ES

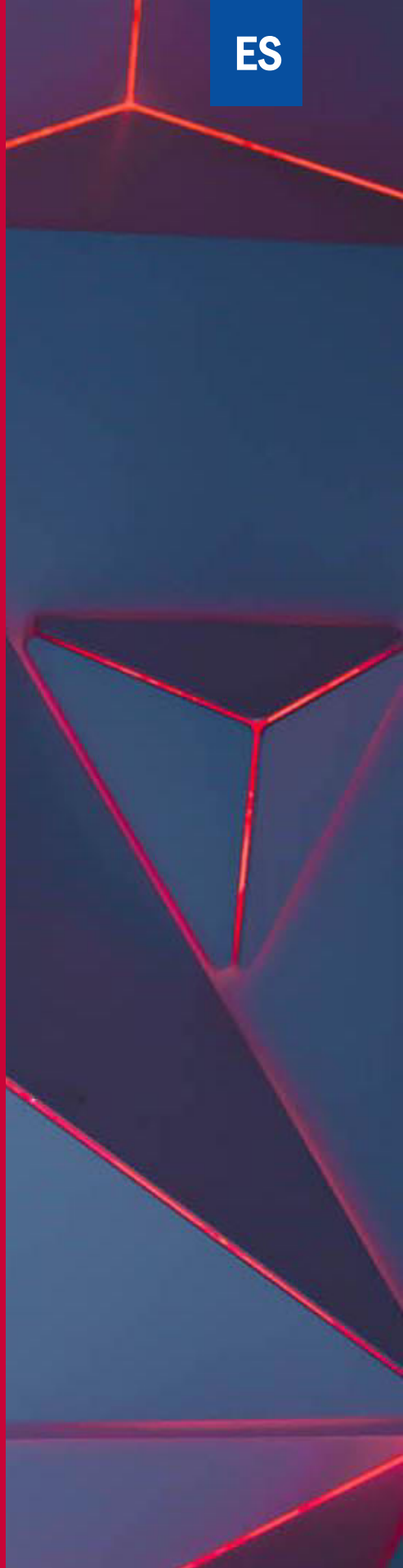
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Manipulación física, daños robos y pérdidas

Panorama de Amenazas de la ENISA



Sinopsis

La manipulación física, los daños, los robos y las pérdidas han cambiado drásticamente en los últimos años. La integridad de los dispositivos es vital para que la tecnología sea móvil y para la mayoría de las implementaciones del Internet de las cosas (IdC). El IdC puede aumentar la seguridad física con soluciones más avanzadas y complejas.[1] De esta manera, los sistemas de seguridad basados en IP con sensores inteligentes, las cámaras Wi-Fi, la iluminación de seguridad inteligente, los drones y los bloqueos electrónicos pueden proporcionar datos de vigilancia que los mecanismos de inteligencia artificial (IA) y de aprendizaje automático (AA) evalúan a fin de identificar amenazas y responder con un retraso mínimo y una precisión máxima.[2] Sin embargo, los edificios inteligentes, los dispositivos móviles y las prendas de vestir inteligentes pueden explotarse para saltarse las medidas de seguridad físicas.[3]

En 2019 se siguieron produciendo ataques físicos relacionados con cajeros y puntos de venta en Europa y en todo el mundo, pero el promedio de pérdidas fue menor que el de la década anterior. La buena noticia es que las empresas, los gerentes de sistemas informáticos y los encargados de tomar decisiones se están decantando por planes de seguridad híbridos cibernéticos y físicos aunque en el pasado la seguridad física no fuera una prioridad.

