التصدّي لتهديدات الأمن الحاسوبي: تطوُّر برنامج المساعدة التابع للوكالة

بقلم فاسيليكي تافيلي

للتحوُّل إلى مجتمعات متصلة رقميًّا بالشبكات، حيث الأنشطة اليومية مترابطة فيما بينها بمساعدة النُّظم الحاسوبية والذكاء الاصطناعي والتكنولوجيات الرقمية، تأثيرٌ كبير على الأمان والأمن النوويين. ولا يمكن المبالغة في الحديث عن الدور الأساسي الذي تضطلع به التكنولوجيات الرقمية في الحفاظ على وظائف الأمان والأمن في المرافق التي تتعامل مع المواد النووية أو غيرها من المواد المشعّة.

وقالت إيلينا بوغلوفا، مديرة شعبة الأمن النووي بالوكالة: "للنُّظم الحاسوبية والتكنولوجيات الرقمية أهمية بالغة بالنسبة للمرافق والأنشطة المرتبطة بها حيث تُستخدم المواد النووية وغيرها من المواد المشعّة"، مؤكّدةً على حاجة جميع البلدان إلى تنفيذ برنامج للأمن الحاسوبي وتحسين الدفاع في العُمق عن الأمن النووي. وأضافت قائلة: "مع تقدُّم التكنولوجيا ، تتطلب حماية سرية وسلامة ومدى توافر المعلومات والأصول الحساسة التزامَ جانب اليقظة بشكل متواصل لدرء المخاطر والتخفيف منها، وبرنامجاً رصيناً لأمن المعلومات والأمن الحاسوبي".

وتمَّ للمرة الأولى تحديد الحاجة للتصدّي لتهديدات الأمن الحاسوبي، والهجمات السيبرانية الخبيثة، وأيّ مواطِن ضعف محتملة قد تُحدثها التكنولوجيات الرقمية، وأهمية الأمن الحاسوبي لأغراض الأمن النووي في قرار الأمن النووي الذي اعتمده المؤتمر العام للوكالة في دورته الخامسة والخمسين عام 2011. فقد أشار القرار إلى الجهود التي تبذلها الوكالة "لإذكاء الوعي بالتهديد المتنامي المتمثل في هجمات الفضاء الإلكتروني وأثرها المحتمل على الأمن النووي". وشجّع هذا القرار أيضاً الوكالة على إعداد وثائق إرشادية مناسبة، وتوفير دورات تدريبية، واستضافة المزيد من اجتماعات الخبراء الخاصة بالأمن السيبراني في المرافق النووية لمساعدة البلدان على حماية نفسها من الهجمات السيبرانية.

وقالت بوغلوفا: "في متابعة قرار المؤتمر العام في عام 2011، أخذت أنشطة الوكالة تركّز على تحسين قدرات الأمن الحاسوبي على مستوى الدولة ومستوى المرافق"، مضيفةً أن هذه الأنشطة أُدرجت بعد ذلك في خطط الأمن النووي اللاحقة الصادرة عن الوكالة، بما في ذلك تفاصيل التنفيذ الراهن لأنشطة الوكالة في مجال الأمن الحاسوبي الواردة في خطة الأمن النووي للفترة 2022-2025.

> **"النمو الملحوظ المتوقع في استخدام التطبيقات النووية السلمية، وتحديداً برامج القوى النووية، يحتّم علينا اعتبار أمن المعلومات والأمن الحاسوبي جزءاً لا يتجزأ من الأمن النووي ".**
>
> — إيلينا بوغلوفا، مديرة شعبة الأمن النووي في الوكالة

كيف تساعد الوكالة البلدان على وضع أو تحسين أمنها الحاسوبي؟

يُعدُّ إنشاء برنامج مُحكَم ومحدَّث للأمن الحاسوبي عنصراً أساسيًّا لحماية البلدان من الهجمات السيبرانية في البنية الأساسية الحساسة بكل أنواعها. وقد سارعت الوكالة إلى تقديم المساعدة للبلدان في جميع مراحل وَضْع البرامج الوطنية لأمن المعلومات والأمن الحاسوبي، بما في ذلك توفير الوثائق الإرشادية والتدريب.

وتوفر أربعة منشورات إرشادية لسلسلة الأمن النووي الصادرة عن الوكالة وثلاثة منشورات تقنية إضافية إرشاداتٍ في مجال أمن المعلومات والأمن الحاسوبي. وتُستخدم الإرشادات كأساس لوضع أطر وطنية للأمن الحاسوبي، بما في ذلك استراتيجيات وطنية، وأيضاً لأغراض لوائح الأمن الحاسوبي والتدريب في هذا المجال.

ويتمثل أحد المبادئ الأساسية للإرشادات الصادرة عن الوكالة في صَوْن الوظائف الحساسة في المرافق النووية من خلال حماية نُظم المعلومات والنُّظم الحاسوبية للحفاظ على بيئة مأمونة وآمنة للمرافق والمواد على حدّ سواء. ويتحقق ذلك من خلال وَضْع برنامج للأمان الحاسوبي (انظر الصفحة 6)؛ وتحديد وظائف الأمن النووي؛ واستخدام إدارة المخاطر لتحديد العواقب المحتملة للأمن المخترَق؛ وتحديد مستوى الأمن الحاسوبي المطلوب للأصول الرقمية الحساسة؛ وتنفيذ نَهْج متدرّج ومفاهيم الدفاع في العمق في مجال الأمن الحاسوبي. وينبغي تصميم هذه العناصر وتنفيذها على نحو يحُول دون الاختراق، ويساعد على تعزيز قدرة المشغّل على اكتشاف الاقتحامات والتصدّي لها، وكذلك التخفيف من التأثير المحتمل للهجمات السيبرانية.

