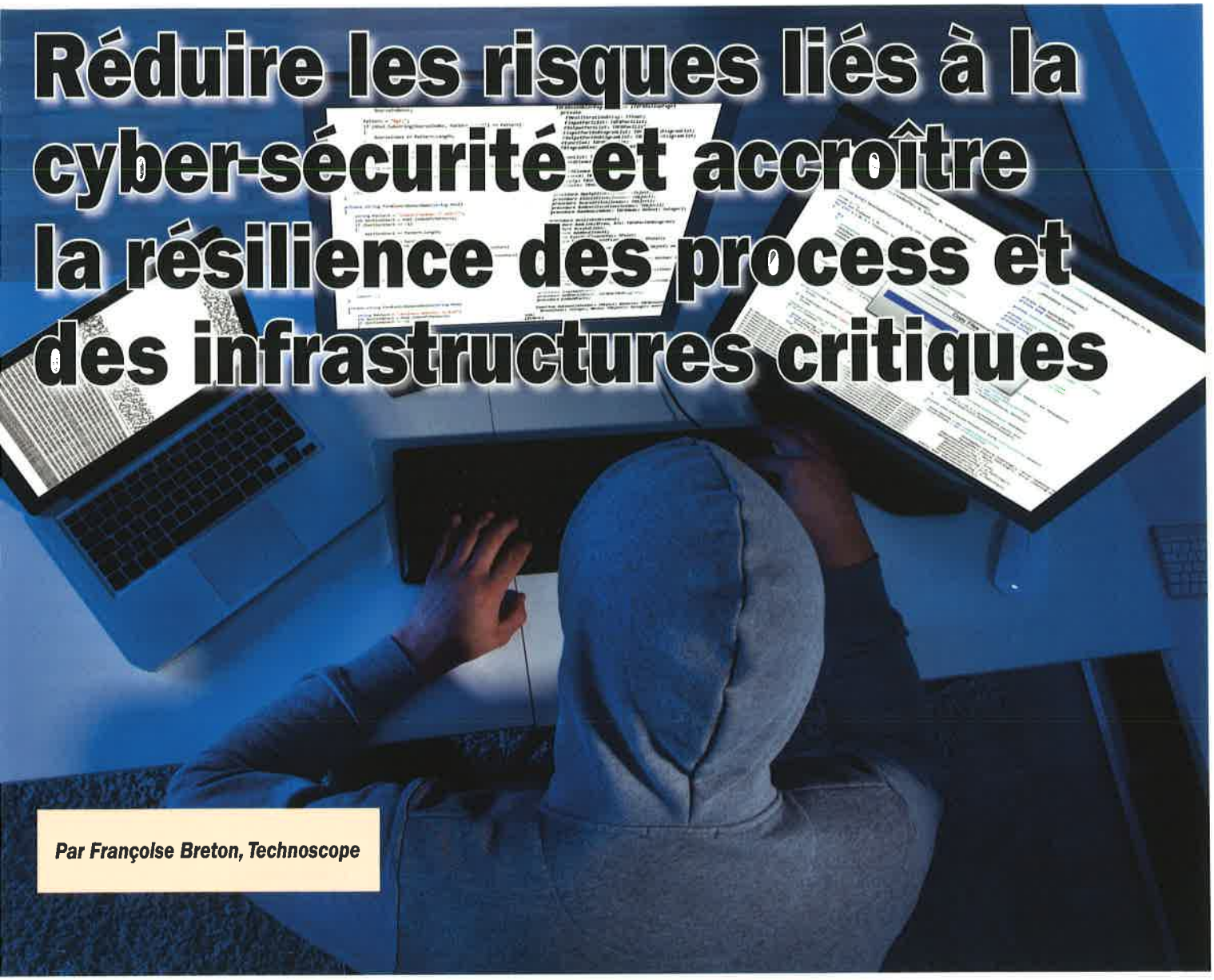
Réduire les risques liés à la cyber-sécurité et accroître la résilience des process et des infrastructures critiques



Par Françoise Breton, Technoscope

ABSTRACT

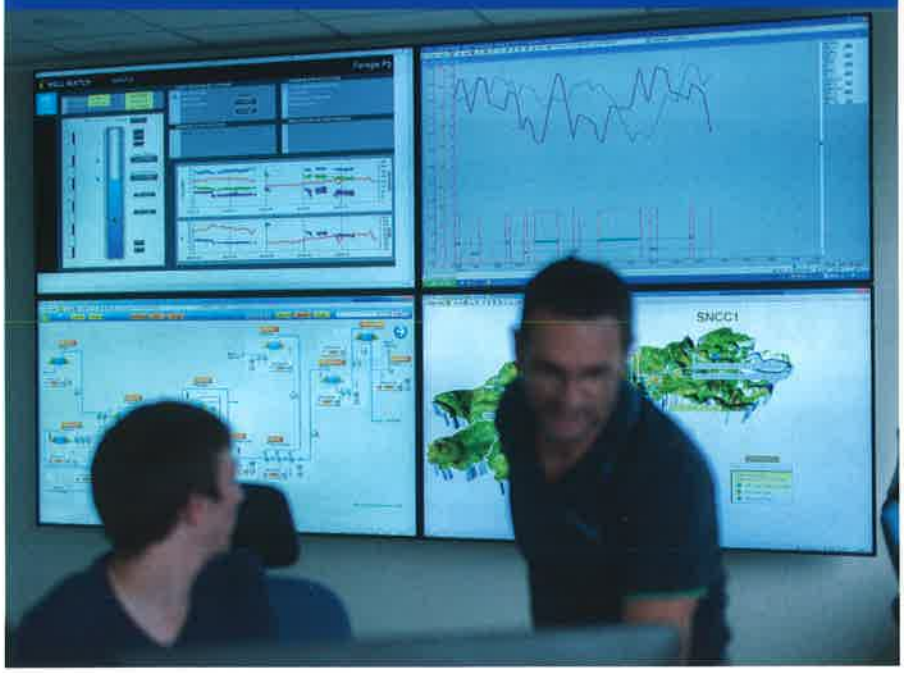
Reducing cybersecurity-related risks and increasing critical process and infrastructure resilience.

