La cybersécurité vue par les fournisseurs d'automatismes

Comment traitent-ils ce sujet dans leurs produits et leurs offres ? Les automates actuels sont-ils sécurisés ? Comment aident-ils les industriels à mettre en place les solutions adéquates ? Comment mettent-ils à disposition les correctifs sur leurs équipements ? Lors d'une table ronde organisée pendant la dernière réunion de l'année du Club Automation, des représentants de plusieurs grands acteurs des automatismes ont répondu aux questions des utilisateurs finaux sur ce sujet.

Participants à la table ronde :

Thierry Vajsman, *responsable de l'activité infrastructure urbaine chez Phoenix Contact.*

Jérôme Poncharal, *ingénieur avant ventes chez Rockwell Automation.*

Laurent Raillier, *responsable marketing sureté de fonctionnement chez Schneider Electric.*

Jean-Christophe Mathieu, *référent réseaux et cybersécurité industriels chez Siemens.*

Les automates « récents » intègrent-ils des fonctions de cybersécurité ? Qu'en est-il du parc existant ?

Avant toute chose, quels sont les risques encourus par un automate industriel ? « *Le vol de propriété intellectuelle, la dégradation, ou tout bonnement la modification du code, afin de détruire les installations pilotées* », commente Jérôme Poncharal, de Rockwell Automation. La question de la vulnérabilité des API n'est donc pas anecdotique… « *Oui, les automates actuels sont protégés, déclare Thierry Vasjman. Nous utilisons des Asics qui intègrent du code compilé pour une complexité de décodage plus importante. Nos API emploient le protocole http avec mot de passe et accès web géré dans le code compilé. En 2014, nous intégrerons le https dans les automates, puis de la cryptographie et de la connexion VPN* ».

Chez Rockwell Automation, « *les automates Logix d'Allen Bradley intègrent la gestion des utilisateurs (authentification, autorisation, audit), le cryptage du programme ou encore le contrôle de signature électronique des firmwares. Les composants communicants font d'ailleurs l'objet de tests spécifiques visant à qualifier leur immunité vis-à-vis des menaces informatiques (exemple : attaques DoS, serveur web durci, limitation des ports accessibles, conformité ODVA…)* », note Jérôme Poncharal. Cependant, « *les investissements industriels en matière d'automatismes portent sur des durées importantes, supérieures à 10 ans. De ce fait, certains équipements vieillissants n'offrent pas*

les garanties suffisantes en matière de cyber protection et ne peuvent être mis à jour pour intégrer ces fonctionnalités. Le recensement des actifs de production est donc critique puisqu'il permet d'identifier les éléments vulnérables. Les plus critiques pourront être remplacés ou protégés en amont (segmentation réseau, accès physique), poursuit-il. Mais attention, l'automate n'est qu'un maillon. Il faut étendre à l'ensemble du réseau et de l'application informatique. »

Chez Schneider Electric, « *non seulement les automates actuels intègrent des fonctions de sécurité, mais les processus de développement aussi ont évolué et la cybersécurité est désormais prise en compte pendant le cycle de vie d'un projet, de la R&D jusqu'à la maintenance des équipements. Pour le parc existant et les systèmes plus anciens, les failles de sécurité, une fois identifiées, sont traitées par des patchs de sécurité et la méthode de réduction de risques* », affirme Laurent Raillier.

Enfin, « *après l'épisode Stuxnet, un plan cybersécurité a été lancé chez Siemens* », commente Jean-Christophe Mathieu. Chez le géant allemand, la cybersécurité est donc partout, depuis la conception des produits à la formation des techniciens, en passant par le codage des codes utilisés.

