#08

SQY INVENTE LA VILLE DU FUTUR

DÉCOUVREZ
L'ÉCOLE DU NUMÉRIQUE

SAINT QUENTIN EN YVELINES
Terre d'innovations

[S]IMMOBILIER SQY
MAGAZINE ÉCONOMIQUE DE SAINT-QUENTIN-EN-YVELINES TERRITOIRE D'AMBITIONS

© Christian Lauté

AIRBUS INVESTIT POUR LA SÉCURITÉ DES BÂTIMENTS INTELLIGENTS

Le projet s'appelle FUSE-IT. Il est développé par un consortium européen et coordonné par Airbus CyberSecurity. Il vise à apporter des solutions concrètes et innovantes pour la cybersécurité des bâtiments intelligents. Explications.

« *À l'origine, le besoin est né d'un constat fait ici, dans nos bâtiments d'Élancourt. Il existe un conflit entre les contraintes d'efficacité énergétiques et l'exigence de sécurité du groupe. Nous avions besoin de connecter les systèmes et de les gérer à distance (par Internet), mais les technologies actuelles ne permettent pas de garantir la sécurité. N'importe quel hacker expérimenté peut prendre le contrôle d'un système de gestion technique du bâtiment à l'état de la technologie actuelle,* explique Adrien Bécue, responsable recherche et innovation d'Airbus CyberSecurity. *D'un côté j'ai un responsable énergie qui exprime ses besoins en outils de gestion des systèmes et de l'autre un responsable sécurité pour qui la chaîne d'énergie, la gestion technique du bâtiment, la bureautique et la sécurité physique doivent être physiquement ségrégués, et l'ouverture des systèmes sur Internet réduite au strict minimum.* » C'est donc là qu'intervient le projet FUSE-IT. Dans le cadre de ce projet, mené par un consortium européen, Airbus a breveté un mécanisme d'authentification qui permet de sécuriser les échanges de données entre objets connectés (IoT). Ce système, unique en Europe, permet de nous prémunir contre des tentatives d'intrusion et d'altération de données par des objets malveillants (*rogue devices*). Par exemple, un attaquant qui tenterait de modifier le relevé de température d'une salle de serveur pourrait causer une surchauffe, une combustion des équipements, voire une explosion engendrant des dégâts matériels et humains. « *Il s'agit d'une des briques qui nous permet de sécuriser tout ce qui concerne le monde des objets connectés* », confie Adrien Bécue. « *L'autre grand intérêt du système est qu'il est capable d'adresser tous les protocoles de communication sans fil existants et peut donc être adapté pour sécuriser la voiture connectée et les autres domaines intégrant massivement des objets connectés, notamment pour la production industrielle.* ». Le deuxième volet du projet consiste à permettre l'authentification et la corrélation entre les incidents physiques et les incidents informatiques. « *Lors d'une intrusion, aujourd'hui il faut deux personnes pour identifier le problème, une pour l'intrusion physique dans le bâtiment et une autre pour la détection du problème lié aux réseaux informatiques. Demain, les infos pourront être corrélées afin de détecter des attaques combinées, de localiser et d'identifier l'attaquant* », explique Adrien Bécue. Ce système intéresse particulièrement les forces armées et les infrastructures critiques telles que les centrales électriques qui ont largement recours à des protections physiques pour assurer la sécurité de leurs systèmes opérationnels. Ce résultat pourrait, lui aussi, connaître un succès considérable sur le marché s'il devait être commercialisé. Au stade de recherche appliquée, reste aujourd'hui à transformer les résultats du projet pour démontrer leur efficacité en milieu réel et les mettre sur le marché. ◆

À L'ABRI DES CYBER-ATTAQUES