



## Sicherheitsforum südliches Sachsen- Anhalt 2004

Leuna, 28.09.2004

Thema: „IT- Unsicherheit – Ein teures Vergnügen“

Referent: Dipl.- Ing. Thomas Koch

... aus dem Inhalt

**Abhängigkeit von IT- und TK-Standorten**

**Risikopotentiale für IT- und Infrastrukturen**

**Untnehmensrisiken = Haftungsrisiken für  
Management und Vorstände**

**Risikoanalysen und Pflichtenhefte = Basis für Entscheidungen**

**Skalierbare Sicherheitslösungen mit Zertifikat**

## Beurteilung Ihrer Sicherheits-Situation



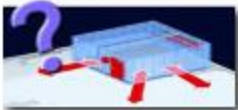
- Kennen Sie das Risikopotenzial für die Sicherstellung Ihrer IT-Funktionen?



- Wie hoch schätzen Sie die Abhängigkeit von der Verfügbarkeit Ihrer IT-Strukturen/-funktionen ein und wie beurteilen Sie hierzu Ihr persönliches Haftungsrisiko im Katastrophenfall?



- Wie viele Stunden bzw. Tage Totalausfall der IT-Funktionen könnte das Unternehmen überstehen?



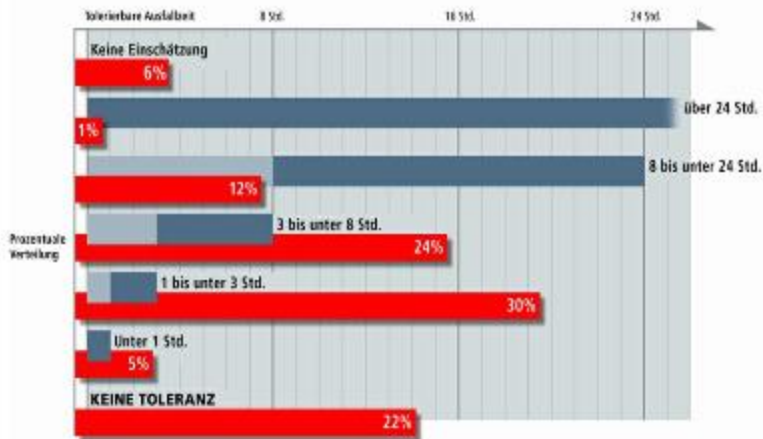
- Wie ist Ihre Vorstellung von den baulichen und sicherheitstechnischen Anforderungen der IT und den IT-Infrastrukturen in den nächsten 5 Jahren?

## Ausfallzeit



### Marktuntersuchung

Tolerierbare Ausfallzeiten als Ergebnis einer Marktuntersuchung bei IT-Managern



### Managementaufgabe:

Permanente Funktionssicherheit der IT-Strukturen

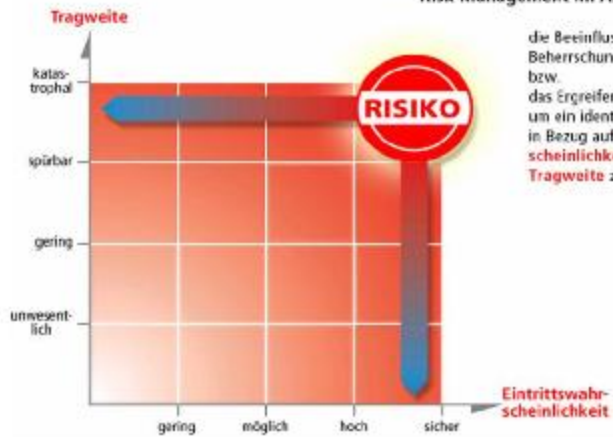


## Risk Management



### Risk Management im Allgemeinen heisst:

die Beeinflussung oder Beherrschung von Störpotentialen, bzw. das Ergreifen von Maßnahmen um ein identifiziertes Risiko in Bezug auf seine **Eintrittswahrscheinlichkeit** und/oder **Tragweite** zu beeinflussen.



## Risk Management



Eine persönliche Notwendigkeit - durch gestiegenes Haftungsrisiko





## Haftungsrisiken KonTraG

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich



„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“



GmbH Gesetz (§43 I, II)

PFLICHT!

