę zgłoszeń i faktycznych incydentów w ujęciu kwartalnym i rocznym oraz ich klasyfikację w różnych kategoriach, wykorzystując przede wszystkim metodę obserwacji naukowej, badania dokumentów, analizy matematycznej oraz wnioskowania. Zidentyfikowano grupy zagrożeń, które cechuje wyraźny wzrost liczby incydentów w ostatnich latach i wobec których wymagana jest intensyfikacja prowadzenia działań zapobiegawczych. Wyniki badania wpisują się w trend obserwowany na całym świecie. Przeprowadzone rozważania wyraźnie pokazują, że w wirtualnym świecie coraz częściej pojawiają się incydenty z grupy złośliwego oprogramowania czy zdarzenia związane z gromadzeniem informacji.

Słowa kluczowe: Bezpieczeństwo teleinformatyczne, ocena ryzyka, incydenty, Krajowy System Cyberbezpieczeństwa

Introduction

Technological development has irrevocably changed the way information is disseminated, allowing access to many data resources via the Internet. Information – from the point of view of cybersecurity - is called a strategic resource, necessary to ensure national security (Milkovski, Bogdanoski, 2015). Therefore, there are resources to which access is strictly limited. Cybersecurity is the subject of many publications. J. Jang-Jaccard and S. Nepal in their article "A survey of emerging threats in cybersecurity" presented various types of cyber-attacks. Therein, the authors describe malware as a tool used in the attack, discuss the exploitation of system vulnerabilities and draw attention to the area where new threats are developing (Jang-Jaccard, Surya, 2014, pp. 973-993). The publication highlights the multidisciplinary nature of cybersecurity. In his article, "The Need for a Paradigm Shift Toward Cybersecurity in Journalism", R. Taylor focuses on the importance of the security of the data that is collected by journalists. He indicates that a higher level of security is also to be ensured by learning correct deletion and overwriting of data (Taylor, 2015, pp. 45-47). The topic of cybersecurity in another sector, medical, is discussed by S. Murphy. In "Is Cybersecurity Possible in Healthcare?", the author points out that patient data is often stolen. He also stresses that virtual data security must take place as soon as possible, due to the continuous development of technologies and tools that can be used in cyberspace. A similar problem was discussed by A. J. Conrado and T. L. Wong, who, in the publication "Healthcare Cybersecurity Risk Management: Keys To an Effective Plan", bring to light the system of cyberthreat management regarding medical data, in which risk assessments are divided into three categories (confidentiality, integrity and availability), and individual categories are combined and standardized according to the level of risk (Coronado, Timothy, 2014, pp. 26-30, You et.al. 2025). These publications are just a few examples.

The background to the considerations contained in this article is Poland, representing the countries of Central and Eastern Europe - a similar indicator of exposure to cybersecurity is characterized by, among others, Lithuania, Hungary and the Czech Republic (Sanetra-Półgrabis, Sapiński, 2020). Resources that must be particularly secured in Poland are ICT resources that are used by units of the public finance sector, units subordinate to the Prime Minister, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, and owners of facilities, installations or critical infrastructure devices. The security of information collected by these entities is supervised by the CSIRT GOV (Governmental Computer Security Incident Response Team). It is one of the three Computer Security Incident Response Teams, together with CSIRT NASK (NASK - Scientific and Academic Computer Network) and CSIRT MON (MON - Ministry of Defence). Pursuant to the Act of 15 July 2018 on the national cybersecurity system, CSIRT GOV operates at the national level and is run by the Head of the Internal Security Agency. Two of the most important tasks of the team are monitoring cybersecurity threats along with ICT incidents, and responding to reported incidents (Journal Laws of 2018, item 1560). Incidents handled by the Security Incident Response Teams cause damage to security and public order, economic or international interests, public institutions, personal rights and civil liberties. They also pose a threat to the life or health of citizens (Journal Laws of 2018, item 1560).

The purpose of this article is to analyze and assess the scale and type of emerging incidents. It was assumed (research hypothesis) that in the virtual world incidents from the group of malicious software or events related to unlawful collection of information are taking place more and more often. This article uses data on incidents coordinated by the CSIRT GOV team. The data was collected on the number of reports and actual incidents on a quarterly and annual basis, as well as their quantitative distribution in individual categories. The information was obtained from the CSIRT GOV team reports from 2010-2020 (https://www.csirt.gov.pl/cer.). On this basis, a method of analysis and assessment of incidents in the area of security and the impact of selected factors on their variability was proposed. The analysis was presented on the basis of Polish reports, however, the observed relationships may indicate global trends.

