Dossier de presse

Cybersécurité industrielle

Les solutions Schneider Electric pour la sécurisation des infrastructures industrielles

Contact Presse
Schneider Electric France
Jean-Pierre Gherardi
Tél. : +33 (0)4 76 60 50 24
jean-pierre.gherardi@schneider-electric.com
www.schneider-electric.com

Contact Presse
Sine Nomine pour Schneider Electric
Nathalie Riera
Tél : +33 (0)6 82 83 34 20
schneider-electric@sinenomine.fr

Sommaire

Industrie connectée : enjeux et défis de la cybersécurité 3

Le programme Cybersécurité de Schneider Electric 4

Des équipes dédiées 4
Un ecosystème de partenaires 4

L'offre produits & services 5

Analyse de risque 5
Audit de conformité des réseaux industriels et SCADA 6
PLC-Log : surveillance d'état automate 6
Pare-feu industriel ConneXium 7
Pare-feu ConneXium TOFINO 7
CNM (ConneXium Network Manager) – Administration réseau industriel 8
Formation 8

Schneider Electric : le spécialiste mondial de la gestion de l'énergie 9

Industrie connectée : enjeux et défis de la cybersécurité

Aujourd'hui connectée, l'industrie est la cible de cyber-attaques de plus en plus nombreuses et sophistiquées. De la négligence à l'acte terroriste, les risques sont réels et les retours d'expérience de ces dernières années nous ont montré que les infrastructures industrielles étaient exposées et les systèmes de contrôle commande mal protégés pour faire face à ces menaces.

Stuxnet, le virus développé en 2010 par les États-Unis et Israël pour nuire au programme nucléaire iranien, aura eu un effet collatéral dont il faut se féliciter : les industriels ont depuis, pris conscience de l'importance de la cybersécurité et l'administration publie des guides de bonnes pratiques via les publications de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

De plus, la législation prend désormais en compte la sécurité des infrastructures industrielles à travers la loi de programmation militaire N° 2013-1168. Celle-ci intègre un volet cybersécurité à destination des opérateurs d'importance vitale (OIV).

Comment les constructeurs d'équipements industriels agissent-ils ?

Certains constructeurs ont déjà fait des pas de géant pour sécuriser leurs nouveaux produits et leurs gammes existantes. Toutefois, en dépit des progrès réalisés par des entreprises travaillant dans des domaines sensibles comme l'énergie ou les transports, la cybersécurité doit encore être promue au sein des directions pour qu'elle soit intégrée dès la phase de conception pour les projets industriels.

Sécuriser les procédés est insuffisant. Les différents acteurs (utilisateurs, constructeurs, intégrateurs) doivent mettre en place une démarche pour créer un cercle vertueux de la cybersécurité. Ce cercle se construit par étapes successives, de l'identification des risques à la formation des opérateurs, en passant par la conception de systèmes de sécurité et la mise en œuvre de dispositifs de protection, avec la réalisation de tests de validation. Parce que les stratégies d'attaque évoluent, il faut aussi que les systèmes de sécurité soient mis à jour et améliorés en permanence, et qu'un plan de maintien en condition de sécurité soit mis en place.

Appréhender la problématique en amont

Pour les équipements en service chez les clients (la base installée), les constructeurs ont eu pour premier réflexe de durcir leurs systèmes : identification de failles de sécurité des systèmes de contrôle-commande, puis mise à disposition de correctifs ou de méthode de mitigation. Mais il s'agit là d'une démarche en réaction à l'augmentation des cyber-attaques, ne constituant pas une réelle réflexion de fond.

Schneider Electric a choisi d'appréhender la problématique de la cybersécurité en amont, dès la conception des équipements. C'est le cas par exemple des automates M580, conçus selon le processus SDL (Secure Development Lifecycle). Ces nouvelles plateformes d'automatisme intègrent nativement des fonctions de sécurité et font l'objet de certifications internationales (Achilles L2).

Pour les industriels, la sécurisation de leurs process est un facteur clé de compétitivité et un enjeu majeur. Elle doit tenir compte des contraintes de production, de l'environnement et des exigences de sûreté de fonctionnement (disponibilité, sécurité, fiabilité et maintenabilité des systèmes). Leader des solutions de gestion de l'énergie et des automatismes, Schneider Electric occupe une place centrale au cœur de l'écosystème industriel. C'est pourquoi le Groupe a œuvré au développement d'une offre complète dédiée à ce segment de marché.

