Überwachung von physikalischen Gefahren in Server- und Technikräumen in Behörden

Autor: Jörn Wehle, Kentix GmbH

Zusammenfassung

Durch physische Einwirkung von Feuer, Wasser oder Strom sowie Fehlbedienung und mutwillige Angriffe können gravierende Schäden für eine Behörde entstehen.
Im Sinne der Erfüllung der IT-Grundschutzanforderungen und der Erhöhung der IT-Verfügbarkeit kann es als fahrlässig angesehen werden, die physikalischen Risiken nicht bzw. nicht durch IT-spezifische Überwachungssysteme abzusichern. Insbesondere vor dem Hintergrund der überschaubaren Investitionskosten.

Umsetzung des IT-Grundschutzes und Anforderungen der ISO 2700X

Die Anforderungen an die Überwachung von kritischen Infrastrukturen müssen heute sehr strengen Normen entsprechen. Dabei spielt das Thema „Compliance“ die zentrale Rolle. Im Rahmen dieser Sicherheitsrisiken werden oft Begriffe und Abwehrstrategien gegen Angriffe auf Behördennetze von außerhalb, bösartigen Programmcode etwa in Form von Viren oder Trojanern oder auch den unautorisierten Zugriff auf Informationen oder Systeme verstanden. Dabei wird oft Risiko durch elementare Gefahren wie Brand, Wassereinbruch und Überhitzung, Zutritt von Unbefugten oder auch Sabotage vernachlässigt. 7 von 10 Behörden haben heute keinen umfassenden Grundschutz in den kritischen Infrastruktureinheiten*.

Moderen Technologien ermöglichen heute eine einfache und komplette Überwachung von Serverräumen und z.B. verzweigten Infrastruktureinheiten. Dabei steht die zentrale Überwachung im Vordergrund mit der Möglichkeit auch netzwerkredundant Warnungen an die entsprechenden Empfänger zu versenden. Die sehr geringen Kosten für diese Systeme, verbunden mit einfacher plug‘n play Installation steigern die IT-Sicherheit signifikant und weisen ein sehr gutes Kosten-/ Nutzenverhältnis auf.

Physikalische Bedrohungen der IT und Infrastruktureinheiten in Behörden

Grundsätzlich können zwei Gruppen unterschieden werden. Die digitalen Bedrohungen für den Bereich IT-Software und Netzwerke und die physikalischen Gefahren für Serverräume, Datacenter sowie kritische Infrastruktureinheiten.

Digitale Gefahren
Zu den digitalen Bedrohungen gehören z.B. Viren, Trojaner, Hacker die einen Angriff auf die Datensicherheit bedeuten. Diese Angriffe finden meist sehr große Aufmerksamkeit in den Medien. Im Bereich der digitalen Gefahren wird heute bereits von den IT-Verantwortlichen entsprechende Vorsorge geleistet. Z.B. ist der Einsatz eines Anti-Virenprogrammes oder einer Firewall selbstverständlich. Der Schutz gegen digitale Gefahren soll hier nicht vertieft werden.

Physikalische Gefahren
Zu den physikalischen Gefahren für IT- und Technikgeräten zählen Kühlprobleme, Ausfall der Spannungsversorgung, Zutritt von Unbefugten, Brände, Leckagen. Teilweise werden diese Risiken durch bereits vorhanden Systeme überwacht. So verfügen entsprechende Gewerberäume über eine Brandmeldezentrale. Die Stromqualität wird häufig über das USV-System gemessen. Klimaanlagen messen die Ein- und Austrittstemperatur in Serverräumen. Insofern gibt es eine gewisse Grundabsicherung in den meisten sensiblen Räumen. Eine IT-spezifische-Auslegung sowie eine integrierte Darstellung dieser Gefahrensektoren ist jedoch in vielen Fällen nicht gegeben.

Moderne Überwachungssysteme sichern mit integrierten Sensoren gegen die elementaren Gefahren und erfassen dabei alle wichtigen Parameter in einem System.

