enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ES

De enero de 2019 a abril de 2020

Amenazas internas

Panorama de Amenazas de la ENISA

Sinopsis

Las amenazas internas son acciones que pueden provocar un incidente ejecutado por una persona o grupo de personas afiliadas o que trabajan para la víctima potencial. Hay varios tipos de patrones asociados a las amenazas internas. Un patrón bien conocido de amenaza interna (que también se denomina «uso indebido de privilegios») se produce cuando agentes externos colaboran con agentes internos para acceder de forma no autorizada a determinados activos. Los infiltrados pueden causar daños de forma accidental por descuido o por falta de conocimiento. Como estas personas infiltradas cuentan con la confianza, privilegios y conocimiento de las políticas, los procesos y los procedimientos de la organización, es difícil distinguir entre el acceso legítimo, malintencionado o erróneo a las aplicaciones y sistemas de datos.[1]

Los cinco tipos de amenazas internas se pueden definir según sus fundamentos y objetivos:

a) los empleados descuidados que no trabajan adecuadamente con los datos, infringen políticas de uso e instalan aplicaciones no autorizadas;

b) los agentes infiltrados que roban información para terceros;

c) los empleados descontentos que quieren hacer daño a la organización;

d) los infiltrados malintencionados que utilizan privilegios existentes para robar información para obtener beneficios personales;

e) terceros irresponsables que comprometen la seguridad mediante inteligencia, acceso indebido o malintencionado para usar u obtener un activo.

Los cinco tipos de amenazas internas deben estudiarse continuamente, ya que saber que existen y cómo operan debería definir la estrategia de la organización en materia de protección de los datos y la seguridad.

Conclusiones

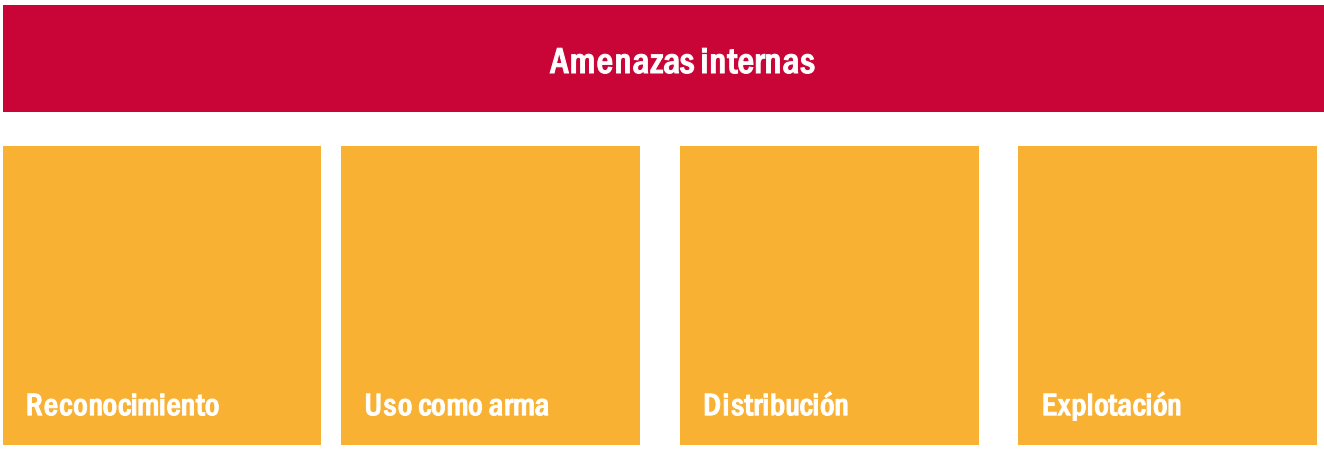
65 %_ **del impacto de las amenazas internas incluye daños a la reputación y a las finanzas de la organización.**[12]

88 %_ **de las organizaciones encuestadas reconocen que las amenazas internas son motivo de alarma.**[10]

11,45_ **millones EUR es el coste medio anual de los incidentes de ciberseguridad causados por una persona infiltrada en la organización.**[8]

40 %_ **de las organizaciones encuestadas se sienten vulnerables a la exposición de información confidencial de la empresa.**[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

Descripción

_El dinero manda

Dado el aumento del coste de otros vectores de ataque, los atacantes están dispuestos a ofrecer grandes cantidades de dinero a infiltrados. El precio de estas personas infiltradas varía según el puesto que desempeñen en la empresa, el tipo de empresa, el tipo de complejidad del servicio que se solicita, el tipo de datos que se quieren extraer y el nivel de seguridad de la empresa. Estas son algunas de las formas de reclutamiento de infiltrados: (1) simplemente enviando una oferta a foros y ofreciendo una recompensa por determinada información; (2) encubriendo sus acciones para que los empleados no se den cuenta de que actúan de forma ilegal, revelando información personal o participando en la actividad del empleado; y (3) con chantaje.[4]