وتوفر الوكالة، بناء على طلب البلدان، فرصاً تدريبية متنوعة لطائفة من الفئات المستهدفة. ويشمل ذلك السلطات المختصة، والمشغلين، والبائعين، والكيانات الأخرى التي يمكن أن تضطلع بمسؤوليات في مجال تنفيذ الأمن الحاسوبي. ويمكن لهذه الفئات أيضاً أن تستفيد من خبرة الوكالة في إجراء تمارين الأمن الحاسوبي كجزء من برنامج الأمن النووي.

بالإضافة إلى ذلك، هناك أربع دورات تعلُّم إلكتروني في مجال الأمن الحاسوبي، وهي متاحة مجاناً باللغات

العربية والصينية والفرنسية والإسبانية والروسية والإنكليزية من خلال منصة الوكالة للتعلم الإلكتروني الخاصة بشبكة التعليم والتدريب، ويمكن الوصول إليها عن طريق التسجيل أو عن طريق حساب على بوابة نيوكليس NUCLEUS. وستتوافر أيضاً قريباً منصة ابتكارية جديدة في مجال التدريب الافتراضي (انظر الصفحة 12).

وعلى نحو موازٍ، تدعم الوكالة تمارين الأمن الحاسوبي الوطنية أو الإقليمية كجزء من جهودها الرامية لزيادة الوعي بتهديد الهجمات السيبرانية وتأثيرها المحتمل على الأمن النووي. وتتضمن التمارين سيناريوهات مختلفة حيث تُستهدف نُظم المعلومات والنُظم الحاسوبية الحساسة بشكل مباشر أو غير مباشر كجزء من هجوم على كلّ من الحماية المادية والنُظم الإلكترونية.

وتأتي البحوث متممةً لأنشطة الأمن الحاسوبي التي تضطلع بها الوكالة، ولا سيما من خلال الآلية الراسخة للمشاريع البحثية المنسَّقة. فقد أُطلقت مشاريع بحثية منسَّقة في السنوات الأخيرة لتعزيز جهود الأوساط البحثية العالمية في مجال أمن المعلومات والأمن الحاسوبي، وزيادة جاهزية التصدّي للتحديات والمخاطر الناشئة (انظر الصفحة 18).

ماذا يُخفي المستقبل؟

برنامج الأمن الحاسوبي لأغراض الأمن النووي التابع للوكالة آخذ بالتطور المستمر. واعتماد المفاعلات النمطية الصغيرة والمفاعلات المتقدمة على التكنولوجيات المتقدمة والأجهزة الرقمية، والتأثير المتوقع للذكاء الاصطناعي، وظهور بيئات التعلُّم الافتراضي كلها أمور تنطوي على تحدّيات وهي مجالات لتوسيع نطاق الدعم المقدَّم إلى الدول.

وقالت بوغلوفا: "نشهدُ وعياً متنامياً على نحو متزايد بالتداعيات المحتملة أو الفعلية على الأمان والأمن النوويين فيما بين البلدان، والهيئات التنظيمية، والمشغلين، وسائر الجهات المعنيّة". وأضافت قائلةً: "النمو الملحوظ المتوقع في استخدام التطبيقات النووية السلمية، وتحديداً برامج القوى النووية، يحتّم علينا اعتبار أمن المعلومات والأمن الحاسوبي جزءاً لا يتجزأ من الأمن النووي"

الهجوم السيبراني

يُستخدم مصطلح "الهجوم السيبراني" لوصف عمل شرير يُنفَّذ بنيّة سرقة بند مستهدف محدد أو تعديله أو منع الوصول إليه أو إتلافه، من خلال الوصول غير المأذون به إلى نظام حاسوبي حساس أو تنفيذ إجراءات داخل هذا النظام. وتستهدف الهجمات السيبرانية سمة واحدة أو أكثر من سمات الأمن الحاسوبي، أي السرية والسلامة والتوافر، فيما يخصُّ معلومات حساسة موجودة في أصل رقمي حساس أو الأصل الرقمي الحساس نفسه، ويمكن استخدامها لتنفيذ أو يسير ارتكاب عمل شرير ضد أحد المرافق أو الأنشطة أو ارتكاب عمل إجرامي أو عمل آخر متعمد غير مأذون به باستخدام مواد نووية أو مواد مشعة أخرى.

ويمكن تنفيذ الهجوم السيبراني عن طريق الوصول المادي المباشر إلى المعلومات أو أصول المعلومات، أو عن طريق الوصول الإلكتروني، أو باستخدام مزيج من الطريقتين، ويمكن أن ينفِّذ الخصم الهجوم مباشرة أو أن ينفِّذه (أو يساعد الخصم على تنفيذه) طرفٌ داخلي، عن علم منه أو دون علم، تحت تأثير الخصم.

وينبغي معاملة الهجمات السيبرانية فور الكشف عنها على أنَّها حادثات متصلة بالأمن الحاسوبي.

هذا التعريف مأخوذ من المنشور المعنون "الأمن الحاسوبي لأغراض الأمن النووي " العدد G-42 من سلسلة الأمن النووي الصادرة عن الوكالة)