_Prácticas de seguridad nuevas y obsoletas

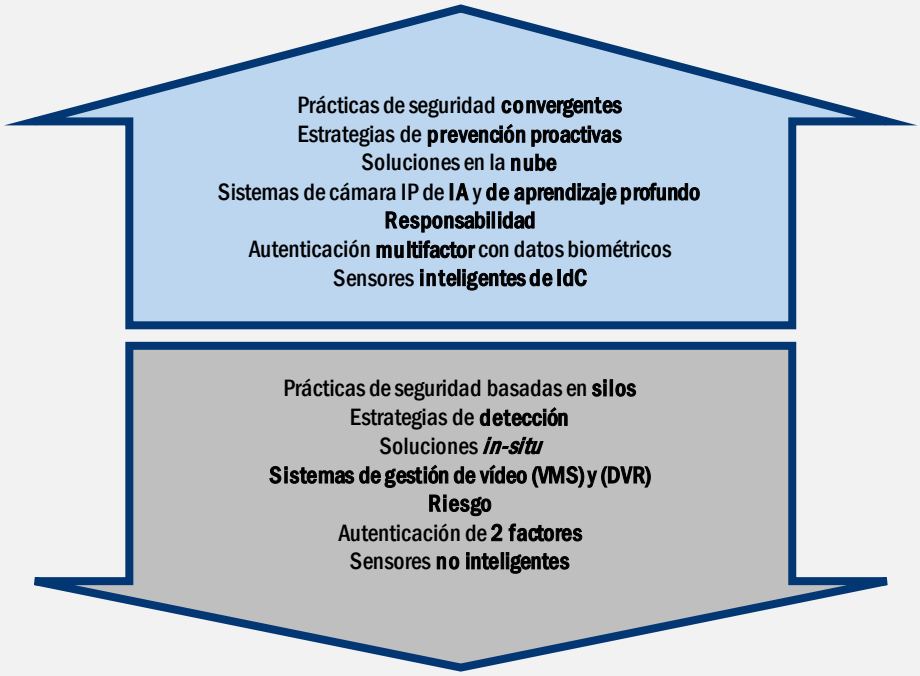
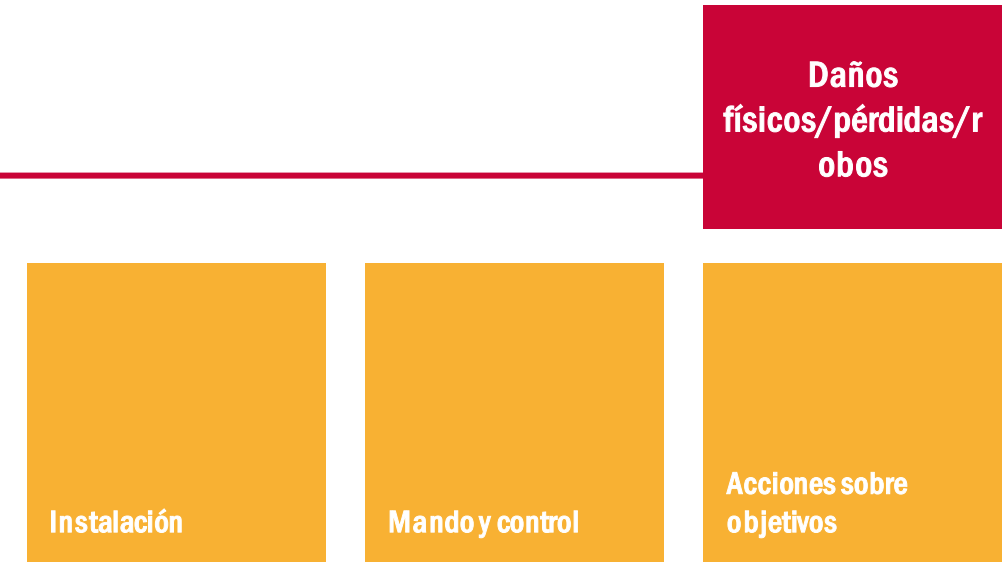


Figura 1 - Fuente: Boonedam blog[4]

Kill chain

Paso del proceso de ataque

Amplitud de la intención



Lockheed Martin desarrolló el marco cibernético de Kill Chain® que adaptó a partir de un concepto militar relacionado con la estructura de un ataque. Para estudiar un vector de ataque determinado, utilice este diagrama de *kill-chain* para trazar cada paso del proceso y anotar las herramientas, técnicas y procedimientos utilizados por el atacante.

