Security

Six facts about smart homes

Clever control systems, intelligent central heating, smart surveillance and security lighting systems: The home of the future can think for itself. While smart homes bring with them the promise of preventing claims in the future, they still too often provide easy ways for online hackers to break into their systems.

The heaters communicate with the smart phone, the refrigerator orders milk when it runs out, roller shutters close automatically in the event of a storm: The smart home of the future is ever more frequently becoming a reality.

According to the figures of the consultancy Mücke, Sturm & Company, more than five million households are to be connected up to a smart home system by 2020 in Germany alone. Though it must be said that the components that will be used are still young and the technology is not proven.

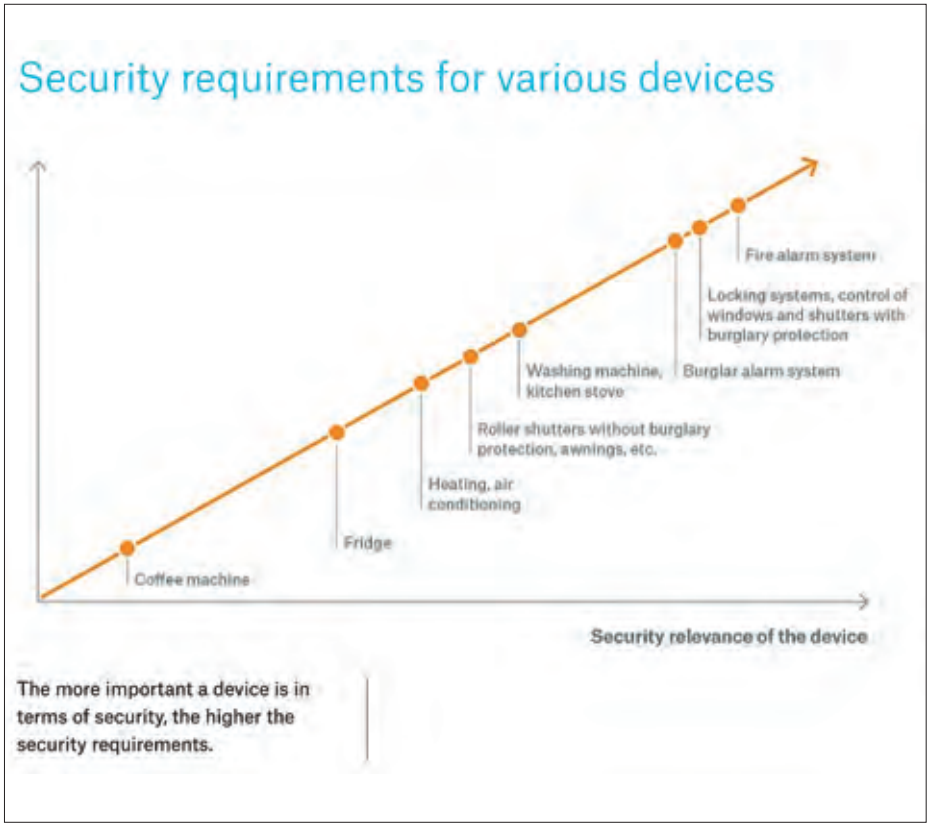
Fact 1

Risks are unavoidable in operation, because market shares are often more important to providers than security strategies.

In many cases, inexpensive components from the Far East are used. These devices have not been subjected to long-term tests, have rudimentary security precautions at best, and yet they are connected to the internet 24/7.

Especially plug-and-play devices are a security concern, because they are designed to enable laypeople to install and operate them. But that is at the expense of security. Add to this the fact that the generic password configuration (12345) is usually only changed by a small number of users – a veritable invitation to third parties to manipulate the home's automatic controls from the outside and to steal data and spy on behavioural patterns.

US consultancy firm Synack tested 16 smart home systems that were already on the market in the spring of 2015. The result: Only one of the systems proved impossible to crack using ordinary hacking tools.



Fact 2

It is unclear who is liable for any losses that may arise.

An example shows how damage can occur that requires a new evaluation: The sauna is turned on from the outside using an app. But the house burns down because a towel lying on the sauna's oven catches fire. This raises legal questions concerning negligence leading to a loss event, risk aggravation as a result of manipulation and/or defective programming, and possible recovery. But who would you sue? The company that installed the sauna, the producer of the app or a cyber criminal? The current legislative framework would make recovery very difficult.

Fact 3

Smart-home tools do not eliminate the need for physical burglary prevention devices.

Simple do-it-yourself smart home starter kits are available for under €200. But these sets only give the user a false sense of security. Even if they work as intended, they can only send a notification that a break-in is taking place: They cannot do anything to prevent it. Thieves are only prevented from breaking in by physical means – not by burglar alarms. Those choosing to open their front door with a smart phone must assume that digital burglars can do the same. Sophisticated security concepts always consist of a combination of physical and electronic components. While policyholders have thus far been able to point to a door that has been forced open as evidence of a break-in, smart home burglary investigations will need to be conducted with a fine-tooth comb in future – and it will no doubt be more difficult for policyholders to prove that a break-in has taken place.

Fact 4

Greater interconnection of the components creates ever more entry points for hackers.

The future of the smart home lies in the interplay of several systems and components. These devices can communicate with their environment via a whole host of interfaces. Operating statuses and error messages are communicated in real time; technical system data can be read and manipulated remotely. In the future, more and more heating and drinking-water pump systems will communicate with other parts of the system and exchange data with the user's mobile devices via local area networks and WiFi. These interfaces, which were created to improve the support and maintenance of the systems, offer hackers new points of attack.

Fact 5

The smart-home standard currently in use is not safe.

Anybody gaining access to the established smart-home standard, the EIB/KNX bus, can seize control of the whole building and cause a great deal of damage. Members of the cyber security industry – hackers included – are well aware of the weaknesses of the KNX bus. When the bus standard was drawn up over ten years ago, little value was placed on security, and security products for the EIB/KNX bus are still a niche product that are rarely used.

Fact 6

Even devices that are not connected to the internet and the user via wireless communication means are susceptible to attack.

And the perpetrator doesn't even have to be in the building to attack it. It suffices, for example, to attach a transmitter to the wiring of a motion detector connected to the building's automation system, or even to an outside power outlet. The transmitter communicates with an external computer, and the building's technical equipment is under the control of an outsider. Clear framework conditions and technical regulations are necessary in order to guarantee the security and reliability of the devices.

Security requirements for various devices

The more important a device is in terms of security, the higher the security requirements.

The benefits for insurers

Insurers are initially set to gain from smart homes thanks to clear benefits in the areas of early warning and loss avoidance. Here are two examples: Storm damage is prevented because open windows close on time in the event of rain or a storm, or water damage is avoided because leaks are recognised quickly and relevant valves closed automatically; Intelligent sensors and actuators help with the early recognition and prevention of events that cause damage.

This includes reducing risk accumulations and minor claims. Claims to the value of €80m could already today be prevented through the use of smart control technology in Germany, Mücke, Sturm & Company says. In 2020, that potential saving is expected to be €340m. Ideally, the insurer's claims management team would be involved from the very beginning, providing advice and know-how to prevent potential losses.

The challenges for insurers

At the same time, however, increased technical complexity will make it more difficult and more expensive to establish the validity of claims and settle them. This is because, in addition to technical failure, insurers will also have to examine whether the loss was the result of an operating error or a targeted attack. More technical expertise is therefore necessary, as are risk models and business models geared towards innovation and new approaches to pricing and product design that enable insurers to become solution finders for their clients, moving away from basic policies and towards full risk management for clients. This requires excellent networks between Claims Management, Product Development and Sales.