Cybersécurité des systèmes embarqués et des objets connectés

PAROLE AUX PARTENAIRES

Sébastien SALAS
Directeur CAP'TRONIC
Grand Sud-Ouest

La thématique qui monte en puissance au sein du programme CAP'TRONIC concerne la cybersécurité des systèmes embarqués et des objets connectés. CAP'TRONIC s'est donc donné pour mission de mieux informer et sensibiliser les PME.

DES FAILLES CONNUES MAIS IGNORÉES

Le phénomène est en plein essor, il n'y a pas une semaine sans que la presse ne nous annonce l'attaque du système d'information d'une entreprise pour un vol de données ou pour faire un acte de malveillance. Selon le cabinet de conseil PWC «En moyenne, douze attaques ont lieu tous les jours » en France et «1 entreprise sur 2 n'a pas de programme de cybersécurité en France»*. Les attaques concernant les objets connectés mal sécurisés ne font que commencer et le phénomène va certainement s'amplifier.
La très grande majorité des attaques ciblent des failles bien connues pour lesquelles existent déjà des correctifs de sécurité, souvent depuis des années, mais que les entreprises n'installent pas. Une des premières préconisations est qu'il est donc capital de faire systématiquement des mises à jour du système d'exploitation.

Pour les entreprises qui développent de l'électronique, elles peuvent utiliser les mécanismes de chiffrement et de protection de la propriété intellectuelle qui sont déjà présents dans les microcontrôleurs contre la copie du logiciel embarqué.

DES SÉMINAIRES DE SENSIBILISATION ET DES FORMATIONS POUR APPRENDRE À SE DÉFENDRE

Le principal problème en termes de sécurité lors du développement d'un produit est la méconnaissance (ou la non-évaluation) de la menace, d'autant plus lorsque ce produit est communiquant et qu'il est développé rapidement. L'impasse sur la sécurité est trop souvent monnaie courante pour des raisons économiques ou de délais de livraison, évidemment à tort.

C'est pourquoi CAP'TRONIC propose de sensibiliser les développeurs à la conception d'architectures sécurisées et aborde dans un séminaire spécifique, la cryptographie et les techniques anti-clonages / antipirates la avec la mise en œuvre du chiffrement des données (DES, RSA, AES...) pour assurer la protection de la propriété intellectuelle. Les prochaines sessions qui auront lieu en juin sur Bordeaux et en octobre sur Montpellier sont en préparation.

TENIR COMPTE DE LA SÉCURITÉ DÈS LE DÉBUT DE LA CONCEPTION

Pour le hardware des équipements industriels souvent complexes, ou pour les systèmes à haute valeur ajoutée aux données sensibles mieux vaut opter pour une sécurité dès la conception pour chaque composant contenant l'accès au logiciel embarqué. C'est aux électroniciens de faire le nécessaire pour la protection des appareils et pour cela, rien de tel que de comprendre comment font les hackers pour attaquer afin de se prémunir et anticiper leurs actions.
CAP'TRONIC aide les PME à faire le premier pas dans la cybersécurité des systèmes embarqués et des objets connectés. La formation mise en œuvre à ce sujet a pour but, entre autres, de mettre en évidence les menaces et la simplicité de certaines attaques pour mieux se prémunir (prochaine session de la formation cybersécurité à Toulouse du 7 au 9 novembre).

LE GUIDE CYBERSÉCURITÉ « PME : COMMENT MAÎTRISER LA CYBERSÉCURITÉ DE VOS OBJETS ET SYSTÈMES CONNECTÉS »

**Pour compléter l'information des PME, CAP'TRONIC a également publié un guide accessible gratuitement en ligne sur www.captronic.fr : « PME : Comment maîtriser la cybersécurité de vos objets et systèmes connectés ? ».
Produit par CAP'TRONIC et soutenu par la Direction Générale des Entreprises (DGE), l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et l'Institut de Recherche Technologique (IRT) Nanoelec, ce guide a pour objectif de présenter les bonnes pratiques à mettre en œuvre pour assurer la cybersécurité des produits et systèmes connectés.**

Plus d'informations : www.captronic.fr

*Source : www.ouest-france.fr/high-tech/internet/les-cyberattaques-coutent-de-plus-en-plus-cher-aux-entreprises-5361685