

ON N'EST JAMAIS TROP PRUDENT

Les défis de la cybersécurité dans l'industrie nucléaire



Chaque année, le nombre d'ordinateurs utilisés augmente et les possibilités de cyberattaques avec lui. (Photo : istockphoto.com)

Le nombre d'ordinateurs utilisés pour interagir augmente chaque année, et les possibilités de cyberattaques avec lui. Par exemple, les automobiles d'aujourd'hui contiennent pas moins de 12 canaux d'entrée/de sortie numérique pour contrôler le moteur, la transmission, la radio, le freinage anti-blocage, le télédéverrouillage, l'antivol, la télématique, etc. Ces derniers peuvent tous avoir des vulnérabilités susceptibles d'être exploitées par des « pirates ».

Les technologies informatiques évoluent très rapidement, à un rythme parfois si soutenu que nous n'avons pas conscience des sources possibles de cybervulnérabilité et, à terme, d'attaque. En outre, les cyberattaques ne se limitent pas au milieu professionnel, elles peuvent aussi cibler la sphère privée.

Les principaux objectifs que l'AIEA se fixe pour améliorer la cybersécurité sont de renforcer la culture de sécurité nucléaire, de susciter un mode de pensée différent et de faire évoluer la manière dont les individus considèrent non seulement l'adoption mais aussi l'utilisation de la technologie.

« Si les spécialistes du nucléaire et leurs familles sont davantage conscients non seulement de l'espace physique qu'ils occupent mais aussi de leur espace numérique, ils seront plus prudents dans le partage des informations en ligne et l'utilisation des technologies. Des informations paraissant anodines, combinées à d'autres informations trouvées sur le Web, peuvent s'avérer dévastatrices. Les

moteurs de recherche comme Google sont souvent les premiers outils que les pirates utilisent pour mettre au point un plan d'attaque », déclare M. Dudenhoeffer.

Ben Govers, coordonnateur national de la lutte contre le terrorisme et de la sécurité au Ministère de la sécurité et de la justice des Pays-Bas, explique que l'industrie nucléaire prend peu à peu conscience de la menace. « L'industrie nucléaire est confrontée à un double défi, qui est d'élargir et d'approfondir ses défenses existantes sur les réseaux informatiques afin de se protéger des cyberattaques. Elle commence — plus ou moins — à mettre au point, exécuter et développer des mesures solides de protection des informations et des systèmes de contrôle des installations nucléaires ».

« L'AIEA peut jouer un rôle de premier plan dans cette évolution dynamique », indique M. Govers.

Une communauté d'entraide

Le virus informatique « Red October » a été découvert en octobre 2012. On estime qu'il a recueilli des informations sensibles dans plus de 60 pays pendant au maximum cinq ans sans être détecté. Les informations collectées sur les réseaux infectés pourraient être réutilisées dans de futures cyberattaques. Ce niveau de complexité de cybercriminalité devient chose courante et constitue un autre défi auquel le personnel chargé de la sécurité nucléaire doit faire face.

L'AIEA aide les États à tous les niveaux à établir des programmes de sécurité informatiques solides et éprouvés. Elle organise des programmes régionaux de formation ; met au point des cours destinés aux spécialistes de la sécurité nucléaire ; publie des principes directeurs de cybersécurité pour les installations nucléaires ; et organise régulièrement des réunions internationales où les spécialistes peuvent échanger leurs connaissances et obtenir des réponses à leurs questions les plus pressantes auprès de collègues praticiens et d'experts de l'AIEA.

L'AIEA inclut en outre des évaluations de la sécurité informatique dans son Service consultatif international sur la protection physique (IPPAS).

Par le biais de ce service d'examen approfondi, à la disposition de tous les pays ayant des matières et installations nucléaires, elle conseille ces derniers pour qu'ils trouvent des moyens plus efficaces de protéger leurs matières nucléaires et radiologiques.

De nombreuses organisations s'emploient à répondre à la menace croissante de cyberattaques. Les partenariats dans ces domaines sont importants. L'AIEA a travaillé en collaboration avec l'Organisation internationale de police criminelle (Interpol) et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) dans le cadre d'exercices internationaux et de la mise au point de documents d'orientation sur la cybersécurité et d'activités de formation.

L'exercice international @TOMIC 2012, couvrant la cybersécurité, les événements de sécurité nucléaire et la criminalistique nucléaire, est un exemple de la participation de l'AIEA aux activités internationales de sensibilisation à la cybersécurité dont l'objectif est de protéger les matières nucléaires et autres matières radioactives. L'exercice, parrainé par les Pays-Bas, a rassemblé 150 participants de 40 pays. Le prochain exercice, @TOMIC 2014, aura lieu en 2014.

« Étant donné que l'AIEA a une position respectée dans le monde nucléaire, elle peut jouer un rôle moteur et stimulant dans l'application des principes directeurs ou protocoles et la sensibilisation aux mesures de cybersécurité », déclare l'organisateur des exercices @TOMIC, M. Govers.

Des menaces qui n'ont pas changé

Selon M. Dudenhoeffer, il est important que les États Membres voient les ressemblances entre les menaces d'aujourd'hui et celles d'il y a 50 ans.

« Les auteurs des menaces restent les mêmes. Il y a toujours eu des individus criminels essayant de vous voler ou de vous faire chanter. Il y a toujours eu des individus agissant contre vos intérêts et votre travail – terroristes

ou employés mécontents. Les installations nucléaires et radiologiques ont toujours dû être protégées contre ces menaces. La grande différence aujourd'hui est que leurs

L'AIEA a entrepris plusieurs programmes pour sensibiliser les États à ces questions, les aider à gérer le problème et contre-attaquer.

auteurs peuvent utiliser des systèmes informatiques sur place ou à distance pour se livrer à leur basse besogne », déclare l'expert en sécurité nucléaire.

Sasha Henriques, Division de l'information de l'AIEA.



Les menaces de cyberattaques sont un défi international. L'AIEA aide les États Membres à établir et à tester des mesures de sécurité informatique pour protéger les installations nucléaires.

(Photo : istockphoto.com)