هجمات سيبرانية مؤتمتة بالذكاء الاصطناعي تهدد الشركات الأمريكية

28 أكتوبر، 2025

تعيش المؤسسات الأمريكية حالة تأهب غير مسبوقة مع تصاعد المخاوف من موجة جديدة من الهجمات الإلكترونية التي باتت تعتمد بصورة متزايدة على تقنيات الذكاء الاصطناعي، الأمر الذي ينذر بمرحلة مختلفة من الصراع الرقمي تتميز بالسرعة والقدرة على التمويه والتخفي.

ويرى خبراء الأمن السيبراني أن الذكاء الاصطناعي لم يعد مجرد أداة مساعدة في عمليات الاختراق، بل تحول إلى عنصر مركزي يمكّن القراصنة من تنفيذ هجمات متكاملة دون تدخل بشري يُذكر، وهو ما يجعل من الصعب اكتشافها أو احتواؤها في الوقت المناسب. وتشير تقديرات إلى أن هذه الهجمات قد تطال قطاعات حيوية تشمل الطاقة والنقل والرعاية الصحية، مسببة خسائر تشغيلية وأضراراً اقتصادية واسعة.

وتفيد تقارير صادرة عن شركات تقنية كبرى بأن مجرمي الإنترنت وفرق القرصنة التابعة لبعض الدول بدأوا في توظيف النماذج التوليدية

للذكاء الاصطناعي لكتابة شيفرات خبيثة واختبار الثغرات الأمنية بطرق معقدة لا يمكن للأنظمة التقليدية التنبؤ بها. وكشفت شركة «جوجل» أن وحدات متخصصة في أمن المعلومات رصدت محاولات متكررة لاستغلال أدوات الذكاء الاصطناعي العامة في إعداد هجمات موجهة ضد شبكات الشركات الكبرى.

وفي هذا السياق، حذر خبراء من أن المرحلة المقبلة قد تشهد ظهور أنظمة هجومية مؤتمتة بالكامل، قادرة على رصد نقاط الضعف وتنفيذ عمليات اقتحام رقمية متزامنة خلال دقائق، من دون الحاجة إلى تدخل الإنسان. ويؤكد مختصون أن السؤال لم يعد حول ما إذا كانت تلك المرحلة ستأتي، بل متى ستبدأ فعلياً.

وتوضح بيانات لشركة «مايكروسوفت» أن حملات التصيد الإلكتروني التي جرى تصميمها بواسطة الذكاء الاصطناعي سجلت معدلات استجابة فاقت 50 في المئة، مقارنة بنسبة 12 في المئة فقط لرسائل التصيد التقليدية. كما ذكر تقرير صادر عن شركة «Deep Instinct» أن نصف العاملين في منشآت البنية التحتية الحيوية واجهوا خلال العام الماضي محاولات اختراق مدعومة بتقنيات الذكاء الاصطناعي، فيما زادت الهجمات ذات الطابع الحكومي من الصين وروسيا وإيران وكوريا الشمالية بنسبة لافتة.

وفي موازاة ذلك، أسهمت تطبيقات الذكاء الاصطناعي المتقدمة في إنتاج محتوى مرئي مزيف يُستخدم في حملات تضليل واحتيال رقمية، مثل إنشاء مقاطع دعائية يظهر فيها مشاهير يروّجون لاستثمارات وهمية أو مشاهد ملفقة تُستغل لاستدرار العواطف وتحقيق مكاسب غير مشروعة.

لكن في المقابل، تسعى الشركات إلى تسخير الذكاء الاصطناعي ذاته لحماية أنظمتها، حيث تعتمد أكثر من 80 في المئة من المؤسسات الكبرى حلولاً مؤتمتة لتحليل الهجمات والتصدي لها، مما مكّن بعضها من تقليص زمن الاستجابة من أسابيع إلى دقائق معدودة.

وتتوقع الجهات الأمريكية المعنية بالأمن السيبراني أن يشهد المستقبل القريب سباقاً محموماً بين الهجوم والدفاع في الفضاء الرقمي، إذ يتجه الذكاء الاصطناعي إلى أن يكون السلاح الرئيس للطرفين. وتقول جين إيسترلي، المديرة السابقة لوكالة أمن البنية التحتية الأمريكية، إن «الأنظمة الدفاعية ستتعلم من كل هجوم لتصبح أكثر ذكاءً وسرعة في صد الاختراقات»، مضيفة أن «من ينجح في تسخير الذكاء الاصطناعي بفعالية سيحسم معركة الفضاء الإلكتروني القادمة».