ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Filtración de información

Panorama de Amenazas de la ENISA

Sinopsis

Las filtraciones de datos se producen cuando la información de la que es responsable una organización se ve afectada por un incidente de seguridad que resulta en la infracción de un acuerdo de confidencialidad, disponibilidad o integridad.[1] Una filtración de datos causa una filtración de información, que es una de las principales ciberamenazas, y afecta a una amplia variedad de información comprometida que va desde datos de identificación de carácter personal, datos financieros almacenados en infraestructuras informáticas, hasta datos médicos personales que se guardan en las bases de datos de los proveedores de servicios sanitarios.

Cuando los titulares de los boletines, *blogs*, periódicos e informes técnicos hablan sobre estas infracciones de la seguridad el foco se suele poner por lo general en los adversarios o en el fallo catastrófico de los procesos y técnicas de ciberdefensa. No obstante, la verdad indiscutible es que, a pesar del impacto o alcance de un evento de este tipo, la infracción suele estar causada por las acciones de una persona o fallo de un proceso de la organización.[2]

Conclusiones

2 013_revelaciones de datos intencionadas confirmadas en 2019.
Durante el primer semestre de 2019 las organizaciones sufrieron un aumento del 11 % de los incidentes de revelación de datos intencionada con respecto a 2018.[5,6]

14 %_de todos los incidentes en el sector financiero fueron revelaciones de datos intencionadas.
En el 47 % de estos casos la víctima fue un banco.[9]

4 100_millones de registros de datos salieron a la luz en todo el mundo en el primer semestre de 2019.
Las direcciones de correo electrónico y las contraseñas estaban en la cabeza de la lista.[10]

5,46_millones EUR es el coste más alto contraído por el sector de los servicios sanitarios.[11]

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.

