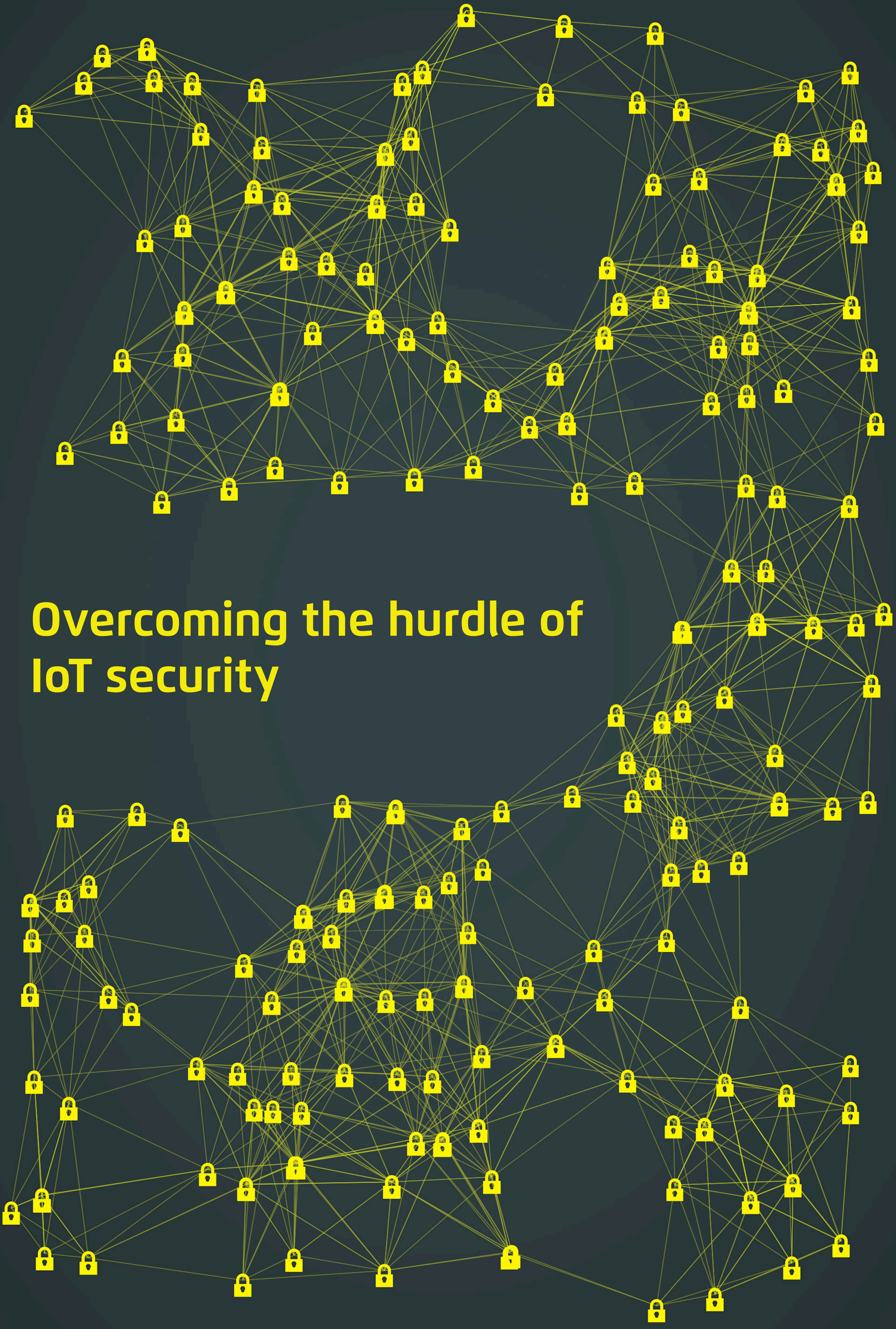
Overcoming the hurdle of IoT security



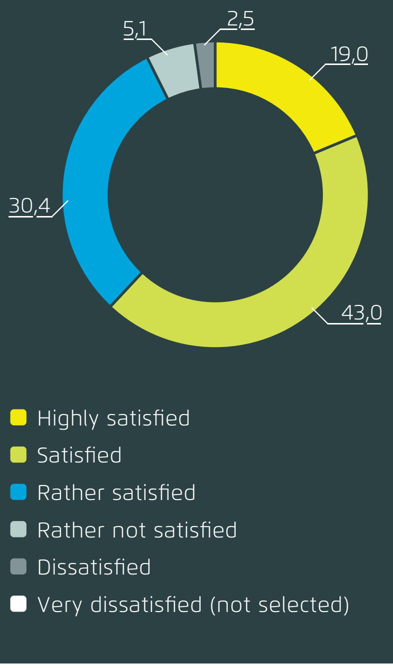
Overcoming the hurdle of IoT security

In this whitepaper we want to dive deep into the problem of, and the solution for IoT security issues. We show you what makes IoT security so special and how security risks hinder a significant share of projects to be conducted.
We give you a deeper understanding about the threats your project may face, and how to realize it however.

IoT projects create significant success. As a 2017 study of Lemonbeat GmbH with IDG Research Services shows, two-thirds of companies are satisfied with the success of the various kinds of IoT projects they have conducted. In terms of increased productivity, lower downtimes, reduced costs, ROI, revenues, and company image.

How satisfied are you with the results of IoT projects?

Numbers in percent. Base: n = 81



Why has your company not yet dealt with the Internet of Things (IoT) topic?

Numbers in percent. Multiple choices possible. Base: n=64

The topic is not relevant for our company	41,2
Currently other priorities	37,5
No added value	25,0
Missing business model	25,0
Lack of know-how	21,9
Security risk	18,8
Uncertainty regarding future development of the IoT	14,1
Too costly	12,5
Immature technology	12,5
Uncertainty regarding future customer needs	12,5
No usable integration platform	7,8
Uncontrollable mass of data	4,7
Other reasons	1,6

However, benefits only come for those who act. So, why are still 80% of the 385 study's participants from German cross-industry companies currently not involved in IoT? Various causes, of course, but a large share of 19% state "security risks" as the reason why they have not conducted IoT projects by now. What are the threats and risks that companies see in IoT? Are they justified? And if yes, how can they be handled?

On the next pages, we show you:

- Companies' current evaluation of IoT security and its consequences
- What makes IoT security special compared to well-known IT security
- The threats of IoT and adequate countermeasures
- A guideline how to deal with IoT security systematically

What are the perceived IoT security issues of companies?

> “Companies face a huge new security challenge when it comes to IoT. It shouldn’t, but it does hinder project execution.”

Dr. Jens Reinelt,
CTO Lemonbeat GmbH

Companies’ fears about IoT security is not without reason: Those organizations who have conducted a project in the past list three security-related issues beyond the four most problematic barriers during project execution. 43.9% see security (new gateway for hackers) as a big technological problem, 39% data security and disaster recovery, and 29.7% operational safety. 51% of the study participants evaluate risks concerning information security as very high or high. Risk evaluations for safety of production facilities (49%) and personal data privacy (48%) are similar. And about 45% of companies see risks for the security of products, security of plant and product data as well as the integrity and correctness of data and service functionalities.

