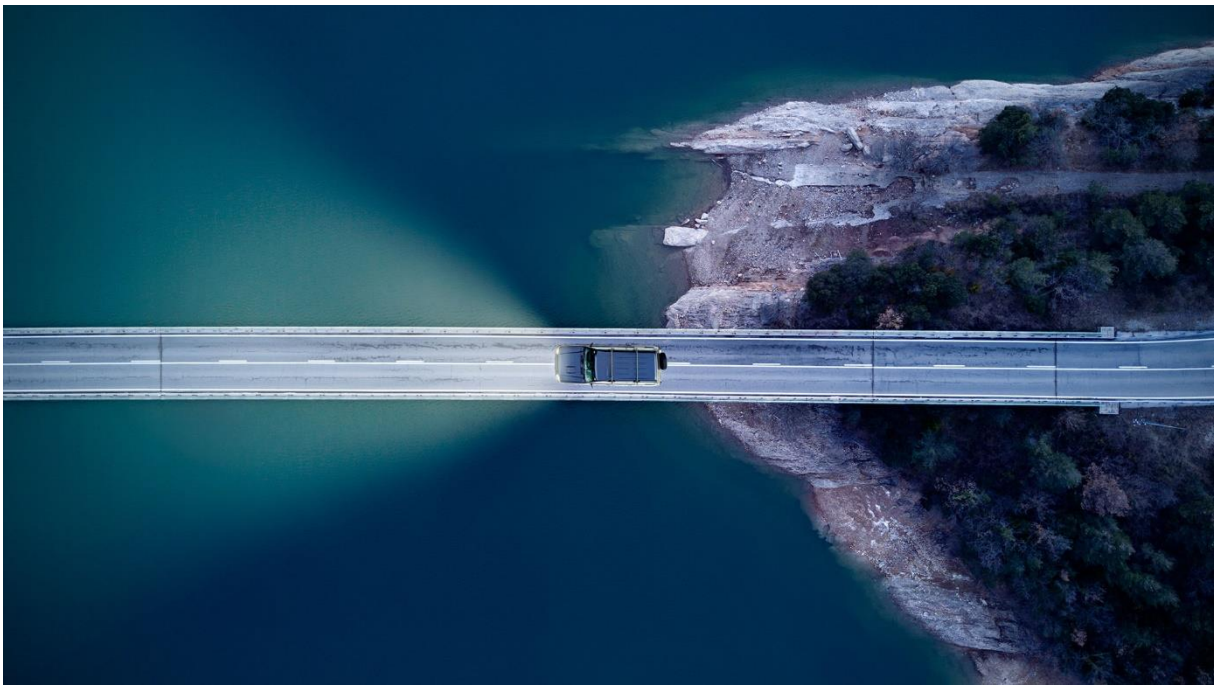

February 2021

Cyber attacks: what ammunitions for car manufacturers?

In 2020, cyber attacks have quadrupled, warns the Elysée Palace at the beginning of this year. Far from being limited to France, this increase is a worldwide phenomenon. According to a study by McAfee and the CSIS (Center for Strategic and International Studies), cybercrime would cost the world economy around 1,000 billion dollars, a figure almost 50% higher than in 2018. For car manufacturers, the stakes are twofold: the industrial risk is combined with the risk to users. The panorama of threats is therefore broad, but they can nevertheless be reduced thanks to certain practices, deciphered by Kevin Gallerin, Managing Director APAC of YesWeHack, a cyber security company specialising in detecting corporate computer faults (bug bounty).

What cyber risks car manufacturers, as industrial players, are exposed to?

Kevin Gallerin: It is not easy to gauge the extent of the automotive industry's exposure to cyber risks, as it has a strong culture of secrecy. However, manufacturers are subject to the same risks as other institutions, such as ransomware or data theft.

But other scenarios must also be considered, such as an attack on the supply chain. For example, this could be like installing a malicious code in a computer component used by the manufacturer and which would be deployed on the vehicles. This type of attack could have the capacity to immobilise a fleet of vehicles overnight. The use of malicious code is at the heart of the large-scale SolarWinds attack that has just shaken the United States.

