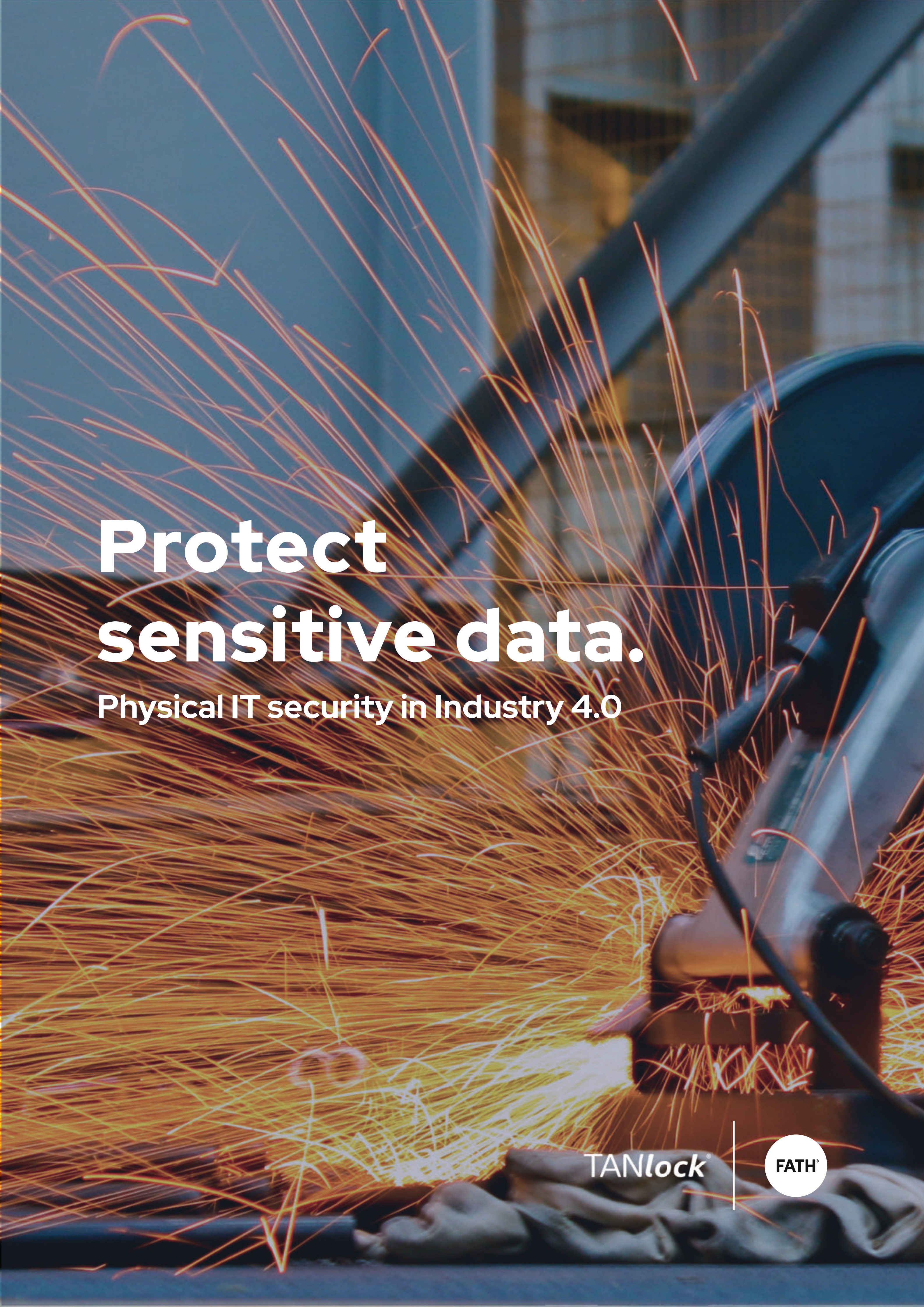


Protect sensitive data.

