

## Physikalische Sicherheit der IT-Infrastruktur

*Die Abhängigkeit von der IT-Infrastruktur wird in vielen Fällen von Unternehmen völlig unterschätzt. Verlässliche Zahlen zur Informations-Sicherheit sind jedoch selten. Aussagen zu selbstkritischen Bestandsaufnahmen, konkrete Angaben zu Schäden und Budgets fehlen und sind schwer zu erlangen. Gerade in mittelständischen Unternehmen ist die Bereitschaft gering, ernsthaft über die Risiken eines Teil- oder Totalausfalles der IT-Infrastruktur nachzudenken.*

### Sicherheits- und Riskmanagement ist gesetzlich gefordert

Viele vergessen, dass ein Sicherheits- und Risk-Management gesetzlich gefordert ist. Ernsthafte Untersuchungen zu den vielfältigen Bedrohungsarten und deren Risikopotentiale mit all ihren Auswirkungen auf den ungestörten Geschäftsbetrieb und auf die Unternehmensziele, eingebettet in ein umfassendes Sicherheits- und Riskmanagementkonzept, fehlen in der Regel.

Sehr oft wird die gesetzlich verankerte **Organisationspflicht** und **Sorgfaltspflicht** mit all den Verflechtungen zu **KonTraG** und **Basel II** vergessen. Es läuft darauf hinaus, ein Sicherheits- und **Riskmanagement** einzurichten (Vorhalten eines Früherkennungs- und Steuerungssystems für kritische Entwicklungen im Unternehmen) und durch präventiv wirkende Sicherheitsmaßnahmen in Kombination mit diesem Risikomanagement sicher zu stellen:

**Auszug KonTraG: Die Gefahr von Verlusten und Schäden, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder in Folge externer Ereignisse eintreten, angemessen einzuschränken oder gar zu verhindern.**

Das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG) verpflichtet zwar die Vorstände von börsennotierten Unternehmen, hat aber auch Ausstrahlungswirkung auch auf die Geschäftsführer anderer Gesellschaftsformen.

Die Organisationspflicht und die Pflicht zum Aufbau eines Risk-Management betrifft besonders die Verantwortlichen für die IT-Infrastruktur. Die wenigsten RZ-Leiter verfügen über verwertbare Untersuchungen, welche Auswirkungen der Ausfall von IT- und TK-Anlagen auf die verschiedenen Unternehmensteile hat und welche finanziellen Folgeschäden entstehen könnten. Viele Unternehmen können große Schadensereignisse, verursacht durch den Ausfall der IT-Infrastruktur mangels ausreichender Finanzierung nicht abfangen und stehen im IT-GAU vor dem Aus. Schon eine einzelne Gefahr wie z.B. ein Brand kann dazu führen.

### Was sind die Gründe für mangelhafte Sicherheit bei IT-Anlagen und IT-Infrastruktur?

**Immerhin erachten 48% der Befragten IT-Verantwortlichen Verstöße gegen Gesetze, Vorschriften oder Verträge als „sehr wichtig“ und immerhin 44% als „wichtig“.**  
(Quelle: Fachzeitschrift <kes>, Sicherheitsstudie – Lagebericht zur Informationssicherheit)

## Physikalische Sicherheit der IT-Infrastruktur

Auf die Frage „Was die IT-Sicherheit am meisten behindert“, ergaben Antworten aber nachfolgendes Resultat:

Bei der Verbesserung der Sicherheit behindern am meisten... (Mehrfachnennungen möglich, Auszug)		genannt von		
		2004	2006	2008
1.	Es fehlt an Bewusstsein bei den Mitarbeitern	51%	59%	69%
2.	Es fehlt an Bewusstsein u. Unterstützung im Top-Management	45%	50%	55%
3.	Es fehlt an Bewusstsein beim mittleren Management	42%	42%	45%
4.	Es fehlt Geld	62%	49%	43%
5.	Es fehlen verfügbare und kompetente Mitarbeiter	33%	39%	43%
6.	Die Kontrolle auf Einhaltung ist unzureichend	29%	37%	41%
7.	Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	32%	35%	38%
8.	Es fehlen die strategische Grundlagen/Gesamt-Konzepte	31%	32%	36%
9.	Die vorhandenen Konzepte werden nicht umgesetzt	21%	26%	27%

