International Journal of Marketing, Communication and New Media

ISSN: 2182-9306. Special Issue on Cybersecurity, Privacy, and Data Protection, FEBRUARY 2023

DOI: https://doi.org/10.54663/2182-9306.2023.sn12.59-76

Research Paper

An Analysis on the Implementation of Secure Web-Related Protocols in Portuguese City Councils

Jackson Júnior *
Pedro Carneiro **
Sara Paiva ***
Pedro Pinto ****

ABSTRACT

The services supporting the websites, both public and private entities, may support security protocols such as HTTPS or DNSSEC. Public and private entities have a responsibility to ensure the security of their online platforms. Entities in the public domain such as city councils provide their services through their websites. However, each city council has its systems, configurations, and IT teams, and this means they have different standings regarding the security protocols supported. This paper analyzes the status of security protocols on Portuguese city council websites, specifically HTTPS and DNSSEC. The study evaluated 308 city council websites using a script developed for the research, and data was collected from the website of Direção Geral das Autarquias Locais (DGAL) on December 14, 2022, and the websites were scanned on December 22, 2022. The results of this assessment reveal that around 97% of city council websites use RSA as their encryption algorithm and around 84% use 2048-bit length keys for digital certificate signing. Furthermore, about 53% of the city council websites are still supporting outdated and potentially insecure SSL/TLS versions, and around 95% of the councils are not implementing DNSSEC in their domains. These results highlight potential areas for improvement in cybersecurity measures and can serve as a baseline to track progress toward improving cybersecurity maturity in Portuguese city councils.

Keywords: Cybersecurity, DNSSEC, HTTPS, SSL/TLS, Security headers, Portuguese city councils, Website security.

* ADiT-LAB, Polytechnic Institute of Viana do Castelo, Portugal. E-Mail: jacksonjunior@ipvc.pt
** ADiT-LAB, Polytechnic Institute of Viana do Castelo, Portugal. E-Mail: pedrocarneiro@estg.ipvc.pt
*** ADiT-LAB, Polytechnic Institute of Viana do Castelo, Portugal. E-Mail: sara.paiva@estg.ipvc.pt
**** ADiT-LAB, Polytechnic Institute of Viana do Castelo, and INESC TEC, Portugal. E-Mail: pedropinto@estg.ipvc.pt

Received on: 2023/02/01
Approved on: 2023/02/28
Evaluated by a double-blind review system

1. INTRODUCTION

Websites of public and private organizations are supported by various services that can use secure protocols such as Hyper Text Transfer Protocol Secure (HTTPS) or Domain Name System Security Extensions (DNSSEC).

Ensuring the security of these online platforms is a legal responsibility of these entities (Portugal, 2019, 2021), which a key role in safeguarding sensitive information and protecting the privacy of their users. Using the most current version of security protocols helps prevent unauthorized access to data, thwart potential cyber-attacks, and maintain the integrity of the information that is transmitted and stored online. By implementing HTTPS and DNSSEC, public and private organizations can ensure they are taking the necessary steps to protect their online platforms and protect the interests of their users.

In addition, errors in security configurations can cause service disruptions for users, as browsers block access to the site, to prevent personal data from being compromised. In the case of the Portuguese Tax Authority, an error in the security certificate (expired certificate) of the Finance Portal prevented access from numerous users who needed to comply with the deadlines of their tax obligations (Nunes, 2022).

In 2021, Portugal had significantly surpassed the global average of weekly computer attacks, with almost 900 attacks recorded just in the first nine months of the year. This represents an increase of 71% from the previous year (while the worldwide increase was 40%) (Andrade, 2021). The Public Administration/Military sector was the second most targeted by hackers, with an average of 1082 attacks per organization. Portugal exceeds the European average of 665 weekly attacks (which had a 65% growth compared to the previous year) (Check Point Research, 2022).

City councils are just one example of entities in the public domain that offer their services through their websites. Since each city council has administrative independence, each independently operates its systems, with different configurations and IT teams, leading to different status in the level of support for secure protocols between city councils. Thus, it is important to assess the status of each city council regarding the levels of support for secure protocols to get deeper understanding of the challenges and opportunities for improving cybersecurity measures in this sector.

This article aims to investigate a research problem on the current state of cybersecurity in Portuguese city councils. The specific focus of the study is on the implementation of two secure Web-related protocols, namely HTTPS and DNSSEC, on their websites. The analysis of the implementation of these protocols serves to respond to this research problem and to understand the evolution of the maturity of cybersecurity of Portuguese city councils. By presenting the main conclusions and contributions, this study will provide stakeholders with valuable information to design and implement appropriate measures to improve cybersecurity and better protect sensitive and personal information of their citizens. The results of this research, combined with the literature review, will contribute to understanding the progress and evolution of cybersecurity maturity in Portuguese Municipal Councils and may be used by decision-makers to design and implement appropriate measures to improve their cybersecurity.

This paper is structured as follows. Section 2 presents the related work. Section 3 describes the methodology used. Section 4 presents and analyzes the results. Section 5 presents the conclusions.

2. RELATED WORKS

Hyper Text Transfer Protocol (HTTP) is widely used for communication and data transfer between servers and clients; however, it was not initially designed to include security mechanisms (Berners-Lee, 1991). Its versions (HTTP/1.0 and HTTP/1.1) have several security and performance issues that can be exploited by attackers, such as Man-in-the-Middle (MitM) and sniffer (Rescorla, 2000) attacks.

The study (Aakanksha et al., 2019) analyzed the performance and security of various commonly used websites using HTTP 1.1, HTTPS, and HTTP 2.0, and proposed measures to improve the performance and security of websites.