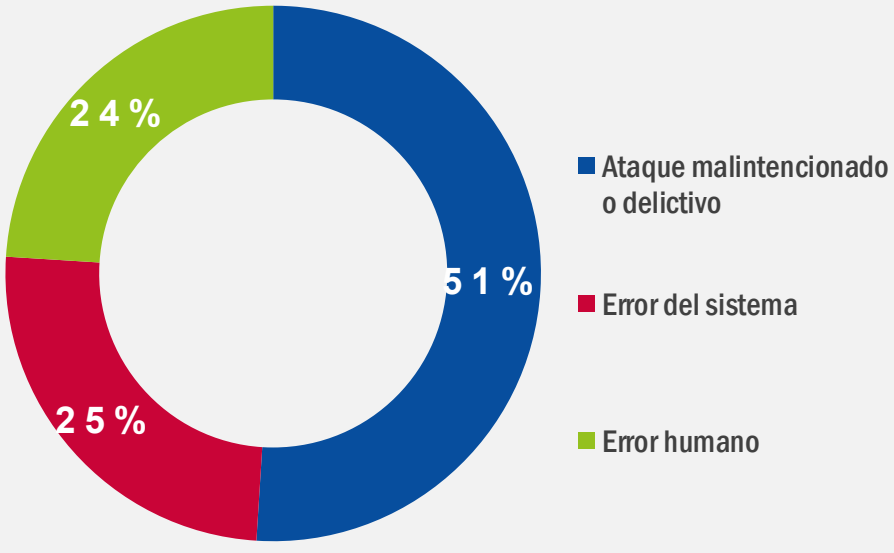
MÁS INFORMACIÓN

Incidentes

Principales incidentes de revelación de datos intencionada

- En enero de 2019 el investigador independiente Troy Hunt encontró las direcciones de correo electrónico y las contraseñas de 773 millones de usuarios en el **servicio de almacenamiento en la nube MEGA**. Hunt bautizó a esta colección de datos expuestos con el nombre de «Collection#1» y se lo notificó al servicio «Have I been Pwned?» para podérselo notificar a los propietarios de las cuentas con el fin de que estos pudieran cambiar sus contraseñas de acceso a la plataforma MEGA.[12] Ese mismo mes, personas malintencionadas expusieron los datos personales, comunicaciones privadas e información financiera de cientos de **políticos alemanes**, con afectados de todos los partidos políticos excepto del partido de extrema derecha AfD (Alternative für Deutschland).[6]
- En febrero de 2019 se extrajeron más de 61 millones de cuentas de 16 sitios *web* y se pusieron a la venta en la *dark web*. Los propietarios de los sitios Whitepages, Dubsmash, Armor Games, 500px y ShareThis vieron que los datos robados de sus clientes se vendían por menos de 20 000 dólares estadounidenses (aprox. 17 000 EUR) en bitcoins.[13]
- En marzo de 2019 cientos de millones de usuarios de **Facebook** e **Instagram** vieron sus credenciales expuestas debido a la mala gestión de almacenamiento de contraseñas de la empresa responsable de estas redes sociales.[14]
- En la India, en abril de 2019, se expusieron las historias clínicas de doce millones y medio de mujeres embarazadas debido a un servidor gubernamental con fugas que pertenecía a una agencia de servicios sanitarios. Los datos médicos expuestos estaban relacionados con la ley de técnicas de diagnóstico en el período de preconcepción y prenatal, una ley india que prohibía la selección prenatal del sexo en un intento de evitar que las familias indias abortaran los fetos de niñas y alteraran la proporción de sexos aumentando el porcentaje de varones.[15]

- En mayo de 2019 **DoorDash**, un servicio de entrega de comida a domicilio, sufrió una filtración de datos que afectó a casi 5 millones de usuarios. La investigación que se realizó a continuación determinó que los responsables habían podido acceder a nombres, direcciones de correo electrónico, direcciones de entrega, historial de pedidos, números de teléfono y contraseñas. La empresa notificó que los cuatro últimos dígitos de las tarjetas de crédito de algunos clientes y números de cuentas bancarias también habían sido expuestos.[16]
- En junio de 2019 la agencia americana de cobros por servicios médicos **AMCA** empezó a notificar a los clientes que se había producido un acceso ilegal al sistema que había expuesto los datos de facturación y médicos de algunos de sus clientes, incluidos 11,9 millones de registros de **Quest Diagnostics**, que es una de las empresas de analíticas de sangre más grandes de Estados Unidos. Según un informe 8K reciente de la Comisión de Valores de Bolsa, una persona no autorizada había estado accediendo al sistema de la AMCA durante casi ocho meses, entre el 1 de agosto de 2018 y el 30 de marzo de 2019.[17]



Causas principales de la divulgación de información. Fuente: Ponemon, IBM Security[22]

Incidentes

Principales incidentes de revelación de datos intencionada

- En julio de 2019 la corporación financiera **Capital One** sufrió una filtración de información que afectó a 100 millones de solicitudes de tarjetas de crédito, a 140 000 números de la seguridad social y a 80 000 números de cuentas bancarias. Capital One notificó que no se habían expuesto números de cuentas de tarjetas de crédito ni credenciales de inicio de sesión. Aun así, la fuga expuso nombres, direcciones, códigos postales, números de teléfono, direcciones de correo electrónico y fechas de nacimiento.[18]

- En agosto de 2019 se dejaron sin cifrar 160 millones de registros de **MoviePass**. Este incidente expuso los números de las tarjetas de crédito de los clientes y otros datos debido a que la base de datos de la empresa no estaba protegida con contraseña. La base de datos siguió estando en línea durante varios días.[19] Mientras tanto, una fuga masiva expuso 27,8 millones de registros biométricos de personal almacenados por la **policía Metropolitana Británica, bancos y contratistas de defensa**. La base de datos estaba administrada por Suprema, una empresa que colabora con la policía británica.[20,21]

- En septiembre de 2019 se piratearon más de 218 millones de cuentas de jugadores de **«Words with Friends»**. La base de datos de los usuarios incluía datos de los jugadores Android y iOS que habían instalado el juego antes del 2 de septiembre. El equipo de piratas informáticos «Gnostic players» accedió a información que contenía los nombres de los jugadores, direcciones de correo electrónico, identidades de inicio de sesión, entre otros.[23]

- En octubre de 2019 Adobe dejó 7,5 millones de registros de usuarios de Creative Cloud en una base de datos insegura. La filtración de información incluyó las direcciones de los usuarios y estado de pago.[24]

