European Research Studies Journal
Volume XXVII, Issue S2, 2024

pp. 444-453

Analyzing Cyber-Attack Trends on an Educational Institution: A Case Study (2021–2023)

Submitted 08/09/24, 1st revision 20/10/24, 2nd revision 06/11/24, accepted 05/12/24

Grzegorz Podgórski[1]

Abstract:

Purpose: *Monitoring changing threats and adapting to the new realities of cyberspace is becoming a priority for security. In this respect, the analysis of threats, attack vectors and sources allow better protection of university resources. They allow the identification of particularly vulnerable areas, as well as the identification of the main targets of cyber criminals. The result of such an analysis is the definition of such places in the IT infrastructure that should be subject to special protection. The result of such an analysis also allows a better and more complete security system to be built.*
Design/Methodology/Approach: *The research method used in the presented article is a case study. In this study, the subject is a unit of a university employing over 340 people. From January 2021 to December 2023, data on network attacks were collected by devices and security systems. The data was then analyzed. Real-time data was collected depicting the current cyber security landscape of a university unit.*
Findings: *Universities, such as public research and education institutions, are particularly vulnerable to all kinds of network attacks. Analyzing the data collected on such threats allows a better understanding of them and appropriate preventive measures to be taken. Identifying elements such as threat categories, the sources of attacks and their target allows better protection of university resources.*
Practical Implications: *The analysis of network attacks on a university unit in the context of information security allows for tangible benefits, especially in increasing the level of information security. It also allows us to define the types of threats such units must face. It also gives the possibility to fine-tune and better adapt existing security solutions or implement new ones.*
Originality/Value: *The article contains a case study of a university unit in Poland in terms of threats related to network attacks. The article presents the actual data collected from the year 2021 to year 2023 on network threats that have been registered in the organization. These are actual data allowing observation of real threats to educational institutions in Poland.*

Keywords: *Case study, information security, network attacks, information security management.*

JEL Code: *M15, K24, L86.*
Paper type: *Case study.*

[1]*PhD., Department of Computer Science, Faculty of Management, University of Lodz, Poland, e-mail: grzegorz.podgorski@uni.lodz.pl;*

1. Introduction

Cybersecurity of universities in Poland is a key issue, especially in the face of the growing digitalization of educational processes and the increasing number of threats related to cybercrime. Modern universities are places of intensive exchange of information, storage of sensitive data and implementation of activities that expose them to various risks related to cyberattacks.

In the global context, from year to year, more frequent and more advanced attempts to attack educational institutions are observed, which become the target of both hackers and organized crime groups. The number of attacks on academic centers may result from several facts.

Firstly, from the belief that these centers are less secure than commercial organizations. Secondly, these centers contain huge amounts of sensitive electronic information: patents, research results, analyses, scientific papers, scientific dissertations, etc. In both cases, the possibility of data theft or infection of a large number of users using university resources means that such entities are still the target of attacks.

As statistics show, the number of cyberattacks in Poland is growing year by year. This situation is also reflected in the world, where this number is growing year by year. The number of incidents in individual years in Poland is presented in table number 1.

Table 1. *Number of security incidents by year.*

Year	Number of incidents
2023	80 267
2022	39 683
2021	29 483
2020	10 420
2019	6 484

Source: *CERT report 2023 (CERT, 2023).*

It is clear to see an increase of over 100% in such incidents in 2023 compared to 2022. The threat of cyberattacks directly translates into the costs caused by damage related to cybercrime. These costs in the case of 2024 were estimated at $9.5 trillion per year (Morgan, 2022).

The development of technology, but also the change that took place in the case of the Covid-19 virus pandemic, meant that universities had to adapt to the new reality. This reality is currently the remote work model for academic and administrative staff, but also the remote teaching model. These changes have led, among other things, to an even wider use of IT systems, which implies an even greater need to protect their resources from cyberattacks.