The concept of cyberspace and ICT incidents

Increasing the level of resistance to cyber threats takes place in parallel with enhancing the level of resistance of information systems that are used in the public, private, civil and military spheres (Zhang, Wang 2025). Capabilities should also be developed in areas such as research, testing and evaluation of cybersecurity solutions. It is advisable to strengthen the defensive potential of the state by ensuring continuous development of the national cybersecurity system and acquiring the ability to conduct a full spectrum of military activities in the cyberspace (National Security Strategy of the Republic of Poland 2020). [36]

There are many definitions of cyberspace. This term means, for example, "space for the processing and exchange of information created by ICT systems (Journal of Laws 2002, No. 117, item 985)," where the ICT system is "a set of cooperating IT devices and software, ensuring the processing, storage, as well as sending and receiving data by telecommunications networks using a specific type of telecommunications terminal device [...]" (Journal of Laws of 2005, No. 64, item 565). Digital space can also be treated as the territory of a given country (Cyberspace and cybersecurity): "cyberspace within the territory of the Polish state and outside its territory, in places where representatives of the Republic of Poland operate" (Buggy, 2022, pp. 198-217). The European Commission defines cyberspace as "a virtual space in which electronic data circulates, processed by PCs from all over the world" (Chałubińska, 2022; Góral, Pawłowski, Nowacki, Wróbel, 2023).

The concept of cybersecurity is directly related to cyberspace. The Cybersecurity Strategy of the European Union: An Open, Secure and Protected Cyberspace of February 3, 2013 describes that cybersecurity is related to security and activities that can be used to protect the cybersecurity domain (both civil and military) against threats that affect its interdependent networks and IT infrastructure and those that can damage networks and infrastructure (Joint communication to the

European Parliament, the Council, the European economic and social committee and the committee of the regions Cybersecurity Strategy for the European Union: An Open, Safe and Secure Cyberspace).

Cybersecurity is based on activities that aim to maintain the availability and integrity of networks and infrastructure, as well as the confidentiality of the information contained therein (Fuster et. al., 2020, pp. 97-115). "Cybersecurity is the result of a targeted activity or process, or a state in which information or communication systems and the information contained therein are protected against damage, unauthorized use, modification or use (Cavelty, Wenger, 2019, pp. 5-32)." Characteristic of each type of security is that its stability is threatened by many factors, the so-called "incidents". An incident is defined as an event that has or may have an adverse impact on cybersecurity. The following types of incidents are distinguished (Journal of Laws of 2018, item 1560):

- critical incident – an incident that results in significant harm to public security or order, international interests, economic interests, public institutions, civil rights and freedoms or human life and health […];
- serious incident – an incident that causes or may cause a serious deterioration in the quality or discontinuity of the provision of a key service;
- significant incident – an incident having a significant impact on the provision of a digital service within the meaning of art. 4 of Commission Implementing Regulation (EU) 2018/151 of January 30, 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council with regard to further specifying the elements to be taken into account by digital service providers for the management of existing risks to the security of network and information systems and the parameters for determining whether an incident has a significant impact;
- an incident in a public entity – an incident that causes or may cause a decrease in the quality or interruption of the performance of a public task carried out by a public entity.

The European Union's cybersecurity strategy stipulates that Member States should stop acting entirely individually on cyber defence. Instead, community members should accelerate the process of creating legal regulations regarding the cybersecurity of the entire European Union. In the case of cyber defence, the European Union relies mainly on cooperation with NATO (Bendiek et. al., 2017, pp. 7).

In Poland, in order to meet increasingly demanding security standards, a national cybersecurity system was established (Journal of Laws Dz.U. of 2018, item 1560). The aim of this entity is to ensure cybersecurity at the national level, including the uninterrupted provision of key and digital services, by achieving an appropriate level of security of the information systems with which the services are provided. A digital service is "a service provided by electronic means…" and a key service is one which "is essential for the maintenance of critical social or economic activities[…]" (Wade, 2020, pp. 9-27, Krupnik, Stryjewski, 2023).

The most important entities responsible for coordinating the process of responding to computer incidents are the CSIRTs (Computer Security Incident Response Team), dealing, among others, with handling reported incidents. Information regarding these incidents, as well as reports on the activities carried out by this CSIRT, is not widely available due to their confidential nature, so this article uses the data made available in the CSIRT GOV Annual Activity Reports. Its activities are closely related to the security of state organizations, hence the member of the „GOV" (from the word government). The basic tasks of this team include, among others, identification, prevention and detection of threats that may bring negative effects on the security or continuity of the functioning of ICT systems of public administration bodies (Karpiuk, 2021, pp. 609-620).