Quelle: <kes> / Sicherheitsstudie 2004 - 2008

**Fazit: Fehlendes Geld und mangelndes Bewusstsein der Mitarbeiter und des Top-Managements sind die Hauptursache für mangelhaftes Sicherheitsmanagement.**

### Was sind die wirklichen Risiken?

Anschläge wie am 11. September 2001 in New York oder am 11. März 2004 in Madrid setzten in Hinsicht auf die Terrorgefahr und deren Auswirkung sicherlich Maßstäbe. Wenn auch die staatlichen Sicherheitsdienste von einer steigenden Gefahr in Deutschland sprechen, die Privatwirtschaft sieht sich davon (noch) nicht betroffen. Im Hinblick auf die Bedrohung durch einen Terroranschlag sicherlich auch nachvollziehbar.

Die eigentlichen Risiken liegen im normalen Umfeld und im „Tagesgeschäft“. Das größte Risiko ist der Mensch. Fahrlässigkeit, Vorsatz, Bequemlichkeit und mangelndes Verständnis für Sicherheitsmaßnahmen sind leider die Regel.

Die allgemeinen Bedrohungsarten und Gefahren und die daraus resultierenden Risiken sind vielfältig und in jedem Unternehmen unterschiedlich ausgeprägt. Besonders hervorzuheben sind zweifellos:

- Der Imageverlust durch Ereignisse mit öffentlicher Wirkung
- Der Schaden durch die Verweigerung von Versicherungsleistungen
- Der Schaden durch Wirtschaftsspionage
- Der Schaden Weitergabe vertraulicher Informationen
- Der Schaden durch Wirtschaftskriminalität
- Der Verstoß oder das nicht Beachten gesetzlicher Regeln und Bestimmungen und die damit verbundenen strafrechtlichen und zivilrechtlichen Folgen

## Physikalische Sicherheit der IT-Infrastruktur

Für die IT-Anlagen und IT-Infrastruktur erwachsen die größten Risiken aus den besonderen Bedrohungen und Gefahren wie z.B.

- Betriebsunterbrechung durch Versagen der technischen Infrastruktur wie
  - Spannungsversorgung
  - Klima- und Lüftungsanlage
- Betriebsunterbrechung oder der Totalverlust bzw. der Teilverlust durch Brand
- Betriebsunterbrechung durch Versagen der Logistikkette
- Deliktische Handlungen wie
  - Einbruchdiebstahl
  - Vandalismus
  - Brandstiftung
  - Sabotage
- Sonstige deliktische Handlungen (siehe Tabelle)
- Schaden durch organisatorische Mängel

Infrastruktur & Technik	Menschen		Höhere Gewalt	
	Mitarbeiter	Externe	Witterung	Katastrophen
<ul style="list-style-type: none"> <li>• Funktionsstörung,</li> <li>• Defekt und Ausfall von               <ul style="list-style-type: none"> <li>• Systemen</li> <li>• Verkabelung</li> </ul> </li> <li>• Stromausfall</li> <li>• Überspannungen,</li> <li>• Erdungsprobleme,</li> <li>• Kabelbrand</li> <li>• Ausfall der Klimaanlage</li> <li>• Verlust der Kommunikationsverbindung</li> </ul>	<ul style="list-style-type: none"> <li>• Computerviren</li> <li>• Missbrauch,</li> <li>• Betrug</li> <li>• Diebstahl</li> <li>• Sabotage</li> <li>• Unachtsamkeit</li> <li>• Unwissenheit</li> <li>• Menschliches Versagen</li> <li>• Zutrittssperre-Evakuierung</li> <li>• Fluktuation</li> </ul>	<ul style="list-style-type: none"> <li>• Computerviren</li> <li>• Hacking</li> <li>• Terroranschlag</li> <li>• Missbrauch</li> <li>• Einbruch</li> <li>• Diebstahl</li> <li>• Sabotage</li> <li>• Spionage</li> <li>• Vandalismus</li> </ul>	<ul style="list-style-type: none"> <li>• Kälte, Frost</li> <li>• Schnee</li> <li>• Wassereintrich</li> <li>• Unwetter, Sturm,</li> <li>• Hochwasser, Erdbeben</li> <li>• Blitzschlag</li> <li>• Spannungsschwankungen</li> <li>• Verlust der Verkehrsverbindungen</li> </ul>	<ul style="list-style-type: none"> <li>• Hochwasser</li> <li>• Überschwemmungen</li> <li>• Feuer, Rauchgase</li> <li>• Chemische Kontamination</li> <li>• Erdbeben</li> <li>• Erdbeben</li> <li>• Flugzeug-Absturz</li> <li>• Verkehrsunfall</li> <li>• Explosion</li> </ul>