Akt Gesetz (§91 II)



Vermeidung der persönlichen Haftung  
der GF oder der Vorstände (§93 II Akt Gesetz)



**Tagelang verhört, weil  
er jahrelang keine  
Fragen gestellt hat.**

„Warum haben Sie nie die IT- u.  
Kommunikationsprozesse in  
Ihrem Unternehmen hinterfragt?“

Quelle: Auszug Anzeige Siemens

Weil der CIO nie Fragen gestellt hat, muss er sich jetzt  
unangenehme gefallen lassen.

**Gehen Sie in die Offensive! Sprechen Sie uns an!**

**Bewertungsrisiko: Basel II**  
Neue Bewertungsrichtlinien bei der Kreditvergabe



**Penible Bewertung des gesamten Unternehmensrisiko:**



**Kredite können verweigert oder gekündigt werden**

- Banken sind gezwungen neue Kunden-Ratings zu erstellen
- Neukredite werden sehr viel schwerer vergeben
- Laufende Kredite können leichter aufgekündigt werden

**Problemsituationen/Risikopotenziale für Daten und Systeme**



## Risikofaktor Feuer

Brände in Rechenzentren und Telekommunikations-Standorten



Brandentstehung:  
20% innerhalb der RZ-Räume  
80% außerhalb der RZ-Räume

**Grundsatzurteil:** „Es entspricht der Lebenserfahrung, dass mit der Entstehung eines Brandes praktisch jederzeit gerechnet werden muss. Der Umstand, dass in vielen Gebäuden jahrzehntelang kein Brand ausbricht, beweist nicht, dass keine Gefahr besteht, sondern stellt für den Betroffenen einen Glücksfall dar, mit dessen Ende jederzeit gerechnet werden muss.“

ORF München 1960 vom 22.12.2007, 10 A 202/08  
VG Odenkirchen, Urteil vom 14.12.1965, 5 K 1522/65

### Brände in Deutschland (2002):

25859 erfasste Brandstiftungen  
davon 13739 vorsätzlich  
und 12120 fahrlässig

Quelle: BGS/Verho, Abt. für die Erdbrandkatastrophik 2002

## Konventionelle F90 Brandwand mit Prüfung nach DIN 4102



**1100°C**

**F90 Betondecke**

**F90 Brandmauer**

Bis zu **200°C** Temperaturerhöhung auf der Innenseite der Brandmauer.

- Keine Abkühlzeit,
- keine Stauwärmentwicklung,
- keine Messung der Luftfeuchtigkeit.

**F90** heißt, dass auf der dem Feuer abgewandten Seite der Temperaturanstieg innerhalb von 90 Minuten nicht mehr als im Mittel 140 Kelvin, punktuell nicht mehr als 180 Kelvin, betragen darf.

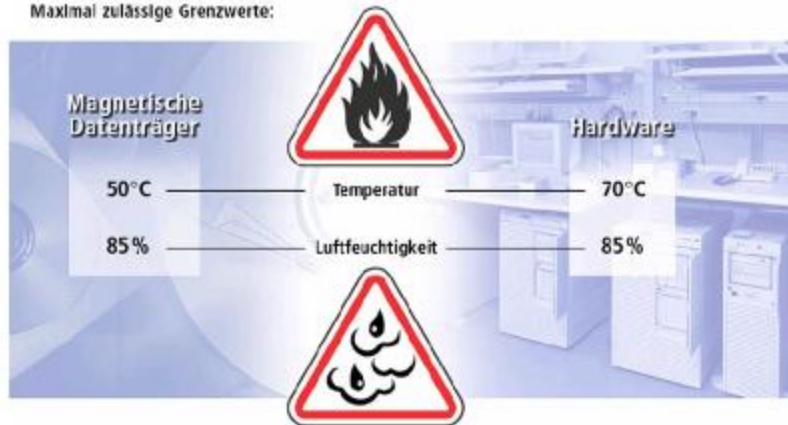
**F90** ist Bauwerkschutz mit dem Schutzziel:  
**Personen und Standsicherheit / Brandüberschlag**

**EDV / IT-Räumlichkeiten brauchen Inhaltsschutz!**

Vorgeschriebener Brandschutz für Telekommunikationssysteme und Datenträger nach EN 1047-2



Maximal zulässige Grenzwerte:



Risikofaktor Rauchgasentwicklung



Bei der Verbrennung von 1 kg PVC entstehen bis zu 5.800 m<sup>3</sup> Rauchgase.

