STUDIA NAD BEZPIECZEŃSTWEM

Nr 9 **s. 107–116** **2024**

ISSN 2543–7321
© Instytut Bezpieczeństwa i Socjologii,
Uniwersytet Pomorski w Słupsku
Przyjęto: 12.12.2024
Zaakceptowano: 12.12.2024

Oryginalna praca badawcza

DOI: 10.34858/SNB.9.2024.006

Tymoteusz Peta
Pomeranian University in Słupsk
e-mail: tymoteusz.peta@upsl.edu.pl
ORCID: 0000-0003-4454-4766

ANALYSIS OF THE CITY OF SŁUPSK'S READINESS FOR CYBERSECURITY THREATS – A CASE STUDY: HACKER ATTACK ON THE SHARED SERVICES CENTRE

ANALIZA GOTOWOŚCI MIASTA SŁUPSKA DO STAWIANIA CZOŁA ZAGROŻENIOM CYBERBEZPIECZEŃSTWA – STUDIUM PRZYPADKU: ATAK HAKERÓW NA CENTRUM USŁUG WSPÓLNYCH

Abstract: In August 2022, a breach occurred on the city servers belonging to the Centre for Shared Services, resulting in the encryption of data stored there, including the personal information of teachers from Słupsk County. The purpose of this article is to analyse the strengths and weaknesses of the city in relation to this situation, based on both official documents and communications, as well as the opinions of the affected individuals.

Zarys treści: W sierpniu 2022 roku doszło do włamania na miejskie serwery należące do Centrum Usług Wspólnych oraz do zaszyfrowania przechowywanych tam danych nauczycieli powiatu słupskiego. Celem niniejszego artykułu jest dokonanie analizy mocnych i słabych stron miasta w odniesieniu do wspomnianej sytuacji zarówno na podstawie oficjalnych dokumentów i komunikatów, jak również opinii środowiskowych pokrzywdzonych osób.

Keywords: cybersecurity, Słupsk, CUW, SWOT analysis, teachers.

Słowa kluczowe: cyberbezpieczeństwo, Słupsk, CUW, analiza SWOT, nauczyciele.

Introduction

The nature of the modern world, marked by a significant and rapid surge in technological advancement, has not only facilitated social development but also introduced new problems and challenges not solely related to social behaviours, attitudes, addictions or diseases. Cybersecurity has emerged as one of the most critical challenges of the contemporary era, where digital infrastructure plays a key role in the daily functioning of societies, economies and governments.

Cybersecurity encompasses all categories directly linked to the broader concept of security, applied specifically to telecommunication and information networks. It addresses issues related to information, communication and network architecture, including threats affecting these domains.[1] As reliance on technology grows and advanced solutions like artificial intelligence, the Internet of Things (IoT) and cloud computing become increasingly prevalent, the risks of cyberattacks also rise. Hackers and organised criminal groups continuously seek new ways to exploit vulnerabilities in systems, putting millions of people at risk of data breaches, service disruptions and significant financial losses. Alongside hate speech and online harassment, cybercrime ranks as one of the greatest challenges for Internet users.[2] Consequently, cybersecurity is not merely a technological concern but also a strategic priority for organizations and governments worldwide.

However, it is worth questioning whether institutions are genuinely prepared to prevent and combat cybercrime. This task is particularly challenging given the rapid evolution of hacking tools and phishing techniques, necessitating constant updates to security measures. This paper aims to examine the case of a hacker attack targeting data belonging to the Shared Services Centre (referred to as CUW), which operates under the Municipal Office of Słupsk, with the goal of conducting a SWOT analysis of the city's services in the context of cybersecurity threats.

---

[1] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, "Cybersecurity and Law" 2019, vol. 2, p. 13.

[2] T. Peta, *Przejawy agresji i mowy nienawiści w Internecie – analiza komentarzy na wybranych stronach portali informacyjnych*, "Social Studies: Theory and Practice" 2021, vol. 1, p. 118.

