كيف تساعد تمارين الأمن الحاسوبي على زيادة التأهب للتصدي للهجمات السيبرانية في سياق الأمن النووي

بقلم إيما ميدجلي

جرت العادة تاريخيًا على أن تركّز المرافق النووية على ضمان أمن ما لديها من المواد النووية ضد الهجمات الشريرة من خلال إرساء تدابير للحماية المادية مثل الأسلحة النارية والحرّاس والبوابات. ولا تزال هذه التدابير تُستخدم بنجاح لتشييد تحصينات حول المرافق النووية من أجل منع سرقة المواد النووية أو المواد المشعة الأخرى أو تنفيذ أعمال تخريبية أو الوصول غير المأذون به إلى نُظم التحكم. بيد أنَّ العقود الأخيرة شهدت تفاقم تهديدات الهجمات السيبرانية في عالمنا الذي تسوده الوسائط الرقمية بصورة متزايدة. وجميع البلدان معرَّضة لهذه الهجمات، حتى البلدان الأكثر تقدُّماً على صعيد برامج القوى النووية وبرامج البحوث. ولذلك فإنَّ وضع أُطر وطنية للأمن الحاسوبي وللتصدي للتهديدات السيبرانية التي تستهدف المرافق النووية قد صار أمراً ضروريًا. ومن خلال عقد التمارين الواسعة النطاق، تدعم الوكالة البلدان في تحسين الحماية من الهجمات السيبرانية وتساعدها على تعزيز الكشف عن الهجمات السيبرانية على المرافق النووية واستراتيجيات التصدي لها.

وقد وضعت الوكالة تمارين للأمن الحاسوبي في محطات القوى النووية والمرافق الإشعاعية، ويجري تنفيذ هذه التمارين على المستوى الوطني في جميع أنحاء العالم. وتمكّن هذه التمارين البلدان من التمرن والتأهب للتصدي لأسوأ سيناريو قد تواجهه، وهو اختراق الأمن السيبراني في أحد المرافق النووية. ويمكن أن يؤدي التمرُّن على السيناريوهات النظرية إلى تحديد مواطن الضعف في السياسات والإجراءات والعمليات؛ والوقوف على الثغرات التي يجب سدها من خلال تقنيات التخفيف من الآثار و/أو بناء القدرات و/أو التغيير المؤسسي. وبالإضافة إلى مساعدة الدول على تنفيذ التمارين الواسعة النطاق لاختبار الأمن الحاسوبي في المرافق النووية، توفر إرشادات الأمن النووي الصادرة عن الوكالة بشأن الأمن الحاسوبي أيضاً مورداً أساسيًا يمكن أن يكفل للبلدان إرساء تدابير مهمة لأغراض الأمن الحاسوبي بغية الكشف عن الهجمات السيبرانية ومنعها والتصدي لها.

وقال السيد ترينت نيلسون، وهو مسؤول أول في مجال أمن المعلومات والأمن الحاسوبي في شعبة الأمن النووي التابعة للوكالة: "لا بدَّ من وضع السياسات وتحديد الأدوار والمسؤوليات وإرساء إجراءات مفصلة للتصدي لحادثات الأمن الحاسوبي قبل وقوع أي حادثة. وهنا يمكن أن تقدم الوكالة المساعدة في جوانب عديدة: من التمارين والإرشادات إلى تقاسم أفضل الممارسات والإجراءات لضمان التواصل الفعال وتوفير تدابير وافية لحماية الأمن".

وتشمل العوامل التي تجعل المرافق النووية عرضة للهجمات السيبرانية العناصر البشرية والتعقيدات التي تنطوي عليها سلسلة الإمداد، وتقاسم المعلومات الحساسة بين جهات معنية متعددة تستخدم نظماً حاسوبية لدعم الوظائف النووية.

وأضاف السيد ترينت نيلسون: "على سبيل المثال، في حال تنفيذ هجوم على جهة موردة وتزييف طلب عمل، مما يدفع موظفاً تقنيًا لديه حق الوصول المأذون به إلى القيام بعمل خاطئ مستتر. وهذا ليس إلا مثالاً واحداً على الأساليب التي يمكن أن تستخدمها الجهات الفاعلة الخبيثة لتخطي النظم الأمنية".

وعند العمل على التقليل من تأثير أي هجوم سيبراني محتمل، يتمثَّل أحد العناصر المهمة في إرساء الوعي والتواصل الفعال بين الأطراف المعنية، لأنَّ الجهات الفاعلة الخبيثة يمكن أن تستهدف أي جماعة أو فرد ضمن هذه الأطراف. وفي سياق الدفاع عن المرافق النووية، هناك أربع جهات فاعلة رئيسية، ألا وهي: الهيئة الرقابية؛ والجهة المشغلة للمرفق؛ ومنظمات الدعم التقني (أفرقة التصدي لحادثات الأمن الحاسوبي و/أو مراكز عمليات الأمن الحاسوبي)؛ ومنظمات الأطراف الثالثة، مثل الجهات البائعة ومنظمات الدعم. ويُعدُّ إجراء التمارين وسيلة جيدة لاختبار التواصل والإبلاغ والإخطار بين الجهات المعنية، وللتأكد والتحقق من الأمان والأمن في الهياكل التنظيمية.

