



Hans - J. Grusewski

Beim Strohhouse 31
20097 Hamburg

Phone: +49 (0) 700 4455-1111

Fax: +49 (0) 700 4455-8888

Mobile: +49 (0) 172 6446 155

Mailto: Hans.Grusewski@Socius-Primus.de

<http://www.socius-primus.de>

IT – Sicherheit

Vom Einstieg in das sensible Thema,
über Risiken erkennen,
Vorsorge treffen,
Notfälle trainieren,
Mitarbeiter einbeziehen,
Kontinuität sicherstellen,
zum Managementprozess,
der Geld sparen hilft.

- ñ **Welchen Einflüssen bin ich als GF./GL. ausgesetzt?**
- ñ **Steht das Management in der persönlichen Haftung?**
- ñ **Welche Kosten & Aufwendungen kommen auf mich zu?**
- ñ **Wer hilft mir, wo gibt es Hilfe?**
- ñ **Welche Bereiche umfasst die IT-Sicherheit?**
- ñ **Wie steht dies zum Ratinggespräch nach Basel II?**
- ñ **Hat dies Auswirkung auf den WP Jahresabschlußbericht?**
- ñ **Welchen Nutzen habe ich als GF./GL.?**

IT - Sicherheit

ist nicht nur eine technische Herausforderung
sondern ein

Managementprozess

in der

Unternehmensführung

mit und für alle Mitarbeiter!

- **Die unternehmerische Verantwortung liegt in den Händen der Unternehmensleitung und muss von dort**
 - **angestoßen,**
 - **kontrolliert und**
 - **unterstützt werden.**

- **Die Einführung eines IT-Sicherheits-Managements ist mit klaren geschäftspolitischen Zielen verbunden,**
 - **die Vorteile mit sich bringen und**
 - **zur Stärkung und Festigung des Unternehmens im Markt führen!**

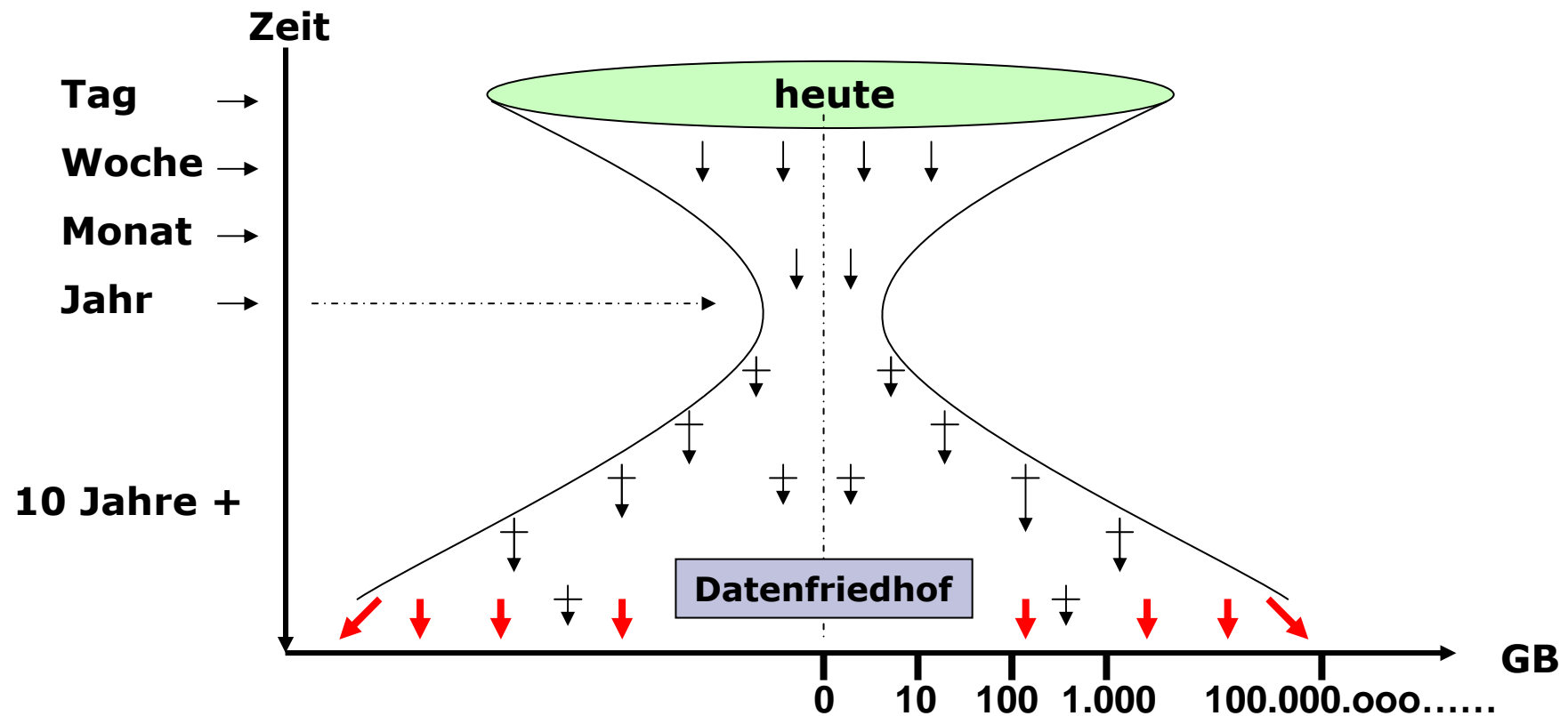
- **Erhalten der in Technik, Information und Forschung investierten digitalen Unternehmenswerte;**
- **Erfüllen gesetzlicher Rahmenbedingungen (Compliance);**
- **Bessere Konditionen für Kredite;**
- **Zeit- und Kostenersparnis bei Audits und Betriebsprüfungen;**
- **Minimieren von System- und Produktionsausfällen;**

- **Vermeiden von Reparatur- und Ersatzkosten;**
- **Reduzieren der Kosten im Schadensfall;**
- **Vermeiden von Imageverlusten;**
- **Vorteile bei der Auftragsvergabe und Kundengewinnung;**
- **Vermarktung von Schutzmaßnahmen als Qualitätsmerkmal.**

Der sichere (IT) - Betrieb

- ñ **Ein Glaubensgrundsatz?**
- ñ **Ein sicheres Versteck?**
- ñ **Ein sicheres Gefühl?**
- ñ **Ein Schutz mit Versicherungspolicen?**
- ñ **Der Einsatz von Risikomanagement?**
- ñ **Der Schutz von Gebäuden?**
- ñ **Der Schutz vor oder für Menschen?**
- ñ **Der Schutz vor Angriffen?**

Wann und wie soll migriert werden?



Sicherheit umfasst:

- ñ **Abwägung von Risiken,**
- ñ **Beobachtungen,**
- ñ **Erkenntnisse,**
- ñ **Gesetze, Richtlinien, betriebl. Vereinbarungen**
- ñ **Notfallübungen,**
- ñ **Reserven,**
- ñ **Überprüfungen,**
- ñ **Sensibilisierungen, Spionage**
- ñ **Schulungen / Trainings / Workshops,**
- ñ **Taten, Umsetzungen,**
- ñ **Veränderungen,**
- ñ **Verantwortung, innere Einstellung und**
- ñ **Vorsorge.**



1995 wurde Siemens bei einer Ausschreibung von Südkorea über die Lieferung von Hochgeschwindigkeitszügen durch den französischen Auslandsgeheimdienst „Direction Générale de la Sécurité Extérieure (DGSE) ausspioniert.

