The Status and Management of Web-Related Security at Higher Education Institutions in Poland

Jackson Barreto[1][a], Paulina Rutecka[2][b], Karina Cicha[3][c] and Pedro Pinto[1,4][d]

[1] *ADiT-LAB, Instituto Politécnico de Viana do Castelo, Viana do Castelo, Portugal*
[2] *Department of Informatics, University of Economics in Katowice, Katowice, Poland*
[3] *Department of Communication Design and Analysis, University of Economics in Katowice, Katowice, Poland*
[4] *INESC TEC, Porto, Portugal*

Keywords: Cybersecurity, DNSSEC, Higher Education Institutions (HEIs), HTTPS, SSL/TLS, Security Headers, Website Security.

Abstract: In an era marked by escalating cyber threats, the need for robust cybersecurity measures is paramount, especially for Higher Education Institutions (HEIs). As custodians of sensitive information, HEIs must ensure secure channels for data transmission to protect their stakeholders. These institutions should increase their cyber resilience, recognizing the heightened risk they face from cybercriminal activities. A breach in an HEI's cybersecurity can have severe consequences, ranging from data confidentiality breaches to operational disruptions and damage to institutional reputation. This paper conducts a comprehensive evaluation of the cybersecurity mechanisms in HEIs within Poland. The focus is on assessing the adoption of important web security protocols—Hyper Text Transfer Protocol Secure (HTTPS) and Domain Name System Security Extensions (DNSSEC)—and the implementation of security headers on HEI websites. This study aims to provide a snapshot of the current cyber defense maturity in HEIs and to offer actionable insights for enhancing web security practices. The findings indicate a high adoption rate of HTTPS among HEIs, yet reveal significant gaps in web security practices. Also, there is a low adherence to security headers and an absence regarding DNSSEC implementation across the surveyed institutions. These results highlight crucial areas for improvement and underscore the need for HEIs in Poland to strengthen their web security measures, safeguarding their data and enhancing the overall cybersecurity resilience.

1 INTRODUCTION

In today's digital landscape, the increased reliance on Internet-based services has led to a heightened risk of cyber threats globally, a concern acutely felt in the education sector. Higher Education Institutions (HEIs) have become prominent targets, with a surge in cyberattacks highlighting their vulnerability to these evolving threats (Emsisoft Malware Lab, 2020; Emsisoft Malware Lab, 2021). This alarming trend is a global phenomenon also evident in Poland, where higher education institutions have seen a significant rise in cyber incidents (TCP World, 2021; Science in Poland, 2021; University World News, 2023). Such developments underscore the urgent need for enhanced cybersecurity measures in the academic arena.

HEIs serve as custodians of sensitive personal and confidential data and are integral to providing critical educational and research services. Cybersecurity breaches in these institutions can lead to severe privacy violations, disrupt operational capabilities, and tarnish their prestigious reputation, resulting in long-lasting damage. With the increasing sophistication and regularity of cyberattacks, it is imperative for HEIs to continually reevaluate and enhance their cybersecurity measures.

This study conducts a focused evaluation of web-related security in HEIs in Poland, aiming to capture a current snapshot of their cybersecurity status. Specifically, it examines the adoption of Hyper Text Transfer Protocol Secure (HTTPS) and Domain Name System Security Extensions (DNSSEC), along with security header implementations in HEIs web portals. The objectives are twofold: firstly, to establish a base-

[a] https://orcid.org/0000-0002-4064-8587
[b] https://orcid.org/0000-0002-1609-9768
[c] https://orcid.org/0000-0003-4575-6381
[d] https://orcid.org/0000-0003-1856-6101

Barreto, J., Rutecka, P., Cicha, K. and Pinto, P.
The Status and Management of Web-Related Security at Higher Education Institutions in Poland.
DOI: 10.5220/0012423000003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 789-798
ISBN: 978-989-758-683-5; ISSN: 2184-4356

line for the current state of web security in HEIs, essential for measuring future improvements; and secondly, to identify key areas where these institutions can strengthen their defenses against an evolving cyber threat landscape.

The subsequent sections of this manuscript are delineated as follows: Section 2 presents an overview of the related work. Section 3 details the research approach adopted. Section 4 reveals the empirical findings. Section 5 discusses the results and the limitations of this analysis. Section 6 presents the conclusions.

2 RELATED WORKS

Hyper Text Transfer Protocol (HTTP) is pivotal in server-client interactions, however, it initially lacked security features, making it susceptible to cyber threats (Berners-Lee, 1991). Vulnerabilities are particularly evident in early versions such as HTTP/1.0 and HTTP/1.1 (Rescorla, 2000). Scholarly research has focused on improving HTTP's security and efficiency. (Aakanksha et al., 2019) analyzed the performance and security of various web protocols, including HTTP 1.1, HTTPS, and HTTP 2.0. Grenfeldt et al. identified vulnerabilities in HTTP request handling, revealing potential security risks (Grenfeldt et al., 2021). Akiyama et al. examined malicious Uniform Resource Locator (URL) redirection, emphasizing the importance of transitioning from HTTP to HTTPS in HEIs (Akiyama et al., 2017).

In the realm of HTTPS communications, Rivest–Shamir–Adleman (RSA) and Elliptic-Curve Cryptography (ECC) are crucial for secure data exchange.RSA relies on the complexity of large number factorization (Randall et al., 2010), while ECC uses elliptic curves for enhanced security (Nir et al., 2018). Comparative studies highlight ECC's superiority in terms of efficiency and security over RSA. Mahto et al. demonstrated ECC's faster encryption and decryption capabilities(Mahto and Kumar Yadav, 2017). Gobi et al. further affirmed ECC's advantages in execution speed and reliability (Gobi et al., 2015).

