ACTION PLAN

Estonian Information System Authority / Riigi Infosüsteemi Amet

CYBER
Interreg Europe

European Union
European Regional
Development Fund

The CYBER involves nine institutional partners, representing different EU countries and regions:

- **Bretagne Development Innovation agency (France),**
- **Institute for Business Competitiveness of Castilla y León (Spain),**
- **Tuscan Region (Italy),**
- **Digital Wallonia agency (Belgium),**
- **Brittany Region (France),**
- **Kosice IT Valley (Slovakia),**
- **Chamber of Commerce and Industry of Slovenia (Slovenia),**
- **Estonian Information System Authority (Estonia),**
- **the European Cyber Security Organisation (Belgium).**

CYBER overall objective is to boost competitiveness of cybersecurity SMEs, thanks to improved public policies. It involves public authorities that can help knock down barriers of market fragmentation, lack of coordination of regional actors and lack of skills. Medium-term aim is to ensure greater coherence between offer and market demand, with a chance to build up skills and merge competences. In the long term, by making the digital world safer, the CYBER initiative contributes to the development of the EU digital market.

During its first phase, CYBER focused on identifying main barriers: lack of coordination between relevant actors, market fragmentation and lack of skills. For each barrier, regional strengths, weaknesses, opportunities and threats were identified, using SWOT analysis. The aim was to identify characteristics and key services that an innovation ecosystem supporting SMEs in the cybersecurity sector should deliver. Based on their level of cyber-development, CYBER partners also identified good practices that represent strengths of their territories and potential solutions to other partners' needs. These good practices fall under two different groups of policy measures: those that support the structure of the cyber innovation ecosystem and those that support advanced services provided within the ecosystem (such as labels, access to public and private funding, capacity building etc.). As a result of this interregional exchange process, good practices and solutions have been selected by partners in a perspective of transfer and adaptation and have been collected into **regional Action Plans**. These Actions Plans represent, for concerned regional authorities, a concrete road map for designing and targeting more and better funding to increase competitiveness of cybersecurity SMEs. Their relevance is also crucial within an EU context, as they provide inputs that can contribute to the European Investment for Growth and Jobs programme and the European Territorial Cooperation programme, as well as to address cybersecurity challenges through the newly proposed NIS2 Directive lenses. Produced by CYBER partners, these Actions Plans are therefore key documents both for regional cooperation across Europe and for policymaking at the EU level.

DETAILS OF THE ACTIONS ENVISAGED

ACTION 1: Development Programme for Implementation of CIIP SMEs Cyber Security Standards and Tools

The background

Based on the territorial needs of Estonia, we have identified a certain lack of operational and risk-assessment activities among the operators of essential services. Thus, we sought for elements from the aforementioned programme, which would be applicable for the SMEs operating in those areas. Although we have not been able to fully transform the mechanism in place in their region (due to needs and differences in respective ecosystems), analysing and discussing the best practices of Slovenia has presented us a wide range of instruments to be used to foster the cybersecurity of SMEs, such as the Public Pen Testing Reports database on GitHub and the OWASP Top Ten Web Application Security Risks toolbox for companies.

Staff exchanges were organised with Slovenia, to inquire about their respective good practice of Cyber Voucher (webinar on business vouchers for CS solutions on April 1st 2020 and bilateral virtual meetings on June 1st and 4th November 2020). As part of the good practices shared between the project partners, Slovenia singled out its policy of Cyber Voucher, which is provided and managed by the Slovenian Enterprise Fund. The purpose of the voucher is to encourage SMEs to increase cybersecurity, thereby increasing their competitiveness, added value, and revenues from sale. The voucher offers co-financing of eligible costs for the system security review and/or penetration test. Micro, small and medium-sized companies with their registered office in the Republic of Slovenia may apply for this voucher. The implementation of the project consists of a system security check and/or penetration test. The applicant has a maximum of 6 months from the date of signing the contract to carry out all the required activities.

The department of Critical Information Infrastructure Protection (CIIP) of the Estonian Information System Authority (project partner) organises regular meet-ups with the operators of essential services, during which the latter inform about the issues they are facing in guaranteeing the high standard of cybersecurity, which is required from them. The CIIP department, based on this information, has identified the areas in need of improvement. As the CIIP department representatives have been involved in the activities of CYBER and the staff exchanges mentioned above, they have grasped several ideas, which would become the cornerstone of a new development project for the essential service provider SME-s. This action contributes directly to the strategic priority of the Estonian Cybersecurity Strategy, which stipulates that *the security of essential services is ensured. To this end, we will systematically manage digital interdependencies and cross-border dependencies, and ensure security testing for the information systems underpinning the most critical databases and information systems.* Specifically, the new initiative is directly connected with activity areas no 1.2 "*Prevention of, readiness for and management of incidents and crises*" and no 1.3 "*Integral management of the sector and shaping a cohesive community*" of the Estonian Cybersecurity Strategy.

The action

RIA has carried out a pilot development programme for water companies. The aim of the programme is to increase the awareness and level of cyber security of smaller essential service providers and subjects of the Cybersecurity Act.

