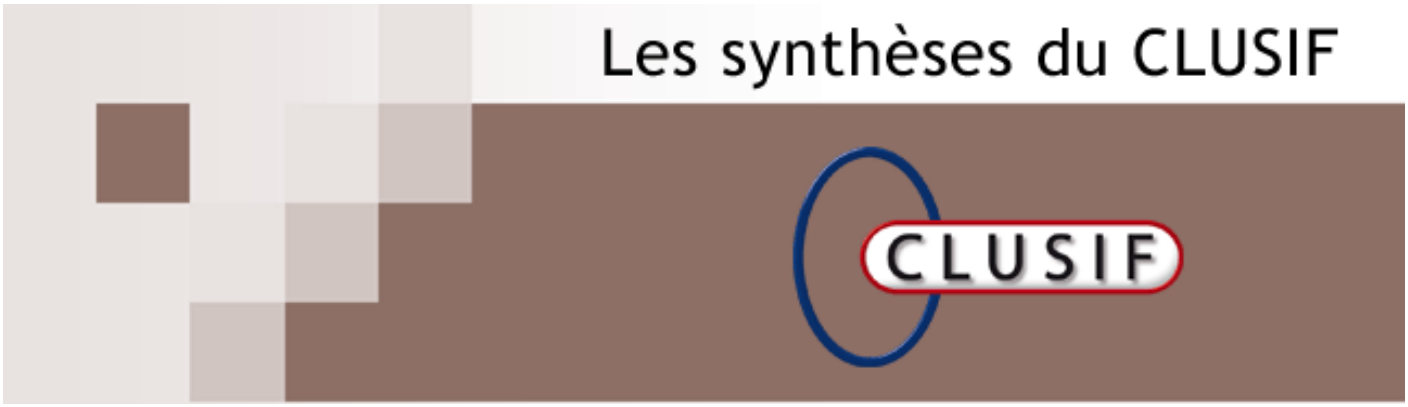

SI Industriels en 2017 : Incidents, enjeux et… parades - *Synthèse de la conférence thématique du CLUSIF du 20 avril 2017.*

Le CLUSIF a souhaité aborder les problématiques de sécurité qui se posent dans le cadre des systèmes d'information industriels. Au cours d'une conférence tenue le 20 avril, le groupe de travail SCADA a présenté le fruit de ses travaux. « *Aujourd'hui, des systèmes industriels informatisés gèrent des réseaux d'importance majeure (eau, énergie, transports). Les enjeux sont importants : il peut s'agir de sécurité des personnes, de santé publique ou de services vitaux qu'il faut défendre contre des incidents parfois graves* », a indiqué Thierry Chiofalo.

Pour ce dernier, dans le cas des SCADA, la démarche de sécurisation peut différer de celle que l'on pourrait appliquer à un système dédié au back office par exemple. Les parties prenantes sont diverses, puisqu'il faut intégrer la direction industrielle, tout comme les facteurs externes (la Loi de programmation militaire). Il peut aussi exister des outils spécifiques.

Apprendre de nos incidents

Anthony DI PRIMA, Wavestone, animateur du Groupe de Travail « Sécurité SCADA » au CLUSIF

Anthony Di Prima, animateur du groupe de travail consacré à la sécurité des systèmes SCADA, a fait un point sur les travaux du groupe qui publiait vendredi 21 avril son document synthétisant des fiches incidents dans ce domaine. Créé en 2013, le groupe a focalisé son activité en 2016 sur les enseignements à tirer en cas d'incidents et d'attaques survenues sur les systèmes industriels. Des fiches ont ainsi été réalisées à partir de cas réels, d'incidents ou de preuves de concept. « *Le document s'adresse bien entendu aux responsables sécurité des systèmes d'information, mais aussi à une population plus large, telle que des techniciens, mainteneurs, intégrateurs, éditeurs, responsables informatiques, responsables d'exploitation et industriels voire des directions générales, amenés à traiter cette problématique* », a précisé Anthony Di Prima.

En se basant sur des sources publiques ouvertes, les membres du groupe ont recensé les incidents connus liés à des SCADA, sans restriction temporelle. Chacun des incidents retenus (une vingtaine) ont fait l'objet d'une fiche. Il s'agit d'événements pour lesquels suffisamment d'éléments étaient disponibles et permettaient de décrire le déroulé de l'attaque et ses impacts. Les incidents devaient avoir atteint le SI industriel ou son environnement proche et être décrits par des sources multiples et concordantes.

Chaque fiche est constituée de deux pages. La première comportant un visuel et la description synthétique de l'attaque (Année, secteur, lieu, impact, scénario, vulnérabilité exploitée). La seconde contient le déroulé et les impacts (niveau de gravité, motivation de l'attaquant, complexité de l'attaque, déroulement, moyens mis en œuvre, enseignements, préconisations et contre-mesures, sources).

