

CONGRÈS

COMPTE RENDU

CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS

Retour sur une journée d'informations et de débats

27 mars 2008
Paris

► Pascal LAMY,
INRS, département Ingénierie des équipements
de travail

Le Club Automation, association loi 1901, se définit comme pôle de rencontres entre automaticiens, informaticiens « temps réel » et responsables de production et d'ingénierie industrielle. Il a organisé le 27 mars 2008, une journée d'informations et de débats sur la cybersécurité des systèmes industriels et de contrôle-commande de machines, du fait de leur ouverture au monde extérieur par l'intermédiaire de connexion Internet.

La journée intitulée « Êtes-vous réellement prêt en cybersécurité ? » a été axée autour de présentations générales de sensibilisation à la cybersécurité et à la cybercriminalité ainsi que de présentations d'actions mises en œuvre chez divers industriels afin de se prémunir contre ce type de risque. L'INRS s'est intéressé aux conséquences de ces nouveaux risques pour la sécurité et la santé des opérateurs.

Au moment de la conception des normes de sécurité fonctionnelle (CEI 61508), les systèmes de contrôle-commande pouvaient encore être considérés comme isolés de l'environnement informatique général. Ils utilisaient en effet des réseaux de communication, des stations de travail, des systèmes d'exploitation spécifiques, ce qui rendait le problème de la vulnérabilité aux intrusions moins critique qu'à présent (cf. *Figure 1* pour l'architecture réseau d'une installation industrielle).

Aujourd'hui, le contexte a changé et il faut envisager la construction d'un programme de sécurité aux intrusions spécifiques au cas des systèmes industriels et de contrôle-commande. La vulnérabilité de ces systèmes s'accroît avec leur ouverture. En effet, la tendance et les développements actuels vont vers

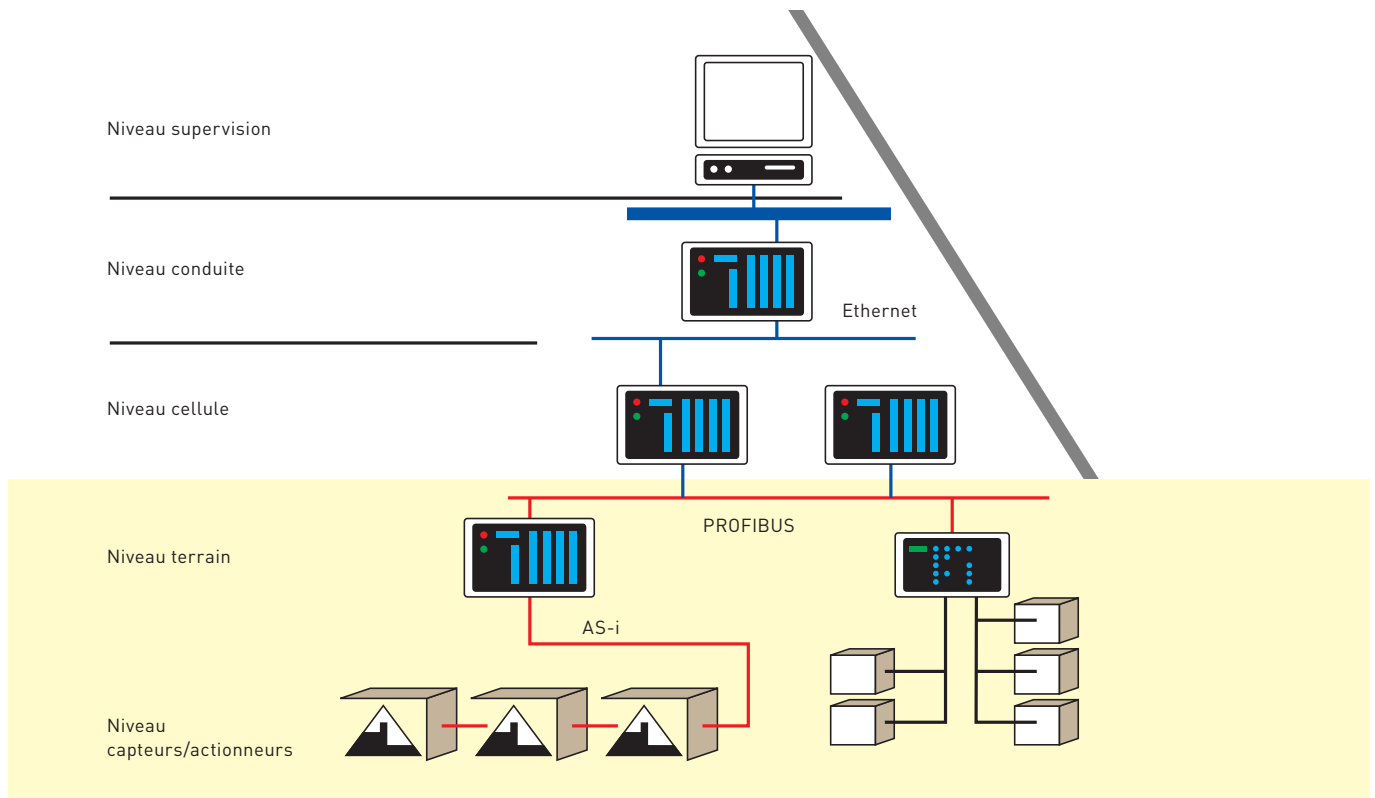
l'utilisation d'Ethernet au plus près du niveau terrain, du fait de l'apparition de standards du type EthernetSafe.

