Media information 27.11.2019

EU Cybersecurity Act: Why the planned regulations will have little success

Attacks by cybercriminals threaten not only the economy, but each and every one of us. The planned EU regulation to standardize cybersecurity aims to improve the security of online services and networked devices. "The problem of insecure products is growing faster than bureaucracy can keep up," comments Mirko Ross, warning of a toothless regulation.

At the EU Cybersecurity Act conference in Brussels, experts discussed the current state of implementation of the law. A key topic was the security of products on the Internet of Things (IoT). Conference topics Mirko Ross, well-known IoT & cybersecurity expert, entrepre- neur and influencer, explains in an interview why we are running out of time and why the experts need to make improvements.

Question: Mr. Ross, can we sit back and trust that legislators will protect us from cyberattacks in the future?

Mirko Ross: I wish! The fact is that we urgently need rules, but the EU's bureaucratic process is moving far too slowly. Until the relevant regulations come into force, cybercriminals have unhindered access to IoT devices - the consequences cannot be estimated, but they can be devastating. Three years ago, for example, the Mirai botnet hijacked hundreds of thousands of cheap, insecure web cameras, creating a cyberweapon for hire. Cyberweapons can be used to attack states, companies, or public infrastructures - I leave it to the imagination of the individual to imagine what that could mean for each of us.

Question: You warn that the planned regulation is toothless. What exactly do you mean by that?

Mirko Ross: If you want to improve the security of IoT devices, you have to hold the manufacturers, i.e. the industry, accountable. There must be guidelines to prevent, for example, unsecured Wi-Fi modules being installed in IoT devices that are not supplied with updates. This invites attackers with an open door, so to speak. This will not really be possible with the regulations envisaged so far.

Question: Can you explain that in more detail?

Mirko Ross: In order to increase the cyber security of products on the Internet of Things, a voluntary seal of approval for products is planned. This is based on the industry's own responsibility and on conscious consumers. The incredible number of insecure devices currently in use speaks for itself: consumers and industry are already overburdened with these roles. It is conceivable, however, that the lack of binding regulations will be supplemented by regulations in European consumer protection, so that we would then have a complicated construct that ultimately prescribes a higher level of safety for consumer products.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

Question: Would such a more or less binding security seal really be the optimal solution?

Mirko Ross: Rather not: one of my criticisms of certification is the scalability of this approach: to ensure thorough certification, you need people to carry it out. But the potential number of available people in companies is limited, and so is the number of certifications that can be performed. The Internet of Things, on the other hand, is growing exponentially - the capacities for certification are thus quickly exceeded. These two worlds therefore do not fit together.

Question: What do you think would be a better approach to optimize safety in the long term?

Mirko Ross: There must be more mandatory rules for securing products, similar to data protection: the DGSVO has made very clear requirements that companies must comply with when handling personal data. In the case of products on the Internet of Things, the manufacturer must be obligated to ensure sufficient security during the life of the product. Products must not be marketed with known security vulnerabilities; security vulnerabilities that arise later must be closed by the manufacturer for an appropriate period of time via updates and patches. Finally, liability is a powerful instrument: only if manufacturers can be held liable for insecure products do they have an interest in making their products more secure. Before that, unfortunately, they do not.

Mr. Ross, thank you for the interview!

Mirko Ross is an iX author and founder and CEO of the start-up asvin and digital worx GmbH. He is involved in IoT security as a member of the expert group for security in the Internet of Things of the European Network and Information Security Agency ENISA. He is also a member of the Internet Of Things Council, a global IoT think tank, and project coordinator in the eHealth research project MITASSIST.

Image

Contact
seidel. agentur für kommunikation
Brunnengasse 3
73650 Winterbach (Stuttgart)
T: +49 7181 / 26 29 376
E: medien@seidel-kommunikation.de