Hausaufgaben “Datenschutz in der Anwendungsentwicklung”

In this article, the author speaks about the growth of smart homes automation devices and which is the security perception of these devices´ users. He later explains why would hackers want to attack your devices (such as for DDoS attacks) and also analyzes some smart home “gear” security to demonstrate that some companies do not worry about the security of the users and why is necessary that users have a real perception of the device(s) that they have at home. He conducts a survey that lists the most important factor the users consider when purchasing a home automation device is the compatibility with other devices. The second one is the price and the third is how easy it is to set up. At the end, the author makes a statement explaining why the users should be educated to worry more about the security and which data do the companies send to others and how they protect their data of the hackers.

Bradley Fizzel, “Security risks of Home automation”,
http://www.cs.tufts.edu/comp/116/archive/fall2015/bfrizzell.pdf

This article begins explaining which different devices and services do companies offer. The author later explains that normally these new machines contains security errors, which can be used to turn a device that help us in our lives into one that is against us. Then they evaluate the security of these smart homes platforms and group the main security problems in two groups: over privileged apps and insecure messaging system. In the first group the author explains the problem of these apps, making clear that developers should let the users choose what aspects should the smart home device app access, instead of grouping them and having to allow the app “full access” to our home. In the group of insecure messaging systems, SmartApps can “impersonate” smart-home

equipment, sending messages that look like messages generated by the real smart home device, then the malicious SmartApp can read the network's ID for the physical device, and create a message with that stolen ID. Allowing the developer of the malware SmartApp fool you and trick your device. At the end, the writer explains that these technologies are so new to have a perfect security but we should be aware of the information that we are exposing of ourselves with these kind of devices.

Earlance Fernandes, Security Risks in the age of smart homes, https://theconversation.com/security-risks-in-the-age-of-smart-homes-58756

This article starts explaining what is a IoT and which are the most popular devices in the market. Then he explains that companies should not worry too much about the security of their users because being IoT a, emerging technology, big enterprises focus more on launching their devices quick to gain more market and they try to have a zero-installation set up, making their security measures very weak. The author also states that some of the problems of these devices are that some of them cannot be updated, some of them cannot be secured with a password and some of them does not have a secured configuration. He gives the idea of a customized security information and event manager that spots when devices are added to the home network, identify them, note what they should or should not be doing, correlate events and look for patterns. This device learns what is normal for users and then provides alerts when something is wrong. The author ends the article writing that these devices are very hard to produce at a good price with an easy setup but the companies should face the challenge.

Gavin Kenny ,"Smart homes need smart security",https://securityintelligence.com/smart-homes-need-smart-security/