Ciberdelincuencia contra las empresas en la UE:

Investigación sobre los retos de la denuncia

Informe de política

En las últimas décadas, las tecnologías digitales han impregnado la vida cotidiana de los ciudadanos y las empresas de la UE. La innovación digital ha fomentado el desarrollo socioeconómico en todos los Estados miembros de la UE, pero también ha dado lugar a una mayor exposición de nuestras sociedades a las ciberamenazas y los ciberataques. La ciberseguridad se ha convertido en un activo fundamental para una Europa igital e interconectada, cuya prosperidad y progreso tecnológico dependen cada vez más de la ciberresiliencia.

Han surgido nuevos retos desde el estallido de la pandemia COVID-19, que ha acelerado la digitalización no sólo en Europa sino en todo el mundo. Además, el conflicto en curso en Ucrania ha acentuado aún más la posible exposición de los individuos, las empresas y las instituciones públicas a la ciberdelincuencia. Los confinamientos y el teletrabajo han constituido, y siguen constituyendo, una oportunidad para los ciberdelincuentes.[1] Entre 2021 y 2022, se han identificado como amenazas cibernéticas más prevalentes el ransomware, el malware, las amenazas de ingeniería social, las amenazas contra los datos y la disponibilidad de los mismos (como los ataques DDoS),[2] así como la puesta en peligro de los datos, incluidos los ataques de alto nivel contra instituciones humanitarias y sin ánimo de lucro.[3] El conflicto entre Rusia y Ucrania ha aumentado la preocupación por la ciberseguridad en la UE. La ciberguerra ha sido parte integrante de la invasión rusa, con supuestos ataques a redes

Puntos Clave

- Los dos tipos más comunes de ciberdelitos contra las PYMES en la UE27 son los **virus, el spyware o el malware** (excluyendo el ransomware), seguidos del **phishing, la toma de posesión de cuentas o los ataques de suplantación de identidad**.
- En 2021, **el 44% de los ciberdelitos** sufridos por las pymes de la UE27 **no fueron denunciados a nadie**.
- Entre los principales **factores de infradeclaración** se encuentran el hecho de que **el incidente se haya resuelto internamente**, que el incidente no merezca ser notificado (demasiado trivial) y **la falta de confianza en la policía** y su competencia digital. Otros factores relevantes son **la falta de un mecanismo único de notificación**, los conflictos de intereses con **la continuidad del negocio** y las brechas en la concienciación sobre ciberseguridad.
- **La cooperación público-privada** es esencial. Puede fomentarse mediante la **armonización** y centralización de los **mecanismos de información** y la creación de asociaciones público-privadas **de confianza**.

[1] Europol (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021.

[2] ENISA. (2022). ENISA Threat Landscape 2022.

[3] ICRC. (2022, January 19). Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people.

Esta publicación está financiada por el Fondo de Seguridad Interior - Policía de la Unión Europea.
El contenido de la publicación representa únicamente la opinión de los autores y es de su exclusiva responsabilidad.
La Comisión Europea no acepta ninguna responsabilidad por el uso que pueda hacerse de la información que contiene.

informáticas y sistemas de información de instituciones públicas y privadas.[4] La frecuente interrelación entre los delitos cibernéticos y los tradicionales (offline) ha aumentado la amenaza delictiva, ya que los delincuentes utilizan cada vez más el Internet para ampliar sus operaciones y encontrar nuevos métodos y herramientas de comportamiento delictivo.

A pesar de la creciente amenaza que suponen los ciberataques y los actores de las amenazas de ciberseguridad, hasta la fecha todavía se dispone de poca información sobre el alcance y el impacto reales de la ciberdelincuencia en la UE, especialmente en lo que respecta a las empresas y las entidades privadas. La falta de conocimiento se debe sobre todo a la falta de denuncias, es decir, una proporción muy pequeña de ciberdelitos llega a la atención del sistema de justicia penal. La infradeclaración es uno de los principales obstáculos para tener una imagen precisa de la ciberdelincuencia contra las empresas, contribuye a la falta de cooperación efectiva entre los sectores público y privado y, en última instancia, conduce a resultados limitados de la justicia penal.