CSIRT GOV handles applications coming from public finance sector entities, entities subordinate to the Prime Minister or supervised by him. The area of activity of the team also includes ICT network systems covered by a single list of facilities, installations, devices and services that are part of the critical infrastructure, as well as ICT systems of owners and holders of facilities, installations or devices of critical infrastructure (Journal of Laws of 2018, item 1560). Incidents are reported to the Computer Security Incident Response Team and may adversely affect activities that violate the integrity, confidentiality, availability or authenticity of data or related services.

ICT incidents coordinated by the CSIRT GOV team over the years 2010-2020

The ICT incidents occurring in the security status reports concern different types of cyber threats, classified according to the following categories:

- offensive incidents;
- malware;
- gathering information;
- burglary attempts;
- burglary;
- availability of resources;
- information security;
- computer fraud;
- other.

Incidents deemed "abusive" include incidents such as spam, discredit and insult, child pornography and violence. Spam is undesirable information that has been sent via email (Ferrara, 2019, pp. 82-91). Discredit or insult is an incident that undermines trust, destroys a person's good name, or diminishes an individual's authority. Offences related to child pornography are defined as offences based on the nature of the information contained. Any pornographic material that is considered as child pornography is defined in Art. 9 point 2 of the Council of Europe Convention on Cybercrime (Council of Europe Convention on Cybercrime drawn up in Budapest on 23 November 2001).

Malware is understood as viruses, network worms, Trojan horses and spyware. By accepting programs as sequences of symbols, and computer systems as environments, viruses can be defined as programs that can attach to other programs and turn them into subsequent viruses (Özdemir et. al., 2020, pp. 239-247). A similar threat are network worms, which can also be defined as self-replicating computer programs. A Trojan horse is a destructive program that does not replicate its own code, works in the system without the user's consent and knowledge, and may contain a malware load. To install a Trojan, an external initiation is required, such as the operation of a network worm (Chumachenko et. al., 2019). Spyware is different in its operation from viruses or network worms. The main purpose of spyware is to monitor user behavior and to steal private information. The spy software tracks how the keys are pressed or how the browser is used (Pierazzi et. al., 2020, pp. 1-38).

Information gathering means scanning, wiretapping and social engineering. Scanning is the detection of systems that operate and are accessible over the Internet and the identification of the services they offer (Pawlisiak, Maslii, 2024). This is done using techniques such as port scanning, ping sweeps and identification of operating systems (Messier, 2021, pp. 155-220). Programs operating in this way are divided into system scanners that examine the local station for system vulnerabilities resulting, for example, from omissions, and network scanners that test the local station through network links in terms of port and service availability, looking for potential vulnerabilities to carry out an attack. Wiretapping involves taking over data without the knowledge and consent of the parties involved in its transmission. In the case of social engineering, incidents are more complex. They concern situations in which data is obtained in an unauthorized manner by means other than by a determined, defined attack. So-called "social engineering in cyberspace" consists in the use of various means and methods of manipulation, which are to result in obtaining protected data (Lehmann et. al., 2020).

Hacking attempts are exploiting known system vulnerabilities, exploiting unknown system vulnerabilities, attempts at unauthorized login. In turn, hacking into a privileged account and ordinary hacking into applications and bots are classified as burglaries. Bots are applications or scripts that were created for the purpose of automating certain activities. However, they can be mis-used in order to take control of the attacked devices.

The availability of resources relates to a blocking attack (DoS), a distributed service blocking attack (DDoS), and a service outage. A blocking attack is easy to execute and has quite severe effects. If such an attack is carried out from several sources, it is called a "DDoS attack. Interruptions in the operation of services are all kinds of failures and blockages that occur for various reasons result in the unavailability of a given node.

An information security group is formed by incidents such as unauthorized access to information and unauthorized modification of information. Both relate to any situation in which information has been made available to users for which it was not intended.

Computer fraud is the unauthorized use of resources, copyright infringement, identity theft, impersonation and phishing. Pursuant to the Act of February 4, 1994 on copyright and related rights, the subject of copyright is any manifestation of creative activity of an individual nature, established in any form, regardless of the value, purpose and manner of expression (Journal of Laws 1994 No. 24 item 83). All forms of violation of this right have been classified as fraud, as have identity theft and impersonation. Phishing, in turn, is the fact that the attacker is fraudulently trying to obtain confidential information from the victim by impersonating a reliable entity (Jagatic et. al., 2007, pp. 94-100).

The "other" group consists mainly of botnets and other types of incidents, not listed in other groups. Botnets can be defined as a large network of personal computers that have been attacked by malware. This creates a network of hundreds of thousands or even millions of machines (Sommer, Brown, 2011).

