Cybersécurité : une culture qui reste à acquérir dans le domaine de l'eau

Patrick Philipon, Technoscope

Depuis le 1er juillet 2016, certains opérateurs importants du monde de l'eau sont tenus de respecter les règles de cybersécurité édictées par la loi. Intégrateurs, fournisseurs d'instruments, d'outils de communication, de logiciels et exploitants doivent désormais se mettre en ordre de marche. Une culture nouvelle dont tous les opérateurs sans exception devraient commencer à s'inspirer…

ABSTRACT
Cybersecurity: a culture that is still to be acquired in the domain of water.
Since 1st July 2016, some of the major operators in the world of water management have been required to adhere to the cybersecurity rules enacted in law. Integrators, providers of instruments, communication tools, software and managers all now have to take the necessary measures. It is a new culture that all operators, with no exceptions, need to begin to build on…

Simple "jeu" de hacker, malveillance, sabotage, extorsion de fonds, déstabilisation étatique ou acte terroriste : les systèmes informatiques des entreprises et des collectivités sont régulièrement soumis à des "cyberattaques" plus ou moins graves. La dernière Loi de Programmation Militaire (LPM) consacre ainsi trois articles à la cybersécurité. Or, la gestion de l'eau figure parmi les douze secteurs d'activités d'importance vitale, déterminés par une liste officielle, concernés par la loi. Selon les termes officiels, l'atteinte de l'un de ces secteurs « *risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation* ».

« *Lorsque le législateur parle de gestion de l'eau, il s'agit évidemment de l'eau potable* », précise Sadio Bâ, coordinateur sectoriel pour l'eau à l'Agence nationale de sécurité des systèmes informatiques (ANSSI). Dans chacun de ces

Locken

Locken a développé une application qui permet à l'utilisateur de se connecter au logiciel d'administration pour récupérer ses droits d'accès. Ceux-ci sont alors transmis en temps réel à la clé grâce au module Bluetooth intégré dans cette dernière. Cela permet d'attribuer des droits d'accès pour une courte durée en fonction des besoins et contribue à renforcer la sécurité sur des sites vulnérables.

secteurs, un certain nombre d'opérateurs clés, dits 'Opérateurs d'importance vitale' (OIV) ont été identifiés. Leur liste, régulièrement remise à jour, n'est évidemment pas rendue publique. Ces OIV sont tenus de mettre leurs systèmes informatiques (SI) en conformité avec les exigences de l'ANSSI. Ou plus précisément, de déterminer parmi leurs SI ceux qu'ils considèrent comme d'importance vitale (ce sont donc des SIIV), d'en communiquer la liste à l'ANSSI et de les mettre en conformité avec les exigences de cette dernière. Ils doivent aussi notifier sans délai tout incident survenu sur l'un ou l'autre de leurs SIIV. Enfin, en cas de crise majeure, le Premier ministre, via l'ANSSI, peut imposer des mesures à prendre immédiatement. « *Cela peut consister, par exemple, à interrompre tous les accès à Internet* », explique Sadio Bâ.

Des règles et des délais à respecter

Après le décret d'application publié en 2015, l'arrêté sectoriel concernant le secteur de l'eau est paru le 1er juillet 2016. Il comprend vingt règles à appliquer. Dès lors, les OIV du secteur se sont mis en ordre de marche. D'autant que parmi les exigences de l'arrêté, figurent des requêtes urgentes : les exploitants ayant reçu la lettre leur indiquant qu'ils sont considérés comme des OIV avaient jusqu'au 1er octobre pour transmettre la liste de leurs SI IV, désigner un "référent LPM", autrement dit un interlocuteur privilégié pour l'ANSSI, ainsi qu'un point de contact utilisable à tout moment (H24J7). « *Lorsqu'une attaque grave a été repérée sur un OIV d'un secteur, tous les autres doivent pouvoir être prévenus immédiatement et réagir* » justifie Sadio Bâ. Les règles à appliquer et délais à respecter ont été co-construits, depuis près de deux ans, par des groupes de travail réunissant l'ANSSI, les prestataires, les fournisseurs (éditeurs de logiciels, fabricants de matériel) et les exploitants. Certains concernaient un secteur comme l'eau, d'autres des sujets plus transversaux comme par exemple les SCADA (Supervisory Control And Data Acquisition).

Bien évidemment, certains exploitants de réseaux d'eau potable n'ont pas attendu l'émergence des exigences réglementaires pour se préoccuper de la sécurité de leur système. Mais le monde de l'eau est-il prêt à ce changement de culture ? « *Le niveau de maturité, en termes de cybersécurité, est très variable selon les secteurs*, analyse Sadio Bâ. *Celui de l'eau, comme bien*

Codm

Panorama™ au Centre de télégestion de la Société des Eaux de Marseille gère à distance plus de 850 ouvrages hydrauliques, collecte et traite près de 95 000 informations recueillies en temps réel.

Certification, qualification : de quoi parle-t-on ?

En termes de cybersécurité, il existe des Critères Communs définis internationalement par les pays les plus avancés. Or, ils sont coûteux et difficiles à mettre en œuvre. C'est pourquoi l'ANSSI a souhaité définir de premiers objectifs atteignables dans des délais et à des coûts à la portée des industriels. Les prestataires, produits ou formations répondant à ces critères obtiennent une Certification de sécurité de premier niveau. Que l'on peut considérer comme une étape intermédiaire vers un niveau plus élevé à atteindre lorsque ce sera possible.

D.R.

L'ANSSI a également mis en place un processus plus long et plus approfondi : la qualification. Un prestataire ou un produit qualifié répond à une double exigence : d'une part la compétence (prestataire) ou la performance (produit), d'autre part la confiance. « *Nous imposons des interlocuteurs et produits qualifiés pour l'administration de l'État* », explique Sadio Bâ.

Il existe un troisième niveau encore plus élevé, réservé aux services régaliens : l'agrément. Le monde de l'eau n'est pas concerné.

Abloy propose une clé CLIQ™ Connect (BLE) permettant de mettre à jour les droits d'accès via smartphone ou d'obtenir des droits d'accès ponctuels en temps réel à l'arrivée sur un site distant.

