La cyber-sécurité des systèmes d'automatisme et de contrôle de procédé

Les cyber-attaques : comment faire face ?

Paris – 26 et 27 juin 2013

Méthodes et pratiques de la cybersécurité industrielle

Thierry Cornu
Responsable Offre Cybersécurité Industrielle
EURIWARE, 1 Pl. Frères Montgolfier, 78280 GUYANCOURT, +33 1 39 48 44 73,
thierry.cornu@euriware.fr

Mots clés : *normes de sécurité industrielle, zones et degrés de sécurité, supervision opérationnelle*

La cybersécurité industrielle constitue un nouveau domaine d'activité pluridisciplinaire. Elle nécessite de faire travailler ensemble des métiers qui n'en avaient pas l'habitude : d'une part les métiers traditionnels de la sécurité informatique et d'autre part les métiers des systèmes de contrôle industriels.

Les différences avec la sécurisation des SI sont fonctionnelles (importance spécifique accordée aux risques de sabotage, contraintes d'exploitation du monde industriel), techniques (vulnérabilités et techniques de protection spécifiques) et réglementaires (environnement normatif complexe et en pleine évolution).

Comme dans d'autres domaines de la sécurité, les premières réponses sont de nature organisationnelle. Puis une architecture de sécurité doit être adoptée, définissant dans les systèmes à protéger des zones de sécurité de degré croissant, dans le cadre d'une stratégie de défense en profondeur. Les mesures de protection et de mitigation sont définies en s'appuyant sur cette architecture et sont plus poussées pour les zones de degré de sécurité élevé. Une infrastructure de supervision opérationnelle de sécurité peut finalement être mise en place si le système est considéré comme particulièrement critique.

Key words: *industrial cybersecurity standards, security-zones and degrees, security operations*

Industrial cybersecurity constitutes a new multidisciplinary field of activity. It requires the collaboration from professionals from different disciplines who where not used to working together, namely IT security professionals on one hand, and automation control professionals on the other.

The differences with IT security are functional (criticality of the risks of sabotage, operation constraints specific to the industrial world), technical (specific vulnerabilities and protection technologies) and regulatory (complex and fast evolving sets of standards).

Not unlike other branches of security, the first answers are usually organizational. Then, a security-architecture is required, defining zones of increasing security degree inside the system to protect, as part of a defence-in-depth strategy. The protection- and mitigation-measures are defined based on this architecture, and reinforced for the zones of highest security degree. Finally, a security-operation infrastructure may be added for especially critical systems.