2. Literature Review

Due to the nature of the article and the research that concerned the case study, the main reliance was on all kinds of publications concerning aspects discussed in the analysis of data related to attacks and threats in the cyber-security environment. This limited the choice of sources to two main categories.

Firstly, to those that collected information about cyber-attacks in Poland and around the world and secondly, to those sources that described potentially important events related to the arena of cyber security activities in Poland and around the world. In this case, such literature allowed for verification of the increases in the number of attacks observed in the university unit under study to critical events related to the increased activity of criminal groups and the publication of information about found security gaps.

In this regard, one of the main sources of data on the security landscape of the Polish Internet were the annual reports of Poland CERT (Cert, 2021; 2022; 2023), which present data reported to Poland CERT in the context of threats, number of attacks, threats by category, as well as areas of activity of organizations that are attacked. This category of documents also included cybersecurity reports presented in Digital Poland (Cyfrowa Polska, 2021).

The second category were reports from the CSIRT Poland team (Computer Security Incident Response Team (CSIRT, 2021; 2022; 2023). In the case of vulnerability data, organizations that collect information on vulnerabilities were reviewed. These included: National Institute of Standards and Technology (NIST, 2024), Cyber Security and Infrastructure Security Agency (2024), OffSec (2024), MITRE (2024), CVEdetails (2024).

3. Research Methodology

The research method used in the presented article is a case study. In this study, the subject is a unit of a university employing over 340 people. Most employees are academics, the rest are broadly understood administration staff. This unit is a highly computerized unit within the university on which it is located. It has its own IT department, which is responsible for help desk, IT network management (wired and wireless), supervision of over ten IT laboratories and development and creation of dedicated IT solutions (systems) used by the unit.

The number of physical workstations in the unit is more than 600 machines, not including the server facilities. The number of students is around 4,000. The unit's ICT resources are located in the local ICT infrastructure as well as in cloud resources. The unit's resources consist of more than 20 servers located in an internal location as well as in cloud resources.

The development of the research methodology took place in several main phases. The first phase included the configuration of security devices so that they would collect interesting traffic. Data on cyber-attacks was collected by various devices and security services. In the same phase, mechanisms were configured to correlate occurring attacks with individual hosts and examine in real time the vulnerabilities of given devices to the occurring threat. In the next phase, this data was transferred to the appropriate database.

The data in the database was then subject to a verification process for its completeness. The last phase was the analysis of the data received. At this stage, the data from the database was analyzed and the results were compared with other data from Poland and from around the world. This analysis was needed for two purposes.

First, to determine whether in selected periods in which an increase in attacks was noted, a similar relationship occurred in Poland and around the world. In this way, it was possible to isolate, for example, beginning cybercriminal campaigns. In the second case, whether the activity of cybercriminals is not related to the detection of a specific vulnerability for a specific host/service or product.

Data were collected from January 1, 2021 to December 31, 2023. The author wanted to keep annual data so that the same periods could be compared. Data has been aggregated to show the actual number of attacks during a given period.

Further data analysis assumed the following elements:

- qualifying attacks – as significant from the point of view of host/service/device security or not.
- separation of the main classes and categories of attacks.
- defining the target of the attack – both in a very general way at the level of the host, device or service, as well as in a detailed way at the level of a specific port, system service, etc.
- determining the source of the attack – both in terms of the specific IP address and the country from which the attack originated.

In terms of attack classification, they were divided into those that were classified as significant and those that were not significant from the point of view of the security of the unit. Attacks classified as significant referred to attacks that targeted devices or services that were vulnerable to attack. Such high-impact events were identified by correlating attacks with target risk, which was determined by passive profiling of devices and their vulnerabilities in real time.

The next step in developing the results was to classify attacks into several categories. The main categories were identified based on the most common attack categories. In connection with this analysis, five main categories were identified, presented below:

- ✓ Web application attack;
- ✓ Network Trojan;
- ✓ Potentially bad traffic;
- ✓ Attempted administrator privilege gain;
- ✓ Attempted user privilege gain.

