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

Les cyber-attaques : comment faire face ?

Paris – 26 et 27 juin 2013

Gestion de la cyber-sécurité inter-département (IT vs Production)

Vincent Esmenjaud
Group Leader Information Networks - Strategic Services Europe
Vincent.esmenjaud@emerson.com

Benoit Paredes
Consultant Engineer - Networks & Systems
Benoit.paredes@emerson.com

Mots clés : *cyber-sécurité, organisation, méthodologie, service production, service informatique*

L'évolution technologique (mobilité, cloud computing, accès distants…) et la standardisation créent des nouveaux besoins au sein des équipes d'exploitation mais engendrent également une augmentation du risque de menaces sur les systèmes de production. La gestion de la cyber-sécurité des systèmes industriels est donc devenue un enjeu majeur. Les parades et les outils de défense sont nombreux mais pas forcément adaptés à tous les environnements. Historiquement, il existe encore aujourd'hui sur les sites industriels des différences franches d'organisation et de méthodologie entre le service informatique et le service de production car l'impact d'une menace sur le site n'est pas le même. Les priorités sont donc différentes et on a l'habitude de dire que la disponibilité des installations est celle du service de production tandis que pour le service informatique la confidentialité et l'intégrité des données sont les points primordiaux. Ces priorités évoluent au sein des deux organisations, et on peut observer de plus en plus de besoins communs vis-à-vis de la stratégie de sécurité. Ceci implique une collaboration étroite entre les deux organisations pour garantir efficacité et cohérence. Cette tendance a fait évoluer le rôle et l'offre des fournisseurs de système d'automatisation et en particulier Emerson Process Management. Ils peuvent désormais intervenir pour identifier les méthodologies et les équipements de sécurité applicables au système de production en fonction de ceux qui sont déjà en place au niveau IT. Ils définissent ensuite les outils et les solutions complémentaires afin de mettre en place une politique de cyber-sécurité sur le système d'automatisation qui répond aux standards en vigueur.

Key words: *Cyber-security, organization, methodology, automation, IT*

The new technologies (mobility, cloud computing, remote access ...) and standardization creates new needs within production teams but also creates an increased risk of threats to production systems. Management of cyber-security in industrial systems has become a major issue. Parry and defence tools are numerous but not necessarily suitable to all environments. Historically, there are major differences in terms of methodology and organization between automation department and IT department, mainly because the impact of a threat to the site is not the same. The priorities are different and we are used to say that availability of facilities is important for the production department while for IT, confidentiality and data integrity are the most important points. These priorities are changing within both organizations and we can see more and more common needs regarding security policy. This requires close collaboration between both organizations to ensure efficiency and consistency. This trend has changed the role and offering of automation system provider's in particular Emerson Process Management. They can now identify methodologies and defence equipment applicable to the production system based on those already in place at the IT level. They can then define the tools and complementary solutions to implement a cyber-security policy on automation system that meets the standards.