4 mai 2016

Un enjeu crucial pour les constructeurs et les conducteurs

Des voitures connectées invulnérables aux pirates informatiques

Il n'existe pas de médaille sans revers, de progrès sans effet pervers. Comme tous les objets, la voiture est appelée à être de plus en plus connectée. Mais du même coup, sa vulnérabilité aux « hackers » va s'accroître. La solution ? Une mobilisation de tous les constructeurs automobiles pour toujours conserver une longueur d'avance sur l'imagination des pirates. Bureau Veritas, en partenariat avec Devoteam, présente pour la rentrée 2016, un guide technique de bonnes pratiques, compatible entre tous les constructeurs et leurs équipementiers.

Des voitures téléguidées, mais par qui ?

Autonome, autopilotée, la voiture du futur est déjà là ! Les constructeurs ont bien compris les aspirations de la clientèle. Certains veulent continuer à vaquer à leurs tablettes tout en roulant. D'autres, jusque-là privées de conduite en raison de leur âge ou de leur handicap, vont apprécier de retrouver la mobilité. C'est assurément un progrès. Sauf qu'une innovation n'est jamais bonne ou mauvaise par elle-même. C'est l'usage qu'en font ensuite les hommes. Or, une personne mal intentionnée pourrait demain prendre le contrôle à distance d'une voiture et la mener où elle veut, sans que ses occupants puissent réagir.

Les risques du cyber piratage

C'est une illustration des risques du cyber piratage. Et le risque de prise de contrôle à distance commence dès que la voiture est connectée. Bureau Veritas a répertorié une liste déjà longue de dangers potentiels, liés à l'utilisation malveillante de technologies de progrès. Elle comprend le vol du véhicule, le vol de données, des atteintes à la sécurité du conducteur, des actes criminels, voire terroristes. Ces derniers peuvent se traduire par des manœuvres d'intimidation : la voiture est contrôlée à distance contre la volonté du conducteur, ou le véhicule est rendu temporairement hors d'usage. Les pires scenarii catastrophe peuvent être imaginés.

L'indispensable concertation des constructeurs

La réplique passe par un bouclier durablement plus puissant que les multiples lances des assaillants. Il faut donc une sécurité sans faille dans le dispositif. L'ennui, c'est qu'il n'existait pas jusqu'à présent de guide commun dans l'industrie. Les équipementiers, constructeurs et développeurs d'outils connectés ont certes tous bien travaillé sur le sujet, mais séparément. Du coup, la chaîne globale est composée de maillons faibles. Pour prendre une image, on blinde les portes d'entrées et on estime qu'on est en sécurité à l'intérieur. Le problème, c'est que les invités – les applications ou outils tiers - laissent la porte ouverte.

Contact Presse

Galivel & Associés - Carol Galivel / Laurent Bartoleschi - 01 41 05 02 02

21-23, rue Klock – 92110 Clichy - Fax : 01 41 05 02 03 - galivel@galivel.com - http://www.galivel.com

Un guide technique de bonnes pratiques pour tous les constructeurs et leurs fournisseurs

C'est la raison pour laquelle, depuis octobre 2015, Bureau Veritas, en partenariat avec Devoteam, a travaillé sur un guide technique de bonnes pratiques pour évaluer la sécurité informatique des systèmes automobiles. Disponible à la rentrée 2016, il sera le premier à être compatible avec tous les modèles de constructeurs et avec tous leurs sous-traitants de rang 1 à rang n.

Il présentera un ensemble d'exigences, réparties en plusieurs niveaux de sécurité, et modélisées pour s'adapter à tous les constructeurs et équipementiers. Le premier niveau, par exemple, consistera à être capable de résister aux quinze vulnérabilités les plus courantes.

Une prise de conscience salutaire

Difficile de se passer désormais d'une voiture connectée, comme nous pourrions difficilement vivre sans smartphone. Mais il faut être conscient de ce que cela suppose. Comme l'explique Franck Sadmi, responsable de la cellule Logiciel et Cyber Sécurité chez Bureau Veritas au Centre Technique Europe, *« le problème, c'est que plus on demande au véhicule de traiter des informations venant de l'extérieur - pour réaliser des fonctions de sécurité ou de confort - plus les risques de piratage augmentent »*, Or dans l'automobile, les risques sont très élevés. Un récent rapport du sénateur américain Ed Markey, ne fait pas dans le détail et estime que 100% des voitures connectées aujourd'hui en circulation peuvent être piratées. Le FBI lui-même vient d'émettre un bulletin officiel pour appeler les constructeurs à réagir. En France, ce devrait être bientôt chose faite.

En lançant un magazine, Bureau Veritas propose un condensé de l'actualité économique qui a retenu l'attention des experts *Bureau Veritas*. Les méthodes qui permettent aux entreprises, petites ou grandes, de mieux maîtriser leur performance grâce à une bonne gestion des risques : une vision nouvelle des métiers de l'inspection, du contrôle et de la certification.

Si vous souhaitez recevoir des informations régulièrement sur le Mag Bureau Veritas, nous vous invitons à vous abonner à la newsletter (http://lemag.bureauveritas.fr/).

A propos du Bureau Veritas
Bureau Veritas est un leader mondial dans l'évaluation de la conformité et la certification. Partenaire de confiance pour ses clients, il offre des services et développe des solutions innovantes pour réduire les risques, améliorer les performances et promouvoir le développement durable.
Une gamme complète de services : de l'inspection et de l'audit au test, à l'analyse et à la certification, notamment dans les domaines de la construction, de la gestion de patrimoine, de l'industrie, etc.

Retrouver en ligne
- Le communiqué de presse complet
- Les images HD
- Toutes les informations sur http://lemag.bureauveritas.fr/

Contact Presse

Galivel & Associés - Carol Galivel / Laurent Bartoleschi - 01 41 05 02 02
21-23, rue Klock – 92110 Clichy - Fax : 01 41 05 02 03 - galivel@galivel.com - http://www.galivel.com