HTTP Request Smuggling (HSR) is an example of an HTTP vulnerability, which occurs when web servers and proxies interpret the length of a single HTTP request differently, potentially allowing attackers to execute malicious activities. Authors in (Grenfeldt et al., 2021) conducted empirical tests to identify parsing behaviors that could lead to HSR on popular web servers and proxies and found 19 vulnerable behaviors, leading to the successful execution of complete or almost complete attacks in a combination of servers and proxies.

In addition, the use of URL redirection mechanisms presents security vulnerabilities that can be exploited by attackers for web-based attacks, which adds to the security issues posed by HTTP. (Akiyama et al., 2017) study contributes to the understanding of the evolution of the malicious URL redirection ecosystem and suggests practical countermeasures against these attacks. The study identifies the growing use of web-based domain generation algorithms (DGAs) to increase the entropy of redirect URLs, which is aimed at thwarting URL blocklisting. The results of this study provide a relevant justification for the analysis conducted in our research, which examines the type of HTTP to HTTPS redirection used by municipal council websites and whether it is for the same or different domains.

In the context of analyzing the use of cryptographic algorithms in HTTPS communications, previous studies have compared the performance and security of the RSA and ECC algorithms. (Mahto & Kumar Yadav, 2017) conducted experiments to compare the time lapse during encryption and decryption using RSA and ECC on sample input data of different lengths. The results showed that ECC outperformed RSA in terms of operational efficiency and security with fewer parameters. Another study (Gobi et al., 2015) also compared RSA and ECC algorithms to encrypt and decrypt text. The analysis showed that ECC performed the best compared to the RSA algorithm in terms of execution time, speed, scalability, flexibility, reliability, and security.

The selection of analysis parameters for the research was supported by these studies, which demonstrated that although RSA is a widely used and secure algorithm, Elliptic-Curve Cryptography (ECC) can provide equivalent security with a shorter key length and faster computation times. Consequently, the choice of algorithm and key length used in HTTPS communications, as well as the minimum version of the SSL/TLS protocol supported by the web server, can have an impact on communication security. Therefore, it is important to consider these factors when examining the usage of these protocols among Portuguese municipal council websites.

However, vulnerabilities in HTTPS and its implementation have been identified, such as the Logjam attack which allows for MitM downgrades to “export-grade” Diffie-Hellman (Adrian et al., 2018).

To address these concerns, security headers have become increasingly important in web services. These headers contain additional fields in HTTP and HTTPS responses that enforce security policies and help prevent attacks such as MitM and code injection.

Within this context, the study (Buchanan et al., 2017) analyzed the adoption of security headers, including content security policy, public key pinning extension for HTTP, HTTP

Strict Transport Security (HSTS), and X-Frame-Options (XFO). The results showed that while the implementation of these headers is increasing, they are still not widely implemented on top sites.

Authors in (Siewert et al., 2022) evaluated the security of parsing security-relevant HTTP headers in modern browsers and found that most browsers do not fully implement the relevant specifications, leading to vulnerabilities such as header injection and spoofing.

According to authors in (Lavrenovs & Melón, 2018), HTTPS websites are more likely to implement security headers than HTTP-Only websites. However, the adoption of security headers is still far from widespread, and there is room for improvement.

The Domain Name System (DNS) is also a key component of the web services of the city councils, which are responsible for resolving domain names into IP addresses.

And DNS also stands as vulnerable to diverse types of attacks, such as string injection (Jeitner & Shulman, 2021) and cache poisoning (Man & Qian, 2021). To mitigate several vulnerabilities, the DNSSEC was proposed (Rose et al., 2005). Which is an extension aiming to secure the DNS protocol by using digital certificates to validate DNS responses and authenticate the origin and integrity of data (Visoottiviseth & Poonsiri, 2019).

Despite the widespread support and implementation of DNSSEC among top-level domains, studies such as (Chung et al., 2017; Lian et al., 2013; Osterweil et al., 2008; Yang et al., 2011) have found that its adoption has been low, due to factors such as lack of support from local resolvers and server misconfigurations.

Overall, while HTTP, HTTPS, DNSSEC and the security headers offer important protections against distinct types of attacks, their correct implementation and adoption are not yet widespread enough.

A study conducted checkpoint analyses of the cybersecurity status of websites in the higher education sector, in Portugal (Felgueiras & Pinto, 2022). The results of these studies showed that there is room for improvement in the adoption of HTTPS and DNSSEC by higher education institutions.

A specific study on the adoption of HTTPS on the official websites of the 308 Portuguese municipalities (Gomes et al., 2019) found that only 3.6% of the municipalities were considered good in terms of secure communication with citizens, while 46.1% did not guarantee minimum conditions. The study identified a link between the adoption of HTTPS and the municipality size but also noted the need for more explanatory factors.

Similarly, the study in (Gomes et al., 2019, 2020), assesses the state of cybersecurity for the websites of Portuguese city councils. It goes beyond evaluating the adoption of HTTPS and the presence of security certificate errors, to also consider the implementation of security headers recommended by the Open Web Application Security Project (OWASP). Furthermore, the susceptibility of these websites to known vulnerabilities and the adoption of DNSSEC will be evaluated. This study aims to provide insight into the state of cybersecurity maturity for these organizations and identify areas for improvement.

3. METHODOLOGY

The methodology used in this study is a quantitative approach, with an exploratory and descriptive objective, based on the analysis of publicly available data from the websites of Portuguese city councils (Silveira & Córdova, 2009).

The study population consisted of 308 city council websites and data were collected from the website of Direção Geral das Autarquias Locais (DGAL), (DGAL, 2021), a central service of the direct state administration integrated into the Ministry of Territorial Cohesion, on December 14, 2022, the last update being on November 3, 2021. It was performed a manual review of all websites and were identified and corrected web addresses for a set of city councils. To adhere to open science principles (Bezjak et al., 2018), the list of city council websites used in this study is available in a public repository (Júnior & Pinto, 2023).