Security headers, beyond the protection offered by HTTPS, safeguard web platforms from vulnerabilities such as Man-in-the-Middle (MitM) and the Logjam attack (Adrian et al., 2018). This research evaluates security headers grounded in the Open WorldWide Application Security Project (OWASP) compilation, encompassing, among others, Strict-Transport-Security, X-Frame-Options, X-Content-Type-Options, and Content-Security-Policy. Research reveals an increasing, yet incomplete, adoption of security headers. Buchanan et al. noted a growing trend in their integration (Buchanan et al., 2018). Lavrenovs et al. found that HTTPS sites are more likely to adopt security headers compared to HTTP-only sites (Lavrenovs and Melon, 2018).

The Domain Name System (DNS), fundamental to the Internet, translates domain names into machine-readable Internet Protocol (IP) addresses, crucial for accessing online services, including those of HEIs. However, DNS's vulnerability to attacks such as cache tampering and string manipulation endangers web service integrity and availability (Man et al., 2021; Jeitner and Shulman, 2021). To counter these threats, DNSSEC enhances DNS by digitally authenticating DNS responses, thereby ensuring their authenticity and bolstering web security (Visoottiviseth and Poonsiri, 2019). Despite its importance, the adoption of DNSSEC at the sub-domain level, including within HEIs, is inconsistent. This gap is attributed to technical knowledge barriers, insufficient support from local resolvers, and server misconfigurations, as observed in various studies (Chung et al., 2017; Lian et al., 2013; Osterweil et al., 2008; Hao Yang et al., 2011).

The strategic deployment and adoption of HTTPS, DNSSEC, and security headers are paramount for shielding Internet-accessible devices and services from cyber threats. However, the uptake of these protective measures is not as universal as required, primarily within HEIs. For instance, research from Brazil unveiled that a mere 2% of HEIs had integrated DNSSEC, and around 15% lacked any Secure Sockets Layer (SSL)/Transport Layer Security (TLS) certification (Barreto et al., 2023). A parallel study in Portugal emphasized the sporadic adoption of DNSSEC and HTTPS services among HEIs, notwithstanding the presence of established security guidelines and best practices (Felgueiras and Pinto, 2022) .

3 METHODOLOGY

This study adopts a quantitative and exploratory approach to aid in enhancing web security in HEIs and establish a cybersecurity benchmark (Silveira and Gerhardt, 2009). Data was collected on November 24, 2022, from 131 public and 216 private HEIs in Poland, and analyzed on September 1, 2023. Public HEIs data came from the Ministry of Education and Science of Poland (Poland, 2022a), while private HEIs data was sourced from the RAD-on system (Poland, 2022b). The English names of HEIs, when not officially available, were suggested using GPT-3.5 and marked distinctly. The analysis focused on DNSSEC, HTTPS implementation, and security headers in the HEIs' websites. This dataset, publicly available (Junior et al., 2023), and aligns with open science principles (Bezjak et al., 2018), constitutes a comprehensive compilation of data from both public and private Higher Education Institutions and includes detailed analysis results of DNSSEC, HTTPS, and security headers implementation on their websites.

4 RESULTS

This section presents the results for the security mechanisms configuration of HEIs in Poland, namely DNSSEC, HTTPS, SSL/TLS key lengths, security headers, and cryptographic algorithms. The results are presented by regions and by their category regarding if they are public or private institutions.

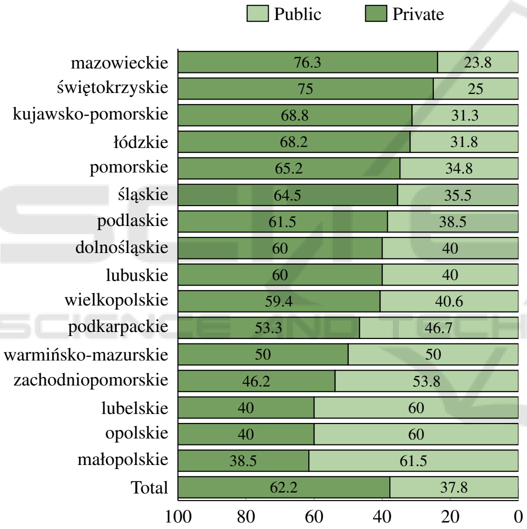

Figure 1: Distribution of Public and Private HEIs by region (%).

Figure 1 shows that public HEIs are more prevalent in regions such as Małopolskie, Opolskie, and Lubelskie, while private ones dominate in mazowieckie, świętokrzyskie, and kujawsko-pomorskie.

4.1 HTTPS

This section presents the results of HTTPS adoption by HEIs and identifies challenges in its deployment.

Fig. 2 illustrates HTTP/HTTPS usage by HEIs in Poland, categorized by the following statuses:

- Invalid: The institution's web portal is non-functional.
- HTTP only: The institution's platform operates solely on HTTP.
- HTTP & HTTPS: The institution supports both protocols but lacks redirection to mandate the use of HTTPS. All entities in this category possess a valid certificate.
- HTTP to HTTPS (other): The institution's platform redirects users to a secure domain outside its primary domain. All entities in this category possess a valid certificate.
- HTTP to HTTPS (same): The institution's platform redirects users to a secure domain within its primary domain, ensuring data protection. All entities in this category possess a valid certificate.
- HTTPS only: The institution's platform operates solely on HTTPS.