It was also analyzed whether the vector of attacks on infrastructure changes in individual years, or whether the level of individual types of qualified threats remain constant. The previous study conducted in 2020-2021 during the coronavirus pandemic clearly showed changes in the vector of attacks.

In addition to determining the IP address from which the attack originated, it was also determined, if possible, which country the attack came from. In the final step of the analysis, an attempt was also made to correlate the dates of attack activity with events in the cybersecurity arena.

4. Research Results and Discussion

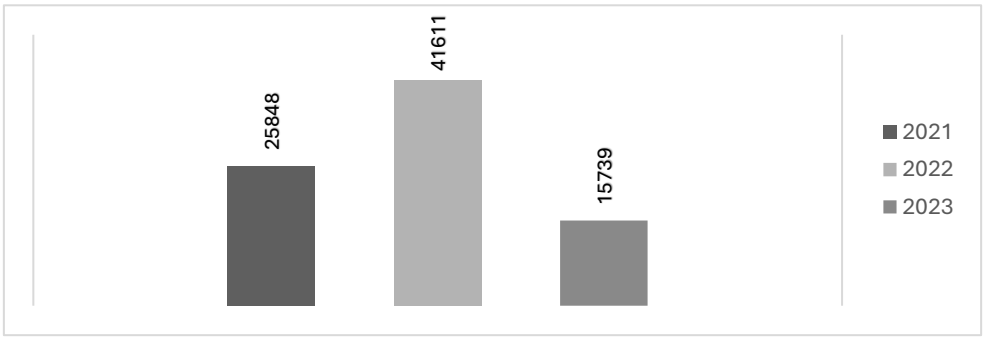
Data was collected from January 1, 2021, to December 31, 2023. Presenting data on an annual basis allows for observation changes in this area as well as comparing analogous periods. It also allows for observing trends and possible changes in the case of attack vectors. The number of attacks in individual years, i.e., 2021-2023, is presented in Figure 2.

In the case of attacks in 2021, only 118 of them could be marked as significant attacks. Of these, 10 were attacks strictly targeted at a specific device or service located in the infrastructure. As you can easily see, the percentage of irrelevant attacks reached 99.54%. This means that less than 1% were classified as significant attacks, targeted at a given university unit.

The data from 2022 is completely different, with 10 781 attacks classified as significant. They constitute 26% of all attacks that were directed at a given entity. These attacks were mainly directed at 17 devices/services. Such a large percentage is already a clear indicator that a given university entity and/or the service and/or device there has become the subject of interest of cybercriminals. For 2023, 3 885 attacks were recorded as significant. In this case, more than 75% of attacks were non-significant. The collected figures for significant and non-significant attacks are presented in Figure 3.

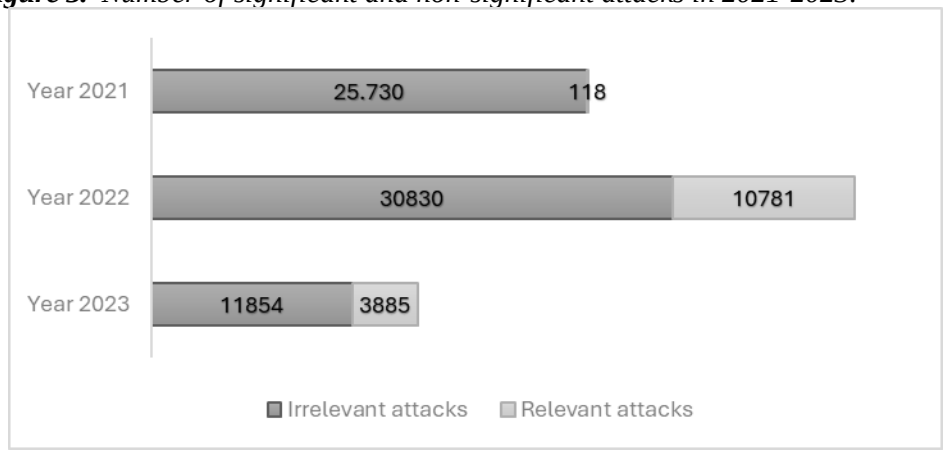
It is worth noting the drastic increase in significant attacks in 2022 compared to 2021. An increase from less than 1% to 26% was observed. We also analyzed whether there was any correlation between the months or days of the week when attacks occur years. Unfortunately, nothing of the sort could be observed. For example, figure number 4 shows the percentage value of attacks divided into given months in 2022.

