POST WEBINAR REPORT

Empowering SMEs: Cybersecurity Strategies for a Secure Digital Future

3 July 2024

Funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SPEAKERS

MODERATOR

Cristina Mancarella
Research Analyst at Trust-IT Services, NERO Comms & Dissemination Lead

KEYNOTE SPEAKER

Athanasios Kosmopoulos
Data Protection Officer at Hellenic Ministry of Digital Governance & National Representative of Greece at the Governing Board of the ECCC

PROJECTS

Charalambos Klitis
R&D Technical Project Manager at eBOS, NERO

Stefan Schauer
Senior Scientist at AIT Austrian Institute of Technology, CyberSecPro

Ulrich Seldeslachts
CEO at LSEC - Leaders in Security, CYSSME

Eduard Paček
Business Development and Partnership Specialist at Excalibur

Konstantinos Votis
Senior Researcher & Director of Visual Analytics Laboratory at CERTH/ITI, smartHEALTH EDIH

SMEs are the backbone of the European economy, crucial for driving innovation, economic growth, and job creation. As the digital landscape evolves with emerging technologies like IoT, AI, and blockchain, SMEs face various cybersecurity threats that can severely affect their operations, financial stability, and reputation. To navigate this rapidly changing threat environment, SMEs must continuously adapt and strengthen their security measures to mitigate potential risks.

On July 3, NERO Cybersecurity hosted its first webinar, focussing on innovative initiatives tailored for small and medium enterprises (SMEs).

This webinar highlighted insights and solutions from our key speakers:

- **Dr. Athanasios Kosmopoulos**, Data Protection Officer at the Hellenic Ministry of Digital Governance and Greece's National Representative on the European Cybersecurity Competence Centre (ECCC) Governing Board, *"An overview of the status of cybersecurity SMEs"*
- **Dr. Charalambos Klitis**, R&D Technical Project Manager at eBOS, *"NERO - Advanced Cybersecurity Awareness Ecosystem for SMEs"*
- **Stefan Schauer**, Senior Scientist at AIT Austrian Institute of Technology, *"CyberSecPro - Agile Cybersecurity Training for Europe's Digital Market"*
- **Ulrich Seldeslachts**, CEO at LSEC - Leaders In Security, *"CYSSME – Digital Europe Uptake CyberSecurity for Micro Enterprises, SMEs in Europe by European innovative CyberSecurity SMEs and associations"*
- **Eduard Paček**, Business Development and Partnership Specialist from Excalibur, *"Excalibur: Seamlessly integrated Privileged Access Management & Multi-Factor Authentication"*
- **Dr. Konstantinos Votis**, Senior Researcher & Director of Visual Analytics Laboratory, Centre for Research and Technology Hellas / Information Technologies Institue (CERTH/ITI , *"smartHEALTH EDIH: Mitigating Cyber Threats Risks Across the Healthcare Ecosystem"*

HIGHLIGHTS

The webinar, "Empowering SMEs: Cybersecurity Strategies for a Secure Digital Future," offered valuable insights and solutions to strengthen cybersecurity resilience. It supported SMEs, public entities, cybersecurity providers, researchers, and industry professionals, helping them develop and implement effective cybersecurity strategies.

Dr. Athanasios Kosmopoulos highlighted a comprehensive approach to SME cybersecurity, emphasizing the need for manageable regulations and support. Key points include:

- The Cyber Resilience Act aims to set essential cybersecurity standards for digital products in the EU while supporting SMEs to meet these standards affordably.
- Regulatory sandboxes are being considered to help SMEs test their cybersecurity products in a controlled environment before market launch.
- SMEs' involvement in standardisation and the use of sandboxes are crucial for innovation and maintaining market competitiveness.

He also discussed new regulations, funding, and support mechanisms to address emerging threats and compliance challenges for SMEs.

The webinar featured innovative cybersecurity solutions and insights from five EC-funded initiatives: NERO, CyberSecPro, CYSSME, Excalibur and smartHEALTH EDIH, dedicated to safeguarding SMEs from cyber threats and advancing overall cybersecurity awareness and resilience.

Dr. Charalambos Klitis, R&D Technical Project Manager at eBOS, presented the overview of the NERO project. NERO aims to **build a comprehensive cybersecurity ecosystem with tools and training to foster a security-first culture in healthcare, transportation and logistics, and finance**. The project will use five interconnected frameworks to enhance cybersecurity, focusing on medical device protection, transportation logistics improvement, and financial system safeguards. NERO will also offer a marketplace for cybersecurity tools and training, integrating with existing systems and addressing sector-specific challenges to boost overall resilience against cyber threats.

Stefan Schauer, Senior Scientist at AIT Austrian Institute of Technology, gave an overview of the CyberSecPro project. This initiative **delivers practical, hands-on cybersecurity training by merging higher education programs with industry needs, focusing on the healthcare, energy, and maritime sectors.** The project aims to enhance cybersecurity competence for SMEs by offering tailored training that addresses specific sector challenges. CyberSecPro is developing a comprehensive curriculum consisting of 12 modules and 75 courses, to propose a new European cybersecurity certification scheme focused on practical skills.

