|  |  |  |
| --- | --- | --- |
|  | ***Introduction – TTC Working Group 9 chairs (Mrs. Lucilla SIOLI, Director DG CONNECT A, European Commission; Mrs. Valentina SUPERTI, Director DG GROW G, European Commission; Mr David DE FALCO, U.S. Department of Commerce Deputy Assistant Secretary, Office of Europe and Eurasia, International Trade Administration, U.S. Department of Commerce)***  Mrs. SUPERTI welcomed the participant and wished for a fruitful meeting. She stated that **“EU-U.S. Trade and Technology Council WG 9 Webinar on Cybersecurity”** is the first webinar dedicated to the topic of cybersecurity for SMEs both in the EU and in the USA. She explained that the Trade and Technology Cooperation (TTC) platform is intended to boost cooperation between the EU and the USA. It is used also for accessing and promoting digital tools for SMEs in the EU and USA.  ***Part 1 - Training for SMEs on Cybersecurity and Q&A (Mr Lucio Gonzalez JIMENEZ, Manager at*** [***SGS Brightsight CyberLab***](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.brightsight.com%2F&data=04%7C01%7Cveronica.bari%40feani.org%7C7399f61e078a44a2936708d9dc1ac77a%7C7c80ce84cf9d47b68e752cfb95c41646%7C0%7C0%7C637782830227006788%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=fuz3ZevIoZyYGNknDrUNpfX24Pe%2B%2FS753p0ETaq%2F7Pg%3D&reserved=0) ***– Mr MJ SHOER)***  *Topic 1: Introduction to cybersecurity, Types of attackers and motivation, Attacks, Security threats and taxonomy*  Mr JIMENEZ and Mr SHOER stated that technology was useful until threats appeared and that hacking is a quite common practice in SMEs across the world. The concept of cybersecurity has changed our perspective about security. Society became more dependent on technologies, especially during the pandemic.  They explained that in security, 4 phases are recognisable: preventing, detecting, responding, and recovering. In terms of security there are two definitions: one relates to physical security (electronic systems, protection of people and infrastructure, procedures, …) and the other to cyberworld.  In terms of security dimensions, it is important to determine the impact of threats to security or information. Each company should consider five aspects of security and information protection: availability, authenticity, integrity, confidentiality, and traceability.  What should SMEs protect?   * Critical assets (e.g., people, design, ideas, innovations, …). * Infrastructure (that might be business, private and/or mixed). * Any piece of data that may impact significantly in business or private life.     As to attacks, they might be in the form of abusive content, information gathering, intrusion, availability, fraud, vulnerable, availability, harmful content, …There are also several strategies that hackers put in place. The life cycle of a cyber-attack is structured as follows: reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives. As to motivation, hackers are skilled professionals (e.g., intelligence, spies, …) that want to break into company systems and data. They are not the stereotype of a hacker (teenager with a hoodie), they run serious business. They are usually one step ahead of security measures, but they don’t change modus operandi frequently. The target could be a single but highly valuable economic, industrial, etc, … value or a distributed treasure in pieces of small values.  *Topic 2: Introduction to security, organisational, technological, and physical measures, Applicable security measures*  A comprehensive security approach base on the convergence of physical and logical security should be adopted. Comprehensive security relates to assets identification, establishment of a security plan, security manual, procedures, and protocols to put in place, audit. SMEs should create trust, credibility, certified technology, and services, use best practices, value of certification and reliability to be more competitive.  In case of being attacked, it is important to know what to do and who to address. It is of paramount importance to address National Authorities, as well as CERTs/CSIRTS, Service Providers, Security manager. Make sure you have a detailed protection policy and remediation measures in your IT services contracts with platform or Cloud services and to understand how to proceed in case of attack.  As to regulation, the purpose of security regulation is to reduce threats and risks for organisations. There are two types of security regulations: mandatory and voluntary. Voluntary regulations examples are:   * ISO 19600/20000, Management Systems Compliance * ISO 22301, Business Continuity * ISO 27001, Information Security Management Systems * ISO 31000, Risk Management in a general context   Mandatory regulations examples are:   * US Regulation: HIPAA, Gramm-Leach-Bliley Act and Homeland Security Act (including FISMA). Also, federal laws as the Cybersecurity Information Sharing Act (CISA) * EU Regulation: the NIS Directive 2016/1148 of networks and information systems protection. Directive 2016/679 GDPR and the Cybersecurity Act   *Topic 3, Main measures to strengthen your developments, Market Barriers, Regulation*  The major measures to strengthen your developments are time to market; reliable products and services will be more and more preferred to acquire; large companies already started to ensure their supply chains are managed in a secure manner therefore, products and services will be recognised as reliable not only because of a very good performance.  