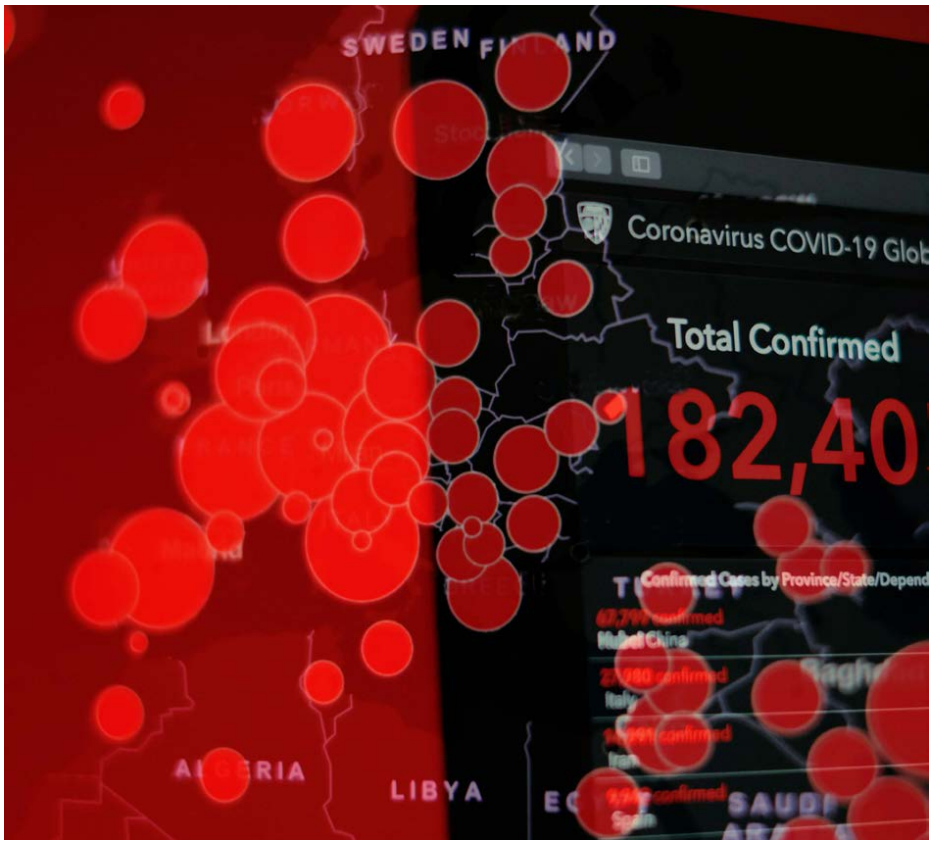
CSupMNE
Straightening Up Cybersecurity Posture of Montenegrin Higher Education system

Co-funded by the Erasmus+ Programme of the European Union

issue# 1, April 2025

newsletter



Word of the Editor

Welcome to the first edition of the CSupMNE newsletter! We're excited to take you on a journey through the ambitious efforts underway to strengthen the cybersecurity resilience of Montenegro's higher education system. This project marks a pivotal step toward modernizing institutional frameworks, boosting digital education quality, and safeguarding students, staff, and partners against the growing landscape of cyber threats. In this and future issues, we'll share project milestones, updates on key activities, expert insights, and the transformative impact of creating a more cyber-aware and digitally secure academic environment across Montenegro. Stay with us as we build a safer future for higher education together.

Prof. dr Ramo Šendelj

Contents:

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project overview

CSupMNE project is designed to conduct sustainable systemic and structural improvements and modernisation of HE system of Montenegro (MNE) aimed on enabling assessment, protection, and management of the ever-increasing business risks and threats that are posed to the MNE HEIs in the digital world, and by doing so will help to ensure their staff, students and partners are protected throughout their journey within the HEIs.

PROJECT REF. NO: ERASMUS-EDU-2024-CBHE-STRAND-3 / ERASMUS2027/ PROJECTID: 101179688

Project sub-objectives:

(1) Increase cyber awareness and build capacities across the MNE HE ecosystem at all levels to facilitate a cultural change to ensure people are continually aware of the business threats and change their perspective on responsibilities around cyber security.