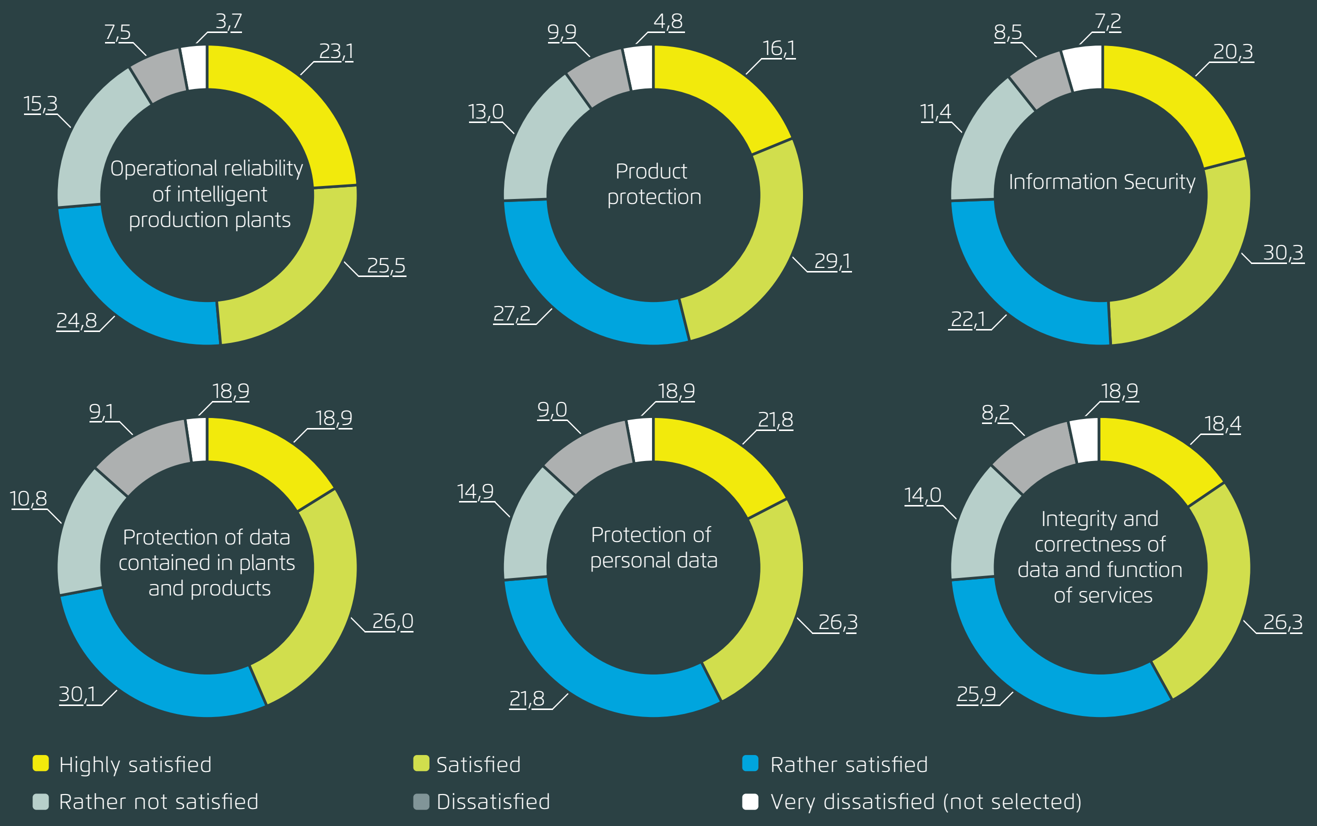
What are the biggest technological challenges in IoT or in implementing IoT project?

Numbers in percent. Multiple choices possible. Base: n = 310

Security (new entrance for hackers)	43,9
Data security / Disaster Recovery	39,0
Safety/Operational reliability	29,7

How high do you rate the security and safety risks associated with IoT?

