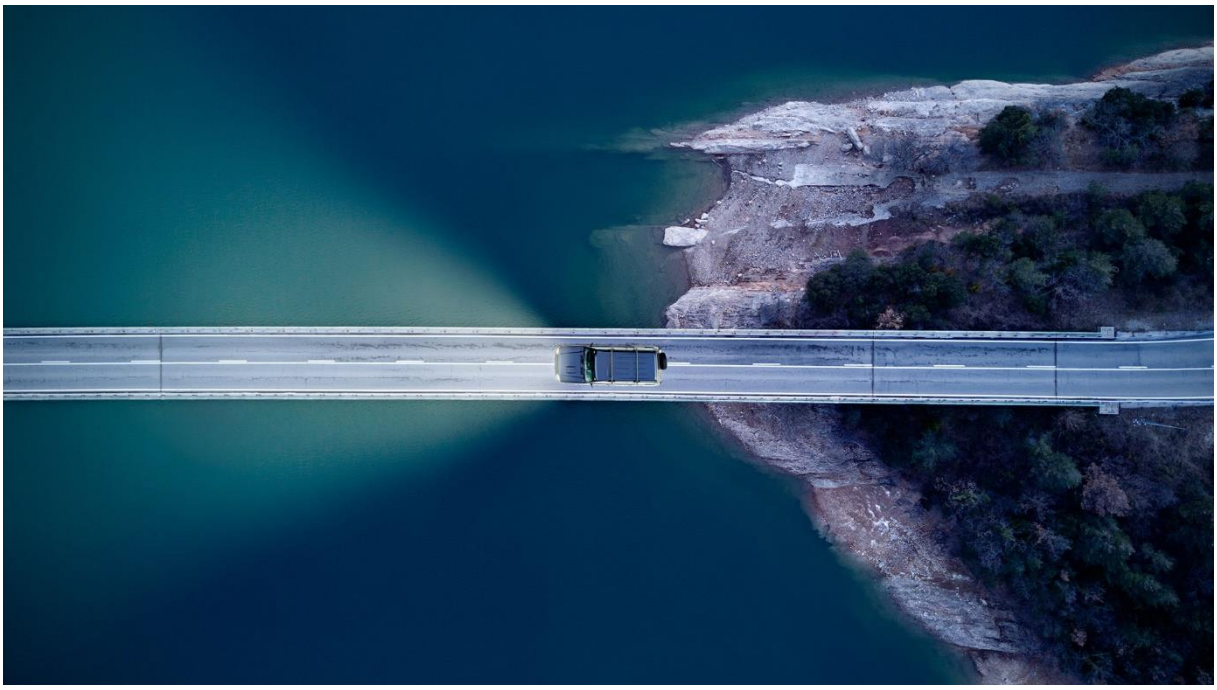

Février 2021

Cyberattaques : quelles armes pour les constructeurs automobiles ?

En 2020, les cyberattaques ont quadruplé, avertit en ce début d'année l'Elysée. Loin de se cantonner à l'Hexagone, cette augmentation est un phénomène mondial. D'après une étude de McAfee et du CSIS (Center for Strategic and International Studies), la cybercriminalité coûterait environ 1 000 milliards de dollars à l'économie mondiale, un chiffre près de 50 % supérieur à celui de 2018. Pour les constructeurs automobiles, l'enjeu est double : au risque industriel se conjugue celui qui pèse sur les usagers. Le panorama des menaces est donc large, mais elles peuvent néanmoins être atténuées grâce à certaines pratiques, décryptées par Kevin Gallerin, Managing Director APAC de YesWeHack, une entreprise de cyber sécurité spécialisée dans la détection des failles informatiques des entreprises (*bug bounty*).

A quels cyber risques sont exposés les constructeurs automobiles, en tant qu'industriels ?

Kevin Gallerin : Il n'est pas évident de prendre la mesure de l'exposition de l'industrie automobile aux cyber risques, car elle fait preuve d'une culture du secret importante. Toutefois, les constructeurs automobiles sont soumis aux mêmes risques que les autres institutionnels, comme le ransomware ou le vol de données. Mais il faut également envisager d'autres scenarios, comme par exemple une attaque sur la *supply chain*. Cela consisterait par exemple à installer un code malicieux dans un composant informatique utilisé par le constructeur et qui serait déployé sur les véhicules. Ce type d'attaque pourrait avoir la capacité d'immobiliser une flotte de véhicules, du jour au lendemain. Le recours à un code malicieux est notamment au cœur de l'attaque de grande ampleur de SolarWinds, qui vient d'ébranler les Etats-Unis.

Quels sont, justement, les cyber risques qui pèsent sur les véhicules ?

Radiofréquence, 4G, 5G, on trouve désormais tous types de connexions sur les véhicules. Ils ont rejoint l'univers de l'IoT, l'internet des objets, et sont soumis aux mêmes types de risques de piratage, mais avec des conséquences sans commune mesure. Les vulnérabilités les plus « classiques » concernent les technologies sans-contact gérant les ouvertures/fermetures ainsi que le démarrage des véhicules, qui peuvent être relativement faciles à abuser. Les méthodes évoluent en fonction des types de clés et technologies employées et permettent notamment d'ouvrir des modèles premiums. Il est aussi possible de mettre à jour des failles permettant d'ouvrir un parc de véhicules à distance, comme des chercheurs l'ont fait au travers du système Connected Drive de BMW, installé sur près de 2,2 millions de véhicules.