The results show that a small percentage (2.3%) of public HEIs do not use HTTPS. However, most have implemented mandatory redirects for secure browsing: 71.8% of public entities redirect within their domain, and 1.5% to external domains. For private entities, 83.8% have internal redirects. Only 1.5% of public entities use exclusively HTTPS, while no private entities do so.

A notable issue is the 12.7% of institutions that support both HTTP and HTTPS without enforcing mandatory redirection, posing a security risk.

Figure 3 showcases the territorial distribution of valid SSL/TLS configurations across HEIs in Poland. The data suggests that 83.2% of public HEIs and 90.7% of private HEIs have correctly configured SSL/TLS protocols.

Effective HTTPS implementation and ongoing management are vital for data security and privacy. (Grenfeldt et al., 2021) study reveals that HTTP Request Smuggling (HSR) threats emerge when servers and proxies interpret HTTP requests inconsistently. These HSR vulnerabilities can lead to cache poisoning, compromising data integrity, and bypassing security controls, allowing unauthorized access to sensitive data such as cookies and form inputs. This issue is especially critical for institutions with suboptimal HTTP and HTTPS setups, where protocol manipulation by attackers could breach data confidentiality and integrity.

In conclusion, while HTTPS adoption is high, it is crucial for HEIs to diligently implement and maintain HTTPS protocols for secure data exchange. Simply having HTTPS is not enough; vulnerabilities in SSL configurations can still pose significant risks to these institutions.

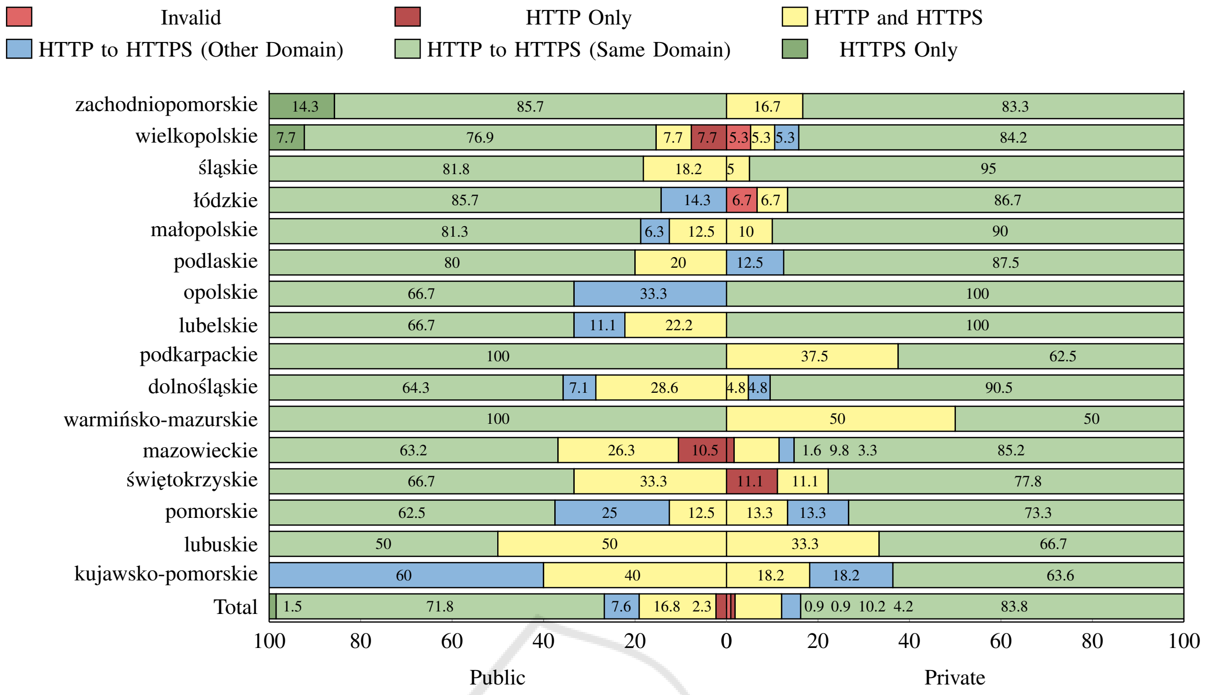

Figure 2: Territorial distribution of HTTPS usage (%).

