Tomasz MULIŃSKI[1]
ORCID: 0000-0002-6305-700X

[1] Chamber of Tax Administration in Lublin
ul. Tadeusza Szeligowskiego 24,
20-883, Lublin, Poland

ICT security in revenue administration - incidents, security incidents - detection, response, resolve

DOI: 10.34739/si.2022.27.04

Abstract. The article shows the author's approach to the methods of acquiring and analyzing reports and security incidents, categorizing their sources in relation to the literature describing ICT security threats, taking into account the legal regulations in force in the Polish public administration. Methods of verification and analysis of detected threats, methods of threat resolution were presented. Tools and procedures used to evaluate reported incidents and assess the threat level of reported incidents were discussed. The incidents and events identified in the period April 2018 - February 2022 were analyzed. Due to the implementation of remote work, there were challenges related to the need to ensure secure remote access to ICT systems of the tax administration. This entailed the need to develop other methods of analysis, response and development of procedures for safe use of workstations by employees providing remote work. The article shows a wide variety of events that members of the security incident response team had to deal with. The obtained results will also be compared with the conducted scientific research on the perception of security threats in public administration and how changes in IT service in the studied organization influenced security management and affect the developed model of combating intentional security threats to information systems.

Keywords. ICT security, security incidents, tax administration Computer Security Incident Response Team

1. Security Incident Response Team

The Cyberspace Protection System of the Republic of Poland (CRP) is a key element ensuring the proper functioning of public services in Poland. In 2017, the Prime Minister introduced by a regulation [14] alert levels for CRP, specifying what tasks are to be performed during their duration by teams of specialists responsible for their implementation. Based on the Regulation, the Minister of Development and Finance defined the tasks of the Security Incident Response Teams (SIRT) implemented during states of emergency [7]. In order to ensure proper operation of the teams, they were established in particular units not only to carry out tasks in case of a state of emergency but also to conduct ongoing monitoring of the information and communication system security status. The scope of tasks is defined in the Standard for ICT Security Incident Management in the Ministry of Finance and in the organizational units of the Ministry of Finance [3]. The tasks of the team include:

- receiving reports and recording, categorizing and prioritizing security incidents, events and requests,
- diagnosing and resolving incidents, events, and requests resulting from SIRT tasks,
- closing of security events and incidents,
- reporting and control of handling security events, incidents and requests.

The SIRT incident management model proposed in the appendix to the regulation focuses only on incident handling and response. The creators also underestimated the importance of non-risk notifications by only covering them in the reduction process, leaving out the aspects of social engineering whose use can be crucial in breaking through security [4]. Due to the fact that in 2017 there was a merger of two separate structures of the tax administration and customs service creating one organization, new challenges arose regarding the need to develop rules, security procedures, unify the management of ICT systems.

The task of building a team and creating an original information security management model with elements using guidelines, standards and knowledge about the impact of social engineering on ICT security, which was a big challenge. In building the SIRT team operating model shown in Figure 1, consideration was given to:

- the need to provide feedback to incident reporters,
- Building a knowledge base, which is the basis for developing tools to improve IT security in an organization,
- raising user awareness
- the need to inform SIRT about irregularities and threats to IT system operation.

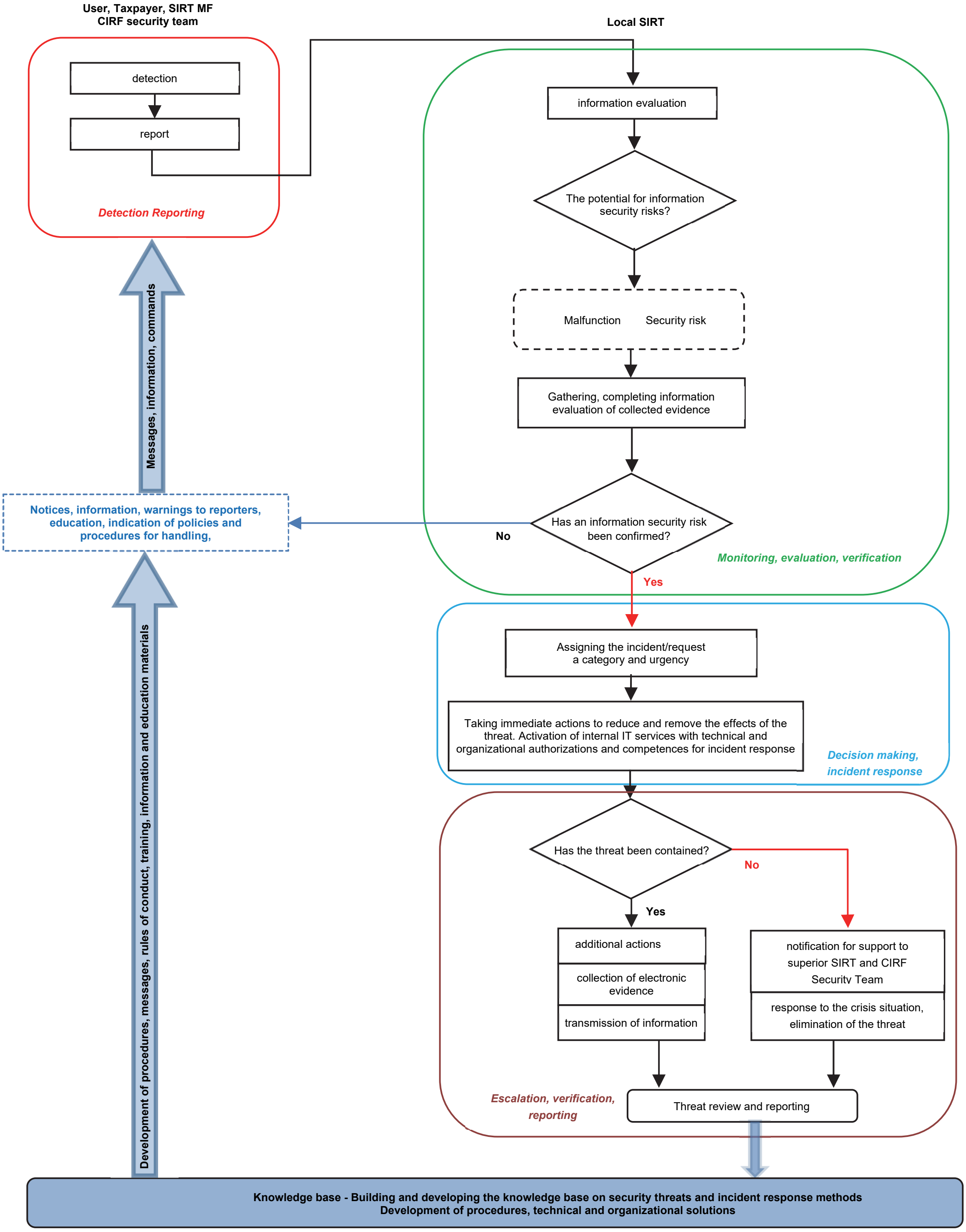
User, Taxpayer, SIRT MF
CIRF security team
detection
report
Detection Reporting
Local SIRT
information evaluation
The potential for information security risks?
Malfunction
Security risk
Gathering, completing information evaluation of collected evidence
Has an information security risk been confirmed?
No
Yes
Monitoring, evaluation, verification
Messages, information, commands
Notices, information, warnings to reporters, education, indication of policies and procedures for handling,
Assigning the incident/request a category and urgency
Taking immediate actions to reduce and remove the effects of the threat. Activation of internal IT services with technical and organizational authorizations and competences for incident response
Decision making, incident response
Has the threat been contained?
No
Yes
additional actions
collection of electronic evidence
transmission of information
notification for support to superior SIRT and CIRF Security Team
response to the crisis situation, elimination of the threat
Escalation, verification, reporting
Threat review and reporting
Development of procedures, messages, rules of conduct, training, information and education materials
Knowledge base - Building and developing the knowledge base on security threats and incident response methods
Development of procedures, technical and organizational solutions