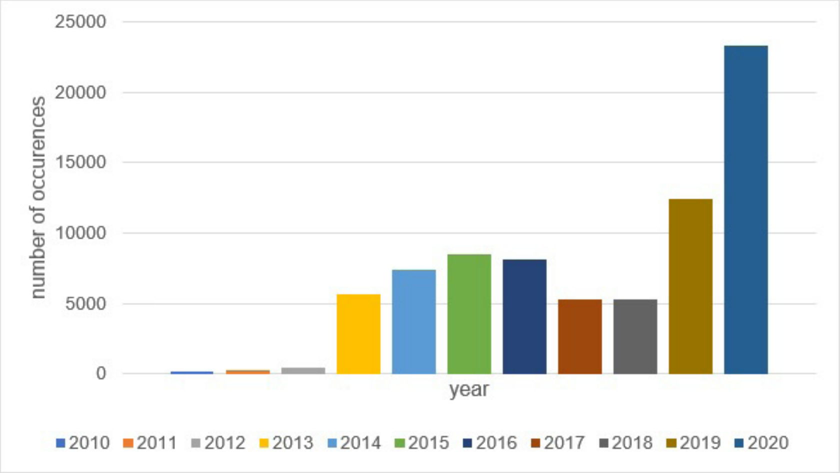

Fig. 1. Change in the number of events over the period 2010-2020

Source: Own study based on the data contained in the Reports on the State of Cyberspace of the Republic of Poland (2010-2020) CSIRT GOV

The analyzed reports on the state of cybersecurity contain information on the type of incidents and their number. In the chart below (Figure 1), the change in the number of ICT incidents over the period 2010-2020 is presented.

The number of ICT incidents in the years 2010-2015 has steadily increased. In 2016, there was a decline, which may result from the development of systems that support the work of analysts. These systems analyze the flows in the network and contribute to determining the actual threats. They are becoming more and more precise, which translates into an increase in the quality of analysis of each of the reported cases and their better verification. Between 2019 and 2020, however, the number of ICT incidents increased sharply.

Incidents from the insulting group occurred initially in a limited number in Polish cyberspace. In 2010, only 10 incidents of this nature were identified. A significant increase was recorded in 2013, when 51 such incidents were recognized. This number decreased to 17 incidents the following year. In 2016, 137 incidents of insulting nature were reported, down to 119 in 2017. The 2020 report contains information on 377 cases, which is the highest result over the years described.

The number of incidents that can be described as malware use is increasing every year. In the 2010 report, 25 such events were recorded, while in 2014, there were already 55. A sharp increase in their number first occurred in 2016, when 540 such cases were reported. This represented an increase of 456 incidents compared to the previous year. The years 2017, 2018 and 2019 can be described analogously. The number of incidents during this period increased from 1868, through 2448, to 7,219 incidents. The year 2020 is characterized by the highest number of malware incidents.

Data on incidents related to the collection of information are included in each 2010-2020 report. Between 2010 and 2016, the number of cases increased from 30 to 382. The 2016 Cybersecurity State of Cyberspace report states that this increase may be due to the nature of the phishing campaigns that fall into this group. Campaigns can be the initiating phase for a broader attack and can be the starting phase for an APT (Advanced Persistent Threat) attack. In 2017, there was a decrease, and 254 such events were recorded. It is worth noting that the 2017 report did not present 551 incidents, as a result of which their type is unknown. In 2018, 636 cases of information collection were reported, and this number increased to 2604 in 2020. This is the highest number of such events during the period under review.

Attempts of hacking are one of the least numerous groups of ICT incidents. In 2010, only two reports related to this type of threat. In the years 2011-2014, their number ranged from 6 to 11. In 2015, the highest number of such incidents was recorded - 72 reports concerned attempts of hacking. In the following years, there was no information about the occurrence of incidents that can be assigned to the described category.

A related group of incidents are hackings. This category is also characterized by a small share in the number of all events. Between 2010 and 2012, the number increased from 8 to 26. In 2013, there was a decrease and there were 5 cases of such situations. The 2014 report included information on 12 such events. In the years 2015-2018, there was no information about the occurrence of events that can be defined as hacking. In 2019, tens of threats of this nature were re-identified - 44 such attacks. In 2020, there were only 8 such incidents.

Incidents from the resource availability group only occurred twice in 2010. This number increased to 31 in 2012, which was significantly influenced by the so-called "ACTA protests". Accordingly, 23 of the 31 incidents that occurred this year were DDoS attacks. A year later, there were only 10 incidents. A sharp increase in their number took place in 2015. At the time, 219 cases were recorded, which was 199 more than in the previous year. Between 2016 and 2018, the number of incidents increased from 76 to 275. In 2020, All told, 350 incidents of this nature were identified, which is the highest value in the period under review.

