EL FINANCIERO

Fecha	Sección	Página
06.10.2020	Economía	13

¿Estamos realmente ciberseguros?

MONEDA EN EL AIRE
Jeanette Leyva Reus
@JLeyvaReus

En Estados Unidos, Canadá y Europa, octubre está dedicado a la ciberseguridad, en México será solamente una semana de un tema que debe ser indispensable conocer y, sobre todo, estar preparados para protegernos, ya que la ciberseguridad no es un tema de las empresas o instituciones financieras, sino de todos.

Los ciberdelincuentes se han modernizado e innovado para robar datos y con ello obtener dinero, lo han hecho en todo el mundo y parecen imparables por momentos, y quizás por eso en este mes dedicado al tema de la ciberseguridad es urgente que gobierno y empresas se unan y hagan un análisis real sobre si están logrando construir un frente lo suficientemente fuerte para poder detectar a tiempo los ataques y evitar ser víctimas.

Desde Londres, la experta Teresa Walsh, directora Global de Inteligencia de FS-ISAC, que es un consorcio de la industria financiera dedicado a la reducción del riesgo cibernético en el sistema financiero global, nos da interesantes reflexiones sobre lo que sucede, por ejemplo, con el *ransomware* que en el pasado era una estrategia de ataque muy específica: los criminales te robaban el acceso a cambio de un rescate; si pagabas el rescate te devolvían el acceso.

Hoy en día, explica, los criminales tienen múltiples formas de generar ingresos con esta táctica: extorsionando a la víctima para prevenir que el criminal publique en línea la información robada; subastando la información robada en la *dark web*; y "*Ransomware-as-a-Service*" donde los criminales menos sofisticados compran a los criminales más avanzados los "kits" para ejecutar los ataques. Así en este negocio de los ciberdelincuentes, esa parte la puede sufrir igual una empresa que una persona, por eso se tiene que cuidar todo lo que se abre en los correos y aplicaciones que se utilizan.

Por la parte de empresas e instituciones financieras más grandes que tienen programas de seguridad muy robustos y cuentan con la capacidad de prevenir ataques de *ransomware* en sus propias redes y sistemas, se ha detectado en sus proveedores la "falla o puerta de entrada" de los ciberdelincuentes, .

Por ello, reconoce que la cadena de suministro es algo que preocupa a los equipos de seguridad de las instituciones financieras, pues los ataques que han sido facilitados por terceros han demostrado ser muy efectivos en la circunvalación de las defensas de ciberseguridad.

Para considerar si se debe o no pagar un rescate, la inteligencia de amenazas es una herramienta invaluable para ayudar a entender al "enemigo", también sirve para identificar y alertar sobre una actividad sospechosa de manera preventiva y solidificar las defensas para protegerse de tácticas específicas de *ransomware*, lo cual al menos por las empresas está siendo aplicado, pero la gran duda queda, si se está haciendo en todas aquellas dependencias con datos sensibles de los mexicanos.

Y en el otro lado de la moneda, lo que no se dijo, pero deben saber del Plan de infraestructura es que lo que se dio a conocer este lunes es solo uno de varios paquetes que la Unidad de Inversiones de SHCP que lleva Jorge Nuño irá presentando conforme se avance en la parte legal en sus diseños y los esquemas que se usarán; lo que se busca es que cuando sean presentados ya estén casi "planchados" en todos los aspectos y puedan ponerse en marcha en las fechas que se pacten. En el sector privado hay miles de ideas y proyectos, pero armarlos y lograr que encajen con el proyecto que tiene el Presidente es un trabajo arduo y en el que ha puesto énfasis la unidad que dirige Nuño, lo que lo ha convertido en el centro

Página 1 de 1
$ 60192.00
Tam: 304 cm2