Effective Monitoring of Physical Dangers to Service and Technical Rooms in Local and State Government Offices

Author: Joern Wehle, Kentix GmbH

Summary

Because of the physical effects of fire, water or power as well as misuse and deliberate attacks, serious damage can occur in local and state government offices.

In compliance with the IT-basic protection requirement and the increased IT availability, it can be viewed as negligence not to secure the physical risks with IT-specific Systems. Especially, in view of the manageable investment costs, an integrated system solution today is a surety for all size enterprises.

Implementation of IT-basic protection and compliance requirements of ISO 2700X

Today, the requirements for the monitoring of critical infrastructures must be in accordance with very strict standards. Compliance plays the central role. Within the context of security risks, terms and defensive strategies are often against attacks on local and state government networks from outside by malicious program codes in the form of viruses or Trojans, or even unauthorized access to information or systems. The risk of elemental dangers, such as fire, flooding and overheating, access by unauthorized persons or even sabotage is being often neglected. 7 out of 10 authorities today have no comprehensive baseline protection in the critical infrastructure units.

Modern technologies today allow easy and complete monitoring of server rooms and branched infrastructure units. In the foreground is central monitoring with the possibility to also send network redundant alerts to the appropriate receivers. The low costs for these systems combined with a simple plug'n play installation significantly increase IT-security and point to a very good cost/use ratio.

Physical threats of IT and infrastructure units in companies
There are basically two groups. The digital threat in the area of IT-software and networks, and the physical threat to server rooms, data center, as well as critical infrastructure units.

Digital Threats
Digital threats include, e.g. viruses, Trojans, hackers who attack data security. Media publicizes these attacks and attracts public attention. Because of this, great attention is being paid by those responsible for IT for comprehensive preventive measures; e.g. use of antiviral programs or a fire wall are common. Protection against digital danger shall no longer be discussed here.

Physical Dangers
Cooling problems, power outage, access of unauthorized persons, fire, leaks are all part of the physical dangers for IT and technical equipment. Current systems already partially monitor such risks. Fire alarm centers are being used by appropriate manufacturing plants. The quality of the power is frequently measured via the USV-System. Air-conditioning systems measure the in- and outlet temperature in server rooms. Thus, it provides a certain basic prevention in the most serviceable rooms. However, in many instances, it does not provide for an IT-specific design and an integrated representation of these hazardous sectors.

Modern monitoring systems secure against the elemental dangers with integrated sensors and thereby capture all important parameters in one system.

- Air – Room temperature
- Humidity
- Dew Point
- Motion detection (intruder)
- Sabotage and vandalism
- Fire, i.e. smoke detection
- Leakage and flooding

Legal basis and guidelines for authorities (ISO 27001)

Against the background of audits by authorities, certain standards must be met. The BSI Standard (German Federal Agency for security and technical information) 100-1 of the IT basic protection defines the requirements of an ISMS (management system for information security). This is fully compatible with ISO 27001. Recommendations of the ISO 27000 standard (specifically 270002, prior ISO 17799) are being taken into consideration. ISO 27001 provides only a generic description of the necessary procedures for the introduction of a management system. ISO 27002 is much more defined. The implementation of security mechanisms will be explicitly taken into account with the aid to protect all values in the value chain. Out of the 11 monitoring areas, two can be clearly associated with the physical threats.

- **Physical Security: Intrusion and access, climate and air-conditioning, fire/water, power**
- **Control of Information Technology access: physical protection, network, systems, applications, functions, data**

Thus, the implementation of ISO 2700x demonstrates a central factor against the defense of physical dangers.

Optimal basic protection requires IT-specific systems.

Theft, technical damage or disturbance of the operating environment: These are the largest physical risks which daily threaten the data and IT-infrastructure in server rooms. In order to guaranty effective protection, it is necessary that several physical prevention mechanisms work together as a unit. The following is a detailed listing of the most important physical sensors and components that ensure this overall protection.

- To secure the server room from theft, sabotage and unauthorized access, a motion detector is necessary that alerts to burglary. It is most important to use a specialized motion detector which is sensitive to the various temperature zones and equipment temperature in an IT room to avoid provoking a false alarm. Ideal are detectors based on radar technology or specialized Passive Infrared detector (PIR) with temperature compensation.