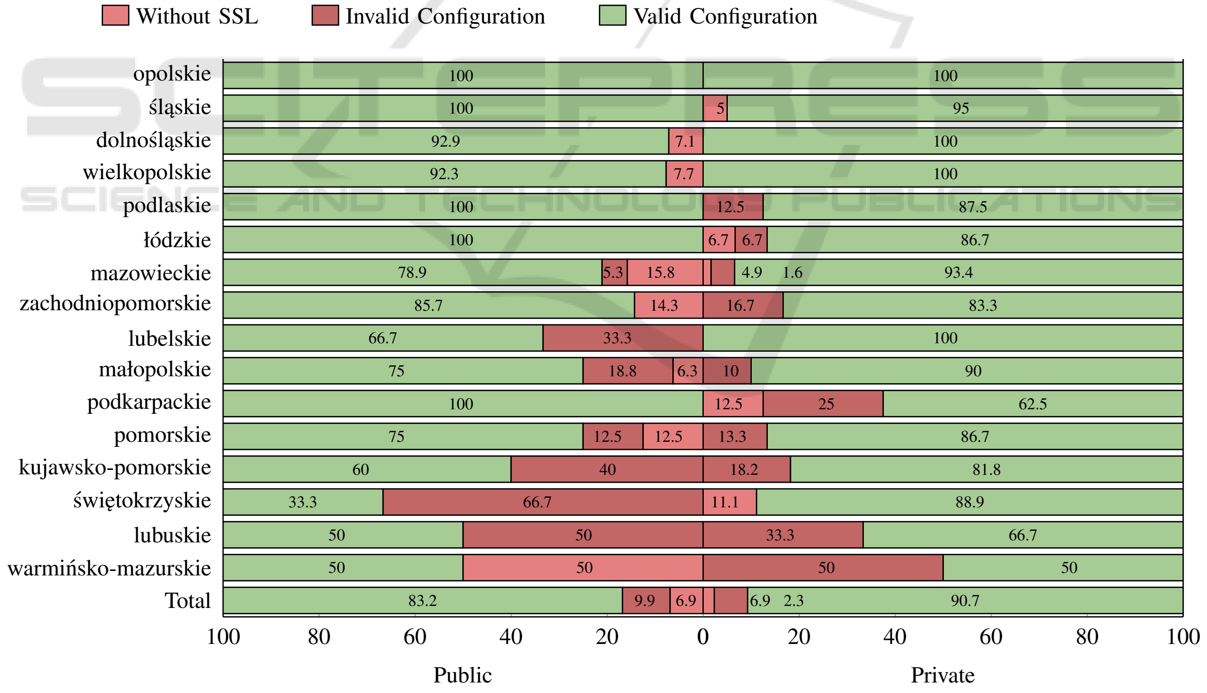

Figure 3: Territorial distribution of valid SSL/TLS configurations (%).

4.1.1 SSL/TLS Cryptographic Protocols

The study of cryptographic protocols within SSL/TLS across HEIs reveals a distinct preference for RSA encryption, as shown in Fig. 4. Specifically, RSA is employed by 90.1% of public and 81.9% of private entities.

The choice of a cryptographic protocol significantly influences the security, integrity, and efficiency of data transmissions. While RSA is renowned for its robustness, studies indicate that ECC offers comparable security with smaller keys and better compu-

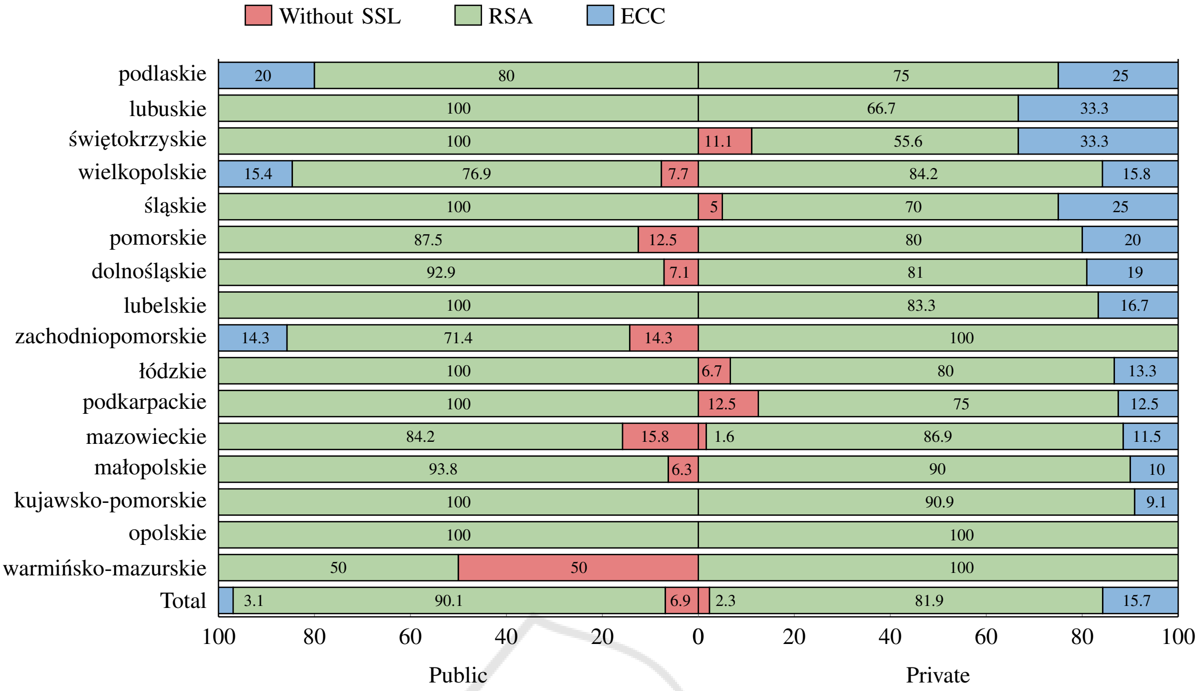

Figure 4: Distribution (in %) of the type of SSL/TLS algorithms used in the HEIs (%).

tational efficiency (Mahto and Kumar Yadav, 2017). This suggests that switching from RSA to ECC for HEIs could result in additional benefits.

4.1.2 SSL/TLS Key Lengths

To comprehend the security landscape within academic institutions, delving into the distribution of key lengths associated with SSL/TLS digital certificates adopted by these entities is pivotal.

Fig. 5 provides an exhaustive depiction of the key lengths associated with SSL/TLS digital certificates across HEIs in Poland. The observed trend in Poland HEIs shows a prevalence for the RSA algorithm, aligning with the minimum key dimension recommended of 2048 bits in (Barker and Roginsky, 2019), similar to Portugal in (Felgueiras and Pinto, 2022).