Information security incidents did not occur in large numbers in Polish cyberspace. In 2010, there were 15 such events, and over the years, this number increased to 143 in 2013, which is the highest result in the period under review. In 2014, 44 information security incidents were recorded, and in 2015 - 74. Reports from 2016-2018 did not include information on this group of incidents. In 2019, 22 incidents threatening information security were identified. In 2020, there were only 13 such incidents.

The frequency of computer fraud has changed over the period described. In the years 2010-2014, their number ranged from 6 to 15 events. Reports from 2015-2017, due to the manner in which the data contained in them were presented, do not contain information on the number of ICT incidents assigned to this group. In 2018, a clear increase in the number of computer frauds compared to previous years was identified. There were 276 of these, and in the following year their number amounted to 1,178 events. The largest number of such incidents occurred in 2020 - there were 1,468 listed cases.

In the category that gathers the remaining incidents, botnets are the most numerous. In 2010, there were 52 events assigned to this group, and the use of the botnet occurred only 2 times. Although the botnet incident only occurred once in 2011, special attention was paid to it. This case referred to a detected client of the "Coreflood" botnet. It was determined that this was a typical botnet used to intercept bank login details. The report draws attention to the fact that such methods can also be used in a wider range, e.g. to obtain passwords for internal systems in institutions (Coronado, Timothy, 2014, pp. 26-30). In 2012, there was an increase and 29 cases of botnet use were identified. In 2013, the number of botnets also increased and 4270 such events were recorded. The software worked on workstations connected to the ICT network of public administration units. A similar trend occurred in 2014.

In 2015, there was a decrease in the category of incidents related to the use of the botnet. The report describes this situation as the result of actions directed against systems that target groups of infected devices that occurred on a global scale. In the years 2016-2019, the number of incidents related to the botnet was constantly decreasing. In 2019, only 37 such events were recorded.

The second largest subgroup in the "other" category is the incorrect configuration of the device. In 2010, such incidents, like the botnet, occurred only twice. In 2013, that number was 36. The biggest increase occurred in 2014, when there were 2,213 incidents related to incorrect configuration of the device. The highest score was achieved in 2016, when 4,158 such events were identified. A significant decrease occurred in 2017, when such incidents occurred 1,847 times. The downward trend also took place in 2018 and 2019, such situations occurred 1138 and 119 times, respectively.

In the further stage of the study, the impact of selected factors on the variability of data contained in the reports was analyzed. It was checked whether their number varies depending on the impact of the year and quarter variable. First, the number of events was analyzed in relation to the year in which they occurred. In Figure 2, a frame graph of the number of events in the studied years is presented.

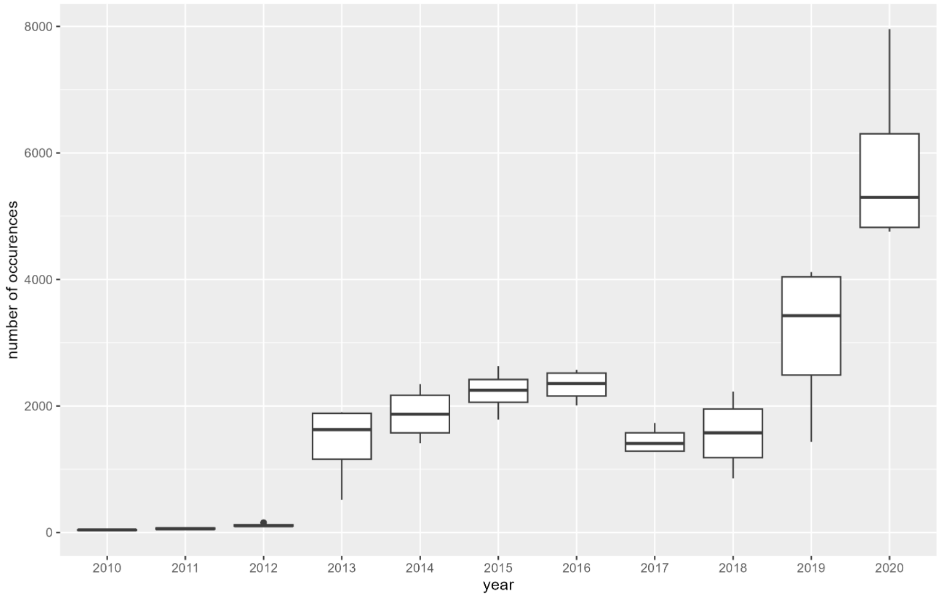

Fig. 2. Frame graph for the number of events in the years 2010-2020

Source: Own study

The number of events in each year varies. Before determining whether these differences are statistically significant, the normality of distributions in individual groups and the heteroscedasticity of variance were assessed (Grzelak et al., 2019). In doing so, the Shapiro-Wilk test was applied to test the normality of the distributions, due to the small sample size (Świderski et al., 2018). The results in individual groups (test statistic value and p-value) are presented in Table 1.