_Acciones fraudulentas «Urbi et Orbi»

Un exempleado que trabajaba como ingeniero de *software* para un proveedor de servicios en la nube se aprovechó de la existencia de un cortafuegos de aplicaciones *web* mal configurado y pudo acceder a las cuentas y registros de tarjetas de crédito de 100 millones de clientes. La empresa solucionó la vulnerabilidad y declaró que los números de las tarjetas de crédito y las credenciales de apertura no se habían visto afectados. Este caso de amenaza interna es de particular interés porque el exempleado convertido en ciberdelincuente no se molestó en ocultar su identidad. El autor del ataque compartió el método de entrada con compañeros del servicio de *chat* de Capital One. El ciberdelincuente también publicó información en GitHub (usando nombre y apellidos) y alardeó de su infracción en las redes sociales. Este tipo de comportamiento es un fenómeno que los psicólogos llaman «escape» en el que el personal interno que planea hacer algo ilícito revela sus planes. Capital One prevé que el ataque costará aproximadamente 150 millones de dólares estadounidenses (aprox. 127 millones EUR).[5]

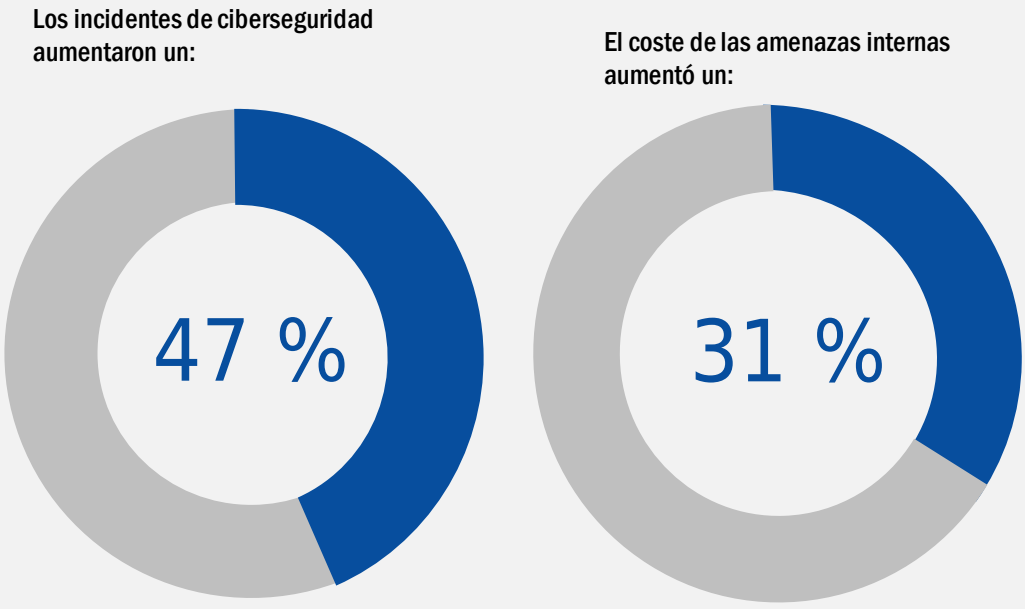


Figura 2: Tendencias de incidentes y costes. Fuente: ObservelT[8]

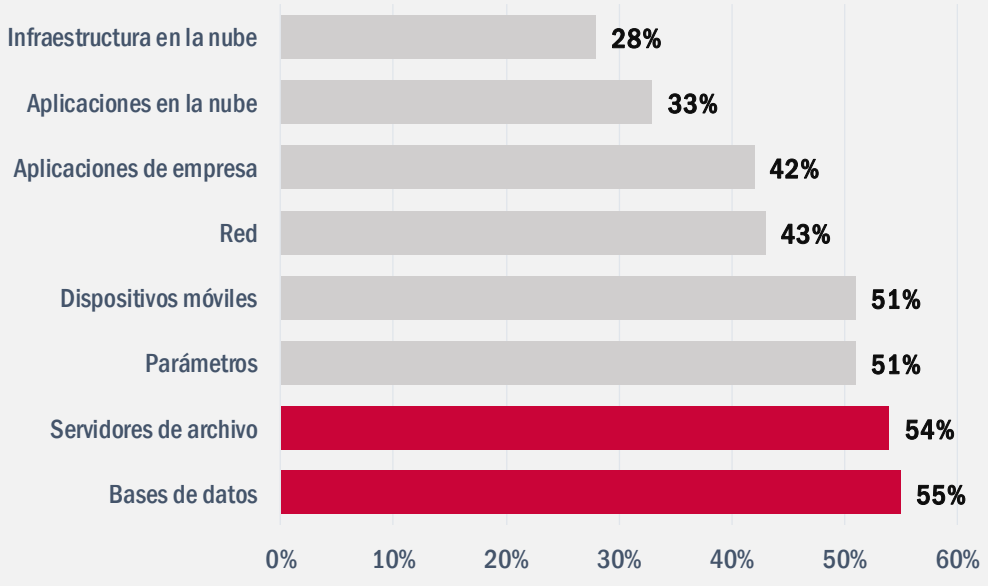


Figura 2: Infraestructura informática vulnerable a las amenazas internas. Fuente: Help Systems[9]