Abloy

d'autres secteurs industriels, n'y était pas très investi. C'est tout-à-fait compréhensible. Il s'agit le plus souvent d'automaticiens habitués à opérer sur des SCADA, et non d'acteurs gérant essentiellement des données sensibles, comme les banques par exemple ».

Kim Cloutet, chargée de communication chez Codra, fournisseur de SCADA, note également que « *l'eau n'est pas forcément le secteur le plus avancé sur ce sujet. Nous avons eu des premiers contacts explicites sur ce thème il y a quelques mois avec un grand opérateur du domaine. Ce qui ne signifie pas qu'ils ne s'en sont pas préoccupés en interne* ».

« *Il n'y a pas de demande impérieuse des clients, sauf de la part de grands exploitants qui ont pris conscience des enjeux. C'est plutôt nous qui tirons le signal d'alarme* », confirme Benoît Quinquenel chez Lacroix-Sofrel. Yann Bourjault, responsable de la cybersécurité chez Schneider Electric, soutient quant à lui que le monde de l'eau s'est réveillé: « *dans beaucoup d'appels d'offres qui sortent en marché public, notamment en régie des eaux, il est maintenant demandé une assistance à maîtrise d'ouvrage en matière de cybersécurité* ».

Un point de vue partagé par Gilles Nguyen, Business Development Director chez ITMATION©. « *C'est pour ces raisons que nous proposons dans nos offres de services, un accompagnement global de la SSI avec un spécialiste de la cybersécurité, C-S. Cette offre intervient sur l'ensemble de la chaîne de valeur: conseil, intégration, services et solutions avec le SIEM PRELUDE (Security Information and Event Management) par exemple* ».

En milieu industriel, on cherche plus à protéger la disponibilité de l'installation de production que les données. Pour les attaquants, les cibles ne sont pas les mêmes que dans un classique système de gestion de données: il s'agit de rendre le système inopérant et de piller des contenus. Les stratégies de protection diffèrent donc également. De ce point de vue, le secteur de l'eau ne se distingue pas. Yann Bourjault souligne tout de même ce qu'il estime être une particularité: « *les opérateurs doivent souvent gérer des sites distants hébergeant des automates logés dans des armoires électriques simplement fermées à clés. Souvent sans dispositif de sécurité spécifique, ces sites distants sont plus exposés que les sites de contrôle* ». Dispositifs anti-intrusion et contrôle d'accès restent des points très sensibles sur les sites décentralisés. Les solutions existent cependant proposées par les spécialistes de la télégestion comme Lacroix-Sofrel, Aqualabo Contrôle, TLGPro ou Mios ou plus spécifiquement par des spécialistes comme Abloy ou Locken. Locken, a par exemple développé une application qui permet à l'utilisateur, en arrivant sur le site, se connecter au logiciel d'administration via son Smartphone pour récupérer ses droits d'accès. Ceux-ci sont alors transmis en temps réel à la clé grâce au module Bluetooth intégrée dans cette dernière. Cela permet d'attribuer des droits d'accès pour une durée très courte en fonction des besoins et contribue à renforcer la sécurité sur des sites vulnérables.

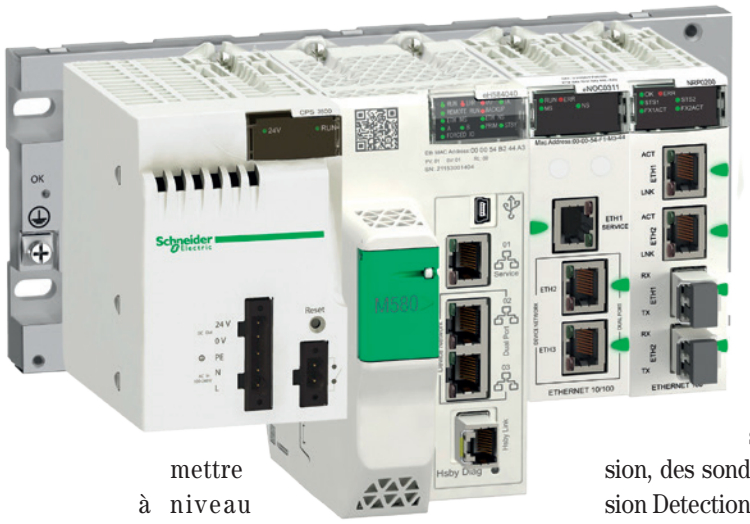
De son côté, Abloy propose également une clé CLIQ™ Connect (BLE) permettant de mettre à jour les droits d'accès via smartphone ou d'obtenir des droits d'accès ponctuels en temps réel à l'arrivée sur un site distant. Le système Protec² CLIQ™ se compose de cylindres, cadenas, serrures de meubles et contacteurs adaptés aux environnements les plus sévères (IP 68, ATEX,…), de clés électroniques transportant les droits, de boîtiers d'actualisation des droits et d'un logiciel d'administration centralisé CLIQ™ Web Manager accessible sur le réseau. Protec² CLIQ™ offre une solution sécurisée grâce à la résistance mécanique des cylindres à disques incrochetables certifiés EN1303, la gestion sur organigramme du parc de clés proposant une double variure mécanique et électronique et une communication cryptée AES conforme aux recommandations de l'ANSSI sur l'ensemble du système. La solution a par exemple été choisie par Eau

Areal

Areal est l'un des tout premiers éditeurs de supervision à répondre aux nouveaux usages et aux exigences de sécurité avec sa nouvelle version 6.0 de Topkapi un serveur web 100 % compatible Html 5.

de Valence. « *Ce qui nous a séduit dans le système Protec² CLIQ™ d'Abloy, c'est que toute l'énergie se situe dans la clé. Il n'y a pas d'alimentation de la serrure et donc très peu de maintenance. Par ailleurs, les cylindres électroniques et mécaniques sont gérés par une même et unique clé* », explique Christophe Nublat, Responsable du Pôle Etude & travaux à Eau de Valence.