Ulrich Seldeslachts, CEO at LSEC - Leaders In Security, presented the CYSSME project. The CYSSME project aims to **enhance cybersecurity for microenterprises and SMEs by providing tailored advisory, tooling, and mentoring to improve their cybersecurity maturity**. It offers a range of technologies and tools, such as network protection and risk assessments, often at no cost or temporarily, through partnerships in the CYSSME consortium. The project supports organisations across various sectors, including industrial, retail, and high-tech, using assessments and training to help them achieve cybersecurity compliance and maturity goals.

Eduard Paček, Business Development and Partnership Specialist from Excalibur, presented their phone-centric, passwordless solution for privileged access management (PAM) and multi-factor authentication. This cost-effective, user-friendly solution leverages biometrics and geolocation to boost security and streamline the login process, integrating seamlessly with various systems and offering features like holistic reporting and multi-tenancy. He emphasized that, given the diminishing cybersecurity perimeters, maintaining robust remote access security is crucial. **Replacing traditional credentials with a secure, user-friendly login tool can enhance SME security while focusing on essential features and affordability improving implementation speed, user experience, and client satisfaction**.

Dr. Konstantinos Votis, Senior Researcher & Director of Visual Analytics Laboratory, Centre for Research and Technology Hellas / Information Technologies Institue (CERTH/ITI) discussed the smartHEALTH EDIH project. This initiative offers comprehensive cybersecurity services specifically designed for the healthcare sector in Greece. The project focuses on **enhancing cybersecurity by protecting sensitive data, improving threat response, and supporting industry stakeholders**. It includes risk assessments, network security, and data encryption to safeguard medical information. Additionally, the project addresses the security of Internet of Things (IoT) devices and medical equipment, providing solutions for threat detection and response. It also supports SMEs in healthcare through skills training, workshops, seminars, and cyber range solutions to improve their cybersecurity readiness and resilience.

PANEL SESSION

Recent research from the Nero project reveals that while SMEs understand the importance of cybersecurity, they often lack the practical knowledge needed to effectively address their security needs.

Questions for consideration: Is the primary issue a lack of awareness or a deficiency in practical knowledge? What are the most pressing challenges in helping SMEs enhance their cybersecurity preparedness, and how can projects like those presented today tackle these challenges?

During the panel discussion, several key issues and perspectives emerged regarding the cybersecurity challenges faced by SMEs. Below is a summary of the insights shared by the speakers:

Dr. Athanasios Kosmopoulos noted that SMEs across various industries face diverse cybersecurity challenges influenced by their sector, data handling, and digital maturity. Key issues include limited resources for effective cybersecurity, vulnerability to phishing and ransomware—32% of all EU attacks last year were ransomware—complex data privacy regulations like GDPR, and risks from third-party vendors. Cloud security remains a concern, and high-value sectors such as healthcare are at risk from advanced persistent threats due to sensitive data and stringent regulations.

Dr. Kosmopoulos recommended that SMEs invest in cybersecurity improvements, staff training, and regulatory compliance while actively seeking funding opportunities to support these efforts. Addressing these challenges effectively requires tailored, sector-specific strategies and continuous training and compliance efforts.

Dr. Charalambos Klitis highlighted that many SMEs operate under the misconception that they are too small to be targeted by cyberattacks, leading to a general disinterest in cybersecurity. This mindset, common among those less familiar with technology, significantly increases their vulnerability as digital threats advance. To counteract this, it is essential to shift their perspective by raising awareness of the escalating risks, regardless of their size, and to encourage proactive cybersecurity training and measures.

Stefan Schauer highlighted that while many SMEs recognise the presence of cyber threats, they frequently overlook cybersecurity due to limited resources and a primary focus on business growth. This oversight makes them especially vulnerable, as smaller organisations often have inadequate defences. To mitigate this risk, it is crucial to offer SMEs tailored, accessible cybersecurity training and to utilise available funding opportunities to enhance their security measures.

Ulrich Seldeslachts emphasized the need to tailor cybersecurity strategies to the unique needs and maturity levels of SMEs, acknowledging their diversity. He recommended providing targeted support and practical guidance to small, high-tech firms that may lack expertise in secure practices. Seldeslachts also stressed the importance of increasing awareness and training programs to help SMEs better understand and manage cybersecurity risks. Continuous mentoring and practical tools should be offered to assist SMEs in effectively monitoring and maintaining their cybersecurity measures. Regular updates to cybersecurity practices are crucial to prevent reliance on outdated solutions. Finally, leveraging established frameworks like Cyber Essentials can enhance overall cybersecurity compliance and resilience among SMEs.

Eduard Paček highlighted that many companies struggle with limited resources and a lack of awareness about cybersecurity regulations, with GDPR being more widely known compared to other regulations. To address these challenges, he emphasized the need for affordable, user-friendly cybersecurity tools tailored specifically for small businesses. Such tools would help bridge the gap for companies that need to comply with regulations but cannot afford complex systems.

