HYPO PHOTOS

CUKY PÉREZ, experta *en data science*, moderó el panel en que participaron Naren Kalyanaraman y Lisa Plaggemier.

PANEL 8

PARTE DE LAS INVERSIONES CRÍTICAS:

"La educación es una de las cosas más baratas que se puede hacer con los mejores resultados"

Asumir que habrá una filtración de datos es el pie inicial para que las organizaciones desarrollen una nueva mentalidad, en la que se van creando capas de defensa ante los ataques.

FELIPE LAGOS R.

A US$ 4.880 millones llegó el costo promedio de incidentes de filtración de datos (*data breach*) según un reporte de 2024 de IBM, que además establece que las empresas han estado gastando más en ciberseguridad y en respuesta a estos incidentes en los últimos años.

La cifra deja en claro el mensaje en que coincidieron los expertos participantes en el panel "Cybermindset: la nueva era de la seguridad empresarial", realizado durante el Cybertech South America 2025 en "El Mercurio".

Naren Kalyanaraman, líder nacional de Ciberseguridad, Privacidad y Delitos Financieros y socio de PwC Canadá, llamó a las empresas a tener la certeza que sufrirán una filtración. "Hablamos bastante de la filtración de datos, pero no entendemos la disrupción que significa", dijo. "Piense en (un incidente en) infraestructura crítica durante un tiempo extendido. El riesgo de seguridad, de salud (...) puede afectar muchas cosas más que solo lo monetario", añadió.

COSTOS Y BENEFICIOS

Kalyanaraman además dijo que hay otros costos derivados de un ataque, como la erosión de la confianza de los clientes, quienes "están muy alerta de la parte ciber de las empresas", señaló. "Si estoy comprando un seguro y mi proveedor no ofrece una autentificación multifactor como algo diferenciador, no estoy seguro de si es donde quiero ir", agregó. En este sentido, el beneficio de invertir en ciberseguridad no solo es evitar el costo de la filtración, sino que también crea oportunidades de negocio para la empresa.

"Invertir en prevención, resiliencia, recuperación; la seguridad del cliente (puede) ser diferenciadora", aseguró Kalyanaraman, adicionando que "si uno opera de manera correcta, con la certeza que tendrá una filtración, se van creando capas de defensa para los ataques. Son inversiones críticas que todos tendríamos que estar haciendo".

Por su parte, Lisa Plaggemier, directora ejecutiva de la Alianza Nacional de Ciberseguridad de Estados Unidos, dijo que invertir en la educación de las empresas presenta grandes oportunidades en ciberprevención, dado que el componente humano es usualmente el eslabón más débil.

"La educación es una de las cosas más baratas que puede hacer con los mejores resultados", enfatizó Plaggemier, advirtiendo que "no es tan caro entrenar a los trabajadores, pero debe ser un cambio cultural completo en cada empresa. Cada persona debe saber cuál es su rol. Y esto es más que el entrenamiento anual para cumplir las normas. Tal vez (deba ser) cada semana. Tener panelistas que hablen de seguridad; un programa robusto para entender lo importante que es para ventas, recursos humanos, contabilidad; entrenamientos para que entiendan cómo pueden ser atacados y su rol en esta defensa".

Asimismo, concordaron en que los directorios de las empresas deben promover la resiliencia en ciberseguridad, o la capacidad para prepararse, resistir, recuperarse y adaptarse a los ciberataques u otras interrupciones de sus sistemas digitales.

PRACTICAR LA RESILIENCIA

Plaggemier enfatizó en la importancia de ejercitar y practicar la resiliencia con ejercicios de simulación (*tabletop exercises*, o TTX en inglés), los que replican la ocurrencia de un incidente para ser analizado por parte del equipo de respuesta de ciberseguridad.

"Ejercitar, ejercitar y ejercitar. Poner las cosas en la mesa", afirmó, porque "si quieren un mejor rendimiento y ejecutivos que entiendan lo que significa un incidente en seguridad, tienen que hacer ejercicios de simulación".

El panel lo comparó con el concepto de *playbook*, o guía paso a paso, que establece cómo lidiar con un incidente de ciberseguridad, pero que muchas veces puede favorecer un clima de complacencia a nivel ejecutivo.

"El *playbook* da la sensación que con tener un libro en la repisa, ya solucioné el problema. Ese no es nunca el caso", matizó Plaggemier. "Nunca he hecho un ejercicio de simulación en el cual no hayamos aprendido algo. Si creen que tienen un *playbook* sólido, hagan un ejercicio de simulación", agregó.

Este escenario cobra más relevancia al considerar las formas en que la IA puede desafiar a los expertos en ciberseguridad. El FBI reportó recientemente que ciberdelincuentes usaron IA para clonar la voz de autoridades, con el fin de acceder a bases de datos.

"Es terrorífico, tengo una amiga que está estudiando las herramientas de IA que dicen poder detectar (posibles fraudes) en audio o video, (pero) no son capaces de detectar cuál es real y cuál es IA", dijo Plaggemier.

"Es muy importante reconocer que algunas herramientas pueden ayudar, pero ninguna es 100% segura. Esa es la realidad hoy", matizó Kalyanaraman.