

10.5. Sécurité informatique contre sécurité de l'automatisation: Les installations industrielles visées par des cyber-attaques ?

Le temps où l'automatisation était déconnectée du reste du monde est révolu depuis longtemps. En raison de la demande de standardisation, le nombre d'équipements et de logiciels - comme Windows ou Ethernet - pour PC ne cesse d'augmenter. L'ouverture en communication est le mot d'ordre, tant entre les modules d'automatisation de diverses marques, que pour les logiciels de gestion. Il faut extraire les données de la production pour la traçabilité et la communication HMI-MES-ERP.

Mais quand on parle de communication entre les systèmes, les départements et les entreprises, on s'approche des eaux dangereuses d'Internet, du cyper-espace et de l'insécurité de l'information. Et donc du risque d'arrêts de production provoqués par des virus malveillants. Un problème sousestimé ou exagéré? Industrie Technique & Management a posé cette question à plusieurs acteurs du marché.

DÉFINITION

Nous parlons ici de risques informatiques contre lesquels nous devons nous protéger, donc de sécurité informatique. Ce thème ne doit pas être confondu avec un autre, plus pointu: la sécurité machines, connue sous le mot de safety. Ce terme touche à la sécurité des machines: des dispositifs physiques sont déployés pour éviter que les opérateurs ne se blessent. La sécurité, que nous abordons dans cet article, concerne la protection du logiciel de l'outil de production et du système d'automatisation de la machine contre des intrusions [malware). Nous parlons donc d'accès informatique jusqu'aux systèmes de contrôle industriel, et des risques apparentés.

LA CHANCE EXISTE

La plupart des responsables d'entreprises considèrent que leur production est déconnectée d'Internet. Il en était probablement ainsi il y a cinq ans de cela. Aujourd'hui, avec l'utilisation des COTS [commercial off-the-shelf technologies], il y a une grande chance qu'un lien informatique relie votre production avec le monde extérieur. Il y a certainement un câble Ethernet entre un PLC et un système de contrôle de processus, celui-ci étant connecté au réseau informatique de l'entreprise. Même si le lien n'est pas direct, n'y a-t-il pas quelque part dans votre système d'automatisation, un routeur qui est connecté, via Ethernet, au département informatique? L'installation ne dispose-t-elle pas d'une imprimante ou d'un scanner intelligent qui sont connectés à un serveur, celui-ci étant connecté au réseau TIC qui communique avec la HMI? Le marché demande actuellement une connectivité déportée pour l'environnement industriel.

Le responsable de la maintenance veut que les fournisseurs de l'installation puissent se connecter au système d'automatisation de production, jusqu'au niveau E/S pour poser un diagnostic, voire effectuer des mises à jour. Ceci afin d'être plus rapidement opérationnel et de réaliser des économies sur les coûts de transport et surtout la durée des voyages des spécialistes et des ingénieurs externes appelés en cas de pannes inopinées. Généralement, ce lien et l'autorisation d'utilisation sont donnés sans que la direction ou le département informatique ne soit mis au courant. Il s'agit là d'une communication privée qui ne se déroule pas [habituellement] via un open internet mais en utilisant des techniques de réseau sécurisées. Aujourd'hui, cela concerne spécifiquement les systèmes basés sur le web, mais les connexions dédiées subissent aussi les assauts de crackers.

On parle même d'une tendance visant à réaliser une sorte de tamis informatique, une informatisation. indirectement insécurisée, pour pouvoir par exemple placer de l'instrumentation supplémentaire dans le cadre d'un problème (dans un process). Si l'on n'y prend pas garde, cette porte ouverte permettra aux pirates d'accéder à l'automatisation de l'entreprise.

PAS CHEZ MOI?

Il faut bien se rendre compte qu'à partir du moment où un lien, quelque part, connecte le système d'automatisation avec l'extérieur, il est théoriquement possible d'être victime d'actes de malveillance qui peuvent neutraliser certaines fonctions du système. En Colombie britannique, des bassins remplis de plantes aquatiques ont ainsi été vidés à la suite d'une opération malintentionnée. Les dégâts étaient importants.

Il convient aussi de faire attention aux attaques de virus. Elles peuvent en effet alourdir et ralentir le trafic du réseau, certains délais de cycles n'étant alors plus activés que sporadiquement (les DoS-attacks, Denial-of-Service, par exemple). Ceci peut générer une déconnexion de l'installation voire des erreurs à des moments inattendus. De nombreux arrêts ont parfois lieu avant que l'on ne se rende compte qu'il s'agit d'un virus et non d'une erreur électronique intermittente. D'après les statistiques, une à deux journées de production sont perdues chaque année à cause de ce type d'attaques.

D'une manière générale, on s'attend à voir les virus provenir du réseau Ethernet. Mais les risques existent aussi lors d'interventions locales. Un technicien de maintenance (externe) qui insère une clé USB porteuse d'un virus dans un PC réservé à l'automatisation peut provoquer des dégâts. À côté des pare-feu, il faut donc aussi prévoir des scanners antivirus sur les installations industrielles. Il faut néanmoins ne pas suivre aveuglément les règles de précaution, car un programme antivirus peut aussi être une source de difficultés et de ralentissements. La mise à jour, quotidienne et inattendue, du programme antivirus n'est pas une bonne chose. Il faut étudier la fréquence et la période pendant laquelle le scannage pourra avoir lieu. En automatisation, une fréquence mensuelle ou trimestrielle est un délai acceptable si cela peut avoir lieu selon une méthode contrôlée. Et après chaque mise à jour, il est bon de faire un test des principales fonctionnalités. Car à l'inverse du secteur informatique où l'intégrité des données est importante, la disponibilité de la production est la base de tout en automatisation.