MÁS INFORMACIÓN

Tendenci

El acceso físico es la puerta trasera más amplia

En abril de 2019, Vishwanath Akuthota, se declaró culpable de vandalismo por haber destruido equipos utilizando un dispositivo USB malintencionado que producía una descarga eléctrica. Los equipos destruidos pertenecían al College of Saint Rose de Albany (Nueva York), el centro educativo donde Akuthota había estudiado. Para este ataque, accedió a 66 estaciones de trabajo y numerosos monitores y podios digitales. El lápiz «USB asesino» que utilizó lo había comprado por Internet. El centro se gastó más de 50 000 dólares estadounidenses (aprox. 42 452 EUR) en reemplazar los equipos y más de 7 000 dólares estadounidenses (aprox. 5 943 EUR) en pagos al empleado que se encargó de resolver el incidente. Akuthota fue sentenciado a 10 años de cárcel y a una multa máxima de 250 000 dólares estadounidenses (aprox. 212 257 EUR).[5]

La seguridad física carece de atención corporativa

Durante 2019 se llevaron a cabo varias encuestas sobre seguridad física. Algunas de estas encuestas se centraron en los directores generales, gerentes de sistemas informáticos y encargados de la toma de decisiones de varias industrias, y los resultados ofrecen una buena idea sobre cómo las empresas tratan el tema de la seguridad física. Los directores generales de varios sectores industriales parecían inclinarse hacia un plan de seguridad cibernético y físico combinado para proteger sus activos contra las amenazas que tenga en cuenta factores como las amenazas internas o la importancia de la infraestructura y la integridad de las redes de la empresa. En estos planes de seguridad combinados, el énfasis, el presupuesto y el personal se asignaban a las inversiones en ciberseguridad (es decir, un 83-86 % de los recursos respectivos), mientras que el 14-17 % de los recursos de la empresa se asignaban a la seguridad física. En Europa la mayoría de los responsables de los sistemas informáticos (77 %) indicaban que la seguridad física de su empresa estaba obsoleta.[7]

_La seguridad física como servicio

Una de las tendencias de 2019 fue la mejora de la seguridad física al permitir soluciones de seguridad alojadas. La mayoría de los planes de seguridad de los responsables de los sistemas informáticos ya habían cambiado a esquemas de nube y de IdC o pensaban hacer este cambio en un plazo de 12 meses. Los responsables de la toma de decisiones indicaron que ya estaban evaluando soluciones de vigilancia por vídeo como servicio (VSaaS) y de control de acceso como servicio (ACaaS) para mejorar la detección de incidentes y reducir los tiempos de respuesta y las tasas de falsos positivos. Las soluciones VSaaS y ACaaS mejoraban la seguridad física y la ciberseguridad, pero solo un número limitado de responsables de sistemas informáticos identificaron la seguridad física como su prioridad.[8]

_La seguridad física de los cajeros ha suspendido la prueba del paso del tiempo

Al igual que se observó en 2018, en el período de este informe, los cajeros estaban expuestos a la manipulación y a daños físicos con el objetivo final de robar el dinero en efectivo que contenían. En Irlanda se notificaron nueve incidentes tan solo en el primer trimestre de 2019.[9] Algunos de los atacantes utilizaron medios muy drásticos, como excavadoras robadas, rotura de muros y el arrastre del cajero a una furgoneta o coche. En otros casos los ataques se efectuaron en cuestión de minutos utilizando explosivos, lazos con cadenas y por el método del alunizaje.[10] En los Países Bajos, tan solo durante un fin de semana de noviembre, se produjeron 71 ataques con bomba a cajeros («*plofkraken*» en neerlandés), frente a los 43 ataques similares que se produjeron en 2018. El banco ABN AMRO tuvo que retirar 70 cajeros vulnerables y la Asociación Bancaria de los Países Bajos (NVB) decidió cerrar todos los cajeros del país de 11 de la noche a 7 de la mañana durante diciembre.[11] El año 2019 es el cuarto consecutivo de aumento de los ataques a los cajeros.

