Abc (Ed. Galicia)
Galicia
26/02/18
Prensa: Diaria
Tirada: 3.966 Ejemplares
Difusión: 1.997 Ejemplares
Cod: 11638804
Página: 65
Sección: LOCAL Valor: 2.618,00 € Área (cm2): 522,3 Ocupación: 64,62 % Documento: 1/1 Autor: R. LIZCANO Núm. Lectores: 7988

# «Hay que aprender que nadie nos va a dar un Iphone por pinchar un link»

**Entrevista**

## Alfonso Ramírez Director general de Kaspersky Lab

R. LIZCANO
SANTIAGO

Hay guerras terrestres, navales y aéreas y, ahora, también, ciberguerras. Conscientes de que la seguridad internacional se juega también en el ciberespacio, expone Alfonso Ramírez Patiño, director general de Kaspersky Lab (empresa dedicada a la seguridad informática presente en cerca de 200 países), los estados definen desde el pasado año los ataques telemáticos como una amenaza más a tener en cuenta. Ramírez Patiño participó el viernes en el III Curso de Ciberseguridad y Delitos Informáticos, una formación organizada por el Sindicato Unificado de Policía (SUP) con el patrocinio de Kaspersky Lab y certificada para los agentes por el Centro de Estudios Universitarios de la Universidad Rey Juan Carlos.

Alfonso Ramírez Patiño. el pasado viernes en A Estrada MIGUEL MUÑIZ

**—¿De qué manera apoya una empresa como Kaspersky Lab la acción de las fuerzas de seguridad?**

—Colaboramos prácticamente con todos los países en los que tenemos presencia, y lo hacemos a distintos niveles. Con la Interpol, por ejemplo, en la desarticulación de bandas de *ransomware* [programas dañinos que infectan los equipos y encriptan los archivos exigiendo un rescate para liberarlos] responsables de ataques como el WannaCry. Con Europol tenemos un proyecto que se llama No More Ransom que ofrece herramientas de descifrado gratuitas para que las víctimas puedan recuperar sus archivos sin pagar a los delincuentes. En España, hemos colaborado en varios casos con la Policía Nacional. Si por ejemplo intervienen un teléfono y no pueden o no tienen recursos, llaman a Kaspersky o a cualquier otro fabricante de seguridad... pero las formas de colaboración son diversas. Ser especialistas en todo es muy difícil y nosotros llevamos 20 años en la ciberseguridad.

**—Ha mencionado el WannaCry, ¿cuántas empresas pagaron?**

—Se bloqueó muy rápido, pero uno de los problemas es que las empresas no te dicen si han pagado o no porque el coste reputacional puede ser alto. En España, Policía y Guardia Civil estuvieron intentando conseguir denuncias y parece que sólo registraron 5-6 cuando se infectaron más de treinta mil empresas. Las que tenían instalado Kaspersky no tuvieron ningún problema.

**—¿Puede citar algún caso público en el que hayan trabajado?**

—Ahora los grande robos de bancos son a través de Internet. Ha habido casos que se han hecho públicos a nivel mundial, como el ataque al Banco Central de Bangladesh. El grupo Lazarus hizo el mayor robo de bancos de la historia y lo hizo hackeando los cajeros. Tuvimos un banco afectado que nos llamó; cogimos un cajero, lo analizamos y detectamos la amenaza.

**—¿Cómo valoraría la preparación de las fuerzas españolas en la materia?**

—Están haciendo un buen trabajo. La policía española es una de las mejores policías en cuanto a delitos telemáticos a nivel mundial. El conocido como Virus de la Policía fue desarticulado por la policía española. Nosotros, en este caso a través del SUP, tenemos un acuerdo de colaboración y también damos formaciones con cursos como el de hoy [por el viernes] en los que abordamos cómo intervenir y procesar aparatos electrónicos para que se pueda sacar la mayor información y no se pierda su valor como prueba, cuáles son las amenazas que vienen o qué cambios de legislación afectan al cibercrimen.

**—¿Cuáles son los ciberdelitos más extendidos?**

—Es que el ciberdelito va desde compartir una foto comprometida de otra persona en whatsapp o acosar a alguien en las redes, desde el día a día más trivial —en donde además hay un montón de gente que no es consciente de que puede estar cometiendo un delito—, a acciones tipo WannaCry, que están haciendo muchísimo daño a las pymes, o las APT, que es una amenaza compleja donde el objetivo es entrar en un sistema y poder quedarse mucho tiempo para ir sacando información. Hablamos de espionaje a nivel industrial o político, o incluso de amenazas de mayor envergadura, como ataques a infraestructuras físicas: controlar una central eléctrica y dejar sin luz a una población, o amenazar a un gobierno con abrir una presa... Desde el año pasado se incluye la ciberguerra como una amenaza más para los países.

**—¿Cómo están las administraciones españolas en ciberseguridad?**

—España está muy avanzada a nivel de organismos públicos, tanto en concienciación sobre esta amenaza como en seguridad. Evidentemente queda mucho por hacer, no porque la administración española no haya hecho lo que tiene que hacer, sino por las amenazas evolucionan muy rápido.

**—Un informe reciente de Kaspersky Lab identifica FIFA2 018 y Bitcoin como los ganchos más recurrentes para robar información...**

—Es lo que se llama *phishing*, que no es más que tirar el anzuelo y ver cuánta gente pica. Tenemos que empezar a aprender que nadie va a regalarnos un Iphone por pinchar un link.

**—¿Falta todavía mucha formación?**

—Al usuario doméstico le falta un poco de formación o de concienciación, pero también a nivel empresarial. En abril llegará una nueva ley a nivel europeo que va a regular qué tiene que hacer una empresa que ha sido hackeada. Hasta ahora podía hacerlo o no público. Ahora, tendrá que comunicar qué datos se han visto comprometidos y habrá un organismo regulador que auditará si la firma puso todos los medios a su alcance para evitar el incidente. Si se concluye que no, podrá verse expuesta a una sanción de hasta un 4% de su facturación, que es muchísimo dinero.