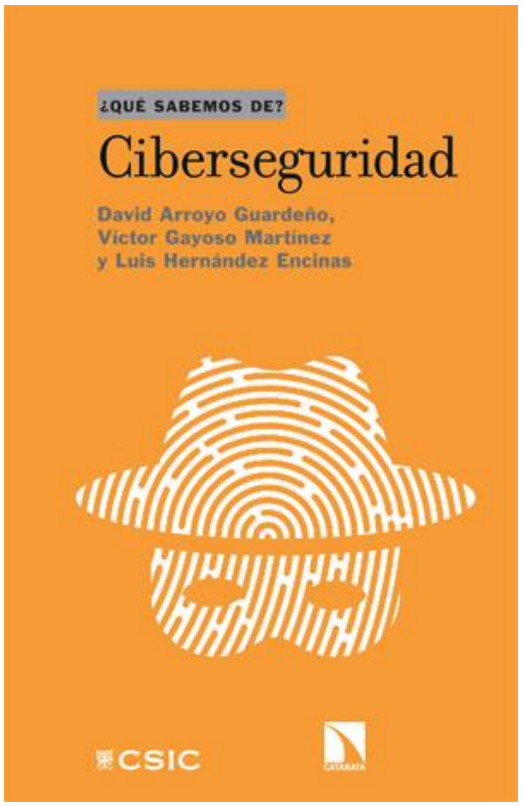
‘Ciberestafas’, robo de datos o sabotajes: un libro del CSIC analiza las nuevas amenazas surgidas en el ciberespacio

- **Ciberseguridad’ explica los riesgos que personas, empresas y estados corren en el mundo digital y propone recomendaciones para afrontarlos**

- **Los especialistas en seguridad de la información David Arroyo, Víctor Gayoso y Luis Hernández firman el último título de la colección ‘¿Qué sabemos de?’ (CSIC-Catarata)**



Madrid, 16 de diciembre de 2020. ¿Qué tiene que ver una web que instala ***cookies*** **de rastreo** sin consentimiento con un **programa informático malicioso** capaz de sabotear una central nuclear? ¿Y con un **correo fraudulento** en el que nuestro supuesto jefe nos ordena hacer una transferencia urgente? ¿O con un ataque en el que millones de dispositivos ‘inteligentes’ convertidos en zombis colapsan una web? Todas estas acciones, estén o no vinculadas, suponen una **amenaza para la ciberseguridad**, una disciplina de reciente cuño a la que está dedicado el último libro de la colección de divulgación ‘¿Qué sabemos de?’, editada por el CSIC y Catarata.

Escrito por **David Arroyo, Víctor Gayoso y Luis Hernández**, investigadores del CSIC en el Instituto de Tecnologías Físicas y de la Información (ITEFI), el texto aborda un problema, el de la seguridad de la información almacenada o transmitida en el ciberespacio, que no ha dejado de crecer en los últimos años. Un ejemplo de ello es que **en 2019 los ciberdelitos aumentaron en España un 35%** con respecto al año anterior. Como resultado, el 10% de todos los delitos cometidos el año pasado (218.302) se realizaron por medios digitales. De ellos, solo el 15% lograron resolverse y más del 88% (192.375) correspondieron a fraudes informáticos o estafas, según recoge la Secretaría de Estado de Seguridad.

CSIC
Área de Cultura Científica
Tlf: 91 568 00 43

Serrano, 117
28006 Madrid
divulga@csic.es

Estas prácticas afectan a particulares, empresas y estados, que sufren sus consecuencias más allá del mundo virtual. "El ciberespacio no es un mero anexo del mundo real, sino uno de los elementos que actualmente lo configuran, por lo que se puede constituir en causa y efecto en el mundo físico", precisan los autores. Así, se han documentado ataques con software que han producido **daños en infraestructuras críticas**, como el que en 2014 impidió el apagado controlado de unos altos hornos en Alemania o el que en 2010 afectó a la central nuclear iraní de Natanz, conocido como **Stuxnet**.

Más allá de los casos en los que se han visto comprometidos sectores estratégicos, Accenture señala que en los próximos cinco años **las empresas del sector privado corren el riesgo de perder alrededor de 5,2 billones de dólares debido a los ciberataques**, lo cual es casi el tamaño de las economías de Francia, Italia y España juntas. Por su parte, la Oficina Europea de Estadística indica que **España es el país de la Unión Europea con más víctimas de robo de identidad registradas:** el 7% de los internautas españoles habría sido víctima de este delito en los últimos 12 meses, en comparación con la media comunitaria del 4%. En muchas ocasiones la suplantación tiene como objetivo realizar compras, transferir dinero desde la cuenta corriente de la persona afectada o abrir nuevas cuentas para el blanqueo de dinero.