Figure 2. *Number of attacks in 2021-2023.*



Source: *Author's calculations.*

Figure 3. *Number of significant and non-significant attacks in 2021-2023.*



Source: *Author's calculations.*

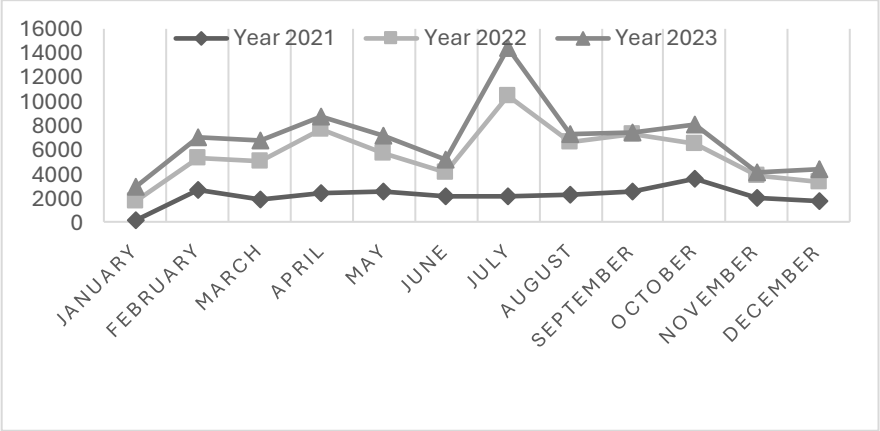
Figure 4. *Percentage of attacks in individual months of 2022.*

	Sprzedaż
January	3,72%
February	6,60%
March	7,61%
April	12,54%
May	7,59%
June	4,98%
July	19,78%
August	10,43%
September	11,60%

Source: *Author's calculations.*

Figure 5 presents data on attacks in individual months for the years 2021-2023.

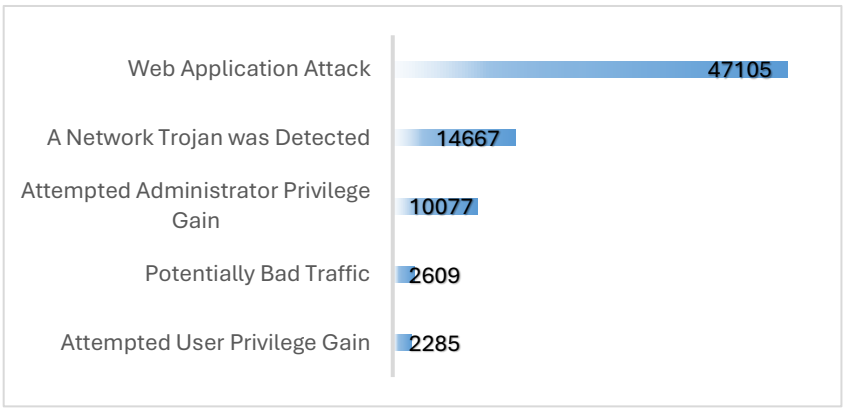
Figure 5. *The number of attacks is divided into years and individual months.*



Source: *Author's calculations.*

In many cases, it was possible to link increased activity on specific days or months with specific cybersecurity events that took place. For example, in the case of 2022, in July, increased attack activity was associated with the development of attack techniques of the UNC1151/Ghostwriter group (Cert, 2022). In the same month, another important vulnerability was CVE-2022-23131: Zabbix (CSIRT, 2022; CVEdetails, 2024). A similar pattern was observed in other years and months. When a significant vulnerability appeared in each product, device, or service, the number of attacks increased. The next analysis of the results obtained concerned the classification of attack categories. It was possible to distinguish four main categories. Data presenting the most important categories of threats is presented in Figure 6.

