Capacities of Western Balkan Economies (and Their Public Sectors) to Respond to Ransomware Attacks**

Djordje Krivokapić*, Andrea Nikolić* and Ivona Živković*
*Faculty of Organizational Sciences, University of Belgrade, Belgrade, Serbia,
Masaryk University, Brno, Czech Republic
djordje.krivokapic@fon.bg.ac.rs
**This article is supported by the European Regional Development Fund (ERDF) project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

***Abstract* - Ransomware became a global cybersecurity threat affecting not only individuals and private companies, but governments and other public bodies. The paper will firstly introduce the concept of ransomware and emphasize the implications of the global rise of ransomware. Secondly, the paper will provide an overview of the regulatory framework in relation to Ransomware in Western Balkan (WB) economies (Albania, Bosnia and Herzegovina, North Macedonia, Montenegro, and Serbia), while an ethical and practical guidance will be proposed. Then, the paper will briefly present Western Balkan Case Studies, including recent key ransomware attacks occurred in the region. Lastly, the paper will provide recommendations regarding prevention and recovery from the ransom attack focusing on WB region.**

Keywords* - *Ransomware; Western Balkan Economies; Cybersecurity; Legal Regulation; Ethics

I. The concept of ransomware

Ransomware is a malicious software on computer servers that encrypts files and disables normal operation of the information systems, with the aim to get the payment in order to restore access to the system [1]. The payment is usually requested through digital currency in exchange for a decryption key, so anonymous crypto-currency payment systems encourage attackers to easier undertake the ransomware attack. The malicious actors do not discriminate. Ransomware affects both private and public sectors, small companies and big corporations, while covering various industries including health care, finance, government, construction, education, etc. The paper will briefly present the regulatory framework and recent key ransomware attacks that occurred in the Western Balkan region emphasizing the useful takeaways and proposing some recommendations regarding prevention and recovery from the ransom attack.

II. The implications of the global rise of ransomware

Cybersecurity attacks have been a growing concern for businesses and organizations around the world, as attackers are becoming increasingly sophisticated in their tactics. While analysts recorded a significant drop in ransomware attacks between 2016 and 2017, the first half of 2018 saw a 229 percent increase compared to the same interval in previous year [2]. In 2021, the FBI's Internet Crime Complaint Center received 3,729 complaints identified as ransomware costing victims over $49.2 million, and anticipated an increase in critical infrastructure victimization in 2022 [3].

The negative implications of ransomware attacks could be various, from paying the ransom itself to suffering some other significant losses. Furthermore, not only the primary target is affected, but the ransomware could cause harm to numerous stakeholders. The potential losses encompass both direct and indirect damages, including discontinuity of business operations, damage to health, loss of life, loss of income, loss of customers, reputational damage, etc. Therefore, the organization under ransomware attack could face legal suits by previous business partners and consumers asking for the compensation [4].

III. The regulatory framework in relation to Ransomware in Western Balkan

The ultimate question is how legal regulation could effectively regulate ransomware attacks and whether the specific regulation is required or the existing regulation is sufficient. Namely, ransomware attacks are already covered by existing regulation primarily in the areas of cybercrime, information security and data protection, but also in various other sectoral regulations, including telecommunication, energy sector, etc. Those regulations pose certain obligations aimed at prevention of the attack and some obligations, i.e. necessary steps that should be taken after the attack. Moreover, general criminal and civil liability standards could be applied to ransomware cases [5].

Cybercrime regulation is established by the Budapest Convention that has been ratified and implemented by 67 states, including Albania, Bosnia and Herzegovina, Croatia, North Macedonia, Montenegro, and Serbia [6]. It seems that Budapest Convention is sufficiently flexible to deal with the criminal law implications of ransomware. As a type of malware, ransomware is incriminated by "Data interference" (Article 4) and "System interference" (Article 5) [7]. National legal systems in practice complement these provisions with other criminal offenses such as extortion, ransom and coercion as well as national offenses related to cybercrime [8]. As the Budapest Convention turns 20, the Second Additional Protocol to the Convention on enhanced co-operation and the disclosure of electronic evidence is adopted and already signed by 35 states, including the Albania, Croatia, North Macedonia and Montenegro, while Serbia is the only one that did ratification [9].

