**RESTART: Resiliencia y formación para Pymes**

**Caso de estudio**

**(Resultado del proyecto 3 - Tareas 3.1. y 3.2)**

|  |  |
| --- | --- |
| **Autor del caso de estudio:** | Internet Web Solutions |
| **Nombre del módulo al que se asigna el caso de estudio:** | Módulo 3: Ciberseguridad en la oficina (desde casa) |
| **Título del caso de estudio:** | WannaCry: la importancia de las actualizaciones |
| **Descripción del caso de estudio:** | La Agencia de Ciberseguridad de la Unión Europea (ENISA) informó en mayo de 2017 del primer caso de cooperación cibernética a nivel europeo, en el que colaboraron con varios Estados miembros utilizando los Procedimientos Operativos Estándar de la UE. Sin embargo, esta cooperación se desencadenó por una situación complicada generada por un ransomware masivo.  Según la formación RESTART, un ransomware es un tipo de malware peligroso que cifra los archivos del disco duro del dispositivo y restringe el acceso al usuario, exigiendo un rescate, normalmente en criptodivisas, a cambio de descifrar los archivos.  **¿Qué pasó?**  El viernes 12 de mayo de 2017 se produjo un suceso que afectó a miles de ordenadores en todo el mundo: el ataque del ransomware "WannaCry". Solo en las primeras horas del ataque, más de 190.000 ordenadores de 150 países se vieron afectados, incluidos sectores y operadores de infraestructuras críticas como sanidad, transporte, educación, energía, finanzas y telecomunicaciones, y plantas de fabricación de varios países de la UE vieron afectadas todas sus líneas de producción.  Esto ocurrió después de que apareciera un mensaje en las pantallas de sus ordenadores indicando que sus sistemas y archivos quedarían bloqueados hasta que se pagara un rescate.  **¿Por qué pasó?**  WannaCry afectó a dispositivos con sistema operativo Microsoft Windows aprovechando la vulnerabilidad MS17-010 a través del código "EternalBlue" utilizado por los hackers.  Aunque el ransomware suele requerir la interacción del usuario con algo, como la descarga de un archivo adjunto de correo electrónico infectado o la visita a un sitio web que descarga malware en el dispositivo, WannaCry solo requería que el dispositivo tuviera la versión vulnerable de Windows para infectarse.  La propagación era muy rápida ya que utilizaba un protocolo llamado "SMBv1" que se comunicaba con impresoras y dispositivos conectados a la misma red para seguir infectando, y principalmente hacía inaccesibles los archivos y bloqueaba los programas informáticos, exigiendo un rescate a cambio de restablecer la actividad normal.  **¿Cómo podría haberse evitado?**  Hoy sabemos que cuando todo esto ocurrió, Windows ya tenía una versión actualizada que corregía la vulnerabilidad que aprovechaba Wannacry. Por tanto, la forma más fácil de evitarlo hubiera sido tener las últimas actualizaciones de seguridad y un antivirus actualizado. Además, otras medidas también ayudan a que el impacto sea menor o inexistente son:   * Realizar copias de seguridad periódicas de todos los archivos. * Realizar campañas de concienciación sobre ciberseguridad con los empleados. * En caso de infección, no pagar el rescate, sino contactar con asistencia experta, ya que el pago no garantiza que los usuarios puedan volver a acceder a sus archivos. |
| **Link para más información:** | <https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level> |
| **Grupo objetivo del caso de estudio:** | Microempresas, pequeñas y medianas empresas (MiPymes)  Empleados de MiPymes  Ecosistema de EFP de la UE  Organizaciones de apoyo a las empresas |
| **ESCO competencies and skills** | |
| * Habilidades y competencias transversales * Habilidades sociales y emocionales * Pensamiento crítico * Pensamiento analítico * Resolución de problemas * Autogestión * Gestión de negocio * Adaptabilidad * Resiliencia * Creatividad * Networking * Iniciativa * Flexibilidad * Sinceridad * Comprensión de la complejidad * Cooperación * Empatía * Innovación * Liderazgo      * Habilidades * Habilidades tecnológicas * Marketing de producto * Marketing digital * Habilidades digitales * Comunicación * Cooperación * Inteligencia emocional      * Conocimiento * Gestión de negocio * Aprendizaje y formación online * Publicidad * Computación en la nube * Big data * Comercio electrónico * Inteligencia Artificial * IoT * Alfabetización digital * Ciberseguridad * Minado y análisis de datos * Sostenibilidad * Bienestar * Cambio climático * Gestión de redes sociales | |