De plus, au travers de la *Figure 2*, nous remarquons que des outils d'ingénierie peuvent être connectés au réseau de l'entreprise et servir de lien avec l'installation automatisée.

La cybersécurité en informatique industrielle a trait à la prévention des risques et à la prise en compte des actes malveillants associés à l'utilisation des systèmes informatiques, réseaux de communication et systèmes d'informations pour les systèmes de contrôle-commande. On peut ainsi citer les tentatives d'intrusions, liées à des actions malintentionnées, au travers des équipements informatiques et des réseaux de communication constitutifs du système.

FIGURE 1

Les différents niveaux « réseaux » d'une installation industrielle



Ces risques peuvent se traduire entre autres par des pertes de production, des pertes de données sensibles, des incidents sur le procédé, la mise en danger des personnels d'exploitation, des atteintes à l'environnement,...

Selon une enquête du British Columbia Institute of Technology, institut universitaire canadien, l'origine principale des cyber incidents, incidents ayant pour origine les connexions réseaux, sur les systèmes de contrôle-commande de procédé a changé totalement de nature. Elle est passée d'une origine accidentelle (défaillance « matérielle » du service) à une origine externe (attaque du type logiciel malveillant par des pirates, des entreprises concurrentes qui veulent s'emparer d'un secret industriel). La part pour les origines externes est ainsi passée de 27 % sur la période 1982-2001 à 61 % sur la période 2002-2005. La part des origines internes, menaces effectuées inconsciemment par des personnes de l'entreprise, par exemple connexion d'un équipement infecté, est quant à elle passée de 15 à 7 %.

Conscient de l'émergence de ces problèmes, le Club Automation, regroupant des membres exerçant une activité dans le domaine des systèmes automatisés et de contrôle-commande, a organisé une journée d'informations et de débats sur le thème de la cybersécurité des installations automatisées et des systèmes de contrôle de procédé.

En introduction à cette journée, Jean-François Pacault, Haut Fonctionnaire du ministère de l'Economie, des Finances et de l'Industrie, est venu présenter un document de sensibilisation élaboré en coopération avec un groupe de grands industriels et destiné aux chefs d'entreprise et à leurs directeurs industriels. Ce document inclut quelques unes des questions ci-dessous et donne les grandes lignes de la démarche de sécurisation.

Plus précisément, un premier test pour les entreprises est de répondre ou de s'assurer d'avoir une réponse aux questions ci-après.

