ES

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De enero de 2019 a abril de 2020

Temas de investigación

Panorama de Amenazas de la ENISA

Sinopsis

Gracias a las actividades de innovación e investigación que llevan a cabo las universidades, la industria y los profesionales de todo el mundo, las ideas y los conceptos del dominio de la ciberseguridad siguen evolucionando. Son pasos importantes porque la velocidad de la innovación por parte de los adversarios (atacantes) es más alta que la de los especialistas en ciberseguridad para encontrar soluciones para frenarlos. En realidad, aparte de unos conocimientos básicos y formación en ciberseguridad, la inversión en investigación e innovación es la opción más viable para que los defensores puedan acercarse a lo que se necesita para mejorar las seguridad del ciberespacio. En este informe ponemos de relieve algunos de los temas de innovación e investigación en materia de ciberseguridad explorados en la UE y en todo el mundo.

Entender mejor la dimensión humana

La ciberseguridad sigue viéndose como la práctica de proteger las redes, los sistemas de información y los datos. Esta definición debe ampliarse más allá de los temas técnicos para incluir los problemas sociales, de comportamiento y económicos, y las diferentes funciones desempeñadas por todas las partes involucradas. Esto debería ser una prioridad en los debates sobre la investigación e innovación en materia de ciberseguridad. Entender mejor la dimensión humana es la clave para la definición de cualquier estrategia de ciberseguridad a fin de que las decisiones de seguridad se tomen para ajustarse a sus necesidades, capacidades y expectativas.

Investigación e innovación en materia de ciberseguridad

Durante 2019 hemos observado un aumento en el número de laboratorios de pruebas y campos de maniobras virtuales[1] que se ofrecen en oficinas y en ofertas en la nube. Estos recursos son esenciales para que los investigadores puedan simular ataques, desarrollar escenarios de explotación, obtener datos operativos y probar estrategias de defensa en entornos virtuales multiuso. No obstante, hay entornos que no pueden replicar el gran número de vulnerabilidades que suelen comprometer la seguridad, como es el caso de los factores de ingeniería y humanos, entre otros. Para mejorar la eficacia es importante investigar e innovar el alcance y la fidelidad de estos laboratorios de pruebas y proponer nuevas soluciones técnicas.

Sinopsis

Seguridad de las redes 5G

El despliegue de las redes de comunicaciones móviles 5G en algunos países empezó en 2019 pero se prevé que el número de instalaciones aumente en 2021. Esta nueva generación de comunicaciones móviles es de extrema importancia para el progreso económico y social de la Unión Europea. Por tanto, la investigación y desarrollo de las soluciones de seguridad 5G es fundamental para la sostenibilidad y fiabilidad de esta tecnología. En 2019 la ENISA publicó un informe con el panorama de amenazas para las redes 5G en el que se revisaban algunos aspectos de seguridad vitales relacionados con esta tecnología emergente.[2] En los temas principales de investigación e innovación de la seguridad de las redes 5G se deberían considerar los aspectos siguientes:

- La investigación y el desarrollo de controles de seguridad para cubrir la protección de la red, los elementos físicos y las capas de datos, a fin de proporcionar una solución de protección multicapa. Con las redes 5G los datos se ubicarán en servidores en la nube centralizados, nodos intermedios (nodos *fog*) y dispositivos periféricos, todo esto aumentará la complejidad de la implementación de una solución de seguridad.

- La investigación y el desarrollo de estándares y requisitos para los controles de seguridad para implementarlos en redes interconectadas de varios propietarios, topologías, operadores y una diversidad de dispositivos y capas de red.

- La investigación y el desarrollo de capacidades de gestión claves que permitan una interoperabilidad segura entre los nodos que conectan los dispositivos periféricos de recursos limitados y los dispositivos IdC. Esta capacidad debe incluir técnicas clave de control, autenticación, criptografía y gestión en los nodos de recursos limitados.

