Crece la concienciación social contra los ciberfraudes, pero también los ataques son más sofisticados

Tanto usuarios como empresas o administraciones están cada vez más concienciados en la necesidad, más que oportunidad, de tomar las medidas precisas para afrontar los cada vez más sofisticados y especializados ataques cibernéticos. Es una de las conclusiones del **II Congreso Internacional de Ciberseguridad y Fraude Digital, organizado por la World Compliance Association** y recién celebrado en Madrid.

La ciberseguridad y el fraude digital se han convertido en temas cruciales en el panorama global debido al crecimiento acelerado de la digitalización. A medida que más sectores adoptan soluciones tecnológicas, aumentan las oportunidades para que ciberdelincuentes exploten vulnerabilidades en sistemas y redes.

La ciberseguridad abarca el conjunto de medidas y prácticas destinadas a proteger sistemas, redes y datos de accesos no autorizados o ataques maliciosos. Según informes recientes, las amenazas cibernéticas se han diversificado, afectando tanto a usuarios individuales como a empresas y gobiernos. Las cifras son determinantes para entender el escenario actual: de cada 10 delitos, 8 fueron ciberfraudes en 2023.

Los ataques más comunes, y que se han puesto de manifiesto en este Congreso, incluyen el ransomware, que consiste en el secuestro de datos mediante encriptación, exigiendo rescates económicos. El 2023 fue un año récord en este tipo de ataques, afectando incluso infraestructuras críticas.

En segundo lugar está el phishing, que lo forman correos fraudulentos diseñados para obtener información confidencial, como credenciales bancarias. Una práctica que, según David Soto, perito informático judicial, “ha aumentado de forma exponencial”. “Lo simulan todo a la perfección”, afirma.

Luego están los ataques DDoS, que consiste en la saturación de redes o servidores para interrumpir servicios, afectando especialmente a grandes empresas y plataformas digitales.

En definitiva, el fraude digital es una amenaza en expansión, en particular contra las empresas y que, como recuerda Emilio Rico, TRC Securitas Advisor, “no todos los ataques lo son a la cadena de suministro. Para esto”, apunta, “son necesarios dos ataques” lo que puede despistar a la postre.

El fraude digital, una categoría dentro de las amenazas cibernéticas, incluye prácticas que engañan a usuarios o sistemas para obtener beneficios financieros. Ejemplos destacados son el Robo de identidad, donde los ciberdelincuentes utilizan información personal para realizar transacciones o acceder a servicios en nombre de otra persona.

También están los fraudes en el comercio electrónico, que incluyen cargos falsos, clonación de tarjetas y ofertas fraudulentas en tiendas online, sin olvidar las criptomonedas y los fraudes financieros. De todos es sabido que, con la popularidad del bitcoin y otras monedas digitales, han surgido estafas piramidales y fraudes en plataformas de inversión.

¿Cómo enfrentar estas amenazas? ¿Qué estrategia pueden seguirse para ello?

Lo primero y principal es la concienciación y la formación. Tanto empresas como individuos deben estar informados sobre las tácticas más recientes de los ciberdelincuentes. Y en este sentido, la noticia es buena: “La concienciación está creciendo”, asevera Andrés Parro, FTI Consulting España.

Las amenazas también deben ser afrontadas con inversiones en tecnología. En este sentido, las herramientas de inteligencia artificial y análisis de datos permiten identificar y prevenir amenazas antes de que se materialicen. Ahora bien, los expertos, como David Soto, advierten que los fabricantes de herramientas, de dispositivos, etcétera “debería tener en cuenta que sus productos, por ejemplo un router, que puede convertirse en una puerta de entrada de ataques, han de estar preparados para afrontarlos”.

Ahí es cuando entran en juego las certificaciones, que en teoría sería garantes de que se cuenta con elementos para contrarrestar los efectos de un ataque, pero, hasta en eso, como avisa Rafael López, EMEA y Latam cibersecurity lecturer, hay que estar al quite: “Los malos te pueden configurar los filtros de tu seguridad”, de modo que esos certificados “no son garantía de que no seré atacado y estaré más protegido”, al menos no necesariamente.

Para rematar, y dado que las propias administraciones son también víctimas propiciatorias de los ciberataques y ciberfraudes, debería proceder a regulaciones gubernamentales más garantistas y protectoras. Leyes como el Reglamento General de Protección de Datos (RGPD) en la UE buscan reforzar la seguridad y privacidad de los datos personales.

Ese es el camino, pero sin olvidar lo dicho con anterioridad, que la concienciación social es clave en todo esto, es la mejor arma de prevención, que no siempre es protagonistas, pues, como recuerda Emilio Rico, “hasta que a uno no le impacta, no existe concienciación suficiente”, tanto por parte de las personas individuales como de los empresarios.

Justo en este punto, Rico pone el acento en el rol que debería desempeñar las empresas que, a su juicio, y mal por ello, “aún piensan en contratar servicios (de seguridad y ciberseguridad) más baratos, pero no tan seguros”.

El espejo en el que mirarse deben ser empresas como Google, Microsoft y Amazon, que han aumentado su inversión en ciberseguridad, mientras que gobiernos han adoptado estrategias nacionales. España, por ejemplo, opera el Instituto Nacional de Ciberseguridad (INCIBE) como eje central en la lucha contra el fraude digital y los ciberataques.

Futuro de la ciberseguridad

El avance de tecnologías como la inteligencia artificial, blockchain y el Internet de las Cosas (IoT) genera nuevos retos en ciberseguridad. Aunque estas tecnologías ofrecen oportunidades para innovar, también incrementan las posibles superficies de ataque. Los expertos predicen un incremento en la colaboración internacional y en la creación de normativas para abordar las amenazas emergentes.

En un mundo cada vez más interconectado, la ciberseguridad y la prevención del fraude digital no son solo una opción, sino una necesidad fundamental para garantizar la confianza en el ecosistema digital.

Fuente: https://delta13news.com/

LINK DE LA NOTICIA