Le programme Cybersécurité de Schneider Electric

En France, les experts Schneider Electric en réseaux industriels et cybersécurité sont à même d'accompagner les utilisateurs dans toutes leurs démarches de sécurisation de leurs systèmes industriels.

Des équipes dédiées

Afin de répondre aux enjeux et exigences spécifiques de la cybersécurité des infrastructures industrielles, Schneider Electric a constitué des équipes et développé des centres de compétence dédiés.

Avec plus de 10 ans d'expérience, les experts en cybersécurité des systèmes industriels assurent une large gamme de prestations : analyse de risque, audit, conseil, conception d'architecture sécurisée, formation. En outre, les experts Schneider Electric disposent d'un grand nombre de certifications, notamment : GSEC, GCIA, GCIH, Hirschmann Belden, Fortinet, Cisco, F5, Checkpoint, Stormshield Network Security / Endpoint Security.

Un écosystème de partenaires

Schneider Electric, acteur incontournable de la filière française de cybersécurité, participe activement aux initiatives de l'ANSSI, et a développé des partenariats avec les acteurs majeurs de cette filière, comme Thales ou encore Airbus Defence & Space Cybersecurity.

L'offre produits & services

Schneider Electric propose un ensemble complet de produits et de services dédiés à la cybersécurité industrielle, depuis l'analyse des risques jusqu'à la formation, en passant par des firewalls spécifiques.

Analyse de risque

L'analyse des risques est une étape essentielle dans un projet de sécurisation. Elle permet d'identifier les vecteurs d'attaque, les scénarios de compromission et leur impact sur le système, et d'évaluer leur vraisemblance.

Forts de leur expérience dans les métiers et les technologies d'automatismes, les experts Schneider Electric assurent un service d'analyse de risques cyber des systèmes industriels afin d'identifier et d'évaluer l'ensemble de ces risques, pour ensuite définir, prioriser et planifier les actions correctrices.

Cette démarche s'appuie sur la méthodologie EBIOS (Expressions des Besoins et Identification des Objectifs de Sécurité) éprouvée dans le domaine de la cybersécurité et recommandée par l'ANSSI. Elle englobe l'ensemble des équipements d'automatisme de marque Schneider Electric ou de marque tierce, incluant principalement :

- Les Systèmes Numériques de Contrôle-Commande (SNCC ou DCS) ;
- Les systèmes de supervision ou Supervisory Control And Data Acquisition (SCADA) ;
- Les Automates Programmables Industriels (API) ;
- Les Interfaces Homme Machine (IHM) ;
- Les réseaux Ethernet ou propriétaires et les équipements réseaux (commutateurs, routeurs, pare-feux).

L'activité humaine étant aussi vecteur de menace, l'analyse de risque couvre l'ensemble des métiers directement liés au système d'automatisme de l'entreprise, dont l'exploitation (comprenant les opérateurs de conduite de production), la maintenance (corrective et préventive, ou autres activités de modification) et tout autre métier interagissant avec le système.

Audit de conformité des réseaux industriels et SCADA

Schneider Electric réalise des audits de conformité des infrastructures industrielles par rapport à un référentiel retenu : ce peut être celui de l'ANSSI ou celui de l'entreprise. Ces audits permettent de :

- Faire un état des lieux de l'existant (architecture automates et réseau industriel) ;
- Lister les écarts par rapport au référentiel retenu ;
- Proposer des recommandations afin d'améliorer la sécurisation des architectures ;
- Proposer un plan d'actions et un accompagnement vers la sécurisation de l'installation.

Partie automatisme

L'**audit de configuration** est l'analyse des programmes comprenant : l'étude détaillée des communications inter-automates, la reconstitution de la cartographie des flux échangés sur le réseau industriel, l'analyse de la charge processeur et la quantification des réserves. Elle établit, les recommandations pour alléger les ressources de communication et ainsi éviter les erreurs de connexion et les perturbations sur le réseau industriel.