Physical IT security in Industry 4.0

TANlock®

FATH®

Physical IT security

Abstract

IoT in industry has a high level of acceptance in most sectors. The majority of respondents to the etventure Digital Transformation 2019 survey stated that digital technologies already play a medium to very large role in their business model. According to the survey, electrical engineering in particular is increasingly relying on digitized processes. A strong trend in this digitized direction can also be seen in other industries, such as mechanical engineering.

For this reason, physical and digital protection of data access is of great importance for various processes. Nevertheless, implementation has often been lacking up to now. Avoidable causes are still to blame for security incidents in IoT environments: from negligent handling of IT resources by employees to theft or loss of devices or media.

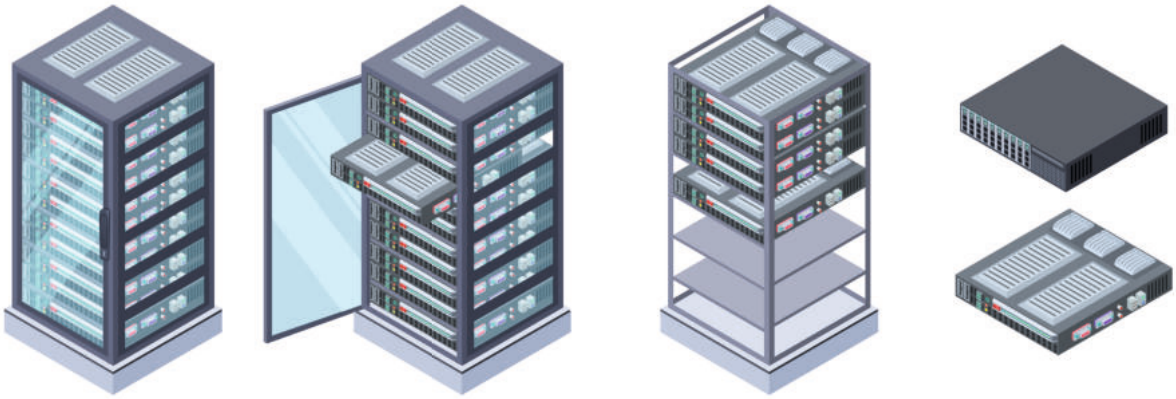
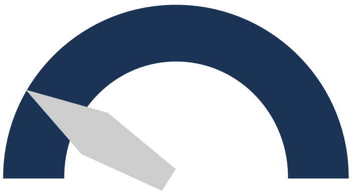


Table of contents

1. Introduction: IT security in industry 4.0 3
2. Threats for the ciritcal infrastructure 4-5
3. Aspects of IT security 6-9
4. Standards and guidelines 10-11
5. Conclusion 11

References 11

1. Introduction:
IT security in industry 4.0



18,3 % of the biggest technological challenges in the IoT use cases is security.[1]

Since the term Industrie 4.0 was coined in 2011, many of the concepts have been put into practice. We are in the midst of the fourth industrial revolution with the digitalization of the production world through the Internet of Things, new data-based business models are emerging and the networking of production facilities continues to develop. This is making companies fit for the future. Proponents of Industry 4.0 are pushing for networked and more efficient production that simultaneously strengthens competitiveness in the market.
It is merging worlds that previously had little to do with each other: Production facilities are highly networked and systems communicate with each other independently, planning systems from the cloud calculate order steps and machine assignments, plant operators monitor and control remotely, and maintenance personnel access and carry out configuration changes worldwide.

On the other hand, increasing networking also increases the vulnerability of manufacturing companies to external attacks. Cyber security in Industry 4.0 goes hand in hand with the physical protection of the IT infrastructure. The upcoming fourth industrial revolution with its strong networking right down to the automation technology on the factory floor has implications for the implementation of IT security. Particularly due to the increased communication of elements, also across companies, the implementation of the protection goals of availability, confidentiality and authenticity as well as integrity are gaining particular importance.

