Cuanto más digitales, más cibervulnerables

La digitalización ha traído consigo las ciberamenzas y la proliferación de delincuencia a través de internet. Resulta crucial que el usuario de las redes conozca bien los riesgos a los que se enfrenta y que tenga los medios para evitarlos.

El vivir en un mundo digital nos convierte en víctimas potenciales de recibir ataques a través de internet. Ninguna persona o empresa está a salvo, y se calcula que a finales de 2020 el coste anual de la ciberdelincuencia para la economía mundial alcanzó los 5,5 billones de euros, el doble de la cifra de 2015. La invasión de Ucrania en 2022 no ha hecho más que agravar la situación, pues ha movilizado a ejércitos de *hackers* y ciberactivistas a favor de uno u otro bando, dispuestos a sembrar el caos y la destrucción en las redes.

La ciberseguridad se ha convertido en la pieza clave de transición digital, pues solamente una estrategia de defensa y protección robusta y efectiva ante las amenazas que proliferan por el ciberespacio puede garantizar una navegación segura en un entorno de confianza. Pero, igual de relevante resulta que los usuarios sean

perfectamente conscientes de los riesgos asociados al uso de tecnología, y que sepan evitarlos.

Año tras año los ciberdelitos aumentan en número e intensidad. En lo que va del año en curso han tenido lugar notables incidentes de seguridad por todo el mundo. La empresa de seguridad Astra destaca los siguientes por su trascendencia:

- En mayo, y en el marco del conflicto de la guerra de Ucrania, la Fundación Skolkovo, que representa el esfuerzo ruso por emular Silicon Valley, sufrió un ataque por parte de hacktivistas ucranianos, que accedieron a los servidores de la organización y a sus archivos.
- Por otro lado, la plataforma de finanzas descentralizadas (DeFi) Jimbos Protocol fue objeto del robo de 4 000 unidades de la ciberdivisa Ether por un valor de 7,5 millones de dólares.
- Y más: grandes empresas británicas, como British Airways, Aer Lingus, Boots, y la BBC, sufrieron el denominado ataque a la cadena de suministro al ser hackeado el software de Transferencia de Archivos Gestionados (MFT) MOVEit que utilizan, sufriendo el robo de grandes cantidades de datos personales de sus clientes. La misma brecha de seguridad en este software afectó a la agencia francesa de empleo, Pôle emploi.
- En el mes de marzo, la Oficina de Registros Criminales del Reino Unido (ACRO) recibió un ciberataque que dejó su web fuera de servicio.
- Por su parte, la web Yellow Pages fue víctima de una acción de *ransomware*, es decir, el secuestro de información sensible mediante su encriptación a cambio de un rescate.
- Finalmente, el colectivo de *hackers* conocido como Medusa robó información personal de los alumnos de la red de centros educativos públicos de Minneapolis, para posteriormente publicarla en la *dark web*.

España se ha convertido en un objetivo preferido para los ciberatacantes. De acuerdo con un informe de la firma eslovaca de ciberseguridad ESET, durante la primera mitad del año nuestro país recibió el 4,9% de todos los ataques a escala mundial, solamente detrás de Japón (9,5%) y Estados Unidos (7,8%). El *ransomware* ha sido una de las modalidades más extendidas en este periodo, y han sufridos delitos de esta clase entidades como el Hospital Clínic de Barcelona, Euskaltel o Telepizza.

El Consejo Europeo ha destacado las principales tendencias en ciberdelincuencia que tuvieron lugar durante 2022, que son:

- El *ransomware* o ataque con programas de secuestro, destacando que el 60% de las organizaciones que lo sufrieron podrían haber pagado el rescate.
- Los ataques distribuidos de denegación del servicio (DDOS en sus siglas en inglés). Parece ser que en julio de 2022 se produjo el más grande jamás lanzado contra un cliente europeo de la empresa de ciberseguridad Akamai.
- Programas malignos o *malware*. Solamente en junio se produjeron 10 millones de descargas de troyanos de *adware*.
- Amenazas de ingeniería social, es decir, las que explotan un error humano.
- Amenazas a los datos consiguiendo acceso a un servidor.
- Ataques que afectan a la disponibilidad de internet.
- Las campañas de desinformación.
- Los ataques a la cadena de suministro, es decir, atacar a una organización aprovechando vulnerabilidades de sus proveedores.

De acuerdo con la revista *Forbes*, ya en el primer trimestre de 2023 los ciberataques globales crecieron un 7% respecto del mismo periodo del año precedente. Igualmente, estima que son detectadas 560 000 piezas de *malware* nuevas cada día, y que existen más de 1 000 millones de estos programas en circulación. Cada vez resulta más difícil mantenerse a salvo en las redes, pues la cifra de personas en el mundo afectadas por brechas de seguridad en lo que llevamos de 2023 asciende a 340 millones. Se dice pronto.