Attack on data – year 2022

The Shared Services Centre (CUW) in Słupsk provides financial and HR services to educational institutions in the city. It also manages student scholarships and debt collection. As a result, it holds sensitive data for approximately 1,200 teachers and additional individuals employed under various agreements, such as contracts for services. Altogether, it is estimated that the CUW stores information on around 1,500 individuals.[3] On 26 August 2022, news broke of a cyberattack on the server of Słupsk's Shared Services Centre. According to the City Hall, no data leakage occurred during the incident; instead, the data was encrypted. The perpetrators demanded a ransom in Bitcoin worth tens of thousands of euros in exchange for decryption. The city refused to pay, citing past incidents where such agreements were not honoured.[4] Teachers were promptly informed of the breach and advised on the possibility of replacing their identification documents or purchasing a paid notification service to alert them if their PESEL number was used for credit fraud. It was also emphasized that the incident would not disrupt salary payments, as the encrypted data was also available in physical, paper form within the CUW's premises. Following consultations with CERT Polska, an organization specialising in responding to cybersecurity incidents, it was determined that the group responsible for the attack had no prior record of stealing data outright. An analysis of data transmission and bandwidth confirmed that no significant data extraction occurred during this attack. The infected server was immediately disconnected from the network. Additionally, rumours of student data being compromised were refuted, as such information is not included in the CUW's databases.[5]

---

[3] P. Woś, *Pracownicy oświaty w Słupsku dostaną wypłaty na czas. CUW odzyskuje dane po ataku hakerskim*, Radio Gdańsk, https://radiogdansk.pl/wiadomosci/region/slupsk/2022/08/26/pracownicy-oswiaty-w-slupsku-dostana-wyplaty-na-czas-cuw-odzyskuje-dane-po-ataku-hakerskim/, (accessed 24.11.2024).

[4] G. Hilarecki, *Atak hakerski na bazę z danymi nauczycieli w Słupsku. Żądają od miasta okupu w bitcoinach*, GP24.pl, https://gp24.pl/atak-hakerski-na-baze-z-danymi-nauczycieli-w-slupsku-zadaja-od-miasta-okupu-w-bitcoinach/ar/c1-16797833, (accessed 24.11.2024).

[5] P. Woś, *Hakerzy nie wykradli danych z CUW w Słupsku. Plików wciąż nie udało się jednak odblokować*, Radio Gdańsk, https://radiogdansk.pl/wiadomosci/region/slupsk/2022/08/31/hakerzy-nie-wykradli-danych-z-cuw-w-slupsku-plikow-wciaz-nie-udalo-sie-jednak-odblokowac/, (accessed 27.11.2024).

In the aftermath, a spokesperson for the Słupsk City Hall initiated an audit of the municipal IT systems to identify any vulnerabilities that might have facilitated the attack. The review confirmed that passwords had not been changed recently, but the security measures, including firewalls, antivirus programs and the IT team's oversight, were deemed adequate. No breaches in protocol were identified.[6]

The police were also notified of the incident and an official report was filed regarding unauthorized access to one of the City Hall's servers. The investigation proceeded under Article 268a of the Polish Penal Code:

"**Article 268a. [Destruction of IT Data]**

§1. Whoever, without authorization, destroys, damages, deletes, alters, or hinders access to IT data, or significantly disrupts or prevents the automated processing, collection, or transmission of such data, shall be subject to imprisonment for up to 3 years.

§2. Whoever commits the act described in §1, causing significant financial harm, shall be subject to imprisonment from 3 months to 5 years.

§3. Prosecution of offences under §1 or §2 is initiated upon the victim's request."[7]

As of now, no information about the apprehension of the perpetrators has been reported.

Encryption of CUW data – perspectives of affected teachers

For the purpose of this article, interviews were conducted with two teachers from educational institutions in Słupsk, including schools and preschools, to present the situation from the perspective of those directly affected by the incident. The interviewees were asked to describe the actions undertaken by the City Hall, other institutions and themselves to prevent and safeguard against data theft, both personally and within their professional communities of fellow teachers.