Proyectos de investigación e innovación de la UE en materia de ciberseguridad

- La UE trabaja para establecer un piloto para la red de competencia en ciberseguridad. CONCORDIA[3], ECHO[4], SPARTA[5] y CyberSec4Europe[6] son los cuatro proyectos piloto ganadores de la convocatoria de 2018 de Horizonte 2020 en materia de ciberseguridad para «establecer y operar un marco piloto para una red de competencia europea en materia de ciberseguridad y desarrollar una hoja de ruta común para la Investigación e innovación de la ciberseguridad europea». La UE prevé reforzar su capacidad de ciberseguridad y abordar los desafíos futuros en esta materia con estos cuatro proyectos piloto para lograr un Mercado Único Digital Europeo más seguro.
- La UE cuenta con un fondo de 38 millones EUR para la protección de infraestructura vital contra las ciberamenazas. La Comisión Europea ha anunciado un fondo de más de 38 millones EUR a través del programa Horizonte 2020 para el programa de investigación e innovación de la UE. El objetivo de este programa es respaldar varios proyectos innovadores en el campo de la protección de infraestructuras vitales contra las ciberamenazas y las amenazas físicas, y lograr ciudades más inteligentes y seguras.[7]
- La UE lanzó una convocatoria de proyectos de 10,5 millones EUR para proyectos de ciberseguridad. La Comisión ha publicado una nueva convocatoria ofreciendo 10,5 millones EUR a través del programa Connecting Europe Facility (CEF) [Mecanismo para conectar Europa] para proyectos dedicados a mejorar las capacidades de ciberseguridad en Europa y la cooperación entre los Estados miembros.[8]

Investigación e innovaci CTI

Difusión rápida de los métodos y contenido de CTI

Durante el período de este informe se identificaron varias necesidades de investigación y las acciones para abordar estas necesidades se proponen aquí. Se han agrupado por categorías para reflejar mejor el alcance. Estas categorías, aunque puedan solaparse, indican las áreas de mejora potenciales en CTI.

- **Es necesario evaluar y representar en un contexto más amplio de CTI los resultados de los proyectos de investigación realizados en este campo** a fin de identificar los solapamientos y las lagunas, y hacerlos comparables a los productos, servicios y prácticas comerciales de CTI existentes. Esto ayudaría a difundir estos resultados a los usuarios. Al mismo tiempo, las lagunas existentes se pueden cubrir con funciones, contenido y procesos adicionales. Los proyectos de la UE (Horizonte H2020) con relevancia para la CTI son candidatos excelentes para esta tarea y contribuyen a mejorar las prácticas en materia de inteligencia sobre las ciberamenazas.
- **Deberá promoverse la provisión y el uso de material de CTI de acceso abierto.** Esto facilitaría el intercambio de conocimiento, pero también reduciría el umbral de las capacidades de CTI. Para este propósito Open-CTI es el candidato perfecto, ya que respalda la recopilación de CTI de varias fuentes en una única base que se puede compartir con varios usuarios y que ofrece, a la vez, un conjunto de funciones para gestionar esta información. Al adoptar Open-CTI los usuarios podrán obtener información valiosa con un umbral de capacidades relativamente bajo.

_Investigaciones que se están convirtiendo en tendencias emergentes

La necesidad de **reforzar la CTI** con otras herramientas de ciberseguridad establecidas requiere la evolución estructural y contextual de este dominio. De forma simultánea, los avances tecnológicos que han aportado las tecnologías emergentes plantean la cuestión de cómo la CTI se puede beneficiar de estos desarrollos. Por lo tanto, las necesidades **prospectivas de investigación** en el área de la CTI contribuyen a mejorar los procesos, funciones, automatización, estructura de contenidos y validación, provisión del servicio, velocidad de llegada al usuario o de difusión, despliegue de la CTI y asignaciones.

La CTI se ha establecido firmemente en el dominio de la ciberseguridad como herramienta esencial para mejorar la agilidad y la eficiencia contra los ataques informáticos.

Investigación e innovación en CTI

Funcionalidad, nivel de automatización y conformidad con los requisitos de madurez