(2) Strengthening the quality of HE through national measure -adopted accreditation standards for digital education, as well as institutional measures- modernized programs in multidisciplinary fields of cyber security, integration of new teaching/learning forms and innovative learning materials

(3) Reform HE operational model at national level to be more proactive in identification and dealing with business risks from cyber threats, by introducing a cyber-security framework which sets the guidelines and governance obligations

(4) Make significant, value-driven changes to HEI infrastructure and implement innovative technology solutions to reduce number and limit the effect of cyber-attack on HEIs' critical information infrastructure

(5) Build capacities and operation mechanisms for proper response and recovery ability to cyber incidents of newly established MNE Academic CSIRT responsible for taking emergency actions and protection of academic community and linked parties, minimizing the risk or impact of the occurred cyber incident

Project background and rationale:

Universities hold critical research data, very important business data and e-services as well as sensitive personal data of numerous staff, students, and alumni. University networks are extraordinarily complex with tens-of-thousands of users logging on daily using a variety of personal devices, hosting a range of cyber security protection. In addition, users log on from a wide range of locations, and have a wide range of motivations for accessing the data that they do. University websites are designed with an inherent level of openness revealing, amongst other data, course tutor, support staff, and research staff details. This is a large and diverse surface area potentially encompassing a huge range of vulnerabilities. This technical landscape creates easier opportunities for perpetrators to launch cyber-attacks, particularly targeting people in jobs that have access to strategic or confidential data. HEIs have become popular cybercrime targets for various adversaries such as state-sponsored actors, criminals, and insiders. Cyberattacks on HE have been on the rise for years, evidence of "actual and potential cyber incidents at institutions of higher education" for the period between 2015-2019 increased by 2880%. HE and research institutions were targeted by an average of 1,065 cyberattacks per week last year—a 75% increase from 2020. The most recent reports show that "Cyber-attacks against HEIs have been increasing in recent years, with the average cost of addressing a cyber-attack amounting to £620,000 in 2021 with the education industry taking the longest to mitigate an attack over all other industries, at over 7.5 hours." According to 2022 Verizon Data Breach Investigations report, "Educational services follows a similar trend to the majority of the other industries; it is experiencing a dramatic increase in Ransomware attacks". All the mentioned facts confirm the belief that HEIs in developed countries do not have sufficiently well-built capacities to respond to contemporary threats in cyberspace. Recent research such as the Cybersecurity Identification and Formulation Study on the Western Balkan (WB) financed by the European Commission confirmed (IPA/2021/429-839, 2022) the general impression that cyber security capacities in Montenegro (MNE) are very limited.

The project resulted with comprehensive assessment report identifying the main aspects characterising the current cybersecurity situation, gaps, and needs:

(1) High-level political commitment to cybersecurity reforms and an increased prioritisation of cybersecurity needs to be adopted and should steam from a recognition that the security of information systems is an integral part of the development of digital services;

(2) Legal framework for cybersecurity-absent or inadequate, therefore manifesting in a deficient legal basis for the activities of the cybersecurity cooperation body, competent authority and CIRT;

(3)Domestic-level cybersecurity risk management frameworks need strengthening, from establishing the capacities and processes necessary for instituting a systematic practice of cyber threat and risk assessments to defining processes for incident reporting and information sharing;

(4) The capacities of the national CIRTs are very limited in terms of both personnel and equipment;

(5) While all WB countries conduct cybersecurity awareness activities to some degree, a strategic or structured approach to cybersecurity awareness raising is, in most cases, not a given; there is no measuring to provide insight into the current levels of societal or target group cybersecurity awareness;

(6) There is varied availability of dedicated graduate and postgraduate cybersecurity education programmes in the WB countries. Limited availability of professors who are qualified to design curricula and teach cybersecurity subjects is broadly reported; and the limited budget of universities and training institutions confines the possibilities of meeting the current market demand for cybersecurity professionals. Improved coordination of efforts between universities regionally and internationally would enable improvement in knowledge exchange in cybersecurity. Some of the educational gaps could also be remedied by academic mentorship programmes, exchange of cybersecurity professors and short-term/ extracurricular education opportunities.

