LITORALPRESS

Fecha: 09-09-2020 **Visitas:** 25.949 **Favorabilidad:** ☐ No Definida
Fuente: Diario Concepcion
Título: **Iniciativa Milenio UdeC elevaría seguridad informática de bancos**

Link: https://www.diarioconcepcion.cl/economia/2020/09/09/iniciativa-milenio-udec-elevaria-seguridad-informatica-de-bancos.html

Iniciativa Milenio UdeC elevaría seguridad informática de bancos Iniciativa Milenio UdeC elevaría seguridad informática de bancos Director del IMO y doctor en Ingeniería Informática entregan claves para robustecer el blindaje de sistemas actuales. Según la Ocde Chile sería top ten en vulnerabilidades ante ataques. Por: Edgardo Mora 09 de Septiembre 2020 Fotografía: Raphael Sierra El desarrollo de llaves cuánticas realizado por el Instituto Milenio de Óptica (IMO) de la Universidad de Concepción (UdeC) que dirige el académico Aldo Delgado. podría elevar la seguridad de los sistemas informáticos que usan los bancos actualmente.


Iniciativa Milenio UdeC elevaría seguridad informática de bancos

De la misma manera, Pedro Pinacho Davidson, doctor en Ingeniería Informática y también académico de la misma casa de estudios superiores entrega claves para robustecer los protocolos de ciberseguridad para evitar que Banco Estado vuelva a cerrar a causa de un ciberataque.

Aldo Delgado, director Instituto Milenio de Óptica de la UdeC Llaves cuánticas Delgado, explica el funcionamiento de las llaves cuánticas de la siguiente forma: “es como esconder el texto en una bóveda cuya llave sólo algunos conocen. El problema está en el proceso para distribuir la llave, el cual puede ser atacado. Por ejemplo, la llave de la bóveda puede ser duplicada. Las leyes de la Mecánica Cuántica permiten implementar varios tipos distintos de método para distribuir llaves. Éstos no pueden ser atacados, pues cualquier ataque dejaría en la llave una huella que puede ser fácilmente detectada”. Respecto de si pueden las llaves cuánticas bajar la ocurrencia de ataques por rasonwares a bancos, detalla que “en principio, las llaves cuánticas son incondicionalmente seguras, es decir, no existe ningún ataque a los equipos que las generan que no pueda ser detectado. No obstante, las llaves son usadas por personas, quienes se transforman en el link más débil de la cadena.

Recientemente supimos por la prensa que Tesla fue objeto de un ataque: a un empleado se le intentó sobornar para instalar un software malicioso”. En cuanto a la posibilidad de crear llaves cuánticas específicas para el sistema informático de los bancos, el director del IMO de la UdeC afirma que “sí, los métodos de generación de llaves han alcanzado una gran sofisticación, tal que pueden ser integrados a los sistemas de comunicaciones vía fibra óptica. ” Pedro Pinacho, doctor en Informática y académico de la UdeC.

Fortalecimiento de protocolos Requerido acerca de cuáles son las probabilidades promedio de ocurrencia de ataques por rasonwares a los sistemas informáticos de los bancos chilenos, Pinacho Davidson, es claro en señalar que “considerando antecedentes de madurez entregados por el BID (Banco Interamericano de Desarrollo) respecto a la ciberseguridad del país, y el último informe de Symantec (donde pone a Chile en el TOP-10 de países propensos a recibir ciberataques), y sumando a esto que este tipo de ataques (ransomwares) están focalizados en organizaciones con poder de pago para secuestros de información, creo que es altamente probable que la banca nacional siga en la mira”. En relación a qué aspectos considera claves para robustecer un protocolo antirasonwares, comenta que “este tipo de amenazas se basan en malware muy sofisticado, para lo cual las organizaciones deben potenciar sus respaldos de datos (backups) para poder recuperar su estado operativo y resguardar la integridad de los sistemas si es que son víctimas de un ataque”. Otro punto relevante para el académico de la UdeC, es que “los equipos técnicos mantengan los sistemas computacionales actualizados y en la medida de lo posible libre de vulnerabilidades importantes conocidas.

Hay que hacer notar que si se confirma los antecedentes técnicos dispuestos en prensa y medios especializados, la vulnerabilidad explotada en BancoEstado es del 2018 ”. Por último, pero no menos importante, “es considerar capacitar al personal de la empresa, debido a que la gran mayoría de estos ataques usan un “vector social” o falla humana, cómo por ejemplo la apertura de un correo (phishing) con el cargador del malware adentro. Una vez dentro el ransomware usa otros mecanismos para replicarse; pero el punto de entrada suele ser un engaño sobre un usuario incauto. ”