LITORALPRESS

Fecha: 27-09-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: Experta advierte escalada de ataques de phishing y suplantación de voz con IA generativa en la región

Pág. : 32
Cm2: 714,2

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

DF DIARIO FINANCIERO

DF LAB
INNOVACIÓN, STARTUPS Y TRANSFORMACIÓN DIGITAL

PAMELA SKOKANOVIC,
DIRECTORA DE CIBERSEGURIDAD DE IBM PARA ARGENTINA, CHILE, URUGUAY Y PARAGUAY

Experta advierte escalada de ataques de phishing y suplantación de voz con IA generativa en la región

La directora de ciberseguridad de IBM dijo que existe un "gran desafío" de gestión de identidad en las empresas, y alertó de nuevas formas de ataque, como el envenenamiento de código en sistemas de inteligencia artificial.

POR MARCO ZECCHETTO

El auge de la Inteligencia Artificial (IA) e IA generativa, con modelos cada vez más avanzados para agilizar tareas, tomar decisiones y procesar el lenguaje natural ha traído beneficios y riesgos para las empresas. Esto último, porque a los ciberdelincuentes les ha permitido sofisticar ataques como el *phishing* (suplantación de identidad) y el robo de credenciales, lo que ha generado altos costos a las empresas de Latinoamérica.

Este miércoles, IBM publicó su informe anual Cost of a Data Breach 2024, el cual analiza filtraciones de datos experimentadas por 604 organizaciones a nivel mundial desde marzo de 2023 hasta febrero de 2024 y que reveló que el costo promedio de una filtración de datos en América Latina es de US$ 2,76 millones. Los vectores de ataque más comunes fueron el *phishing* (16% de los incidentes), con un costo promedio de US$ 2,91 millones por filtración, y el robo de credenciales (14%), con US$ 2,89 millones.

La directora de ciberseguridad de IBM para Argentina, Chile, Uruguay y Paraguay, Pamela Skokanovic, afirmó que estos ataques han escalado en la región por el avance de la IA generativa, y que existe preocupación principalmente por campañas más avanzadas de *phishing* y *deepfakes* (archivos de imagen, audio o video alterados a través de IA para que parezcan reales) de suplantación de voz.

"El *phishing* diseñado por IA es uno de los ataques que más se está utilizando en la región, ya sea por correo y ahora también por audio generado. Como contexto, el phishing con *deepfake* experimentó un aumento global de 3.000% en 2023", afirmó.

Skokanovic también señaló que el reporte anual de inteligencia de amenazas de la compañía de este año, situó a América Latina como la cuarta región del mundo más atacada por cibercriminales en 2023, siendo Brasil (68% de los ataques), Colombia (17%) y Chile (8%) los países más atacados.

Según este informe, los incidentes se relacionaron con filtraciones de datos, extorsión o afectación a la reputación de la marca, donde un 22% de los ciberataques fueron realizados a través de cuentas válidas con accesos ilegítimos, y a nivel de industria, retail, finanzas y seguros fueron las más afectadas.

Identidad y "audio generativo"

Skokanovic advirtió que hoy el "gran desafío" está en la gestión de la identidad en las organizaciones de la región, y que la "explotación de la identidad" se ha transformado en uno de los principales vectores de ataque.

"Los cibercriminales están utilizando las identidades de los usuarios para comprometer a las empresas, e inician sesión a través de cuentas válidas en lugar de hackear alguna red o un usuario. Este cambio de estrategia genera facilidad de adquirir credenciales de usuarios válidas en vez de explotar vulnerabilidades", dijo.

En el caso de Chile, comentó que la industria de servicios y el sector financiero son los más avanzados en la adopción de soluciones para proteger los sistemas y los datos de la empresa, mientras que educación y salud, "aún tienen un camino que recorrer y deben mejorar sus protocolos de seguridad".

"El phishing diseñado por IA es uno de los ataques que más se está utilizando en la región, ya sea por correo y ahora también por audio generado. Como contexto, el phishing con deepfake experimentó un aumento global de 3.000% en 2023", afirmó.

Por otro lado, Skokanovic indicó que la principal preocupación de la industria en torno a los ataques por *deepfake* radica en el "audio generativo".

"Los atacantes crean artificialmente la voz de algún ejecutivo, y la utilizan para realizar llamados a los trabajadores y darles una orden. Luego estos terminan ejecutando una acción que no está bien. Y eso se está dando mucho en Latinoamérica", alertó.

Nuevas formas de ataque y Ley Marco

Skokanovic comentó que desde la irrupción de los grandes modelos de lenguaje (LLM, en inglés), por ejemplo, ChatGPT en 2022, han surgido nuevas formas de ataque, como envenenamiento de modelos de código abierto, es decir, la introducción de códigos dañinos en *software* y sistemas de IA para manipular sus datos de entrenamiento y alterar el comportamiento del modelo.

También señaló que la *dark web* ofrece una serie de servicios de ciberataques por encargo, de suplantación de identidad, además de *software* maliciosos como FraudGPT, que permite generar códigos para manipular sistemas informáticos.

"Los ciberdelincuentes están experimentando su propia transformación con la IA. Se dan cuenta que pueden atacar más rápido, escalar y tener más resultados, entonces es mayor su capacidad de monetización con este tipo de herramientas. Ahora, no existe IA buena o mala, es la intención que tenemos para utilizarla", comentó.

Respecto de la nueva Ley Marco de Ciberseguridad en Chile, Skokanovic valoró la regulación como un avance para que las empresas puedan mejorar la detección y respuesta ante amenazas, pero advirtió que no es suficiente para detener los ciberataques porque "no hay manera de frenar a los atacantes", lo seguirán haciendo.*