This white paper explores ways to improve the physical IT security of your data center by looking at data center structure, government regulations, threats, and current security standards.

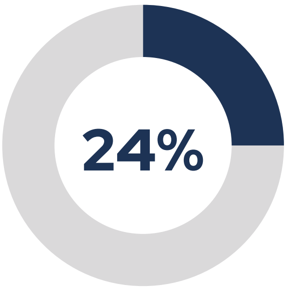
[1] Plusserver: Studie Internet of Things (2022). Page 4.

2. **Physical threats** for critical infrastructres

$4.24 Million

are the average costs of a data leak in the industry.[2]

Threats to data centers can come from outside or inside. They can therefore take the form of environmental factors such as fire, gas, smoke, water or particles such as dust. One of the most feared threats in data centers is fire, which can cause significant damage by releasing aggressive gases into the IT infrastructure. For this reason, most data center components are tested at a standard temperature curve of more than 1,100°C. Temperature sensors are a good solution to prevent servers from overheating or to stop a fire before it can spread. Dust is another physical threat. The fine particles in the air may not be noticeable at first glance, but they can cause servers to overheat and seriously damage the data center. Dust in heat sinks and fans impedes heat dissipation over time, and the tiny dirt in a data center's raised floor affects underfloor air conditioning, raising operating temperatures, reducing life expectancy and increasing failure rates. Dust can affect everything from energy efficiency to critical equipment failures by causing contact breaks in connectors. In addition, particles from clothing, cardboard, paper and other seemingly harmless sands can build up static charge and disrupt servers, causing data loss, incorrect commands, reboots and other problems.



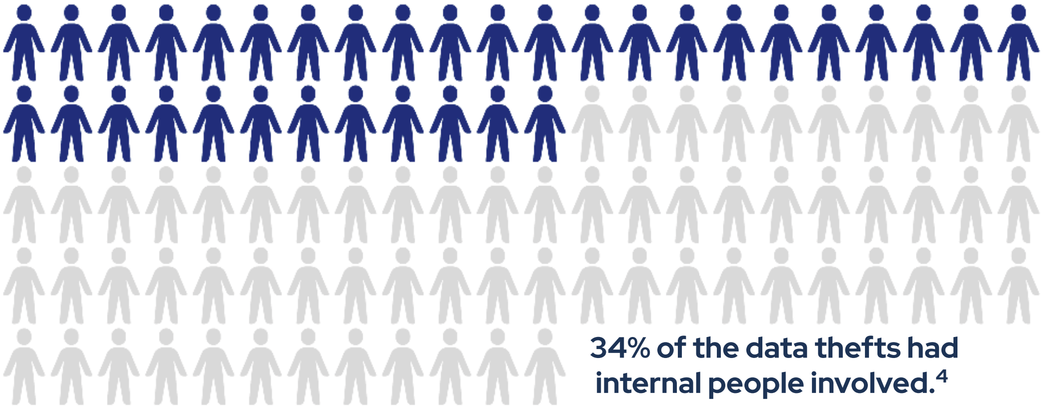
of data leaks are due to human factors.[3]

[2] IBM: Cost of a Data Breach Report 2021. Page 11.
[3] IBM: Cost of a Data Breach Report 2019. Figure 13.

The most obvious threat, however, is water. A broken water pipe or even automatic sprinkler systems in the event of smoke or fire can also damage the data center. But not all water damage in a data center, server room, production facility or warehouse has to be severe. A water intrusion often causes only a short circuit. Larger floods, however, will almost certainly cause significant data center damage.