## Risikofaktor Wasser



### Millionenschaden: Lager brannte den ganzen Tag Mit 1600 Liter pro Minute gelöscht

... erst nachdem einige Verblindungen abgeschraubt werden konnten, gelang durch den Einsatz eines Weidestrahlrohrs, das 1600 Liter pro Minute auf den Brandherd pumpte, ein erster Durchbruch.

Die größten Schäden, so die Geschäftsleitung, dürften durch das Löschwasser im zweiten Stock entstanden sein. Dort nämlich lagerte versandfertige Ware.

Quelle: Westfälische Post/bois / 20.01.2009

### Übergroßer Koffer richtet auf Flughafen Millionenschaden an

A<sup>3</sup> Frankfurt / Main. Ein übergroßer Koffer hat auf dem Flughafen Frankfurt rund 1 Mill. DM Schaden angerichtet. Wie die Flughafen-Gesellschaft mitteilte, stieß der metallene Kofferkoffer in der Gepäckförderanlage an eine Speiselinienanlage und beschädigte sie.

Dadurch traten rund 3000 Liter Wasser aus, die einen darunter liegenden Telekommunikationsraum überfluteten und die darin befindliche computergesteuerte Telefonanlage lahmlegten.

Quelle: Spiegel online/Steinberg / 05.02.2003



**Fazit: Gemauerte Räume erfüllen nicht die Sicherheitsanforderungen nach EN 1047-2**

## Risikofaktor Explosion



Kritische IT-Strukturen werden zukünftig möglicherweise das Ziel terroristischer Anschläge sein. Lampertz-Sicherheitslösungen bieten sehr hohe Schutzwerte gemäß SEAF (UK).



## Kennen Sie Ihre IST-Situation?

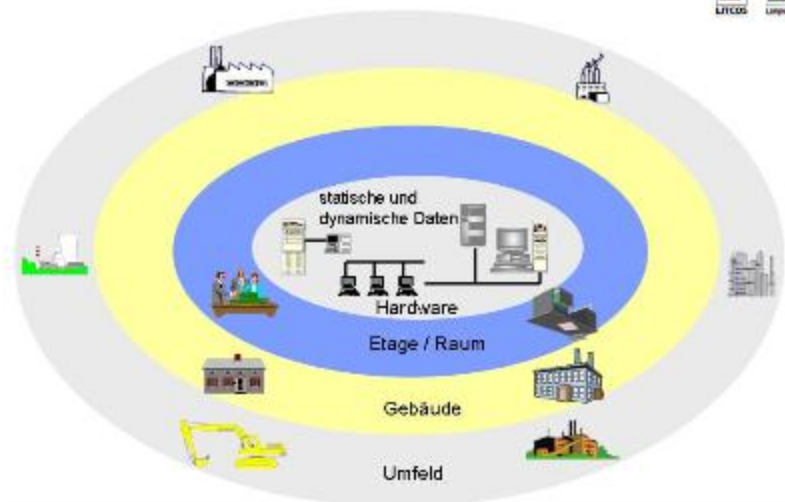
Vorausschauend und am individuellen Bedarf geplante IT-Sicherheit- die Grundlage für ein Höchstmaß an Betriebssicherheit. Damit werden Sie der persönlichen und wirtschaftlichen Verantwortung gegenüber Ihrem Unternehmen gerecht. Der erste Schritt auf diesem Wege ist die von Spezialisten durchgeführte Analyse der IST-Situation in Ihrem Hause. So entsteht Transparenz des Bestehenden und Orientierung über Notwendigkeiten - optimale Entscheidungsgrundlage für eine bedarfsgerechte und wirtschaftliche Sicherheitsplanung.



