

احذروا كلّ الحذر

تحديات أمن الفضاء الإلكتروني في الصناعة النووية



يتزايد عدد الحواسيب التي تُستخدَم سنوياً، مما يوجد فرصاً أكثر لعمليات الهجوم على الفضاء الإلكتروني.

(الصورة من: istockphoto.com)

يتزايد

عدد الحواسيب التي يستخدمها الأشخاص ويتفاعلون معها سنوياً، مما يوجد فرصاً أكثر لعمليات الهجوم على الفضاء الإلكتروني. فعلى سبيل المثال، تحتوي السيارات المعاصرة على ما لا يقل عن ١٢ من قنوات الإدخال/الإخراج الرقمية للسيطرة على المحرك والإرسال والراديو ونظام منع انغلاق الفرامل، والتحكّم في السيارة عن بعد، ومنع السرقة، وتطبيقات الاتصالات السلكية واللاسلكية والمعلوماتية، وما إلى ذلك من التطبيقات. ويُحتمل أن تنطوي كل هذه النظم على نقاط ضعف قد تجعلها عرضةً للقرصنة.

وتتطور التكنولوجيا الحاسوبية والمعلوماتية بسرعة كبيرة، بما يتجاوز أحياناً وعينا بالموارد الممكنة لنقاط الضعف في الفضاء الإلكتروني وللتهجم النهائي عليه. وبالإضافة إلى ذلك، لا تقتصر عمليات الهجوم في الفضاء الإلكتروني على مكان العمل، بل يمكنها أن تستهدف الحياة الشخصية للأفراد.

ومن بين الأهداف الرئيسية للوكالة في تحسين أمن الفضاء الإلكتروني تعزيز ثقافة الأمن النووي وتغيير كيفية تفكير الأشخاص وتغيير كيفية تقييمهم ليس فقط لاعتماد التكنولوجيا، بل وكذلك لاستخدامها.

يقول دودينهوفر: "إذا كان الأخصائيون الفنيون في المجال النووي وأسرهم أكثر وعياً ليس فقط بفضائهم المادي، وإنما أيضاً بفضائهم الرقمي، فسوف يتوخون الحذر أكثر فيما يتعلق بتقاسم المعلومات الإلكترونية واستخدام التكنولوجيا. فالمعلومات التي تبدو بلا ضرر يمكن أن تتمزج بمعلومات أخرى يُعثر عليها

في مكان آخر على الإنترنت ويمكن أن يتبيّن أنها تلحق أضراراً جسيمة. فمحرّك البحث غوغل وما شابهه من محرّكات البحث على الإنترنت هي الأدوات الأولى التي يستخدمها قراصنة الإنترنت في الكثير من الأحيان لوضع خطة هجومية."

يقول بين غوفيرز، المنسّق الوطني المعني بمكافحة الإرهاب وبالأمن في وزارة الأمن والعدل في هولندا إنّ فهم هذا التهديد قد بدأ ينتشر رويداً رويداً في الصناعة النووية. ويضيف قائلاً: "إنّ الصناعة النووية تواجه تحدياً يتمثل في ضرورة توسيع وتعميق آلياتها الدفاعية القائمة في الشبكات الحاسوبية والمعلوماتية التي وُضعت لمكافحة تهديدات الفضاء الإلكتروني. وهذه الصناعة هي -إلى حد ما- في نقطة الانطلاق من وضع تدابير قوية وتنفيذها وتوسيعها لحماية نظم المعلومات والمراقبة في المرافق النووية."

ويقول غوفيرز: "إنّ الوكالة تستطيع أن تؤدي دوراً رائداً في هذا التطور الديناميكي."

أوساط المساعدين

اكتُشف الفيروس الحاسوبي "أكتوبر الأحمر" في تشرين الأول/أكتوبر ٢٠١٢. ويُقدّر أنّ هذا الفيروس قد جمع معلومات حساسة في أكثر من ٦٠ بلداً لمدة وصلت إلى خمس سنوات بينما ظلّ خارج نطاق الكشف عنه. ويمكن إعادة استخدام المعلومات التي جُمعت من الشبكات التي أصيبت بالفيروس في هجمات مقبلة على الفضاء الإلكتروني. وقد أصبح هذا المستوى من التطور في

الناقمون عليكم . وكانت المرافق النووية والإشعاعية تحتاج دائماً إلى حمايتها من هذه التهديدات . والفرق الكبير الآن هو أن هذه

جرائم الفضاء الإلكتروني شائعاً أكثر فأكثر، وهو يمثل تحدياً إضافياً يجب على العاملين في مجال الأمن النووي مواجهته .

