Industriels en guerre contre le Cyber-Terrorisme

L'ouverture des réseaux d'entreprise sur Internet et l'introduction de standards de la communication bureautique jusqu'aux plus bas niveaux des architectures d'automatismes ne manque pas de réveiller chez certains la crainte de nouvelles menaces pour la sécurité des systèmes de contrôle distribués, SCADA, API et autres réseaux de contrôle industriels.

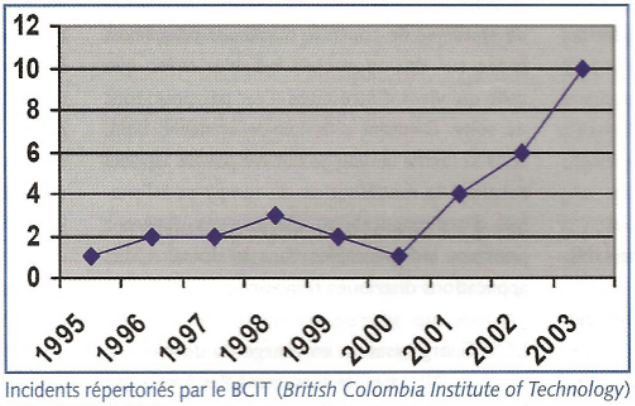
Aux premiers rangs de ces menaces, les possibilités d'infections par des virus informatiques ou encore les conséquences de mauvaises procédures de tests et d'architectures mal conçues sont de loin celles qui sont prises le plus au sérieux. Mais d'autres menaces, liées notamment aux intrusions volontaires et violations des systèmes par des personnes mal intentionnées, deviennent des sources d'inquiétudes. Outre Atlantique, on n'hésite pas à parler de guerre industrielle contre le cyber-terrorisme. Les risques sont-ils réels ?

Depuis une dizaine d'années, les systèmes de contrôle industriels ont vu une augmentation significative de la part des technologies issues de la bureautique (Ethernet, TCP/IP, HTTP, etc.) employées pour les communications de terrain et pour les échanges d'informations entre les équipements de contrôle distribués (PCI, API, etc.) et les systèmes de supervision. Beaucoup d'usines sont équipées de serveurs fournissant aux utilisateurs des couches hautes (bureaux, business) la possibilité d'accéder en temps réel aux données issues des équipements de terrain, voire la possibilité de se connecter à distance à des sessions Windows embarquées.

Néanmoins, si l'utilisation de ces technologies a permis de réduire les coûts de la communication industrielle tout en améliorant les échanges entre les couches hautes et basses des architectures, celle-ci a également rendu les systèmes plus vulnérables qu'ils ne l'étaient auparavant.

Des raisons culturelles

Pour mesurer l'importance du problème, il est essentiel de garder présent à l'esprit que les technologies de la communication bureautique et d'Internet sont enracinées dans une culture totalement étrangère aux problématiques des réseaux de contrôle. Celles-ci sont même, d'un certain point de vue, en parfaite opposition.



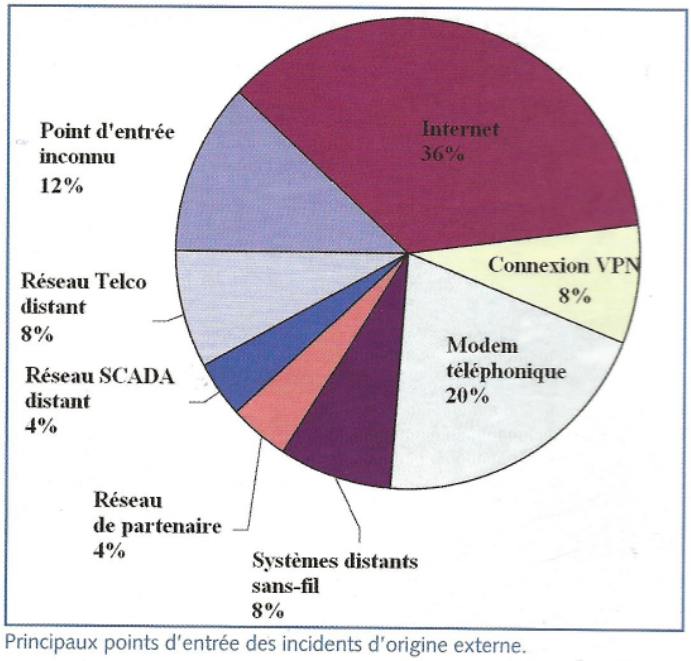
Incidents répertoriés par le BCIT (*British Colombia Institute of Technology*) entre 1995 et 2003

Dans un bureau, si les pannes sont indésirables, elles sont néanmoins tolérées. Comme chacun le sait, les « plantages » des outils bureautiques sont fréquents. Toutefois, il suffit bien souvent de « rebooter le système » pour que tout rentre dans l'ordre sans perte ni fracas. Le but essentiel de la sécurité n'étant pas là de protéger l'utilisateur final ou son PC, mais les données de l'entreprise, en plaçant au centre des dispositifs de sécurité les principaux serveurs.

