IOT INSPECTOR

IOT SECURITY REPORT 2021

UNCLEAR RESPONSIBILITIES, INADEQUATE SECURITY MEASURES: IN MANY COMPANIES, IOT SECURITY COMES UP SHORT

EXECUTIVE SUMMARY:

- A survey of 260 IT decision-makers in the DACH region confirms widespread use of IoT devices in companies of all sizes and industries
- The majority of respondents considers the Internet of Things to be insecure or not very secure, and prevention measures for securing IoT devices inadequate
- The survey highlights unclear responsibilities and insufficient measures for risk prevention in the majority of organizations, while specific risks of attacks against IoT devices are underestimated

It's no secret among expert that IoT security is still a blind spot in many companies. The new figures from our IoT Security Report 2021 are nevertheless alarming.

In the IoT Security Report 2021, we surveyed 260 IT decision-makers in the DACH region on the topic of IoT security. Slightly more than half of all participants stated that they were in a leadership role — i.e., in the executive board (38%) or in management (13%). Another 14% of all respondents work in technology and development. We were able to represent a solid mix of industries (e.g., industry, IT, consulting, science, or telecommunications) and company sizes (from microenterprises with less than 10 employees to large organizations).

Widespread use of IoT devices in companies

As diverse as our respondents' companies were, a very clear picture emerged when asked about the prevalence of IoT: Smart devices of all kinds have become an integral part of modern business operations. Routers and Wi-Fi access points are used almost everywhere, and network printers can now be found in nearly three quarters of all companies (71%). VoIP telephone systems (35%) and smart A/V conference room systems (29%) are used in around a third of all participating companies. An increasing number of companies are also relying on IoT devices for access security, for example through network cameras (24%) or keyless access systems (18%). In modern production especially (Industry 4.0), sensors (29%) and IoT components in production control (15%) are on the rise.

Uncertainty about security of IoT devices

But as widespread as IoT devices have become in both private and professional environments, the reputation of the Internet of Things is equally dubious. Only 7% of all respondents consider the Internet of Things to be secure, and only 3% very secure! The vast majority of all respondents consider the Internet of Things not very secure (71%) or insecure (14%).
Our respondents are also pessimistic when it comes to risk prevention: Only just under one-fifth of them stated that the measures for securing IoT devices were sufficient (12%) or partially sufficient (9%). More than two-thirds consider the measures to be insufficient (71%).
Furthermore, the vast majority of participants in our survey believe that hackers have already focused on misusing IoT devices (85%). The damage caused by hacked IoT devices in the DACH region is estimated by most of the decision-makers we surveyed (35%) at 20 to 50 million euros... per year!

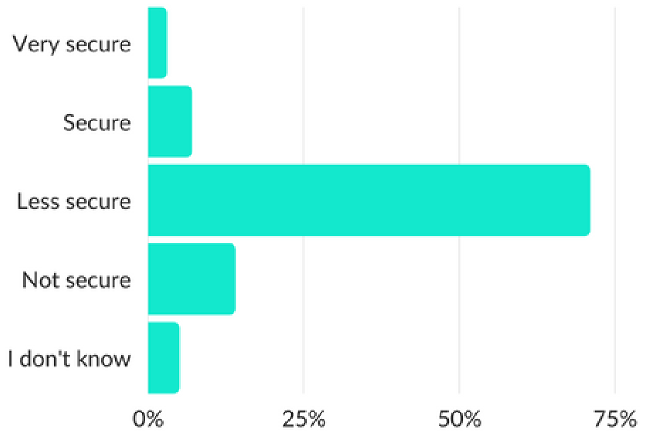
Inadequate IoT security standards in many organizations

It is all the more worrying that, despite these pessimistic assessments, IoT security is still a blind spot for many companies in Germany, Austria, and Switzerland.

According to the study, 42% of all participating companies lack internal compliance regulations for the security of IoT devices. Nevertheless, such regulations are already in place in about a third of all companies. In many places, there are also no clear security guidelines in place (yet) for the procurement of new IoT devices (42%).
At least 37% of all participating companies already have such regulations in place.
21% of respondents were unable or unwilling to provide any information on this.

