

La agencia europea para la ciberseguridad publica su informe anual 2022

La invasión rusa de Ucrania dispara hasta el 24% los ciberataques patrocinados por los Estados contra Gobiernos de la UE

- El ransomware y el ciberataque de denegación de servicios ocupan los primeros puestos en el periodo analizado
- Los hackers alquilan sus servicios y golpean cada vez más las cadenas de suministros y a los proveedores de servicios
- Aiuken Cybersecurity pide a la UE a través de Allurity que destine más fondos para que Europa se defienda mejor ante estas amenazas

Madrid, 14 de noviembre de 2022.- El conflicto de Ucrania ha provocado una mayor amenaza para la ciberseguridad europea y ha disparado hasta un 24,2% los ciberataques patrocinados por países contra los estados miembros de la UE, en concreto contra sus gobiernos y administraciones públicas.

Así lo pone de manifiesto en una de sus conclusiones principales el Informe *Panorama de Amenazas de ciberseguridad 2022*, elaborado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y recogido por la multinacional española Aiuken Cybersecurity, recientemente adquirida por el fondo de capital privado Trill Impact para crear Allurity, un gigante paneuropeo de la ciberseguridad.

La agencia asegura en su informe que la invasión de Ucrania por Rusia ha "exacerbado algunos cambios" en el ciberespacio que se venían produciendo "como la actividad hacker" o el "ciberactivismo desarrollado en colaboración con acciones militares cinéticas, el cibercrimen o la financiación de estos por parte de los Estados".

La geopolítica ha pasado de esta forma a situarse en el centro del tablero de las operaciones cibernéticas. "Actores estatales han fomentado ataques destructivos", desatando una "nueva ola de hacktivismo", en la que la "desinformación" se ha convertido en un arma de la ciberguerra incluso antes de que se produjera la invasión, en lo que el informe califica como "una actividad preparatoria" por parte de Rusia.

El estudio destaca que el ransomware y los ciberataques, especialmente los de denegación de servicio, han sido las principales amenazas a la ciberseguridad identificadas en el periodo analizado. Y señala dos hechos que también han aumentado de forma preocupante. Por un lado, la extensión del modelo de negocio del "hacker como servicio", esto es, los hackers alquilan sus servicios. Y por otro, los golpes cada vez más frecuentes y eficaces sobre las cadenas de suministros, con el impacto que estas prácticas tienen sobre la economía mundial. En 2020 supusieron solo un 1% de los ataques, frente a entre el 17% y el 66% del total en 2021.

Bots y Deepfakes

Aiuken ve relevante tomar conciencia de la gravedad de las amenazas ya que, de acuerdo con el informe de ENISA, estas son innovadoras, híbridas y emergentes, y marcan el horizonte de la ciberseguridad. Entre ellas adquieren especial relevancia el uso de inteligencia artificial como herramienta para potenciar la desinformación o el recurso a los *deep fakes* y a los *bots* para alterar procesos participativos y dañar la reputación de organismos institucionales.

El informe suma otros elementos que han suscitado una mayor atención por parte de los ciberdelincuentes, como el *machine learning*, el incremento de los datos almacenados o los ataques a la tecnología operacional (OT) con el consiguiente incremento de riesgos en la industria.

Ante la gravedad de este análisis y en un contexto geopolítico tan inestable, Aiuken Cybersecurity, que protege a las grandes empresas, los sistemas de telecomunicaciones y las infraestructuras críticas, ha pedido a través de Allurity a las autoridades comunitarias un compromiso de los fondos europeos NextGenerationEU con la ciberseguridad, de manera que se destinen más dinero que le permite defenderse mejor de estas amenazas.

Para Juan Miguel Velasco, CEO de Aiuken Cybersecurity, este informe nos presenta las importantes consecuencias que los ciberataques están produciendo en nuestra propia casa, Europa. Si queremos que Rusia y otros actores no continúen interfiriendo negativamente en nuestra economía y seguridad, la UE tiene que intervenir rápida y efectivamente para detener esta situación”.

Acerca de Aiuken Cybersecurity

Aiuken Cybersecurity es una empresa internacional con sede en España que protege a las grandes empresas, los sistemas de telecomunicaciones y las infraestructuras críticas. La empresa ofrece un conjunto completo de servicios de vanguardia: detección, identificación y protección contra amenazas cibernéticas, respuesta a incidentes, e implementación y gestión de las últimas tecnologías de seguridad 24/7.

Contacto Aiuken Cybersecurity

Departamento comunicación
info@aiuken.com
Tlf. 912909805

Ion, Imagen y Comunicación

Carolina Morales/Eduardo Lobillo
carolina@ioncomunicacion.es
eduardo@ioncomunicacion.es
Tlf. +00 34 915 76 05 88
www.ioncomunicacion.es