Nota de prensa

Madrid, 04 de marzo de 2022

AXA recoge la visión de 20 expertos mundiales sobre la grave amenaza de los ciberataques

- **"Todo apunta a que la invasión de Ucrania por parte de Rusia y la escalada militar que se está viviendo catapulte a los ciberataques al primer plano de la actualidad"**

AXA Research Fund* (el Fondo para la Investigación del Grupo AXA) ha reunido en un informe los trabajos de 20 expertos procedentes de medios académicos, gubernamentales y de organizaciones internacionales para arrojar un poco de luz sobre el diseño y creación de la resiliencia informática necesaria para hacer frente a un desafío sin precedentes, como es la guerra cibernética. Entre ellos están los españoles David Ríos, catedrático AXA de análisis de riesgos adversarios en el ICMAT (CSIC) y miembro de la Real Academia de Ciencias Española; y Antonio Acín, profesor de investigación de ICREA en el Instituto de Ciencias Fotónicas (ICFO).

"Si en los primeros meses de 2020, con el inicio de la pandemia mundial, los ataques informáticos en EE. UU. aumentaron un 300% y el envío de correos maliciosos en todo el mundo lo hizo un 70%, todo apunta a que la invasión de Ucrania por parte de Rusia y la escalada militar que se está viviendo, catapulte a los ciberataques al primer plano de la actualidad", afirma Josep Alfonso, director de Comunicación, Responsabilidad Corporativa y Relaciones Institucionales de AXA.

La crisis sanitaria ha llevado aparejada una serie de cambios en los hábitos de vida que persistirán en el tiempo, como el trabajo en remoto, las actividades de compras y bancarias *on line*, o las consultas médicas digitales. Y si bien este desarrollo tecnológico ha permitido, entre otras cosas, mejorar o mantener los niveles de productividad de muchos sectores, también abre la puerta a un espacio hacia lo desconocido, lleno de desafíos y amenazas de una naturaleza ignota y en constante evolución.

Para Josep Alfonso “la incertidumbre a la que nos enfrentamos y la complejidad de los riesgos informáticos están poniendo de manifiesto las limitaciones de nuestros modelos de previsión”.

Además del aumento del número de ciberataques, cada año se observa un cambio sustancial: se ha pasado de la sustracción de datos personales, a ataques contra infraestructuras críticas, como redes de distribución, reservas hídricas y hasta sistemas sanitarios. Y los daños producidos por los delitos informáticos crecen también a un ritmo vertiginoso.

Las empresas y organizaciones se ven obligadas a hacer frente simultáneamente a una variedad de situaciones de alerta, la detección de vulnerabilidades, la aplicación de medidas de seguridad en una diversidad de sistemas y puntos terminales, y a una evaluación con mayor exactitud y en tiempo real de los datos referentes a posibles amenazas. Dada la complejidad de estas tareas, tanto empresas y como organizaciones están cambiando su posición en materia de seguridad, de una actitud defensiva a un enfoque más realista y resiliente.

Resiliencia

Si bien el desarrollo de nuevas tecnologías ofrece mayores oportunidades para los ciberataques, por otra parte, surgen nuevas técnicas de gestión de riesgos informáticos, tanto a partir de los sistemas tradicionales como de las propias nuevas tecnologías. Los riesgos informáticos son más evidentes en el caso de los sistemas de infraestructuras críticas, donde se refleja más claramente el impacto del mundo digital sobre el físico. Pero además de las técnicas físicas generadoras de resiliencia, se están desarrollando nuevos campos de conocimiento por parte de las propias máquinas y de análisis de riesgos *bajo ataque*, con el fin de generar sistemas de aprendizaje automáticos y robustos frente a acciones maliciosas. La creación de mecanismos de defensa más sólidos basados en la anticipación, el conocimiento de la estrategia del atacante y la asimetría en la información que tienen el atacante y el defensor están en la base de este enfoque orientado a lograr una mayor resiliencia.

De manera colateral, junto al reto de hacer frente a esta nueva forma de violencia, se encuentran aspectos de gran calado, como la posible vulneración de derechos fundamentales de los ciudadanos. Las actividades maliciosas en el ciberespacio se combaten con soluciones de inteligencia artificial que pueden ser invasivas e incluso poner en riesgo importantes valores sociales que las tecnologías informáticas deberían respetar. En este sentido, por ejemplo, se está trabajando en métodos experimentales para comprobar la autenticidad de la identidad personal a través de procedimientos digitales

anónimos que permitan comprobar la presencia de personas reales sin necesidad de identificarlas.

Los retos para el sector asegurador

Y en lo que respecta al sector asegurador, el camino por recorrer no es menor. A pesar del progresivo incremento de los riesgos informáticos y del reconocimiento de este problema como asunto de vital importancia tanto por parte de los expertos como del público en general, el número de gobiernos y de empresas que suscriben seguros en materia informática es todavía relativamente bajo en todo el mundo. Como consecuencia, la mayoría de las pérdidas causadas por delitos informáticos no están protegidas, hoy en día, por ningún seguro. No obstante, la demanda está creciendo, por lo que se hace necesario acelerar la preparación del sector asegurador en cuanto a coberturas se refiere.

Sin embargo, los datos referentes a situaciones de riesgo informático son demasiado escasos como para poder reconocer patrones que permitan asignar precios a los productos, la modelización en materia informática se halla todavía en una etapa inmadura, y las amenazas informáticas están en constante evolución, con impactos considerables y pérdidas muy elevadas.

Como respuesta a este problema, se han desarrollado recientemente nuevos modelos alternativos capaces de captar los efectos multiplicadores de los eventos informáticos junto con sus interacciones. Pero para alcanzar un mayor desarrollo, el sector asegurador necesita tener un mayor conocimiento y experiencia sobre este tipo de riesgos; y hacer partícipe de él a otros actores claves, como agentes y corredores de seguros.

Consulta aquí el informe
Desarrollo de resiliencia informática. Riesgos, activadores y previsión

***SOBRE AXA RESEARCH FUND**

AXA Research Fund (El Fondo para la Investigación del Grupo AXA) fue creado en 2008 con el fin de estudiar los principales riesgos que enfrenta el planeta. A través de él, AXA ha dedicado un total de 250 Millones de € en todo el mundo a la investigación científica y ha financiado 665 proyectos de investigación en áreas clave, como: riesgos para la salud, el clima y el medio ambiente; y problemas socioeconómicos. La misión filantrópica del AXA Research Fund es financiar y apoyar investigaciones científicas con potencial transformador y facilitar la toma de decisiones

MÁS INFORMACIÓN:

Relaciones con los Medios:
Gema Rabaneda: 91 538 8603/ 669465054
gema.rabaneda@axa.es
Juan Jiménez: 91 538 87 36// 625042118
juan.jimenez@axa.es
Patricia García: 91 349 0169/ 652812527
Patricia.garcia@axa.es

informadas y basadas en la ciencia, tanto en el sector público como el privado, a través de actividades de difusión y divulgación.