Factores que hacen que no se denuncie la ciberdelincuencia

La falta de denuncias sigue siendo uno de los principales problemas para conocer el alcance real de la ciberdelincuencia. La limitación de las denuncias repercute en el registro de los ciberdelitos y, por tanto, en la disponibilidad de datos precisos sobre la ciberdelincuencia. Una reciente investigación sobre la ciberdelincuencia contra las pequeñas y medianas empresas (PYME) en los Estados miembros de la UE confirma que la denuncia a la policía sigue siendo escasa, ya que el 44% de los ciberdelitos sufridos por las PYME no se denuncian a nadie.[5]

Se ha argumentado que hay varios factores que influyen en la falta de notificación por parte de las empresas. Uno de los factores más recurrentes está relacionado con la percepción de que el incidente era demasiado trivial y/o no valía la pena denunciarlo, o de que el incidente se resolvía internamente. Otros factores son el miedo al daño a la reputación y la falta de confianza en la policía. En cuanto al primero, a las empresas les preocupa que los ciberincidentes se hagan públicos cuando las autoridades inicien la investigación, y que esto pueda tener posibles efectos negativos en la confianza de clientes e inversores. En cuanto al segundo factor, las empresas no suelen confiar en la competencia digital de las autoridades policiales y, por tanto, no informan del ciberincidente.

Otro factor importante, especialmente para las empresas pequeñas o para aquellas que no suelen interactuar con la policía, es la falta de un mecanismo único de notificación. Según un experto en ciberdelincuencia de la Interpol, sería beneficioso contar con una oficina cibernética centralizada que se ocupara de las denuncias cibernéticas especializadas. Esto reduciría el gran número de canales y obligaciones de denuncia existentes en muchos países, que se perciben como una disminución de la eficacia del mecanismo de denuncia.

La denuncia de la ciberdelincuencia también puede verse obstaculizada por un conflicto de intereses con la continuidad del negocio, relacionado con las diferencias entre las prioridades de las empresas y las autoridades policiales tras un ciberataque. Desde la perspectiva de las empresas, la prioridad tras un ciberincidente es mantener el negocio en funcionamiento. Esto implica recuperarse del ataque, lo que incluye recuperar el acceso a los datos (encriptados), así como evitar grandes pérdidas de tiempo y daños financieros. Por ejemplo, en 2021 la pérdida de negocio fue la mayor parte de los costes tras una filtración de datos de empresas de todo el mundo.[6] Por lo tanto, notificar a las empresas de seguridad privada, resolver los problemas técnicos y recuperar los activos suele ser más prioritario que preservar las pruebas penales.

Por último, las brechas en la concienciación sobre la ciberseguridad y la obligación de informar a los altos cargos y a las autoridades competentes pueden dar lugar a que no se denuncie a la policía. Algunas empresas, en particular las PYME, no suelen ser conscientes de haber sido víctimas de este tipo de delitos, ya que carecen de personal formado o de recursos para detectar incidentes, e incluso si

[4] CSIS. (2022, June 16). Cyber War and Ukraine.

[5] European Commission. (2022). Flash Eurobarometer 496 SMEs and cybercrime.

[6] IBM Seurity. (2021). Cost of a Data Breach Report.

se detecta un incidente, las empresas pueden no denunciar el ataque porque subestiman su gravedad.[7]

Factores de infradeclaración como reto a nivel de la UE

La ciberdelincuencia y el entorno empresarial general en los diferentes Estados miembros parecen tener un impacto limitado en las razones de la infradeclaración. Un examen más detallado de tres países diferentes de la UE, a saber, Bulgaria, los Países Bajos y España, ofrece un buen ejemplo. Los tres países tienen un panorama empresarial muy diferente en cuanto a la proporción de empresas grandes y PYMES y la alfabetización digital. Mientras que los Países Bajos albergan un número relativamente elevado de grandes empresas, España y Bulgaria tienen una población empresarial formada por un elevado número de PYME.[8] Además, los tres países objetivo tienen diferentes niveles de madurez de digitalización y transformación de las empresas, incluidos los instrumentos políticos para la privacidad y la seguridad digitales. Sin embargo, los tres países se enfrentan a retos similares en cuanto a los factores de infradeclaración por parte de las empresas. Por ejemplo, aproximadamente una de cada diez empresas de cada Estado miembro declaró que el desconocimiento de que la policía se ocupaba de los incidentes de ciberdelincuencia era una razón común para no denunciar este tipo de delitos.[9]

