El experto en ciberseguridad Patrick Mcilwee:

"Chile no ha tenido que enfrentarse todavía a las grandes amenazas que vienen en cibercrimen"

El consultor del Business Continuity Institute, de Inglaterra, visitó el país y se reunió con la subsecretaria de Telecomunicaciones y con entidades privadas.

GABRIEL PAREC

Patrick Mcilwee saca de su bolsillo un *smartphone* y dice: "este es el único celular en Chile que no se puede hackear". Así de seguro está este experto irlandés sobre el sistema de seguridad antiataques que tiene en su teléfono móvil.

El consultor del Business Continuity Institute, de Inglaterra, explica que está visitando Chile —invitado por el Grupo Solunegocios— para reunirse con reparticiones públicas y empresas privadas y hablar de un tema que conoce bien: la ciberseguridad.

De hecho, la semana pasada estuvo con la subsecretaria de Telecomunicaciones, Pamela Gidi. Ya en 2010 había visitado Chile luego del maremoto del 27-F para asesorar a distintas instituciones.

Mcilwee sabe que el robo cibernético de 10 millones de dólares al Banco de Chile, la filtración de los datos de tarjetas de crédito de 80 mil clientes de BancoEstado o el hackeo a los *e-mails* de la Cámara de Diputados tienen al Gobierno y a las empresas en alerta.

"Si antes la gente creía que los ataques venían solo de un *hacker* adolescente, estaban muy equivocados. Hoy existe crimen organizado transnacional con grandes objetivos", afirma Mcilwee, en visita a "El Mercurio".

Atton: "Ingresará proyecto sobre delitos informáticos"

Jorge Atton.

Luego de los episodios de vulneración de la seguridad en bancos y otras instituciones, el gobierno de Sebastián Piñera decidió nombrar a Jorge Atton como asesor presidencial en ciberseguridad, afincado en el Ministerio del Interior.

Atton dijo a "El Mercurio" que se trabaja en una agenda que incluirá el ingreso de un proyecto de ley sobre delitos informáticos en los próximos 15 días. La idea es que se tipifiquen los ciberdelitos para que la legislación chilena se encuentre acorde a la Convención Internacional de Budapest, que abordó la cibercriminalidad y entró en vigor en 2004. Se establecerán sanciones respecto del mal uso de bases de datos o la interceptación de información confidencial de las personas, explicó Atton.

"Hay una política nacional de ciberseguridad que fue aprobada en 2017 y esa política fue visada por el Presidente Piñera. En esa política se establece además que se debe crear una ley marco de ciberseguridad", agrega el ex subsecretario de Telecomunicaciones.

De acuerdo al cronograma legislativo que han establecido, el proyecto para esa ley marco debería ingresar en noviembre.

Mientras tanto, afirma, trabajan en un plan de contingencia que permita coordinar las acciones de los distintos ministerios y empresas públicas, manteniendo contacto con el sector privado para combatir estas amenazas.

El experto irlandés muestra su celular con un *software* antiataques y sus tarjetas protegidas por una placa metálica, para evitar clonaciones.

> "Los criminales están cambiándose de países y de continentes hacia donde hay un **menor desarrollo cibernético**".

> "Yo mismo, asesorando a un banco, **le robé medio millón** de dólares a modo de ejemplo. Los devolví, claro".

—¿Cómo actúa este crimen organizado?

—En ocasiones, hay un "lobo solitario", el que no es el típico *hacker* adolescente. Hablamos de personas altamente capacitadas. En otras, hay verdaderas instituciones del crimen con cientos de personas actuando, muy entrenadas. Puede tratarse de grupos con objetivos políticos, como Anonymous, u organizaciones delictuales con objetivos muy específicos, como robo de bancos o la clonación de tarjetas de crédito.

—¿Latinoamérica es más vulnerable?

—En Asia, Europa o Estados Unidos se han ido tomando acciones contra este crimen organizado. Ya saben quiénes son los actores, así que los criminales están cambiándose de países y de continentes hacia donde hay un menor desarrollo cibernético.

—En Chile, uno de los mayores ataques fue el robo de 10 millones de dólares al Banco de Chile. ¿Es débil el grado de seguridad en el país?

—El tema no es que la seguridad sea débil, sino que Chile no ha tenido que enfrentarse todavía a las grandes amenazas que vienen en cibercrimen. Como le digo, en una institución pública o privada pueden tener a 4 o 5 personas encargadas de ciberseguridad, pero tendrán que enfrentar ataques del crimen organizado que a veces son organizaciones de 200 o más personas. El punto es ver cuánto dinero están preparados para invertir y solucionar ciertas brechas.

—Los bancos, al parecer, todavía no están preparados...

—Yo mismo, asesorando a un banco, le robé medio millón de dólares a modo de ejemplo. Los devolví, claro. Hay mucha gente que puede entrenarse con la información que está en internet para hackear sitios. Pero las organizaciones que preparan estos crímenes son verdaderos carteles con objetivos muy claros. También hay casos curiosos. Un miembro de Anonymous era durante el día jefe de seguridad en Google y de noche atacaba informáticamente a instituciones. De día protegía y de noche atacaba negocios y sitios de gobierno. No hablamos de niños.

—¿Cuáles son los pasos que las empresas e instituciones públicas deberían dar?

—Tienen que aprender a compartir información acerca de las amenazas. No deben guardársela. También deben crearse sistemas y protocolos frente a estos ataques. En Europa, cualquier tipo de pérdida de datos personales implica multas para las empresas. Además se debe agudizar el monitoreo al interior de las empresas porque a veces el atacante está dentro de la compañía.