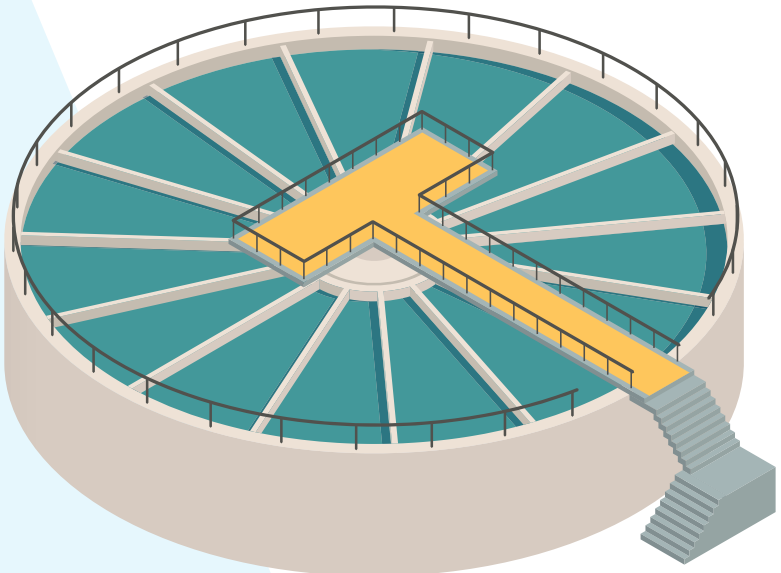
STORMSHIELD

Cybersécurité
en milieu sensible :

Immersion dans l'industrie de l'eau

Livre blanc



Trois jours...

Voilà l'espérance de vie d'un être humain privé d'eau. C'est dire l'importance vitale de cette ressource.



Mais l'eau est également nécessaire aux activités agricoles, industrielles et au confort des foyers. Combien de temps les sociétés pourraient-elles continuer de fonctionner normalement une fois le robinet coupé, *a fortiori* dans un contexte de réchauffement climatique?

Il est du ressort des acteurs du secteur de l'eau – collectivités et entreprises privées en délégation de service public – que nous n'ayons pas à le découvrir. Ceux-ci sont ainsi investis d'une double responsabilité envers les populations et l'environnement. D'une part, ils doivent assurer la continuité de la production et de la distribution d'eau potable, tout en garantissant la sécurité sanitaire. De l'autre, il leur revient de traiter les eaux usées, pour éviter les pollutions lors de leur rejet en milieu naturel ou de leur réutilisation.

En France, le secteur est donc suffisamment sensible pour être coordonné par le Ministère chargé de l'Écologie et suivi au quotidien par un coordinateur sectoriel de l'ANSSI, au sein d'une sous-direction Stratégie « Bureau énergie, transport et environnement ».

Or, cet écosystème industriel dense, composé d'usines de production d'eau potable ou encore de stations d'épuration dont certaines sont classées opérateurs d'importance vitale (OIV) en France et/ou opérateurs de services essentiels (OSE) à l'échelle européenne, s'appuie sur des infrastructures et des technologies vieillissantes qui le rendent vulnérable. En outre, ces systèmes opérationnels sont aujourd'hui beaucoup plus exposés au risque cyber car, sous l'effet de la numérisation du secteur et de l'arrivée de nouvelles technologies, ils se retrouvent de plus en plus souvent connectés au réseau informatique.

Ce phénomène de convergence IT/OT est illustré par l'implantation de l'Ethernet IP jusque dans les usines ou encore le développement de solutions Cloud de supervision industrielle. Une surface d'attaque favorable aux cyber-attaquants, souvent plus compétents sur les technologies informatiques traditionnelles que sur des protocoles industriels spécifiques.

D'ailleurs, que ce soit aux États-Unis ou en Israël, les exemples de cyberattaques ciblant des entreprises de l'eau se multiplient depuis quelques années. Et, dans le monde entier, les entreprises

et organismes publics liés au secteur de l'eau prennent progressivement conscience du besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels.

Ce risque cyber accru traduit aussi la fragilité d'un secteur victime de sous-investissement. En Europe comme de l'autre côté de l'Atlantique, les infrastructures de l'eau sont ainsi gérées en majorité par de petites structures et génèrent peu de marges. Leurs outils industriels s'amortissant beaucoup moins vite qu'un réseau bureautique, elles sont souvent équipées d'automates d'ancienne génération, qui augmentent leur vulnérabilité. Et puisqu'un investissement en matériel cyber a un impact direct sur le prix du litre d'eau, ces structures doivent aussi faire face à la nécessité de maîtriser le coût, afin de préserver l'accès à la population.

Par manque de moyens, mais aussi de maturité face au sujet, les gestionnaires de réseaux d'eau se sont longtemps focalisés sur la protection de la santé de la population, mettant de côté celle de leurs systèmes d'information.—

L'objectif de ce livre blanc est donc de permettre aux responsables informatiques ainsi qu'à tout l'écosystème de sous-traitants (intégrateurs et constructeurs) du secteur de se plonger dans un état de l'art de la question de la cybersécurité de l'industrie de l'eau.



Pour cela, nous vous proposons dans les pages qui suivent de décrypter les problématiques du secteur et de vous offrir un inventaire opérationnel des solutions possibles.

Sommaire

Chiffres à retenir

• **Infographie —** Cartographie du monde de l'eau

PARTIE I.
Pourquoi l'industrie de l'eau doit-elle prendre le sujet cyber au sérieux ?

PARTIE II.
Vers des (cyber) guerres de l'eau ?

• **Entretien client #1 —** Point de vue : la cybersécurité, un réflexe en cours d'acquisition dans l'industrie de l'eau

PARTIE III.
Quelles problématiques agitent la cybersécurité de l'industrie de l'eau ?

• **Infographie —** Les principales vulnérabilités du secteur

PARTIE IV.
Quelles règlementations cyber autour de l'industrie de l'eau ?

PARTIE V.
Et demain ?

• **Entretien client #2 —** La sécurisation d'un réseau distribué

Chiffres
à retenir

33 200

ouvrages de prélèvement de l'eau recensés en France (FP2E, 2019). Pour éviter leur pollution, les lois sur l'eau de 1992 et 2006 prévoient trois périmètres de protection des captages (immédiat, rapproché, éloigné) et un dispositif contre les pollutions diffuses sur les aires d'alimentation des dits captages. Pas de mention de la cybersécurité à l'époque.

40 à 45%

Il s'agit **du taux de fuite** des réseaux de distribution d'eau des villes de New York, Londres et Rome (contre 20 à 25 % en moyenne ailleurs selon Les Échos Investir, 2021). Autant de brèches que la télégestion et la maintenance prédictive entendent colmater.