Tendencias

_ Manipulación de cajeros

Durante 2019 las formas principales de manipulación de cajeros fueron el secuestro de tarjetas, el secuestro de dinero y la reversión de la transacción. La imagen general para este año es el descenso en la manipulación de los cajeros y de los surtidores de gasolina gracias al aumento de los pagos con el estándar EMV. Este estándar, denominado así por las empresas que lo presentaron por primera vez (Europay, Mastercard y Visa), describe las especificaciones para tarjetas inteligentes, terminales de pago y cajeros. Las tarjetas EMV (tarjetas con Chip y PIN o tarjeta de *chip*) llevan *chips* de circuitos integrados. La adopción de tarjetas EMV alteró el fraude con tarjetas, por lo menos parcialmente.[12] Por desgracia, las tarjetas EMV aún no se han implementado extensamente ni dentro ni fuera de Europa, y solo unos cuantos países han adoptado el control geográfico, una función antifraude de estas tarjetas.[13]

_Incidentes

- El delito perpetrado con el dispositivo USB pone de relieve la necesidad de seguridad física. Vishwanath Akuthota: un alumno del centro educativo College of Saint Rose en Albany (Nueva York) se declaró culpable de haber vandalizado los equipos del centro utilizando un dispositivo USB malintencionado.[5]
- Unos delincuentes utilizan una excavadora para robar en cajeros de Irlanda del Norte. El número de ataques físicos a los cajeros aumenta en toda la Unión Europea.[9]
- Dutch Plofkraken. Ataques con explosivos (denominados «*plofkraken*») a los cajeros de los Países Bajos. La mayoría dirigidos contra cajeros del banco ABN AMRO por su vulnerabilidad. Los ataques hicieron que el banco retirara unos 470 cajeros en los Países Bajos.[11]

Conclusiones

4 %_ de las filtraciones fueron causadas por acciones físicas.[12]

20 %_ de los incidentes de ciberseguridad empezaron o acabaron con una acción física.[12]

5º_ puesto en la lista de acciones malintencionadas contra activos - ataques físicos a los cajeros automáticos.[12]

54 %_ de las filtraciones de datos en todos los sectores incluyeron el ataque físico como método principal.

48 %_ de los responsables de los sistemas informáticos utilizaron vigilancia de vídeo en la nube o control de acceso.[8]

72 %_ de los empleados consideran que dejar información sensible en áreas públicamente accesibles es la amenaza más seria para la seguridad de los datos.[14]

65 %_ de más de 1 000 empleados encuestados declaró haber tenido comportamientos y adoptado prácticas identificados como de riesgo para la seguridad física.[15]

Mitigación:

Acciones propuestas

- Utilizar el cifrado en el almacenamiento de los datos y flujo fuera del perímetro de seguridad (dispositivos, redes, servicios en la nube, etc.).
- Utilizar inventarios de activos para seguir la pista a los dispositivos de los usuarios y recordar a sus propietarios que comprueben la disponibilidad.
- Asegurarse de limitar el acceso a las áreas que contienen información o equipos sensibles.
- Implantar políticas de seguridad bien documentadas e integrar medidas de seguridad físicas con medidas digitales para conseguir un enfoque exhaustivo.
- Utilizar pólizas de seguros para cubrir pérdidas relacionadas con los riesgos físicos y cibernéticos.
- Elaborar guías del usuario de dispositivos móviles (teléfonos inteligentes, tabletas, portátiles, etc.) y seguir las mejores prácticas.
- Establecer procedimientos bien comunicados para la protección física de los activos, incluidas las pérdidas, los daños y los robos.
- Asegurarse de que los dispositivos se retiran de la circulación tras haber borrado de forma segura toda la información personal o sensible.[6]
- Reducir el tiempo de respuesta en casos de robo, daños o pérdidas.
- Implantar la autenticación multifactor que combine credenciales de usuario con datos biométricos, tarjetas inteligentes y otros identificadores físicos.[16]
- Inspeccionar los dispositivos periódicamente para ver si han sufrido alteraciones o sustituciones.[6]
- Implantar procesos para detectar visitantes autorizados o empleados y asignar derechos de acceso apropiados.[6]
- Implantar sistemas de monitorización de acceso, sistemas de control de acceso, credenciales de acceso robustas y dispositivos de acceso inteligente (p. ej., sistemas de bloqueo inteligente, claves inteligentes) para las áreas que contengan equipos sensibles.[6]