The websites were scanned on December 22, 2022, using the script on GitHub (Junior, 2022), build for the current research. The software was developed in Python programming language. The software records its results in a Comma Separated Values (CSV) file.

The results were analyzed using Python scripts run on Jupyter Notebooks, using libraries such as Pandas and Numpy o perform the analyses, which were saved in CSV files. The analyses were conducted in 6 areas:

- DNSSEC use by district
- HTTPS use by district
- SSL/TLS key length by district
- Use of security headers by district
- Type of SSL/TLS algorithm by district
- Worst SSL/TLS version by district.

The websites were accessed using the HTTP and HTTPS versions to evaluate the use of secure protocols. In case a website was not available or loaded correctly, it was considered not to have HTTPS. The forced redirect from HTTP to HTTPS was also tested, in this case, false redirects such as HSTS that only work on browsers were also considered.

The analysis of security headers was based on the OWASP list of active security headers. These headers are an important aspect of website security, as they help to mitigate various types of attacks, such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF). Some of the security headers that we analyzed include:

- Strict-Transport-Security
- X-Frame-Options
- X-Content- Type-Options
- Content-Security-Policy
- X-Permitted-Cross-Domain-Policies
- Referrer-Policy
- Clear-Site-Data
- Cross-Origin-Embedder-Policy
- Cross-Origin-Opener-Policy
- Cross-Origin-Resource-Policy
- Cache-Control (OWASP Foundation, n.d.)

The following information was recorded for each website:

a) for analysis of the HTTP/HTTPS protocol
    - has-https
    - forced- redirect-to-https
    - https-redirect-to-same-domain

b) for SSL/TLS analysis
    - Issuer
    - valid-from
    - valid-until
    - key-size
    - algorithm- key
    - signature-algorithm
    - ssl2
    - ssl3
    - tls1-0

- tls1-1
- tls1-2
- tls1- 3
- grade

c) for analysis of security headers, it was based on the OWASP list

d) DNSSEC

- has-dnssec
- dnssec-is-valid
- dnssec- algorithm

4. RESULTS

The Results section presents the findings of the study on the use of security protocols by Portuguese city councils. This section provides an analysis focused on six key areas: the use of DNSSEC, HTTPS, SSL/TLS key length, security headers, SSL/TLS algorithm, and worst SSL/TLS version.

The findings are presented in figures, showing the distribution of each area by district. The results provide valuable information on the current state of security practices among city councils and may help identify areas for improvement to ensure the privacy and security of information transmitted.

4.1 HTTP/HTTPS

The HTTPS secure communication protocol is essential to ensure the privacy and security of information exchanged between users and websites. However, it is still possible to observe some difficulties in the implementation and maintenance of this protocol on website servers. In this sense, this subsection will assess the use of HTTPS by Portuguese city councils, as well as any problems faced in this process.

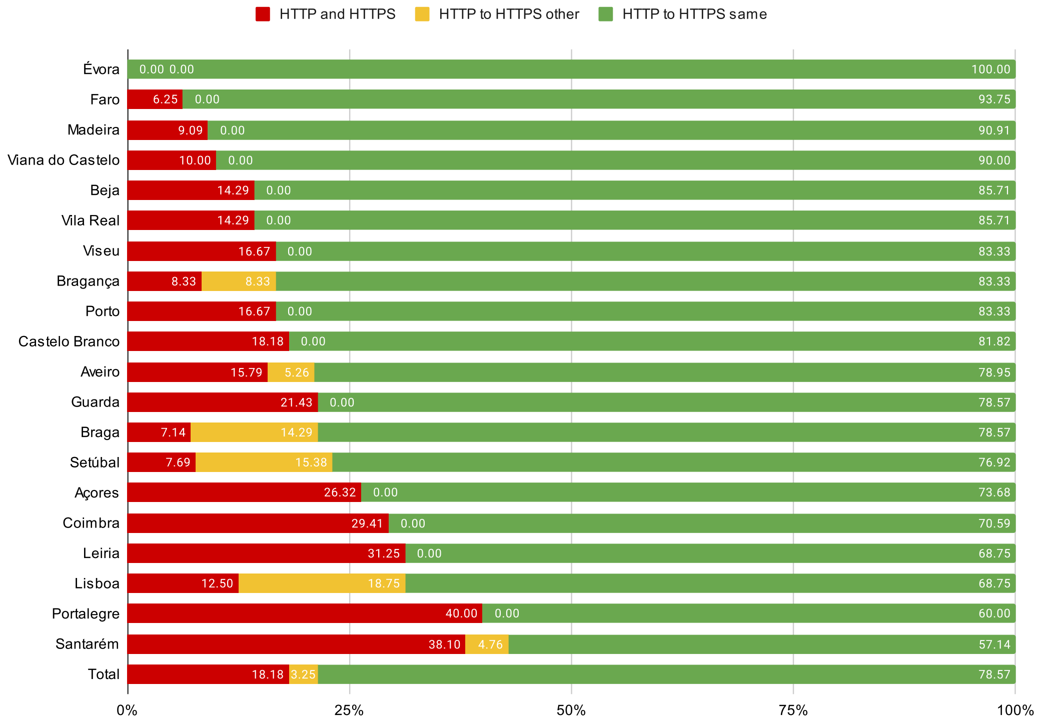

Figure 1. Distribution of the use of the HTTP/HTTPS protocol

Figure 1 shows that the majority (78.57%) of the city councils correctly use the HTTPS protocol, which includes the redirection from HTTP to HTTPS in the same domain. This result correlates with (Akiyama et al., 2017) study, which highlights the increasing use of web-based domain generation algorithms (DGAs) to increase the entropy of redirect URLs and prevent URL blocklisting, making the use of the forced redirection to the same domain more crucial to secure communication.