400

Le nombre d'habitants de Chatsworth (Géorgie du Nord, États-Unis) qui n'ont pas pu utiliser l'eau du robinet pendant plusieurs jours en 2013. La raison : une intrusion dans le système de supervision d'une installation d'eau potable de la ville et une modification des réglages des taux de fluor et de chlore.

46

Le nombre d'essais infructueux pour pénétrer les systèmes d'information d'une station d'épuration en Australie en 2000. Malheureusement, au 47e, l'ancien prestataire technique de l'usine a réussi à en prendre le contrôle avant de déverser des eaux usées dans les fonds marins.

3

Le nombre de crises cyber liées à l'eau subies par le seul pays d'Israël sur l'année 2020. Entre avril et décembre, des cyberattaques ont ainsi touché des stations de pompage et de traitement des eaux, des pompes à eau et un réservoir d'eau recyclée.

Plus de 3 vulnérabilités sur 5

dans les systèmes d'information industriels peuvent conduire à l'indisponibilité totale de l'outil de production si elles sont correctement exploitées. Et 72 % d'entre elles peuvent l'être à distance. *(Claroty, 2020).*

52%

de la population mondiale vivra dans des conditions de stress hydrique d'ici 2050 *(Nations Unies, 2019)*. De quoi renforcer les enjeux déjà stratégiques liés à cette ressource.

x2

Les systèmes opérationnels de l'industrie de l'eau présentent plus du double de vulnérabilités par rapport au secteur de la santé, pourtant particulièrement exposé pendant la crise sanitaire. *(Claroty, 2020).*

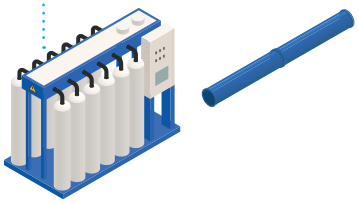
Infographie

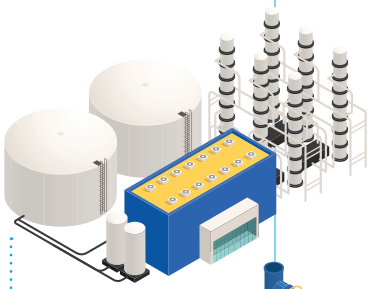
Cartographie du monde de l'eau

De son prélèvement à son utilisation, en passant par son traitement et transport, le cycle de l'eau est tout sauf un long fleuve tranquille. Plongée dans une liste non-exhaustive des acteurs de l'industrie de l'eau.

Le réseau d'eau potable

Prélèvement de l'eau brute
(nappes souterraines, plans d'eau, cours d'eau)

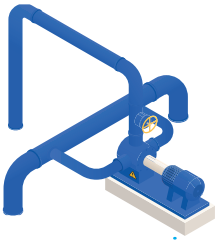




Potabilisation
(usines de production d'eau potable, usines de dessalement)

Stockage d'eau potable
(châteaux d'eau principalement)

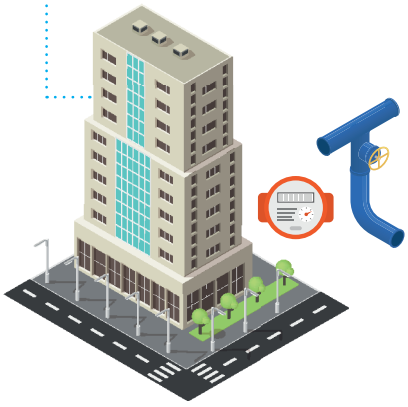




Distribution
via un réseau de canalisations

Les lieux de consommation ou d'utilisation

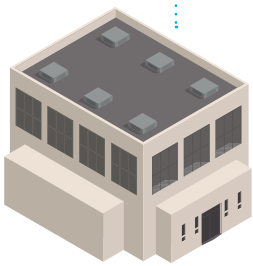
Les logements, les commerces et les entreprises





Les exploitations agricoles et les élevages

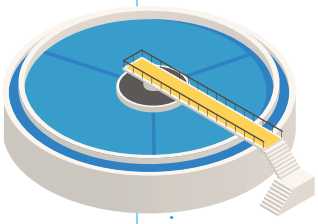
Les industries



Le réseau d'assainissement des eaux usées



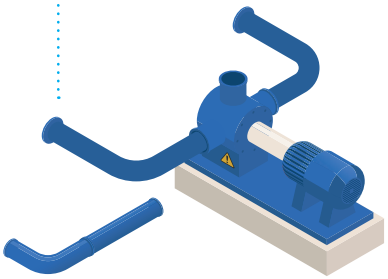
Collecte :
tout-à-l'égout pour les eaux usées domestiques



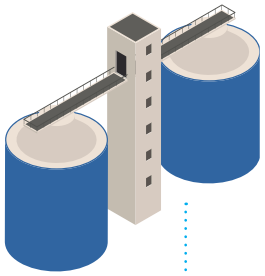
Traitement :
usines de retraitement des eaux

Station d'épuration ou stations de traitement des eaux urbaines avec bassins de traitement

Rejet :
systèmes d'évacuation de l'eau épurée

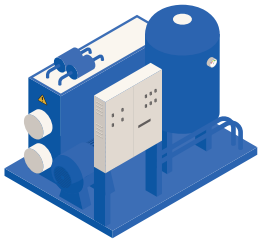


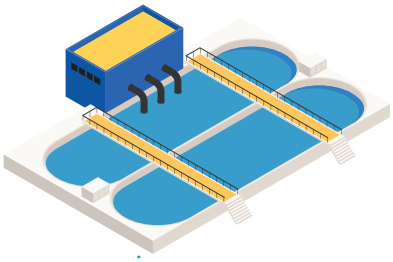
Le réseau d'eaux pluviales



Stations de pompage de défense contre les crues

Stations de pompage de relèvement des eaux de voirie

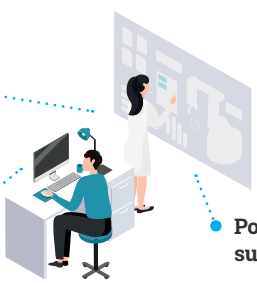




Bassins de rétention

Au sein d'infrastructures différentes, les systèmes d'information mélangent souvent quantité d'éléments hétéroclites.

Autant d'éléments qui représentent une surface d'attaque cyber conséquente.



Actifs fixes (postes de travail, serveurs, etc.)

Postes nomades

Poste central de supervision



Automates de télégestion

Capteurs communicants de l'IIoT (Internet des Objets Industriels)

Environnements cloud



Pourquoi l'industrie de l'eau doit-elle prendre le sujet cyber au sérieux ?

Partie I.

Entre santé publique, pollution et géopolitique, les enjeux de cybersécurité dans le secteur de l'eau sont particulièrement critiques. Pourtant, malgré la multiplicité des risques, engendrés notamment par la vétusté de ses réseaux, l'industrie peine à acquérir les réflexes de sécurité numérique.



