EUROPEAN CLUSTER
COLLABORATION PLATFORM

Collaborate to protect: Network intelligence for cybersecurity

Summary

EUCLUSTERS TALKS

EU Clusters Talks
18 October 2023, 8:30 – 9:45 CET

An initiative of the European Union

Collaborate to protect: Network intelligence for cybersecurity

The European Cluster Collaboration Platform organised this EU Clusters Talk on 18 October, 8:30 – 9:45 CET, to raise awareness to the importance of having protective mechanisms in place and learn how SMEs and clusters are handling cybersecurity in their network.

Agenda of the meeting

Moderation: Chris Burns

1. News from the European Cluster Collaboration Platform
   Nina Hoppmann, team member, European Cluster Collaboration Platform
2. EU cybersecurity policies
   Boryana Hristova-Ilieva, Legal Officer, DG CNECT, European Commission
3. Panel debate
   Filippo Bosi, CEO, Imola Informatica, Vice-President of Clust-ER Innovate
   Miroslav Lučinskij, CEO, Critical Security, member of BCCS Cluster
   Stelian Brad, Professor in Intelligent Robotics and Innovation Engineering, President Cluj IT Cluster
   Teofilo Redondo, Manager of Technology and Innovation, Bidaidea, member of AEI Ciberseguridad
4. Funding opportunities
   Nina Hoppmann, team member of the European Cluster Collaboration Platform

Key messages

- The Cyber Resilience Act will be relevant for 99% of the hardware manufacturers and software developers in the EU market.
- Operational resilience and robust frameworks are the key to SMEs' safety against cyber-attacks.
- Basic tools, awareness, and education are needed across all organisation levels.
- Red teaming and specific tools can help in being prepared, as they simulate attacks and help practice defence strategies in a controlled setting.
- Clusters can be a platform to support their companies in their cybersecurity by providing expertise and exchanges.
- Technology advancements mean a constant adaptation of an organisation's cybersecurity policies.

1. News from the European Cluster Collaboration Platform

Nina Hoppmann, team member, European Cluster Collaboration Platform

The following news item were presented:

1. Public consultation: Reporting requirements for businesses and Member States to reduce administrative burden
2. Online Training Session on "InvestEU in action" offered by the Enterprise Europe Network
3. Invitation to join the European SME Week 2023 in Bilbao, Spain
4. Invitation to come to the EU Raw Materials Week 2023 in Brussels
5. Register to attend the next "Clusters meet Regions" events
6. Join the ECCP discussion groups on LinkedIn

2. EU cybersecurity policies

Boryana Hristova-Ilieva, Legal Officer, DG CNECT, European Commission

Boryana Hristova-Ilieva explained the evolution of EU cybersecurity legislation, starting with the NIS (Network and Information Systems) Directive in 2016, which established foundational cybersecurity protocols across the EU. This directive required Member States to create national cybersecurity authorities and strategies. The **NIS 2 Directive**, which entered into force in January 2023, updates the original NIS Directive, addressing the increased cybersecurity risks and digitalisation accelerated by events like COVID-19 and the war in Ukraine. It includes provisions for incident handling, business continuity, and supply chain security. The three main pillars are Member State capabilities, risk management and reporting, and cooperation and information exchange. The NIS 2 Directive pays special attention to SMEs, incorporating them into national cybersecurity strategies and ensuring they receive support and assistance. It recognises the critical role of SMEs in the economy and the unique challenges they face in cybersecurity.

The **Cyber Resilience Act** was proposed in September 2022. This act aims to strengthen supply chain security by setting cybersecurity standards for products with digital elements, from design to development stages. The act proposes cybersecurity rules for the placing on the market of hardware and software (objective-driven, technology-neutral and risk-based essential cybersecurity requirements), and defines obligations for manufacturers, distributors and importers. The act will be relevant for **99% of the hardware manufacturers and software developers in the EU market** and have a positive impact on the competitiveness and internal market. The estimation for the reduction of cybersecurity incidents for businesses lies between 20 % and 33 %.

Boryana Hristova-Ilieva stressed that the EU offers **various support mechanisms for SMEs**, including Horizon Europe, Digital Europe programs, and digital innovation hubs. The goal is to strengthen cybersecurity while protecting and supporting the industry.

3. Panel debate

The panellists discussed the challenges and strategies in cybersecurity for SMEs, existing tools and joining forces to deal with cyber-attacks, the need for education across all organisation levels, and government programmes and regulations for a strong framework.

A key focus of the discussion was operational resilience, which is of particular importance for SMEs. Filippo Bosi emphasised the need for SMEs to establish **robust frameworks** to not only withstand cyberattacks but also to maintain business operations during such events. His expertise, drawn from years in financial services advisory, shows that only few SMEs are really prepared, and that it is imperative for them to have a system in place, especially with the advancing digitalisation.

Miroslav Lučinskij presented the 'Cyber Range' tool, a virtualised environment developed through a collaborative effort involving universities and companies. This tool is designed to allow SMEs to **simulate and practice** defence strategies in a controlled setting, reflecting the practical needs of these enterprises in dealing with cybersecurity threats. In general, the concept of **red teaming** can be an effective strategy for testing and enhancing an organisation's cyber defences. This approach, which involves simulated cyberattacks, helps organisations identify vulnerabilities and improve their security measures.

All speakers are members of clusters, and they agreed that clusters, as collaborative networks, can help foster a supportive environment for SMEs in cybersecurity. The clusters enable knowledge sharing, awareness raising, and access to essential tools and resources. They bridge the gap between academia and industry, creating a **synergistic platform** for addressing cybersecurity challenges.

The speakers also underlined the **necessity of basic tools** like password managers and the importance of employee awareness to prevent attacks. These foundational elements are often overlooked but are crucial in building a strong first line of defence against cyber threats. All speakers stressed the importance of **awareness and training** in cybersecurity across all organisational levels. Educating employees and professionals about potential cyber threats and appropriate responses is vital for maintaining a secure digital environment.

Furthermore, the panellists emphasised the importance of implementing robust **cybersecurity policies** within organisations. Such policies provide a structured approach to managing and mitigating cyber risks, aligning with best practices and regulatory requirements. Looking at the rapid advancement of artificial intelligence and its potential implications for cybersecurity, the panellists highlighted the need for **ongoing vigilance and adaptation** of cybersecurity strategies to keep pace with technological advancements.

Government support and effective regulations were identified as crucial in enhancing cybersecurity for SMEs. The panellists cited examples like Israel's government-led cybersecurity education programs and the importance of cyber insurance, showcasing how top-down initiatives can significantly impact SMEs' cybersecurity posture.

Addressing the financial constraints faced by SMEs, the speakers suggested solutions such as cost-sharing through clusters and access to **free or open-source tools**. These approaches can help SMEs initiate their cybersecurity measures without substantial financial burdens.

4. Funding opportunities

Nina Hoppmann, team member of the European Cluster Collaboration Platform

Closing the EU Clusters Talk, Nina Hoppmann shared the following examples of funding opportunities:

1. Supporting competitiveness and innovation potential of SMEs; deadline 7 November 2023
2. EIT Manufacturing: Empowering SMEs Call; deadline 11 December 2023
3. Opportunities for SMEs: Calls from Euroclusters; published on European Cluster Collaboration Platform
4. Invitation to join the C2Labs to work on project proposals