Les pays les plus touchés sont les plus industrialisés (USA/Europe). Anthony Di Prima note toutefois qu'il existe une réglementation aux États-Unis, imposant aux entreprises de signaler certains incidents, ce qui peut expliquer la prépondérance des événements liés à ce pays dans l'étude. Parmi les enseignements du document publié par le groupe de travail SCADA du CLUSIF, on retiendra que les attaques de gravité majeure sont d'un niveau de complexité élevé, voire très élevé : elles sont rendues possibles si l'attaquant dispose de moyens financiers et matériels conséquents et d'un haut niveau d'expertise. En effet, une attaque sur un système industriel

nécessite une connaissance pointue du métier et des processus associés. Ce qui explique peut-être pourquoi de telles attaques sont encore peu nombreuses.

Par ailleurs, l'augmentation croissante ces dernières années du nombre d'incidents s'explique sans doute par une généralisation des technologies de l'information : la plupart des protocoles industriels sont à présent déclinés sur TCP/IP, et de plus en plus de logiciels de niveau 2 (supervision, historisation) voire des composants de niveau 1 (PLC, RTU) fonctionnent sur des systèmes d'exploitation issus du monde IT classique. L'interconnexion des réseaux industriels avec les réseaux de bureautique, dans des objectifs de performance, de reporting et d'économie impacte probablement ces systèmes, tout comme la sous-traitance des projets, les astreintes distantes et l'externalisation de la maintenance qui multiplient les accès aux réseaux industriels.

Le groupe de travail relève que le contrôle des flux logiques et physiques aux interconnexions entre le SI de gestion et le SI industriel et au sein de ce dernier auraient constitué des mesures efficaces pour contrer les incidents. Tout comme la maîtrise des accès externes avec authentification forte et des procédures d'isolement en cas d'alerte.

Avec cette liste de « fiches incidents », le CLUSIF espère contribuer à une prise de conscience du niveau du risque dans le domaine des SCADA, afin que des plans de sécurisation ambitieux soient déployés rapidement, avant que des incidents graves ne surviennent.

En effet, le CLUSIF note que les États se dotent d'un arsenal cyber afin d'être en mesure de mener des opérations sur le théâtre cyber. Or, les systèmes industriels sont des cibles de premier choix pour la déstabilisation d'un État au regard des impacts que peuvent engendrer les attaques. Parmi les fiches du document, on trouve par exemple des incidents qui ont interrompu la production d'électricité ou qui ont abouti à un empoisonnement de l'eau potable. En outre, La « démocratisation » des logiciels d'attaque, comme par exemple la publication du code source Mirai, permet à des acteurs disposant de moyens limités, de réutiliser ces outils à moindre frais : à chaque attaque étatique (Stuxnet, Shamoon, Ukraine) on assiste à un transfert d'idées et d'outils. Avec l'émergence de l'industrie 4.0, l'introduction massive des objets connectés au niveau terrain risque d'étendre considérablement le niveau d'exposition des SI industriels. Leur utilisation en contexte urbain introduit également des problématiques liées à la protection des données à caractère personnel (jusqu'à présent restreintes aux SI de gestion).

Au cours de la conférence du CLUSIF, trois entreprises (Michelin, Engie et RTE) ont présenté des retours d'expérience en matière de protection des SCADA.

La sécurité des SI Industriels aujourd'hui et demain

Pierre RAUFAST et David ARNOLD, MICHELIN

Pierre Raufast et David Arnold ont ainsi rappelé que Michelin comptait près de 70 usines dans 17 pays, avec différentes activités et donc différents types d'outils industriels. Les contraintes sont multiples. La disponibilité attendue est de 24 heures sur 24, sept jours sur sept avec une obsolescence (mécanique et automatisme) subie. L'équipe informatique industrielle est par ailleurs restreinte et n'est donc pas présente en permanence sur tous les sites.

Michelin a commencé par procéder à un inventaire des systèmes existants ainsi que des vulnérabilités avant de procéder à une séparation des réseaux industriels et de gestion. Parmi les challenges à venir, l'entreprise note « l'usine 4.0 » et l'Internet of Things portés par la volonté de « digitaliser » l'entreprise. Mais également une augmentation des cyber-attaques industrielles dans un contexte difficile de sécurisation des automates et où la surface d'attaque augmente (mobilité, IoT, ATAWAD, BYOD).

Pour Michelin, une grande coopération entre la direction des systèmes d'information et de l'informatique industrielle est un facteur de succès.

Panorama des menaces et stratégie de réponse

Faiz DJELLOULI, ENGIE

Faiz Djellouli a pour sa part évoqué les actions d'Engie dans le domaine. Il a également pointé l'importance de l'engagement corporate à travers toutes les entités afin de couvrir à la fois l'information technology (IT) et l'operational technology (OT).

