Por **José Roberto Arteaga**

EL AÑO DE LOS HACKERS

ELLOS SE HAN CONVERTIDO EN LOS PRINCIPALES ENEMIGOS DE LA DIGITALIZACIÓN. LOS EXPERTOS EN CIBERSEGURIDAD ADVIERTEN QUE EMPRESAS Y GOBIERNO REQUIEREN DE UNA ESTRATEGIA INTEGRAL PARA ENFRENTAR LAS AMENAZAS EN INTERNET.

Los expertos tienen una sola certeza frente a los *hackers*: en cualquier lugar y cirunstancia nunca estarás 100% protegido frente a un ciberataque. Pero, en este campo de batalla entre delincuentes, ciudadanos y gobiernos, no está todo pérdido.

"La preocupación número uno de muchos directores y dueños de empresas es la parte de ciberseguridad y qué pasaría en caso de un ciberataque", asegura Juan Francisco Aguilar, General Manager de Dell Technologies.

Mientras crece la adopción tecnológica de los negocios y las operaciones virtuales cobran fuerza a velocidades vertiginosas, los ciberdelincuentes se han convertido en el lado más sombrío de internet, además de una amenaza para la recuperación económica.

"En febrero pasado, se registraron 15 millones de ciberataques en México; y, en los primeros ocho meses del año, los datos son iguales que el total de 2020", de acuerdo con datos del reporte "Panorama de Amenazas en América Latina 2021", elaborador por la firma Kaspersky.

El panorama de la ciberseguridad no parece tener fin en cuanto al riesgo latente de sufrir un ataque, pero sí existe una ruta para prevenir y reforzar los controles de seguridad de grandes compañías, así como de Pequeñas y Medianas Empresas (Pymes) o firmas.

"Definitivamente, hemos visto un incremento bastante grande en los ciberataques y no sólo es en número, sino también en las capacidades de los atacantes", comenta Jorge Rodríguez, director nacional de la Maestría en Cibserseguridad del Tecnológico de Monterrey (Tec).

La necesidad de conformar una estrategia entre el sector público y el privado es urgente frente a las amenazas crecientes que hay en internet, o el camino inexorable será perder competitvidad frente a países más conscientes de las amenazas que se ciernen sobre la sociedad.

Y es que los ciberdelincuentes pueden marcar un alto parcial a la

© FREEPIK PREMIUM

DEFINITIVAMENTE, HEMOS VISTO UN INCREMENTO BASTANTE GRANDE EN LOS CIBERATAQUES Y NO SÓLO ES EN NÚMERO, SINO TAMBIÉN EN LAS CAPACIDADES DE LOS ATACANTES"

JORGE RODRÍGUEZ
DIRECTOR NACIONAL DE LA MAESTRÍA EN CIBERSEGURIDAD DEL TEC DE MONTERREY

digitalización de las empresas. "Ha sido un freno para la adopción de estas tecnologías, y no tanto porque las organizaciones no lo quieran enfrentar, sino porque realmente es complejo entender cuál es el tipo de tecnología que se debe incorporar y dar cumplimiento al tema regulatorio", dice Gabriel Oropeza, director de Innovación y Desarrollo de Negocios de DocSolutions.

El costo promedio de la pérdida de datos en los últimos 12 meses fue superior a los 648,000 dólares, en tanto que el costo promedio por el tiempo de inactividad no planificado de los sistemas en el mismo periodo rebasó los 254,000 dólares, de acuerdo con información proporcionada por el estudio "Índice Global de Protección de Datos (GDPI) de 2021".

DIGITALIZACIÓN

Las transacciones han vivido un profundo proceso de digitalización y, sobre todo, cuando el corazón del negocio se basa en la documentación para otorgar un crédito, evitar fraudes o lavado de dinero y recabar información de plataformas basadas en datos biométricos, por mencionar sólo algunos servicios.

"Hemos visto una transformación real del momento físico al mundo de las plataformas digitales y biométricas. Es una tendencia que ya existía [antes de la pandemia]: el declive de las transacciones en papel y una eventual masificación de operaciones electrónicas, cada vez más digitales; pero la pandemia lo aceleró", dice Gabriel Oropeza, director de Innovación y Desarrollo de Negocios de DocSolutions.

Esta empresa mexicana cuenta con más de 20 años en el mercado nacional. Dentro de los servicios que ofrece se encuentra el desarrollo de soluciones y tecnología enfocada en documentos, con un total de 500 clientes, principalmente en sectores como el financiero, manufactura y salud.

La digitalización abrió huecos que dan paso a fraudes o suplantación de identidad, lo que profundiza la necesidad de disminuir los riesgos de operaciones de lavado de dinero y conocer al cliente de servicios financieros.

En el año 2020, se robaron 30,000 millones de registros de datos, más que en los 15 años anteriores juntos, según Canalys.

Sin embargo, las firmas también se han encontrado con el reto de hallar tecnologías accesibles y económicas en la ruta de la transformación digital de las organizaciones, con énfasis en blindar su operación de fraudes.