Vectores de ataque

_Cómo

Según una encuesta reciente[14], los grupos son las amenazas internas más peligrosas en empresas y otras organizaciones.

Según expertos en ciberseguridad[15], el *phishing* (38 %) es la mayor vulnerabilidad en el caso de amenazas internas no intencionadas. En un puesto inferior de la lista está el *phishing* dirigido (*spear phishing*) (21 %), las contraseñas débiles o reutilizadas (16 %), las cuentas huérfanas (10 %) y las visitas a sitios sospechosos (7 %).

_Área de impacto de los incidentes de amenazas internas

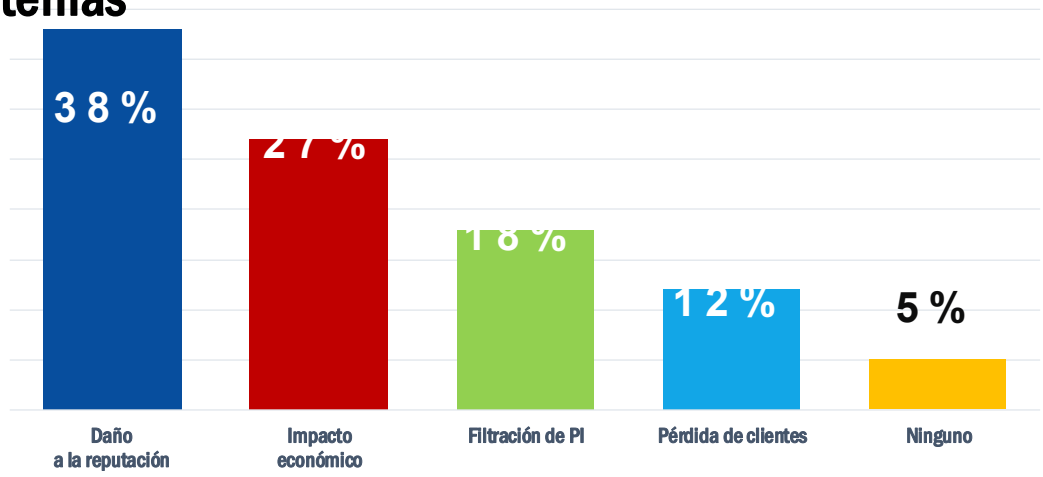


Figura 3 - Fuente: Egress[12]

«Los infiltrados pueden causar daños de forma accidental por descuido o por falta de conocimiento».

en PAE 2020

Mitigación

Acciones propuestas

- Desplegar la tecnología de inspección profunda de paquetes (deep packet inspection, DPI) para detectar anomalías que ofrezca a los usuarios del sector industrial una plataforma de confianza para vigilar el flujo de los procesos de mando y control y los datos de telemetría, y les proteja contra las amenazas externas. Al mismo tiempo, mitigar el riesgo de interferencias de infiltrados con conocimientos avanzados, como los ingenieros, operadores de SCADA u otro personal interno con acceso directo a los sistemas.[16]
- Introducir un plan de contramedidas para amenazas internas en la estrategia y políticas globales de seguridad. Este plan suele incluir un marco de trabajo de gestión de riesgos, un plan de continuidad de la actividad, un programa de recuperación de desastres, políticas de gestión financiera y de contabilidad, y una gestión jurídica y reglamentaria.[1]
- Elaborar un programa de seguridad que incluya: la realización de actividades de búsqueda de amenazas, hacer un estudio de la vulnerabilidad y pruebas de penetración, implantar medidas de seguridad para el personal, emplear medidas de seguridad físicas, establecer soluciones de seguridad de red, emplear soluciones de seguridad en puntos terminales, aplicar medidas de seguridad de datos, emplear medidas de gestión de identidad y acceso, establecer capacidades de gestión de incidentes, contratar servicios de criminalística digital y el uso de métodos de inteligencia artificial (IA) para prevenir ataques internos.
- Diseñar una política de seguridad contra amenazas internas basada en la concienciación de los usuarios, que es uno de los controles más eficaces para este tipo de ciberamenaza.
- Establecer controles técnicos robustos. Las medidas tradicionales de seguridad suelen estar enfocadas a las amenazas externas, pero por lo general no son eficaces para identificar los riesgos internos que emanan de la organización. Para proteger los activos, implementar herramientas como las de prevención de pérdidas de datos (data loss prevention, DLP) para evitar la fuga de datos.[1]

