استهدف هجوم إلكتروني متطور خط أنابيب الغاز الطبيعي الأمريكية كان يجري الإعداد له منذ عدة أشهر، وهو ما يثير مخاوف جديدة بشأن احتمال تعرض البنية التحتية الحيوية في البلاد لخطر قراصنة الحواسيب.<?lmx:ecapseman prefix = o />

وأشارت صحيفة فايننشال تايمز إلى أنه لم تتوفر معلومات عن مصدر أو دافع الهجوم، لكن خبراء الصناعة أشاروا إلى احتمالين: محاولة للسيطرة على خطوط أنابيب الغاز لتعطيل الإمداد، أو محاولة للولوج إلى معلومات عن التدفقات لاستخدامها في تداول السلع في البورصة.

وقد حذرت وزارة الداخلية الأمريكية من هذا الهجوم. وقال الفريق المعني بأنظمة المراقبة الصناعية في الوزارة مؤخرًا: إنه حدد حملة واحدة وراء محاولات الاختراق المتعددة لعدة شركات خطوط أنابيب مختلفة منذ ديسمبر الماضي.

وأصدر الفريق المعني تحذيرات وعقد اجتماعات مع مشغلي خطوط أنابيب النفط والغاز لتلقينهم كيفية رصد علامات الهجوم، وقال: إنه كان على تواصل مستمر مع الهيئات التي تضررت لإعداد خطط لتخفيف حدة التوتر وإزالة التهديد وتدعيم الشبكات ضد الإصابة بالعدوى مجدداً.

ويشار إلى أن التحذير الأصلي جاء من شركات كانت قد لاحظت رسائل إلكترونية مزيفة مرسلة إلى الموظفين، وهذا الهجوم يستخدم ما هو معروف في مصطلح أمن الحواسيب بـ"التصيد"، وهو استخدام فيسبوك أو مصادر أخرى لجمع المعلومات عن موظفي شركة ما ثم محاولة الإيقاع بهم لكشف المعلومات أو النقر على روابط مُفَيْرسة (تتضمن فيروسات) بإرسال رسائل إلكترونية مقنعة بزعم أنها من زملاء العمل.

وقال الفريق: إن التفاصيل الإضافية عن الهجوم التي تم تداولها في التحذير الموجه لمشغلي خطوط الأنابيب، تعتبر حساسة ولا يمكن نشرها عبر القنوات العامة أو غير الآمنة.

وأفادت كاثي لاندري من جمعية إنترستيت للغاز الطبيعي في أميركا مجموعة مشغلي خطوط الأنابيب، بأن "هذه التطفلات للاستطلاع، لكننا لا نعرف هل كانوا يحاولون الولوج إلى أنظمة مراقبة خطوط الأنابيب أم إلى معلومات الشركة؟".

ومن الجدير بالذكر أن حساسية أنظمة حواسيب صناعة الطاقة قد تعرضت لحادثتين كبيرتين في العامين الماضيين. فقد تتبعت حملة القرصنة المعروفة باسم "نايت دراغون" عنوانًا في الصين وجمعت بيانات حساسة تجاريًا عن حقول النفط والغاز ومعلومات أخرى من شركات الطاقة. وأُلقي الضوء على الهجوم في تقرير للكونجرس الأميركي من وكالات استخبارات أميركية كبيرة العام الماضي والتي حذرت من أن "التجسس الصناعي والاقتصادي الأجنبي ضد الولايات المتحدة يمثل تهديداً كبيرًا ومتناميًا لرخاء وأمن البلاد".

والحادثة الثانية هي فيروس ستكسنت عام 2010 الذي سبب تعطلاً كبيرًا لبرنامج إيران النووي.

وأشارت الصحيفة إلى أن تهديد الهجمات على أنظمة تكنولوجيا المعلومات قد دفع السلطات الأميركية لمضاعفة جهودها الأمنية في السنوات الأخيرة ومنها تشكيل الفريق المعني بأمن أنظمة المراقبة الصناعية ضد الهجمات الإلكترونية لحماية البنية التحية الحساسة مثل شبكات الاتصال اللاسلكية وإمدادات الغذاء والماء والمفاعلات النووية وخطوط أنابيب النفط والغاز.

وكان مدير المخابرات المركزية آنذاك ليون بانيتا قد حذر العام الماضي بأن الهجوم الإلكتروني يمكن أن يكون "بيرل هاربر القادم".

كاتب المقالة :
تاريخ النشر : 10/05/2012
من موقع : موقع الشيخ محمد فرج الأصفر
رابط الموقع : www.mohammdfarag.com