However, clearly defined security guidelines in the procurement process are only one of several measures that every company should definitely take into account! After all, many IoT devices are connected to a corporate network according to the "Plug, Play & Forget" principle.

How secure do you think the Internet of Things is?



Source: IoT Security Report 2021, powered by IoT Inspector. n = 260

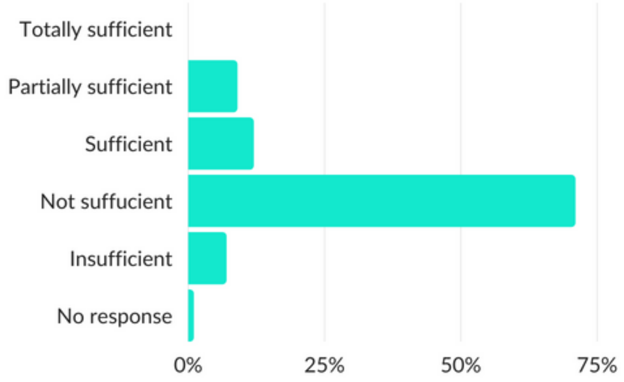
But just like laptops, smartphones or server systems, they should be regularly maintained, updated to the latest firmware version and, in the worst case, discarded (for instance, if a manufacturer discontinues support for a particular device).

Small vulnerabilities, big consequences

More than half of all respondents to our survey stated that they had not (yet) experienced security incidents in connection with IoT devices (27% did not know).
However, a single critical vulnerability in an IoT device can have far-reaching consequences: attackers can exploit such vulnerabilities to gain access to a company's, government agency's or organization's entire network via the IoT device. From then on, they can temporarily or permanently shut down the entire network (or parts of it) (Permanent or Distributed Denial of Service), abuse servers specifically for crypto mining or spam, and of course engage in data theft or industrial espionage.

However, cybercriminals often attempt to extort ransom money (so-called ransomware attacks) — as was the case in the fall of 2020 at the University Hospital in Düsseldorf.

Do you think sufficient effort is put into ensuring the security of IoT devices?



Source: IoT Security Report 2021, powered by IoT Inspector. n = 260

Using a known vulnerability in an IoT device firmware from the manufacturer Citrix, attackers could install a backdoor, thereby gaining access to the hospital's IT infrastructure - and completely paralyze it. The attackers, however, dropped their original ransom demand when they realized that their extortion attempt was seriously endangering human lives. Nevertheless, the damage to the University Hospital was tremendous, and it took almost a month before the facility was able to return to its normal operations.

Inadequate protective measures

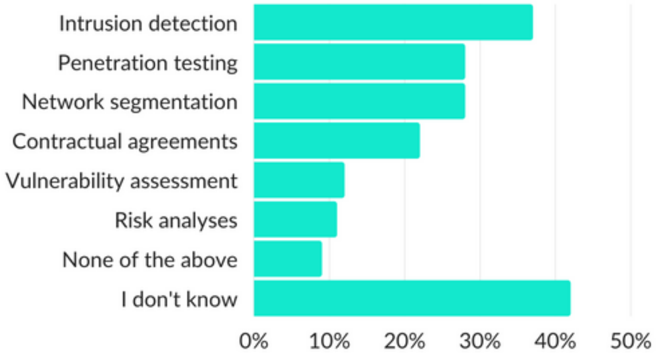
It is all the more alarming that almost half of all respondents (42%) did not know which measures their company implements to secure its IoT infrastructure. The rest of the respondents reported a wide range of security measures (multiple answers possible) — from intrusion detection (37%) to penetration testing and network segmentation (28% each) as well as vulnerability assessments and threat analyses (12% and 11% respectively). Just under a quarter of all enterprises (22%) rely on contractual agreements with vendors. While such agreements are a good additional protective measure, they are no substitute for extensive in-house protection of the entire IT and IoT infrastructure!

