Famille 4 - version 1 Date : 26/02/2016

Cybersécurité

Description / Définition

Les programmes informatiques sont devenus parties intégrales du fonctionnement des systèmes de production, et ce à tous les niveaux de l'entreprise (commande numérique, machine connectée, MES, ERP, CRM, email d'entreprise, intranet,…). De leur bon comportement, dépendent de nombreux aspects d'un environnement industriel : le pilotage des outils de production, leur infrastructure de collaboration, la mise en œuvre des réseaux logistiques, ou la gestion de l'entreprise. Or les découvertes régulières de failles de sécurité permettant de prendre la main sur de larges ensembles de processus et de données supposés sécurisés (ex : « Heartbleed », cyber-attaque contre l'Aciérie Allemande) rappellent régulièrement les enjeux d'intégrité, de confidentialité et de disponibilité des systèmes informatisés.

Face à cet état de fait, deux types d'approches complémentaires se dégagent :

- La conception, l'implémentation, la validation et la mise en production de nouveaux composants sécurisés. Cette approche se concentre principalement sur les trois briques fondamentales de la sécurité : les supports d'exécutions ou Operating Systems, les supports de communication et leurs protocoles, et les supports cryptographique
- La mise en œuvre de méthodes et d'outils de sécurisation de composants, à travers une évaluation de leur sécurité, et pouvant être accompagnés d'un processus de certification. Cette approche concerne l'intégralité des activités d'évaluation, et en particulier les analyses de risque, les analyses de protocoles, et les analyses de code.

Enjeux (avantages)

Les menaces sur ces programmes sont nombreuses, et en croissance, motivées par les enjeux considérables que représentent l'intégrité, la confidentialité et la disponibilité des entités qu'ils pilotent. Garantir une réelle immunité des systèmes d'importance critique face à des entités hostiles est ainsi devenu en quelques années un enjeu majeur, en termes de productivité mais aussi d'image de marque. De nouvelles technologies existent pour assurer cette protection, et fournir des méthodes et des composants permettant d'assurer la sécurité des composants logiciels critiques.

Sur le plan technologique

Les domaines d'application sont multiples :

- Sécurisation des process
- Maîtrise des incertitudes liées à la flexibilité
- Certification de chaînes numériques et physiques complexes.

Sur le plan numérique

- Indépendance des logiciels métiers par rapport au firmware machine
- Confidentialité des données chiffrées et de leur traitement par une entité extérieure
- Analyse des logiciels critiques et preuve d'absence des classes de vulnérabilités les plus courantes
- Surveillance automatisée de logiciels tiers
- Mise en œuvre de systèmes de sécurisation des communications
- Détection d'intrusions sur les réseaux, même lorsque ceux-ci sont reconfigurables
- Maîtrise de la diffusion du risque de compromission d'une entité pour éviter les effets cascade (cloisonnement, résilience,…).

Sur le plan économique

- Continuité opérationnelle, préservation des secrets industriels
- Communication externe en mettant en avant l'image d'entreprise de confiance.

Sur le plan de la transformation de l'entreprise

- Toutes les fonctions de l'entreprise peuvent être impliquées, en fonction de la criticité de leurs systèmes d'information et de leurs contraintes opérationnelles
- Sensibilisation et transformation de la culture d'entreprise et des pratiques à travers la maîtrise du risque cyber.

Sur le plan environnemental, sociétal

Amélioration de la responsabilité de l'entreprise en termes de maîtrise des risques et de préservation des libertés informatiques. Formation sur un nouveau profil de compétence dédié à la cybersécurité.

Les clés de la réussite

Les PME françaises, pour investir utilement sur la cybersécurité de leurs activités, doivent bâtir une véritable stratégie industrielle, et un plan de communication afférent, autour de 5 piliers non séparable : l'économie (rentabilité, CA), la production (performance, qualité), l'intégration (process, système d'information, évolution), le réglementaire (directives, normes) et l'humain (valorisation, conditions de travail).

Au niveau numérique

- Documenter la structure et le fonctionnement des systèmes existants
- Identifier les standards de certification adéquats
- Etablir la provenance et s'assurer de la confiance à accorder aux composants numériques de l'entreprise.

Au niveau des compétences à mobiliser, des connaissances et de la formation

- Impliquer les équipes métier dans l'analyse de cybersécurité et la sélection de solutions. S'appuyer sur des spécialistes de la cybersécurité pour s'initier à son écosystème.

Les questions à se poser

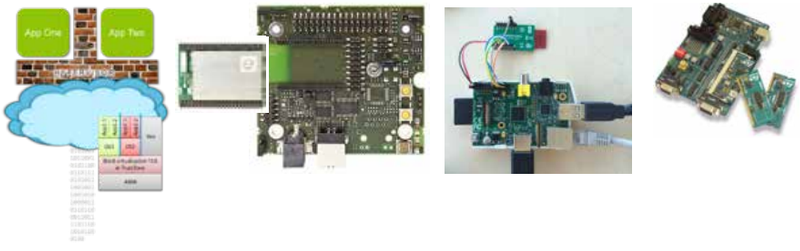
- Quelles sont les informations dont la diffusion ou la modification doivent être maitrisées ?
- Quel est l'impact d'une faille de sécurité (production, image, compétitivité ?)
- Quels sont les moyens mis en œuvre pour parer à cette éventualité ?
- Comment l'efficacité de ces moyens est-elle évaluée ?

Maturité de l'offre et de l'adoption

Emergent	Laboratoire	**Prouvé**	**Mature**	Fréquent	Répandu

Illustrations

Composants de sécurité des exécutions et des communications



Outils d'analyse de code

Liens utiles

Guide ANSSI de la Cybersécurité des systèmes industriels
http://www.ssi.gouv.fr/administration/bonnes-pratiques/systemes-industriels/
CEA-LIST
http://www-list.cea.fr/index.php/en/innovating-for-industry/our-assets-for-industry
GIMÉLEC
http://www.gimelec.fr/Cybersecurite-Big-Data-et-Open-Data