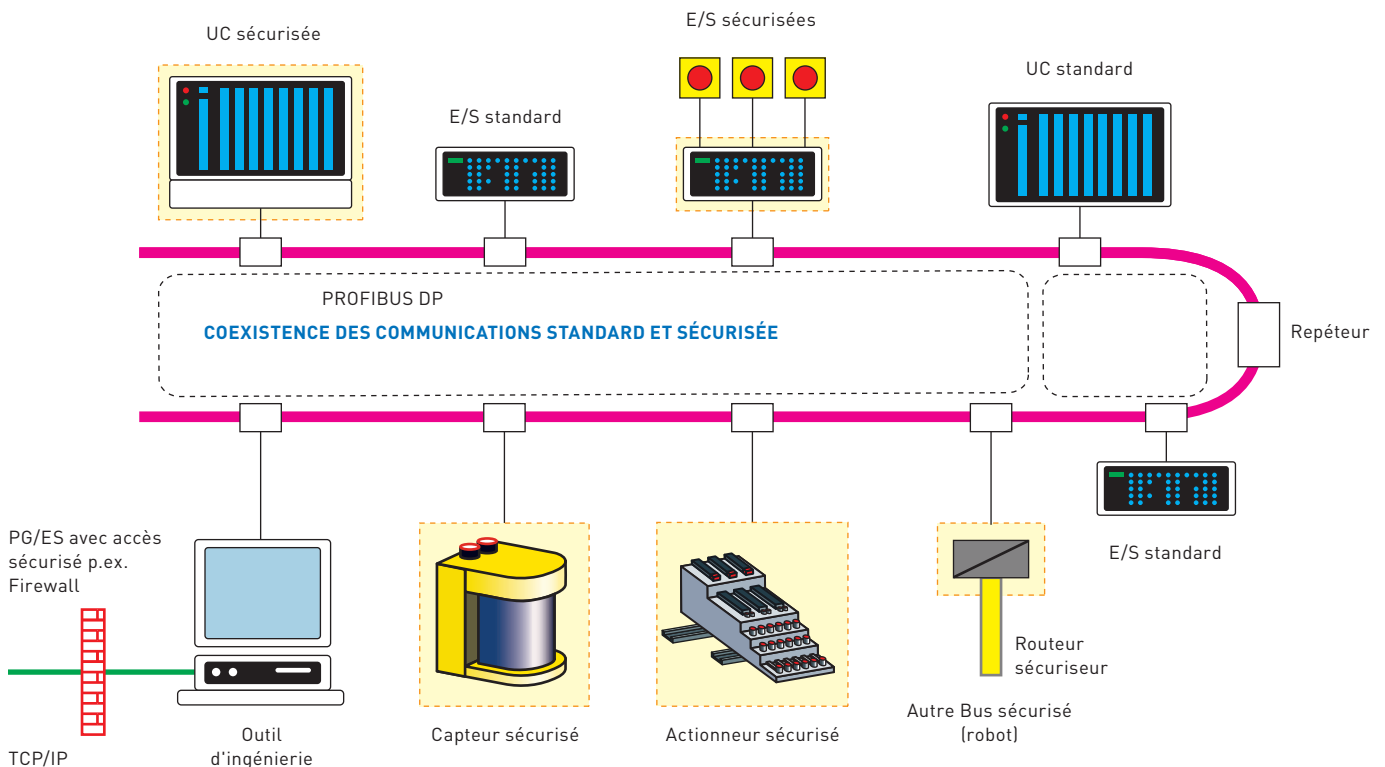
SAVEZ-VOUS SI VOUS ÊTES VULNÉRABLES ?

LES ATTAQUES COURANTES SUR LA BUREAUTIQUE SONT IMPOSSIBLES SUR L'INFORMATIQUE INDUSTRIELLE (VIRUS, EXPLOITATION DE VULNÉRABILITÉS, MALVEILLANCES INTERNES...) : VRAI OU FAUX ?

Faux : l'une et l'autre utilisent les mêmes produits (Windows, Unix...) et les mêmes protocoles (IP en général). Elles présentent donc le même genre de vulnérabilités et les mêmes malveillances qui auront les mêmes effets informatiques (mais pas les mêmes conséquences sur l'entreprise). Par exemple, en janvier 2003, le virus Slammer s'est introduit dans les ordinateurs de commande de la centrale nucléaire américaine Davis Besse par une connexion non sécurisée avec le réseau bureautique. Impact : un système de contrôle de la sûreté de la centrale est resté indisponible pendant près de 5 heures !

FIGURE 2

Architecture d'une installation et connexions au réseau de l'entreprise



SAVEZ-VOUS SI VOS RÉSEAUX D'INFORMATIQUE INDUSTRIELLE SONT BIEN PROTÉGÉS DU RESTE DE L'ENTREPRISE ET DU MONDE EXTÉRIEUR ?