L'**audit de sécurité** porte quant à lui sur l'implémentation des fonctions de cybersécurité disponibles dans la gamme automate concernée, les recommandations des fonctions à mettre en œuvre, l'analyse de l'exposition aux vulnérabilités découvertes, et la proposition de plan d'actions correctives.

Partie réseau industriel

L'**audit d'architecture réseau** analyse la configuration des équipements réseaux (commutateurs, routeurs) selon le protocole de redondance retenu, ainsi que les logs des équipements. Ce process mesure également les flux en différents points stratégiques du réseau afin d'analyser la bande passante et les éventuelles erreurs de communication.

L'**audit de sécurité** analyse le paramétrage des équipements réseaux d'un point de vue sécurité.

PLC-Log : surveillance d'état automate

PLC-log est une solution permettant de surveiller les automates programmables Schneider Electric du réseau industriel et d'afficher de façon centralisée les écarts de fonctionnement des automates (variation des temps de cycles, anomalies liées aux communications, modification des firmwares, etc.) qui pourraient révéler une cyber-attaque

PLC-log est constitué d'une sonde industrielle embarquant une application qui interroge cycliquement les automates de gammes Schneider Electric. Sa fonction est de détecter toute variation de performance ainsi que les modifications des logiciels embarqués (firmwares, applicatifs). Ces informations sont remontées vers une supervision de sécurité via les protocoles Syslog et OPC.

Caractéristiques techniques

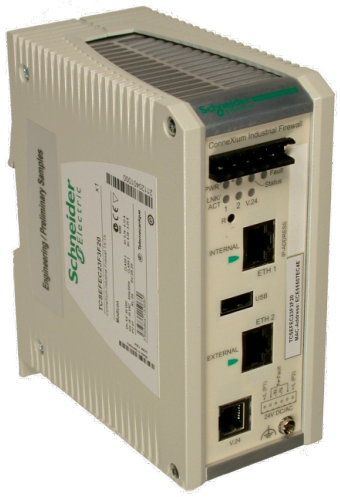
PLC-Log est supporté par un PC industriel Schneider Electric Magelis iPC conçu pour environnements sévères.

De maintenance simplifiée (sans ventilateur, disque dur statique), Magelis iPC propose des options haute disponibilité (disque dur RAID et batterie de secours) et une surveillance du système intégrée. La tenue en température, aux vibrations et aux chocs mécaniques lui permet de fonctionner en continu dans des environnements très difficiles.

PLC-Log fournit aux industriels un moyen de détection d'attaques sur leurs systèmes comme par exemple la modification de firmwares, les tentatives d'intrusion, ou encore le déni de service.

Pare-feu industriel ConneXium

Le pare-feu industriel ConneXium est un dispositif de sécurité conçu pour aider à protéger les réseaux industriels et les systèmes d'automatismes de menaces externes. Les règles de filtrage intégrées au pare-feu permettent d'appliquer une politique de gestion des flux (autoriser/interdire des flux) en fonction du protocole de communication et des services. Des fonctions de redondance permettent d'intégrer ce firewall dans des architectures sécurisées (en mode Transparent et Routé).



Le pare-feu industriel ConneXium intègre un ensemble de règles de filtrage permettant de :

- Limiter le trafic réseau aux périphériques autorisés ;
- Limiter le trafic réseau aux types de services de communication autorisés ;
- Séparer physiquement le réseau Process des autres réseaux (supervision, bureautique, etc.) ;
- Masquer un réseau ou un périphérique grâce à la fonction de Translation d'Adresse (NAT).

Ce firewall permet ainsi le cloisonnement et le filtrage entre des entités fonctionnelles en proposant des outils intégrés de pointe : segmentation, VPN, tentative d'intrusion, déni de service, alarmes au format Syslog.

Pare-feu ConneXium TOFINO

TOFINO gère la sécurité des protocoles industriels utilisés dans les réseaux d'automatisme (Modbus, Ethernet IP, OPC, etc.). Les règles de filtrage permettent de configurer les requêtes de communication autorisées vers les systèmes de contrôle-commande et les SCADA (lecture/écriture des registres applicatifs, commandes systèmes RUN, STOP, etc.).