Figure 1. Diagram of the SIRT incident handling model in revenue administration. Source: Own study.

The built model has been operating since 2018 in the tax administration and seems to be increasingly contributing to improving user awareness, responding to unusual behavior of systems. As part of the model improvement in the area of communication, the number of messages was also increased, the information security management system was cleaned up. Changes occurring in the 2020 - COVID pandemic, separation of IT services from the organization to Informatics Centre of the Ministry of Finance (CIRF-BT) in 2021 required procedural and organizational changes, but the model itself until the moment of writing the article fulfills its role and it seems that thanks to it the probability of incidents in the ICT infrastructure that could lead to serious consequences for the organization has been reduced.

This article is written at a time when Russian aggression in Ukraine is ongoing, the third alert level for the Republic of Poland's cyberspace CHARLIE-CRP is currently in place [9-13]. The SIRT team is therefore involved not only in monitoring and responding to reported potentially dangerous events in cyberspace, but also proactively informs about the responsibilities of users of ICT systems, provides guidance and guidelines to raise awareness and ensure a sense of security for tax administration employees.

At the current time, false information, exploitation of the dramatic situation in Ukraine to obtain information about the infrastructure through pishing, and attempts to infect ICT systems through crafted emails containing malware or directing to sites where attacks on IT resources are possible are particularly dangerous. The difficulty of spam detection necessitates the use of machine learning for header or content analysis of emails [16] while maintaining the efficiency of such solutions. The number of spam and pushing reports received indicates that security systems are still not always able to correctly identify emails with undesirable content or containing malware attachments.

- Internal - information received from departmental security teams and employees of the Ministry of Finance, including a few notifications received through departmental security teams from external entities, such as the Internal Security Agency, information from hardware and software manufacturers, which were supplemented with guidelines or instructions for local SIRT,
- External - information obtained from: publicly available government and non-government sources, ICT security organizations, software and hardware manufacturers.

Bearing in mind the above general division of information sources, a detailed analysis of the received reports on potential incidents was made, assigning them to four sources:

- CIRF BT - information on potential threats resulting from the analysis of IT security system logs (unwanted network traffic, large number of logins attempts to unknown accounts, detected threats in the local infrastructure, etc.).
- SIRT Local - information obtained based on: owned access to ICT security tools.
- Local reports - information originating from local users of ICT systems.

- External - information obtained from: publicly available government and non-government sources, ICT security organizations, ICT software and hardware manufacturers.

Figure 2 shows the percentage breakdown of the sources of reports of potential incidents during the analysis period. Of the 831 reports, over 60% came from the central departmental security team, reports from local users accounted for over 26% of all reports, detected incidents by the local SIRT team accounted for 11.6% of all reports, external sources accounted for 1.4%.

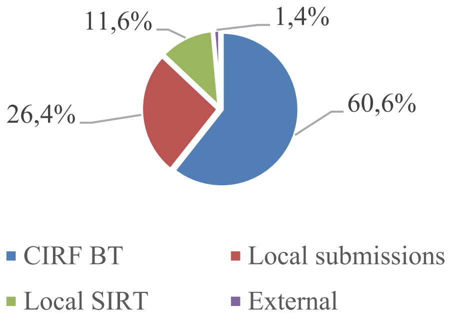

Figure 2. Percentage distribution of sources of potential incident reports to the local SIRT. Source: Own study.

It is reasonable to analyze the distribution over time of the number of reports from each source, in Figure 3 it is apparent that the entry into the COVID-2 pandemic period significantly affected the number of reports reported to SIRT. Already in early 2020, it is apparent that there was a significant increase in the number of reports from CIRF BT, which increased its analysis of log events and began reporting issues largely due to problems with updating passwords in browser-based information systems resulting in a significant increase in the number of reports handled by the SIRT team.

During the period from April to July 2020, the most issues with potential threats were identified and methods were developed to mitigate such incidents, including making changes to domain policies which contributed to a significant decrease in the number of reports from this source. In the final phase of the large influx of reports from the CIRF BT source, the local team took proactive measures to improve the security of local ICT systems. Detected issues in securing workstations, servers resulted in escalation to administrators of noticed vulnerabilities in systems and their elimination contributed to a significant decrease in submissions. It was not until August 2021 that a significant number of threats were identified that affected the level of ICT security of the surveyed organization. Reports from local users show four periods of increased number of detected incidents, which were largely due to receiving emails that were spam, phishing attempts, or contained malware.