UNE APPROCHE ET UNE ÉQUIPE PARTICULIÈRES

En fait, la sécurité dans l'industrie ne peut [généralement] pas être un «copier-coller» de ce que le département TIC met en place pour l'environnement de bureau. Même si la sécurité de processus est indubitablement liée à la sécurité informatique de l'entreprise. La sécurité de process est aussi liée à la process-safety dans le cadre d'un contexte de production.

Nous ne disons donc pas que la sécurisation TIC ne serait pas construite de manière assez complexe et ne pourrait être implantée. L'implémentation au sein d'une automatisation doit satisfaire à d'autres règles que celles qui sont d'application dans l'environnement de bureau. Cela commence avec une différence dans l'ordre des priorités. Dans les systèmes pour bureaux, les priorités sont: la confidentialité, l'intégrité des données et seulement la disponibilité. Dans un environnement industriel, on retrouve d'abord la disponibilité, puis l'intégrité des données et enfin la confidentialité.

Prenez la disponibilité de l'installation: personne, dans un environnement de process de production, ne pense un instant à interrompre un programme en plein milieu d'un process. Du style: « votre scanner de virus/système opératoire est mis à jour, dans une minute, votre PC sera initialisé et redémarré ». Dans l'environnement de bureau, il s'agit là, par contre, d'une pratique courante.

La sécurisation informatique dans un environnement industriel doit donc être assurée par la production selon une étape logique, et en concertation avec le département TIC de l'entreprise. Ceci englobe des méthodiques sur les scanners de virus, le patch management, le rôle based access control, l'account management, les secure architectures, les demilitarized zones, l'IP hardening, les firewalls, les virtual private networks, les policies and procedures, etc.

Ces éléments sont désignés sous l'appellation Defense in depth dans ISA99. Et pour les liens entre deux réseaux, il faudra prévoir des accords entre les services de maintenance classiques de la production et le département TIC classique.

Il est important d'établir une méthodique pour les zones grises. Pensez aux systèmes de suivi de production et aux systèmes de planning de production, au suivi des stocks couplé à un usage en production. Ces systèmes sont de plus en plus alimentés en ligne depuis l'ERP et sa base de données de bons de commande qui imposent les quantités, les types, les délais et les priorités, alors que la base de données de production mentionne ce qui est finalisé, les machines qui sont disponibles, ce qui est en rework".

UN MODELE REUSSI

Bien que l'implémentation diffère fortement, il y a des règles de base comme dans tout système de sécurisation TIC. Dans les deux cas, il s'agit de contrer la pénétration de virus malveillants et d'éléments non autorisés en plaçant des barrières. En seconde instance, lors d'une intrusion, il faut s'assurer que les dégâts seront ramenés à un minimum. La règle de base de chaque concept de sécurité est de répartir l'environnement de production en security cells. Cette répartition se fait sur la base de protections physiques (des barrières via des routeurs intelligents, des réseaux distincts qui peuvent uniquement communiquer via un mur pare-feu ou qui peuvent délivrer des données et non en recevoir) et fonctionnelles. Par ailleurs, à cause de l'importance de la continuité dans l'environnement de production, il faut s'assurer que la production puisse tourner même sans liens informatiques comme l'ERP.

Si vous souhaitez en savoir plus sur ce sujet, nous vous conseillons le site ISA-99.com ou la documentation se rapportant à IEC 62443. Ces sources décrivent les catégories de sécurité pour les manufacturing and control systems et les outils disponibles et méthodes appropriées. Pour l'industrie de process, il existe un groupe de travail issu de NAMUR qui se penche sur l'intégration d'ISA 99 dans l'industrie de process. Ceci démontre bien l'actualité du sujet. Néanmoins, il faut réaliser qu'on n'arrivera jamais à créer un environnement sûr à 100%. Il subsistera toujours un écart entre les objectifs de sécurité, l'impact des mesures de sécurité sur l'environnement de travail et le prix de revient pour atteindre les objectifs.

L'ANALYSE DE RISQUES

Pour trouver un bon équilibre entre les mesures nécessaires pour se protéger d'attaques malveillantes et l'investissement paranoïaque basé sur le pire des cas, une analyse de risque s'avère être la seule base saine. Ce qui est aussi très important, c'est qu'il faut bien réaliser que chaque implémentation de sécurité, incluant les matériels et les logiciels, doit pouvoir être entretenue par la production, donc par l'ingénierie et la maintenance! D'après les réactions que j'ai reçues des fournisseurs et des intégrateurs, il est clair que chacun vend son approche idéale et sa consultance. Et pour eux, [l'avenir est prometteur.

www.industrie.be

INDUSTRIE TECHNIQUE & MANAGEMENT SEPTEMBRE 2011