Protect sensitive data.

The importance of physical IT security

TANlock®

FATH®

Physical security

Executive summary

As businesses become more dependent on the internet of things (IoT), so does the need for digital and physical security. IoT demands a significant amount of physical security to safeguard data, servers and networks. Physical security is defined as the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. Unrestricted physical access to a computer or a network is immediately a security threat. As more and more critical data is digital, so securing the hardware in data centers is just as important as the digital safety.

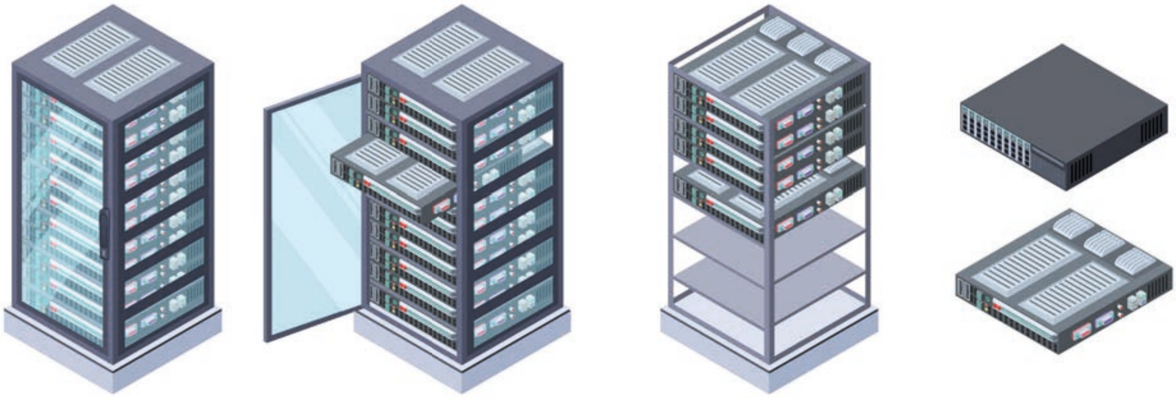


Table of contents

1. Introduction: The importance of physical IT security

15% of data breaches were Misuse by authorized users. [1]

Physical IT security is an important part of any IT safety management system. Unrestricted physical access to a computer or a network is immediately a security risk. If a hacker has physical access to your rack, stealing information is easy. Due to the Covid-19 pandemic, the demand for cloud storage increased enormously. Therefore, more and more critical data is digital, so securing the hardware in data centers is just as important as digital safety. If someone has physical access to a rack, it can easily be damaged, or data could get stolen. Securing this vulnerability of the network is fundamental for general server safety as well as the guaranteed data protection. Although it can be as easy as installing a lock, the digital century requires monitoring and controlling. Not only unauthorized access can be harmful, but also the staff inside your building. This is where monitoring comes into play. Unauthorized access to the rack can be prevented, logged in case of abuse and your management system can be notified.

This white paper explores ways to improve the physical IT Security of your data center by looking at the structure of data centers, official regulations, threats as well as current safety standards.

[1] Verizon: 2019 Data Breach Investigations Report. Figure 3.

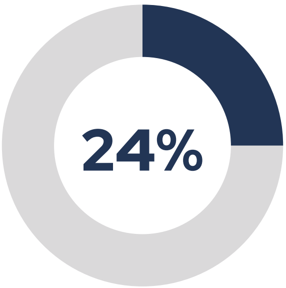
2. Physical threats to the infrastructure

$4.24 million

is the global average cost of a data breach.[2]

Threats to colocation centers might be internal or come from the outside. Therefore, they can be in form of environmental factors such as fire, gas, smoke, water, or particles like dust. One of the most dreaded threats in data centers is fire, which can cause significant damage by releasing aggressive gas into the IT infrastructure. That is the reason why most components in data processing centers are tested at a standard temperature curve at more than 1.100° C. Temperature sensors are a good solution for preventing server overheating or stopping a fire before it can start to spread.

Dust is another physical threat. Those fine dust particles called airborne may not be seen at first, but they might cause the servers to overheat, causing serious damage to the data center. Dust in heat sinks and fans obstructs heat dissipation over time, and dust on the raised floor of a data center affects the underfloor air conditioning system, raising operating temperatures, lowering life expectancy, and increasing failure rate. It can have an impact on everything from energy efficiency to critical equipment failure by causing contact interruption in connectors. Furthermore, particles from clothing, cardboard, paper, and other seemingly innocuous sands can become statically charged and interfere with servers, resulting in data loss, incorrect commands, restarts, and other issues.



