EN BREVE

En desarrollo

CRECIMIENTO GRADUAL. Según los datos de Cyberzaintza, de 2022 a 2023 el cibercrimen ha crecido un 34,8% en Euskadi y, de cara al año que viene, esa tendencia al alza se mantiene con un porcentaje similar.

Estafas

EL CIBERDELITO HABITUAL. Los delitos por medios digitales con motivación económica son los más comunes, tanto cuando uno intenta comprar en páginas maliciosas como si recibe correos en los que los delincuentes solicitan información personal.

Prudencia

VERIFICAR. Para prevenir ser objeto de un delito por medios digitales la prudencia es primordial. Siempre se debe verificar la web en la que se realiza una compra.

El uso de la IA

EN ATAQUE Y EN DEFENSA. Los ciberdelincuentes hacen uso de la Inteligencia Artificial para promover que sus estafas sean más sofisticadas, pero también se hace uso desde el punto de vista policial.

Lucha

DOS OBSTÁCULOS. En la lucha contra el cibercrimen hay dos escollos grandes. Uno es la atribución de quién ha cometido el delito y el otro la jurisdicción del país en el que se ubica el delincuente.

das de documentos como el DNI, el pasaporte o el carné de conducir. Son documentos que se suelen solicitar cuando hay un proceso de registro. Sin embargo, se pueden robar para hacerse pasar por uno de forma fraudulenta. "Es todo un negocio y las organizaciones que perpetran estos delitos están muy preparadas", avisa.

¿Cuál es el perfil de víctima más vulnerable a un ciberdelito? Javier Diéguez asevera que en el caso de las estafas cualquiera es susceptible de caer en una trampa. "Hay algunos colectivos que son más sensibles a ciertos ataques, que son de contenido abusivo, como el *bullying*, la violencia de género o los ataques por ideología o identidad de género", expone el director general de Cyberzaintza. No obstante, "en las estafas no hay un perfil concreto", si bien es cierto que son más indefensos los colectivos que no están digitalmente alfabetizados. Es el caso de la gente de mayor edad, por ejemplo. "También hay personas que saben utilizarlo y autenticarse en la banca *online*, pero no son conscientes de los riesgos que puede haber alrededor de todo este tipo de actividad", asevera el ingeniero informático.

De hecho, la prudencia es lo único que puede proteger a uno de ser víctima de un cibercrimen. "Si algo es demasiado favorable, a lo mejor es que no es real. No hay que creerse más listo que nadie", advierte Diéguez. Por ello, a la hora de evitar caer en una estafa *online*, por ejemplo, es conveniente verificar la web a través de personas que han comprado ahí previamente o analizar las reseñas que tiene. En esa línea, evidencia que "el nivel de concienciación de la sociedad sobre cómo actuar para protegerse no es muy alto y, sin embargo, su preocupación al pensar que pueden ser víctimas sí que lo es". De hecho, según el Departamento de Seguridad, al 70% de los vascos le angustia esa posibilidad.

PROBLEMA EN AUMENTO "Se estima que este año van a rondar los 8.000 trillones de dólares el volumen de dinero que se va a defraudar a través de este tipo de actividades. Es más dinero que el que mueve conjuntamente la trata de seres humanos, la droga y el tráfico de armas", expone Javier Diéguez para dar cuenta de la magnitud de esta nueva modalidad de delinquir. El responsable de Cyberzaintza confirma que una de cada cuatro denuncias que recibe la Ertzaintza es por delitos que se han cometido por medios electrónicos. Y matiza que "muchas veces las estafas no se denuncian porque a lo mejor son cuantías pequeñas". Según los datos del Departamento de Seguridad, en lo que va de año en Euskadi se han registrado 17.061 estafas, un 29% más que en el mismo periodo de 2022. En cualquier caso, la ciberdelincuencia "es algo que no tiene pinta de que vaya a parar, sino que más bien va a crecer".

En ese sentido, hace tiempo que se lleva empleando la Inteligencia Artificial (IA) en materia de ciberdelincuencia. "Tanto en ataque como en defensa", puntualiza Diéguez. Por una parte, el uso de la IA permite que el ataque se haga de "forma más automatizada" y, por lo tanto, "más amplia". Así, las estafas se han hecho más creíbles. "Hace unos años en los ataques de *phishing* y *smishing*, que consiste en el envío de correos electrónicos o mensajes de SMS buscando datos, cambiaban de un idioma a otro, por lo que solían cometer faltas ortográficas o incorrecciones en el diseño", evidencia. Ahora todo eso está superado y estas comunicaciones son mucho más sofisticadas. Por otro lado, la IA también está al servicio de la industria de la protección, de forma que también la emplean las empresas que desarrollan la protección antimalware o el análisis de correo malicioso.

