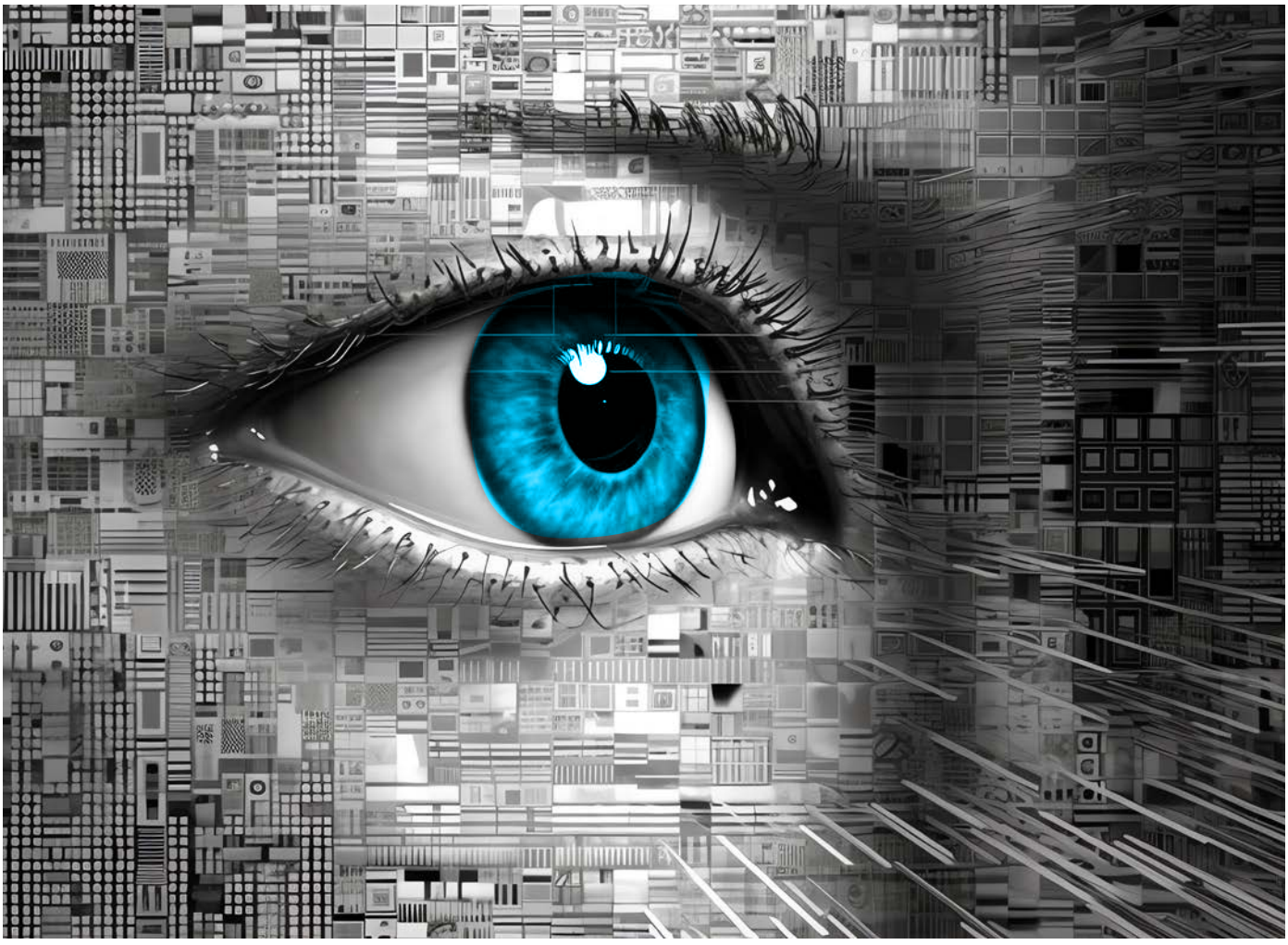
Entender a la IA, el primer paso para prevenir un ciberataque

La Inteligencia Artificial potencializa la forma en la que atacan los malware, sin embargo, aún existen formas para evitar caer en sus trampas, de acuerdo con Miguel del Olmo, director de la práctica de Consultoría en Baker Tilly México.