Table 1. Shapiro-Wilk test for groups resulting from the year of the incident

Year	Value of test statistics t	*p*-value
2010	W = 0.90218	0.442
2011	W = 0.9719	0.8532
2012	W = 0.88978	0.3821
2013	W = 0.85128	0.2303
2014	W = 0.94477	0.6836
2015	W = 0.99547	0.9835
2016	W = 0.91859	0.5291
2017	W = 0.88423	0.357
2018	W = 0.97555	0.8755
2019	W = 0.88227	0.3484
2020	W = 0.82935	0.1661

Source: Own study

All distributions were found to be consistent with the normal distribution. The heteroscedasticity of the variance was then assessed by utilizing Bartlett's test. The test statistic of K-squared = 70.597, and p-value =3.4*10^(-11) means that the assumption of heteroskedasticity of variance was not met (Jaroń et al., 2022). However, due to some resistance, ANOVA variance analysis was performed in parallel with the non-parametric Kruskal-Wallis test (Borucka, Grzelak, 2019) . The results of the ANOVA analysis are presented in Table 2.

Table 2. Results of ANOVA variance analysis

	number of degrees of freedom,	F-Statistics	p-value
Year	10	24.33	1.98 10^{-12}

Source: Own study

As the K-W test statistic result is chisquared = 37.355 and p-value = 4.912 10-5, all results confirm that there are at least two distributions that differ significantly from each other. To further investigate the differences between all groups, a Tukey test was then performed. This allows finding groups that differ significantly. The results are shown in Table 3.

Table 3. Tukey test results

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
2010	1	1	0.169	0.019	0.003	0.001	0.145	0.091	0.000	0.000
2011		1	0.186	0.021	0.003	0.002	0.160	0.102	0.000	0.000
2012			0.229	0.028	0.004	0.002	0.198	0.128	0.000	0.000
2013				0.996	0.825	0.715	1.000	1.000	0.041	0.000
2014					1.000	0.997	0.998	1.000	0.302	0.000
2015						1.000	0.861	939	0.754	0.000
2016							0.761	0.871	0.856	0.000
2017								1.000	0.050	0.000
2018									0.082	0.000
2019										0.000

Source: Own study

Here, values p that are below 0.05 indicate significant differences in the averages in the studied groups. They apply to pairs marked with color (Table 4). This confirms that in the analysis carried out above, the number of incidents for most couples varies significantly. A similar study was carried out for the quarter variable. Figure 3 presents a frame chart of the number of events in individual quarters.

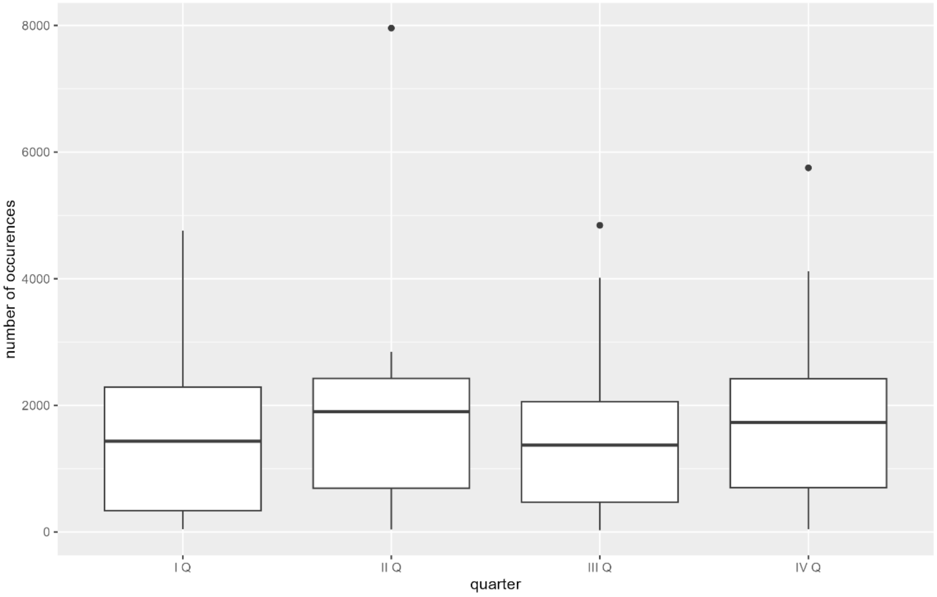

Fig. 3. Frame-graph for the number of events in each quarter
Source: Own study

Again, before checking whether the differences between the number of events in individual quarters are statistically significant, the normality of distributions (Shapiro-Wilk test) in individual groups (Tab. 4) and the heteroskedasticity of variance (Bartlett's test) (Table 5) were assessed.

