IOT SECURITY REPORT 2022

Serious Vulnerabilities: The Need for IoT Protection

Executive Summary

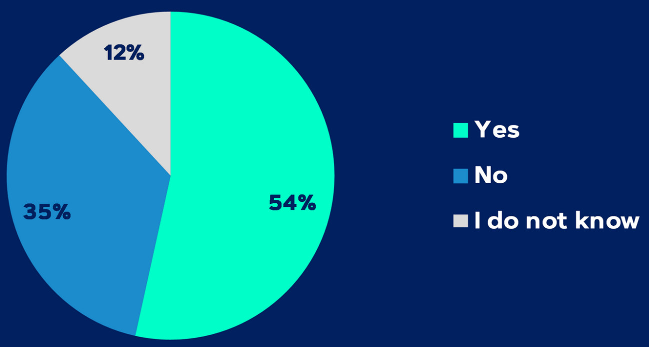
The Internet of Things (IoT), including Industrial IoT (IIoT) and Operational Technology (OT) connects a multitude of devices and systems - this revolution of inter-connectivity and smart automation illustrates that the present and future of efficient manufacturing lies in the degree of networking.

However, networked devices have one thing in common: they all come with a variety of proprietary software systems and firmware components that so far have received little attention in the procurement and use of IT technology. The IT security company ONEKEY surveyed a total of 318 corporate specialists and executives, and the decisive results are available here as the IoT Security Report 2022.

Hardly any compliance

Overall, the industry draws a mixed picture – the uncertainty around the topic of IoT security is high. As a result, only a few companies have to date established compliance rules: Only about half of the 318 industry representatives surveyed say that they have compliance rules for IoT security in place at their companies, 35 percent have no rules.

Does your organization have compliance policies in place for IoT device security?



Source: IoT Security Report 2022, powered by ONEKEY n = 318

> "Connected manufacturing is as efficient as it is dangerous. Facilities have numerous hardware devices that use their own firmware and are now more targeted than ever by hackers."
> Jan Wendenburg, CEO ONEKEY

The majority of respondents consider the security provided by the manufacturers to be partially or not at all sufficient.

Survey of 318 IT industry professionals & executives reveals major uncertainties in the area of IoT security.

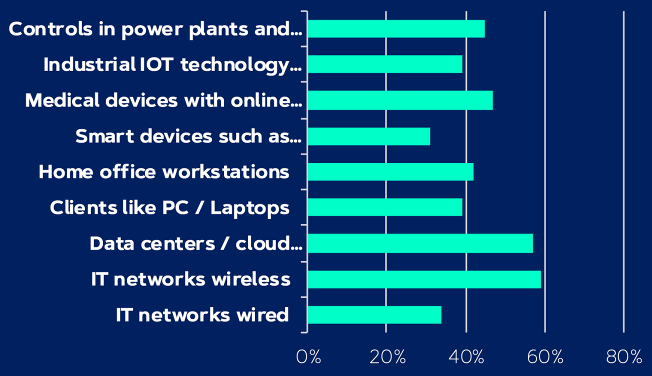
Survey shows unclear responsibilities and lack of controls at majority of companies.

The demand for a proof of origin - the software bill of materials - is becoming increasingly clear.

The most vulnerable areas include IoT devices in health (47 percent), critical infrastructure (45 percent) and manufacturing (39 percent). The majority of all companies rely on threat intelligence (50 percent) and contractual requirements for suppliers (42 percent) to secure IoT infrastructure. Although this settles the question of liability in case of doubt, a determined attack on production facilities can threaten a company's economic existence within a few days.