What exactly are the cyber risks that could threaten vehicles?

Radio frequency, 4G, 5G, all types of connections can now be found on vehicles. They have joined the world of IoT, the Internet of Things, and are subject to the same types of hacking risks, but with far-reaching consequences. The most "classic" vulnerabilities concern contactless technologies managing the opening and closing as well as the starting of vehicles, which can be relatively easy to abuse. Methods are evolving according to the types of keys and technologies used and make it possible, in particular, to open premium models. It is also possible to uncover security flaws to open a fleet of vehicles remotely, as researchers have done through BMW's Connected Drive system, which is installed in nearly 2.2 million vehicles.

Today's vehicle has a lot of subsystems on board and many have their own technology. A tyre valve, for example, sends air pressure information to the vehicle's central unit. This information can be intercepted, replayed, modified and thus falsify behaviour. It is also possible to envisage an attack on brake systems. Finally, vehicles communicate with servers and transmit data and metadata of all kinds. There is also a risk with these environments, which are sometimes poorly secured. In the United Kingdom, for example, hackers have managed to hack the data of 400,000 BMW drivers before trying to sell them on the black market and make some of it public on the Internet.

For the moment, no attack has been made on the entire fleet of a manufacturer. If all the models are not exposed to the same flaws, a very large scale operation nevertheless remains quite plausible.

It should also be noted that manufacturers are subject to the same types of threats everywhere in the world. The difference is not so much based on the markets as on the degree of connectivity of the brands' ranges. The flaws are, however, better documented in Europe and the United States than in Asia. China, in particular, has a strong culture of secrecy regarding cyber attacks on manufacturers and their connected vehicles, a market in which it is well positioned.

What objectives do hackers pursue with these types of attacks?

They are of several kinds. The search for profit, with ransomware or data theft, which is very lucrative; the search for a financial impact on the company, on the stock market price for example, or with the theft of industrial data - a relatively common practice. The hacker can also act for glory, with the aim of publishing his discovery.

This last option must be turned into an asset, as France, through the ANSSI (national agency for the security of information systems) and Singapore have understood very well. They encourage the search for and the reporting of vulnerabilities that could affect companies, local authorities and public systems, thus enabling their resolution.

Is it possible to estimate the damage caused by cyber attacks to manufacturers?

If a company's production line is hacked, it is easy to calculate the loss of earnings. But most scenarios are more complex. When data on the journeys of a brand's users is published on the internet, what is the impact on that brand? How many potential buyers will then prefer a competitor to it? There is also the question of the road accidents that would occur following a cyber attack on vehicles. We know that remote control of a car is possible, the experiment was done on a Chrysler Jeep Cherooke.

What measures are there in the face of an ever-changing risk?

Prevention is essential and is organised in various ways. Bug bounty, i.e. the search for flaws in a company's systems by external players, is extremely effective, as it is impossible to have all the skills in-house. In 95% of cases, this uncovers a critical flaw that could jeopardise the business. Tesla therefore calls in specialists in bug bounty. Renault has also put a vulnerability disclosure policy online that explains how to report any identified flaws in its systems. Manufacturers should all set up a dedicated and secure communication channel with researchers.

IT security must be integrated as early as possible in the design of products and manufacturers must take into account the entire life cycle of their applications and equipment. Once a million vehicles have been sold, they must continue to be secured. It must be possible to take action at a global level, and manufacturers are aware of this. Some manufacturers now incorporate updating systems in vehicles that can be activated across the entire range. This was not the case until recently.

What role can cyber insurance play?

They play a very important role, because it is impossible to cover all risks upstream. Cyber risk goes far beyond hacking, it can be a loophole or a failure that was never envisaged.

Insurers must also act by educating. They can encourage good practices, perhaps by playing on premiums. Some cyber insurers take over the payment of ransomwares, which is damaging for all players. This pushes hackers to continue this lucrative practice and does not encourage virtuous behaviour on the part of companies, which rely on their insurance. Insurers are very mature in terms of cyber protection for their own entities, and can undeniably contribute to the evolution of corporate behaviour by encouraging the implementation of more effective prevention measures.