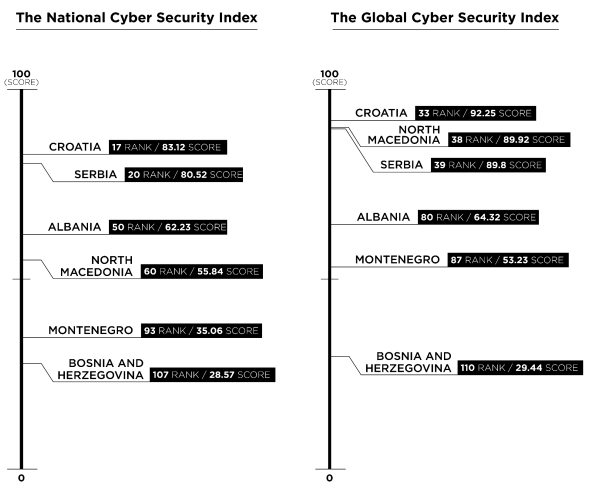
Further, an appropriate level of cyber resilience should be reached by developing various organizational, technical and legal measures regulated by information security, data protection and other sectoral regulation that impose preventative and reactive security measures on operators of information systems.

Directive on Security of Network and Information Systems ("NIS Directive") [10] established legal measures to improve cybersecurity in the EU. Recently, a review of the performance of the Directive has been performed, which led to the improvement by enacting the second version of the Directive in the last days of 2022 [11]. The review of the Directive catalyzed the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mindset by expanding scope of public and private entities subject to the regulation. General Data Protection Regulation (GDPR) [12] on the contrary has a unified approach toward all EU members, and an extraterritorial reach, imposing the application of appropriate technical and organizational measures by all personal data controllers [13]. All these frameworks establish a risk based approach, meaning that the security measures are not set in stone but they require risk assessment, application of appropriate measures and constant monitoring and adaptation. The common tool to perform data security risk assessment is ISO 27001, the international standard for an information security management system [15].

Western Balkan economies are obliged to align their national legislations with the *acquis communautaire*, as a necessary step in the accession process to the EU. North Macedonia and Serbia have harmonized their national laws with GDPR, while Albania has partially harmonized its national law. Bosnia and Herzegovina and Montenegro have not harmonized their laws, but new draft laws harmonized with GDPR are in procedure. On the other hand, the harmonization with the NIS Directive of the Western Balkan economies has a different status. Albania mainly harmonized it by adopting the Law on Cyber security in 2017. In Bosnia there is no law on information security on a national level. However, there is a draft Law on Information Security and Security of Network and Information Systems. The similar situation is in North Macedonia that has no overarching cyber security law, but there have been three Draft Laws, with the latest being published in July 2021 and is in line with the NIS directive. Finally, Montenegro and Serbia are mainly harmonized with the NIS Directive. Namely, Montenegro has adopted Law on Information Security, Law on Determining and Protecting the Critical Infrastructure and Law on Data Secrecy, while Serbia has adopted the Law on Information Security in 2016 which was amended in 2019 to further harmonize with the NIS directive.

Preparedness of WB economies to prevent cyber threats and to manage cyber incidents is assessed by two indexes: National Cyber Security Index [15] and Global Cybersecurity Index [16], which are presented in the table I below.

TABLE I. National and Global Cyber Security Index



The threat of ransomware attacks became an imminent and foreseeable threat due to the rapid increase of ransomware attacks in recent years. Thus, ransomware should be treated with special care, including mandatory conduct of the risk analysis and applying a set of appropriate measures on a case to case basis.

IV. Ethical and other dilemmas regarding paying the ransom

Even though ransom payments are not criminalized per se, it can put the victim in a problematic position [17],

but the question is: is paying a ransom morally right or wrong? A second important question that arises from this ethical dilemma is whether payment of ransom encourages this type of criminal behavior?

On one side by refusing to pay the ransom to the abductors we have potentially discredited their attempts to make an illegal financial gain [18]. However, as it is always the case with moral decision-making, an additional question arises, how to justify a situation in which we refuse to pay for the ransom and lose data that are of enormous material and logistical importance to the organization?

The situation is further complicated in cases where human lives are, directly or indirectly, affected. Medical institutions are, for example, one of the most frequent victims of ransomware attacks. In those cases potential loss of data on medical history or diagnoses could lead to irreversible damage to patients' lives [19]. Also, in an organizational sense, the damage that would be caused to the company could lead to job loss and consequently a series of social and economic problems that would be borne by the employees [20].