- En noviembre de 2019 Facebook otorgó acceso inapropiado a los datos de los perfiles de sus 70 000 clientes a cerca de 100 desarrolladores de aplicaciones. Uno de ellos robó datos personales que luego se utilizaron para estafar a sus propietarios.[25]

- En diciembre de 2019 un **político de los Países Bajos** se enfrentó a 3 años de cárcel por piratear las cuentas en la nube (iCloud) de 100 mujeres y divulgar fotos de desnudos. Se confirmó que el político había podido piratear las cuentas de iCloud de estas mujeres con credenciales obtenidas en violaciones anteriores de bases de datos públicas.[26] Durante el mismo mes, los datos de más de 10,7 millones de clientes del complejo hotelero **Metro-Goldwyn-Mayer (MGM)** se expusieron en un foro de piratas informáticos. La información filtrada incluía nombres y apellidos, direcciones domiciliarias, números de teléfono, direcciones de correo electrónico y fechas de nacimiento.[27]

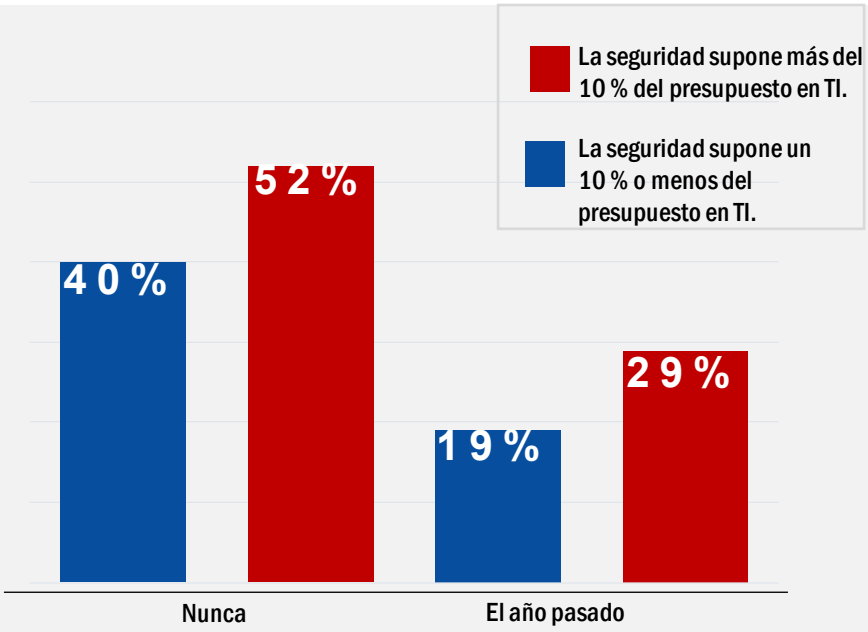


Figura 1: Tasas de incidentes de filtraciones por nivel de presupuesto de seguridad. Fuente: CNET[14]

Vectores de ataque

_Cómo

El primer vector de ataque en los casos de filtración de datos son las personas infiltradas. Este término se utiliza para describir a una persona con un interés en sacar información interna importante actuando para un tercero. Otros vectores de ataque comunes utilizados por esta amenaza son las malas configuraciones, las vulnerabilidades y los errores humanos.

