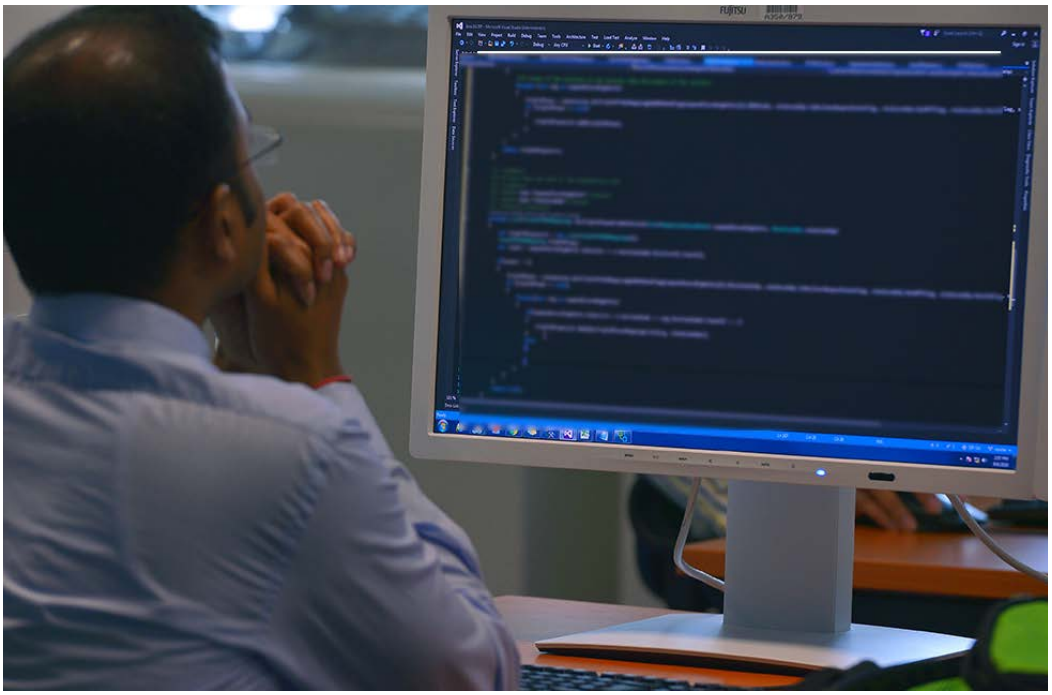
بنادق وحرس وبوابات ومهووسون بالحواسيب: رومانيا تعزز الأمن الحاسوبي في المنشآت النووية

بقلم لورا غيل



(الصورة من: د. كالل/الوكالة الدولية للطاقة الذرية)

باستطاعة هجمة إلكترونية ما أن تمسح جميع المعلومات المخزَّنة على حاسوبك أو حتى أن تحُول دون تشغيله. ويكفينا سوء هذا الأمر. غير أن هجمة إلكترونية على محطة قوى نووية قد تقود إلى التخريب أو سرقة مواد نووية. ويمثل الأمن الحاسوبي، المعنيّ بحماية البيانات الرقمية وحماية النُظم والشبكات من الأفعال الكيدية، جانبًا حاسمًا من جوانب الأمن النووي.

ويقول دونالد دودينهويفر، مسؤول أمن تكنولوجيا المعلومات في الوكالة الدولية للطاقة الذرية: "ما شهدته الحواسيب من تقدُّم واستخدامها في جميع جوانب العمليات النووية أحدث تغيرًا في النموذج الأمني". "يجب أن يُنظر إلى أمن المعلومات والأمن الحاسوبي كجوانب من خطة الأمن النووي الشاملة".

واستحوذت الحماية المادية على الأمن النووي منذ عهد بعيد - وهو ما يُشار إليها في العادة بـ "البنادق والحرس والبوابات" - غير أن المجرمين اليوم تبنوا الحواسيب كوسيلة وأيضًا كهدف للهجمات. وقد تقود هجمة إلكترونية إلى فقدان معلومات الأمن النووي، وتخريب المنشآت النووية، وعند اقترانها بهجمة مادية ربما تقود إلى سرقة مواد نووية أو مواد مشعة أخرى. وتتولى الحواسيب في الوقت الحاضر دورًا أساسيًا في أمان المرافق النووية وأمنها وإدارتها؛ ومن الأهمية الحيوية أن يتم تأمين جميع النظم على نحو ملائم من أي اقتحامات كيدية.

وهنا يقول دودينهويفر: "علينا جميعًا أن نكون متأهبين لحماية أنفسنا من البيئة غير الحميدة للإنترنت والحقبة الرقمية". "نحن جميعًا نستخدم الحواسيب، وعلينا جميعًا أن نزيد وعينا بالتهديدات والمخاطر ووسائل الحماية". ويزداد وعي الرقابيين والمشغلين المعنيين بالمنشآت النووية وهم يسعون لتعزيز برامج الأمن النووي لديهم. ووفقًا لدودينهويفر تُعدُّ رومانيا حالة نموذجية.

