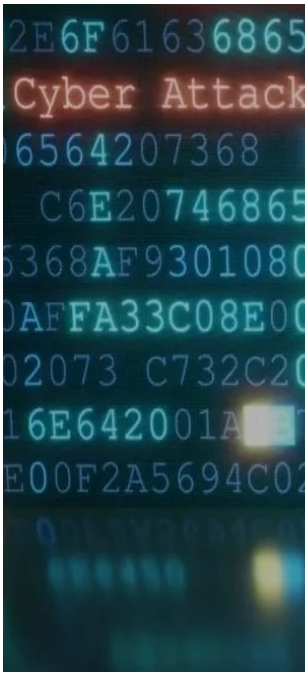
الهجمات السيبرانية ترتفع بنسبة 50% في المملكة المتحدة



كشف المركز الوطني للأمن السيبراني البريطاني "NCSC"، اليوم الثلاثاء، عن ارتفاع حاد في الهجمات السيبرانية في المملكة المتحدة خلال العام الماضي، بنسبة بلغت 50%.

ووفقاً للمركز التابع لمقر الاتصالات الحكومية "GCHQ"، فقد اعتبر المسؤولون هذا التصاعد "دعوة للتأهب"، محذرين من أن اعتماد المجتمع المتزايد على التكنولوجيا يُضاعف من حجم التهديدات الإلكترونية، وعلى رأسها هجمات برامج الفدية.

وبحسب التقرير السنوي للمركز، تعاملت أجهزة الأمن السيبراني مع 429 حادثة إلكترونية خلال العام الماضي، صُنف نصفها تقريباً كحوادث ذات أهمية وطنية، في حين تم تصنيف 18 منها على أنها "بالغة الخطورة"، لما لها من تأثير مباشر على الحكومة، والخدمات الحيوية، والبنية التحتية، والسكان، والاقتصاد.

وأشار موقع صحيفة "الغارديان" البريطانية، إلى أن القيادات الأمنية والوزراء حذروا المؤسسات

العامة والخاصة، من "احتمالية توقف البنية التحتية الرقمية في أي لحظة"، مطالبين بوضع خطط طوارئ فورية.

وفي رسائل موجهة إلى مئات من كبرى الشركات، دعا وزراء، المالية راشيل ريفز، والأمن دان جارفيس، والتكنولوجيا ليز كيندال، والأعمال وبيتر كايل، إلى جعل المرونة السيبرانية مسؤولية على مستوى مجالس الإدارة، شيرين إلى أن الهجمات باتت "أكثر كثافة وتكراراً".

وحدد التقرير السنوي الصين وروسيا وإيران وكوريا الشمالية كأبرز مصادر التهديد الخارجي، لافتاً إلى أن الهجمات غالباً ما تُنفذ عبر برامج فدية تقودها جماعات إجرامية تسعى للابتزاز المالي.

وأكدت مديرة "GCHQ"، آن كيستر-بتلر، على أهمية الإدارة الفعالة للمخاطر السيبرانية، قائلة: "لا تكن هدفاً سهلاً، اجعل إدارة المخاطر جزءاً من حوكمة المؤسسة، وقُد الاستجابة من القمة".

وأشار المركز أيضاً إلى تهديدات داخلية متزايدة، حيث تم مؤخراً اعتقال مراهقين يبلغان من العمر 17 عاماً في هيرتفوردشاير، على خلفية اختراق سلسلة حضانات "كيدو" وتسريب بيانات حساسة.
وتسببت هجمات برامج الفدية في أضرار كبيرة لمؤسسات بارزة، من بينها "ماركس آند سبنسر" و"كو-أوب".

كما يخضع الهجوم الأخير الذي شل خطوط إنتاج "جاكوار لاند روفر" لتحقيق أمني، وسط تقارير عن احتمال تورط جهات روسية، وهو ما رفض المركز التعليق عليه مباشرة.

ووفقًا للمركز، يُعد العام الماضي الأعلى في معدلات التهديد السيبراني منذ تأسيسه قبل تسعة أعوام.

وخلال الأشهر الـ12 الماضية، كشفت المملكة المتحدة وحلفاؤها عن وحدة عسكرية روسية تنفذ هجمات سيبرانية، وأصدرت تحذيرات بشأن حملة إلكترونية صينية تستهدف آلاف الأجهزة، ولفتت الانتباه إلى تحركات إيرانية في هذا السياق.

ورغم عدم تسجيل أي هجوم مباشر عبر الذكاء الاصطناعي حتى الآن، حذر المركز من أن هذه التكنولوجيا "ستُشكل تحديات كبرى في مجال الأمن السيبراني حتى عام 2027 وما بعده".
وأشار إلى استخدام المهاجمين أدوات الذكاء الاصطناعي بشكل متزايد لتحسين كفاءة عملياتهم.

وقال ريتشارد هورن، الرئيس التنفيذي للمركز الوطني للأمن السيبراني: "نشهد تطوراً متسارعاً في قدرات المهاجمين، ما يسمح لهم بإلحاق أضرار فادحة بالمؤسسات، والضرر لا يتوقف عند الأنظمة، بل يمتد ليشمل الموظفين والعملاء وسلاسل التوريد".

وأكد هورن، أن الأثر النفسي للهجمات لا يقل خطورة عن الأثر التقني، مضيفاً: "جلستُ مع العديد ممن تأثروا بهذه الهجمات، والقلق والاضطراب الذي يشعرون به واقعي ومؤلم".