اختراق موقع وزارة الخارجية النمساوية عبر مزوّد خدمة خارجي والوصول إلى بيانات التواصل الخاصة بالدبلوماسيين



اخترق مهاجمون موقعًا تابعًا لوزارة الخارجية النمساوية يديره مزوّد خارجي يومي 12 و13 نوفمبر، وطالوا أسماء الموظفين وبيانات التواصل الرسمية. وتقول الوزارة إن الحادثة جرى احتواؤها ولم تتأثر بيانات الجمهور.

- وقع الاختراق بين 12 و13 نوفمبر على موقع يديره مزوّد خدمة خارجي.
- طال الوصول أسماء الموظفين وبيانات التواصل الرسمية في المقر بفيينا وفي البعثات الدبلوماسية بالخارج.
- تفيد الوزارة بأن الحادثة جرى احتواؤها وأن البيانات الشخصية للجمهور لم تتعرض للاختراق.
- لم تُحدَّد هوية المهاجمين، ولا يزال غير واضح كيف تمكنوا من الدخول أو ما إذا كانت بيانات قد سُرقت فعلاً.

- أبلغت الوزارة الجهات النمساوية المعنية بالأمن السيبراني وحماية البيانات، ولم تنسب الحادثة إلى أي جهة.

أعلنت وزارة الخارجية النمساوية تعرّض أحد مواقعها الإلكترونية لاختراق. ووفق بيان للوزارة نقلته هيئة الإذاعة النمساوية (ORF)، وقع الاختراق يومي 12 و13 نوفمبر وطال موقعًا يديره مزوّد خدمة خارجي.

ما هو معلوم

تمكن المهاجمون من الوصول إلى أسماء الموظفين وبيانات التواصل الرسمية في مقر الوزارة بفيينا وفي البعثات الدبلوماسية النمساوية بالخارج. وتؤكد الوزارة أن الاختراق جرى احتواؤه وأن البيانات الشخصية للجمهور لم تتعرض للخطر.

لكن جوانب كثيرة ما زالت غير واضحة؛ فلم تُحدَّد هوية المهاجمين، ولم تُعلن طريقة الدخول، ولا يُعرف ما إذا كانت أي معلومات قد سُرقت فعلاً. وامتنعت الوزارة عن الإفصاح عن تفاصيل تقنية لأسباب أمنية، وقالت إنها لم تنسب الحادثة إلى أي جهة. وقد أبلغت الجهات الوطنية المعنية بالأمن السيبراني وحماية البيانات.

وتزامن الحادث مع انقطاع عالمي في خدمات Microsoft أرجعته الشركة إلى خلل برمجي وأعطال في البنية التحتية، ولم تثبت السلطات النمساوية وجود صلة بين الحدثين.

لماذا يهم المؤسسات في المملكة

تبيّن الحادثة أن موقعًا يديره طرف ثالث قد يكشف بيانات دليل الموظفين في جهة حكومية. وحتى الأسماء وبيانات التواصل الأساسية قد تُستغل في التصيّد الموجَّه والهندسة الاجتماعية. وينبغي للمؤسسات المنظمة في المملكة التي تعتمد على مزوّدين خارجيين لاستضافة المواقع والبوابات أن تتحقق من البيانات التي تحتفظ بها تلك البيئات ومن مسار التصعيد عند وقوع الحوادث.

ما يجب فعله الآن

1. حصر المواقع والبوابات التي يديرها مزوّدون خارجيون وتوثيق البيانات التي يحتفظ بها كل منها عن الموظفين أو العملاء.
2. التأكد من أن عقود الأطراف الثالثة تُلزم بالإبلاغ الفوري عن الحوادث وإتاحة سجلات الدخول ودعم الاحتواء.
3. الحدّ من بيانات دليل الموظفين المنشورة علنًا بما تقتضيه الحاجة التشغيلية.
4. تنبيه الموظفين، لا سيما المدرجة أسماؤهم في أدلة عامة، إلى محاولات التصيّد الموجَّه وانتحال الهوية.
5. مراجعة خطط الاستجابة للحوادث للتأكد من تغطيتها اختراقات الأطراف الثالثة والتزامات الإبلاغ للهيئة الوطنية للأمن السيبراني، وعند الاقتضاء لسدايا أو البنك المركزي السعودي.