Voitures connectées : qui est responsable de la sécurité ?

Le parc de voitures connectées ne cesse d'augmenter. Beaucoup s'en félicitent, mais en cas de piratage d'un véhicule, qui est responsable ? Le conducteur ? Le constructeur ? L'équipementier ?

Face à des véhicules toujours plus intelligents, la cybersécurité devient une priorité à la fois pour les constructeurs, les équipementiers et les conducteurs. Le foisonnement de technologies embarquées laisse entrevoir de belles promesses en termes de sécurité routière, de réduction des émissions de CO2 et d'expérience de conduite. Mais il entrouvre aussi de multiples failles dans lesquelles les cybercriminels peuvent s'engouffrer pour accéder aux systèmes des véhicules. Les données personnelles et même la vie des conducteurs et passagers sont alors en danger. Aujourd'hui, plus besoin d'accéder physiquement à un véhicule pour en prendre le contrôle. D'où l'importance pour l'industrie automobile de se projeter au-delà de la seule protection physique de ses véhicules.

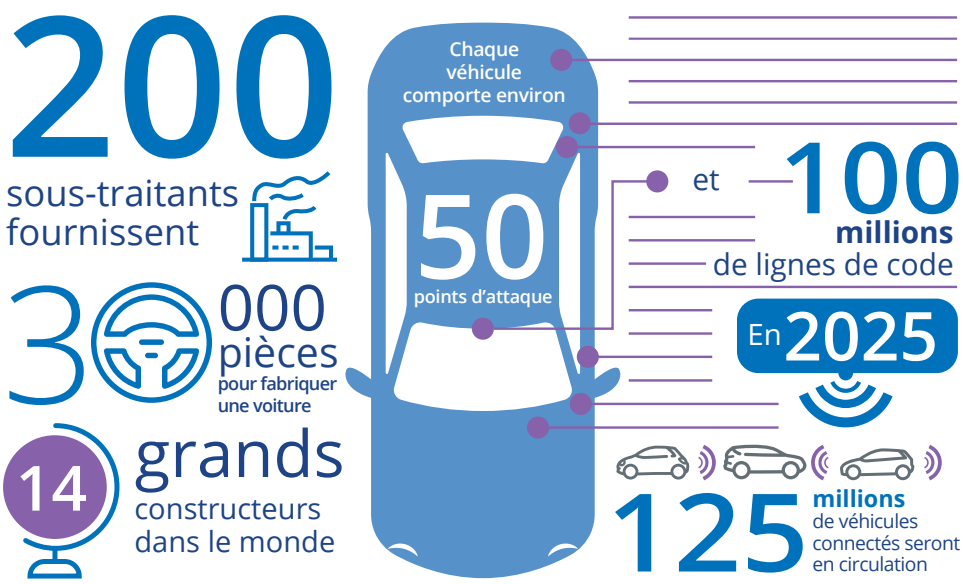
Assurance connectée

À l'heure du tout-connecté, les constructeurs vont devoir affûter leurs arguments pour convaincre les automobilistes de la sécurité des véhicules autonomes et connectés (VAC). Les compagnies d'assurance exigeront elles aussi des garanties dans leurs polices.

Pour les assureurs, la sécurité routière constitue le grand avantage des véhicules sans conducteur et tous se préparent au jour où la majorité des véhicules en circulation seront autonomes. Ceci dit, le chemin est encore long. Les véhicules avec et sans conducteur devront continuer à se partager les routes pendant encore un bon moment. Et dans ce contexte de cohabitation, certaines lois, comme l'Automated and Electric Vehicles Act 2018 au Royaume-Uni, imposent que tous les véhicules (avec ou sans conducteur) sur la voie publique soient assurés à 100 %. Le législateur cherche ainsi à garantir qu'en cas d'accident, les victimes soit dédommagées par l'assureur, et non par le constructeur au terme d'une action en justice. Cette loi stipule toutefois que l'assureur concerné est en droit de se retourner contre le constructeur au cas où un défaut du véhicule est à l'origine de l'accident. Vu ainsi, les choses semblent claires. Mais il reste encore un certain nombre de questions majeures en termes

52 % des entreprises dans le monde pensent que les réseaux de transport pourraient être compromis par des cybercriminels.
Risk:Value

Graphique 1 La supply chain des véhicules connectés est extrêmement complexe et les assureurs veulent savoir qui est responsable de la sécurité : le fournisseur, le constructeur ou le conducteur ?



de responsabilité. Les constructeurs voudront notamment s'assurer qu'en cas de litige, le propriétaire du véhicule soit dans l'obligation de prouver qu'il a bien mis à jour les logiciels embarqués.

