Repenser la cyber-sécurité

par ***Robert Mick***

En dépit de la sophistication galopante des menaces face à la cyber sécurité, industriels et activités mettant en œuvre des systèmes de contrôle semblent garder la maîtrise de leur process. Cependant, un manque de visibilité, des questionnements récurrents et de nouvelles exigences, sont autant de raisons qui poussent à remettre à plat certaines problématiques de sécurité.

Les cyber attaques et les parades de la cyber sécurité continuent leur escalade sous couvert d'une incroyable inflation de technologies sophistiquées des deux cotés du pare-feu. Fort heureusement (pour l'industrie !), la plupart des attaques se concentrent sur des cibles commerciales telles que les banques, et individuelles par exemple via un vol d'identité. Quoi qu'il en soit, la plupart de ces attaques et outils de protection peuvent concerner le monde de la production, mais la situation est cependant différente.

Les différents types d'exploitation industrielle se basent sur des systèmes variés (par exemple des systèmes de contrôle) avec des niveaux de risque différents (par exemple sécurité des personnes, risque de pollution…). Cela nécessite la mise en place de groupes de réflexion dédiés à ces questions. Ces groupes existent certes depuis de nombreuses années, mais certains problèmes persistent. En outre, émergent de nouvelles exigences pour lesquelles les pratiques aujourd'hui en place ne devraient plus être appliquées. Il est pourtant certain que nous devons continuer à investir les programmes et initiatives en cours, mais nous avons aussi besoin d'identifier les problématiques non résolues et persistantes, examiner les nouveaux besoins, pour finalement trouver de nouvelles issues.

Pourquoi une remise à plat aujourd'hui ?

Il existe de nombreuses raisons qui poussent à aborder la cyber sécurité selon différentes perspectives. La plupart d'entre elles sont listées dans le tableau ci-contre. Cependant, la plus percutante est relative au fait que l'activité de la cyber sécurité soit relativement mature. Et pourtant, les activités professionnelles continuent à se développer dans un contexte de risque élevé. Il est temps de repenser certaines problématiques. Que proposons-nous pour remettre à plat la cyber sécurité dans un contexte d'exploitation industrielle ? Tout d'abord, il convient de concentrer les travaux sur des pistes plus efficaces. Il s'agit de trouver les voies dans la lignée des tendances actuelles.

Stratégies de remise à plat

En 2009, ARC Advisory Group a démarré une étude de marché sur la cyber sécurité dans l'industrie. Cette étude a permis d'identifier, investiguer et analyser les nouveaux concepts de sécurité dont certains sont évoqués ci-après. Il est important de rappeler que cette étude est réalisée dans une perspective d'exploitation industrielle. Il est certain que les systèmes sur sites ont chacun leurs besoins propres, et il existe d'autres sujets différent de leur problématique tels que les spam de messagerie ou les hameçonnages (pishing scams).

Systèmes de contrôle « résistant »

La plupart des systèmes de contrôle installés ne sont pas conçus de façon native pour aborder les problématiques de cyber sécurité. La majorité des protocoles traditionnels n'ont pas anticipé les aspects de sécurité.

Les composants ont été conçus pour admettre soit un environnement éprouvé, soit un environnement ou d'autres composants assurent des protections variables. La complexité galopante des menaces, voire des menaces internes, remet en cause perpétuellement ce contexte.

Un concept intéressant de Resilient Control System (RCS) a été proposé dans un article de l'IEEE (Craig Rieger, David Gertman et Miles McQueen de l'Idaho National Laboratory) lors de la 2e conférence internationale « *Human Systems Interaction* » (mai 2009).

Le concept RCS prend l'hypothèse d'attaquants malveillants, entre autres, non initialement considérée lors de la conception des systèmes de contrôle. Il propose un cadre pour étendre et appliquer différemment notre mode de pensée traditionnel sur les systèmes de contrôle.

Un process véritablement transversal

Les tâches liées à la cyber sécurité implémentent habituellement les aspects de conception et de protection, avec la formation des personnes. De quoi résoudre les problèmes au fur et à mesure qu'ils surviennent. Cependant, la cyber sécurité est une activité véritablement dynamique où le succès est directement lié à la vitesse de réaction et d'exécution. Nombre de ces activités dépasse les limites organisationnelles et du système. Tout cela montre bien que la cyber sécurité est une problématique similaire à d'autres thèmes transversaux, tel que le process de fabrication et de suivi de l'ordre de fabrication à la vente. La cyber sécurité peut donc bénéficier des mêmes analyses et méthodes de suivi automatisées.

