IMPETUS
Center for Internet, Development and Good Governance

Recommendations to address Key Cybersecurity Challenges in North Macedonia

Contents

Date: June 2023

Introduction and Methodology:

The policy brief design gathered more than 30 representatives from different sectors and stakeholders. The researchers gathered relevant and up-to-date information on the cybersecurity landscape in the country, including current policies, regulations, and practices. They were able to Identify the specific cybersecurity challenges faced by the intended audience, whether it's the government, non-governmental sector, media, or other stakeholders. There were several setbacks due to the very recent change in the government in Ministry of Information Society and Administration (MISA), which brought new vision in regards of developing digital eco-system.

Namely, the new Minister pointed out that the establishment of the Digital Agency is actively being worked on, which will focus on digital inclusion, digital public services, which will improve the country's economy, transparency, and accountability of the institutions. Strategic documents are being actively developed with the sole purpose of keeping up with the digital strategy of the EU "Digital Compass".

The process of developing ICT and Cyber Security Strategies is taking place at an accelerated pace, with the help of international donors. However, there is still no active Cybersecurity strategy document.

Regarding the reforms in the public administration, the new Strategy for RJA (2023-2030) has been finalized; In line with our strategic priority for EU membership, this comprehensive eight-year document is designed to guide our country towards European Union membership by 2030; then the Law on Public Sector Employees and the Law on Administrative Officers, which are already in government procedure, were finalized; also active work is being done on the process of reorganization and optimization of the state administration bodies, agencies and inspection services. This should be aligned with the vision and mission of the MISA as a lead champion in workforce development in digitalization of services.

Emphasizing the deep commitment to free media that serve the highest public interest, the minister emphasized that the new Law on Audio and Audiovisual Media Services is already in the parliamentary procedure and is expected to be voted on quickly, the second part of the law will be completed soon, and soon the working group will start working on the Media Law: "*As a result, we will promote transparency, protect freedom of expression and encourage responsible journalism to strengthen the foundations of a democratic society*," said Minister Aliu.

In Identification of Policy Issues there was a period of analyzing the research findings to identify the key policy issues related to cybersecurity. This may include gaps in legislation, inadequate infrastructure, lack of awareness, or coordination challenges.

Therefore, we suggest having two Policy briefs, in accordance with the targeted stakeholder and due to different challenges we have identified and prioritized the policy issues based on their impact and urgency.

In specifying the targeted Audience, we determined two very important group of stakeholders:

1. Policymakers and government officials
2. NGO sector and Media

The developed Recommendations are based on the identified policy issues, with clear and actionable recommendations to address the cybersecurity challenges. Ensure that the recommendations are practical, feasible, and align with the country's context and resources.

Policy Brief 1 for Policymakers and Government officials.

Policy Issue: The growing reliance on digital technologies and the interconnectedness of global networks have led to an increased risk of cyber threats in North Macedonia. This policy brief focuses on addressing key cybersecurity challenges that the country faces, with a particular emphasis on improving the resilience of critical infrastructure and enhancing cybersecurity awareness among the general population.

Target Audience: This policy brief is primarily targeted at the policymakers and government officials of North Macedonia responsible for cybersecurity and critical infrastructure protection. It also aims to inform relevant stakeholders, including private sector organizations, civil society, and the public.

Recommendations:

Enhancing Cybersecurity Legislation, Strategy, Policies and Regulation:

a. Strengthen and update existing cybersecurity laws and regulations to align with international standards and best practices, considering emerging threats and technologies. Adoption of Cybersecurity Strategy should be considered urgently.

b. Establish clear guidelines and requirements for the protection of critical infrastructure, including the identification of essential sectors and the implementation of robust security measures. The recommendation from the General Secretary of the Government to implement cybersecurity training is not considered efficiently enough. Specific standards and guidelines should be drafted and address the vast administrative workforce knowledge and skill improvement.

Strengthening Cybersecurity Governance and Coordination:

a. Establish a centralized national authority or agency responsible for cybersecurity governance and coordination, providing clear leadership, oversight, and coordination of cybersecurity efforts across different sectors.

b. Enhance collaboration and information sharing between government agencies, private sector organizations, and international partners to effectively respond to cyber incidents and share threat intelligence.

Promoting Cybersecurity Awareness and Education:

a. Develop and implement comprehensive cybersecurity awareness programs targeting the general population, businesses, and educational institutions to enhance the understanding of cyber threats, safe online practices, and the importance of reporting incidents.

b. Integrate cybersecurity education and training into the formal education system, with a focus on building the skills and knowledge required for a cyber-resilient workforce.

Encouraging Public-Private Partnerships:

a. Foster closer collaboration between the public and private sectors to jointly address cybersecurity challenges, share best practices, and promote information exchange.

b. Establish incentives, such as tax breaks or grants, to encourage private sector organizations to invest in cybersecurity measures and adopt internationally recognized security standards.