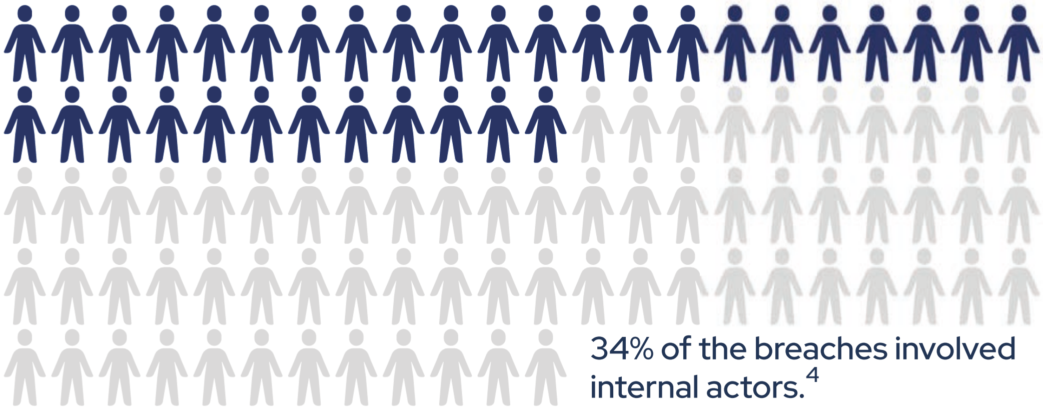
of data breach rooot causes are due to human error.[3]

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

The more obvious menace is water. A broken water pipe, but also automatic water sprinklers in case of smoke or fire could potentially damage the computing center as well. However, not every water damage in a data center, server room, manufacturing facility, or warehouse has to be serious. Water intrusion frequently causes only a short circuit. Larger floods will almost certainly cause significant damage to the computing center.

“Human risk factor..“

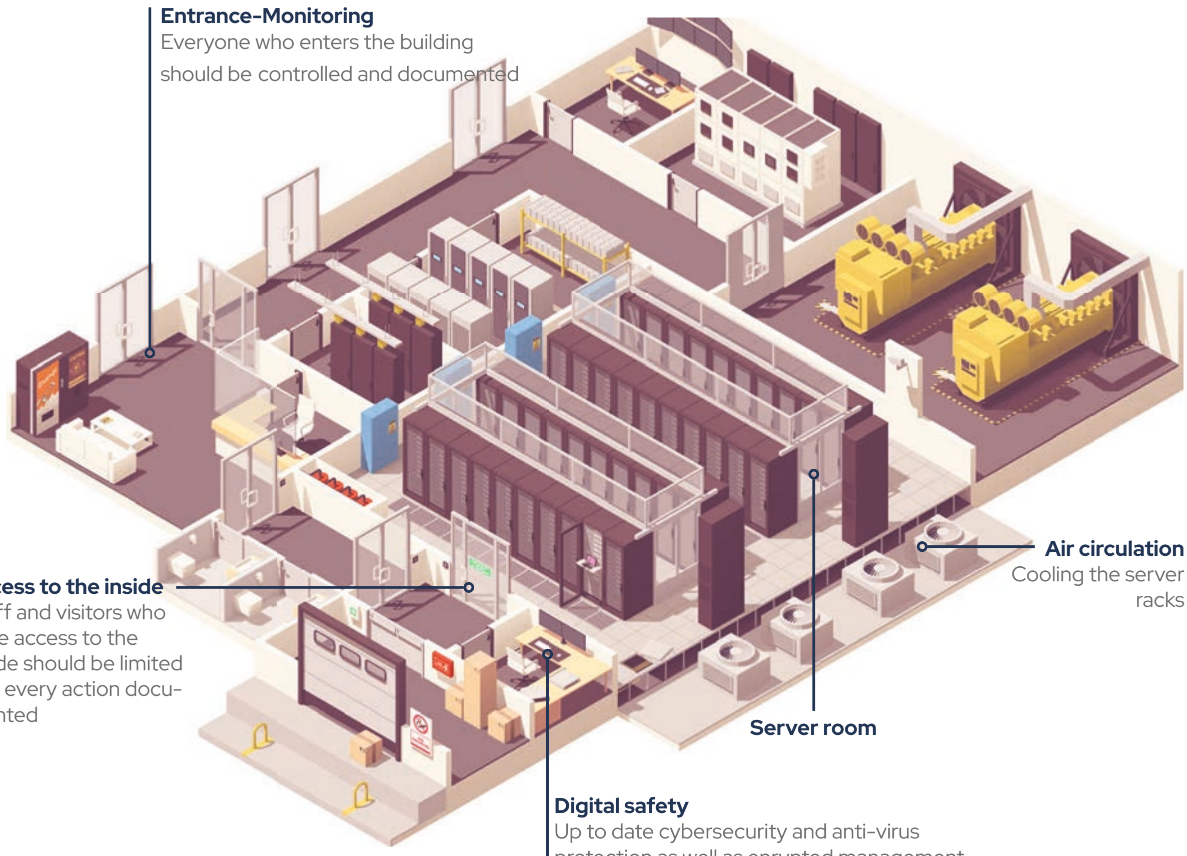
While the threats above can be minimized by using according sensors, like humidity-, temperature-, smoke detection- or vibration sensors, or by using an IP-proof rack, the risk of employees or even external persons having unauthorized access is still present. Therefore, given the human risk factors, the need of an efficient security management system which can monitor any activity is necessary. Usually, data centers are very well protected, as the intruders need to pass the reception, cameras, and security personal first. But for example, employees obtaining unpermitted access and stealing or damaging data is not as obvious at first. With the right measures, all of these threats are avoidable.



