«La Región es la comunidad que más fraudes electrónicos sufre»

Andrés Soriano
Director del departamento de Ciberseguridad (Ciso) de Universae

«Uno de los principales desafíos de la sociedad digital es la protección de los datos que se entregan a los proveedores de servicios de internet»

RAÚL HERNÁNDEZ

MURCIA. Multinacionales, organismos públicos, particulares e incluso Estados. Nada ni nadie está a salvo de los ciberdelincuentes (o 'crackers'). En los nueve primeros meses de 2022 (últimos datos que ofrece el Ministerio del Interior) se registraron 217.571 infracciones penales cometidas Internet. Representa un aumento de la ciberdelincuencia de casi un 90% respecto al 2019, año anterior a la pandemia de la Covid-19, en el que se contabilizaron 114.946 ciberdelitos. Pero esta cifra se quedará corta cuando se presente el balance anual completo de 2022, ya que a la progresión es imparable. En esta guerra sin cuartel que se libra en la Red, la Región de Murcia está en el centro del foco de los 'crackers', puesto que es la comunidad española en la que más creció la ciberdelincuencia, entre enero y septiembre del año pasado, con un incremento del 163% con respecto al mismo periodo de 2019.

Asimismo, los especialistas vaticinan que las cifras de los ciberdelitos seguirá creciendo año a año. Así lo indica el guardia civil en excedencia Andrés Soriano, que durante 12 años desempeñó funciones de analista en ciberinteligencia y ciberterrorismo. Ahora es director del departamento de Ciberseguridad (Ciso) de Universae, donde forma a profesionales de alto nivel para dirigir departamentos de ciberseguridad.

–¿A qué se debe este incremento de ciberataques y quiénes están detrás?

–La sociedad digital e interconectada en la que nos encontramos inmersos hoy en día nos aporta innumerables beneficios, tanto a nivel social, ciudadano, como corporativo. Sin embargo, este cambio de paradigma en los modelos de producción y desarrollo no está exento de riesgos. Y por ello, los ciberdelincuentes se han constituido en verdaderas células del crimen organizado, con millones de dólares en investigación y desarrollo en el análisis de vulnerabilidades, captación de datos empresariales y herramientas con las que explotar tales vulnerabilidades. Todo ello, ha supuesto que en los últimos años la industria del cibercrimen ocasione en torno a 260 millones de dólares en pérdidas a nivel mundial. Y por supuesto, en España no somos ajenos a este fenómeno, pues el informe sobre la cibercriminalidad refleja como los ciberdelitos han crecido en los últimos años un 89%. Y en este año 2023, se espera que estas cifras sigan aumentando. Ejemplo de ello son los ciberataques a infraestructuras críticas españolas, como los sufridos durante estos años al Ministerio de Hacienda, al Consejo Superior de Investigaciones Científicas, o esta misma semana en el Hospital Clinic de Barcelona.

–¿Por qué la Región de Murcia es la comunidad que más ciberataques sufre?

–El estudio sobre el balance de la criminalidad, evidencia como el cibercrimen ha aumentado de forma significativa en todo el país y la Región se erige como una de las comunidades como mayor número de denuncias, sobre todo por fraudes electrónicos, y en ello influye las compras por internet. Tenemos que sumarle que estamos en una comunidad turística y costera, lo que favorece la proliferación de estafas vacacionales. También podemos destacar el gran impulso que la Región está haciendo en favor de nuevas modalidades laborales como el teletrabajo. Que si bien tiene innumerables beneficios, es cierto que los trabajadores deben tener concienciación en ciberseguridad junto a formas de comunicación seguras, por ejemplo a través de servicios de VPN con sus respectivas empresas.

Andrés Soriano en el laboratorio de ciberseguridad de Universae.

INCREMENTO DE ATAQUES

«Los ciberdelitos han crecido en los últimos años un 89%. Y en 2023 se espera que las cifras sigan aumentando»

PROTECCIÓN EN EMPRESAS

«La seguridad total no existe. Sin embargo, debemos mitigar los riesgos»

–¿Están adecuadamente protegidos nuestros datos?

