COMPTE-RENDU
ATELIER SCADA ET CYBERSÉCURITÉ

Animateur

Marc BRAMI, *Rédacteur en chef*
Global Security Mag

Participants

David EUDELINE
DGA

Aurélien PERROT-DELAHOUSSE
AIRBUS DEFENSE AND SPACE

Philippe LOUDENOT
CESIN

Guillaume MALGRAS
ENGIE INEO DEFENSE

David EUDELINE
DGA

Des actions de plusieurs natures ont été prises au sein du Ministère :

- L'élaboration d'un guide méthodologique de classification des systèmes avec l'ANSSI (« Méthode de classification et mesures principales ») ;
- La déclinaison d'une directive au sein d'un groupe de la DGSIC ;
- Un travail d'expertise pour être capable d'améliorer le niveau de sécurité. Deux thèses sont notamment en cours de rédaction à Grenoble, thèses qui sont soutenues par la DGA (dont une sur la détection d'entrée sur le SCADA).

Une étude a été réalisée aux Maldives pour évaluer la menace et essayer de mettre en œuvre une solution sur des bâtiments de la Marine.

« La durée des projets est limitée, il est donc primordial de penser la sécurité dès la conception même des équipements. »

Mise en exergue de l'importance de la rédaction du cahier des charges :
Les partenaires d'un contrat se retrouvent souvent face à des problèmes de coûts. Est-ce dû à la mauvaise rédaction du cahier des charges ou est-ce seulement un problème de compétence ? Est-ce que le donneur d'ordre dans son cahier des charges a précisé ce qu'il voulait côté cyber ? Ces questions doivent se poser si l'on veut travailler à une meilleure sécurité des systèmes. Les industriels commencent tout juste à comprendre la nécessité de mettre des adresses IP dans les équipements.

Un autre problème lié aux investissements industriels est la durée : la durée des projets est limitée, il est donc primordial de penser la sécurité dès la conception même des équipements. Les systèmes d'informations se retrouvent souvent cloisonnés et cela aboutit à un problème de coordination des différents acteurs impliqués. Cela mène à une mauvaise pratique et une mauvaise utilisation de ces systèmes.

La question de la mobilité doit être posée : est-il nécessaire de se déplacer pour la maintenance des systèmes, ou peut-on le faire à distance ? Aujourd'hui, on ne se déplace plus qu'en fonction du nombre des objets à maintenir. Les systèmes SCADA permettent en effet de limiter le nombre de déplacements faits par les techniciens.

« Il faut éviter que les moyens de contrôle ne tombent en panne ou soient détruits par des actes de malveillance. »

Aurélien PERROT-DELAHOUSSE
AIRBUS DEFENSE AND SPACE

Trois axes de développement interne sont développés chez ADS :

- L'axe « *Enterprise automation* » : c'est à dire tout ce qui est en rapport avec les contrôles d'accès, le « HVAC » (chauffage, ventilation et climatisation), le contrôle de l'alimentation électrique, l'éclairage, et la prévention des incendies. Il faut éviter que les moyens de contrôle ne tombent en panne ou soient détruits par des actes de malveillance.
- L'axe « *Industrial tools* » : les machines-outils, l'industrie 4.0… Le problème des SCADA se pose aussi car l'humain est de plus en plus en contact avec les outils industriels automatisés. La chaîne de production est de plus en plus automatisée et l'impact d'une attaque sur elle serait donc d'autant plus important du fait de la présence des systèmes d'informations.
- L'axe « *Products* » : lanceurs, satellites, avions, moyens au sol... Airbus a pour volonté de développer ses systèmes industriels automatisés dans ces domaines.

« La chaîne de production est de plus en plus automatisée et l'impact d'une attaque sur elle serait d'autant plus important. »

Trois axes de développements en externes (cybersécurité) :

- « Promouvoir la sécurité nativement intégrée dans les produits » : c'est à dire le développement des services de sécurité avec de plus petites structures, comme les PME. De l'autre côté, Airbus développe son offre autour de l'audit et de l'analyse de risque (pour savoir s'ils ont un impact et connaître l'état de leur système). Stormshield est en partenariat avec Schneider Electric et Gemalto pour la sécurité des terminaux mobiles par exemple. Le rôle des assurances rentre aussi en compte dans cette promotion de la sécurité, car l'assureur doit sensibiliser ses clients et se doit de recommander un audit de sécurité.
- « Traiter le défi du manque de professionnels qualifiés » : Airbus a une chaire en cybersécurité des infrastructures critiques, portée par Télécom Bretagne. La Cyberweek, quant à elle, leur permet d'avoir des professionnels de plus en plus qualifiés. Ils ont notamment proposé durant cet événement des « cyber challenges » avec des défis techniques à résoudre.