Dans le cas d'un système de contrôle-commande industriel, au contraire, l'objectif principal est d'assurer la protection des personnes ainsi que la continuité de fonctionnement de l'installation, et ce durant des mois, voire des années. Toute défaillance est par conséquent inacceptable. Contrairement aux réseaux bureautiques, les éléments les plus importants aux yeux de la sécurité seront les équipements terminaux (API, drives, etc.) responsables du bon fonctionnement du système, bien plus que les serveurs d'informations, qui, dans de nombreux cas, ne servent qu'à stocker des données, certes importantes, mais néanmoins non-vitales.

Etant donné ces différences de besoins et de culture, l'intégration des nouvelles technologies de l'information ne doit pas être réalisée de façon aveugle sur le terrain. Or les responsables de réseaux de contrôle commande, habitués à avoir affaire à des technologies propriétaires et

par conséquent sûres, sont peu familiers des problèmes de cyber-sécurité. Souvent, ils ne disposent pas des budgets nécessaires, et considèrent même que la sécurité constitue un frein à la disponibilité. De leur côté, les responsables des IT ne sont pas familiers 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 nécessairement comprendre les bénéfices de l'application des technologies de l'information au niveau contrôle.



Principaux points d'entrée des incidents d'origine externe.

Pas de garanties

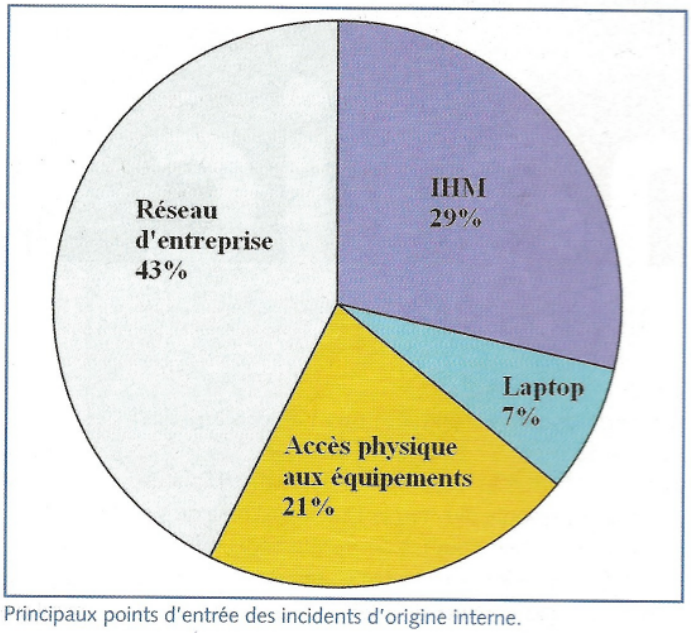
L'ensemble des raisons qui viennent d'être citées expliquent que les ingénieurs de contrôle se retrouvent aujourd'hui en face de systèmes distribués vulnérables à différents types de menaces :

- physiques, tout d'abord, par le biais des failles des réseaux LAN (Ethernet, Wireless, etc.) ou via les médias (CD, disquettes, etc.)
- sur les communications, ensuite, via les failles des protocoles IP, TCP, UDP, etc.
- ou enfin ciblées sur les applications, visant essentiellement les systèmes d'exploitations (Windows ou Linux) ou encore les bases de données, les serveurs mail, web, etc.

Malgré les recherches et les avancées réalisées dans la lutte contre les attaques de virus et de hackers, la plupart des systèmes hôtes Internet ne présentent qu'un faible niveau de sécurité, par exemple à base de mots de passe faciles à deviner, ce qui constitue une violation des règles les plus élémentaires de la sécurité.

