مواجهة التهديدات في عالم مُرقمَن على نحو متزايد

بقلم: فولفغانغ بيكو

في أيار/مايو 2022، أصبح المعهد النمساوي للتكنولوجيا (AIT) أول مركز متعاون مع الوكالة لأمن المعلومات والأمن الحاسوبي لأغراض الأمن النووي. ويقدّم المعهد النمساوي للتكنولوجيا الدعم للدورات التدريبية والتمارين الإقليمية والدولية في مجال الأمن الحاسوبي لفائدة المرافق والأنشطة النووية، وسيُعِدُّ وحدات إيضاحية تقنية بهدف زيادة الوعي بالتهديدات السيبرانية، وسيسهم في إعداد المواد التدريبية للمركز التدريبي والإيضاحي الجديد في مجال الأمن النووي في زايبرسدورف. ولفهم هذا التعاون بشكل أفضل، تحدّثنا إلى هيلموت ليوبولد، رئيس مركز الأمان والأمن الرقميَّين في المعهد النمساوي للتكنولوجيا.

ما المخاطر والتهديدات الناشئة في الأمن الحاسوبي بشكل عام؟

يُصنَع العديد من الأجهزة الرقمية الحديثة اليوم مع الأخذ في الحسبان وجود شبكات أوسع نطاقاً. والعديد منها بحاجة إلى الوصول إلى الإنترنت لكي تعمل. وينطوي كلُّ تطوير للبرمجيات على أخطاء محتملة يمكن أن تتسبَّب بمواطِن ضعف. من شأن الواجهات البينية ضعيفة الحماية والمستخدمين الذين يتصرفون بشكل غير مسؤول زيادة عدد التهديدات الأمنية لتشغيل نُظم تكنولوجيا المعلومات. يستغل المهاجمون مَواطِن الضعف في الأنظمة الرقمية من أجل النفاذ إليها.

وتتطور أساليب وأدوات الهجوم بما يتماشى مع تطوُّر عمليات الابتكارات الرقمية. وباتت برمجيات المخترقين "الهاكرز" متاحة الآن بسهولة على الإنترنت، ما يجعل شنّ الهجمات أسهل – حتى بالنسبة للمهاجمين الذين هُم أقلّ تأهيلاً. ونحن نواجه منظومة متنوعة للهجمات السيبرانية المدفوعة بالجريمة المنظمة، والتجسس الاقتصادي والصناعي، والإرهاب السيبراني.

لذلك، تهدّد اليومَ مجموعة واسعة من الهجمات السيبرانية المستخدمين والشركات والسلطات، ويمكنها مهاجمة البنية الأساسية الرقمية لدول بأكملها بالتزامن مع حملات التضليل المستهدفة، ما يهزُّ أُسسَ مجتمعاتنا.

هل تواجه الصناعة النووية التحديات نفسها؟

تستخدم الشركات والمستهلكون الأفراد في المقام الأول تكنولوجيا المعلومات القائمة على البيانات والموجهة نحو الاتصالات. وفي المقابل، تستخدم المرافق الإنتاجية والبنى الأساسية الحيوية ما يُسمّى بالتكنولوجيا التشغيلية التي ترصد وتتحكم في سلوكيات ونتائج عمليات إنتاجية محدَّدة.

وتقليديًا، كانت التكنولوجيا التشغيلية أقلّ ترابطاً بكثير من تكنولوجيا المعلومات. ومع ذلك، ومع تقدُّم التكنولوجيا، تقارَب المجالان، ويتم وَصْل برمجيات وأجهزة التكنولوجيا التشغيلية على نحو متزايد بشبكات أوسع نطاقاً.

”نحن نعمل بشكل وثيق مع زملائنا في الوكالة الدولية للطاقة الذرية في إعداد وحدات تدريبية، وعروض توضيحية، وتمارين للمركز التدريبي والإيضاحي في مجال الأمن النووي.“

— هيلموت ليوبولد، رئيس مركز الأمان والأمن الرقميَّين، المعهد النمساوي للتكنولوجيا

ويثير هذا التطور إشكاليةً، فالوعي بالأمن السيبراني أقلّ انتشاراً في مجال التكنولوجيا التشغيلية منه في مجال تكنولوجيا المعلومات.

وبالتالي، تصبح هذه التهديدات الجديدة لأمن تكنولوجيا المعلومات ذات أهمية للتكنولوجيا التشغيلية الخاصة بالإنتاج الصناعي والبنية الأساسية الحسّاسة. وتزداد أيضاً أهمية ذلك بالنسبة للصناعة

النووية، التي كانت تقليديًا تتّبع نهجاً متحفظاً وأبقت أنظمة التحكم معزولة.

ما الأنشطة التي يقوم بها المعهد النمساوي للتكنولوجيا لتعزيز الأمن السيبراني في مجال الأمن النووي؟

يقوم برنامج البحوث في المعهد النمساوي للتكنولوجيا بدراسة متمعّنة عن كيفية تأثير سيناريوهات التهديد الناشئة في نُظم التكنولوجيا التشغيلية ويهدف إلى تطوير الدراية والتوصل إلى حلول جديدة لزيادة مرونة البنى الأساسية الحيوية ضدّ الهجمات السيبرانية. وهذا العمل هو الأساس لوضع معايير أمان عالمية جديدة، وإجراءات اعتماد لعناصر النُظم الحاسمة الأهمية وهياكل النُظم الجديدة لتضمين تدابير الأمن السيبراني المتينة في نُظم التكنولوجيا التشغيلية عند البدء بتصميمها.

