Sécurité nucléaire : des exercices de sécurité informatique pour se préparer à répondre aux cyberattaques

Par Emma Midgley

Historiquement, la protection des matières nucléaires contre les attaques malveillantes était assurée dans les installations nucléaires par des moyens de protection physique tels que des armes, des gardes et des barrières. Aujourd'hui encore, ces moyens sont utilisés pour ériger des forteresses autour des installations nucléaires, empêchant le vol de matières nucléaires ou d'autres matières radioactives, le sabotage ou l'accès non autorisé aux systèmes de contrôle. Cependant, ces dernières décennies, dans un monde de plus en plus informatisé, la menace de cyberattaques a grandi. Tous les pays, même ceux qui ont les programmes électronucléaires et de recherche les plus avancés, peuvent être vulnérables à une attaque. Il est devenu nécessaire d'élaborer des cadres nationaux de sécurité informatique face aux cybermenaces visant les installations nucléaires. Par des exercices à grande échelle, l'AIEA aide les pays à améliorer leur protection contre les cyberattaques et leurs stratégies de détection et d'intervention face aux cyberattaques contre les installations nucléaires.

L'AIEA a conçu des exercices de sécurité informatique pour les centrales nucléaires et les installations radiologiques, qui ont été effectués au niveau national dans le monde entier. Ces exercices permettent aux pays de s'entraîner et de se préparer à faire face au pire scénario : une atteinte à la cybersécurité dans une installation nucléaire. Les scénarios théoriques peuvent mettre en évidence les faiblesses des politiques, procédures et processus, ainsi que les lacunes à combler par des techniques d'atténuation, le renforcement des capacités ou des changements organisationnels. En plus d'aider les États à exécuter des exercices à grande échelle pour tester la sécurité informatique de leurs installations nucléaires, les orientations sur la sécurité nucléaire de l'AIEA concernant la sécurité informatique constituent également une ressource essentielle permettant aux pays de mettre en place d'importantes mesures de sécurité informatique pour détecter et prévenir les cyberattaques, et y faire face.

« Il est essentiel d'élaborer des politiques, de définir les rôles et les responsabilités et d'établir des procédures détaillées pour faire face aux incidents de sécurité informatique avant qu'ils ne se produisent », souligne Trent Nelson, responsable de la sécurité de l'information et de la sécurité informatique au sein de la Division de la sécurité nucléaire de l'AIEA. « C'est là que l'AIEA peut apporter son aide à bien des égards : exercices, conseils, mise en commun des meilleures pratiques et procédures pour garantir une communication efficace et une protection solide de la sécurité. »

Les facteurs qui rendent les installations nucléaires vulnérables aux cyberattaques sont notamment le personnel, la complexité de la chaîne d'approvisionnement et le partage des informations sensibles entre les nombreuses parties prenantes qui utilisent les systèmes informatiques appuyant les fonctions nucléaires.

« Prenons l'exemple d'une attaque où la compromission d'un fournisseur et la falsification d'une commande de travail amèneraient un technicien de confiance disposant d'un accès autorisé à effectuer une action subtilement incorrecte », poursuit Trent Nelson. « Ce n'est qu'un des moyens que des acteurs malveillants pourraient utiliser pour contourner les systèmes de sécurité. »

Un élément important pour réduire les incidences potentielles de toute cyberattaque est la sensibilisation des parties prenantes et la communication efficace entre elles, car n'importe quel groupe ou membre d'un groupe peut être la cible d'acteurs malveillants. Quatre acteurs principaux interviennent dans la défense des installations nucléaires : l'organisme de réglementation, l'exploitant de l'installation, les organismes d'appui technique [équipes d'intervention en cas d'incident de sécurité informatique (CSIRT), centres opérationnels de sécurité informatique] et les organisations tierces, telles que les fournisseurs et les organismes d'appui. Les exercices sont un bon moyen de tester les communications, la transmission de rapports et les notifications entre les parties prenantes et de vérifier et valider la sûreté et la sécurité des structures organisationnelles.

Un élément important pour réduire les incidences potentielles de toute cyberattaque est la sensibilisation des parties prenantes et la communication efficace entre elles

L'idéal serait que les systèmes de sécurité informatique des installations nucléaires soient impénétrables mais la nature évolutive des acteurs malveillants et la faillibilité humaine font qu'il est pratiquement impossible de prédire comment se passera la prochaine attaque de grande envergure. Il est donc essentiel de détecter rapidement les attaques. Lors d'un récent exercice en Slovénie, une simulation de cyberattaque a permis de vérifier et de valider les capacités de détection et défense contre les cyberattaques.

« La sécurité informatique n'est pas un projet ni un processus mais un cheminement sans fin qui nécessite des efforts, une attention et un entraînement constants », explique Samo Tomažič, chef de la division de la cybersécurité de l'Administration slovène de sûreté nucléaire. « Des exercices tels que celui effectué en Slovénie permettent à toutes les entités concernées du secteur nucléaire d'évaluer la solidité de leurs plans d'intervention en cas de cyberattaque réussie. »

En cas d'incident grave de sécurité informatique, qui pourrait donner lieu à un événement de sûreté ou de sécurité nucléaire, une CSIRT devrait intervenir en plus des parties prenantes habituelles à une installation nucléaire. Un tel incident pourrait entraîner par exemple la violation des politiques ou des procédures de sécurité, des répercussions sur des actifs ou des systèmes numériques sensibles, ou encore la perte d'informations sensibles et du contrôle de fonctions essentielles à la sûreté nucléaire.

Dans ce cas, dès qu'un incident de sécurité informatique ou une compromission de celle-ci sont décelés, la CSIRT travaille avec les parties prenantes de l'installation pour enquêter sur l'incident, recueillir des données criminalistiques, analyser les faits et les lieux, et aider à contenir et à annihiler l'intrusion pour que les exploitants puissent remettre l'installation nucléaire en service. À la fin de l'intervention, des preuves informatiques judiciaires sont réunies pour aider toute enquête criminelle sur l'attaque et assurer un partage efficace des informations afin de renforcer les mesures de sécurité informatique dans l'installation nucléaire pour l'avenir.

Lors de l'exercice en Slovénie, la détection des cyberattaques était essentielle pour répondre à la simulation d'incident et pour tester et valider les procédures d'intervention. Ces exercices permettent de tester la relation entre la sûreté, la sécurité et la préparation des interventions d'urgence, et de renforcer les régimes de sécurité nucléaire en déterminant leurs faiblesses potentielles et en procédant aux changements nécessaires pour mieux les préparer aux éventuelles menaces de cybersécurité. Ils permettent également de tester les voies nationales et internationales de notification et de transmission de rapports. D'une manière générale, la conduite régulière d'exercices de sécurité informatique est un aspect important du maintien de la sécurité des installations nucléaires.