El estado de la seguridad en internet

Para poder llevar una vida digital hay que asegurar que las redes son seguras y fiables para el usuario. No obstante, las ciberamenazas han seguido creciendo en importancia y cantidad durante el año.

Hablamos de la confianza y de la seguridad en internet como palancas de la digitalización porque son factores necesarios para garantizar la actividad de ciudadanos y empresas en las redes. Solamente un entorno estable puede asegurar un crecimiento armónico de la vida digital. En este sentido, los principales peligros que atentan contra la confianza de los usuarios de tecnología son la ciberamenazas y la desinformación.

En el primer caso hablamos de ciberataques dirigidos a dañar sistemas o robar información, que pueden ser perpetrados por ladrones que buscan algún tipo de beneficio económico, como los ataques de *ramsonware*, que encriptan la información de la víctima para exigir un rescate, activistas, que persiguen atraer la atención sobre una causa, terroristas, dedicados al sabotaje y la extorsión, y *hackers* que solamente pretenden destruir y causar el mayor daño posible. En el segundo, se trata de la manipulación de la información con el objeto de condicionar la opinión pública, ya sea con fines comerciales o políticos e ideológicos.

La Agencia de la Unión Europea de Ciberseguridad (ENISA) señaló en su informe anual las principales amenazas y ataques que tuvieron lugar sobre los sistemas informáticos entre julio de 2021 y julio de 2022, y constató que el *ransomware* y el *malware* han seguido encabezando la lista de ciberataques, al igual que en el informe del año anterior. En el primer caso, se trata de la encriptación de datos de la organización y la solicitud de un rescate económico para restablecer la información, y, en el segundo, son programas maliciosos que desarrollan procesos no autorizados con efectos adversos en la integridad o disponibilidad de un sistema.

En tercer lugar en importancia, ENISA destaca amenazas relacionadas con la ingeniería social, seguida de las amenazas contra los datos que tienen que ver con brechas y fugas de información en las compañías, y amenazas contra la disponibilidad basadas en la denegación del servicio (especialmente ataques DDoS). El *cryptojacking*, ciberdelito mediante el que el criminal utiliza secretamente el poder de computación de la víctima para minar criptodivisas, figuraba entre los más destacados en 2021, pero parece que ha perdido relevancia en 2022, pues no aparece en la lista correspondiente.

Las campañas de desinformación siguen presentes en el palmarés del ciberdelito, y han sido impulsadas por el conflicto de Rusia y Ucrania, iniciado en febrero de 2022, como forma de condicionar la opinión pública en favor de uno u otro bando. No obstante, aparece en el ranking 2022 una nueva amenaza de peso, que son los ataques a la cadena de suministro, concebidos por ENISA como aquel en que tanto la empresa y su proveedor son objetivos de la agresión.

El informe de ENISA ha podido identificar cuatro tendencias claras que parecen guiar las ciberamenazas en 2022:

El impacto de la geopolítica, y, muy en concreto, de la guerra en Ucrania. Resulta evidente que el conflicto ha reconfigurado el escenario del ciberdelito. Las operaciones llevadas a cabo por hacktivistas (*hackers* que actúan por una causa) se han intensificado en este periodo, y han estado a menudo alineadas con acciones militares físicas. En paralelo, el empleo de la desinformación como arma de combate empezó a tener lugar incluso antes de la invasión física a Ucrania, en forma de acciones preparatorias de la campaña para condicionar a la opinión pública.

Los ciberatacantes aumentan su capacidad de hacer daño. ENISA ha detectado un uso relevante de ataques de día cero (*zero-day-attack*), que explotan la vulnerabilidad de los sistemas de defensa de las organizaciones, así como de los modelos *hacker-as-a-service*, que ponen la ciberdelincuencia al alcance de cualquiera sin necesidad de que tenga conocimientos avanzados de informática. Igualmente, aparece un aumento de los ataques a la cadena de suministro, como se ha comentado más arriba.

Los ataques de tipo ransomware continúan siendo los más extendidos. En este sentido, una encuesta internacional de Sophos llevada a cabo en febrero de 2022 arrojaba que el 66% de las empresas habían sufrido este tipo de ciberataque (en 2020 fueron el 37%). Los efectos son devastadores: el 90% vio afectada su capacidad operativa y el 86% sufrió pérdidas de ingresos como consecuencia de la agresión. En España, la proporción de empresas que han sufrido un ciberataque de *ransomware* ha aumentado del 14% en 2021 al 22% en 2022, de acuerdo con la información ofrecida por Hiscox.

No obstante, en el periodo estudiado también han cobrado importancia los ataques DDoS, en gran medida asociados al conflicto entre Rusia y Ucrania, que están ganando complejidad y dirigiéndose hacia las redes móviles y hacia las redes del internet de las cosas (IoT).

