La cybersécurité taillée pour l'Industrie du Futur

On attend aujourd'hui d'une installation industrielle qu'elle assure son rôle premier à savoir, la fabrication ou la transformation. Mais elle doit aussi opérer en toute sécurité au niveau humain, au niveau matériel ou encore, environnemental. Du bon sens et quelques précautions techniques permettent de prévenir les risques issus du numérique.

La mise en place d'une politique de cybersécurité dans l'entreprise industrielle passe d'abord par une information de l'ensemble du personnel sur la réalité des risques et sur les bonnes pratiques. Elle implique aussi de former aux technologies de communication, tous les intervenants directement concernés par la gestion et l'exploitation des systèmes d'automatisation. Viennent ensuite, l'organisation du travail et la mise en place de procédure en complément des solutions matérielles mises en place pour bloquer les intrusions, détecter les menaces et s'assurer de l'intégrité numérique de l'installation.

Force est de reconnaître que c'est dans les services IT que l'on trouve les collaborateurs les plus sensibilisés aux enjeux de la cybersécurité. En leur apportant une culture orientée vers la production, il est possible de les mobiliser afin qu'ils contribuent significativement à la mise en place des bonnes pratiques découlant de la politique de sécurité choisie jusqu'au plus profond de l'appareil industriel.

Ces recommandations de bon sens énoncées, voici une présentation de quelques-unes des offres en matériels, logiciels et services qui constituent les solutions de cybersécurité adaptées aux installations industrielles.

Convergence entre safety et security chez Rockwell Automation

Selon Rockwell Automation, la nécessité d'arriver à un suivi en temps-réel de la production industrielle, débouche obligatoirement sur la création de données numériques en grand volume. Ces informations issues des sites de production doivent circuler entre les réseaux OT et IT, ce qui oblige à repenser la sécurité informatique en profondeur.

A cette fin, le constructeur a constitué une équipe de consultant spécialisés qui compose le département Network Security Services (NSS), avec par exemple, une dizaine de personnes mobilisées en Europe. Rockwell Automation s'est aussi engagé dans un partenariat avec Cisco pour par exemple, accompagner les collaborateurs des entreprises vers les certifications CINS (Cisco Industrial Networking Specialist) qui constitue le pendant industriel du cursus IINS de la Cisco Networking Academy.

L'alliance entre Rockwell Automation et Cisco prend aussi la forme d'une ingénierie de réseau clé-en-main baptisée Converged Plantwide Ethernet (CPwE). Il s'agit d'une stratégie permettant de comprendre les besoins, les risques, d'identifier les étapes et l'ordre des mises en œuvre afin notamment, que la cybersécurité soit intégrée à toutes les étapes du processus. Cette stratégie s'appuie sur des référentiels qui prennent la forme de guides de mise en œuvre des architectures et de notes techniques d'application pour maîtriser la mise en place d'accès distants, la création de DMZ ou encore l'intégration d'extensions telles que les services d'identification (Identity Service Engine).

Automates, capteurs-actionneurs, dispositifs de contrôle-commande et logiciels chez Rockwell Automation sont mis en conformité avec la norme IEC 62443 qui constitue le référentiel en matière de cybersécurité. La technologie étant un des maillons du système de protection, les automates de Rockwell Automation intègrent en standard des fonctions de sécurité comme un compte d'administration et des clés de fonctionnement, etc. Ces prémisses permettent la création d'un domaine d'administration reposant sur un annuaire de type Active Directory. Une telle approche permet d'administrer les autorisations de manière centralisée ; un connecteur logiciel assurant la mise en relation avec les automates concernés. Cette fonction s'appuie sur les logiciels Factorytalk Directory qui recense la base de données des utilisateurs et Factorytalk Security qui fait le lien entre les utilisateurs référencés et les composants matériels et logiciels du système de contrôle-commande.

L'intégrité des micro-logiciels est aussi un élément essentiel de la cybersécurité. Chez Rockwell Automation, ils sont signés électroniquement, ce qui permet de garantir leur intégrité et leur authenticité en vue de leur déploiement sur les systèmes en service. Il en va de même pour les programmes destinés à s'exécuter sur l'automate qui peuvent eux-aussi, être signés numériquement grâce au logiciel Factorytalk Asset Center chargé de recenser une base de données

DESTACO PRODUCTS

Automation and Workholding

PINCES ET CHANGEURS D'OUTILS

Conçus pour les applications exigeantes et pour tout type d'environnements

- Très grande précision et répétabilité
- Capacité de chargement élevée
- Modularité et flexibilité
- De nombreux accessoires et options

SYSTÈMES DE BRIDAGE

Une gamme de serrages manuels et pneumatiques

- Robustesse
- Durée de vie et cadences
- L'expérience dans le domaine du serrage

L'INDEXEUR INTELLIGENT

NOUVEAUX INDEXEURS série MDE & HDE Premier boitier flexible du marché

- Sans jeu
- Très Haute précision
- Mouvements souples
- Hautes cadences

Contactez nous pour plus d'infos: **europe@destaco.com**

DESTACO
A DOVER COMPANY

Precision in Productivity™

destaco.com

End Effectors | Grippers | Indexers
Manual Clamps | Power Clamps | Remote Handling

des applications. Ce logiciel est ensuite capable de vérifier que les programmes qui s'exécutent sur les automates programmables de l'entreprise, sont bien authentiques. Factorytalk Asset Center joue aussi le rôle de coffre-fort virtuel pour les applications de l'entreprise dont il conserve une sauvegarde. Ce logiciel est donc en mesure de restaurer les applications en cas d'incidents.