34% of the breaches involved internal actors.[4]

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

3. The structure of a data center + current safety standards


Entrance-Monitoring
Everyone who enters the building should be controlled and documented

Access to the inside
Staff and visitors who have access to the inside should be limited and every action documented

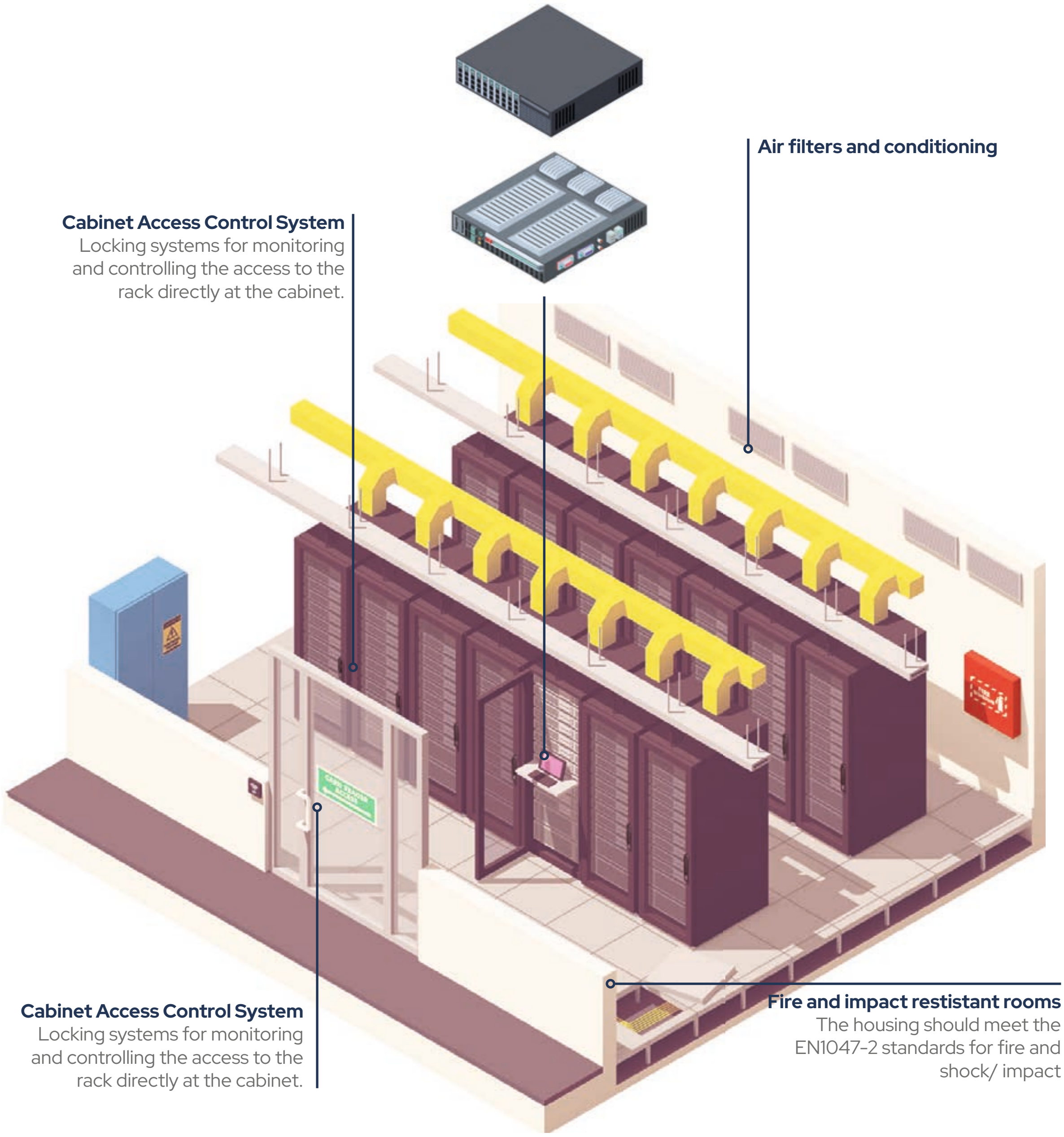
Air circulation
Cooling the server racks