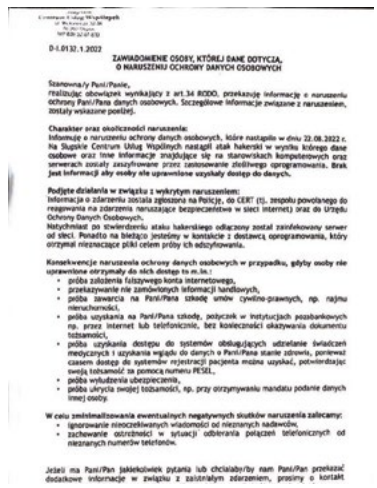
Respondent 1 stated that she did not take any additional measures to protect her personal data. Despite concerns among her preschool department

[6] K. Pyszkowska, *Atak hakerski na słupski magistrat i prywatne firmy*, Zawsze Pomorze, https://www.zawszepomorze.pl/artykul/4734,atak-hakerski-na-slupski-magistrat-i-prywatne-firmy, (accessed 27.11.2024).

[7] Penal Code Act of 6 June 1997, Dz.U. (Journal of Laws) 2025, item 383.

colleagues, she placed her trust in the city's assurances that the stored data was secure and that their financial well-being was not at risk. However, she emphasised that the first few days following the disclosure of the attack were the most stressful. The respondent noted that teachers were the first to be informed of the incident, receiving notification via letter. A copy of the notification is presented below:

Figure 1. Notification of a Personal Data Protection Breach, sent in August 2022 by CUW to teachers



D-I.0132.1.2022

ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowna/y Pani/Panie,

realizując obowiązek wynikający z art.34 RODO, przekazuję informację o naruszeniu ochrony Pani/Pana danych osobowych. Szczegółowe informacje związane z naruszeniem, zostały wskazane poniżej.

Charakter oraz okoliczności naruszenia:
Informuje o naruszeniu ochrony danych osobowych, które nastąpiło w dniu 22.08.2022 r. Na Słupskie Centrum Usług Wspólnych nastąpił atak hakerski w wyniku którego dane osobowe oraz inne informacje znajdujące się na stanowiskach komputerowych oraz serwerach zostały zaszyfrowane przez zainstalowanie złośliwego oprogramowania. Brak jest informacji aby osoby nie uprawnione uzyskały dostęp do danych.

Podjęte działania w związku z wykrytym naruszeniem:
Informacja o zdarzeniu została zgłoszona na Policję, do CERT (tj. zespołu powołanego do reagowania na zdarzenia naruszające bezpieczeństwo w sieci internet) oraz do Urzędu Ochrony Danych Osobowych.
Natychmiast po stwierdzeniu ataku hakerskiego odłączony został zainfekowany serwer od sieci. Ponadto na bieżąco jesteśmy w kontakcie z dostawcą oprogramowania, który otrzymał niezwłocznie pliki celem próby ich odszyfrowania.

Konsekwencje naruszenia ochrony danych osobowych w przypadku, gdyby osoby nie uprawnione otrzymały do nich dostęp to m.in.:
- próba założenia fałszywego konta internetowego,
- przekazywanie nie zamówionych informacji handlowych,
- próba zawarcia na Pani/Pana szkodę umów cywilno-prawnych, np. najmu nieruchomości,
- próba uzyskania na Pani/Pana szkodę, pożyczek w instytucjach pozabankowych np. przez internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości,
- próba uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskania wglądu do danych o Pani/Pana stanie zdrowia, ponieważ czasem dostęp do systemów rejestracji pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL,
- próba wyłudzenia ubezpieczenia,
- próba ukrycia swojej tożsamości, np. przy otrzymywaniu mandatu podanie danych innej osoby.

