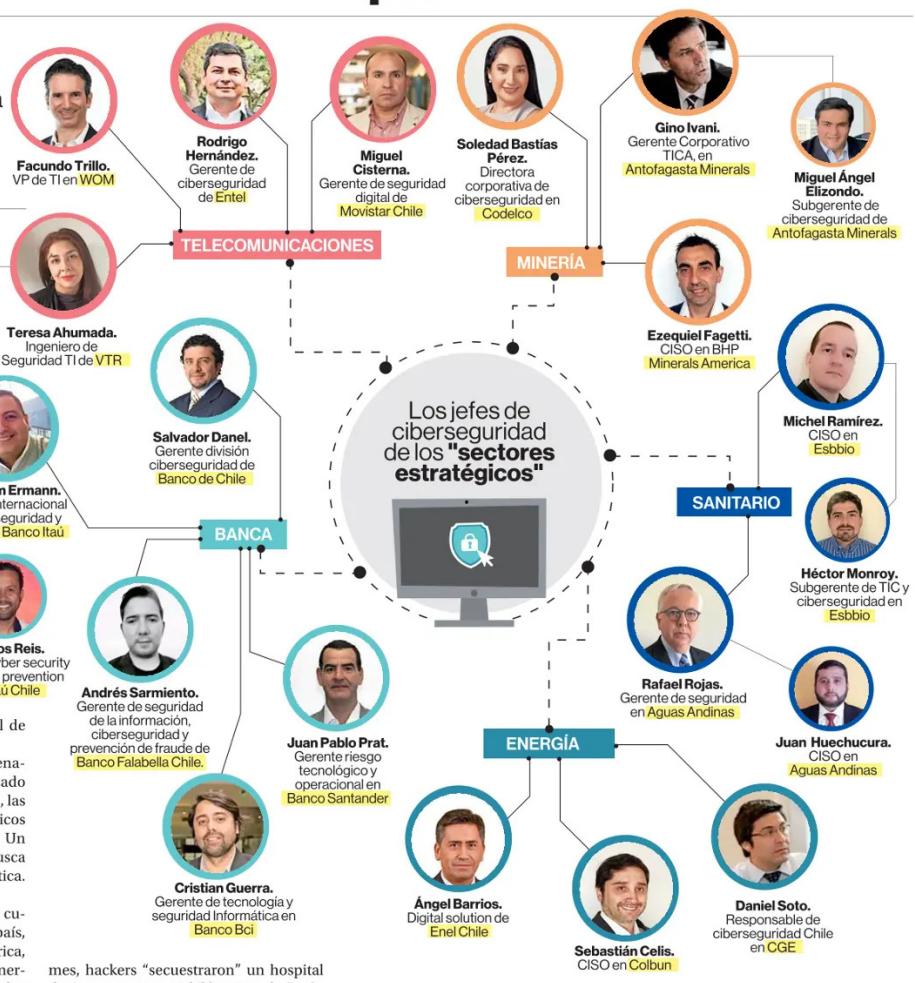
Los intentos de hackeos van en aumento exponencial

Cómo trabajan las "empresas críticas" chilenas para enfrentar ola de ataques informáticos

En el Congreso se tramita una ley que define la infraestructura crítica de información, pero las empresas no pueden esperar.

Por Felipe O'Ryan y Sergio Sáez



En los próximos días, está programado que los principales bancos chilenos experimenten intentos masivos de "hackeos". Esta vez, todo es parte de un simulacro a gran escala que llevará a cabo la Comisión para el Mercado Financiero (CMF) para poner a prueba a uno de los sectores "estratégicos" del mundo privado. Esto, en el contexto de un creciente número de ataques informáticos que todas las grandes empresas están registrando en el último tiempo y que ya en el sector público ha causado estragos con las vulneraciones a entidades como el Estado Mayor Conjunto, el Sernac y la Comisión Nacional de Acreditación.

Simulacros, inversiones y reordenamientos en sus gobernanzas han marcado la agenda de empresas como la banca, las telecomunicaciones, los servicios básicos e incluso la minería (ver recuadro). Un proyecto de ley, hoy en el Senado, busca transformarlas en infraestructura crítica. Pero el proyecto corre contra reloj.

"Si hoy se vulnerara una empresa cuyo funcionamiento es crítico para el país, como por ejemplo una empresa eléctrica, parte del país se podría quedar sin energía. Legalmente, no estamos preparados para un panorama así. Solo lo que las empresas han estado haciendo por su parte", comenta la directora de Ciberseguridad de NTT Data Chile, Carolina Pizarro.