Der Auftrag ging an die Franzosen, die den TGV lieferten!

Bereiche die jeder kennt:

Schifffahrt: Schwimmwesten, Rettungsboote, Notfallübungen

Flugzeug: Einweisung durch die Stewardess, Notausgänge, Sauerstoffmasken, Sitzhaltung wenn ...

Katastrophenübungen: Rettungsdienste (Feuerwehr, THW, BW, DRK, ASB) Polizei, Fa. mit schwerem Gerät, usw.

Aus der Werbung:

Toffifee: Reserve im Küchenschrank,

TicTac: Vorsorge für frischen Atem,

AEG: Aus Erfahrung Gut.

Der Sorglose

„Es ist doch immer gut gegangen.“

Der Glückspilz

„Das hätte auch richtig schief gehen können.“

Der Ungläubige

„Das hätte ich nie gedacht.“

Wieviel Ausfall können Sie sich leisten?

18 Tage oder 5 Minuten pro Jahr?

Verfügbarkeit

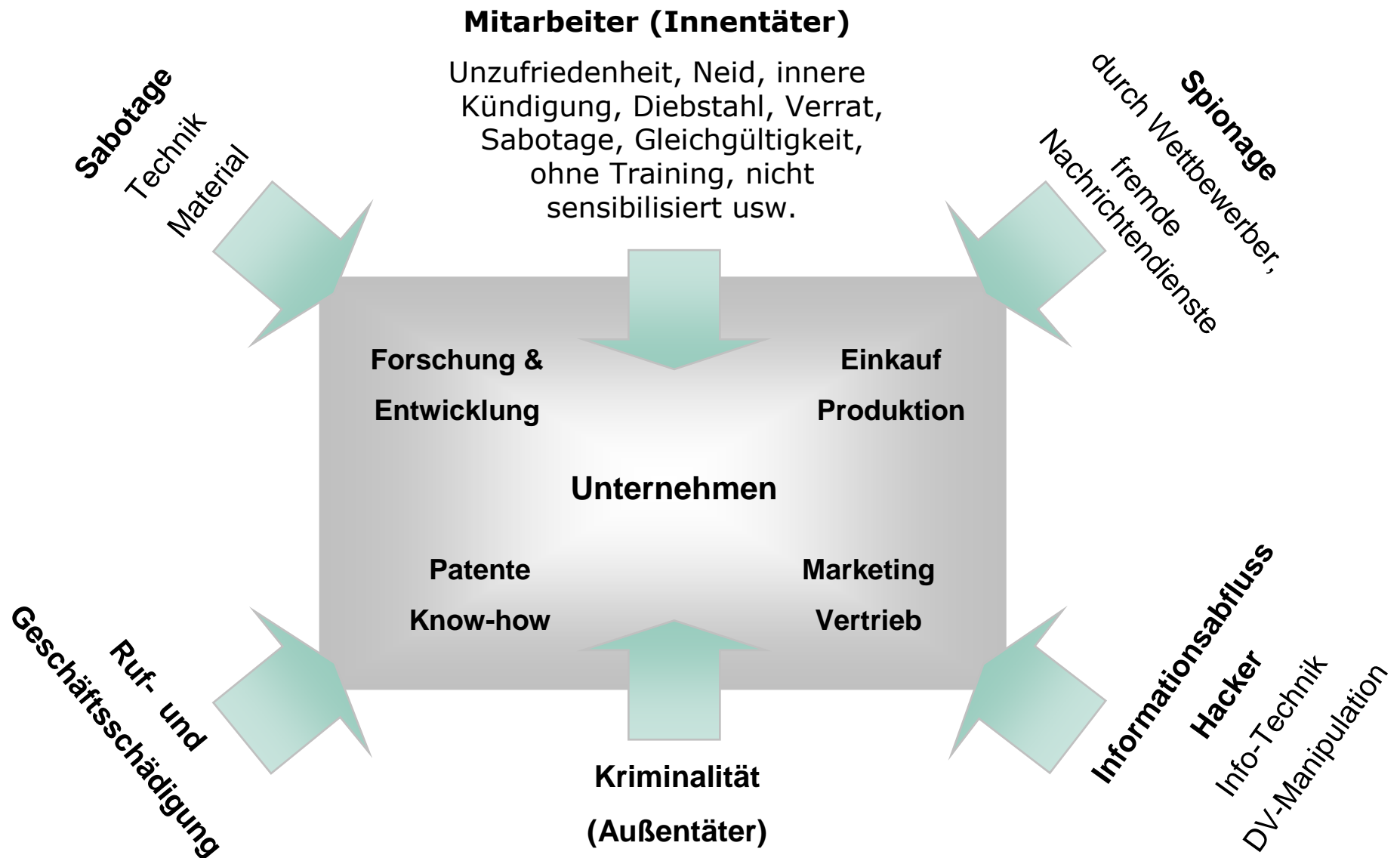
Systemausfall (30Tage)

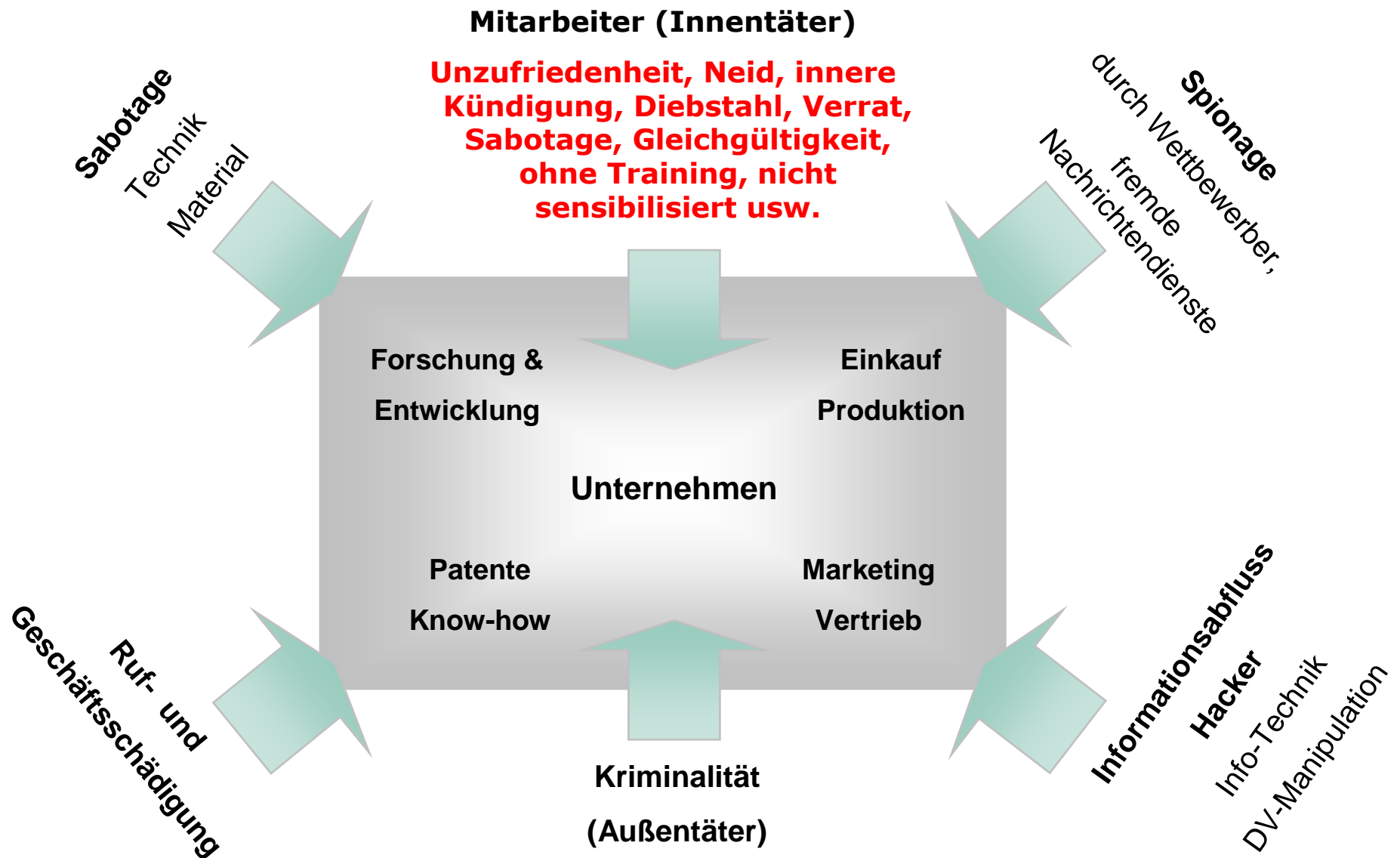
	pro Jahr	pro Monat
95%	18 Tage	1,5 Tage
98%	7 Tage	14 Stunden
99%	3,5 Tage	7 Stunden
99,999%	5 Minuten	25 Sekunden