_Alternativas preferidas para las credenciales de los usuarios en la autenticación multifactor

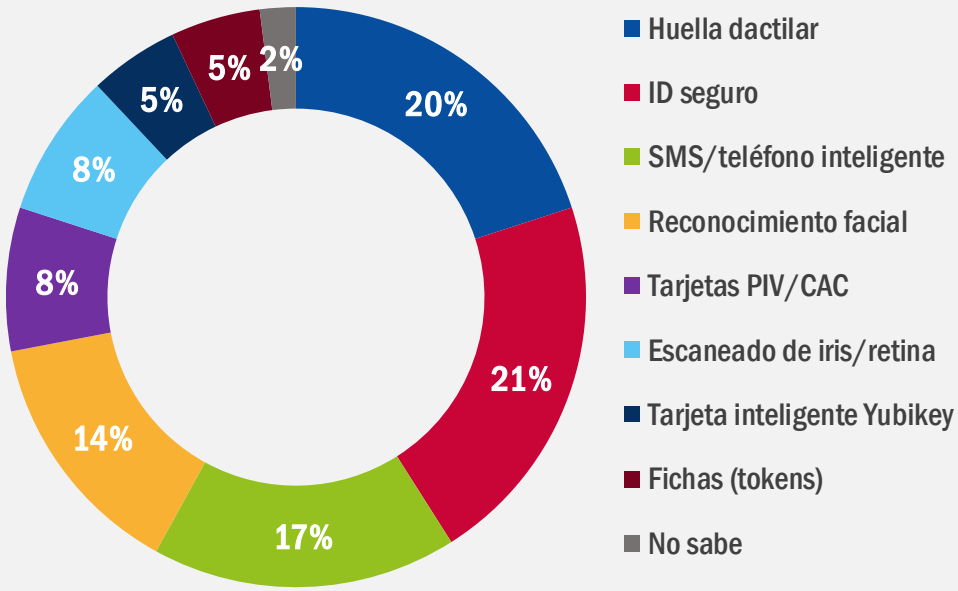


Figura 2 - Fuente: ORACLE & KPMG[16]

Bibliografía

1. "Physical Security Guide". Kisi. https://pages.getkisi.com/physical-security-guide

2. Jonathan Wackrow. "Security Convergence: Addressing Evolving Cyber and Physical Security Threats". 2019. Teneo. https://www.teneo.com/vision-book/2019/security-convergence-addressing-evolving-cyber-and-physical-security-threats/

3. Pierluigi Paganini. "Modern Physical Security Awareness Is More Than Dumpster Diving [Updated 2019]". 27 de agosto de 2019. Infosec Institute. https://resources.infosecinstitute.com/modern-physical-security-awareness-is-more-than-dumpster-diving/#gref

4. Pierre Bourgeix. "2019: What's In & Out in Physical Security". 2019. Boon Edam. https://blog.boonedam.us/2019-whats-in-out-in-physical-security

5. Danny Bradbury. "Killer USB Breach Highlights Need For Physical Security". 23 de abril de 2019. Infosec Magazine. https://www.infosecurity-magazine.com/infosec/usb-breach-physical-security-1-1-1/

6. "PCI DSS Quick Reference." Julio de 2018. PCI Security Standards Council. https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

