CASE- Center for Social and Economic Research

Mapa de las ciberamenazas para las micro, pequeñas y medianas empresas de la UE

Resumen ejecutivo

La Estrategia de la Comisión Europea para las PYMEs para una Europa sostenible y digital reconoció la vulnerabilidad de las PYMEs ante las ciberamenazas e identificó la ciberseguridad como uno de los aspectos clave de la formación digital. También a nivel mundial, las ciberamenazas aparecen entre los principales riesgos globales a corto plazo (Foro Económico Mundial, 2021) y se convierten en una amenaza constante para la mayoría de las empresas en el contexto de la acelerada transformación digital inducida por la crisis de Covid-19 (OCDE, 2021).

Este informe identifica los incidentes basados en Internet, incluyendo el phishing, el malware y los ataques basados en la web, como las ciberamenazas más frecuentes relevantes para las PYMES de la UE. En consonancia con ENISA (2020), otras ciberamenazas importantes incluyen también el spam, la denegación de servicio, el robo de identidad, las violaciones de datos, la amenaza interna, las redes de bots, la manipulación y los daños físicos, la fuga de información, el ciberespionaje y el criptojacking. Al mismo tiempo, mientras que el acceso a Internet y el trabajo a distancia podrían aumentar la exposición de las microempresas a los riesgos de ciberseguridad, el factor humano es otra fuente importante de vulnerabilidad digital, ya que alrededor del 84% de todos los ciberataques en la UE se basan en la ingeniería social para atraer a las personas a divulgar información sensible o hacer clic en el enlace que puede contener archivos maliciosos (ENISA, 2020).

Los análisis por países presentados en este informe subrayan además la creciente importancia de los temas de ciberseguridad a nivel nacional y confirman el relativamente bajo grado de conocimiento sobre ciberseguridad entre las PYMEs. Según los resultados del Eurobarómetro 2020, el porcentaje de encuestados que declararon estar "no bien informados" sobre los riesgos de la ciberdelincuencia fue del 67% en Rumanía e Italia, del 55% en España y del 43% en Polonia. Además, a nivel de empresa, sólo el 7% de las PYMES de Rumanía concienciaron a sus empleados de sus obligaciones en materia de seguridad de las TIC mediante cursos de formación obligatorios. Las PYMES de España, Polonia e Italia, por su parte, obtuvieron resultados más cercanos e incluso superiores a la media de la UE, con cifras del 20%, 30% y 34%, respectivamente. Sin embargo, cuando se considera la brecha entre las PYME y las grandes empresas, Rumanía e Italia tienen una de las brechas más pequeñas de toda la UE: sólo 21 y 23 puntos porcentuales, respectivamente. Si bien España tiene una brecha relativamente más alta, del 27%, logró mantenerse por debajo de la media de la UE-27, de 30 puntos, y de la brecha de 35 puntos registrada en Polonia.

Así pues, las microempresas de la UE suelen ir a la zaga de las grandes empresas en lo que respecta a la concienciación y la preparación para hacer frente a la proliferación de ciberamenazas. Y lo que es más importante, las mayores y más frecuentes ciberamenazas son también aquellas sobre las que el nivel de concienciación en la UE sigue siendo más bajo. La falta de concienciación y compromiso por parte de los directivos, en particular, es el reto común y más citado (ENISA, 2021). Como resultado, solo el 30% de las PYMEs de la UE recurren a algo más que a medidas básicas de ciberseguridad y menos del 30% de las PYMEs de la UE-27 conciencian a sus empleados de sus obligaciones en materia

With the support of the Erasmus+ programme of the European Union. This document and its contents reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union

de seguridad de las TIC a través de cursos de formación obligatorios, casi dos veces menos en comparación con las grandes empresas.

Otros retos estructurales que merman una mayor preparación de las microempresas son la escasa concienciación del personal en materia de ciberseguridad, la inadecuada protección de la información crítica y sensible, la falta de presupuesto, la falta de especialistas en TI y ciberseguridad y la falta de directrices de ciberseguridad adecuadas y específicas para las PYMEs

Una serie de iniciativas a nivel de la UE, que incluyen, entre otras, la Estrategia de Ciberseguridad de la UE, la Agencia de Ciberseguridad de la UE, así como los marcos SMESEC y Make_SME_Digital, permiten colmar las lagunas de cualificación y reforzar la resistencia colectiva frente a las ciberamenazas. Además, las iniciativas nacionales -por ejemplo, la Plataforma Nacional de Ciberseguridad de Polonia y el Programa de Cooperación en Ciberseguridad de PWCyber y el Marco Nacional de Ciberseguridad de Italia y el Consorcio Nacional Interuniversitario de Tecnologías de la Información (CINI)- establecen marcos nacionales de ciberseguridad y apoyan el desarrollo de las competencias digitales a nivel local.

Sin embargo, como se analiza en este informe y en los perfiles individuales de cada país, se necesitan acciones políticas más amplias para abordar la falta sistémica de capacidades de ciberseguridad entre las microempresas de la UE. Estas deberían centrarse en el fortalecimiento:

(i) **concienciación cibernética** entre las microempresas y las PYMEs, promoviendo una mejor comprensión de la ciberseguridad en general y adaptando el contenido y los canales de las campañas de divulgación al contexto de las microempresas y a las necesidades sectoriales.

(ii) **la resiliencia cibernética** de las microempresas y las PYMEs mediante la creación de normas y directrices de ciberseguridad centradas en las microempresas, la promoción del uso de marcos de gestión de riesgos cibernéticos dentro de las microempresas y una mayor accesibilidad a la ciberseguridad.

(iii) **la capacidad de respuesta cibernética** de las microempresas y las PYMEs mediante la promoción de formaciones voluntarias y obligatorias entre los empleados y el apoyo al desarrollo de protocolos de seguridad simplificados.

With the support of the Erasmus+ programme of the European Union. This document and its contents reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union