“Human risk factor..“

While the above hazards can be minimized through the use of appropriate sensors, such as humidity, temperature, smoke, or vibration sensors, or through the use of an IP-protected rack, the risk of unauthorized access by employees or even outside individuals still exists. Therefore, considering the human risk factors, an efficient security management system that can monitor all activities is required. Normally, data centers are very well protected, as unauthorized individuals must first pass through reception, cameras and security personnel. But when, for example, employees gain unauthorized access and steal or damage data, it is not so obvious at first. With the right measures, all these dangers are avoidable

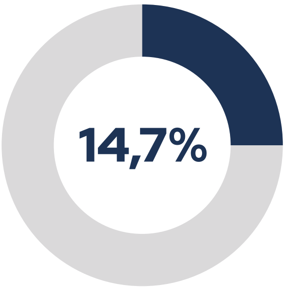


34% of the data thefts had internal people involved.[4]

[4] Verizon: 2019 Data Breach Invesitagtions Report. Figure 4.

3. Aspects of IT security

When planning a secure data center, one needs a well thought-out concept to ensure the appropriate security requirements. Building security, climate control, efficiency, scalability and incident management are all points to consider. Not only are companies and organizations obligated to secure data storage due to compliance and EU directives, there is of course an economic interest involved.



of the biggest organizational challenges in IoT use cases is the shortage of IT professionals.[5]

Building security and access control

An access control system that controls and logs every entry is a must. Only in this way can users keep track of which people were in which (server) room at what time. Biometric access systems, key cards, personal separation systems and camera surveillance have proven to be a reliable standard.

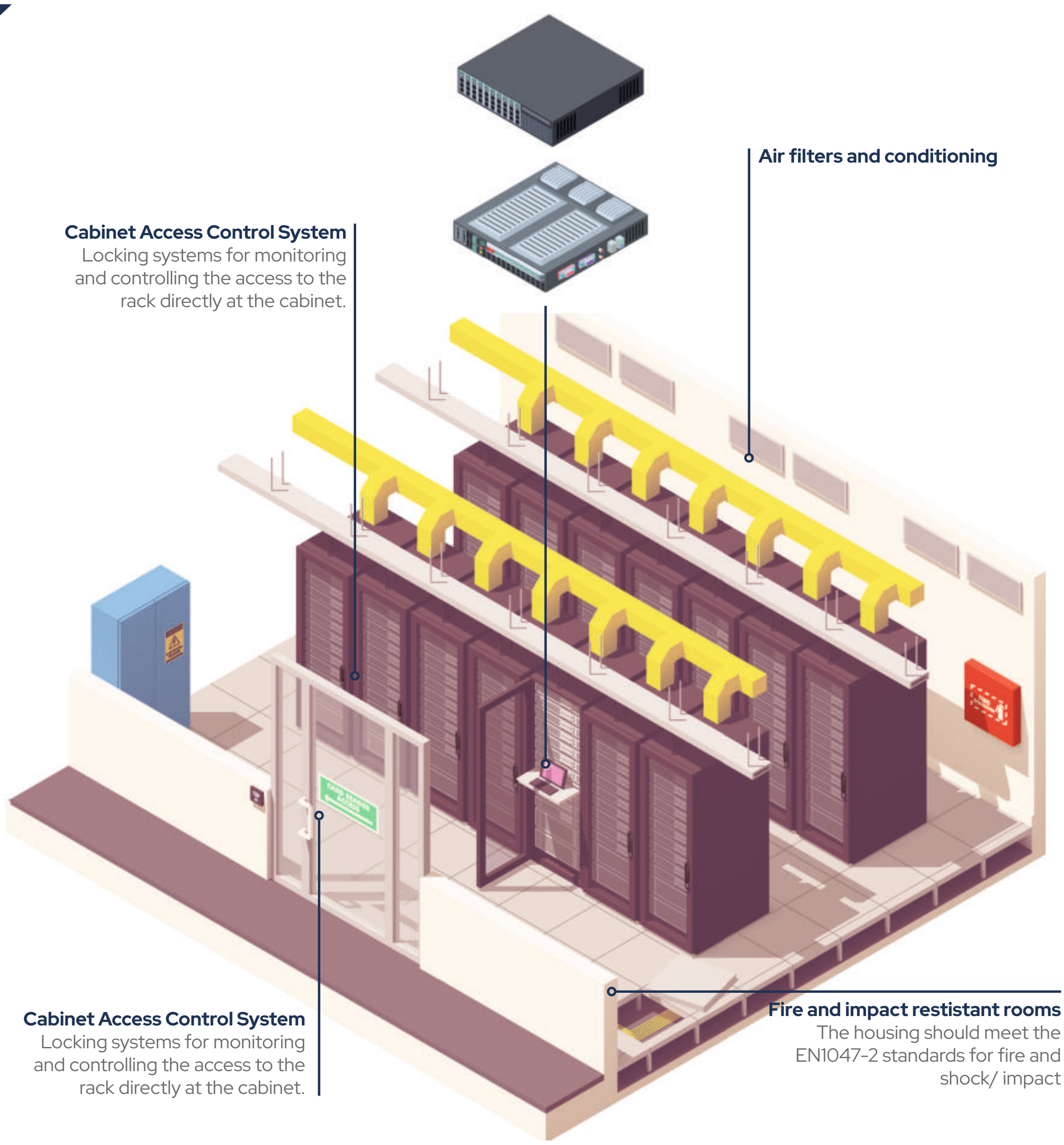
Physical security essentially consists of two components: access control and surveillance. Different devices and technologies are used in both areas. Nevertheless, it makes sense to integrate both into a unified security system.