Das gemeinsame Ziel:  
Ein individuelles Sicherheitskonzept Ihrer IT-Infrastruktur



## Notwendig: Risikoerkennung



## Rekonstruktion nach dem K-Fall?



Quelle: vom 8/2010

## Dienstleistungsangebot / Risikoanalyse

**Risikoanalyse IT-Bereiche**  
 Serverraum  
 TK-Anlage  
 Netzverteilerraum

• Erfassung der IT-Strukturen  
 • Erfassung der Ausfalltoleranz  
 • Erfassung von Backup-Konzepten

• Definition des Bedrohungspotentials  
 • Definition der Abhängigkeit von der IT  
 • Definition bestehender Normen

Erfassung der  
 baulichen Situation

Erfassung der  
 Energieversorgung

Erfassung der  
 Sicherheitstechnik

Erfassung der  
 Klimatechnik

Erfassung der  
 Betriebsorganisation  
 und Datenbackup

Bewertung der B-Situation nach  
 bestehenden Normen z.B.  
 - EN 1047, Teil 1+2 - NFPA 76 Standard  
 - BSI Standard - BS 7799 Standard

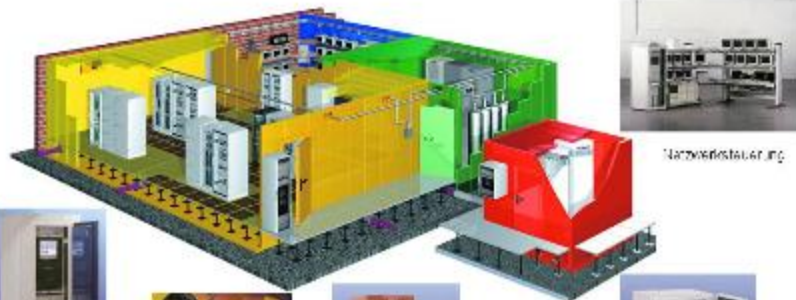
Maßnahmenvorschläge zur Reduzierung  
 der vorhandenen Risiken mit  
 • Prioritätenplan  
 • Grobkostenschätzung

Präsentation vor der Geschäftsleitung  
 • der Ist-Situation  
 • der Problemlösungen



## IT-Sicherheit: Die Kernkompetenz von Lampertz im Wandel!

Eine komplette Lösungspalette für den EDV-User.



Netzwerkstruktur



Hardwareabsicherung



Risk-Management



Backup-System



Daten Backup

TEC INO-DATA Sicherheitssystem III

Lampertz GmbH & Co. KG

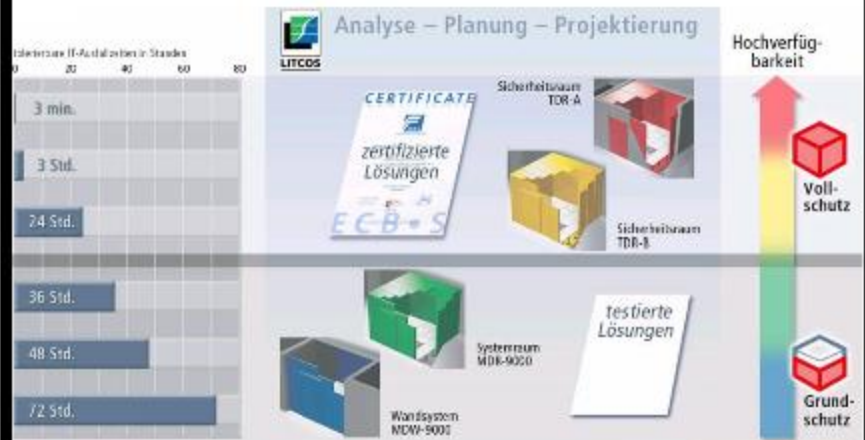
Transparanzkass. 7/2004

25

FRIEDHELM LOH GROUP

## Produktreihe: Testierter Grundschatz - Zertifizierter Vollschutz

skalierbar - flexibel - modular



Länger als 3 Tage: Undefinierte Anforderungen und Lösungen (konventionell nicht zuzuordnende IST-Situationen)

