# Mehr Sicherheit für Gebäude / Rechenzentrum

## Von der Prävention zur Reaktion bei infrastrukturellen Schadensereignisse

## – dezentrales Notfallmanagement zur Vermeidung von Informationsverlusten

**Workshop Informationssicherheit, Hochschule Bremen**

**06. November 2009**

## Inhalte

- Einleitung – Warum reden wir darüber
- Gefährdungspotentiale und geeignete Gegenmaßnahmen
- Schutz und Sicherungsmaßnahmen - Referenzszenarien
- Meldeketten
- Prävention
- Allgemeine Rahmenbedingungen und Informationen

# Das sagen Sicherheitsfachleute

## Wirtschaft: Angriffe auf IT größter Risikofaktor

**Gefährdungen bleiben auf hohem Niveau – Budgets für Sicherheit steigen weiterhin an**

„Die höchste aktuelle und künftige Gefährdung für die Wirtschaft stellen für eine Mehrheit der Sicherheitsexperten Angriffe auf die **IT und Telekommunikation** dar. Zu diesem Ergebnis kommt die neunte WIK/ASW-Sicherheits-Enquête. Aber auch die Gefährdungen durch Spionage, allgemeine Kriminalität und Terrorismus bleiben auf anhaltend hohem Niveau und werden nach Meinung der Sicherheitsfachleute in den nächsten Jahren wachsen.“

**Quelle: BHE - September 2009**

# Das sagen Sicherheitsfachleute

**Studie der Association of British Insurers**

- **Alle 2,8 Jahre treten unternehmenskritische Ereignisse auf.**
- **In 88% der Fälle sind Unternehmensbereiche betroffen, für die es keine konkrete Notfallplanung gibt.**
- **In 43 % der Fälle dauerte es länger als 2 Monate, bis die Folgen derartiger Schadensereignisse beseitigt waren.**
- **Der Betriebsunterbrechungsanteil der Schäden steigt stetig.**

# Warum wir darüber reden

## Die Sicherheitslage in Deutschland

- Im Gewerbe, in Verkaufsstätten, aber auch im Büro und Kanzleien und privaten Bereich entstehen jährlich hohe Schäden durch Einbruchdiebstahl und Schadenfeuer.

- So weist die „Polizeiliche Kriminalstatistik“ für das Jahr 2006 1.018.165 „schwere Diebstähle“ mit einer Schadenssumme von 1.480 Mio. Euro aus.

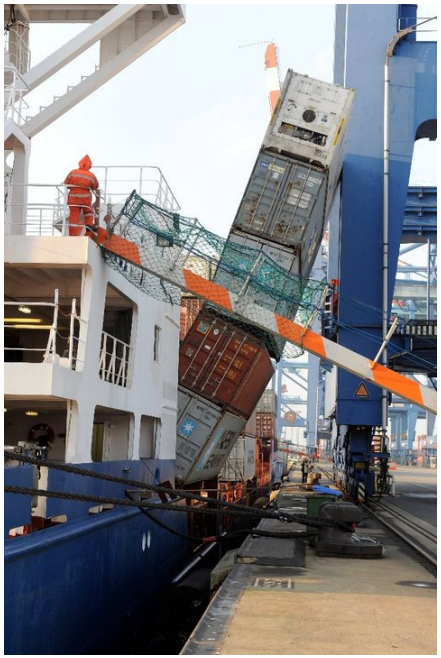
- Nach Angaben des „Deutschen Feuerwehr Verbandes“ verursachten die 10 größten Brände in Handel, Gewerbe und Industrie in den letzten Jahren eine Schadenssumme von 390 Mio. Euro.

  Der größte Einzelschaden belief sich dabei auf 117 Mio. Euro.

# Aktuelle Ereignisse*

* Brandkatastrophe am 27.10.2009 in Bremen, bei der Finnforest GmbH

# Aktuelle Ereignisse*



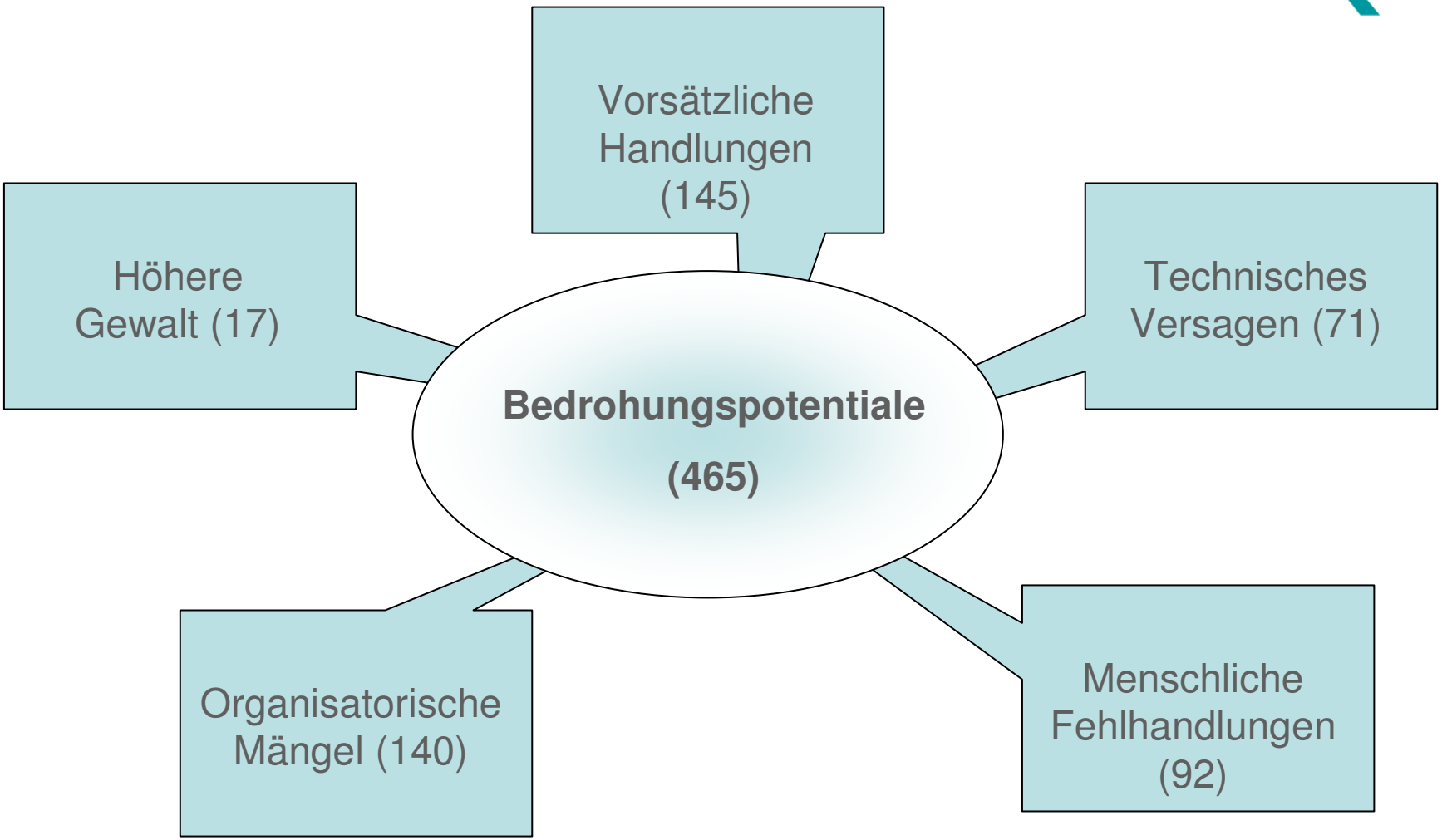
* 18 Container stürzen in die Weser – 34 weitere auf dem Schiff verutscht (BHV, 03.11.2009