Deux grands types d'acteurs exploitent les infrastructures de l'eau en France : des collectivités et des sociétés privées délégataires. Il est donc difficile de dresser un portrait homogène de la prise en compte de ces enjeux, et notamment sur les investissements en cybersécurité. Un point pourtant central quand plus de 3 vulnérabilités sur 5 dans le système d'information industriel peuvent conduire à l'indisponibilité totale de l'outil de production si elles sont correctement exploitées (source : rapport 2020 de Claroty).

Trop peu mis à jour et vieillissants, les systèmes opérationnels de l'industrie de l'eau présentent ainsi plus du double de vulnérabilités par rapport au domaine de la santé (d'après le même rapport de Claroty).

Mais rares sont les entreprises du secteur de l'eau à communiquer ouvertement sur les cyberattaques qu'elles déjouent ou dont elles sont victimes. Contrairement à d'autres industries comme le transport ou l'énergie, le secteur de l'eau commence tout juste à se fédérer pour échanger autour de ces enjeux de cybersécurité. On peut néanmoins citer le travail de veille du réseau Water ISAC, actif depuis 2002 aux États-Unis. En France, l'Association Scientifique et Technique pour l'Eau et l'Environnement (ASTEE) a initié un groupe de travail cybersécurité en 2021. L'objectif est de compléter le guide « Protection des installations d'eau potable » vis-à-vis des actes de malveillance, paru en 2017, qui n'abordait pas la question de la cybersécurité des systèmes d'information.

Pourtant, le secteur n'est pas épargné, comme l'a rappelé le cas d'une réserve d'eau floridienne en février 2021. Très médiatisée, la cyberattaque déjouée dans la petite ville d'Oldsmar démontre le manque de sécurisation d'un certain nombre d'infrastructures de l'eau : le cyber-criminel a pu exploiter un logiciel de prise de main à distance trop peu sécurisé (TeamViewer) et modifier le

« Dans un monde de plus en plus connecté et contraint à des évolutions rapides par l'épidémie de Covid-19, un problème de cybersécurité peut vite engendrer un problème de sûreté, voire poser la question de la sécurité nationale dans certains cas extrêmes »

Khobeib Ben Boubaker
Head of Industrial Security Business Line Stormshield

paramétrage en hydroxyde de sodium, utilisé pour réguler le pH dans le réseau de traitement des eaux. Heureusement pour les 15 000 habitants d'Oldsmar, un agent de la station a rapidement détecté l'anomalie (11 100 parties par million au lieu de 100) et corrigé la concentration. Même si les dispositifs ancrés dans ces environnements pour garantir la sûreté de fonctionnement peuvent agir comme des garde-fous, l'historique des cyberattaques contre l'univers de l'eau nous montrent que les cyber-criminels savent les contourner.

Si, historiquement et culturellement, **la sûreté des personnes a toujours primé sur la sécurité informatique** dans le secteur de l'eau, les deux sujets tendent aujourd'hui à se rejoindre. **La particularité de la cybermenace dans le monde de l'eau** tient aux motivations des cyber-attaquants. Peu lucratif, ce secteur sensible est en effet rarement ciblé pour le profit. Il peut cependant être ciblé pour des coups médiatiques, comme ce fut le cas en janvier 2021 en Californie : un cybercriminel a réussi à effacer certains programmes utilisés par une usine dans le processus de traitement de l'eau potable dans la baie de San Francisco.

Mais attaquer les infrastructures d'eau d'une région reste avant tout un important outil de déstabilisation réel qui peut être utilisé à des fins politiques, comme nous le verrons dans la partie suivante.—

Vers des (cyber) guerres de l'eau ?

Partie II.

Parce qu'elle constitue une ressource vitale, l'eau a toujours occupé une place stratégique dans les relations internationales. Une dimension géopolitique renforcée par le changement climatique à l'œuvre, qui transforme l'or bleu en une ressource toujours plus précieuse.



À l'heure où les systèmes d'approvisionnement et de traitement de l'eau sont pour la plupart connectés à d'autres réseaux, informatiques cette fois, leur vulnérabilité s'accroit. En France, cela explique que certaines infrastructures du secteur revêtent le statut d'OIV et doivent se conformer à des obligations règlementaires strictes. Au niveau européen, la directive NIS désigne également des opérateurs de services essentiels (OSE) parmi les acteurs de l'industrie de l'eau.

La cybersécurité dans le secteur de l'eau est donc particulièrement critique, puisqu'elle contribue à la sécurité d'une activité nécessaire à la survie et la santé des populations. Sa maîtrise est également gage de l'indépendance d'un pays.—

L'exemple d'Israël et les 3 vagues d'attaques en un an

Le contexte géopolitique et géographique d'Israël exacerbe les enjeux autour de l'eau. Cette situation l'a conduit à miser, comme les pays du Golfe, sur la technologie. Ainsi, 80 % de l'eau potable consommée en Israël provient d'usines de dessalement.

En mars 2020, Israël a déjoué une série de cyberattaques visant à prendre la main sur les systèmes de contrôle industriel de plusieurs de ses installations hydrauliques. L'objectif de ces attaques aurait été d'augmenter les niveaux de chlore dans l'eau (afin de la rendre dangereuse pour la consommation) et de déclencher la fermeture automatique des pompes. Plusieurs milliers d'habitants auraient ainsi été privés d'accès à l'eau pendant une période de forte chaleur. Le gouvernement israélien tiendrait l'Iran pour responsable et aurait mené à son tour une cyberattaque contre le port iranien de Shahid Rajaee en représailles.

Deux mois plus tard, ce sont des pompes à eau agricoles qui ont été visées par une seconde vague d'attaques, sans dommage. Enfin, en décembre 2020, c'est dans un réservoir d'eau que des cyber-attaquants ont réussi à s'introduire en exploitant une Interface Homme-Machine (IHM) mal sécurisée.

Ces exemples israéliens montrent combien les cyberattaques font aujourd'hui partie intégrante de l'arsenal des États dans le cadre de conflits plus ou moins ouverts ou de démarches de renseignement. Dans un autre domaine, la Russie et la Chine ont ainsi été pointées du doigt récemment à la suite des cyberattaques dont l'Agence européenne des médicaments (EMA) a été victime en 2020.—



Le secteur de l'eau est-il prêt pour la cyberguerre?

De manière générale, l'industrie de l'eau présente un niveau de cyber-protection hétéroclite. Si certains opérateurs ont intégré depuis plusieurs années des mentions de cybersécurité dans leurs appels d'offres, le risque cyber est encore peu pris en compte au niveau des collectivités. Ce qui explique en partie comment des attaques relativement basiques peuvent parfois infecter des systèmes industriels. Néanmoins, toute l'industrie de l'eau semble aujourd'hui résolue à rattraper son retard sur d'autres secteurs comme l'énergie ou la banque, sensibilisés avant elle.

