Cyber Security for Europe

Policy Recommendation

Support research in SMEs cybersecurity

Context and Findings

SMEs are the backbone of the EU economy and are also among **the most vulnerable groups to cyberattacks and cybercrimes**. The COVID-19 pandemic, which accelerated existing trends in remote work and e-commerce, has made their cybersecurity condition even worse. Additionally, SMEs are **often resource-constrained and suffer many other challenges** that affect their cybersecurity posture.

SMEs might substantially benefit from affordable and free cybersecurity solutions developed through the EU and the Member States-funded research projects. However, **many of these cybersecurity solutions, unfortunately, fall short of their needs**, **while others do not reach the majority of relevant SMEs**.

Therefore, the EU funding instruments and the Member States should **prioritise and encourage cybersecurity projects targeting sector-specific SMEs, as well as those with efficient and actionable plans for attracting participants and disseminating findings**.

The Problem

Small and Medium-sized Enterprises (SMEs) make up a major portion of the European Union (EU) economy[1]. They are, unfortunately, the group that is most vulnerable to cyberattacks and cybercrimes. The COVID-19 pandemic has made the situation even worse with the introduction of a new digital realm where telecommuting and online businesses are increasingly becoming the norm for SMEs' functioning. Additionally, the majority of SMEs also face resource limitations and other difficulties, such as low management awareness and commitment to cybersecurity[2], which restrict their ability to invest and develop capability in cybersecurity.

In such a situation, European SMEs might benefit from free and affordable security solutions resulting from the EU and its Member States' funded projects. However, most of such security solutions do not fulfil the need of SMEs, and some that may meet them do not reach the needful SMEs.

The Scene

Digitalisation and security ought to work together. The digital transformation of European SMEs is progressing rapidly. This transformation has been acknowledged as a critical component of competitiveness for businesses and an engine of growth and welfare for the European economy and territories[3]. While it is obvious that the digitalisation of European SMEs is paramount, there are many aspects that need to be considered in order to realise its opportunities. However, underlying all of that is cybersecurity, which is absolutely fundamental[4]. There is no efficient digitalisation without cybersecurity.

Therefore, cybersecurity should be a core component of SMEs' digital transformation strategy. The European SMEs must realise that the benefit of cybersecurity is not limited to defending businesses against cyber threats but is much more. Cybersecurity can help SMEs to gain customers' and business partners' trust and confidence which are of paramount importance to doing business in the digital era[5]. Additionally, cybersecurity-ready SMEs can have a strategic growth advantage over competitors since they will experience less business disruption as a result of cybersecurity issues and can therefore concentrate their resources on innovation and creating more valuable organisations.

The Implications

SMEs play a crucial role in the European economy and innovation. Thus, they cannot be left unprotected from ever-changing and growing cyber threats. This becomes more critical if considering the fact that for many SMEs, essentially, small-SME and micro-SME, sustaining a major cyberattack can be tremendously difficult; reputational damage, financial losses, and penalties levied after a cyber-attack could force them out of business. Additionally, many SMEs are connected to one another, as well as with large enterprises. Therefore, the consequences of a major cyberattack on one SME may not limit to that SME alone but also spread to many other associated businesses and communities.

A rapid progression of digitalisation in European SMEs and continuously growing cyber threats both in quantity and complexity, contribute to increasing attack surface and making SMEs increasingly susceptible. On the other hand, SMEs are still substantially behind in adopting cybersecurity.

The future of European SMEs cannot be deemed secure without significant action and assistance from the EU and the Member States. However, it is unlikely that the situation of the European SMEs could change unless some radical actions are taken to encourage SMEs' participation and engagement in projects as stakeholders, both as information providers and end-users of the results.

Policy Recommendations

We offer the following two policies for EU funding instruments and the Member States to promote and uplift SMEs' cybersecurity and make them more competitive:

1) **Encourage cybersecurity research projects targeting sector-specific SMEs, as well as with efficient and actionable plans to attract relevant SMEs.**

   Building cybersecurity solutions (e.g., cybersecurity technologies, guidelines, approaches, and standards) for SMEs require their satisfactory participation and consultation in the project to understand their requirements. This is of utmost significance for the project's outcomes and success. There are also industry-specific security needs. While certain threats are global in nature, many SMEs must fight against specialized threat actors. For example, healthcare must protect IT infrastructure, patient data, and smart medical devices, while retail & wholesale must secure the customer and payment card data. However, it appears that the majority of cybersecurity projects funded by the EU and its Members States are aimed at SMEs as a whole than at specific sectors. The same has been evident from the low usefulness and applicability of most project-produced cybersecurity solutions for SMEs that are funded by the EU and its Member States[2]. This poor-quality results from projects can also be attributed to the enormous difficulties of attracting and engaging with SMEs, which most projects do not adequately consider and plan for. The two potential strategies to address the quality issue of cybersecurity solutions produced from projects are as follows:

   - It is well known and often has been acknowledged that the majority of SMEs lack adequate human and financial resources. Cybersecurity projects should therefore be well-publicised with the reassurance of clear and immediate benefits for the participating SMEs.
   - Cybersecurity research projects should target sector-specific SMEs and have efficient and actionable plans to attract a large number of participants or relevant SMEs.

2) **Encourage cybersecurity research projects with efficient and actionable plans for large-scale dissemination of their results to relevant SMEs.**

   The cybersecurity solutions developed by projects supported by the EU and its Member States should ideally reach and be adopted by all applicable SMEs to make the best use of the resources and efforts invested in them. Every relevant SME in the region is entitled to use and benefit from these project-produced cybersecurity resources. However, most EU and its Member States funded projects struggle to reach a few hundred, and in exceptional cases to a few thousand SMEs (this is insignificant given the number of SMEs in the millions) with the present dissemination methods or practices. Particularly, such projects to reach out to micro and small SMEs, who could greatly benefit from the project-produced cybersecurity solutions, as well as make their results accessible and attractive for them is a key challenge. These projects cannot continue to operate on the premise that relevant SMEs will find and utilise the cybersecurity solutions they have produced simply because these resources have been made available online on the websites. Therefore, cybersecurity research projects should have efficient and actionable plans for large-scale dissemination of their results, and such projects should receive high priority for funding.

References

[1] European Commission. (2022). Entrepreneurship and small and medium-sized enterprises (SMEs), https://single-market-economy.ec.europa.eu/smes_en

[2] ENISA (June 2021). Cybersecurity for SMES: Challenges and recommendations, ISBN: 978-92-9204-409-1 – DOI: 10.2824/770352

[3] Interreg Europe. (April 2022). Fostering the digital transformation of SMEs, https://www.interregeurope.eu/sites/default/files/2022-04/Policy%20brief%20on%20digital%20transformation.pdf

[4] World Economic Forum. (May 2017). There can be no digital economy without security, https://www.weforum.org/agenda/2017/05/there-can-be-nodigital-economy-without-security/

[5] G. Lloyd (February 2020). The business benefits of cyber security for SMEs, Computer Fraud & Security, Elsevier.

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact Person : Sunil Chaudhary sunil.chaudhary@ntnu.no | cybersec4europe.eu

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the view of the authors, and the Commission is not responsible for any use that may be made of the information it contains.