Una completa taxonomía de amenazas

En la detallada descripción de ataques que recoge el libro, el ***phishing*** (homófono inglés de *fishing*: 'pesca') recibe especial atención por ser uno de los más extendidos. "En este fraude se sustituyen las direcciones de páginas de Internet legítimas con otras parecidas pero controladas por los atacantes, de manera que el usuario acaba introduciendo datos confidenciales en la web falsa creyendo que se trata de la original", aclaran los investigadores del CSIC.

El *phishing* suele estar relacionado con **ataques de 'ingeniería social'**, que buscan engañar a los usuarios para que faciliten de manera voluntaria información personal confidencial (contraseñas o datos bancarios) que permita el acceso a un equipo e instalar software malicioso (*malware*). "Es una práctica común porque, en ocasiones, **es más sencillo engañar a un usuario que vulnerar la seguridad de sus equipos informáticos**", apuntan los autores. Un ejemplo de esto es "el llamado **fraude del director ejecutivo**, en el que un empleado con capacidad para acceder a datos de las cuentas bancarias recibe un correo, supuestamente de su director, solicitándole ayuda para una operación financiera confidencial y urgente", añaden. Este tipo de estafas se conoce como *whaling* (caza de ballenas) por tratarse de un *phishing* dirigido a 'peces gordos' (ballena o *whale*).

Los **ataques de denegación de servicio** (DDoS) contra sitios web, en los que se hace un uso masivo de dispositivos conectados a la Internet de las cosas o de teléfonos móviles

que no están protegidos convenientemente; el **robo de datos personales** por piratas informáticos, pero también por empresas y estados, como demuestra el caso de **Cambridge Analytica**; o las vulnerabilidades que afectan a la mayoría de los fabricantes de procesadores, **como Intel, AMD y ARM**, son otras de las tantas amenazas analizadas en *Ciberseguridad*.

El riesgo del teletrabajo

Los autores critican que **las herramientas de teletrabajo,** que desde marzo de 2020 han experimentado un crecimiento estimado del 84%, **se han adoptado de modo improvisado**: "es deseable que todos los teletrabajadores sigan unas buenas prácticas de ciberhigiene, como evitar la instalación de software no autorizado por los responsables de ciberseguridad, no conectarse a redes wifi públicas o no responder correos sospechosos de *phishing*. Ahora bien, una buena política de seguridad no asume sin más que esas normas de ciberhigiene se van a cumplir, sino que establece mecanismos de control para salvaguardar la seguridad en caso de incumplimiento. Pues bien, en la crisis de la COVID-19 el teletrabajo se desplegó, en muchos casos, sin que los trabajadores tuvieran arraigada esa disciplina de ciberhigiene y sin que su empresa tuviera diseñada una política de seguridad adecuada".

Esta situación ha propiciado que **"el virus biológico y el virus cibernético hayan progresado casi a la par",** ya que "los 'malos' —como diplomáticamente, y de forma habitual, uno se refiere a los atacantes— son conscientes de que el usuario medio es el eslabón más débil en la cadena de seguridad, por lo que sus ataques se dirigen a quienes le oponen menos resistencia", agregan.

¿Quién está detrás de los ciberataques?

El libro distingue entre tres tipos de profesionales de la seguridad: los ***hackers* de sombrero blanco o éticos**, cuyo objetivo es ayudar a mejorar la seguridad de la entidad para la que trabajan; los ***hackers* de sombrero gris**, que buscan mejorar la seguridad, pero utilizan métodos que no son éticos, como la divulgación de vulnerabilidades; y los ***hackers* de sombrero negro**, que persiguen una ganancia personal a través de actividades maliciosas o de amenazas.

Estos últimos son los **'ciberdelincuentes'**, que a su vez pueden dividirse en dos grupos: los 'profesionales', que proceden del mundo empresarial o son pagados por los gobiernos generalmente con el fin de robar datos confidenciales, y 'ladrones', que utilizan datos o identidades robadas para obtener un ingreso monetario. Se estima que, en 2018, **más del 80% de la actividad dañina se debió a los ciberdelincuentes**, cuyas principales formas de actuación son la propagación de código *malware* a través del correo electrónico –**más del 60% del tráfico mundial de correo electrónico en 2018 contenía software dañino**–, el *phishing* basado en técnicas de ingeniería social y

la puesta en marcha de plataformas en las que se ofrecen servicios para llevar a cabo ciberdelitos.

Otros perfiles mencionados en el libro son los **'ciberterroristas'** y los ***hacktivistas***, que, junto a la acción de otros estados, constituyen la principal amenaza para la ciberseguridad nacional. "La mayor parte de los gobiernos sufren ataques desarrollados en otros países, ya sean desplegados por los propios estados o por grupos subvencionados por tales estados", afirman Arroyo, Gayoso y Hernández. "Los principales objetivos de estos ataques son conseguir información política y estratégica y el sabotaje, es decir, la interrupción de la normal prestación de servicios esenciales y tratar de influir en la opinión pública de los países atacados", explican.

