Un tercio de la información empresarial sensible ingresada en apps de IA son datos personales

- *El uso de IA generativa se ha triplicado en 12 meses, pero las organizaciones aún luchan por equilibrar la habilitación segura con la gestión de riesgos.*

Ciudad de México, 18 de julio de 2024.- Netskope, líder en Secure Access Service Edge (SASE), publicó una nueva investigación que muestra que los datos personales regulados (*datos que las organizaciones tienen el deber legal de proteger*) constituyen **más de un tercio de la data sensible que se comparte con aplicaciones de IA generativa (genAI)** en las empresas, presentando un riesgo potencial para las compañías de costosas brechas de datos.

La nueva investigación de Netskope Threat Labs revela que tres cuartas partes de las empresas encuestadas ahora bloquean completamente al menos una aplicación genAI, lo que refleja el deseo de los líderes tecnológicos empresariales de limitar el riesgo de exfiltración de datos sensibles.

Sin embargo, con menos de la mitad de las organizaciones aplicando controles centrados en los datos para prevenir que información sensible sea filtrada, la mayoría presenta retrasos en la adopción de soluciones avanzadas de prevención de pérdida de datos (DLP) necesarias para habilitar de manera segura la genAI.

Utilizando conjuntos de datos globales, los investigadores encontraron que **el 96% de las empresas ahora usan genAI**, un número que **se ha triplicado en los últimos 12 meses.** En promedio, las empresas ahora usan casi 10 aplicaciones genAI, frente a tres el año pasado, con los principales adoptantes utilizando un promedio de 80 aplicaciones, un aumento significativo desde 14.

Con ese aumento en el uso de este tipo de apps, las empresas han experimentado un aumento en el intercambio de código fuente propietario dentro de las aplicaciones genAI, representando el 46% de todas las violaciones documentadas de políticas de datos. Estas dinámicas cambiantes complican cómo las empresas controlan el riesgo, lo que exige un esfuerzo más robusto en DLP.

Netskope señala que existen señales positivas de gestión proactiva del riesgo en el matiz de los controles de seguridad y pérdida de datos que las organizaciones están aplicando: por ejemplo, el 65% de las empresas ahora implementan capacitación en tiempo real para guiar las interacciones de los usuarios con las aplicaciones genAI. Según la investigación, la capacitación efectiva de los usuarios ha jugado un papel crucial en la mitigación de los riesgos de datos, llevando al 57% de los usuarios a alterar sus acciones después de recibir alertas de capacitación.

"Asegurar la genAI necesita más inversión y mayor atención a medida que su uso se permea en las empresas sin señales de que disminuirá pronto", dijo James Robinson, Director de Seguridad de la Información de Netskope. *"Las empresas deben reconocer que los resultados de la genAI pueden exponer inadvertidamente información sensible, propagar desinformación o incluso introducir contenido malicioso. Se requiere un enfoque robusto de gestión de riesgos para salvaguardar datos, reputación y continuidad del negocio*".

El Informe de Nube y Amenazas de Netskope: Aplicaciones de IA en la Empresa también encuentra que:

- ChatGPT sigue siendo la aplicación más popular, con más del 80% de las empresas utilizándola
- Microsoft Copilot mostró el crecimiento más dramático en uso desde su lanzamiento en enero de 2024, con un 57%
- El 19% de las organizaciones han impuesto una prohibición total a GitHub CoPilot

Conclusiones clave para las empresas
Netskope recomienda que las empresas revisen, adapten y personalicen sus marcos de riesgos específicamente para la IA o genAI utilizando esfuerzos como el Marco de Gestión de Riesgos de IA de NIST. Los pasos tácticos específicos para abordar el riesgo de genAI incluyen:

- **Conozca su estado actual:** Comience evaluando sus usos existentes de IA, aprendizaje automático y aplicaciones genAI. Identifique vulnerabilidades y brechas en los controles de seguridad.
- **Implemente controles básicos:** Establezca medidas de seguridad fundamentales, como controles de acceso, mecanismos de autenticación y cifrado.
- **Planifique para controles avanzados:** Más allá de lo básico, desarrolle una hoja de ruta para controles de seguridad avanzados. Considere la modelación de amenazas, la detección de anomalías, la monitorización continua y la detección de comportamientos para identificar movimientos de datos sospechosos en entornos en la nube hacia aplicaciones genAI que se desvíen de los patrones normales de usuario.
- **Mida, comience, revise, iterativamente:** Evalúe regularmente la efectividad de sus medidas de seguridad. Adaptarlas y redefinirlas basándose en experiencias del mundo real y amenazas emergentes, es fundamental.

Descargue el informe completo de Nube y Amenazas: Aplicaciones de IA en la Empresa aquí. Para más información sobre amenazas habilitadas por la nube y los últimos hallazgos de Netskope Threat Labs, visite el Centro de Investigación de Amenazas de Netskope.

Sobre Netskope
Netskope, empresa líder global en SASE, ayuda a las organizaciones a aplicar principios de confianza cero (Zero Trust) e innovaciones en Inteligencia Artificial/Machine Learning para proteger datos y defenderse contra amenazas cibernéticas. Rápida y fácil de usar, la plataforma Netskope One y su motor de confianza cero

patentado proporcionan acceso optimizado y seguridad en tiempo real para personas, dispositivos y datos en cualquier lugar donde se encuentren. Miles de clientes confían en Netskope y en su poderosa red NewEdge para reducir riesgos y obtener una visibilidad sin igual en cualquier actividad en la nube, la web y aplicaciones privadas, proporcionando seguridad y acelerando el rendimiento de los sistemas. Obtén más información en https://www.netskope.com/