Le Modicon M580 de Schneider Electric permet une gestion transparente des communications depuis le niveau entreprise jusqu'au niveau instrumentation. Il est doté de fonctions avancées de sécurité afin de faire face aux nouvelles menaces de cyber-attaques.



Schneider Electric

Les intégrateurs en première ligne

Pour comprendre les enjeux de la cybersécurité dans le domaine de l'eau potable, il est plus simple d'examiner ce que la loi attend de chaque catégorie d'acteurs. Les intégrateurs, à commencer par les grands tels Actemium, Apilog ou Schneider Electric tout d'abord. « *L'ANSSI ne peut pas tout faire seule. Il nous a fallu identifier des prestataires qui soient à la fois compétents et de confiance pour décupler notre action. Nous avons ainsi qualifié une vingtaine d'auditeurs. Quelques spécialistes de la détection d'incidents, ainsi que de la réponse sont en cours de qualification* » précise Sadio Bâ.

Début 2017, Schneider Electric est ainsi devenu le premier intégrateur conforme au référentiel ANSSI pour la sécurisation des installations industrielles. « *Aujourd'hui, des prestataires d'audit ont la qualification ANSSI mais ce qui intéresse nos clients n'est plus de savoir si leurs infrastructures sont vulnérables, mais de savoir comment les sécuriser* », pointe Yann Bourjault, responsable de la cybersécurité pour la France chez Schneider Electric. Il explique que son équipe s'attache à « *rencontrer les exploitants, leur expliquer la LPM et ses enjeux et en quoi ils sont assujettis à l'ensemble de ses impositions* ».

Deux situations se présentent alors. Parfois, le client nourrit un projet de modernisation, et il est alors possible de choisir des équipements "cybersûrs" par conception et de construire la meilleure architecture possible. Dans la plupart des cas, cependant, les exploitants ont installé il y 10, 15 ou 20 ans un parc qui fonctionne encore parfaitement. Tout naturellement, ils souhaitent se mettre à niveau du point de vue sécurité sans avoir à tout changer. Ce qui est généralement possible, sauf pour certains équipements trop anciens.

En collaboration avec Stormshield, la branche "cyber" du groupe Airbus, Schneider Electric a en particulier développé un pare-feu industriel appelé SNi40. Développé grâce à un investissement d'avenir sur la demande de l'ANSSI, c'est le premier pare-feu industriel qu'elle ait qualifié. Il peut s'installer sur un rail DIN, comme un automate. Il entre dans les protocoles industriels et autorise ou interdit le transit d'information entre automates. Il peut aussi fonctionner comme un VPN sur un site distant en filtrant les connexions à ce site. « *Il filtre très efficacement toute requête d'un assaillant, qu'elle soit faite localement ou à distance. Il est commercialisé depuis mai 2016. Nous l'intégrons très régulièrement, et notamment dans le monde de l'eau* » affirme Yann Bourjault. « *Il faut un certain nombre de formations et certifications pour installer ce produit, et aujourd'hui, sur la dimension industrielle, Schneider Electric est l'intégrateur de référence ayant toutes les qualifications requises* » ajoute-t-il.

De son côté, Ignition proposera dans sa prochaine version, des sondes au format IDMEF (Intrusion Detection Message Exchange Format, le format d'interopérabilité des SIEM). Associé aux fonctions existantes de sécurisation, comme la signature de tous les composants logiciels ou les zones de sécurités, Ignition disposera de tous les atouts pour une intégration efficace à l'ensemble de l'architecture de cyber sécurité.

Sur les sites centraux, les intégrateurs déploient des stratégies communes à tous les sites industriels, quel que soit le domaine. Un site opérationnel central peut être connecté un peu plus haut, vers l'informatique d'entreprise pour différents besoins (remontée, export, données, tendances, administration…). On applique alors un processus classique de protection périmétrique (des "clôtures" filtrant les entrées) et de défense en profondeur, ce qui signifie qu'on rajoute, à l'intérieur du domaine protégé par les "clôtures", des couches de sécurité en fonction de la criti-

Quand des hackers prennent le contrôle d'une station d'épuration….

Ne cherchez pas qui est la Kemuri Water Company (KWC), elle n'existe pas. Cette appellation générique a été inventée par l'opérateur américain Verizon pour éviter de compromettre cette importante station d'épuration située aux États-Unis qui, elle, est bien réelle, et a fait l'objet d'une cyberattaque en règle en 2015.


D.R.

Par simple jeu, des hackers se sont introduits dans le système de contrôle-commande de la station d'épuration et ont modifié les niveaux de dosage de différents produits chimiques utilisés pour le traitement de l'eau. L'intrusion a eu lieu depuis l'extérieur via une infrastructure informatique très ancienne, installée en 1988. Le serveur hacké gérait les automates programmables industriels (API) chargés de réguler les pompes doseuses et les vannes qui régulaient le débit de l'eau et des produits chimiques utilisés dans le cadre du traitement…

L'affaire a été révélée lorsque l'exploitant, qui avait constaté des modifications inexpliquées de dosage dans les produits injectés dans l'eau a décidé de faire appel aux équipes chargées du cyber-risque de Verizon pour renforcer son système d'information et anticiper tout problème éventuel. Le piratage durait depuis deux mois….

Cybersécurité : un cadre commun au sein de l'Union

Après 3 années de négociation, le Parlement européen et le Conseil de l'Union européenne ont adopté le 6 juillet 2016 la directive sur la sécurité des réseaux et des systèmes d'information connue sous l'appellation "directive NIS".

Cette nouvelle directive prévoit l'établissement de normes de cybersécurité communes et le renforcement de la coopération entre les pays de l'Union pour aider les entreprises à se protéger elles-mêmes et prévenir les attaques contre les infrastructures connectées des pays européens.

La nouvelle législation européenne prévoit des obligations en matière de sécurité et de suivi pour les "opérateurs de services essentiels" dans des secteurs tels que ceux de l'énergie, des transports, de la santé, des services bancaires et d'approvisionnement en eau potable.