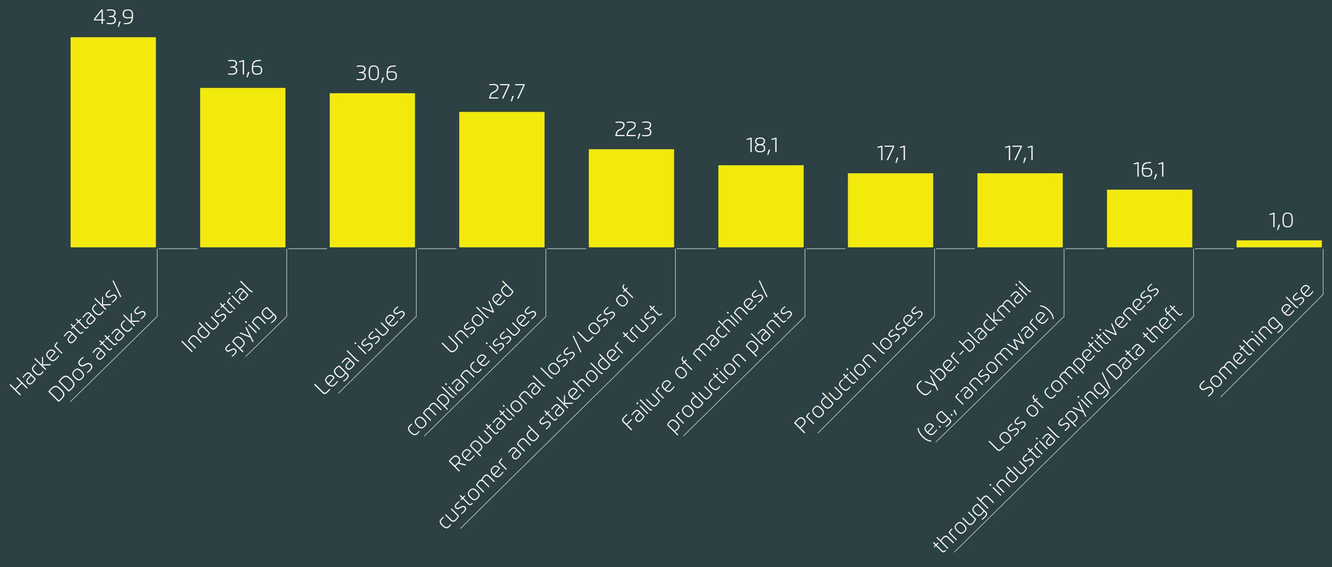
Numbers in percent. Rating on a scale of 1 (very high) to 6 (not big at all). Base = 309



Which are the fears that these risk evaluations result from? The biggest are DDOS and other hacker attacks (43.9%) as well as industrial spying (32%). Legal problems (31%) and compliance issues (28%) come next, followed by reputational damage (22%), losses in production (18%) and blackmailing with cyberattacks (17%).

Security and safety are seen as one of the obstacles facing IoT.

Numbers in percent. Multiple choices possible. Base: n = 310



The above listed survey results show that security, safety, and privacy are topics that hinder a significant share of projects to be done. But why are those topics such a big issue in a professional world that knows computer networks and, therefore, IT security measures for decades? On the following pages, we give you the most important facts about the special security complexity in IoT and a guideline how to handle it.

Why security is an issue of new complexity in IoT

Since decades IT security is a battleground where hackers and other computer criminals are often one step ahead of antivirus programs and security specialists, while administrators and developers try to shelter from the never-ending attacks. So, how big must be the challenges in the IoT field where virtual and physical world melt and therefore even more unprotected flanks exist? Two different worlds with their own challenges and experts to conquer them. But the crucial question is: Do the experts of both worlds have sufficient knowledge about the other one to be well positioned in the fight against malicious intruders.

On the one side, there are the cybersecurity specialist and security practitioners who have often outstanding IT knowledge and knew a lot about securing their networks and ensuring the basic security principles like confidentiality, integrity and non-repudiation. But when it comes to fault-tolerant product safety designs of physical IoT devices, they are more or less beginners. On the other side, there are the engineers from different disciplines — like chemical, electrical, mechanical, automotive — who are experts in making their products safe for customers by design, but for whom device controlling and data gathering and transferring over the internet as well as the security issues associated are a new challenge.