« *En France, depuis l'adoption de la Loi de programmation militaire et de la directive européenne NIS, les ministères et l'ANSSI ont beaucoup sensibilisé les collectivités et les entreprises concernées à cette question*, explique David Giorgis, Responsable Sécurité IT et OT Région France et Responsable de l'informatique industrielle chez Suez France. *Auparavant, la cybersécurité était évoquée très succinctement dans les appels d'offres rédigés par les collectivités sauf exception. Aujourd'hui, le sujet occupe souvent plusieurs pages, avec des attentes de réponses étayées. C'est le signe d'une prise de conscience et d'une montée en compétence rassurante pour l'avenir* ».—

Entretien client

Point de vue : la cybersécurité, un réflexe en cours d'acquisition dans l'industrie de l'eau

Responsable Sécurité IT et OT et Responsable de l'informatique industrielle chez Suez France, David Giorgis est aux premières loges pour observer les évolutions de l'industrie de l'eau. Nous avons pu lui poser quelques questions et plonger avec lui sous la surface de la cybersécurité du secteur.

David Giorgis — « *Environ 90 % des cyber-incidents que nous observons concernent l'informatique de gestion, c'est-à-dire la bureautique, les postes de travail, la messagerie, les applications. Il faut dire que les données de millions de clients directs sont présentes dans notre CRM et que notre SI doit être accessible pour le suivi de consommation entre autres. Ce sont autant d'actifs à sécuriser, qui s'ajoutent aux vulnérabilités classiques autour des messageries par exemple.*

Heureusement, du côté des projets informatiques chez Suez, l'approche security by design est devenue systématique. Sur des projets purement industriels, le réflexe n'était pas encore installé partout, car ils sont souvent gérés localement et la cybersécurité progresse pour devenir partie intégrante de la culture. Cela signifie que ces projets OT sont de plus en plus sécurisés. C'est pourquoi Suez met en place une démarche globale de cybersécurité pour obtenir un maximum de performance opérationnelle. La difficulté que l'on rencontre, quand on s'attèle à cyber-sécuriser des systèmes opérationnels, se situe bien souvent au niveau des protocoles industriels. Certains grands fabricants ont en effet apporté des spécificités aux protocoles standards et les outils de sécurité s'améliorent pour les comprendre. L'analyse est donc limitée, le temps que l'éditeur de solutions de cybersécurité développe un module spécifique.

D'où l'importance pour les acteurs du secteur de travailler ensemble. »

Dans le cadre de ses fonctions, David Giorgis intervient régulièrement auprès des collectivités clientes de Suez France. Nous lui avons demandé quelles étaient les recommandations le plus souvent émises dans le champ de la cybersécurité industrielle de l'eau :

DG — « *Une nouvelle collaboration commence toujours par une analyse de l'existant pour s'assurer que les informations dont on dispose correspondent à la réalité. À partir de là, on entame généralement une phase de négociation visant à renouveler le matériel obsolète et à mettre à jour les équipements en place. En réalité, l'objectif est d'être "le plus à jour possible" : nous sommes parfois obligés de rester sur d'anciens systèmes d'exploitation, car les applications métier ne sont pas compatibles avec les versions les plus récentes de ces OS.*

L'autre grand axe d'amélioration consiste à segmenter le réseau opérationnel. Cela représente un gros travail. Il faut également bien séparer SI industriel et SI de gestion, c'est une règle importante pour Suez ou en cas d'exception, veiller à sécuriser les points de connexion entre les deux. Cela passe par le déploiement d'un socle de base de sécurité (antivirus, mise à jour, firewall, etc.). Ce sont des actions très classiques pour le monde de l'informatique de gestion, mais encore nouvelles pour le secteur industriel en général et de l'eau en particulier. »

Devant l'ampleur de la tâche, la question du ressenti des équipes sur le terrain se pose : perçoivent-elles généralement la cybersécurité comme un frein à leurs projets ?

DG — « *On parle beaucoup plus ces dernières années des enjeux de cybersécurité donc globalement, les équipes industrielles sont très conscientes de son importance. J'ajouterais que le rôle du responsable de la sécurité des systèmes d'information n'est pas de stopper un projet, mais bien de l'accompagner pour qu'il intègre telles et telles conditions de sécurité. Notre philosophie consiste à orienter les informaticiens industriels sur place vers des solutions packagées complètes, sécurisées et nationales. Nos équipes centrales et notre filiale Suez Smart Solutions, spécialisée dans les systèmes industriels et leur cybersécurité, sont également à leur disposition pour les aider dans la mise en œuvre de ces solutions.* »—

Une approche pragmatique et collaborative qui souhaite à terme positionner la cybersécurité comme une véritable fonction support dans le quotidien des équipes opérationnelles.

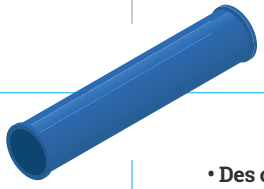
Quelles sont les problématiques qui agitent la cybersécurité de l'industrie de l'eau ?

Partie III.

Au-delà des motivations étatiques ou criminelles, qu'est-ce qui fait de l'industrie de l'eau une cible privilégiée des cyber-attaquants ? Nous avons listé les principales problématiques cyber du secteur selon trois perspectives : humaine, technologique et opérationnelle.



En préambule, il convient de préciser que dans le monde de l'eau, la cybersécurité vise essentiellement à garantir la disponibilité et l'intégrité des processus industriels. La notion de confidentialité est également mobilisée, mais dans le cadre moins critique de la relation client : l'intégrité de la donnée est d'une très grande importance dans le contexte de la télémétrie pour garantir la justesse de la facturation, mais les enjeux sont sans commune mesure avec le fait de garantir l'approvisionnement en eau potable par exemple.



Perspective humaine

• D'importants risques humains inhérents au secteur
Comme nous l'avons détaillé dans la partie précédente, l'approvisionnement en eau potable et le traitement des eaux usées constituent des activités critiques, car nécessaires à la survie des populations et à leur santé. Les conséquences d'une rupture de barrage ou d'une contamination des eaux seraient en effet dramatiques.

• Des risques d'erreurs ou d'actes malveillants
Pour ces raisons, la composante humaine, qu'elle soit le résultat d'une erreur ou d'un acte malveillant volontaire, est une des composantes les plus redoutées par les métiers et opérateurs industriels. Et conduit à imaginer différents scénarios pour une sureté de fonctionnement optimale.

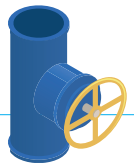
• Des collaborations parfois complexes
D'un point de vue métier, la gestion coordonnée de la cybersécurité informatique et opérationnelle suppose d'arriver à répondre au besoin de l'automaticien tout en réduisant les risques identifiés par le RSSI ou responsable de la sécurité informatique.