Certains fournisseurs de services numériques - les marchés en ligne, les moteurs de recherche et les services d'informatique en nuage - devront prendre des mesures pour assurer la sécurité de leur infrastructure et devront signaler les incidents majeurs aux autorités nationales.

La transposition de la directive NIS en France sera assurée par l'ANSSI en lien avec l'ensemble des acteurs concernés.

cité des composants et de leur exposition.

Recenser tous les intervenants et tous les comportements

Outre le rôle de supervision propre à tout intégrateur, Schneider Electric a développé un certain nombre d'outils destinés à intervenir ponctuellement à différents niveaux d'un système informatique industriel. La détection des incidents fait partie des obligations énumérées par l'arrêté, qui exige même que les exploitants utilisent des sondes qualifiées (voir encadré), opérées par des intervenants eux-mêmes qualifiés. Schneider Electric développe ainsi une "sonde de surveillance automates", PLC-Diag. Placée au plus près des automates, elle les interroge régulièrement et envoie une alarme si elle détecte une modification de comportement par rapport à un relevé opéré il y a une heure ou la veille, par exemple. Elle est utilisable même sur des automates anciens, qui n'ont pas été conçus pour envoyer des alarmes. « *L'information transite, via des protocoles propriétaires, vers le site central qui pourra l'utiliser en disant par exemple « attention, cela fait trois cycles d'affilée que l'automate est chargé à 100 % alors que d'habitude sa charge moyenne est de 40 % ». Ce n'est pas forcément une cyberattaque mais un comportement anormal qui peut déclencher une intervention* » explique Yann Bourjault. Tout cela s'entend sur des automates Schneider Electric. « *D'autres acteurs de la détection d'intrusion travaillent avec tous les constructeurs, mais généralement leurs solutions sont passives : ce sera à l'équipement de remonter l'information. Nous, nous pouvons interroger de vieux automates Schneider Electric, muets, et les faire parler* ».

Autre problème courant dans le domaine de l'eau : un certain nombre d'opérateurs de maintenance peuvent intervenir sur site, avec leurs propres outils informatiques en général utilisés sur différents clients. « *Il existe une vraie problématique d'intégration de virus par les consoles de maintenance* » estime Yann Bourjault. Pour y faire face, Schneider Electric a développé la Cybertec, une console de maintenance sécurisée. Elle comporte l'ensemble des logiciels métier nécessaires, et uniquement ceux-là (programmation des automates par exemple). Il est impossible d'y implanter tout autre logiciel ou fichier. De même, l'opérateur de maintenance ne dispose que d'une clé USB, fournie par l'exploitant et où ne peuvent s'inscrire que des fichiers possédant l'extension correspondant aux besoins. « *Tout cela pour interdire tout détournement de la console de maintenance, car elle est placée au plus près du process, sur des sites distants, et on ne peut pas maîtriser cela* », souligne Yann Bourjault.

L'approche d'eWON, fabricant de routeurs industriels VPN, va dans ce sens. L'entreprise a choisi d'adopter une approche sécurité sous forme de couches, aussi appelée "Defense in Depth Approach" pour assurer l'intégrité et la confidentialité des informations transitant par ses modems et son Cloud "TALK2M". Cette approche est notamment basée sur les lignes de conduites et des bonnes pratiques dictées par des standards de sécurité tels que l'ISO 27002, IEC 62443-2-4 et NIST Cyber Security Framework 1.0. D'un point de vue fonctionnel, la solution eWON permet notamment une authentification au niveau des routeurs, une double authentification (SMS) et un renforcement des mots de passe au niveau de l'application, un historique des accès utilisateurs, des règles de firewall et de droits d'accès, un cryptage OpenVPN en utilisant le protocole SSL-TLS, le tout au travers de serveurs VPN hébergés sur des datacenters certifiés SOC 1, SOC 2/SSAE 16 and ISO 27001:2005.

eWON a choisi d'adopter une approche sécurité sous forme de couches, aussi appelée « Defense in Depth Approach » pour assurer l'intégrité et la confidentialité des informations transitant par ses modems et son Cloud « Talk2M ». Cette approche est notamment basée sur les lignes de conduites et des bonnes pratiques dictées par des standards de sécurité tels que l'ISO 27002, IEC 62443-2-4 et NIST Cyber Security Framework 1.0.

eWON

Lacroix-Sofrel

Avec le S4W, Lacroix-Sofrel, très en pointe sur le sujet, répond aux mesures de sécurité nécessaires à la cybersécurité des réseaux d'eau.

Fournir des logiciels et systèmes "durcis"

Les éditeurs d'outils de supervision tels Arc Informatique, Areal,

Le contrôleur PFC100 de Wago embarque son propre serveur Web pour des visualisations en HTML5. On peut en plus mettre en place des connexions VPN directement du contrôleur.

Wago

Codra, Wonderware, Prisma Instruments, Centreon, Elutions ou Technilog doivent à la fois "durcir" les logiciels déjà installés et concevoir une prochaine génération intégrant d'emblée les fonctions de sécurité.

« *Un des paradoxes sécuritaire auquel notre système SCADA doit faire face lors de l'élaboration et l'installation des applications chez nos clients, et où réside une des difficultés de l'exercice, est de fournir un système à la fois très "ouvert et connectable" afin que les applications puissent continuellement évoluer et pouvoir ajouter autant d'équipements divers et variés que nécessaire, tout en restant pour autant suffisamment "fermé" afin d'éviter les failles de sécurité*, explique Hervé Combe, Responsable R&D Supervision chez Elutions. *Le niveau de maturité dans le domaine de l'eau reste loin derrière celui du domaine bancaire avec des données sensibles ultra sécurisées, et ce malgré des risques sanitaires non négligeables (ex. menaces terroristes, contamination…)* ». Aussi, outre l'utilisation de LDAP pour une authentification forte des utilisateurs et de certificats Java et Verisign pour venir signer et exécuter le code "autorisé" ainsi que l'intégration possible d'appareils biométriques, Elutions préconise vivement à ses clients de mettre leur système de supervision sur un réseau isolé ne communiquant pas avec l'extérieur et travail de concert avec les équipes IT sur place pour assurer une architecture système fiable.