Was fällt Ihnen zu den Schlagwörtern wie:

- ñ **Ausscheiden eines Mitarbeiters**
- ñ **Brandschutz**
- ñ **Business Continuity**
- ñ **Eskalationsprozesse**
- ñ **Ersatzbetrieb**
- ñ **Notfallplanung**
- ñ **Notfallübungen**
- ñ **Virenbefall**
- ñ **Vorsorgemaßnahmen**
- ñ **Wiederanlaufkonzept**

ein?





Kriterien:

Länge: Anzahl der Zeichen

Kombinationen: Groß- /Kleinschreibung, Zahlen, Sonderzeichen

Wechsel: 1x pro Woche, Monat, Jahr



Rechenbeispiele zur Veranschaulichung

Länge PW	26 klein	52 gr.&kl.	62 gr.&kl.&Ziff.	95 + Sonderz.
5 schuh	39 Sek.	21 Min.	51 Min.	7,2 Std.
6 Hans01	17 Min.	18 Std.	2,2 Tage	28 Tage
7 MkdWnmS	7,4 Std.	39 Tage	135 Tage	7,4 Jahre
8)p9T>°k*	8 Tage	5,6 Jahre	23 Jahre	700 Jahre

Voraussetzung für diese Berechnung:

Der Rechner testet ca. 300.000 Kombinationen pro Sekunde.

Komplexität des Themas Sicherheitstechnik (Bau, Technik, Organisation und Prozesse)

Gesetz- und Vorschriftenschungel

Basel II

KonTraG (Kontrolle u. Transparenz im Unternehmensbereich)

ECB-S (European Certification Board)

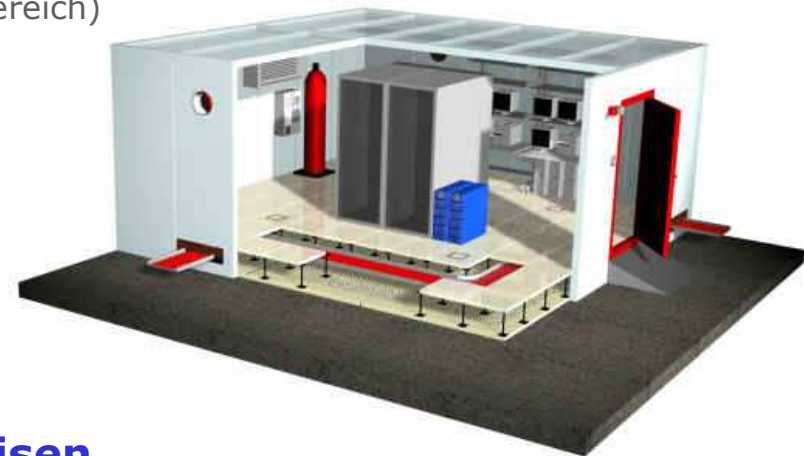
BSI (Bundesamt f. Sicherheit i.d. Informationstechnik)

VdS (Verband der Sachversicherer)