Server room

Digital safety
Up to date cybersecurity and anti-virus protection as well as enrypted management software secure the digital infrastructure

Data centers require security in multiple areas. These include the access to the building itself, to the server room as well as to the cabinets. They are supposed to be monitored, as well as the access to the inside. Staff and visitors should be limited, and every action controlled and documented. Air is being circulated to cool off the racks. Furthermore, a ferromagnetic detection system could keep smartphones or SD cards out of the server room. Access control manages the locks to the server rooms, so that authorized staff can enter. These need to be monitored. But most importantly, the cabinet itself also needs extra protection. Besides that, firewalls or encrypted management software ensure the digital safety.

The access control directly at the server cabinet is essential. In the event of a security breach, most organizations would want to know who had access to the server and when. With an access control system at the door to the server room and server rack itself, organizations have control over who can access data, as well as a complete history of access. Access control systems, like the TANlock, ensure that only authorized staff is able to unlock the server cabinet, whilst also monitoring any activity. Also, the walls of data storage rooms should meet the EN 1047-2 standards for fire and shock/ impact resistance. With all these measures taken into account, the data center meets the basic requirements for safe hardware.



Air filters and conditioning

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

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

4. Ways to secure your critical infrastructure

You can secure your infrastructure by managing who has access to the data center through multi-level security systems, query of biometric characteristics for unique recognition or documentation of the entry and exit of persons. Is the building secured and monitored? The combination of on-site security personnel and camera monitoring of all critical and important indoor and outdoor areas with subsequent long-term archiving of the image data has proven itself in practice and can be helpful to secure your critical infrastructure. Not to forget the Burglar-proof doors, windows and burglar alarm systems.

Can unauthorized access to your technology inside the data center, or even to the server rack directly, by other customers of the data center provider, among others, be avoided? If not, a locking system at the door and the server rack itself is neccesary.

Nonetheless, there should be an additional camera or separate access systems and motion detectors to ensure the safety. Sensitive leakage systems in the data center core that detect entering water can prevent water damage. Also very useful is dividing the data center into different fire compartments, room-in-room solutions, fire walls and state-of-the-art fire suppression systems.

Fire doors and windows, fire compartmentation of pathways and fire safety regulations can prevent or at least reduce the damage of fires.

Regarding fires, you should also be asking yourself these questions:

Do hand-held fire extinguishers exist and is there an early fire detection system? How are the security and the fire department informed internally? Sensors and detectors that react to temperature increases as well as to smoke and smoldering gases which are installed in the raised floor can act as an early warning system. In case of fire, is extinguishing gas used that does not harm the technology? Degassing, ventilation and pressure relief systems should be in place as well.

In other words, can IT operations be maintained if a section or room is on fire? All of these ways to secure the data center are basic safety measurements.

There are additional products for incereased security. If your infrastructure meets all of the basics, you could look at optional measures.

5. Official regulations and norms

For all the above-mentioned security measures, the following data regulations have to be complied with. The norms are not mandatory, yet they ensure competitive advantage and safety.

General Data Protection Regulation (GDPR)

The GDPR is Europé s data privacy and security law, which came into force in 2018. It mandates, that all organizations who conduct business in Europe must comply with the data protection regulation. Therefore, all personal data, both electronic and physical, must be unavailable to unauthorized persons. This means access to private data must be limited. The maximum fine for contravention is either up to 20 million Euros or 4 percent of the annual turnover, whichever is higher.

