Nouvelle France industrielle
Véhicule autonome

Axe « sécurité »

Sadio Bâ
Agence nationale de la sécurité des systèmes d'information
IRT System'X – 25 mai 2016

NE PAS REDIFFUSER SANS AUTORISATION DE L'EMETTEUR

Contexte général

L'ANSSI : Agence nationale de la sécurité des systèmes d'information

Agence dépendant du Premier ministre, avec une double mission

- Autorité nationale de sécurité des systèmes d'information (**prévention**)
  - Référentiels et guides
  - Politique industrielle et labellisation
  - Audits, inspections et contrôles
  - Assistance technique
  - Recherche et développement
  - Formation et sensibilisation
  - Élaboration des textes réglementaires
  - Planification et exercices
  - Relations internationales
  - Gestions de clés cryptographiques
  - …
- Autorité nationale de défense des systèmes d'information (**réaction**)
  - Veille, analyse et évaluation de la menace
  - Détection des attaques
  - Réponse aux attaques

Écosystème

Un large périmètre à sécuriser

- Administrations et opérateurs sous tutelle
- Opérateurs d'importance vitale (OIV)
- Acteurs économiques (industriels, entreprises…)
- Particuliers

Avec l'aide de prestataires et de produits qualifiés

- Prestataires de confiance
  - Prestataires de service de certification électronique (PSCE)
  - Prestataires d'audit de la sécurité des systèmes d'information (PASSI)
  - Prestataires de détection d'incidents de sécurité (PDIS)
  - Prestataires de réponse aux incidents de sécurité (PRIS)
  - Prestataires de service d'horodatage électronique (PSHE)
  - Prestataires de services sécurisées d'informatique en nuage (*Cloud*)
- Produits qualifiés
  - Chiffrement, infrastructure de gestion de clés, mobilité, pare-feu, poste de travail, ressources cryptographiques, signature électronique et Gestion de la preuve, titres d'identité électroniques

L’automobile : un secteur en mutation

Une solide culture systémique et de sûreté de fonctionnement…

- Un secteur où la sureté de fonctionnement (*safety*) est consubstantielle
- Le véhicule autonome est une illustration de l’internet des objets

…sous le joug d’une numérisation inéluctable

- Une surface d’attaque toujours plus grande
- Une adoption des systèmes et des technologies standards ou connus
- Des nouveaux usages et services
- Un développement du télé diagnostique/maintenance
- E-call

Architecture du modèle de l'internet des objets

Plateforme de service

- (Stockage, traitement et analyse des données)

Communication sans fil

- Spectre hertzien (3G/4G LTE, Wifi G5…)

Objets

- Mobiles, Véhicules,…

Quelques recommandations de sécurité

Quelques recommandations de sécurité

- Intégrer les enjeux et besoins de sécurité tout au long du projet
- Privilégier les approches de sécurité « par conception » pour le logiciel et le matériel
- Sensibiliser, former et outiller les développeurs et intégrateurs
- Adopter le concept de défense en profondeur (barrières technologiques, organisationnelles ou humaines)
- Utiliser des composants labellisés
- Évaluer le risque cyber, homologuer ses systèmes (homologation de référence)
- Il est possible d'obtenir un bon niveau de sécurité sans efforts démesurés

Bonnes pratiques

- Contrôle d’accès physique aux équipements
- Cloisonnement des réseaux, brider les interfaces, chiffrement
- Protection antivirale
- Gestion des médias amovibles
- Durcissement des configurations, environnement dédié, pas de services superflus
- Politique de sauvegarde
- Gestions des journaux d’événements et d’alarmes
- Détection des intrusions
- Gestion des configurations
- Mise à jour des correctifs

Enjeux majeurs

- La supervision (SOC d’une flotte de véhicules)
- La mise à jour à distance
- La réception du véhicule

Besoins et opportunités

La dualité : sûreté *vs* sécurité

Les exigences de sécurité sont très fortes et multi factorielles (confidentialité, intégrité, disponibilité, traçabilité)

- La cybersécurité impacte directement la sûreté de fonctionnement
- Les cycles d'évolution de la cybersécurité et de la sûreté de fonctionnement ne sont pas synchrones

Les contraintes d'exploitation sont extrêmement élevées

- Le maintien en condition de sécurité est difficile à concilier avec la sûreté de fonctionnement
- Certaines bonnes pratiques sont impossibles opérationnellement (identification systématique, authentification, journalisation, droits d'accès, cloisonnement natif, filtrage…)
- Le nécessaire recours à des médias amovibles
- La télé maintenance depuis des postes non maitrisés
- La détection n'est pas nativement implémentée

De bonnes raisons de considérer la cybersécurité

Satisfaire les exigences de cybersécurité est une **nécessité**

- Pour certains clients afin de respecter les dispositions de l'article 22 de la Loi de Programmation militaire 2014-2019.
- Pour beaucoup afin de respecter la directive européenne sur la sécurité des réseaux et des systèmes d'information en Europe adoptée début 2016 (directive NIS pour *Network and Information Security*).
- Pour tous afin de garantir la sécurité du véhicule autonome. **La cyber sécurité est dorénavant indissociable de la sûreté de fonctionnement**.

La cybersécurité est aussi une **opportunité**

- Pour les industriels du secteur :
  - Rendre les produits plus attractifs
  - Capitaliser sur les points forts nationaux (cryptographie, composant de sécurité, évaluation)

Le rôle de l'ANSSI

Aider les industriels à sécuriser leurs produits

- Guides et recommandations : www.ssi.gouv.fr
- Échanges techniques et collaborations de recherche
- Orientation de la R&D
- Évaluation et labellisation de sécurité
- Contributions aux travaux normatifs
- Nouvelle France Industrielle, plan cybersécurité piloté par l'ANSSI

Merci !

Questions ?

sadio.ba@ssi.gouv.fr