MES, IoT et Cybersécurité

Thierry LAVEILLE, Responsable Produit, COURBON Software

Dans le cadre de l'industrie 4.0 et des capacités technologiques récentes, les industriels ont la possibilité et l'intérêt de récupérer un maximum d'informations depuis les objets connectés. Toutes ces données sont contextualisées et exploitées par le MES.
Ces communications et l'ouverture des réseaux rendent les sites industriels vulnérables aux attaques.

Les risques sont-ils avérés ? pour quels impacts ?

Au vu des événements récents (Wannacry, Industroyer, Stuxnet …) et des statistiques[1], la question n'est plus de savoir si une entreprise risque d'être compromise, mais quand elle le sera.
Les risques induits peuvent se traduire par

- la mise en danger du personnel
- des pertes de production, de qualité …
- des pertes de données sensibles
- des atteintes à l'environnement

⇨ L'approche Cybersécurité est la réponse à ces vulnérabilités.

Pourquoi le MES est au cœur de la Cybersécurité ?

Le MES est au cœur de toutes ses connexions industrielles dans la mesure où il doit pouvoir au minimum contextualiser ces données et les exploiter pour améliorer la performance industrielle :

- Amélioration de la performance machine, de la gestion de la maintenance (réactive, préventive, prédictive)
- Amélioration de la qualité des produits par la surveillance et le contrôle des process, des produits …
- Amélioration de la consommation énergétique
- Ajustement de recettes, personnalisation des produits
- Optimisation du pilotage
- …

Toutes ces connexions IoT amènent à créer de multiples ouvertures dans le système d'information industriel qui sont autant de failles de sécurité potentielles.
Le MES étant au cœur du pilotage, il est à l'interconnexion entre le monde OT des équipements, automates … et le monde IT des outils informatiques centraux ERP, PLM …
Les couches logicielles et surtout les infrastructures réseaux supportant le MES sont donc au cœur des besoins de sécurisation.

Comment assurer la sécurité lors de la mise en place d'un projet Industrie 4.0 ?

La sécurisation est incluse dans la culture des « informaticiens » en charge des couches IT / réseaux d'entreprises bureautiques … mais ce n'était pas le cas des « personnes du contrôle de procédé » en charge jusqu'à aujourd'hui des couches OT.
C'est notamment à partir de ce constat et des cas identifiés de cyber-attaques que divers travaux ont été menés pour aboutir à l'ISA99 ou à des parutions faites par l'ANSII (Agence nationale de la sécurité des systèmes d'information) tel que le document "20151005_NP_ANSSI_SDE_4067_PJ6_serveur_mes_moyen_terme_PJ6.vfp_"

L'application de ces différents éléments mettent en évidence le besoin de disponibilité des systèmes de contrôle et le besoin d'intégrité de données. Ils servent de référence pour la sécurisation d'une installation existante mais aussi pour la mise en place de projets industrie 4.0 intégrant par exemple de l'IoT, un MES … Cela met en lumière l'importance de faire de la sécurisation par la conception même des réseaux (mise en place de zone / VLAN, de firewall) mais aussi de la sécurisation des logiciels (dont le MES) avec de l'authentification … Cette sécurisation peut également inclure la mise en place d'outils d'analyse réseau / sondes permettant d'analyser des intrusions, des échanges non prévus entre automates.

Se protéger et détecter les anomalies est la première étape ; encore faut-il savoir réagir rapidement en cas de problème. Afin d'avoir un maximum de réactivité, les détections doivent être remontées sur des portails dédiés mais aussi au MES qui a l'avantage d'être exploité en continu par les utilisateurs, notamment en l'absence de SOC dédié (Centre d'opérations de sécurité).

[1] : Quelques chiffres :
99% des ordinateurs possèdent des vulnérabilités
81% des entreprises françaises ont été visées par une cyberattaque en 2015
64 % des entreprises envisagent d'augmenter leur budget cybersécurité
Augmentation de 31% des attaques contre des outils de production en 2017 (vs. 2016).
250 000 entités impactées par Wannacry dans 150 pays
1 425 % le retour sur investissement du piratage par *ransomware*, selon le cabinet de conseil Solucom
9 semaines en moyenne pour réparer les dégâts suite à une attaque
1,4 milliards d'identifiants et mots de passe en libre service