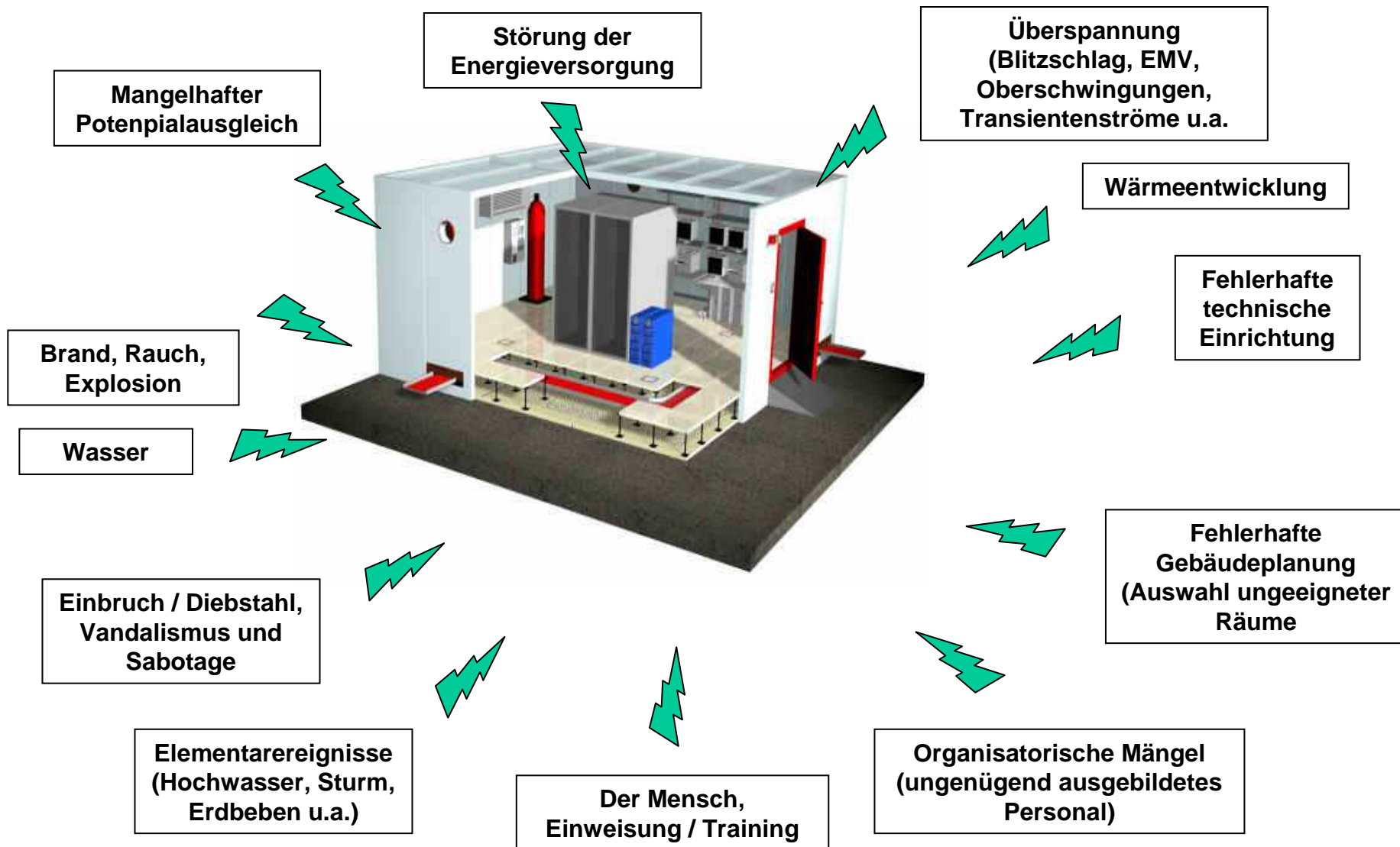
ISO 17799

TÜV IT-Trust Site Infrastructure-Zertifikat

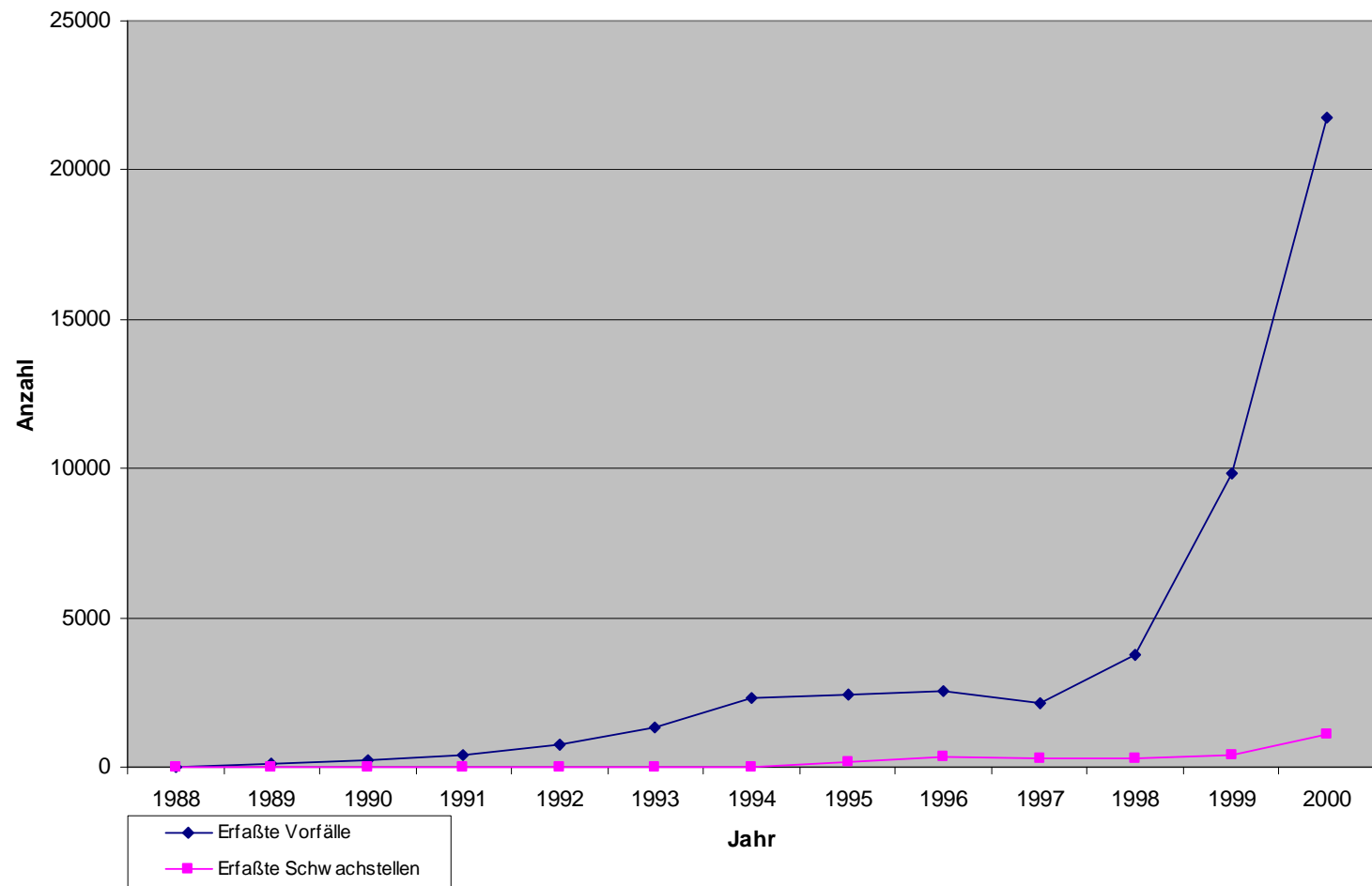
VDE / IEC-Normen



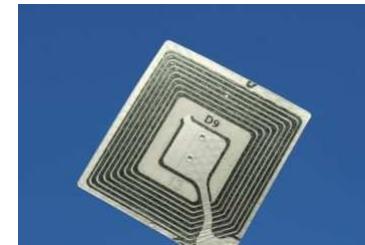
Notwendigkeit von Fach- und Spezialwissen

