خطأ من مايكروسوفت يتسبب في كشف رسائل بريد إلكتروني سرية لأداة الذكاء الاصطناعي Copilot

قبل يومين

يحفظ يشارك

ليف ماكماهون

مراسل متخصص في التكنولوجيا

صور غيتي

أقرت شركة مايكروسوفت بوجود خطأ تسبب في وصول مساعد العمل المدعوم بالذكاء الاصطناعي الخاص بها إلى رسائل البريد الإلكتروني السرية لبعض المستخدمين وتلخيصها عن طريق الخطأ.

لقد روجت شركة التكنولوجيا العملاقة لبرنامج Microsoft 365 Copilot Chat باعتباره وسيلة آمنة لأماكن العمل وموظفيها لاستخدام روبوت الدردشة القائم على الذكاء الاصطناعي التوليدي.

لكنها قالت إن مشكلة حديثة تسببت في ظهور معلومات لبعض مستخدمي المؤسسة من الرسائل المخزنة في مجلدات المسودات والبريد الإلكتروني المرسل - بما في ذلك تلك المصنفة على أنها سرية.

تقول مايكروسوفت إنها طرحت تحديثًا لإصلاح المشكلة، وأنها "لم توفر لأي شخص إمكانية الوصول إلى معلومات لم يكن مصرحًا له بالفعل برؤيتها".

ومع ذلك، حذر بعض الخبراء من أن السرعة التي تتنافس بها الشركات لإضافة ميزات جديدة للذكاء الاصطناعي تعني أن هذا النوع من الأخطاء أمر لا مفر منه.

يمكن استخدام برنامج Copilot Chat داخل برامج Microsoft مثل Outlook و Teams، ويستخدم للبريد الإلكتروني ووظائف الدردشة، للحصول على إجابات للأسئلة أو تلخيص الرسائل.

قال متحدث باسم مايكروسوفت لبي بي سي نيوز: "لقد حددنا وعالجنا مشكلة حيث يمكن لـ Microsoft 365 Copilot Chat إرجاع محتوى من رسائل البريد الإلكتروني المصنفة على أنها سرية والتي كتبها المستخدم وتم تخزينها ضمن المسودات والعناصر المرسلة في Outlook على سطح المكتب".

وأضافوا: "على الرغم من أن ضوابط الوصول وسياسات حماية البيانات لدينا ظلت سليمة، إلا أن هذا السلوك لم يلب تجربة Copilot المقصودة، والتي صُممت لاستبعاد المحتوى المحمي من الوصول إلى Copilot".

"تم نشر تحديث للتكوين على مستوى العالم لعملاء المؤسسات."

تم الإبلاغ عن هذا الخطأ لأول مرة من قبل موقع **Bleeping** الإخباري التقني ، والذي ذكر أنه رأى تنبيهًا من **Computer** الخدمة يؤكد المشكلة.

وأشارت إلى إشعار من مايكروسوفت يقول إن "رسائل البريد الإلكتروني للمستخدمين التي تحمل علامة سرية تتم معالجتها بشكل غير صحيح بواسطة دردشة Microsoft 365 Copilot".

وأضاف الإشعار أن علامة تبويب العمل داخل تطبيق Copilot Chat قد لخصت رسائل البريد الإلكتروني المخزنة في مجلدات المسودات والمرسلة الخاصة بالمستخدم، حتى عندما كانت تحتوي على علامة حساسية وسياسة منع فقدان البيانات مهيأة لمنع مشاركة البيانات غير المصرح بها.

تشير التقارير إلى أن شركة مايكروسوفت علمت بالخطأ لأول مرة في يناير.

كما تم نشر إشعارها بشأن الخلل على لوحة دعم للعاملين في NHS في إنجلترا - حيث يُعزى السبب الجذري إلى "مشكلة في التعليمات البرمجية".

يشير جزء من **الإشعار الموجود على موقع دعم تكنولوجيا** إلى أنه قد تأثر **المعلومات التابع لهيئة الخدمات الصحية الوطنية**.

لكنها صرحت لبي بي سي نيوز بأن محتويات أي مسودة أو رسائل بريد إلكتروني مرسلة تتم معالجتها بواسطة Copilot Chat ستبقى مع منشئيها، ولم يتم الكشف عن معلومات المرضى.

"سيحدث تسريب للبيانات"

غالبًا ما تحتوي أدوات الذكاء الاصطناعي للمؤسسات مثل Microsoft 365 Copilot Chat - المتاحة للمؤسسات التي لديها اشتراك Microsoft 365 - على ضوابط أكثر صرامة وحماية أمنية لمنع مشاركة المعلومات المؤسسية الحساسة.

لكن بالنسبة لبعض الخبراء، لا تزال هذه المسألة تسلط الضوء على مخاطر اعتماد أدوات الذكاء الاصطناعي التوليدي في بيئات عمل معينة.

قال نادر حنين، محلل حماية البيانات وحوكمة الذكاء الاصطناعي في شركة غارتنر، إن "هذا النوع من الأخطاء لا مفر منه"، نظراً لتكرار "قدرات الذكاء الاصطناعي الجديدة والمبتكرة" التي يتم إصدارها.

وقال لبي بي سي نيوز إن المؤسسات التي تستخدم منتجات الذكاء الاصطناعي هذه غالباً ما تفتقر إلى الأدوات اللازمة لحماية نفسها وإدارة كل ميزة جديدة.

وقال هينين: "في الظروف العادية، تقوم المنظمات ببساطة بإيقاف تشغيل هذه الميزة وتنتظر حتى تلحق بها الحوكمة".

وأضاف: "لسوء الحظ، فإن حجم الضغط الناجم عن سيل الضجة الإعلامية غير المثبتة حول الذكاء الاصطناعي يجعل ذلك شبه مستحيل".

قال البروفيسور آلان وودوارد، خبير الأمن السيبراني بجامعة ساري، إن ذلك أظهر أهمية جعل هذه الأدوات خاصة بشكل افتراضي ولا تتطلب سوى الاشتراك.

وقال لبي بي سي نيوز: "لا بد من وجود أخطاء في هذه الأدوات، خاصةً مع تقدمها بسرعة فائقة، لذلك حتى لو لم يكن تسريب البيانات متعمداً، فإنه سيحدث".