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy:
- ignorowanie nieoczekiwanych wiadomości od nieznanych nadawców,
- zachowanie ostrożności w sytuacji odbierania połączeń telefonicznych od nieznanych numerów telefonów.

Jeżeli ma Pani/Pan jakiekolwiek pytania lub chciałaby/by nam Pani/Pan przekazać dodatkowe informacje w związku z zaistniałym zdarzeniem, prosimy o kontakt

Source: the private archive of respondent.

The respondent noted that aside from exercising additional caution when handling messages or phone calls from unknown senders, the CUW did not suggest taking any specific steps, such as replacing identification documents or subscribing to BIK (Credit Information Bureau) notifications. These notifications alert individuals if their data is used to apply for loans or credit or sign contracts.[8] Actions of this nature were initiated independently by teachers and their acquaintances. When asked to evaluate the city's response, the respondent expressed no criticism, considering the measures taken to be sufficient.

In contrast, the second respondent displayed significantly less composure. She admitted that nearly her entire teaching team, after receiving the letters from the CUW, experienced a mild panic. Many decided to replace their identification documents and monitor their credit information. Additionally, some

[8] *Alerty BIK 24/7*, BIK, https://www.bik.pl/klienci-indywidualni/alerty-bik, (accessed 27.11.2024).

individuals filed separate reports of the crime at the local police station alongside the City Hall's notification. Although these reports were supported by the opinion of an IT forensic expert from the District Court in Słupsk, the case was eventually dismissed. It is noteworthy that the suggestion to subscribe to BIK services or secure personal ID documents originated directly from the school's administration. Despite assurances that there was no immediate threat of data leakage, the administration sought to protect its employees. The respondent recalled that the first few weeks following the incident were stressful for most of her colleagues. Many worried about their financial security, anxiously seeking updates on the apprehension of the perpetrators or fearing that loans might be fraudulently taken out in their names. Even as time passed, the respondent remained critical, believing that the City Hall could have done more to protect and prevent such incidents.

These responses highlight differences in crisis reactions; some individuals displayed greater initiative, while others placed more trust in the city authorities. However, it is clear that the perceived level of threat among most teachers was similar. The data breach was a highly stressful event, raising concerns about personal safety, financial security and data protection.

New personal data protection policy

On 31 October 2024, Directive No. 18/2024 of the Director of the Shared Services Centre of the Słupsk County came into effect, introducing the Personal Data Protection Policy. Chapter II of the document states that its purpose is to safeguard personal data processed by the CUW, establish rules for their storage and codify principles and standards for their management.

The directive outlines several key elements of the data protection system. Notable preventative measures include:

- conducting risk analyses to assess potential violations of the rights and freedoms of individuals whose data is processed,
- maintaining a registry of individuals authorized to process personal data,
- ensuring that personal data processing occurs in conditions that prevent access by unauthorized persons,
- keeping a data processing register,
- enhancing protection for both digital and non-digital data,

- appointing a Data Protection Officer (DPO) to oversee and monitor the personal data processing process,
- implementing a contractor evaluation procedure in cases where data must be processed by third parties.[9]

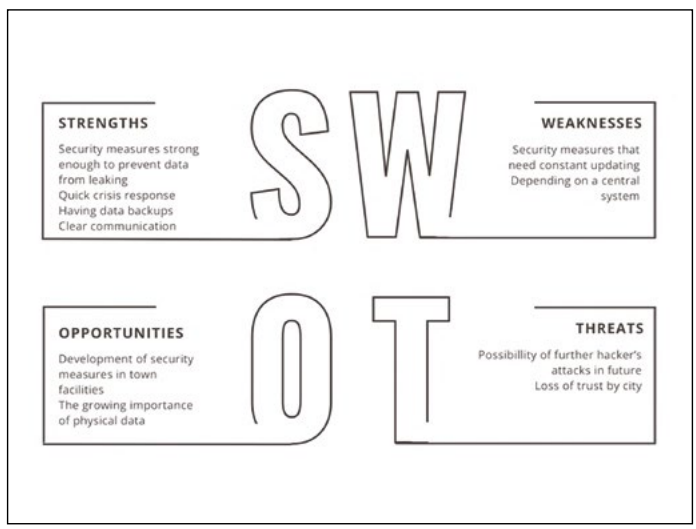
These measures aim to enhance the cybersecurity of entities operating under the Słupsk City Hall.