Previous studies have highlighted the comparative advantages of ECC over RSA in cryptographic operations, particularly within HTTPS contexts. The efficiency of ECC and the lower computational requirements have been demonstrated in (Mahto and Kumar Yadav, 2017). The superior processing speed, scalability, and security of ECC were highlighted in (Gobi et al., 2015).

Given these insights, the current dataset highlights the potential benefits of transitioning to longer key lengths, by embracing the ECC algorithm to bolster security measures. The uses of ECC with further key lengths could offer greater security without impinging on operational efficiency.

4.1.3 Certification Authorities

This section explores the landscape of Certification Authority (CA) preferences among HEIs in general, as depicted in Fig. 6. The analysis of CA selections across the board provides insight into the overarching trends and potential implications of CA choices, offering valuable information for institutional policymakers.

The data indicates that R3 is the most prevalent CA, representing approximately 21.6% of the total CAs utilized. Close behind is GEANT OV RSA CA 4, accounting for just over 21% of usage. These two CAs are followed by Certum Domain Validation CA SHA2 and Certyfikat SSL, each constituting around 14.7% of the CA market share within HEIs. The CA known as nazwaSSL is also notable, comprising roughly 9.9% of the total. Collectively, a variety of other CAs make up 18% of the CA selections, indicating a diverse range of preferences beyond the leading entities.

The findings suggest a relatively balanced distribution among the top CAs, with no single authority dominating the landscape. This diversity in CA choice among HEIs could be indicative of a competitive market where factors such as trustworthiness, cost, and specific service offerings play significant

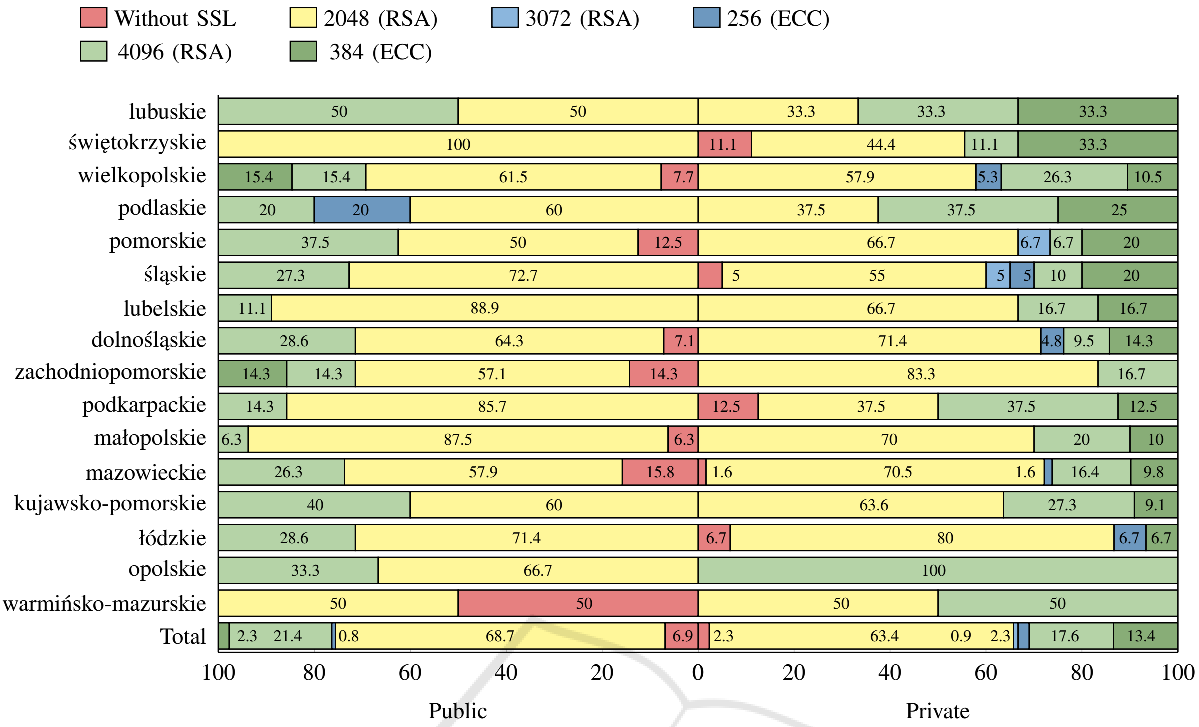

Figure 5: Territorial distribution of SSL/TLS digital certificate key lengths within HEIs (%).

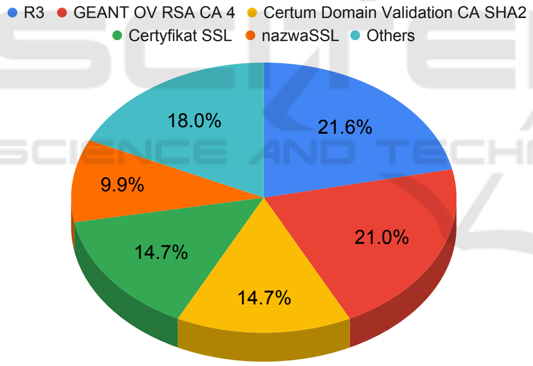

Figure 6: Leading 5 Certification Authorities within HEIs.

roles in the selection process. The preference for R3 and GEANT OV RSA CA 4 as the leading CAs may reflect their alignment with the security requirements and trust levels expected by educational institutions. The prominence of these CAs underscores their perceived reliability and the value they provide in securing digital communications within the academic sector.