POR ELIZABETH VARGAS



La Inteligencia Artificial (IA) permite que laspersonas puedan acceder a información de manera más sencilla, incluso, ya es utilizada en algunas empresas para hacer más eficaces sus procesos.

No obstante, su uso le abre la puerta a formas de **ciberataques más sofisticadas**, ya que ahora los malwares, que son potencializados por algunos algoritmos, tienen el poder de entender la forma en la que los internautas reciben información para atacar de forma más certera.

Miguel del Olmo, director de la práctica de Consultoría en Baker Tilly México, explica que en la actualidad los softwares malignos diseñados con IA pueden llegar a través de correos electrónicos u otros medios de comunicación digitales, por lo tanto, es necesario redoblar esfuerzos e incrementar las medidas de ciberseguridad.

El analista comenta que, si bien, al momento de abrir un archivo que software maligno parece que no pasó nada se podría estar cimbrando un ciberataque. Esto quiere decir que comenzará a analizar la conducta de los internautas y con ello los criminales sabrán la forma en la que una persona actúa a través de la red.

85%
DE LOS CIBERATAQUES
son responsabilidad de los colaboradores

"Así es como un negocio puede recibir un correo con malware que venga disfrazado del correo de un cliente que pida una nota de crédito por una deficiencia de un producto. Este modo de operar proviene de un hackeo muy inteligente", detalla Miguel del Olmo.

Atrás quedaron los días en los que los cibercriminales intentaban estafar a las personas enviando correos impersonales y de fuentes con las que no tienen contacto. Ahora, detrás de cada virus potencializado con IA existe todo un proceso de análisis.

IA y el entendimiento de la conducta

"¿Por qué mis colaboradores han comenzado a utilizar IA?" Al responder esta pregunta los líderes podrían salvaguardar la integridad de su empresa, expone el experto de **Baker Tilly México**.

Entender y analizar el uso que se le da a la nueva tecnología son los primeros pasos que se pueden tomar para minimizar los riesgos ante un mundo lleno de malware cada vez más sofisticado. Para prevenir ese tipo de escenarios empresas tan grandes como Apple le han prohibido a sus equipos utilizar herramientas como **ChatGPT.**

A pesar de que muchas personas comienzan a ver el uso de las nuevas tecnologías con desconfianza, debido a las noticias que aseguran que la IA eliminará puestos laborales, la mayoría de los usuarios siguen apostando por estas herramientas.

Ya sea a través de una aplicación de mensajería instantánea, el uso de computadoras para el trabajo, las pantallas inteligentes o asistentes virtuales, los humanos diariamente le dan la bienvenida al aprendizaje automático.

Miguel del Olmos menciona que es normal utilizar cualquier equipo electrónico de forma diaria, sin embargo, lo que no es normal es temerle y para evitar caer en este escenario, lo mejor es imaginarse las peores consecuencias que puede ocasionar el mal uso de la IA en la empresa. Este es el principio básico del enfoque **Zero Trust.**

"Existe un enfoque Zero Trust que es muy saludable y se basa en pensar en el peor escenario y a partir de ahí empezar a desarrollar cuáles son los procesos de control que van a mitigar esos riesgos".

Al aplicar esta metodología los colaboradores podrán cerciorarse de que la información que le dan es la adecuada y que no pone en riesgo a la organización. Además, en caso de que los empleados alimenten las herramientas con información confidencial sobre su organización, el departamento de TI y las demás áreas sabrán cómo actuar para mitigar los daños.

"Los criminales abusan de la buena voluntad"

Un estudio de la Universidad de Standford y Tessian encontró que cerca del 85 por ciento de los ciberataques en las compañías fueron consecuencia del descuido de los colaboradores. Eso significa que una gran parte de la seguridad de las empreas recae en los hombros de sus equipos.