Comme le précise Mohammed Belkhalem, spécialiste MES&APC chez Yokogawa France : *« personne ne peut garantir l'inviolabilité totale de son système d'information. La preuve en est que l'on découvre plus de 4000 vulnérabilités par an. Auparavant, lorsque les technologies employées étaient propriétaires, les risques étaient moindres, puisque par définition peu de personnes disposaient d'une connaissance suffisamment approfondie des systèmes. Aujourd'hui les technologies utilisées sont pour la plupart des standards, dont les failles sont connues et exploitées pour le développement de virus. De fait, les anti-virus ont toujours un train de retard. Néanmoins, les mises à disposition de patch sont de plus en plus rapides. Par exemple, pour le virus Blaster, il n'a fallu attendre que 25 jours ».*

Aujourd'hui la plupart des industriels sont réticents à l'idée de dévoiler publiquement les problèmes de cyber-sécurité qu'ils rencontrent. C'est pourquoi il est extrêmement difficile d'évaluer le nombre, les principales origines ou encore la gravité des conséquences de ces problèmes. Néanmoins, un certain nombre d'évènements reportés depuis quelques années semblent indiquer qu'il s'agirait, dans plus de 50 % des cas, d'incidents d'origine interne causés par des employés. Ce sont là les conclusions d'un projet initié par le BCIT/IEL (British Columbia Institute of Technology Internet Engineering Lab) visant à répertorier les problèmes de cyber-criminalité impliquant des systèmes de contrôle industriels. Ces conclusions corroborent les résultats d'une étude menée par le FBI et le CSIC (Computer Security Institute on Cybercrime) en 2000, qui montrait que 71 % des problèmes de cyber-sécurité déclarés impliquaient des employés.

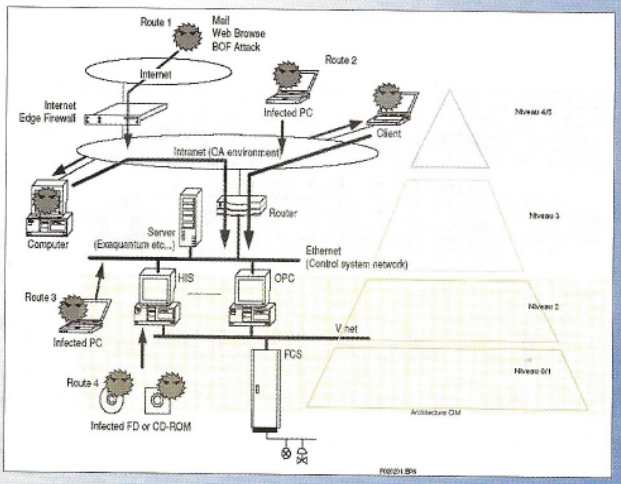


Principaux points d'entrée des incidents d'origine interne.

De nombreux exemples d'incidents sont cités dans « Worlds in Collision-Ethernet and the factory floor », un document co-écrit par plusieurs membres du BICT. Ce document mentionne notamment le cas d'un employé Australien qui fut condamné à deux ans de prison pour avoir piraté au mois d'octobre 2001 un système de traitement des déchets, causant le déversement de millions de litres d'eaux usées dans les parcs environnants et les rivières. Il a plus tard avoué avoir commis cet acte malveillant suite au rejet de sa candidature à un poste d'ingénieur de contrôle au sein de l'usine. Le rapport de la cour incriminerait un réseau sans fil utilisé pour le contrôle SCADA, par le biais duquel l'individu aurait réussi à pénétrer le système.

Et même lorsque les incidents ne sont pas d'origine malveillante, les conséquences peuvent s'avérer catastrophiques pour l'entreprise. Le même document mentionne un problème survenu en 1998 dans une grande papeterie de la côte Est des Etats-Unis. Celle-ci venait d'effectuer une mise à niveau de ses installations et avait pour l'occasion dévoilé à certains cadres dirigeants les mots de passe permettant d'accéder aux ordinateurs du système de contrôle. A la fin du projet, personne n'avait pris la peine de changer ces mots de passe. Les ennuis commencèrent environ un mois plus tard lorsque l'un des ingénieurs décida d'utiliser le réseau étendu (WAN) de l'entreprise pour accéder au système de contrôle de la papeterie, située

Les Principaux Chemins d'Infection



Route 1 : Internet

- Récupération (puis propagation) de fichiers infectés via les téléchargements, les échanges d'e-mail
- Attaques délibérées (dénis de service, Buffer overflow…)

Route 2 : D'un PC infecté connecté au réseau bureautique

- Attaques en rebond

Route 3 : D'un PC infecté connecté au réseau process

- Attaques endogènes

Route 4 : D'un support extérieur copié sur le système

- Infection par les médias amovibles (Disquette, CD-ROM, Clé USB)

à plusieurs centaines de kilomètres de l'endroit où il se trouvait. Ce dernier avait besoin de recueillir des données pour l'un de ses projets en cours. Une fois connectée au LAN de la papeterie, il fut capable de se connecter au système de contrôle par le biais d'une liaison normalement réservée à la supervision. Il installa ensuite un petit programme sur l'une des stations graphiques du système de contrôle, une station UNIX, demandant à cette dernière de lui renvoyer de façon cyclique (toutes les cinq minutes) les données des équipements du système de contrôle.