Sur le plan organisationnel, il arrive souvent que plusieurs acteurs travaillent en délégation pour une même métropole par exemple. Celle-ci peut elle-même avoir conservé une partie de la gestion en interne. C'est alors un véritable écosystème de gestion de l'eau qui doit apprendre à travailler ensemble.

• Une cybersécurité industrielle souvent hors périmètre
Comme dans d'autres industries, il est courant que les équipes en charge de la cybersécurité opérationnelle soient placées sous la responsabilité du directeur ou de la directrice d'usine plutôt que dans le périmètre du responsable informatique de la collectivité. Dans certains autres cas, le responsable informatique préconisera des règles cyber que l'exploitant du service sera libre d'appliquer. Ou pas…

> ***« Les réseaux industriels sont parfois négligés lors de l'évaluation des risques de cybersécurité ou de la récupération après une cyberattaque »***

Tarik Zeroual
Global Account Manager Stormshield



Perspective technologique

• Une frontière floue entre cybersécurité informatique et industrielle

Avec la fin du RTC (Réseau de Téléphonie Commuté), l'industrie de l'eau migre progressivement vers des technologies de communication comme Ethernet, la 4G, voire la 5G. Cette évolution s'inscrit dans une tendance globale ces dernières années de convergence entre IT et OT. Les réseaux industriels sont donc plus exposés qu'avant car ils sont entrés dans le périmètre d'une potentielle cyberattaque via le réseau informatique.

• Un Internet des Objets Industriels (IIoT) à sécuriser

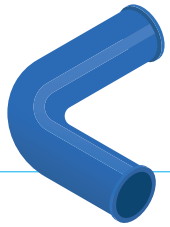
L'IIoT désigne tout objet connecté qui envoie une information (température, vanne ouverte, taux de chlore, etc.) à une machine. Relativement peu chers, ces capteurs « intelligents » s'intègrent très facilement aux systèmes existants, ce qui explique leur succès dans les milieux industriels. Malheureusement, ils sont aussi très vulnérables car la cybersécurité est encore trop rarement prise en compte au moment de leur conception.

• Une protection à étendre aux environnements virtuels

Avec l'adoption du cloud, notamment alimenté en données par l'IIoT, et le recours aux machines virtuelles, toute une partie du SI des entreprises de l'eau a été déportée. Il faut donc sécuriser ces liaisons cloud pour éviter les cyberattaques par rebond sur l'infrastructure des sites industriels. À condition de bien identifier à qui incombe cette responsabilité, entre métiers et services managés.

> ***« La maintenance prédictive est l'une des principales applications opérationnelles de l'IIoT. Les données remontées par les capteurs servent à des calculs de prédiction qui permettent d'éliminer la maintenance inutile et de réduire les probabilités de panne »***

Tarik Zeroual
Global Account Manager Stormshield



Perspective opérationnelle

• De fortes disparités de maturité
En Europe, la prise en compte de la cybersécurité des infrastructures de l'eau est très variable selon le degré de sensibilisation et les ressources de la collectivité en charge du sujet.

• Le multisite au cœur de la complexité cyber du secteur
Dans la pratique, cybersécuriser les infrastructures critiques de l'eau n'est pas chose aisée, car il s'agit d'un secteur très décentralisé et contraint au multisite pour alimenter l'ensemble du territoire. Entre connexions internet et télémaintenance, il existe donc de forts enjeux autour des accès à distance qui permettent de s'assurer du bon fonctionnement des sites éloignés.

• Une mise en œuvre cyber difficile sur le terrain
Du fait de leur répartition éclatée, certaines infrastructures de l'industrie de l'eau présentent des contraintes spécifiques, d'humidité ou de température par exemple.

• Des équipements de production sensibles
Il n'est pas rare de constater qu'un automate en exploitation dans une station d'épuration a déjà 10, 15 voire 20 ans. Ces équipements vieillissants disposent rarement de mécanismes de cyber-protection intégrés et utilisent des protocoles industriels peu sécurisés et sont donc vulnérables.

• Une architecture réseau perméable
Ces systèmes sont encore trop souvent organisés selon une architecture réseau « à plat », c'est-à-dire sans cloisonnement ou segmentation. Un vrai danger face à la propagation des malwares.

• Une contrainte du temps réel
La sensibilité de ces équipements tient également à la contrainte opérationnelle du temps réel. Dans l'industrie de l'eau, il est primordial de déclencher chaque opération instantanément et donc de réduire au minimum le délai entre l'instruction et l'action. Les équipements de sécurité doivent donc engendrer le moins de latence possible pour ne pas perturber le processus industriel. Cela pourrait en effet aboutir à un arrêt de la production.

• Une multiplicité d'acteurs qui peut brouiller la visibilité
L'ancienneté de la plupart des systèmes industriels de l'eau implique que l'exploitant actuel ne maîtrise pas toujours l'historique des modifications. Le recours à de nombreux prestataires, opérateurs ou intégrateurs contribue également à accentuer le phénomène.

> ***« Ces réseaux distribués sont également plus exposés aux intrusions physiques. Cela implique de penser la cybersécurité différemment. Cet enjeu autour de la sûreté rajoute de la complexité dans la démarche de cybersécurisation d'une station d'épuration ou d'un château d'eau »***

Vincent Nicaise
Industrial Partnership and Ecosystem Manager Stormshield

Infographie

Les principales vulnérabilités du secteur

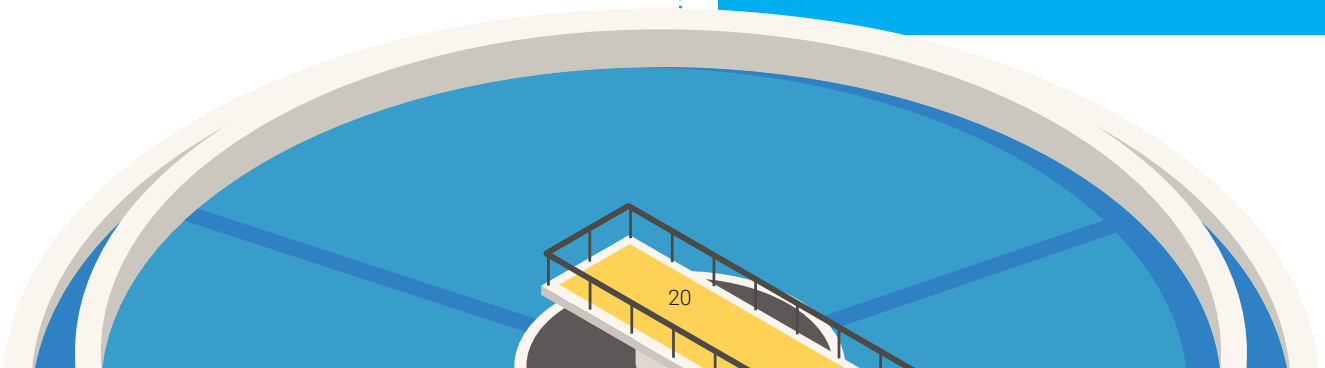
Ces dernières années, l'inquiétude des professionnels de la cybersécurité porte en particulier sur le déploiement de «l'Internet industriel des Objets» (IIoT). Pour autant, il ne doit pas faire oublier un certain nombre de vulnérabilités structurelles présentes dans ces systèmes industriels.