SWOT analysis

SWOT analysis is a method of organising information that facilitates drawing conclusions for the strategic evaluation of entities. It considers both tangible and intangible factors, as well as internal and external aspects.[10]

Taking into account all the information presented above, a SWOT analysis form was created to identify strengths, weaknesses, opportunities and threats. This is outlined below.

Figure 2. SWOT Analysis Sheet of the Shared Services Centre of the Słupsk County



Source: own study.

[9] Zarządzenie nr 18/2024 Dyrektora Centrum Usług Wspólnych powiatu słupskiego, https://bip.cuw.powiat.slupsk.pl/pliki/powiatslupski-cuw/zalaczniki/193/polityka-ochrony-danych-osobowych-2024-sig.pdf, (accessed 3.12.2024).

[10] Ł. Szałata, J. Zwoździak, *Analiza SWOT jako podstawowe narzędzie w zarządzaniu środowiskiem*, "Rocznik Ochrona Środowiska" 2011, vol. 13, pp. 1105–1106.

Analysing the actions of the CUW in relation to the cyberattack of 2022, both positive and negative aspects can be identified. First and foremost, a strong point of the institution is the security measures that were sufficiently advanced to only allow encryption of the data, without any leakage. Additionally, thanks to a quick response, the infected system was almost immediately disconnected upon detecting the breach. The facility was able to continue its operations due to physical backup copies of data, which also constitutes a strength. Finally, it is worth appreciating the direct communication from the city regarding the issues – every person affected by the crisis was informed about the situation. The media were also kept up to date with the ongoing actions, without any attempts to conceal information. This demonstrates the confidence of the authorities.

In terms of weaknesses, it is important to mention aspects resulting from the nature of technological devices and the Internet. The constant development of technology and the emergence of new solutions means that the security systems used in the institutions must be constantly updated to keep pace with new methods of breaching them. Furthermore, the situation revealed problems related to the use of a centralised system – a failure of the central unit causes paralysis in all dependent entities. These are, however, aspects that can be improved on or eliminated.

There are also opportunities arising from the resolved situation. The crisis, among other things, led to the development of security measures used by the City Hall, as well as the updating of data processing procedures aimed at improving security and further preventing potential leaks. The new conditions include both digital and physical data storage and access control measures – the most important changes were outlined in the previous subsection. The second category, in particular, is encouraging – physical data remains crucial, despite the ongoing digitisation process; the crisis only reinforced this conviction. Of course, this does not mean that digitisation should be abandoned. It is a completely natural process associated with the inevitable technological progress. However, especially at the administrative level, security measures should be maintained at an appropriately high level. The current crisis should serve as a reason for improvements in this area; this could include the use of modern encryption methods such as AES or DES. An increasingly common solution is also the creation of VPNs, virtual private networks that provide secure, private environments for individuals and corporations. Finally, artificial intelligence can also be used to enhance the security of stored data.

However, the fact remains that threats continue to exist. Of course, the servers of the institutions belonging to the city are still exposed to future attacks as such risks cannot be fully eliminated, as they are constant threat. The situation also contributed to a partial loss of trust in the city's institutions, but this is a natural consequence that the City Hall had little control over. A crisis occurred, a response was initiated, and it was resolved, however, certain concerns and questioning of the effectiveness of the security measures and actions of the institutions remain. Now, it is up to the city to overcome the mentioned threats.