ويقدّم المعهد النمساوي للتكنولوجيا أيضاً تدريباً وتعليماً شاملَيْن للتأهُّب ضد هجمات الأمن السيبراني. وفي عمليات المحاكاة المعقدة لنظم تكنولوجيا المعلومات 'الافتراضية'، أو ما يُسمّى 'النطاقات السيبرانية'، يتفاعل المستخدمون ومطوّرو النُظم وموظفو التشغيل وممثلو الحكومات مع سيناريوهات واقعية للهجمات السيبرانية. وتُعدُّ عمليات المحاكاة بالغة الأهمية لضمان صمود نُظم تكنولوجيا المعلومات والتكنولوجيا التشغيلية والتي يمكنها صدّ التهديدات السيبرانية بشكّل فعال.

ما مزايا بيئة التعلم الافتراضية التي طوّرها المعهد النمساوي للتكنولوجيا والوكالة الدولية للطاقة الذرية؟

التجربة العملية هي عملية التعلُّم الأكثر فعاليةً. وقام كلّ من المعهد النمساوي للتكنولوجيا والوكالة الدولية للطاقة الذرية بتطوير 'النطاق السيبراني' الذي يوفر إنشاء 'توائم رقمية' للبنى الأساسية الرقمية الحيوية القائمة، والذي يوفر أيضاً التدريب على سيناريوهات التطبيق الواقعية للغاية.

وهنا، يمكن للمستخدمين من الحكومة والصناعة تقييم واختبار فعالية آليات الحماية وعمليات الأعمال.

وتدعم التجارب من 'النطاق السيبراني' إنشاء قدرات دفاعية مستدامة للمؤسسات العامة والخاصة على حدّ سواء.

إلى جانب التدريب الافتراضي، كيف يسهم عمل المعهد النمساوي للتكنولوجيا وخبراته في مجال الأمن الحاسوبي في تعزيز الأمن النووي؟

يمكننا المساعدة على درء هجمات المهاجمين، على سبيل المثال، بتطوير برمجيات ترصد الأجهزة "الطرفية" التيعادةً ما تربط الشبكات الداخلية للمؤسسات بالإنترنت. غالباً ما يستخدم المهاجمون هذه الأجهزة كنقاط دخول للنُظم قبل أن يتسببوا في الضرر.

ونحن نستخدم خبرتنا في كشف الاختلالات لتدريب البرمجيات التحليلية التي ترصد الأجهزة الطرفيّة المستخدَمة عادةً في نوع معيّن من المرافق النووية.

وويمكن لهذه البرمجيات أن تطلق إنذاراً أو أن تتخذ إجراءات مضادّة في حال تصرّف جهاز ما بطريقة غريبة. ونتيجة لذلك، يمكن للمشغلين اكتشاف الهجمات السيبرانية وردعها بالسرعة اللازمة قبل أن تتمكّن من إحداث ضرر كبير.

قبل عام واحد، عُيّن المعهد النمساوي للتكنولوجيا كأول مركز متعاون مع الوكالة لأمن المعلومات والأمن الحاسوبي لأغراض الأمن النووي، وما يزال المركز الوحيد من هذا القبيل اليوم. ماذا يعني هذا بالنسبة لعمل المعهد النمساوي للتكنولوجيا؟

نحن فخورون للغاية بتعييننا كمركز متعاون ونواصل دعم تقديم دورة تدريبية إقليمية بشأن الأمن الحاسوبي لنُظم القياس والتحكم في المجال النووي. وعُقدت الدورة مرّتين في عام 2022، بالاستعانة ببعض نتائج مشروعنا المشترك لتطوير منصة تعليمية افتراضية.

وشاركنا أيضاً في أنشطة تتعلق بالأمن الحاسوبي في تطوير مفاعلات نمطية صغيرة.

وحاليًا، نساعد الوكالة في الاستعدادات الجارية للمؤتمر الدولي بشأن الأمن الحاسوبي في العالم النووي 2023: الأمن من أجل الأمان، حيث سنجري عروضاً توضيحية لمنصة التدريب الافتراضية الخاصة بنا، وسنترأس جلسات نقاشية، وسنقدّم أوراقاً تتعلق ببحوثنا في هذا القطاع، إلى جانب أنشطة أخرى.

ما مشاركة المعهد النمساوي للتكنولوجيا في المركز التدريبي والإيضاحي في مجال الأمن النووي؟

نحن نعمل بشكل وثيق مع زملائنا في الوكالة الدولية للطاقة الذرية في إعداد وحدات تدريبية، وعروض توضيحية، وتمارين للمركز التدريبي والإيضاحي في مجال الأمن النووي. ونحن ندمج وحدات الأمن الحاسوبي في الدورات التدريبية المرتبطة بالحماية المادية للمواد النووية والمواد المشعة الأخرى، وكذلك تلك المرتبطة بالكشف عن المواد النووية والمواد المشعة الأخرى غير الخاضعة للتحكم الرقابي والتصدّي لها. والهدف من هذا الترتيب هو ترسيخ مفهوم أن الأمن الحاسوبي هو جزء لا يتجزأ من الأمن النووي ولا ينفصل عنه.