Most of the reports did not constitute an information security risk incident, however, there were undesirable events that required taking action to remove and reduce the effects. There were no events that required starting central units or business continuity recovery procedures. There were no significant threats to the security of information processed in ICT systems, single events concerned a small amount of data that did not leak directly from the ICT systems and did not constitute a threat to personal data under the GDPR [8] Act. Due to the need to maintain the security and protection of this information, detailed analysis will not be presented in this article.

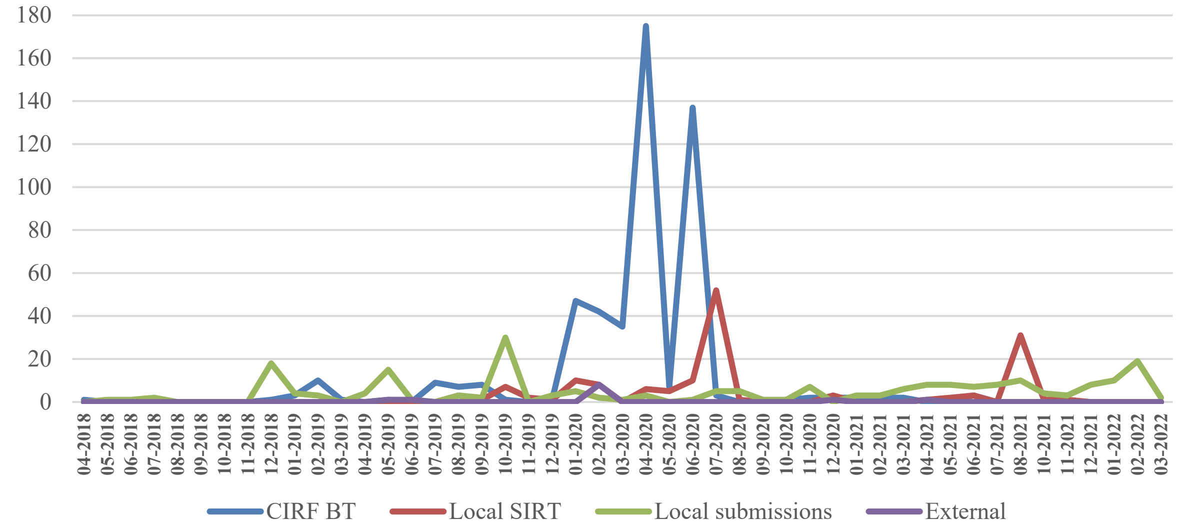

Figure 3. Time distribution of sources of reports to the local SIRT of potential incidents. Source: Own study.

2. Identification and classification of potential threats to the security of ICT systems

In the analyzed period, 831 events were reported to the Security Incident Response Team, which, as part of the handling model, were not only analyzed in terms of incident occurrence and decision-making on how to resolve the report, but also classification of reports was made. This classification allowed for the identification of eleven types to which each of the received notifications could be classified:

- High volume of failed logins - Network traffic detected by network analyzers indicating multiple attempts to use invalid credentials. The cause of the alarms identified by SIRT was the storage of authentication data in web browsers, which after updating the password was not updated by the user for web applications used in the tax administration. Most often, it was the bar with url shortcuts enabling quick access to selected websites that were the source of the alarms, because even when the user did not attempt to log in, according to the analyzes carried out, the browser periodically asked the sites using the old credentials. 439 cases were detected and analyzed, with some workstations generating hundreds or even several thousand alerts during one day.

- Malware - malicious software detected by ICT protection systems, which was located on local disks of workstations, removable media and in e-mail attachments. 108 cases of this type were identified and this is the second largest number of reports handled by the SIRT team.
- Unusual network traffic - network traffic detected by network analyzers, deviating from normal traffic, using unusual ports, sending messages indicating network querying for configuration, or using equipment to watch full HD video transmission, significantly burdening WAN lines.
- Phishing - reports from users who received e-mails with links to confirm the e-mail address, refer to a website with malware, or make contact in order to use social engineering methods that may lead to the disclosure of credentials for ICT systems or phishing financial resources.
- Spam - reports from users who received e-mails with content indicating that it contains advertising, undesirable or irrelevant information for the recipient and is not considered a form of phishing.
- Personal data - reports on errors related to the transfer of data from ICT systems to the wrong recipients. SIRT is obliged to handle such incidents and, in the event of disclosure of data, report such fact to the Office for Personal Data Protection. Sporadic cases were resolved without any serious consequences for individual persons, as incorrect data transmission concerned individual persons, and sometimes there was a loss of paper data due to the fault of the postal operator delivering the parcel. In all other cases, it was possible to lead to a situation in which the wrong recipient of the information returned it to the office or removed it from the ICT system (in the case of information sent electronically).
- Attempted blackmail - one of the less common threats, but classified as a separate category of social engineering attacks. The source of the reports were e-mails in both Polish and English in which the author demanded a fee in bitcoins for non-disclosure of alleged films intended to compromise the recipient of the e-mail.
- User error - events identified by SIRT that resulted from non-compliance with security procedures. Examples were the use of applications not approved for use, errors in device configuration, requesting changes to network policies without consulting the SIRT team.
- Attack on a workstation - cases of scanning mobile stations in order to break authentication security, detected by departmental security systems. Three such

situations occurred in the case of providing remote work and using a private network to establish a secure connection with the infrastructure of the tax administration. The incidents resulted from the fact that the Internet operator or an employee at the place of remote work did not protect the local network against attacks, so that the attacker had access to it and, using the detected vulnerabilities, attempted to break the security of the mobile station. The detection of this fact resulted in an order to immediately disconnect the mobile station from the home Internet, deliver the device to the workplace to verify that there was no security incident. Such an employee was forbidden to work remotely due to insufficient security of the Internet network at the place of remote work, which led to attempts at attacks on the work device.

- Other - a report that could not be classified into any of the other groups, usually these were reports resulting from user caution, incorrect configuration of the device generating network traffic, received regular e-mail, which cannot be classified as spam or phishing.

The threat types listed above are sorted by number of occurrences from highest to lowest. A detailed breakdown of individual threats is presented in Figure 4. Table 1 shows the breakdown of individual sources of threats, discussed in the previous part of the article. It should be noted that the threats detectable by technical security measures (high number of failed logins, unusual network traffic) accounted for the largest number of 520 identified potential security threats. Undoubtedly, having hardware solutions that detect threats and SIEM type analyzers enable the automation of monitoring and taking actions to prevent the escalation of the threat, which also resulted in the fact that such incidents accounted for 62.58% of all reports to the SIRT team.

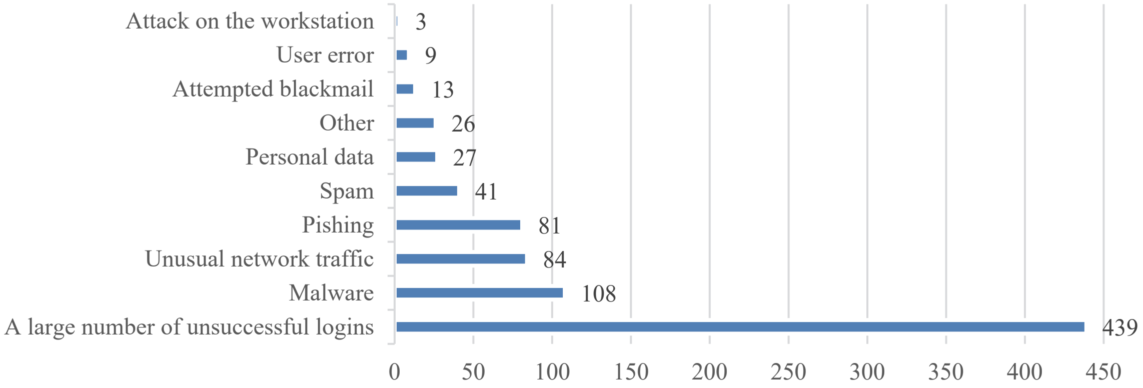

Figure 4. Distribution of report types to local SIRT of potential incidents. Source: Own study.

A very interesting issue is that users reported threats from most of the incident types, but the most common were identified threats in e-mails that were phishing, spam, or malware. Users do not have tools for assessing and monitoring threats, and based on the knowledge provided by SIRT on how to prevent threats and react to system malfunctions, as well as knowledge of security procedures, 219 events were reported, which constituted 26.35% of all analyzed notifications. The local SIRT team largely relied on reports from local users and CIRF BT, but having access to some security systems within its competence, resources monitored and analyzed the potential threats detected, which accounted for 11.55% of all reports.

Table 1. Reports to the SIRT team by type and source. Source: Own study

Threat type	CIRF BT	Local submissions	Local SIRT	External
A large number of unsuccessful logins	438	1	0	0
Malware	17	44	47	0
Unusual network traffic	36	2	46	0
Phishing	4	76	0	1
Spam	1	31	0	9
Personal data	1	26	0	0
Other	1	20	3	2
Attempted blackmail	0	13	0	0
User error	3	6	0	0
Attack on the workstation	3	0	0	0
Summary	504	219	96	12

Table 2. Number of reports to the SIRT in each year by type of incident. Source: Own study.

Threat type	Period				
	04.2018 12.2018	2019	2020	2021	01.2022 02.2022
Attack on the workstation	0	0	1	2	0
User error	2	4	1	2	0
Attempted blackmail	3	4	2	4	0
Other	1	4	1	12	8
Personal data	0	3	4	19	1
Spam	1	2	15	11	12
Phishing	14	24	22	16	5
Unusual network traffic	0	23	22	38	1
Malware	3	58	33	10	4
A large number of unsuccessful logins	0	0	435	3	1

When analyzing the reports, it can be noticed that in 2020 the highest number of unsuccessful logins was detected, which was associated with the monitoring by the CIRF BT security team from the logs of departmental security systems. Unfortunately, after the IT services left the organization at the beginning of 2021, the local SIRT team does not have this type of information, because the handling of these incidents takes place inside the CIRF, which took over the tasks in this area. Table 2 presents the distribution of individual types of threats in the analyzed period, there is a noticeable decrease in threats related to malware, which is dangerous for ICT systems, but the implementation of new anti-virus protection solutions and anti-spam filters significantly reduced the number of potential threats. In 2020, there were 43% fewer such reports compared to 2019, and in 2021 there were almost 70% fewer reports compared to 2020. Reports on other types of threats were at a similar level year-on-year, but it seems that 2022 will see many more reports of spam emails and the use of pishing. This trend is most likely due to the geopolitical situation and the number of reports that SIRT kept about these two types of threats in connection with the guidelines for users on the need to report potential threats in connection with the introduction of the third CHARLIE-CRP alert level in Polish cyberspace [9-13].

3. Tools and methods for resolving reports about potential threats

The incident management system shown in Figure 1 is a set of principles for a consistent and effective approach to information security incident and incident management, including information on events, threats and vulnerabilities. Defining these rules enables a quick reaction to emerging security notifications, and thus reducing the effects of their impact on business processes. The GDPR Act [8] imposes an obligation on the business administrator to report to the supervisory authority within 72 hours of the detection of an incident that may result in a risk of violating the rights or freedoms of natural persons.

All notifications received by SIRT are recorded. After receiving the notification, SIRT members proceed to analyze and evaluate the received and obtained information in order to determine whether the incident actually took place. If it is determined that the security incident has not occurred, the report is closed. If it is found that the event is related to the discovery of a new vulnerability or the use of a known vulnerability, SIRT informs the system owner about this fact in order to remove it or take other protective measures. In the case of confirmation of the occurrence of a security incident, SIRT conducts a detailed analysis of the incident, starting with collecting additional information, in particular by:

- determining the scale of the asset threat,
- identifying the source of the attack,
- identifying the tools / methods of attack.

When analyzing an incident or a safety request, the SIRT takes into account in particular:

- domain knowledge and professional experience,
- SIRT's internal knowledge base,
- identification of asset monitoring devices, including system logs, information from knowledge bases available on the Internet and tips on threats, e.g.: viruses, worms, trojan horses, attack methods, etc.

The analysis of the reports made it possible to work out the division of reports based on the type of threat. Technical threats include those in which: vulnerabilities or weaknesses of ICT systems were identified, attacks were detected using ICT tools, it was identified that the behavior of the ICT system deviates from the normal state, malware was detected in the system (active or inactive, located on electronic media). This type of threats includes: a large number of failed logins, malware, unusual network traffic, attacks on a workstation.

Another group is the social engineering threats that use the weakest and most susceptible to this type of attacks element of ITC security, which is human. These attacks use various methods in the field of psychology aimed at leading the user of the system to perform actions that are to bring tangible benefits to the attacker, such as infecting the system, obtaining credentials, confirming the correct email address or obtaining funds from a blackmailed victim. Four types of threats have been identified in this area: phishing, spam, blackmail, email malware. The remaining reports belong to the third group, which includes the following types of threats: personal data, other, user error.

If there is a suspicion that: malware has been run on the workstation, protection systems have detected unusual network traffic, the workstation is malfunctioning, it is necessary to take measures to reduce the potential effects of malware, protect traces that allow detection of the type of attack and its consequences, implementation of corrective actions removing the threat, restoring the system to the state it was in before the attack. The first step from the technical side is disconnecting the station from the network, then the system and anti-virus software logs were secured. In order to verify the endpoint infection, tools launched from external media are used - Live-CD distributions that connected to the Internet, after updating the version and virus signature databases, performed a comprehensive check of data media installed in the workstation.

In order to avoid the failure to detect malware, several (2-3) anti-virus programs were used to minimize the failure to detect malware, logs or summary information of the endpoint scan were saved from each verification. If the removal of threats from the ICT system was successful and no other potential threats were noticed on the basis of the log analysis, then the device was allowed to be used again. In a situation where it is not possible to remove the threats, it is uncertain whether the threats have been removed or there is a suspicion that the workstation may be vulnerable to repeated attacks after being connected to the ICT network, a decision was made to reinstall the operating system with the implementation of the necessary security rules. In this case, user data is archived for threat verification and restoration on a secured workstation.

Another method of combating threats was used when there was a high probability of no endpoint infection. The most common cases were: detection of threats during scanning of data carriers, blocking access to websites or malicious scripts on the website, blocking attachments or dangerous content in e-mails. If a threat was detected, it was verified whether the user was running the software, opening attachments, accessing websites listed in phishing e-mails, and whether the system was not working properly. If the collected information did not ensure that the identified threat was of a warning nature, a scan was performed with the use of on-line antivirus programs other than the one installed on the workstation. Detecting threats required taking the actions described in the previous case, when it was necessary to disconnect the computer from the LAN, perform corrective actions and restore it to the state before the incident occurred. Such situations happened sporadically and in the vast majority of cases, the service of the report ended with the removal of dangerous software from the carriers by antivirus programs, deletion of emails with malware, the user received recommendations to observe the functioning of the used workstation in terms of its malfunction and immediately report this fact to the IT services.

The third method of resolving reports is used for social engineering attacks carried out with the use of e-mails, the content of which is suspicious or the information contained in it is incomprehensible to the recipient (spam). A significant part of the reports received from users was of a warning nature, as a series of information campaigns, trainings and implemented procedures increased the users' alertness to dangerous and unwanted e-mails. The most frequent cases occurred in which the analysis of the content and attachments allowed for taking preventive measures consisting in removing unwanted e-mails from the mailbox. In the case when the recipient and the content of the e-mail indicated correctly directed information, but there were doubts as to whether the attachments do not contain malicious software, the possibility of previewing the content in MS Outlook of text attachments such as doc, docx, pdf or odt was used. If it was not possible to decide whether the attachment or link in the e-mail was safe, the virustotal.com website was used, where over fifty scanners verified the attachment in terms of threats. On this page, it is also possible to verify links to websites whether they contain malicious scripts or will not try to infect the workstation. Foreign-language e-mails, in particular in Russian, caused difficulties in assessing, due to the high probability of social engineering attacks.

Due to the fact that the tax administration units provide customs services to Russian-speaking people, it was necessary to verify whether the e-mail could relate to customs matters or whether it was typical spam or phishing. An additional problem that increased the number of this type of messages is the availability of e-mail addresses of customs departments, which is noticeable especially among units located at the state border, and therefore reports of Russian-language e-mails that were considered potentially suspicious due to their content were most often received. Situations when a user opened an attachment or clicked on a link in the message occurred much less frequently, in which case the above-described threat verification procedures were used. Massive phishing actions took place several times (an increase in local reports shown in Figure 1), but thanks to the information about the content of the e-mails, the SIRT team was able to quickly respond to emerging threats by providing users with appropriate messages about the existing wave of social engineering attacks and how to deal with unsolicited e-mail, which resulted in limiting the number of entries.

4. Assessment of threats and consequences for ICT systems

The analysis of the reports made it possible to distinguish three groups of security threats. Based on the typology of ICT systems security [5], intentional external threats, internal and external accidental threats were identified. Figure 5 shows the distribution of threats and the percentage distribution of notifications in individual areas. Reports classified as internal accidental threats constitute the largest group, their characteristic feature is that they can potentially cause serious consequences for the security of ICT systems.

The number of reports resulting from the detection of unusual behaviors of ICT systems is high and amounts to over 93.5% of all incidents in its group, which seems to distort the image of ICT systems security. In the group of targeted external threats, the dominance of typical amateur hacker attacks such as spam, malware and phishing are visible, constituting 93.5% of all incidents in its group, and in this case the distribution of incidents seems to be correct.

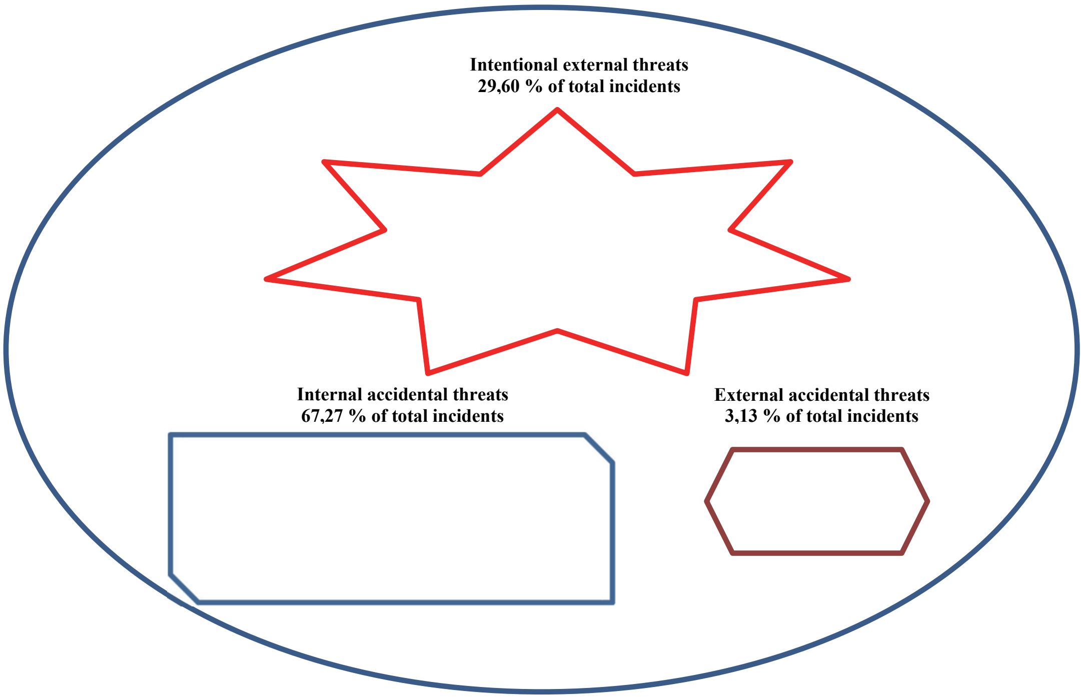
Intentional external threats
29,60 % of total incidents
Internal accidental threats
67,27 % of total incidents
External accidental threats
3,13 % of total incidents

Figure 4. Threat model based on notifications to the local SIRT with the use of ICT systems security typology. Source: Own study [5].

In order to analyze the threats and verify the detected statistical relationships, data on incidents in 2018 and 2022 were interpolated, in which the records did not cover the full year. When calculating the number of incidents, the data from the current year was taken into account, and the results obtained for individual groups were rounded down to a whole number. Table 3 shows the results of the data interpolation. In order to verify that the interpolations do not change the variance to a significant extent, the Fisher test was used for tables 1 and 3 and the obtained result was 1, which proves that the data interpolation method was properly selected.

Table 3. Number of reports to the SIRT in individual years by type of incidents. Source: Own study.

Threat type	Year					Variance	Mean deviation
	2018	2019	2020	2021	2022		
Attack on the workstation	0	0	1	2	0	0,64	0,72
User error	2	4	1	2	0	1,76	1,04
Attempted blackmail	4	4	2	4	0	2,56	1,44
Other	1	4	1	12	49	333,04	14,24
Personal data	0	3	4	19	6	43,44	5,04
Spam	1	2	15	11	74	741,04	21,36
Phishing	19	24	22	16	30	22,56	3,84
Unusual network traffic	0	23	22	38	6	181,76	11,84
Malware	4	58	33	10	24	363,36	15,76
A large number of unsuccessful logins	0	0	435	3	6	29968,56	138,48

The variance calculated for each type confirms the earlier observations that a large number of failed logins occurred in a short period of time, which results in a variance of 30,000. The situation is similar for the calculated mean deviation, where the mentioned type of incidents clearly differs from the others. For four threats with the variance ranging from 181 to 741. It is noticeable that changes in the geopolitical situation affect the increase in threats, the results obtained in the two months of 2022, interpolated for the whole year, indicate a significant increase compared to the years previous ones. Based on the collected data and the assessment of the degree of threat, the analyzes of North Electric Reliability Corporation [6] and Fortinet [2] have adopted a five-point scale of ITC security threats and assigned levels to individual types of incidents, which are presented in Table 4. It was assumed that level 1 means the lowest risk and level 5 means the highest security risk for ICT systems in the examined organization.

Table 4. Threat levels for the types of incidents reported to the SIRT. Source: Own study.

Threat type	The level of the threat	Threat type	The level of the threat
Attempted blackmail	1	Unusual network traffic	3
Spam	1	A large number of unsuccessful logins	3
User error	2	Phishing	4
Other	2	Attack on the workstation	5
Persona data	2	Malware	5

Based on the data from Tables 2 and 3, the matrix of security threats for individual types of threats was calculated, supplemented with additional calculations of the average level of threats in a given year, both for all types of threats and for each type individually, the results are presented in Table 5.

Table 5. Matrix of security risk levels for individual types of events. Source: Own study.

Threat type	Year					Total Threat Level	Average annual level of threats
	2018	2019	2020	2021	2022		
Attack on the workstation	0	0	5	10	0	15	3
User error	4	8	2	4	0	18	3,6
Attempted blackmail	4	4	2	4	0	14	2,8
Other	2	8	2	24	98	134	26,8
Personal data	0	6	8	38	12	64	12,8
Spam	1	2	15	11	74	103	20,6
Phishing	76	96	88	64	120	444	88,8
Unusual network traffic	0	69	66	114	18	267	53,4
Malware	20	290	165	50	120	645	129
A large number of unsuccessful logins	0	0	1305	9	18	1332	266,4
Total level of threats	107	483	1658	328	460		
Medium single threat level	3,45	3,96	3,09	2,80	2,36		

The obtained results indicate that the incidents classified as "external intentional" incidents significantly affect the decrease in security, which results not only from the adopted scale of threat levels, but also from the number of occurrences. Both in the analyzed period and the calculated average annual level of threats, they occupy the leading places, which is shown on the map of threats - Figure 4. Spam was characterized by a slightly lower total level of threats, which due to the low level of a single threat on an annual basis, contributed much less to the increase in the level of threats. On the other hand, attacks on workstations, which are one of the most dangerous due to the real threat of security breaches, only slightly increased the level of ITC security threat, as they were incidental.

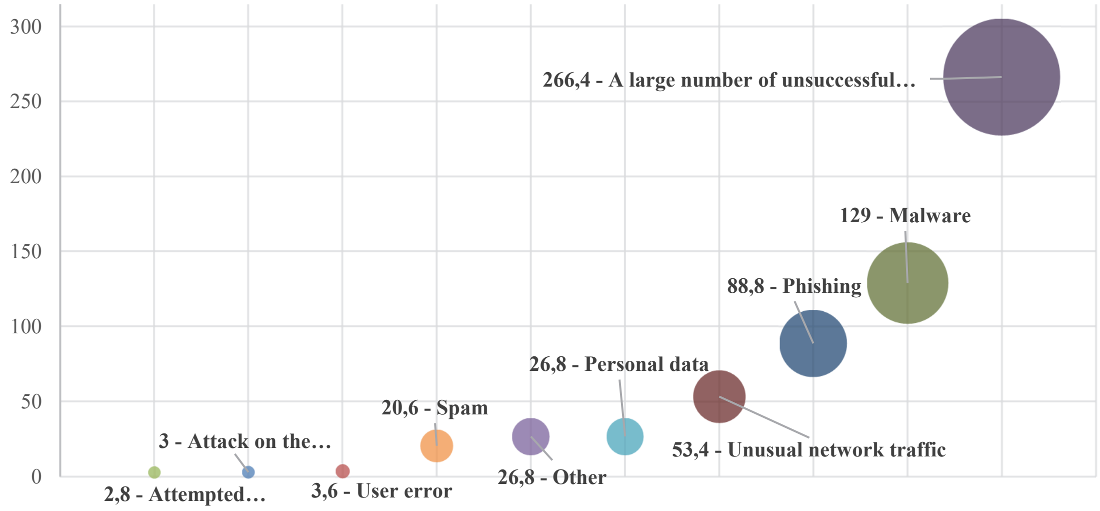

Figure 4. Average-annual level distribution map of hazard types based on notifications to the local SIRT. Source: Own study

When analyzing the level of threats, it is justified to examine how it was distributed in particular years and what was the average level of threats of the reported events. Figure 5 shows how significantly disrupted the distribution of threats in 2020, in which 1,305 events related to a large number of unsuccessful logins were identified. If these incidents were at the level of 100-200, we would deal with a relatively regular distribution of threats in the analyzed period. It should also be noted that in 2018 a new SIRT team was created, which was systematically equipped with ICT tools and procedures enabling the efficient identification of threats and information campaign, which translated into a relatively regular number of incidents reported in the following years. The analysis of the level of threats was supplemented by the calculation of the average level of threat of a single report in order to assess whether they relate to incidents with a high level of threat or whether they are events with a low level of risk for ICT systems. In 2019, after the implementation of new anti-virus protection systems, there was a significant increase in the level of threat of detected events, which resulted from the scanning of ICT systems for vulnerabilities and malware.

These activities allowed to reduce the level of risk of a single incident in the following years, and in particular in 2020, when 1,305 incidents related to login errors were identified. The following years brought a decrease in the level of risk of a single event, it is related to changes in the field of IT service, which was excluded from the organization, which resulted in less availability of information about incidents from departmental security systems and limited knowledge about incidents detected by security systems. The forecast for 2022 indicates an increase in the number of incidents, including those with a high level of threats, but there will be a noticeable decrease in the threat index by 0.34 points.

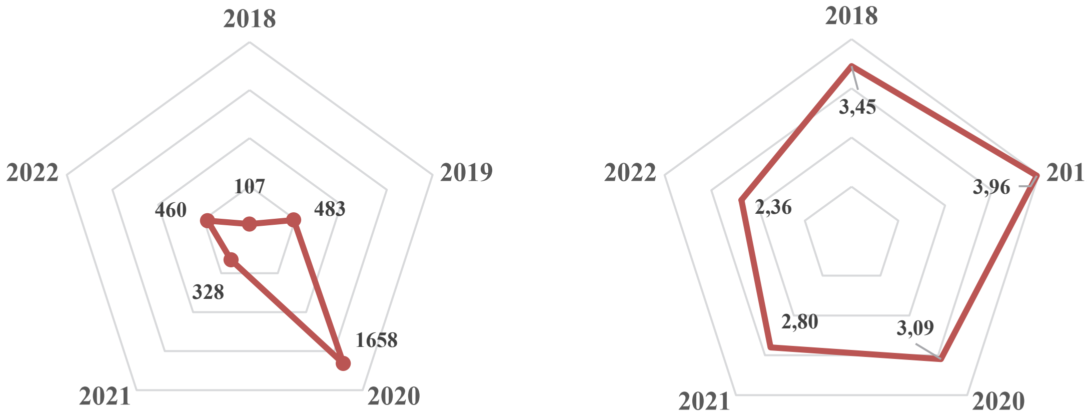

Figure 5. Total distribution of threats, the average level of threat of a single event in 2018-2022. Source: Own study.

It should be emphasized that the calculated indicators of risk levels relate to the situation when all reports materialized and turned into security incidents. The conducted research on the perception of security threats indicated that groups of organized or unorganized hackers pose the greatest threat to ICT systems [5]. When analyzing who is the source of threats on the basis of the analysis of reports to the SIRT, four groups of incident actors were excluded, as there was no evidence that the manner of carrying out the incidents, the degree of harmfulness and the effects of threats indicate cyber-attacks carried out by these groups. Figure 6 shows the results obtained in [5]. Actors who did not generate incidents in the analyzed period were distinguished in a light color.

This indicates that intentional external incidents should be classified as cybercriminal activities. The conducted research on the perception of the level of ICT threats [5] shows that cybercrime is less likely to weaken the security of ICT systems. The conducted research indicated that 95% of respondents believe that cybercriminal activities may significantly weaken the security of ICT systems. An important factor blocking cyber-attacks, limiting the likelihood of their effects, are hardware and software solutions for securing information systems.

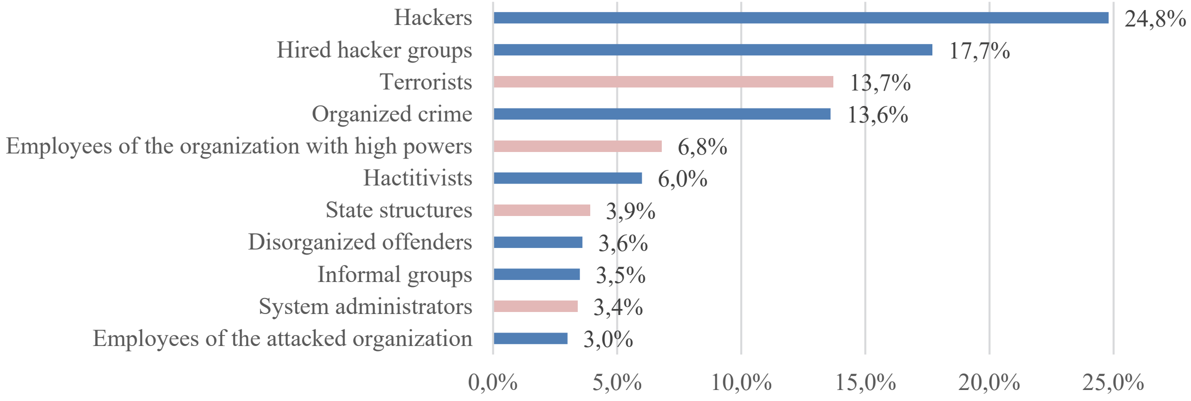

Figure 6. Groups that pose the greatest threat to e-administration IT systems. Source: Development on the basis of [5] p. 206.

The respondents indicated the importance of implementing an information security management system as a factor that has a significant impact on ensuring ICT security [5]. The above analysis of the reports in combination with the research on the perception of security of the respondents confirms the correctness of the implemented hardware, software and legal solutions. In most cases, the security measures and the appropriate reaction of users allowed for the avoidance of incidents and damage to ICT systems. Moreover, there was no case where it was necessary to escalate the notification to the departmental SIRT team and launch business continuity plans in order to restore the ICT system to the state it was in before the attack.

The research on the frequency of various types of threats conducted by North Electric Reliability Corporation [6] has shown that cyberterrorism is a phenomenon that occurs less frequently, but the effects of such attacks bring more serious losses to the organization and significantly destabilize the functioning of ICT systems. Russia's aggression against Ukraine has shown that state structures can also participate in cyber-terrorist activities and pose a particularly serious threat in the initial phase of an attack [1, 15]. Even before the start of hostilities, Ukraine's critical systems were attacked and partially blocked, which shows what technical and human capabilities are at the disposal of a country that is one of the world powers.

At the moment, it seems that the IT infrastructure of the tax administration is sufficiently secured. The introduced and binding CHARLIE-CRP alert state as well as the conclusions collected from the hitherto conducted cyberspace war and the security measures implemented by Internet operators and IT services responsible for the security of Polish cyberspace indicate that ICT systems are prepared for potential cyber-attacks, therefore the impact and effects of incidents will be limited.

References

1. Drabczuk M., Cyber-attacks as a tool of pressure on Ukraine and the West, Institute of Central Europe, https://ies.lublin.pl/komentarze/cyberataki-narzedziem-presji-na-ukraine-i-zachod/, access date (2022.04.08),
2. Fortinet Inc., High Performance Network Security, Sunnyvale 2013,
3. Management of ICT security incidents in the Ministry of Finance and in organizational units of the Ministry of Finance, Ministry of Finance - Department of Security and Information Protection, Warsaw 2015,
4. Mitnick K., Simon W. L., The Art of Deception: Controlling the Human Element of Security, Wiley, 2002,
5. Muliński T., Security threats to e-administration IT systems, CeDeWu, Warsaw 2015,
6. North American Electric Reliability Corporation, Cyber Attack Task Force - Final Report, Atlanta 2012,
7. Ordinance of the Minister of Development and Finance of July 3, 2017 on the definition of procedures for the implementation of projects for the Ministry of Finance and subordinate or supervised units for the implementation of projects carried out in individual alarm levels and CRP alarm levels, Official Journal of the Minister of Development and Finance 2017, item 133,

8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1,
9. Regulation no. 32 of the Prime Minister of February 15, 2022 on the introduction of the CRP alert level, Prime Minister, Warsaw 2022,
10. Regulation no. 40 of the Prime Minister of February 21, 2022 on changing the alert level of CRP, Prime Minister, Warsaw 2022,
11. Regulation no. 52 of the Prime Minister of 04/03/2022 on the introduction of the CRP alert level, Prime Minister, Warsaw 2022,
12. Regulation no. 62 of the Prime Minister of March 15, 2022 on the introduction of the CRP alert level, Prime Minister, Warsaw 2022,
13. Regulation no. 71 of the Prime Minister of March 31, 2022 on the introduction of the CRP alert level, Prime Minister, Warsaw 2022,
14. Regulation of the Prime Minister of July 25, 2016 on the scope of projects carried out in individual alert levels and alert levels of CRP, Journal of Laws 2016, item 1101,
15. Szydłowski O., Zaniewicz M., Cyberattack on Ukraine, commentary no 10 (2022), The Polish Institute of International Affairs, Warsaw 2022,
16. Świtalski P., Kopówka M., Machine Learning Methods in E-mail Spam Classification, Studia Informatica. System and information technology, vol. 23, no 1-2 (2019), UPH, Siedlce 2019.