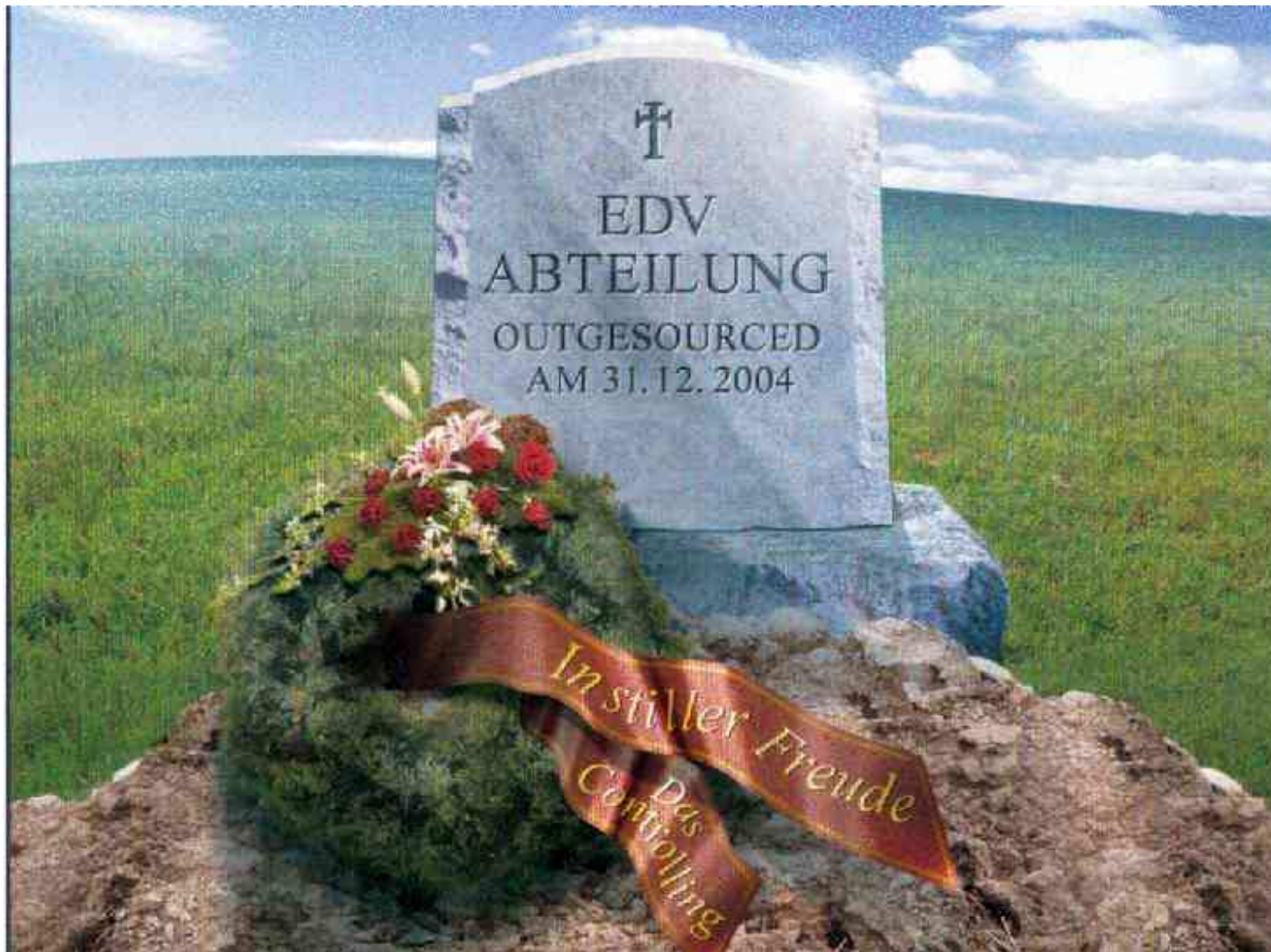


CERT/CC Statistik 1988-2000



Mobile (IT) Geräte





Fahrzeughalter

Werkstatt

<ul style="list-style-type: none">ñ wählt Fahrzeugtyp und -art, wählt Werkstattñ ist verantwortlich für die Einhaltung von gesetzlichen Vorschriften, der Verkehrssicherheit des Fahrzeuges und des ordnungsgemäßen Zustandsñ haftet für evtl. Schäden (hierfür Versicherung)ñ kann u.U. Schadensersatz von Werkstatt fordern	<ul style="list-style-type: none">ñ führt im Auftrage und in Absprache des Kunden Kontrollen und Reparaturen durchñ wählt ihr Arbeitsinstrumentarium (Werkzeuge, Messinstrumente, Maschinen und Geräte)ñ ist für die ordnungsgemäße Durchführung verantwortlich und haftet dafür
<ul style="list-style-type: none">ñ „Herr der Daten“ / Datenverantwortlicherñ verantwortlich für Anwendungssystemeñ erstellt, pflegt Daten und arbeitet mit diesenñ legt fest, was unter Sicherheitsbestimmungen laufen muss (Risikoklassifizierung)ñ ist für die Korrektheit seiner Arbeitsergebnisse verantwortlich und damit auch für die Sicherheitñ haftet gegenüber Dritten (s. BDSG)ñ kann Revisionen bzw. Gutachten über die Prozessabläufe und deren Sicherheit veranlassen	<ul style="list-style-type: none">ñ „Serviceanbieter“ñ wählt Maschinen (Hardware)ñ wählt System- und Systemnahme Softwareñ wählt Tools und Utilities für RZ-Abläufeñ entscheidet über seine interne Organisationsformñ muss die vereinbarten Leistungen (und damit auch die Sicherheitsansprüche) erfüllenñ haftet gegenüber Dritten (siehe u.a. BDSG)

IT-Anwender

IT-Dienstleister

1. Schritt:

Ist – Aufnahme:

**Nur wer seinen
Standort kennt,
kann seinen
Kurs
bestimmen!**



2. Schritt:

Die Umsetzung

Alle machen mit!

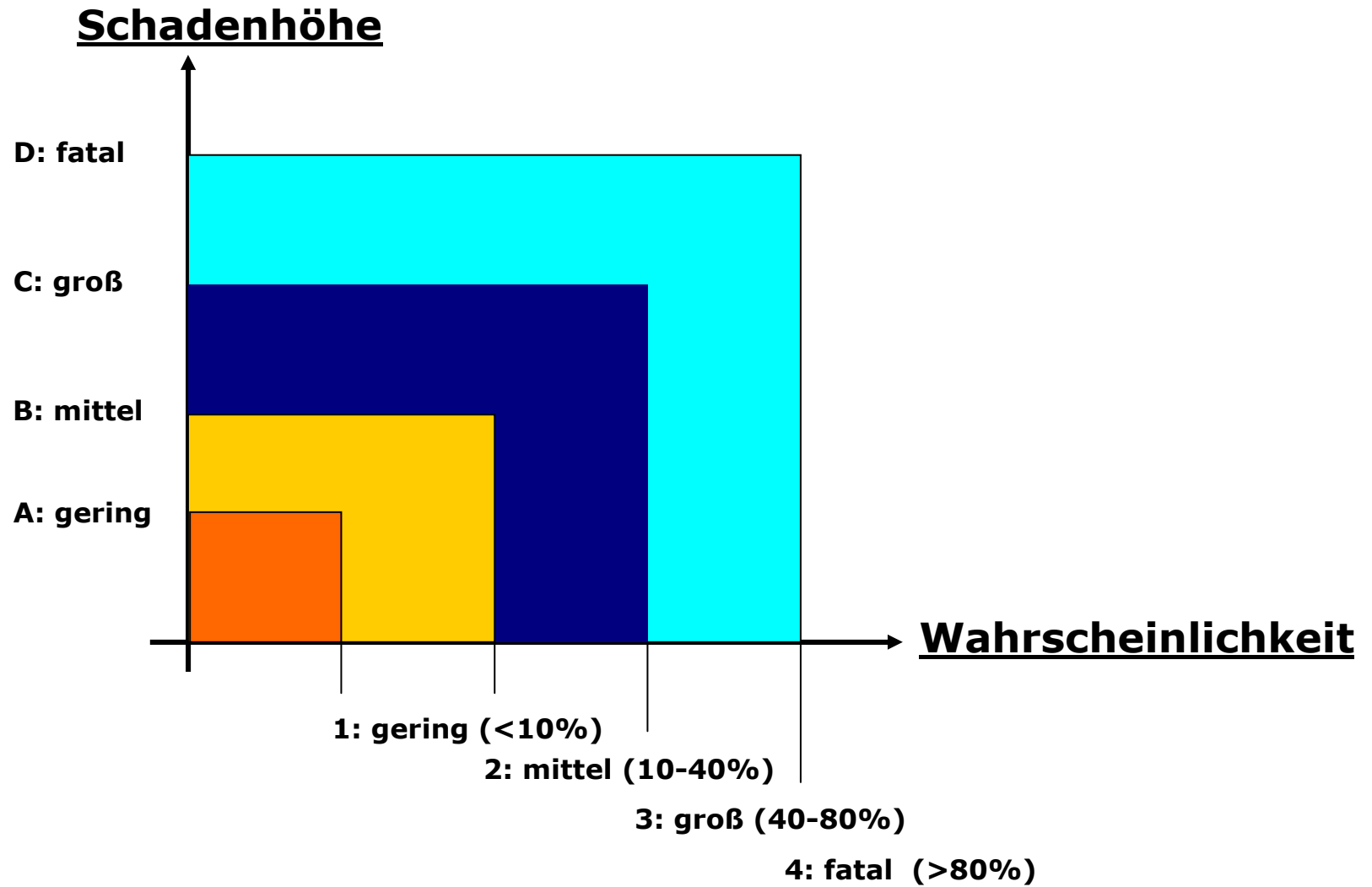
SOCIUS ñ PRIMUS



- Um Ausfälle vorzubeugen
- Zur Absicherung meines Arbeitsplatzes als GF/GL
- Zur Absicherung von MA Arbeitsplätzen
- Zur Fortführung der Geschäftstätigkeit nach K-Fall
- Als Aushängeschild, bin gegen Risiken gewappnet
- Um Gesetze einzuhalten
- Um Vorschriften zu genügen
- ...