Bulgaria

La información sobre incidentes de ciberseguridad y ciberdelitos en el país la recogen el Equipo Nacional de Respuesta a Emergencias Informáticas (CERT) y la Dirección General de Lucha contra el Crimen Organizado (GDBOP) de Bulgaria. El CERT de Bulgaria informó de que en 2020 se registraron aproximadamente 2.100 ciberincidentes, la mayoría de los cuales consistieron en ataques de phishing y malware. Además, según informó la Asociación Búlgara de Ciberseguridad, en 2021 hubo un aumento del 70% en los ciberataques contra las PYME en Bulgaria en comparación con el año anterior. En cuanto al GDBOP, las entrevistas con expertos señalaron que la unidad recibe diariamente unas diez notificaciones por ciberdelitos o intentos de ciberdelitos en su número de teléfono. Los tipos más frecuentes de ciberdelitos contra las empresas denunciados al GDBOP son el Business Email Compromise (BEC), los ataques de phishing, el ransomware, los ataques DDoS (sobre todo para sitios gubernamentales) y los ciberataques de antiguos empleados. En particular, los BEC suelen afectar a las empresas que operan en el ámbito del comercio exterior.

En cuanto a los factores de la falta de denuncia, los más frecuentes son el desconocimiento de la normativa de ciberseguridad que obliga a denunciar los ciberataques (Ley de Ciberseguridad), la escasa confianza en las autoridades policiales y la falta de concienciación en materia de ciberseguridad, también en relación con el papel que pueden desempeñar las empresas en la prevención y denuncia de la ciberdelincuencia. Las empresas búlgaras a menudo no están preparadas para los ciberataques debido a la falta de experiencia en ciberseguridad, inversiones en TI, formación de los empleados y medidas de ciberprotección. El miedo al daño a la reputación, especialmente para las grandes empresas, es otro factor clave.[10]

Países Bajos

La Oficina Central de Estadística de los Países Bajos (CBS) indica que el número de incidentes de ciberdelincuencia en el país disminuyó durante el período 2016-2020. En 2016, casi el 40% de las empresas neerlandesas experimentaron algún tipo de incidente de ciberseguridad; en 2019 dicha cifra representó menos del 20% para las grandes empresas.[11] Además, los incidentes relacionados con los ataques DDoS representaron 1.610 en 2020, lo que supone un aumento del 75% en comparación con 2019.

[7] Williamson, J. (2016, February 10). Cyber-attack impact severely underestimated by SMEs. The Manufacturer.

[8] Eurostat. (n.d.). Structural business statistics overview.

[9] European Commission. (2022). *Op. cit.*

[10] Entrevistas con expertos de las fuerzas del orden, el centro CERT, las asociaciones de ciberseguridad y el mundo académico.

[11] CBS. (2021). Cybersecuritymonitor 2020. Central Bureau of Statistics.

Según el reciente estudio de la Comisión Europea, las pymes neerlandesas encuestadas informaron mayoritariamente de haber sufrido -en los últimos 12 meses- ataques de phishing, de toma de posesión de cuentas o de suplantación de identidad (21% de las pymes), seguidos de virus, spyware o malware (excluyendo el ransomware) (17%), y el acceso no autorizado a archivos o redes (6%). Los incidentes más graves se produjeron a través de estafas y fraudes (34%) y software malicioso (21%).[12] Estos resultados están en consonancia con estudios anteriores, que señalan el malware, el fraude electrónico, el phishing y la piratería informática como las formas más frecuentes de ciberdelincuencia contra las PYME en los Países Bajos.[13]

En cuanto a la denuncia de ciberdelitos, aproximadamente el 5-10% de las empresas neerlandesas que son víctimas de un ciberataque externo lo denuncian realmente.[14] En este sentido, existen diferentes factores para no denunciar los ciberdelitos. Las razones más frecuentes para no denunciar están relacionadas con el hecho de que la empresa se ocupó del incidente internamente, la sensación de que la policía no podía hacer nada al respecto -por lo tanto, una confianza limitada en la policía y su competencia cibernética- y el hecho de que el ciberincidente o el ataque no eran tan importantes y/o no merecían ser denunciados.[15]