However, 18.18% of the chambers maintain joint use of the HTTP and HTTPS protocols, which is when the user can access the website through both versions of the protocols, without any redirection method.

The districts with the best performance in the use of HTTPS (with forced redirection to the same domain) are Évora with all municipalities, Faro (93.75%), and the autonomous region of Madeira (90.91%). The councils that lead the joint use of both protocols are Porto Alegre (40%), followed by Santarém (38.10%) and Leiria (31.25%).

The implementation and maintenance of HTTPS protocols on website servers are crucial to ensure the privacy and security of information exchanged between users and websites. The literature review showed that vulnerabilities in HTTP and its implementation have been identified, such as HTTP Request Smuggling (HSR) that can potentially allow attackers to execute malicious activities (Grenfeldt et al., 2021). Presently, around 18% of the city councils expose their users to these risks.

4.1.1 SSL/TLS

This subsection presents the results of an analysis of the use of SSL/TLS protocols by Portuguese city councils. The analysis focused on the most used encryption algorithms (RSA or ECC), the length of keys used for the signing of digital certificates, and the worst versions of the protocols still supported by the websites of city councils. The findings of this analysis provide valuable information on the current state of SSL/TLS usage among city councils and may help identify improvements to improve security.

The results presented in Figure 2 suggest that most Portuguese municipal councils are using SSL/TLS, which indicates that they are concerned about protecting the privacy and security of transmitted data. The literature review supports this finding, as previous studies have shown that RSA is a more widely used encryption algorithm than ECC, which can make the implementation more common for city councils (Gobi et al., 2015).

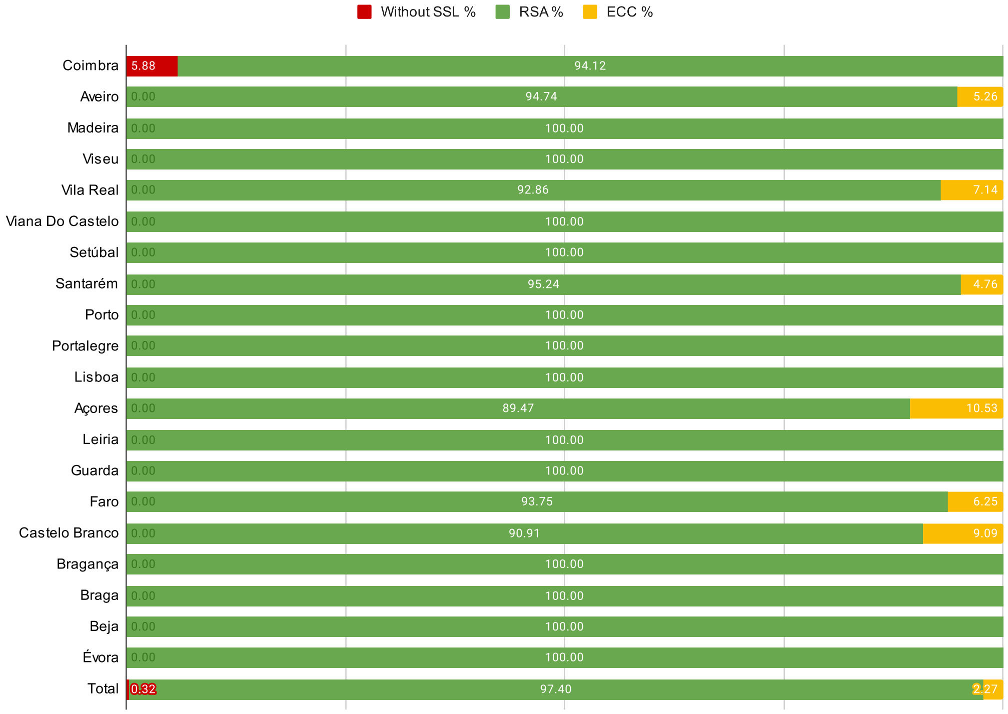

Figure 2. Distribution of the type of SSL/TLS algorithms used in the municipal councils of Portugal by districts

