Die Checkliste

# Wie gut ist die IT von Stadtwerken und Versorgern gegen physische Schäden gesichert?

Neben der Sicherheit auf der informationstechnischen Ebene unterschätzen viele IT-Verantwortliche die physikalischen Gefahren, die in Server- und Technikräumen die technische Infrastruktur lahmlegen können. Dazu zählen beispielsweise Schmorbrände von fehlerhaften Isolierungen, die zu einem Brand führen können, Wassereinbrüche, zu hohe Temperatur und Feuchtigkeit oder unberechtigte Zutritte in nicht öffentliche Bereiche. Die fehlende physische Absicherung ist auch der Teil des ISO 27001 Audits zur Einführung eines erforderlichen Informationssicherheits-Managementsystem (ISMS), bei dem Auditoren am häufigsten die größten Mängel feststellen. Laut einer Studie von Hewlett-Packard erleiden etwa 77 % aller Unternehmen jährlich Systemausfälle, wobei es eine Reihe von Gründen für diese gibt. Neben Softwarefehlern und menschlichem Versagen gehören insbesondere physikalische Gefahren zu den bekanntesten Ursachen.

Der Spezialist für die physische Überwachung von Rechenzentren Kentix hat eine Checkliste über 10 Fragen zusammengestellt, die IT-Systeme in Stadtwerken, Versorgern und KRITIS-Betreibern erfüllen sollten.

**Selbsttest: Wie sicher ist meine kritische Infrastruktur? – 10 einfache Fragen:**

1. Ist die IT in einem speziell vorbereiteten Serverraum bzw. ein Rechenzentrum untergebracht?
*Risiko*
Räume für die IT-Nutzung sollten für die besonderen Anforderungen hergestellt bzw. angepasst werden und folgende Eigenschaften haben: Brandschutztüren und entsprechende Brandschutzmaßnahmen, sichere Fenster, angepasste Stromkreise, keine Wasserführenden Leitungen, keine artfremde Zusatznutzung.

2. Wird die Entstehung von Bränden frühzeitig gemeldet und können sofort Maßnahmen eingeleitet werden?
*Risiko*
Ein Großteil der Brände entstehen in elektrischen Anlagen und Geräten. Diese entwickeln sich in der Regel langsam durch Schmorbrände. Elektroverteilungen, USV-Systeme, Klimaanlagen und Netzteile stellen potenzielle Gefahren für Brände dar.

3. Wird beim Anstieg der Raumtemperatur frühzeitig die zuständige Abteilung informiert, um Gegenmaßnahmen einzuleiten? Erhält diese in Echtzeit Informationen über das Raumklima?
*Risiko*
Beim Ausfall der Klimaanlage kann es zu einer Überhitzung der Server kommen. Dies führt meist innerhalb kurzer Zeit zu einem Totalausfall der IT. Weitere kritische Zustände sind zu hohe Luftfeuchte oder Betauung nach Ausfällen von Klimaanlagen.

4. Werden Wasserleckagen durch Rohrbrüche oder einer defekter Klimaanlage automatisch gemeldet, bevor Schäden entstehen?
*Risiko*
Das Eindringen von Wasser in Serverräume durch Hochwasser oder Defekte an Heizungsanlagen und Klimageräten etc. kann binnen kürzester Zeit zu einem Totalausfall der IT führen.

5. Ist im Falle eines Spannungsausfalles bekannt, wie lange dieser andauert und ob die USV korrekt arbeitet?
*Risiko*
Bei einem Spannungsausfall kann es zu unerwarteten Störungen der USV kommen und damit zu einem Totalausfall der IT. Spannungsschwankungen werden oft auch durch Industrieanlagen verursacht und können zu USV- bzw. Netzteilfehlern führen.

6. Wurden aktive Maßnahmen gegen Einbrüche getroffen und kann trotzdem im Falle eines Vorfalls umgehend reagiert werden?
*Risiko*
Einbruch oder Diebstahl sind die offensichtlichsten Bedrohungen. Hier kann es neben dem physischen Diebstahl von Hardware auch zu logischen Zugriffen und Attacken kommen. Zugängliche Konsolen stellen hier kritische Angriffspunkte dar.