Dr. Konstantinos Votis emphasizes that, beyond updating outdated technology, SMEs require enhanced access to training resources to effectively understand and address cybersecurity threats. He points out that challenges differ across various sectors, making a one-size-fits-all approach insufficient. Therefore, it is crucial to develop tailored cybersecurity tools and solutions that cater to the specific needs of different industries, including healthcare, retail, and Industry 4.0.

DOWNLOAD THE PRESENTATIONS

WEBINAR IN NUMBERS

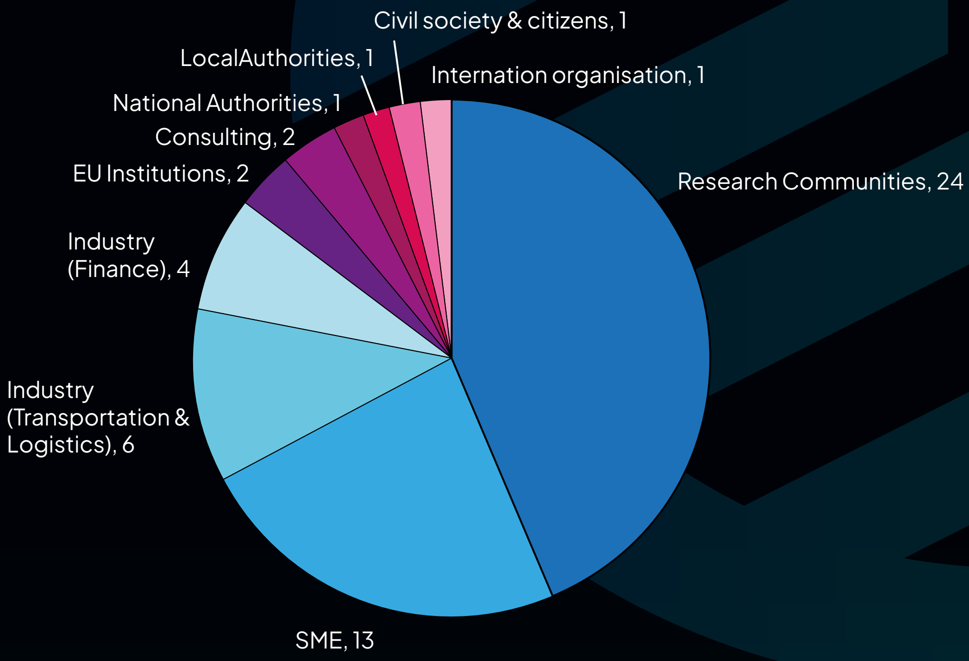
The webinar was free to attend and attracted a diverse audience from various disciplines, including representatives from SMEs, public entities, cybersecurity providers, researcher, and industry professionals and organisations from across Europe. Below, you'll discover a detailed breakdown of registrants and attendees categorised by stakeholder type.

Registrants: 55

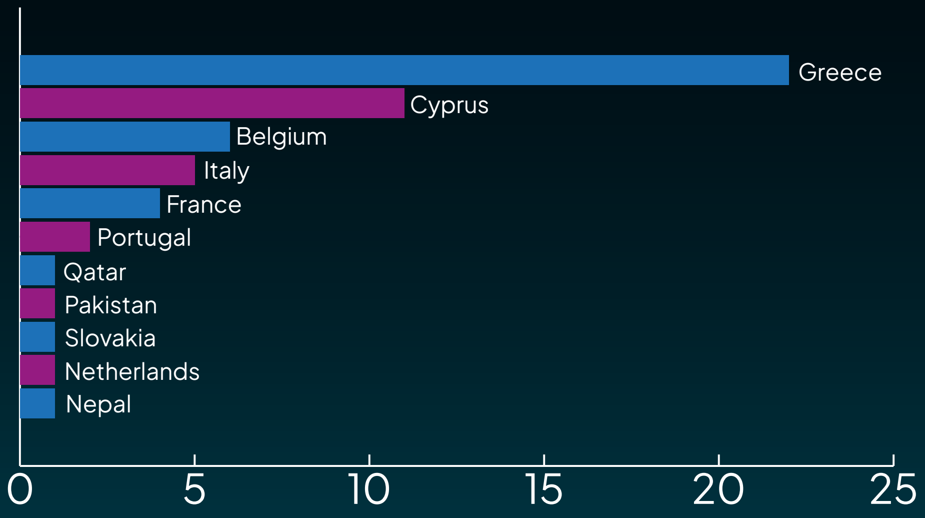
Attendees: 49

Duration: 90 mins

REGISTRANTS BY STAKEHOLDER GROUP



COUNTRY REPRESENTATION



WATCH THE RECORDING

@NEROcybersec

@NEROcybersec

nerocybersecurity.eu

company/nero-cybersecurity/

zenodo/communities/nerocybersec