Toutefois, la plus grande problématique pour les assureurs est celle du cybercrime. Les piratages de véhicules connectés ont fait grand bruit ces dernières années, avec pour conséquence des rappels massifs de véhicules et une image sérieusement entachée pour les constructeurs. Désormais, les compagnies d'assurance doivent maîtriser une nouvelle catégorie de risques. Par exemple, les ransomwares peuvent immobiliser un véhicule jusqu'au paiement d'une rançon. Certains hackers pourront même tenter de prendre le contrôle d'un véhicule pour porter directement atteinte à sa sécurité, celle de son conducteur, de ses passagers et des autres usagers de la route.

Qui saura apporter aux assureurs toutes les garanties de sécurité d'un véhicule ? Comment souscrire des polices en l'absence d'un corpus de données historiques suffisamment riche ? Mais surtout, qui est l'ultime responsable de la sécurité d'un véhicule : le constructeur, les équipementiers ou le conducteur lui-même ?

« Le marché de la cyber-assurance automobile est en pleine croissance, mais la supply chain soulève encore de nombreuses questions de sécurité. »

Kai Grunwitz, NTT Security

Véhicule ou ordinateur ?

Les véhicules connectés et autonomes s'appuient sur plus de 100 millions de lignes de codes, soit plus qu'un avion de ligne, un avion de chasse et Facebook réunis. S'ajoute à cela plus de 30 000 composants, entre 30 et 100 unités de contrôle électronique (ECU) et environ 25 Go de données créées toutes les heures. Bref, les VAC sont des ordinateurs ultra-sophistiqués qui nécessitent d'être sécurisés et régulièrement mis à jour.

Rien d'étonnant, donc, à ce qu'ils deviennent de plus en plus la cible d'attaques. Et en cas de compromission, l'assureur devra bien trouver un responsable.

Sécurité par défaut

Pour déterminer si oui ou non un véhicule est sécurisé, les compagnies d'assurance se pencheront en premier lieu sur le constructeur, en l'occurrence son profil de risque, ses usines de fabrication et les caractéristiques techniques du véhicule lui-même. À l'heure de l'Industrie 4.0, l'hyper-connectivité des environnements de production augmente le risque de cyberattaque, mettant en péril l'intégrité des produits finaux. La Société 5.0 pointe elle aussi à l'horizon. Et dans cette société 100 % connectée, c'est la sécurité intrinsèque des VAC qui constituera vraisemblablement le terrain de bataille entre les constructeurs et les assureurs en cas de litige. De leur côté, les attaquants saisiront n'importe quelle occasion d'accéder au réseau d'un véhicule, à commencer par les ECU qui en contrôlent chaque aspect, de la radio jusqu'aux systèmes de freinage et de direction assistée.

L'industrie l'automobile se trouve face à une équation particulièrement difficile. D'une part, les véhicules connectés sont extrêmement complexes et impossibles à fabriquer sans quelques vulnérabilités. D'autre part, la supply chain est fragmentée en un réseau de centaines de sous-traitants produisant chacun des pièces et ECU selon ses propres standards et spécifications. Et même lorsque les composants individuels sont au-dessus de tout soupçon, tout défaut d'intégration peut faire apparaître des failles.

Les assureurs pourront par ailleurs demander à examiner les plans du véhicule produits par le bureau d'études, de manière à vérifier la présence d'un dispositif de sécurité sur chaque composant matériel et logiciel. Bricoler un système de sécurité après-coup ne fait qu'augmenter la complexité et la vulnérabilité d'un véhicule. C'est donc au constructeur de prendre les devants et de concevoir ses véhicules dans une optique de cybersécurité.