All aforementioned findings are even more relevant when considering academic ecosystem (HEIs and all third-party suppliers) in MNE, which cyber protection is subjected under new MNE Cyber Security Strategy for the period 2022-2026 defining strong support from universities and the Ministry of Education:

(i) Enhancing human capacities in the field of cyber security,

(ii) Establishing efficient mechanisms for responding to cyber incidents,

(iii) Improving prevention measures and cyber security education, and

(iv) Developing and enhancing cooperation with national and international partners.

Furthermore, emphasizing the significance of MNE educational system in establishing a more effective national cyber security system, the MNE Cyber Security Strategy clearly defines the obligation of the Ministry of Education, Science and Innovations to, within its Strategy for the digitization of the educational system, defines the needs for appropriate operational activities with aim to establish:

(i) Strategic Guidance cybersecurity in HEIs: Providing strategic guidance on cybersecurity initiatives, aligning them with organizational goals, and ensuring a holistic and adaptive cybersecurity strategy;

(ii) Human Capacity Development: Designing and enhancing cybersecurity training programs, incorporating the latest industry trends, threat intelligence, and practical exercises to cultivate a skilled and resilient workforce;

(iii) Operational Optimization: Optimizing cybersecurity operations through the implementation of efficient processes, advanced technologies, and collaboration with cross-functional teams for a cohesive and proactive security posture;

(iv) Incident Response Planning: Establish National Academic CSIRT, Developing and refining incident response plans, conducting simulations, and ensuring organizations are well-prepared to handle and recover from cybersecurity incidents;

(v) Industry Collaboration: Facilitating collaboration between educational institutions and industry partners to bridge the gap between cybersecurity education and industry needs, ensuring graduates are job-ready and equipped with relevant skills;

(vi) Continuous Improvement: Implementing a culture of continuous improvement by staying abreast of the latest cybersecurity trends, evaluating the effectiveness of security measures, and recommending enhancements to adapt to evolving threats.

Therefore, CSupMNE project is designed to assess, protect, and manage the ever-increasing business risks and threats that are posed to the MNE HEIs in the digital world, and by doing so will help to ensure their staff, students and partners are protected throughout their journey within the HEIs. The project intervention logic is aimed on supporting sustainable systemic and structural improvements and modernisation of MNE HE system, creation of sustainable operational links with national cyber security ecosystem as well as at international level.

Project partners:

Ministry of Education, Science and Innovation of Montenegro, Montenegro

Cybersecurity in Higher Education: Perspective on Threats and Mitigation

Furtwangen University, Germany

The higher education sector, encompassing universities and colleges, has emerged as a significant target for cyberattacks. This vulnerability stems from the vast and diverse data repositories these institutions maintain, including sensitive personal information of students and staff, valuable intellectual property resulting from research activities, and financial data related to institutional operations. The unique characteristics of the academic environment further exacerbate these risks.

Factors Contributing to University Vulnerability

The cybersecurity landscape of higher education is characterized by a complex interplay of structural, philosophical, and practical challenges that significantly elevate institutional vulnerability to cyber threats. At the core of these vulnerabilities lies the academic sector's traditional commitment to open information exchange and collaborative research, which often manifests in less restrictive network security policies that inadvertently create entry points for malicious actors. As noted by Durojaiye, T., Mersinas, K., & Watling, D (2020), higher education institutions (HEIs) often have lack of enough policies for guiding user behavior and they often prioritize accessibility over strict security protocols, resulting in an inherent tension between openness and security. This inherent openness is compounded by decentralized IT governance structures, where individual departments and schools maintain autonomous control over their technological ecosystems, resulting in inconsistent security practices that undermine comprehensive protective strategies. As highlighted in a study by Liu et al. (2020), universities with centralized IT governance were associated with fewer breaches. Decentralization results in inconsistent security practices, outdated infrastructure, and fragmented incident response capabilities, all of which undermine the effectiveness of institution-wide cybersecurity strategies.