Table 4. Shapiro-Wilk test for groups resulting from the quarter in which the incident occurred

quarter	Value of test statistics	p-value
I Q	W = 0.89219	0.1481
II Q	W = 0.76413	0.00318
III Q	W = 0.88538	0.1217
IV Q	W = 0.89635	0.1668

Source: Own study

Almost all of the distributions turned out to be in line with the normal distribution, with the exception of the second quarter. In the Bartlett test, the test statistic K-squared = 2.1299, p-value = 0.5459 implies that the assumption about the heteroskedasticity of variance was met, which authorizes the use of ANOVA analysis. The results are presented in Table 5.

Table 5. Results of ANOVA variance analysis

	umber of degrees of freedom,	F-Statistics	p-value
quarter	3	0.222	0.881

Source: Own study

The results show that all the studied groups do not differ significantly from each other, so the quarter has no impact on the number of recorded incidents. Therefore, there are no periods of the year in which it can be concluded that there is an increase in attacks. Studying the types and frequency of cyber attacks is important because it allows for an understanding of evolving cyber threats. This allows science to provide more precise tools and strategies to defend against these attacks. In addition, analysing these attacks helps to identify vulnerabilities in the digital infrastructure and contributes to improving security standards. As a result, this research is essential for the continuous improvement of the field of cyber security and data protection in an increasingly computerised world.

Conclusions

As the conducted analyses indicate, we are dealing with an increasing number of detected incidents over time. Many factors influence this state of affairs. It should be mentioned, among others, that potential attackers have a growing interest in the government networks of Poland. Another important issue is the continuous development of the systems used by the CERT GOV Team, which, due to the work carried out, are becoming more and more precise in monitoring the network and in determining the actual threats to Poland's computer systems and networks. This state of affairs significantly increases the quality of analysis of each registered case.

The results of this study are in line with the trend observed throughout the world. The conducted considerations clearly show that in the virtual world, incidents from the group of malware or events related to the collection of information occur more and more often. These groups are marked by a marked increase in the number of incidents in recent years. A worrying trend is sure to affect preventive action. Extremely dangerous consequences are brought about by events that concern actions aimed at obtaining sensitive information.

BIBLIOGRAPHY

[1] 52013JC0001, Joint communication to the European Parliament, the Council, the European economic and social committee and the committee of the regions Cybersecurity Strategy for the European Union: An Open, Safe and Secure Cyberspace /* JOIN/2013/01 final */

[2] Act of 15 July 2018 on the national cybersecurity system (Journal Laws of 2018, item 1560).

[3] Act of 17 February 2005 on the computerisation of the activities of entities performing public tasks (Journal of Laws of 2005, No. 64, item 565, as amended).

[4] Act of 21 June 2002 on the state of emergency (Journal of Laws 2002, No. 117, item 985, with later as amended).

[5] Act of February 4, 1994 on copyright and related rights (Journal of Laws 1994 No. 24 item 83).

[6] Annegret, B., Bossong, R. and Schulze, M., 2017. The EU's revised cybersecurity strategy: half--hearted progress on far-reaching challenges., 7.

[7] Borucka, A. 2018. Risk analysis of accidents in Poland based on ARIMA model. Transport Means.

[8] Borucka, A. and Grzelak, M., 2019. Application of Logistic Regression for Production Machinery Efficiency Evaluation. Applied Sciences 9, 22, 4770.

[9] Buggy, S., 2022. Cybersecurity of countries in the 21st century on the example of the Republic of Poland. Homeland Security Review 14.27.

[10] Cavelty, M. D. and Wenger, A., 2019. Cyber security meets security policy: Complex technology, fragmented policy, and networked science. Contemporary Security Policy 41.1.

[11] Chałubińska-Jentkiewicz, K., 2022. Cyberspace as an Area of Legal Regulation. Cybersecurity in Poland, 23.

[12] Chumachenko, D., Chumachenko, K. and Yakovlev, S., 2019. Intelligent simulation of network worm propagation using the code red as an example. Telecommunications and Radio Engineering 78.5.