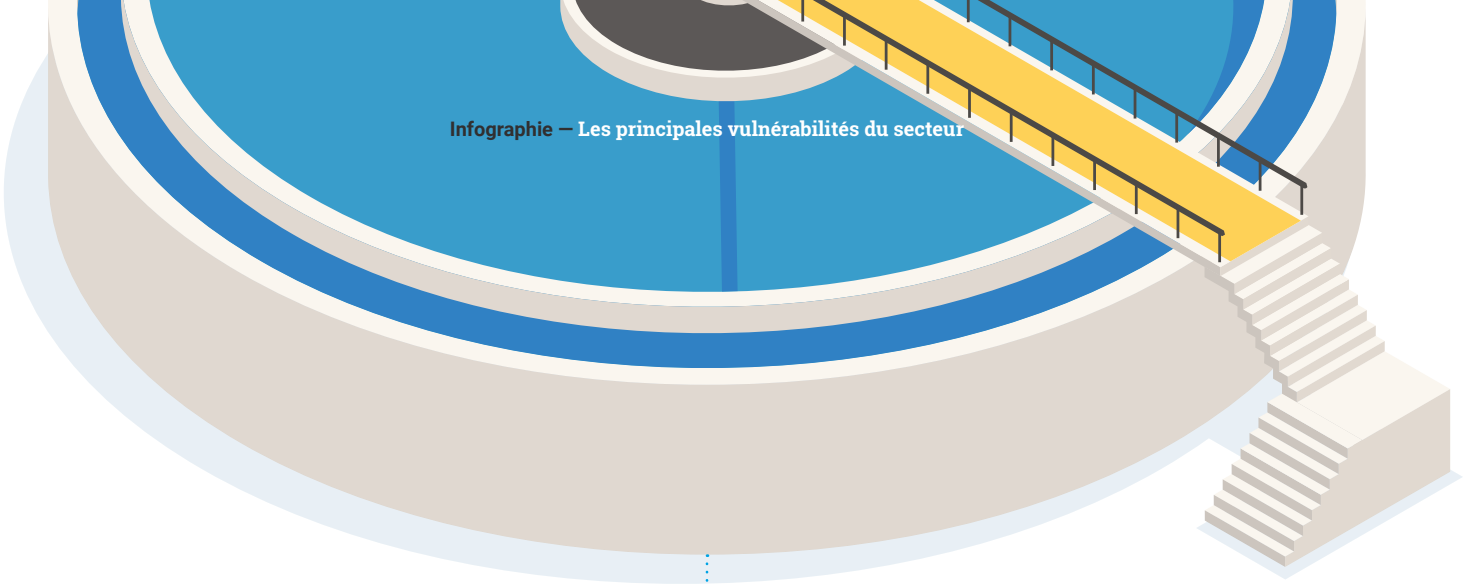
Les systèmes industriels dans leur ensemble (ICS pour *Industrial Control Systems*) peuvent présenter des vulnérabilités aux niveaux :

Des équipements opérationnels (software, hardware et firmware)

aux technologies disparates, vieillissantes et/ou peu sécurisées. Parmi eux figurent ainsi pêle-mêle le système de contrôle du processus industriel (DCS pour *Distributed Control System*), les interfaces homme-machine (IHM), les automates programmables industriels (PLC pour *Programmable Logic Controllers*), les solutions de contrôle et d'acquisition de données SCADA et autres logiciels de supervision, ou encore les capteurs IIoT et plateformes cloud avec lesquels ils communiquent. L'ensemble formant une surface d'attaque considérable.

En février 2020, une vulnérabilité a été découverte dans les IHM C-more du fabricant américain AutomationDirect. Ceux-ci sont utilisés entre autres par des opérateurs de l'industrie de l'eau. En exploitant cette faille (CVE-2020-6969), les cybercriminels pourraient découvrir des identifiants et d'autres informations sensibles dans les fichiers projet non protégés.—





Infographie — Les principales vulnérabilités du secteur

Du réseau et de ses périphériques

Bien souvent conçus en architecture « à plat », les réseaux industriels ne sont pas toujours isolés les uns des autres, selon les principes de la segmentation. En plus d'être un terreau fertile à la propagation de malwares, les équipements réseau comptent chaque jour de nouvelles vulnérabilités – car obsolètes et peu mis à jour. Des vulnérabilités qui peuvent également venir de la télégestion, qui se fait encore trop souvent de manière non sécurisée.

Des systèmes d'exploitation des postes de supervision ou de programmation

Déconnectés, ces systèmes sont rendus obsolètes d'un point de vue cyber par manque de mise à jour. Mais ces systèmes d'exploitation s'avèrent dans le même temps être les seuls à faire fonctionner correctement certaines applications métiers historiques, incompatibles avec des systèmes plus récents.

Des protocoles

Le recours à des protocoles en clair et peu sécurisés, comme Modbus, est courant en supervision industrielle.

Des utilisateurs

Les opérateurs et mainteneurs en charge du processus industriel ne sont pas tous encore très sensibilisés aux questions de cybersécurité. Les politiques d'utilisateurs, de mots de passe ou encore de gestion d'accès sont ainsi des éléments trop rarement déployés auprès des systèmes industriels.–

Quelles règlementations cyber autour de l'industrie de l'eau ?

Partie IV.

En plus de son encadrement strict sur le plan sanitaire et environnemental, le secteur de l'eau fait l'objet de réglementations nationales et internationales sur le plan cyber.



« Avec la mise en œuvre des décrets en 2016, on a commencé à voir une accélération cyber du côté des opérateurs. Côté collectivités, cela a demandé un peu plus de temps et on a vu de premières évolutions sur le sujet entre 2017 et 2018 »

Khobeib Ben Boubaker
Head of Industrial Security Business
Line Stormshield

En plus de son encadrement strict sur le plan sanitaire et environnemental, le secteur de l'eau fait l'objet de réglementations nationales et internationales sur le plan cyber.

Au vu des enjeux de santé publique décrits précédemment, on comprend aisément que l'activité de certains acteurs du secteur soit considérée comme critique. En France, les acteurs en charge de l'approvisionnement et de la distribution en eau potable disposent du statut d'OIV (Opérateurs d'Importance Vitale) au sens de la Loi de programmation militaire (LPM) française (2013). Ils doivent donc se conformer aux 20 règles que fixe la LPM pour les SI les plus critiques : cartographie des SI, veille, règles d'identification et d'authentification, notification des incidents, recours à des solutions de sécurité qualifiées au plus haut niveau, etc.