Lampertz GmbH & Co. KG

Transparanzkass. 7/2004

25

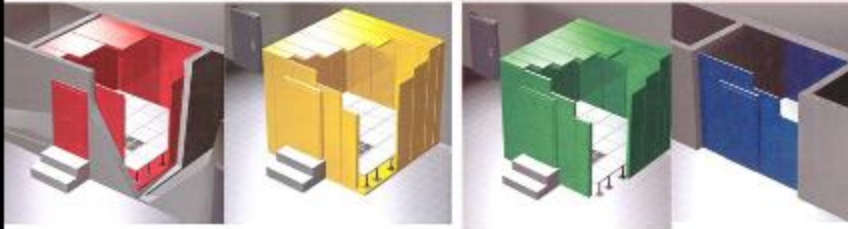
FRIEDHELM LOH GROUP

## IT-DataCenter von Lampertz mit skalierbaren Wertigkeiten gegen vielfache Risiken durch Raum-im-Raum-Systeme oder Haus-im-Haus-Systeme



Problemlösung für Backup und IT-Systeme mit verteilten Datenklassen R 30.3

Glückschutz für IT- und TK-Standorte und technische Infrastruktur



### Lampertz TECHNO-DATA IT-Sicherheitsraum TDR-A, Haus-im-Haus-System

Einzigartige Kombination aus Schutz und Flexibilität. Einmalige Investition, langfristige Nutzung.

Hersteller: Lampertz GmbH, Industriestraße 10, 42699 Solingen, Tel. +49 (0) 212 300-1000, Fax +49 (0) 212 300-1001, www.lampertz.de

### Lampertz TECHNO-DATA modulier IT-Sicherheitsraum TDR-B/W, Haus-im-Haus-System

Einzigartige Kombination aus Schutz und Flexibilität. Einmalige Investition, langfristige Nutzung.



Hersteller: Lampertz GmbH, Industriestraße 10, 42699 Solingen, Tel. +49 (0) 212 300-1000, Fax +49 (0) 212 300-1001, www.lampertz.de



### Lampertz MODUL-DATA IT-Systemraum MDS-BE33, Haus-im-Haus-System

Einzigartige Kombination aus Schutz und Flexibilität. Einmalige Investition, langfristige Nutzung.

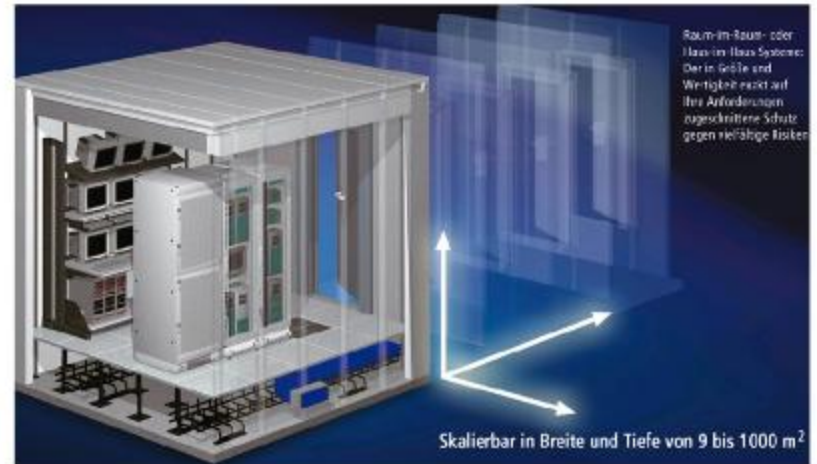
Hersteller: Lampertz GmbH, Industriestraße 10, 42699 Solingen, Tel. +49 (0) 212 300-1000, Fax +49 (0) 212 300-1001, www.lampertz.de

### Lampertz MODUL-DATA IT-Systemraum MDS-5050

Einzigartige Kombination aus Schutz und Flexibilität. Einmalige Investition, langfristige Nutzung.

Hersteller: Lampertz GmbH, Industriestraße 10, 42699 Solingen, Tel. +49 (0) 212 300-1000, Fax +49 (0) 212 300-1001, www.lampertz.de

## Maßgeschneidert - für optimale Sicherheit



Raum-im-Raum- oder Haus-im-Haus-Systeme: Der in Größe und Wertigkeit exakt auf Ihre Anforderungen zugeschnittene Schutz gegen vielfache Risiken

Skalierbar in Breite und Tiefe von 9 bis 1000 m<sup>2</sup>

## Komplettservice



## Projektausführung

Die komplette Realisierung Ihres IT-DataCenters!