In a process of trying to make an ethical decision, of whether to pay for ransom or not we can engage two main ethical approaches that can help us in the decision making process. The first one values the common good rather than putting individuals interests at the forefront. That approach is better known as a consequentialist or utilitarian approach. The main argument that stands behind utilitarian viewpoint in a case of not paying ransom is that when we calculate the consequences of having to pay the ransom it will potentially lead to an increase in the number of such cases in the future [21]. This could be explained by the fact that if we follow the utilitarian logic, we could say that they value the quantity of the aggregate people to be saved from future attacks rather than risking all of them for the sake of one person's interest [22].

Another crucial element that is valuable to mention is related to the problem of reputation (company, stakeholders or a country) in the case of ransom payments. In this case, the calculation is clear: the entity that once pays the ransom is targeted as a favorable victim to which the attackers will return in the future.

On the other hand, if we consider the second most represented school of ethical thought, the decision of whether to pay the ransom or not seems quite simple. Deontological approach is built around a list of morally prohibited acts- simpler acts that are prohibited no matter what [23]. Therefore, a deontological approach can unequivocally lead us to the conclusion that under no circumstances we can pay a ransom. Main principle of deontology says that the action we conduct must be fundamentally morally good as it is. However, this dilemma is not as simple as it seems, especially when it comes to paying a ransom in cases where human lives are involved.

In any case the decision whether to pay the ransom or not depends on many factors. So, we can conclude that there is no unified answer to the primary set question. But there are several factors that we need to consider. The most important ethical consideration is what consequences would be on people’s lives, their personal data, and critical infrastructure. Beside that we need to consider the outcomes of our action on a stakeholder. Also, we need to be prepared for damage mitigation, since whatever decision we choose, it will cause some damage. At the end we need to consider what are the effects of our decision on our reputation. As mentioned, if we choose not to pay, we will probably build a good reputation and potentially save ourselves from future attacks. On the other hand, we need to deal with outcomes that this decision brings and the ability to deal with potential losses.

V. Recent key ransomware attacks in Western Balkan

In recent years, and especially during the second half of 2023., there have been several high-profile incidents that have made headlines in the Western Balkans.

A. Serbia

In March 2020, a ransomware attack on critical infrastructure occurred at the public utility company "Informatika" in Novi Sad, Serbia [24]. This incident was the first publicly known case of a ransomware attack on critical infrastructure in Serbia. The attack resulted in the inability to access Informatika servers, compromising around 2000 accounts, preventing employees from accessing email servers, compromising backup copies, causing city cameras to stop working, and making it impossible to pay through the company's counter or process wages, sick leave records, and other personnel records. The city administration of Novi Sad worked with external IT companies and Informatika's own expert team to create a new hardware-software architecture for the company's information system to prevent any future attacks. Two years later, in June 2022., the Republic

Geodetic Institution (RGI) announced that their recent computer sabotage was carried out from abroad using the Ransomware Phobos virus. The attack has been qualified as an attack on sovereignty of the Republic of Serbia, 28 services of RGI were unavailable for at least a week which caused numerous consequences for citizens, businesses and public administration [25]. No breach of personal data occurred and no ransom note was found in the attack messages according to the RGI [26]. The institution was able to restore the full functionality of the system within a one month, through phased implementation, with the support of external experts from Serbia, EU, USA and Russia [27]. *The compliance of the security teams was closely monitored to ensure the recovery process was not hindered. More than 3000 computers, several hundred servers and more than 3 petabytes of data were thoroughly checked, using three different security systems, to ensure all viruses were cleaned and not left behind, which prevented any subsequent remote activation or reactivation system blockages.* Access to the web services from outside of Serbia is blocked and still active as a preventive measure which reduced daily cyber attacks on RGI on average from 26.000 to only 3 [28].

B. Montenegro

On August 20th, 2022, the well-known hacker group Cuba Ransomware targeted and successfully breached the server infrastructure of the state institutions of Montenegro [29]. The group claims to have obtained a significant amount of data, including financial documents, source code, and correspondence with bank employees. The attack caused widespread disruption, including the inability to use official emails, the unavailability of e-governance services, and the shutdown of the government's website and other web services. The attack also affected critical infrastructure systems, such as the power supply and water supply systems. In response to the attack, the FBI Cyber Action Team, NATO, US, France and the Great Britain embassy have all become involved in the investigation. The consequences of the attack have been severe, with services unavailable for at least 20 days, and at least 2471 workstations and 150 workstations within 11 institutions compromised and locked [30]. The government of Montenegro has also announced that data has been compromised, and at least 500 eGovernment services and numerous email servers are unavailable. The Agency for National Security claimed that coordinated Russian security services are behind the cyber attack, qualifying this attack as politically motivated [31].