Êtes-vous sûr que les connexions vers l'extérieur de votre système de contrôle de processus, et notamment les accès Wi-Fi, sont correctement recensées et sécurisées ?

Il n'est pas rare de découvrir par hasard des bornes Wi-Fi et des modems reliés au réseau téléphonique public dont les administrateurs système ignorent l'existence.

Exemples : en 2006, sur une durée d'un an environ, des pirates ont espionné les connexions Wi-Fi des caisses de la chaîne de supermarchés américains TJX qui n'étaient pas sécurisées. Ils ont ainsi récupéré des millions de numéros de cartes bancaires qu'ils ont utilisés au détriment des clients de TJX. Dans l'exemple précité de la centrale nucléaire

Davis Besse, le virus Slammer s'est introduit par une connexion non sécurisée alors que les équipes croyaient être protégées par un pare-feu.

Êtes-vous certains que les ordinateurs portables et PDA qui se connectent occasionnellement au système de contrôle de processus, ou les clés USB qui y sont parfois introduites, ne peuvent pas y introduire de code malveillant, au moins sans détection immédiate ?

Cette cause d'infection est de plus en plus fréquente sur les réseaux bureautiques : pourquoi pas sur l'informatique industrielle ?

Êtes-vous certains que les connexions temporaires du système de contrôle de processus (pour des mises au point diverses, pour des mises à jour, pour la télémaintenance...) vers l'extérieur sont surveillées quand elles sont établies et sont désactivées quand elles ne sont plus nécessaires ?

Savez-vous si tous les équipements actifs qui supportent le système de contrôle de process sont équipés d'un antivirus et s'il est tenu à jour quotidiennement ?

Le cycle de parution des virus n'est pas régulier, plusieurs mises à jour des signatures peuvent intervenir dans la même semaine.

Vos procédures de mise à jour et de configuration de votre système de contrôle de processus permettent-elles de retracer l'origine des éventuels incidents ultérieurs ?

Êtes-vous certains que seules des personnes autorisées se connectent aux systèmes industriels de votre entreprise ?

Savez-vous ce que deviennent les disques durs de vos systèmes lorsqu'ils sont mis au rebut ?

PENSEZ-VOUS QU'EN CAS DE DYSFONCTIONNEMENT DE VOTRE INFORMATIQUE INDUSTRIELLE, QU'IL SOIT ACCIDENTEL OU DÙ À UNE MALVEILLANCE, VOS ÉQUIPES SAURAIENT RÉAGIR PROMPTEMENT ET EFFICACEMENT POUR EN LIMITER LES CONSÉQUENCES NÉFASTES ?

AVEZ-VOUS RÉFLÉCHI AUX MENACES QUI PÈSENT SUR VOTRE INFORMATIQUE INDUSTRIELLE ?

MON SYSTÈME N'INTÉRESSE PAS LES PIRATES QUI PROLIFÈRENT SUR INTERNET. VRAI OU FAUX ?

Faux : ces pirates sont en permanence à l'affût des systèmes vulnérables et les détectent. Ils les attaquent dès qu'ils en ont la possibilité.

MES CONCURRENTS N'AURAIENT PAS LES COMPÉTENCES NÉCESSAIRES POUR ATTAQUER MON SYSTÈME, ET D'AILLEURS ILS N'OSERAIENT PAS RECOURIR À DE TELLES PRATIQUES. VRAI OU FAUX ?

Faux : car il serait imprudent de l'affirmer. D'une part, il est facile de louer les services de pirates compétents, notamment à l'étranger. D'autre part, comme les attaques informatiques restent souvent anonymes, ce n'est pas la crainte d'être découvert qui dissuade beaucoup les malveillances. Enfin, puisqu'on voit régulièrement, en informatique générale, des exemples d'attaques informatiques de la part de concurrents peu scrupuleux, il n'y a pas de raison qu'il ne s'en produise qui visent l'informatique industrielle. Cela est d'autant plus vrai si ces installations sont, pour l'attaquant, moins difficiles à pénétrer.

AUCUNE ATTAQUE INTERNE N'EST À CRAINDRE ? VRAI OU FAUX ?