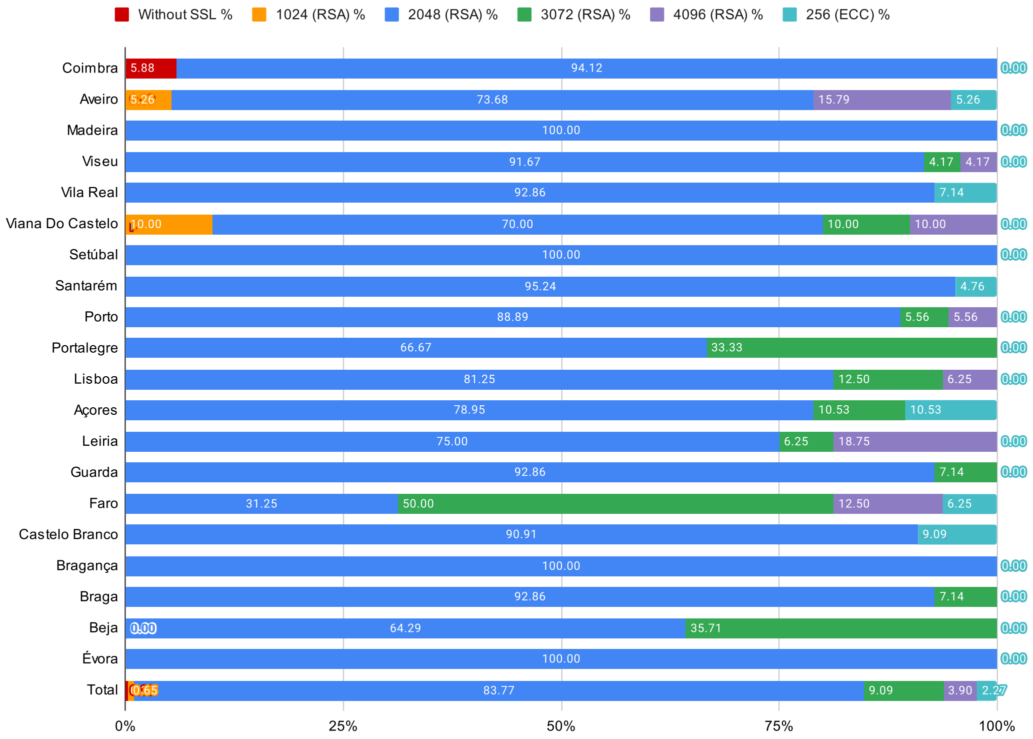

Figure 3. Distribution of the length of SSL/TLS digital certificate signing keys in Portugal by districts

Figure 3 provides additional information on the key lengths used in SSL/TLS certificates by municipal councils. Most districts in Portugal (84%) use 2048-bit RSA encryption, which is the key length recommended by the National Institute of Standards and Technology (NIST) and provides a high level of security. However, some districts also use longer key lengths such as 3072-bit RSA encryption, which provides an even higher level of security, as is the case of Faro (50%), Beja (35%), and Portalegre (33%). Although previous studies have shown that ECC can provide equivalent security with shorter key lengths and faster computation times compared to RSA (Mahto & Kumar Yadav, 2017), its implementation is still limited, representing only a small percentage (2.3%) of municipal councils.

Overall, the results suggest that most Portuguese municipal councils are using secure protocols and encryption algorithms to protect against potential security threats. However, there is still room for improvement, particularly in the adoption of more advanced encryption algorithms, such as ECC, which can provide enhanced security with longer key lengths. By doing so, a higher level of security can be achieved while maintaining the same computational cost currently associated with the RSA encryption algorithm

(Mahto & Kumar Yadav, 2017).

Figure 4 presents the worst version of the supported SSL/TLS protocol. The results show that a small percentage (4.2%) of the municipal councils in Portugal still support outdated and insecure versions of the SSL protocol. However, a significant majority of city councils (42.2%) have adopted the latest versions of the TLS protocol (TLSv1.2 and TLSv1.3) as the minimum acceptable versions on their websites. This indicates a proactive approach to ensure the security of online communications. Despite this, around half of the municipalities (48.7%) are still allowing connections using TLS version 1.0, which has known vulnerabilities and is considered less secure than later versions. This highlights the need for regular review and updating of server configurations hosting these websites to ensure they follow the best security practices.

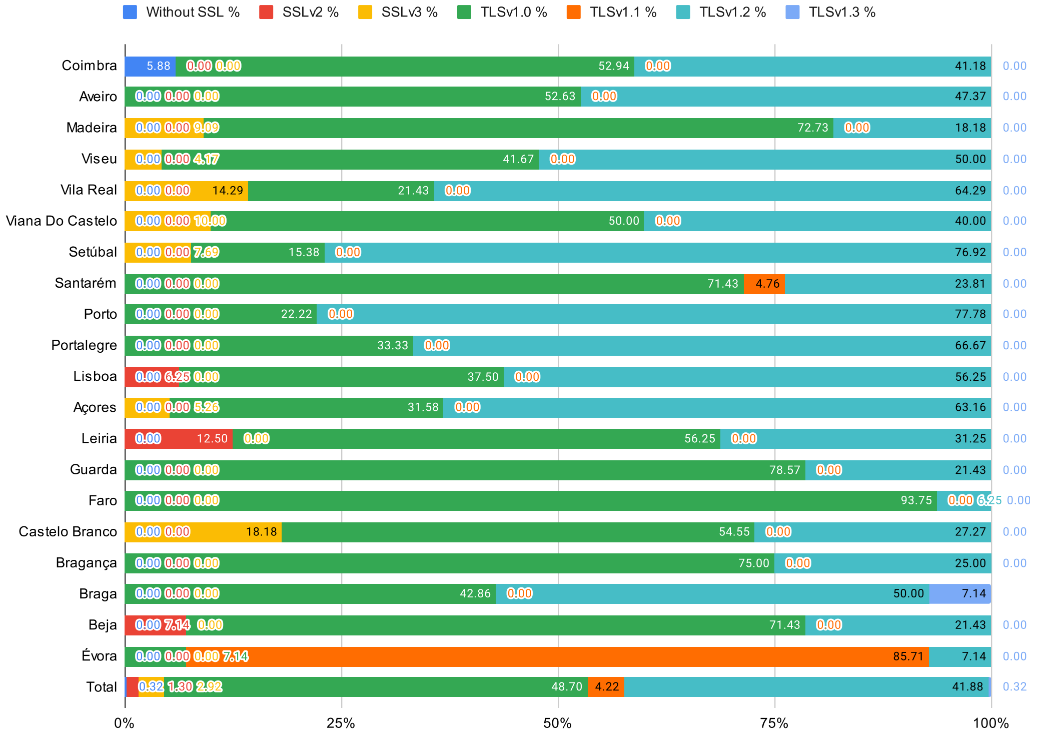

Figure 4 . Worst version of the SSL/TLS protocol

Overall, the results suggest a balanced use of secure protocols among districts, with almost half of the connections using secure versions of TLS, but the other half still vulnerable due to the use of outdated or less secure versions. Therefore, it is essential to ensure that all connections use the most up-to-date and secure versions of these protocols. Disabling older and potentially weaker versions is as important as enabling the most recent ones.