Las motivaciones económicas muestran que los *hackers* no son

individuos aislados, sino miembros de organizaciones ilegales que operan para alimentar sus ganancias. "Al tener este incremento en capacidades, obviamente van a intentar diversificar sus mercados y a quienes atacan, así que ya no sólo le pegan a las empresas grandes, sino a las Pymes", comenta Jorge Rodríguez.

UN PLAN

Jorge Rodríguez, del Tec de Monterrey, cree que no se debe perder de vista al sector financiero, energía y servicios públicos, ya que pueden colocarse como los amenazados por los ciberdelincuentes.

"Es necesario que le pongamos mucho énfasis a estos elementos porque, si no, vamos a ver en los próximos años cómo algunos segmentos de la población se quedan sin agua o luz, porque estos sectores fueron atacados por criminales", dice el académico, al plantear un escenario hipotético.

Las empresas fintech son nativas digitales que pueden tener una mayor claridad en lo tocante a las estrategias de seguridad en internet. Es una ventaja competitiva frente a la banca tradicional, pero no una forma de eliminar el riesgo.

Aún se tiene la percepción de que la ciberseguridad es un gasto y no una inversión para proteger el negocio. Es una de las barreras que deben vencerse para avanzar en la mitigación de amenazas, sin importar el tamaño de la compañía.

Un 65% de las empresas enfocadas al e-commerce y fintech sólo destina entre el 1 y el 5% de su presupuesto total a la ciberseguridad, de acuerdo con el Panorama del Ecosistema de Ciberseguridad, desarrollado por Endeavor, con el apoyo de PayPal y KIO Networks.

Los esfuerzos deben encaminarse a generar una estrategia, pero también un ecosistema de ciberseguridad que tome en cuenta al gobierno, academia, empresas y a todo usuario de internet.

En este sentido, la formación de talentos también será necesaria en las estrategias de seguridad en línea. El académico del Tec de Monterrey asegura que existe un déficit, a nivel internacional, de profesionales capacitados en este rubro. "Esto requiere una interacción entre academia e industria", dice.

Las empresas comenzarán a invertir en la integración de *hubs* en México. "La innovación debe nacer segura y debemos agregarle seguridad, es decir, de forma integrada al nacimiento", dice Jorge Rodríguez.

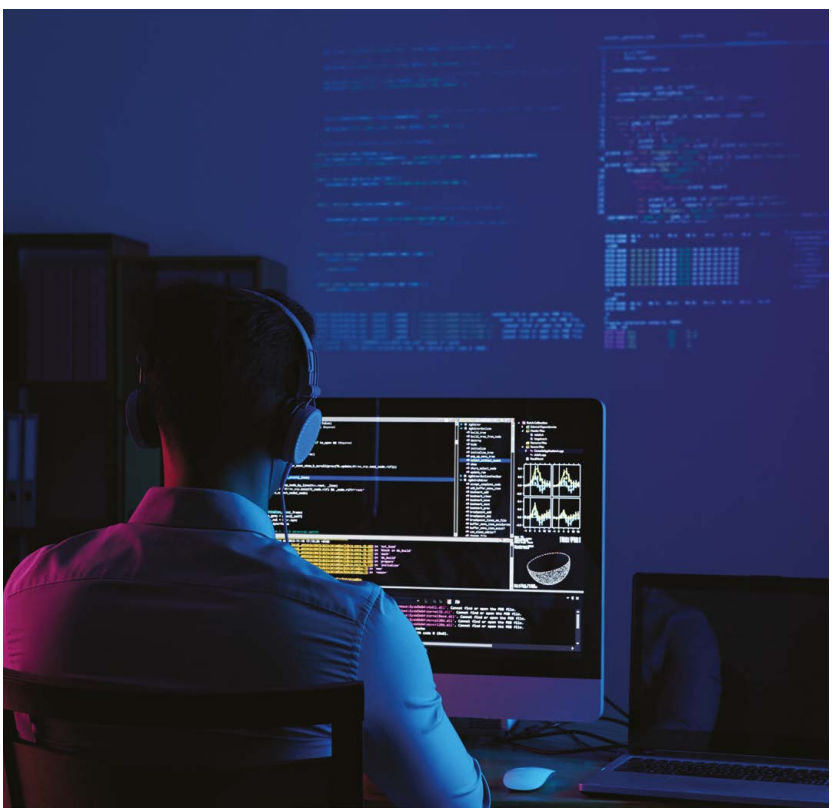
LA ESTRATEGIA

La Guardia Nacional, y el gobierno en general, tienen iniciativas para atacar el cibercrimen; sin embargo, no es suficiente. "Hace falta mucha política pública para poder legislar cuáles son los crímenes y cómo se pueden sancionar [...] ya que cambian tan rápido las amenazas que la ley se ha quedado muy corta en la estrategia de política pública", dice el especialista del Tec.

Ni el sector privado ni el público comparten, en muchos de los casos, las prácticas y experiencias en temas de ciberseguridad, a pesar de que el sector financiero es uno de los más avanzados en el desarrollo de este tipo de estrategias.