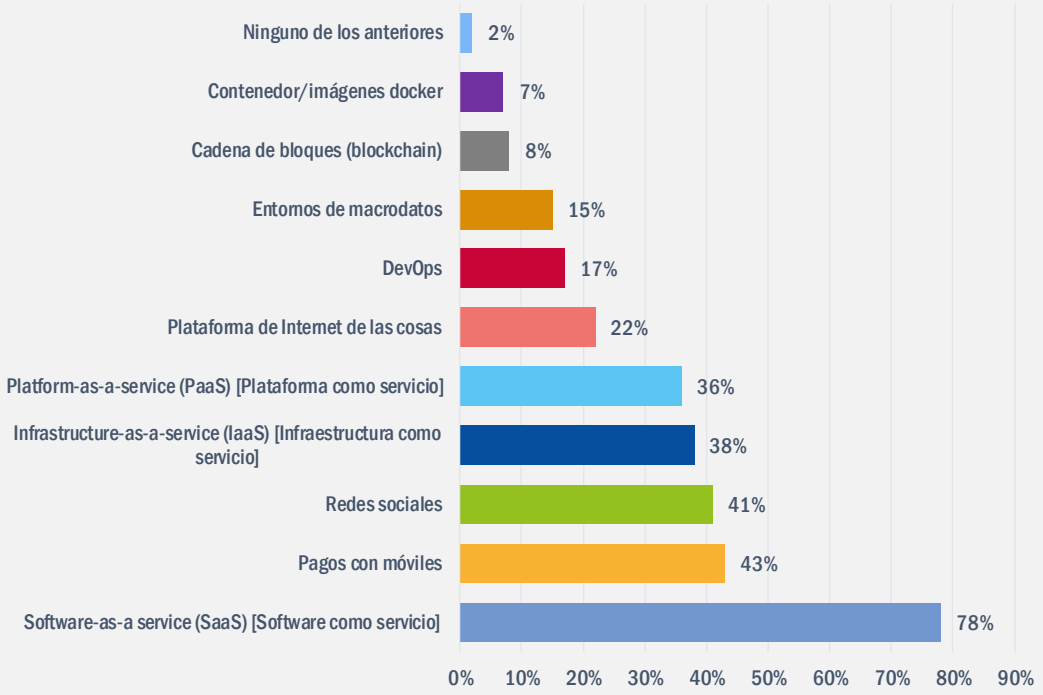


Figura 2: Tipos de datos sensibles o regulados almacenados. Fuente: Thales[40]

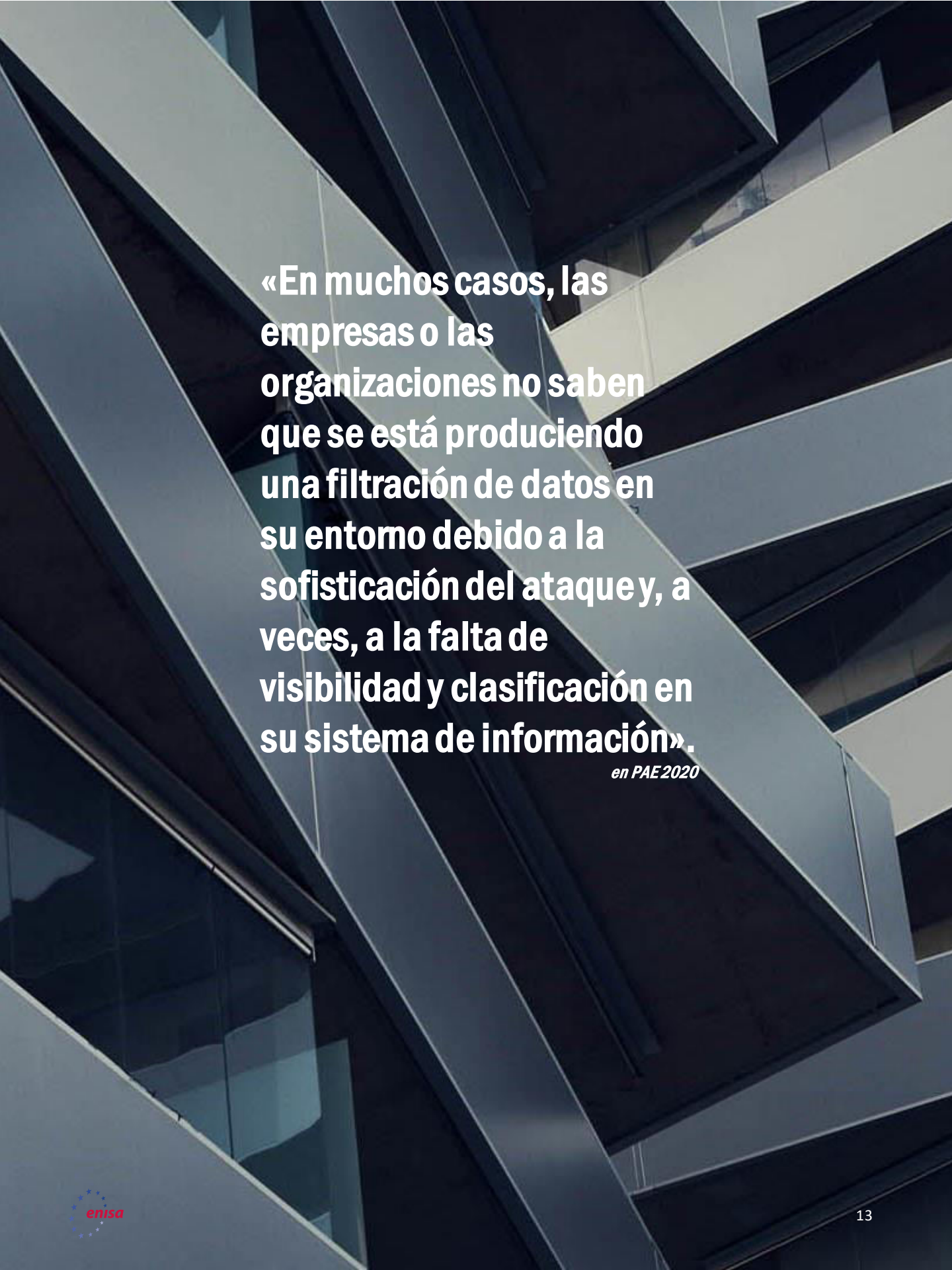
«Una filtración de datos suele causar una filtración de información, que es una de las principales ciberamenazas, y que afecta a muchos tipos de datos comprometidos».