- « Continuer l'effort de R&D » : 20% du chiffre d'affaires d'Airbus est consacré à la recherche et au développement, avec une priorité sur les ICS (Industrial Control Systems), pour créer des produits (ou adapter les produits actuels) aux besoins des industriels (gestion des vulnérabilités, outils d'analyse et de supervision du SOC (Security Operating Center), sondes, pare-feu). La compagnie développe également la cryptographie en lien avec l'Europe.

« L'assureur doit sensibiliser ses clients et se doit de recommander un audit de sécurité. »

Airbus travaille avec SystemX sur des véhicules connectés et avec l'ANSSI pour former des automaticiens (sensibilisation à la cybersécurité) et des logiciels pour la protection nationale.

DISCUSSION

L'analyse de risque des systèmes SCADA :
Les systèmes SCADA permettent de faire des choses plus simples si on élargit le spectre de ce qu'ils peuvent atteindre. Il est essentiel de voir le système SCADA dans tout son ensemble. L'exemple d'une attaque de pirates en Ukraine a mis en valeur les impacts très sensibles qu'une attaque peut avoir si elle est faite au bon moment et au bon endroit.
Il faut donc connaître les risques et l'état de la sécurité de son système (points d'accès et d'interconnexions), pour mettre en place des mesures simples (mesures techniques type firewalls, sondes, mesures organisationnelles), mais qui permettent de réduire le risque.

Les bonnes pratiques :

- La clé USB : utiliser seulement des clés USB qui ne peuvent échanger des documents qu'entre deux ordinateurs connectés sur le même réseau. Une fois utilisées sur un autre réseau, il ne faut pas les réutiliser sur le réseau initialement prévu, pour ne pas risquer de le compromettre.

« Ces bonnes pratiques doivent permettre d'éviter le pire scénario qui puisse arriver : celui d'une attaque sur les centrales électriques : il y aurait un arrêt complet de toutes les infrastructures critiques (eau, hôpitaux, transports). »

- qu'entre deux ordinateurs connectés sur le même réseau. Une fois utilisées sur un autre réseau, il ne faut pas les réutiliser sur le réseau initialement prévu, pour ne pas risquer de le compromettre.

- Appel d'offre : lors d'un appel d'offre, il faut réclamer le H-Code auprès du fournisseur et le vérifier régulièrement. Cela permet notamment de contrôler qui le commande à distance.

- Analyse de risque : voir ce que l'on veut analyser et à quel niveau (ce qui permet d'aller vite et de ne pas s'éparpiller).

Ces bonnes pratiques doivent permettre d'éviter le pire scénario qui puisse arriver : celui d'une attaque sur les centrales électriques : il y aurait un arrêt complet de toutes les infrastructures critiques (eau, hôpitaux, transports).

« Il faut connaître les risques et l'état de la sécurité de son système, pour mettre en place des mesures simples mais qui permettent de réduire le risque. »

Evolution des métiers :
Il est aujourd'hui nécessaire d'être capable de revenir en arrière et de savoir utiliser les équipements du passé même si cela prend plus de temps. En effet, si un jour nous n'avons plus accès aux systèmes modernes auxquels nous sommes habitués, serions-nous capables d'utiliser des moyens antérieurs ? L'exemple du tunnel comme cas d'étude proposé par l'ANSSI a permis de mettre en évidence notre dépendance aux systèmes d'informations (éclairage, HVAC, etc).

Cela permet par ailleurs à l'industriel de se construire un certain nombre de mesures afin de limiter voir même de supprimer les menaces (même s'il n'a pas besoin de toutes les appliquer in fine).
En conclusion, il est nécessaire de sensibiliser l'utilisateur aux risques. Les objets connectés peuvent se retourner contre nous, il faut les utiliser, sans en être dépendant, pour garder une marge de sécurité.



CE QU'IL FAUT RETENIR

⧫ Il est donc primordial de penser la sécurité dès la conception même des équipements.

⧫ La chaîne de production est de plus en plus automatisée et l'impact d'une attaque sur elle serait d'autant plus important.

⧫ Il faut connaître les risques et l'état de la sécurité de son système, pour mettre en place des mesures simples mais qui permettent de réduire le risque.

⧫ Ces bonnes pratiques doivent permettre d'éviter le pire scénario qui puisse arriver : celui d'une attaque sur les centrales électriques : il y aurait un arrêt complet de toutes les infrastructures critiques