Technilog, en complément du durcissement de ses offres en matière de sécurité (certification, authentification des utilisateurs) a initialisé des développements permettant l'interopérabilité de ses solutions avec des produits tiers de cybersécurité, notamment la possibilité d'échanger avec des offres SIEM. Pour rappel, la mise en œuvre d'un SIEM permet de détecter au sein de tous les étages d'une infrastructure industrielle (Automates, routeurs, frontal de communication, SCADA), des comportements anormaux via la consolidation croisée d'un nombre colossal d'évènements. Technilog alimente ses référentiels de données et permet ainsi à des équipes spécialisées de détecter plus rapidement une attaque ciblée.

Conçue dès l'origine comme une plateforme d'entreprise full web, Ignition multiplie de son côté les fonctions de sécurité: multi-plate-forme (Linux, macOS, Windows), composants open source, communication entre les serveurs et les clients utilisant HTTPS, communication avec les équipements avec OPC-UA (TCP binaire avec encryption et authentification) ou MQTT (Message Queue Telemetry Transport), communication entre les serveurs via WebScockets et TLS (Transport Layer Security). Pour garantir la meilleure sécurité et une intégration simple entre OT et IT, il est possible de mettre en place des architectures réparties avec EdgeWareX. Par exemple, un protocole Modbus RTU ou TCP sera transformé dès l'armoire de contrôle en OPC-UA ou MQTT. Il en résulte des performances accrues (publish/subscribe vs polling) et une sécurité du meilleur niveau.

Actif dans tous les secteurs industriels, dont l'eau, Codra édite et commercialise, avec son outil Panorama, un ensemble de solutions logicielles dédié au monde de l'eau. Pour Kim Cloutet: « *tous les travaux que nous menons en termes de cybersécurité sont génériques: rien n'est spécifique au domaine de l'eau, mais tout y est utile* ». C'est pourquoi Codra a d'ores et déjà déterminé une roadmap des améliorations à apporter à Panorama pour obtenir rapidement une Certification de sécurité de premier niveau (CSPN, voir encadré), puis une éventuelle qualification. Sans attendre, les premières améliorations devraient apparaître dès cet été sur Panorama. Par exemple un protocole de surveillance de l'infrastructure (le fait que les machines soient présentes sur réseau, actives, quel est leur état, possibilité de les démarrer, arrêter etc.), sera renforcé. « *De manière générale, nous changeons la philosophie de Panorama, qui jusqu'ici était ouvert par défaut. Nous fermons désormais les portes* », explique Kim Cloutet. Par exemple, une interface permet-

Les API ciblés par les ransomwares ?

Le ransomware, de la famille des malwares, sévit en cryptant les codes de sa cible, la prenant ainsi en otage, avant de demander à son propriétaire une rançon en échange de la clé qui permettra à ce dernier d'en reprendre le contrôle.

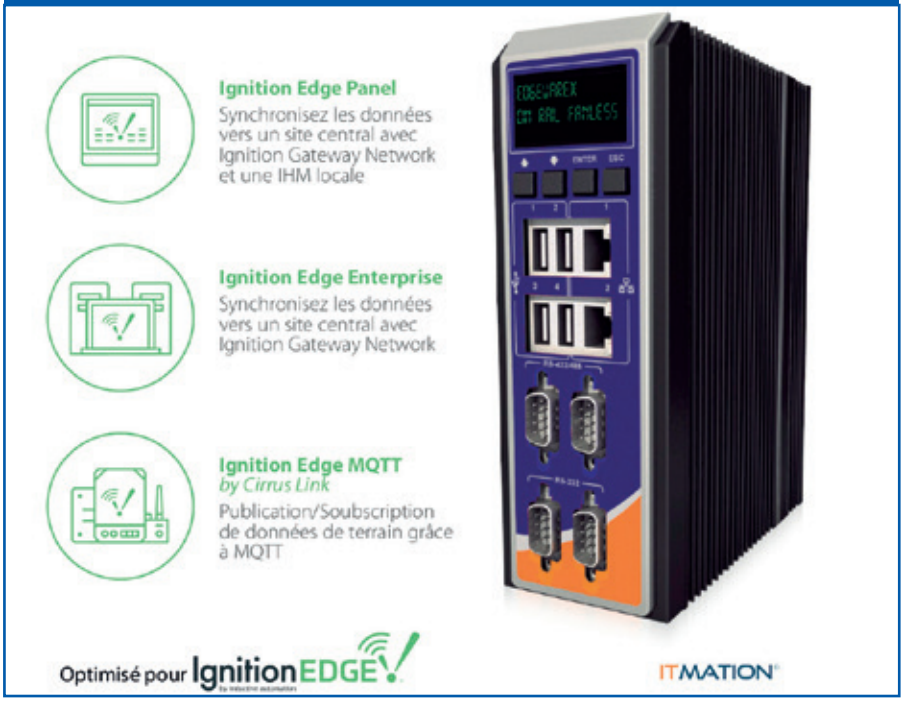
Georgia Institute of Technology

Une menace de plus en plus réelle si l'on en croit les chercheurs en sécurité du Georgia Institute of Technology qui viennent de prouver leurs dires en développant LogicLocker, un ransomware capable de s'attaquer à certains automates programmables industriels (API) en charge de la désinfection de l'eau, d'extraire leur code et de le remplacer par un code malveillant. LogicLocker serait également capable de modifier le mot de passe d'accès afin d'empêcher les ingénieurs de reprendre la main…

Pour l'heure, les attaques répertoriées à ce jour visant à détruire ou manipuler volontairement ou à des fins agressives un ouvrage de gestion de l'eau sont très peu nombreuses. Les chercheurs du Georgia Institute of Technology, qui affirment avoir pu exploiter des vulnérabilités leur permettant de prendre le contrôle d'API et des instruments associés, craignent cependant une prochaine montée en puissance du phénomène.

http://www.rh.gatech.edu/news/587359/simulated-ransomware-attack-shows-vulnerability-industrial-controls.