7. "76% Security Professionals Face Cybersecurity Skills Shortage: Report." 7 de mayo de 2020. CISOMAG. https://cisomag.eccouncil.org/security-leaders-lack-cybersecurity-skills/

8. '2019 Landscape Report: Hosted Security Adoption In Europe.' 2019. Morphean. https://morphean.com/whitepaper/

9. Catalin Cimpanu. "Crooks use digger to steal ATMs in Northern Ireland as ATM physical attacks rise across the EU." 16 de abril de 2019. ZDNet. https://www.zdnet.com/article/crooks-use-digger-to-steal-atms-in-northern-ireland-as-atm-physical-attacks-rise-across-the-eu/

10. Jovi Umawing. "Everything you need to know about ATM attacks and fraud: Part 1." 29 de mayo de 2019. Malwarebytes Labs. https://blog.malwarebytes.com/101/2019/05/everything-you-need-to-know-about-atm-attacks-and-fraud-part-1/

11. 'ATM Explosive Attacks - Dutch ATMs to be shut down overnight to counter ATM explosive attacks.' 19 de diciembre de 2019. European Association for Secure Transactions (EAST). https://www.association-secure-transactions.eu/dutch-atms-to-be-shut-down-overnight-to-counter-atm-explosive-attacks/

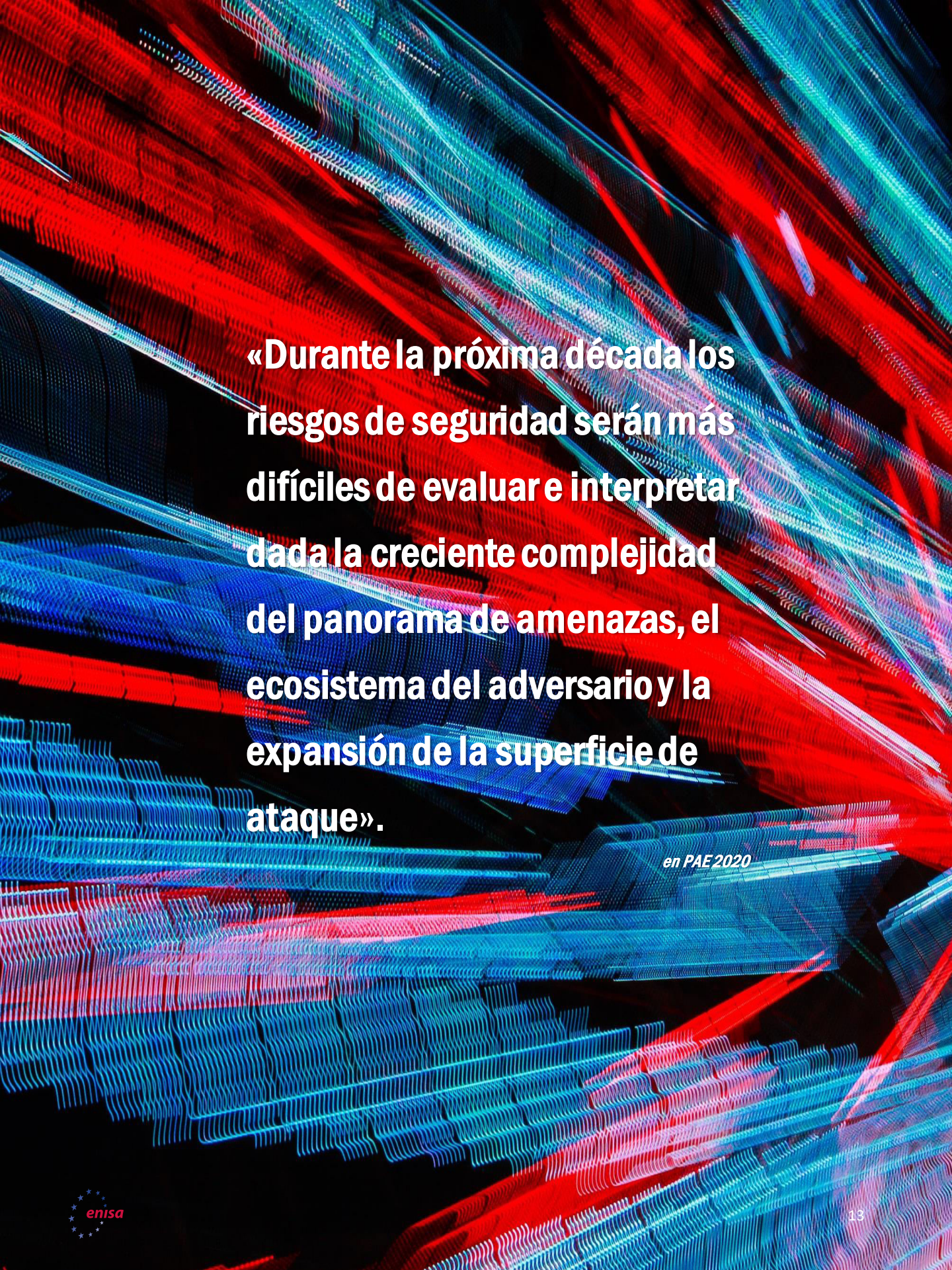
12. '2019 Payment Security Report', 2019 Data Breach Investigations Report. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

