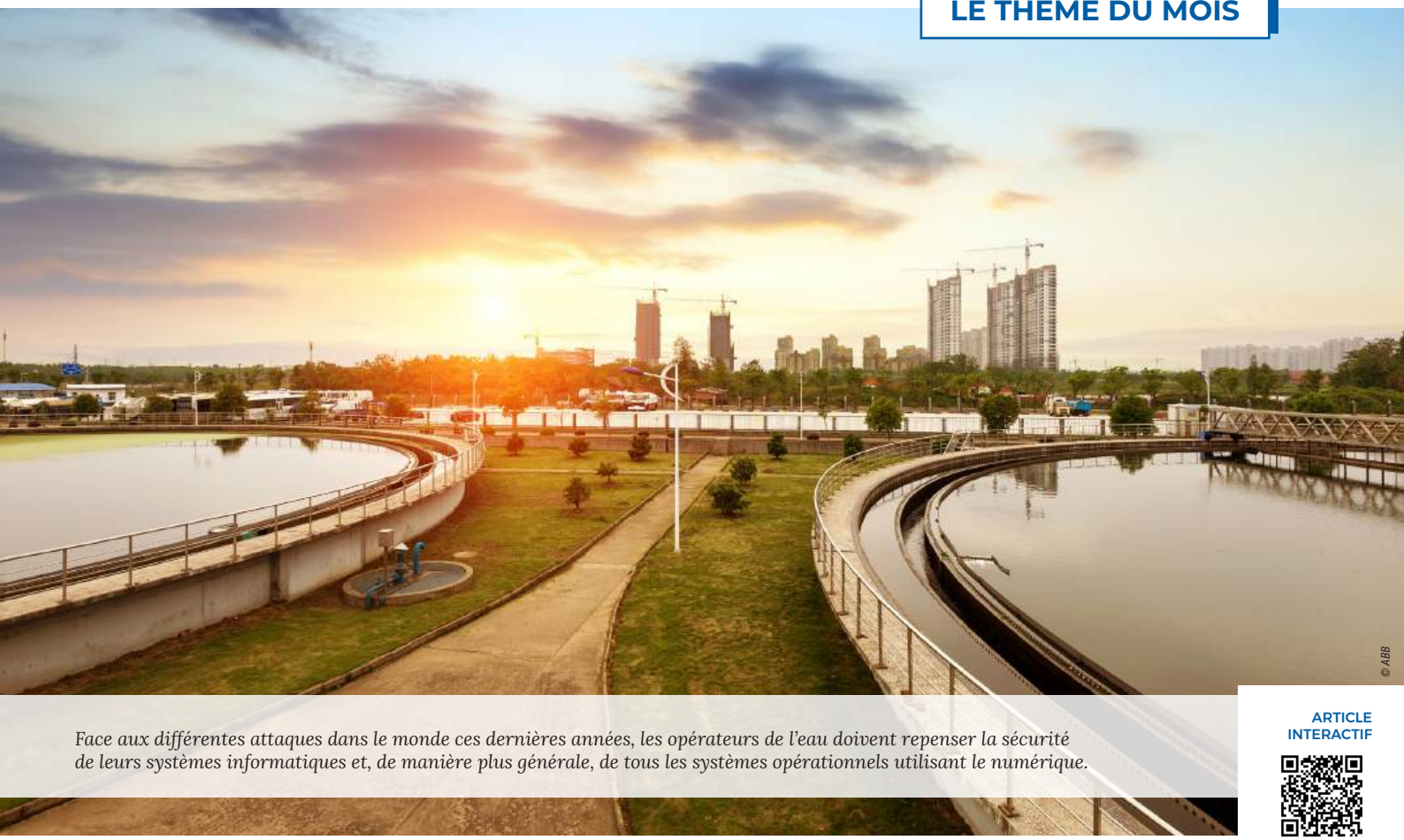


© ABB

Face aux différentes attaques dans le monde ces dernières années, les opérateurs de l'eau doivent repenser la sécurité de leurs systèmes informatiques et, de manière plus générale, de tous les systèmes opérationnels utilisant le numérique.

ARTICLE INTERACTIF

Cybersécurité : évaluer les risques pour sécuriser les infrastructures

Patrick Philipon

Abstract

As the transposition of the new EU Cybersecurity Directive looms, the water industry faces a critical need to upgrade. From the evolving threat landscape and necessary countermeasures to emerging regulatory requirements, here is a brief roundup of the situation.

Avec la transposition désormais imminente de la nouvelle directive européenne sur la cybersécurité, le monde de l'eau doit se mettre à jour. Nature des risques, contre-mesures à mettre en place, nouvelles contraintes réglementaires : petit tour de la question.

Début 2020, les infrastructures hydriques israéliennes subissaient des intrusions cybernétiques attribuées à des acteurs étatiques liés à l'Iran, dont l'objectif était de manipuler le dosage des produits chimiques dans les stations de traitement de l'eau. En mai 2022, l'entreprise italienne Alto Calore Servizi, responsable de l'approvisionnement en eau potable d'environ un demi-million de personnes, était victime d'une attaque par rançongiciel provoquant de sérieuses interruptions techniques. Le 14 mai 2023, le SMDEA (Syndicat mixte départemental de l'eau et de l'assainissement) dans l'Ariège faisait face à une cyberattaque sur sa structure informatique, etc.

Nous pourrions encore allonger cette liste mais le fait est là : le monde de l'eau n'est plus épargné par la cybercriminalité. Le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques),


© Perax

Les collectivités doivent s'assurer que leur infrastructure est saine, donc doivent transmettre les contraintes NIS 2 à leurs fournisseurs. Perax est à même de donner des conseils de base sur les implications informatiques de la directive.

une division opérationnelle de l'Anssi[1], a ainsi publié en novembre 2024 un rapport[2] sur l'état de la menace informatique dans le secteur de l'eau. L'Astee[3] a, pour sa part, édité le guide[4] d'application « La cybersécurité, un enjeu majeur dans les domaines de l'eau et de l'assainissement ».

