el Periódico Mediterráneo

Tribuna

Ciberdelincuencia y ciberseguridad

Los ciberataques en sus múltiples plataformas han pasado de ser noticias puntuales a ya habituales en periódicos de todo el mundo

FRANCISCO
Toledo*

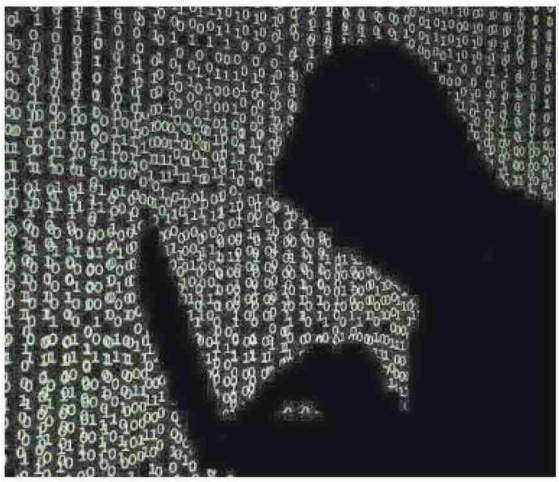
El 12 de mayo del 2017, 360.000 ordenadores de miles de empresas de 150 países (entre las que se encontraban Renault, Nissan, FedEx y en España, Telefónica) sufrieron la encriptación (el cifrado) de sus archivos y sus usuarios no pudieron acceder a ellos. La actividad de las compañías se paralizó y pasaron días antes de recuperar la normalidad.

El culpable fue un *ransomware* (así se denominan los programas dañinos que secuestran los datos) llamado *wannacrytor* (aunque más conocido como *wannacry* –efectivamente los afectados querrían llorar–). Se calculó que las pérdidas globales alcanzaron 4.000 millones de euros. Fue el ciberataque más dañino hasta esa fecha y alertó de la gravedad que podía tener este nuevo tipo de delincuencia.

Desde entonces han sido muchas las compañías e instituciones que han sufrido ciberataques con grandes pérdidas (el pasado año Maerks, la primera naviera mundial, sufrió un ataque, mediante el *ransomware* conocido como *NotPetya*, que paralizó el movimiento de contenedores en sus terminales de todo el mundo, con unas pérdidas económicas de 255 millones de euros). También multitud de entidades públicas han sido víctimas de ciberataques (seguro que recordarán los ataques en 2021 al Ayuntamiento de Castelló y al Ministerio de Trabajo).

Ransomware es uno de los tipos de *malware* (software malicioso), pero no el único. Otros son los virus, *spyware* (o software espía), troyanos, gusanos, *phishing* y Ddos. Con diversas técnicas, todos comparten el objetivo de infiltrarse en el ordenador sin el consentimiento de su propietario y obtener un beneficio económico de ello, bien sea por el robo de información con la que se comerciará, bien por el rescate que se pide para recuperar el control o directamente por estafas al conseguir las claves de acceso a cuentas o tarjetas bancarias.

Desgraciadamente los ciberataques en sus múltiples formas han pasado de ser noticias puntuales a ser noticias habituales en periódicos de todo el mundo. También han pasado de atacar a grandes empresas a atacar a cualquiera. La inmensa mayoría hemos sufrido intentos de ciberestafas (en lo que a mí respecta, puedo asegurar que es raro el día que no recibo un email que intente estafarme electrónicamente con tretas de lo más variadas) y los datos de multitud de tarjetas de crédito han sido robados cuando se hacen compras electrónicas para hacer cargos fraudulentos en esas tarjetas (revise a menudo los cargos porque suelen hacerse con cantidades pequeñas para que las estafas pasen desapercibidas y puedan reiterarse).



Las pymes, además de ser vulnerables, tienen muchas dificultades para superar un ciberataque

La pandemia del covid-19 ha tenido como consecuencia un aumento considerable de ciberataques en todo el mundo y también la diversificación de sus modus operandi. El hecho de que trabajadores de empresas y administraciones se vieran obligados a trabajar desde casa, sin que las entidades tuvieran tiempo para implementar el trabajo remoto con todas las medidas de ciberseguridad necesarias, ha tenido como consecuencia que el 86% de las organizaciones fueran afectadas *exitosamente* por un ataque cibernético, según el Cyberthreat Defense Report 2021. Un dato sorprendente de este informe es que el 57% de las víctimas de *ransomware* pagaron rescates a los ciberdelincuentes, pero a pesar de ello, casi una cuarta parte no consiguieron recuperar sus datos.

En lo que respecta a nuestro país, según el informe Panorama actual de la Ciberseguridad en España, encargado por Google a The Cocktail Analysis, el 99,8% del tejido empresarial español no se considera un objetivo atractivo para un ciberataque. Como consecuencia, casi 3 millones de empresas en España están poco o nada protegidas contra ciberdelincuentes (sea por falta de medios, de tiempo, e incluso de concienciación). Las pymes, además de su vulnerabilidad, tienen muchas dificultades para superar un ciberataque (el 60% de las pymes europeas que son víctimas de ciberataques desaparecen en los seis meses siguientes al incidente, muchas veces lastradas por el coste del ataque).

¿Y cómo estamos respecto a otros países? Según la consultora tecnológica estadounidense BitSight19, las empresas españolas se sitúan por debajo de la media europea en el ranking de ciberseguridad, mientras que países como Francia, Reino Unido y Alemania lideran el mundo, por encima de Estados Unidos y Japón.

Sin embargo, España está entre los países más avanzados en el marco legal contra la ciberdelincuencia, aunque la lucha legal choca con muchos problemas como que los ataques son globales, no vinculados a un país concreto, el anonimato inherente a internet y la dificultad de identificar el origen del ciberataque. Otra buena noticia es que en nuestro país tenemos 104 equipos de investigación en ciberseguridad, 94 de ellos en universidades, que son una buena garantía para defenderse de este tipo de delincuencia y a la vez posibilita capacidad de formación de profesionales.

Tenemos que ser conscientes de que la ciberdelincuencia está creciendo y se verá favorecida por la mayor conectividad industrial en el futuro, por la tendencia inexorable a la digitalización, por la extensión del internet de las cosas, o por el 5G con mayor ancho de banda y capacidad. Todo ello multiplica las posibilidades de ciberataques, aumenta la vulnerabilidad de empresas y particulares y hacen que la ciberseguridad sea cada vez necesaria (se calcula que en Europa se necesitarán 350.000 profesionales del sector en los próximos tres años). Recuerde que nadie está a salvo de ciberataques, así que tomemos las máximas precauciones.

***Catedrático de Ciencias de la Computación de la Universitat Jaume I de Castelló**