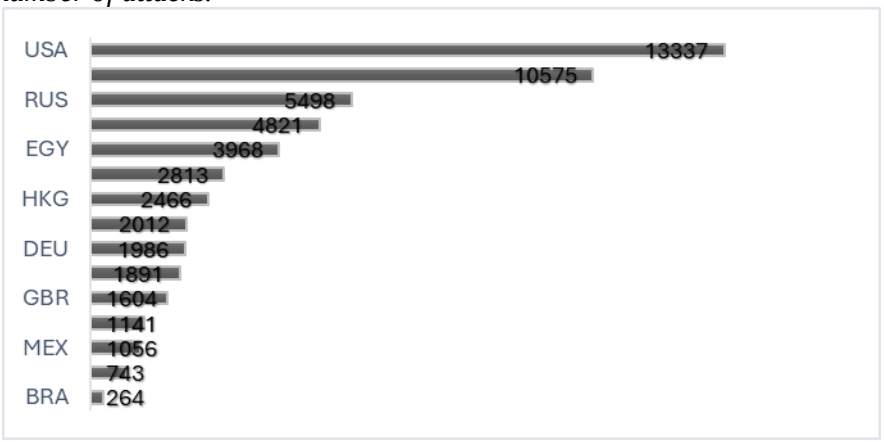
Figure 6. *Classification of attacks in specific years.*



Source: *Author's calculations.*

Another important aspect was to link the countries from which attacks on a given university unit are coming. This is particularly important for Poland, which is exposed to the effects of hybrid warfare by the Russian state, which is also manifested on the Internet. The sources of attacks for individual years are presented in Figure 7.

Figure 7. *Sources of attacks on the university unit in 2021-2023, divided by country and number of attacks.*



Source: *Author's calculations.*

As you can easily see, the country from which the university unit was most often attacked is the United States. This fact is confirmed in all kinds of reports on threats on the Internet (CERT 2021; 2022; 2023; CSIRT 2021; 2022; 2023). This is due to the detection of the largest number of C&C (Command and Control) servers in this country (CERT 2022). Russia was in third place. It should be remembered that this is a country that is actively participating in the hybrid war directed against Poland.

When it comes to the cumulative value of attacks by continent, the largest number of them comes from Europe, followed by Asia and North America – Figure 8.

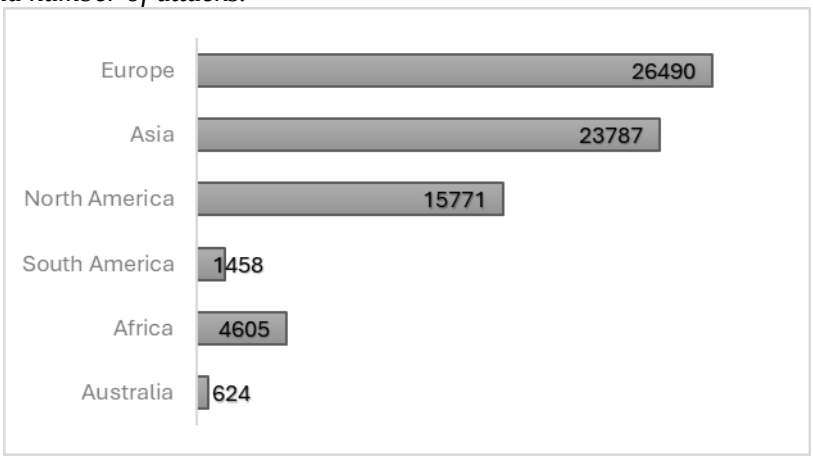
5. Conclusions, Proposals, Recommendations

The purpose of the article was to present the results of research related to network attacks on the university unit in the period from January 2021 to December 2023. The types of attacks and their nature were analyzed. Universities, such as public research and education centers are particularly vulnerable to all kinds of network attacks.