Un véhicule d'aujourd'hui embarque énormément de sous-systèmes et beaucoup ont leur propre technologie. Une valve de pneu, par exemple, envoie à l'unité centrale du véhicule des informations sur la pression d'air. Ces informations peuvent être interceptées, rejouées, modifiées et ainsi falsifier un comportement. Il est aussi possible d'envisager une attaque portant sur les systèmes de freins. Enfin, les véhicules communiquent avec des serveurs et leur transmettent des données et métadonnées de tout type. Un risque pèse également sur ces environnements qui sont parfois mal sécurisés. Au Royaume-Uni, des hackers ont ainsi réussi à pirater les données de 400 000 conducteurs de BMW, avant d'essayer de les vendre sur le marché noir et d'en rendre une partie publique sur internet.

Pour l'instant, aucune attaque n'a porté sur l'ensemble de la flotte d'un constructeur. Si tous les modèles ne sont pas exposés aux mêmes failles, une opération de très grande ampleur demeure néanmoins tout à fait plausible.

Notons également que les constructeurs sont soumis aux mêmes types de menaces partout dans le monde. La différence ne se fait pas tant en fonction des marchés que du degré de connectivité des gammes. Les failles sont cependant mieux documentées en Europe et aux Etats-Unis qu'en Asie. La Chine, notamment, pratique une forte culture du secret quant aux

cyberattaques qui touchent les constructeurs et leurs véhicules connectés, un marché sur lequel elle est d'ailleurs bien positionnée.

Quels objectifs poursuivent les hackers avec ces types d'attaques ?

Ils sont de plusieurs ordres. La recherche de profit, avec le ransomware ou le vol de données, qui est très lucratif ; la recherche d'un impact financier sur l'entreprise, sur le cours de Bourse par exemple, ou avec le vol de données industrielles - une pratique relativement courante. Le hacker peut aussi agir pour la gloire, dans l'objectif de publier sa découverte.

Cette dernière option doit être transformée en atout, la France, au travers de l'ANSSI (agence nationale de la sécurité des systèmes d'information) et Singapour l'ont très bien compris. Ils encouragent la recherche et la remontée de failles pouvant toucher les entreprises, les collectivités, les systèmes publics, permettant ainsi leur résolution.

Peut-on estimer les préjudices des cyberattaques pour les constructeurs ?

Si l'entreprise se fait pirater sa chaîne de production, il est facile de calculer le manque à gagner. Mais la plupart des scenarios sont plus complexes. Lorsque les données concernant les trajets des utilisateurs d'une marque se retrouvent publiées sur internet, quel est l'impact sur cette marque ? Combien d'acheteurs potentiels lui préfèreront ensuite un concurrent ? Se pose également la question des accidents de la route qui se produiraient suite à une cyberattaque sur des véhicules. On sait que la prise de contrôle à distance d'une voiture est possible, l'expérience a été faite sur une Jeep Cherooke de Chrysler.

Quelles mesures existe-t-il face à un risque en constante évolution ?

La prévention est essentielle et s'organise de diverses manières. Le *bug bounty*, c'est-à-dire la recherche de failles dans les systèmes d'une entreprise par des acteurs extérieurs, est extrêmement efficace, car il est impossible d'avoir toutes les compétences en interne. Dans près de 95 % des cas, cela met à jour une faille critique capable de mettre en péril l'activité. Tesla fait ainsi appel à des spécialistes du bug bounty. Renault a également mis en ligne une politique de divulgation des vulnérabilités qui explique comment lui remonter toute faille identifiée dans ses systèmes. Les constructeurs devraient tous mettre en place un canal de communication dédié et sécurisé avec les chercheurs.

La sécurité informatique doit être intégrée au plus tôt lors de la conception des produits et les constructeurs doivent prendre en compte tout le cycle de vie de leurs applications et équipements. Une fois qu'un million de véhicules ont été vendus, il faut continuer à les sécuriser. L'action doit pouvoir se faire à un niveau global, les constructeurs en prennent conscience. Désormais, certains intègrent dans les véhicules des systèmes de mise à jour, actionnables à l'échelle de toute la gamme. Ce n'était pas le cas jusqu'à il y a peu.

Quel rôle les cyber assurances peuvent-elles jouer ?

Elles jouent un rôle très important, car il est impossible de couvrir tous les risques en amont. Le cyber risque va bien au-delà du piratage, cela peut être une faille ou une panne qui n'a jamais été envisagée.

Les assureurs doivent également agir en faisant de la pédagogie. Ils peuvent encourager de bonnes pratiques, peut-être en jouant sur les premiums. Certaines cyber assurances prennent en charge le paiement des ransomwares, ce qui est dommageable pour tous les acteurs. Cela pousse les hackers à poursuivre cette pratique lucrative et ne favorise pas les comportements vertueux de la part des entreprises, qui se reposent sur leur assurance. Les assureurs font preuve d'une grande maturité en matière de cyber protection pour leur propre entité, ils peuvent indéniablement contribuer à l'évolution des comportements des entreprises, en favorisant la mise en place de mesures de prévention plus efficaces.