Umfassende Generalunternehmerschaft einschließlich der gesamten technischen Infrastruktur mit Festpreisgarantie, Projektsteuerung und Bauüberwachung.

- Modulare Hochverfügbarkeits-IT-Sicherheitsräume
- Modulare IT-Systemräume
- Klimatisierung
- Brandfrüherkennung
- Brandmelde- und Löschanlagen
- Elektrotechnische Ausführung
- USV-Anlagen/Netzschutzanlagen
- Zutrittskontrollsysteme

**Ziel:** Turn-Key-Lösungen aus einer Hand



## Zertifizierung



### Die Zukunft: Zertifizierte und auditierte IT-Infrastrukturen!

Innovative Ansätze als Antwort auf gestiegene Anforderungen

- Neue Rechtsgrundlagen und Unternehmensbewertungen (Basel II) führen zur Verschärfung
- Fehlende Standards in der Risikoanalyse und -bewertung vergrößern die Problematik

Die Lösung sind neue, spezifische IT-Sicherheitskonzepte, die in eine Zertifizierung der vollständigen IT-Infrastruktur münden und selbstverständlicher Teil des unternehmensweiten Risikomanagements sind – auch TÜV-zertifiziert.

**Ziel:** Sicherheit durch neutrale Bewertung.



## Lampertz IT-Sicherheitsraum - der modulare Aufbau -



## Produktreihe: Testierter Grundschutz - Zertifizierter Vollschutz für denzentrale Standorte oder als Mini-Rechenzentrum



Tolerierbare IT-Ausfallzeit in Std.

0 20 40 60 80

Schutzbedarf  
Verfügbarkeit



## Lampertz-TECHNO DATA Modulsafe = Denken in Gesamtlösungen



## Referenzen

- ein Auszug (über 2.000 DataCenter - made by Lampertz)



AT&T, Brasilien - Audi AG, Ingolstadt - Bank of America, Madrid - Bayer AG, Leverkusen  
- BFA, Berlin - BMW Rolls-Royce, Berlin - BNP, France - BRAAS, Heusenstamm -  
British Airways, UK - Citibank, France, USA & Canada - Commerzbank, Frankfurt -  
Daimler-Chrysler, Sindelfingen - DEBIS, München - Deutsche Bank, Frankfurt &  
Luxembourg - Deutsche Flugsicherung, Offenbach - Deutsche Telekom, Düsseldorf -  
D.H.L., UK - DINERS CLUB, Belgien - DVS, Berlin - EMI Electrola, Köln - Ericsson,  
Spanien - Eurocontrol, Belgien - Gillette, Berlin & Spanien - Gerling, Köln - Hans Grohe,  
Schitach - Gruner & Jahr, Berlin - Hewlett Packard, UK - Hyundai Motor, Korea - IBM,  
Berlin, Stuttgart, Israel & Belgien - Langnese - Iglo, Hamburg - L'OREAL, France - MAN,  
Augsburg - Mercedes Benz, Sindelfingen & Spanien - Mercury, Israel - Ministere de la  
Defense, France - Mobil Oil, UK - Nestlé, Mexico - Nissan, UK - Nokia Telecom, FIN -  
OCÉ, Holland - ORACLE, France - Peugeot, France - PHILIPS, Belgien - Pittsburg  
State University, USA - Prominvest-Bank, Ukraine - SAP, Holland - Schlund &  
Partner, Karlsruhe - Securities Commission, Malaysia - Siemens AG, München &  
Brasilien - SHELL, Malaysia - Sony, Canada & UK - Spoerle, Dreieich - Staatl.  
Umweltamt, Münster - Stadt Hagen, Hagen - STATIOL, Norway - Unilever, France -  
UNISYS, Canada - VAG Leasing, Braunschweig - Warsteiner Brauerei,  
Warstein - Web.de, Karlsruhe, West LB, Polen etc. ...



„Die Natur steht immer auf der Seite  
des verborgenen Fehlers und damit  
gegen den agierenden Menschen“

Edward A. Murphy Jr.,  
Ingenieur US Airforce