Sure, security practitioners could try to adopt the necessary knowledge from the engineering world. But this world is so widespread that it seems to be a wild-goose chase. A close cooperation of both sides seems necessary to familiarize engineering experts with the necessary tools of the security trade to enable them to plan not only safe, but also secure products by design. To be prepared for possible security issues at an early stage and to include sound and economically reasonable measures against them will be the only way to get effective, but also affordable security in the field of IoT. However, which measures seem to be sound and reasonable will vary depending on which smart things are produced in which field of engineering.

In the end, each device or system is as weak as its weakest link. So, all parties involved in the lifecycle of an IoT device must keep in mind that IoT security can only be achieved if everybody felt responsible, from the third-party equipment manufacturers to the design manufacturers and the cloud providers. Furthermore, liaisons between the different engineering disciplines will be helpful. Threats against devices and the whole IoT world are not threats against a unique device, company or discipline; they often have impact on multiple fields. In the worst case, a vulnerable smart sensor in a school, a hospital, or even an atomic power plant can offer access to the network, thus rising potential risks and hazards.

IoT under attack

Frequent attacks carried out against IoT devices and most successful measures against them.

Wired and wireless scanning and mapping

Attack method:

Uses the same paradigms as network scanning in regular IT attacks to attack wireless communication protocols to get information about IoT devices — with the risks of taking control, for example, over light, door opener, etc.

Countermeasures:

- Preventive network port scanning
- Preventive vulnerability scanning

Protocol-related attacks

Attack method:

Each protocol has its limitation in terms of security. For example, a possible loophole is the pairing process where network keys are prone to sniffing during the exchange — with risks of loss of confidentiality.

Countermeasures:

- Recognizing the limitation of each protocol used
- Implement or strengthen measures on other layers instead

Cryptographic algorithm and key management attacks

Attack method:

Getting access to computers, devices or networks by compromised keys — with the risks of decrypting and modifying data.

Countermeasures:

- Strong encryption based on cryptography
- Counter modes
- Digital signatures
- Random number generation
- Block chaining modes

Eavesdropping attack

Attack method:

Listening on traffic between devices or between devices, gateway and the cloud by gaining access to data path in the network (sniffing) — with the risks of loss of confidentiality.

Countermeasures:

- Check of key binaries
- Remove unused services
- Fully encrypted communication

Denial of service and jamming

Attack method:

Attempt to alter the behavior of computers, applications and services or to force their shutdown by sending invalid data or flooring them with traffic. Furthermore, the blocking of traffic to prevent access for authorized users and to couse a denial of service.

Countermeasures:

- Continuity of operation planning (COOP)
- Sufficient throughput for each node to withstand ODS attacks
- Close loopholes by checking messaging infrastructure, data structure and use of variables

Physical security attacks

Attack method:

Theft and demolition of physical devices to gain access to processor, memory, etc. — with the risks of getting hold of sensitive data like key material, passwords and configuration data.

Countermeasures:

- Tamper evidence control
- Tamper response mechanism (e. g., automatic memory wiping)
- Cryptographic modules to protect cryptographic variables
- Mitigation planning
- Protect debug ports with passwords
- No hard-coded passwords
- Implementation of only absolutely vital physical ports (e. g., USB)

Access control attacks

Attack method:

Privilege escalation via social engineering and elevation of privileges as well as identity spoofing by falsely assuming IP addresses and phishing — with the risks of modifying, rerouting or deleting data.

Countermeasures:

- Enhancing staff awareness
- Control assets for unusual behavior
- Sensible levels of authentication
- Sensible levels for administrator capabilities
- Separation of administrative and user level functions

14 things to consider creating trustworthy IoT networks

When planning and designing IoT devices and systems, it's good to have not only security, but also safety and privacy requirements always in one's sight. Furthermore, all parts of the system should be taken into considerations by all persons involved. With one thought always in mind: IoT and security is not only about losing data and confidentiality, it is also about dangers for human beings, for example, when a manipulation targets not a garage door but a pacemaker instead.

