# Building a security team in academia: proposal of a new concept

Martin Havránek[1,*,†], Václav Lohr[1,†] , Pavel Ambruz[1,†], Martin Lukáš[1,†], Miloš Ulman[1,†]

[1] *Czech University of Life Sciences Prague, Faculty of Economics and Management, Kamýcká 129, 16500 Praha -Suchdol*

## Abstract

In this idea paper we provide a comprehensive overview of the role computer security incident response team (CSIRT) and analyse the challenges of building a CSIRT in the academic environment. We describe an academic CSIRT schema of operation, propose its operations and risk assessment template, and discuss key threats to tackle, catalog of services, knowledge base and incident handling. The proposed CSIRT concept is tailored specifically to university environment and will be verified at a selected university.

## Keywords

CSIRT, university, threat, risk assessment, knowledge base.

## 1. Introduction

The academic environment is characterised by openness and free information sharing between students, teachers and researchers. The user base is diverse, including different groups with different needs and access rights.

Academic freedom and research independence must be preserved, which may conflict with strict security measures. Institutions work with various data, including personal data and research results, and face frequent technological change. Users are often mobile, requiring flexible and secure remote access.

International collaboration adds another layer of complexity to data security and communication. Compliance with regulations such as the General Data Protection Regulation (GDPR) is essential [23]. Financial constraints often affect the ability to invest in security technology and personnel. IT infrastructure is large and heterogeneous, often

*The 10th International Conference on Socio-Technical Perspectives in IS (STPIS'24) August 16-17 2024 Jönköping, Sweden.*

[*] Corresponding author.

[†] These authors contributed equally.

havranek@pef.czu.cz (M. Havránek); lohr@pef.czu.cz (V. Lohr); ambruzp@pef.czu.cz (P. Ambruz) ; lukas@pef.czu.cz (M. Lukáš) ; ulman@pef.czu.cz (M. Ulman)

0000-0001-5218-5391 (M. Havránek); 0000-0002-2688-4049 (V. Lohr); 0009-0001-6234-0620 (P. Ambruz); 0000-0003-0356-5480 (M. Lukáš); 0000-0001-9556-7672 (M. Ulman)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

including legacy systems that may be more vulnerable. And finally - given the evolving regulatory landscape, it will soon be necessary to implement measures in compliance [24] with the NIS2 directive [25] - by October 17, 2024. [1]

Although a computer security incident response team (CSIRT) should be a common practice in all types of organisations, there are only 56 teams in research and education organisations out of 581 CSIRT in the EU [2]. Yet, the high initial and operating costs of maintaining a CSIRT, lack of qualified staff and generally low awareness of cybersecurity threats are root causes of the current state. “Cross-CSIRT organisations have played a key role in facilitating exchanges and collaboration among national CSIRTs and the wider CSIRT and cyber security communities, around the world and within some geographic regions.” [3]

The aim of this paper is to propose a new concept for building a security team in an academic environment. We want to outline strategies to effectively protect sensitive data and information systems without compromising academic freedom and creativity. We will also address the specific challenges academic institutions face in the area of cybersecurity taking into account the unique needs and dynamics of educational institutions.

# 2. Background

## 2.1. Current state of the art

CSIRT represents a specialized team of experts whose primary responsibility is to respond to cyber incidents, including but not limited to DDoS attacks, malware, data breaches, misuse, or the outage of entire infrastructures [4]. CSIRT may have variable utility despite its clearly defined goal, as the protected infrastructure is not always perceived as critical [5]. In this regard, the structure of the CSIRT team can be divided into several levels, specifically university, corporate or business, and government teams [26]. As implied by the respective designations, each of these has its specifics, which may vary, although they share the same goal [6].

The fundamental differences among the individual teams lie in their purpose, authorities, and, of course, finances. It is not possible to unequivocally determine which team is the best, as each has its own specifics. For example, a governmental CSIRT will primarily focus on protecting critical elements of the state, whereas a university team will primarily concentrate on safeguarding research databases and, generally, school infrastructure. A corporate CSIRT, on the other hand, will unequivocally endeavor to protect its infrastructure and ensure the continuous operation of its business [7].