- Luft-Raumtemperatur
- Luftfeuchte
- Taupunkt
- Zutritt durch Unbefugten
- Sabotage und Vandalismus
- Rauch bzw. Feuer
- Leckage und Wassereinbruch

Gesetzlich Grundlagen und Richtlinien für Behörden (ISO 27001)

Vor dem Hintergrund der Auditierung von Behörden müssen bestimmte Standards erfüllt werden. Im Standard BSI (Bundesamt für Sicherheit und Informationstechnik) 100-1 des IT-Grundschutzes werden Anforderungen an ein ISMS (Managementsystem für Informationssicherheit) definiert, dieser ist voll kompatibel zur ISO 27001. Empfehlungen der Standardfamilie ISO 27000 (speziell 27002 vormals ISO 17799) werden berücksichtigt. In der Norm ISO 27001 sind die notwendigen Maßnahmen für die Einführung eines Managementsystems für Informationssicherheit nur sehr generisch gelistet. ISO 27002 führt die geforderten Maßnahmen von ISO 27001 etwas definierter aus. Die Implementierung von Sicherheitsmechanismen wird explizit berücksichtigt mit dem Ziel, sämtliche Werte in der Wertschöpfungskette zu schützen. Aus den 11 Überwachungsbereichen können zwei Bereich klar den physikalischen Bedrohungen zugeordnet werden

- **Physische Sicherheit: Zutritt und Zugang, Klima und Lüftung, Brand/Wasser, Energie**
- **Zugriffskontrolle: physischer Schutz, Netzwerk, Systeme, Anwendungen, Funktionen, Daten**

Somit stellt die Abwehr von physikalischen Gefahren einen zentralen Bestandteil der Umsetzung der ISO 2700x dar.

Optimaler Grundschutz erfordert IT-spezifische Systeme

Diebstahl, technische Schäden oder die Störung der Betriebsumgebung: Das sind die größten physikalischen Risiken, die die Daten und die IT-Infrastruktur in Serverräumen täglich bedrohen. Um effektiven Schutz zu garantieren, müssen mehrere physikalische Schutzmechanismen sinnvoll ineinandergreifen. Im Folgenden ist eine Aufstellung der wichtigsten physikalischen Sensoren und Komponenten, die diesen Rundumschutz gewährleisten, zusammengefasst.

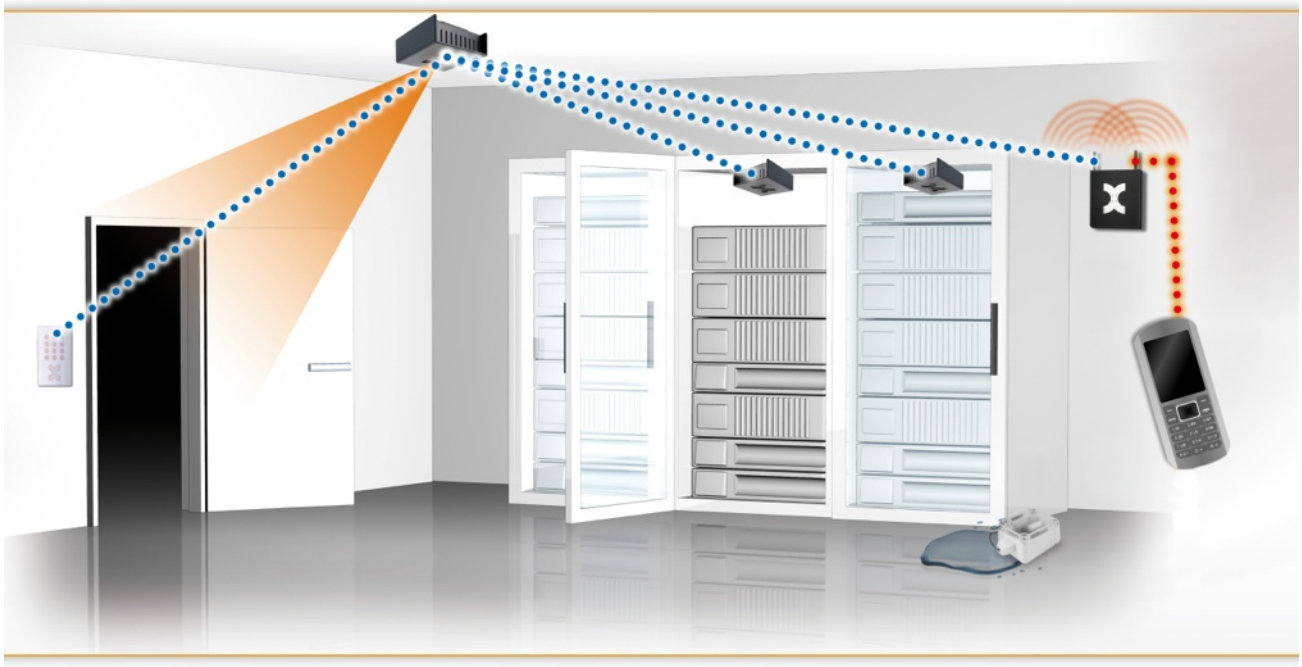
- Um den Serverraum vor Diebstahl, Sabotage und unbefugtem Zutritt zu sichern, benötigt man einen Bewegungsmelder, der bei Einbruch alarmiert. Der Melder wird innerhalb des Serverraums montiert. Wichtig ist es, hierbei einen spezialisierten Bewegungsmelder einzusetzen, der die verschiedenen Temperaturzonen und Gerätetemperaturen in einem IT Raum berücksichtigt und keine Fehlalarme provoziert. Ideal sind Melder basierend auf Radartechnologie oder spezialisierte Passiv Infrarotmelder (PIR) mit Temperaturkompensation.