Faux bien sûr. D'abord les employés peuvent parfois causer des dommages importants parce qu'ils sont mal formés, inconscients ou négligents : il faut donc prendre soin de leur formation comme de leur sensibilisation, promulguer une charte d'utilisation des moyens infor-

matiques et veiller à ce que les procédures appliquées minimisent les risques de négligence. Ensuite, il peut arriver que certains employés, mécontents ou soumis à des pressions externes, commettent des malveillances et la tentation est plus grande s'ils pensent qu'ils ne seront pas identifiés : une précaution indispensable est que les actions critiques ne puissent être effectuées que par certaines personnes et soient commodément imputées à leurs auteurs.

AVEZ-VOUS ÉVALUÉ LES CONSÉQUENCES D'ATTAQUES OU D'INCIDENTS SUR VOTRE INFORMATIQUE INDUSTRIELLE ?

AVEZ-VOUS RECENSÉ LES INFORMATIONS CONFIDENTIELLES QUE TRAITÉ VOTRE INFORMATIQUE INDUSTRIELLE (PAR EXEMPLE PROCÉDÉS ET SECRETS DE FABRICATION, TYPES DE FABRICATION EN COURS) ? AVEZ-VOUS ÉVALUÉ LES CONSÉQUENCES QUI RÉSULTERAIENT DE LEUR DIVULGATION ?

AVEZ-VOUS ESTIMÉ LE COÛT DES PERTURBATIONS ÉVENTUELLES DE VOS CHÂÎNES DE FABRICATION ?

AVEZ-VOUS ÉVALUÉ LES DOMMAGES QUE CAUSERAIENT, SUR VOS EMPLOYÉS VOIRE SUR LES VOISINS, DES DYSFONCTIONNEMENTS PLAUSIBLES DE VOTRE INFORMATIQUE INDUSTRIELLE, QU'ILS SOIENT ACCIDENTELS OU PROVOQUÉS PAR MALVEILLANCE ?

Bien que le sujet soit nouveau et orienté dans sa majeure partie pour la protection du patrimoine de l'entreprise et de son savoir-faire, des conséquences plus graves peuvent avoir lieu pour le salarié ou la sécurité du voisinage.

La technologie allant beaucoup plus vite que la conscience du risque lié aux cyber-attaques, un travail d'éducation et de sensibilisation à ce nouveau risque est nécessaire. Il faut dans un premier temps, sensibiliser la hiérarchie à ce type de risque pour ensuite effectuer une analyse des risques et un bilan au niveau de l'entreprise pour savoir où

elle se situe et quelles sont les solutions qu'il faudra mettre en œuvre. Le choix des solutions résultera d'un compromis entre le coût de développement et les contraintes d'utilisation, d'une part, et celui des conséquences des risques résiduels, d'autre part.

La deuxième intervention, réalisée par une personne de la Direction de la Surveillance du Territoire (DST), a montré quels étaient les principaux risques :

- atteinte à l'intégrité des systèmes, le plus connu étant de faire écrouler le système de messagerie, mais aussi des atteintes possibles au process de fabrication,

- atteinte aux données confidentielles de l'entreprise,

- atteinte à l'image de l'entreprise pour la déstabiliser,

- atteinte à des sites industriels sensibles dans l'industrie du process.

Les motivations pour les attaques ont évolué puisque l'on est passé d'attaques généralement motivées par la vantardise de leurs auteurs à des attaques à but lucratif (société de renseignement privé, service de renseignement d'autres états, concurrence, mafia) pour viser le cœur de l'entreprise.

Cette présentation a donc surtout été axée sur la perte des données stockées sur des supports informatiques et sur la réalité de la menace pour les entreprises. Des cas concrets d'extorsion d'informations ont été présentés, comme le piratage des informations stockées sur une clé USB à l'aide d'un scanner installé sur l'ordinateur sur lequel vous allez connecter votre clé, l'extorsion de données par le réseau Wi-Fi puisque le signal peut être capté à des distances allant jusqu'à 10 km de l'entreprise ou le risque de perte de données professionnelles confidentielles stockées sur un ordinateur portable lors de son utilisation à des fins personnelles lors de connexion Internet, notamment lors de connexions à des sites d'échange peer-to-peer.

Ainsi, il a été précisé que 30 % des connexions Internet sont utilisées pour réaliser des attaques à l'aide d'outils nomades pour se connecter au réseau de l'entreprise.