en PAE 2020

Mitigación:

Acciones propuestas

- Anonimizar, pseudoanonimizar, minimizar y cifrar los datos en conformidad con el RGPD de la UE, la Ley de privacidad del consumidor de California (CCPA) y la Protección multinivel de la seguridad de la información (MLPS 2.0) de China.[28,29,30,31] Es necesario comprobar siempre los compromisos normativos de las entidades equivalentes que no entran dentro de iniciativas bilaterales o multilaterales.[32, 33,34]
- Almacenar datos solo en infraestructuras informáticas seguras.[35]
- Limitar los privilegios de acceso de usuarios siguiendo el principio de necesidad de saber.[35,36] Quitar los privilegios de acceso a todo aquel que no sea un empleado.[35]
- Educar y formar al personal de la organización periódicamente.[35,37]
- Usar herramientas tecnológicas para evitar posibles filtraciones de datos, como herramientas de escaneado de vulnerabilidades, escaneado de *malware* y de prevención de pérdida de datos (data loss prevention, DLP). Desplegar el cifrado de datos, de sistemas portátiles y de dispositivos, y usar pasarelas seguras.[36,38]
- El plan de continuidad de la actividad (businees continuity plan, BCP) es crucial para afrontar una filtración de datos. Este plan describe los tipos de datos que se almacenan y su ubicación, y qué obligaciones potenciales podrían surgir al implementar acciones de seguridad de datos y de recuperación. Un BCP conlleva una respuesta eficaz ante incidentes, cuyo objetivo es abordar, gestionar y rectificar los daños producidos por el ataque.[39]



«En muchos casos, las empresas o las organizaciones no saben que se está produciendo una filtración de datos en su entorno debido a la sofisticación del ataque y, a veces, a la falta de visibilidad y clasificación en su sistema de información».

en PAE 2020

Bibliografía

1. "What is a data breach and what do we have to do in case of a data breach?" European Commission. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

2. "The humn factor of cyber security." CSO. https://www.csoonline.com/article/3504813/the-human-factor-of-cyber-security.html

3. Howard Poston. "Common causes of large breaches (Q1 2019)." 1 de mayo de 2019. INFOSEC Institute. https://resources.infosecinstitute.com/common-causes-of-large-breaches/#gref

4. J. Clement. "Average cost of data breaches worldwide from 2014 to 2019." 13 de agosto de 2019. Statista. https://www.statista.com/statistics/987474/global-average-cost-data-breach/

5. "2019 Data Breach Investigations Report." 2019. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

6. "Cyber Threatscape Report." 2019. iDefense – Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

7. "Cybercrime will cost businesses over $2 trillion by 2019." 12 de mayo de 2015. Juniper Research https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

8. "How much would a data breach cost your business?." 2019. IBM. https://www.ibm.com/security/data-breach