The development programme is based on the Center of Internet Security TOP 20 (CIS20) measures, from which each participating company selects the most suitable and necessary, based on their needs and idiosyncrasies. The role of RIA is advisory and supportive, all the choices are made by each company according to their own risks and opportunities. Also, the Slovenian Cyber Voucher programme offers for their SMEs not only penetration testing and security checks, but their role is also to give advice on correcting weaknesses found during the process. Differing from the Slovenian Cyber Voucher, RIA as the national cybersecurity agency, does not offer financial aid to companies (as opposed to its Slovenian counterpart, which has that particular area of activity), but assists with its own expertise. The development programme was set up to be as practical as possible for entities, where cybersecurity is often the responsibility of a sole employee, who also oversees the management of physical infrastructure. For the purposes of this programme, RIA ordered the translation of the Centre for Internet Security Top 20 Controls and Resources manual from English to Estonian. At the beginning of the programme, the status quo of the companies' cybersecurity was assessed by the expert of RIA, together with the company's employees. If the companies deemed it necessary, the expert from RIA helped them to guide the first steps to implement the basic processes necessary for ensuring cyber security. In the latter phase of the programme, the expert proposed suitable tools (ie. automation processes) for simplifying IT administration and ensuring cyber security.

The main activities of the programme:

1) Assessment of the current situation of the company against CIS20;

2) Regular meetings with water companies to discuss and share experiences on the implementation of measures and appropriate tools;

3) Implementation of measures by companies;

4) Post evaluation of the company and feedback to the pilot programme.

We have implemented the same policy management methodology as the Slovenian colleagues for this action, namely in communication and the post evaluation approach. Our experts analysed the manner Slovenian counterparts have used toolboxes and pen testing practices and as a consequence, based on the needs and differences for the Estonian ecosystem, we decided to initially implement the CIS 20 measures, which were in our opinion more concise for companies with limited financial and human resources. The exact manuals (OWASP, GitHub databases) used by the Slovenian counterparts will be up for consideration for the follow-up activities.

Players involved

The Ministry of Economic Affairs and Communication – overviewing the implementation of the Cybersecurity Strategy, approving the actions of the Information System Authority.

The Information System Authority – drafting the action plan; communication with the stakeholders; implementing the action and providing the courses.

Estonian water companies – target group, participating in the action and giving feedback.

Timeframe

Participation in the development programme is free for the companies and the programme lasted from May to December 2020.

2020 first quarter – drafting and examining the means for activities.

2020 second quarter – concluding cooperation and confidential agreements with companies, beginning of the first actions with the target group.

2020 third and fourth quarters - Implementation of the action.

2021 first semester - Measurement of the result, conclusions and possible further actions. In January 2021, the cybersecurity or IT experts of the participating companies provided overview of the programme to the executives of the respective companies. In February 2021, RIA gathered feedback from the companies in regards to the measures taken after the completion of the

March 9th 2020 to inquire further details about the organisation of that forum. The action serves the Estonian Cybersecurity Strategy's strategic priority: *We will support effective cooperation between state, academia and the private sector's key partners. To this end, we will launch a cluster that facilitates both domestic and international cooperation.* Cyberbreakfast initiative contributes directly to the activity area no 2.1 "Supporting and promoting cybersecurity R&D and research-based enterprises" of *the strategy.*

The action

Thanks to the mapping done for the CYBER project regarding the Estonian cybersecurity ecosystem and its SMEs, we are able to set up a community, who would regularly convene to discuss the ongoing R&D issues, opportunities for funding to participate in the EU projects, etc. Academia and public sector are also involved, but they would direct the message they deliver to the SMEs.

The Estonian Information System Authority, alongside with the Estonian Information Security Association (EISA), as the organisers of those events, would invite speakers, who would speak about concrete technological advancements. The events will take place in various locations, as the role of the host of the event will rotate between SMEs. The company hosting the event will be able to introduce the activities of the company to other participants.

Players involved

The Ministry of Economic Affairs and Communication – overviewing the implementation of the Cybersecurity Strategy, approving the actions of the Information System Authority.

The Information System Authority – drafting the action plan; communication with the stakeholders; implementing the action and organising the meet-ups.

Estonian Information Security Association – an association uniting cybersecurity SME-s and academia, which will be the co-organiser of the events. Their input will be of vital importance, as they have the necessary network within SME-s.

Regional SME-s – participating in the meetings, providing their input, comments and raising topics to discuss.

Cybersecurity experts – giving lectures on selected issues.

Timeframe

2020 first semester – drafting and examining the means for activities.

2020 second semester – first meet-ups.

2021 – 2023 (and beyond) - Implementation of the action.

First event took place on 10 September 2020, the second one was planned for 10 November 2020, but was cancelled due to COVID-19-related restrictions. The next meeting is planned as soon as the sanitary situation allows.

Cost

Expected cost is indicatively 1000€ per year. Costs will be dedicated mostly to provide catering service. Although we count on attracting speakers to the event who take no fees, we have a small buffer in case a wanted speaker asks for a fee

Funding sources

The Estonian Information System Authority budget, in-kind contributions and contributions for paying for the catering services from SMEs.

Monitoring and indicators

- Number of meet-ups per year (target 6).
- Number of SMEs participating (target by May 2023 is 15).
- Number of experts involved (target by May 2023 is 60).

As RIA is the main organiser of the event, the sustainability of this action falls somewhat under our responsibility. Nevertheless, as SMEs have understood the benefits of this platform, we do believe that these meetings would continue even without RIA-s initiative. The project manager of CYBER from RIA will monitor these activities and indicators.

Date 26.08.2021

Signature

Stamp of the organisation

CYBER
Interreg Europe

European Union
European Regional
Development Fund