Factorytalk est une infrastructure logicielle globale qui se subdivise en briques, certaines gratuites, d'autres payantes. Les services de cybersécurité par exemple, sont gratuits, ce qui ne sera pas le cas de Factorytalk Studio, Factorytalk Asset Center ou encore, Factorytalk View qui permet de connaître l'état des équipements (automates, actionneurs, capteurs intelligents, etc.) présents sur le réseau.

Les grands groupes industriels aujourd'hui et à plus ou moins brève échéance, les TPE et certaines PME vont connaître la convergence de leurs réseaux IT et OT. Rockwell Automation préconise le recours à des commutateurs Ethernet industriels Stratix sur la partie OT associé à des commutateurs Cisco pour la partie IT conformément à la norme IEC 62443 qui préconise la segmentation de l'infrastructure en trois couches comportant accès, distribution et cœur de réseau avec la mise en place d'une DMZ servant d'interface entre la partie IT et la partie OT. Cette dernière peut par exemple, prendre la forme d'un équipement Stratix 5950 qui concentre les fonctions de firewall temps-réel, de serveur VPN, d'analyseur de protocoles de contrôle-commande tout en assurant la détection, la prévention et le reporting des tentatives d'intrusion.

Schneider Electric, des équipements et des services dédiés

En tant que constructeur d'équipements industriels, Schneider Electric considère qu'il est de son devoir d'assurer la sécurisation des produits proposés à ses clients, tant pour les nouvelles installations que pour les infrastructures déjà opérationnelles.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a provoqué le rapprochement entre la société Stormshield – devenue filiale à 100% d'Airbus Defense & Space Cybersecurity – et Schneider Electric pour le développement d'un pare-feu industriel de confiance labéllisé afin d'offrir une plateforme matérielle aux opérateurs d'importance vitale (OIV).

La commercialisation de cette solution passe par le réseau d'intégrateurs de Schneider Electric, premier distributeur en mesure d'assurer sa mise en œuvre par des intervenants titulaires de certifications reconnues. Volontairement proposé à un prix attractif, cet équipement compact peut être placé au plus près des automates. Parallèlement, Schneider Electric fait évoluer ses équipements pour faire descendre la sécurité directement au cœur des installations industrielles. Le contrôleur d'automatismes Modicon M580 par exemple, intègre déjà un coupleur VPN/IPSec.

Pour le constructeur français, la maîtrise de la cybersécurité industrielle implique aussi de disposer d'un département spécialisé s'appuyant sur une équipe aux compétences larges. Elles s'étendent des automatismes à la sécurité informatique sans perdre de vue les impératifs de production, ce qui passe par une adaptation fine et précise des moyens mis en œuvre : vérification et sécurisation des postes de travail, surveillance des terminaux dédiés à la maintenance, mise en place de dispositifs de sécurité périmétrique, etc. Cette équipe intervient chez les clients équipés, en tout ou partie, en matériels siglés Schneider Electric.

L'accompagnement d'un projet de sécurité comporte des étapes quasi incontournables comme l'inventaire des équipements déployés et la cartographie de l'infrastructure de communication. A cela s'ajoute l'obligation d'intégrer la sûreté de fonctionnement (safety) pour prioriser les actions en phase avec les préoccupations des clients (budgets, arrêts ou mise à jour en adéquation avec les impératifs de production, le maintien des performances, la maintenance, etc.).

Outre une réflexion approfondie sur les besoins en ressources matérielles et logicielles, l'équipe de Schneider Electric porte un soin particulier à la formation des opérateurs qui prennent directement en charge de la maintenance de l'installation. Ainsi, les ingénieurs du département cybersécurité peuvent procéder à des mises à jour de micro-logiciels (firmware) mais en collaboration avec l'équipe de maintenance interne qui va apprendre à réaliser elle-même ces opérations afin d'être en mesure de les reproduire.

Une veille technologique est aussi assurée au niveau des logiciels embarqués au sein des équipements Schneider Electric pour identifier les vulnérabilités éventuelles, les référencer et les répertorier par appareils, par famille et évidemment, proposer des correctifs. Il peut s'agir d'une fonctionnalité utile comme par exemple, un service ftp qui peut être ouvert par défaut et qui doit donc être fermé pour éviter les risques. Il en va de même pour ce qui concerne les procédures d'accès par identifiant et mot de passe qui sont l'objet de véritables campagnes de sensibilisation pour que les opérateurs changent les valeurs enregistrées par défaut.

Enfin, Schneider Electric intervient aussi en tant qu'organisme de formation agréé dans la cybersécurité qui comprend évidemment, le déploiement et l'intégration du SNI 40.