- **La automatización de los procesos asumirá una función clave en la CTI**. Mientras que los ataques cibernéticos se hacen cada vez más automatizados, las organizaciones se intentan defender contra ellos de forma manual o parcialmente automatizada. Es una competición desigual que ralentiza la velocidad y la capacidad de respuesta. Investigar la potencial automatización de los procesos de CTI será vital para alcanzar el equilibrio entre los atacantes y los defensores. Para lograrlo será necesario hacer un análisis en profundidad de los pasos del proceso de CTI y de las opciones para automatizarlos mediante tecnologías disponibles y emergentes.
- **Los requisitos de madurez de la CTI deberán identificarse con más detalle**. Aunque algunos criterios y requisitos utilizados para seleccionar las funciones de CTI (p. ej., las plataformas de inteligencia contra amenazas o TIP) han sido desarrollados para diversos perfiles de usuario de CTI, será necesario establecer requisitos similares para desarrollar más productos, servicios y herramientas de CTI. Estos requisitos irán asociados a varios niveles de madurez del usuario y gastos y tipos de CTI. Es necesario utilizar criterios o requisitos similares para el resto de los elementos de la infraestructura de CTI, como las herramientas, buenas prácticas, uso compartido de plataformas, etc. Por lo tanto, aparte de desarrollar los modelos de madurez de la capacidad de CTI, se necesita investigar para ver cómo las funciones de CTI se corresponden con los diversos niveles de madurez.
- Este trabajo contribuirá a aumentar la velocidad de adopción de prácticas de CTI.
- **Utilización de IA/AA en la CTI debe investigarse con más detalle** Así se podría reducir el número de pasos manuales en el análisis de la CTI y aumentaría el valor de las funciones de aprendizaje automático en las actividades de inteligencia contra las ciberamenazas.

Tender puentes a áreas relacionadas

- **Es necesario desarrollar nuevos planteamientos para introducir el conocimiento de CTI** en los dominios que se puedan beneficiar de ello. Los campos de maniobras virtuales (*cyber-ranges*), las amenazas híbridas, las cadenas de suministro, las evaluaciones geopolíticas y las crisis son unos ejemplos. Entre las preguntas que surgen al respecto: ¿Cuáles son los puntos en los que la CTI puede tenerse en cuenta? ¿Qué contenido de la CTI es relevante? ¿Cuáles son los criterios de validación de la corrección de la información de CTI? ¿Cómo se puede asociar la CTI a información sobre el dominio concerniente? ¿Qué tipo de información de estos dominios se puede añadir a la CTI? Las sinergias que se reflejan en estas cuestiones podrían impulsar casos de uso y calidad del contenido de una forma omnidireccional.

- **La CTI es esencial para una serie de disciplinas**. Como ejemplos cabe citar la evaluación y gestión de riesgos, y la definición de los requisitos de protección y certificación. Para esas disciplinas sería beneficioso usar la CTI correctamente. La contribución de estas disciplinas a la CTI se puede identificar usando información, como los modelos de amenaza, información sobre el agente responsable de la amenaza (capacidades, motivos, etc.), métodos de ataque y programas intrusos. Aunque se dispone de algún material relevante (p. ej., marco de ataque de ATT&CK[9]), es necesario realizar bastante trabajo para identificar y estandarizar estas interfaces de información.

Investigación e innovación en CTI

Eficacia de las operaciones de CTI

- **Los métodos para usar la CTI de forma eficaz serán una herramienta para la toma de decisiones.** Estos métodos para desplegar la CTI de forma eficaz ayudarán a los encargados de la toma de decisiones a entender el valor de esta inteligencia y a los profesionales a evaluar el rendimiento de la inversión en CTI. Estos métodos o indicadores del rendimiento deberán considerar factores que van más allá de la CTI, y tener en cuenta las mejoras conseguidas en todo el ciclo de vida de la gestión de la seguridad y la mitigación de riesgos. Sería óptimo que la cuantificación de la eficacia de la inversión en CTI formara parte de una consideración mucho más amplia de la economía de la ciberseguridad en varias clases de organizaciones (p. ej., según los requisitos de seguridad, niveles de madurez, etc.).

- Aunque las herramientas de bajo coste predominan para agregar, analizar y diseminar la CTI, **podría ser necesario hacer un estudio sobre las herramientas automatizadas para gestionar la CTI** consumida y producida. Aparte de los formatos de datos estándar (p. ej., CSV STIX, TAXII), las funciones de CTI estándar podrían ser objeto de dichos estudios, seguidos por el desarrollo de herramientas de acceso abierto de bajo coste que respalden esas funciones.

Evolución de la estructura y del contenido de la CTI

- Dado que la CTI está penetrando en otros dominios, **la información sobre estos contextos debe ser notificada a la base de conocimiento de CTI original**. Por ejemplo, para captar información sobre amenazas híbridas y geopolíticas es necesario definir las estructuras de CTI. Lo mismo se puede aplicar a la relevancia de la CTI para los riesgos, incidentes, análisis forense, niveles de garantía, etc. Los formatos de CTI existentes deben evolucionar para captar la información que emana de estas dependencias de la inteligencia sobre las ciberamenazas.