100% security does not exist. But for a modest cost, it is possible to provide protection against a large number of low-level attacks. Devices are available and best practices guidelines, published by ANSSI, help in adopting the correct behaviours as security is first and foremost a question of corporate culture. These first steps are essential at a time when an increasing number of industrial sites are falling prey to hackers and where the new military programming law requires critical operators to provide their own cybersecurity.

La sécurité 100 % n'existe pas. Mais pour un coût modique, il est possible de se protéger efficacement d'un grand nombre d'attaques de bas niveau. Les dispositifs existent et des guides de bonnes pratiques, édités par l'ANSSI, aident à adopter les bons comportements car la sécurité est avant tout une question de culture. Des premiers pas indispensables à réaliser au moment où de plus en plus de sites industriels deviennent la proie de hackers et où la nouvelle loi de programmation militaire fait obligation aux opérateurs d'importance vitale d'assurer leur cyber-sécurité.

Aujourd'hui, les systèmes industriels ne sont plus à l'abri de la cyber-criminalité. Ils constituent de plus en plus fréquemment des cibles pour les pirates, voire des cibles militaires, comme l'attaque du virus Stuxnet sur les équipements nucléaires iraniens en 2010, ou encore des cibles économiques. « *Nous avons pris conscience que des outils informatiques pouvaient porter atteinte à un outil industriel*, explique Thomas Houdy, spécialiste de la cyber-sécurité chez Lexsi, une société de conseil en cyber-sécurité informatique qui s'est investie dans la

Dans le cadre de la nouvelle loi de programmation militaire, les opérateurs d'importance vitale vont devoir sécuriser leurs infrastructures et remonter à l'Agence nationale de la sécurité des systèmes d'information tout incident de sécurité.

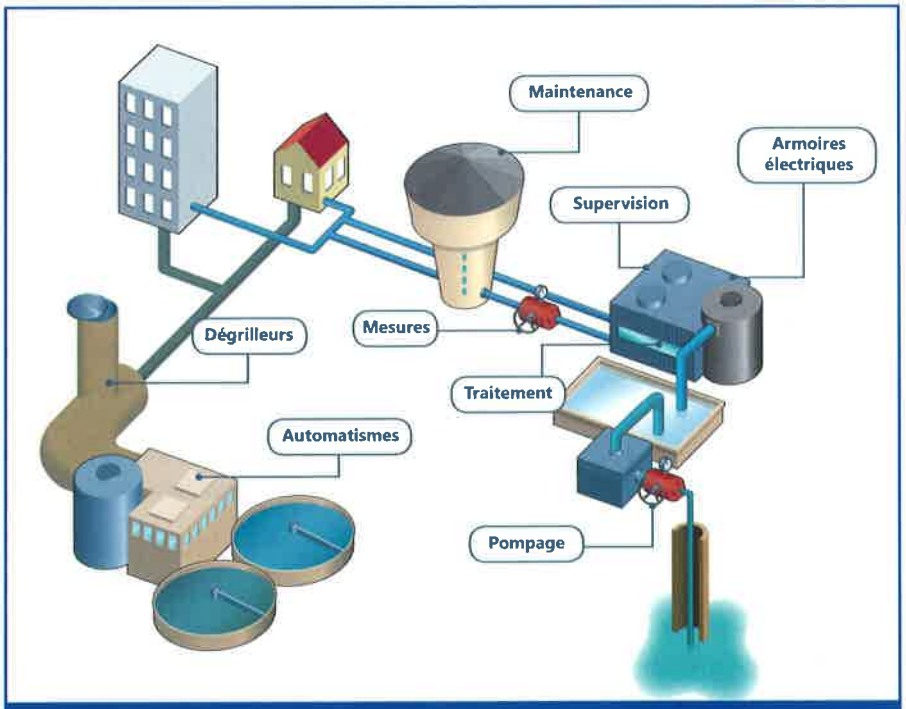


Lyonnaise des Eaux

sécurité industrielle depuis cinq ans. *Or les infrastructures industrielles, les systèmes de contrôle-commande et les automates qui constituent le centre névralgique de l'usine d'aujourd'hui ne bénéficient généralement pas de mécanismes de protection et de sécurité suffisants. Pourtant, l'interconnexion de plus en plus prégnante des mondes industriels et informatiques les rend accessibles aux attaques directes mais également, et plus simplement encore, à tous les virus et autre cheval de Troie qui sommeillent sur l'Internet* ».

