Les systèmes de contrôle face à la cybercriminalité

L'ISA-France organisait à Nice, les 10 et 11 mai dernier, un séminaire international sur le thème de la cybersécurité dans le domaine du contrôle des procédés industriels. Placées sous le haut patronage du ministre délégué à l'industrie François Loos, ces deux journées de conférences avaient pour objectifs de sensibiliser aux risques encourus, ainsi qu'aux moyens de s'en prémunir.

En Europe, force est de constater qu'aujourd'hui les risques qui résultent de l'ouverture des systèmes de contrôle-commande, pour la production, pour la sécurité des biens mais également pour la sécurité des personnes, restent largement peu pris en compte. Les responsables des systèmes de contrôle-commande, habitués à avoir affaire à des technologies propriétaires et par conséquent sûres, restent en effet peu familiarisés avec les problèmes de cybercriminalité. De leur côté, les responsables des systèmes d'information ne sont pas toujours à l'aise avec les problématiques des réseaux de contrôle. Ils ne sont pas habitués à répondre à des besoins de disponibilité 24h/24, et peuvent ne pas comprendre les bénéfices de l'application des technologies de l'information au niveau du contrôle-commande. Au-delà de cela, de nombreuses questions se posent : celle, tout d'abord, de savoir si l'on n'est pas en train de crier au loup ; puis celle, inévitable, une fois que les risques encourus ont été admis, du retour sur investissement. Questions ô combien difficiles… d'autant plus qu'on le sait, en matière de sécurité : plus les investissements portent leurs fruits, moins les résultats sont mesurables…

L'ISA-France organisait, les 10 et 11 mai dernier, un séminaire international sur le thème de la cybercriminalité.

Un sujet d'actualité

Cette journée de conférences organisée par l'ISA démarrait par l'intervention d'un représentant du ministre de l'économie, des finances et de l'industrie, revenant sur les enjeux de la cybersécurité : *« Il s'agit d'un sujet majeur et d'actualité, qui ne doit pas être négligé. On sait maintenant que de nombreux produits informatiques comportent des failles et que l'architecture des systèmes n'est pas toujours conçue dans un souci de sécurité. Les systèmes de contrôle, qui maintenant incorporent des produits d'usage général comme des systèmes d'exploitation et sont raccordés aux réseaux généraux des entreprises, sont dorénavant exposés au même genre d'attaques que celles que subissent en permanence les systèmes d'informatique générale. Afin de protéger nos usines d'attaques dévastatrices qui pourraient avoir des conséquences bien plus graves encore qu'en informatique générale, il est urgent de faire évoluer la culture des entreprises industrielles, afin que celles-ci prennent le problème de la cybercriminalité à bras le corps, au travers d'une démarche structurée : analyse de risques méthodique, certains risques étant bien spécifiques aux systèmes de contrôle, mise en place de procédures convenables, sensibilisation du personnel, prise en compte de la sécurité dans la réalisation des systèmes et le choix des produits, surveillance de l'évolution du niveau de sécurité au cours du temps…»*.

Des besoins spécifiques

Les mesures de sécurité traditionnelles, bien connus des responsables des systèmes d'information, consistent à introduire au sein du système de communication des barrières et restrictions permettant d'assurer la confidentialité des informations, l'intégrité des données échangées, l'authentification des utilisateurs et la disponibilité du réseau. Typiquement, les mécanismes de protection usuels reposent sur : la mise en place d'un Firewall, chargé de filtrer les échanges entre un réseau non sécurisé (Internet) et un ré-

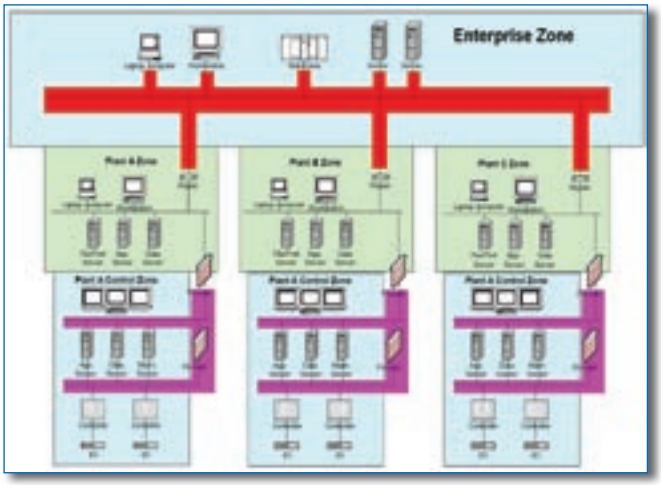
seau sécurisé (intranet) ; l'utilisation de scanners de sécurité, qui pistent les failles liées à des logiciels sensibles, l'administration et les activités des utilisateurs ; l'implémentation de systèmes de détection d'intrusion, dont le rôle est d'examiner le trafic en amont ou en aval des pare-feux et de contrôler l'authenticité des utilisateurs ; le recours au cryptage des données, de telle sorte que celles-ci ne soient exploitables que par les détenteurs de la clé de décryptage ; la mise en œuvre d'un tunnel VPN (Virtual Private Network), qui permet le transfert sécurisé de données sur un réseau IP public.