# Beispiel aus der Praxis

# Gefährdungspotential

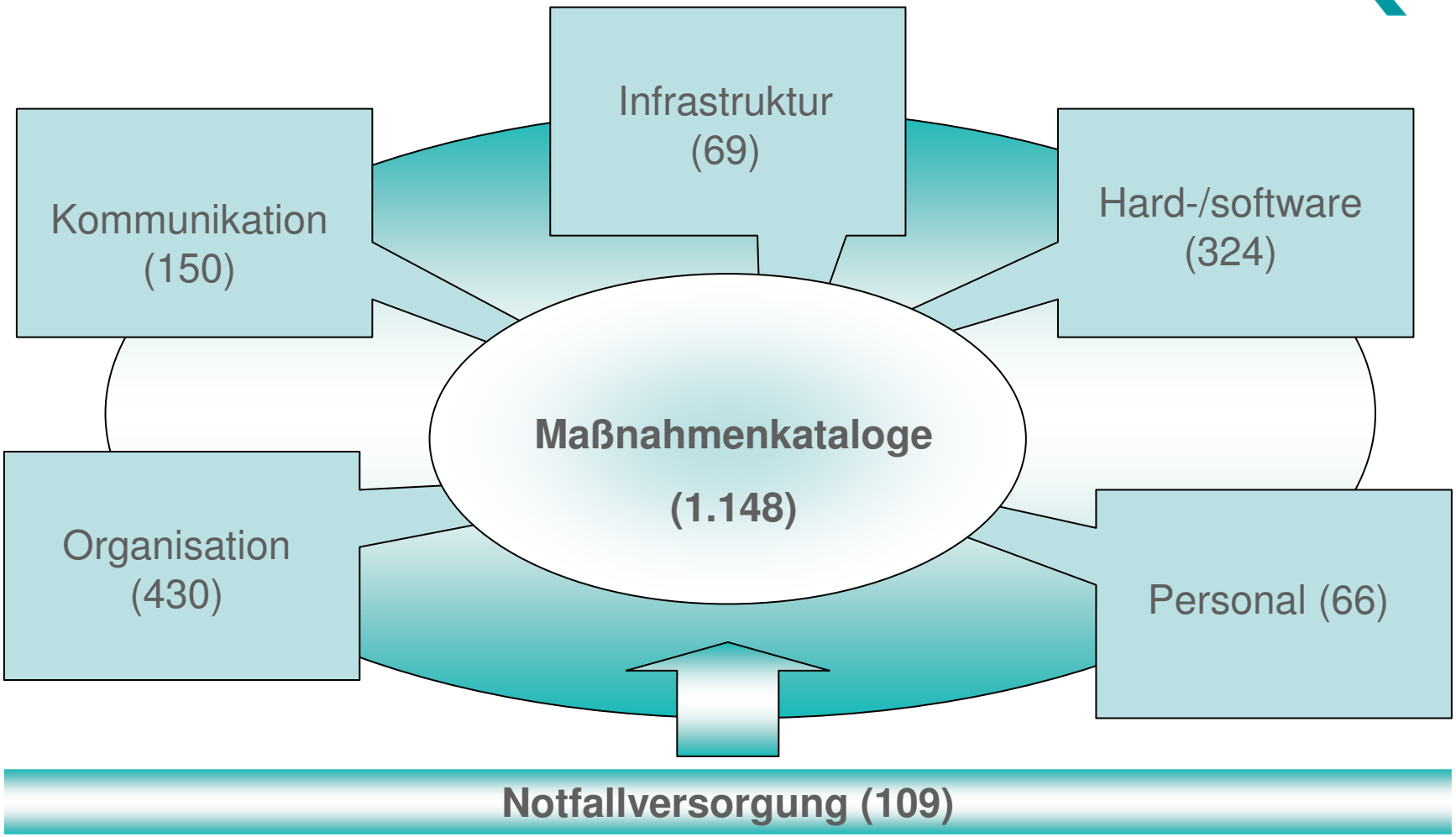
| Art der Gefahr | Möglicher Zustand | Mögliche Wirkung |
|---|---|---|
| Blitz, Feuer, Wasser | Hohes Schädigungspotential | Beeinträchtigung des Personals, der Kunden, des Gebäudes und Anlagen |
| Nutzung von Gebäudebereiche durch Fremdfirmen | Zutritt wurde nicht angemeldet | Bedrohung der Personen im Brandfall |
| Unbefugter Zutritt zu schutzbedürftigen Räumen | Hohes Schädigungspotential | Beeinträchtigung von Anlagen und Geräten |
| **Diebstahl kritischer Geräte oder Informationen** | Hohes Schädigungspotential | Beeinträchtigung von Daten und Unterlagen **Reputationsverlust** |
| Vorsätzliche Handlung mit IT-Systemen | Schnelle Verbreitung von Informationen | Beeinträchtigung von Daten oder Produkten **Reputationsverlust** |
| Öffentliche und halb-öffentliche Bereiche | Unkontrollierter Zutritt | Beeinträchtigung von Personal und Unterlagen **Reputationsverlust** |
| **Sprengstoffanschlag** | Hohe Zerstörungskraft | Beeinträchtigung des Personals, der Kunden und Anlagen, Trümmerbildung |