Se protéger de la cyber-criminalité: une obligation

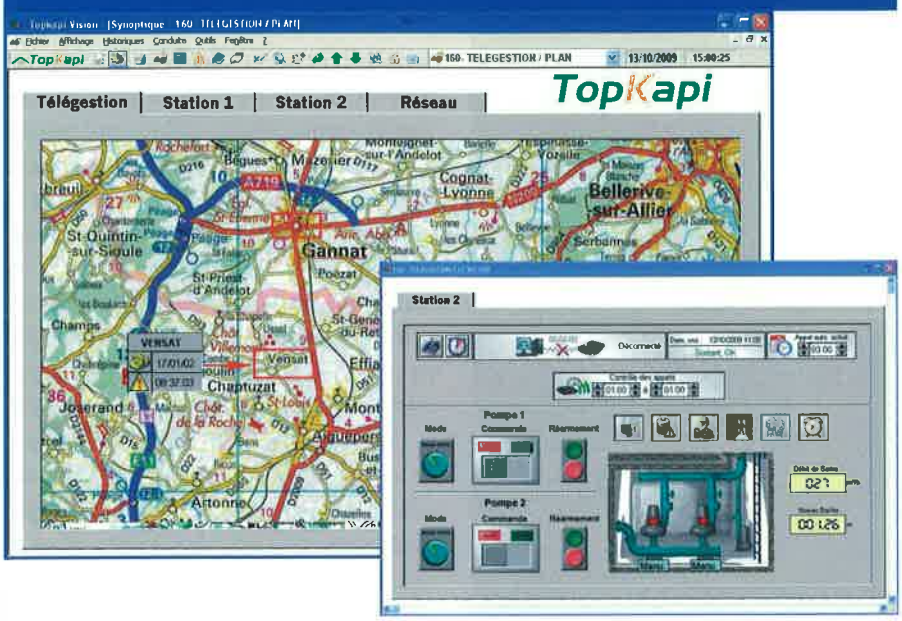
Face aux menaces croissantes de cyber-attaque, les opérateurs d'importance vitale (OIV) vont avoir l'obligation, dans le cadre de l'article 22 de la nouvelle loi de programmation militaire 2014-2019, de sécuriser leurs infrastructures, de remonter à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) tout incident de sécurité et d'auditer ou de faire auditer régulièrement leur système de sécurité pour s'assurer du niveau de sécurité de leurs systèmes. « *On retrouve dans cet article, les règles de sécurité que les opérateurs d'infrastructures critiques devront mettre en place pour renforcer la cybersécurité*, précise Stéphane Meynet, chef de projet sécurité des systèmes industriels à l'Agence nationale de la sécurité des systèmes d'information (ANSSI). *Un décret d'application, suivi d'arrêtés sectoriels, devrait sortir prochainement pour préciser les règles exactes à mettre en place ainsi que les délais d'application* ». Les infrastructures de traitement et de distribution d'eau potable, tout comme les stations d'épuration, font partie des opérateurs d'importance vitale puisque leur dysfonctionnement, leur arrêt ou leur indisponibilité, volontaire ou non, affecterait directement un grand, voire un très grand nombre de personnes. Bien que les contraintes et les enjeux soient différents selon qu'il s'agisse d'une usine d'eau potable alimentant une agglomération de moyenne ou grande taille, ou bien d'une petite unité de province faiblement automatisée et peu voire pas connectée, cette dernière devra néanmoins également veiller à sa sécurité. En effet, si elles ont moins à redouter d'être prises directement pour cibles - les cyber-attaques relevant plus de l'exception que de la règle - elles ne sont pas à l'abri d'une contamination par un logiciel malveillant introduit involontairement, par exemple, via la clé USB personnelle d'un employé ou d'un sous-traitant. Ce "malware" peut se révéler dommageable pour le système de contrôle-commande de l'exploitation et conduire à une dégradation des équipements de production, par exemple endommager les pompes qui vont tourner à vide à la suite de la fermeture inopinée d'une vanne en amont. Ce risque est décuplé avec la généralisation d'Ethernet ainsi que le développement des technologies M2M et des interventions à distance qui permettent de réduire les coûts d'exploitation (télégestion, télésurveillance ou télémaintenance). Ces nouvelles technologies multiplient en effet les portes d'entrées des systèmes. À plus grande échelle, la généralisation de l'interconnexion dans le cadre du



Actemium

La maîtrise des risques humains, économiques et environnementaux est un enjeu lié à la sécurité process. Actemium intervient sur l'ensemble du cycle de l'eau : pompage, traitement, stockage, distribution, épuration.

Aréal développe des solutions logicielles destinées à protéger les communications avec l'extérieur et propose de nombreux utilitaires pour, par exemple, verrouiller l'environnement Windows en fonction des droits d'accès et protéger les disques durs en écriture.