España

En España, la información sobre la ciberdelincuencia y los ataques de ciberseguridad está disponible principalmente a través de las estadísticas reportadas por el Instituto Nacional de Ciberseguridad (INCIBE) al Ministerio del Interior. Las últimas cifras sobre entidades privadas indican que el INCIBE-CERT gestionó un total de 109.126 incidentes de ciberseguridad en España en 2021. Las dos formas más comunes de ciberdelincuencia fueron el malware (29,88%) y el fraude (28,60%), seguidos de los ataques a sistemas vulnerables (18,9%) y la intrusión (6,5%).[16] En lo que respecta a la infradeclaración de los ciberdelitos en España, se han esbozado recientemente dos razones principales: el hecho de que las PYMES traten el incidente internamente (57% de los encuestados), seguido de que el incidente se considere demasiado trivial y/o no merezca la pena denunciarlo (33%).[17]

¿Qué sigue?

La concienciación sobre la ciberseguridad es uno de los aspectos clave que deben adquirir las entidades privadas (y los particulares), con el apoyo activo de las autoridades públicas, incluidas las fuerzas del orden. Estos avances no sólo son necesarios para aumentar la alfabetización digital, sino también para que las empresas conozcan mejor a las autoridades pertinentes y competentes en caso de ciberincidentes. Las estrategias efectivas de información y cooperación operativa en materia de ciberdelincuencia deben:

- Abordar los factores comunes para no denunciar, entre todos la falta de confianza en la policía, la complejidad de los mecanismos de denuncia, así como la continuidad de la actividad, a la que a menudo se da más prioridad que a la preservación de las pruebas penales.
- Recurrir a las iniciativas existentes para crear sinergias y seguir aplicando las mejores prácticas. Entre las iniciativas y formas de colaboración actuales se encuentra el portal No More Ransom, lanzado en 2016 por Europol y otros socios para apoyar a las víctimas en el descifrado de sus disposi-

[12] European Commission. (2022). *Op. cit.*

[13] Veenstra et al. (2015). Cybercrime among companies. Lectoraat Cybersafety: Leeuwarden

[14] CBS. (2021). Op. cit.; see also Veenstra et al. (2015). *Op. cit.*

[15] European Commission. (2022). Op. cit.; van de Weijer, S. et al (2021). Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context: The human factor in victimization, offending, and policing (pp. 303–325). Springer.*

[16] López Gutiérrez et al. (2022). Informe sobre la cibercriminalidad en España 2021. Ministry of Interior: Government of Spain.

[17] European Commission. (2022). *Op. cit.*

tivos o archivos electrónicos. Dicha plataforma y su conjunto de herramientas de descifrado tienen como objetivo interrumpir las posibles relaciones de tipo comercial entre las empresas afectadas y los atacantes, es decir, que los ciberdelincuentes ofrezcan a las víctimas descuentos por utilizar servicios de descifrado específicos.

- Promover la denuncia de la ciberdelincuencia como algo fundamental en la lucha contra los delitos que se producen en el ciberespacio, para arrojar luz sobre el alcance real de la ciberdelincuencia y, en última instancia, limitar su impacto (económico) en las entidades privadas.

La introducción de un proceso único y centralizado de información sobre la ciberdelincuencia también favorecería la presentación de informes. El primer paso para la introducción de un mecanismo único de notificación podría ser la armonización de los mecanismos de notificación existentes y las asociaciones público-privadas (APP) bien establecidas para facilitar el intercambio de información. Además, dicho mecanismo se beneficiaría de los procesos de creación de confianza desarrollados a través de APP, de los canales de comunicación seguros y centralizados y de los protocolos y formatos de datos normalizados. La confianza entre las empresas y las autoridades policiales es fundamental para promover las asociaciones existentes y las nuevas, así como los mecanismos de intercambio de información de confianza (incluidas las plataformas seguras) que, en última instancia, pueden mejorar la colaboración mutua entre los diferentes actores en la lucha contra la ciberdelincuencia.