Los ciberataques en Euskadi crecen un 48% en dos años

» J. R.

Cada mes, Euskadi registra una media de 3.500 eventos relacionados con softwares maliciosos que pueden tener impacto en organizaciones locales. Es decir, más de 40.000 incidentes potencialmente dañinos al año. Así lo advierten desde Cyberzaintza, la Agencia Vasca de Ciberseguridad, que constata un aumento del 48% en los ciberataques entre 2022 y 2024.

«Un volúmen muy significativo, porque estamos hablando únicamente de aquellos eventos que creemos que pueden tener un impacto en organizaciones vascas», explica Javier Diéguez, director general de Cyberzaintza. Entre estos ataques, los más comunes incluyen alertas sobre vulnerabilidades conocidas y explotadas activamente por grupos criminales.

Fraudes y contenido dañino

«El fraude y la estafa motivados por razones económicas representan más de la mitad de los incidentes registrados, tanto por nuestra agencia como por la Ertzaintza», subraya. Pero no solo eso: también están presentes ataques relacionados con la divulgación de contenido dañino, como la pornografía o mensajes que hieren la sensibilidad de colectivos vulnerables.

«Tenemos lo que llamamos contenido abusivo, que incluye agresiones dirigidas a menores, mujeres, o personas con identidades vulnerables», añade. Y, por otro lado, explica que también están los ataques a la disponibilidad, que buscan reducir el acceso a servicios digitales esenciales, aunque en Euskadi por ahora esto suele afectar más a páginas web corporativas. La inteligencia artificial, una espada de doble filo, también está cambiando el juego. «No solo ha aumentado el volumen de contenidos maliciosos, sino que estos son ahora más creíbles y sofisticados». Explica que antes era más fácil detectar fraudes o suplantaciones; ahora, con la IA, todo es más difícil de identificar».

Respecto a los sectores más atacados, el sector público lidera la lista. En marzo, casi la mitad de las alertas recibidas correspondieron a organismos públicos, muy por delante del ámbito privado. Ese mismo mes se detectaron 45 campañas de phishing dirigidas a la ciudadanía vasca y se confirmaron tres incidentes de ransomware

Además, un grupo prorruso, conocido como Nounen 057, llevó a cabo ataques de denegación de servicio que afectaron a 12 instituciones públicas solo en marzo, dejando claro que nadie está libre de riesgos. «No diría que hay organizaciones más o menos vulnerables, todas estamos expuestas una vez que nos conectamos a Internet».

Finalmente, el mensaje para la ciudadanía es claro: «Hay que ser prudentes para no caer en estafas y proteger especialmente a los menores, cuidando la información que compartimos sobre ellos y denunciando cualquier agresión cuanto antes». Para colectivos vulnerables, la recomendación es similar: «No deben dudar en denunciar cualquier abuso». A las organizaciones, públicas o privadas, Javier Diéguez anima a «adoptar medidas que protejan frente a las amenazas más comunes. «Es fundamental formar y concienciar a la plantilla, ya que el tiempo de detección de un ataque es clave para minimizar daños. Hay tres áreas clave en las que se debe trabajar: la detección, la prevención y, por último, la respuesta y recuperación ante los incidentes».

¿Quiénes son el blanco?

En marzo, el 42% de las llamadas recibidas por Cyberzaintza provenían del sector público, frente al 25% del privado. Además, se registraron:

» 3 casos de ransomware confirmados.

» 45 campañas de phishing desmanteladas.

» 12 instituciones públicas afectadas por ataques de denegación de servicio del grupo prorruso NoName057.

Ciberamenazas más habituales

» **Fraude y estafa:** motivados por intereses económicos, son los más frecuentes y representan la mayoría de incidentes tanto en Cyberzaintza como en la Ertzaintza.

» **Ataques a la disponibilidad:** afectan a servicios digitales como páginas web, intentando inutilizar temporalmente sistemas de empresas e instituciones.

» **Divulgación de contenido dañino:** relacionado con la difusión de materiales sensibles, como pornografía o contenidos ofensivos.

» **Contenido abusivo:** ataques dirigidos contra colectivos vulnerables por razones de edad, género, identidad o situación social.

¿Quién ataca?

El perfil del atacante ha cambiado. Ya no se trata de individuos aislados, sino de organizaciones estructuradas, globales y profesionalizadas. Hay dos grandes grupos:

» Activistas, como NoName057, que buscan desestabilizar.

» Grupos de ransomware, con estructuras corporativas, departamentos de negociación y hasta centros de trabajo, cuyo único fin es el beneficio económico.

GAIKER

Gaiker desarrolla bioignifugantes seguros y sostenibles

» Redacción SRB

El Centro Tecnológico Gaiker investiga en una nueva generación de retardantes de llama de base biológica, seguros para la salud y el medio ambiente, con el objetivo de sustituir las actuales alternativas tóxicas por otras más sostenibles.

Esta investigación se lleva a cabo en el proyecto Biosafire, coordinado por Gaiker y financiado por la Unión Europea dentro del programa Horizon Europe. En ella, se funcionalizarán aditivos de origen biológico con el objetivo de emplearlos como retardantes de llama en diversos sectores industriales. Asimismo, con el objetivo de garantizar la seguridad, sostenibilidad y funcionalidad de estos nuevos productos, se llevará a cabo una continua evaluación en las distintas fases de desarrollo empleando el método SSbD (Safe and Sustainable by Design). Estos resultados se utilizarán de forma iterativa en el diseño y la optimización de las tecnologías.

En este proyecto participa toda la cadena de valor de los materiales para poder elevar los nuevos retardantes de llama a un nivel tecnológico TRL7 y utilizarlos en cinco aplicaciones para diferentes sectores industriales: naval, ferroviario, electrodomésticos y construcción.

Gaiker llevará a cabo algunos ensayos en su laboratorio de fuego certificado.

Una de las líneas estratégicas de Gaiker, dentro de su ámbito de especialización Composites Sostenibles, se centra en la investigación de aditivos bioignifugantes. Desde este ámbito y, en colaboración con otros socios, se estudiará, dentro del proyecto Biosafire, la compatibilidad de los nuevos bioignifugantes desarrollados con matrices termoestables y termoplásticas. Asimismo, se fabricarán algunas piezas para su posterior caracterización. Entre dichas caracterizaciones, Gaiker se encargará de llevar a cabo algunos de los ensayos de fuego pertinentes, ya que cuenta con un laboratorio de fuego acreditado con certificación ENAC y Certifer y con una amplia experiencia.

A su vez, desde su ámbito de Biotecnología, el Centro Tecnológico se encargará de llevar a cabo algunos de los ensayos recogidos en el marco SSbD para determinar la seguridad de los productos a desarrollar.

Biosafire promoverá el uso del marco de SSbD y proporcionará un sólido análisis tecnológico que garantizará la futura comercialización de los materiales biobasados desarrollados.