[13] Coronado, A. J. and Timothy, L. W., 2014. Healthcare cybersecurity risk management: keys to an effective plan. Biomedical instrumentation & technology 48.s1.

[14] Council of Europe Convention on Cybercrime drawn up in Budapest on 23 November 2001 (item 728)

[15] CSIRT GOV, [online], Available at: https://www.csirt.gov.pl/cer [Accessed: 6 February 2023].

[16] Ferrara, E., 2019. The history of digital spam. Communications of the ACM 62.8, 82-91.

[17] Fuster, F., González, G. and Jasmontaite, L., 2020. Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights. The ethics of cybersecurity, 97-115.

[18] Góral, P., Pawłowski, P., Nowacki, W., Wróbel, J., 2023. Electronic anti-theft protection for vehicles of people with special needs. Military Logistics Systems, 59(2). https://doi.org/10.37055/slw/186380

[19] Grzelak, M., Borucka, A., and Buczyński, Z. 2019. Forecasting the demand for transport services on the example of a selected logistic operator. Archives of Transport, 52.

[20] Jagatic, T. N., Johnson, N.A., Jakobson, M. and Menczer F., 2007. 'Social phishing.' Communications of the ACM 50.10, 94-100.

[21] Jang-Jaccard, J. and Surya, N., 2014. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences 80.5, 973-993.

[22] Jaroń, A., Borucka, A. and Parczewski, R., 2022. Analysis of the Impact of the COVID-19 Pandemic on the Value of CO2 Emissions from Electricity Generation. Energies, 15(13):4514.

[23] Karpiuk, M., 2021. The Local Government's Position in the Polish Cybersecurity System. Lex Localis 19.3, 609-620.

[24] Krupnik, D., Stryjewski, T., 2023. Security of the development of the construction industry in conditions of macroeconomic market uncertainty. Military Logistics Systems, 59(2), 189-208. https://doi.org/10.37055/slw/186383

[25] Lehmann, D., Johannes K. and Pradel M., 2020. Everything old is new again: Binary security of webassembly. Prokedings of the 29th USENIX Conference on Security Symposium.

[26] Messier, R., 2021. Scanning Networks.

[27] Milkovski, N. and Bogdanoski, M., 2015. Information as a strategic resource critical to military operations and defense of the nation, Contemporary Macedonian 28 XV.

[28] National Security Strategy of the Republic of Poland 2020, Warsaw, Poland.

[29] Özdemir, N., Sümeyra, U., Beyza, B. and İskender, E., 2020. Dynamical analysis of fractional order model for computer virus propagation with kill signals. International Journal of Nonlinear Sciences and Numerical Simulation 21.3-4.

[30] Pawlisiak, M., Maslii, O., 2024. Internet of things as a tool for ensuring material security of Military Units and Institutions. Military Logistics Systems, 60(1), https://doi.org/10.37055/slw/193856

[31] Pierazzi, F. and et al., 2020. A data-driven characterization of modern Android spyware. ACM Transactions on Management Information Systems (TMIS) 11.1.

[32] Sanetra-Półgrabis, S. and Sapiński A., 2020. The issue of social security within the functioning of Euroregions.

[33] Sommer, P. and Brown, I., 2011. Reducing systemic cybersecurity risk. Organisation for Economic Cooperation and Development. Working Paper No. IFP/WKP/FGS, 3.

[34] Świderski, A., Borucka, A., and Skoczyński, P. 2018. Characteristics and assessment of the road safety level in Poland with multiple regression model. In Transport Means-Proceedings of the International Conference.

[35] Taylor, R., 2015. The need for a paradigm shift towards cybersecurity in journalism. National Cybersecurity Institute Journal 1.3.

[36] The Act of 15 July 2018 on the national cybersecurity system (Journal of Laws Dz.U. of 2018, item 1560).

[37] Wade, P., 2020. Cybersecurity - sectoral regulatory aspects. Antitrust and Regulatory Quarterly (iKAR) 9.2.

[38] You, D., Liu, S., Li, F., Liu, H., Zhang, Y., 2025. Reliability Assessment Method Based on Small Sample Accelerated Life Test Data. Eksploatacja i Niezawodność – Maintenance and Reliability, 27(1). https://doi.org/10.17531/ein/19217.

[39] Zdzikot, T., 2022. Cyberspace and cybersecurity. Cybersecurity in Poland: Legal Aspects, 9-21.

[40] Zhang, H., Wang, Q. (2025). Risk identification model of aviation system based on text mining and risk propagation. Eksploatacja i Niezawodność – Maintenance and Reliability, 27(1). https://doi.org/10.17531/ein/192767