Translated article "IT-Security ist Vertrauenssache!," E&E-Kompendium 2018

IT security is all about trust!

Data security is shaping up to be significantly more difficult than expected for both private individuals as well as for companies. Many customers are uncertain which manufacturers and corporations they should allow access to their sensitive data.

Friedhelm Pickhard is the Chairman of the Board of Management at ETAS GmbH, whose subsidiary ESCRYPT develops security solutions for embedded systems

The situation is serious. According to the Federal Office for Information Security, half of the companies in Germany have been the target of cyber-attacks in the last two years. Using ransomware such as "WannaCry" and "Petya", attackers were recently able to bring the production and business processes of notable companies to a standstill for days on end. Cybercrime is not the exception in our connected world, but rather the rule for many businesses and institutions. Large companies are now being subjected to thousands of hacks every day. Even if only one of these is successful, the damage to the company could still amount to millions of euros – not including immaterial losses. These attacks are just like break-ins in that they are followed by a period of profound uncertainty. Which processes, data, and computers are still safe to use?

Everyone understands how anti-theft devices on doors and windows work. But where IT security is concerned, this is usually a closed book for amateurs who cannot understand the hackers' methods or the countermeasures, and this only further undermines their confidence. But ultimately, IT users have to rely on the expertise of security specialists – which means having to put a great deal of trust in them. Modern vehicles are now part of the connected world. However, the integration into the Internet of Things, updates and over-the-air upgrades, and the planned exchange of data between vehicles and infrastructure make in-vehicle IT systems prone to attack. If cyber criminals were able to manipulate functions in individual vehicles – or worse – infiltrate an entire interconnected fleet of vehicles, this would have far-reaching consequences, putting people's lives at risk and, in the long term, jeopardizing the economic stability of the vehicle manufacturers affected. Customers would naturally be unsettled: who would still trust the car manufacturer after such an attack?

It is not only the success of business models for connected services that depends on the security of in-vehicle IT systems. The reputation and integrity of the entire automotive industry depends on it. Manufacturers have to be able to assure their customers that data input into their vehicles is secure in every way ensuring confidentiality and privacy, integrity and authenticity of software and data. Original Equipment manufacturers (OEMs) and suppliers are aware of these challenges and are turning to outside companies with expertise in IT security to stay one step ahead of the hackers. A great deal of trust is placed in these external security companies with the in-depth IT knowledge they have at their disposal. Inevitably, they also need to gain a deep insight into their customers' structures and processes so that they can secure their entire IT infrastructure. This requires holistic approaches: IT security begins with the planning phase before predevelopment of a model, protects all production processes as well as vehicle operation with the end user, and stops when the vehicle is scrapped after all cryptographic keys have been revoked.

External security companies thus have access to restricted areas and highly sensitive data. Therefore vehicle manufacturers and suppliers need to ask themselves who they should allow to have such an extensive knowledge of their structures and processes and which external partners they can – and want to – trust. Some IT security companies have admitted to their roots in criminal circles and even used them as a selling point, whereas other companies are recruiting staff from these circles, some with highly interesting expertise. As understandable as this may seem considering the lack of IT specialists, the motives, values, and principles of these players remain unclear. Who can ensure that they do not have their own agenda, that they have cut all ties with their notorious past, and that sensitive data is in safe hands? IT security is all about trust. Partnerships should be built on mutual trust and shared values. OEMs and suppliers are advised to carefully screen their automotive security partners, because not only in-vehicle IT networks are open to attack, but also the vehicle manufacturers themselves.