EdgeWareX est une appliance robuste (Linux, OpenVPN) qui inclut Ignition Edge, une version adaptée d'Ignition pour les architectures distribuées et sécurisées. Disposée au plus près des équipements, elle sécurise intégralement les communications entre les sites (OpenVPN, MQTT, WebSocket, TLS) tout en apportant des fonctions locales comme une IHM web et une historisation avec store-and-forward.



Ignition

tant d'accéder aux données du serveur est actuellement visible par défaut. Un utilisateur susceptible d'être "client" d'une application Panorama n'a qu'à s'authentifier pour y accéder. Bientôt, cette interface sera invisible par défaut. Le "client" ne pourra y accéder (après s'être authentifié) que si l'intégrateur ou l'exploitant a explicitement mis en place des mécanismes permettant de l'exposer. « *Cela renforce la nécessité pour l'intégrateur et/ou l'utilisateur final de prendre conscience de ce qu'il fait. Pour, au total, une meilleure responsabilisation de l'ensemble des acteurs* » estime-t-elle..

Comme Codra avec Panorama, Areal, qui développe le logiciel Topkapi, a participé au groupe de travail de l'ANSSI sur les SCADA. « *Les développements actuels et futurs prennent déjà en compte les recommandations de l'ANSSI et se traduisent concrètement dans la version 6.0 de Topkapi qui a présentée à l'occasion du salon Pollutec 2016* » explique Arnaud Judes, le directeur commercial. Il s'agit là aussi d'obtenir la certification dès que l'ANSSI sera en mesure de le faire pour les SCADA. « *Nous expliquons à nos clients comment nos solutions répondent aujourd'hui aux enjeux de cybersécurité. Nous les informons également sur les bonnes pratiques à respecter de façon générale, que ce soit dans l'utilisation du SCADA ou dans ses interactions avec son environnement d'exploitation (communication avec les équipements d'automatisme par exemple)* » ajoute Arnaud Judes.

Lacroix-Sofrel, qui développe des outils de télégestion, est également très avancée sur le sujet. L'entreprise a présenté son dernier né, le S4W, en décembre 2016, lors du salon Pollutec. Fruit de cinq années de développement, c'est un système fonctionnant entièrement en IP. « *Auparavant, on fonctionnait sur les réseaux téléphoniques. Depuis que l'on a muté vers des réseaux IP, la sécurité est devenue indispensable*, explique Benoît Quinquenel. *Les postes de télégestion font aujourd'hui partie des systèmes d'information. Cela signifie qu'en termes de sécurité, ils ne peuvent plus fonctionner seuls mais font partie intégrante d'un écosystème. Il y aura des systèmes d'administration, de sécurisation des communications, de chiffrement, de détection d'incidents… il faudra qu'a minima, nos solutions de télégestion (ou des composants) soient compatibles avec le niveau le plus haut rencontré dans ces métiers* ». Le S4W intègre nativement des fonctions de sécurité permettant de mettre en place de la défense en profondeur avec de l'authentification par certificats, du chiffrement via 4 composants dont S4 Keys qui gère les certificats. SG-4000, pierre angulaire de l'écosystème S4W, permet ainsi de sécuriser la communication GPRS/3G entre les différents postes locaux par la création d'un VPN.

Autre composant essentiel, S4-Manager qui centralise de nombreuses fonctions dont l'administration des configurations des postes locaux, des utilisateurs mais aussi des droits d'accès qui leur sont associés. Un serveur SYSLOG centralise et notifie en continu toute activité concernant la sécurité et la sureté de fonctionnement de S4W et permet aux exploitants d'exercer une réelle surveillance sur leur réseau.

Le développement de S4W n'empêche pas Lacroix-Sofrel de "durcir" les produits précédents, déjà installés, comme le S500, en renforçant par exemple la gestion mots de passe ou en intégrant des logiciels de sécurisation des accès internet dans les tunnels VPN.

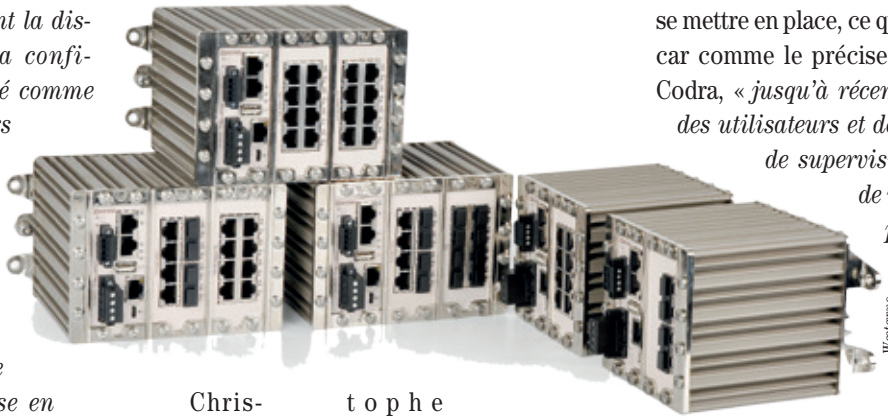
L'instrumentation est également concernée

Les systèmes d'automatismes développés par des automaticiens comme Crouzet Automation, Factory Systèmes, Phoenix Contact, Rockwell Automation ou Wago sont bien évidemment concernés tout comme les fournisseurs de solutions réseaux comme eWon, ATIM, Adeunis RF, IP Systemes, Ql3D. Les solutions proposées sont nombreuses et consistent d'abord intégrer des sécurités au plus près du terrain. Wago propose ainsi des automates intégrant directement des fonctionnalités de pare-feu et de client/serveur VPN. Les contrôleurs PFC100 et PFC200 disposent ainsi d'un pare-feu évolué, permettant la création de règles au niveau des couches 3 (IP) et 4 (TCP/UDP).