Les opérateurs de l'eau doivent donc repenser la sécurité de leurs systèmes informatiques (matériels et immatériels) et, de manière plus générale, de tous les systèmes opérationnels utilisant le numérique et susceptibles d'être attaqués par cette voie. Un pas important à franchir pour des acteurs pas forcément au fait des dernières évolutions de ce domaine. Dès lors, par où commencer ? Quelles sont les obligations des opérateurs ? Contre quoi – ou qui – faut-il se défendre ? Par quels moyens ?

UN CADRE RÉGLEMENTAIRE DEVENU PLUS CONTRAIGNANT

La directive[5] (UE) 2022/2555 du Parlement européen et du Conseil européen, « *concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union* », plus connue sous le nom de directive NIS 2 (pour *Network and Information Security*), est entrée en vigueur le 16 janvier 2023, pour une transposition par les États membres au plus tard le 17 octobre 2024. Elle remplace la version précédente (NIS 1), transposée en France en 2018.

Grande nouveauté : les « *entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées* », autrement dit l'assainissement collectif, rejoignent les « *fournisseurs et distributeurs d'eaux destinées à la consommation humaine* » (l'eau potable) parmi les secteurs considérés comme « hautement critiques ». Dans ces secteurs, il existe des « entités essentielles » et des « entités importantes ». « *Les entités comptant plus de 250 employés et réalisant un chiffre d'affaires supérieur à 50 millions d'euros sont considérées comme essentielles, tandis que celles en-dessous de ces deux nombres sont classées comme importantes. Les entreprises de moins de 50 employés et dont le chiffre d'affaires est inférieur à 10 M€ sont exemptées de l'application de la NIS 2* », résume Xavier Cardeña, responsable du développement du marché de l'eau et expert cybersécurité chez HMS Networks.

La nouvelle directive renforce également les obligations pour les entités concernées et les sanctions en cas de non-respect. « *Il s'agit d'un renforcement global avec de futures obligations intégrant la protection physique des infrastructures informatiques, ainsi que l'alerte et la levée de doute rapide en cas d'intrusion proche de ces infrastructures* », explique, par exemple, Antoine Ancel, directeur Cybersécurité du groupe Suez.

« *Parmi ses aspects les plus importants, on note l'approche globale de la gestion des risques, avec des responsabilités clairement définies pour la direction générale, garantissant que le respect de la directive soit intégré dans la prise de décisions stratégiques. La directive introduit également des obligations de notification rapide aux autorités compétentes – en France, l'Anssi – pour signaler les incidents de cybersécurité significatifs, renforçant ainsi la capacité de réaction face aux menaces critiques. Bien que les exigences imposées aux entités essentielles et importantes soient similaires, les sanctions en cas de non-conformité diffèrent sensiblement. De plus, la surveillance de la conformité est beaucoup plus stricte pour les entités considérées comme essentielles* », complète Xavier Cardeña (HMS Networks).

En résumé, les entités concernées doivent mettre en œuvre une véritable politique d'analyse des risques et de sécurité des systèmes informatiques. En termes techniques, elles utiliseront, entre autres, la cryptographie, le contrôle d'accès pour le personnel et des procédures d'authentification des communications. Elles sont également tenues de notifier les incidents significatifs et de disposer d'un plan pour assurer la continuité de leurs activités en cas d'attaque.

En France, le projet de loi du 15 octobre 2024 « *relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité* » a été adopté au Sénat en mars 2025. Le 10 septembre 2025, il a franchi une nouvelle étape avec le vote en commission spéciale de l'Assemblée nationale. L'examen du texte[6] par les députés n'ayant toujours pas eu lieu, en partie à cause de l'instabilité politique actuelle, la France est sérieusement en retard dans sa transposition de NIS 2. La Commission l'a déjà souligné par deux fois, en adressant des mises en demeure en novembre 2024 et mai 2025. Quoi qu'il en soit, le projet de loi français reprend peu ou prou les mêmes lignes que la directive.

QUI EST CONCERNÉ DANS LE MONDE DE L'EAU ?

Les critères de chiffre d'affaires et de nombre d'employés retenus pas la directive NIS 2 ne sont guère adaptés à des administrations publiques qui, en France, sont responsables des services d'eau potable et d'assainissement. Le projet de loi français, s'il reprend les critères de NIS 2 pour les entreprises privées, prend en compte cette question.

1. *Agence nationale de la sécurité des systèmes d'information, <https://cyber.gouv.fr/>*
2. *Voir <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-011.pdf>*
3. *Association française des professionnels de l'eau et des déchets, voir <https://www.astee.org/>*
4. *Voir < https://www.astee.org/publications/guide-dapplication-la-cybersecurite-un-enjeu-majeur-dans-les-domaines-de-leau-et-de-lassainissement/>*
5. *Voir <https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fr>*
6. *Voir <https://www.assemblee-nationale.fr/dyn/17/textes/l17b1112_projet-loi#>*

Seront donc également considérées comme « entités essentielles », entre autres pour les activités de l'eau potable et de l'assainissement, les métropoles, les communautés urbaines, les communautés d'agglomération, les communes – et leurs EPA[7] – ou les syndicats qui fournissant des services à plus de 30 000 habitants. Les communautés ou les communes – et leurs EPA – desservant moins de 30 000 habitants seront considérées comme « entités importantes ». Il n'y a pas de seuil inférieur : tous les services d'eau et d'assainissement sont considérés comme, au moins, « importants ».