[5] Studie Internet of things, 2019.

Access control often starts at the property boundary. Employees, customers, suppliers and other guests are granted access through the fence via an entrance gate. This is often manned by a gatekeeper or some other form of access control to verify that the appropriate people are authorized to enter the property. In this way, an initial level of protection is already established. Before entering the building, a further check is made to prevent unwanted visitors from entering. For this purpose, a door intercom is often used, but access control by smart card or smartphone is also very popular. It is usually necessary to implement further access controls inside the building – for example, to individual departments or offices. However, securing the server rooms as well as the server cabinets should not be neglected either. These are one of the places most worthy of protection, as all data is processed and stored there. Therefore, it is also a must to implement an appropriate access control system there.

Securing the server room

This is a very important aspect. Access to as many server rooms as possible should be restricted. This is best done through an access control system. Don't forget access points such as windows, intermediate doors, ventilation shafts and balconies to various rooms. If an attacker can access your servers through an open window, this needs to be changed as soon as possible. Edge data centers, IoT gateways and other systems at the network perimeter must be comprehensively protected from risks such as fire, overheating or moisture. But it's not just protecting the space itself that's important. For additional security, a control system must be implemented directly at the server rack. This is a fundamental step in securing the infrastructure. Today, every second IT failure is due to physical causes. It is not only important to monitor permanently – critical conditions must also trigger automatic alarms in real time. In addition, all information should be integrated into a central monitoring system. Healthcare facilities should therefore not lose sight of the issue of physical security.



Cabinet Access Control System
Locking systems for monitoring and controlling the access to the rack directly at the cabinet.

Air filters and conditioning

Cabinet Access Control System
Locking systems for monitoring and controlling the access to the rack directly at the cabinet.

Fire and impact restistant rooms
The housing should meet the EN1047-2 standards for fire and shock/ impact

Basic IT protection

With the current crises, such as the Corona pandemic, we have developed a sense of the consequences that the shortage of resources can have. So-called critical infrastructures (CRITIS) exist to prevent equipment and systems from failing, which would lead to lasting supply bottlenecks or even endanger public safety. They make, for example, the IT-Grundschutzkompendium, IEC 62443 or the IT Security Act with strict specifications on how security concepts are to be systematically applied. For automated production, data and change management is becoming increasingly important, because it allows many of these requirements to be implemented with often relative ease.

Fire protection

The events in Strasbourg at OVHcloud have shown it: Fires in data centers can lead to economic consequences for companies that threaten their existence. For this reason, there are now early detection systems that permanently check the air in the data center and sound the alarm at even a low level of soot particles.

When it comes to fire protection, the division into different fire compartments is also elementary, and fire doors, walls and windows are a must. But it is also important to know, for example, whether degassing, ventilation and pressure relief systems are in place and whether systems can continue to operate after a fire.