7. Kann nachvollzogen werden, wer wann und wie lange im Raum war?
*Risiko*
IT-Räume sind adäquat gegen unbefugte Zutritte zu sichern und diese wo immer möglichst zu dokumentieren. Sehr oft finden Angriffe auf die IT aus den Unternehmen heraus selbst statt.

8. Erhalten Verantwortliche bei Ausfällen aktiver Komponenten bzw. von Netzwerkverbindungen jederzeit in Echtzeit Benachrichtigungen?
*Risiko*
Beim Ausfall aktiver oder passiver Komponenten wie Router, Switches und Telefonanlagen kann es zu massiven Störungen der IT-Infrastruktur kommen. Systemausfälle von mehreren Stunden bis Tagen können hier schnell sehr große Schäden verursachen.

9. Werden Auswirkungen menschlichen Fehlverhaltens frühzeitig automatisch gemeldet und können diese Meldungen auch unabhängig von Ihrer IT übertragen werden?
*Risiko*
Falsche Bedienung, offene Fenster, Missachtung von technischen Anweisungen, ungeschicktes Verhalten – all dies führt regelmäßig zu teuren IT-Ausfällen. Zur Vermeidung tragen organisatorische Maßnahmen bei, die durch schnelle und redundante Benachrichtigung von Unregelmäßigkeiten an mehrere Personen unterstützt wird.

10. Können zu jedem Zeitpunkt Ereignisse nachvollzogen und rekonstruiert werden (auch über mehrere Monate), um zukünftige Fehler zu vermeiden?
*Risiko*

Dokumentation und Aufzeichnung von normalen und kritischen Systemzuständen über Monate oder Jahre sind vielfach Grundanforderungen von QS- und Zertifizierungssystemen. Eine lückenlose Dokumentation entbindet Sie möglicherweise von Haftungsrisiken.

**Gefahren werden unterschätzt, ganzheitliche Lösungen sind einfach zu implementieren**

Viele Stadtwerke, Versorger und KRITIS-Betreiber unterschätzen die physikalischen Gefahren, denen ihre kritischen Infrastrukturen ausgesetzt sind. Um die erforderliche Sicherheit zu gewährleisten, werden mitwachsende, skalierbare „All-in-One Systeme“ benötigt, die sich den steigenden Anforderungen anpassen können. Ein ausreichender Grundschutz ist jedoch bereits mit überschaubarem Investitions- und Installationsaufwand möglich. Hierzu gehört ein integriertes System aus ganzheitlichem Monitoring von Umgebungsparametern wie Temperatur, Luftfeuchte, Taupunkt, Spannung, Feuer und Einbruch sowie einem Zutritts- und Zugriffsmanagement mit permanenter Videoüberwachung. Sind die Komponenten IP-fähig, können die Verantwortlichen über ein Online-Dashboard auf die verschiedenen Bereiche wie Zutritt, Alarm, Klima, Energie und Video zugreifen und sie bequem und in Echtzeit aus der Ferne steuern. Damit können auch dezentrale Systeme zentral mit wenig Personalaufwand verwaltet werden.

**Über Kentix**

Kentix ist der Spezialist für ganzheitliche und skalierbare IoT-Lösungen zum Schutz geschäftskritischer Infrastrukturen. Vom einzelnen Serverschrank über Data-Center bis hin zu großen Infrastrukturen überwachen Kentix-Lösungen schutzbedürftige Räume und erkennen physische Gefahren präventiv. Das hauseigene KentixOS analysiert, verarbeitet und verwaltet die gesammelten Daten, um sie dem zuständigen Personal einfach und intuitiv zur Verfügung zu stellen. Die unkompliziert installierbaren Hard- und Softwareprodukte auf IoT-Basis decken Anwendungsfälle in den Bereichen Umgebungsmonitoring, Zutrittskontrolle, Videoüberwachung sowie Energiemonitoring ab und ermöglichen so durch den All-in-One-Ansatz höchstes Schutzniveau aus einer Hand.
Unternehmen aus allen Branchen sichern durch Produkte der Kentix GmbH mit Sitz in Idar-Oberstein ihr Geschäft gegen physische Gefahren sowie menschliches Fehlverhalten ab und halten gesetzliche Anforderungen ein. Die Entwicklung und Produktion erfolgt ausschließlich in Deutschland.