9. G. Dautovic. "Top 25 Financial Data Breach Statistics for 2020." 11 de marzo de 2020. Fortunly. https://fortunly.com/statistics/data-breach-statistics#gref

10. Davey Winder."Data Breaches Expose 4.1 BIllion Records In First Six Months of 2019." 20 de agosto de 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#40479be4bd54

11. "Cost of a Data Breach Report." 2019. Ponemon Institute – IBM. https://databreachcalculator.mybluemix.net/executive-summary/

12. Troy Hunt. "The 773 Million Record "Collection #1." Data Breach". 17 de enero de 2019. Troy Hunt. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

13. Lewis Morgan. "List of data breaches and cyber attacks in February 2019 – 873,919,635 records leaked." 26 de febrero de 2019. IT Governance. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2019-692853046-records-leaked

14. Rae Hodge. "2019 Data Breach Hall of Shame: These were the biggest data breaches of the year." 27 de diciembre de 2019. CNET. https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/

15. Catalin Cimpanu. "Indian govt agency left details of millions of pregnant women exposed online." 1 de abril de 2019. ZDNet. https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

16. Shelby Brown. "DoorDash data breach affected 4.9M customers, drivers, merchants." 26 de septiembre de 2019. CNET. https://www.cnet.com/news/doordash-data-breach-affected-4-9-million-customers-workers-and-merchants/

17. Jessica Davis. "11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach." 3 de junio de 2019. HealthITSecurity https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach

18. Alfred Ng, Mark Serrels. "Capital One data breach involves 100 million credit card applications." 30 de julio de 2019. CNET. https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/

19. Shelby Brown. "Data breaches timeline: EasyJet cyberattack exposes over 9M people, and more." 19 de mayo de 2020. CNET. https://www.cnet.com/how-to/equifax-mgm-resorts-beyond-every-major-security-breach-and-data-hack-update/

20. Josh Taylor. "Major breach found in biometrics system used by banks, UK police and defence firms." 14 de agosto de 2019. The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

21. Guy Fawkes. "Report: Data Breach in Biometric Security Platform Affecting Millions of Users." 16 de junio de 2020. vpnMentor. ttps://www.vpnmentor.com/blog/report-biostar2-leak/

22. "Cost of a Data Breach Report." 2019. Ponemon - IBM Security. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

23. Oscar Gonzalez. "Zynga data breach exposed 200 million Words with Friends players." 1 de octubre de 2019. CNET. https://www.cnet.com/news/people-rarely-change-their-passwords-after-a-data-breach-study-says/

24. John E Dunn. "Adobe database exposes 7.5 million Creative Cloud users." 28 de octubre de 2019. Naked Security. https://nakedsecurity.sophos.com/2019/10/28/adobe-database-exposes-7-5-million-creative-cloud-users/

25. "Insider Sold 68K Customer Records to Scammers: Trend Micro." 8 de noviembre de 2019. CISOMAG. https://www.cisomag.com/insider-sold-68k-customer-records-to-scammers-trend-micro/

26. Catalin Cimpanu. "Dutch politician faces three years in prison for hacking iCloud accounts and leaking nudes." 3 de diciembre de 2019. ZDNet. https://www.zdnet.com/article/dutch-politician-faces-three-years-in-prison-for-hacking-icloud-accounts-and-leaking-nudes/

27. Corinne Reichert. "MGM Resorts confirms data breach of 10.7 million guests." 19 de febrero de 2020 https://www.cnet.com/news/mgm-resorts-confirms-data-breach-of-10-million-guest-accounts/

28. Reglamento (UE) n.º 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). 27 de abril de 2020. Parlamento Europeo, Consejo de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32016R0679

29. "AB-375 Privacy: personal information: businesses, Assembly Bill No. 375, Chapter 55." 29 de junio de 2018. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

30. Shrub Chandrasekaran, Justin Fishman. "China's Cybersecurity Future and its Impact on U.S. Business." 31 de octubre de 2019. Jolt Digest. https://jolt.law.harvard.edu/digest/chinas-cybersecurity-future-and-its-impact-on-u-s-business

31. Reed Smith LLP. "MLPS 2.0: China's enhanced data security multi-level protection scheme and related enforcement updates." 9 de octubre de 2019. Lexology. https://www.lexology.com/library/detail.aspx?g=36c6932b-bf41-4e08-b430-e3bc839a2328