- If the room gets too hot, the temperature rises too rapidly or temperature fluctuations are too high, this shortens the life of the technical equipment, or it could lead to the server being shut down. This needs a temperature sensor which protects by monitoring the room temperature and the functioning of the heating and cooling systems.

- To avoid technical damage and server outage because of water condensation, humidity as well as dew point can be monitored. To spot water on the floor of the server room, the use of a leakage-sensor is recommended.

- To detect fire you need a fire detector – ideally a carbon monoxide sensor, with a practical release point between 20 and 200 ppm. A finer adjustment provides or an early detection of the danger.

- The external network power supply should also be monitored. Power outages must be reported and in an ideal situation immediately bridged. In case of a power outage, the system should have an emergency power supply to ensure functioning of the alarm per GSM. Without any power, there is no LAN and no e-mail notification possible. This redundancy in transmission significantly increases safety.

- In order to detect errors in the operating environment early, climate data such as humidity, room temperature and voltage fluctuations should be collected and evaluated in addition to the actual monitoring. Because of the real time-monitoring of the operating parameters in the server room, some potential dangers can be recognized early on and prevented.

Modern Monitoring Solutions are cross-linked and signal disruptions in real time

In case of a disruption or alarm, the inserted components send messages to a central system unit – the alarm manager. It is here that all information of the sensors is collected and evaluated. Since the server rooms to be secured in practice usually are completely equipped (and the sensors so to speak are to be installed during operation), there is no need for a signal transmission using wire: this is expensive, it would entail knocking out walls and laying wire. An effective network of sensors and the alarm manager is done server in rooms per LAN or radio (z.B. ZigBee). Should one of the sensors detect a theft or technical damage, the information gets to the alarm manager in real time, which will react accordingly depending on the type of alarm.

External alarm devices such as sirens and flashlights can be controlled via signal outputs, for example. These bring a lot of attention, but there is no guarantee that in case of alarm the proper personnel are being notified early enough. To make this possible, an additional silent alarm system should be installed in any case, which would notify selected personnel.

The silent alarm is via SMS, email, SNMP, or telephone call and can be adjusted individually - depending on the type of alarm. Furthermore, it is possible by using switches to activate additional uses, for example, an external light which increases security. An effective interplay and a functional network of all the components are necessary to protect the server room from central dangers and to react correctly in case of alarm.

Multi-sensor systems merge all important sensors in one device

In classical danger signal systems, a separate sensor is responsible for recognizing each of the dangers mentioned. To secure a server room, a technician must install and program various components in different locations. A complete monitoring concept in accordance with the philosophy “all out of one hand” , however, is not achievable, since most of these systems although warning of any danger cannot collect and evaluate the decisive climate data of the operation environment (e.g. humidity, room temperature and voltage fluctuations).

Here lies the strength of a multi sensor-system for IT and Server Rooms. In this All-in-One-Solution all physical sensors, matched to protect server rooms, are integrated in a compact housing. It is possible to integrate third-party components into the monitoring system, but not necessary to effectively protect the server room. The multi-sensor protects from dangers and collects relevant climate data, the alarm manager evaluates, documents, and alarms – even the multi-sensor housing contains a signal. A multi-sensor solution thus is all: climate-, fire- and intrusion panel – a complete package for the physical security for these serviceable rooms.

Comparison of possible costs as a result of negligence in securing against physical dangers and the costs to invest in an integrated multi-sensor technology

Potential costs in case of the above-described physical risks
Considerable costs to replace computer hardware and software for damage sustained in server room and Datacenter. Additional costs due to loss of productivity as a result, e.g. the server being down due to overheating. It could also have an impact on the image of the enterprise in the public's view.

The investment for the purchase, installation and start-up operations for a system to monitor and protect IT-Infrastructure units is less than $1,000.

Conclusion
In compliance with the IT-basic protection requirement and the increased IT availability, it can be viewed as negligence not to secure the physical risks with IT-specific Systems, especially considering the manageable investment costs.