وفي حين أنَّ السيناريو الأمثل هو أن يستحيل على المهاجمين السيبرانيين اختراق نظم الأمن الحاسوبي في المرافق النووية، فالجهات الفاعلة الخبيثة سريعة التطور والبشر معرضون لارتكاب الأخطاء بطبيعتهم، ومن ثم فمن شبه المستحيل التنبؤ بما ستنطوي عليه الهجمة الكبيرة المقبلة. ولذلك فالكشف عن الهجمات في الوقت المناسب أمر جوهري. وعُقد مؤخراً في سلوفينيا تمرين انطوى على هجوم سيبراني نظري من

> **"لا بدَّ من وضع السياسات وتحديد الأدوار والمسؤوليات وإرساء إجراءات مفصلة للتصدي لحادثات الأمن الحاسوبي قبل وقوع أي حادثة."**
>
> — السيد ترينت نيلسون، مسؤول أول في مجال أمن المعلومات والأمن الحاسوبي في شعبة الأمن النووي التابعة للوكالة

أجل المساعدة على التأكد والتحقق من قدرات الكشف والتصدي للدفاع ضد الهجمات السيبرانية.

وقال السيد سامو تومازيتش، رئيس شعبة الأمن السيبراني في إدارة الأمان النووي في سلوفينيا: "إنَّ لأمن الحاسوبي ليس مشروعاً ولا عملية إجرائية، بل هو رحلة تدوم مدى الحياة وتتطلب بذل الجهد والانتباه والتمرُّن بصورة مستمرة. والتمارين من النوع الذي عُقد في سلوفينيا تمكِّن جميع الكيانات المعنية في القطاع النووي من تقييم مدى إحكام خططها للتصدي للحادثات في حال النجاح في تنفيذ هجوم سيبراني".

وفي حالة وقوع حادثة خطيرة تتعلق بالأمن الحاسوبي ويمكن أن تتسبب في حدث متصل بالأمان النووي أو الأمن النووي، يجب أن يتدخل أحد أفرقة التصدي لحادثات الأمن الحاسوبي، بالإضافة إلى الأطراف المعنية المعتادة في المرفق النووي. وعلى سبيل المثال، يمكن أن تترتب على الحادثات من هذا القبيل مخالفة السياسات أو الإجراءات الأمنية؛ أو تأثيرات تمس بالأصول أو النظم الرقمية الحساسة؛ أو فقدان معلومات حساسة وفقدان السيطرة على وظائف جوهرية للأمان النووي.

وفي هذه الحالة، ففور الوقوف على وقوع حادثة مرتبطة بالأمن الحاسوبي أو على الإخلال بالأمن الحاسوبي، يعمل فريق التصدي لحادثات الأمن الحاسوبي مع الأطراف المعنية بالمرفق من أجل تحري الحادثة، وجمع بيانات التحليل الجنائي، وتحليل ماهية الحادثة ومكان وقوعها، والمساعدة على احتواء حالة التسلُّل والقضاء عليها لمساعدة الجهات المشغلة على إعادة المرفق النووي إلى حالة الاتصال العادية. وفي نهاية عملية التصدي، تُجَمّع أدلة التحليل الجنائي الحاسوبي للمساعدة على إجراء أي تحقيقات جنائية بشأن الهجوم، ولضمان تقاسم المعلومات بفعالية لزيادة تعزيز إجراءات الأمن الحاسوبي في المرفق النووي في المستقبل.

وفي التمرين الذي عُقد في سلوفينيا، كان الكشف عن الهجمات السيبرانية عاملاً أساسيًا في تمكين التصدي للحادثة الأمنية النظرية واختبار إجراءات التصدي للحادثات والتحقق منها. وتدعم هذه التمارين اختبار العلاقة بين الأمان والأمن والتأهب للطوارئ، وتُعزز نظم الأمن النووي من خلال تحديد مواطن الضعف المحتملة وإعداد التغييرات اللازمة لتحسين تأهبها بوجه عام من أجل التصدي للتهديدات التي يمكن أن تمس بالأمن السيبراني. وبالإضافة إلى ذلك، تتيح هذه التمارين فرصة لاختبار قنوات الاتصال الوطنية والدولية المستخدمة في الإخطار والإبلاغ. وعموماً، يُعدُّ إجراء تمارين الأمن الحاسوبي بانتظام جانباً مهمًّا من المحافظة على أمن المرافق النووية.

يتمثَّل أحد العناصر المهمة في التقليل من احتمال تأثير أي هجوم سيبراني في إرساء الوعي والتواصل الفعال بين الأطراف المعنية.

(صورة: أدوبي شوك)