DIARIO FINANCIERO®

Fecha: 28/01/2025 Audiencia: 48.450 Sección: ACTUALIDAD
Vpe: $6.379.731 Tirada: 16.150 Frecuencia: OTRAS
Vpe pág: $7.443.240 Difusión: 16.150 Ámbito: SUPLEMENTO
Vpe portada: $7.443.240 Ocupación: 85,71% Sector: ECONOMIA

TRUSTTECH

Ciberseguridad, Resiliencia y Regulación de la IA: Claves para la Protección de Datos

La compañía especializada en ciberseguridad lleva más de 10 años investigando el robo masivo de credenciales. "Solo el 2024, reportamos más de 150 mil credenciales robadas, afectando a millones de personas. Para afrontarlo, es indispensable un buen plan de resiliencia", indica Felipe Hott, Director de Ciberseguridad, quien además alerta respecto de la urgencia de regular y legislar el uso de la IA.

Sin duda, la cooperación público-privada para mejorar la ciberseguridad y resiliencia de los datos de los chilenos plantea un gran desafío para toda la industria. Si bien los nuevos lineamientos y obligaciones de base que plantea la nueva ley de protección de datos personales son un tremendo cambio en todo sentido, aún existen vicios en procesos, procedimientos y sistemas que se utilizan a diario.

"Debemos estar preparados para una fuga masiva a gran escala de millones de datos. En TRUSTTECH llevamos cerca de 10 años investigando el robo masivo de credenciales a los mismos usuarios, robo que se produce principalmente por malware instalado en los computadores del usuario final. Solo en 2024, reportamos a diferentes instituciones más de 150 mil credenciales robadas", explica Felipe Hott, Director de Ciberseguridad de TRUSTTECH.

De esa cifra, cerca del 50% corresponde a claves únicas, y el resto se reparte entre accesos a plataformas bancarias, sistemas de salud e incluso sistemas de infraestructuras críticas. El problema, según Hott, es que absolutamente todas las credenciales robadas son para acceder a sistemas que hasta hoy no requieren doble factor de autenticación, es decir que, haciendo uso de usuario y contraseña, no tienen una validación extra.

Felipe Hott dando una charla sobre robo de datos personales en una conferencia de ciberseguridad en México.

De esa manera, señala el especialista, millones de chilenos han sido víctimas del robo de credenciales desde hace años, permitiendo a delincuentes e incluso al mercado negro de tráfico de información, acceder a diversa información sin que nadie haga algo al respecto. "Puedo asegurar que esa información ya está en manos de más de un oportunista o un delincuente, esperando el momento para utilizarla, venderla o sencillamente liberarla", afirma Hott. De ahí la urgencia de un muy buen plan de resiliencia en las diferentes instituciones que nunca han querido implementar un simple, pero importante doble factor de autenticación.

No es paranoia o que esté pensando en Terminator. La IA se debe regular y legislar ahora ya, a nivel mundial", enfatiza Felipe Hott.

Un muy buen plan de resiliencia es indispensable en las diferentes instituciones que nunca han querido implementar un simple, pero importante doble factor de autenticación.

IA y protección de datos

Otra urgencia en relación a la protección de datos es la regulación de la Inteligencia Artificial (IA). "Se debe legislar y regular ahora ya. Estamos atrasados y en mucha desventaja", asevera Felipe Hott.

De acuerdo al Director de Ciberseguridad de TRUSTTECH, lo que se ha diseñado es el modelo de aprendizaje y los algoritmos para que la IA procese la información con la cual es alimentada. Sin embargo, no se ha diseñado lo que la IA es capaz de hacer en base a su propio aprendizaje, ya que carece de algo esencial: criterio. "Esto está demostrado a nivel mundial, con diversos eventos, donde por la falta de criterio ha sido posible evadir los controles que se han diseñado para que la IA interprete y ejecute acciones retorcidas y peligrosas", comenta Felipe Hott.

Lo anterior, aplica también a la protección de datos. "Creemos tener el control de nuestros datos y, lo que es peor, que tenemos el control sobre los procesos que la IA ejecuta sobre ellos; confiamos sin medir las consecuencias", sostiene el especialista.

Por lo mismo, se hace imprescindible regular y legislar con urgencia, pues la IA y el alcance que tiene sobre los datos personales está totalmente a la deriva y fuera de control. "Durante años, millones de personas en el mundo, adultos y niños, le han regalado sus datos personales a la industria de la IA, a través de correctores de voz, apps para ver su versión joven o anciana, traductores en tiempo real, entre otros. Así y todo, nos asombramos de los videos deepfake o del bullying de carácter sexual en los colegios", comenta Hott.

Para el Director de Ciberseguridad de TRUSTTECH nosotros mismos somos los que hemos provocado aquello, regalando a la industria de la IA los datos personales, información biométrica, conductas personales y sociales, sin saber el alcance de los sistemas que hay detrás. "Alimentamos sistemas de IA que no sabemos en qué minuto pueden tener un fallo, con datos suficientes para suplantar nuestra identidad e incluso para que nos reemplacen en ciertos escenarios", detalla.

Sumado a eso, está el abuso de uso de la IA que está produciendo toda una generación incapaz de pensar, de resolver problemas y de crear soluciones, porque la IA lo hace por uno. Entonces cabe preguntar ¿quién tendrá la ventaja el día de mañana cuando, sin darnos cuenta, una IA más avanzada mire al ser humano como material desechable? "No es paranoia o que esté pensando en Terminator, es una señal de alerta, como experto en ciberseguridad, para indicar que la IA se debe regular ahora ya y se debe legislar al respecto a nivel mundial", resalta Felipe Hott.

www.trusttech.cl