Aréal

développement des "Smartcities" qui permettra aux collectivités de disposer d'une vue centralisée de tous les flux (énergie et transport mais aussi la gestion de l'eau, du gaz, de l'électricité) devrait contribuer à multiplier les composants communicants et donc le nombre de failles potentielles à identifier et sécuriser.

Se protéger est donc d'autant plus indispensable que cela ne nécessite pas d'investissements très coûteux. La plupart du temps, les failles de sécurité sont dues à des systèmes configurés qui n'ont pas suffisamment pris en compte la sécurité, avec des identifiants et des mots de passe par défaut, des ports USB non protégés, des automates équipés de petits serveurs web embarqués et connectés sur Internet pour la maintenance à distance dépourvus d'accès spécifique, etc. « *Ces erreurs sont fréquemment identifiées dans nos audits*, indique Thomas Houdy. *Elles permettent d'accéder facilement, à partir d'Internet, à des automates, des stations de communication d'opérateurs ou bien à un système de vidéo surveillance par exemple. Or Internet est un milieu dans lequel les pirates ont des outils très sophistiqués et des compétences d'expert!* ».

Identifier les failles, contrôler les accès, détecter les attaques

Des guides de bonnes pratiques permettant l'auto-évaluation et l'auto-sécurisation ont été mis en ligne par l'ANSSI en janvier 2014 pour assister les exploitants dans leur démarche. De même, l'ANSSI a récemment publié une série de profils de protection qui contiennent un ensemble de mesures de sécurité que doivent respecter les équipements ou les logiciels. « *Ces documents listent les mesures de sécurité que devront intégrer ces équipements s'ils veulent être certifiés d'un point de vue sécurité* », souligne Stéphane Meynet. Car l'ANSSI délivre deux certifications, un label de premier niveau et un label plus large, susceptible d'intégrer des reconnaissances possibles à l'international. « *Nous encourageons les équipementiers à faire certifier leurs produits*, indique Stéphane Meynet, *car intégrer des fonctions de sécurité dans un produit ou un logiciel, c'est bien, mais il faut encore s'assurer qu'elles soient robustes* ».

Les guides sur la cyber-sécurité ont été établis par des groupes de travail regroupant des équipementiers, des intégrateurs, des experts en cyber-sécurité et des utilisateurs. Dans le domaine de l'eau, de nombreux acteurs sont concernés. C'est par exemple le cas des groupes spécialisés dans les automatismes industriels comme Schneider Electric, Siemens, Mitsubishi Electric, Rockwell Automation, Factory Systèmes, GE Intelligent Platform, des spécialistes de la télégestion comme Lacroix Sofrel, Perax, Wit ou Mios, des sociétés de conseil comme Lexsi, des intégrateurs comme Actemium ou Apilog.

Les éditeurs d'outils de supervision comme Aréal, Arc Informatique ou Codra sont également concernés. « *La première chose à faire est de réaliser un inventaire afin d'être en mesure d'identifier les composants susceptibles d'être piratés et d'évaluer les risques associés, c'est-à-dire les conséquences prévisibles d'une cyber-attaque ou d'un dysfonctionnement de ces composants*, indique Jérôme Poncharal, spécialiste de la cyber-sécurité chez Rockwell Automation fournisseur de solutions de contrôle commande incluant automates, réseaux et logiciels. *Une fois les vulnérabilités identifiées, il s'agit d'y pallier par des contre-mesures appropriées, c'est-à-dire choisies en fonction de l'impact d'une attaque et de sa probabilité d'occurrence* ».

Il faut donc surveiller les accès et protéger les connexions essentielles en authentifiant les utilisateurs, en limitant et en déterminant les droits et en bloquant tout flux non autorisé, par exemple en établissant des listes blanches d'applications qui sont censées être en usage sur un poste donné. Des logiciels comme "Trendmicro", distribué par Factory Systèmes, permettent de bloquer à l'exécution toutes les applications ne figurant pas sur une telle liste. Il est également indispensable de détecter les tentatives d'intrusion et de les faire remonter par des alarmes. En effet, depuis 2010, les stratégies des pirates ont évolué. « *Il ne s'agit plus de détruire mais de passer inaperçu pour récupérer le plus de données possible*, précise Thomas Houdy. *En 2014, deux virus spécifiques des environnements industriels ont été capables de s'introduire sur des réseaux de contrôle-commande, de scanner le réseau à la recherche de machines OPC, puis de prendre des informations et de les exfiltrer. Ils peuvent infecter en toute discrétion une petite station car elle peut constituer une porte d'entrée pour remonter vers des réseaux encore plus sensibles* ».

Des solutions peu coûteuses pour sécuriser les équipements

« *Les premières mesures pour sécuriser les équipements et les infrastructures ne sont pas toujours coûteuses*, souligne Stéphane Meynet. *Le fait, par exemple, d'utiliser une clé USB qui ne sort pas du site professionnel pour échanger des données entre deux postes, permet de supprimer un certain nombre de risques sans que cela ne génère de coûts. Ces mesures, simples, permettent d'éliminer bon*

La mise en sécurité des process et des sites doit être méthodique et va bien au-delà des solutions techniques. Elle implique des changements de comportements et des mises à jour régulières car c'est un domaine en perpétuelle évolution.