CESNET CSIRT provides cyber security for academic and research institutions in the Czech Republic. Its main tasks include monitoring network traffic, detection and rapid response to security incidents, implementation of preventive measures, provision of expert advice and support, organisation of training and educational events, cooperation with national and international security organisations, processing of incident reports and research in the field of cyber security. However, little is known in the literature about how to build academic CSIRT and how to align them with the national and international structures of CSIRT [8].

The first essential step is to conduct a feasibility study to determine whether the establishment of a CSIRT team is truly necessary. This study must encompass all key aspects associated with project implementation, including a clear answer to the question of whether a CSIRT team is needed. Regardless of the team's level, it is crucial to clearly define its goals, responsibilities, and workflow. These criteria are pivotal for designing an appropriate CSIRT team structure and preparing all necessary documentation for its establishment. Unfortunately, despite all these measures, finances remain paramount, as only a sufficiently large budget can secure all required material and human resources for the project [9].

## 2.2. Review of existing solutions

This review focused on the unique challenges and characteristics of academic CSIRTs and compared them to national and enterprise CSIRTs. We reviewed academic articles, official documents, standards such as RFC 2350, and practical examples of CSIRTs to understand current trends and best practices.

The information was organised into sections for each type of CSIRT, detailing their main tasks and characteristics. National CSIRTs secure critical state infrastructure and cooperate at the international level. Corporate CSIRTs benefit from better financial support and use artificial intelligence for decision-making. Academic CSIRTs face funding issues and staff turnover but emphasise research and publishing.

We compared the strengths and weaknesses of each type of CSIRT and highlighted the specific needs of academic teams. We concluded the review with key findings and recommendations for improving the performance of CSIRTs and provided insights for further development in cybersecurity with a focus on academic CSIRTs.

The structure of the CSIRT team that we are examining focuses primarily on three categories: national, corporate, and academic CSIRT teams. Although these teams are fundamentally similar, each has a distinct role that makes their existence essential.

### 2.2.1. National CSIRT

National CSIRT teams have several primary missions [10], including:

1. Providing security services.
2. Collaboration with entities within the state.
3. Transnational cooperation with the global CSIRT community.

National CSIRT primarily focuses on the critical infrastructure of the state and strives to secure key institutions for its proper functioning. Currently, cybersecurity is a significant topic globally, and every state is actively seeking to engage in measures in this area.

An important factor is that each national CSIRT team adheres to RFC 2350 [11] to comply with established standards and to better communicate with others. For example, the Polish CSIRT team [12] essentially shares the same goal as all others but has minor deviations in its definition of critical infrastructure, which is entirely normal as it is not always possible to defend everything. Therefore, an initial feasibility study of the entire CSIRT team project is crucial to clearly identify what is considered critical infrastructure and how to protect it. Another example is the Spanish CSIRT team (Home, n.d.), which also adheres to standards but has minor deviations in the definition of critical infrastructure. To ensure that the national CSIRT team is a quality partner in the field of cybersecurity, it is necessary to adhere to general standards in the construction and purpose of the CSIRT team [13].

### 2.2.2. Corporate CSIRT

The corporate CSIRT team is usually better financially supported than the national team and also has sufficient resources and opportunities for the professional development of its members. The main focus of the corporate team is to ensure the secure operation of the company and prevent unauthorized access to the internal network. From a cybersecurity perspective, end-user devices utilized by company employees are the most vulnerable [14].

The corporate team typically has the advantage of not needing to connect with various public entities and is not required to operate from any specific public location. This simple rule enables easier monitoring of entry points into the internal network compared to government or university teams. The key elements of the corporate team include proper structure, allocation of responsibilities, and prompt responses to cyber incidents. Smaller units within the team also play an important role, requiring efficient and rapid communication. The final integral component is the security manager, who decides on the course of action in resolving the specific cyber incident. It is important to note that currently, the majority of incidents are addressed automatically, with decision-making handled by artificial intelligence (UI) [15].