–La experiencia que nos aportan estos ciberincidentes nos revelan que todavía no estamos en el nivel de seguridad que se debería exigir por parte de los ciudadanos, pues no es de recibo que se mantengan dispositivos obsoletos, con softwares desactualizados, y algunos de ellos ya sin ni siquiera soporte técnico de sus desarrolladores. Por su parte, las empresas y organismos están realizando esfuerzos importantes con los que poder mitigar a estas organizaciones de cibercriminales. Existe ciertas prácticas que deben incluirse en cualquier plan director de seguridad de una empresa, como la concienciación y formación de los empleados, pues el eslabón más débil de la cadena siempre es el factor humano; también se debería implementar medidas de ciberinteligencia y monitorizar este tipo de grupos criminales y tipologías de ataques. Y pese a todo ello, hay que indicar que la seguridad total no existe.

–¿Qué ciberdelitos son los más frecuentes?

–Los podríamos clasificar en dos ámbitos. Por un lado, los ciberdelitos orientados al fraude de ciudadanos y empresas. El más frecuente sigue siendo el 'phishing' (envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario). Por otro lado, nos encontraríamos otro tipo de ciberataques mucho más complejos y específicos, como son los orquestados por Amenazas Avanzadas Persistentes (APT), que son organizaciones de cibercriminales amparadas bajo algún Estado, Gobierno o Servicio de Inteligencia, cuya misión es mermar las infraestructuras críticas o el normal funcionamiento de los servicios de un país ajeno a sus intereses ideológicos, como por ejemplo provenientes de China, Rusia, Corea, Irán, etc...

–¿Cuáles son los principales desafíos a los que se enfrenta la sociedad en un mundo cada vez más digitalizado?

–Sin duda alguna la protección de los datos que entregamos a los distintos proveedores de servicios de internet, desde las conocidas redes sociales hasta las aplicaciones móviles más diversas. Los datos son oro, con ello podemos tener una mejor experiencia en internet, donde nos pueda ofrecer contenidos realizados específicamente para nosotros. Pero, por otra parte, la securización de esos datos es una parte fundamental que a veces falla, y cuando esto ocurre, nuestros datos están expuestos a cualquiera. Por eso el principal reto será defender y anonimizar esos datos.

La Comunidad repele cada mes más de 60 ciberataques, el doble que antes de la pandemia

RAÚL SÁNCHEZ

MURCIA. El ciberataque que sufrió el Hospital Clínico de Barcelona, procedente del extranjero y que obligó a anular hasta 3.000 visitas, ha puesto de relieve de nuevo la importancia de salvaguardar los sistemas informáticos contra la cibercriminalidad, cada vez más innovadora. Ante este tipo de ataques, la Región de Murcia cuenta con una estrategia de ciberseguridad que hasta el momento ha impedido con éxito numerosas embestidas de los 'crackers'. La Comunidad repelió hasta 66 ataques en el último mes, el doble de lo que se recibía antes de la pandemia, según datos de la Dirección General de Informática y Transformación del Gobierno regional.

«La situación que vivimos todas las administraciones públicas, pero también las empresas privadas es de guerra cibernética, estamos en guerra», señala Javier Martínez, director del organismo de la Región encargado de rechazar cualquier intento de desestabilización del sistema o robo de información. «Estamos recibiendo ataques de manera constante, unos más leves y otros más críticos», prosigue el informático.

Para afrontar esta problemática, la Comunidad colabora de manera permanente con el Centro Criptológico Nacional (CCN-CERT), dependiente del Centro Nacional de Inteligencia (CNI). «Trabajamos de manera conjunta y a diario», subraya el máximo responsable de informática de la Región. Los ciberataques se han duplicado tras la pandemia y, sobre todo, por la guerra de Ucrania, pasando de los 30 a los 60 al mes. Para darle una mayor consistencia a la digitalización, el Gobierno presentará en breve la Agencia de Transformación Digital que se creó en noviembre.

«Es la primera agencia a nivel regional que tiene todas las competencias en materia de digitalización, informática, telecomunicaciones y ciberseguridad», asegura Martínez, quien advierte que «la eliminación del riesgo de ataques cibernéticos al cien por cien lamentablemente no existe».