Tractor – IN, Scooter – OUT: The legislation mandating automakers to protect against hackers has hit the road

Starting in July, protection against cyber attacks will be mandated for all new vehicles in Europe. The head of the UN group that led the legislation clarifies why it is important to protect even a tractor – but not a scooter. Israeli cybersecurity companies are inundated with inquiries from manufacturers.

Udi Etzion – *Calcalist*
January 14, 2022

In recent months, some of the cyber companies in the country have received a wave of inquiries from car manufacturers, with requests for urgent projects, mainly from China. The reason: UN ECE WP.29[1] – in other words, the new UN Vehicle Cybersecurity standard (R 155), which has already been adopted by the EU, Japan and South Korea, and will also be implemented in the United States. As cars sold in Israel comply with European and American standards, this standard will also apply to the Israeli market.

The device will take effect gradually. From July 2022, automakers will be required to provide full protection against cyber attacks for each new model they launch – not only during development and production, but also to update its capabilities in the face of new threats throughout its life. Older models, which are already on the production line, will have to meet the same requirements starting in 2024.

François Guichard, head of the Autonomous and Connected Vehicle group at the UN. To protect vehicles (Photo: @FG)

François Guichard, head of the Autonomous and Connected Vehicle group at the UN headquarters in Geneva, says that "thanks to the new regulation, the cars we will purchase in the future will be much more protected from cyber attacks."

How is it that we have not encountered to date widespread hostile attacks against cars?
"A vehicle connected to the internet is a fairly new concept. That's why most of the attacks we've seen to date have been carried out by researchers from academia or from the cyber industry. But that certainly doesn't mean we should be complacent."

[1] https://unece.org/transport/vehicle-regulations

What will the new standard that your group approved mean, in effect?
"Regulation applies to the full life cycle of the vehicle, and to the entire supply chain. We have invested much thought so that manufacturers will not be tempted to neglect old models, which have only a few years left on the production lines. In a competitive market they will always have other things to do with their money. So now the regulation is uniform for everyone; No one will lose a competitive advantage by devoting resources to upgrading the cybersecurity of older models."

Will you require cybersecurity only in cars?
"Cars, buses and trucks, as well as two- or three-wheeled vehicles equipped with autonomous driving features. We are now discussing whether to include tractors, because cyber attacks could endanger food production. Micro-mobility vehicles, such as scooters, are not part of the requirement. The cyber risks for them are lower, because there is rarely connectivity between the motor/drive system and the part of the vehicle linked to the internet. Europe, South Korea and Japan have already announced that they will adopt the regulation. Compliance works differently in the US auto market, but the Washington administration has already announced it will adopt the standard's principles."

Are cars sold today protected from cyber attacks?
"Most already have elements of protection, but no one will commit to 100% protection in any area. In cars that have been manufactured in recent years, too, efforts have already been made in that direction."

For how many years will a manufacturer be responsible for the vehicle's cybersecurity? Will it require a fee?
"According to the approved standard, most elements of cybersecurity will be for the life of the car. The matter of payment will be decided according to market decisions. In the end, the goal of the standard is to continue to improve cars in all areas, including safety and air pollution. Consider the cars that were involved in "Dieselgate" – even they were much less pollutant than diesel vehicles sold in the past. In terms of cyber, as well, the cars we buy in the future will be much more protected than those sold now."

The automotive cybersecurity market will reach $10 billion by 2030
The new regulation applies to a market of 20 million new cars a year, according to estimates by the management consulting company McKinsey. They estimate that the automotive cybersecurity market will double within a decade, by 2030, to $10 billion.

David Barzilai, one of the founders of Karamba Security.
"**Urgent inquiries from the auto industry**"

How much of this amount will go to the local cybersecurity industry? There are several companies in the country that specialize in cybersecurity for vehicles, such as the older Arilou and Argus, and the newer Karamba Security[2] and Upstream. "Israeli companies are not alone in the field, but they continue to set the tone in the industry. Although there are no comprehensive statistics, on the ground there is a sense that it is mainly the Israeli firms," says David ("Dudi") Barzilai, one of Karamba's founders and VP of Sales and Marketing. Karamba employs over 30 people, and Barzilai estimates that in Israel the companies in this sector already employ hundreds of workers in total, and continue to recruit.

Barzilai: "The issue of cybersecurity has always been somewhat veiled in a cloud, with not all automotive manufacturers being equally proactive in light of conflicting messages from various government bodies. In the United States, for example, treatment of the issue halted during the Trump era. Only recently have we seen a major supplier hire an executive to lead cybersecurity, just six months ago. And now many urgent inquiries are being received from various players in the industry, with an emphasis on Asia, who have finally realized that they must get organized quickly in order to be prepared. They announce an RFP, and give only a month in which to submit bids."

What will be the impact on the local industry?
"In our opinion, the regulation will drive the demand for cybersecurity in the automotive industry. The industry is looking for a complete solution package: not just a point solution, but accompaniment in planning and throughout the lifecycle of the model, identifying threats and preparing software updates to handle them. Because Israel has an excellent reputation in the cybersecurity field, Karamba, as an Israeli company, is experiencing a significant increase in the number of referrals who, due to regulatory requirements, seek a comprehensive cyber solution and not one that is narrowly focused. But it is not only Karamba benefiting from the increase in demand. For example, in order not to delay our customers, and to meet the aggressive schedules set by the standard, we have brought in a number of partners from the Israeli and global ecosystem."

Today, when all vehicle systems are connected, how will the standard affect the aftermarket installation of features/accessories?

"It is likely that the aftermarket scope will be limited in the coming years. Automakers will seek to block add-ons that could jeopardize the cybersecurity they have planned. There are also vulnerabilities in the area of electric vehicle (EV) charging stations, and there is a standard on the way for them, as well."

Originally published in Hebrew: *https://www.calcalist.co.il/local_news/car/article/sy3hftrnk*

[2] https://www.karambasecurity.com