4.2 Security Headers

In this subsection, it is analyzed the use of security headers, over the HTTPS protocol, by municipal councils in Portugal.

The use of security headers has been shown to be an effective way to improve website security against cyber threats. The review of the literature reveals that although the implementation of security headers is increasing, they are still not widely adopted on top sites. The presence of security headers was analyzed in this research, specifically under the HTTPS protocol. As noted in previous studies (Lavrenovs & Melón, 2018), HTTPS sites are more likely to implement security headers than HTTP-only sites.

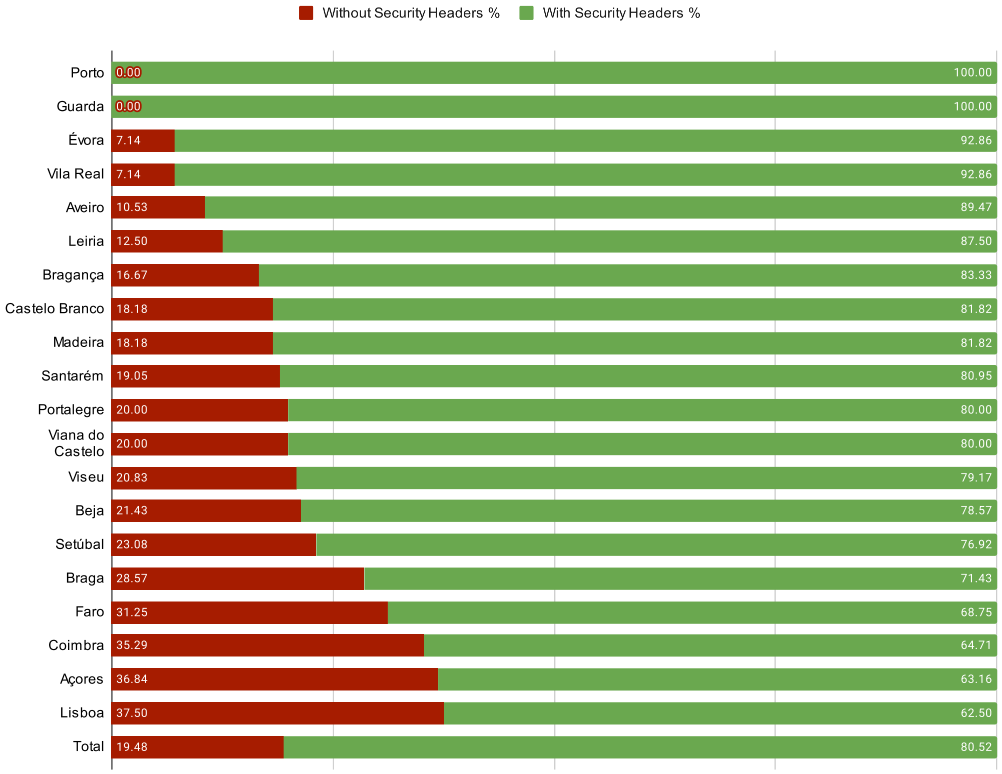

Figure 5. Distribution of the use of Security Headers

Figure 5 presents the distribution of the use of security headers. The results show that while 80.52% of city councils have at least one of the 11 security headers on their websites, the adoption of security headers varies significantly by district, with some districts performing up to five times worse than others. Also, all city councils in Porto and Guarda districts make use of at least one of the 11 security headers analyzed, making them the top performers in this area. Évora and Vila Real also have a high adoption rate of 92.8% each. On the other hand, the Coimbra districts (35.2%), Azores (36.8%) and Lisbon

(37.5%) have the lowest adoption rates for security headers.

Nonetheless, the discrepancies in the adoption of security headers among districts indicate that there is still scope for enhancement in this domain. Further research is required to comprehend the aspects that influence the adoption of these security headers and to investigate the use of each security header individually.

4.3 DNSSEC

The DNSSEC subsection of this work assesses the use of the DNSSEC protocol by municipal councils in Portugal. Figure 6 presents the use of the DNSSEC protocol in Portugal by district. The results show that most municipal councils in Portugal do not use DNSSEC, with only 5.5% of the districts implementing the protocol. Some districts, such as Viseu, Coimbra, Porto, Castelo Branco, Viana do Castelo, Lisbon, Évora and the Autonomous Region of the Azores, do not have any city council using DNSSEC. The reviewed literature suggests that the low adoption of DNSSEC by municipal councils in Portugal is not unique in this context. Despite the widespread support and implementation of DNSSEC among top-level domains, studies have found that its adoption by lower-level domains, such as municipal councils, has been low (Chung et al., 2017; Lian et al., 2013; Osterweil et al., 2008; Yang et al., 2011).

