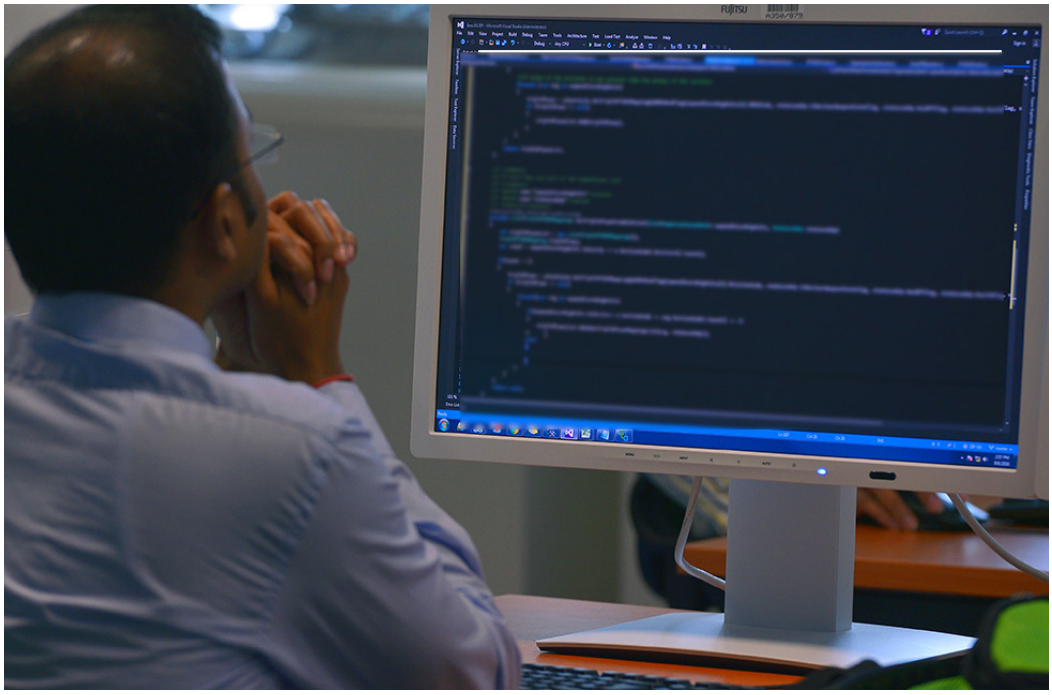
Les installations nucléaires roumaines à la pointe de la cybersécurité

Par Laura Gil



[photo : D. Calma (AIEA)]

Un cybercriminel pourrait dérober toutes les données stockées sur votre ordinateur ou l'empêcher de fonctionner. C'est fâcheux, mais il y a encore plus grave. Une cyberattaque perpétrée contre une centrale nucléaire pourrait entraîner le sabotage ou le vol de matières nucléaires. C'est pourquoi la cybersécurité, c'est à dire la protection des données numériques et la défense des systèmes et réseaux contre les actes malveillants, est devenue une composante essentielle de la sécurité nucléaire.

« Les progrès de l'informatique et l'omniprésence des ordinateurs dans les opérations nucléaires ont modifié le paradigme de la sécurité », déclare Donald Dudenhoeffer, responsable de la sécurité informatique à l'AIEA. « La sécurité de l'information et la cybersécurité doivent être considérées comme des éléments à part entière du plan général de sécurité nucléaire. »

La sécurité nucléaire a longtemps été axée sur la seule protection physique, mais il faut désormais composer avec les ordinateurs, qui font aussi bien partie des cibles que de l'arsenal des criminels. Une cyberattaque pourrait entraîner la perte d'informations ayant trait à la sécurité nucléaire, le sabotage d'installations nucléaires et, combinée avec une attaque physique, le vol de matières nucléaires ou d'autres matières radioactives. Les ordinateurs jouent désormais un rôle essentiel dans la sûreté, la sécurité et la gestion des installations nucléaires. Il est crucial que tous les systèmes soient correctement protégés contre les intrusions.