C. Bosnia and Herzegovina

Bosnia and Herzegovina has seen an increase in ransomware incidents in recent years, particularly in 2022. In 2020, numerous Bosnian municipalities were under ransomware attacks [32]. In 2022 the Parliament of Bosnia and Herzegovina was attacked by a crypto-locker virus which caused the following consequences: personal workstations of employees were out of operation, mail servers were offline, web pages were unavailable, and certain databases were locked [33]. According to the officials' statements, the Parliament was not the only target: "Bosnia and Herzegovina's Presidency and the Council of Ministers have been targeted too." [34]. These incidents demonstrate the growing threat of cyberattacks in Bosnia and Herzegovina and the Intelligence and Security Agency of Bosnia and Herzegovina has also warned of the increasing risk of cyber attacks in the country and urged all state institutions and private companies to take immediate protective measures. The Federal Police Administration has confirmed that four reports of hacker attacks were received дуринг Аугуст 2023, which is consistent with the recent trend [35].

D. North Macedonia

The website of the Ministry of Education was recently targeted in a hacker attack in September 2022 [36]. The Ministry claimed that the attack did not cause any damage as there are no background databases on the website. Another attack at the same time targeted the Agriculture Ministry by the ransomware group BlackByte. The Ministry confirmed that some documents were compromised during the attack and its work blocked for some time, but it denied having lost any significant documents and data in the process [37].

E. Albania

On July 18, 2022, the Albanian government announced that it had to temporarily close access to online public services and other government websites due to disruptive cyber activity [38]. The incident was investigated by Microsoft Detection and Response Team (DART), which were engaged by the Albanian government. Microsoft stated that they had high confidence that the Iranian government sponsored the cyber-attack, and that the attack was conducted on July 15, 2022, and it caused disruption to government websites and public services [39]. After a wave of cyber-attacks targeting state institutions during 2022, the private data of thousands of

individuals has been published online without any remedy for affected individuals [40].

F. Conclusion

Overall, these case studies, which are only the most prominent cases amongst many, demonstrate the significant impact that cybersecurity attacks can have on critical infrastructure in the region, causing widespread disruption and sometimes even forcing organizations to pay significant ransoms to regain access to their systems. All the attacks were carried out from abroad, highlighting the need for better security measures and international collaboration to prevent such attacks in the future.

Regarding the attacks on the public sector, it is evident that incident response included cybercrime police and prosecution, national security agencies, mechanisms of international cooperation as well as many private actors from country and abroad. Recovery has been performed with more or less success but minimal progress on investigation and prosecution of attackers has been made (or publicly available). Considering that no perpetrator has been prosecuted and that it is unlikely that the cyberattackers will face any legal consequences for their actions, it seems that similar cyber attacks can be expected in the future.

Transparency of the incidents to the public has been very low and only in situations when citizens were already being affected by the attacks. Public reports on the incidents were not made available except in Serbia, where the Commissioner on data protection and National CERT made short statements on their website. The authorities usually did not inform public or expert community on specific consequences of the attacks and their resolutions. Finally, while there are occasional reports from private sector on necessity of ransom payment, there is no such confirmation from public sector. In general, it seems that low and unclear transparency with very limited proactivity further undermined public trust in the capacities of states to counter cyber attacks.

Case studies are packed with examples of the impact of cyber attacks on public sector targets, business entities and citizens. Potential losses are a consequence of business interruptions, incident response costs and third party damages (material and non-material), especially in situations when public sector operations have been interrupted. However, there have been no studies on the assessment of the impact of the attacks. Finally, there is no process available to affected parties to report or claim damages nor any accountability by the governments.

The motivation behind the attacks seems to be double: financial gain but more frequently in the last period of time, we can identify ideological motivation in the context of international relations.

VI. Recommendations regarding prevention and recovery from the ransom attack

The Western Balkan economies should further undertake the regulatory reform and build capacities to respond to the cyber threats. Firstly, all countries should develop their cybersecurity capacities by aligning with the revised NIS Directive. Additionally, they should adopt GDPR standards in their data protection legislation. Finally, they should improve their capacities for international collaboration in the area of cybercrime by conducting ratification of the Second protocol to Budapest convention. However, regulatory changes are just the precondition for building resilience of Western Balkan economies from ransomware and other cyber threats.