Enfin, les compagnies d'assurance pourront imposer une surveillance V-SOC (Vehicle Security Operation Centers) de tous les véhicules. Chaque donnée sera ainsi transmise en temps réel au V-SOC pour analyse. L'idée est de détecter rapidement une attaque en cours et d'engager instantanément des actions correctrices. Là encore, ce sera au constructeur de mettre en place une telle infrastructure.

Un ensemble de composants

Pour ne pas endosser seul la responsabilité de la sécurité, le constructeur se tournera quant à lui vers son écosystème de sous-traitants. En règle générale, les constructeurs ont un cahier des charges très strict sur les aspects techniques, mais restent assez vagues sur le volet cybersécurité. Et rares sont les cas où ils exigent l'utilisation de standards ou frameworks spécifiques. Par ailleurs, les sous-traitants sont souvent réticents à l'idée de créer leurs propres standards, de peur que le constructeur n'en impose un autre.

En 2015, des hackers sont parvenus à pirater un Jeep Cherokee depuis un ordinateur portable situé à des kilomètres. Ils voulaient ainsi prouver que l'on peut aisément prendre le contrôle d'un véhicule, de son système de freinage, de direction et de transmission. Résultat : Chrysler a dû rappeler 1,4 million de véhicules.

En 2016, des API non sécurisées ont permis à des hackers de prendre le contrôle d'un modèle Nissan Leaf.

Il faudra pourtant sortir de cette impasse pour intégrer la sécurité au processus de conception des véhicules. En tant qu'assembleur final, le constructeur doit veiller à ce que tous les composants soient sécurisés au moment de leur conception et de leur interconnexion.

N'oublions pas l'utilisateur final

Les compagnies d'assurance calculent depuis longtemps les primes sur le bonus/malus des conducteurs. Aujourd'hui, ils vont un cran plus loin avec le Pay How You Drive (PHYD), un principe qui consiste à offrir des primes plus avantageuses aux bons conducteurs. Un boîtier électronique transmet ainsi des données télématiques sur le comportement du conducteur au volant, ce qui permet à l'assureur d'établir son profil de risque.

Le risque de cybersécurité reste toutefois difficile à évaluer.

Si l'industrie automobile prend peu à peu conscience des enjeux de la cybersécurité, les conducteurs, eux, sont relativement peu sensibilisés aux risques. Plutôt inquiétant pour ceux qui sont censés les assurer. Le degré de vigilance augmente lorsqu'un cas de piratage est relayé dans les médias, mais les vieilles habitudes reprennent vite le dessus. Un changement s'impose. Les assureurs demanderont aux conducteurs de s'engager à mettre à jour les systèmes logiciels embarqués et à ne pas installer de logiciel sur leur smartphone susceptible de compromettre la sécurité des véhicules une fois l'appareil connecté.

Un point sur les menaces

La conception, la construction et la maintenance de véhicules sûrs passent par une bonne compréhension du paysage des menaces, une circulation fluide de l'information tout au long de la supply chain et un accès à la Threat Intelligence de sources externes. C'est une pratique courante dans des secteurs comme les services financiers. Elle permet aux parties prenantes de profiter de la puissance du collectif face à des criminels bien organisés.

Toutefois, avant que les assureurs ne puissent calculer la moindre prime, les acteurs de la supply chain automobile devront désigner un orchestrateur de la sécurité tout au long de la fabrication. D'ici là, il leur faudra parfaitement maîtriser les questions de sécurité et de Threat Intelligence, et connaître les mesures de prévention et de réponse possibles. Conseillers gouvernementaux, assureurs, constructeurs, sous-traitants, professionnels de la sécurité… l'heure est venue de réunir toutes les parties prenantes pour plancher sur ces problématiques et créer un modèle de bonnes pratiques de sécurité pour les véhicules connectés. En attendant, la responsabilité incombe à tous – et à personne – en même temps.

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.