Uninterruptible power supply

This has long been standard for business-critical components. But the entire data center must meet this safety criterion just as well. Therefore, it should be asked whether it is possible to maintain uninterrupted business operations independent of the public power grid and how long these redundant systems can run under the full load that is then required. In addition: Are there lightning protection devices and galvanic isolation of the lines?

Cooling and humidity

Air conditioning plays an important role in view of the heat emitted by IT equipment, which is why it should also be upgraded several times. It can be a major challenge to keep temperature and humidity within the ideal range. When planning, excess capacity must also be factored into air conditioning, especially as IT equipment changes more quickly and consumes increasing amounts of energy.

Network connection

As a component for external data exchange, a reliable network connection is essential. This means, for example, providing an additional connection through a second network operator, or emergency plans with directional radio or satellite.

4. Standards and Guidelines

For all the above security measures, the following data regulations must be complied with. The standards are not mandatory, but ensure a competitive advantage.

BSI: IT Security Act 2.0

The Security Act 2.0 of the German Federal Office for Information Security (BSI) has come into force for all critical infrastructure sectors (CRITIS). It states that affected companies must have an information security management system (ISMS) in accordance with ISO/IEC 27001.

Operators of critical infrastructures are required to implement systems for attack detection. In future, reporting obligations will also apply to companies that are of particular public interest, such as companies in the defense industry and classified IT, companies that are of particular economic importance due to their high value added, and companies that are subject to regulation under the Major Accidents Ordinance. The draft contains a provision prohibiting the use of critical components for which certification is mandatory.

ISMS

The Information Security Management System (ISMS) defines the controls that an organization must implement to ensure that it meaningfully protects the confidentiality, availability, and integrity of assets from threats and vulnerabilities. At the core of the ISMS is information risk management, a process that involves assessing the risks an organization must deal with in managing and protecting assets and communicating the risks to all appropriate stakeholders. As part of information security management, an organization can implement an ISMS and other best practices included in the ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27035 information security standards.

International Organization for Standardization (ISO)

The ISO 2700 family is generally the best known standard for IT security in collocation centers. It is a standard for managing the security of confidential information and data. ISO/IEC 27001:2013 is specifically for IT security management systems. A large part of implementing ISO 27001 in the data center is following organizational rules to minimize security breaches for both the organization itself and its customers. All eleven sections must be implemented without expectation in order for a company to receive the seal of approval.

Data Protection Regulation (GDPR)

The GDPR (General Data Protection Regulation) is the European data protection and security law that came into effect in 2018. All organizations doing business in Europe must comply with the GDPR. Therefore, access to all personal data, both electronic and physical, must be inaccessible to unauthorized persons. The maximum fine for non-compliance is either up to €20 million or 4 percent of annual turnover, whichever is greater.

