اقتصاد, تقنية وسيارات

19 يوليو 2024 20:53 مساء

خبراء لـ «الخليج»: تحديث وراء خلل «كراود سترايك».. ونظرية التسلل مستبعدة

دبي: حمدي سعد

أثار الخلل التقني لانقطاع برمجيات «مايكروسوفت» و«كراود سترايك»، الجمعة، ردود أفعال جهات حكومية وشركات متخصصة في الأمن الالكتروني والسيبراني على مستوى دولة الإمارات والعالم، والتي دعت إلى الحذر من ناحية أو تفسير أسباب هذا الخلل وكونه هجوماً تقنياً من عدمه.

وتسببت الخلل في توقف الخدمات بالمطارات والشركات وأسواق المال وغيرها من المؤسسات والشركات في العديد من دول العالم، وسط حالة من الخوف والترقب لآثاره المتوقعة في استمرارية الخدمات الرقمية واستقرارها.

وفي السياق تباينت آراء شركات متخصصة في الأمن السيبراني والإلكتروني تجاه هذا الخلل والنصائح التي يجب العمل بها خلال الفترة الحالية.

ثغرة برمجية •

قال كيفن ريد، الرئيس التنفيذي لشؤون أمن المعلومات بشركة «أكرونيس»: «من المرجح أن الانقطاع الذي أصاب مؤخراً، يُعزى على الأرجح إلى ثغرة برمجية لم يتم اختبارها بشكل كامل، CrowdStrike» «خدمات «كراود ستريك ضمن تطبيق الكشف عن استجابة النقاط الطرفية الخاص بهم. وقد أدى ذلك إلى تعطيل واسع النطاق طال .المؤسسات، التي تستخدم حلول «كراود ستريك» على مستوى العالم

كيفن ريد

وأضاف «يستلزم تحديث «كراود ستريك» المعيب، تدخلاً يدوياً لإعادة تشغيل الأنظمة في (الوضع الآمن)، وحذف ملف التشغيل الخاطئ. تمثل هذه العملية تعقيداً إضافياً وتجعل الأنظمة عرضة للثغرات الأمنية بشكل مؤقت، وهو ما .«يُشكل بيئة مواتية للهجمات الانتهازية

وتابع: «يسلط هذا الحادث الضوء على أهمية تطبيق منهجية اختبار صارمة، واعتماد نهج تحديث مرحلي لتطبيقات كشف واستجابة النقاط الطرفية. وعادةً ما تتطلب عمليات الاختبار لكل إصدار مدة زمنية تتراوح بين أيام وأسابيع، وفقاً لحجم التحديث أو التغييرات المُدخلة. كما أن قابلية حذف ملفات تعريف التشغيل الخاصة بهم بسهولة تثير .«التساؤلات، حول فاعلية آليات الحماية الذاتية المضمنة ضمن برمجيات «كراود ستريك

وقال ريد: في ضوء هذه الحادثة، نوصي بأن تضمن جميع المؤسسات تطبيق حلول نسخ احتياطي فعالة، كما ندعو إلى .اعتماد مزودي خدمات الأمن لديها بروتوكولات اختبار أكثر صرامة

تحديثات غير مجربة •

فيما قال دارين أنستي، المدير التقني للأمن في شركة «نتسكاوت»: «يبدو أن الانقطاع العالمي في تكنولوجيا .«المعلومات، نجم عن تحديث برمجي خاطئ تم تطبيقه تلقائياً، وليس عن هجوم سيبراني

دارين أنستي

وأضاف «من المؤكد أن هذا الانقطاع سيثير العديد من التساؤلات، حول كيفية تحقيق التوازن بين الحاجة إلى تحديثات أمنية منتظمة للدفاع والامتثال وغيرهما، وبين مخاطر تطبيق تحديثات غير مجربة على الأنظمة وأن غالبية برمجيات المؤسسات تخضع لعمليات اختبار وتوزيع محكم، قبل أن يتم نشرها على نطاق واسع، لكن يبدو أن هذا لم يكن الحال .«في هذه الواقعة

اختبار التحديثات •

مارك جو

أكد مارك جو، مدير الحلول الأمنية في منطقة أوروبا والشرق الأوسط في شركة «جيجامون»:» «يوضح هذا الانقطاع في خدمات «مايكروسوفت»، الحاجة إلى حلول أكثر قوة ومرونة، بحيث يمكن حل هذه المشكلات بسرعة دون التسبب في فوضى واسعة النطاق أو مخاطر أمنية ويجب على كل مزود لتكنولوجيا المعلومات والأمن أن يمتلك نظاماً قوياً لاختبار التحديثات عبر دورة حياة تطوير البرمجيات، لضمان عدم وجود ثغرات أمنية في التحديثات قبل إطلاقها».