Veolia - Ken Choi

nombre de difficultés potentielles, mais il ne faut pas s'arrêter là et considérer qu'elles suffisent ». Outre les bonnes pratiques qui sont à la base de toute stratégie de sécurité, il est nécessaire d'installer des protections physiques ou logicielles aux endroits vulnérables. Il n'est cependant pas toujours possible d'adopter directement les dispositifs utilisés dans le domaine de l'informatique classique. Utiliser un antivirus sur certaines stations, par exemple, peut dégrader leur performance, voire provoquer un arrêt inopiné de certains équipements. Mais il existe déjà sur le marché des solutions de protection adaptées au monde de l'eau. « *Tous nos automates de télégestion intègrent depuis plusieurs années des dispositifs de sécurité intégrés qui permettent de gérer le risque d'attaque du réseau interne,* explique Olivier Barthel, responsable de la partie développement chez Perax, Groupe Aqualabo. *Ils peuvent être protégés par des mots de passe et être paramétrés pour prévenir des essais d'intrusion mais ces fonctionnalités devraient être plus souvent utilisées. La sécurité est une affaire de culture!* ». Ce constructeur intègre aujourd'hui systématiquement dans sa gamme P400XI des VPN (virtual private network) qui assurent l'authentification de la communication et le cryptage des données entre un superviseur et les différents équipements ou bien entre les équipements eux-mêmes. Lacroix Sofrel fournit également de gros efforts sur l'ensemble de ses équipements pour assurer une meilleure sécurisation des accès aux postes de télégestion. « *La dernière version de S500 répond aux exigences de l'ANSSI visant à promouvoir les bonnes pratiques comme le durcissement des mots de passe ou le filtrage des adresses IP,* souligne Jean-Marie Laurendeau, Chef de marché Télégestion Eau chez Lacroix Sofrel. *Notre objectif est de permettre à nos clients de renforcer la sécurité informatique de leurs installations, facilement et à moindre coût, grâce à une mise à jour logicielle des équipements existants. Nous avons également travaillé étroitement avec les principaux exploitants pour les accompagner dans leur démarche* ».

Les dispositifs de protection se développent. Le Stratix 5700 de Rockwell Automation permet par exemple de vérifier la légitimité du trafic au niveau des contrôleurs, et le routeur de service Stratix 5900 est bien adapté à la protection des infrastructures en site distant et au transfert sécurisé des données sur un réseau extérieur. Ce routeur s'assure que la personne cherchant à se connecter est habilitée à le faire (authentification) et empreinte un tunnel VPN pour transférer des informations cryptées. « *La technique VPN est très aboutie et offre le meilleur niveau de confiance dans des rapports qualité/prix raisonnables,* souligne Jérôme Poncharal, spécialiste cyber-sécurité chez Rockwell Automation. *Ce dispositif peut également servir à l'intérieur de l'usine, pour protéger des machines des interférences de communication. C'est une mesure simple et efficace* ».

Le développement actuel des objets connectés, des réseaux de communication et du M2M industriel crée d'autres vulnérabilités. « *Il peut être judicieux par exemple d'utiliser un système de radiofréquence qui offre un niveau de sécurisation supérieur à Ethernet ou wifi, ou bien de privilégier, sur des réseaux télécom ou classique sur IP, le protocole sécurisé MQTT (message queue telemetry transfert),* souligne Gregory Guiheneuf. *Nos capteurs libelium véhiculent par exemple les informations sur ce protocole* ». Factory Systèmes dispose également d'un Modem INSYS qui fonctionne sur le réseau Ethernet ou avec une carte Sim sur un réseau d'opérateur télécom, et est géré, de façon centralisée, sans administration complexe, par un service hébergé dans le cloud (Insys connectivity service). Ce service permet de créer une communication VPN très simplement entre un utilisateur et une application selon des règles définies par l'exploitant par exemple l'ouverture du tunnel sous condition d'autorisation d'accès seulement. « *Ce système offre souplesse et sécurité, aussi bien pour le prestataire que pour l'administrateur du réseau,* précise Gregory Guiheneuf. *En souscrivant à ce service,*

Perax intègre dans sa gamme P400XI des VPN (virtual private network) qui assurent l'authentification de la communication et le cryptage des données entre un superviseur et les différents équipements ou bien entre les équipements eux-mêmes.

Codra renforce la sécurité de la dernière version 6 de Panorama E² : tous les éléments (fichiers exe, dll) sont tous signés et vérifiés par Norton Secured de Symantec, garantissant ainsi pour l'utilisateur, comme le centre de télégestion de la Société des Eaux de Marseille, l'authenticité des programmes Panorama dès leur installation.

Codra

les clients peuvent administrer l'ensemble de leurs modems Insys pour une cinquantaine d'euros par an et par équipement. C'est un gain énorme pour les exploitants qui peuvent ainsi réaliser sans se déplacer un premier niveau d'intervention ».

