NIS2 DIRECTIVE IMPLICATIONS FOR HYDROPOWER PLANTS

Ing. Marian MÁRIK, PhD.
VODOHOSPODÁRSKA VÝSTAVBA, ŠTÁTNY PODNIK, Dunajská 1477/78
GABČÍKOVO, 930 05, +421 905 124 589, marian.marik@vvb.sk
Bc. Gábor JANÍK,
VODOHOSPODÁRSKA VÝSTAVBA, ŠTÁTNY PODNIK, Dunajská 1477/78, GABČÍKOVO, 93005

ANNOTATION
Hydropower companies play a vital role in providing electricity and energy solutions across wide regions. Any disruption to this industry would have far-reaching consequences, affecting both the economy and society and potentially causing environmental repercussions.

This study deals with the cyber security requirements and recommendations for critical infrastructures based on the new Network and Information Security Directive (NIS2), which entered into force on 16 January 2023.

KĽÚČOVÉ SLOVÁ
Cybersecurity, hydropower plant, NIS2

1. INTRODUCTION <<Arial 12 pt., bold>>

The EU NIS2 Directive, adopted in December 2022, represents a pivotal step in bolstering cybersecurity across the European Union. It broadens the scope and introduces stringent measures aimed at enhancing the resilience of critical infrastructure, including the energy sector, which encompasses hydropower plants. Given Slovakia's reliance on hydropower as a renewable energy source, understanding and implementing NIS2 Directive requirements is crucial for maintaining operational security and compliance.

2. SCOPE AND APPLICABILITY <<Arial 12 pt., bold>>

The NIS2 Directive expands its coverage to include more sectors and entities than its predecessor, reflecting the increased complexity and interconnectivity of modern infrastructures. For Slovakia, this means that all medium and large hydropower plants fall within the directive's purview, necessitating robust cybersecurity measures. This includes plants involved in power generation, grid operations, and other critical processes.

3. CORE REQUIREMENTS

3.1 Risk Management and Security Measures

Hydropower plants in Slovakia are required to implement comprehensive risk management processes to address cybersecurity threats. The directive mandates a set of core security measures, including:

- Access Control: Ensuring that only authorized personnel have access to critical systems and data.
- Incident Management: Developing and maintaining effective incident response plans to mitigate the impact of cyber incidents.
- Supply Chain Security: Assessing and managing risks associated with third-party vendors and partners.

3.2 Reporting Obligations

Entities must report significant incidents to national authorities promptly. This includes incidents that lead to substantial operational disruptions or unauthorized access to critical systems. The directive stipulates specific timelines and protocols for incident reporting, which hydropower operators in Slovakia must adhere to in coordination with national cybersecurity agencies.

4. REPORTING OBLIGATIONS

4.1 Enhancing Collaboration

Collaboration between hydropower operators, the Slovak government, and European cybersecurity agencies is vital. Sharing information on threats and vulnerabilities can improve response strategies and enhance overall security posture.

4.2 Training and Awareness

Investing in cybersecurity training for employees at all levels is essential. This includes regular drills and updates on emerging threats, ensuring that staff can recognize and respond to potential cyber risks effectively.

4.3 Technological Upgrades

Hydropower plants should consider modernizing their technological infrastructure to incorporate advanced cybersecurity solutions. This includes deploying intrusion detection systems, firewalls, and other tools designed to safeguard against sophisticated attacks.

5. CONCLUSION

The implementation of the NIS2 Directive in Slovakia's hydropower sector is a critical step towards securing essential services against cyber threats. By adhering to the directive's requirements and adopting recommended practices, hydropower plants can enhance their resilience, ensuring a stable and secure energy supply for the country. Continued collaboration and investment in cybersecurity will be crucial as the landscape of threats continues to evolve..

6. REFERENCES

[1] *EUR-Lex - Access to European Union Law. EU NIS2 Directive: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555*

[2] *European Commission. NIS2 Directive Overview: https://ec.europa.eu/newsroom/cipr/items/753540/en ting Obligations*