وزارة العمل والمعاشات البريطانية تعطّل خدماتها الإلكترونية بعد حادث سيبراني



عطّلت وزارة العمل والمعاشات البريطانية بعض خدماتها الإلكترونية احترازياً إثر حادث سيبراني لم تُكشف طبيعته، مع التأكيد على أن صرف المعاشات والإعانات يجري كالمعتاد.

- أعلنت الوزارة وقوع حادث سيبراني وعطّلت بعض خدماتها الإلكترونية كإجراء احترازي.
- لم تُفصح الوزارة عن طبيعة الحادث.
- أكدت أن صرف المعاشات والإعانات الدورية لم يتأثر.
- تعمل الوزارة مع المركز الوطني للأمن السيبراني البريطاني ومركز التنسيق السيبراني الحكومي للتحقيق وإعادة الخدمات.
- أفاد المركز البريطاني مؤخراً بارتفاع ملحوظ منذ سبتمبر في الهجمات المدعومة بالذكاء الاصطناعي.

أعلنت وزارة العمل والمعاشات البريطانية (DWP) يوم الجمعة أنها تعرّضت لحادث سيبراني، وأنها عطّلت بعض خدماتها الإلكترونية كإجراء احترازي.

ما هو معروف

لم تكشف الوزارة طبيعة الحادث. وقال متحدث باسمها إن صرف المعاشات والإعانات الدورية لم يتأثر وسيستمر كالمعتاد. والوزارة هي الأكبر في الحكومة البريطانية من حيث الإنفاق، وتدير المعاش التقاعدي الحكومي وعدداً من الإعانات التي يعتمد عليها ملايين الأشخاص في تغطية نفقاتهم الأساسية.

وذكرت أنها تعمل بشكل وثيق مع المركز الوطني للأمن السيبراني (NCSC) ومركز التنسيق السيبراني الحكومي للتحقيق وإعادة الخدمات في أسرع وقت ممكن.

السياق الأوسع

يأتي الحادث بعد أيام من إعلان المركز الوطني للأمن السيبراني البريطاني رصد ارتفاع ملحوظ منذ سبتمبر في الهجمات السيبرانية المدعومة بالذكاء الاصطناعي. وكانت الحكومة البريطانية قد أقرّت في وقت سابق من هذا العام بأن نهجها الممتد لسنوات في تأمين أنظمتها كان معيباً، وبأن تحقيق هدف حماية جميع الجهات الحكومية من الثغرات وأساليب الهجوم المعروفة بحلول 2030 لن يكون ممكناً، ووصفت المخاطر السيبرانية في القطاع العام بأنها مرتفعة للغاية.

أهمية الخبر للجهات المنظّمة

يعكس الحادث نمط استجابة شائعاً: عزل القنوات الرقمية أولًا، وحماية عمليات الدفع الأساسية، وإشراك الجهات الوطنية المعنية بالأمن السيبراني مبكراً. ولا تزال التفاصيل محدودة، لذا لا ينبغي الجزم بالسبب أو الأثر. ويمكن للجهات التي تقدّم خدمات أساسية الاستفادة منه لاختبار جاهزية خطط الاحتواء والتواصل لديها.

ما يجب فعله الآن

1. تأكد من قدرتكم على إيقاف خدمات رقمية بعينها بسرعة مع استمرار عمليات الدفع والمعاملات الأساسية.
2. راجعوا خطط الاستجابة للحوادث بما يضمن إبلاغ الهيئة الوطنية للأمن السيبراني مبكراً، وإبلاغ البنك المركزي السعودي أو الجهة التنظيمية القطاعية عند الاقتضاء.
3. اختبروا نماذج التواصل مع العملاء والجمهور لتوضيح تعليق الخدمة احترازياً دون ذكر تفاصيل غير مؤكدة.
4. تحققوا من أن خطط استمرارية الأعمال تحدد أولويات الاستعادة وفترات التوقف المقبولة للبوابات الموجهة للعملاء أو المستفيدين.
5. أدرجوا سيناريوهات الهجمات المدعومة بالذكاء الاصطناعي، مثل التصيد الأكثر إقناعاً، في تقييم التهديدات القادم ومواد التوعية.