Une chose est sûre, « *on ne conçoit plus les automates comme il y a 10 ans. Désormais, ces aspects sont pris en compte dès le début. On peut d'ailleurs retarder la sortie d'un produit s'il n'est pas « cyber ». C'est déjà arrivé », note le spécialiste. Côté matériel, « Les plateformes actuelles intègrent, en ce qui concerne le programme actif, le chiffrement, la protection contre le copie et des mécanismes contre la manipulation frauduleuse de code, et, pour la partie communication et accès, l'authentification, un pare-feu, le filtrage d'adresse pour les accès console et le VPN, ainsi que la communication chiffrée avec les pupitres opérateurs », déclare Jean-Christophe Mathieu, de Siemens. « Pour les anciens systèmes, nous préconisons la défense en profondeur. De plus l'adjonction de coupleur de communication permet d'augmenter significativement le niveau de sécurité des installations existantes.* »

Attention, toutefois, « *certes, un automate est plein de trous mais le vrai point sensible, c'est la télémaintenance, la prise de contrôle à distance* », rappelle Jean-Christophe Mathieu. Quid du sans-fil ? « *Le sans-fil n'est pas robuste vis-à-vis de la sécurité. Il faut encadrer l'utilisation de ces technologies* », recommande Jérôme Poncharal. Pour autant, certains systèmes ne peuvent pas fonctionner sans technologie sans fil. Le problème n'est donc pas si simple à aborder. Le vrai danger ? « *Le brouillage de fréquence qui paralyserait le système* », ajoute Jean-Christophe Mathieu.

Comment choisir le bon niveau de protection ? Comment mettre en place cette solution ?

« *Le niveau de protection doit être adapté en fonction du type d'installation mais aussi du risque, de la vraisemblance de l'impact des événements redoutés. Avant de parler technique, il faut classifier l'installation pour déterminer la cible de ce que l'on a à protéger. Les moyens techniques arrivent en dernier lieu* », commente Jean-Christophe Mathieu. Selon le spécialiste de Siemens, la bonne démarche implique donc une analyse de risque qui associe sûreté de fonctionnement et cyber sécurité. Les question à se poser : « *quels sont les actifs à protéger et les menaces auxquelles ces actifs sont exposés et quelles conséquences peuvent-elles engendrer (pertes financières, impact environnemental, etc.) ?*, détaille Jérôme Poncharal. *Des solutions peuvent ensuite être proposées pour réduire le risque à un niveau acceptable pour l'exploitant. Les solutions technologiques proposées peuvent aller d'une simple formation des utilisateurs à la mise en œuvre d'un arsenal complet de contremesures. C'est le concept de défense en profondeur repris par le projet de norme IEC62443 (automates, réseaux, informatique, accès…). Enfin, la nature des menaces évoluant constamment, les contremesures en place doivent être régulièrement réévaluées et adaptées.* »

Thierry Vajsman.

Jérôme Poncharal.

Quelles solutions adopter ? Elles sont nombreuses. Selon Thierry Vasjman, il est possible d'assurer la protection en amont des API et des réseaux IP par l'intégration de firewalls industriels à tous niveaux et la création de cellules auto protégées, avec la notion de DMZ, une « zone démilitarisée », partie du réseau protégée, invisible et inaccessible à partir d'Internet. Concrètement, Phoenix Contact et sa filiale spécialisée Inominate préconisent notamment l'utilisation de certificats x.509v3 avec RSA PSK, d'encryptages AES 256,


Laurent Raillier.

Jean-Christophe Mathieu.

le filtrage de ports, de protocoles, voire horaire, la mise en place de communications VPN, la redondance de firewall, le mode transparent Stealth, ou encore le scan journalier des répertoires et la gestion des alertes (CIFS integrity monitoring).

Doit-on aller vers des communications sécurisées sur les réseaux ? « *On ne chiffre pas les communications entre les entrées/sorties et les automates pour des raisons de temps réel. Entre automates, on peut le faire sans rajouter d'équipements supplémentaires, mais le chiffrage aboutit à une dégradation des performances* », répondent les spécialistes. A noter également, l'ensemble des fournisseurs optent généralement pour des solutions dites de white listing, c'est-à-dire de définition de « listes blanches » d'outils et d'utilisateurs autorisés.