National Cyber Security Index and Global Cybersecurity Index represent some sort of a guidelines indicating a need to improve current prevention measures and procedures during a cyber incident. However, the index status did not correspond with real risks and damages suffered by WB economies. For example, Albania was well positioned on the Index scale, but has suffered the greatest damage.

There are several best practices that organizations can follow to help prevent and mitigate the impact of ransomware and other cybersecurity attacks. All organizations need to have preventive cybersecurity measures in place to protect against attacks, and to be prepared to respond if an attack does occur. This includes regular backups, software updates, and staff training. Additionally, having incident response plans in place can help organizations quickly and effectively respond to a ransomware attack if one were to occur. This plan should include steps for identifying, containing, and eradicating the malware, as well as steps for restoring the affected systems and data. It's also important to have a plan for communication and coordination with internal stakeholders as well as external parties such as law enforcement, legal team, and cyber insurance providers.

References

[1] ENISA Threat Landscape an annual report on the status of the cybersecurity threat landscape. 2021 available at: www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[2] Help Net Security, “Ransomware back in big way”, 2018, available at:

www.helpnetsecurity.com/2018/07/11/2018-sonicwall-cyber-threat-report/

[3] FBI, Internet Crime Report 2021, available at: www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Rep- ort.pdf

[4] Krivokapić, Đ., Nikolić, A., Stefanović, A. and Milosavljević, M., "Financial, Accounting and Tax Implications of Ransomware Attack", Studia Iuridica Lublinensia, vol. 32, no. 1, p. 197. 2023. available at: https://journals.umcs.pl/sil/article/view/14957

[5] Krivokapić, Đ., and Nikolić, A., "Legal Obligations and Liability in a Ransomware Attack", Zbornik radova Kopaoničke škole prirodnog prava – Slobodan Perović , pp. 185-192, 2023.

[6] Parties and Observers to the Budapest Convention. available at: www.coe.int/en/web/cybercrime/parties-observers

[7] T-CY Guidance Note #7 of the Explanatory Report of the Budapest Convention, available at: https:// rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTM Content?documentId=09000016802e 70b4

[8] Putnik, N., Milošević, M., and Cvetković, V., "Rensomver kao pretnja bezbednosti - društveni i krivičnopravni aspekti (Ransomware as a Security Threat – Social and Criminal Legislation Aspects)", Sociološki pregled, No. 1, 328-353, 2022.

[9] Signatures and ratifications of Treaty 224. available at: www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

[10] Directive 2016/1148/EU of the European Parliament and of the Council concerning meas- ures for a high common level of security of Network and Information Systems across the Union, OJ C218/1, 2016.

[11] Directive EU 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

[12] Regulation on the protection of natural persons with regard to the processing of person- al data and on the free movement of such data, and repealing Directive 95/46/EC - Data Protection Directive.

[13] Šarkić, N., Prlja, D., Damnjanović K., Marić V., Živković, V., Vodinelić, V., and Mrvić-Petrović, N., Pravo informacionih tehnologija. Pravni fakultet Univerziteta Union and Službeni glasnik, 2009, p. 156.

[14] ISO/IEC 27001 - Information security management, available at: www.iso.org/isoiec-27001-infor- mation-security.html

[15] National Cyber Security Index. available at: https://ncsi.ega.ee/methodology/

[16] Global Cybersecurity Index. available at: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

[17] Krivokapić, Đ., Nikolić, A., Stefanović, A. and Milosavljević, M., "Financial, Accounting and Tax Implications of Ransomware Attack", Studia Iuridica Lublinensia, vol. 32, no. 1, pp.191-211. 2023. available at: https://journals.umcs.pl/sil/article/view/14957

[18] Dutton, Y.M., "Funding Terrorism: The Problem of Ransom Payments", San Diego L. Rev., vol. 53, p.335, 2016. available at: https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1079&context=sdlr

[19] Flashpoint, How Ransomware has become an 'Ethical' Dilemma in the Eastern European Underground, 2017. available at: https://flashpoint.io/blog/ransomware-ethical-dilemma-eastern-european-underground/

[20] Hofmann, T., !How organisations can ethically negotiate ransomware payments!, Network Security, vol. 10, pp.13-17, 2020. available at: https://www.sciencedirect.com/science/article/pii/S1353485820301185