Quelle: KRAISS SECURITY CONSULT

Die entstehenden bzw. vorhandenen Risikopotentiale sind innerhalb eines Industriestandortes (Freigelände, Nutzungsart eines Gebäudes wie z.B. Lager, Produktion, Verwaltung, Forschung und Entwicklung) unterschiedlich ausgeprägt und abhängig von vielen Einzelfaktoren. Auf der Basis von **Verfügbarkeitsanforderungen** (z.B. 99,5 prozentige Verfügbarkeit) und des Ist-Zustandes ergibt sich das damit verbundene **Risikopotential**.

**Bedrohungsszenarien in IT-Welt sind oft nur auf logische und physische Gefahren ausgerichtet – aber was ist mit der Firewall für den Rucksack?**

Vielfach wird vergessen, dass durch die kumulierende Wirkung kleiner Ereignisse (Zusammenwirken mehrerer Schwachstellen oder auch die Verkettung unglücklicher Umstände), verheerende Folgen haben können.

**Eine übergreifende und konzeptionelle Betrachtung der Gefahren und der damit verbundenen Risikopotentiale findet nur zu selten statt, hat aber elementare Bedeutung in der Risikobetrachtung.**

## Physikalische Sicherheit der IT-Infrastruktur

Die wenigsten Unternehmen haben eindeutige und gerichtsverwertbare Unterlagen zum Schutzkonzept, der Risikobewertung, der Sicherheitsmaßnahmen, der Revisionsmaßnahmen und des Risk-Managements. Dieser Umstand kann im Fall der Fälle verheerende Folgen für die verantwortlichen Personen und das Unternehmen haben.

Verstöße gegen Organisationsverpflichtungen bergen erhebliche Haftungsrisiken und strafrechtliche Konsequenzen für das Management. Finanzielle Risiken, z.B. Verweigerung von Versicherungsleistungen im Schadensfall, sind gängige Praxis und nicht auszuschließen.

### Wo werden die meisten Fehler gemacht?

Wie so oft steckt der Teufel im Detail. Kleinigkeiten werden absichtlich oder unabsichtlich übersehen. Die Analyseergebnisse zeigen die meisten Fehler und Mängel:

#### Mangelhafter Brandschutz

- Schadhafter baulicher Brandschutz an Wänden, Decken, Böden und Türen
- Unvollständige Brandfrüherkennung bzw. Brandfrühesterkennung in Kombination mit automatischen Löschanlagen
- Mangelhafter organisatorischer Brandschutz in Form fehlender eindeutiger Interventionsmaßnahme und Verhaltensweisen im Brandfall
- Fehlende Routine im Umgang mit besonderen Ereignissen durch zu wenig Notfallübungen

#### **Beispiel 1**

Die Rechnerräume werden mit einer Brandmeldeanlage überwacht weil zwingend vorgegeben. Die benachbarten Räume nicht. In diesen werden hohe Brandlasten gelagert. In einem der benachbarten Räume bricht ein Feuer aus. Es kann sich entwickeln und erzeugt hohe Hitze. Die Wände übertragen die Hitze auf den Rechnerraum (geht sehr schnell und wird nicht erkannt). Die elektronischen Bauteile werden nachhaltig zerstört obwohl es im überwachten Rechnerraum keinen Brand gibt.

