www.jusletter-it.eu

Jurius

For a Safe Handling of the Internet of Things

The 24th semi-annual report of the Reporting and Analysis Centre for Information Assurance (MELANI), published on 20 April 2017, addresses the most important cyber incidents of the second half of 2016 both in Switzerland and abroad. The focal point of the report is the internet of things, which is becoming increasingly significant.

Category: News
Region: Switzerland
Field of law: Cybercrime

Citation: Jurius, For a Safe Handling of the Internet of Things, in: Jusletter IT 18 May 2017

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

[Rz 1] According to estimates, more than 6 billion devices attributable to the internet of things were already connected to the internet in 2016. That figure is set to be around 20 billion by 2020. Everything is being connected to the internet, from so-called «wearables», i.e. applications that are sewn into clothes or worn on the user's body, such as smartwatches and fitness trackers, to self-driving cars and control systems in large building complexes. However, the manufacturers and users often fail to pay enough attention to the security aspects. The semi-annual report demonstrates the problem and gives recommendations for a safe handling of the internet of things.

[Rz 2] Espionage campaigns with a link to Switzerland even though Switzerland was not the actual target of the operations became public in the second half of 2016. During the reporting period, the World Anti-Doping Agency and the Court of Arbitration for Sport were in the centre of attention. Switzerland was thus in focus because the latter institution has its headquarters in Lausanne. In the case of the World Anti-Doping Agency the obvious target was the anti-doping data of certain athletes worldwide. In the case of another attack that took place quite some time ago but became known only recently with the publication by the group «Shadow Brokers», three servers at the University of Geneva were affected. The semi-annual report examines these attacks and gives the reasons why Switzerland can also become the indirect target of cyber espionage.

[Rz 3] Also in the second half of 2016, MELANI noticed numerous attempts at cyber fraud that could result in primarily companies losing a lot of money. Distributed Denial of Service (DDoS) attacks and encryption Trojans likewise remain extremely popular with attackers for blackmailing their victims. The report looks at this issue, describes some incidents and provides recommendations for protecting against such attacks.

Source: Press Release of MELANI Nr. 66420 of 20 April 2017