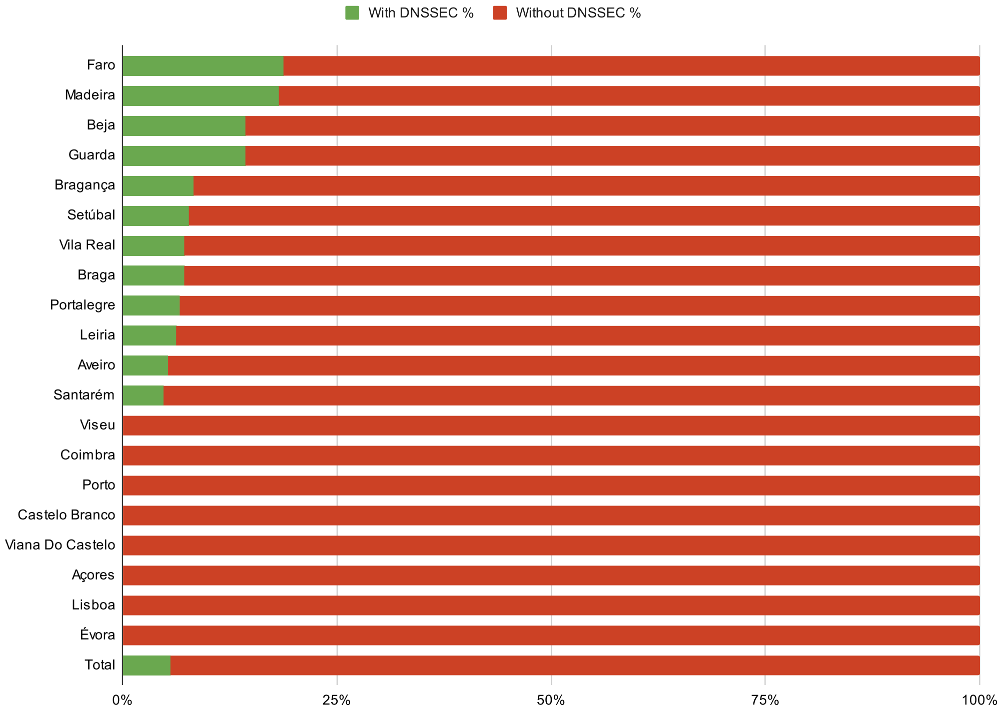

Figure 6. Use of the DNSSEC protocol in Portugal by districts

Further research is required to gain a deeper understanding of the reasons behind the low implementation of DNSSEC among municipal councils. Some potential factors that could explain this situation include a lack of awareness regarding the importance of this security protocol or a deficiency in technical expertise required to implement it. Examining these hypotheses could help identify the root causes of the low adoption of DNSSEC and enable the development of more effective strategies to promote its implementation in the future. According to research results, a significant majority of municipal councils, accounting for about 94% of them, are at risk of facing string injection and cache poisoning attacks in the process of resolving domain names for their websites (Jeitner & Shulman, 2021; Man & Qian, 2021).

5. CONCLUSION

This article aims to evaluate the current state of cybersecurity for the websites of Portuguese city councils. Through this analysis, we sought to understand the existing measures in place to protect these public institutions and identify potential areas for improvement. By creating a baseline of this information, we hope to establish a framework with which to track the evolution of cybersecurity maturity among these cities in the future.

The analysis focused on six key areas: the use of DNSSEC, HTTPS, SSL/TLS key length, security headers, SSL/TLS algorithm, and worst SSL/TLS version.

The results indicate that a substantial proportion of city council websites (81.8%) implement HTTPS for network security, with the majority (97.4%) utilizing RSA as the encryption algorithm and (83.7%) employing 2048-bit length keys for digital certificate signing. Additionally, a substantial portion (80.5%) of the websites adopt at least one of the recommended security headers by OWASP.

However, the study also identified several areas for improvement, such as the fact that over half (52.9%) of city council websites still support outdated and potentially insecure SSL/TLS versions, and (94.4%) have not implemented DNSSEC on their domains.

Further research could explore factors that contribute to the use of security headers and the latest versions of SSL/TLS protocols in different districts across city councils. It could also assess the evolution of cybersecurity measures over time. Expanding the scope of the study to include other public administration organizations, such as schools and hospitals, could provide a more comprehensive understanding of the state of cybersecurity in the public sector.

In conclusion, the research provides valuable information into the current state of cybersecurity for Portuguese city council websites. Establishing a baseline of this information identifies potential areas for improvement and lays the foundation for future implementations of cybersecurity best practices. This framework provides a means to track the evolution of cybersecurity maturity in these cities over time. As a truism from the field of quality improvement says, “What you cannot measure, you cannot improve” (Blumenthal & McGinnis, 2015).

6. ACKNOLEDGEMENTS

This study was developed in the context of the Master of Cybersecurity Program at the Instituto Politécnico de Viana do Castelo, Portugal.

This work was supported by the Norte Portugal Regional Operational Program (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (ERDF), within the project “Cybers SeC IP” (NORTE-01-0145-FEDER-000044).

REFERENCES

Aakanksha, Jain, B., Saxena, D., Sahni, D., & Sharma, P. (2019). Analysis of Hypertext Transfer Protocol and Its Variants. In B. K. Panigrahi, M. C. Trivedi, K. K. Mishra, S. Tiwari, & P. K. Singh (Eds.), *Smart Innovations in Communication and Computational Sciences* (pp. 171–188). 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., & Zimmermann, P. (2018). Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. *Commun. ACM*, *62*(1), 106–114. https://doi.org/10.1145/3292035

Akiyama, M., Yagi, T., Yada, T., Mori, T., & Kadobayashi, Y. (2017). Analyzing the ecosystem of malicious URL redirection through longitudinal observation from honeypots. *Computers and Security*, *69*, 155–173. https://doi.org/10.1016/J.COSE.2017.01.003

Andrade, F. (2021, October 7). *Organizações portuguesas registam 871 ciberataques por semana*. ECO. https://tek.sapo.pt/noticias/internet/artigos/organizacoes-portuguesas-registam-871-ciberataques-por-semana

Berners-Lee, T. (1991). *The HTTP Protocol As Implemented In W3*. https://www.w3.org/Protocols/HTTP/AsImplemented.html

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., & Heller, L. (2018). *Open Science Training Handbook*. Zenodo. https://doi.org/10.5281/zenodo.1212496

Blumenthal, D., & McGinnis, J. M. (2015). Measuring Vital Signs: An IOM Report on Core Metrics for Health and Health Care Progress. *JAMA*, *313*(19), 1901–1902. https://doi.org/10.1001/jama.2015.4862

Buchanan, W. J., Helme, S., & Woodward, A. (2017). *Analysis of the adoption of security headers in HTTP*. https://doi.org/10.1049/iet-ifs.2016.0621

Check Point Research. (2022). *Cyber Security Report 2022*. https://www.checkpoint.com/downloads/resources/cyber-security-report-2022.pdf

Chung, T., van Rijswijk-Deij, R., Chandrasekaran, B., Choffnes, D., Levin, D., Maggs, B. M., Mislove, A., & Wilson, C. (2017). A Longitudinal, End-to-End View of the DNSSEC Ecosystem. *Proceedings of the 26th USENIX Conference on Security Symposium*, 1307–1322.