- Wird der Raum zu heiß, steigt die Temperatur zu schnell oder sind die Temperaturschwankungen zu hoch verkürzt sich die Lebensdauer des technischen Equipments, sogar ein Ausfall der Server ist möglich. Hier schütz ein Temperatursensor, der die Raumtemperatur und auch die Funktion von Kühl- oder Heizanlagen überwacht.
- Um technische Schäden und Serverausfälle durch Kondenswasser zu vermeiden, lässt sich die Luftfeuchte ebenso überwachen wie der Taupunkt. Um Wasser, das auf dem Boden des Serverraumes steht zu erkennen, empfiehlt sich der Einsatz eines Leckage-Sensors.
- Um Feuer zu detektieren, ist ein Brandmelder erforderlich – im Idealfall ist dies ein Kohlenmonoxid-Sensor, mit einer sensiblen Auslöseschwelle im Bereich zwischen 20 und 200 ppm. Je empfindlicher die Einstellung, desto frühzeitiger wird die Gefahr erkannt.
- Ebenfalls überwacht werden sollte die externe Netzspannung. Spannungsausfälle müssen gemeldet und im Idealfall gleich überbrückt werden. Bei einem Stromausfall sollte das System eine Notspannungsversorgung haben, sodass in jedem Fall noch die Alarmierung per GSM funktioniert. Denn ganz ohne Strom gibt es auch kein LAN und keine E-Mail-Benachrichtigung. Diese Redundanz der Übertragungswege erhöht die Sicherheit erheblich.
- Um Störungen in der Betriebsumgebung frühzeitig zu erkennen, sollten neben der reinen Überwachung auch noch Klimadaten wie Luftfeuchtigkeit, Raumtemperatur oder Spannungsschwankungen erfasst und ausgewertet werden. Denn durch ein Echtzeit-Monitoring der Betriebsparameter im Serverraum lassen sich manche Gefahrenpotentiale bereits im Vorfeld erkennen und abwenden.

Moderne Monitoringlösungen sind vernetzt und melden Störungen in Echtzeit.

Im Stör- oder Alarmfall senden die eingesetzten Komponenten eine Meldung an eine zentrale Systemeinheit – den AlarmManager. Hier laufen alle Informationen der Sensoren zusammen und werden ausgewertet. Da die zu sichernden Serverräume in der Praxis meist komplett eingerichtet sind (und die Sensoren sozusagen im laufenden Betrieb zu installieren sind), entfällt die Möglichkeit der Signalübertragung per Draht: Ein zu hoher Aufwand, schließlich müssten hier Wände aufgeklopft und Leitungen gelegt werden. Eine wirksame Vernetzung von Sensoren und dem Alarmmanager erfolgt in Serverräumen per LAN oder Funk (z.B.: ZigBee). Wird dann ein Diebstahl oder ein technischer Schaden von einem Sensor erkannt, gelangt die Information in Echtzeit an den AlarmManager, der daraufhin, je nach Alarmquelle, entsprechend reagiert. Über Meldeausgänge beispielsweise lassen sich externe Alarmierungsgeräte wie Sirene und Blitzleuchten ansteuern. Diese sorgen zwar für viel Aufmerksamkeit, garantieren aber noch nicht, dass im Alarmfall die richtigen Personen rechtzeitig informiert werden. Hierfür sollte auf jeden Fall zusätzlich eine stille Alarmierung eingerichtet werden, die zuvor festgelegte Personen gezielt benachrichtigt.

