OT : MENACES CYBER ET RÉPONSES

CONFÉRENCE CLUSIF

23 JUIN 2022

ACCOMPAGNER NOS FOURNISSEURS

Partage de pratiques

David Arnold – Michelin

COMMENT TOUT A COMMENCÉ

1. Usine arrêtée suite à propagation d'un malware via clé USB
2. Tests d'intrusion sur l'IT avec rebonds sur l'OT

- Déploiement de FW pour séparer IT/OT dans les 70 usines du groupe
- Service CYBER-OT au sein du Manufacturing

- Référentiel sécurité OT (N2-N3 puis N1)
- Rôles, responsabilités et modèle d'organisation usine
- Tests et qualification de solutions adaptées à l'OT
- Outillage maison (inventaire auto, indicateurs …)
- RSSI hors organisation IT et RSSI industriel
- Contrôle Interne
- Rapprochement des compétences IT/OT
- Evènements sécurité OT remontés dans le SIEM IT

Mais partant de ce constat:

- De nouvelles machines industrielles à connecter, avec des niveaux de protection variable
- Des achats de machines en local ou en central
- Des fournisseurs internes ou externes à sensibiliser
- Des contrats de maintenance MCO qui n'incluent pas de MCS

Comment mettre la cale ?

UNE INTÉGRATION MAITRISÉE

Avant d'exiger des contraintes sécurité à nos fournisseurs, il faut être prêt à les accueillir.

Mise en place d'une architecture standard:

- DMZ par fournisseur ayant besoin de se connecter à distance
- Accès VPN avec les outils fournis par le groupe
- Remontée de données sur internet bloquée par défaut

Discussions avant-projet:

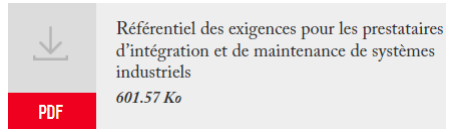
- [Sauvegardes] Quels sont les éléments virtualisables et manageables par les hyperviseurs existants ?
- [Inventaire/Monitoring/Veille patching] Les agents préconisés peuvent-ils être installés ?
- [Comptes] Les systèmes s'intègrent-ils dans l'AD industrie ?
- [Système] Les bases de temps du système peuvent-ils se mettre à jour sur nos serveurs NTP ?
- [Maintenance] Le contrat de maintenance couvre-t-il le MCS an plus du MCO ?

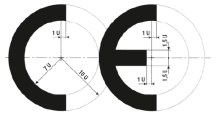
Ces discussions permettent aussi d'évaluer la maturité cybersécurité du fournisseur

UN CERTIFICAT « ICS CYBERSECURITY »

Le besoin: s'assurer que les machines industrielles, installées en usine:
- respectent un niveau de cybersécurité minimum dès leur installation
- sont prévues pour maintenir ce niveau pendant toute leur durée d'exploitation

En mettant en œuvre, dès le processus d'achat, un jeu de contrôles.





Mise en place d'un certificat:
- par Fournisseur: suite à validation du Plan d'Assurance Sécurité, le fournisseur auto-certifie que les machines livrées sont conformes au chapitre cybersécurité du Cahier des Charges, qu'elles s'intègrent dans une architecture réseau validée et que le MCS est prévu (contrat de maintenance ou pas).
- par type de Machine: une revue de conformité est effectuée par un groupe d'experts (info indus et automatismes)

Intégration dans les **protocoles de réception** machine industrielle (FAT, SAT) des contraintes cybersécurité:
- check-list revue et signée par le fournisseur et le chef de projet, et fournie au responsable informatique site

Le **responsable informatique** du site a le droit et le devoir de ne pas connecter une machine non réceptionnée

DES ANNEXES SÉCURITÉ DANS LES CONTRATS

Le constat: plus de projet industriels qui n'embarquent pas d'IT, OT, IIoT !
La sécurité de nos données et de nos systèmes dépend de plus en plus des mesures de sécurité techniques et organisationnelles du fournisseur et de sa chaîne de sous-traitants

Processus d'appel d'offre:

- Questionnaire cybersécurité demandé à chaque fournisseur
- Analyse des réponses et évaluation de la maturité cybersécurité

Contractualisation:
Une annexe sécurité plus ou moins détaillée ajoutée au contrat. Elle comprend des clauses sur la sécurité SI du fournisseur:

- Existence d'une PSSI, Sensibilisation des employés
- Infrastructure IT et PC protégés

Mais aussi des clauses sur les services

- SLA sur le patching sécurité
- Gestion des incidents de sécurité (Qui et comment nous informer)

L'acheteur doit s'assurer que ces points sont traités

ET SI ON NE FAIT RIEN ?

Si on ne s'en préoccupe pas, outre le risque cybersécurité, on court aussi le risque de ne plus pouvoir adresser le marché

Des règlements de plus en plus présent:

- RGPD
- LPM, directive NIS2
- Dans le monde automobile (embarqué/débarqué), UNECE R155 et R156

Des exigences client de plus en plus fortes:

- Questionnaires cybersécurité (Airbus, Toyota, …). Simple sondage, questionnaire, preuves à fournir
- Certifications ISO27k, SOC2
- Certifications TISAX – Trusted Information Security Assessment eXchange
    - Audits par organisme externe qualifié

UN CERTIFICAT POUR UNE RECONNAISSANCE PLUS LARGE

Le certificat Michelin ayant une portée limitée pour un fournisseur, pourquoi ne pas s'appuyer sur la norme IEC62443?

Nous nous posons la question aussi pour les machines industrielles que nous pourrions vendre.

Il est prévu dans cette norme une certification « système »: 62443-3-3
Une machine industrielle est bien un « système », c'est-à-dire un ensemble de composants dans une architecture réseau.

Merci pour votre attention