المركز الوطني للأمن السيبراني البريطاني يحذّر من هجمات فدية مدعومة بالذكاء الاصطناعي على البنية التحتية الحرجة بحلول 2028



يرى المركز الوطني للأمن السيبراني البريطاني أن من المرجّح جدًا استخدام برمجيات خبيثة مدعومة بالذكاء الاصطناعي في هجوم فدية على البنية التحتية الوطنية الحرجة بحلول 2028، وأن الخطر ناتج عن ثغرات قديمة لا عن أساليب هجوم جديدة.

- يفيد تقرير حالة الأمن السيبراني الوطني بأن من المرجّح جدًا استخدام برمجيات خبيثة مدعومة بالذكاء الاصطناعي في هجوم فدية على البنية التحتية الحرجة في المملكة المتحدة بحلول 2028.
- خلال عامين، يُرجّح بشدة أن يزيد استخدام الجهات المعادية للذكاء الاصطناعي من حجم وكفاءة هجمات الفدية والهندسة الاجتماعية واستغلال الثغرات.
- يؤكد الرئيس التنفيذي للمركز أن الخطر ينبع من اكتشاف ثغرات جرى التساهل معها طويلاً واستغلالها على نطاق واسع، لا من ابتكار الذكاء الاصطناعي لأساليب جديدة.

- من الخيارات الموصى بها: استثمار كافٍ في التقنية، وتجنب الاتصال غير الضروري بالإنترنت، واعتبار Cyber Essentials نقطة بداية لا غاية.
- أعلنت الحكومة البريطانية تمويل درع سيبراني وطني ومركزًا لرصد التعرض للثغرات ومركز تميّز في أمن الذكاء الاصطناعي.

نشر المركز الوطني للأمن السيبراني في المملكة المتحدة، التابع لهيئة GCHQ، تقريره «حالة الأمن السيبراني الوطني». ويحذّر التقرير من ضرورة استعداد البنية التحتية الوطنية الحرجة لهجوم فدية يتضمن برمجيات خبيثة مدعومة بالذكاء الاصطناعي بحلول 2028، ومن أن استخدام الجهات المعادية للذكاء الاصطناعي سيزيد خلال عامين، بدرجة مرجّحة جدًا، من حجم وكفاءة هجمات الفدية والهندسة الاجتماعية واستغلال الثغرات.

ما يقوله المركز

يطرح الرئيس التنفيذي للمركز، الدكتور ريتشارد هورن، المسألة بوصفها مسألة أساسيات لا جِدّة. فهو يرى أن ارتفاعًا غير مسبوق في الحوادث احتمال حقيقي، لكن ليس لأن الذكاء الاصطناعي ابتكر طرق هجوم جديدة، بل لأن ثغرات جرى التساهل معها طويلاً يمكن اليوم اكتشافها واستغلالها على نطاق لم يكن متصورًا. ويصف مرحلة «التقنية الرخيصة» بأنها يجب أن تنتهي.

ويدعو التقرير المؤسسات إلى الاستفادة من الأدوات والمعايير والأطر القائمة والمثبتة فعاليتها في الحماية من الهجمات التقليدية والمدعومة بالذكاء الاصطناعي. ومن الخيارات المحددة: الاستثمار الكافي في التقنية، وعدم ترك الأنظمة متصلة بالإنترنت دون حاجة، واعتبار Cyber Essentials نقطة البداية، مع بناء مستوى أعلى من المرونة بحسب الحجم والتعقيد والمخاطر.

الاستجابة الحكومية

تمضي المملكة المتحدة في مشروع قانون الأمن السيبراني والمرونة وخطة العمل السيبراني الوطنية المرتقبة. ومن التمويل المعلن: 60 مليون جنيه إسترليني للمرحلة الأولى من درع سيبراني وطني، و70 مليون جنيه لمركز وطني لرصد التعرض والثغرات في الوقت الفعلي، ومركز تميّز لأمن الذكاء الاصطناعي في مانشستر يديره المركز.

الأهمية للمؤسسات السعودية

التقرير تقييم بريطاني، لكن رسالته تنطبق على أي جهة خاضعة للتنظيم: الذكاء الاصطناعي يقلّص الفترة بين وجود الضعف واستغلاله. ويمكن اعتباره دافعًا لمراجعة الأساسيات والتعرض الخارجي ومستوى الاستثمار في ضوء التزامات الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي القائمة.

ما يجب فعله الآن

1. مراجعة الأصول المكشوفة على الإنترنت، وإزالة أو تقييد أي نظام لا يحتاج إلى هذا الانكشاف.
2. التأكد من أن إدارة التحديثات والثغرات تشمل الأنظمة القديمة، مع تحديد المسؤوليات والجداول الزمنية.
3. التحقق من تطبيق الضوابط الأساسية بالكامل في الضوابط الأساسية للأمن السيبراني (ECC) وإطار الأمن السيبراني للقطاع المالي (SAMA CSF) حيثما ينطبق، قبل إضافة ضوابط جديدة.
4. تحديث خطط الاستجابة لهجمات الفدية والتعافي منها، واختبارها وفق سيناريو استغلال أسرع وأوسع

نطاقًا.

5. إطلاع الإدارة التنفيذية ومجلس الإدارة على مخاطر نقص الاستثمار في التقنية والأمن استنادًا إلى تقييم المخاطر الخاص بالمؤسسة.