SEGURIDAD INFORMÁTICA

**Las amenazas a la seguridad informática que serían tendencia hoy y mañana**

*Ataques a infraestructuras críticas, como los vistos este año contra EPM y Sanitas podrían cobrar protagonismo el próximo año. El desarrollo del machine learning y la inteligencia artificial también presuponen vectores de riesgo a la seguridad informática.*

**Por Julián M. Zappia.  
Diplomatic Week.**

La seguridad informática está cobrando cada vez más protagonismo en nuestra cotidianidad, y esto es así por la irrupción que está teniendo la tecnología. En países como Colombia, la pandemia impulsó la denominada transformación digital en las empresas, que no es más que reemplazar procesos que antes se hacían de forma análoga a digital.

Esto, si bien traduce en grandes beneficios para las organizaciones, también conlleva a la necesidad de más y mejores soluciones de seguridad informática, porque si estas tecnologías son mal administradas, podrían convertirse en puertas de entrada útiles para los cibercriminales.

Lo propio sucede en nuestros hogares, ya que no solo celulares y televisores se conectan a la red Wi-Fi, sino también dispositivos inteligentes (también conocidos como IoT) como lámparas, heladeras, asistentes de voz, aspiradoras y cortinas, entre una amplia lista que se hace más larga conforme pasan los años.

La premisa es la misma: dispositivos o tecnologías que mal administradas pueden convertirse en vectores de riesgo contra la seguridad informática y privacidad de sus usuarios.

La lista de “buenas prácticas” para protegerse de ataques es extensa, desde contraseñas robustas que mitiguen el riesgo de hackeo, por no conectarse a redes Wi-Fi públicas desconocidas, y no respondiendo correos de extraños que nos piden información a cambio de supuestas promociones o regalos. Todo esto daría para una serie de estrategias.

La firma de seguridad ESET, con base en el actual panorama de reportes de seguridad informática y la penetración de nuevas tecnologías, elaboró un reporte con lo que creen que será tendencia el corto y mediano plazo.

**Ataques a infraestructuras críticas.**

Se entiende como infraestructura crítica todo aquello que es de vital importancia para el funcionamiento de la sociedad. Ejemplo de esto son los servicios públicos, los sistemas de movilidad, educación y salud, entre otros.

Este año, Colombia ha visto cómo parte de sus infraestructuras críticas han sido el blanco de cibercriminales. Está el caso de Empresas Públicas de Medellín (EPM, que es una compañía prestadora de servicios públicos en Antioquia), la cual hace unas semanas reportó un ataque que la obligó a suspender la atención al público, tanto presencial como virtual, para evitar que la amenaza ganara más terreno en la compañía.

Otro ejemplo, en Argentina, hace pocos días el Instituto Nacional de Tecnología Agropecuaria (INTA) sufrió un grave ataque sobre sus sistemas informáticos.

También está el reciente ejemplo del ataque a la EPS Sanitas, en donde los crackers (delincuentes que adelantan acciones de hackeo) vulneraron la seguridad informática, accedieron a ciertos archivos personales de los usuarios y causaron el bloqueo de la plataforma virtual de la empresa.

Las previsiones de ESET apuntan a que el próximo año seguiremos viendo este tipo de ataques.

“Desde hace varios años que desde ESET hemos investigado la actividad de grupos de APT (Amenazas Persistentes Avanzadas, por sus siglas en inglés) responsables de ataques informáticos dirigidos a plantas de energía eléctrica y otro tipo de infraestructuras críticas, así como también ataques de grupos de cibercriminales que persiguen intereses económicos.

Lo que ocurrió en 2022 es que con el conflicto geopolítico entre Rusia y Ucrania comenzaron a detectarse campañas de malware (archivos de código malicioso, comúnmente conocidos como virus) con fines destructivos apuntando a organizaciones críticas en Ucrania.

Y esto ocurrió en varias oportunidades en ataques que desplegaban distintos tipos de malware que no habían sido documentados previamente.

En América Latina, los ataques de ransomware (amenazas informáticas que secuestran la información de sus víctimas) a organismos gubernamentales tuvieron una actividad importante en 2022. En Costa Rica provocaron que el gobierno decretara la emergencia nacional con varios servicios públicos afectados”, detalla la compañía.