Tout cela aurait pu fonctionner parfaitement bien si la nouvelle tâche programmée n'avait pas provoqué la surcharge de l'une des passerelles de communication, entraînant la perte du contrôle de l'un des moteurs de l'application. Le problème put être réglé grâce à un ingénieur qui remarqua que le phénomène se produisait à des intervalles de temps réguliers, laissant à penser que la faille était d'origine logicielle. Après avoir passé en revue la totalité des tâches tournant sur les ordinateurs du système, il put isoler la tâche incriminée et remettre le système en état de fonctionnement. Mais ce fut au prix d'une perte de productivité substantielle. Comble de l'histoire : entre temps l'ingénieur responsable de ce fâcheux incident avait changé de travail, il avait été embauché par la concurrence…

Les solutions

Comme le précise Mohamed Belkhalem : *« La mise en œuvre de solutions de sécurité résulte d'un nécessaire compromis. Il convient dans un premier temps de cibler les zones à risques, c'est-à-dire les zones à protéger. Ensuite il faut évaluer la valeur du bien et la comparer aux coûts de la protection. Si par la suite on décide de mettre en œuvre une solution de protection, plusieurs recommandations peuvent être formulées. Typiquement on pourra segmenter le réseau à l'aide de switches ou de routeurs, et mettre en place des systèmes de contrôle d'accès, de filtrage, de firewall, de manière à obtenir une protection périmétrique et diviser le réseau en niveaux ou zones de confiance ».*

Mais si un firewall constitue un premier niveau de sécurité indispensable, il faut également surveiller le trafic et être capable d'identifier les activités suspectes sur le réseau. Pour cela il existe des systèmes, connus sous le nom de SDI (Systèmes de Détection des Intrusions), capables de réagir en cas de détection d'anomalies. Par exemple, la détection d'anomalies peut être basée sur une analyse des données statistiques du système : changement de mémoire, utilisation excessive du CPU, etc. Le SDI signalera les divergences avec le fonctionnement normal du système et pourra éventuellement, le cas échéant, mener des actions correctives.

« Mais ce type de protection ne suffit pas », souligne Mohamed Belkhalem. *« Il faut également se montrer suffisamment dissuasif, bien informer en interne le personnel sur les risques informatiques et promouvoir les réflexes de sécurité ».* Par exemple en convaincant les employés de ne pas ouvrir les e-mail d'inconnus, de ne pas effectuer de téléchargement sur les sites web non sécurisés, ou encore de passer l'antivirus avant de copier les fichiers issus d'un CD ou d'une clé USB. Si cela ne suffit pas il faudra peut-être aller jusqu'à condamner les accès aux lecteurs, ports USB, etc.

Enfin, il convient de développer une stratégie de réponse, définissant les actions à mener en cas d'incident : isolement des machines infectées, procédures de back-up, etc. *« Dans tous les cas, il convient d'adopter une approche pragmatique et de bon sens avec l'aide du DSI (Directeur des Systèmes d'Information) et du RSSI (Responsable de la Sécurité des Systèmes d'Information), en intégrant les automatismes dans des plans tels que Marion ou Mehari »*, conclut Mohamed Belkhalem.

A l'heure actuelle de nombreux organismes travaillent pour répondre aux besoins émergeants des industriels en termes de sécurité des systèmes d'information des réseaux de contrôle. C'est notamment le cas de l'ISA SP-99 (Instrumentation, Systems and Automation) ainsi que du CIDX (Chemical Industry Data Exchange). Le premier a récemment publié deux rapports techniques décrivant les principales technologies de sécurité et la façon de les appliquer aux systèmes de contrôle (ISA TR99.00.01), et donnant les bases de la création de programmes de sécurité efficaces, incluant politiques, procédures et technologies indépendamment du secteur industriel considéré (ISA TR99.00.02). Le CIDX œuvre quant à lui à la résolution des problématiques spécifiques à l'industrie chimique, tout en partageant une grande partie de son travail avec l'ISA SP-99.