Media Information

asvin - more security for the Internet of Things

Extortion, data theft, sabotage - when cybercriminals hijack devices on the Internet of Things, the consequences can be devastating. The risk for companies is high, because industrial IoT devices are preferred targets for cyber attacks. Security vulnerabilities due to a lack of updates play a central role in this.
To make the Internet of Things more secure, the Stuttgart-based start-up asvin.io has developed a solution that secures and monitors the software lifecycle from development and distribution to operation on devices.

Every year, attacks by hackers cause total damage of over 100 billion euros to the German economy. In order to take over systems, attackers exploit security vulnerabilities of Internet-connected machines or systems.
In addition, Industry 4.0 solutions are built using increasingly complex software supply chains: Even one insecure component can then plunge an entire production plant into uncertainty. Long life cycles of industrial plants and inadequate maintenance of the software increase the risks for the industry.

Security often fails due to lack of know-how

Among the most dangerous vulnerabilities in IoT devices is a lack of updates. For medium-sized manufacturers, it is often not feasible in practice to provide several hundred thousand sold IoT products with updated versions of the software. Unlike large corporations, small companies lack the manpower and know-how to design and implement a secure OTA infrastructure for updates without great effort and expense.

Updates and patches as an important building block

Stuttgart-based start-up asvin is tackling this issue and has developed a secure, robust solution to close security gaps in IoT devices via updates and keep them functional in the long term. The software platform and decentralized infrastructure provided by asvin distribute updates and patches for IoT end devices, the process is documented and thus secures the delivery of updates against manipulation.

As "Software as a Service", this solution is easy to use, reliable and cost-effective. With asvin's offering, individual update rollout plans are possible, as is the automatic rollout of rapid security updates in the event of a crisis.
At the same time, it ensures that manipulation attempts by attackers can be quickly detected and repelled. In addition, the asvin Chain-of-Trust creates the basis of trust for software supply chains from the certification of a software to the update of a device and the operation of the software.

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

The elegant solution from asvin

Following the motto make or buy, manufacturers of IoT devices can simply buy "software as a service" with asvin. The effort for providing updates and monitoring by asvin can be reliably calculated in advance. Thus, the service and support offered by asvin is more efficient than an in-house developed and operated solution. The advantage for industrial users of IoT devices is obvious: devices and systems are better protected against cyberattacks, their function can be maintained or quickly restored.

Reprint free of charge, please provide proof (print, scan) or link.

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