Ermitteln Sie mit Hilfe eines erfahrenen Beraters das individuelle Risikopotential Ihres Betriebes!



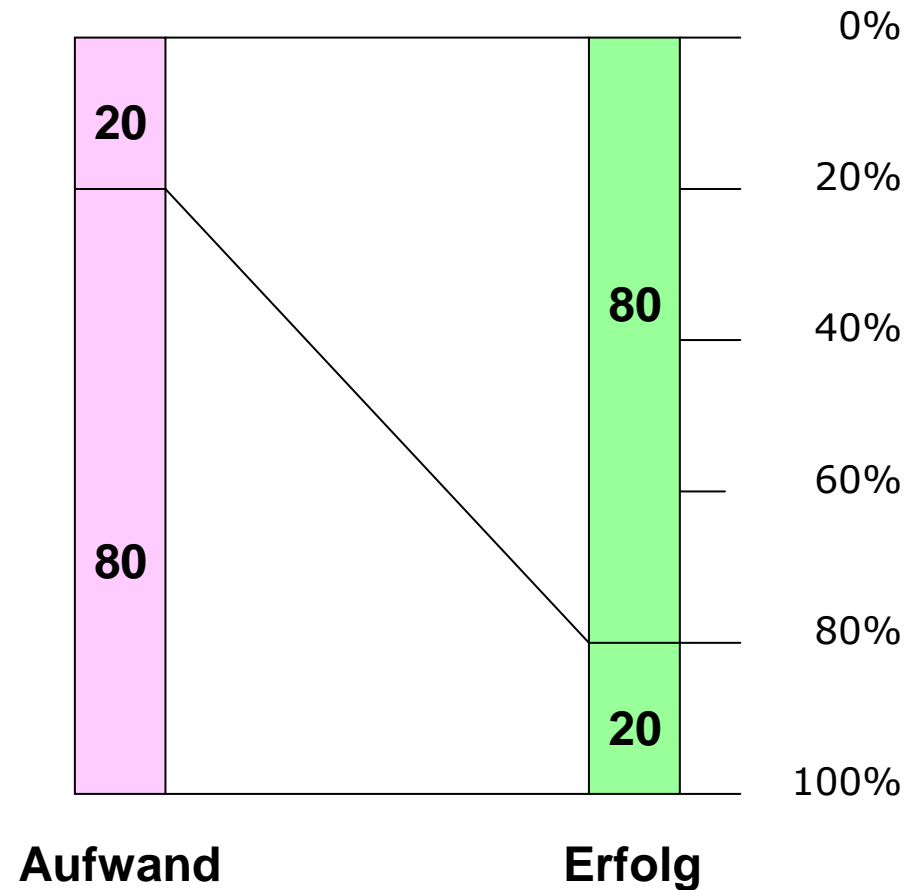
Wieviel kostest es mich, wenn...

- Die Konkurrenz meine Konstruktionspläne hat?
- die Konkurrenz meine besten Mitarbeiter abwirbt?
- die Konkurrenz meine Kalkulation kennt?
- die Konkurrenz meine Kunden kennt?
- die Konkurrenz meine Lieferanten kennt?
- die Konkurrenz meine Schwachstellen weiß?
- die Konkurrenz meine Marketingstrategien kennt?
- etc. etc. etc.