Factory Systèmes propose également des solutions simples de prévention pour éviter le transfert de virus à l'intérieur de l'usine comme le scan antiviral de l'éditeur américain Bluecoat qui permet de certifier les clés USB avant de pouvoir les utiliser sur les systèmes SCADA de l'exploitation. « *L'entrée de virus par les ports USB constitue le premier risque*, note Gregory Guiheneuf. *L'idée est de créer des zones protégées pour les postes sans anti-virus. Nous proposons également un anti-virus sur clé USB, conçu par un autre leader du domaine de la cyber-sécurité "Trendmicro", qui scanne le PC pour identifier la présence éventuelle de virus et lancer des correctifs le cas échéant. Cette solution plaît beaucoup car elle permet également de sensibiliser les utilisateurs* ». Factory Systèmes propose des pare-feu industriels, Radiflow et Tofino, dédiés aux systèmes très distribués et qui surveillent les protocoles utilisés sur le terrain, ainsi qu'une solution de protection par datadiode, Fox IT, qui permet de garantir une communication unidirectionnelle entre deux points et, par conséquent, l'impossibilité de prendre la main sur un poste fonctionnant en automatique la nuit par exemple.

En supervision, Aréal développe de son côté des solutions logicielles destinées à protéger les communications avec l'extérieur. « *Nous préconisons de créer ce qu'on appelle une zone DMZ (demilitarized zone), c'est-à-dire un sous-réseau isolé du reste de l'installation et auquel on accède par un serveur web avec un pare-feu et des filtres sur les flux de données entrant*, explique Arnaud Judes d'Aréal. *Nous installons un logiciel qui permet d'entrer sur la machine mais ne permet pas d'aller plus loin* ». Aréal propose également des utilitaires pour verrouiller l'environnement Windows en fonction des droits d'accès pour différentes opérations (supervision, installation de nouveaux logiciels) et protéger les disques durs en écriture. « *Ces questions figureront bientôt dans les cahiers des charges*, indique Arnault Judes. *Nous contribuons à la définition de ces préconisations pour les systèmes SCADA en participant aux groupes de travail de l'ANSSI. Et nous ferons les développements nécessaires pour être labellisés* ».

Codra, qui participe également à ces groupes de travail SCADA de l'ANSSI, a souhaité renforcer la sécurité de la dernière version 6 de Panorama E², sortie récemment. « *Les éléments (fichiers exe, dll) de Panorama E² sont ainsi tous signés et vérifiés par Norton Secured de Symantec, garantissant ainsi pour l'utilisateur l'authenticité des programmes Panorama dès leur installation* » souligne Cyril Rolland, Responsable Marketing chez Codra.

Actemium, la marque de VINCI Energies dédiée au process industriel, propose de surcroît des dispositifs pour protéger les procédés essentiels de production, par exemple pour détecter une modification anormale de la concentration de chlore en eau potable, en comparant des unités redondantes, en faisant remonter des alarmes en cas de modification inopinée de programme des automates, etc. « *Un autre moyen de surveillance consiste à mettre en place des analyseurs de réseau (sniffer) qui permettent de vérifier que les commandes transitant sur les réseaux*

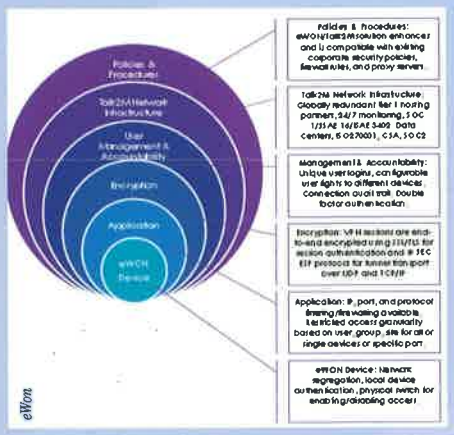
D.R.

Une fois l'intrusion détectée, se pose la question de comment réagir puis comment revenir en conditions opérationnelles. Pour être efficaces le moment venu, ces opérations doivent être anticipées et faire l'objet de procédures.

Connecter ingénieurs de maintenance et équipements industriels

La solution d'accès à distance industrielle développée par eWON consiste à pouvoir établir des connexions internet entre ingénieurs de maintenance d'une part, équipements industriels et machines distantes d'autre part, grâce aux routeurs Internet industriels que cette entreprise fabrique et un « cloud » Talk2M, ensemble de serveurs VPNs.

L'ensemble des mesures de sécurité et le respect de l'intégrité du système d'information de la solution eWON Talk2M se basent sur les lignes de conduites et des bonnes pratiques dictées par des standards de sécurité tels que l'ISO27002, IEC 62443-2-4 ainsi que le « NIST Cyber security framework 1.0 ».