De même, il rappelle que les systèmes de contrôle industriels ont une obsolescence comprise entre 10 et 20 ans tandis que les systèmes d'information traditionnels ont une obsolescence de deux à trois ans. Si ces derniers peuvent subir des arrêts en dehors des horaires de bureau, ce n'est pas le cas des premiers qui doivent offrir un fonctionnement stable vingt-quatre heures sur vingt-quatre 365 jours par an.

Pour Faiz Djellouli, comme pour les autres intervenants, l'attaque d'une centrale nucléaire iranienne par Stuxnet a marqué les esprits. D'une possibilité, on est passé à une réalité avec une attaque ciblée très sophistiquée.

Concilier fiabilité et sécurité

Frédéric LENOIR, RTE

Pour Frédéric Lenoir de RTE, la problématique SCADA est centrale. Ces systèmes longtemps difficiles à atteindre et donc peu ciblés, le sont désormais. En outre, il convient désormais d'appliquer l'arrêté sectoriel du domaine « électricité » de la Loi de programmation militaire sur le périmètre le plus sensible du SI (systèmes SCADA et Contrôle commande).

Trois grandes évolutions sont intervenue au sein de RTE : la centralisation du système SCADA de téléconduite, une transformation des réseaux TCM de collecte et l'environnement est devenu plus « hostile » avec la multiplication des cyber menaces. Frédéric Lenoir note que les coûts des cyber-attaques sont trois fois supérieurs à ceux des catastrophes naturelles contre lesquelles les entreprises sont généralement bien protégées.

Table ronde

Animée par Henri CODRON, Vice-Président du CLUSIF
Participants : Jean CAIRE (RATP), Christian MEYER (EDF), Patrice BOCK (SENTRYO), Frédéric DANIEL (Orange Cyberdefense), Arnaud SOULLIER (Wavestone)

Au cours de la table ronde qui a suivi les retours d'expérience, Frédéric Daniel, d'Orange Cyberdefense, a rappelé les problèmes rencontrés par les organisations dans le cadre des SCADA : patch management, systèmes d'exploitation obsolescents, gestion des utilisateurs tant sur les systèmes que sur les lieux physiques, gestion des malwares presque inexistante, difficulté de ségrégation des réseaux. Pour Orange Cyberdefense, il est très important de faire un état des lieux du SI industriel.

Patrice Bock, de SENTRYO, explique que toutes les entreprises pour lesquelles il a opéré des prestations de conseil pendant six ans étaient infectées par des virus. L'une d'entre elles a été arrêtée pendant une semaine pour cette raison. Selon lui, les cryptolockers et autres ransomwares se multiplient même si une grande partie des incidents ne deviennent pas publics. Autre principale source d'incidents : la maintenance, les salariés ou les stagiaires qui peuvent provoquer des incidents, même non-intentionnellement.

Pour Jean Caire, de la RATP, il est souvent difficile de convaincre des gens des systèmes industriels d'un risque cyber. D'autant que dans le domaine du transport sur rail, identifier des scénarios fonctionnels permettant de provoquer un accident est une tâche très compliquée. Le ferroviaire demande une connaissance très poussée des systèmes et il est rare, voire impossible de trouver des prestataires extérieurs pouvant apporter ce type de scénarios. Par ailleurs, il est plus simple et bien moins coûteux de provoquer un accident avec une attaque physique. Ceci étant dit, la cyber-sécurité est imposée par l'État dans le cas de la RATP même si les méthodes à suivre officielles sont peu fournies. Jean Caire souligne par ailleurs que lorsque les systèmes sont homologués, il devient difficile d'appliquer des patchs. Enfin, « *on mesure mal l'impact des mesures de sécurité pour les systèmes sur les personnels en période de stress dû à un incident* », précise-t-il.

Christian MEYER, en charge de la cyber-sécurité des centrales nucléaires pour EDF a pour sa part rappelé que le numérique apporte aussi de nombreuses choses positives comme le monitoring. Le danger vient, selon lui, des passerelles qui se créent entre systèmes en période de « digitalisation » d'une entreprise. Dans le cas des centrales, il a indiqué qu'un opérateur en salle doit avoir la main sur la réaction nucléaire pour un arrêt manuel. L'Agence internationale de l'énergie atomique (AIEA) s'est intéressée au sujet cyber et a poussé des règlementations avec une approche graduée sur la sécurité des systèmes, a-t-il précisé.

Enfin, Arnaud SOULLIER de Wavestone, a présenté un projet de recherche et développement (Diode) qui permet d'améliorer la sécurité des systèmes SCADA en rendant les flux unidirectionnels, comme pour le cas des export de fichiers industriels vers le SI de gestion ou le partage d'écran pour télémaintenance sans possibilité d'agir sur la machine.