LITORALPRESS

Fecha: 25-11-2021
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Actualidad
Título: “Apostar por las personas, sus competencias y conciencia en ciberseguridad es parte de la ecuación, más que solo más fierros y bytes”

Pág. : 14
Cm2: 461,7
VPE: $ 650.961

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

Pedro Huichalaf Roa, Centro de Investigación en Ciberseguridad de la Universidad Mayor

“Apostar por las personas, sus competencias y conciencia en ciberseguridad es parte de la ecuación, más que solo más fierros y bytes”

Si bien, a juicio del especialista, han crecido los niveles de preparación y seguridad de la información de la industria financiera chilena, así como la cantidad de técnicos y profesionales en las distintas áreas tecnológicas, falta que estos se sumen a la decisión estratégica en las organizaciones. Y es que la ciberseguridad es un tema clave que debe ser asumido como tal a nivel de directorios.

¿Cuáles son las principales amenazas de ciberseguridad en entidades financieras?

Hoy por hoy los ataques y brechas de ciberseguridad están tanto por el lado del cliente de las instituciones financieras como en las mismas empresas. Así, por el lado de los clientes, las técnicas de phishing o estafas han proliferado, mediante el intento de engañar simulando el envío de mensajes, sitios web o información sobre cambios de claves, por ejemplo, como si fueran oficiales de las instituciones financieras. En tanto, por el lado de aquellas, los malwares, especialmente ransomware y los que atacan vulnerabilidades zero day son las más recurrentes.

¿El trabajo remoto o híbrido ha afectado a la seguridad de esta industria?

Impacta en la medida en que no exista una correcta información para todos los funcionarios de las empresas financieras sobre las medidas de seguridad y la aplicación de políticas, pero, por otro lado, los cambios de hábitos en cuanto a la nueva forma de trabajar, requieren también mayor conciencia y cultura en ciberseguridad de todos los intervinientes en procesos financieros. El aumento de personas conectadas, crecimiento del comercio electrónico, mayor número de transacciones y volúmenes de ventas digitales es un espacio ideal que atrae a los delincuentes informáticos. Por eso es tan necesario contar con medidas de prevención, más que de reacción.

¿Qué nuevos retos se enfrentan en este contexto?

La aceleración en la transformación digital que conllevó la pandemia, el tsunami digital de mayores conexiones, el aumento de transacciones electrónicas y, en general, el cambio de hábitos en la forma de relacionarnos con la tecnología, es un proceso sin marcha atrás, por lo que debemos entender que este nuevo mundo seguirá y se fortalecerá en el ámbito digital.

¿Qué nivel de preparación y conciencia existe en las instituciones financieras nacionales?

Hoy existe una normativa específica relacionada con ciberseguridad emanada de la Comisión del Mercado Financiero (CMF), pero que es bastante reciente y surgió producto de un ataque a un gran banco nacional. También hay que recordar que hace casi cuatro años atrás Chile ratificó el convenio de Budapest y, además, aún está

LITORALPRESS

Fecha: 25-11-2021
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Actualidad
Título: **“Apostar por las personas, sus competencias y conciencia en ciberseguridad es parte de la ecuación, más que solo más fierros y bytes”**

Pág. : 15
Cm2: 493,0
VPE: $ 695.093

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

“Somos unos de los países más conectados de la Región, somos líderes en la incorporación de tecnología, por ejemplo, en telecomunicaciones, pero aún estamos rezagados en cuanto a mayor impulso de la ciberseguridad a todo nivel”

en el congreso un proyecto de ley que regula los delitos informáticos. Esto significa que como país debemos seguir avanzando en robustecer la política y normativa en ciberseguridad y debemos hacerlo de la mano de sector privado, siendo las instituciones financieras nacionales copartícipes de este trabajo público-privado.

A nivel latinoamericano, ¿cómo califica a la industria financiera nacional en seguridad de la información?

Las empresas chilenas han aumentado sus niveles de preparación y seguridad de la información. También ha crecido la cantidad de técnicos y profesionales en las distintas áreas tecnológicas. Sin embargo, aún falta que estos especialistas se sumen a la decisión estratégica, que se encuentren en las direcciones ejecutivas de la organización, es decir, comprender que dentro del directorio de cualquier organización debe existir no tan solo una mirada, sino uno o más especialistas que las integre.

Si uno ve y analiza rankings internacionales a nivel mundial o incluso a nivel regional, aún Chile tiene varios aspectos que mejorar y superar. Somos unos de los países más conectados de la Región, somos líderes en la incorporación de tecnología, por ejemplo, en telecomunicaciones, pero aún estamos rezagados en cuanto a mayor impulso de la ciberseguridad a todo nivel.

¿Deben las instituciones financieras estar obligadas por ley a reportar incidentes de seguridad?

Hoy no existe una Ley de Infraestructura de Comunicaciones, tampoco una Ley marco de Ciberseguridad y no se ha concretado la nueva Ley de Delitos Informáticos ni cambios en la Ley de Protección de Datos Personales. Solo existen regulaciones sectoriales, emitidas por entidades reguladoras, que establecen obligaciones de reportar incidentes, con parámetros más o menos concordantes. Sin embargo, aún creo que es necesario una regulación legal más expresa y pensando en el ecosistema más que en una industria en particular.

¿Qué estándares de ciberseguridad deben implementar los bancos?

Existen estándares técnicos, normas ISO de seguridad de la información, buenas prácticas, e incluso, en algunos casos, exigencias regulatorias de otros países (cuando instituciones se relacionan con otros mercados). Debemos avanzar en incorporar mayor tecnología predictiva de posibles delitos (existen desarrollos de Inteligencia Artificial en ese sentido), pero requerimos mayor cantidad y calidad de nuestro capital humano. Apostar por las personas, sus competencias y conciencia en ciberseguridad es parte de la ecuación, más que solo incorporar más fierros y bytes.

En general, hay una falta de talento humano en ciberseguridad...

La industria puede generar más requerimiento de capital humano, pero es necesario que desde el nivel educativo (incluyendo escolar, universitario y técnico profesional) se enfoque más la oferta educacional orientada a este sector que, todos sabemos, cada vez demanda más técnicos y profesionales. Todos entendemos que los que se desempeñan en esta área deben tener formación continua y permanente para avanzar al mismo tiempo como cambian las tecnologías y hábitos de uso.

Es necesario que esta mirada global de ciberseguridad sea parte de una política nacional en serio, con visión de futuro y trabajo colaborativo. Tengo confianza en que así será y que avanzaremos con un plan de ruta común. G

Pedro Huichalaf Roa es Abogado de la Universidad de Valparaíso, Magíster (c) en Derecho Informático y de las Telecomunicaciones de la Universidad de Chile, y Especializado en Telecomunicaciones y Tecnologías de Información y Comunicaciones.
Desde marzo de 2014 a octubre de 2016 fue Subsecretario de Telecomunicaciones de Chile.
Actualmente es Consultor nacional e Internacional en tecnologías, telecomunicaciones e innovación y Docente e Investigador del Centro de Investigación en Ciberseguridad de la Universidad Mayor.