LITORALPRESS

Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: Cinco cosas que debieran hacer todas las organizaciones, al tiempo que los atacantes utilizan la IA

Pág. : 16
Cm2: 567,6

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida


# Cinco cosas que debieran hacer todas las organizaciones, al tiempo que los atacantes utilizan la IA

Por: **Derek Manky,** Jefe de Estrategia de Seguridad y VP Global de Inteligencia de Amenazas en FortiGuard Labs.

***La inteligencia artificial (IA) beneficia a nuestra sociedad de muchas maneras, pero los cibercriminales están utilizando esta nueva tecnología con fines maliciosos. Desde la recopilación de datos de manera más eficiente hasta el uso de grandes modelos de lenguaje para elaborar comunicaciones de phishing, tanto los actores de amenazas experimentados como los novatos confían en la IA para agilizar sus esfuerzos.***

Las organizaciones de todo el mundo están empezando a notarlo y los ejecutivos están implementando esfuerzos para combatir éste y otros cambios en el panorama de amenazas. El 62% de los líderes empresariales dice que exigirán capacitación en ciberseguridad en forma de certificaciones para el personal de TI y seguridad. Casi la misma cantidad (61%) dice que está implementando nuevos programas de capacitación y concienciación sobre seguridad para todos los empleados.

## ¿Qué hacer para protegerse de las amenazas impulsadas por la IA?

Los actores maliciosos están aprovechando cada vez más la IA para aumentar el volumen y la velocidad de sus ataques. También están utilizando esta tecnología para hacer que el phishing y las amenazas relacionadas sean más creíbles que nunca. Si bien existen numerosos pasos que su equipo puede tomar para proteger mejor a su organización, aquí hay cinco cosas que puede hacer hoy para que todos en la empresa sean más conscientes y estén mejor preparados para defenderse de un panorama de amenazas cada vez más complejo.

1 **Construir una cultura de ciberseguridad:** La ciberseguridad es tarea de todos, no solo de los equipos de seguridad y TI. Para crear una cultura de ciberseguridad en la organización, hay que empezar por asegurarse de que los empleados de todos los niveles conozcan los riesgos cibernéticos comunes y comprendan el papel que desempeñan en el mantenimiento de una seguridad sólida. Para ello, los ejecutivos de todos los departamentos deben tener una visión compartida de la ciberseguridad y comunicar la importancia de proteger a la empresa periódicamente. Otras actividades deben incluir la realización de sesiones de formación en ciberseguridad, la implementación de planes de concienciación a largo plazo y la realización de simulacros para poner a prueba los conocimientos de los empleados sobre las ciberamenazas actuales.

2 **Educar a los colaboradores:** Los empleados siguen siendo objetivos de gran valor para los actores de amenazas, pero con el conocimiento adecuado, también pueden ser una sólida primera línea de defensa contra los intentos de intrusión. A medida que los ciberdelincuentes adoptan la IA, la educación continua en ciberseguridad debe ser una parte fundamental de su estrategia de gestión de riesgos. Si actualmente la empresa cuenta con un programa de educación de concienciación cibernética, es importarte reevaluarlo y actualizarlo con frecuencia para reflejar el cambiante panorama de amenazas. Si aún no ha implementado una iniciativa de educación, existen muchas ofertas basadas en SaaS disponibles, como el Servicio de capacitación y concientización sobre seguridad de Fortinet, que ofrece material de capacitación oportuno, y le permite realizar un seguimiento del progreso de los usuarios y personalizar el contenido de acuerdo con las necesidades de su organización o industria.

3 **Desarrollar (o reevaluar) los procesos y planes de ciberseguridad:** En lo que respecta a los incidentes de ciberseguridad, ya no se trata de si una organización sufrirá una intrusión, sino de cuándo. Casi el 90% de las empresas sufrieron al menos una intrusión durante el último año. La ciberseguridad

LITORALPRESS

Fecha: 31-07-2025
Medio: Revista Gerencia
Supl. : Revista Gerencia
Tipo: Noticia general
Título: Cinco cosas que debieran hacer todas las organizaciones, al tiempo que los atacantes utilizan la IA

Pág. : 17
Cm2: 560,8

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

ESPECIAL

# Ciberseguridad & IA

no es una cuestión de "configurarla y olvidarse". El desarrollo de un programa continuo de gestión de la exposición a amenazas permite a las empresas evaluar y reevaluar sus esfuerzos, lo que garantiza que cuentan con las personas, los procesos y la tecnología adecuados para gestionar el riesgo organizacional. Estas comprobaciones periódicas les permiten identificar posibles brechas de seguridad antes de que se conviertan en un problema.

*Los actores maliciosos están aprovechando cada vez más la IA para aumentar el volumen y la velocidad de sus ataques. También están utilizando esta tecnología para hacer que el phishing y las amenazas relacionadas sean más creíbles que nunca.*

**4 Implementación de autenticación multifactor y estrategia Zero Trust Network Access:** Tomando en cuenta que más del 80% de las brechas de datos se debe al robo de credenciales mediante ataques de fuerza bruta, es fundamental implementar la autenticación multifactor (MFA) y el acceso a la red de confianza cero (ZTNA). La MFA agrega otra capa de seguridad al exigir a los usuarios que verifiquen su identidad de varias maneras, como mediante una combinación de una contraseña y datos biométricos como una huella digital. Esto reduce significativamente el riesgo de que los ciberdelincuentes obtengan acceso no autorizado a su red, incluso si las credenciales de un usuario están comprometidas. Agregar ZTNA aumenta el acceso seguro a la información confidencial a través de túneles cifrados, controles de acceso granulares, acceso por aplicación y monitoreo de conexión continuo.

**5 Parcheo constante de software y aplicaciones:** La falta de parches en software y aplicaciones sigue siendo un factor importante en las brechas de seguridad. Según nuestro reciente Informe sobre el panorama de amenazas globales, en casi el 90% de los casos, la vulnerabilidad era conocida y había un parche disponible. Es fundamental mantener todo el software, los sistemas operativos y las aplicaciones actualizados con los últimos parches de seguridad. Si no cuenta con un proceso de gestión de parches, establezca uno hoy mismo para ayudar a agilizar las actualizaciones y garantizar que los parches se implementen rápidamente. En muchos casos, la IA puede ayudar a automatizar las tediosas tareas de aplicación de parches.

A medida que los atacantes perfeccionan su juego, las organizaciones deben reforzar sus defensas. Implementar iniciativas de educación y concientización sobre ciberseguridad ayuda a sentar las bases de una cultura de ciberseguridad. Desarrollar prácticas de ciberseguridad sólidas, que van desde MFA hasta ZTNA, y adoptar las tecnologías adecuadas también contribuyen en gran medida a proteger los activos digitales de su organización, recordando que la colaboración en toda la organización es vital para el éxito. La seguridad no es solo responsabilidad de sus equipos de seguridad y TI. Por sobre todas las cosas, las medidas sólidas de gestión de riesgos requieren que la ciberseguridad sea tarea de todos, ya que cada persona de su organización tiene un papel que desempeñar para interrumpir el cibercrimen. G