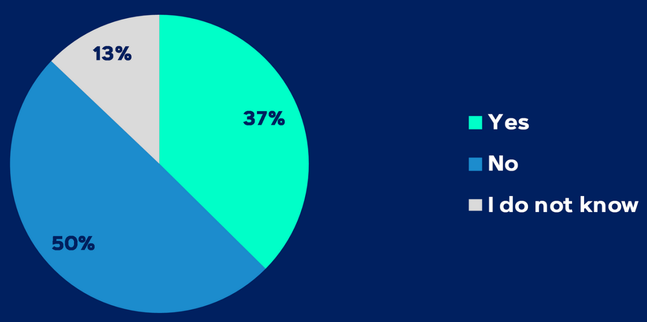
And this is taking its toll - because numerous companies have already had to report incidents caused by hacked endpoints. Among the 318 company representatives surveyed for the IoT Security Report 2022 alone, 37 percent confirmed security-related incidents with endpoints that are not a normal PC client. IT experts agree that the number of networked devices in a wide variety of functions - including manufacturing - will exponentially increase in the coming years.

Which of the following IT systems require the most protection from attackers?*



* Multiple responses
Source: IoT Security Report 2022, powered by ONEKEY n = 318

Has your company experienced any security incidents related to IoT devices?



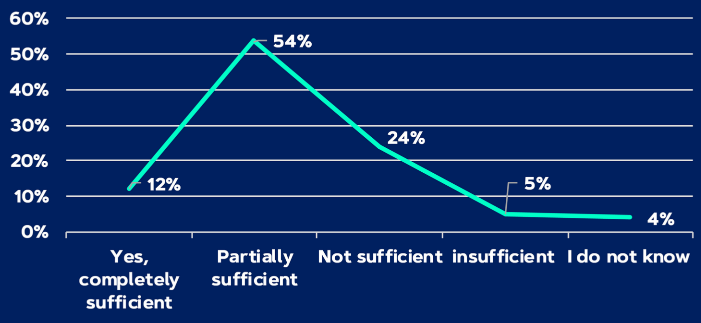
Source: IoT Security Report 2022, powered by ONEKEY n = 318

Low confidence in own security

The company representatives surveyed were unanimous about the security provided by manufacturers for IoT systems: only 12 percent consider the measures for hacker protection to be sufficient, 54 percent see them as partially sufficient, 24 percent as insufficient, and 5 percent even as deficient.

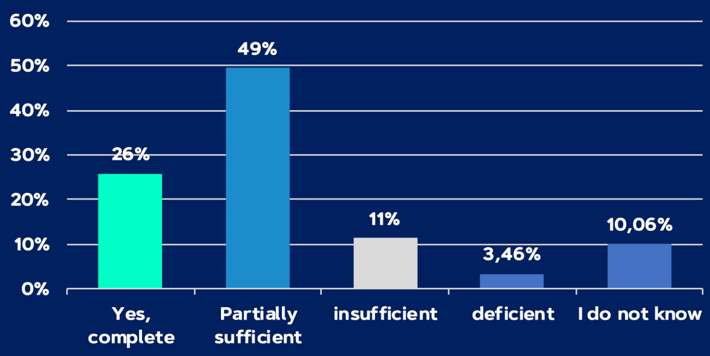
Only 26 percent therefore consider their company's own IoT security to be fully sufficient, 49 percent only partially sufficient. Almost 15 percent, on the other hand, declare their own measures even to be insufficient or deficient.

In your opinion, are IoT device manufacturers doing enough to ensure the security of their products?



Source: IoT Security Report 2022, powered by ONEKEY n = 318

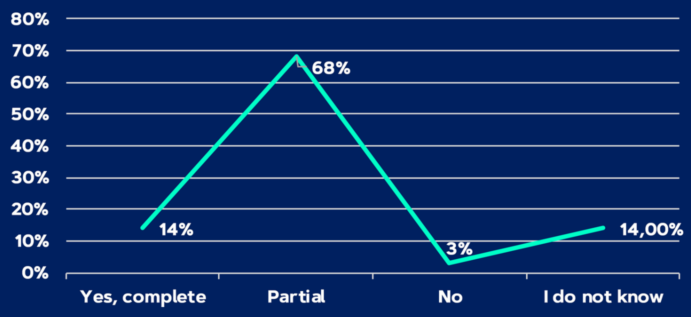
Is enough being done to secure IoT devices in your organization?