Les fournisseurs sont globalement très impliqués dans la définition des méthodes à suivre. « *Schneider Electric a publié plusieurs documents, livre blanc, guides de mise en œuvre et travaille depuis plusieurs mois dans des groupes de travail avec des confrères et l'Anssi à la rédaction de guides clairs et pratiques, note Laurent Raillier. Par ailleurs, nous pouvons également proposer des interventions sur le site du client à travers notre équipe d'experts et avec des partenaires spécialisés lorsque cela est nécessaire.* » En règle générale, les fournisseurs ont d'ailleurs des spécialistes IT chez eux et/ou se font assister par des partenaires.

Point important, « *quelle que soit la solution retenue, elle devra s'inscrire dans le cadre d'un système de gestion adressant tous les aspects de la sécurité : organisation, procédures, technologies…* », explique Jérôme Poncharal. Et « *lorsque cela est possible, l'analyse de risque doit être intégrée au projet afin de traiter de la sécurité sous tous ses aspects : sûreté de fonctionnement et cyber sécurité* », note Jean-Christophe Mathieu. Le problème : faire travailler ensemble les automaticiens et les informaticiens. Enfin, « *il peut également y avoir un problème de comportement des intégrateurs et des utilisateurs. Une protection par mot de passe aurait pu arrêter Stuxnet… Désormais, pour éviter cela, dans nos automates, le firmware impose de changer les mots de passe.* »

Comment informer l'utilisateur des dernières mises à jour et des correctifs s'ils existent ? Et avec quelle réactivité ?

Quel que soit le fournisseur, Internet constitue l'outil privilégié pour informer les utilisateurs. Chez Phoenix Contact, tout passe par exemple par le site de sa filiale Inominate, qui permet notamment les mises à jours automatiques des firewalls et les informations sur les évolutions majeures sont disponibles sur site du fournisseur. « *Nous informons également les utilisateurs par les ingénieurs réseaux et via un routage e-mailing mensuel vers nos clients utilisateurs* », annonce Thierry Vasjman.

Chez Rockwell, « *un site web dédié à la sécurité informatique a été mis en place. Ce lien permet de consulter les alertes relatives à la découverte de nouvelles menaces et de télécharger les correctifs correspondants. L'utilisateur du site peut également s'abonner aux alertes pour bénéficier de notifications automatiques* », commente Jérôme Poncharal. Et le fabricant d'automate met l'accent sur la réactivité. « *Lorsqu'une vulnérabilité est identifiée, par un utilisateur ou en interne, celle-ci est immédiatement qualifiée par une équipe dédiée avant d'être publiée sur le site Rockwell Automation Security, sous 2 à 3 jours. Cette alerte est accompagnée de recommandations visant à se prémunir du risque détecté. Un correctif définitif (patch, mise à jour firmware, palliatif) est ensuite proposé dans un délai moyen de deux à trois semaines suivant la notification* », poursuit Jérôme Poncharal.

Chez Schneider, on pousse l'information de façon ciblée. « *Les utilisateurs peuvent s'abonner à notre site web où notre CERT publie les failles de sécurité ainsi que les patchs de sécurité et les méthodes de réduction des risques. Ces informations peuvent être transmises automatiquement via un flux RSS. Nous proposons par ailleurs des contrats de maintenance qui nous permettent de gérer le déploiement des patchs après vérification de la non dégradation des performances par des tests sur une plateforme équivalente au système de production* », annonce Laurent Raillier.

Enfin, Siemens travaille en direct avec les industriels sous couvert de confidentialité. « *Nos clients peuvent suivre en ligne et gratuitement toutes les informations concernant la sécurité de nos composants d'automatismes et logiciels associés. Il est également possible de d'abonner au flux RSS et newsletter pour recevoir dans un délai très bref les informations de mise à disposition* », déclare Jean-Christophe Mathieu.

Attention, « *ce n'est pas parce qu'un patch est édité qu'il faut l'appliquer. On ne pousse pas à la mise à jour* », note Jérôme Poncharal. En particulier s'il y a un risque de voir le système d'exploitation « planter » après la mise à jour… ▮