Par rebond, les délégataires (Saur, Suez, Veolia…) devront mettre en œuvre ces mesures, même si la collectivité délégante est légalement responsable de sa cybersécurité. « *Ce nouveau cadre réglementaire marquera un changement d'échelle significatif : en tant qu'opérateur de services d'eau, nous passerons d'un nombre limité de contrats concernés par la réglementation à potentiellement plusieurs centaines. En outre, il ne s'agira plus seulement de sécuriser quelques systèmes sensibles mais l'ensemble des infrastructures numériques liées à des activités critiques* », souligne Antoine Ancel (Suez).

Quelle que soit la date finale d'adoption du projet de loi en France, les entités concernées ont tout intérêt à prendre dès à présent leurs dispositions. L'Anssi leur recommande d'anticiper leur mise en conformité – par exemple, grâce à l'outil[8] d'autoévaluation MonEspaceNIS2 – et de commencer à identifier les écarts entre leurs pratiques actuelles et les futures exigences.

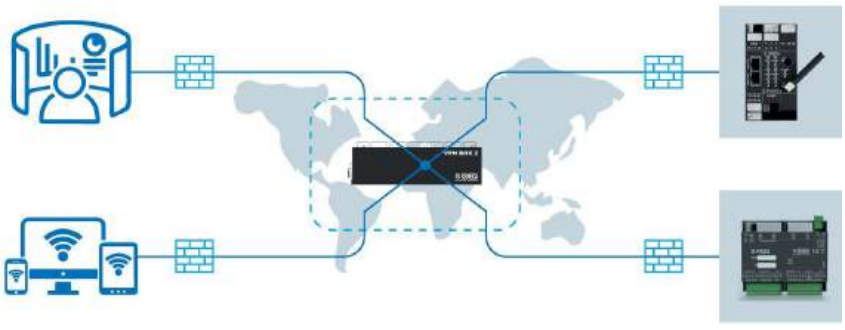
Par ailleurs, même s'ils ne constituent pas en eux-mêmes des entités directement concernées, les fournisseurs, équipementiers et installateurs vont devoir prendre en compte les exigences de cybersécurité. « *Parmi les obligations énumérées dans l'article 21 de la directive NIS 2 figure "la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs". Les collectivités devront donc évaluer et gérer les risques de cybersécurité non seulement dans leurs opérations internes, mais également tout au long de leur réseau de fournisseurs. Cela comprend les entreprises qui conçoivent, développent, fabriquent et livrent des produits et composants, ainsi que les intégrateurs de systèmes* », explique en effet Xavier Cardeña (HMS Networks).

« *Finalement, par ruissellement, tout le monde va être impacté* », estime ainsi Ludovic Pertuisel, Product Manager chez Lacroix Environnement. Même constat pour Loïc Daniau, responsable du bureau d'études Électronique et informatique chez Perax : « *Les collectivités doivent s'assurer que leur infrastructure est saine, donc doivent transmettre les contraintes NIS 2 à leurs fournisseurs. Chez Perax, en tant que fournisseur, nous conseillons nos clients EE et EI qui intègrent nos produits sur les implications informatiques de la NIS 2. En parallèle, nous travaillons avec un cabinet externe spécialisé en cybersécurité, qui audite et certifie nos produits, et qui apporte son expertise sur le sujet* », explique-t-il.

« *Le Cyber Resilience Act*[9] *européen de 2024, applicable à partir du 11 décembre 2027, obligera d'ailleurs tous les fabricants de produits numériques de l'Union européenne à divulguer les failles de cybersécurité de leurs produits. Ils devront également amener régulièrement des correctifs et des mises à jour de sécurité* », ajoute Ludovic Pertuisel (Lacroix Environnement). D'ores et déjà, les fabricants peuvent se référer aux normes internationales CEI 62443 et ISO/CEI 27001. Et, depuis août 2025, les équipements communiquant par radio doivent se conformer à la norme européenne EN 18031.

Le secteur de l'eau est de plus en plus exposé aux menaces informatiques et aux exigences strictes imposées par la directive NIS 2 – elle prescrit la protection des infrastructures critiques et la continuité du service. Dans ce contexte, la plateforme Let's de Seneca représente une solution complète de connectivité, d'automatisation et de sécurité pour les réseaux et les installations de pompage, d'épuration et de distribution. Basée sur le serveur VPN (*Virtual Private Network*) BOX 2, *Let's permet des connexions « Always On » (télécontrôle/Single* LAN) *et « On Demand »* (téléassistance P2P) avec authentification sécurisée, cryptage TLS et gestion automatique des certificats.

Les dispositifs Edge Let's intègrent des fonctions de passerelle IIoT, de routeur LAN/Wi-Fi/4G, d'enregistreur de données, de gestion des alarmes, de micro-contrôle de type if-then-else et de softPLC Straton IEC 61131-3. Compatibles avec les principaux automates programmables industriels et les protocoles MQTT, OPC UA et IEC 60870-5-104, ils offrent une interopérabilité et une surveillance en temps réel. L'envoi d'alarmes vocales, les logiques de contrôle distribué et la connectivité cloud garantissent la gouvernance des données et la maintenance prédictive. Certifiée et validée par des tests de pénétration, la plateforme Let's contribue à la cyber-résilience du cycle de l'eau, en combinant automatisation, protection et durabilité numérique.



© Seneca

Basée sur le serveur VPN BOX 2, Let's de Seneca permet des connexions « Always On » (télécontrôle) et « On Demand » (téléassistance) avec authentification sécurisée, cryptage TLS et gestion automatique des certificats.