The strong presence of the "Others" category highlights that a significant number of HEIs opt for wide range of CAs, which may be influenced by unique institutional needs, regional partnerships, or specific technological compatibilities. This variety may signal that HEIs choose a CA that best fits their security posture and budgetary constraints.

In summary, the CA landscape within HEIs is characterized by a wide variety of specialized entities.

4.2 Security Headers

This section assesses the utilization of security headers in HEIs in Poland, a key aspect of web security. As shown in Figure 7, there's a disparity in security headers implementation across public and private HEIs.

Security headers are a relevant protection against a set of attacks and, in this study, and similarly to global trends (Buchanan et al., 2018), a considerable number of HEIs have not integrated essential security headers, such as 'content-security-policy', leaving them vulnerable to XSS attacks and data breaches (Lavrenovs and Melon, 2018; Siewert et al., 2022). For instance, XSS attacks can lead to unauthorized data access, significantly impacting data confidentiality and institutional reputation.

The data reveals regional disparities in adoption rates where few regions show complete adoption, while others fall behind. This inconsistency underscores the need for a more unified approach to web security within HEIs.

Given the critical role of headers such as 'strict-transport-security' in preventing man-in-the-middle attacks, the limited adoption in many HEIs poses a high risk. This study's findings highlight the urgency for HEIs, particularly those lagging, to enhance their

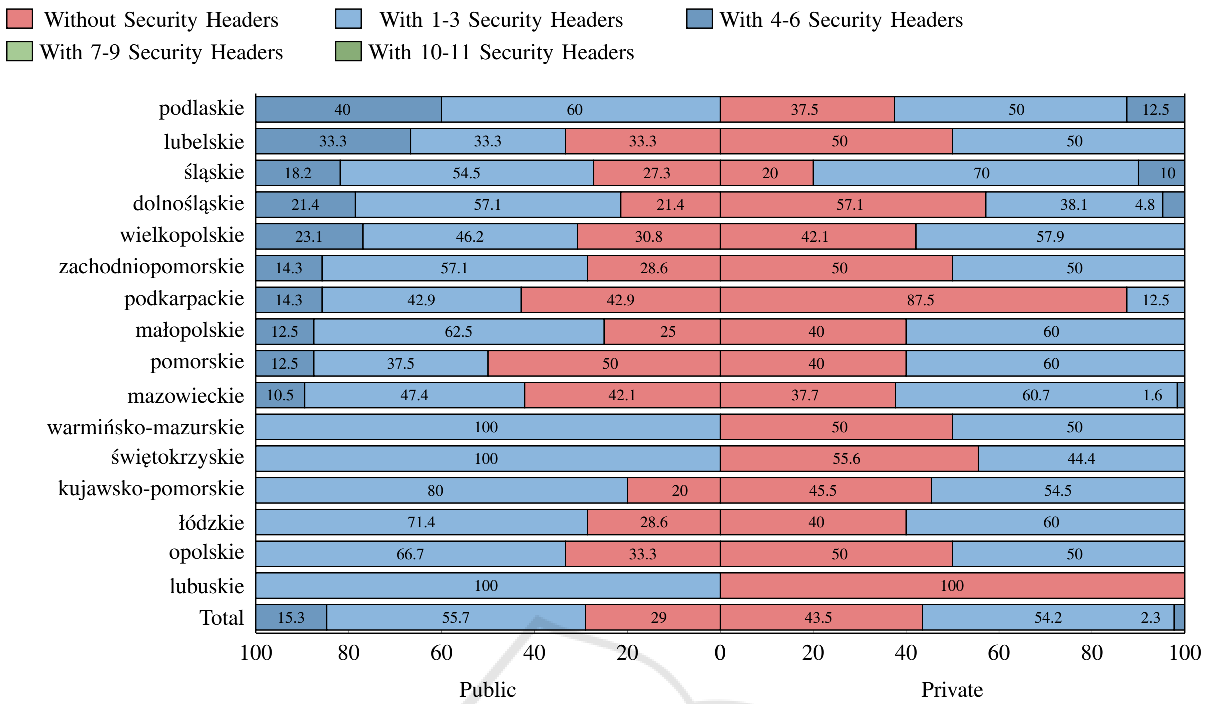

Figure 7: Regional distribution of Security Headers utilization (%).

web defenses by adopting a comprehensive set of security headers, as recommended by OWASP. Further research should explore the barriers to adoption and strategies to overcome them.

4.3 DNSSEC

Regarding the adoption and implementation of DNSSEC it was verified that none of the Polish HEIs have configured it. The absence of DNSSEC configurations should be a concern since it exposes these institutions to DNS cache poisoning attacks and string injection during domain name resolutions (Jeitner and Shulman, 2021; Man et al., 2021). Such attacks can redirect users to fraudulent websites, mimicking HEIs' official pages.

Existing research corroborates the observed trend of limited DNSSEC adoption among HEIs in Poland. Several studies have highlighted that, despite the prevalent deployment of DNSSEC at top-level domains (for example, '.pl'), its uses remain scarce in subordinate domains, such as those of HEIs (Chung et al., 2017; Lian et al., 2013; Osterweil et al., 2008; Hao Yang et al., 2011).

A deeper inquiry is warranted to discern the underlying factors contributing to the subdued uptake of DNSSEC within HEIs. Potential rationales could encompass a limited cognizance of the protocol's significance or a shortfall in the requisite technical understanding for its deployment. Probing these conjectures might unveil the primary deterrents to DNSSEC adoption, paving the way for crafting efficacious strategies to advocate its broader implementation.

5 DISCUSSION

This section discusses ethical considerations upheld throughout the research and acknowledge the limitations inherent in our study.

