Avances, desafíos y amenazas frecuentes

La importancia de la protección de datos en la banca

Actualmente, los bancos cuentan con diversos mecanismos de seguridad, con el fin de resguardar la información personal de los clientes y evitar posibles vulneraciones.
Por: Jorge Aliaga Sandoval

La banca constantemente actualiza sus sistemas de seguridad, incorporando tecnologías más robustas. Los avances más prometedores en este momento surgen de la aplicación de inteligencia artificial a la ciberseguridad en la banca. "Una idea que nos entusiasma es usar tecnología de aprendizaje desatendido (machine learning) para ir de la biometría comportamental, que es una antigua técnica de reconocer a alguien por sus movimientos o hábitos, a la inteligencia comportamental, que es una técnica para que los sistemas de banca digital nos reconozcan sin necesidad de ningún esfuerzo de nuestra parte", dice Alejandro Musgrove, experto en ciberseguridad.

El principal desafío es el fraude digital. Para la banca digital en América Latina, la modalidad de fraude más común es el

> Pallavicini Consultores **> www.pallavicini.cl**

Protección de datos en pandemia:

Riesgos de ciberseguridad en modalidad de teletrabajo

Las empresas aplicaron teletrabajo, resolviendo la continuidad operativa del negocio, pero un gran porcentaje, descuidó la seguridad de la información, incluida la ciberseguridad.

En estos meses de pandemia, en que la gran mayoría de las empresas están con sus usuarios en modalidad de teletrabajo, ¿por qué han aumentado los ciberataques en nuestro país?

"Esto se debe a que la ciberdelincuencia, al detectar nuevas vulnerabilidades, cambia sus estrategias y adecua sus formas de atacar, y además, lo hace en forma rápida y con recursos ilimitados. Las empresas, en cambio, sobre todo en las que sus directivos no le asignan la importancia debida a la gestión de seguridad de la información y ciberseguridad, no implementan mecanismos de defensa efectivos para protegerse de los ciberataques, que son cada vez más profesionales", explica César Pallavicini, CEO de Pallavicini Consultores, empresa de asesoría en gestión de riesgo operacional, seguridad de la información, continuidad de negocio y derecho informático.

Adicionalmente, la pandemia hizo que muchas empresas resolvieran utilizar la modalidad de teletrabajo como solución de contingencia. Sin embargo, a juicio de Pallavicini, esto se hizo en forma improvisada, sin darse el tiempo para capacitar a los usuarios y, lo que es más grave, sin definir políticas y protocolos formales de seguridad de la información. "En otras palabras, se privilegió la continuidad operativa en desmedro de la protección de la información de la compañía. Esto lo saben muy bien los ciberdelincuentes y lo aprovechan en su favor para realizar su negocio. No es casualidad que los ciberataques hayan aumentado 500% en este año", detalla César Pallavicini.

Foto: Pallavicini

César Pallavicini, CEO de Pallavicini Consultores.

Desafíos del teletrabajo

Es fundamental tener una visión de gobierno corporativo y cumplimiento, donde el directorio y la alta administración se involucren en las estrategias de gestión de riesgo operacional, para mitigar riesgos en el teletrabajo.

Hay que revisar aspectos que son básicos pero muy importantes: distinguir los usuarios que están conectados con equipos de propiedad de la empresa y usuarios que utilizan equipos propios. En relación a estos últimos, aplicar controles de seguridad por medio de verificar que: a) el software de acceso remoto sea licenciado, b) la red WiFi sea segura, con password robusta, c) el antivirus y antispam estén actualizados, d) la conexión sea VPN (red privada virtual), y e) el sistema operativo esté actualizado.

"Es recomendable adoptar los lineamientos que señalan las normas ISO 27001 de seguridad de la información y la ISO 27032 de ciberseguridad e implementar una política de teletrabajo y uso de equipos móviles, y muy importante, desarrollar un plan de sensibilización y capacitación permanente de todos los colaboradores de la organización", agrega este especialista.