- **Las tecnologías emergentes, como la IA,** podrían usarse para validar la CTI analizada. Estas herramientas podrían aumentar o reemplazar el análisis manual de la CTI y también ofrecer apoyo durante todo su ciclo de vida (p. ej., comprobar la relevancia de la CTI basándose en información existente sobre incidentes). Estos enfoques novedosos para la CTI mejorarán la calidad y la relevancia de la información.

Bibliografía

1. La Agencia Europea de Defensa (AED) fue la que definió inicialmente, en 2013, el concepto de «campo de maniobras virtual o *cyber range*» en el informe «Common staff target for military cooperation on cyber ranges in the European Union» como un entorno multiusos para respaldar tres procesos primarios: desarrollo de conocimiento, garantía y difusión.

2. "ENISA threat landscape for 5G Networks". 21 de noviembre de 2019. ENISA https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

3. https://www.concordia-h2020.eu/

4. https://echonetwork.eu/

5. https://www.sparta.eu/news/

6. https://cybersec4europe.eu/

7. https://ec.europa.eu/programmes/horizon2020/en/news/eu-grants-%E2%82%AC38-million-protection-critical-infrastructure-against-cyber-threats

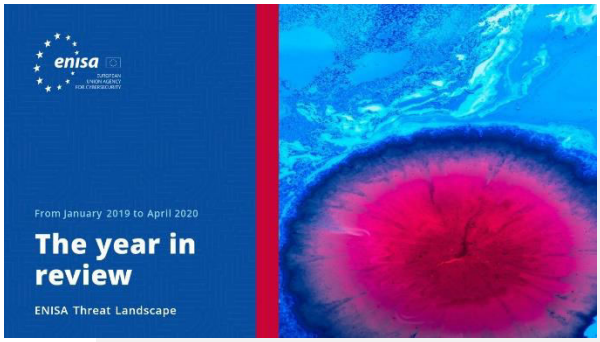
8. https://ec.europa.eu/digital-single-market/en/news/eu105-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and

9. https://attack.mitre.org/

«La CTI se ha establecido firmemente en el dominio de la ciberseguridad como herramienta esencial para mejorar la agilidad y la eficiencia contra los ataques informáticos».

en PAE 2020

Lecturas relacionad



LEER EL INFORME

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

Un resumen de las tendencias en materia de ciberseguridad de este año.

LEER EL INFORME

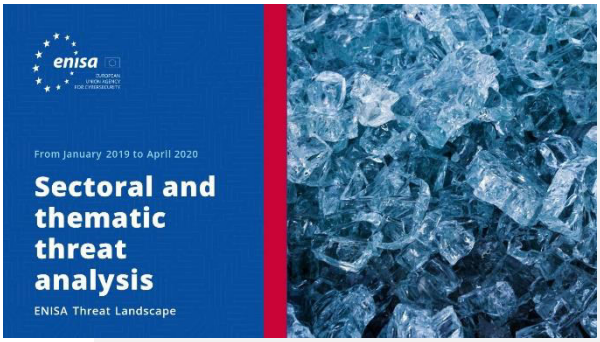
Informe Panorama de Amenazas de la ENISA
Lista de las 15 amenazas principales

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 **Incidentes principales en la UE y en el resto del mundo**

Incidentes de ciberseguridad principales que se han producido entre enero de 2019 y abril de 2020.



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

Otras publicaciones

Hoja de ruta para la cooperación entre los equipos de respuesta a incidentes de seguridad informática (CSIRT) y las fuerzas policiales

Una hoja de ruta sobre la cooperación entre los CSIRT, en particular entre las fuerzas y cuerpos de seguridad y las judicaturas nacionales y gubernamentales.

LEER EL INFORME

Informe sobre el estado del desarrollo de la respuesta de los Estados miembros de la UE ante incidentes

Un estudio dirigido al análisis de la configuración operativa actual de respuesta ante incidentes de los sectores de la Directiva sobre Ciberseguridad donde se identifican los cambios recientes.

LEER EL INFORME

ENISA Modelo de evaluación de la madurez de los CSIRT

Una versión actualizada sobre los retos para los equipos de respuesta a incidentes de seguridad informática (CSIRT) en Europa en 2016: Estudio sobre la madurez de los CSIRT publicado por ENISA en 2017.

LEER EL INFORME

«La sofisticación de las capacidades de amenaza aumentó en 2019, y hubo muchos adversarios que usaron programas intrusos, robo de credenciales y ataques multietapa».

en PAE 2020

¿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 CTI 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