Quizás comunas enteras sin luz o agua por culpa de hackers le suena como algo sacado de una película de acción, pero la realidad es otra. En el 2021, un ataque informático a los oleoductos de la empresa Colonial Pipeline cortó todos sus suministros de gasolina y combustibles a la costa este de Estados Unidos. Hay casos más preocupantes. Hace poco más de un mes, hackers "secuestraron" un hospital de 1.000 camas a 23 kilómetros de París, pidiendo US$10 millones para liberar sistemas que quedaron bloqueados.

Los expertos creen que es cosa de tiempo para que esto se replique en Chile.

"El agua, la salud, el transporte público, la electricidad, están siendo blancos de ataques de este tipo en todo el mundo. Son hackers con perfiles muy sofisticados. En países como España, China o Singapur se define por ley qué es infraestructura crítica para estos casos, pero acá en Chile no está definido (...) Se requerirá un estándar de ciberseguridad muy alto. Las empresas deberán gastar bastante", advierte el Cyber Risk Services Partner de Deloitte, Nicolás Corrado.

El conflicto con las leyes

Ingresada el 10 de marzo y hoy en segundo trámite legislativo en el Senado, la Ley de Gobernanza de Ciberseguridad y Protección de Infraestructura Crítica de Información definirá, entre otras cosas, qué industrias y sistemas informáticos serán considerados como críticos para el país. Entre las empresas que entrarían en esta categoría, explica el senador (ind) Kenneth Pugh, se considerarían el transporte, la banca, los servicios públicos como la generación, transmisión y distribución eléctrica, además del sanitario. También se considerará la minería.

Hoy, si hay un ataque informático a una de estas compañías clave, éstas no están obligadas a informar a las autoridades. Pero la ley definirá una serie de obligaciones y multas para estas empresas en esos casos, con lo que busca mejorar los estándares de ciberseguridad.

La minería está tomando fuerza como blanco de los ataques

A medida que la minería industrial ha ido adoptando nuevas tecnologías, como la inteligencia artificial o los vehículos autónomos, también han surgido nuevos peligros, como los ciberataques a estos sistemas. En octubre del año pasado, se levantó la primera gran alerta mundial para la industria. La firma de servicios a la minería Weir, en EE.UU., sufrió un ataque informático que la misma empresa explicó en ese entonces, afectaría sus resultados de ese trimestre en entre US$13 y US$27 millones. Un 70% de las grandes mineras del mundo afirmaron en 2021 haber visto un aumento en ciberataques según EY.

Sin ir más lejos, el grupo de hackers Guacamaya Roja -el mismo que se adjudicó la filtración de datos del Estado Mayor Conjunto en Chile el pasado mes-, también se adjudicó vulneraciones al Proyecto Minero Fénix en Guatemala en marzo de este año, a la Empresa Nacional de Minería en Ecuador y a la chilena Quiborax en agosto.

En Chile, el proyecto de ley que tiene entre sus objetivos incluir a la minería entre las empresas de infraestructura de la información crítica, explica que uno de los factores para tener esta clasificación son las "pérdidas financieras potenciales por fallas o ausencia del servicio a nivel nacional o regional asociado al PIB".

"Un ataque potente que afecte a la minería podría parar la economía del país", explica el senador Kenneth Pugh.

> "Es clave incorporar los requerimientos de ciberseguridad en las etapas iniciales de los proyectos". **Soledad Bastías, Codelco**

En esa línea, empresas como Codelco son ya conscientes de la importancia de la ciberseguridad, explica la directora corporativa de Ciberseguridad IT/OT de Codelco, Soledad Bastías.

"Somos la mayor productora de cobre del mundo y hoy desplegamos una transformación digital que incorpora, cada vez más, la tecnología a los procesos críticos del negocio minero. Si consideramos que nuestra visión a mediano plazo es la automatización de nuestras operaciones, es clave incorporar los requerimientos de ciberseguridad en las etapas iniciales de los proyectos que ejecutamos, y así lo hacemos", explica.

En el plano normativo, en octubre de 2021 la corporación estatal desarrolló una nueva Norma Corporativa sobre Ciberseguridad IT/OT y Seguridad de la Información, NCC N° 49, marco regulatorio que provee una base reglamentaria para la definición, implementación, tratamiento y control de esta materia.

> El mundo financiero a nivel internacional tiene miles de ataques al día". **José Manuel Mena,** Asociación de Bancos.

Expertos creen, eso sí, que esto podría entrabar el trámite legislativo, alargando la discusión por años y dejando abierta una falencia incluso para la seguridad nacional.