Pour solliciter ce service de la DST pour une présentation : groupe.conferences@interieur.gouv.fr

La troisième intervention de la journée par Colette Rodionoff (EDF) a fait un parallèle entre les systèmes d'information de gestion et les systèmes d'information industrielle, mettant en avant les risques de corruption des informations. Les équipements mobiles du type ordinateur portable, PDA, clé USB sont de plus en plus présents et peuvent maintenant venir corrompre des données, même dans la partie informatique industrielle de l'entreprise. De même, les opérations de télémaintenance ouvrent une brèche dans le système d'information industrielle et peuvent de ce fait introduire des codes malveillants (virus, etc.) qui viendront mettre en défaut l'installation. Les solutions recommandées sont de durcir les couches logicielles, de maintenir à jour les systèmes d'exploitation, d'assurer la protection des postes (anti-virus, pare-feu pour les PC industriels), de séparer les domaines réseau (entreprise et industriel) alors que la volonté est souvent d'avoir un réseau communiquant commun entre l'informatique de gestion et l'informatique industrielle, de limiter voire interdire la connexion au réseau industriel d'équipements nomades non sûrs pour l'entreprise comme ceux des sous-traitants.

La quatrième intervention, de J.P. Dalzon (ISA France), visait à présenter la norme ISA99 traitant de la cyber-sécurité des systèmes de contrôle-commande industriels. Ce document a été développé par un groupe de travail d'industriels et institutionnels issus essentiellement des domaines de l'industrie des procédés du type chimique, énergie, pharmacie et agroalimentaire.

Les travaux de normalisation du comité ISA SP99 visent à permettre la conception et l'implémentation d'une politique optimale de protection des systèmes de contrôle-commande contre les cyber-attaques, en bénéficiant de l'effort de recherche des Etats-Unis et des travaux de normalisation sectorielle (eau, énergie, chimie, ...). Le document ISA 99, publié fin 2007, est décliné en 2 parties. La première, à vocation informative, vise à définir les concepts, la terminologie et les modèles en vue de permettre la compréhension de la cyber-sécurité dans l'environnement des systèmes de contrôle-commande et d'automatisation industrielle. Cette partie propose une double modélisation (physique et fonctionnelle) des systèmes de contrôle-commande vis-à-vis de la sécurité

et introduit un concept de découpage des systèmes de contrôle-commande en zones de sécurité avec l'identification des conduits d'information à protéger entre ces différentes zones.

La partie 2 de ce document à caractère normatif constitue un guide pour le développement d'un programme de sécurité des systèmes de contrôle-commande et d'automatisation industrielle. Il fournit des procédures détaillées sur le processus à mettre en œuvre et les éléments clés pour l'établissement d'une organisation d'un système de gestion de la cyber-sécurité.

Ce standard est utilisé actuellement par les ingénieurs conseils aux États-Unis.

La cinquième intervention, de S. Lueders (CERN), a montré sous forme d'exemples quels étaient les problèmes de sécurité des systèmes de contrôle-commande (arrêt du système de surveillance de la centrale nucléaire de Davis Besse par le virus Slammer, inondation du sous-sol de l'Hôtel Hyatt Regency par un piratage sans fil (46 fois de suite) de la station d'épuration, arrêt d'un pipeline suite à un test de pénétration ayant pour cible le système de contrôle-commande. Le cas particulier de l'analyse par le banc de test des vulnérabilités Ethernet des 125 systèmes automatisés utilisés pour le système de contrôle-commande de l'anneau d'accélération de particules du CERN a été présenté. En effet, aujourd'hui, de plus en plus de systèmes de contrôles sont interconnectés par le réseau Ethernet en utilisant la couche TCP/IP. Ces systèmes ont hérité des avantages de l'Internet standard, par exemple des automates sont équipés de serveurs Web et permettent d'envoyer des e-mails. Malheureusement, la cybersécurité a souvent été complètement ignorée. Les systèmes industriels, du fait de leur durée de vie plus importante, sont en retard sur l'équipement grand public alors qu'ils utilisent des équipements standards (ordinateurs portables, automates standards), des systèmes d'exploitation (par exemple Windows), des protocoles de communication standards voire sans fil.

