

Protection des zones sécurisée : les pare-feux à vocation industrielle

Bruno Lequeux

Ingénieur Application

Belden France, 24 Av de La Demi-Lune 95700 Roissy

06 82 80 97 40, bruno.lequeux@belden.com

Mots clés : *Pare-feux, firewalls, antivirus, défense en profondeur.*

Firewalls, IDS, antivirus... Beaucoup d'éléments informatiques existants s'offrent déjà à nous pour assurer la protection des réseaux industriels. Cependant, la protection dans le monde industriel doit répondre à des buts et contraintes souvent bien différents du monde informatique :

- environnements difficiles, gestion du risque, fiabilité, performances, fonctionnements 24*7, produits et protocoles spécifiques, réglementations, séparations par zones (ISA-99), etc.
Les ingénieurs en automatisme ne sont pas des experts IT, mais ils connaissent parfaitement ce qu'ils doivent protéger. Les firewalls informatiques notamment sont trop complexes et nécessitent des ressources considérables, ils sont encore plus difficiles à configurer correctement sur un réseau usine.
Comme en son temps l'adoption de produits industriels pour les réseaux Ethernet usine, le temps est venu aujourd'hui d'adopter des solutions de sécurité à *véritable* vocation industrielle.
- filtrage de contenu, reconnaissance des protocoles d'automatisme, stratégie de défense en profondeur (zones ISA-99) mais aussi : disponibilité, durcissement et configurations adaptées aux automaticiens.

Autant de critères nouveaux qui font une véritable différence avec le monde informatique et qui deviendront vite essentiels dans les années qui viennent.

Key words: *firewalls, IDS, antivirus, defense in depth.*

Firewalls, IDS, antivirus... Many existing IT components are already available to protect the industrial networks. However, protection in the industrial world must meet goals and cope with constraints which are often very different from the IT world:

- Difficult environments, risk management, reliability, performance, 24 * 7 operation, specific products and protocols, regulations, zone segmentation (ISA-99), etc.
Automation engineers are not IT experts, but they know exactly what they need to protect. IT-style firewalls are too complex and require considerable resources and they are even harder to set up properly on the plant floor.
As the adoption of industrial products for Ethernet plant networks was accepted in its time, the time has come to adopt security solutions with *actual* industrial vocation.
- Content filtering, recognition of automation protocols, defense-in-depth (ISA-99 zones) but also availability, ruggedizing and easy configurations for automation engineers.

So much new criteria which make a true difference with the IT world and will quickly become essential in the coming years.