Aparecen formatos de ataques nuevos e híbridos. El escándalo relacionado con el programa espía Pegasus -que ha llegado a afectar a miembros del Gobierno de España- ha destapado el riesgo que presenta este tipo de *software* para el control y la vigilancia de la sociedad civil. Otra modalidad en auge es el *phishing* consentido, en el que la víctima da acceso a programas maliciosos en su dispositivo al hacer clic en un enlace enviado por el atacante. Los sistemas de inteligencia artificial basados en aprendizaje automático (*machine learning*) se están convirtiendo cada vez más en diana de los cibertataques. Finalmente, la propia inteligencia artificial se utiliza de forma creciente para crear y difundir *fake news* y *deep fakes* (vídeos falsos comprometedores).

El ámbito de la ciberseguridad también presenta tendencias en las prácticas de prevención y detección de riesgos. GlobalData enumera las novedades en este campo, entre las que se pueden destacar:

El uso creciente de los servicios de seguridad gestionados (*Managed security services – MSS*). Básicamente se trata de delegar la ciberseguridad de la organización en manos de un proveedor especializado, que reemplace el uso de recursos de seguridad internos. En el Reino Unido en 2022, el 40% de los negocios tienen contratado un servicio de este tipo.

Entorno zero trust o de confianza cero. Es una filosofía de ciberseguridad que parte del principio de que no se confía en nada ni nadie, aunque esté dentro de la red de la organización, ya sea un empleado de esta o sea un flujo de comunicación necesario entre dos aplicaciones: la confianza es considerada vulnerabilidad. En consecuencia, nunca se da acceso al entorno por defecto. Se trata de una aproximación totalmente opuesta al modelo de seguridad perimetral, presente en muchas empresas, que parte de la idea “confiar y verificar”.

Detección y respuesta extendidas (Extended detection and response – XDR). Consiste en un modelo de seguridad que recopila y correlaciona detecciones y datos de actividad profunda en múltiples capas de seguridad: correos electrónicos, endpoints, servidores, workloads en la nube y redes. Los análisis automatizados de este superconjunto de datos ayudan a identificar las amenazas mucho más rápido para poder prevenir y hacerlas frente.

De media, casi el 17% de las empresas españolas sufrieron en 2022 algún incidente de seguridad, de acuerdo con el Instituto Nacional de Estadística, aunque esa proporción varía ampliamente según el tamaño. Así, el 41,5% de las de 250 y más empleados tuvieron percances de seguridad, frente al 26% de las de entre 50 y 249, y el 14% de las de menos de 50 de plantilla. Sin embargo, el citado informe anual sobre ciberseguridad que realiza Hiscox destaca que la cantidad de empresas de nuestro país que han perdido clientes como

consecuencia de un ciberataque se duplicó con creces en los últimos dos años.

La ciberseguridad en España tiene un serio problema que es la falta de especialistas, algo que ocurre también en otros países de nuestro entorno. Una sociedad y una economía cada vez más digitales requieren de cada vez más protección en las redes. La pandemia ha hecho que hayamos intensificado nuestra vida digital, puesto que cada vez trabajamos y nos divertimos más en internet. Las tendencias nos dirigen hacia una economía dirigida por el dato en la que la tecnología y la información se convierten en factores de producción esenciales para cualquier sector de actividad. El teletrabajo, aunque ha perdido cierto peso respecto de las tasas que tuvieron lugar en 2020, es una modalidad en ascenso. Todo ello nos hace cada vez más dependientes del ciberespacio, y, por tanto, más necesitados de una protección efectiva ante las amenazas que acechan en internet. Por tanto, el disponer de los recursos necesarios para garantizar la ciberseguridad en nuestro país se convierte en un tema acuciante, que necesita ser abordado y resuelto con premura.

Observaciber ha calculado el volumen del desfase que se produce actualmente entre la oferta y la demanda de profesionales de ciberseguridad, que implica una carencia de talento en esta área. De esta forma, ha calculado que actualmente existe una oferta de algo más de 39 000 profesionales, que en 2024 puede haber alcanzado la cifra de 42 283. Sin embargo, la demanda puede estar en torno a los 63 200 puestos ahora mismo, y podría alcanzar los 83 000 en 2024.

ENISA (2022) “ENISA Threat Landscape 2022”

GlobalData (2022) “Cybersecurity”

Hiscox (2022) “Informe de Ciberpreparación de Hiscox 2022”

INE (2022) “Encuesta sobre el uso de TIC y comercio electrónico en las empresas”

Observaciber (2022) “Análisis y diagnóstico del talento de la ciberseguridad en España. Marzo 2022”

Sophos (2022) “El estado del *ransomware* 2022”