SMART HOME INVESTIGATION

FOOD FOR THOUGHT

This document, and the toolkit in general, aims to highlight the risks and vulnerabilities of our smart home environments, viewed through a critical lens, for once. Although smart devices are not designed to be vulnerable nor intended to be malicious, these risks should not be ignored.

Source: *Security in Smart Houses – Investigation of IT Products on the Norwegian Market*, Teknologirådet, 2023.

What happens to the collected data? Where does my data go?

Smart homes make you feel protected in a safe *'techno-cocoon'*, but in reality, data collected often *'escapes the house'*.

Data is processed and stored on servers all over the world and is frequently shared with third-party entities such as large US tech companies or Chinese manufacturers – exploiting your data to improve their services and serve their interests – or *'data brokers'* – selling your data to make profits.

Data collected, processed, and shared can be very sensitive since these technologies are part of our most intimate moments and sometimes even close to our bodies. Among the most private data are photos, videos, voice recordings, texts and emails, health information, biometric data, and political opinions.

Many smart home devices require the installation of a smartphone application to work effectively and remotely. This process introduces an additional source of risks and vulnerabilities. Indeed, such apps often request access to a large amount of information, such as the user's location, contact list, saved files, and the ability to see which other apps are being used on the device. Additionally, the smartphone itself is another entry point for failures and hacking.

What are the general risks and vulnerabilities of IoT?

Smart homes are exposed to specific risks and vulnerabilities, such as technology failure, hacking, tracking, espionage, and depriving household members of access to functionalities of basic home appliances.

The more technologies, the greater the complexity! As the number of products and suppliers that must work together increases, it becomes more difficult to keep track. Cloud services and long value chains mean that a failure in one link can lead to a product not working. Several technologies can interoperate or malfunction together, causing even more damage.

Risks and vulnerabilities arise from at least three entry points:

- **The smart object** can fail, malfunction, or be hacked, especially if its software has not been updated for a long time.
- **The smartphone app** used to control the smart object can disclose and exploit users' data for marketing purposes.
- **The servers** used to process and store the collected data can fail, be attacked, or simply belong to a foreign country, subjecting them to different regulations.

But the biggest security risk with IoT devices is probably that we do not consider them as a risk. Users may not think twice about giving their name and address when setting up the device because it doesn't 'publish it' anywhere. But attackers can use these objects as gateways to penetrate more sensitive systems, a threat called 'lateral movement'.

For instance, attackers could use a smart thermostat to break into a family's network, using it as a backdoor to the devices it connects to. Thermostats don't usually have the same built-in protections as phones and computers, so they offer an easier route to do damage. For instance, a cyberattack on a smart thermostat might involve cranking up the heat in the house and lock it at this high temperature to extort a ransom.

Most common cybersecurity risks associated with smart products

Password Attacks refer to situations where the attacker cracks the password of a computer system. Once the password is compromised, the attacker can gain unauthorised access to the system.

Malware is malicious software designed to damage, disrupt, or gain unauthorised access to a computer system.

Denial of Service (DoS) is an attack designed to disrupt the normal functioning of a computer system by flooding it with traffic, making it difficult for legitimate users to access the system.

Man-in-the-Middle (MITM) is an attack where the attacker intercepts communication between two parties. The attacker can eavesdrop on the communication or alter the data being transmitted.

Social Engineering is when the attacker tricks the user into revealing sensitive information. This information can be used to gain unauthorised access to the system, perform blackmail, or extortion.

What can be the harm and consequences for people and goods?

Smart homes have the particularity of putting household members at risk of being seriously harmed, both mentally and physically. On a larger scale, several smart homes malfunctioning together can disrupt key services and destabilise a part of society.

- **Goods and property** can be damaged; products that are supposed to protect the home's safety or ensure a stable ecosystem can lose function or be manipulated.
- **Information** can leak, be misused or exploited, either by criminals, foreign intelligence, or commercial companies.
- **Infrastructure (electrical, transport, etc.)** may be exposed. This applies in particular to power-demanding equipment such as electric vehicle chargers and hot water tanks.
- **People and welfare services** may be at risk: it can be a matter of life and death if equipment used for health and care loses access or changes function.