Case Study: The 2023 Cyberattack on Furtwangen University (HFU)

In September 2023, Furtwangen University (HFU) in Germany became the victim of a cyberattack. This incident paralyzed the university's IT infrastructure and disrupted academic and administrative operations for weeks, highlighting the critical need for robust cybersecurity measures in higher education.

Timeline and Immediate Response: The attack occurred on the night of September 18, 2023, as confirmed by HFU in public statements and social media posts. In response to the breach, the university immediately shut down all its systems, including email services, learning platforms, and file storage, in an effort to contain the damage and protect sensitive data (HFU, 2023a). The shutdown was comprehensive as the HFU stated on a dedicated emergency webpage. Access to all services requiring university login credentials was disabled, including off-campus access (Schwarzwälder Bote, 2023). The university quickly informed students and staff through Facebook and their website. The Konstanz Police Headquarters confirmed the attack but noted that a cross-state cybersecurity authority had taken over the investigation. The severity of the incident required external support and the engagement of a specialized IT crisis management team, including input from the Cyber Security Agency of Baden-Württemberg. In a follow-up statement dated September 29, 2023, HFU confirmed that unauthorized access to data had occurred and that data exfiltration was part of the incident. The university disclosed that some of the compromised data could be of significant relevance under data protection law and that it was possible the stolen data could be made accessible to third parties (HFU, 2023b). Under Articles 33 and 34 of the EU General Data Protection Regulation (GDPR), HFU fulfilled its obligation to notify both the State Data Protection Commissioner (LfDI) and affected individuals.

Mitigation and Recovery Strategy: Following the attack, HFU began an extensive and phased rebuilding of its IT infrastructure. According to the university, this includes both technical and organizational reforms, informed by recommendations from external cybersecurity consultants, law enforcement, and government agencies. The HFU cyberattack offers several important insights into the state of cybersecurity in higher education:

1. Preparedness is essential: HFU's quick shutdown of systems likely prevented further escalation. This highlights the value of having pre-established incident response plans and decision-making protocols.
2. Communication matters: The university's frequent updates and open acknowledgment of

the breach helped maintain trust among students and staff during a disruptive period.

3. Data protection must be proactive: The delayed discovery of data exfiltration underscores the critical importance of network monitoring, threat detection, and data encryption.
4. Recovery is a long-term process: HFU's experience shows that full IT restoration after a major attack can extend over months, especially when rebuilding from scratch.

The HFU case is part of a broader pattern of increasingly sophisticated cyberattacks targeting educational institutions worldwide. These are often perpetrated by state-affiliated groups from Russia and usually pursue hybrid warfare (Center for Strategic & International Studies, 2025). The open and collaborative nature of universities—while essential for academic freedom—also creates vulnerabilities that cybercriminals can exploit.

Conclusion

Cybersecurity in higher education is a complex and evolving challenge that demands a proactive and research-informed approach. Universities must prioritize cybersecurity as an institutional imperative, integrating it into all aspects of their operations. By adopting the evidence-based strategies, educational institutions can significantly reduce their risk profile, protect their valuable assets, and maintain the trust of their stakeholders. Continuous research and adaptation are essential to stay ahead of the ever-changing threat landscape.

References:

Durojaiye, Tai, Konstantinos Mersinas, and Dawn Watling. "What Influences People's View of Cyber Security Culture in Higher Education Institutions? An Empirical Study." *The Sixth International Conference on Cyber-Technologies and Cyber-Systems*. 2020.

Liu, C. W., Huang, P., & Lucas Jr, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from US higher education institutions. *Journal of Management Information Systems*, *37*(3), 758-787.

HFU. (2023a, September 29). *Datenschutzrechtliche Informationen zum Cyberangriff*. Hochschule Furtwangen. Retrieved from: https://www.hs-furtwangen.de/zukunft-erleben/aktuelles/datenschutzrechtliche-informationen-cyberangriff

HFU. (2023b, September 20). *Cyberangriff auf die Hochschule Furtwangen*. Facebook (https://www.facebook.com/profile/100064519911292/search/?q=cyberangriff&locale=en_GB).