Les accès aux différents services de l'automate peuvent ainsi être restreints au plus juste, à des adresses ou plages d'adresses IP. Ces contrôleurs supportent également des connexions VPN de bout en bout, grâce à OpenVPN ou IPsec. Les canaux sont ainsi sécurisés jusque dans les automates, prévenant tout risque d'interception de données au-delà du routeur. Factory Systèmes propose de son côté la gamme de switch industriels RadiFlow qui intègre dans un seul et même produit trois fonctionnalités : Firewall, Modem et Switch.

Chez Westermo, le Redfox series, un boîtier durci intègre les fonctions switch/routeur et firewall ainsi que des routeurs sans fils sécurisés pour les accès distants.

Westermo intègre un département cybersécurité et travaille dans ce domaine depuis de nombreuses années. « *Nous répon-*


Westermo

Le Redfox series de Westermo est un boîtier durci qui intègre les fonctions switch/routeur et firewall ainsi que des routeurs sans fils sécurisés pour les accès distants.

dons aux 4 cibles de la cybersécurité qui sont la disponibilité, l'intégrité, la confidentialité et l'authenticité comme très peu de constructeurs en sont capables dans le domaine industriel, explique Olivier Bughin Managing Director chez Westermo. *Par ailleurs, notre département Cybersécurité a mis en place une cellule de gestion de crise en cas d'alerte de faille de sécurité connue ou reportée par un client avec des étapes strictes et des temps maximums impartis pour répondre à chacune d'entre elles. Enfin, nous possédons notre propre plateforme ATP (Achilles Test Platform) ainsi qu'un scanner de vulnérabilité NESSUS pour une identification et une gestion complète des vulnérabilités dans l'ensemble de nos produits* ».

Concepteur de ses propres concentrateurs et gateways IP interopérables, Mios a intégré dans ses produits déjà depuis plusieurs années la dimension sécuritaire nécessaire à la gestion de tout réseau informatique. En effet les modules de communication, qu'ils soient filaires ou radio, sont partie intégrante d'un système d'information qui a nécessairement sous IP sa logique sécuritaire notamment si ce système d'information est connecté à Internet donc au monde extérieur. Le pilotage à distance par lien VPN, l'authentification par certificats sécurisés et le chiffrement sont des fonctions de sécurité proposées nativement dans les sous-systèmes de communication Mios. La récente gamme MiosCube présente les caractéristiques décrites ci-dessus et peut être également sécurisée par des modules de sécurité logiciel pour le cryptage des données dans le cadre de leur transmission ou de leur stockage dans le Cloud par exemple. La gamme intègre tous les outils nécessaires pour s'adapter aux exigences de sécurité du client.

En bout de chaîne, l'instrumentation est tout aussi concernée. Emerson Process Management fournit de l'instrumentation, des transmetteurs de données (pression, température, débitmétrie, etc.), des vannes, des automates, en fait tout ce qui va de la couche la plus "basse", les instruments, au contrôle-commande. Or, selon Christophe Pinède, « *la plupart du temps, les attaquants visent justement les composants que nous fournissons : contrôle-commande ou vannes et instruments, en les rendant aveugles ou inopérants alors qu'ils peuvent avoir une fonction de sécurité ou de process* ». C'est pourquoi, à la demande des clients, Emerson Process Management a commencé à se préoccuper de la protection de ces systèmes. Avec des objectifs clairs : les systèmes fournis doivent être protégés et capables de se mettre en position de repli en cas d'attaque sérieuse. Et au minimum d'émettre une alarme.

Schneider Electric commercialise également un nouvel automate, le M580. Non seulement il interdit toute connexion non autorisée, comme le font les automates déjà existants, du moins ceux des générations récentes, mais de plus il lance une alerte vers le centre de supervision. Il intègre dès sa conception des fonctions de sécurité. « *Par exemple, le firmware du M580 est chiffré et signé, et son intégrité est vérifiée avant d'être chargé dans l'automate ou à son redémarrage. Les services inutilisés (FTP, HTTP…) peuvent être désactivés. Et enfin, toutes les modifications de programme peuvent être protégées par mot de passe* » explique Yann Bourjault.

Les exploitants en première ligne

Tous les intervenants, qu'il s'agisse de l'ANSSI, des fournisseurs de matériels ou de solutions logicielles ou des intégrateurs, insistent toutefois sur le fait que, quels que soient les dispositifs déployés, la sécurité n'existe que si l'utilisateur applique les règles de base et met constamment son installation à niveau. Une culture de la sécurité doit donc se mettre en place, ce qui n'a rien d'évident car comme le précise Kim Cloutet chez Codra, « *jusqu'à récemment, la priorité des utilisateurs et des éditeurs d'outils de supervision était d'obtenir de nouvelles fonctions plus rapides, plus ergonomiques, plus faciles à mettre en œuvre. Or, tout ce que l'on va proposer en matière de sécurité n'apportera pas de fonction nouvelle à l'utilisateur* ». L'exploitant aura juste la certitude qu'il est conforme aux exigences de sécurité, voire à celles de l'ANSSI s'il est OIV.

Cela signifie que les produits sont désormais livrés avec des instructions. « *Nous informons systématiquement nos clients sur les bonnes pratiques à respecter de façon générale que ce soit dans l'utilisation d'un outil de supervision ou dans ses interactions avec son environnement d'exploitation, comme par exemple la communication avec les équipements d'automatisme* », souligne ainsi Arnaud Judes, chez Aréal. Mais c'est aux intégrateurs, qui sont au plus près du terrain, de prendre en charge la diffusion de cette culture. Et en particulier de dispenser des formations. Schneider Electric propose ainsi en catalogue deux formations à la cybersécurité. SENCYB qui dure une journée, forme les directeurs d'usine, opérateurs de maintenance et même l'ensemble des agents pour les sensibiliser au risque. Plus poussée (trois jours), la formation CYBINDUS est conforme aux exigences de l'ANSSI. « *Elle est délivrée par les personnes de mon équipe, qui sont des experts en cybersécurité industrielle et donc connaissent les questions concrètes des exploitants* » souligne Yann Bourjault.