Source: IoT Security Report 2022, powered by ONEKEY n = 318

Even penetration testing - often referred to as the pinnacle of IT security - is not fully trusted: only 14 percent consider it to be an efficient way to test the security of an infrastructure, 68 percent see it as partially efficient.

In your opinion, is penetration testing the most efficient way to verify the security of an infrastructure?



Source: IoT Security Report 2022, powered by ONEKEY n = 318

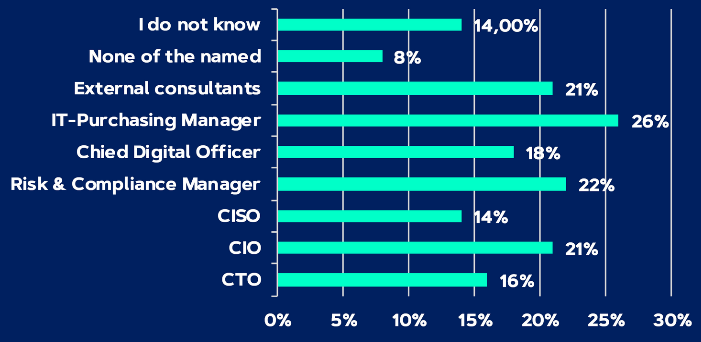
> "The problem needs to be addressed at the root, directly during the development and production of systems and machines connected to a network. The IT industry could take a cue from the process industry - the pharmaceutical industry, for example. There, it is a legal requirement to provide complete traceability and transparency for every component of a product. This should equally be standard in the IT sector - for hardware as well as all software components!"
> Jan Wendenburg, CEO ONEKEY

IoT technology is in use for a long time

Another risk is the long period of use of such technologies. Industrial control, production equipment and other smart infrastructure endpoints are often in company use for more than ten years. However, the lack of compliance strategies makes it difficult to implement an update policy that allows important security features to be implemented by overwriting the previous firmware by an updated version.

In addition, in many companies the question of responsibility is unresolved. Among the 318 company representatives surveyed, different people and departments are responsible for IoT security. These range from CTO (16 percent) to CIO (21 percent) to Risk & Compliance Manager (22 percent) to IT Purchasing Manager (26 percent). In 21 percent of the companies, external consultants even handle the purchasing of IoT devices and systems.

Who is responsible for the security of your (I)IoT devices in your company?

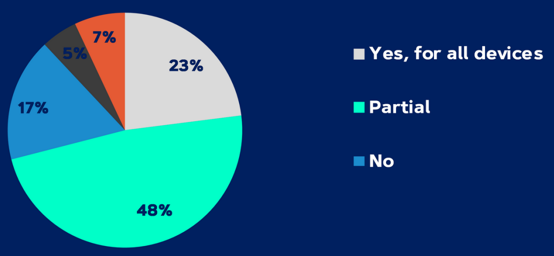


* Multiple responses
Source: IoT Security Report 2022, powered by ONEKEY n = 318

No In-house Controls

Surprisingly, only 23 percent of the companies performing security test, i.e. in form of an analysis of the included system and device firmware for security vulnerabilities.

Do you practice firmware testing - i.e., checking the IoT device's internal software for security vulnerabilities?



Source: IoT Security Report 2022, powered by ONEKEY n = 318

The awareness for the requirement of IoT security analysis appears fairly low.

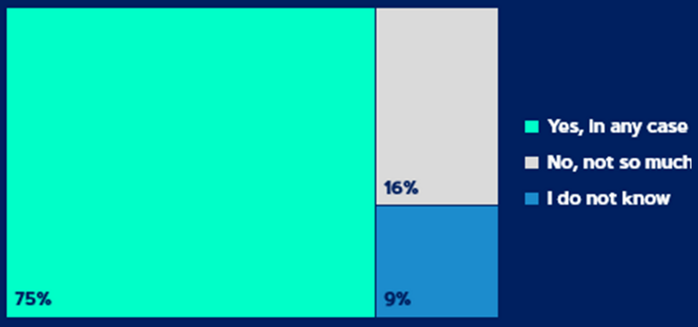
For typical (Windows) PC & clients, security actions, i.e. firewalls, anti-virus etc. are mandatory - throughout the IoT devices, such requirements appear mostly non existent. Advanced, automated platforms offering full automated software analysis in just a few minutes, and the result provides clear information about the risks and their classification into risk levels.