Plusieurs bénéfices découlent d'une stratégie « sécurité » en perspective. Certains process de sécurité tels que la gestion de patch et d'identité nécessitent plus d'intégration et d'automatisation pour réduire les coûts et les risques. Une analyse du process facilite aussi le développement des bonnes pratiques et fige un cadre pour la standardisation des informations de sécurité et de la communication. Finalement, une meilleure structuration et l'automatisation des process de sécurité générera des mesures de sécurité et de visibilité bénéfiques pour la maîtrise des coûts.

Partenariat Etat/entreprises

En termes simples, les gouvernements ont sous leur responsabilité la protection des nations (et des citoyens), mais le monde professionnel aussi bénéficie de cette protection en matière de cyber sécurité. Par conséquent, des perspectives de partenariat doivent naître de la relation Etat-Entreprises dans le domaine de la cyber sécurité.

ARC Advisory Group pour Jautomatise

Peu de visibilité dans l'industrie

L'activité en matière de sécurité perdure, en général, par de mauvaises expériences associées à des exploits ahurissants de hackeurs… mais cela ne suffit pas induire une attention pérenne sur ce thème. Personne ne devrait être surpris par le fait que des intrusions puissent se produire maintenant et que des outils d'attaque en pleine évolution pourront le faire encore plus facilement demain. La sécurité se joue dans les détails et il importe de se baser sur des situations et des incidents réels afin de donner la priorité à certaines actions de sécurité, tout autant que d'apprendre des différentes expériences.

Certes, un reporting des incidents a jusque là été réalisé, mais il importe de gagner en visibilité et nous avons besoin de remettre à plat précisément les besoins et comment y satisfaire.

Tandis que de nombreux industriels continuent à contribuer aux progrès de la cyber sécurité, certains problèmes persistent… Cet état de fait suggère combien il importe de repenser l'approche jusqu'alors menée. Cela peut être accompli selon plusieurs voies, simplement examiner les problèmes dans le contexte actuel, en essayant d'appliquer des techniques issues d'autres disciplines. Tout d'abord, nous avons besoin d'identifier une brève liste de problèmes récurrents à résoudre. Qu'en est-il de votre liste ?

Problématique de sécurité	Explication
Coûts élevés	Le coût d'implémentation et de maintenance de la sécurité est élevé. Il n'ajoute rien à la valeur de la plupart des produits manufacturés et les objectifs de sécurité ne sont pourtant jamais atteints à 100 %… Quel que soit le montant d'investissement dans la lutte contre les cyber attaques.
La motivation qui pousse à investir dans la sécurité évolue	La motivation qui pousse traditionnellement à investir dans la cyber sécurité a été associée à la notion de risque perçu, qui varie bien évidemment d'une activité à une autre. Ces dernières années, l'implication des Etats et les phénomènes de réglementation ont conduit à réaliser des investissements en matière de sécurité, notamment pour les infrastructures industrielles critiques. La réglementation tend à élargir et à propager ce mouvement aux autres industries. Cela fera évoluer significativement les stratégies de sécurité.
Résoudre des problèmes de sécurité persistants	Il existe plusieurs problèmes de cyber sécurité apparemment non-résolvables. Par exemple, les patches ne peuvent être testés et installés assez vite pour les systèmes en exploitation, du fait de la trop large variété d'applications et de configuration de systèmes. Conséquemment, la période de forte exposition à des attaques réussies est beaucoup trop longue. Ce phénomène montre combien les différentes activités industrielles évoluent dans un contexte à haut risque.
Sécurisation des accès distants	La maintenance effective des actifs (machines, systèmes...) nécessite de plus en plus souvent un lien distant afin que le prestataire de services puisse contrôler et agir. Actuellement, le risque résultant de la connexion à ces actifs est élevé. Une large variété d'approches est exploitée, mais les industriels et prestataires de services ont besoin d'une solution peu coûteuse et hautement sécurisée.
Accélération des standards de développement	Les standards sont critiques pour améliorer la sécurité, mais les processus de rédaction sont beaucoup trop lents et dans la plupart des cas les résultats sont à peine adaptés aux besoins. La majorité des standards doivent être adaptés et étendus aux applications en exploitation.
Etre certain de se trouver sur la bonne piste	En général, les industriels adoptent une approche de la sécurité partant du bas vers le haut, résolvant un problème à la fois et répondant de façon incrémentale aux nouvelles menaces. L'activité de la cyber sécurité est intense et c'est justement le bon moment de prendre du recul pour être certain de travailler sur les bons problèmes et les bonnes solutions.

Les multiples raisons de repenser les problèmes de sécurité persistants.