**Fazit: Die benachbarten Räume müssen überwacht werden und dürfen keine hohen Brandlasten aufweisen! Brandwände (F90) schützen zwar vor Brandüberschlag aber nicht vor Temperaturübertragung. Das gleiche gilt für Feuerabschlusstüren!**

#### **Beispiel 2**

Die Brandfrüherkennung mittels Rauchmelder ist gut. Die Brandfrühesterkennung mittels Rauchansaugsysteme - möglichst direkt an den Objektschränken - ist besser. Die bereits in der frühesten Phase entstehenden Rauch- und Brandgase werden durch die aktive Rauchansaugung früh erkannt und gemeldet. Weit bevor der eigentliche Brand in Form eines offenen Feuers entsteht, kann reagiert werden. Dank neuer Laser- und Scannertechniken werden bekannte Störgrößen wie z.B. Staub ausgefiltert. Bei Infoalarm (drei Alarmstufen sind üblich: Infoalarm, Voralarm und Hauptalarm) kann bereits reagiert werden. Anhand ansteigender Messwerte ist zu erkennen, ob es sich um eine echte „Brandentwicklung“ handelt oder nicht.

**Fazit: Es bleibt genügend Zeit den möglichen Brandherd zu verifizieren und zu beseitigen. Der RZ-Betrieb muss nicht unterbrochen werden. Es kommt zu keinen Ausfallzeiten.**

## Physikalische Sicherheit der IT-Infrastruktur

### Mangelhafter Objektschutz

- Inkonsequente Zutrittskontrolle in Verbindung mit fehlender Türoffenzeitüberwachung
- Fehlende Vereinzelungsmaßnahmen in Kombination mit einer eindeutigen Personenidentifikation
- Fehlende oder mangelhafte Interventionsmaßnahmen
- Keine mechanischen Sicherungsmaßnahmen in Verbindung mit fehlenden Widerstandszeitwerten

#### **Beispiel 1**

Die Zutrittskontrolle ist obligatorisch. Die Türoffenzeitüberwachung in Kombination mit einer akustischen und optischen Alarmierung vor Ort und einer sofortigen Alarmierung an einer zentralen Stelle, wird wenig angewandt. Die optische Überwachung fehlt. Keiner weiß was los ist. Die Tür kann unkontrolliert offen stehen. Das Risiko „Mensch“ macht die Sicherheitsmaßnahme Zutrittskontrolle zunichte.

**Fazit: Zwangsläufigkeiten müssen die Sicherheitsmaßnahmen unterstützen und die Schwachstelle „Mensch ausschalten.**

#### **Beispiel 2**

Die Hauptstränge der IT- und TK-Leitungen werden durch nicht überwachte Bereiche geführt und können absichtlich oder unabsichtlich zerstört werden. Erschwerend kommt hinzu, dass sie nicht redundant verlegt wurden.

**Fazit: Die Gefährdung der IT-Anlagen hört nicht an der Grenze des RZ-Bereiches auf, sondern erstreckt sich auch auf die leitungstechnische Infrastruktur.**

### Mangelhafte technische Gebäudeausrüstung

- Fehlende oder zu gering dimensionierte unterbrechungsfreie Stromversorgung (USV). Fehlende Redundanzen in den Systemen und den Leistungsnetzen, oft gepaart mit inkonsequentem Brandschutz (redundante Leitungen oder Systeme befinden sich im gleichen Brandabschnitt)
- Fehlende Überspannungsschutzeinrichtungen und Maßnahmen zum Potentialausgleich
- Fehlende Vorsorge gegen elektromagnetische Unverträglichkeit
- Keine zweite Telekommunikationseinspeisung
- Keine zweite Mittelspannungseinspeisung
- Fehlende Spannungsausfallüberwachung an wichtigen Stromkreissicherungen
- Keine Brückenschaltungen an wichtigen Regelkreisen

#### **Beispiel 1**

Die USV-Anlage versorgt alle wichtigen Komponenten des Rechenzentrums. Die Dimensionierung ist ausreichend. Eine Brandmeldeanlage ist vorhanden. Eine elektrisch verträgliche Löschanlage fehlt. Im Falle eines Brandes wird zwar gemeldet aber nicht automatisch gelöscht. Besonders tragisch, wenn die Mittelspannungsanlage und die Hauptniederspannungsanlage ebenso mangelhaft ausgerüstet ist.

**Fazit: Die Kette der Sicherheitsmaßnahmen muss geschlossen sein, um im Ernstfall zu wirken.**

## Physikalische Sicherheit der IT-Infrastruktur

### Beispiel 2

Der Überspannungsschutz ist auf der Stromversorgungsseite hervorragend aufgebaut. Bei den Daten- und TK-Leitungen fehlt er aber gänzlich.

