Javier Diéguez, director general de Cyberzaintza: "El trabajo en red es importante, perseguir el cibercrimen y proteger las infraestructuras sensibles del país es un trabajo compartido".

Cyberzaintza, la Agencia Vasca de Ciberseguridad, es un organismo público, creado para combatir, de una manera integral y transversal, las amenazas derivadas del uso de Internet y las tecnologías digitales en Euskadi.

La Agencia está adscrita al Departamento de Seguridad del Gobierno Vasco, y cuenta con las herramientas y recursos necesarios para afrontar de manera global los riesgos sobre ciberseguridad. Hemos estado hablando con Javier Diéguez, el director general:

¿De dónde proviene Cyberzaintza?

Cyberzaintza es la evolución natural del Basque Cyber Security Centre (BCSC), que desde 2017 ha venido trabajando con éxito en la difusión de la cultura de la ciberseguridad en Euskadi. El modelo del BCSC presentaba limitaciones para afrontar los retos actuales de la sociedad vasca. Por ello, Cyberzaintza cuenta con un nuevo marco de competencias más amplio.

¿Por qué surge ahora?

La progresiva digitalización de las relaciones personales y en especial de las transacciones económicas han traído consigo una intensificación del número de delitos que se producen en el entorno digital.

Los datos lo indican con absoluta claridad: una de cada cuatro denuncias recibidas por la Ertzaintza son originadas por ciberdelitos, y de ellas, el 90% corresponden a ciberestafas.

En el último año, los ciberdelitos han aumentado de forma notable: a cierre del tercer trimestre de este año, se habían notificado 17.533 ciberdelitos, un 35% más que en el mismo periodo de 2022.

Por otro lado, según una encuesta realizada este mismo año por el Gabinete de prospección sociológica del Gobierno Vasco, el 70% de la sociedad vasca está muy preocupada o bastante preocupada por el riesgo de ser víctima de un ciberdelito. El 46% afirma que solo se ve parcialmente o en parte protegida de ese riesgo.

Y la previsión es que todo vaya en aumento. Estamos en un escenario sin precedentes.

"Vamos a trabajar para que la ciudadanía vasca, las instituciones públicas y el tejido empresarial nos reconozcan como la organización pública de referencia en ciberseguridad. "

¿Cuáles son los principales objetivos?

Cyberzaintza nace para informar, sensibilizar y capacitar a nuestra sociedad y a la administración pública vasca, en primera instancia, sobre la ciberseguridad, como ya veníamos haciendo con el tejido empresarial.

Cyberzaintza será el socio de confianza en la Comunidad Autónoma Vasca para los organismos de ciberseguridad del Gobierno de España, concretamente INCIBE (ciudadanía y empresas) y el Centro Criptológico Nacional (administraciones públicas). En la lucha contra el cibercrimen la colaboración no solo es clave, es indispensable.

¿Cuáles son los ámbitos de actuación?

Ciberdelincuencia: apoyo a la acción de la Ertzaintza y a los organismos judiciales para perseguir el cibercrimen, protegiendo también, dentro de este marco de colaboración, las infraestructuras sensibles del país.

Protección de infraestructuras y datos públicos: velaremos por el adecuado funcionamiento de las infraestructuras digitales del sector público vasco, en acción coordinada con este.

Protección de infraestructuras y datos empresariales: en coordinación con el departamento del Gobierno Vasco competente en materia de promoción económica.

Y, en resumen, trabajaremos para impulsar proyectos y acciones que reviertan en el desarrollo digital seguro de la Comunidad Autónoma Vasca. Realizaremos también campañas permanentes de concienciación.

Trabajaremos en red con todo tipo de organismos y agentes públicos y privados relacionados con la ciberseguridad (Ertzaintza, Osakidetza, universidades, Cybasque, etc.). El trabajo en red es importante en este sector, de modo que trabajar en la seguridad pública de Euskadi, perseguir el cibercrimen y proteger las infraestructuras sensibles del país es un trabajo compartido.