تطوير البرمجيات •

أوضح أليكسي لوكاتسكي، المدير الإداري ومستشار أعمال الأمن السيبراني في شركة «بوزيتف تكنولوجيز»: «تذكرنا هذه الحالة بأهمية تطوير البرمجيات الآمن، حيث إنه في هذه الحالة على الأرجح كان السبب هو نقص الفحص أو من جانب المستخدمين، الذين قاموا بتثبيت جميع التحديثات CrowdStrike للتحديثات سواء من جانب شركة التي وصلتهم تلقائياً، ما أدى إلى انقطاع عالمي واسع النطاق. باستثناء تلك الدول التي لا تستخدم منتجات الأمن السيبراني من هذه الشركة الأمريكية».

أليكسي لوكاتسكي

وإضافة إلى ذلك، تظهر الحادثة مدى ترسخ تقنيات المعلومات في حياة الناس وفي العمليات التجارية المختلفة، وكيف يمكن أن تكون العواقب كارثية عند حدوث تأثير عرضي أو غير مصرح به أو ضار على البنية التحتية لتكنولوجيا المعلومات. بعبارة أخرى، تواجه الشركات مهمة تقييم الأحداث غير المحتملة ذات العواقب الكارثية، التي يمكن أن تحدث في أنشطتها بسبب تأثيرها في البنية التحتية لتكنولوجيا المعلومات.

وتابع لوكاتسكي: «هذه ليست الحالة الوحيدة ذات النطاق المماثل. لقد حدثت حالات مشابهة من قبل. على سبيل في عام 2010. وحدثت مشكلة مشابهة مع تحديثات نظام McAfee المثال، تحديث برنامج مكافحة الفيروسات من ما أدى إلى عدم قدرة المستخدمين Microsoft Defender نفسه، وكذلك مع تحديثات حماية Windows التشغيل على أداء وظائفهم العادية».

نظرية تسلل المهاجمين •

وقال لوكاتسكي: «في الوقت الحالي، يبدو أن السبب الجذري، بناءً على نطاق الحادث وطريقة حدوثه، هو عدم اتباع ممارسات التطوير الآمن. ولكن هناك نظرية لا يمكن استبعادها: لم يتم العثور على أي تأكيد لها حتى الآن، ولكن لا يمكننا كخبراء في مجال الأمن السيبراني إنكارها تماماً. وهي تسلل المهاجمين إلى عملية تطوير البرمجيات في ما أدى إلى إدخال وظائف ضارة في التحديث التالي، وأدى في النهاية إلى هذا الفشل الكبير CrowdStrike».

وهي شركة أمريكية أخرى، والتي عانت حادثة مشابهة قبل SolarWinds وأضاف لوكاتسكي «الجميع يتذكر قصة بضع سنوات عندما اخترق المهاجمون عملية التطوير، وأدخلوا وظائف ضارة في تحديث تم طرحه لأجهزة الكمبيوتر

.«SolarWinds لما يقرب من 20 ألف عميل من عملاء

وأوضح لوكاتسكي: «الشيء الوحيد الذي يمكن أن يشير إلى أن هذه الأعمال غير مرجحة كونها أعمالاً خبيثة من قبل مجرمي الإنترنت، الذين تسللوا إلى عملية التطوير هو أن الهدف عادةً في هذه الأنواع من الحوادث هو البقاء غير .«مكتشف لأطول فترة ممكنة، بهدف اختراق شبكات الشركات التي يتم تثبيت البرمجيات الضارة فيها

وبيّن لوكاتسكي: «في هذه الحالة، أدى التحديث تقريباً فوراً إلى تعطيل أجهزة الكمبيوتر، وهو ما لا يعد هدفاً لمعظم التي يكون هدفها عادةً ليس تعطيل الأنظمة، بل الحصول على (APT) مجموعات الهجمات المتقدمة المستمرة البيانات التي يمكن بيعها بعد ذلك، أو ابتزاز الشركة الضحية، أو أداء بعض الوظائف الأخرى المتعلقة بالتجسس .«السيبراني