Esto no es más que un llamado para que organizaciones, tanto privadas como públicas, activen o refuercen programas de seguridad informática, contratando soluciones o personal idóneo en la materia, diseñando campañas de educación y sensibilización con sus colaboradores, y creando protocolos de acción ante eventuales ataques informáticos, entre otras estrategias.

**Inteligencia Artificial y Machine Learning.**

La Inteligencia Artificial (IA, por sus siglas en inglés) seguramente es una de las expresiones que más cobró protagonismo este año.

Una definición sencilla sería toda aquella tecnología capaz de pensar de forma similar a la de un humano. Su aplicación ha sido diversa, desde procesos de selección de hojas de vida (con la capacidad de filtrar cientos o miles de curriculums en cuestión de minutos), pasando por aplicaciones que crean obras artísticas y llegando a chats capaces de interactuar con humanos y atendiendo conversaciones con preguntas complejas.

El Machine Learning es similar, porque es toda tecnología que le permite aprender a estas máquinas con inteligencia artificial.

Un ejemplo es una máquina que selecciona manzanas. Con base en una información previamente añadida esta podría separar las de mejor calidad pero, podría mejorar su eficiencia aprendiendo sobre la marcha y creando nuevos criterios como el color de la fruta, su tamaño, brillo, forma, etc.

Como con cualquier otra tecnología, su uso también puede ser malintencionado. Desde hace unos años hemos visto aplicaciones capaces de quitar la ropa de personas en una fotografía; poner el rostro de una persona a otra en videos o fotos, y hasta hacer que una persona diga cualquier cosa en un video.

A esto se le conoce como deep fakes (la evolución de las fake news), y se convierte en un problema porque desdibuja la línea que separa lo real de lo falso.

Un atacante, por ejemplo, podrían elaborar un video haciendo que una figura pública diga o haga algo que le podría acarrear serias implicaciones, o utilizar el mismo para labores de extorsión.

“En 2022 se registraron varios casos en los que se utilizaron para suplantar la identidad de personalidades como Elon Musk, el CEO de Binance o el CEO de FTX”, detalló ESET.

Seguramente, mientras más avanzan este tipo de ataques también cobrarán más protagonismo los analistas digitales forenses, quienes son capaces de develar la autenticidad o falsedad de un video, audio o fotografía.

**Metaverso y criptoactivos.**

Las criptomonedas no pierden vigencia en este listado de previsiones. Este año hemos visto estafas que se han cometido con estas, y el que viene no será la excepción.

La recomendación sigue siendo la misma: no invertir en algo que no se conoce, saber que nunca hay que confiar en promesas de altos réditos financieros, y ser conscientes que el precio de un cripto activo lo determina la especulación sobre el mismo, de allí que puedan llegar a ser tan volátiles.

“En el caso del metaverso, empresas como Meta, Google y también Microsoft ya están trabajando en sus propios proyectos de mundo virtual al que las personas podremos conectarnos a través de dispositivos especiales para pasar tiempo interactuando en una realidad alternativa. Según Bloomberg, se trata de la próxima gran plataforma tecnológica que tiene el potencial de convertirse en una industria con un valor de 800 mil millones para el 2024. ¿Pero qué pasará con la seguridad en estos entornos virtuales?”, cuestiona ESET.

Hace unos meses conocimos del primer caso de violencia sexual cometido en Meta, y hay quienes creen que este tipo de plataformas también podrían ser usados para suplantación de identidad, vulneración de privacidad y estafas con la compra y venta de NFT (toquens no fungibles, por sus siglas en inglés, que no son más que activos digitales acompañados de un certificado de propiedad).

“Algunas de estas tendencias consideramos van a tener un impacto el próximo año y otras más adelante. Está claro que no tenemos una bola de cristal para predecir lo que sucederá en el corto y mediano plazo. Pero si tomamos nota de los antecedentes históricos, los desafíos que se presentaron en el pasado con cada innovación tecnológica, y la velocidad con la que ocurren los cambios, estaremos mejor preparados para afrontar los desafíos que están sobre la mesa de la ciberseguridad y también aquellos que están cocinándose para más adelante”, concluyó ESET.