The analysis of network attacks on a university unit in the context of information security allows for tangible benefits, especially in terms of increasing the level of information security. It also allows defining the types of threats that such unit's face.

It also provides an opportunity to refine and better adapt existing security solutions or implement new ones.

Figure 8. *Sources of attacks on the university unit in 2021-2023, divided by continent and number of attacks.*



Source: *Author's calculations.*

As data analysis showed, one of the main attack vectors was the exploitation of vulnerabilities related to specific devices, services or products that are in the organization. As vulnerabilities were detected, the number of attacks carried out on the university unit increased.

The second very important aspect of the analysis results was the continued high level of attacks related to web applications. In all the analyzed periods in the annual settlement, this attack vector was in first place. The next attack vector, which was in second place in terms of the number of attacks carried out, were network Trojans. In third place in the category were noted attempts to obtain administrator privileges.

One of the limitations in confronting foreign studies is the lack of reference to threats related to phishing. However, due to the specificity of such a threat, which directly affects users, it was not possible to implement in the case of the data analyzed. Such a threat is mainly aimed at direct channels of contact with the user, e.g. e-mail or SMS messages.

Cybersecurity of universities in Poland is a major challenge, especially in the face of the dynamic development of digital technologies used by universities. The greater the degree of use of these technologies, the greater the number of threats related to cyberattacks. The increasing number of cyberattacks indicates the need to strengthen security and implement comprehensive data protection solutions.

Universities wishing to maintain an appropriate level of security of their resources

must face the need to integrate both technical solutions and focus on education and awareness among employees and students.

Monitoring changing threats and adapting to new cyberspace realities is becoming a priority element of security. In this aspect, the analysis of threats, attack vectors and sources allow for better protection of university resources. They allow for the identification of particularly vulnerable areas, as well as the indication of the main targets of cybercriminals.

The result of such an analysis is the definition of such places in the IT infrastructure that should be subject to special protection. In this aspect, the future of universities in the context of digital security depends on their ability to flexibly respond to threats and constant investment in modern data protection technologies. This will ensure the creation of a safe educational environment that will not only enable the implementation of scientific goals, but also ensure the protection of sensitive information.

References:

CERT Report 2021. Raport roczny z działalności CERT POLSKA 2021. https://cert.pl/uploads/docs/Raport_CP_2021.pdf.

CERT Report 2022. Raport roczny z działalności CERT POLSKA 2022. https://cert.pl/uploads/docs/Raport_CP_2022.pdf.

CERT Report 2023. Raport roczny z działalności CERT POLSKA 2023. https://cert.pl/uploads/docs/Raport_CP_2023.pdf.

CISA Vulnerabilities Catalog. https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

CSIRT, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku. https://www.csirt.gov.pl/download/3/204/RaportostaniebezpieczenstwacyberprzestrzeniRPw2021compressed.pdf.

CSIRT, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku. https://www.csirt.gov.pl/download/3/214/RaportostaniebezpieczenstwacyberprzestrzeniRPw2022.pdf.

CSIRT, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku. https://www.csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf.

CVEdetails, Vulnerabilities Data. https://www.cvedetails.com/.

Cyfrowa Polska, Cyberbezpieczeństwo w Polsce w 2021r.: cyberataki na urządzenia końcowe. https://cyfrowapolska.org/wp-content/uploads/2022/01/Cyfrowa_Polska-Raport_Cyberzagrozenia2021.pdf.

MITRE, MITRE ATT&CK. https://attack.mitre.org/.

Morgan, S. 2023. Cybercrime to cost the world 8 trillion annually in 2023 https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/.

OffSec Exploit Database. https://www.exploit-db.com/.

NIST, National Vulnerability Database. https://nvd.nist.gov/.