Product safety is a classic design aspect of the engineering world. Since IoT devices are physical things: it is important to ensure their safety by conducting a risk analysis or using a safety tree to detect possible dangers for life, limb and property. On the other hand, IoT devices are often used to aggregate data from different devices, which are then gathered on a gateway and send, for example, to the cloud. This entails that there must be a secure communication configuration on both ends, the IoT devices and the backend. And finally, IoT security: It's a good idea to install threat modeling combined with security and safety trees from the start. When designing a device or system, threat modeling means to look out and list all potential threats to a service or system that could compromise it; whereas an attack tree starts from the other end by imagining how an attacker would try to gain access or tamper and harm the device or system.

So, when designing for the IoT, companies should plan security and safety measures from the start and to a reasonable extent. What seems sound and reasonable and how widespread, pervasive, and sophisticated countermeasures have to be, has to be discussed on a case to case basis; depending on the field of engineering, the smart things to be produced, and the kind of possible security issues and dangers related to them, and so on. The higher the risks and the damage and the more sensitive the industrial sector or the possible field of use, the more meticulous advanced planning and countermeasures should be considered and used.

So, keep in mind that the following aspects only present one model approach for planning secure and safe IoT projects. In practice, which aspects are relevant must be decided for each case individually.

Hardware Design and Planning:

1. Factor 3rd parties into the planning.
   3rd party cooperation through SLA and privacy agreements and approved list for 3rd party soft- and hardware.
2. Choose a good and suitable MCU and RTOS.
   A good MCU already brings things like a cryptographic boot loader, secure memory protection, tamper protection, reverse engineering protection; and a RTOS should be appropriate for the specific discipline or industry.

Process Models and Testing:

3. Use threat modelling as well as security and safety tree methods to detect danger, risks, vulnerabilities, and flaws.
4. Establish clear and secure coding guidelines, and check and analyze code by a combination of peer previews and analysis tools.
5. Perform penetration testing, for example, grey box testing for software, firmware, hardware, protocol configuration and, if used, radio frequency (RF) to detect vulnerabilities.

Authentication/Privacy/Certification:

6. Assign unique identifier to each IoT device, for example, Electronic Serial Number (ESN) or Serialized Global Trade Item Number (SGTIN). Provide certificates for authentication and authorization and introduce a secure update process.
7. Use strong password, encrypted data and secure key material, and store the certificates in trusted stores.
8. Registration and enrollment by secure bootstrapping for initial provisioning of secure passwords, credentials, network information, etc.
9. Plan a good identity management by maintaining identity and update credentials on a regular basis.
10. Ensure confidentiality and fulfill privacy requirements by planning secure data mining and establishing compliance regulation.
11. Observe customers privacy.
    IoT devices like sensors gather a huge amount of data. These and also metadata (for example, tracking of persons via MAC addresses in wearables) can contain data that are covered by data protection regulations. So, the system must be able to distinguish between regular data and sensitive data.

Ongoing Maintenance:

12. Provide patches and updates via a secure update process.
13. Monitor hosts and networks for anomalies as well as accounts and credentials, and plan sensible account suspension (for analysis purpose) or deletion.
14. Consider the security of the physical IoT device in the field — is the location safe, is a theft easily possible, is tampering or a memory dumb possible, can an intruder update the firmware, etc.

The guideline above helps you to get started with IoT projects. It provides a fundamental understanding of what to consider in terms of security. It gives an overview of what to discuss with your IT or the service providers you are working with.

Thereby it should reduce both, your felt and your real risk regarding IoT security. By overcoming this hurdle, you can take part in the profitable market of IoT.

Interested in realizing a secure IoT solution?

Get in touch with Jens Reinelt,
Security Expert of Lemonbeat: j.reinelt@lemonbeat.com

lemonbeat GmbH

Deutsche Straße 5
44339 Dortmund

Tel.: +49 (0)231 – 586 937 0
Mail: info@lemonbeat.com
Web: www.lemonbeat.com