7. *Etablissement public à caractère administratif*
8. *Voir <https://monespacenis2.cyber.gouv.fr/>*
9. *Voir <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>*

purecontrol

OPTIMISEZ
votre gestion de l'eau

GRÂCE À L'IA

-30%
de consommation d'énergie

7j/7
contrôle des équipements en temps réel

-40%
d'impact environnemental

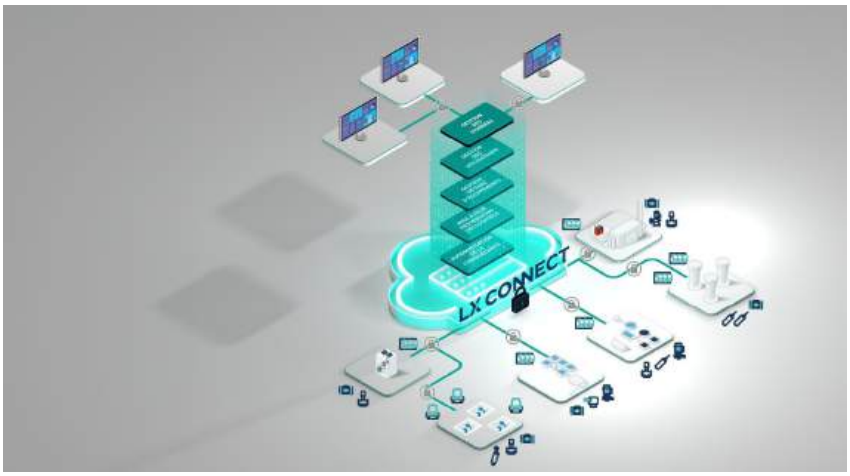
Flambée des **tarifs de l'énergie**, exigence de **réduction des émission de gaz à effet de serre**, renforcement des réglementations environnementales...

Purecontrol offre une solution innovante de **régulation intelligente** des infrastructures de gestion de l'eau.

- Une solution de pilotage unique qui va **au-delà des recommandations**
- Une solution **souple et rapide** à mettre en œuvre **en 3 mois** seulement
- Une solution **qui a fait ses preuves** : stations d'épuration, poste de relèvement, stockage et distribution d'eau potable

Réduisez votre empreinte carbone et **gagnez en efficacité** en tirant le meilleur parti de vos installations existantes, **sans investissement supplémentaire.**

purecontrol.com



© Lacroix Environnement

Lacroix Environnement propose la plateforme de centralisation LX Connect, qui gère la cybersécurité de l'ensemble du système, et ce de manière transparente pour le client.

Toujours dans le cadre du renfort de la cyber-résilience industrielle, Rockwell Automation a d'ailleurs lancé l'offre complète de cybersécurité industrielle SecureOT, élaborée pour aider les fabricants et les infrastructures stratégiques à protéger les opérations critiques et à créer des environnements sécurisés. Un grand nombre de systèmes hérités n'ont pas été conçus en tenant compte de la cybersécurité, et les outils informatiques traditionnels ne parviennent souvent pas à protéger des environnements industriels complexes et vieillissants face à une forte augmentation des cybermenaces ciblant les systèmes de production (OT). La nouvelle offre a été développée pour combler cette lacune, en aidant les entreprises à sécuriser leur infrastructure OT grâce à des technologies et une expertise adaptées à la réalité du terrain. SecureOT regroupe la plateforme éponyme, les services professionnels et les services de sécurité dédiés de Rockwell Automation au sein d'une solution unifiée qui offre une protection de bout en bout pour des systèmes industriels complexes, vieillissants et hautement réglementés.

QUELLE(S) MENACE(S) ?

Pour se défendre efficacement, encore faut-il savoir contre quoi. Les opérateurs d'infrastructures de production-distribution d'eau potable ou d'assainissement collectif doivent donc commencer par évaluer leurs risques en matière de cybersécurité. La question de la menace peut se décomposer en « que veulent – et qui sont – les attaquants ? », d'une part, et « comment (par où) pourraient-ils entrer ? », d'autre part.

Dans son guide d'application, l'Astee évoque des « *risques multiples : rançonnage, atteinte à la réputation au travers de la publication de fausses informations, indisponibilité des outils numériques, détournement de fonds au travers des fonctionnalités de paiement à distance… Dans le cas des installations de traitement d'eau, des cyberattaques permettant d'agir sur leurs consignes de pilotage peuvent avoir des conséquences directes dans le monde physique : perturbation de l'alimentation en eau potable de la population, pollution du milieu naturel, endommagement des ouvrages, modification des procédés des usines, etc.* ».

Le rapport du CERT-FR distingue, pour sa part, les attaques à des fins lucratives (demandes de rançon ou captation de données), des fins de déstabilisation (déni de service, divulgation d'informations, sabotage informatique), des fins de prépositionnement (en cas de tension préalable à un conflit) ou des fins d'espionnage (exploitation de données sensibles). « *Le ransomware (logiciel de demande de rançon) reste le type d'attaques le plus courant, mais il existe également des attaques disruptives ou destructives, dont l'objectif est d'interrompre, d'endommager ou même de détruire des systèmes et des opérations. Leurs effets peuvent aller d'interruptions temporaires de service à des dommages irréversibles sur les infrastructures ou les processus opérationnels* », confirme Xavier Cardeña (HMS Networks).