Die stille Alarmierung erfolgt dabei wahlweise per SMS, E-Mail, SNMP oder Telefonanruf und lässt sich individuell – je nach Alarmursprung – einstellen. Ferner ist es möglich, über Schaltausgänge weitere Verbraucher zu aktivieren, zum Beispiel eine externe Beleuchtung, was die Sicherheit ebenfalls erhöht. Ein wirksames Zusammenspiel und eine funktionale Vernetzung all dieser Komponenten sind erforderlich, um den Serverraum vor den zentralen Gefahren zu schützen und im Alarmfall richtig darauf zu reagieren.



MultiSensor-Systeme fusionieren alle wichtigen Sensoren in einem Gerät

Bei klassischen Gefahrenmeldeanlagen gibt es für das Erkennen jeder der genannten Gefahren je einen eigenen Sensor. Um einen Serverraum abzusichern muss z.B. ein Facherrichter verschiedene Komponenten an unterschiedlichen Orten installieren und programmieren. Ein vollständiges Überwachungskonzept entsprechend der Philosophie „alles aus einer Hand“ lässt sich damit jedoch nicht realisieren, da die meisten dieser Systeme zwar bei Gefahren warnen, aber nicht die entscheidenden Klimadaten der Betriebsumgebung (z.B.: Luftfeuchtigkeit, Raumtemperatur und Spannungsschwankungen) erfassen und auswerten.

Hier liegt die Stärke eines MultiSensor-Systems für IT- und Serverräume. In diesen All-In-One-Lösung sind alle physikalischen Sensoren, die speziell auf den Schutz der Serverräume abgestimmt sind, in einem kompakten Gehäusen integriert. Das Einbinden von Fremdkomponenten ins Überwachungssystem ist zwar möglich, aber für einen effektiven Schutz des Serverraumes nicht nötig. Der Schutz vor Gefahren und die Erfassung der relevanten Klimadaten erfolgt hier durch den MultiSensor, die Auswertung, Dokumentation und ggfs. Alarmierung durch den AlarmManager – wobei auch das MultiSensor-Gehäuse einen akustischen Signalgeber enthält. Eine MultiSensor-Lösung ist somit Klima-, Brand- und Einbruchmeldezentrale für Serverräume in einem – ein Komplettpaket für die physikalische Sicherheit für diese hochsensiblen Räume.

Gegenüberstellung der möglichen Kosten, infolge fahrlässiger Absicherung gegen physikalischen Gefahren und der Investitionskosten für eine integrierte MultiSensor-Technologie

Potenzielle Kosten beim Eintritt der beschriebenen physikalischen Risiken
Der Verlust bzw. die Beeinträchtigung der Geräte in Serverräumen und Datacenter für zu erheblichen Kosten für den Ersatz der Hardware- und Datenbeständen. Zusätzlich entstehen erhebliche Kosten durch den IT-bezogenen Produktivitätsverlust infolge von z.B. Ausfall des Servers durch Überhitzung. Nicht auszuschliessen sind auch eine Verschlechterung des Images von Behörden in der Wahrnehmung der Gesellschaft.

Das Investitionsvolumen für die Anschaffung, Installation und Inbetriebnahme für ein System zum Monitoring und Überwachung von IT-Infrastruktureinheiten liegt bei weniger als 1.000,- Euro.

Schlussfolgerung

Im Sinne der Erfüllung der IT-Grundschutzanforderungen und der Erhöhung der IT-Verfügbarkeit kann es als fahrlässig angesehen werden, die physikalischen Risiken nicht bzw. nicht durch IT-spezifischen Systemen abzusichern. Insbesondere vor dem Hintergrund der überschaubaren Investitionskosten.

Quellen: *eigenen Erhebung aus 100 Telefoninterviews