Conclusions

Considering all the above findings, an overall summary of the city of Słupsk's readiness for cybersecurity threats can be made. The city seems to be prepared to counteract cybercriminal attacks, characterised by a quick response time, clear communication with institutions, the media and affected individuals, as well as updated methods for preventing such crises. Achieving 100% security is impossible, so regardless of public sentiment, the readiness should be assessed positively. The strengths outweigh the weaknesses and there are more opportunities than direct threats. However, it should be remembered that cybersecurity involves ongoing efforts to improve security measures and thus, with proper attention dedicated to this issue, the city is capable of preventing future attacks.

The 2022 situation served as a valuable lesson for the City Hall, and it would be good if this lesson was well-learned. For this to happen, the development of infrastructure should progress in both the physical and digital management areas. In the physical domain, efforts should focus on minimising human errors through proper training and preparing employees for data management, as well as ensuring the appropriate preparation and storage of physical data backups. In the digital domain, it would be highly advisable to use modern solutions that can enhance the security of city administration, such as advanced encryption, AI and VPNs.

Bibliography

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, "Cybersecurity and Law" 2019, vol. 2.

Peta T., *Przejawy agresji i mowy nienawiści w Internecie – analiza komentarzy na wybranych stronach portali informacyjnych*, "Social Studies: Theory and Practice" 2021, vol. 1.

Szałata Ł., Zwoździak J., *Analiza SWOT jako podstawowe narzędzie w zarządzaniu środowiskiem*, "Rocznik Ochrona Środowiska" 2011, vol. 13.

Alerty BIK 24/7, BIK, https://www.bik.pl/klienci-indywidualni/alerty-bik, (accessed 27.11.2024).

Hilarecki G., *Atak hakerski na bazę z danymi nauczycieli w Słupsku. Żądają od miasta okupu w bitcoinach*, GP24.pl, https://gp24.pl/atak-hakerski-na-baze-z-danymi-nauczycieli-w-slupsku-zadaja-od-miasta-okupu-w-bitcoinach/ar/c1-16797833, (accessed 24.11.2024).

Pyszkowska K., *Atak hakerski na słupski magistrat i prywatne firmy*, Zawsze Pomorze, https://www.zawszepomorze.pl/artykul/4734,atak-hakerski-na-slupski-magistrat-i-prywatne-firmy, (accessed 27.11.2024).

Woś P., *Hakerzy nie wykradli danych z CUW w Słupsku. Plików wciąż nie udało się jednak odblokować*, Radio Gdańsk, https://radiogdansk.pl/wiadomosci/region/slupsk/2022/08/31/hakerzy-nie-wykradli-danych-z-cuw-w-slupsku-plikow-wciaz-nie-udalo-sie-jednak-odblokowac/, (accessed 27.11.2024)

Woś P., *Pracownicy oświaty w Słupsku dostaną wypłaty na czas. CUW odzyskuje dane po ataku hakerskim*, Radio Gdańsk, https://radiogdansk.pl/wiadomosci/region/slupsk/2022/08/26/pracownicy-oswiaty-w-slupsku-dostana-wyplaty-na-czas-cuw-odzyskuje-dane-po-ataku-hakerskim/, (accessed 24.11.2024).

Zarządzenie nr 18/2024 Dyrektora Centrum Usług Wspólnych powiatu słupskiego, https://bip.cuw.powiat.slupsk.pl/pliki/powiatslupski-cuw/zalaczniki/193/polityka-ochrony-danych-osobowych-2024-sig.pdf, (accessed 3.12.2024).

Penal Code Act of 6 June 1997, Dz.U. (Journal of Laws) 2025, item 383.

Summary

In recent years, particularly during the cyberattack on Słupsk's Shared Services Centre, the city faced a significant test of its preparedness to counter cybercrime. Clear communication, a swift response and the modernisation of existing security protocols have led to an overall positive assessment of these efforts. However, it remains true that the opinions of those directly affected by the attack vary and, given their emotional nature, are often critical of the City Hall. Regardless of these evaluations, the dual approach to data storage, both electronic and physical, deserves recognition.