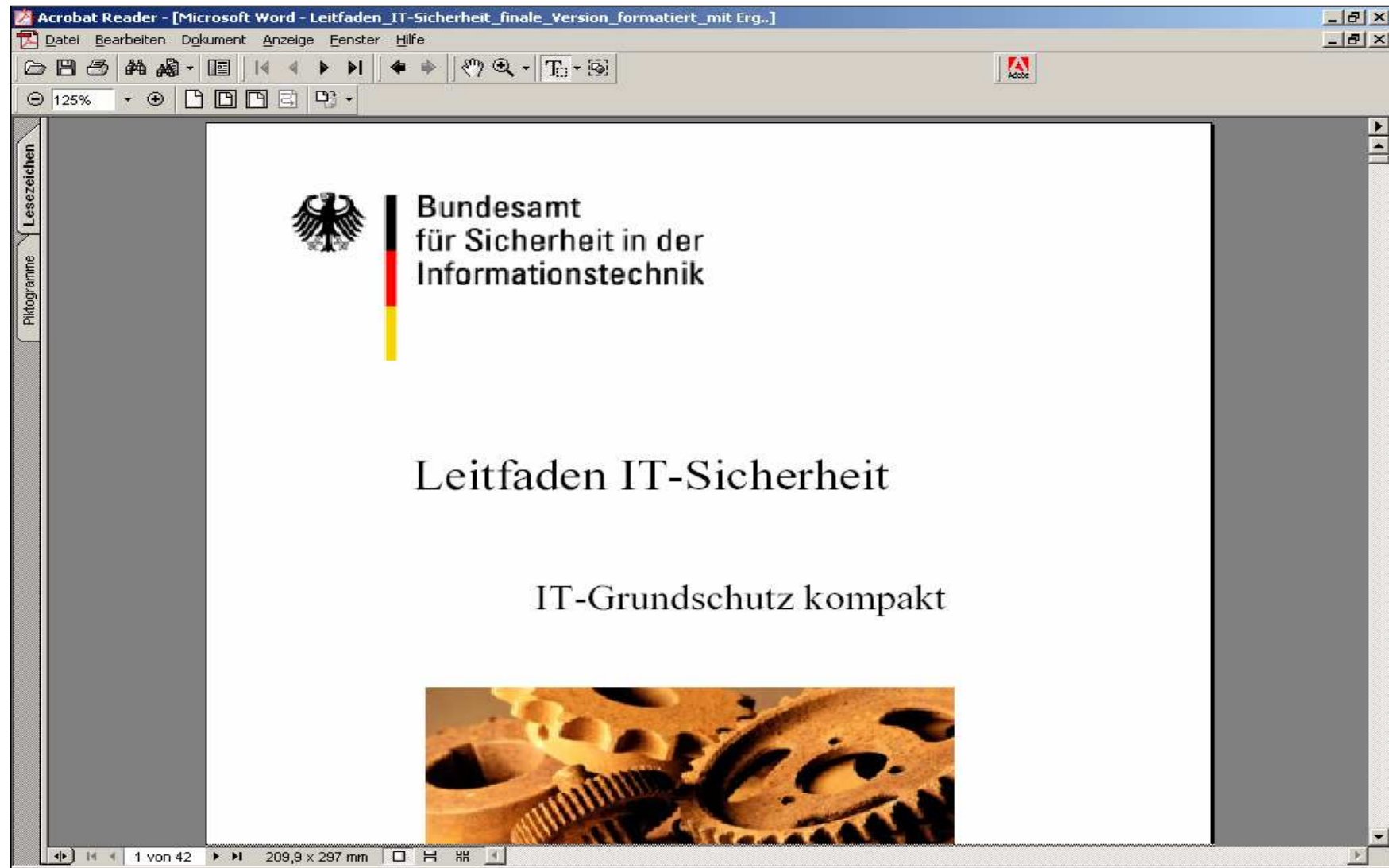
2. Die 20/80 Frage

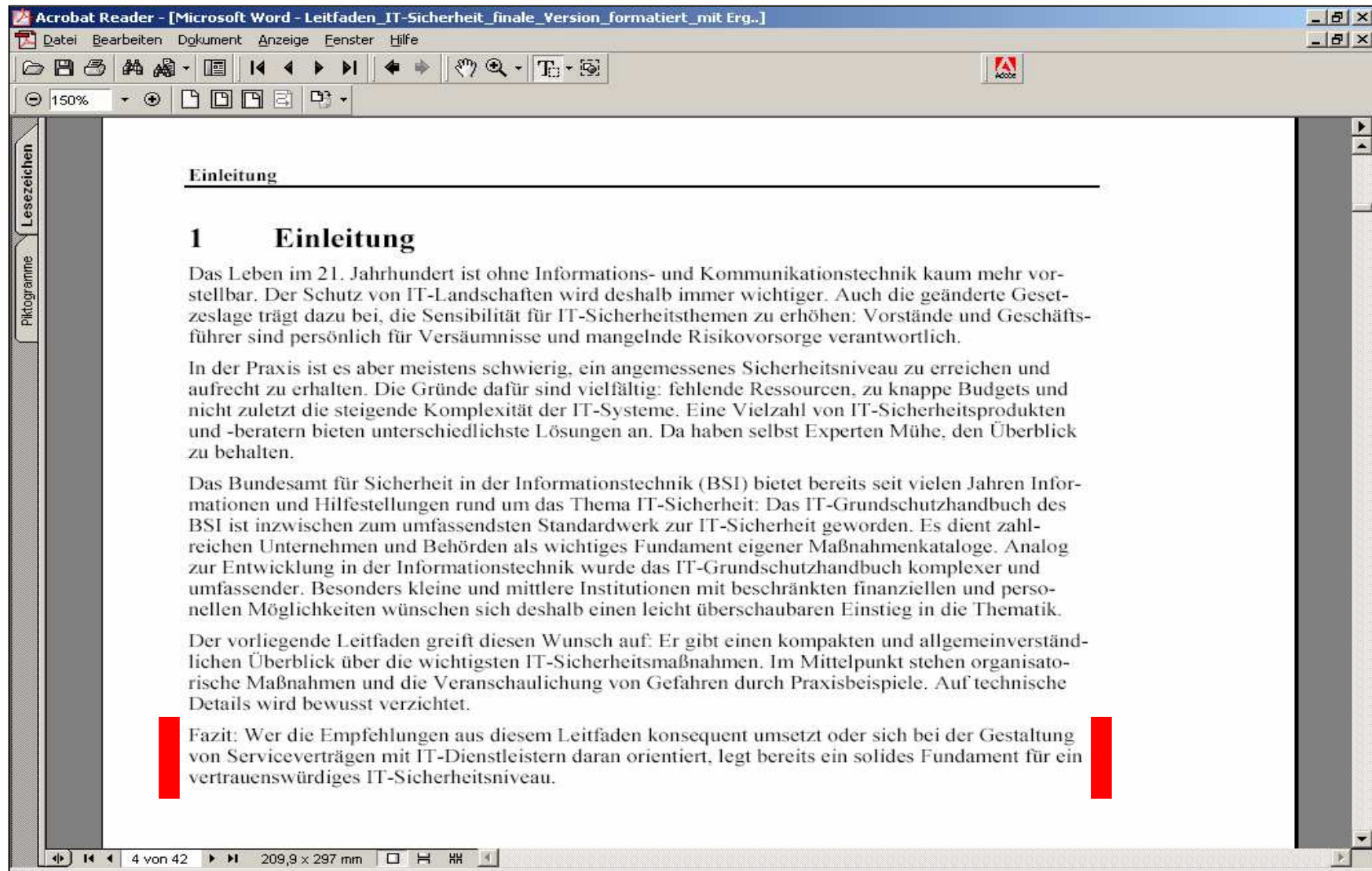
Mit 20% Aufwand lassen
sich 80% Erfolg erreichen!
(Das Pareto-Prinzip)

Reichen Ihnen 80% oder
brauchen Sie 100%?



Wer unterstützt mich?





- **Datenintegrität:**
Unversehrtheit, keine Manipulation
- **Datenvertraulichkeit:**
Mitlesen der Kommunikation
- **Datensicherheit:**
Informationsdiebstahl
- **Datenverfügbarkeit:**
Ausfall der Systeme

gewährleisten Datenintegrität, -vertraulichkeit & -verfügbarkeit

Berührte Gesetze:

➤ **KonTraG**

Gesetz zur Kontrolle u. Transparenz im Unternehmensbereich

➤ **KWG**

Kreditwesengesetz

➤ **GoB / GoDV**

Grundsätze ordentlicher Buchhaltung/ Datenverarbeitung

➤ **ProdHaftG**

Gesetz über die Haftung für fehlerhafte Produkte

➤ **BDSG**

Bundesdatenschutzgesetz

➤ **STGB**

Strafgesetzbuch (§202a Ausspähen von Daten, §263a Computerbetrug, §269 Fälschung beweiserheblicher Daten, § 303a Datenveränderung, § 303b Computersabotage)

➤ **SOX** (Sarbanes-Oxley-Act.)

➤ **Signaturgesetz**

Normen u. ä.:

➤ **Qualitäts-Management** **ISO 9000:2000**

➤ **Security-Management**

- ISO / IEC 17799
- ISO 27001
- BS 7799
- IT-GSHB (BSI)

➤ **Modell (Prozesse)**

- ITIL
- Cobit

➤ **GDPdU**

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen mit § 146 u. § 147 Abgabenordnung (Archivierung).

Übergreifende Vorschriften:

➤ **BaFin**

➤ **MaRisk** (alt = MaH, MaK)

➤ **IDW**

Institut der Wirtschaftsprüfer

➤ **Basel II**

Haftungsrisiko der GL:

➤ **Kontrollverschulden**

Wenn keine Kontrollmechanismen (Revision, Controlling, IT-Governance etc.) im Unternehmen installiert wurden.

➤ **Auswahlverschulden**

Wenn sich der falsche Mitarbeiter an einem falschen Ort befindet.

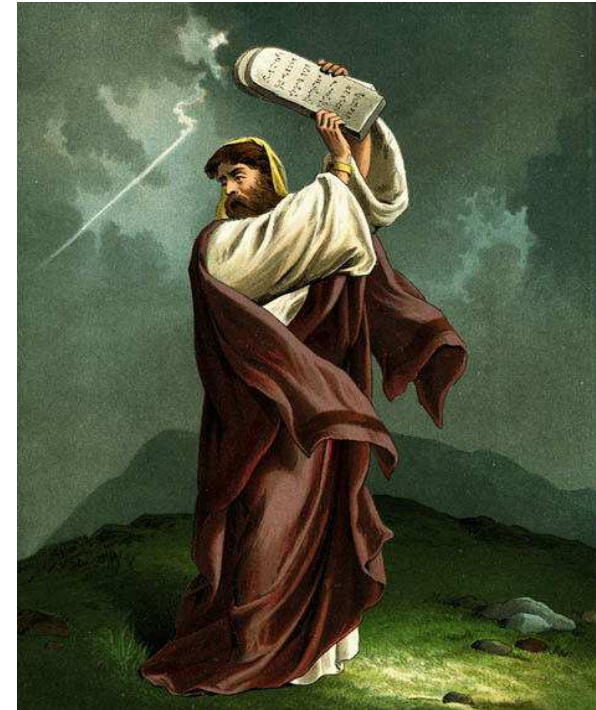
➤ **Einweisungsverschulden**

Wenn Mitarbeiter nicht ordnungsgemäß in Aufgaben eingewiesen wurden.