# Gefährdungskataloge (BSI* - IT-Grundschutzkataloge)




*Budesamt für Sicherheit in der Informationstechnik

# Maßnahmenkataloge (BSI* - IT-Grundschutzkataloge)




*Budesamt für Sicherheit in der Informationstechnik

# Gefährdungskataloge u. Maßnahmen

## (BSI* - IT-Grundschutzkataloge) - Beispielhafter Auszug

| Höhere Gewalt | Organisatorische Mängel | Menschliche Fehlhandlungen | Technisches Versagen | Vorsätzliche Handlungen |
|---|---|---|---|---|
| **Gefährdungskataloge** | | | | |
| ■ Personalausfall<br>■ Blitz<br>■ Feuer<br>■ Wasser | ■ Defizitäre Reglements<br>■ Zutrittsregelungen<br>■ Sicherheitsverständnis<br>■ Einstufung von Bereichen öffentlich, halböffentlich | ■ Zuverlässigkeit<br>■ Sorglosigkeit<br>■ Bedienfehler<br>■ Verletzung von Brandschottungen | ■ Versagen der Informationstechnik<br>■ Ausfall der Stromversorgung<br>■ Ausfall vorhandener Sicherheitssysteme | ■ Unbefugtes Eindringen<br>■ Diebstahl<br>■ Vandalismus<br>■ Anschlag |
| **Maßnahmenkataloge** | | | | |
| ■ Vertreterregelungen<br>■ Bauliche Abschottung<br>■ Brandschutz<br>■ Unkontrollierten Eintritt verhindern | ■ Reglementieren/ sensibilisieren, schulen „clean desk policy“<br>■ Schlüsselordnung<br>■ Sicherheitskultur<br>■ Zutrittsregelung | ■ Sicherheitsüberprüfungen oder -vereinbarungen<br>■ Sensibilisieren<br>■ Unterweisen<br>■ Audits und Berichte | ■ Betriebsersatzlösungen<br>■ Redundanzen<br>■ Ständige Kontrolle bzw. Betriebsersatzlösungen | ■ Infrastrukturelle Sichh.<br>■ organisatorische Maßnahmen<br>■ Zusammenarbeit mit Behörden<br>■ Präventive Maßnahmen<br>■ Informationsbeschaffung |

*Budesamt für Sicherheit in der Informationstechnik

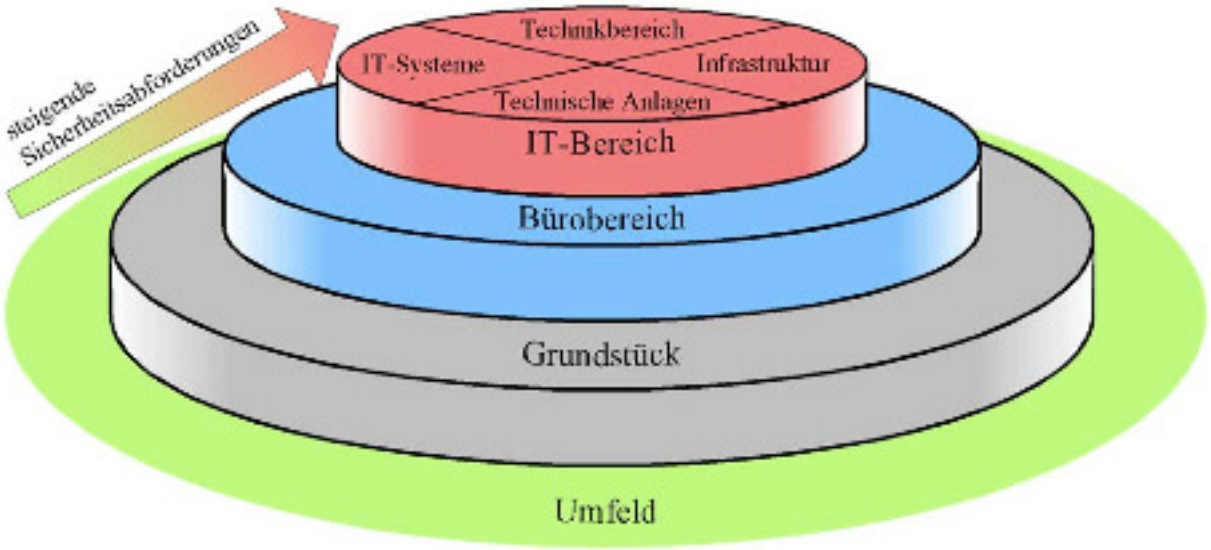
# Schutzziele einer Gefahrenabwehr

- Schutz von Leib und Leben
- Schutz von Know-how und Sachwerten
- Kontinuität der betrieblichen Prozesse
- Frühzeitige Erkennung und Meldung von Schadensereignisse
- Schaffung von Interventionsmöglichkeiten durch eine sinnvolle Kombination von Sicherungsmaßnahmen
- Anpassung der Sicherungsmaßnahmen an die betrieblichen Gegebenheiten

## Schutz vor Schadensereignisse

- Um die Schutzziele zu erreichen bedarf es eines  sinnvollen, dem jeweiligen Sicherungsziel angepasstes Schutzkonzept.
- Wie bei einer Zwiebelschale erfolgt von außen nach innen eine Festlegung von Sicherheitszonen.
- Den Sicherheitszonen werden geeignete Schutzmaßnahmen zugeordnet.
- Dabei werden bauliche, technische und organisatorische Sicherungsmaßnahmen kombiniert.

# Schutz vor Schadensereignisse




Quelle: BSI – Anordnung der Sicherheitszonen

# Schutz vor Schadensereignisse

## baulich

- **Mechanische Sicherungen der Außengrenzen**
- Einbruchhemmende Ausführung von Fenstern und Türen
- Massive Bauweise von Wänden, Decken, Böden und Dach
- Einhaltung von Brandschutzvorschriften
- Äußere Blitzschutzanlage

## technisch

- Perimterschutz
- Überfall- und Einbruchmeldeanlage
- Diebstahlsicherung
- Brandmeldeanlage
- Videotechnik
- **Zutrittskontrolle unter Berücksichtigung von Flucht und Rettungswegen**
- Innerer Blitzschutz
- Notstromversorgung
- Fernanzeige von Störungen

## organisatorisch

- Zutrittsregelung zu schutzbedürftigen Räumen
- Geeignete Aufbewahrung von mobilen IT-Geräten
- Geeignete Aufbewahrung von dienstlichen Unterlagen
- Raumbelegung unter Berücksichtigung von Brandlasten
- **Geeignete Aufstellung von Druckern, Kopierern und Faxgeräten**
- Verfügbarkeit von aktueller und vollständiger Dokumentation

**Voraussetzung ist immer geschultes Personal**

# Schutz vor Schadensereignisse

## Referenzszenarien

Automobillogistik & Maschinenbau

- Bereich Außenflächen
  - Selbst umfassende Sicherheitskonzepte vernachlässigen häufig die Außenbereiche.
  - Unverständlich, denn gerade die Außenbereiche sind leicht erreichbare Ziele für Sabotage und Vandalismus.
  - Auch weitläufige Freiflächen können effektiv geschützt werden.

- Sicherheitslösungen für Außenflächen
  - Eine Zaunanlage zur klaren Kennzeichnung der Außengrenze.
  - Eine Videoüberwachung ermöglicht die Fernüberwachung.
  - Installierte Zaunüberwachungsanlagen haben zusätzlich eine abschreckende Wirkung.
  - Im Ereignisfall ergreift der Werkschutz anhand differenzierter Meldungen sofort die richtigen Interventionsmaßnahmen.

# Sicherung der Außengrenzen

## Anforderungen an eine Zaunanlage

- Ziel ist es, das Übersteigen und das Durchdringen zu erschweren.
  - Ausreichende Zaunhöhe inkl. Übersteigschutz.
  - Feste Verankerung der Zaunpfosten im Erdreich.
  - Zaunelemente sollten demontagesicher mit den Zaunpfosten verbunden sein.
  - Streifen- und Kontrollweg vorsehen.
  - Übersteighilfen und/oder Deckungsmöglichkeiten sollten entfernt werden.

# Sicherung der Außengrenzen

## Anforderungen an eine Zaunanlage

# Sicherung der Außengrenzen

## Anforderungen an eine Zaunanlage

# Sicherung der Außengrenzen

## Anforderungen an eine Zaunanlage

# Schutz vor Schadensereignisse

## Referenzszenarien

Bürogebäude der IT, Telekommunikation & Energieindustrie

- Sicherheitslösungen Eingangsbereich

  - Eine Videoüberwachung eignet sich ideal zur Fernüberwachung des Eingangsbereichs z.B. von der Pförtnerloge aus.
  - Zudem schützt eine Videoanlage im Innenbereich vor Betriebsspionage.
  - Als Teil der Zutrittskontrolle fährt der Aufzug nur die Stockwerke an, für die sich der Mitarbeiter oder Besucher zuvor per Chipkarte autorisiert hat.

# Sicherung der Außenbereiche

## Videoüberwachungsanlage

- Rechtliche Zulässigkeit
- Gerichtsverwertbarkeit digitaler Bilder
- Digitale versus analoge Videotechnik – Vor- und Nachteile

# Videoüberwachungsanlage

## Rechtliche Zulässigkeit – Videoüberwachung in Betrieben

- Betriebsverfassungsgesetz, § 87 Abs. 1

  Der Betriebsrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, in folgenden Angelegenheiten mitzubestimmen:

  Nr. 6. Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.

- Diese Mitbestimmung nach dem Gesetzeszweck dient aber nicht der Verhinderung einer Einführung der Videoüberwachung.

- Die Interessen beider Seiten sollen berücksichtig werden.

- Bei stichhaltigen Gründen kann sich der Betriebsrat nicht gegen die Einführung einer Videoüberwachung aussprechen.

**Empfehlung**: Rechtzeitige Einbindung des Betriebsrats schon in der Planungsphase.

# Videoüberwachungsanlage

## Rechtliche Zulässigkeit – Videoüberwachung in Betrieben

- Einigung über folgende Punkte treffen:
  - Beschaffung erfolgt unter Wahrung der Arbeitnehmerinteressen
  - Festlegung der Zweckbestimmung
  - Bestimmung aller Anlagenkomponenten
  - Regelung der Zugriffsberechtigungen auf die Bilddatenbank
  - Art und Aufbewahrungsdauer der Speichermedien
  - Wie und wann erfolgt die Speicherung von Daten
  - Wie sollen die Bildinformationen genutzt werden
  - Wie und unter welchen Umständen werden Informationen weitergegeben
  - Wer hat Zugriff auf die Videoanlage
  - Zeitpunkt der Inbetriebnahme
  - Festlegung der geplanten Betriebszeit

**Empfehlung**: Die Regelungen über den Einsatz einer Videoanlage sind in einer Betriebsvereinbarung schriftlich zu dokumentieren.

# Sicherung der Außenbereiche

## Videoüberwachungsanlage – Gerichtsverwertbarkeit digitaler Bilder

Der Grundsatz: Die Gerichte entscheiden in richterlicher Unabhängigkeit, welche Beweise Sie in einem Prozess zulassen.

Videosysteme: Das Ziel ist Straftaten zu verhindern und/oder kriminelle Vorgänge zu dokumentieren.

Problematik: Im deutschen Rechtssystem müssen Beweismittel bestimmten Anforderungen genügen.

- Die geschlossene Beweiskette:
  - Sicherstellung, dass Beweisbilder die Bilder des Vorfalls sind
  - Manipulationssichere Ablage der Bilddaten auf einem Datenträger
  - Aussagefähiger Dateiname sollte vom System bestimmt werden
  - Bei Datenspeicherung sollten die Namen der anwesenden Personen mit Datum und Uhrzeit mit gespeichert werden
  - Der Datenträger sollte von dem Ermittler unveränderbar gekennzeichnet werden
  - Aussagekräftige Bilder

# Sicherung der Außenbereiche

## Videoüberwachung – Digitale versus analoge Videotechnik

### Vorteile

- Durch höhere Auflösungen bessere Detailerkennung
- Einfachere Konfiguration
- Schneller Systemerweiterung von einzelnen Kameras
- Weniger Störeinflüsse durch digitale Signalübertragung
- Bei kleineren Anlagen ist die Nutzung der vorhandenen Infrastruktur möglich

### Nachteile

- Lichtempfindlichkeit, Farbtreue bei wenig Licht und Dynamik oft nicht ausreichend
- Bildraten oft nicht in Echtzeit möglich
- IP-Kameras verschiedener Hersteller untereinander nicht kompatibel
- Bei Bewegtbildern kommt es bei der Bedienung von Schwenk/Neige-Kameras häufig zu Latenzzeiten

**Videoüberwachungsanlagen beobachten das Geschehen vor Ort**

# Sicherung der Außenbereiche

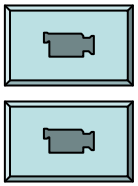
## Videoüberwachungsanlage

# Sicherung der Außenbereiche

## Videoüberwachungsanlage

# Sicherung der Außenbereiche

Videoüberwachungsanlage

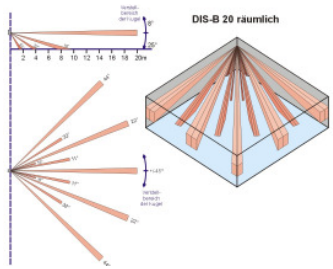


# Schutz vor Schadensereignisse

## Referenzszenarien

Museen und Galerien

- Sicherheitslösungen Außenhaut
  - Eine Einbruchmeldeanlage sichert Türen und Fenster gegen Durchstieg und unerlaubtes Öffnen.
  - Eine Videoanlage im Innenbereich ermöglicht eine ereignisgesteuerte Überwachung.
  - Im Einbruchsfall wird ein Alarm an eine „Hilfe-Leistende-Stelle“ weitergeleitet.



# Schutz gegen Einbruchdiebstahl

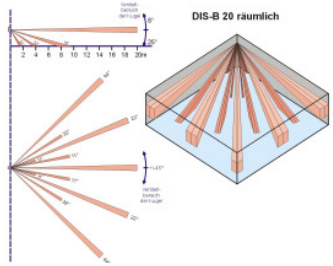
## Einbruchmeldeanlage

- Um die Anforderungen an eine Überfall- und Einbruchmeldeanlage erfüllen zu können, wurde von den Sachversicherern eine Richtlinie für die Planung und den Einbau herausgegeben.

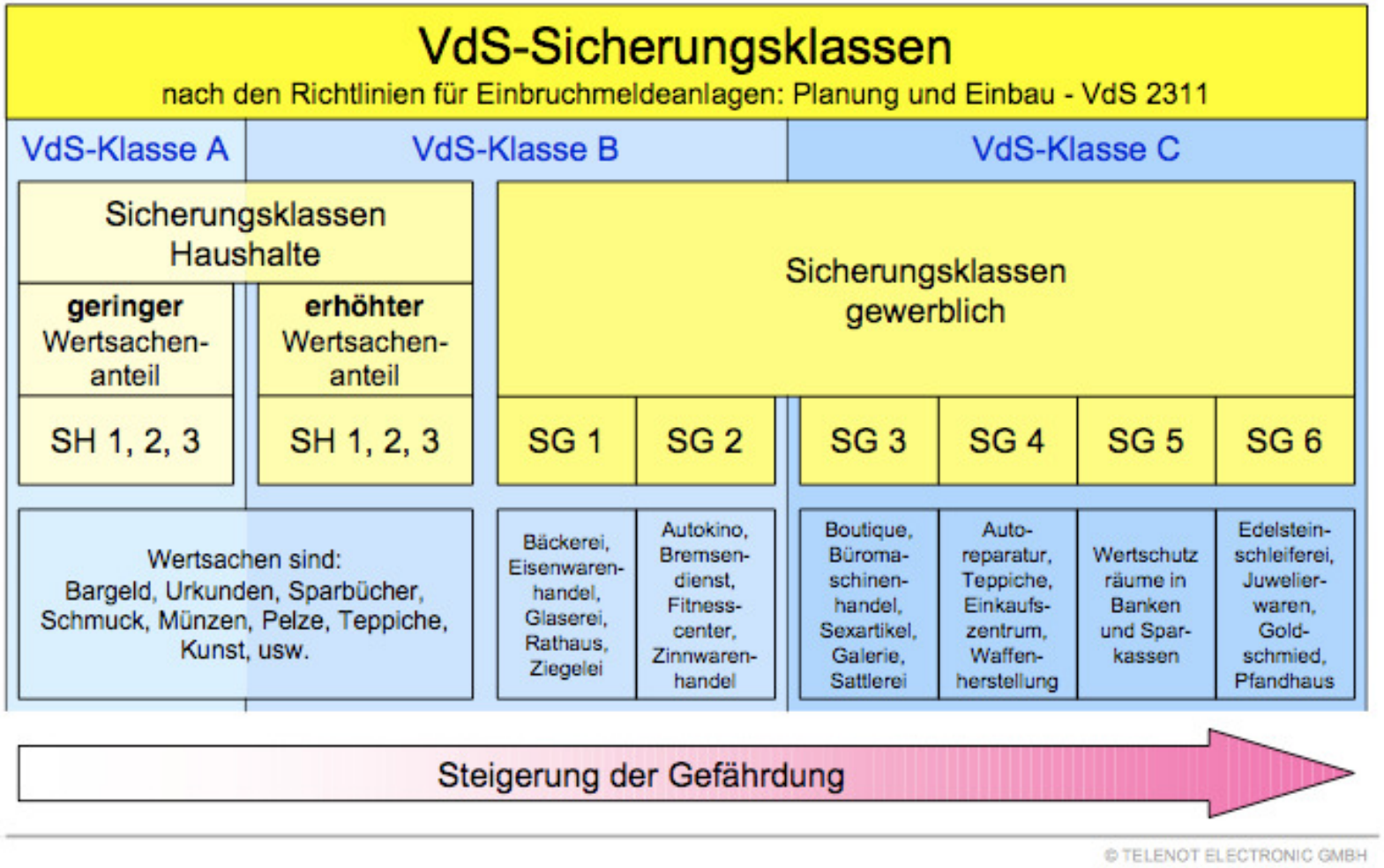
- Der Umfang der erforderlichen Überwachungsmaßnahmen richtet sich dabei nach der Gefährdung des Objektes.

- Zur Differenzierung werden die zu überwachenden Objekte in Sicherungsklassen eingeteilt.

- Die Richtlinie beinhaltet ein „Betriebsartenverzeichnis“, aus dem für die unterschiedlichsten Gewerbeobjekte die entsprechende Sicherungsklasse herausgesucht werden kann.



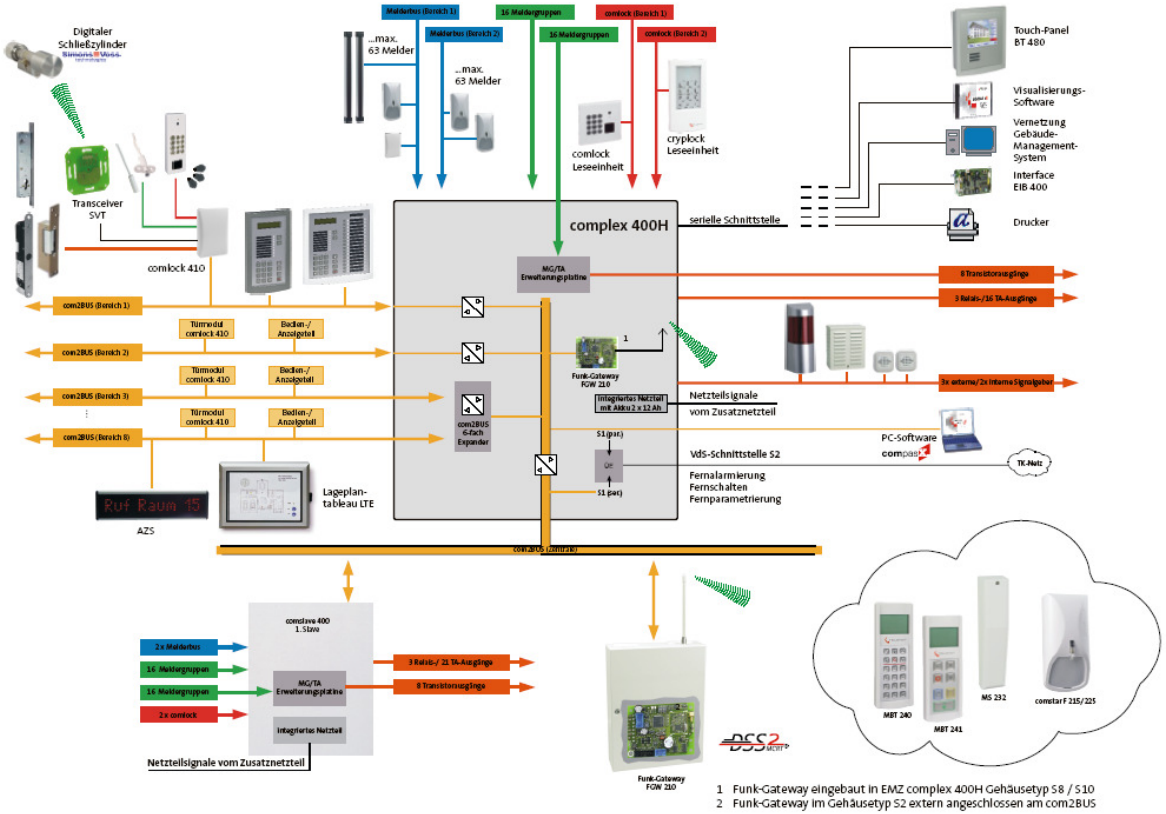
# Schutz gegen Einbruchdiebstahl




**Einbruchmeldeanlagen machen auf den Einbruch aufmerksam**

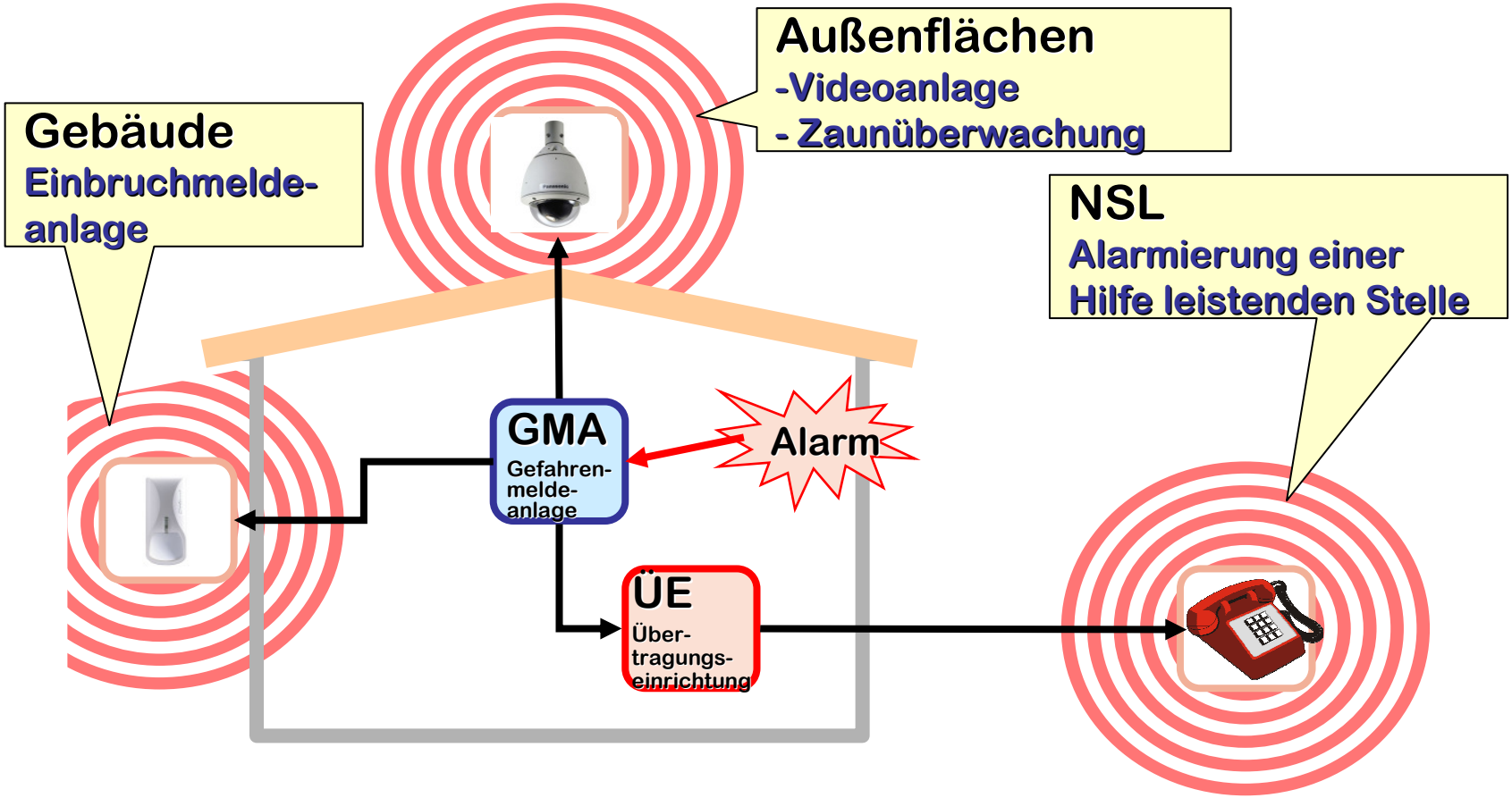
# Schutz vor Schadensereignisse

## Gefahrenmeldeanlagen



# Schutz vor Schadensereignisse

## Gefahrenmeldeanlagen



# Schutz vor Schadensereignisse

## Referenzszenarien

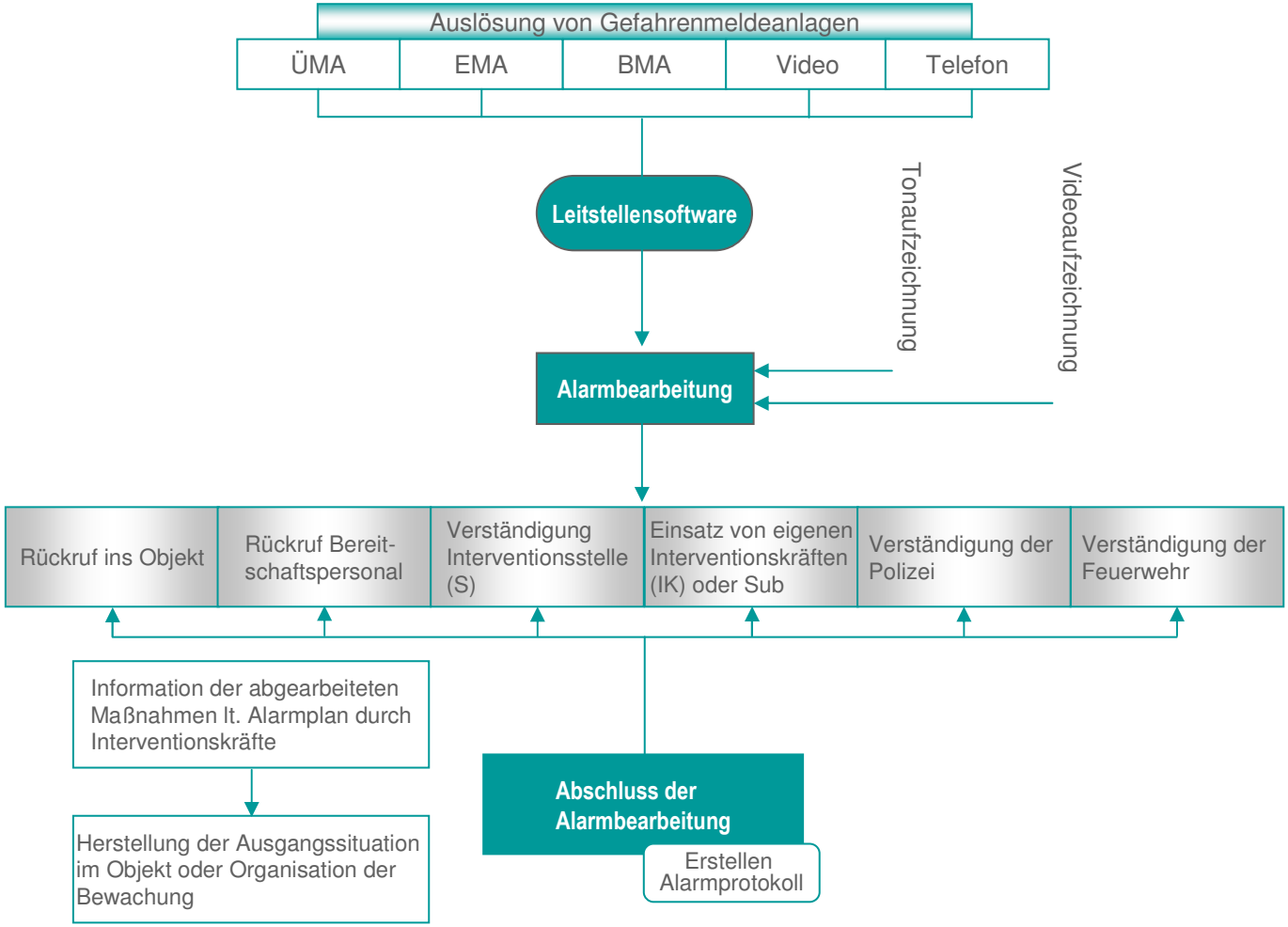
Hafenlogistik

- Sicherheitslösungen Gate - Zufahrts- u. Zutrittskontrollen

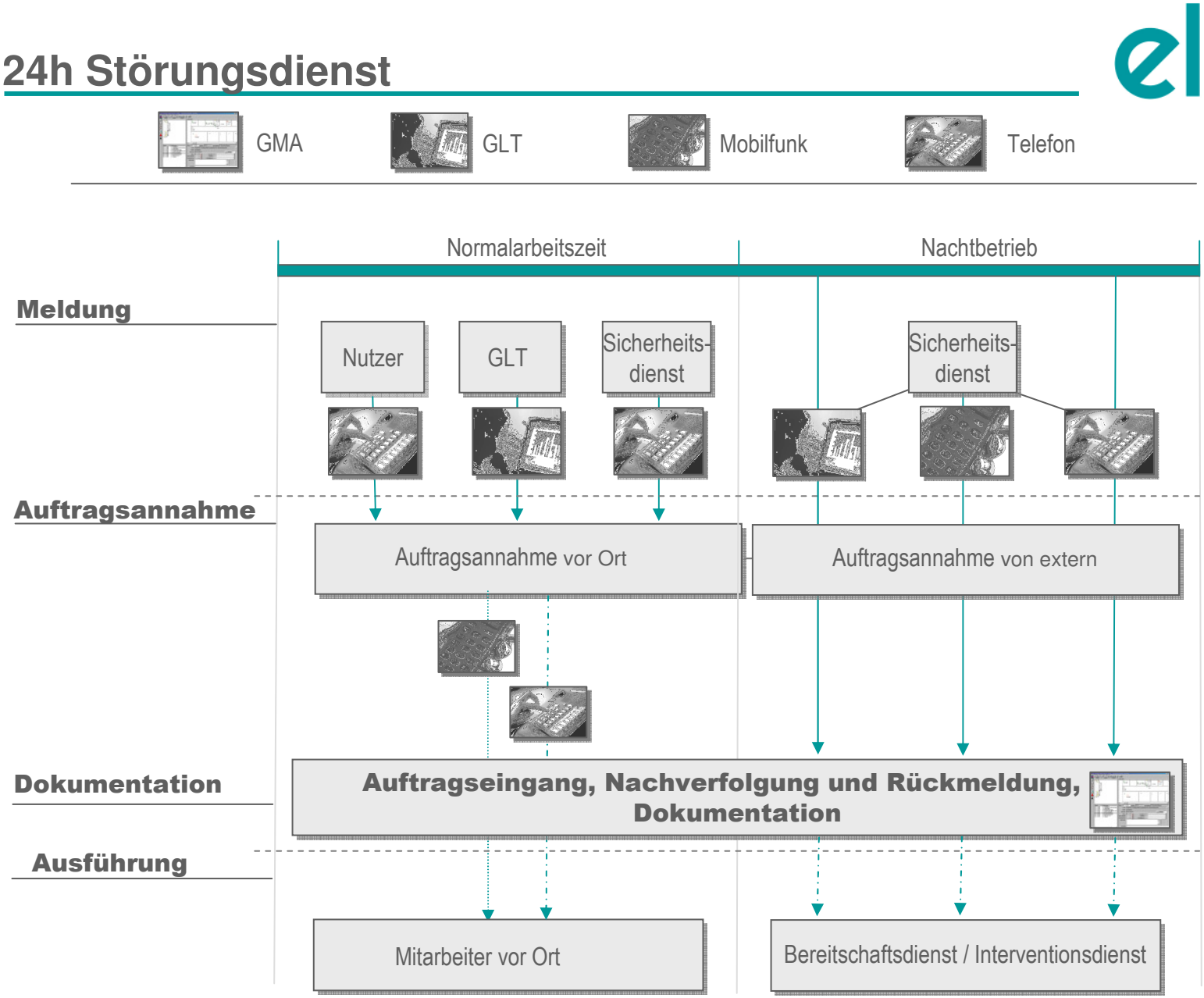
  - Diese Bereiche benötigen baulich-/technische-, personelle- u. organisatorische Lösungen.
  - Personen-, Fahrzeuge und Ladungen müssen kontrolliert werden.
  - Ein Schiebetor und eine Schranke schützen die Zufahrt.
  - Kameras überwachen den gesamten Bereich.
  - Vor Eintritt von außen schützt eine Vereinzelungsanlage mit Zutrittskontrolle.
  - Sicherheitspersonal u. Behörden führen die Kontrollen durch.

