

رئيس الأمن السيبراني البريطاني يحذّر من «عاصفة مثالية» مع تسارع الذكاء الاصطناعي والتوترات الجيوسياسية



قال رئيس المركز الوطني للأمن السيبراني في المملكة المتحدة في مؤتمر CYBERUK إن التقدم السريع في الذكاء الاصطناعي والتوترات الجيوسياسية يخلقان حالة من عدم اليقين، ودعا إلى جعل الأمن السيبراني جزءًا من مهمة كل فرد.

- ألقى الدكتور ريتشارد هورن، الرئيس التنفيذي للمركز الوطني للأمن السيبراني البريطاني، كلمة في مؤتمر CYBERUK في غلاسكو يوم 22 أبريل.
- وصف التغير التقني السريع مع التوترات الجيوسياسية بأنه «عدم يقين مضطرب» يستدعي تحولاً ثقافياً في الدفاع السيبراني.
- عدد الحوادث التي يتعامل معها المركز مستقر نسبياً، لكن معظم الحوادث ذات الأهمية الوطنية باتت تنشأ بصورة مباشرة أو غير مباشرة من دول.

- أكد أن الفضاء السيبراني يقع «بين السلم والحرب» وأن العمليات السيبرانية أصبحت جزءًا أصيلاً من النزاعات.
- الذكاء الاصطناعي المتقدم يمكّن من اكتشاف الثغرات القائمة واستغلالها على نطاق واسع، ما يكشف سريعًا مواطن القصور في أساسيات الأمن السيبراني.

ما الذي قيل

خلال كلمته في مؤتمر CYBERUK في غلاسكو، قال الدكتور ريتشارد هورن، الرئيس التنفيذي للمركز الوطني للأمن السيبراني في المملكة المتحدة، إن بلاده تواجه «عاصفة مثالية». وأشار إلى اجتماع ثورة تقنية جديدة يقودها الذكاء الاصطناعي مع تصاعد التوترات الجيوسياسية، ووصف ذلك بأنه مرحلة من «عدم اليقين المضطرب».

ورأى أن نطاق الأمن السيبراني يتسع؛ فتأمين التقنيات التي تتحكم بالروبوتات والأنظمة الذاتية والأجهزة المدمجة بجسم الإنسان يتجاوز كثيرًا ما كان مفهومًا قبل عقد، ما يتطلب من المنظمات إعادة التفكير في المفهوم باستمرار.

صورة التهديد

وبحسب الكلمة، فإن عدد الحوادث التي يعالجها المركز مستقر نسبيًا، لكن مصدرها تغيّر؛ فمعظم الحوادث ذات الأهمية الوطنية تنشأ الآن بصورة مباشرة أو غير مباشرة من دول. وقال إن الفضاء السيبراني جزء من فضاء متنازع عليه بين السلم والحرب، وإن روسيا تطبق دروسًا تعلمتها في ساحة المعركة في أوكرانيا خارجها، وإن العمليات السيبرانية أصبحت جزءًا أصيلاً من النزاعات.

وفي ما يخص الذكاء الاصطناعي المتقدم، قال إنه يمكّن بسرعة من اكتشاف الثغرات القائمة واستغلالها على نطاق واسع، ما يظهر مدى سرعة انكشاف الأساسيات التي لم تُعالج بعد.

لماذا يهم ذلك

تمحورت الرسالة الأساسية حول الثقافة: الأمن السيبراني مسؤولية الجميع، من مجلس الإدارة إلى مكتب الدعم الفني، والمنظمات التي لا تعدّ قاعدتها التقنية جوهرية لازدهارها لا تدرك واقع اليوم. ورغم أن الكلمة تخص المملكة المتحدة، فإن محاورها تنطبق على أي جهة منظمة تعتمد على الخدمات الرقمية.

ما يجب فعله الآن

1. إطلاع مجلس الإدارة والإدارة التنفيذية على العلاقة بين التوترات الجيوسياسية ونشاط الدول وملف المخاطر الخاص بالجهة.
2. مراجعة وضوح مسؤوليات الأمن السيبراني لكل دور وظيفي، من القيادة العليا إلى الدعم الفني، وتعزيزها ببرامج التوعية.
3. التحقق من الأساسيات كحصر الأصول وإدارة التحديثات والثغرات، في ظل تسارع استغلال الثغرات المعروفة بالذكاء الاصطناعي.
4. إعادة تقييم نماذج التهديد وخطط الاستجابة للحوادث والتعافي منها لسيناريوهات مرتبطة بجهات حكومية، واختبارها بتمارين.
5. مواءمة هذه الأولويات مع برنامج الضوابط وفق الضوابط الأساسية للأمن السيبراني (NCA ECC)

وإطار الأمن السيبراني للقطاع المالي (SAMA CSF) وتسجيل الفجوات في سجل المخاطر.