Ces mesures ont été organisées sous la forme de 6 couches concentriques (voir schéma), décrites en remontant de la couche inférieure vers la couche supérieure:

- Couche routeur: authentification local, respect de la séparation réseau machine/réseau local, activation/désactivation de la communication.
- Couche applicative: gestion pare-feu, gestion des accès aux équipements, avec restriction d'accès en fonction d'un utilisateur, groupe d'utilisateur vu de chaque routeur, des groupes ou l'ensemble des routeurs.
- Couche encryptage: encryptage type SSL/TLS au sein du tunnel VPN avec authentification préalable par rapport à l'accès au tunnel et du transport des données.
- Couche gestion/administration du compte Talk2M: gestion des droits d'accès au système Talk2M, avec politique de sécurisation/renouvellement de mot de passe, traçabilité des connexions.
- Couche infrastructure réseau Talk2m: hébergement au travers de partenaires « Tiers 1 » avec respect des normes ISO27001 et SSAE 16/ISAE 3402, serveurs VPNs redondants et dispersés géographiquement, monitoring 7J/7, 24h/24, ...
- Couche procédures et directives entreprises: assurer la compatibilité maximum avec les directives et mesures de sécurité adoptées par les entreprises avec intrusion minimum et trafic IP sortant uniquement.

entre supervision et automates sont bien autorisées par rapport aux droits d'accès utilisateurs, indique Frédéric Tarcy, Chef d'entreprise d'Actemium Arras. *Ils permettent aussi de détecter une intrusion sur le réseau industriel* ».

Un problème de culture avant tout

La mise en sécurité doit être méthodique et va bien au-delà des solutions techniques. Elle implique des changements de comportements et des mises à jour régulières car c'est un domaine en perpétuelle évolution. « *Les collectivités territoriales doivent également penser à insérer systématiquement dans les cahiers des charges et appels d'offres des clauses ayant trait à la cyber-sécurité*, souligne Stéphane Meynet. *Plus les mesures sont intégrées en amont dans les projets, moins elles coûteront cher* ».

« *La sécurité n'est pas un problème qui se traite simplement par la mise en place de produits*, prévient de son côté Gregory Guiheneuf. *Parfois, nous recommandons des anti-virus ou la désactivation de certains ports de communication, mais sauf si l'entreprise dispose de services informatiques conséquents, la plupart du temps ils ne sont pas mis à jour* ». Autrement dit, la porte blindée n'est qu'une piètre protection si la fenêtre est ouverte, tout comme l'alarme si elle n'est pas branchée! Comme dans beaucoup d'autres domaines, on a tendance à négliger la question tant que l'on n'est pas directement confronté à une attaque.

C'est pourquoi tous les acteurs s'y mettent. C'est le cas dans le domaine des réseaux comme chez Wago, eWon, ATIM, Adeunis RF, IP Systèmes, QI3D, chez les automaticiens comme Crouzet Automation, Factory Systèmes, Phoenix Contact ou Rockwell Automation, chez les éditeurs d'outils de supervision comme Aréal, Codra, Arc Informatique, Wonderware, Prisma Instruments, Centreon ou Elutions ou encore chez des intégrateurs comme Actemium, Apilog, Aquatrix ou Lexsi qui proposent, souvent en partenariat, des formations destinées à sensibiliser les exploitants à la cyber-sécurité. WebAccess 8.0, commercialisé et mis en œuvre en France par Prisma Instruments, est un outil de controle et de supervision. L'application permet la conduite et la gestion d'infrastructures industrielles, d'équipements dédiés à l'eau potable ou aux eaux usées, la gestion et la surveillance de plateformes aéroportuaires, portuaires ou autoroutières. « *La particularité de la solution WebAccess est d'avoir été développée sur navigateur internet, à la différence de la quasi-totalité des applications équivalentes développées sous Windows*, indique Abdallah Boukli-Hacene, directeur général de Prisma Instruments. *Ainsi, WebAccess se déploie nativement sur tous les réseaux IP et intègre nativement les fonctionnalités Cloud très prisées aujourd'hui. Les modes de conduite et d'accès en mode local ou distant sont inhérents à l'application. De ce fait, WebAccess a dû intégrer dans son fonctionnement de base, la gestion des aspects liés à la sécurité et à l'intégrité du système et des installations pilotées* ». Outre les outils de sécurité mis à disposition par le système d'exploitation de la machine hôte, souvent insuffisants, WebAccess autorise les accès des utilisa-

Lacroix Sofrel

Durcissement des mots de passe, filtrage des adresses IP.... Lacroix Sofrel a fourni de gros efforts sur l'ensemble de ses équipements pour promouvoir les bonnes pratiques et assurer une meilleure sécurisation des accès aux postes de télégestion.