13. "2019 Payment Threats and Fraud Trends Report." 9 de diciembre de 2019. European Payments Council. https://www.europeanpaymentscouncil.eu/document-library/other/2019-payment-threats-and-fraud-trends-report

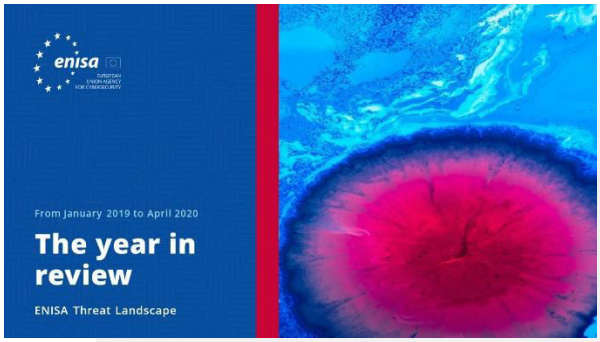
14. "2019 Eye on Privacy Report." 2019. MediaPRO. https://pages.mediapro.com/Eye-on-Privacy-Report-2019-LP.html

15. 'Report: 2020 State of Privacy and Security Awareness." 2020. MediaPRO. https://www.mediapro.com/report-2020-state-of-privacy-security-awareness/

16. "Oracle and KPMG Cloud Threat Report." 2019. ORACLE & KPMG. https://www.oracle.com/fr/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf


«Durante la próxima década los riesgos de seguridad serán más difíciles de evaluar e interpretar dada la creciente complejidad del panorama de amenazas, el ecosistema del adversario y la expansión de la superficie de ataque».
en PAE 2020

Lecturas relaciona



LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Revisión anual**

Un resumen de las tendencias en materia de ciberseguridad durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

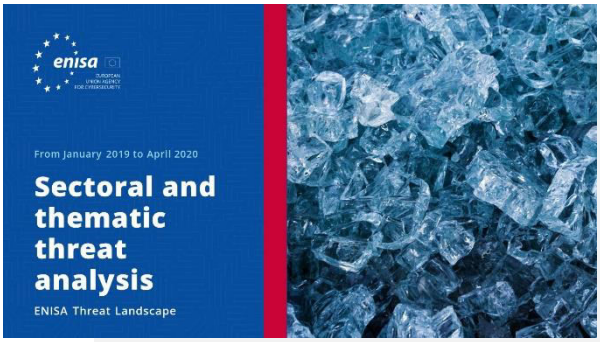
Informe Panorama de Amenazas de la ENISA
Lista de las 15 amenazas principales

Lista de la ENISA con las 15 amenazas principales durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA
Temas de investigación

Recomendaciones sobre temas de investigación de varios cuadrantes de la ciberseguridad y de la inteligencia sobre las ciberamenazas.