Le test de pénétration par l'intermédiaire des connexions Ethernet sur les différents systèmes automatisés du CERN a montré qu'il y avait encore, au début de 2007, 15 % de leurs systèmes

qui ne passaient pas le test et qui ont autorisé l'accès ou ont eu l'une de leurs fonctions désactivées, ainsi que 17 % des systèmes qui se retrouvaient isolés de l'installation, sans communication possible du fait que le protocole de communication était rompu. Un travail en profondeur est à faire sur les automates industriels afin de les rendre plus robustes face à des attaques par le réseau de communication. Ce travail nécessite une coopération entre tous les interlocuteurs : gérants, utilisateurs, experts et fournisseurs.

La dernière présentation de B. Minvielle, expert technique chez Hirschmann, société spécialisée en transmission de données dans le monde industriel, pionnier et leader des équipements de réseaux Ethernet Industriel, a été aussi l'occasion de mettre en évidence que la sécurité d'accès aux contrôleurs et automates industriels est une réalité du monde de l'automation. Les systèmes étant de plus en plus critiques, il convient d'étendre la sécurité à d'autres approches comme la disponibilité du système, la sécurité des flux applicatifs et industriels, la sécurité liée à l'interconnexion entre réseaux de différentes natures.

Par exemple, pour la sécurisation des flux, il ne faut pas que les données critiques soient perturbées par les informations fonctionnelles. On peut aussi mettre en place des administrations sécurisées pour les réseaux sensibles afin de dissocier les flux d'information, mais aussi utiliser des protocoles sécurisés comme https. Pour les interconnexions réseau du type réseau bureau-tique et usine, il faut assurer le contrôle des flux, la provenance et la destination, contrôler les applications et le trafic et pour les utilisateurs distants, contrôler les accès, identifier et authentifier les utilisateurs comme dans le cas de la télémaintenance.

Au travers de cette journée d'échanges et de débats, on constate que le cyber-risque des installations automatisées ou des systèmes de contrôle-commande est un risque émergent qui peut avoir des conséquences pour l'opérateur intervenant sur cette installation. À l'heure actuelle, les industriels essaient de garder la séparation physique entre le réseau industriel et le réseau de l'entreprise, mais il devient de plus en plus difficile de préserver cette séparation puisque le système de gestion de l'entreprise a tendance à descendre de plus

en plus bas et à se rapprocher du niveau capteur/actionneur des installations automatisées.

Cette évolution nécessite d'être vigilant et de préparer un travail de sensibilisation à ce risque d'un nouveau type pour les installations automatisées, à plus forte raison si le lien entre les installations automatisées et le réseau public tel qu'Internet devenait une réalité mise en œuvre par les industriels.

La démarche de sécurisation comprend les étapes suivantes :

- analyser les enjeux, notamment prise de conscience de tous les responsables de l'entreprise et sensibilisation à tous les niveaux,

- identifier les points sensibles et les systèmes qui doivent être protégés (confidentialité de données, disponibilité de processus, intégrité de paramètres techniques,...),

- analyser les risques (identifier les menaces et évaluer les vulnérabilités),

- déterminer une architecture adaptée aux risques,

- prévoir les mesures d'accompagnement de sécurité physique des locaux, du personnel, des procédures,

- faire le bilan des risques résiduels.

Le choix des solutions relève de chaque entreprise et nécessite de convaincre plus spécifiquement les hommes et plus particulièrement l'encadrement. Les solutions seront un compromis entre leurs coûts et le coût des conséquences des risques résiduels.

Pour plus d'informations, l'ensemble des actes de cette journée est disponible auprès du Club Automation : www.clubautomation.org

BIBLIOGRAPHIE

- Protégez votre informatique industrielle, document édité par la Direction Générale des Entreprises, ministère de l'Industrie.

- ANSI/ISA - TR 99.00.01 - Security Technologies for Manufacturing and Control Systems.

- ISA - 99.00.01 - 2007 - Security for Industrial Automation and Control Systems Part1: Concepts, Terminology and Models.

- ISA - 99.00.02 - Part 2: Establishing an Industrial Automation and Control System Security Program.

- Vos réseaux sont-ils en cybersécurité ? Revue Mesures n° 805, mai 2008.

- www.securite-informatique.gouv.fr