No Clear Responsibility for IoT Security

Responsibility for IoT and IIoT security is just as ambiguous as the protective measures implemented. In around a quarter of companies, the responsibility for these falls to the Risk & Compliance Manager (28%), while elsewhere the CIO (17%), IT Purchasing (17%), CTO (15%) or CISO (7%) are responsible for the security of IoT devices. In just over a fifth of all companies (21%), responsibility is outsourced to external consultants, while again just over a quarter of respondents did not even know who was in charge (28%).

In many companies, there is clear lack of responsibilities when it comes to IoT — a gross negligence! We recommend companies approach IT security and IoT security holistically and create a central point of contact within each company: "The person in charge of IoT security must be the same person who is responsible for the rest of IT security," says IoT Inspector CEO Jan Wendenburg.

What measures does your company take to ensure the security of its IoT infrastructure?



*Multiple responses.
Source: IoT Security Report 2021, powered by IoT Inspector. n = 260

Risk of Attack Grossly Underestimated

The study participants consider the following to be particularly at risk of hacker attacks: PCs and laptops (72%), industrial systems (71%) and servers (68%).

VoIP telephones (14%), networked medical technology and network printers (28% each), on the other hand, are considered to be the least at risk. Wendenburg: "This is a serious misjudgment that may have been valid ten years ago. Today, every device — from routers to video conferencing systems to keyless entry systems — is a potential Trojan horse for attacks on companies and organizations."

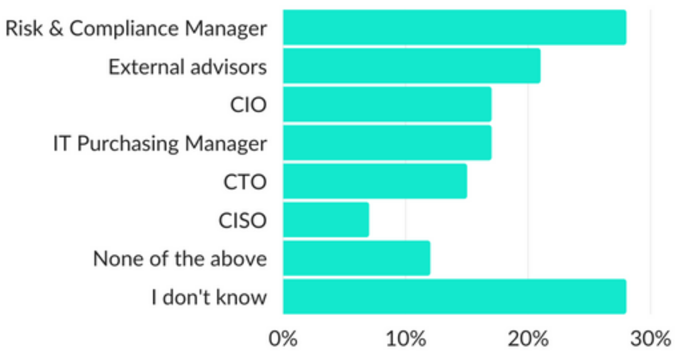
Targeted analysis of IoT firmware, i.e., checking the device's internal software for security vulnerabilities, is only performed punctually: barely 19% of all companies surveyed use such analyses at least in part, while 12% want to start doing so soon. Yet, in many cases it is primarily the device firmware that harbors critical security vulnerabilities!

3 IMPORTANT STEPS FOR INCREASED IOT SECURITY

IoT security may still be unknown territory for many companies, but in reality, three steps are all it takes to minimize the security risks posed by IoT devices:

- Procurement: Define internal security guidelines and check new IoT devices for security and compliance during the procurement process
- Inventory: Conduct an inventory and analysis of the existing IoT infrastructure
- Monitoring: Continuously check for new vulnerabilities and compliance breaches

Who is charge of (I)IoT device security in your company?



*Multiple responses.
Source: IoT Security Report 2021, powered by IoT Inspector. n = 260

About IoT Inspector

IoT Inspector is the leading European platform for automated security and compliance testing of IoT device firmware.

Using IoT Inspectors' powerful platform, manufacturers across all industries automatically detect vulnerabilities and compliance breaches throughout the IoT product lifecycle. By deeply integrating IoT security into their product development processes, our customers save valuable time and resources while reducing risks. Product integrators benefit from an independent quality gate and increased supply chain transparency when purchasing components from external suppliers.

The powerful binary analysis automatically delivers instant results, is scalable and cost-effective: IoT Inspector requires no source code, no network connectivity, and no physical device access.

Since 2015, IoT Inspector has generated worldwide attention by identifying critical security vulnerabilities affecting millions of IoT devices from global vendors. International leaders such as ATOS, Swisscom, TUEV, Zyxel, and others benefit from IoT Inspector's powerful automated platform and services.

Request your free trial today at sales@iot-inspector.com!