Informe Panorama de Amenazas de la ENISA **Análisis de las amenazas por sectores y temas**

Análisis contextualizado de las amenazas durante el período de enero de 2019 a abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Tendencias emergentes**

Principales tendencias en ciberseguridad observadas entre enero de 2019 y abril de 2020.

LEER EL INFORME

Informe Panorama de Amenazas de la ENISA **Sinopsis de la inteligencia sobre las ciberamenazas**

Situación actual en materia de inteligencia sobre las ciberamenazas en la UE.

LEER EL INFORME

¿Quiénes somos?

_ La agencia

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. La agencia se estableció en 2004, se ha visto reforzada por el Reglamento sobre la Ciberseguridad y contribuye a la política cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC con programas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE y ayuda a Europa a prepararse para los desafíos cibernéticos del futuro. A través del intercambio de conocimientos, la capacitación y la sensibilización, la Agencia coopera con las partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para proteger digitalmente a la sociedad y a la ciudadanía de Europa. Puede encontrarse más información sobre la ENISA y su labor en www.enisa.europa.eu.

Colaboradores

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) y *todos los miembros del grupo de partes interesadas de la CTI (inteligencia sobre las ciberamenazas) de la ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) y Thomas Hemker.

Editores

Marco Barros Lourenço (ENISA) y Louis Marinos (ENISA).

Datos de contacto

Las consultas acerca de este informe deben realizarse a través de enisa.threat.information@enisa.europa.eu.

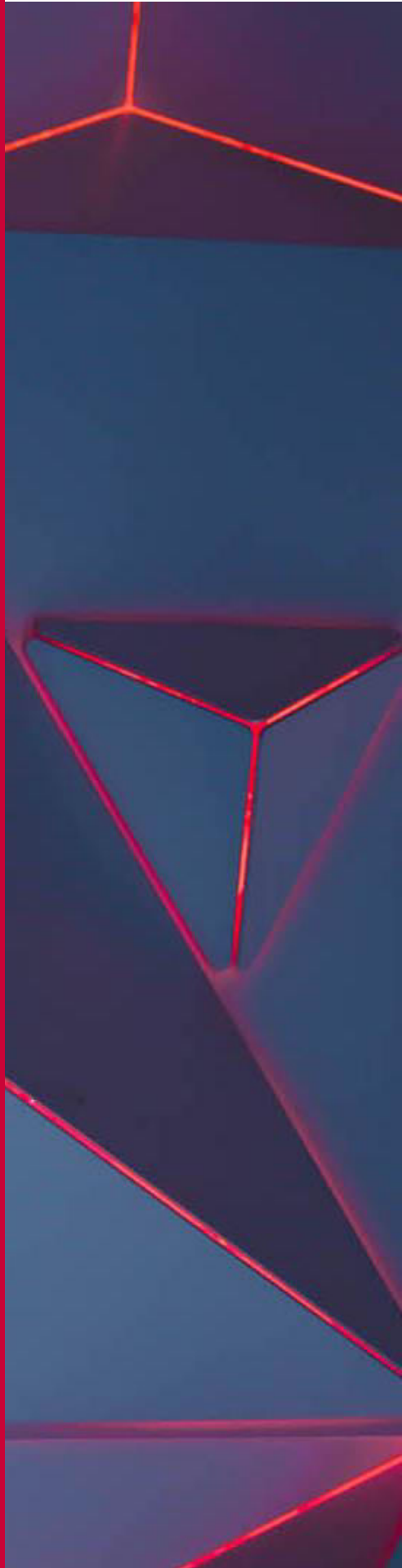
Las consultas de los medios de comunicación acerca de este informe deben realizarse a través de press@enisa.europa.eu.

Nos gustaría conocer su opinión sobre este informe

Le pedimos que dedique unos minutos a rellenar el cuestionario. Para acceder al cuestionario haga clic aquí.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu



enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu