Educación sobre ciberseguridad, necesidad ante avance de bancarización con la pandemia: Data Warden

José Antonio Rivera
08 de agosto de 2021, 13:42
EL ECONOMISTA

Prevenir a los usuarios sobre posibles riesgos será cada vez más importante y requiere esfuerzos compartidos, dijo Jesús Navarro, director general de Data Warden.

El temor a contagiarse de Covid-19 y los confinamientos que en una o varias ocasiones han decretado diversos países en todo el mundo desde la primera mitad de 2020 se han reflejado en una aceleración de la adopción de la tecnología financiera. Pero ese efecto social implicó algunos riesgos y necesidades.

De acuerdo con el Informe Global de Amenazas de CrowdStrike, el miedo, la preocupación y la curiosidad sobre la pandemia de coronavirus generaron condiciones necesarias para un aumento récord en los ataques de ingeniería social por parte de diversos actores del crimen cibernético en todo el mundo.

En este contexto, Jesús Navarro, director general de Data Warden, destacó en entrevista con El Economista la necesidad de la prevención a través de herramientas tecnológicas y, sobre todo, a través de la educación de los usuarios internos y externos de las empresas, así como de concientizar a los negocios.

“Hay pérdidas dolorosas”

De acuerdo con el experto, es necesario distinguir primero que las afectaciones por un ciberataque pueden ser observadas en tres aristas: las que sufren los usuarios externos e internos, por una parte, y las que sufren las propias empresas. “Las tres con diferentes consecuencias, pero todas son muy dolorosas”.

“Un usuario externo puede dejar expuesta información personal, copias de pasaportes o de actas de nacimiento, que puede ser vendida o mal utilizada y

convertirse en una verdadera pesadilla porque con tu identidad un hacker puede sacar un crédito y dejarte afectaciones financieras importantes", dijo.

"Ahora, ese mismo usuario, desde el punto de vista de la empresa, puede generar también un alto impacto, pero con la información del negocio. Quizás esa persona tiene un perfil de acceso particular en cuestión de información clave o sensible que al estar expuesta implica un gran riesgo", añadió Navarro.

El tercer punto desde el cual puede experimentarse un ciberataque, el de la empresa, tiene dos costos: la pérdida de dinero y confianza. "No hay un número exacto porque es variable según la industria, pero un promedio podría ser de medio millón de dólares, y si pagas un rescate se va al doble el promedio".

Pero para este experto, la principal pérdida de una empresa que es víctima de un ciberataque es la segunda. El principal problema es el no tener garantías sobre la operación, traducido en la incapacidad de ofrecer confianza a los clientes y colaboradores de un servicio seguro e ininterrumpido.

"Se necesita educar al usuario"

De acuerdo con Data Warden, el eslabón más débil en esta cadena siempre es el usuario y en especial el usuario interno: "la gran mayoría de los incidentes de seguridad viene por una mala configuración o perfilación de los accesos, descuidos con ligas de malware o un correo electrónico de phishing".

Actualmente, sólo 56% de los mexicanos están dentro del sistema financiero, de acuerdo con la Encuesta Nacional de Inclusión Financiera del Inegi y la CNBV, aunque en el país, 65% de las personas tienen teléfonos inteligentes. De acuerdo con Navarro, esto significa que la cifra de ataques crecerá.

"De la mano con el aumento en el nivel de bancarización los ciberataques serán más ya que habrá una mayor base de usuarios y de víctimas potenciales, pero el tema

principal es la educación. Por ahora no hay suficiente y a la gente se le hace más fácil no hacer uso de las aplicaciones bancarias", dijo.

Es por ello que destacó la necesidad de coordinar esfuerzos entre todas las instituciones gubernamentales interesadas y el sector privado, con el objetivo de dar educación sobre ciberseguridad a los usuarios, debido a la inminente aceleración de la bancarización que implicará esfuerzos en la materia.

Sobre las empresas, insistió en la necesidad de que estas sean responsables sin importar si trabajan con su propia tecnología o contratan los servicios de un tercero en la nube. "Esto es porque el costo de la prevención siempre será menor de la reacción. La recomendación es tomar mucha conciencia".

Vía:
https://www.eleconomista.com.mx/tecnologia/Educacion-sobre-ciberseguridad-necesidad-ante-avance-de-bancarizacion-con-la-pandemia-Data-Warden-20210808-0015.html