Même si ces attaques ne sont évidemment pas signées, les acteurs distinguent plusieurs grandes catégories d'agresseurs. « *Il existe plusieurs niveaux d'attaquants. D'abord des "opportunistes", par exemple quelqu'un qui a travaillé pour une société, qui a toujours son login et son mot de passe et veut se venger, par exemple, d'un licenciement, en bloquant ou sabotant un aspect opérationnel. Il y a également des organisations (ou des individus) criminelles, qui ne visent pas spécialement une entité mais vont sur Internet, scannent tout ce qui passe, et repèrent des portes ouvertes. Ces groupes pratiquent plutôt la demande de rançon ou le vol de données. Enfin, certaines organisations liées à des États disposent de très gros moyens et poursuivent des fins plus politiques. Ces acteurs chercheront à déstabiliser le réseau d'eau d'un pays avec lequel ils sont en conflit. Ils pourront, par exemple, arrêter le pompage, saboter des vannes, modifier l'injection de chlore…* », énumère Ludovic Pertuisel (Lacroix Environnement).

« *Il existe plusieurs catégories d'attaquants mais tous mènent les mêmes types d'action, même si ce n'est pas forcément sur les mêmes cibles. Par exemple, les attaques à but lucratif viseront plutôt les serveurs de données, alors que les agressions politiques concerneront plutôt les outils opérationnels. Les deux types de serveurs peuvent être visés pour des demandes de rançon* », précise Loïc Daniau (Perax).

Cela posé, par où entrent les attaquants ? Autrement dit, quelles sont les « portes ouvertes » ? Le monde de l'eau présente à cet égard des vulnérabilités particulières. « *Le secteur est la cible de différents types d'acteurs malveillants qui cherchent à exploiter plusieurs faiblesses telles que l'héritage d'installations anciennes, le dispersement* [sic] *géographique des sites ou le faible budget alloué à la sécurité. L'hétérogénéité des opérateurs, en termes de statut, de taille d'organisation et de maturité de la sécurité des systèmes d'information (SI) constitue également des opportunités d'action pour les attaquants* », explique, par exemple, le rapport du CERT-FR.

« *La télégestion est fortement employée pour optimiser la maintenance des différentes infrastructures physiques réparties sur le territoire. Si elle n'est pas accompagnée d'efforts de sécurisation, elle peut conduire à l'exposition directe*

ALCEA
ASSA ABLOY

une solution matérielle et logicielle pour garantir la sûreté des infrastructures du monde de l'eau.

Intégrez, surveillez et protégez vos équipements grâce à un système global de sûreté centralisé.

- **Contrôle d'accès :** Gardez le contrôle en temps réel
- **Solutions de verrouillage** : Idéales pour protéger vos sites isolés
- **Gestion des clés :** Gagnez du temps grâce à la traçabilité de vos ressources partagées
- **Gestion des sous-traitants :** Simplifiez votre quotidien en supervisant leurs parcours
- **Détection intrusion** : Protégez zone par zone et restez informés
- **Vidéoprotection** : Améliorez votre réactivité grâce à la levée de doute

alceaglobal.com
alcea france

contactez nous
pour découvrir nos solutions

d'interfaces métier d'équipements industriels ou d'interfaces d'administration d'équipements périphériques», ajoute le même rapport.

«*Dans le domaine du traitement de l'eau potable, les services sont généralement plus décentralisés, tandis que les systèmes d'eaux usées présentent une structure plus interconnectée. Cependant, les deux secteurs font face à des problèmes communs : infrastructures obsolètes, ressources humaines et techniques limitées, et coordination insuffisante en matière d'échange d'informations et de renseignements sur les menaces*», confirme Xavier Cardeña (HMS Networks).

En fait, tous les points d'une infrastructure d'eau potable ou d'assainissement peuvent être vulnérables, d'un simple capteur ou d'un automate aux plateformes centrales de supervision ou d'hypervision. «*Si l'attaque concerne un équipement unique, elle crée un problème local. Les attaquants sont aveugles, cependant : ils avancent en fonction de ce qu'ils trouvent, et il y a plus de probabilité de trouver une faille sur un serveur central que sur un équipement isolé. Mais il ne faut pas oublier que les composants périphériques peuvent constituer des points d'entrée pour rebondir ensuite sur les serveurs centraux*», rappelle Loïc Daniau (Perax)

«*L'un des vecteurs d'attaque les plus critiques est l'accès à distance, qui peut permettre des mouvements vers d'autres systèmes disposant d'un accès libre à plusieurs équipements, ce qui signifie que l'infection d'une seule machine peut se propager rapidement au reste et, même, atteindre les systèmes de supervision. D'autant qu'il existe aujourd'hui, dans le monde de l'eau, une forte tendance à connecter des systèmes hérités du passé à de nouvelles plateformes numériques, alors que ces anciens systèmes n'ont pas toujours été conçus pour s'intégrer de manière sécurisée*», souligne, pour sa part, Xavier Cardeña (HMS Networks).

UNE RÉPONSE AUSSI BIEN ORGANISATIONNELLE QUE TECHNIQUE

Face à cela, la réponse se fait en trois volets : analyser les risques, établir un cadre de gouvernance de la cybersécurité et appliquer les mesures techniques nécessaires pour protéger l'infrastructure et minimiser les risques. Même si l'Anssi a mis en ligne une méthode[10] d'auto-évaluation des risques (méthode *Ebios Risk Manager*), ce n'est évidemment pas le métier des opérateurs de systèmes d'eau potable ou d'assainissement.

«*L'identification et la gestion des risques constituent l'un des piliers fondamentaux de la directive NIS 2. L'évaluation des risques peut être réalisée par l'opérateur avec ses équipes internes, par des entreprises agréées ou par des audits externes – une option courante et recommandée – ainsi qu'avec des prestataires externes spécialisés en cybersécurité opérationnelle*», explique Xavier Cardeña. «*Ce n'est pas le cœur de métier des gérants de services d'eau d'identifier, de comprendre et d'appliquer les réglementations de cybersécurité. La plupart des régies ou prestataires importants ont certes des équipes IT mais elles ne sont pas toujours suffisamment formées à la cybersécurité*», affirme, lui aussi, Loïc Daniau (Perax).