استحدثت الوكالة عدداً من البرامج لتوعية الدول حول هذه القضايا، ومساعدتها على التعامل مع هذه المشكلة والتصدي لها .

الجهات المهتمة تستطيع استخدام النظم الحاسوبية في الموقع أو عن بعد للقيام بعملها القدر، هذا ما جاء على لسان خبير الأمن النووي .

ساسا هنريكينز، شعبة الإعلام العام في الوكالة .

وتقدم الوكالة الدعم إلى الدول على جميع المستويات في جهودها الرامية إلى وضع برامج قوية وتم اختبارها في مجال المعلومات والأمن الحاسوبي . وتنظم الوكالة برامج تدريب إقليمية وتعد دورات للفنيين العاملين في مجال الأمن النووي؛ وتنشر مبادئ توجيهية لأمن الفضاء الإلكتروني فيما يتعلق بالمرافق النووية؛ وتعد اجتماعات دولية منتظمة يستطيع الفنيون خلالها تقاسم الخبرات والحصول على أجوبة على أكثر أسئلتهم إلحاحاً من قبل زملائهم الممارسين في هذا المجال والخبراء في الوكالة .

وتعمل الوكالة كذلك على دمج تقييمات أمن المعلومات في الخدمة الاستشارية الدولية المعنية بالحماية المادية التي تقدمها الوكالة .

وتقدم الخدمة الاستشارية الدولية المعنية بالحماية المادية، وهي استعراض شامل متاح لكل البلدان التي لديها مواد ومرافق نووية، المشورة للدول حول الأساليب الأكثر فعالية لحماية موادها النووية والإشعاعية .

وتعمل عدة منظمات على التصدي لتهديد الفضاء الإلكتروني المتزايد . وإقامة الشراكات في هذه المجالات مسألة مهمة . وقد عملت الوكالة بالاشتراك مع المنظمة الدولية للشرطة الجنائية - الإنتربول ومع الوكالة الأوروبية لأمن الشبكات والمعلومات في العمليات الدولية وفي إعداد وثائق إرشادية وأنشطة تدريبية في مجال أمن الفضاء الإلكتروني .

وتعتبر العملية الدولية 2012 TOMIC @ بشأن أمن الفضاء الإلكتروني وأحداث الأمن النووي، بما في ذلك الكيمياء الشرعية النووية، أحد الأمثلة عن مشاركة الوكالة في الأنشطة الدولية الرامية إلى زيادة الوعي بأمن الفضاء الإلكتروني لحماية أصول المواد النووية وغيرها من المواد المشعة . وضمت هذه العملية، برعاية هولندا، 150 مشاركاً من 40 بلداً . وستنظم العملية المقبلة في عام 2014، ويطلق عليها: @TOMIC 2014 .

يقول غوفيرز، منظم أحداث TOMIC @: "نظراً لأنّ للوكالة مكانة مرموقة في العالم النووي، فإنها تستطيع القيام بدور محفّز ورائد في وضع المبادئ التوجيهية أو البروتوكولات، وفي إذكاء الوعي بتدابير أمن الفضاء الإلكتروني ."

التهديدات القديمة ذاتها

يرى دودينهورف أن من الضروري أن تلاحظ الدول الأعضاء أوجه التشابه بين التهديدات الحالية والتهديدات التي واجهتها منذ 50 عاماً خلت .

"فالجهات المهتمة ما زالت هي ذاتها . وقد كانت هناك دائماً عناصر إجرامية تحاول سرقتكم أو ابتزازكم . وكانت هناك دائماً جهات تقف ضدكم وضد عملكم - إنهم الإرهابيون أو الموظفون

تهديدات الفضاء الإلكتروني هي أحد التحديات الدولية . وتقدم الوكالة الدعم إلى الدول الأعضاء في جهودها الرامية إلى بناء تدابير للأمن الحاسوبي واختبارها من أجل حماية المرافق النووية .
(الصورة من : istockphoto.com)