Toutefois, comme le soulignait Patrick Brassier, Chef de Produits chez Siemens A&D, venu présenter les réponses apportées par le fournisseur allemand d'automatismes aux problèmes de la cybercriminalité : *« Les solutions de sécurité existantes sont souvent inadaptées aux besoins propres à l'automatisation industrielle. En plus des besoins standard, il existe des besoins spécifiques, tels que la protection contre les interférences entre cellules de production, ou encore celle de segments de réseau composés de robots, automates programmables ou autres équipements, non compatibles avec les techniques de cryptage, VPN et autre mécanismes existants. Par ailleurs, les utilisateurs ne sont pas forcément des spécialistes réseaux, c'est pourquoi pour des installations de petites et moyennes tailles, les solutions doivent être faciles à mettre en œuvre et à maintenir, afin de pouvoir être prises en charge par des automaticiens/électrotechniciens responsables des installations. Enfin, l'introduction des solutions de sécurité doit pouvoir être réalisée au sein des infrastructures existantes, sans en entraîner la modification ».*

Par ailleurs, si face aux menaces modérées (virus ou vers habituels, script kiddies,…), les parades classiques (pare-feux, authentification forte, détection d'intrusions) peuvent s'avérer efficaces, elles deviennent insuffisantes pour contrer des attaquants puissants et déterminés. Comme le remarquait Tom Phinney, coordinateur technique du comité IEC 65, venu présenter les travaux de normalisation menés par le comité ISA-SP99 : *« La protection contre des attaques malveillantes diffère fondamentalement de celle visant à se prémunir des risques liés à des évènements naturels, tels que les pannes d'équipements ou les dommages causés par des intempéries. De nouvelles vulnérabilités sont découvertes tous les jours, les menaces évoluent de manière continue, le personnel ne se plie pas toujours aux mesures de protection mises en place, ou trouve des moyens de les contourner… Mettre en œuvre une politique de protection efficace contre les conséquences de telles actions ne peut être le fruit que d'une analyse minutieuse et d'une collaboration permanente entre les opérateurs, les ingénieurs, les responsables de la sécurité des systèmes d'information, et occasionnellement les autorités locales et nationale. A ce titre, la sécurité de ne doit pas être considéré comme un but à atteindre mais comme un processus continu ».*

Une normalisation en cours

Entamés depuis la fin de l'année 2002, les travaux de l'ISA-SP99 dans le domaine de la cybercriminalité visent à établir un guide industriel pour la conception et l'implémentation d'une politique optimale de protection des systèmes de contrôle contre les intrusions et les cyber-attaques. Deux rapports techniques ont déjà été publiés en 2004, discutant des différentes technologies de protection existantes, de leur l'applicabilité et de leur implémentation effective au sein des systèmes d'automatisation et de contrôle industriels. Ces deux rapports constituent le point de départ la norme ISA-SP99, constituée d'une série de quatre volumes, dont les deux premiers devraient être publiés dans un avenir très proche. *« Les normalisations internationales et/ou sectorielles vont se renforcer, le standard ISA SP99 apporte la possibilité de se situer par rapport à la meilleure pratique. Un approche pragmatique et proactive est préconisée, en intégrant le cycle de vie de la sécurité à l'intérieur du cycle de vie global du système, en adaptant le niveau de protection au risque associé à chaque fonction du système, en utilisant des produits aptes à être situés face aux standards SP99 et en développant une stratégie de défense en profondeur pour les applications les plus critiques »*, soulignait Jean-Pierre Dalzon, Responsable technique ISA-France.



Exemple de modélisation des zones suivant la norme ISA-SP99.

Le premier volume de la norme ISA-SP99 tient lieu d'introduction indispensable à la compréhension des concepts développés dans les volumes suivants. Y sont explicités : la portée du standard, les concepts de base, les modèles ainsi que la terminologie. Le second volume, dont la phase de révision s'est achevée à la fin du mois de mai dernier, fournit quant à lui des recommandations pour le développement d'un programme de protection des systèmes d'automatisation et de contrôle industriels. Il fournit un éclairage détaillé sur les activités process, et livre les éléments clés permettant de mettre en oeuvre un système de protection contre la cybercriminalité. Les travaux autour des deux derniers volumes du standard n'ont pour l'heure pas encore débuté. Le troisième volume devrait aborder la question de la conduite d'un programme de sécurité, une fois les étapes de conception et d'implémentation achevées. Il définira notamment un certain nombre de méthodes permettant d'en mesurer l'efficacité. Le quatrième et dernier volume définira quant à lui les caractéristiques différenciatrices des systèmes d'automatisation et de contrôle industriels, par rapport à d'autres systèmes basés sur les technologies de l'information. Puis il établira les pré-requis spécifiques qui en découlent en matière de sécurité.