Améliorer les techniques de détection des anomalies de sécurité informatique au moyen des projets de recherche coordonnée

Par Rodney Busquim e Silva et Andrea Rahandini

La détection d'anomalies dans l'exploitation des systèmes informatiques qui contrôlent les fonctions critiques de sûreté et de sécurité nécessite de vastes compétences, et les mesures nécessaires doivent être testées, analysées et modifiées afin d'en garantir la robustesse.

« La détection des anomalies joue un rôle important dans l'évaluation rapide des menaces qui pourraient viser les systèmes informatiques des installations nucléaires et radiologiques », fait observer Scott Purvis, chef de la Section de la gestion de l'information à la Division de la sécurité nucléaire de l'AIEA. « D'ordinaire, les techniques de détection des anomalies reposent sur des applications d'intelligence artificielle telles que l'apprentissage automatique, les méthodes fondées sur les statistiques, les connaissances ou d'autres technologies », explique-t-il. Ces technologies sont utilisées pour déceler les écarts par rapport aux communications réseau ou mesures de processus prévues, qui peuvent être le premier signe d'un contournement des défenses d'un système informatique par un intrus, et peuvent ainsi détecter les cyberattaques en temps réel.

Elles sont importantes parce qu'un malfaiteur très habile peut introduire des logiciels malveillants qui compromettent les fonctions de sûreté ou de sécurité d'un système informatique en falsifiant les données provenant des capteurs et les indicateurs envoyés à un exploitant. L'exploitant peut donc ignorer qu'une activité malveillante est en train de se produire et réagira d'abord en fonction de ce qui est affiché dans la salle de commande, ce qui peut l'induire en erreur et lui faire prendre des mesures inappropriées. Seule la détection automatique des moindres anomalies dues à une telle cyberattaque permettra à un exploitant d'être correctement informé.

Pour agir dans ce domaine de travail important et relever d'autres défis de sécurité informatique, l'AIEA a lancé en 2016 un projet de recherche coordonnée (PRC) spécifique.

La recherche-développement dans le cadre des PRC constitue un élément indispensable des activités de l'AIEA dans le domaine de la sécurité informatique pour la sécurité nucléaire. Ces projets génèrent un ensemble de résultats de recherche et de conclusions exploitables qui complètent les efforts constants de l'AIEA pour renforcer les capacités des pays en matière de prévention et de détection des incidents de sécurité informatique susceptibles de compromettre directement ou indirectement la sûreté et la sécurité des installations nucléaires et radiologiques, d'intervention face à tels incidents et de relèvement après leur survenance.

« Les adversaires sont de plus en plus ingénieux et leurs cybercapacités rendent de plus en plus difficile la mise au point d'outils de détection d'anomalies », indique Scott Purvis. « La mise au point de techniques de détection des anomalies nécessite l'accès à un réseau réaliste et physiquement cohérent et aux données sur les processus de l'installation afin d'entraîner et de tester les modèles de détection ».

Scénario de cyberattaque pour renforcer les capacités

Le PRC de 2016, intitulé « Amélioration de l'analyse des incidents de sécurité informatique dans les installations nucléaires », a produit des résultats notables, permettant notamment des travaux de recherche plus poussés sur des outils et des techniques ciblés, qui n'avaient pu être effectués jusqu'alors sans risquer d'exposer des informations sensibles d'installations nucléaires et radiologiques.

Composée de chercheurs de 13 pays et de 17 organisations, l'équipe du PRC a créé une installation fictive appelée « centrale nucléaire d'Asherah », et un simulateur (ANS) de l'installation a été mis au point par l'Université de São Paulo. Ensemble, les chercheurs ont élaboré des scénarios réalistes de cyberattaques d'une installation nucléaire. Ces scénarios de cyberattaque ont permis de tester et d'évaluer l'efficacité des mesures de sécurité informatique ainsi que les conséquences potentielles de la compromission d'un actif numérique pour l'exploitation de l'installation. En outre, l'équipe a travaillé à la collecte et à l'analyse de données et à la mise au point et à l'essai de techniques de détection des cyberattaques.

« Nous avons mis au point et utilisé l'ANS pour générer un ensemble de données afin d'entraîner nos modèles d'apprentissage automatique et d'en évaluer l'efficience. Le PRC de l'AIEA a réuni des partenaires internationaux pour effectuer des recherches et produire de nouvelles connaissances dans ce domaine, indique Ricardo Marques, professeur à l'École polytechnique de l'Université de São Paulo (Brésil). La coopération entre les participants au PRC a été essentielle pour la validation du travail accompli ».

En outre, les résultats du PRC ont été mis à profit pour la formation théorique et pratique continue de nombreux étudiants de troisième cycle et de chercheurs dans diverses disciplines, renforçant ainsi la recherche et les efforts déployés pour améliorer constamment la sécurité informatique dans les installations nucléaires et radiologiques.

L'Université de São Paulo a mis au point un simulateur à partir d'une installation fictive appelée « centrale nucléaire d'Asherah ».
(Photo : AIEA)

« J'ai effectué une partie des recherches de mon doctorat à l'aide de l'ANS et son interface homme-machine mise au point dans le cadre du PRC de l'AIEA, qui permet à l'utilisateur d'observer le simulateur et de communiquer avec lui », explique Si Wen, doctorante de l'Université de Tsinghua (Chine). « J'ai effectué des recherches sur les techniques de détection des anomalies et l'ANS était essentiel à la production des données nécessaires à l'entraînement et à l'évaluation d'un algorithme de détection mis au point pour les centrales nucléaires. Sans la collaboration entre tous les instituts participants et sans les outils mis au point par l'équipe du PRC, je n'aurais pas pu effectuer mes recherches doctorales sur la cybersécurité des systèmes informatiques des centrales nucléaires », ajoute-t-elle.

Les résultats du PRC — l'ANS, les outils et les orientations — sont accessibles aux instituts de recherche intéressés du monde entier. Ils peuvent être obtenus en soumettant à l'AIEA, par l'intermédiaire de l'autorité nationale compétente, un formulaire de demande disponible sur le Portail d'information sur la sécurité nucléaire de l'AIEA (NUSEC).

Plus récemment, en 2023, l'AIEA a lancé un nouveau PRC intitulé « Amélioration de la sécurité informatique des systèmes de détection des rayonnements » pour étudier les méthodologies et les techniques permettant d'améliorer la sécurité informatique du matériel de détection des rayonnements. Les projets de recherche prévus dans le cadre de ce nouveau PRC, auquel participent 12 organisations (laboratoires nationaux, universités et instituts de recherche nationaux) de 11 pays, porteront sur l'utilisation des technologies numériques émergentes, telles que l'informatique en nuage, et permettront de continuer à étudier et à mettre au point des techniques innovantes de détection des anomalies.