COMMENT LES SERVICES EAU ET ASSAINISSEMENT PEUVENT MUSCLER LEUR CYBERSÉCURITÉ

De plus en plus connectés et automatisés, les services eau et assainissement s'exposent à des cyberattaques. Un risque que le référentiel du groupe de travail cybersécurité de l'Astee, présenté au Carrefour des gestions locales de l'eau, vise à contenir.

« *Que ce soient les réseaux d'eau ou d'assainissement, aujourd'hui tout est interconnecté… Ces services sont extrêmement automatisés,* souligne Joël Rivallan, coanimateur du groupe de travail cybersécurité de l'Association scientifique et technique pour l'eau et l'environnement (Astee). *Les hackeurs vont plus facilement s'attaquer à l'informatique de gestion qui est la plus ouverte, plus accessible par internet. Mais le risque existe aussi pour l'informatique technique et ses automates.* »

L'Agence nationale de la sécurité des systèmes d'information (1) (Anssi) a ainsi traité 31 incidents de sécurité entre janvier 2021 et août 2024 dans le secteur de la gestion de l'eau. Ils visaient principalement la facturation de l'eau, le pilotage et la supervision de la distribution de l'eau potable ou l'assainissement des eaux usées. Comme cela a pu être le cas, en avril dernier, pour une collectivité française qui a vu son système d'information chiffré par un rançongiciel. Parmi les services affectés : la supervision de la distribution et la téléintervention. La commune a toutefois pu assurer la continuité du service avec un fonctionnement dégradé.

Des motivations essentiellement financières

Les motivations des cybercriminels en France ? Principalement financières, avec une demande de rançon. « *Les cybercriminels déterminent aujourd'hui ces montants en fonction de critères comme la taille des entités et de leur chiffre d'affaires quand celui-ci est public*, a précisé l'Anssi dans un rapport consacré à la question. *Une étude de l'éditeur de sécurité Sophos indique que la rançon demandée aurait augmenté cette dernière année pour les secteurs de l'eau et de l'énergie, pour atteindre 2,5 millions de dollars américains en moyenne, en 2024.* »

“ Quand il y a des délégations de services publics ou des prestataires extérieurs, il est important de savoir qui fait quoi ”*Joël Rivallan, Astee*Toutefois en mars 2024, selon l'Anssi, un groupe russe a revendiqué la prise de contrôle d'une centrale hydroélectrique dans l'Yonne… Une opération sans conséquences, car en réalité l'attaque a porté sur un logiciel de contrôle d'un moulin, dans la Marne, une installation de petite taille opérée par un particulier. De la même manière, ni l'ouvrage ni les habitants n'ont subi d'incidences. « *Le ciblage de plusieurs entités du secteur du petit cycle de l'eau ou pouvant être apparentées au secteur de l'eau de manière plus globale, s'inscrit dans un contexte géopolitique tendu, où des acteurs cherchaient à tirer profit de la médiatisation des Jeux olympiques et paralympiques à des fins de déstabilisation* », analyse néanmoins l'Anssi.

En attendant la transposition de la directive Nis 2

Sur le plan européen, la seconde version de directive Sécurité des réseaux et de l'information (directive NIS 2) de décembre 2022 vise précisément ces questions et devrait améliorer le niveau de cybersécurité global. Pour la transposer en France, un projet de loi (2) a été déposé en octobre 2024, mais sans que les travaux aient beaucoup évolué depuis. « *Nous attendrons de connaître les limites et surtout les arrêtés de mise en application*, indique Joël Rivallan. *Mais le texte devrait s'appliquer aux collectivités les plus importantes et laisser de côté les petites et moyennes entités.* »

Pour apporter une aide à l'ensemble des collectivités, l'Astee a lancé un groupe de travail *ad hoc*. De leurs réflexions a émergé un référentiel de règles et de bonnes pratiques dévoilé, ce mercredi 22 janvier, à l'occasion du Carrefour des gestions locales de l'eau (CGLE) à Rennes. Ce dernier identifie 13 thématiques décomposées en 56 actions.

Pour anticiper les attaques, la première étape consiste à bien définir son niveau de risque. « *L'idée n'est pas de réaliser un audit détaillé, mais de connaître son niveau de protection et de définir ses objectifs d'améliorations techniques mais aussi organisationnels et humains, mais également les priorités* », développe Joël Rivallan.

Définir la responsabilité des acteurs

Autre point à ne pas négliger : l'organisation des services et la responsabilité des acteurs. « *Quand il y a des délégations de services publics ou des prestataires extérieurs par exemple, il est important de savoir qui fait quoi. Comment sont répartis les actions et, pour chacune d'entre d'elles, sur un appareil, qui en a la responsabilité* », souligne le coanimateur. *Il faut également bien connaître le système informatique industriel, disposer d'éléments très complets, le programme des automates par exemple. Comme pour un plan, si nous ne les avons pas le jour où tout est bloqué, pour reconstruire, c'est compliqué.* »

Les accès physiques comme virtuels doivent être contrôlés. « *C'est intéressant de ne pas avoir trop de Wi-Fi par exemple pour les aspects d'informatique industrielle* », précise Joël Rivallan.

Une attention doit également être portée à la configuration des équipements (mise à jour, versions, organisation, etc.) ainsi qu'à la maintenance (les responsables et leurs interventions), mais également à la détection et au suivi des incidents. « *Beaucoup d'attaques ne font que laisser ce que nous pourrions appeler un virus ou un petit programme qui pourra être actionné ultérieurement* », explique Joël Rivallan.

Garantir la continuité du service

Afin de permettre le maintien des activités, les services devront s'assurer que les sauvegardes de l'ensemble de leurs programmes sont à jour, comme leur plan de continuité et de reprise du service. « *Par exemple, si tel automate est bloqué, comment peut-on le mettre en marche manuellement en mode dégradé ?* » illustre Joël Rivallan.

Le référentiel explore également le contrôle continu, mais également les éléments contractuels à définir avec les délégataires, les actions de formation et de sensibilisation. « *Le critère humain intervient beaucoup,* note Joël Rivallan. *La sensibilisation peut porter sur des choses simples, comme ne pas apporter sa clef USB que nous avons prêtée la veille à notre fils pour enregistrer un jeu !* »

Le document propose également aux collectivités de s'évaluer de 0 à 5 pour chaque thématique abordée et hiérarchise les actions à engager en fonction de la taille de la collectivité. « *C'est vraiment un guide à s'approprier collectivité par collectivité* », conclut Joël Rivallan.

https://www.actu-environnement.com/ae/news/cybersecurite-eau-assainissement-nis-2-referentiel-astee-informatique-technique-45453.php4