Les risques de cyberattaques se multiplient contre les centrales nucléaires

Chatham House vient de publier un rapport de 53 pages, résultat d'une enquête de 18 mois dans 7 pays et du témoignage d'une trentaine de responsables nucléaires.

La centre EDF de Graveline.
© EDF

Le nucléaire, industrie la plus sûre du monde ? De moins en moins. Selon le rapport *Cyber Security at Civil Nuclear Facilities : Understanding the Risks* (en français : *Cybersécurité dans les centrales nucléaires : comprendre les risques*) publié lundi dernier par le think tank britannique Chatham House, « *le risque d'une cyberattaque sérieuse sur les installations nucléaires s'accroît d'autant que les centrales s'appuient sur des systèmes d'information qui font de plus en plus appel à des logiciels commerciaux sur étagère* ».

Ce rapport de 53 pages recueille les témoignages anonymisés d'une trentaine de responsables nucléaires (industriels, hauts fonctionnaires, spécialistes de cybersécurité) et d'experts qui ont participé à des tables rondes. Pour sa part l'enquête a duré 18 mois et s'est déroulée sur sept pays exploitant des réacteurs nucléaires (Allemagne, Canada, États-Unis, France, Japon, Royaume-Uni, Ukraine).

Parmi les enseignements du rapport de Chatham House, il y a la croyance partagée par les opérateurs nucléaires que toutes leurs centrales sont déconnectées de l'Internet public. Or c'est un mythe. « *Un certain nombre d'entre elles sont bel et bien connectées à Internet, certes via des réseaux privés virtuels (VPN : Private Virtual Networks). Mais les opérateurs nucléaires n'en sont même pas toujours conscients*, rapportent les auteurs Caroline Baylon, Roger Brunt et David Livingstone. *Pour preuve, les moteurs de recherche sont capables d'identifier les composants des infrastructures critiques au travers de ces connexions VPN.* » En outre, même si les usines sont déconnectées d'Internet, cette protection n'est qu'apparente car il est facile de la casser avec un disque dur portable ou un clé USB. Au final, il y aurait une certaine culture du déni en matière de cybermenace chez les opérateurs nucléaires, trop confiants en leur sécurité.

Le risque grandit avec la numérisation croissante de l'industrie nucléaire, offrant de nouvelles cibles pour quatre types d'« attaquants », selon le rapport : des « hacktivistes » antinucléaires, le crime organisé – qui peut monnayer son intrusion dans le système d'une centrale –, des États et services secrets, ou des groupes terroristes – au premier rang desquels Chatham House cite le groupe Etat islamique. « *De nombreuses centrales sont connectées à des réseaux extérieurs, et il existe différentes voies par lesquelles un acteur malveillant peut exploiter ces dépendances pour entraîner un incident de sécurité* », indiquent les auteurs. A les lire, on constate qu'une petite partie seulement des incidents est répertoriée et fait l'objet d'une communication publique.

A cela s'ajoute le manque de vigilance dans la logistique d'approvisionnement en composants informatiques. D'où les risques d'intrusion dans le système d'information. Pour leur part, les Russes essaient de le réduire au maximum, note le rapport. Enfin, le facteur humain continue ici aussi de peser lourd. Le rapport note ainsi un manque de formation à la cybersécurité, une communication défaillante entre les ingénieurs et les responsables de la sécurité qui ralentit la mise en œuvre des procédures clés de cybersécurité par le personnel, le manque pro-activité des centrales qui les conduit à se rende compte d'une attaque informatique une fois celle-ci déjà enclenchée...

Rappelons ainsi l'exemple de l'Iran. En 2010, le programme nucléaire de la République islamique avait été attaqué par un virus, Stuxnet, fruit d'un programme lancé en 2007 par les États-Unis, alliés avec Israël. Stuxnet a été introduit au moyen d'une simple clé USB. Cette attaque avait gravement perturbé l'activité des centrifugeuses iraniennes du centre d'enrichissement de l'uranium de Natanz. Il avait lourdement retardé la mise en service de la centrale électrique de Bouchehr construite par Rosatom. Or cette attaque est devenue une référence majeure chez les pirates qui en ont profité pour améliorer leurs techniques d'attaque ainsi que leurs moyens de diffuser le virus dans un grand nombre d'applications à visée malveillante ou de logiciels qui les hébergent de façon cachée.

Ici, la cyber-guerre menée par des États n'a fait que ralentir un programme industriel. Mais on ne peut exclure le risque de représailles ou d'escalade dans les hostilités. En décembre 2014, le groupe public d'électricité sud-coréen KHNP a été victime d'une attaque. Heureusement, les pirates n'ont pu atteindre le cœur technologique des centrales au point de rendre leur exploitation dangereuse. Reste que l'opération a été revendiquée depuis Hawaï par un groupe antinucléaire. Les hackers avaient eu accès à des données internes, publiées sur Twitter... D'autres exemples sont cités dans le rapport, notamment des virus introduits dans la centrale lituanienne d'Ignalina et trois centrales américaines dans les années 1990-2000.

Selon les réactions sur Twitter à un article du Monde, la communauté nucléaire montre qu'elle a déjà commencé à s'en inquiéter. On a pu s'en rendre compte lors de la conférence internationale sur la sécurité informatique dans le monde nucléaire organisée par l'Agence internationale de l'énergie atomique (AIEA) en collaboration avec Interpol qui avait réuni à Vienne (Autriche), début juin,

650 experts de 92 pays. « *Les cyberattaques ou les tentatives de cyberattaques sont désormais une occurrence quotidienne* », avait alors prévenu Yukiya Amano, le directeur général de l'AIEA qui constatait que « *les terroristes et autres criminels sont à la tête de réseaux internationaux et sont susceptibles de frapper partout* ». L'industrie nucléaire « *n'est pas une exception* », avait-il ajouté, en 2014 « *il y a eu des cas d'attaques aléatoires de programmes malveillants contre des centrales nucléaires et des installations prises pour cibles spécifiquement* ». La coopération internationale commence à se mettre en place et à se renforcer.

Reste à former les personnels aux meilleures pratiques de lutte contre la cybercriminalité et d'anticipation de la cybermenace.

Erick Haehnsen