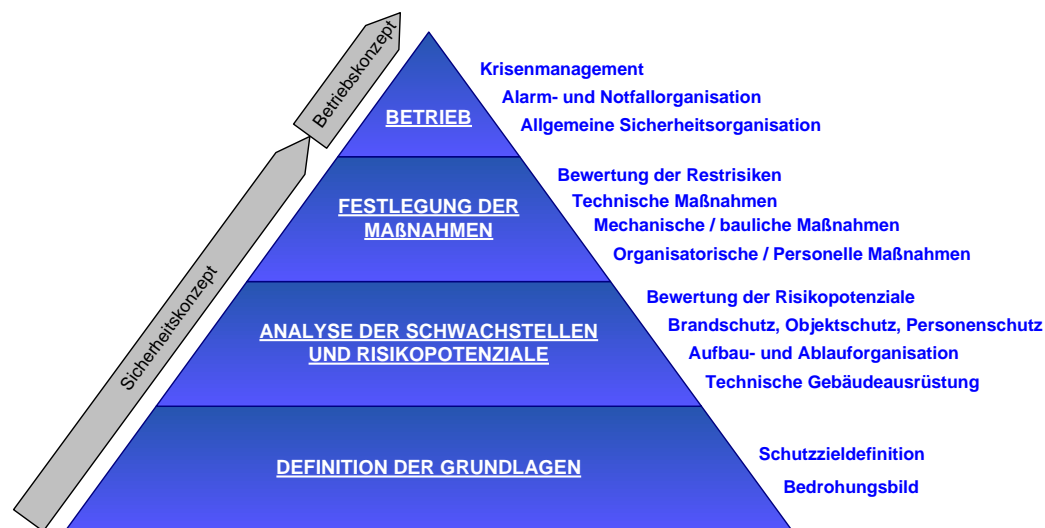
**Fazit: Die Kette der Sicherheitsmaßnahmen muss geschlossen sein, um im Ernstfall zu wirken.**

### Mangelhafte Vorbereitung auf den Fall „Was ist Wenn“

- Fehlende oder mangelhafte Alarm- und Notfallorganisation mit detaillierten Angaben sicherheitsrelevanten Verfahren und Abläufen (Ablauforganisation).
- Keine lückenlose Dokumentation der technischen Einrichtungen (Fehlersuche wird erschwert und dauert entsprechend lang)
- Keine eindeutige Vorgaben und Verfahren für Fehlersuche und Störungsbeseitigung
- Fehlende Empfangsstelle mit 7/24-Betrieb, die alle relevanten Meldungen aus Objektschutz, Brandschutz und Gebäudetechnik empfängt und kompetent erforderliche Interventionen einleitet und kontrolliert.
- Fehlende einheitliche Managementoberfläche für Sicherheit und Technik mit eindeutigen Interventionsvorgaben
- Fehlende Interventionskräfte, die sich kompetent um die Wiederherstellung des Sollzustandes kümmern
- Zu geringe Interventionszeiten (Zeit zwischen Eingang der Meldung und Wiederherstellung Sollzustand), die eine zeitgerechte Beseitigung der Ursache sicherstellen

### Wie ist der Weg zum strukturierten und gerichtsfesten Sicherheitsmanagement?

Die systematische Vorgehensweise ist entscheidend, gerade dann, wenn eine geschlossene und gerichtsverwertbare Dokumentation erstellt werden soll. Es ist zu empfehlen, die Durchführung durch eine neutrale und externe Einrichtung oder einen Berater durchführen zu lassen, da dann eine unbelastete und objektive Bewertung erfolgt.



Quelle: KRAISS SECURITY CONSULT

## Physikalische Sicherheit der IT-Infrastruktur

Eine Bewertung der verbleibenden Restrisiken muss erfolgen und im Rahmen des Risk-Managements müssen die getroffenen Maßnahmen regelmäßig kontrolliert werden. Übungen für den Fall der Fälle sind wichtig.

KRAISS SECURITY CONSULT  
Sandeldamm 16  
63450 Hanau  
Telefon 06181 / 78 05 35  
Telefax 06181 / 78 05 65  
Email [kontakt@kraiss-consult.de](mailto:kontakt@kraiss-consult.de)  
Website [www.kraiss-consult.de](http://www.kraiss-consult.de)