Moser, H. (2023, September 20). *Hacker legen IT-Systeme der HFU lahm*. Schwarzwälder Bote. Retrieved from: https://www.schwarzwaelder-bote.de/inhalt.cyberangriff-hochschule-furtwangen-hacker-legen-it-systeme-der-hfu-lahm.8da71f9e-27fb-4da6-92b3-1bac9a5103bf.html

Center for Strategic & International Studies. (2025). *Russia's Shadow War Against the West*. Retrieved from: https://www.csis.org/analysis/russias-shadow-war-against-west

PROJECT NEWS

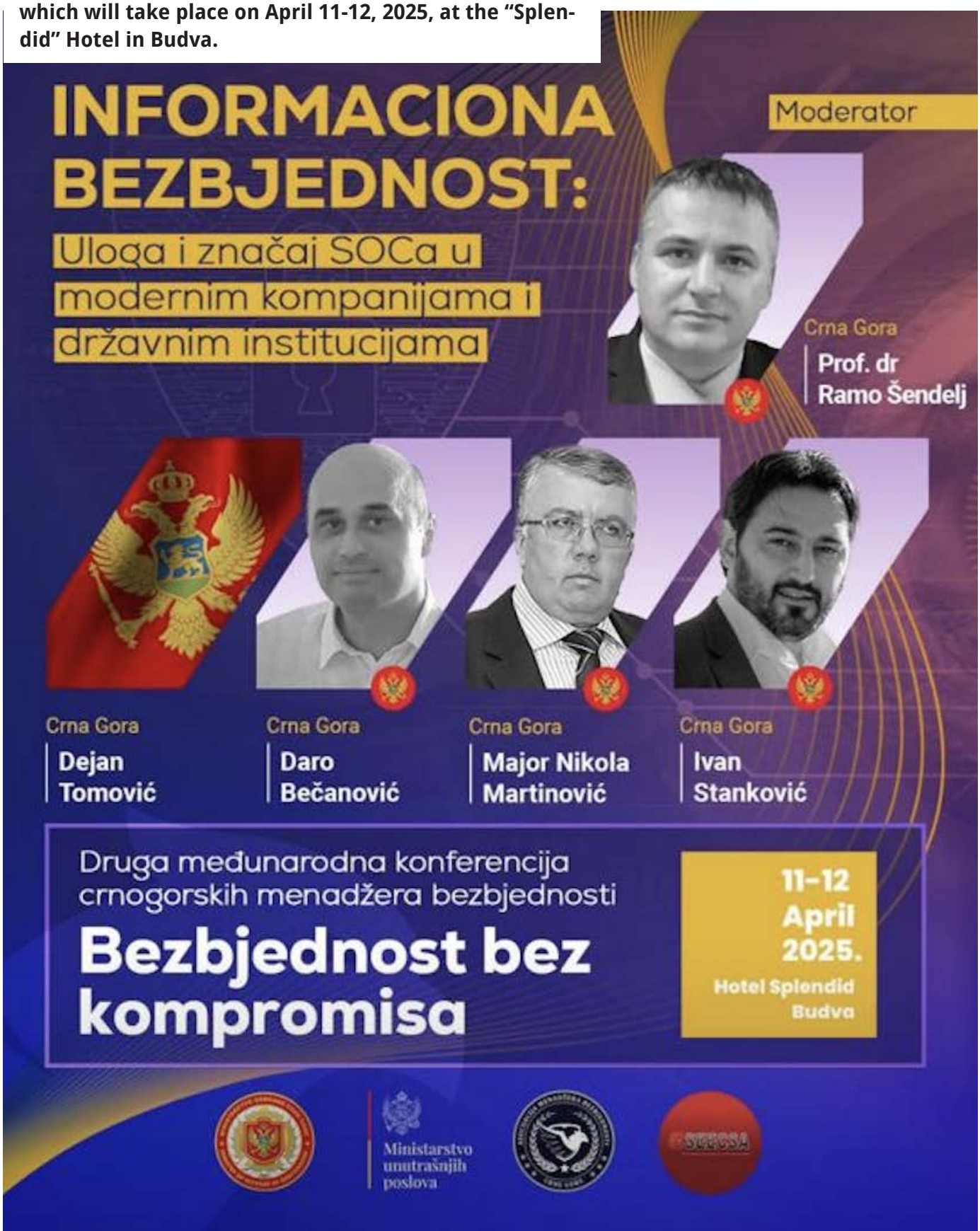
CSupMNE: Strengthening Cybersecurity in the Academic Sector – Sharing Knowledge and Experience in Kraków