Vers une économie de la cybersécurité

Il ne faut pas se le cacher : tout cela a un prix. La sécurité n'est pas gratuite. Une véritable économie de la cybersécurité est en train de se mettre en place dans le secteur de l'eau, et le monde industriel en général. Kim Cloutet, Codra, souligne ainsi l'impact pour intégrateurs « *qui, jusqu'à*

Impliquer l'ensemble des collaborateurs, des informations et des systèmes

Pour évaluer les risques qui pèsent sur les services d'eau et qualifier la typologie et la provenance des cyberattaques potentielles, Trend Micro, spécialisée dans la fourniture de solutions de sécurité, a mis en place en 2013 un système virtuel de gestion de la pression dans un réseau de distribution d'eau d'une ville de taille moyenne. L'application, répliquée à une quinzaine d'exemplaires, a été localisée dans 15 pays différents avant d'être connectée à l'Internet. « *Nous avons pu observer de nombreuses connections illégitimes avec notamment des tentatives d'intrusion et de détournement du fonctionnement du process*, souligne Loïc Guézo, responsable de la Stratégie cybersécurité Europe du sud chez Trend Micro. *Même si beaucoup d'entre-elles relèvent de l'intrusion anodine, sans véritable objectif, d'autres se sont avérées nettement plus virulentes avec, dans certains cas, une prise de contrôle partielle du système de gestion de la pression. Nous avons également subi des attaques de type phishing conduisant à l'exfiltration de fichiers factices que nous avions placés dans l'application* ». La typologie des attaques a révélé des modes opératoires assez différents selon leur origine géographique, avec de nombreuses opérations de connaissance venant de Russie et des intrusions parfois très actives venant de Chine.

Cette expérimentation a mis en lumière le degré d'exposition élevé des services de distribution d'eau potable, très exposés du fait de leur architecture décentralisée. « *En France, nous sommes plutôt bien placés sur la partie sensibilisation au risque de même qu'au niveau de la perception*, souligne cependant Loïc Guézo. *C'est plutôt en termes de mise en œuvre et de moyens que la question se pose* ». Une chose est certaine : dans le secteur de l'eau, les OIV, et plus généralement, l'ensemble des services de distribution d'eau, vont devoir prendre en charge de manière beaucoup plus stricte que par le passé, l'aspect sécurité de leurs systèmes d'information.

Mais par quoi commencer ? « *La première chose à faire, c'est de mettre en place une structure de gouvernance chargée de faire vivre ce projet de mise et de maintien en sécurité du service*, explique Loïc Guézo. *Cela veut dire, très pragmatiquement, désigner une personne qui sera responsable de cette démarche et qui bénéficie de l'appui d'un élu ou d'un responsable suffisamment important pour pouvoir faire bouger les lignes* ». Il s'agira de déterminer le périmètre et les objectifs de la démarche avant de définir un budget et une feuille de route. La première étape de ce travail consiste bien souvent à recenser, identifier et cartographier l'ensemble des composants du système d'information du service, à commencer par les automates industriels, en décrivant pour chacun d'entre eux, leur fonction, leur paramétrage et leur niveau de sécurité. « *Il s'agit d'intégrer chacun de ces composants dans un plan de rénovation plus général dont le seul objectif est d'être capable de garantir le niveau de sécurité de l'ensemble*, souligne Loïc Guézo. *Cette démarche effectuée, il faudra dans bien des cas, hiérarchiser les priorités, car le vrai danger pour ces services, c'est de se voir proposer un upgrade généralisé de leurs équipements qu'elles n'ont pas toujours les moyens d'engager* ». Il s'agira de sécuriser les systèmes en les protégeant des accès illicites tout en préservant l'intégrité et la confidentialité des données, qu'elles soient opérationnelles ou commerciales. « *La grosse difficulté, c'est de faire dialoguer deux mondes qui ont tendance à s'ignorer*, explique Loïc Guézo. *Celui de l'IT, l'informatique, qui repose avant tout sur la confidentialité et l'intégrité des données, et celui de l'OT (operationnal technologies) qui concerne d'abord les systèmes industriels et leur disponibilité. La cybersécurité n'est pas qu'une affaire de technologie. Au-delà des infrastructures, une stratégie efficace doit impliquer l'ensemble des collaborateurs, des informations, des systèmes, des processus du service de l'eau* ».

présent, n'avaient pas intégré ces problématiques dans le chiffrage de leurs offres. Or la sécurité exige du temps, s'étudie, s'analyse, se met en place… ». Lorsqu'ils n'en disposent pas déjà, les intégrateurs mettent en place des équipes dédiées à la cybersécurité, et certains éditeurs envisagent également d'y allouer des moyens humains. Christophe Pinède, chez Emerson Process Management, explique qu' « *il est de la responsabilité des exploitants d'analyser les faiblesses et de définir le niveau de risque qu'ils acceptent. Puis ils investissent pour se protéger. Firewalls, composants réseau, blocages de ports, solutions de sauvegarde et restauration avec politiques de rétention, cryptage, gestion des utilisateurs tout cela a un coût rend encore les professionnels frileux en ce moment* ».

La question ne se pose pas pour les OIV qui sont légalement obligés de se conformer au niveau de sécurité défini par l'ANSSI. Reste à convaincre les autres opérateurs qu'ils y ont tout intérêt. « *Il n'y a qu'un nombre limité d'OIV dans le domaine de l'eau, mais la cybersécurité concerne tous les exploitants. Nous souhaiterions que tous mettent en œuvre les 20 règles* », souligne Sadio Bâ à l'ANSSI. Car la menace n'est pas qu'une vue de l'esprit. Un fournisseur de matériel affirme ainsi répertorier chaque année environ 20 millions d'attaques de tous genres et de toutes gravités sur son propre système. Même si une infime minorité de ces tentatives arrive à franchir les protections, la menace n'est est pas moins réelle. Et rien n'est jamais acquis en matière de cybersécurité. « *Dès qu'on a quitté le site, une nouvelle faille peut potentiellement être découverte. Il faut donc mettre à jour régulièrement cette sécurité et sensibiliser agents pour qu'ils l'utilisent à bon escient* ». Une nouvelle culture, qui, pour beaucoup, reste à acquérir… ■