- Reducir el número de usuarios con privilegios y el acceso a información sensible. Si un empleado no necesita acceder a determinada información para hacer su trabajo, es mejor restringir lo que puede ver para evitar accesos inapropiados.[17]
- Endurecer el entorno digital, que incluye aumentar la seguridad de la red, los sistemas, las aplicaciones, los datos y las cuentas.[1]

Bibliografía

1. "Insider Threat Report", 2019. Verizon. https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

2. "Insider Threat Statistics Facts and Figures". Ekran System. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

3. "CyberEdge 2019 CDR Report" 2019. CyberEdge. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

4. "Corporate Security Predictions 2020". 2019. 3 de diciembre de 2019. Kapersky.

https://securelist.com/corporate-security-predictions-2020/95387/

5. "Famous Insider Threat Cases", septiembre de 2019. Security Boulevard.
https://securityboulevard.com/2019/09/famous-insider-threat-cases-insider-threat-awareness-month/

6. "The rise of insider threats: Key trends to watch" 2019. Tech Beacon.

https://techbeacon.com/security/rise-insider-threats-key-trends-watch

7. "Cost of Cybercrime study" 2019. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

8. "Cost of Insider Threats", 2020. Observer IT. https://www.observeit.com/cost-of-insider-threats/

9. "Cybersecurity Insiders 2019 Insider Threat Report", 2019. Help Systems.https://www.helpsystems.com/cta/2019-cybersecurity-insiders-insider-threat-report

10. "Forcepoint Insider threat Data Protection" 2017. Force Point.

https://www.forcepoint.com/sites/default/files/resources/files/brochure_insider_threat_data_protection_en.pdf

11. "State of Insider Threats in the Digital Workplace" 2019. Better Cloud. https://www.bettercloud.com/monitor/wp-content/uploads/sites/3/2019/03/BetterCloud-State-of-Insider-Threats-2019-FINAL.pdf

12. "Insider Data Breach Survey 2019". 2019. Egress. https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

13. "Insider Threat Report". 2019. Nucleos Cyber. https://nucleuscyber.com/wp-content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf

14. "Insider Threat Report". 2019. Haystax. https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

15. "Insider Threat Report". 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

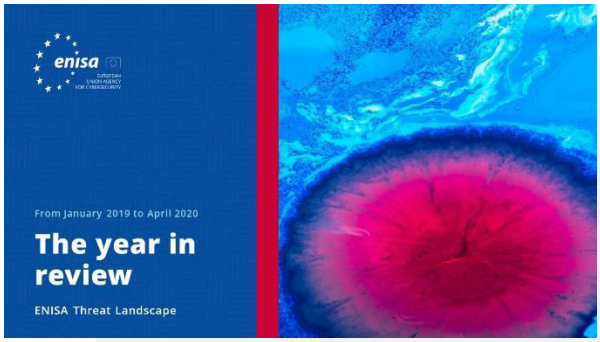
16. "Kaspersky Industrial CyberSecurity: solution overview 2019". 2019. Kaspersky.
https://ics.kaspersky.com/media/KICS-Solution-overview-2019-EN.pdf

17. "Post-vacation cybersecurity tuneup: Get your company ready!". 1 de septiembre de 2017. Panda.
https://www.pandasecurity.com/mediacenter/adaptive-defense/cyber-security-get-company-ready/

«El aumento de la complejidad de las aplicaciones *web* y sus servicios extendidos crea retos a la hora de protegerlos contra las amenazas con diversos motivos, desde financieros o daños a la reputación, hasta el robo de datos vitales o personales».

en PAE 2020

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

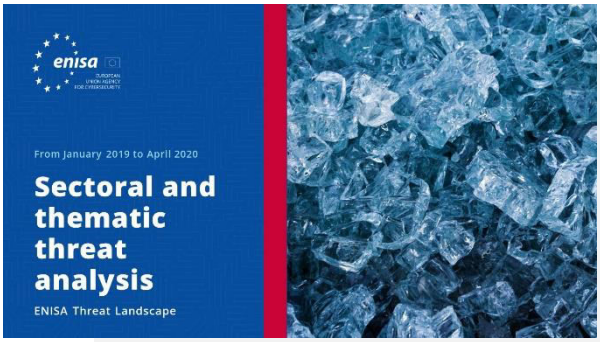
Informe Panorama de Amenazas de la ENISA **Lista de las 15 amenazas principales**

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.



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 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.

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