# Alarmbearbeitung

## Am Beispiel einer Notruf- u. Serviceleitstelle (NSL)



# 24h Störungsdienst



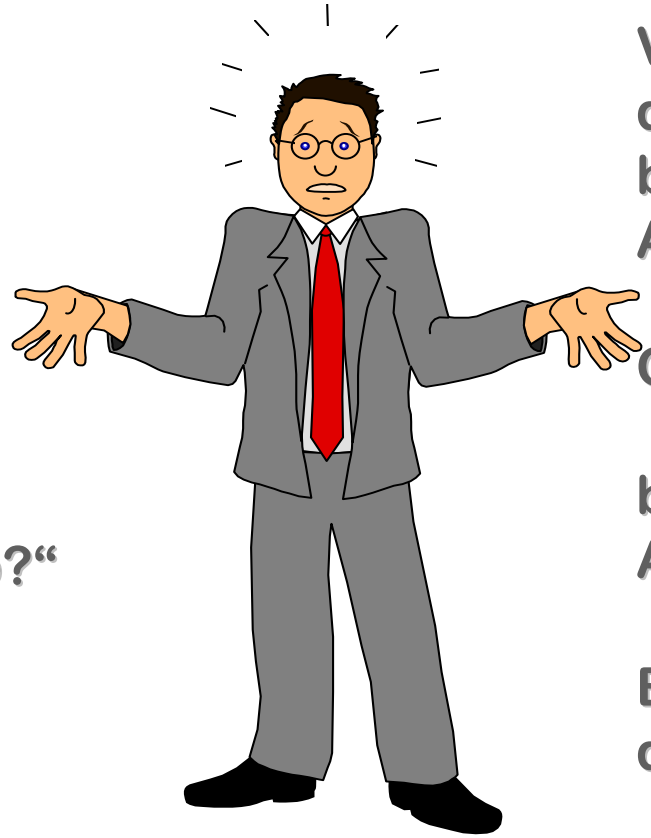
## Schutz vor Schadensereignisse

Gefährdung durch

Brand
Einbruch
Vandalismus

Zutrittskontrolle
„Wer ist im Betrieb?“

Überwachung
technischer
Anlagen



Verantwortung für
den Schutz der
beschäftigten
Arbeitnehmer

Gesetze

behördliche
Auflagen

Bestimmungen
des Versicherers

usw.

# Präventive Gefahrenabwehr - Prinzipsskizze

**Security Assessment**

**Infrastruktur**
Erfassung bestehender Infrastruktur

**Gefährdungsszenarien**
Denkbare Bedrohungen und Gefahrensituationen

**Auswirkungsszenarien**
Auswirkungen bei Eintritt/worst case scenario

**Wahrscheinlichkeit**
Wahrscheinlichkeit des Eintrittsfalls/Likelihood

**Prävention**
Vorbeugung und Gefahrenabwehr

**Eintrittsfall**
Maßnahmen zur Krisenbewältigung

# Anforderungen an ein Sicherheitskonzept

**Am Anfang der Planung steht immer eine individuelle Prüfung der örtlichen Begebenheiten – der Analyse!**

**Kriterien für ein Sicherheitskonzept:**

- ✓ **Beachtung sämtlicher objektspezifischer Begebenheiten**
- ✓ **Optimale Überwachung**
- ✓ **Hoher Widerstandswert der Absicherung**
- ✓ **Frühzeitige Gefahrenerkennung**
- ✓ **Einfache Handhabung**
- ✓ **Zuverlässigkeit der Alarmabgabe, Bearbeitung u. Dokumentation**
- ✓ **Regelmäßige Wartung (Technik) bzw. Überprüfung (Prozesse)**
- ✓ **Problemlose Erweiterung/ Anpassung des Konzeptes**
- ✓ **Einweisung, Sensibilisierung, Schulung des Personals**
- ✓ **Durchführung von Sicherheitsübungen**
- ✓ **Regelmäßige Kontrollen und Auswertungen**

***…ein Sicherheitskonzept muss immer flexibel sein und sich den Begebenheiten anpassen – nicht umgekehrt…!!***

# Maßnahmenkatalog - Notfallvorsorge

- Durchführung von Sicherheits- u. Risikoanalysen
- Erstellung eines Notfallhandbuches
- Alarmierungs- u. Notfallplans
- Regelmäßige Audits
- Durchführung von Übungen
- Durchführung von Schulungen
- Dokumentation und Berichtswesen – Auswertung u. Anpassung der Maßnahmen
- Verantwortung der Kommunikation und Steuerung von Informationen
- Versicherungsschutz
- Beschaffungsplan u. Lieferantenvereinbarungen
- Kooperation mit Sicherheitsbehörden u. -dienstleistern
- Ausfallplanung – Sicherstellung der Betriebstätigkeiten (ggf. Notbetrieb) und Wiederanlaufplan

# Was können Sie tun?!

- Augen auf…
- Daten immer sichern…
- keine sensiblen Daten/ Informationen offen liegen lassen…
- IT immer ausschalten, bzw. vor unbefugtem Zugriff schützen…
- Regeln einhalten…
- Sich selbst und andere ständig „überprüfen“…
- Verschwiegenheit…
- Zuverlässigkeit…
- Meldewesen

# Sicherheitspolitische Rahmenbedingungen

- Globale Sicherheitslage
- Vernetzung von internen und extern Leistungen bei den „Bedarfern“
- Sicherheitsrelevante Gesetzesinitiativen (national u. international)
    - + Sicherheit von Hafenanlagen (VO (EU) 725/2004*[1] und 65/2005*[2])
    - + Sicherheit im Luftverkehr „Reglementierter Beauftragter“ u. „Sicherer Versender“
    - + Zollcodex (EU) „zugelassener Wirtschaftsbeteiligter“ (ZWB)
    - + Transportkettensicherheit (100% Containerscanning 2012, „Antiterrorgesetz“)
    - + EU-Initiative „Sicherheit in der Transportkette“
    - + EU-Initiative „Sicherheit von gefährdeter Infrastruktur“

**Diese Rahmenbedingungen fordern spezialisierte und integrierte Branchenlösungen!**

*[1] Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ISPS-Code)

*[2] Erhöhung der Gefahrenabwehr in Häfen

# Schutz vor Schadensereignisse

## Gesetzliche Grundlagen, Verordnungen, Richtlinien, Vorgaben

- VDE 0100 „Starkstromanlagen bis 1000 V“
- VdS 2095 „Planung und Einbau BMA“
- VdS 2311 „Planung und Einbau EMA“
- Ausführung und Nutzung des Gebäudes
- Landesbauordnung, Feuerwehrbestimmungen
- Forderungen des Versicherers
- Gerätenormen
- DIN 31051 „Instandhaltung
- Nationales Baurecht
- Arbeitsstättenverordnung
- IT-Grundschutzkataloge BSI
- ...

# Zertifizierte Qualität

**Ein ausgeprägtes Qualitätsbewusstsein kennzeichnet das Handeln des Dienstleisters. Die Voraussetzungen hierfür sind die Gestaltung sicherer Abläufe auf der Grundlage von Zertifizierungen:**

- **DIN 77200 – Anforderungen an Sicherheitsdienstleistungen**
- **DIN EN ISO 9001:2000 – Qualitätsmanagement**
- **VdS-Zertifizierte Notrufleitstellen – Typ: A, B, C**
- **VdS anerkannte Errichterfirma für Einbruchmeldeanlagen**
- **VdS anerkannte Errichterfirma für Brandmeldeanlagen**
- **Fachfirma für Brandmeldeanlagen gem. DIN 14675**

# Interessante Verbände und Informationen

- Bundesverband deutscher
  Wach- und Sicherheitsunternehmen e.V. (BDWS)

- Bundesvereinigung deutscher
  Geld- und Werttransporteure e.V. (BDGW)

- Verband für Sicherheit in der Wirtschaft
  Norddeutschland e.V. (VSWN)

- Bundesverband der Hersteller- und Errichterfirmen
  von Sicherheitssystemen e.V. (BHE)

- Verband der Sachversicherer (VdS)

## Vielen Dank!

**)) Ihre Sicherheit ist unser Erfolg!**