Resistance Class (RC)

The norm RC uses a six-level classification system to determine the skills of the perpetrator. The spectrum ranges from an inexperienced perpetrator/vandal without tools to an experienced, highly motivated perpetrator who has a whole range of powerful power tools at his disposal.

International Organization for Standardization (ISO)

The ISO 2700 family, in general, is the best-known standard for IT security in colocation centers. It’s a standard for managing the security of confidential information and details. ISO/IEC 27001:2013 is specifically for IT security management systems. A large part of implementing ISO 27001 in the data center boils down to following organizational rules to minimize security vulnerabilities for both the company itself and its customers. All eleven sections must be implemented without expectations for a company to receive the seal of approval.

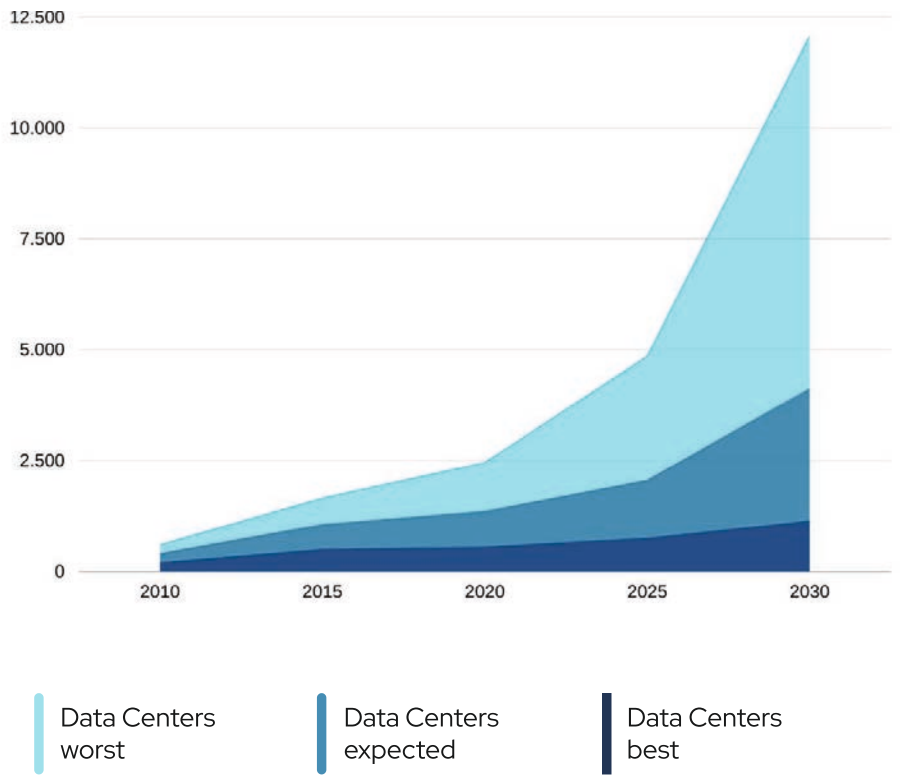
Leadership in Energy and Environmental Design (LEED)

LEED was developed by the U.S. Green Building Council – it is a set of rating systems for the design, construction, operation and maintenance of green buildings. LEED has developed a certification for sustainable design and construction of data centers. Less than five percent of all U.S. data centers have LEED certification. However, it is becoming a lot more relevant for the future of a sustainable data center.

6. Outlook for the future

Data centers are with an estimated consumption of 200 terawatt hours (TWh) each year among the highest consumers of power today. But with the internet of things, growing big data and expanding connectivity, the need for more and more of these facilities is inevitable. Data center sustainability is becoming a priority. For example, low-impact, direct liquid-cooling systems are now being used to limit the active movement of air over the servers – eliminating the need to cool the entire data hall and reducing energy consumption and cost. for the safety standards as well as the efficiency, modular data centers might be a good solution. More data centers are also replacing wasteful, traditional water evaporation cooling systems with innovative closed-loop systems, which utilize recycled water rather than fresh in order to reduce the burden on local water systems.

