توقيف موظف في OpenAI للاشتباه في زرع جهاز تسجيل خفي في قاعة اجتماعات الإدارة التنفيذية



أُوقف موظف في OpenAI يبلغ 35 عاماً ووُجهت إليه تهمة زرع جهاز تسجيل خفي في قاعة اجتماعات تنفيذية بمكاتب الشركة في سان فرانسيسكو. وتذكّر القضية بأن مخاطر الداخل تشمل التنصت المادي.

- المشتبه به هو عبدالرحمن الفوزان (35 عاماً)، سعودي الجنسية وموظف في OpenAI.
- يُتهم بوضع جهاز تسجيل خفي في قاعة اجتماعات تنفيذية بمكاتب الشركة في سان فرانسيسكو.
- يُزعم أن الجهاز كان لتسجيل محادثات حساسة دون علم المشاركين.
- التهمة هي استخدام جهاز أو محاولة استخدامه لاعتراض اتصالات شفهية.
- لا يتضمن المقتطف المتاح تفاصيل إضافية عن التحقيق أو نتيجته.

أُوقف مواطن سعودي يعمل في OpenAI للاشتباه في وضعه جهاز تسجيل خفياً داخل قاعة اجتماعات تنفيذية في مكاتب الشركة بسان فرانسيسكو. ويُدعى المشتبه به عبدالرحمن الفوزان (35 عاماً)، وهو متهم بمحاولة تسجيل محادثات حساسة دون علم أصحابها.

ما الذي يُزعم

وُجهت إليه تهمة استخدام جهاز إلكتروني أو ميكانيكي أو غيره لاعتراض اتصالات شفهية، أو محاولة ذلك. وما ورد حتى الآن ادعاءات؛ فالمقتطف المتاح لا يوضح كيف اكتُشف الجهاز ولا ما جرى تسجيله ولا مسار القضية، ولا نفترض شيئاً في هذه النقاط.

أهميتها للجهات المنظمة

تركّز برامج الأمن عادة على الشبكات والحسابات ومخازن البيانات. وتشير هذه القضية إلى قناة مختلفة، هي الكلام المسموع في القاعات التي تُناقش فيها الاستراتيجية والاستجابة للحوادث والمسائل التنظيمية. فالجهاز الذي يضعه شخص يملك صلاحية دخول مشروعة يتجاوز الضوابط التقنية بالكامل.

وفي البنوك وشركات التأمين وسائر الجهات المنظمة في المملكة، كثيراً ما تتناول قاعات مجالس الإدارة والاجتماعات التنفيذية معلومات خاضعة لالتزامات السرية. لذا ينبغي التعامل مع هذه القاعات بوصفها أصولًا حساسة ضمن ضوابط الأمن المادي ومخاطر الداخل.

يحسن النظر إلى الحادثة كدافع لمراجعة الضوابط القائمة، لا كدليل على حملة أوسع؛ فلا يشير المصدر إلى تأثر جهات أخرى.

ما يجب فعله الآن

1. تحديد القاعات المستخدمة لاجتماعات مجلس الإدارة والإدارة التنفيذية والاستجابة للحوادث والشؤون التنظيمية وتصنيفها مناطق حساسة.
2. إضافة فحص مادي دوري لهذه القاعات، يشمل الكشف التقني عن أجهزة التنصت عندما تبرر المخاطر ذلك.
3. تقييد الدخول إلى قاعات الاجتماعات الحساسة وتسجيله، بما في ذلك دخول فرق النظافة والصيانة والمقاولين.
4. وضع قواعد واضحة لإدخال الأجهزة القادرة على التسجيل إلى الاجتماعات الحساسة ولترك المعدات دون مراقبة.
5. تضمين التنصت المادي في برامج التوعية بمخاطر الداخل، وتوفير وسيلة بسيطة للإبلاغ عن أي جهاز غير مألوف.
6. الاتفاق مسبقاً على آلية حفظ الجهاز المشتبه به وتصعيد الأمر وإبلاغ الإدارة القانونية وقيادة الأمن.