teurs en fonction des droits associés à leurs identifiants. Pour chaque serveur du système (qui peut en comporter un nombre illimité), les droits de chaque utilisateur sont configurés à l'aide d'une matrice définissant strictement les accès et les actions possibles de l'utilisateur. Cette matrice de sécurité comporte pour chaque serveur 32 zones de responsabilité et 127 niveaux de mots de passe. Ainsi, chaque utilisateur ne peut accéder au système et agir que dans la zone strictement associée à son identifiant. « *Pour que cette procédure soit pleinement efficace, il faut bien entendu que les administrateurs du système gèrent de manière dynamique les accès et droits utilisateurs. En effet, l'ingéniosité et les capacités des cyber-criminels sont sans limite et un système statique, quelles que soient les solutions mises en œuvre, ne résistera que peu de temps à des tentatives d'intrusion* », souligne Abdallah Boukli-Hacene. Parmi les fonctionnalités de base de la Solution WebAccess, il y a la possibilité par simple déclaration de disposer d'une redondance intégrale pour chaque poste serveur. Le serveur de secours, miroir parfait du serveur secouru, peut être installé à distance sur une autre localisation géographique. Il peut ainsi disposer de protection contre les intrusions, différentes des protections du serveur secouru et constituer une solution de repli réellement sécurisée.
ATIM intervient de son côté sur de nombreux projets où la sécurité est primordiale. « *Bien que la communication de nos modems radio puisse être cryptée, ceux-ci ne sont qu'un moyen de transport de l'information d'un point A à un point B*, souligne Francis Raimbert chez ATIM. *Ce sont les automates de sécurité qui sont de chaque côté de la chaîne qui assurent cette fonction essentielle de sécurisation des informations. Dès l'instant que la communication radio est coupée, le système passe en alarme et stoppe tous les éléments mobiles afin d'éviter des accidents. Afin d'éviter ces arrêts machines qui peuvent avoir un coût important dans une production, notre but est de fournir une communication radio fiable même dans un environnement industriel très perturbé* ».
La formation est également essentielle. « *Nous avons créé une formation de 3 jours qui réunit des sociétés expertes et complémentaires sur la sécurité*, précise Gregory Guiheneuf chez Factory Systèmes. La société spécialisée dans la cyber-sécurité industrielle Lexsi traite de la sécurité industrielle et des aspects normatifs, de gouvernance et de lexicologie de la cyber-sécurité. *Nous présentons, de façon très pratique, les contraintes spécifiques des systèmes SCADA et les outils de sécurisation existants. Enfin, l'éditeur du logiciel Diateam montre, sur une plateforme de stimulation piratée volontairement, comment on peut rapidement et simplement protéger son système de contrôle-commande* ».

Réagir en cas d'intrusion ou de malveillance

« *Il n'y a pas de sécurité à 100 %*, insiste toutefois Jérôme Poncharal chez Rockwell Automation. « *Les menaces évoluant, on parle de niveau de confiance des protections ou encore de niveau de SAL (security assurance level) en référence à la norme IEC62443 traitant de la sécurité des systèmes de contrôle industriels. Cette norme, en cours d'élaboration, vise à devenir le standard international industriel en matière de sécurité informatique. Point notable, elle couvre l'ensemble du cycle de vie des IACS (Industrial Automation and Control Systems) et s'adresse aux fabricants, intégrateurs et utilisateurs finaux. On peut se protéger de la majeure partie des logiciels malveillants mais il reste nécessaire de prévoir des procédures de repli et de restauration en cas d'attaque sérieuse* ». En effet, une fois l'intrusion détectée, se pose la question de comment réagir puis comment revenir en conditions opérationnelles. Pour être efficaces le moment venu, ces opérations doivent être anticipées et faire l'objet de procédures. Actemium s'appuie sur sa double compétence en traitement de l'eau et en cyber-sécurité pour proposer une formation personnalisée sur ce versant de la sécurité. « *Nous simulons l'installation des opérateurs sous différents scénarios d'attaque pour mieux identifier les risques et définir les réactions appropriées*, explique Sylvain Reumeau, Responsable de l'innovation chez Actemium. *Cela permet d'identifier comment mettre l'installation en repli puis la remettre en fonctionnement rapidement pour assurer une continuité d'exploitation dans les meilleures conditions possibles. Nous exploitons aussi des outils de simulation appliqués aux systèmes de distribution électrique qui représentent également une partie importante de l'usine à sécuriser* ». Ces outils permettent, par exemple, d'identifier à l'avance comment contrer une attaque sur un château d'eau en isolant la partie ciblée et en basculant sur d'autres réservoirs afin d'assurer temporairement la continuité de service. « *Ce sont des cas concrets envisagés dans le cadre de la protection de site en cyber-sécurité mais nous mettons également cette démarche en œuvre pour la gestion des crues, par exemple, quand il faut faire basculer des systèmes de pompage en adoptant la meilleure stratégie possible* », précise Frédéric Tarcy, Chef d'entreprise d'Actemium Arras.

Maintenir le système de sécurité dans le temps

Les systèmes de protection en place, il ne faut pas baisser la garde car les menaces évoluent en permanence. Il faut s'assurer que le niveau de sécurité suit au même rythme en procédant à une mise à jour régulière des anti-virus et autres contre mesures.
Il est nécessaire pour cela de consulter les bulletins émis par un centre d'alerte et de réaction aux attaques informatiques (CERT) ou de s'abonner à un service de notification automatique d'alerte dédié à la sécurité qui informe sur comment se protéger en isolant du réseau et en appliquant une contre-mesure appropriée.
La cyber-sécurité relève d'une démarche permanente, sans cesse recommencée, sans que rien ne soit jamais acquis.
Reste une question délicate, celle de la responsabilité : en cas de cyber-attaque, qui devra supporter les dégâts et leurs conséquences financières ? « *Il est important de bien délimiter les responsabilités. C'est un sujet compliqué mais incontournable, qui doit être traité en amont* », prévient Stéphane Meynet. ■

Les guides dédiés à la cybersécurité des systèmes industriels édités par l'ANSSI sont disponibles à l'adresse : http://www.ssi.gouv.fr/systemesindustriels