The new scenario for producers is that now we have more vulnerability due to more connectivity. Technological dependence on digital services is increasing. Vendors need secured products. Electronic payments and digital signature or identities are very well developed since around 100 countries had enacted laws making identity cards compulsory. Therefore, vendors and service providers need relevant support to better implement security measures at design stage. There is the need to manage the security life cycle of security functions from the design stage up to disposal.  Over 90% of the market is not prepared and do not have enough digital maturity. SMEs do not put efforts and money is security. The CSA will enable a free circulation of products across European members states and in case of substantial and high security levels also in the American market. Lightweight schemes harmonisation will take more time. Certification schemes will be running on 2022 starting with ICT security named EUCC. Other schemes are under preparation, e.g., Cloud systems, 5G, medical devices.  *Conclusions*  Mr JIMENEZ and Mr SHOER concluded their speech with a series of recommendations to SMEs. The stated that there is the need to reconsider about how security is implemented within organisations, production, and commercial capacities. The market will start requiring and demanding more secure and reliable products. Security is a need in the digital world as much as in the physical world. Regulations are not only to comply but also can bring higher value. SMEs should understand security and the procedures to implement it.  ***Part 2 - Experiences of SMEs with cybersecurity and recommendations, European speakers***  **Mr Matthias KAMPMANN, IT security Cluster Regensburg (Germany)**  [**/cisis12.de/en/**](https://cisis12.de/en/)  Mr KAMPMANN briefly touched upon the “Compliance and Information Security: a 12-step approach, CISIS12”. CISIS12 is based on twelve steps:   1. *Drawing up a policy* 2. *Raising awareness of employees* 3. *Establishing an information security team* 4. *Determining the IT documentation structure* 5. *IT-service management processes* 6. *Compliance, process, and applications* 7. *Analysing the IT structure* 8. *Risk management* 9. *Target actual comparison* 10. *Planning and executing implementation* 11. *Internal audit* 12. *Review*   **Mr. Iulian FLORESCU, Cornerstone Technologies (Romania)**  [**/cornerstoneisit.com/**](https://cornerstoneisit.com/)  Mr. FLORESCU gave some recommendations to SMEs, e.g., using protected Wi-Fi networks (employees and guests); usage of powerful credentials by many people (creating different ones); storing info of customers with regulations with competent authority to check for them.  **Mr Pietro PERLO, I-FEVS (Italy)**  [**/www.ifevs.com/**](https://www.ifevs.com/)  Mr PERLO stated that I-FEVS is the only SME in Europe performing physical crash tests meeting the most stringent regulations. Full frontal, off-axis, lateral, poll, extended fatigue, and crash tests. He added that I-FEVS expect the EU to help SMEs being more cyber-security further promoting collaboration with leading institutions.  **Mr Ulrich SELDESLACHTS, 3if.eu – lsec.eu Digital Innovation Hub (Belgium)**  [**/www.leadersinsecurity.org/3if-be.html**](https://www.leadersinsecurity.org/3if-be.html)  Mr SELDESLACHTS stated that maturity assesments in SMEs are difficult, sicne there is no literacy on cybersecurity. The EU should push more on this matter.  ***Part 2 - Experiences of SMEs with cybersecurity and recommendations, US speakers***  **Mr Kyle NEUMAN, Zeva (U.S.A.)**  [**/www.zevainc.com/**](https://www.zevainc.com/)  Mr NEUMAN stated that identity is the new boundary and that SMEs need to start readdressing their infrastructures in that manner. The focus should be on trust and interoperability across nations. He provided the example of external digital identity security case. How to authenticate a person who is not your employee? Someone you trust but that is not part of the company? Multifactoral authentication reduces the risks in that sense.  **Mr Karl CURETON, Council Exchange Board of Trade (USA)**  [**/www.council.exchange/**](https://www.council.exchange/)  Mr CURETON briefly touched upon two publications: Cybersecurity is Everyone’s Job, A Publication of the National Initiative for Cybersecurity Education Working Group Subgroup on Workforce Management at the National Institute of Standards and Technology. The second one is the Cybersecurity Framework. Both publications are available at these links:   * Cybersecurity is Everyone's Job <https://www.nist.gov/document/cybersecurityiseveryonesjobv10pdf> * Cybersecurity Framework   <https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx>  ***Conclusion - TTC Working Group 9 chairs (Mrs. Lucilla SIOLI and Mrs. Valentina SUPERTI, European Commission, Mr David DE FALCO, U.S. Department of Commerce)***  Mrs. SUPERTI, Mrs. SIOLLI and Mr DE FALCO thanked the participants for their involvement. The next webinar “*SME digital skills and developing strategies for companies”* is scheduled for Tuesday, 8 March 2022. |  |