Une fois le risque évalué et les vulnérabilités repérées, il faut établir un cadre de gouvernance de la cybersécurité. Et, enfin, prendre des mesures concrètes pour protéger l'infrastructure. «*Cela inclut l'installation de pare-feu, le contrôle d'accès et une authentification robuste, la gestion des identités, l'authentification multifactorielle et la définition d'un plan de réponse aux incidents, en veillant à ce que seul le personnel autorisé ait accès aux systèmes critiques*», énumère, par exemple, Xavier Cardeña (HMS Networks).

Et, de fait, entre les pare-feu, la segmentation des réseaux, les restrictions d'accès, la détection des intrusions ou le cryptage des données, les outils numériques ou organisationnels ne manquent pas. Reste à les utiliser de manière cohérente pour sécuriser globalement les infrastructures. «*En effet, un pare-feu est indispensable mais il doit surtout être adapté au monde industriel. C'est dans ce contexte que nous avons développé une nouvelle gamme de pare-feu mGuard et une nouvelle version de la plateforme de télémaintenance mGuard Secure Cloud*», indique le chef de produits Cybersécurité de chez Phoenix Contact.

Les systèmes d'eau potable ou d'assainissement se répartissent en deux grands types d'architecture. Classiquement, ce sont des infrastructures fermées comprenant, à la périphérie, des capteurs, des *data loggers* (enregistreurs de données) et des automates, remontant leurs données vers un SCADA et des serveurs centraux. «*Ces architectures classiques sont robustes, durables et autonomes. Les opérateurs les maîtrisent et ont accumulé beaucoup d'expérience. En revanche, elles sont complexes à maintenir. Et surtout, elles font l'objet d'une cybersécurité "réactive", c'est-à-dire que les mises à jour sont manuelles et, parfois, sont effectuées sur site, équipement par équipement*», explique Ludovic Pertuisel (Lacroix Environnement).

La société propose donc une nouvelle brique s'insérant dans ce genre d'architecture : une plateforme de centralisation, appelée LX Connect, qui gère la cybersécurité de l'ensemble du système

© HMS Networks

Les pare-feu Anybus Defender de HMS Networks intègrent la fonctionnalité DPI qui analyse les protocoles industriels et qui permet, par exemple, d'empêcher des requêtes d'écriture vers un automate programmable tout en autorisant la lecture des données.

10. *Voir < https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide>*

(renouvellement des certificats d'authentification, mise à jour des systèmes, sécurisation des flux et des accès, normalisation des formats, etc.), et ce de manière transparente pour le client. Cette plateforme, qui évolue constamment, vient d'ailleurs d'intégrer une fonction de cartographie du parc d'équipements.
L'autre grand type d'architectures, ouvertes, repose sur l'Internet des objets (IoT). Les équipements périphériques communiquent entre eux et avec les éléments centraux via le cloud. « *L'avantage est que l'on peut faire plein de choses à distance, mais l'inconvénient, c'est que tout est interconnecté et qu'Internet est un réseau ouvert* », souligne Ludovic Pertuisel (Lacroix Environnement). « *Les barrières à mettre en place dans ce cadre-là concernent l'ensemble de l'infrastructure du client, et pas seulement l'équipement pouvant servir de porte d'entrée* », renchérit Loïc Daniau (Perax).
Createch 360°, fournisseur de solutions numériques de pilotage optimisé, a d'ailleurs délibérément choisi d'éviter le recours au cloud. « *Nous proposons l'implémentation locale de nos plateformes CREApro, hébergées sur un PC sur site. Nous évitons ainsi le passage par Internet, et nos solutions sont ainsi bien plus faciles à installer et sécuriser* », affirme Lynne Bouchy, Product Line Manager chez Createch 360°. À l'inverse, Purecontrol a une approche totalement orientée sur le cloud. « *Aujourd'hui, il ne viendrait plus à l'idée de personne de dire qu'un serveur mail auto-hebergé est plus sécurisé que la suite logicielle Microsoft 360. C'est contre-intuitif mais l'expérience montre que des ouvrages totalement déconnectés du réseau étaient particulièrement vulnérables (y compris pour des sites sensibles, comme l'a illustré l'attaque avec le ver informatique StuxNet). Dans notre cas, l'accès à des données externes (par exemple, la météo ou les tarifs énergétiques) et la capacité de remonter des informations pour la détection d'anomalies sont essentielles. Ce besoin en connectivité nécessite toutefois une démarche cybersécurité rigoureuse. Par ailleurs, elle offre souvent à nos clients l'opportunité de moderniser la sécurité de leurs anciens systèmes de communication, tels que les* data loggers *ou les mécanismes historiques de remontée de données vers les serveurs centraux, en s'appuyant sur ces nouvelles approches plus sûres* », explique Gautier Avril, directeur technique de Purecontrol.