La colaboración más habitual se dará en dos ámbitos principalmente. Por un lado, en aspectos preventivos y por otro, en aspectos más relacionados con la respuesta post incidente.

El sector bancario ha intensificado su apuesta por internet. ¿Cómo afronta este sector, tan sensible, la ciberseguridad? ¿Cuáles son las amenazas más relevantes?

El sector financiero es, según todos los estudios, el más maduro en la protección de sus activos. Este sector, centra su foco en proteger dinero e información. Las amenazas suelen basarse en suplantar a la entidad y suele realizarse sobre todo a través de SMS (smishing), aunque a veces también se producen por teléfono (vishing) o por correo electrónico (phishing).

Dada la gran incidencia de las estafas en el ámbito de los delitos informáticos, hemos tratado de abordar este tema de manera prioritaria. Para ello, hemos establecido canales de colaboración con entidades ampliamente utilizadas por la población y la red de empresas de Euskadi. Así, nuestras primeras entidades colaboradoras están siendo Laboral Kutxa y Kutxabank, con las que tenemos una

"El Bizum será tan seguro como la entidad bancaria de la que seamos cliente"

colaboración fluida para informarnos bidireccionalmente de campañas maliciosas y actuar para desmantelarlas con la mayor diligencia posible.

Pagar a través de Bizum se ha extendido y puede dar la sensación de que no está tan protegido como el pago con tarjeta o la transferencia. ¿Está igualmente protegido?

Bizum apoya su esquema de protección en las aplicaciones de banca online que ofrecen las propias entidades. Es decir, será tan seguro como la entidad bancaria de la que seamos cliente. Las estafas vienen siempre provocadas porque se envía un mensaje a la víctima solicitando hacer un envío de dinero, muchas veces sin que la víctima sea consciente de que el mensaje recibido es eso: una solicitud de autorización para que el atacante pueda recibir dinero. Es un tipo de estafa muy habitual en webs de segunda mano. La web de Bizum ofrece información completa sobre estos ataques y cómo reclamar.

Las compras por Internet aumentan, ¿qué medidas tomamos para no sufrir ciberataques?

Los fraudes más habituales tienen estas características: muy buenas ofertas, productos gratuitos que se pueden conseguir con un simple clic, webs de tiendas que se hacen pasar por otras, correos electrónicos de phishing y mensajes que nos obligan a descargar un programa o aplicación.

Antes de comprar se debe tener cuidado con las ofertas que parezcan demasiado buenas. Se debe asegurar que la página en la que se va a realizar la compra es fiable, fíjarse en la referencia https del navegador, revisar las valoraciones de otras personas, etc. Además, no se debería llegar a esa página a través de enlaces que hayan llegado en emails, porque podrían derivar a páginas similares a las oficiales, pero fraudulentas. Lo mejor es teclear en el navegador la dirección de la página.

No se debe comprar a través de una wifi pública y es mejor si se utiliza una tarjeta virtual, con la seguridad de la doble autentificación. Tampoco se deben compartir las claves del banco con nadie más.

Después de la compra se debe comprobar en la cuenta bancaria que no haya cargos no autorizados. Hay que tener cuidado con los emails o SMS de empresas de transporte que urgen confirmar la dirección de entrega, y en caso de duda, es mejor confirmar directamente con la tienda.

Si por lo que sea se es víctima de estafa, hay que denunciar.

Principales retos

• **Ciudadanía**: Sensibilizar y capacitar a la población para que ellos mismos sean conscientes de los peligros existentes y se salvaguarden de posibles ataques. La autoprotección es la clave.

• **Administración pública:** Hacer red y establecer relaciones de confianza con el entramado administrativo de Euskadi, para compartir conocimiento y fortalecer la infraestructura tecnológica del país para evitar las ciberamenazas.

• **Tejido empresarial:** apoyaremos su capacitación y desarrollo digital seguro en coordinación con el departamento competente en materia de promoción económica y estableceremos la colaboración necesaria.

"Desde Cyberzaintza, vamos a trabajar para que nos reconozcan como como la organización pública de referencia en ciberseguridad".