[21] Howard, J.W., "Kidnapped: The Ethics of Paying Ransoms", Journal of Applied Philosophy, vol. 35, pp.675-688, 2018. available at: https://www.sciencedirect.com/science/article/pii/S1353485820301185

[22] Kumar, Y., Baktybayev, B. and Anuarbek, Y., Ransom Dilemma: An ethical problem for the government?, 2021. available at: https://repository.apa.kz/xmlui/bitstream/handle/123456789/587/RANSOM%20DILEMMA%20-%20AN%20ETHICAL%20PROBLEM%20FOR%20THE%20GOVERNMENT.%ea%88%90%e0%b3%a6.pdf?sequence=1&isAllowed=y

[23] Loi, M. and Christen, M., Ethical frameworks for cybersecurity. Springer International Publishing, 2020, pp. 73-95. available at: https://library.oapen.org/bitstream/handle/20.500.12657/47324/9783030290535.pdf?sequenc#page=88

[24] Share Foundation, Kako je Novi Sad otet i zaključan, 2021. available at: www.sharefoundation.info/sr/kako-je-novi-sad-otet-i-zakljucan/

[25] Politika, Hakerski napad na katastar, 2022. available at: www.politika.rs/scc/clanak/509880/Hakerski-napad-na-katastar

[26] The record of the performed inspection supervision. available at: www.sharefoundation.info/wp-content/uploads/Nadzor-RGZ-Zapisnik.pdf

[27] The Interview with the Director of the Republic Geodetic Authority of the Republic of Serbia. available at: www.rgz.gov.rs/content/Vesti/2022/07/Intervju.png

[28] The Director of the Republic Geodetic Authority of the Republic of Serbia at the Kopaonik Business Forum. available at: www.rgz.gov.rs/vesti/5514/vest/direktor-rgz-a-na-kopaonik-biznis-forumu

[29] Bloomberg, Ransomware Attack Sends Montenegro Reaching Out to NATO Partners, 2022. available at: www.bloomberg.com/news/articles/2022-09-01/ransomware-attack-sends-montenegro-reaching-out-to-nato-partners?leadSource=uverify%20wall

[30] Antena M, Camaj: Sajber napad direktno uticao na 150 računara u 10 institucija, kriptovano 17 informacionih sistema, 2022. available at: www.antenam.net/politika/264774-camaj-sajber-napad-direktno-uticao-na-150-racunara-u-10-institucija-kriptovano-17-informacionih-sistema

[31] Security Week, Montenegro Reports Massive Russian Cyberattack Against Govt, 2022. available at: www.securityweek.com/montenegro-reports-massive-russian-cyberattack-against-govt/

[32] Klix, Napadi na općinske baze podataka u FBiH sve učestaliji: Uoči izbora ugroženi matični registri, 2020. available at: https://archive.vn/lyoCU

[33] The record, Bosnia and Herzegovina investigating alleged ransomware attack on parliament, 2022. available at: https://therecord.media/bosnia-and-herzegovina-investigating-alleged-ransomware-attack-on-parliament

[34] N1, Bosnia's state IT systems disabled for two weeks now due to cyber attack, 2022. available at: https://n1info.ba/english/news/hina-bosnias-state-it-systems-disabled-for-two-weeks-now-due-to-cyber-attack/

[35] BHRT, Postoje indicije da bi CIK BiH mogao biti hakovan na dan izbora, 2022. available at: https://bhrt.ba/postoje-indicije-da-bi-cik-bih-mogao-biti-hakovan-na-dan-izbora

[36] Radio Slobodna Evropa, Hakovana web stranica Ministarstva prosvjete i nauke Sjeverne Makedonije, 2022. available at: www.slobodnaevropa.org/a/severna-makedonija-hakeri-ministarstvo-obrazovanja/32027577.html

[37] Balkan Insight, North Macedonia Ministry Denies Covering up Ransomware Attack, 2022. available at: https://balkaninsight.com/2022/09/26/north-macedonia-ministry-denies-covering-up-ransomware-attack/

[38] Mandiant, Likely Iranian Threat Actor Conducts Politically Motivated Disruptive Activity Against Albanian Government Organizations, 2022. available at: www.mandiant.com/resources/blog/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against

[39] Microsoft, Microsoft investigates Iranian attacks against the Albanian government, 2022. available at:

www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

[40] Balkan Insight, Albanians Mull Options as Data Security Takes New Hit, 2023. available at: https://balkaninsight.com/2023/01/25/albanians-mull-options-as-data-security-takes-new-hit