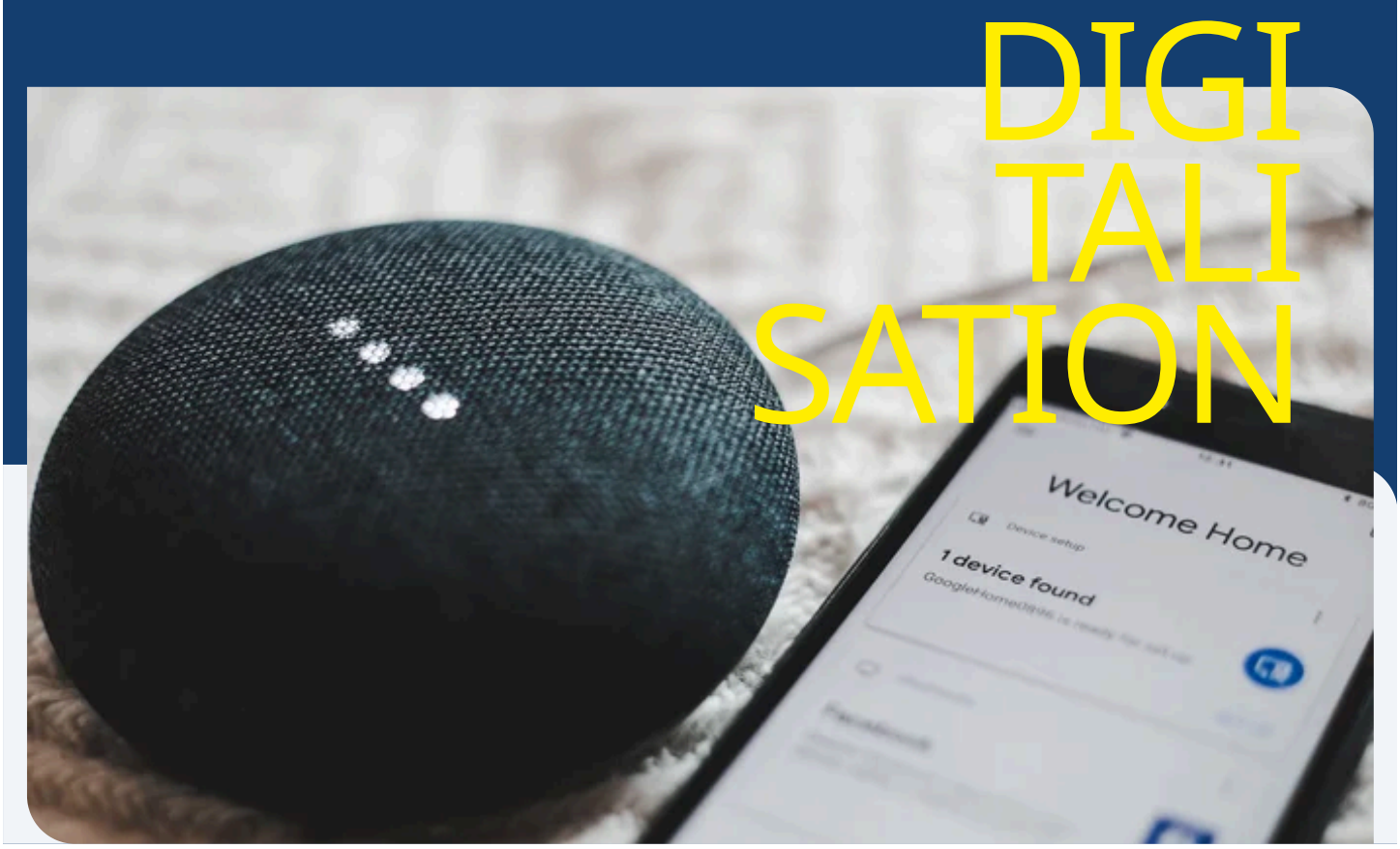
COMMENT DIGITALISATION INNOVATION

Smart home: No access for hackers

06.11.2023 / Österreich / Karin Bornett



For buildings to become smart, they need to collect data. What data that is. And how to prevent it falling into the wrong hands. An overview.

Modern buildings are intelligent. Thanks to networked, digital sensors and monitoring systems, they can control their own heating, cooling, shading, lighting and even watering the garden. This saves human resources in operation and maintenance. Automated building systems are also more energy efficient. And they recognise and report weak points or technical faults at an early stage.

The data

Depending on their design, smart buildings can record and process a wide range of different data: Temperature, humidity, light intensity, CO2 content of the air. The number of people in a room, energy consumption, operating data from devices such as the operating time of the heating or the capacity of the PV system, the operating status of lifts or data from access and other security systems. Without this data, buildings remain costly to maintain, slow to rectify faults and more difficult to calculate - for example in terms of energy supply or operating costs. Overall, smart buildings are more efficient than conventional buildings. According to the Deloitte Smart Building Study 2023, the operating costs of twenty smart buildings analysed were up to 26% lower than those of conventional buildings. Energy consumption was 34% lower on average. At the same time, the level of comfort in the smart buildings analysed was perceived as very high. In order to achieve climate targets and in view of rising construction and energy costs, buildings will not be able to do without smart systems in the future.

The dangers

(c) generated with bing

The other side of the coin shows very worrying scenes in extreme cases: Cameras are used to spy on residents, the power supply is manipulated or the access system is deactivated by strangers. Insecure systems open the door to hackers. Literally. Possible motives: stealing data for the black market, blackmailing operators or taking control for burglary and theft on site. In April 2022, for example, hackers broke into the control system of St Stephen's Cathedral in Vienna and caused its bells to ring for a good twenty minutes at 02:00 in the morning. Fortunately, apart from the brief irritation of the population, no damage was caused. The motive for this offence? Unclear. But even if the case could be dismissed as a juvenile prank, incidents like this make it clear how important the cybersecurity of buildings is - and not just in new buildings.

The measures

To protect against external attacks and ensure smooth operation, every intelligently networked building must have a comprehensive security concept - for both operational and information technology. The data-based solutions and services of smart buildings utilise cloud platforms and Internet of Things infrastructures. To protect data and systems from attacks, all connections are encrypted and provided with secure passwords and access codes. Responsibility for the cyber security of entire buildings lies with the owners or operators. It is important that the security concept is continuously evaluated and adapted. And anyone who uses smart home systems at home should also take the following measures to ensure cybersecurity:

- Only buy smart home devices that fulfil DIN VDE V 0826-1.
- Ensure that connections are encrypted in accordance with current standards.
- Use a firewall and an anti-virus programme.
- Make sure you set up secure passwords.

- In Germany, the Federal Office for the Protection of the Constitution warns of cyberattacks by Chinese hacker groups on private individuals at the end of August 2023. These would become more frequent and mainly occur via smart home systems.

The conclusion

Intelligently networked, well-protected buildings save resources while offering a high level of comfort. They are important for achieving climate targets. Although cyberattacks are a threat, sophisticated security concepts and technologies provide a comprehensive, virtual protective shield over the systems. Awareness among owners and companies is high and will continue to grow. According to Statista, a total of around EUR 7.8 billion will be spent on IT security in Germany in 2022 and around USD 71 billion worldwide. In 2025, expenditure in Germany is expected to total around EUR 10.3 billion.