Le pare-feu ConneXium TOFINO pour réseaux Ethernet industriels est un dispositif de sécurité conçu pour protéger les réseaux industriels, les systèmes d'automatisme, les systèmes SCADA et les process contre les attaques informatiques externes.

Il offre une protection sur mesure pour la base installée et les nouvelles installations exigeant un niveau de sécurité renforcé, et permet de délimiter des zones sécurisées au sein d'un système global. TOFINO inclut les trois modules de sécurité suivants :

- *Pare-feu* : permet de créer des règles qui identifient les équipements autorisés à communiquer à l'aide des protocoles spécifiés ;
- *Modbus TCP, Ethernet IP, OPC « enforcers »* : inspection approfondie des paquets pour détecter et bloquer tous les messages non autorisés ;
- *Consignation d'événements* : maintient un fichier-journal des événements de sécurité et permet l'accès à ce journal.

TOFINO n'a pas d'adresse IP : il est quasiment indétectable avec des moyens classiques. Pour plus de sécurité, le paramétrage du pare-feu s'effectue hors ligne. Il protège ainsi le parc automates et les SCADA des menaces cyber, notamment en sécurisant les protocoles industriels, en bloquant les requêtes d'écritures et les tentatives de mise en STOP des API, et en assurant le filtrage des équipements connectés.

CNM (ConneXium Network Manager) – Administration réseau industriel

Lorsque les composants individuels d'un réseau doivent être regroupés en un système intégral, ConneXium Network Manager (CNM) constitue une solution permettant de configurer et de surveiller l'ensemble des équipements de l'architecture client : commutateurs, routeurs, pare-feu, équipements wifi, qu'il s'agisse d'équipements Schneider Electric ou de produits d'autres fabricants.

CNM est configuré pour des systèmes industriels de gestion d'un haut degré d'exigence et s'intègre sans difficulté dans des applications SCADA. Il comporte un serveur SNMP /OPC intégré. Son interface opérateur graphique est disponible comme contrôle ActiveX. La dernière version de CNM offre plusieurs nouvelles fonctionnalités et perfectionnements :

- Architecture hiérarchique de serveurs pour la gestion de réseau ;
- Programmation de tâches (Task Scheduler) ;
- Multiples configurations de règles de sortie de données VLAN ;
- Affichage du numéro de série du produit dans l'onglet Device ;
- Affichage du délai de réponse et du timeout d'un équipement ;
- Réacheminement des événements ;
- Accès à la ligne de commande CLI (Command Line Interface).

Formation

Afin de sensibiliser et de former le personnel d'une entreprise, Schneider Electric a développé des modules de formation dédiés à la cybersécurité des systèmes industriels. Les stages sont dispensés dans les locaux de Schneider Electric ou sur site client. Les formateurs sont des experts « terrain » confrontés quotidiennement aux contraintes industrielles de leurs clients. Décomposé en trois niveaux, le parcours de formation est ainsi adapté aux exigences et aux différents interlocuteurs de l'entreprise.

	Production maintenance	Ingénierie, travaux neufs	Administration RSSI
Basique (1j) Sensibilisation du personnel. Les bonnes pratiques au sein de l'entreprise.	☑		
Avancé (2j) Méthodologie, standards de cybersécurité. Utilisation, paramétrage de firewalls.	☑	☑	
Expert (3j) Spécificités et protection des systèmes de contrôle-commande industriels.		☑	☑

Schneider Electric : le spécialiste mondial de la gestion de l'énergie

Schneider Electric est le spécialiste mondial de la gestion de l'énergie et des automatismes et a réalisé 25 milliards d'euros de chiffre d'affaires en 2014.

Nos 170 000 collaborateurs répondent aux besoins de clients dans plus de 100 pays en les aidant à gérer leur énergie et leurs processus de manière sûre, fiable, efficace et durable.

Des interrupteurs les plus simples aux systèmes d'exploitation les plus complexes, nos technologies, logiciels et services permettent à nos clients d'optimiser la gestion et l'automatisation de leurs activités.

Nos technologies connectées contribuent à repenser les industries, à transformer les villes et à enrichir les vies de leurs habitants. Chez Schneider Electric, nous appelons cela : **Life Is On**.

www.schneider-electric.com

Découvrez Life is On

Suivez-nous sur :