أوبر تُبلغ نحو 150 ألف سائق بسرقة بياناتهم إثر اختراق مزوّد البنية التحتية للذكاء الاصطناعي Fireworks



تبلغ أوبر نحو 150 ألف سائق بأن بياناتهم سُرقت عندما اخترق مهاجمون مزوّد البنية التحتية للذكاء الاصطناعي Fireworks في أوائل أكتوبر. الحادثة تذكير بمخاطر الأطراف الثالثة.

- تبلغ أوبر نحو 150 ألف سائق بوقوع اختراق للبيانات.
- سرق المهاجمون بيانات السائقين بعد اختراق Fireworks، وهي مزوّد للبنية التحتية للذكاء الاصطناعي.
- وقع اختراق Fireworks في أوائل أكتوبر.
- بحسب المقتطف المتاح، نشأ التعرض لدى مورّد وليس داخل أنظمة أوبر نفسها.

ما الذي أُعلن

بدأت أوبر بإبلاغ نحو 150 ألف سائق بأن بياناتهم سُرقت. ووفق التقرير، اخترق المهاجمون شركة Fireworks، وهي مزوّد للبنية التحتية للذكاء الاصطناعي، في أوائل أكتوبر، وأدى ذلك إلى الحصول على بيانات السائقين.

ولا يوضح المقتطف المتاح أنواع البيانات المتأثرة، ولا كيفية وصول المهاجمين، ولا إجراءات المعالجة المتخذة. ولذلك ينبغي عدم افتراض شيء في هذه النقاط إلى حين توفر معلومات أوفى.

أهمية الأمر للجهات المنظمة

تُظهر الحادثة كيف يمكن أن تتعرض البيانات الشخصية عبر مورّد يقف خلف علامة تجارية معروفة. فالمنظمات تستخدم منصات وبنى تحتية خارجية للذكاء الاصطناعي بصورة متزايدة، وكل بيانات شخصية تُشارك معها توسّع نطاق المخاطر ومسؤولية الجهة عن تلك البيانات.

وبالنسبة للجهات في المملكة، يمس ذلك إدارة مخاطر الأطراف الثالثة، وحوكمة مشاركة البيانات، والجاهزية للإبلاغ عن الحوادث، وهي مجالات تتوقع الجهات الرقابية فيها مسؤوليات واضحة وأدلة موثقة.

النهج المقترح

لا داعي للقلق، لكنها فرصة مناسبة للتأكد من البيانات الشخصية والسرّية التي يحتفظ بها موردو الذكاء الاصطناعي وغيرهم من مزودي البنية التحتية، ومن أن العقود وإجراءات الحوادث لديكم تتيح التصرف سريعاً إذا تعرّض أحدهم للاختراق.

ما يجب فعله الآن

1. حصر الموردين، وبخاصة منصات الذكاء الاصطناعي والحوسبة السحابية، الذين يعالجون بيانات شخصية أو سرّية لديكم، وتوثيق البيانات التي يحتفظ بها كل منهم.
2. مراجعة العقود للتأكد من مدد الإبلاغ عن الاختراقات والالتزامات الأمنية وحقوق التدقيق.
3. تقليل البيانات المشاركة مع مزودي الذكاء الاصطناعي، باستخدام الإخفاء أو إزالة الهوية حيثما أمكن.
4. إدراج سيناريوهات اختراق المورّدين في خطط الاستجابة للحوادث واختبارها.
5. التأكد من توثيق عملية تقييم الاختراقات والإبلاغ عنها وفق نظام حماية البيانات الشخصية (PDPL) وتحديد المسؤولين عنها.