MULTIPLIER LES OBSTACLES

HMS Networks, qui fournit des systèmes de connexion et de communication pour différentes branches industrielles, propose, pour sa part, des solutions basées sur le cloud, et doit donc prendre les contre-mesures nécessaires pour assurer la sécurité dans un tel environnement. Ainsi, les routeurs d'accès à distance Ewon et le service Talk2m sont-ils certifiés selon la norme ISO/CEI 27001.
« *Nous disposons également de switches* [commutateurs, NDR] *managés de couche 2, tels que le NT5000 de NTron, conçu avec une approche globale de la sécurité réseau. Cet équipement intègre le chiffrement des mots de passe, le contrôle d'accès multi-niveaux, la sécurité MAC et l'authentification à distance via la norme IEEE 802.1X avec un serveur RADIUS*[11]*. De plus, le NT5000 permet de superviser en temps réel de l'état du réseau grâce aux journaux d'événements et au syslog, offrant des notifications immédiates en cas de tentatives d'accès non autorisées ou de modifications de configuration. S'il détecte des tentatives d'accès sans succès, le système peut désactiver automatiquement les identifiants utilisateurs ou les ports concernés* », précise Xavier Cardeña (HMS Networks).
Par ailleurs, les pare-feu Anybus Defender, conçus pour les environnements opérationnels, intègrent la fonctionnalité DPI (*Deep Packet Inspection*) qui analyse les protocoles industriels tels que Modbus ou DNP3 et qui définit précisément les opérations autorisées et celles qui doivent être bloquées. « *Par exemple, il est possible d'empêcher des requêtes d'écriture vers un automate programmable tout en autorisant la lecture des données. De plus, Anybus Defender peut analyser le trafic enregistré et générer automatiquement un ensemble de règles adaptées aux protocoles détectés* », ajoute-t-il.
Perax continue également à « durcir » ses produits. Dans le monde de l'eau, ses produits les plus utilisés sont l'automate de télégestion P400 (en général, relié au SCADA par un réseau Interne ou cellulaire sécurisé) et le deltaX (appareils autonomes, dispersés et communiquant leurs données en cellulaire sécurisé). Perax met régulièrement à disposition de ses clients les versions logicielles de ses produis. Ainsi les utilisateurs maîtrisent les périodes de mises à jour selon leurs process métier. « *Après une trentaine d'années de déploiement et de maintien opérationnel, l'automate P400XI arrive aujourd'hui à sa limite de développement en termes de cybersécurité sur les architectures ouvertes. Pour les clients souhaitant relier en direct*

© Westermo

Les passerelles Merlin de Westermo assurent une connexion fiable, même sur les sites les plus isolés, une résistance aux environnements les plus exigeants et une protection optimale en parfaite conformité avec l'Anssi et la directive NIS 2.

11. *RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur.*

leur automate à Internet, nous achevons la validation, par des experts indépendants, d'une nouvelle version plus sécurisée. Cette version intègre de fait des capacités de calcul supérieures et une interface homme-machine (IHM) plus moderne et ergonomique. Le P400 IoT – c'est son nom – sera disponible fin 2025-début 2026 », affirme Loïc Daniau (Perax). Pas besoin, pour autant, de remplacer les P400xi en place : pour les faire évoluer en P400Iot, il suffira de changer la carte de calcul.

« *Disposer d'un pare-feu est primordial mais il faut aussi s'équiper de produits (automates, produits de connexion sans fil,* switches*) fiables et qui disposent de couches de cybersécurité. Dans nos produits comme les automates* PLCnext*, les* WLAN*, les* switches *manageables des séries* 2000*,* 3000 *et* 4000*, des fonctionnalités de cybersécurité sont intégrées et permettent déjà de mettre en place une couche de sécurité. De plus, la sécurité est ancrée dans l'ensemble du cycle de vie de nos produits développés selon le processus de développement* CEI 62443-4-1*, bon nombre d'entre eux étant également déjà certifiés selon la norme* CEI 62443-4-2 », ajoute le chef de produits Cybersécurité de Phoenix Contact.

Les passerelles Merlin de Westermo représentent une nouvelle génération de solutions pour la connectivité et la sécurité des réseaux industriels. Grâce à leurs versions 4G, 5G, LTE-M et fibre optique, avec double carte SIM pour la redondance, elles assurent une connexion fiable, même sur les sites les plus isolés, et résistent aux environnements les plus exigeants. Mais c'est surtout sur le plan de la sécurité que la gamme Merlin se distingue. Conforme à la norme IEC 62443, les passerelles intègrent un module TPM pour le stockage sécurisé des clés, un Secure Boot pour empêcher l'exécution de *firmwares* non autorisés, un pare-feu avec inspection d'état, des fonctions VPN et chiffrements avancés ainsi qu'un contrôle d'accès et un filtrage de flux précis. La gamme Merlin assure ainsi aux entreprises une protection optimale en parfaite conformité avec l'Anssi et la directive NIS 2.

Au-delà de la sécurité, Merlin facilite la gestion et la supervision des réseaux industriels via la plateforme Activator. Celle-ci offre un déploiement automatisé et sécurisé (*Zero Touch Deployment*), une gestion centralisée des routeurs, une supervision en temps réel, l'application rapide des correctifs et le maintien de la conformité réglementaire. Cette approche intégrée permet aux opérateurs industriels de gagner en efficacité tout en maintenant un haut niveau de sécurité sur l'ensemble de leur infrastructure. Dans le secteur de l'eau, des centaines de routeurs Merlin LTE ont été déployés pour connecter et sécuriser les armoires électriques « intelligentes » sur plusieurs sites. Ce projet a permis d'assurer des communications chiffrées, un contrôle strict des accès distants et une maintenance à distance efficace, réduisant les interventions sur site et renforçant la continuité de service.

© Siemens

Siemens apporte une expertise spécifique à la sécurisation des plateformes industrielles, notamment dans le monde de l'eau avec son système de supervision PCS 7 et la technologie WinCC, en y intégrant des systèmes de protection robustes et adaptés.

Du côté de Siemens, le groupe propose une offre complète, certifiée IEC 62443 de solutions de cybersécurité et couvrant tous les aspects, de l'audit de sécurité, l'analyse de risques et des vulnérabilités jusqu'à la formation des équipes en passant par le *consulting* et les Pentest (*Penetration Testing Services*). Ses technologies incluent un SOC (*Security Operations Center*) industriel, des pare-feu, des accès distants sécurisés (Sinema Remote Connect), des solutions d'antivirus et de liste blanche, la gestion des correctifs et la gestion des vulnérabilités (Vilocify). Le fabricant intègre également des outils spécialisés comme Sinec Inspector, Sinec Security Monitor, Sinec INS, Sinec NMS, Sinec Security Guard, ainsi que des composants matériels sécurisés tels que S7-1500, SC-600, XCxxx. Siemens apporte une expertise spécifique à la sécurisation des plateformes industrielles, notamment dans le monde de l'eau avec son système de supervision PCS 7 et la technologie WinCC, en y intégrant des systèmes de protection robustes et adaptés.

