

# Protégez votre informatique industrielle

## Pensez vous que :

### Les attaques courantes sur la bureautique sont impossibles sur l'informatique industrielle ?

**Faux :** l'une et l'autre utilisent les mêmes produits et les mêmes protocoles, elles présentent donc le même genre de vulnérabilité !

C'est ainsi par exemple qu'en janvier 2003 le ver 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.

### Votre système n'intéresse pas les pirates qui prolifèrent sur internet ?

**Faux :** ces pirates sont en permanence à l'affût des systèmes vulnérables et les détectent pour les attaquer dès que possible.

### Vos réseaux d'informatique industrielle sont bien protégés ?

**Attention :** les accès Wifi ne sont pas toujours tous recensés et sécurisés ; les ordinateurs portables et PDA qui se connectent occasionnellement au système de contrôle des processus, les clés USB qui y sont parfois introduites peuvent introduire un code malveillant qui n'est pas immédiatement détectable. Les disques durs des systèmes lorsqu'ils sont mis au rebut peuvent être récupérés.

### Aucune attaque interne n'est à craindre ?

**Faux :** les employés peuvent causer des dommages importants s'ils sont mal formés, inconscients ou négligents. Des employés mécontents ou soumis à des pressions externes peuvent aussi commettre des malveillances.

L'informatisation des systèmes de commande et de contrôle des outils industriels, qui s'était au départ appuyée sur des solutions spécifiques adaptées à chaque process s'est aujourd'hui rapprochée des autres systèmes. Le réseau est souvent relié à celui de l'informatique de gestion, les ordinateurs fonctionnent généralement sous Windows ou Unix et les bases de données sont des produits du

commerce. Le réseau est par nature le point sensible de l'installation. L'interconnexion avec des réseaux ouverts, sur l'internet même à travers des pare-feux, l'usage des liaisons sans fil dans des bandes de fréquence ouvertes à tous créent de nouveaux points d'entrée pour des attaques de nature diverses (espionnage, piratage, sabotage, voire terrorisme...)

## Comment se protéger ?

Il n'existe pas de réponse unique. Le choix des solutions relève de chaque entreprise et 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 définition d'une politique de protection de l'informatique industrielle s'inscrit dans le cadre de la politique de protection de son patrimoine, de ses employés et de son environnement. Elle implique une analyse des risques pesant sur l'ensemble des activités de l'entreprise, une prise de conscience de tous les responsables et leur implication, ainsi que la sensibilisation de tous les employés.

La démarche de sécurisation comprend les étapes suivantes :

- analyser les enjeux
- identifier les points sensibles et les systèmes qui doivent être protégés (pour confidentialité, disponibilité de processus, intégrité de paramètres techniques...)
- identifier les menaces et évaluer les vulnérabilités
- déterminer une architecture de sécurité adaptée aux risques
- prévoir les mesures d'accompagnement de sécurité physique des locaux, du personnel, des procédures...
- faire le bilan des risques résiduels

Il faut également développer des procédures d'alerte et d'intervention en cas d'incident, sensibiliser et former le personnel, analyser les risques induits par les sous-traitants, les partenaires, les clients, les fournisseurs...

Ces principes généraux sont ceux de la norme SP-99 et des documents qui l'accompagnent (ISA-TR99.00.01, « Technologies de sécurité pour le contrôle de processus » et ISA-TR99.00.02, « Intégration de la sécurité électronique dans les systèmes de contrôle de processus »), publiés par l'association ISA (disponibles sur <http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821>). Ce sont les seuls textes disponibles actuellement qui traitent de façon organisée la sécurité de l'informatique industrielle. Ils constituent un bon point de départ pour prendre en compte de façon méthodique la problématique de la sécurisation des systèmes d'information à vocation industrielle, avec au besoin l'aide d'un consultant compétent.