« Nous devons tous être préparés à nous défendre contre l'environnement potentiellement hostile que constituent l'internet et l'ère numérique », poursuit M. Dudenhoeffer. « Nous utilisons tous des ordinateurs et devons donc être mieux informés des menaces, des risques et des moyens de protection. » Les responsables de la réglementation et les exploitants d'installations nucléaires sont de plus en plus conscients de l'importance de la cybersécurité et cherchent à améliorer leurs programmes de sécurité nucléaire. Selon M. Dudenhoeffer, la Roumanie est un exemple à suivre.

« Nous mesurons l'importance de la protection contre toutes les formes de menaces qui pourraient entraver l'exploitation sûre, sécurisée et fiable de nos installations nucléaires, notamment les menaces dirigées contre la sécurité de l'information et la cybersécurité », explique Madalina Tronea, coordonnatrice au sein de l'Unité des réglementations et normes nucléaires de la Commission nationale pour le contrôle des activités nucléaires (CNCAN), à Bucarest (Roumanie).

En 2012, un groupe de spécialistes de l'AIEA a effectué une mission du Service consultatif international sur la protection physique en Roumanie. Il a présenté aux autorités du pays une liste de recommandations, les invitant à poursuivre la mise en place d'un cadre réglementaire adéquat pour la protection des installations nucléaires contre diverses menaces, y compris les cyberattaques.

Peu après, une équipe de responsables de la réglementation nucléaire de la CNCAN s'est mise à élaborer une réglementation, qui est entrée en vigueur en novembre 2014. Celle-ci porte sur la protection des systèmes, équipements et composants, y compris le logiciel des systèmes de contrôle-commande, qui sont importants pour la sûreté et la sécurité nucléaires, les garanties et les interventions d'urgence. Outre cette réglementation, la CNCAN a publié un document dans lequel elle présente les cybermenaces dans les grandes lignes, en tenant compte des nouveaux types d'attaques et des récentes atteintes à la cybersécurité survenues dans l'industrie ailleurs dans le monde.

« Nous sommes attentifs au contexte mondial et aux évolutions que connaissent aussi bien les menaces que les contre-mesures », poursuit Mme Tronea. « À partir de là, nous faisons de notre mieux pour garantir une prévention et une protection adéquates contre les atteintes à la cybersécurité, ainsi que des interventions efficaces pour y faire face, s'il s'en produisait. »

La même année, le gouvernement roumain a approuvé une stratégie nationale de sûreté et de sécurité nucléaires qui comprend des objectifs d'amélioration continue de la cybersécurité dans le secteur nucléaire.

Quand les personnes sont le problème et la solution

Des études montrent que la majorité des atteintes à la cybersécurité sont dues à des erreurs humaines.

« La mise en valeur des capacités humaines est l'un des meilleurs investissements qui soient », estime M. Dudenhoeffer. « Nous n'avons pas besoin d'un monde rempli d'experts de la cybersécurité. Nous avons besoin que le public, et à plus forte raison les employés et les responsables d'installations nucléaires, soient conscients des risques de cyberattaques et connaissent les mesures élémentaires qui permettent de s'en défendre. »

Grâce aux cours de l'AIEA auxquels la Roumanie participe depuis 2013, le pays a créé un solide réseau de parties prenantes qui partagent des données d'expérience ayant trait à la sécurité nucléaire et unissent leurs efforts pour mettre au point des programmes viables de sécurité de l'information et de cybersécurité.

Dans le cadre de cours nationaux, de modules d'apprentissage en ligne, de réunions d'experts et de programmes de formation de formateurs, l'AIEA coopère avec les dirigeants nationaux et les acteurs de l'industrie nucléaire pour mieux comprendre les cybermenaces et adopter de bonnes pratiques permettant d'améliorer la cybersécurité. Selon M. Dudenhoeffer, les cours nationaux font partie des activités les plus utiles qu'organise l'AIEA dans le domaine de la cybersécurité.

« Lorsque vous êtes en charge de la protection physique d'installations nucléaires, vous pouvez voir ce que vous protégez et visualiser les scénarios d'attaque probables », fait observer M. Dudenhoeffer. « Dans le cyberespace, en revanche, les cibles potentielles sont beaucoup plus nombreuses et ne se trouvent pas nécessairement sur le site. Vous pourriez même être victime d'une attaque chez vous. Nous devons apprendre à raisonner comme les criminels pour mieux comprendre comment nous protéger contre les cyberattaques, où que nous soyons. »

(Photo : CNCAN)