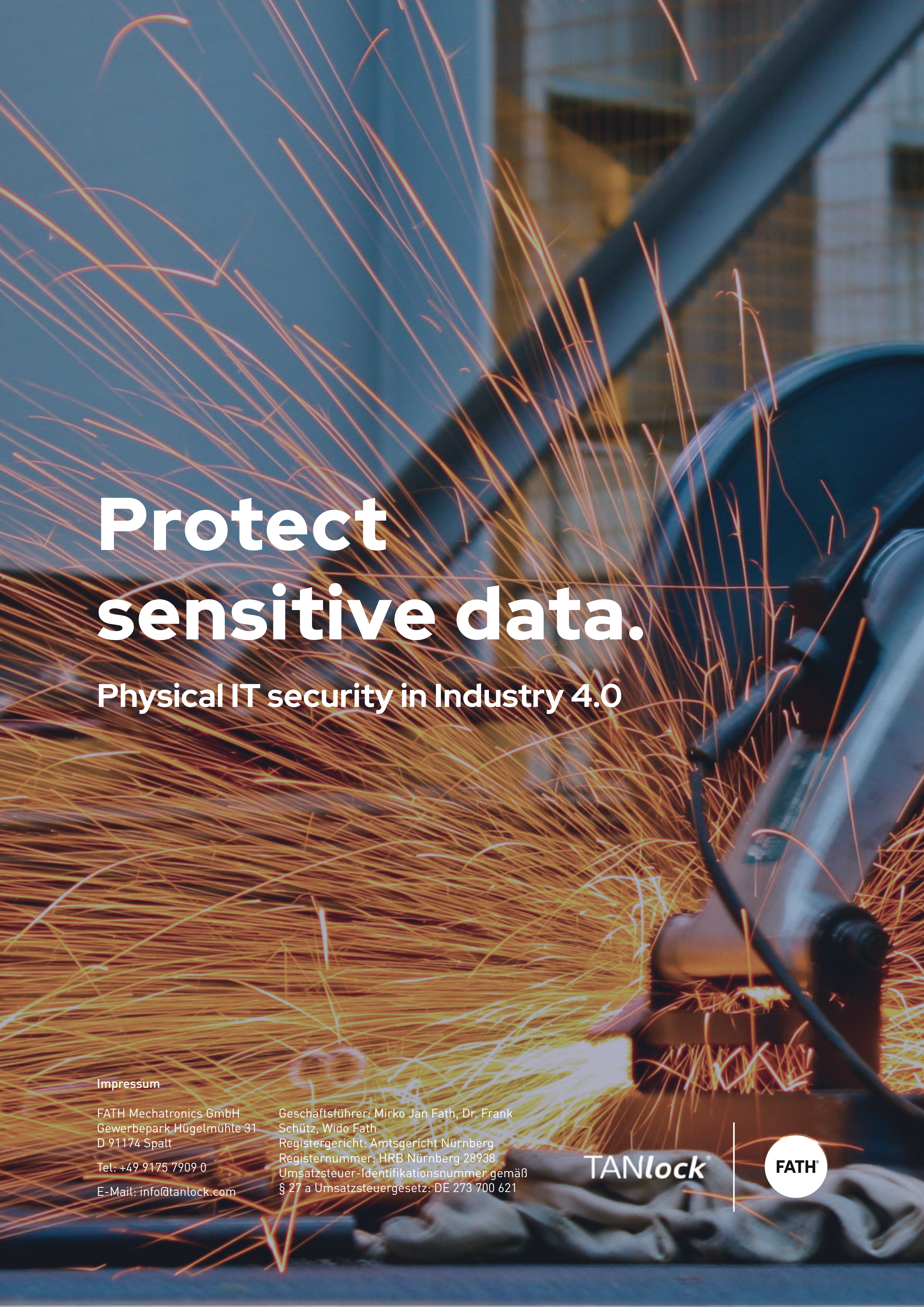
5. Conclusion

While digitalization in Industry 4.0 brings a lot of benefits, it also poses dangers. This is why strict security measures must be taken in this area in particular, in order to rule out any interference with production and also the supply chain. After all, these supply chains are now also considered critical infrastructures.

References

1 Plusserver: Studie Internet of Things, 2022. Page 4.
2 IBM: Cost of a Data Breach Report, 2021. Page 11
3 IBM: Cost of a Data Breach Report, 2019. Figure 13
4 Verizon: 2019 Data Breach Invesitagtions Report. Figure 4
5 Studie Internet of things, 2019.

Images: All rights reserved by Adobe Stock and FATH Mechatronics GmbH.



Protect sensitive data.

Physical IT security in Industry 4.0

Impressum

FATH Mechatronics GmbH
Gewerbepark Hügelmühle 31
D 91174 Spalt

Tel: +49 9175 7909 0

E-Mail: info@tanlock.com

Geschäftsführer: Mirko Jan Fath, Dr. Frank Schütz, Wido Fath
Registergericht: Amtsgericht Nürnberg
Registernummer: HRB Nürnberg 28938
Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE 273 700 621