Electricity usage (TWh) of Data Centers 2010-2030 [5]



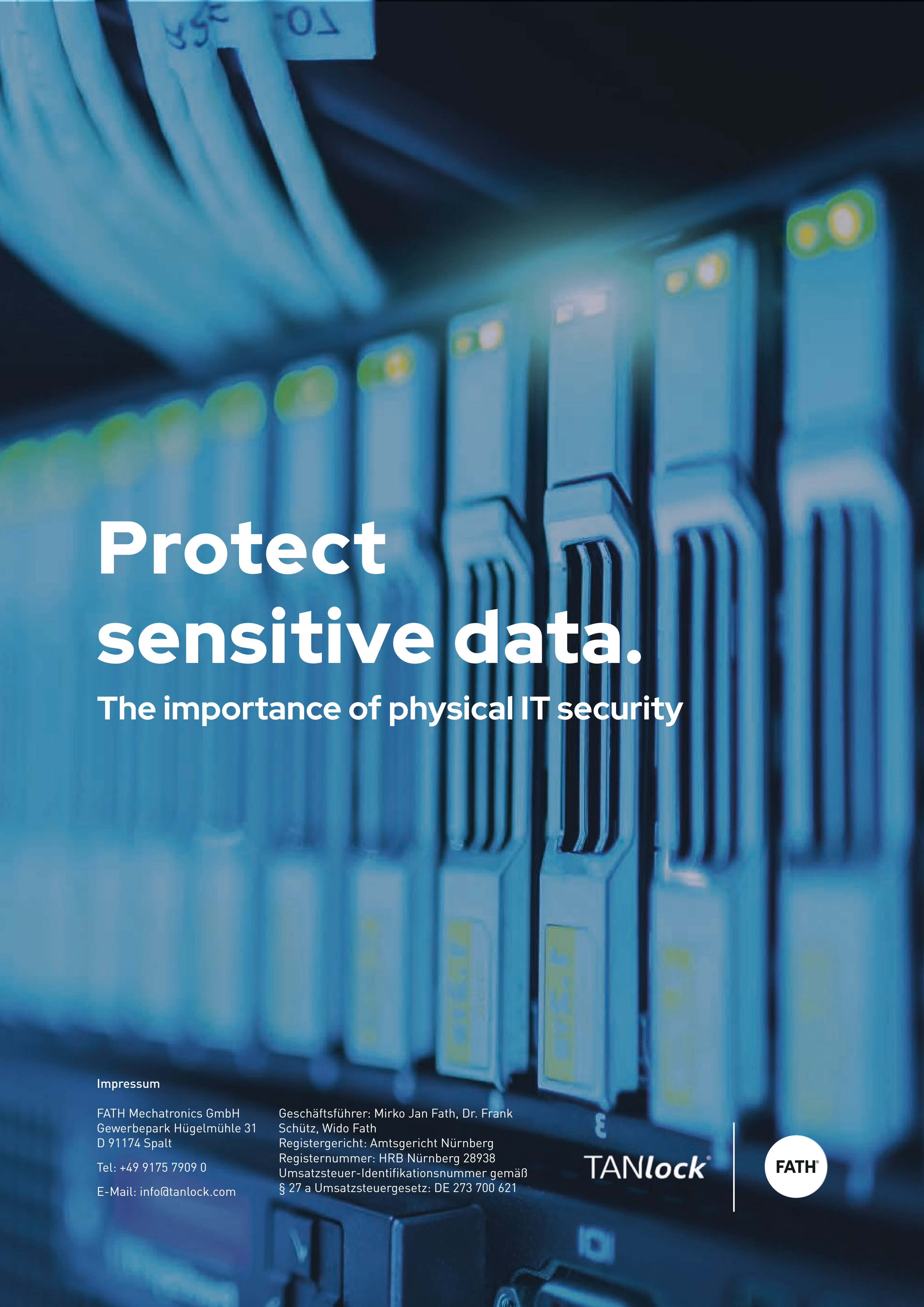
[5] Andrae, A. & Edler, T. Challenges 6, 117–157 (2015). Figure 4.

However, not only the power supply can be designed sustainably. Europe alone generated 12 million tons of electric waste in 2019, including components from data centers. This waste can easily be reduced by either reusing certain parts of the collocation center or switching out the broken parts only. More and more data centers are now much more modularly planned and built, as it is far more sustainable. The main reason for this sustainability of modular infrastructure components is that it creates significantly less e-waste to replace modules or small parts rather than the component itself. It simplifies the repairing of the electronic waste instead of replacing the whole piece. Another plus is that it is easier to obtain the latest security standards while only switching out smaller parts instead of immediately replacing the whole component. As our future depends on sustainable decisions to protect the environment and lower CO2- Emissions, a lot more of these as well as other solutions will be implemented. Future goals are to better the power efficiency and extend the lifespan of the products.

References

1 Verizon: 2019 Data Breach Investigations Report. Figure 3
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 Andrae, A. & Edler, T. Challenges 6, 117–157 (2015). Figure 4.

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



Protect sensitive data.

The importance of physical IT security

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