Ethical integrity was paramount in our methodology, with all procedures being non-invasive and designed to avoid any negative impact on the infrastructures of the HEIs. The reporting of our findings was carefully managed to prevent the disclosure of specific vulnerabilities of individual HEIs. By focusing on regional data aggregation, this study highlights broader cybersecurity trends rather than identifying specific institutional weaknesses. Such an approach not only aligns with ethical research practices but also contributes constructively to the cybersecurity domain by providing region-specific insights and recommendations. Our commitment to the principle of beneficence guided us to contribute positively to the HEIs' efforts in bolstering their cybersecurity defenses, thereby supporting their educational and research endeavors in a digitally secure environment.

Regarding the limitations of the current research, it can highlighted that this study provides a temporal snapshot of cybersecurity practices in Polish HEIs, which might not fully represent ongoing security enhancement efforts. Its geographical focus on Poland may limit the extrapolation of our findings to HEIs operating in different cybersecurity environments. Data collection dependencies on network conditions and the study's quantitative nature, excluding qualitative perspectives, might have influenced the data's breadth and depth. Although this research sheds light on potential cybersecurity risks, it does not directly link these to the incidence or severity of actual security breaches in HEIs. These limitations highlight the necessity for future research that incorporates longitudinal, qualitative, and comprehensive impact assessments to deepen the understanding of cybersecurity practices in the higher education sector.

These limitations underscore the need for future research incorporating longitudinal, qualitative, and impact-focused approaches to provide a more comprehensive understanding of cybersecurity practices in higher education.

6 CONCLUSION

This paper provides an analysis of web-related security issues in HEIs in Poland, providing a comprehensive overview of current practices and identifying critical areas for improvement.

The investigation into DNSSEC, SSL/TLS algorithms and key lengths, valid SSL/TLS configurations, HTTPS implementation, and security headers reveals a multifaceted cybersecurity environment within Polish HEIs.

While the adoption of HTTPS is widespread, the study identifies a minority of HEIs that are yet to align with this protocol, potentially exposing them to security risks. On a positive note, many institutions enforce mandatory redirections to secure web pages, thereby bolstering data protection.

The study notes a preference for the RSA algorithm with a 2048-bit key in the majority of HEIs, while also recognizing the potential benefits of adopting the ECC algorithm with longer key lengths for enhanced security without compromising performance. Furthermore, there is a need for continued vigilance in updating and phasing out older, less secure SSL/TLS versions, as some institutions still rely on outdated protocols such as SSLv3.0 and TLSv1.0.

Security headers, essential in mitigating web threats, show varied adoption rates, with about half of the institutions implementing at least one of the 11 headers recommended by OWASP. Notably, there is an absence of DNSSEC implementation in the HEIs examined.

The findings highlight the crucial need for HEIs in Poland to continually evaluate and enhance their cybersecurity strategies. By addressing the identified areas for improvement, these institutions can strengthen their defenses against the evolving cyber threat landscape and uphold best practices in web security, thereby safeguarding their data and protecting their stakeholders.

Future research directions in the realm of web security within HEIs should encompass a variety of focal points. Firstly, examining regional disparities in cybersecurity adoption is crucial, particularly how administrative autonomy and lack of unified cybersecurity guidelines contribute to regional variations in HEIs' web security measures, along with the financial resource allocation for cybersecurity. Understanding the barriers to DNSSEC implementation is another vital area, involving research into the awareness and challenges faced by Information Technology (IT) professionals in HEIs, potentially through surveys and interviews. Additionally, the limited implementation of security headers deserves investigation, focusing on their perceived effectiveness and the barriers to adoption. Exploring the impact of web cybersecurity on the public perception and trust in HEIs will provide insights into the consequences of security breaches on institutional reputation. Finally, extending this research to include comparative studies within the European Union (EU) can offer more general context, highlighting best practices, and underscoring the cultural and regulatory differences in cybersecurity among HEIs.

ACKNOWLEDGEMENTS

This study was developed in the context of the Master's Program in Cybersecurity at the Escola Superior de Tecnologia e Gestão of the Instituto Politécnico de Viana do Castelo, Portugal, in collaboration with the University of Economics in Katowice, Poland.

REFERENCES

Aakanksha, Jain, B., Saxena, D., Sahni, D., and Sharma, P. (2019). Analysis of Hypertext Transfer Protocol and Its Variants. In Panigrahi, B. K., Trivedi, M. C., Mishra, K. K., Tiwari, S., and Singh, P. K., editors, *Smart Innovations in Communication and Computational Sciences*, pages 171–188, Singapore. Springer Singapore.

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., and Zimmermann, P. (2018). Imperfect forward secrecy. *Communications of the ACM*, 62(1):106–114.

Akiyama, M., Yagi, T., Yada, T., Mori, T., and Kadobayashi, Y. (2017). Analyzing the ecosystem of malicious URL redirection through longitudinal observation from honeypots. *Computers and Security*, 69:155–173.

Barker, E. and Roginsky, A. (2019). Transitioning the use of cryptographic algorithms and key lengths. Technical report, National Institute of Standards and Technology, Gaithersburg, MD.

Barreto, J., Almeida, H., and Pinto, P. (2023). An overview of https and dnssec services adoption in higher education institutions in brazil. In *2023 25th International Conference on Advanced Communication Technology (ICACT)*, pages 180–185.

Berners-Lee, T. (1991). The HTTP Protocol As Implemented In W3.