### 2.2.3. Academic CSIRT

The university CSIRT is highly specific due to its functionality, as it requires various user and application approaches, and additionally involves research databases and projects in general. Universities often face inadequate financial support for this type of project, and they frequently rely on assistance from public companies or the government. From a certain perspective, they have an advantage in recruiting team members due to the possibility of involving students. However, this leads to team instability, and frequent turnover of members may not guarantee sufficient expertise within the team [16].

Given the scope of applications, end-user devices, and other server equipment, the university network is relatively unique and capable of addressing specific cyber incidents. The university CSIRT primarily focuses on three main areas:

1. Identifying end users within the university network.
2. Investigating cyber incidents.
3. Publishing results and research from the university CSIRT team.

The university CSIRT team places particular emphasis on research, as the range of security aspects is the broadest among all types of CSIRT teams [17].

According to [18] The cybersecurity team of the future will be intrinsically multidisciplinary, composed of internal and external expertise (consisting of both people and artificial intelligence) from multiple diverse relevant fields. The people involved will have a proclivity for combining their deep areas of expertise with others on the team who possess complementary deep knowledge, abilities, and experiences. Because of cybersecurity's inter-dependencies across core business functions, members of the cybersecurity team will examine each business process to determine acceptable levels of risk. They will also protect the organization by ensuring that business solutions, products, and services are designed, developed, provided, and maintained with full consideration of the latest security risks to the customers.

## 3. A proposal of a university department CSIRT

In this chapter, we will focus on the process of establishing a CSIRT team and describing its schema of operation. This study focuses on the creation of a team for a specific part of the university, such as a department, faculty, etc. This approach differs from the creation of a CSIRT for the entire university, which views the university as a whole. In this case, the study is centered on the security of projects conducted within individual parts, which are often independent of the overall university infrastructure and have a certain degree of autonomy, including responsibility for security. The main tasks of a CSIRT are: risk identification, compiling a service catalog, and incident response. Considering the dynamic nature of the entire process, it is necessary to periodically review threats, vulnerabilities, and new services.

Based on the research of existing solutions, the following CSIRT schema of operation (Figure 1) was proposed. Solution is proposed based on previous literature research with choosing suitable techniques found in materials described in previous chapter.

After establishing a CSIRT, it is necessary to identify (i) threats and vulnerabilities, (ii) the service catalog, and (iii) controls identification (protection options for services). These three factors then feed into the risk assessment. Within this step, (i) risk identification, (ii) risk estimation, and (iii) risk evaluation are performed.

In the event of an incident, the first level of support determines whether relevant measures can be taken using playbooks established in the knowledge base. If the incident cannot be resolved at the first level of support, it is escalated to specialized second and third-level teams. The record of the resolution procedure is stored in the knowledge base in case of a recurring incident. If a new threat is identified, it is necessary to reassess the risks in relation to the operational service catalog.