Las empresas han tenido la necesidad de proteger la operación de sus colaboradores en internet a través de la detección de intrusos y otras amenazas, además de formular un plan de acción tras un ataque de los *hackers*, dice Juan Francisco Aguilar, General Manager de Dell Technologies.

El objetivo es que las empresas estén conscientes de las amenazas en internet y, en caso de un ataque, retomen sus operaciones en el menor tiempo posible. "Una estrategia de ciberseguridad no debe ser sólo en cuestión de protección o de detección, ya que es probable que te vaya a



© FREEPIK PREMIUM

atacar; ¿qué vas a hacer en este punto para proteger la información de tus empleados, clientes o transacciones?", cuestiona el ejecutivo de Dell.

Hay tres cosas a considerar my especialmente al analizar el problema de los ciberataques: 1) nunca vas a estar protegido al 100%; 2) los mejores defraudadores están intentando ingresar en tus operaciones y robar tu información; 3) la oferta existente de seguros y servicios.

"En México, todavía no existe una estrategia integral, en términos de seguridad", dice el General Manager de Dell Technologies, quien explica que muy pocas empresas tienen en realidad un plan de acción.

Los empleados se han convertido en uno de los eslabones más vulnerables para las compañías. Dell realizó una encuesta que arrojó que más de 70% de las organizaciones requieren de datos, pero no saben cómo administrarlos.

Los sectores financiero y de telecomunicaciones son los que más demandan soluciones del grueso de la economía.

"La pequeña y mediana empresa tiene mucha hambre de tecnología. Vemos que están tratando de aprovechar tecnologías en la nube", dice el directivo, quien sabe que las Pymes son cruciales para mantener el cuidado de las grandes empresas en el negocio.

El ejecutivo asegura que cada vez que pregunta si una empresa tiene un plan de acción frente a un ciberataque, ocho de cada 10 compañías responden de forma negativa al cuestionamiento.

HACKERS ÉTICOS

Mauricio Gómez es parte de los empresarios que participan en el negocio de la ciberseguridad. Este ingeniero químico de profesión es experto del *hacking* ético y ha decidido viajar desde Colombia, su país natal, a Estados Unidos para operar su propia empresa.

Fluid Attacks es una firma dedicada a ofrecer servicio de *hacking* ético y pruebas de penetración para las compañías de tecnología. Su fin es participar en las etapas del desarrollo de software y realizar pruebas de seguridad para identificar sus vulnerabilidades.

Con su socio, Rafael Álvarez, el empresario confundó la firma en 2001, y no ha dejado de aprender sobre vulnerabilidades de software e internet.

"Hoy prestamos pruebas de seguridad desde Canadá hasta la Argentina, excepto Brasil", dice el colombiano, quien forma parte del equipo de quienes realizan los ataques para poner a prueba todos los sistemas que se consideran seguros.

Las firmas del sistema financiero realizan pruebas de seguridad una vez al año para cumplir con la regulación y verificar sus sistemas. Uno de sus objetivos ha sido explicar los informes de manera clara, para no incurrir en falsos positivos.

Un 85% de las vulnerabilidades se inyecta durante la etapa del desarrollo del software, refiere Gómez, con base en datos de Verizon, lo que muestra la importancia de actuar desde fases tempranas en las empresas.

La etapa de la emergencia sanitaria generó una mayor conciencia respecto a las amenazas de ciberataques y saldar la deuda que se tenía en materia de prevención desde las primeras etapas del desarrollo.

"Han aumentado los ataques, pero también la conciencia. Los clientes comienzan a dejar pruebas puntuales y continuas", dice el cofundador de Fluid Attacks.

Las vulnerabilidades más recurrentes se presentan al utilizar un software obsoleto, no validar los datos de entrada y emplear código fuente con información sensible.

"Vamos a seguir pagando una deuda técnica y corregir lo que ya hemos escrito, y a no escribir mal, sino construir tecnología, es decir, construir para resistir [...] la tecnología evoluciona y no va a parar [esto]", dice. F

15 millones
DE CIBERATAQUES SE REGISTRARON EN MÉXICO DURANTE FEBRERO PASADO, Y EN LOS PRIMEROS OCHO MESES DEL AÑO LOS DATOS SON IGUALES QUE EL TOTAL DE 2020

65%
DE LAS EMPRESAS ENFOCADAS AL E-COMMERCE Y FINTECH SÓLO DESTINAN ENTRE 1 Y 5% DE SU PRESUPUESTO TOTAL A LA CIBERSEGURIDAD

18%
DE LAS ORGANIZACIONES ACUDEN A UNA EMPRESA ESPECIALIZADA EN CIBERSEGURIDAD

59%
UTILIZA PERSONAL PROPIO DENTRO DEL ÁREA DE TI

30,000
MILLONES DE REGISTROS DE DATOS SE ROBARON DURANTE 2020, MÁS QUE EN LOS 15 AÑOS ANTERIORES JUNTOS, SEGÚN CANALYS

Fuente: "Panorama de Amenazas en América Latina 2021", elaborador por Kaspersky; "Panorama del Ecosistema de Ciberseguridad", de Endeavor, con el apoyo de PayPal y KIO Networks

© FREEPIK PREMIUM