On April 9–10, 2025, Kraków will become a hub for experience and knowledge sharing as part of the CSupMNE project, hosted by AGH University of Krakow. The event will bring together experts and practitioners to share experiences and best practices in cybersecurity management within the academic sector. Participants will engage with AGH units responsible for security operations and incident response, and explore the SOCCER program – a strategic initiative focused on enhancing cybersecurity across higher education institutions. A session with the academic team behind the university's Cybersecurity degree program will highlight educational approaches and curriculum design. Additionally, representatives from the Ministry of National Defense's Expert Cybersecurity Training Center will present insights into the development of national professional training frameworks in cybersecurity. The program will feature interactive discussions, presentations, and study visits to AGH's key cybersecurity facilities.

Budva: Security Without Compromise

The Association of Security Managers of Montenegro, in cooperation with the Association of Corporate Security Managers of Southeast Europe (SEECSA), is organizing the Second International Conference of Montenegrin Security Managers, "Security Without Compromise," which will take place on April 11-12, 2025, at the "Splendid" Hotel in Budva.

This conference presents a unique opportunity for experts and professionals in the field of security to come together to explore contemporary challenges and innovative solutions. Through panel discussions, workshops, and various sessions, the focus will be on promoting best practices, new technologies, and strategies that enhance security systems.



The conference theme, "Security Without Compromise," highlights the importance of a proactive approach to security in today's world and will be addressed through five panels:

1. The Strong Hand of Technology: Artificial Intelligence in the Modern Security Environment
2. Industrial Espionage: Foundations of Internal Investigations in Modern Organizations
3. Key Factors in Crisis Management of Critical Infrastructure: Prevention and Response
4. Information Security: The Role and Importance of the SOC (Security Operations Center) in Modern Companies and Government Institutions
5. Effectiveness of Current Security Measures at Airports: What Can Be Improved?

Prof. Dr. Ramo Šendelj, head of the postgraduate master's study program in Information Systems Protection and Cyber Security at the University of Donja Gorica and coordinator of the Erasmus+ project CSupMNE, will moderate the panel "Information Security: The Role and Importance of the SOC (Security Operations Center) in Modern Companies and Government Institutions." During this panel, he will present the planned project activities, as well as the significance and role of the Academic CSIRT, within which a Security Operations Center for higher education institutions will operate.

CYBERSECURITY NEWS

Cybersecurity in Slovenia: Emerging Strategic Trends

In the past few years, Slovenia has made significant progress in strengthening its cybersecurity framework, both due to national ambitions and EU directives. Through the *Digital Slovenia 2030* strategy, cybersecurity has become a cornerstone of the Slovenia's digital transformation.

Between 2023 and 2025, some milestones included the alignment with the EU NIS2 Directive, updates to the Information Security Act, and the launch of the *National Cybersecurity Strategy*. These actions led to the establishment of a National Cybersecurity Center, and expanded cybersecurity education across institutions.

By this year, security tools supported with artificial intelligence have started to be adopted. Many organizations also participate in cyber awareness trainings, which have became standard practice. Other emerging trends in cybersecurity include:

- Security-as-a-Service models that allow organizations to access advanced cybersecurity functionalities without in-house teams.
- Growing importance of supply chain security, with companies evaluating third-party risks and enforcing compliance with cybersecurity standards.
- More companies are turning to cyber insurance as part of their risk management strategy to cover costs associated with data breaches and ransomware incidents.
- Organizations are establishing Incident Response Teams to prepare for and contain cyber threats.

With these actions, Slovenia is building a more resilient digital environment and proactively working on cyber defense.

Subscribe for CSupMNE newsletters:
https://csupmne.me/newsletters.php