Au niveau européen, ils peuvent également être identifiés comme des OSE (Opérateurs de Services Essentiels) selon la directive NIS (2016). La France avait pris un peu d'avance lors de sa transposition dans le droit national pour y inclure les acteurs de l'assainissement : une harmonisation européenne est en vue, puisque ce secteur devrait être intégré au texte de la directive lors de sa révision prévue pour la fin d'année 2021, au même titre que la gestion des déchets.

Enfin, certaines structures, souvent de petites collectivités, ne sont considérées ni comme des OIV ni comme des OSE : sans obligation règlementaire, elles procèdent donc en fonction de leurs moyens et de leur niveau de conscience de la menace. Pour les aider, l'ANSSI a publié plusieurs guides de bonnes pratiques, permettant l'autoévaluation et l'autosécurisation. Et pour celles qui souhaitent aller encore plus loin, de nombreux standards existent – parmi lesquels la norme internationale de cybersécurité industrielle IEC 62443-3-3 ou le référentiel américain NIST.—

Et demain ?

Partie V.

Le numérique est un levier majeur de la défense de l'eau : prélever seulement le nécessaire, optimiser l'empreinte environnementale des usines, ou assurer l'acheminement d'une eau de qualité sans fuite sont autant de défis qui vont s'accentuer dans les prochaines années.



Pour optimiser les forages et le fonctionnement des pompes grâce au machine learning, capter des signaux faibles annonciateurs de sécheresse ou encore prédire les flux, le secteur de l'eau intègre toujours plus de technologies.

Avec la poursuite de la numérisation de la filière, la frontière entre IT et OT va continuer à s'effacer, renforçant le risque cyber auquel le secteur est déjà exposé. L'industrie de l'eau doit donc impérativement rehausser son niveau de cybersécurité et organiser sa cyber-résilience, pour faire face à des attaques qui seront de plus en plus fréquentes et virulentes.

Un public pleinement sensibilisé et une règlementation renforcée

À l'avenir, la cybersécurité doit donc faire partie intégrante du maintien du process industriel. Cela représente un chantier conséquent, quasiment tout l'existant devant être sécurisé. Mais on observe des signaux encourageants.

« Les intégrateurs automaticiens adressent de plus en plus les enjeux de sécurité des systèmes industriels. Il faut aussi saluer le nombre d'appels d'offres de conception ou de rénovation de systèmes qui intègrent dorénavant un volet cyber »

Vincent Nicaise
Industrial Partnership and
Ecosystem Manager Stormshield

Pour accompagner ce processus, la tendance des prochaines années sera au renforcement du cadre règlementaire en matière de cybersécurité, d'après David Giorgis. Pour le Responsable Sécurité IT et OT et Responsable de l'informatique industrielle de Suez France, la prochaine révision de la directive NIS constitue une première étape qui sera suivie par de nombreuses précisions apportées, entre autres, à la Loi de programmation militaire. La coopération transfrontalière devrait figurer parmi les axes forts de ces nouvelles règlementations dont l'ambition est, selon l'ANSSI, de « *renforcer la cyber résilience de l'Union européenne et de ses membres* ».

C'est donc prendre un temps d'avance que de suivre le conseil de Tarik Zeroual, Global Account Manager, Stormshield, qui incite dès maintenant à « *aller au-delà de la conformité a minima* ».

Des solutions technologiques éprouvées

Le futur de l'industrie de l'eau sera immanquablement teinté de menaces cyber, mais les éditeurs et les chercheurs en cybersécurité sont à pied d'œuvre pour proposer des solutions adaptées aux problématiques récurrentes comme émergentes.

• Protéger les réseaux par la segmentation
La segmentation des réseaux est primordiale, car elle permet d'éviter la propagation d'une cyberattaque en isolant les sous-systèmes. Des firewalls comme ceux de la gamme Stormshield Network Security (SNS) peuvent être utilisés à cet effet.

• Valider le trafic
Il est également important de disposer de solutions capables de vérifier la légitimité des commandes réalisées par les automates. « *Il s'agit de se prémunir d'attaques man-in-the-middle, mais*

aussi de vérifier l'intégrité des données via leur inspection », indique Stéphane Prévost, Product Marketing Manager Stormshield.

• Gérer les accès à distance

Dans un secteur aux infrastructures parfois très éloignées les unes des autres, il est impératif de mettre en place des systèmes permettant de gérer et de sécuriser les accès distants (télémaintenance, gestion d'alarmes, etc.). Pour garantir des communications sécurisées entre les différents sites et les différentes machines, la solution SNS prévoit le chiffrement des données grâce à la création de tunnels VPN et l'authentification des utilisateurs.

• Acquérir une vue d'ensemble

Pour faciliter la gestion de multiples solutions SNS distribuées, Stormshield a développé une plateforme de management centralisé baptisée Stormshield Management Center (SMC). Stormshield propose également une solution de log management, Stormshield Log Supervisor (SLS), qui offre une meilleure visibilité sur l'état et les journaux des réseaux informatiques. Des solutions qui permettent également de prendre en compte l'augmentation de trafic entre l'IT et l'OT, grâce à une politique de sécurité unifiée entre les deux mondes.

• Protéger les postes

La protection des terminaux est essentielle, que ce soient les postes d'ingénierie ou les postes de supervision, car ce sont eux qui pilotent les paramètres du processus opérationnel et qui permettent d'obtenir une vue en temps réel de l'état des systèmes. Une cyberattaque sur les postes de supervision rendrait par exemple les équipes opérationnelles complètement « aveugles » et empêcherait la bonne conduite des processus industriels. C'est pourquoi la solution Stormshield Endpoint Security (SES) combine un moteur d'analyse comportementale, un moteur de contrôle des périphériques et une capacité à effectuer un whitelisting d'applications, rendant inactive tout logiciel qui n'est pas strictement nécessaire, pour une meilleure protection. Et pour une protection encore plus efficace, la solution SES permet de maintenir une sécurité proactive, même lorsque le poste n'est pas connecté à un réseau de gestion ou à Internet.

• Adapter les équipements aux contraintes de l'industrie de l'eau

L'industrie de l'eau possède un certain nombre de contraintes physiques, qui lui sont propres (la forte humidité, les larges plages de températures, l'isolement de certains sites, etc.) ainsi que des contraintes opérationnelles de continuité d'activité.

SNi40 et SNi20, les solutions de firewalls industriels

En collaboration avec Schneider Electric, Stormshield a conçu des boitiers renforcés pour répondre aux besoins des environnements à fortes contraintes comme l'industrie de l'eau. Optimisés pour de faibles latences induites et dotés d'une fonctionnalité bypass (mode sûreté favorisant le maintien en condition opérationnelle), ils peuvent être installés facilement au plus près des équipements à protéger et résister aux conditions particulières de cette industrie. Niveau réglementation, le SNi20 et le SNi40 ont obtenu tous les deux la qualification Standard de l'ANSSI. Un gage de robustesse et de confiance.—

Cette industrie requiert alors des équipements qui répondre à ces contraintes environnementales. Les capacités des firewalls SNS et leur fonctionnalité bypass (mode sûreté) sont également de véritables atouts pour l'industrie de l'eau, car ils garantissent la disponibilité du processus opérationnel.