"Hoy existe un proyecto de ley marco de ciberseguridad que fusiona la definición de los sectores denominados infraestructura crítica de la información y gobernanza de ciberseguridad. Creemos que es necesario centrarse en este último punto, principalmente para darle la celeridad que se requiere, porque podríamos ver oposición de algunas empresas de infraestructura crítica para el primer punto. ¿Cuáles serán los sectores que van a regular? ¿Con qué nos podrían multar? ¿Cómo nos van a multar? Son preguntas que tienen, y esto se podría entrampar en una discusión mucho más compleja en el Congreso", explica Pizarro.

"Es preocupante que se pueda hacer un lobby contra esta ley. Es algo que está funcionando en Estados Unidos y Asia hace años. Si una empresa en Chile no se preocupó antes, deberá ponerse al día", dice Jorge Atton, exasesor presidencial de ciberseguridad.

"Lo que pasa en Chile es que ocurre un evento como el del EMCO, y nos preocupamos, pero no nos ocupamos. La ley de delitos informáticos se aprobó, pero estuvimos 30 años esperándola. Efectivamente, muchas veces en el sector privado se genera incomodidad, entonces hay que ver cuál es el modelo de regulación", dice el investigador del Centro de Sistemas Públicos de la U. de Chile Alejandro Barros.

> ¿Qué sectores se regularán? ¿Con qué podrían multar? Son preguntas que tienen las empresas" **Carolina Pizarro,** NTT Data Chile.

> En Chile nos preocupamos, pero no nos ocupamos". **Alejandro Barros,** Centro de Sistemas Públicos U. de Chile.

Qué hacen las empresas

Unos US$4 millones en promedio puede costarle a una empresa un ataque informático, dice un estudio de Deloitte.

El monto aumentó un 2,6% el 2021 frente al 2020 en EE.UU., dado que los atacantes se han vuelto más sofisticados, se lee en un informe de IT Security.

Según Deloitte, un 31% de las organizaciones respondieron que el motivo por el que se producen tantos incidentes informáticos es porque los "ciberadversarios" están mejor financiados que las mismas empresas.

Chile tampoco está libre. Solo recordar el robo de US$10 millones al Banco de Chile en 2018 por un ataque informático.

Por esto, las empresas han ido tomando medidas por su cuenta para adelantarse a los ataques. Además de coordinaciones y simulacros, como el de la CMF, o el Coordinador Eléctrico Nacional, que definió estándares para la industria, otras empresas que podrían ser catalogadas como críticas han aplicado medidas.

En el 2018, el Banco de Chile creó el puesto de gerente de División Ciberguridad (ver infografía) como ejecutivo de primera línea. Esto es lo que sugieren los expertos, para que la ciberseguridad tome protagonismo dentro de la organización.

Tras el bullado ataque a la entidad financiera, otras empresas también encendieron alarmas. Las de telecomunicaciones están entre las más avanzadas.

Entel creó ese año la Gerencia de Ciberseguridad, la que en conjunto con 22 BISOs (Business Information Security Officer) conforman la Organización de Ciberseguridad de Entel.

"Así, en el 2021 no se registraron incidentes de ciberseguridad relacionados con la infraestructura, la pérdida de información o nuestros sistemas", dice el gerente de Ciberseguridad de Entel, Rodrigo Hernández.

Movistar, de la española Telefónica, apunta al estándar europeo.

"Contamos con plataformas de monitoreos en tiempo real, herramientas de protección avanzada para identificar y diferenciar tráficos lícitos de tráficos ilícitos, entre otras. Además, todos nuestros procesos de seguridad son gestionados durante las 24 horas por nuestro SOC (Security Operation Center), uno de los más grandes de Telefónica en Latinoamérica, que está ubicado en Santiago", cuenta el gerente de Seguridad Digital de Telefónica Movistar Chile, Miguel Cisterna.

Las compañías tienen centros de monitoreo que están operativos las 24 horas, particularmente en el mundo financiero, uno de los sectores más expuestos. "Por eso la industria tiene una creciente inversión, ya que el mundo financiero a nivel internacional tiene miles de ataques al día", comenta José Manuel Mena, presidente de la Asociación de Bancos.

En Banco Falabella, por ejemplo, han desarrollado "una estrategia de ciberseguridad y políticas robustas (tales como Framework FFIEC y principios Zero Trust), focalizadas en controles cibernéticos para detectar, mitigar y gestionar en forma temprana cualquier amenaza", explica Andrés Sarmiento, gerente de Seguridad de la Información, Ciberseguridad y Prevención de Fraude.

Todas las empresas consultadas registran aumentos semana a semana en el número de intentos de ciberataques.