Sentryo, ICS Cybersecurity

Sentryo est une startup créée en juin 2014 par Laurent Hausermann et Thierry Rouquet, deux spécialistes de la cybersécurité qui travaillaient précédemment chez Arkoon Network Security.

En quelques mois, cette entreprise a créée en collaboration avec des partenaires tels que le CEA, la solution ICS CyberVision. Elle permet une étroite collaboration entre automaticiens et experts en informatique ; ce qui est un facteur clé de succès pour la protection des réseaux industriels.

ICS CyberVision permet de prévenir les risques de compromission de l'infrastructure OT en apportant aux responsables concernés, une connaissance approfondie de tous les composants connectés au réseau, des flux de communication qu'ils échangent et des points de faiblesse. ICS CyberVision permet ensuite au travers de la constitution automatique d'un modèle de fonctionnement normal, de détecter les événements atypiques. Il facilite enfin la réponse à incident en rassemblant l'ensemble des informations nécessaires au travail d'investigation.

ICS CyberVision s'appuie sur des sondes qui analysent les flux applicatifs sur le réseau pour en extraire des métadonnées caractérisant le fonctionnement du réseau de contrôle commande. Ces informations sont ensuite agrégées sur le serveur CyberVision qui génère dynamiquement une carte de l'infrastructure qui délivre une vision instantanée de la situation : quel équipement est connecté, avec quels autres systèmes échange-t-il, quelles sont les points de faiblesses, etc. Ces sondes sont placées sur le réseau en fonction de sa topologie

Serveur et sonde de la solution ICS Cybervision.

Un vol de données sensible ou le piratage d'une application commence toujours par une opération anodine.

et des risques spécifiques (typiquement sur le réseau de contrôle derrière les stations Scada, derrière les connexions extérieures comme les pare-feux, les routeurs Wi-Fi, devant certains automates, voire sur le bus de terrain).

ICS CyberVision ne nécessite aucune modification de la topologie du réseau. Les sondes sont plug and play et fonctionnent à l'instar de diodes, ce qui garantit leur totale transparence tant pour le réseau que pour les dispositifs qui lui sont connectés.

Premier avantage, ICS Cybervision permet de faire de la prévention en fournissant une vision détaillée du réseau industriel. Le système permet par exemple, d'identifier si des patchs de mise à jour ou de sécurité doivent être appliqués et sur quels automates. Il repère aussi les accès déportés restés ouverts alors que le sous-traitant concerné n'a plus de raison d'intervenir. Il permet encore de savoir qu'un équipement nouvellement installé se connecte périodiquement à Internet pour récupérer des mises à jour alors que cela va à l'encontre des règles de sécurité et bien sûr, il identifie les mots de passe par défaut non changés, recense les serveurs web, ftp ou telnet ouverts, etc.

L'interface utilisateur est facile d'accès et simple d'emploi afin que la solution puisse être utilisée par des personnes qui ne sont pas spécialisées dans la sécurité informatique. Par exemple, les rapports consolident les données dans des fichiers au format PDF ou XLS. Il s'agit d'une caractéristique primordiale puisqu'elle permet aux automaticiens de mieux collaborer avec les équipes IT.

Sentryo dispose d'un laboratoire de sécurité technique qui entretient une base de connaissances pour tous les événements globaux relevant de la sécurité informatique industrielle (menaces, vulnérabilités connues des automates, tactiques de hacking, etc.). Les données alimentent une base de sécurité qui va ensuite être diffusée vers les serveurs ICS Cybervision afin d'assurer une surveillance des réseaux industriels en ayant la capacité de détecter les comportements suspects avec une acuité sans cesse remise à jour. ▮

Cypress, nouvel entrant attendu en… 2017

FPC Ingénierie et Netceler, deux sociétés installées en Rhone-Alpes ont constitué un consortium d'entreprises soutenu par la Région pour créer une solution de cybersécurité spécialement conçue pour les installations industrielles.

Leur effort porte sur la mise au point d'un système de détection d'intrusion (IDS) baptisé Cypress. Ce dernier vise à rétablir la connaissance du fonctionnement du système industriel pour connaître sa constitution matérielle et logicielle, maîtriser son fonctionnement et son comportement, gérer les évolutions du système sur toutes les couches, identifier les comportements suspects avant qu'ils aient un impact fonctionnel et enfin, détecter les intrusions et s'en protéger.

Pour cela, le système qui est encore en développement à l'heure actuelle, se propose de recenser les machines (type, rôle, etc.) et les protocoles utilisés et d'apprendre la dynamique des échanges pour constituer une base de connaissance servant de référentiel. Une fois cette étape élémentaire accomplie, il devient possible de détecter les écarts et d'émettre des alertes avant que la situation ne se dégrade au point d'entraîner un impact sur le fonctionnement de l'installation.

L'originalité de cette solution réside dans sa capacité à descendre jusqu'au niveau des échange de données entre les applications déployées au sein des systèmes industriels qu'il s'agisse d'automates programmables, d'IHM ou de systèmes de contrôle.

MANUFACTURING.FR