Implementing such automated security & compliance analysis into Firmware Development Lifecycles (SDLC) or into the procurement process may help to improve IoT security substantially.

Software Bill Of Materials (SBOM)

The call for a proof of origin of the included device software - and thus also for a security check - is therefore clearly voiced in the study. As part of the "IoT Security Report 2022" study, 75 percent of the 318 IT industry professionals and executives surveyed are in favor of precise proof of all software components, a so-called "Software Bill of Materials" (SBOM) for all components, including all software contained in an endpoint.

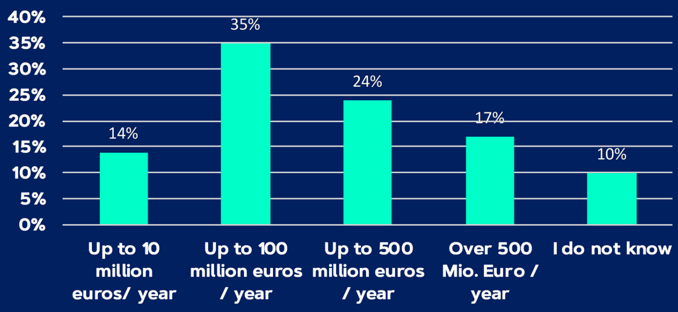
In many industries, proof of all components of a product is required. Experts are calling for this for software as well. Does this initiative make sense?



* Multiple responses
Source: IoT Security Report 2022, powered by ONEKEY n = 318

Moreover, according to the industry experts, the potential damage from hacked IoT devices can quickly swallow up sums in the millions: 35 percent of the IT managers and decision-makers surveyed for the study consider an annual damage of up to 100 million euros to be realistic, with a further 24 percent even up to 500 million, and 17 percent more than 500 million euros. In the meantime, the threat situation is likely to have worsened. The survey took place before Russia's invasion of Ukraine, and cyber attacks have been part of the aggressors' hybrid warfare worldwide since the start of the war at the latest.

How high do you estimate the annual economic damage in Germany caused by attacks on IoT devices?



Source: IoT Security Report 2022, powered by ONEKEY n - 318

IoT Not in Good Shape - needs more attention!

Generally speaking, security in the IoT sector is not in good shape - this conclusion is clearly supported by the study. Companies have hardly any guidelines, manufacturers work on a random basis, and only when the systems are in operation the beta tests for security take place. The damage could become worse in the coming years as the degree of networking in the economy increases. In addition, there will be stricter liability issues, which will also put the onus on decision-makers in the companies in the future. It is obvious that in the foreseeable future, the management will be directly held liable for omissions in IT security.

Initiator of the study:

ONEKEY is the leading European platform for automated security & compliance analysis for devices in industry (IIoT), manufacturing (OT) and the Internet of Things (IoT). Using automatically generated "Digital Twins" and "Software Bill of Materials (SBOM)" of devices, ONEKEY autonomously analyzes firmware for critical security vulnerabilities and compliance violations, all without source code, device or network access. Vulnerabilities for attacks and security risks are identified in the shortest possible time and can thus be specifically remedied. Easily integrated into software development and procurement processes, the solution enables manufacturers, distributors and users of IoT technology to quickly and automatically check security and compliance before use and 24/7 throughout the product lifecycle. Leading companies, such as SWISSCOM, VERBUND AG and ZYXEL, are using this platform today - universities and research institutions can use the ONEKEY platform for study purposes free of charge.

Errors, changes and availability of the presented products, services, features and possible applications are reserved. None of the given information and decisions are legally binding or to be interpreted as such.

ONEKEY GMBH
Kaiserswerther Straße 45
40477 Duesseldorf
Germany
https://onekey.com/