**RESTART: Resilience and Training for SMEs**

**Case study template**

**(Project Result 3 - Task 3.1. & Task 3.2)**

|  |  |
| --- | --- |
| **Author of the case study:** | Internet Web Solutions |
| **Name of the module to which the case study is assigned:** | Module 3: Cybersecurity in the (home) office |
| **Title of the case study:** | WannaCry: the importance of updates |
| **Description of the case study:** | The European Union Agency for Cybersecurity (reported in May 2017 the first case of cyber cooperation at the European level, in which they worked together with several Member States using the EU Standard Operating Procedures. However, this cooperation was triggered by a complicated situation generated by a massive ransomware.  According to RESTART training, a ransomware is a dangerous type of malware that encrypts files on the device’s hard drive and restricts access to the user, demanding a ransom, usually in cryptocurrencies, in exchange for decrypting the files.  **What happened?**  On Friday 12 May 2017, an event occurred that affected thousands of computers worldwide: the "WannaCry" ransomware attack. In the first few hours of the attack alone, more than 190,000 computers in 150 countries were affected, including critical infrastructure sectors and operators such as healthcare, transport, education, energy, finance and telecommunications, and manufacturing plants in several EU countries had their entire production lines affected.  This came after a message appeared on their computer screens stating that their systems and files would be locked until a ransom payment was made.  **Why did it happen?**  WannaCry affected Microsoft Windows operating system devices by exploiting the MS17-010 vulnerability through the "EternalBlue" code used by the hackers.  Although ransomware usually requires user interaction with something, such as downloading an infected email attachment or visiting a website that downloads malware to the device, WannaCry only required the device to have the vulnerable version of Windows to be infected.  The spread was very fast as it used a protocol called "SMBv1" that communicated with printers and devices connected to the same network to continue infecting, and mainly made files inaccessible and blocked computer programs, demanding a ransom in exchange for restoring normal activity.  **How could it have been avoided?**  Today we know that when all this happened, Windows already had an updated version that fixed the vulnerability that Wannacry exploited. Therefore, the easiest way to avoid this would have been to have the latest security updates and an updated antivirus. In addition, other measures also help to make the impact less or non-existent:   * Having regular backups of all files. * Conducting cybersecurity awareness campaigns with employees. * In case of infection, do not pay the ransom, but contact expert assistance as payment does not guarantee that users will be able to access their files again. |
| **Link for further information:** | <https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level> |
| **Target group of the case study:** | Micro, Small & Medium Enterprises (MSMEs)  Employees of MSMEs  The EU VET ecosystem  Business support organizations |
| **ESCO competencies and skills** | |
| * Transversal skills and competences * Social and emotional skills * Critical thinking * Analytical thinking * Problem-solving * Self-management * Business management * Adaptability * Resilience * Creativity * Networking * Initiative * Flexibility * Openness * Understanding complexity * Cooperation * Empathy * Innovation * Leadership      * Skills * Technological skills * Product marketing * Digital marketing * Digital skills * Communication * Cooperation * Emotional intelligence      * Knowledge * Business management * Online learning and training * Advertising * Cloud computing * Big data * E-commerce * Artificial intelligence * IoT * Digital literacy * Cybersecurity * Data mining and analysis * Sustainability * Well-being * Climate change * Social media management | |