Por último, los especialistas del CSIC se ocupan del **personal interno**: "usuarios normales o con privilegios, *insiders*, que por negligencia o por maldad pueden resultar dañinos a una empresa u organización". Se estima que **alrededor del 25% de los incidentes en entornos corporativos se debe a personal interno**.

Buenas prácticas de ciberseguridad

El texto incluye numerosos **consejos para preservar la seguridad de los usuarios**. No abrir correos electrónicos de remitentes desconocidos, comprobar que las páginas visitadas sean legítimas, utilizar contraseñas robustas que mezclen mayúsculas y minúsculas, números y signos de puntuación o guardar las contraseñas en un sitio seguro son algunas de las medidas propuestas para evitar la suplantación de identidad.

Para quienes utilicen **ordenadores**, los autores insisten en la necesidad de mantener actualizado el sistema operativo y el software, utilizar programar *antimalware* o limitar los accesos con roles de administrador a la computadora. En el caso de los **móviles**, subrayan la importancia de **utilizar un PIN o un patrón gráfico de desbloqueo que contenga entre seis y ocho dígitos o puntos de malla**, no conectarse mediante redes públicas no confiables (bares, restaurantes, hoteles o aeropuertos) si se van a transmitir datos confidenciales o personales o no conectar el dispositivo a puertos USB que no sean de confianza. También recomiendan no descargar software de lugares no confiables o revisar los permisos que las aplicaciones solicitan: "**si un usuario desea instalarse una lupa o una linterna, no debería consentir que tal aplicación pidiera permiso para acceder a sus contactos o a la agenda**".

En ambos tipos de dispositivos, los científicos aconsejan el **uso de herramientas antiseguimiento**: extensiones o complementos de los navegadores que bloquean elementos como *scripts*, ventanas emergentes, *cookies*, botones sociales o anuncios. "Casi todos hemos notado que, poco después de haber consultado una web para buscar un hotel, un vuelo o un curso, cuando visitamos otra web dicha página nos ofrece publicidad sobre eso que habíamos consultado poco tiempo antes: esto se debe a que hemos sido víctimas de un seguimiento", denuncian.

Soberanía digital y derechos de ciberciudadanía

Más allá de lo que pueda hacer cada usuario individual, *Ciberseguridad* pone el foco en las medidas colectivas. Una de ellas es **recuperar la 'soberanía digital': el hecho de que un estado**, **pueda desarrollar sus propias tecnologías y capacidades ofensivas y defensivas de ciberseguridad.** "La falta de mascarillas en los inicios de la crisis COVID-19 en Europa nos pone en aviso sobre los problemas de la externalización generalizada de la producción. Esto no es exclusivo del sector biosanitario: en el modelo de telesociedad que se adoptó desde marzo de 2020 en Europa, un grueso muy notorio de los recursos que permitieron dar continuidad al trabajo y la enseñanza estuvieron basados en tecnología no europea, lo cual puede suponer un problema en términos de seguridad nacional", señalan los autores.

Otro de los cambios propuestos es "**generar una cultura de ciberseguridad que impulse una sólida alfabetización digital"** y ayude a los usuarios a identificar las tecnologías que pudieran estar erosionando sus derechos, como el derecho a la privacidad. "Si contribuimos a reducir el volumen de datos de los que dispondrían los atacantes y los adversarios en el tablero cibergeopolítico, estos tendrán más dificultades para entrenar sus modelos de inteligencia artificial y construir operaciones de información para desestabilizar el espacio de toma de decisión en nuestra sociedad", indican.

Para terminar, los especialistas del CSIC hacen una defensa de los '**derechos de la ciberciudadanía'**: "**hace falta un nuevo giro copernicano para situar al ciudadano en el centro del ciberespacio"**, concluyen.

Ciberseguridad es el número 119 de la colección de divulgación '¿Qué sabemos de?' (CSIC-Catarata). El libro puede adquirirse tanto en librerías como en las páginas web de Editorial CSIC y Los Libros de la Catarata. Para solicitar entrevistas con los autores o más información, contactar con carmen.guerrero@csic.es (91 568 0043).

Sobre los autores

David Arroyo es ingeniero y doctor de Telecomunicación, y científico titular del CSIC. Su actividad se centra en el análisis, diseño y evaluación de sistemas para la protección de la seguridad y de la privacidad de la información.

Víctor Gayoso es ingeniero y doctor de Telecomunicación. Trabaja en el ITEFI-CSIC, donde investiga, diseña y desarrolla aplicaciones criptográficas y analiza aplicaciones y protocolos de ciberseguridad.

Luis Hernández es doctor en Matemáticas y director del Departamento TIC del ITEFI-CSIC. Su investigación incluye la criptografía de criptosistemas de clave pública, esquemas de firma digital, protocolos de autenticación e identificación o *blockchain*, entre otros.