References:

Promovirani program "Digitalna era" MIOA-e omogućit će građanima brze administrativne usluge, (April 2023)

https://www.slobodenpecat.mk/hr/promovirana-programata-digitalna-era-na-mioa-kje-obezbeduva-brzi-administrativni-uslugi-za-gragjanite/

Council of Europe. (2019). Cybersecurity Strategy Guide. Retrieved from https://rm.coe.int/cybersecurity-strategy-guide/1680906055

European Union Agency for Cybersecurity (ENISA). (2020). National Cybersecurity Strategy. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

National Cybersecurity Strategies Guidelines & tools. Retrieved from

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools

North Macedonia National CERT. (2021). Cybersecurity Situation in North Macedonia. Retrieved from https://www.intellinews.com/north-macedonia-steps-up-security-after-cyber-attacks-and-bomb-hoaxes-linked-to-ukraine-war-270736/

World Bank. (2019). The Cybersecurity Capacity Maturity Model for Nations (CMM). Retrieved from https://mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf

Policy Brief 2 for the Non-Governmental Sector and Media in North Macedonia

Policy Issue: The non-governmental sector and media play a crucial role in promoting democracy, human rights, and public discourse in North Macedonia. However, they face significant cybersecurity challenges that threaten their operations, integrity, and the privacy of individuals associated with them. This policy brief focuses on addressing key cybersecurity challenges in the non-governmental sector and media, with specific recommendations to enhance their cybersecurity resilience.

Target Audience: This policy brief is primarily targeted at media regulation and civil society in North Macedonia.

Scope: All media and NGOs that collect, store, process, or transmit sensitive information using electronic devices and networks.

Purpose: The purpose of this policy is to establish guidelines and standards for cybersecurity practices in North Macedonia to protect the media and non-governmental sector's digital assets and systems.

Recommendations:

Establishing Cybersecurity Guidelines and Best Practices:

a. Develop and disseminate cybersecurity guidelines and best practices specifically tailored for non-governmental organizations (NGOs) and media outlets. These guidelines should address topics such as secure communications, data protection, incident response, and staff training.

b. Collaborate with international organizations and civil society representatives to leverage existing resources and expertise in developing comprehensive cybersecurity frameworks.

Enhancing Capacity Building and Training:

a. Provide specialized cybersecurity training programs and workshops for staff members of NGOs and media organizations. These programs should cover essential topics such as phishing awareness, secure online communications, and incident reporting.

b. Foster partnerships between NGOs, media outlets, and cybersecurity professionals to facilitate knowledge exchange, mentorship, and technical support.

Encouraging Information Sharing and Collaboration:

a. Establish platforms or networks where NGOs and media organizations can share information and collaborate on cybersecurity threats and incidents. This will enable them to collectively address common challenges and benefit from shared experiences and expertise.

b. Facilitate partnerships between NGOs, media outlets, and cybersecurity service providers to improve access to threat intelligence, incident response services, and security assessments.

Promoting Legal and Policy Frameworks:

a. Review and update existing laws and regulations to address cybersecurity concerns specific to the non-governmental sector and media organizations. Ensure that legal frameworks strike a balance between protecting individuals' privacy rights and enabling cybersecurity measures to be implemented effectively.

b. Encourage the adoption of self-regulatory mechanisms within the non-governmental sector and media organizations, emphasizing the need for transparent cybersecurity practices and accountability.

References:

European Union Agency for Cybersecurity (ENISA). (2020). Cybersecurity Challenges for NGOs. Retrieved from https://www.enisa.europa.eu/topics/ngo-security

Freedom House. (2021). Freedom in the World 2021 - North Macedonia. Retrieved from https://freedomhouse.org/country/north-macedonia/freedom-world/2021

UN University. Civil Society Organizations Cyber Resilience. Retrieved from https://collections.unu.edu/eserv/UNU:8262/Civil_Society_Organizations_Cyber_Resilience.pdf

The International Republican Institute's, (2023). Retrieved from https://www.iri.org/news/cybersecurity-for-civil-society-a-case-study/

Reviewsed (2022). Cybersecurity Guide for Journalists. Retrieved from https://www.reviewsed.com/cybersecurity-guide-for-journalists/

DCAF Democratic governance challenges of cyber security, (2015)

https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf

"Defending Politically Vulnerable Organizations Online," by CLTC Research Fellow Sean Brooks https://cltc.berkeley.edu/wp-content/uploads/2018/07/CLTC_Defending_PVOs.pdf

GCA, 2019, https://www.globalcyberalliance.org/the-importance-of-civil-society-in-the-world-of-cybersecurity/

Policy Statement:

All entities shall adopt and implement a cybersecurity framework based on industry best practices, such as the NIST Cybersecurity Framework, to protect their digital assets and systems.

All entities shall implement multi-factor authentication for remote access to their networks and systems.

All employees and contractors shall receive regular cybersecurity training to ensure they are aware of the risks and threats associated with cyber-attacks and are equipped to identify and report any security incidents promptly.

All entities shall conduct regular vulnerability assessments and penetration testing to identify and address vulnerabilities in their systems.

All entities shall implement access controls to ensure that only authorized personnel have access to sensitive information.

All entities shall implement data encryption to protect sensitive information at rest and in transit.

All entities shall establish an incident response plan and regularly test it to ensure it is effective in responding to security incidents promptly.

All entities shall report any security incidents promptly to the relevant authorities and take appropriate action to mitigate the impact of the incident.

Review and Revision: This policy will be reviewed periodically and revised in focus groups with the targeted sector as necessary to ensure its effectiveness in protecting Media and NGO sector's digital assets and systems against evolving cybersecurity threats and risks.