Bezjak, S., Clyburne-Sherin, A., Conzett, P., Fernandes, P., Görögh, E., Helbig, K., Kramer, B., Labastida, I., Niemeyer, K., Psomopoulos, F., Ross-Hellauer, T., Schneider, R., Tennant, J., Verbakel, E., Brinken, H., and Heller, L. (2018). *Open Science Training Handbook*. Zenodo.

Buchanan, W. J., Helme, S., and Woodward, A. (2018). Analysis of the adoption of security headers in HTTP. *IET Information Security*, 12(2):118–126.

Chung, T., Van Rijswijk-Deij, R., Chandrasekaran, B., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A., and Wilson, C. (2017). A longitudinal, end-to-end view of the dnssec ecosystem. In *Proceedings of the 26th USENIX Conference on Security Symposium*, SEC'17, page 1307–1322, USA. USENIX Association.

Emsisoft Malware Lab (2020). The State of Ransomware in the US: Report and Statistics 2020. https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/.

Emsisoft Malware Lab (2021). The State of Ransomware in the US: Report and Statistics 2021 . https://blog.emsisoft.com/en/40813/the-state-of-ransomware-in-the-us-report-and-statistics-2021/.

Felgueiras, N. and Pinto, P. (2022). An Overview of the Status of DNS and HTTP Security Services in Higher Education Institutions in Portugal. In Paiva, S., Li, X., Lopes, S. I., Gupta, N., Rawat, D. B., Patel, A., and Karimi, H. R., editors, *Science and Technologies for Smart Cities*, pages 457–469, Cham. Springer International Publishing.

Gobi, M., Sridevi, R., and Rahini, R. (2015). A Comparative Study on the Performance and the Security of RSA and ECC Algorithm. *Special Issue Published in Int. Jnl. Of Advanced Networking and Applications*.

Grenfeldt, M., Olofsson, A., Engström, V., and Lagerström, R. (2021). Attacking Websites Using HTTP Request Smuggling: Empirical Testing of Servers and Proxies. In *2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC)*, pages 173–181.

Hao Yang, Osterweil, E., Massey, D., Songwu Lu, and Lixia Zhang (2011). Deploying Cryptography in Internet-Scale Systems: A Case Study on DNSSEC. *IEEE Transactions on Dependable and Secure Computing*, 8(5):656–669.

Jeitner, P. and Shulman, H. (2021). Injection attacks reloaded: Tunnelling malicious payloads over DNS. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 3165–3182. USENIX Association.

Junior, J., Rutecka, P., and Pinto, P. (2023). Higher education institutions in poland dataset. https://doi.org/10.5281/zenodo.8333574.

Lavrenovs, A. and Melon, F. J. R. (2018). HTTP security headers analysis of top one million websites. In *2018 10th International Conference on Cyber Conflict (CyCon)*, pages 345–370. IEEE.

Lian, W., Rescorla, E., Shacham, H., and Savage, S. (2013). Measuring the Practical Impact of DNSSEC Deployment. In *Proceedings of the 22nd USENIX Conference on Security*, SEC'13, pages 573–588, USA. USENIX Association.

Mahto, D. and Kumar Yadav, D. (2017). RSA and ECC: A Comparative Analysis. *International Journal of Applied Engineering Research*, 12:9053–9061.

Man, K., Zhou, X., and Qian, Z. (2021). DNS Cache Poisoning Attack: Resurrections with Side Channels. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 3400–3414, New York, NY, USA. ACM.

Nir, Y., Josefsson, S., and Pegourie-Gonnard, M. (2018). Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier. Technical report, IETF.

Osterweil, E., Ryan, M., Massey, D., and Zhang, L. (2008). Quantifying the operational status of the DNSSEC deployment. In *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, IMC '08, pages 231–242, New York, NY, USA. ACM.

Poland (2022a). List of public universities supervised by the minister responsible for higher education - public academic universities. https://www.gov.pl/web/edukacja-i-nauka/wykaz-uczelni-publicznych-nadzorowanych-przez-ministra-wlasciwego-ds-szkolnictwa-wyzszego-publiczne-uczelnie-akademickie.

Poland (2022b). Rad-on-system - data of institutions of higher education and science system. https://radon.nauka.gov.pl/dane/instytucje-systemu-szkolnictwa-wyzszego-i-nauki.

Randall, J., Kaliski, B., Brainard, J., and Turner, S. (2010). Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS). Technical report, IETF.

Rescorla, E. (2000). HTTP Over TLS. RFC 2818.

Science in Poland (2021). Cyber attacks on Polish universities some of the worst in the world, says report. https://scienceinpoland.pl/en/news/news%2C89064%2Ccyber-attacks-polish-universities-some-worst-world-says-report.html.

Siewert, H., Kretschmer, M., Niemietz, M., and Somorovsky, J. (2022). On the Security of Parsing Security-Relevant HTTP Headers in Modern Browsers. In *2022 IEEE Security and Privacy Workshops (SPW)*, pages 342–352. IEEE.

Silveira, D. T. and Gerhardt, T. E. (2009). *Métodos de pesquisa*. UFRGS, Porto Alegre.

TCP World (2021). More cyberattacks on Polish universities: study. https://tvpworld.com/55563789/more-cyberattacks-on-polish-universities-study.

University World News (2023). Where universities face emerging threats and crises. https://www.universityworldnews.com/post.php?story=20230915123512200.

Visoottiviseth, V. and Poonsiri, K. (2019). The Study of DNSSEC Deployment Status in Thailand. In *2019 IEEE 6th Asian Conference on Defence Technology (ACDT)*, pages 13–18. IEEE.