"Data protection if there's no Brexit deal." 13 de septiembre de 2018. GOV. UK, Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

33. Eduardo Ustaran, "Brexit and data protection: Laying the odds." 21 de septiembre de 2018. Privacy Perspectives, iapp. https://iapp.org/news/a/brexit-and-data-protection-laying-the-odds/

Ibrahim Hasan. "Data protection and Brexit." 5 de septiembre de 2016. Gazette. https://www.lawgazette.co.uk/legal-updates/data-protection-and-brexit/5057412.article

35. Eric Dosal. "5 Tips to Prevent Data Leakage at Your Company." 15 de marzo de 2018. Compuquip Cybersecurity. https://www.compuquip.com/blog/5-tips-to-prevent-data-leakage-at-your-company

36. "10 ways to protect sensitive business data." 28 de octubre de 2019. QuoStar. https://www.quostar.com/blog/10-tips-to-help-prevent-a-data-leak/

37. "Annual Cybersecurity Report." 2018. Cisco https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

38. "Cybercrime tactics and techniques: Q2 2018." 2018. Malwarebytes Labs

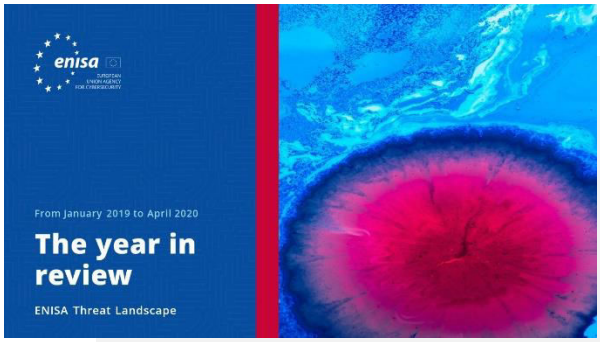
https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf

39. Mona Mangat. "81 Eye-Opening Data Breach Statistics for 2020." 27 de enero de 2020. phoenixNAP. https://phoenixnap.com/blog/data-breach-statistics

40. "2020 Data Threat Report – Global Edition." 2020. Thales Group. https://www.thalesesecurity.com/2020/data-threat-report

41. Oscar Gonzalez. "Zynga data breach exposed 200 million Words with Friends players." 1 de octubre de 2019. C | net. https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/

Lecturas relacionadas



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

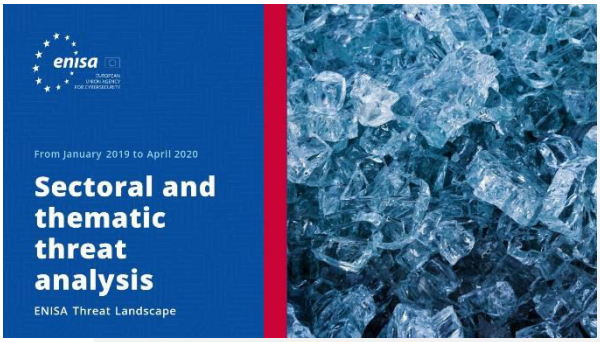
Informe Panorama de Amenazas de la ENISA
Lista de las 15 amenazas principales

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.



LEER EL INFORME

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.

¿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 sus 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.

Aviso legal

Salvo que se indique lo contrario, la presente publicación refleja las opiniones e interpretaciones de la ENISA. Esta publicación no constituye en ningún caso una medida legal de la ENISA ni de los organismos que la conforman, a menos que se adopte en virtud del Reglamento (UE) 526/2013. La información tampoco refleja necesariamente el estado actual de la técnica y la ENISA se reserva el derecho a actualizarla en todo momento.

Las correspondientes fuentes de terceros se citan cuando proceda. La ENISA declina toda responsabilidad por el contenido de las fuentes externas, incluidos los sitios *web* externos a los que se hace referencia en esta publicación.

Esta publicación tiene un carácter meramente informativo. Además, debe poder accederse a la misma de forma gratuita. Ni la ENISA ni ninguna persona que actúe en su nombre aceptan responsabilidad alguna en relación con el uso que pueda hacerse de la información incluida en la presente publicación.

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