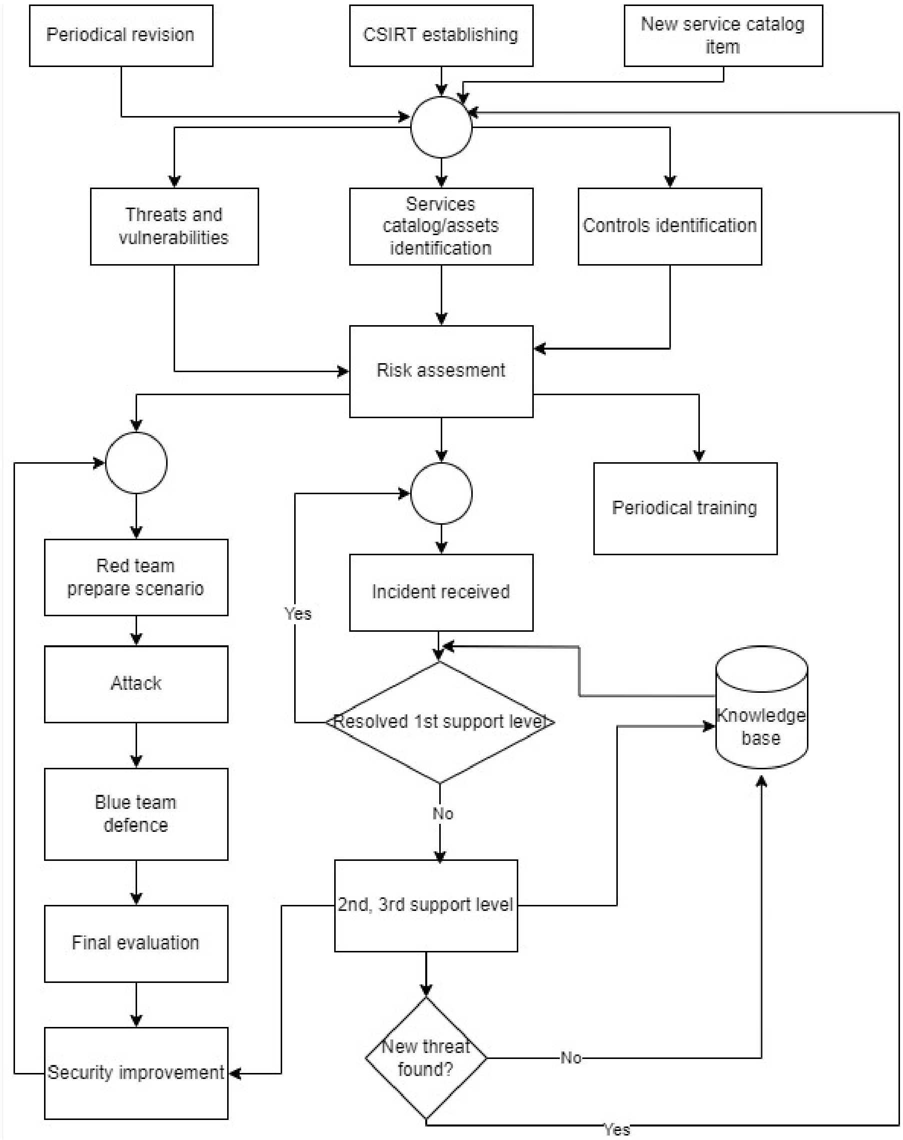

Figure 1: Proposed CSIRT schema of operation

## 3.1. CSIRT establishing

According to [19] minimal requirements on CSIRT are Information security incident management (vulnerability management, vulnerability discovery/research, vulnerability analysis, vulnerability disclosure and vulnerability response), Situational awareness, Knowledge transfer and Information security event management

There are different roles in CSIRT. Blue and red teams play complementary roles in ensuring the organization's cybersecurity posture is robust and resilient against threats.

The blue team's primary focus is on defense and response. They are responsible for continuous monitoring of network traffic, system logs, and other data to detect potential security incidents, utilizing tools such as Security Information and Event Management (SIEM) systems for data aggregation and analysis. When a security incident is detected, the blue team acts swiftly to contain, eradicate, and recover from it by following predefined incident response plans and employing forensic tools to investigate breaches. Additionally, they manage vulnerabilities by regularly scanning systems for weaknesses and ensuring timely application of patches and updates. The blue team also gathers and analyzes threat intelligence to stay ahead of emerging threats and proactively defend against them. Furthermore, they are involved in educating employees on security best practices, phishing awareness, and other aspects of cybersecurity hygiene.

The red team focuses on attack and testing. They conduct penetration testing to simulate attacks on the organization's systems, networks, and applications to identify vulnerabilities and weaknesses, using both automated scans and manual testing techniques. This team also tests the organization's resilience against social engineering attacks, such as phishing or pretexting, to identify human vulnerabilities. They perform advanced, targeted attack simulations, like Advanced Persistent Threat (APT) scenarios, to test the organization's detection and response capabilities under realistic conditions. After completing their assessments, the red team documents their findings and provides detailed reports on vulnerabilities, attack vectors, and potential impacts, along with recommendations for improving defenses. Collaboration with the blue team is crucial, as it involves addressing identified weaknesses, improving incident response plans, and enhancing overall security measures.

### 3.2. Risk assesment

Risk assessment can be divided into three areas.

The first area (User-focused threats) includes attacks targeted at users. These are mainly social engineering attacks, attacks using computer viruses, and attacks on insufficiently secured accounts. This category also includes insider threats, where the attacker exploits access to local network resources. However, this type of attack can also result from an insufficiently secured or compromised employee account.

The second area (Application-focused threats) includes attacks focused on application security and the security of system infrastructure. In practice, these are attacks on operating systems, hypervisors, web servers, database systems, and the applications themselves.

The third area (Network-focused threats) covers network infrastructure and network protocols. Some of these attacks fall within the competence of the Internet Service Provider (ISP). Other attacks target the vulnerabilities of individual protocols such as DNS, SMTP, IP, etc. In most universities, the network infrastructure is centrally managed in collaboration with connectivity providers. Therefore, only significant threats from this area are included here, as they must be considered, but they cannot be influenced much in terms of the proposed solution.

Table 1
Threats identification (based on [20])

| User-focused threats | Application-focused threats | Network-focused threats |
|---|---|---|
| Online frauds | Injection flaws | DDoS |
| Phishing | Broken authentication | MitM |
| Scam | Sensitive data exposure | Packet Sniffer |
| Spam | XML external entities | IP Spoofing |
| Identity theft | Security misconfiguration | Flood Attack |
| Social engineering | XSS | DNS Spoofing |
| Vishing | Insecure deserialization | |
| Smishing | Insufficient logging & monitoring | |
| Login credentials | Password attack | |
| Malware | Session Hijacking | |
| Insider Threats | SSL Hijacking | |
| | Compromised key | |
| | Brute Force attack | |
| | Malware | |
| | Database attack | |

Table 1 was created by selecting relevant threats from [20], where is full list of threats. From the original list of threats, only those relevant to the purposes of this study were identified. Therefore, only threats related to the operation of the subsystem within the department were selected.

Despite the categorization of threats (Table 1), it is important to note that some risks can be mitigated in multiple ways. For this reason, risk assessments must always be conducted comprehensively, utilizing all possible defense options. Additionally, some security systems can conflict with each other. For example, sensitive data exposure or MitM (Man-in-the-Middle) attacks can be eliminated by implementing encrypted communication. However, some security systems perform SSL inspection to test communication for malware, which reduces the security of sensitive data [22].

The risk assessment will be recorded in a two-dimensional table, with individual threats in the rows and assets in the columns. The assessment involves three metrics: impact (I), threat (T), and vulnerability (V). All metrics are defined on a scale from 1 to 4, where 1=low, 2=medium, 3=high, and 4=critical. The risk level is determined by formula R=I x T x V and finally is evaluated as Low (1-16), Medium (17-31), High (32-47), Critical (48-64). An example of risk level assessment is provided in Table 2. The values presented in the table are illustrative only. The actual determination of risk levels will be possible after the analyses are conducted.

Table 2
Risk assessment template. Source: own.

| Threat\Asset | Student projects | Department research |
|---|---|---|
| Identity theft | I=1 T=3 V=2 | I=4 T=2 V=2 |

| | | |
|---|---|---|
| | R=6 | R=16 |
| XSS | I=1 T=3 V=1<br>R=3 | I=2 T=3 V=1<br>R=6 |
| Compromised key | I=2 T=1 V=1<br>R=1 | I=3 T=2 V=2<br>R=12 |
| Spam | I=1 T=1 V=1<br>R=1 | I=2 T=1 V=1<br>R=2 |
| **Total** | **11** | **36** |

## 3.3. Catalog of services / asset identification

The identification of assets and provided services is crucial for determining the resources that need protection. It is recommended to start with a minimal, yet precisely specified set of resources, and then add and expand as necessary [21]. A common issue is the introduction of new assets without including them in the risk assessment. Therefore, the proposed solution includes a periodic review of operated assets followed by a new risk assessment.

## 3.4. Knowledge base

Knowledge base provides a centralized repository for all the information relevant to incident response. This includes documentation of past incidents, response procedures, technical details, threat intelligence, and more. A playbook in the context of a CSIRT and knowledge base is a set of predefined procedures and actions to be taken in response to specific types of incidents. Each playbook provides step-by-step guidance on how to handle a particular scenario.

Given the expected frequent turnover of CSIRT members from students, it is essential to ensure effective knowledge transfer. Therefore, the knowledge base is a crucial component of the proposed solution, and it is necessary to precisely document the resolution of incidents in the form of a playbook for future use.

## 3.5. Incident handling

According to [21], the incident is reported to first-level support staff. At this level, it is assumed that the incident will be classified and a solution found using the knowledge base. Support staff will also request more detailed information and look up relevant sources for the incident. If a solution is not found using the knowledge base and the first-level support staff cannot resolve it, the incident is escalated to second and third-level support specialists. These are previously unresolved or complex cases. After the successful investigation of the incident, the problem record is described in the knowledge base in case the incident recurs. If a new threat is identified, it is necessary to perform a repeated risk assessment (i.e., it is necessary to verify the impact of the new threat on the service catalog).

## 4. Discussion and conclusion

The proposed solution is based on a review of available sources, from which a CSIRT schema of operation diagram was created. The diagram includes both periodic activities (review of threats and vulnerabilities) and responses to changes in the operated systems (New service catalog item). The primary goal of the CSIRT is continuous testing of resilience against cyber threats and response to incidents. Emphasis is placed on a knowledge base for faster response to past incidents. Given the expected higher turnover of CSIRT members (students are only involved during their studies), it is necessary to ensure a sufficiently reliable knowledge transfer.

Compared to other solutions, the proposed solution is tailored specifically for deployment in an academic environment. It is primarily focused on preventing attacks on data and the misuse of research and student projects. Less emphasis is placed on network security, which is managed by the university's system administration. More emphasis is placed on newly deployed software systems, which, unlike in a corporate environment, have greater flexibility during deployment and thus become more frequent targets of attacks.

A key strength of this study is the compilation of the latest insights for creating a CSIRT. At the same time, it is tailored to the needs and specifics of the university's department. Individual departments often have autonomy, within which they can create websites, computer systems, and projects to support teaching, which are not part of the university's system and therefore do not fall directly under the control of university-wide security. However, this also brings the responsibility for the operated systems and their security. This study can be compared to the relationship between a university and an ISP. An ISP uses its own security team, just like a university, but the purpose and functioning of each team differ. Similarly, in this study, the university acts as the ISP, and the departments are the system operators.

A potential threat may predominantly lie in the relationship between the university department's CSIRT and the university's infrastructure. Additionally, greater involvement of students and internal staff from the department is expected, which will often lead to increased turnover. Therefore, it is necessary to adhere to the principles of maintaining a knowledge base for repeated incident resolution.

We will utilize the proposed CSIRT operation within a selected university. The experience and collected feedback will be used in a follow up full research paper.

# REFERENCES

[1] European Commission. "NIS2 Directive." Digital Strategy, 2023. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[2] European Union Agency for Cybersecurity (ENISA). "CSIRTs by Country - Interactive Map." Available at: https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map (Accessed: 28 May 2024).

[3] Kassim, S. R. B. M., & Arief, B. (2023). Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions. doi:10.1145/3609230.

[4] Van der Kleij, R., Kleinhuis, G., Young, H. (2017). Computer security incident response team effectiveness: A needs assessment. In Frontiers in Psychology, 8 (DEC), art. no. 2179. Available at: https://www.frontiersin.org/articles/10.3389/fpsyg.2017.02179/full, doi:10.3389/fpsyg.2017.02179 (Accessed: 28 May 2024).

[5] Forum of Incident Response and Security Teams, Inc. (2019). Computer Security Incident Response Team (CSIRT) Services Framework. Available at: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf (Accessed: 28 May 2024).

[6] Wara, Y.M. and Singh, D. (2015). A Guide to Establishing Computer Security Incident Response Team (CSIRT) For National Research and Education Network (NREN), 8(2). [7] Brecht, D. (2018). The Skills and Experience Needed to Support A CSIRT SOC or SIEM Team. InfoSec Resources, February 2018. Available at: https://resources.infosecinstitute.com/skills-experience-needed-support-csirt-soc-siem-team/

[8] Bada, M. et al. (2020). Computer Security Incident Response Teams (CSIRTs) An Overview. Available at: https://ssrn.com/abstract=3659974Avai

[9] Mooi, R. and Botha, R.A. (2015). Prerequisites for building a Computer Security Incident Response capability. In 2015 Information Security for South Africa (ISSA), pp. 1–8. Available at: https://doi.org/10.1109/ISSA.2015.7335057.

[10] Home - CSIRT (2024). Available at: https://csirt.cz/en/ (Accessed: 28 May 2024).

[11] Guttman, E. and Brownlee, N. (1998). Expectations for Computer Security Incident Response. Request for Comments RFC 2350. Internet Engineering Task Force. doi:10.17487/RFC2350.

[12] Team, T.C.S.I.R. (2024). The Computer Security Incident Response Team. Available at: https://csirt.gov.pl/cee (Accessed: 28 May 2024).

[13] Morgus, R. et al. (2015). NATIONAL CSIRTs AND THEIR ROLE IN COMPUTER SECURITY INCIDENT RESPONSE, p. 36.

[14] Mitchell, B. (2020). CORPORATE CYBERESPIONAGE: IDENTIFICATION AND PREVENTION PART 1. EDPACS. Available at: https://www.tandfonline.com/doi/abs/10.1080/07366981.2020.1798594 (Accessed: 9 May 2024).

[15] Mohd, N. et al. (2016). CSIRT Management Workflow: Practical Guide for Critical Infrastructure Organizations. In P. Silva, A. Guerreiro, and R. Quaresma (eds) Proceedings of the 10th European Conference on Information Systems Management,

pp. 138–146. Available at: https://www.webofscience.com/wos/woscc/full-record/WOS:000400275000018 (Accessed: 8 May 2024).

[16] Najiyya, A. and Wulandari, S.S. (2023). Eksplorasi Implementasi Kebijakan Pembentukan Computer Security Incident Response Team (Csirt) di Kementerian Perdagangan: Sebuah Studi Kualitatif. JRAM (Jurnal Riset Akuntansi Multiparadigma), 10(1), pp. 50–55. Available at: https://doi.org/10.30743/akutansi.v10i1.7246.

[17] Andrade, R.O. et al. (2019). Information security management in university campus using cognitive security. Int. J. Comput. Sci. Inf. Secur. 13 (4)

[18] Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2019). Educating Future Multidisciplinary Cybersecurity Teams. Computer, 52(3), 58–66. https://doi.org/10.1109/MC.2018.2884190

[19] Cybersecurity, E. U. A. for, & Taurins, E. (2020). *How to set up CSIRTs and SOCs – Good practice guide*. https://doi.org/doi/10.2824/056764

[20] Alothman, B., Alhajraf, A., Alajmi, R., Farraj, R. al, Alshareef, N., & Khan, M. (2022). Developing a Cyber Incident Exercises Model to Educate Security Teams. *Electronics*, *11*(10), 1575. https://doi.org/https://doi.org/10.3390/electronics11101575

[21] Villegas-Ch, W., Ortiz-Garces, I., & Sánchez-Viteri, S. (2021). Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. *Computers*, *10*(8), 102. https://doi.org/https://doi.org/10.3390/computers10080102

[22] O'Neill, M., Ruoti, S., Seamons, K., & Zappala, D. (2017). TLS Inspection: How Often and Who Cares? *IEEE Internet Computing*, *21*(3), 22–29. https://doi.org/10.1109/MIC.2017.58

[23] N. A. Zaguir, G. H. de Magalhães and M. de Mesquita Spinola, "Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions," in *IEEE Access*, vol. 12, pp. 81608-81630, 2024, https://doi.org/10.1109/ACCESS.2024.3406724

[24] Vostoupal, J., Stupka, V., Harašta, J., Kasl, F., Loutocký, P., Malinka, K. The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond. Computer Law & Security Review. vol. 53, 2024. ISSN 0267-364. https://doi.org/10.1016/j.clsr.2024.105988

[25] Vandezande, N. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, vol. 52, 2024. ISSN 0267-3649. https://doi.org/10.1016/j.clsr.2023.105890

[26] Dsouza, Z. Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security?. Federal Communications Law Journal, vol. 69. Washington.