وهنا تقول مادالينا ترونيو، المنسقة في وحدة اللوائح والمعايير النووية، اللجنة الوطنية لمراقبة الأنشطة النووية في بوخاريست، رومانيا: "نحن نفهم أهمية الحماية من جميع أنواع التهديدات التي قد تؤثر في أمان وأمن منشآتنا النووية وتشغيلها على نحو موثوق، ومنها التهديدات المحيقة بالأمن الحاسوبي وأمن المعلومات".

وفي عام ٢٠١٢، قام فريق من أخصائي الوكالة الدولية للطاقة الذرية ببعثة الخدمة الاستشارية الدولية المعنية بالحماية المادية في رومانيا. وزوَّد

الفريق السلطات هناك بقائمة من التوصيات للاستمرار في تطوير إطار رقابي ملائم لحماية المنشآت النووية من مختلف التهديدات، ومنها الهجمات الإلكترونية.

وبعد ذلك بفترة وجيزة، بدأ فريق من الرقابيين النوويين لدى اللجنة الوطنية لمراقبة الأنشطة النووية العمل على لائحة دخلت حيز النفاذ في تشرين الثاني/نوفمبر ٢٠١٤. وتركز اللائحة المذكورة على حماية النظم والمعدات والمكونات – ومنها البرامج الحاسوبية الخاصة بالأجهزة وأنظمة التحكم – ذات الأهمية بالنسبة للأمان النووي، والأمن، والضمانات، والتصدي للطوارئ. وإلى جانب اللائحة، أصدرت اللجنة الوطنية لمراقبة الأنشطة النووية وثيقة تبيِّن تهديدات الفضاء الإلكتروني مع الأخذ في الحسبان التهديدات الجديدة وحوادث الأمن الحاسوبي الأخيرة في الصناعة حول العالم.

وهنا تقول ترونيا: "نحن نولي اهتمامًا للسياق العالمي والتغيرات التي طرأت على كل من التهديدات والتدابير المضادة". "ونحن نبذل كلَّ ما في وسعنا لضمان وقاية وحماية ملائمتين في وجه حادثات الأمن النووي وأيضًا استجابة فعالة لمثل هذه الحوادث في حال وقوعها".

وفي تلك السنة ذاتها، وافقت الحكومة الرومانية على استراتيجية وطنية للأمان والأمن النوويين، وتشمل تلك الاستراتيجية أهدافًا تنصبّ على التطوير المستمر للأمن الحاسوبي في القطاع النووي.

الناس: المشكلة والحل

تُظهر الدراسات أن غالبية حادثات الأمن الحاسوبي تتسبَّب بها أخطاء بشرية.

وهنا يقول دودينهويفر: "الناس: تنمية القدرات البشرية من أفضل مجالات الاستثمار". "لسنا بحاجة إلى عالم مليء بخبراء في مجال الأمن الحاسوبي. نحن بحاجة إلى عالم مليء بناس مدركين لمخاطر الأمن الحاسوبي والتدابير الدفاعية الأساسية. نحن بحاجة إلى قوى عاملة وقيادة مستنيرتين".

وبفضل الدورات التدريبية التي عقدتها الوكالة الدولية للطاقة الذرية وشاركت بها رومانيا منذ عام ٢٠١٣، أقام هذا البلد شبكة مستدامة من أصحاب المصلحة. ومن خلال هذه الشبكة، يتقاسم أصحاب المصلحة الآن خبراتهم في مجال الأمن النووي ويعملون معًا لبناء برامج قوية في مجال الحاسوبي وأمن المعلومات.

(الصورة من: اللجنة الوطنية لمراقبة الأنشطة النووية)

ومن خلال البرامج التدريبية الوطنية، والتعلم عبر الإنترنت، واجتماعات الخبراء وبرامج تدريب المدرِّبين، تعمل الوكالة الدولية للطاقة الذرية مع قيادات وأصحاب المصلحة على المستوى الوطني في الصناعة النووية لفهم التهديدات الإلكترونية بشكل أفضل وتطوير الممارسات الجيدة الكفيلة بتعزيز الأمن الحاسوبي. ويقول دودينهويفر إن الدورات التدريبية الوطنية تُعدُّ من أقيم الأنشطة التي تعقدها الوكالة الدولية للطاقة الذرية في مجال الأمن الحاسوبي.

وهنا يقول دودينهويفر: "في الحماية المادية، يمكن أن ترى ما الذي تحميه وأن تتصور سيناريوهات الهجمات المحتملة". "لكن في الفضاء الإلكتروني لدى المجرمين عدد أكبر بكثير من الأهداف، منها أهداف ليست في المرفق نفسه، ويمكن أن تهاجَم حتى في منزلك. يتعيَّن علينا أن نفكر بالطريقة التي يفكر بها المجرمون لنفهم بشكل أفضل كيفية الحماية من الهجمات الإلكترونية أينما كنا".