El porcentaje arrojado por el análisis no significa que los empleados diariamente tengan la intención de arriesgar los datos de sus lugares de trabajo, al contrario, muchos de ellos de lo único que son víctimas es de la falta de conocimiento, asegura el analista.

"Es necesario entender que los procesos de comunicación de los negocios están establecidos bajo un ámbito de confianza, por eso cuando recibes una solicitud para brindar un servicio de buena fe inicias un proceso. Es ahí cuando los criminales aprovechan la circunstancia", dice.

"LO DELICADO DE LOS ATAQUES ES QUE SON MÁS SOFISTICADOS PORQUE HAY UN PROCESO DE ENTENDIMIENTO DE CONDUCTA. PUEDE LLEGAR SPAMWARE CUANDO RECIBES CORREO, LO ABRES Y DESCARGAS UN PDF".

Tener la mente fría. Esa es una de las máximas recomendaciones que hace **Miguel del Olmo** a todos los colaboradores. Sin importar lo prometedora que sea la información que alguien recibe es mejor que antes de abrir un mensaje o correo electrónico la persona se pregunte si la dirección de donde le enviaron el mensaje es confiable.

Este es el punto en el que las empresas necesitan saber que para mantener la ciberseguridad en la empresa, no solamente es necesario que los expertos de tecnología de la información estén preparados para luchar contra un malware y prevenir su ataque. También otras áreas, como la de recursos humanos, deben involucrarse para brindar información a los empleados.

Más allá de ver a los colaboradores como posibles cómplices de los cibercriminales, es mejor verlos como aliados potenciales para minimizar las amenazas a las que una empresa ya está expuesta por el simple hecho de utilizar equipos digitales.

Las puertas de entrada a los malwares potencializados con IA

A pesar de que los criminales utilizan tecnología cada vez más sofisticada para acceder a las redes de las empresas, la forma en que intentan robar la información no ha cambiado mucho.

De acuerdo con el **director de la práctica de Consultoría en Baker Tilly México**, los delincuentes continúan engañando a sus víctimas a través de correos electrónicos, que contienen archivos adjuntos o links a páginas apócrifas, y mensajes de WhatsApp.

Para evitar caer en una trampa, es mejor prevenir que lamentar, por eso, el especialista explica que los empleados deben tener la suficiente confianza con el encargado del área de tecnología para pedir su ayuda si reciben un correo de dudosa procedencia.

"Debemos ser suspicaces y revisar antes de actuar. Tenemos que recordar que incluso hay ataques de ransomware que se han materializado por el solo hecho de cumplir un reto, por eso siempre es mejor extremar precauciones".

¿Cómo actuar antes de ser víctima de un ciberataque?

Para el experto es prioritario que los comités de auditoría que comparten información con el consejo de administración de las empresas hablen abiertamente sobre los peligros y las brechas de ciberseguridad que los acechan. Solo así es como se podrá implementar un ambiente de control en toda la organización.

Con el uso de la IA en el diseño de malwares ya no es una opción hablar de este tema en las reuniones más importantes, al contrario, es una necesidad.

"En todo comité de auditoría debemos de dejar un apartado para saber cómo se deben de abordar los riesgos de ciberseguridad y el tema presupuestal", añade.

13% DEL PRESUPUESTO
de una organización debe destinarse a temas de ciberseguridad

Miguel del Olmos recomienda a las organizaciones destinar entre el 6 y el 13 por ciento del presupuesto de tecnología para atender temas de ciberseguridad. Ese fondo debe ser utilizado para brindar a la fuerza laboral el entrenamiento necesario y con ello evitar ser víctimas de un engaño.

"Los datos son uno de los activos más importantes de las organizaciones, pero muchos directivos tienen información delicada en su celular personal y sin elementos de ciberseguridad. Aquí es donde se entiende lo urgente que es capacitarlos".

Elizabeth Vargas *es reportera y traductora senior de MIT Sloan Management Review México. Se especializa en el mercado de criptomonedas a nivel mundial y en temas relacionados con las finanzas, management, innovación, entre otros.*