DGAL. (2021, November 3). *Portal Autárquico - Lista de Municípios*. http://www.portalautarquico.dgal.gov.pt/pt-PT/subsetor-da-administracao-local/entidades-autarquicas/municipios/

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

Gobi, M., Sridevi, R., & 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*.

Gomes, H., Zúquete, A., Dias, G. P., & Marques, F. (2019). Usage of HTTPS by Municipal Websites in Portugal. In Á. Rocha, H. Adeli, L. P. Reis, & S. Costanzo (Eds.), *New Knowledge in Information Systems and Technologies* (pp. 155–164). Springer International Publishing.

Gomes, H., Zúquete, A., Dias, G. P., Marques, F., & Silva, C. (2020). Evolution of HTTPS Usage by Portuguese Municipalities. In Á. Rocha, H. Adeli, L. P. Reis, S. Costanzo, I. Orovic, & F. Moreira (Eds.), *Trends and Innovations in Information Systems and Technologies* (pp. 339–348). Springer International Publishing.

Grenfeldt, M., Olofsson, A., Engström, V., & Lagerström, R. (2021). Attacking Websites Using HTTP Request Smuggling: Empirical Testing of Servers and Proxies. *2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC)*, 173–181. https://doi.org/10.1109/EDOC52215.2021.00028

eitner, P., & Shulman, H. (2021). Injection Attacks Reloaded: Tunnelling Malicious Payloads over {DNS}. *30th USENIX Security Symposium (USENIX Security 21)*, 3165–3182. https://www.usenix.org/conference/usenixsecurity21/presentation/jeitner

Junior, J. (2022). *WebSecureScout* (1.0). https://github.com/jacksonbarreto/WebSecureScout

Júnior, J., & Pinto, P. (2023). *Official-Websites-of-the-Portuguese- Municipalities: v1.0.0*. Zenodo. https://doi.org/10.5281/zenodo.7575903

Lavrenovs, A., & Melón, F. J. R. (2018). HTTP security headers analysis of top one million websites. *2018 10th International Conference on Cyber Conflict (CyCon)*, 345–370. https://doi.org/10.23919/CYCON.2018.8405025

Lian, W., Rescorla, E., Shacham, H., & Savage, S. (2013). Measuring the Practical Impact of DNSSEC Deployment. *Proceedings of the 22nd USENIX Conference on Security*, 573–588.

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

Man, K., & Qian, Z. (2021). DNS Cache Poisoning Attack: Resurrections with Side Channels. *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 3400–3414. https://doi.org/10.1145/3460120.3486219

Nunes, F. (2022, November 30). *Portal das Finanças indisponível. Certificado de segurança passou a validade*. ECO. https://eco.sapo.pt/2022/11/30/portal-das-financas-indisponivel-certificado-de-seguranca-passou-a-validade/

Osterweil, E., Ryan, M., Massey, D., & Zhang, L. (2008). Quantifying the Operational Status of the DNSSEC Deployment. *Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement*, 231–242. https://doi.org/10.1145/1452520.1452548

OWASP Foundation. (n.d.). *OWASP Secure Headers Project*. Retrieved December 28, 2022, from https://owasp.org/www-project-secure-headers/

Portugal. (2019). Lei 58/2019. *Diário Da República*, 3–40.

Portugal. (2021). Decreto-Lei 65/2021. *Diário Da República*, 8–21.

Rescorla, E. (2000). *HTTP Over TLS* (Issue 2818). RFC Editor. https://doi.org/10.17487/RFC2818

Rose, S., Larson, M., Massey, D., Austein, R., & Arends, R. (2005). *DNS Security Introduction and Requirements* (Issue 4033). RFC Editor. https://doi.org/10.17487/RFC4033

Siewert, H., Kretschmer, M., Niemietz, M., & Somorovsky, J. (2022). On the Security of Parsing Security-Relevant HTTP Headers in Modern Browsers. *2022 IEEE Security and Privacy Workshops (SPW)*, 342–352. https://doi.org/10.1109/SPW54247.2022.9833880

Silveira, D. T., & Córdova, F. P. (2009). A pesquisa científica. In *Métodos de pesquisa. Porto Alegre: Editora da UFRGS, pp. 33-44*.

Visoottiviseth, V., & Poonsiri, K. (2019). The Study of DNSSEC Deployment Status in Thailand; The Study of DNSSEC Deployment Status in Thailand. *2019 IEEE 6th Asian Conference on Defence Technology (ACDT)*, 13–18. https://doi.org/10.1109/ACDT47198.2019.9072934

Yang, H., Osterweil, E., Massey, D., Lu, S., & Zhang, L. (2011). Deploying Cryptography in Internet-Scale Systems: A Case Study on DNSSEC. *IEEE Transactions on Dependable and Secure Computing*, *8*(5), 656–669. https://doi.org/10.1109/TDSC.2010.10

How to cite this article:

Júnior, J.; Carneiro, P.; Paiva, S.; & Pinto, P. (2023). An Analysis on the Implementation of Secure Web-Related Protocols in Portuguese City Councils, *International Journal of Marketing, Communication and New Media*, *Special Issue on Cybersecurity, Privacy, and Data Protection*, February 2023, 59-76.