La multiplication des équipements supportant une connectivité Ethernet facilite l'accès à distance mais amène une exposition au risque beaucoup plus importante. Aussi, il est important de mettre en œuvre le principe de défense en profondeur. Que ce soit au niveau organisationnel (formation des équipes, règles sur les mots de passe), au niveau physique (locaux ou armoires sécurisés) ou au niveau réseau (VLAN, VPN, pare-feu), l'idée est de multiplier les couches de défense afin de prévenir de la défaillance d'une strate.

À cet effet, les automates de télégestion de Wago intègrent nativement de nombreuses fonctionnalités. Grâce à leur base sous le système d'exploitation Linux, ils héritent de composants logiciels éprouvés, déjà installés et utilisés sur des millions de systèmes Linux. Parmi ces applicatifs, on retrouve le pare-feu IPtables, le système de journalisation Syslog-ng, les applicatifs VPN OpenVPN et Strongswan (IPsec), ou encore wpa_supplicant pour l'authentification 802.1X.

À tous les niveaux, le recours à une plateforme Linux ouverte facilite les échanges entre automaticien et DSI, puisque les automaticiens continuent d'utiliser un outil de programmation

© Wago

Grâce à leur base sous Linux, les automates de télégestion de Wago, qui intègrent nativement de nombreuses fonctionnalités, héritent de composants logiciels éprouvés, déjà installés et utilisés sur des millions de systèmes Linux.

classique, tandis que les DSI peuvent se concentrer sur la mise en place de leur politique via des applicatifs et mécanismes connus et maîtrisés. Le recours à des protocoles chiffrées est également primordial, avec, notamment, l'OPC UA ou le MQTT – ce dernier est particulièrement bien adapté à la gestion multi-site – , que les automates de Wago supportent.

Reste qu'aucune technologie, aussi sophistiquée soit-elle, ne peut garantir une totale immunité. « *Il n'y aura jamais d'installation parfaite. Il faut surtout multiplier les obstacles et les contraintes, sur l'ensemble du système, pour retarder – et si possible décourager – les attaquants* », estime Loïc Daniau (Perax). Par exemple, la protection physique d'un « simple » automate comportera le portail d'entrée du site, l'accès au bâtiment puis les clés de l'armoire électrique. « *Si l'intrus a franchi ces barrières physiques, il lui faut maintenant "entrer" dans le logiciel de l'automate, protégé par des mots de passe et autres barrières numériques. S'il réussit, il pourra commencer à nuire. Restent tout de même encore les systèmes contrôleurs de réseau, qui détectent les changements d'adresse ou les comportements suspects des équipements, et qui peuvent les bloquer* », énumère Loïc Daniau. Bien évidemment, les infrastructures ouvertes utilisant le cloud reposent uniquement sur des outils numériques pour assurer leur sécurité.

UNE CULTURE À PROMOUVOIR… ET À MAINTENIR DANS LE TEMPS

La cybersécurité d'une infrastructure ne repose pas seulement sur des dispositions organisationnelles ou techniques installées une fois pour toutes. C'est l'affaire de tous les agents et de tous les instants, d'où la nécessité d'insuffler une véritable « culture » de la cybersécurité parmi le personnel. « *La réglementation en vigueur ne se limite pas à la protection technologique : elle considère la formation et la sensibilisation du personnel comme un pilier essentiel pour garantir la sécurité globale. De même, il est nécessaire de désigner un responsable ou une équipe de contact en matière de cybersécurité* », souligne ainsi Xavier Cardeña (HMS Networks). « *Une attaque par Internet pourra par exemple provenir de la maladresse d'une personne qui aura ouvert un point d'accès dans un mail et exposé, de ce fait, toute l'infrastructure. C'est sur cela aussi qu'il faut sensibiliser les équipes* », ajoute Loïc Daniau (Perax).

Ce qui fait dire à Lenze qu'au-delà des aspects techniques, la cybersécurité est avant tout une culture à entretenir dans la durée. Le fabricant apporte une réelle valeur ajoutée grâce à un accompagnement à la conformité réglementaire (NIS 2, Cyber Resilience Act, normes CEI 62443 et ISO 27001) – cybersécurité intégrée dès la conception (*Security by Design*) dans les solutions, analyse des risques, définition des politiques de sécurité, gestion des incidents, etc. –, à des solutions techniques adaptées aux infrastructures critiques, à une expérience terrain et une adaptation aux spécificités du marché français (y compris dans le secteur de l'eau), à un engagement dans la certification et la transparence ainsi qu'à la sensibilisation et la culture de la cybersécurité (formation et sensibilisation des équipes).

En plus d'un ensemble de solutions (contrôleurs, passerelles et logiciels, pare-feu, authentification avancée, gestion centralisée des accès…), Lenze met également à disposition des outils de supervision, de détection d'intrusion et de gestion des certificats, tout en assurant la sécurité de la chaîne d'approvisionnement, conformément à l'article 21 de la directive NIS 2. Son équipe PSIRT (*Product Security Incident Response Team*) assure une réponse rapide en cas d'incident. En étant certifié ISO/IEC 27001 pour son système de management de la sécurité de l'information, le fabricant s'engage à divulguer les vulnérabilités et à fournir des correctifs réguliers, conformément au Cyber Resilience Act. ●