Engaños reinventados en la web: todo lo que no sabemos de ciberseguridad

No hay que desconocer que hoy en día cualquiera puede ser blanco de un ciberataque

Miguel Ángel Mendoza y Cecilia Pastorino, especialistas en seguridad informática de ESET Latinoamérica, nos contaron en entrevista sobre los puntos más importantes a tener en cuenta cuando hablamos de ciberataques.

¿Cuál es la diferencia entre un *hacker* y un cibercriminal?
Miguel: De acuerdo con las definiciones de la RAE, un *hacker* es un pirata informático, es decir, una persona que accede ilegalmente a sistemas informáticos ajenos, para apropiárselos u obtener información secreta.

Sin embargo, en 2017, se agregó una nueva acepción para el anglicismo *hacker*, que lo define como una persona experta en el manejo de computadores, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora. Si bien, esta definición representa la inclusión de una idea que la comunidad de seguridad reclamaba, continúa generando ambigüedades.

Aunque no se trata de la definición que muchos esperaban, es un enunciado que intenta reivindicar los logros de los profesionales de la informática que han contribuido para que podamos disfrutar de la tecnología en un ambiente cada vez más seguro.

En el ámbito de la informática, diversos personajes pueden ser considerados *hackers*, ya que sus conocimientos y habilidades han sido encausados para desarrollar nuevas y mejores tecnologías, haciéndolas cada vez más seguras.

Por el contrario, cuando personas con habilidades similares utilizan su talento para afectar a usuarios de la tecnología o llevan a cabo delitos informáticos tipificados con el fin de obtener algún tipo de beneficio, los consideramos *crackers*, atacantes o cibercriminales.

> *"Uno de los objetivos es crear, fomentar y difundir la cultura de ciberseguridad, pero para ello se requieren más años"*
> Miguel Ángel Mendoza, experto en seguridad informática

¿Qué tipo de obstáculos enfrentan las compañías en términos de ciberseguridad?
Cecilia: Con ciberataques, fugas de datos y la creciente ola de casos en los que se han reportado fallos en el control de la privacidad de clientes y usuarios, más que nunca los ojos estarán puestos en asegurar la seguridad de nuestros activos. Por lo tanto, los objetivos prácticos de la seguridad de la información deberán estar enfocados en salvaguardar la confidencialidad, integridad y disponibilidad de los sistemas informáticos y los datos. En este sentido, un hilo que atraviesa casi todas nuestras reflexiones a lo largo de este documento es el foco en protección de datos y privacidad.

En este contexto, se vaticinan cambios regulatorios para una nueva política de privacidad. Esta regulación sobre la seguridad de la información personal desencadenó modificaciones en las leyes de países latinoamericanos que impactan de forma directa a las empresas locales.

Otro desafío es la inclusión de dispositivos con internet de las cosas. Su instalación en el sistema empresarial puede significar un riesgo si no se toman las medidas necesarias. Debido a la diversidad de fabricantes y modelos, las pautas de desarrollo seguro no siempre se cumplen, por lo que es importante realizar un análisis de riesgo previo.

Finalmente, el *malware* dedicado a la criptominería es otro de los escenarios para este año. En 2018, las detecciones de mineros aumentaron 186% respecto a 2017. La mayor capacidad de procesamiento, la popularidad de las criptomonedas y la masificación de herramientas de minado desataron el *boom* del *cryptojacking*.


| FOTOLIA

¿Los ataques globales nos han mostrado qué tan vulnerables somos?
M: Totalmente. Es una realidad que los riesgos en el ámbito de la ciberseguridad se vuelven cada vez más complejos, masivos y diversos, donde los ataques de alcance mundial han mostrado la manera en la que las amenazas de la actualidad pueden afectar a cualquier usuario de la tecnología. Los ataques globales son la muestra del ambiente de riesgo actual.

Cada día son identificadas una gran cantidad de vulnerabilidades en los sistemas y aplicaciones de uso cotidiano (2018 fue el año con el mayor número de fallas reportadas con más de 16.500), mientras que, por otro lado, son identificadas una gran cantidad de amenazas. Los ataques buscan materializar los riesgos, mismos que están definidos en función de que una vulnerabilidad pueda ser aprovechada por alguna amenaza.

¿Cree que el mundo será más seguro?
M: Actualmente, se observa una tendencia a identificar más vulnerabilidades y amenazas, lo que significa mayores riesgos. Sin embargo, desde la perspectiva de seguridad, todos los días se trabaja para ofrecer productos y servicios cada vez más seguros.

Uno de los objetivos es crear, fomentar y difundir la cultura de ciberseguridad, pero para ello se requieren más años y un mayor impacto dentro de la sociedad, por ejemplo, la ayuda de los medios de comunicación, como elementos de difusión. En este contexto, es difícil predecir si en 10 años el ambiente será más o menos seguro, esto depende de qué bando lleve a cabo más y mejores acciones. Por ello, es importante que cada vez más usuarios nos preocupemos y ocupemos en nuestra seguridad digital.

¿El comportamiento de una fuerza laboral más joven, con costumbres más laxas en cuanto a seguridad, podría convertirse en una amenaza para las empresas?
M: Probablemente los comportamientos relajados en torno a la seguridad puedan representar un riesgo para las empresas, sin embargo, es importante mencionar que también cuentan con mayores habilidades en el uso de la tecnología y el acceso a la información, por lo que estos elementos juegan a su favor. En otras palabras, se puede sacar provecho de sus hábitos, para procurar la seguridad en las empresas.

| MONICA GARZÓN - PUBLIMETRO

¿Cómo proteger el material sensible de un *smartphone*?

- Utilizar solo tiendas oficiales para descargar aplicaciones.
- Revisar la cantidad de descargas y las opiniones y reputación de la aplicación.
- Revisar los permisos que solicitan las aplicaciones y evitar conceder permisos innecesarios a aplicaciones desconocidas.
- Actualizar siempre el sistema operativo y las *apps* del dispositivo.
- Realizar una copia de seguridad de todos los datos en el equipo.
- Usar el bloqueo de pantalla.
- Cifrar el contenido del dispositivo.
- Utilizar redes conocidas y privadas.