• Tendre vers le *security by design*, même dans l'OT

L'approche *security by design* consiste à prendre en compte la cybersécurité dès la conception des systèmes. Une démarche plus pertinente et préférable dans l'industrie de l'eau face à une intégration *a posteriori* de mesures cyber. Car les temps de développement sont relativement longs, les problématiques de bases installées encore plus importantes qu'en bureautique et les défis techniques de compatibilité avec l'existant nombreux. Intégrateurs et experts ont donc bien conscience que le *security by design* est la clé d'une industrie mieux protégée à l'avenir.

De nouveaux profils au service de la cybersécurité du monde l'eau

Nous l'avons vu, garantir la cybersécurité dans le secteur de l'eau nécessite aujourd'hui de s'appuyer sur de plus en plus d'outils. De nombreuses compétences différentes sont donc nécessaires pour les appréhender, les comprendre et les exploiter au mieux.

Pour que les équipes de veille et d'intervention (CSIRT, SOC, etc.) disposent des meilleurs profils, il est donc important que les automaticiens se forment à la cybersécurité informatique. Et inversement, que les spécialistes en cybersécurité acquièrent une bonne connaissance du monde industriel.—

« C'est justement dans l'idée de faire en sorte que nos équipes se connaissent et travaillent mieux ensemble que nous organisons chaque année un exercice cyber dont le scénario intègre les systèmes industriels et auquel participent nos spécialistes OT »

David Giorgis
Responsable Sécurité IT et OT et Responsable de l'informatique industrielle chez Suez France.



Après celle de leurs systèmes, la convergence des équipes IT et OT est-elle lancée? L'avenir nous le dira, mais la cybersécurité du monde de l'eau dans les prochaines années semble bien dépendre de la capacité des experts industriels et cybersécurité à travailler ensemble pour la co-construction de solutions pertinentes.

Vous avez un sujet complexe de cybersécurité ? Un projet de sécurité autour d'une infrastructure ? Nos experts internes sont à votre disposition pour échanger et vous accompagner au mieux.
Contactez-nous.

Entretien client

La sécurisation d'un réseau distribué : comment optimiser la cybersécurité de la régie d'eau d'une métropole

La métropole d'une grande région française a choisi de confier la gestion du service public de production, de transport, de stockage et de distribution d'eau potable sur la majeure partie de son territoire à un interlocuteur unique, après plusieurs années à travailler avec trois opérateurs différents.

1,3 million d'habitants

60 communes

100 châteaux d'eau

Moderniser son infrastructure informatique et élever son niveau de sécurité

Cette rationalisation du service a également été l'occasion pour la métropole de revoir son architecture informatique pour la rendre plus moderne et plus sécurisée.

L'opérateur de référence sélectionné par le client a fait appel à Stormshield pour l'accompagner dans la sécurisation de cet environnement industriel et mettre en œuvre les principales fonctionnalités attendues, à savoir le contrôle et le filtrage de chaque communication (grâce à une inspection profonde des paquets – *Deep Packet Inspection*, DPI – et une attention particulière au protocole Modbus) et la mise en place d'une solution de VPN IPSec pour protéger les communications.

Des firewalls ont été mis en place pour segmenter et mieux protéger les différents réseaux opérationnels (réseau bureautique

IT, concentrateurs VPN centraux, informatique industrielle et de sûreté, ainsi que sites distants).

Une réponse industrielle adaptée aux contraintes de secteur de l'eau

La sécurité du site central a ainsi été renforcée par la mise en place de firewalls entre le réseau bureautique et les installations métiers. Ces installations sont réparties entre deux réseaux distincts (sûreté et industriel), chacun protégé par un cluster de firewalls destinés à assurer les fonctionnalités de concentrateur VPN.

Cette architecture permet d'interconnecter ces mêmes applications aux différents châteaux d'eau. Ceux-ci ont été équipés individuellement de deux clusters de firewalls durcis SNi40, pour sécuriser les flux entre les différents sites et les applications.

Le client a également été fortement séduit par de la fonctionnalité de Stateful DPI des protocoles industriels, qui permettra une évolution de la sécurité de ces systèmes sensibles, en parallèle de la modernisation des infrastructures.

Des services conçus pour ces environnements industriels complexes

Pour garantir le service aux usagers et répondre aux problématiques d'accessibilité et de sensibilité de certains sites, Stormshield et l'opérateur retenu ont déployé un accompagnement adapté, qui comprend :

- la mise en œuvre d'une procédure qui permet à un agent technique n'ayant pas de compétences réseau/sécurité de remplacer un firewall défaillant et de remettre le site en mode opération avec le bon niveau de sécurité,

- une activation d'une fonctionnalité bypass (mode sûreté favorisant le maintien en condition opérationnelle) pour les 5 % de sites équipés d'un seul pare-feu unique et non d'un cluster,

- une offre de services professionnels pour guider la métropole dans son process d'industrialisation de la configuration sur les premiers sites pilotes.—

Trois facteurs clés pour une réponse efficace

– Une forte implication du **binôme opérateur/éditeur**, qui permet de gérer le projet et son déploiement de bout en bout avec succès et dans les meilleurs délais.
– Une **offre industrielle Stormshield qui s'adapte** aussi bien à la gestion de sites standard qu'à celle d'environnements avec de fortes contraintes industrielles (température, humidité, rail DIN, alimentation industrielle, bypass).
– Un **seul et même firmware** déployé sur l'ensemble de la gamme Stormshield Network Security et une **console d'administration unique**, Stormshield Management Center, pour gérer l'ensemble du parc de firewalls.—

STORMSHIELD

Le choix européen de la cybersécurité



Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin de s'appuyer sur des partenaires de confiance pour accompagner leur transformation numérique et assurer la cybersécurité de leurs infrastructures, de leurs utilisateurs et de leurs données. Les technologies Stormshield, certifiées au plus haut niveau européen (EU Restreint, OTAN Restreint, Critères Communs EAL3+/EAL4+, qualifications et visas ANSSI), répondent aux enjeux de l'IT et de l'OT afin de protéger vos activités. **Nos solutions de sécurité vous redonnent la liberté d'entreprendre en toute sérénité.**

www.stormshield.com

Toute diffusion, reproduction ou représentation, même partielle de ce livre blanc, à d'autres fins qu'une utilisation privée sur un quelconque support, est interdite et pourrait engager la responsabilité civile et pénale de la personne qui ne respecterait pas cette interdiction.