

المركز الوطني للأمن السيبراني البريطاني: جهات حكومية معادية وراء 75% من الهجمات على البنى التحتية الحرجة



أدار المركز الوطني للأمن السيبراني البريطاني أكثر من 200 حادثة سيبرانية استهدفت البنى التحتية الحرجة حتى مايو 2026، وثلاثة أرباعها مرتبطة بجهات حكومية معادية تشمل روسيا والصين وإيران.

- أكثر من 200 حادثة سيبرانية استهدفت البنى التحتية الحرجة البريطانية أدارها المركز الوطني للأمن السيبراني حتى مايو 2026
- حوالي 75% من هذه الحوادث مرتبطة بجهات حكومية معادية تشمل روسيا والصين وإيران
- المدير التنفيذي للمركز يحذر من ضرورة التعامل مع الأمن السيبراني كمواجهة مستمرة مع خصوم أكفاء وليس مجرد مخاطر تُدار
- من المتوقع استخدام قدرات سيبرانية معززة بالذكاء الاصطناعي على نطاق واسع ضد الأنظمة القديمة في البنى التحتية الحرجة بحلول 2028
- دعوة المؤسسات للتركيز على فهم التعرض للتهديدات وبناء دفاعات أقوى وضمان استمرارية

التحديات المدعومة من دول معادية تهيمن على هجمات البنى التحتية الحرجة

كشف رئيس المركز الوطني للأمن السيبراني البريطاني أن جهات حكومية معادية كانت وراء ما يقارب ثلاثة أرباع الحوادث السيبرانية التي استهدفت البنى التحتية الوطنية الحرجة خلال العام الماضي. أفاد الدكتور ريتشارد هورن، المدير التنفيذي للمركز، بأن الوكالة أدارت أكثر من 200 حادثة من هذا النوع في العام المنتهي في مايو 2026، مع تحديد روسيا والصين وإيران كمصادر تهديد رئيسية.

وفي كلمته أمام معهد الخدمات الملكية المتحدة، شدد الدكتور هورن على أن **الأمن السيبراني** يجب ألا يُنظر إليه كمجرد عملية لإدارة المخاطر بل كمواجهة مستمرة مع خصوم أكفاء. وأشار إلى أن العديد من الحوادث الكبيرة اليوم تبقى ممكنة لأن الضوابط الأمنية الأساسية غير مطبقة، محذراً من أن الثغرات المتسامح معها في وقت السلم ستُستغل أثناء النزاعات.

الذكاء الاصطناعي سيسرّع المشهد التهديدي بحلول 2028

يقدر المركز الوطني للأمن السيبراني أنه بحلول عام 2028، سيستخدم المهاجمون على الأرجح **قدرات سيبرانية معززة بالذكاء الاصطناعي** لاستغلال الثغرات المعروفة في الأنظمة القديمة على نطاق واسع عبر البنى التحتية الوطنية الحرجة. وأكد الدكتور هورن على ضرورة التحرك العاجل، مشيراً إلى أن المؤسسات تخوض بالفعل صراعات الغد في الفضاء السيبراني اليوم.

ودعا كل عضو في مجلس الإدارة وكل مسؤول تنفيذي إلى تعزيز المرونة السيبرانية من خلال ثلاث قدرات أساسية: فهم التعرض للتهديدات، وبناء دفاعات أقوى قائمة على أساسيات الأمن المثبتة، وضمان القدرة على مواصلة العمل والتعافي بسرعة بعد الهجوم. وقد نشر المركز إرشادات لمساعدة المؤسسات على مواجهة الهجمات المدعومة بالذكاء الاصطناعي من خلال تحسين الأمن السيبراني الأساسي الآن.

ما يجب فعله الآن

1. مراجعة مدى تعرض مؤسستكم للجهات المهددة المدعومة من دول، خاصة تلك التي تستهدف قطاعات البنى التحتية الحرجة والخدمات الأساسية
2. تقييم ومعالجة الضوابط الأمنية الأساسية عبر بيئتك التقنية، مع إعطاء الأولوية للثغرات المعروفة في الأنظمة القديمة قبل استغلالها على نطاق واسع
3. إنشاء أو تعزيز فهم مجلس الإدارة للأمن السيبراني كمواجهة مستمرة مع خصوم تتطلب استثماراً متواصلاً وليس مجرد عملية تخفيف مخاطر لمرة واحدة
4. تطوير واختبار قدرات استمرارية العمليات والتعافي لضمان قدرة مؤسستكم على الحفاظ على الوظائف الأساسية أثناء وبعد الحوادث السيبرانية
5. تقييم جاهزيتكم للهجمات المعززة بالذكاء الاصطناعي بحلول 2028، مع التركيز على الاستغلال الآلي للثغرات المعروفة عبر أصولكم التقنية
6. تطبيق القدرات الأساسية الثلاث التي حددها المركز الوطني للأمن السيبراني: فهم التعرض للتهديدات، وبناء دفاعات قائمة على أساسيات مثبتة، وضمان التعافي السريع