Datos al desnudo en la era de Internet

Si de algo peca el usuario en Internet es de excesiva confianza con su información personal. Su protección es uno de los mayores retos de la ciberseguridad, que mantiene en vilo hasta a los gobiernos más poderosos del mundo. Investigadores de la Universidad Complutense de Madrid analizan las amenazas y los retos del ciberespacio con motivo del Día de la Protección de Datos en Europa que se celebra este sábado.

La ciberseguridad protege la ingente cantidad de datos vertidos en la red. / Ana Ramírez de Arellano.

MARÍA MILÁN | ¿Cuántas veces rellenamos formularios e introducimos datos personales en páginas web sin saber a dónde irán a parar? Desde 2006, la Comisión Europea, el Consejo de Europa y las autoridades de protección de datos de los Estados miembros de la Unión Europea promueven el Día de la Protección de Datos cada 28 de enero.

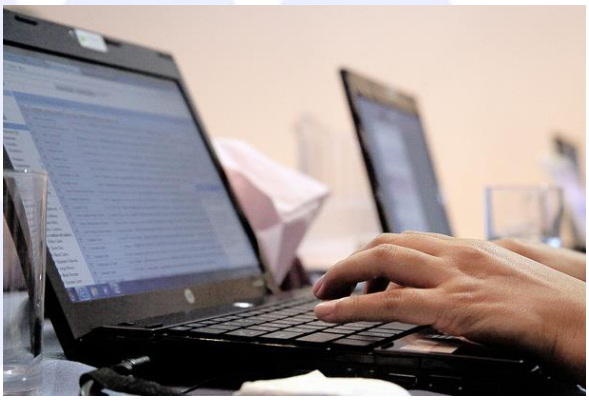
“El uso de Internet permite avances en muchas áreas y el intercambio rápido de información. El problema es establecer ese intercambio de manera segura, utilizando otras capas que permitan un mínimo de seguridad y privacidad”, puntualiza Robson de Oliveira Albuquerque, miembro del Grupo de Análisis, Seguridad y Sistemas (GASS) de la Universidad Complutense de Madrid (UCM).

Este sábado se conmemora la firma del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. El objetivo de esta efeméride es “promover el conocimiento entre los ciudadanos acerca de cuáles son sus derechos y responsabilidades en materia de protección de datos”, según la Agencia Española de Protección de Datos.

En el ciberespacio juega un papel crucial la ciberseguridad, “el conjunto de técnicas de seguridad para la protección de los equipos y redes interconectadas”, explica Luis Javier García Villalba, director de GASS y coautor de un artículo publicado en *The Journal of Supercomputing,* donde los investigadores analizan el impacto de estas técnicas en la sociedad.

“La ciberseguridad también aborda la protección lógica de los datos que son procesados, transportados o almacenados en dichos entornos”, añade García Villalba.

Criptografía renovada



El Día de la Protección de Datos en Europa vela por los derechos de los ciudadanos en el ciberespacio. / Ministerio TIC Colombia.

La ciberprotección puede llevarse a cabo a través de dos herramientas: criptografía y dispositivos o *softwares* externos. La primera convierte la información que se está manejando en ilegible, con códigos secretos.

Según Ana Lucila Sandoval, también coautora del trabajo e investigadora de GASS, esta forma clásica de protección –de la que Alan Turing fue uno de sus máximos exponentes– está abriendo nuevas puertas y renovándose gracias al auge de las criptografías cuántica y homomórfica (con cifrado algebraico).

La criptografía puede combinarse con dispositivos y *softwares* externos, como cortafuegos, sistemas de detección de intrusiones, antivirus o herramientas de análisis de datos masivos. Un campo en constante desarrollo en el que cada día surgen herramientas con funciones distintas. “Dependen mucho más del propietario de la información que de la tecnología”, matiza Sandoval.

“La ciberseguridad es una tarea cíclica y continua. Es mucho más que una herramienta”, mantiene de Oliveira. De esta forma, actúa contra los ataques a la seguridad realizados a través de Internet de las cosas, contra el *software* malicioso, contra equipos y dispositivos conectados directamente a Internet sin capas de protección y contra la falsedad y el robo de información de los Estados.

Gobiernos vulnerables

En las últimas semanas han salido a la luz casos de ciberataques entre diferentes potencias, que incluso podrían haber influido en el resultado electoral de Estados Unidos.

Según de Oliveira, los ataques cibernéticos se pueden evitar, pero es imprescindible un correcto uso de la red por parte de gobiernos, empresas y usuarios. El investigador de la UCM propone a la administración trabajar en leyes que limiten los cibercrímenes, fomentar la investigación apoyando a las universidades y establecer redes de colaboración nacional e internacional sobre seguridad de la información.

“Internet, por definición, no es seguro. El proceso de confianza en la red es distinto del usado para las relaciones humanas. El ser humano no confía plenamente en el otro antes de un proceso de aprendizaje, pero con Internet confía directamente”, advierte de Oliveira.

En cuanto a las empresas, según el estudio, algunas herramientas efectivas son las políticas de seguridad internas, mecanismos contra ciberataques y que los empleados estén más concienciados de estos riesgos.

Por último, según de Oliveira, es imprescindible que el usuario final “desarrolle su propia conciencia y conocimiento acerca de la seguridad de la información, y cómo el uso de capas de seguridad protege sus datos privados contra ataques”.

El experto alerta sobre los peligros de las redes sociales, plataformas en las que los individuos abren las puertas de su intimidad a otros usuarios. Pecar de exceso de confianza en Internet, a la larga, puede salir muy caro si no protegemos nuestros datos como lo hacemos en el entorno real.

Referencia bibliográfica: Robson de Oliveira Albuquerque, Luis Javier García Villaba, Ana Lucila Sandoval Orozco, Rafael Timóteo de Sousa Júnior y Tai-Hoon Kim. “Leveraging information security and computational trust for cybersecurity”, *The Journal of Supercomputing,* 72 (10), octubre de 2016, DOI: 10.1007/s11227-015-1543-4.