Las tendencias observadas por la empresa del sector SonicWall presentan un aumento espectacular en 2022

de los ataques dirigidos al internet de las cosas (IoT), es decir, a los dispositivos conectados a las redes, en concreto, un 87%. También creció con fuerza el *cryptojacking* o secuestro de un dispositivo electrónico sin el consentimiento o conocimiento del usuario, para aprovechar sus recursos en el minado de criptomonedas; hasta el 43%, más de 139 millones de casos. Los accesos no autorizados a sistemas aumentaron en una proporción más modesta, un 19%, y el uso de *malware* en los ciberataques tan solo el 2%.

Por otro lado, SonicWall subraya que las amenazas relacionadas con la encriptación y el *ransomware* disminuyeron respecto al ejercicio anterior, si bien este último ha llegado a registrar más de 490 millones de casos en el periodo considerado. El cambio de tendencia en la evolución del *ransomware*, que conoció grandes incrementos de actividad en años pasados, lo atribuyen los autores del informe a los problemas que atraviesa Rusia, nación que origina gran parte de este tipo de ciberataques (en torno a las dos terceras partes). A su juicio, las sanciones internacionales estarían afectando la capacidad de mover cantidades de dinero de los cibercriminales. No obstante, el *ransomware* sigue siendo el principal motivo de preocupación en términos de ciberseguridad para el 91% del público, según los resultados de una encuesta incluida en el informe. Igualmente, un 66% de los encuestados manifestó estar más preocupado por los ciberataques que el año anterior.

Algo que parece claro es que las mejoras en conectividad y el desarrollo de tecnología más potente son factores que juegan a favor de los cibercriminales. Por una parte, la rápida difusión de la fibra óptica y del estándar de telefonía móvil 5G posibilita el lanzar ataques más rápidos a cada vez más personas y organizaciones, a medida que las comunicaciones de banda ancha se universalizan. A la vez, la innovación en tecnologías como la inteligencia artificial pone en manos del delincuente herramientas para hacer daño progresivamente más sofisticadas y peligrosas, permitiendo crear ataques capaces de esquivar las medidas de ciberseguridad.

Ser más digitales nos hace más cibervulnerables. Por ejemplo, el teléfono móvil, un dispositivo que lleva todo el mundo en el bolso o el bolsillo, se ha convertido en un objetivo destacado para los ciberdelincuentes, de forma que, según Statista, a finales de 2022 se producían más de dos millones de ataques a móviles al mes en el mundo. Una de las prácticas más comunes de fraude es el *smishing* o envío de un mensaje de texto por parte de un delincuente a un usuario simulando ser una entidad legítima, con el objetivo de robarle información privada o realizarle un cargo económico.

Pero, a medida que la tecnología se introduce en todos los aspectos de nuestras vidas, los peligros aumentan. Pensemos en los automóviles actuales que progresivamente van incorporando más y más conectividad, ya sea a través de Bluetooth o wifi, lo que les convierte en altamente hackeables, si no cuentan con las medidas de seguridad adecuadas. Este problema se acentuará con la llegada de los vehículos autónomos, que dependen completamente de las redes para funcionar.

En suma, la ciberseguridad debe estar en el corazón de cualquier estrategia de digitalización, si bien, como se ha mencionado al principio, el usuario es la pieza más vulnerable de cualquier sistema de seguridad, y, por ello, resulta un factor crítico que conozca perfectamente los peligros a los que se enfrenta en el ciberespacio, y que disponga de los conocimientos y las herramientas para defenderse de ellos.

Imagen de Gerd Altmann en Pixabay

Brooks, C. (2023) "Cybersecurity Trends & Statistics; More Sophisticated And Persistent Threats So Far In 2023" en *Forbes*. Disponible en: https://www.forbes.com/sites/chuckbrooks/2023/05/05/cybersecurity-trends–statistics-more-sophisticated-and-persistent-threats-so-far-in-2023/?sh=27fcc8a67cb6

Consejo Europeo (2022) "Infografía – Principales ciberamenazas en la UE". Disponible en:

https://www.consilium.europa.eu/es/infographics/cyber-threats-eu/

Duggal, N. (2023) “Top 20 Cybersecurity Trends to Watch Out for in 2023” en Simplilearn. Disponible en: https://www.simplilearn.com/top-cybersecurity-trends-article

James, N. (2023) “Recent Cyber Attacks – 2023” en Astra. Disponible en: https://www.getastra.com/blog/security-audit/recent-cyber-attacks/

Ruiz de Arcaute, M. (2023) “España es el país europeo que más ciberataques recibe” en *El Debate*. Disponible en: https://www.eldebate.com/ciencia/20230714/espana-pais-europeo-mas-ciberataques-recibe_127997.html

SonicWall (2023) “2023 SonicWall Cyber Threat Report”