Sin embargo, en la lucha contra la ciberdelincuencia hay escollos grandes que superar. "Una es la localización o la atribución de quien ha perpetrado el crimen", expone Javier Diéguez, quien puntualiza que las organizaciones, además, suelen estar muy bien financiadas y cualificadas. "Son capaces de ocultar muy bien sus huellas", asevera. El segundo obstáculo consiste en que, incluso en los casos en los que se puede lograr la atribución, podría suceder un problema de jurisdicción. Es lo que ocurriría "si se identifica que la organización está en Corea del Norte o en un país que tenga una jurisdicción a la cual no se pueda acceder para judicializar el proceso". ●

Cyberzaintza, una agencia para promover la seguridad digital "más ambiciosa"

El nuevo servicio amplía su competencia a la ciudadanía y al sector público

✎ *Ane Araluzea*

DONOSTIA – "No somos un cuerpo policial", aclara Javier Diéguez, director general de Cyberzaintza, Agencia Vasca de Ciberseguridad, creada recientemente como una red para dotar de herramientas a la sociedad vasca con el objeto de que tome el control de su seguridad digital. La entidad capitaneada por este ingeniero informático no parte de cero, sino que previamente ya existía, desde 2017, Basque Security Center, si bien estaba adscrito al Departamento de Desarrollo Económico. Sin embargo, el contexto actual, tras una pandemia que reforzó el uso de los medios digitales, apremió a que se configurara alrededor del Departamento de Seguridad, para que pudiera actuar sobre las instituciones públicas y la ciudadanía. "Se tomó la decisión de crear algo más ambicioso que cubriese un espectro más amplio", revela Diéguez sobre su marco de competencia.

Así, la agencia, que se dio a conocer ayer en un acto presidido por el consejero de Seguridad, Josu Erkoreka, amplía su labor en la difusión de la cultura de la ciberseguridad en Euskadi a la ciudadanía y al sector público. En ese sentido, Javier Diéguez indica que su consejo de administración está formado por representantes del Gobierno Vasco, las tres diputaciones forales, los ayuntamientos de las tres capitales de la CAV y Eudel.

A nivel interno, además, la agencia colabora con otros países. "La Ertzaintza tiene sus redes de confianza en Europa, la Europol, y a nivel internacional, con la Interpol", detalla el responsable de Cyberzaintza. Javier Diéguez concreta que cuando se trata de la investigación de un delito todo cauce surge en el ámbito policial. "Aunque cuando hay que hacer una acción que no necesariamente es policial, por ejemplo, desactivar un dominio que ha sido identificado como origen de una campaña maliciosa de correo electrónico, pueden acudir a Cyberzaintza para pedirnos que a través de las redes internacionales no policiales podamos pedir la desactivación temporal o definitiva de ese dominio", ejemplifica.

De la experiencia previa con la que parten, desde Cyberzaintza concretan que en el ámbito empresarial hay "mucha reticencia a compartir experiencias negativas. Es una asignatura pendiente, no solo en Euskadi, sino en todo el sur de Europa". El principal motivo para no darlo a conocer suele ser "el miedo a la pérdida de reputación". "No es lo mismo sufrir un incidente y salir con cara de incredulidad a que tengas el mismo incidente y salgas a comunicarlo diciendo que sabes lo que hay que hacer", afirma Diéguez, quien indica que "es importante gestionar bien los protocolos de actuación porque puede haber ámbitos a los que tengas que comunicar no de manera voluntaria, sino porque hay alguna regulación que te lo exige".

Javier Diéguez, director general de Cyberzaintza. *Foto: Oskar González*

"Cyberzaintza se fundó tras la decisión de crear algo más ambicioso que cubriese un espectro más amplio"

"Compartir experiencias negativas es una asignatura pendiente, no solo de Euskadi"

JAVIER DIÉGUEZ
Director general de Cyberzaintza

Es en las empresas donde se suelen dar algunos tipos de cibercrimen concretos, como el espionaje industrial. A diferencia del *ransomware*, un tipo de estafa mediante coacción en el que uno es consciente del ataque porque no puede acceder a su información o utilizar su servicio, el espionaje "es más de guante blanco". Alguien entra en el sistema pero no quieren que se sepa. "A lo mejor están dentro de un modo latente y en un determinado momento empiezan a filtrar información de determinado tipo de interés, pero van a intentar que no te enteres para poder extraer más información", manifiesta. ●