➤ **Organisationsverschulden**

Wenn keine angemessene Organisation erarbeitet und installiert wurde (insbesondere auch Sicherheitsmanagement).

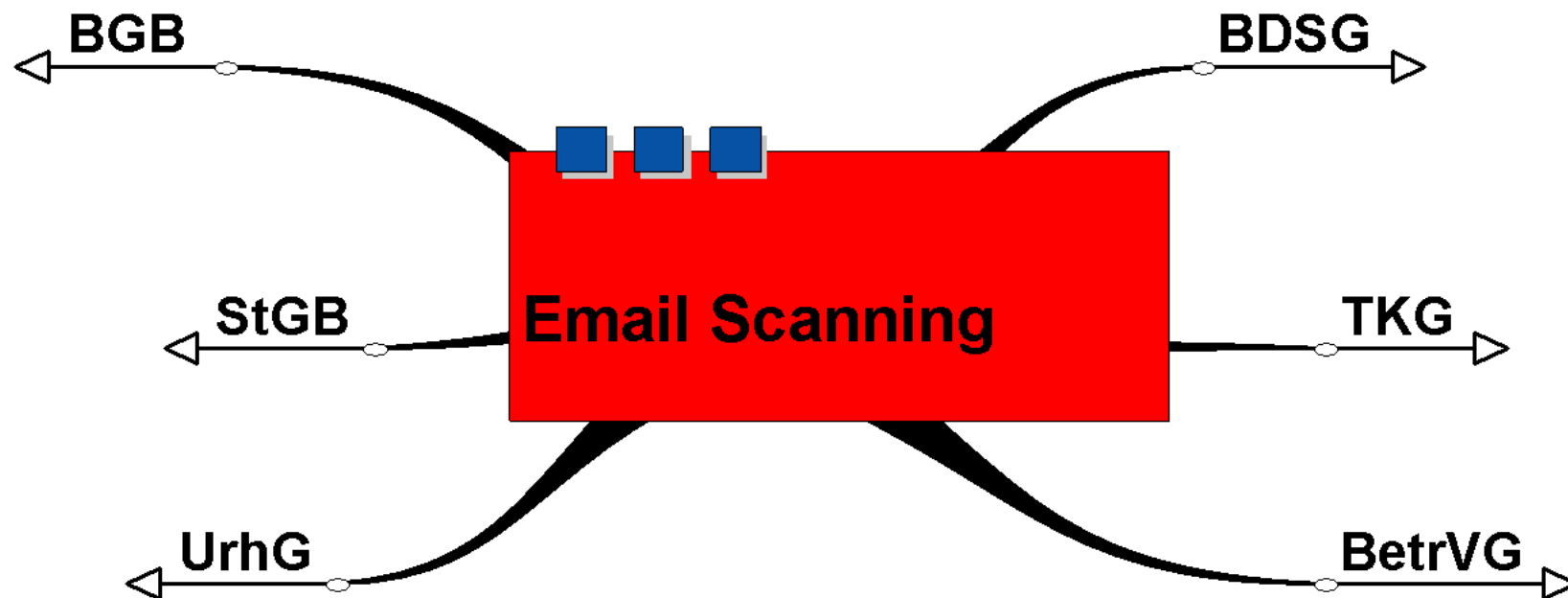
- **Strafrecht**
- **Datenschutzrecht**
- **Telekommunikationsrecht**
- **Zivilrecht und Wettbewerbsrecht
(Tun, Unterlassen, Schadenersatz)**
- **Handelsrecht (Bilanzierung, Lagebericht)**
- **Arbeitsrecht
(Individualrecht & Kollektives Recht)**



Problem	Haftungsrisiko	Strafraumen bis
Mitarbeiter nutzt kostenpflichtige Seiten kostenlos mit geknackten Passworten.	§ 263a StGB Computerbetrug	5 Jahre
Mitarbeiter dürfen ohne Richtlinien eigene Software installieren, schleppen Viren oder trojanische Pferde ein.	§ 43 BDSG	1 Jahr
Mitarbeiter sendet strafbare Inhalte:	<p>§ 184 Abs. 1 StGB Verbreitung pornographischer Schriften an Minderjährige.</p> <p>§ 184 Abs. 3 StGB Verbreitung harter Pornographie.</p> <p>§ 184 Abs. 3 StGB Verbreitung von Kinderpornographie</p> <p>§ 86 StGB Verbreiten von Propagandamitteln verfassungswidriger Organisationen</p>	<p>1 Jahr</p> <p>3 Jahre</p> <p>3 Monate bis 5 Jahre</p> <p>3 Jahre</p>

Problem	Haftungsrisiko	Strafraahmen bis
Mitarbeiter bricht in fremde Unternehmensnetze ein, installiert trojanische Pferde, schießt fremde Rechner ab.	§ 202a StGB Ausspähen von Daten	3 Jahre
	§ 303a StGB Datenveränderung	2 Jahre
	§ 303b Datensabotage	5 Jahre
private Telefongespräche werden kontrolliert ohne besondere Vereinbarung.	§ 43 BDSG	1 Jahr
	§ 206 StGB	5 Jahre
private Mails von Mitarbeitern werden gelesen	§ 206 StGB	5 Jahre
	§ 202a StGB	3 Jahre

„intern“ zum Mitarbeiter



... auf der Suche nach Viren

§ 201 StGB Verletzung der Vertraulichkeit des Wortes

§ 202 a StGB Ausspähen von Daten

§ 203 StGB Geheimnispflicht besonderer Berufsgruppen

§ 206 StGB Post- und Fernmeldegeheimnis

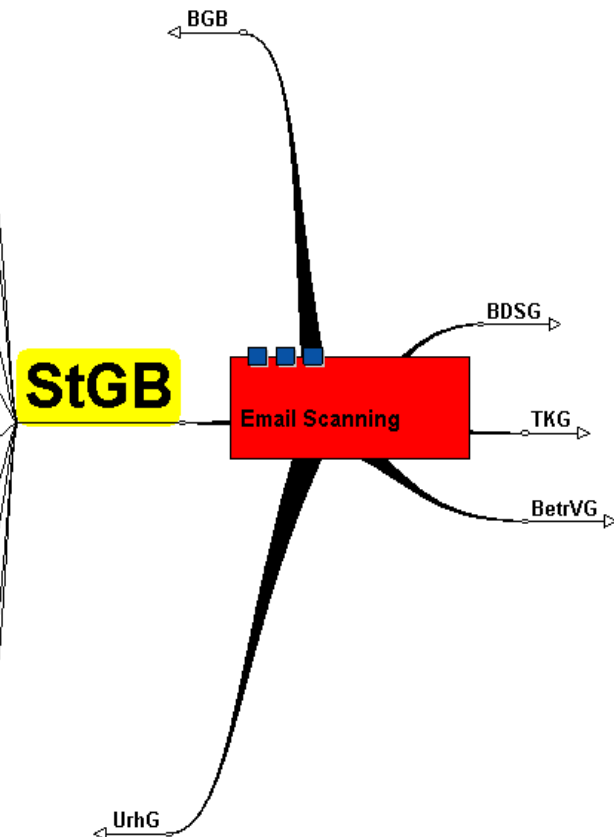
§ 263 a StGB Computerbetrug

§ 268 StGB Fälschung technischer Aufzeichnungen

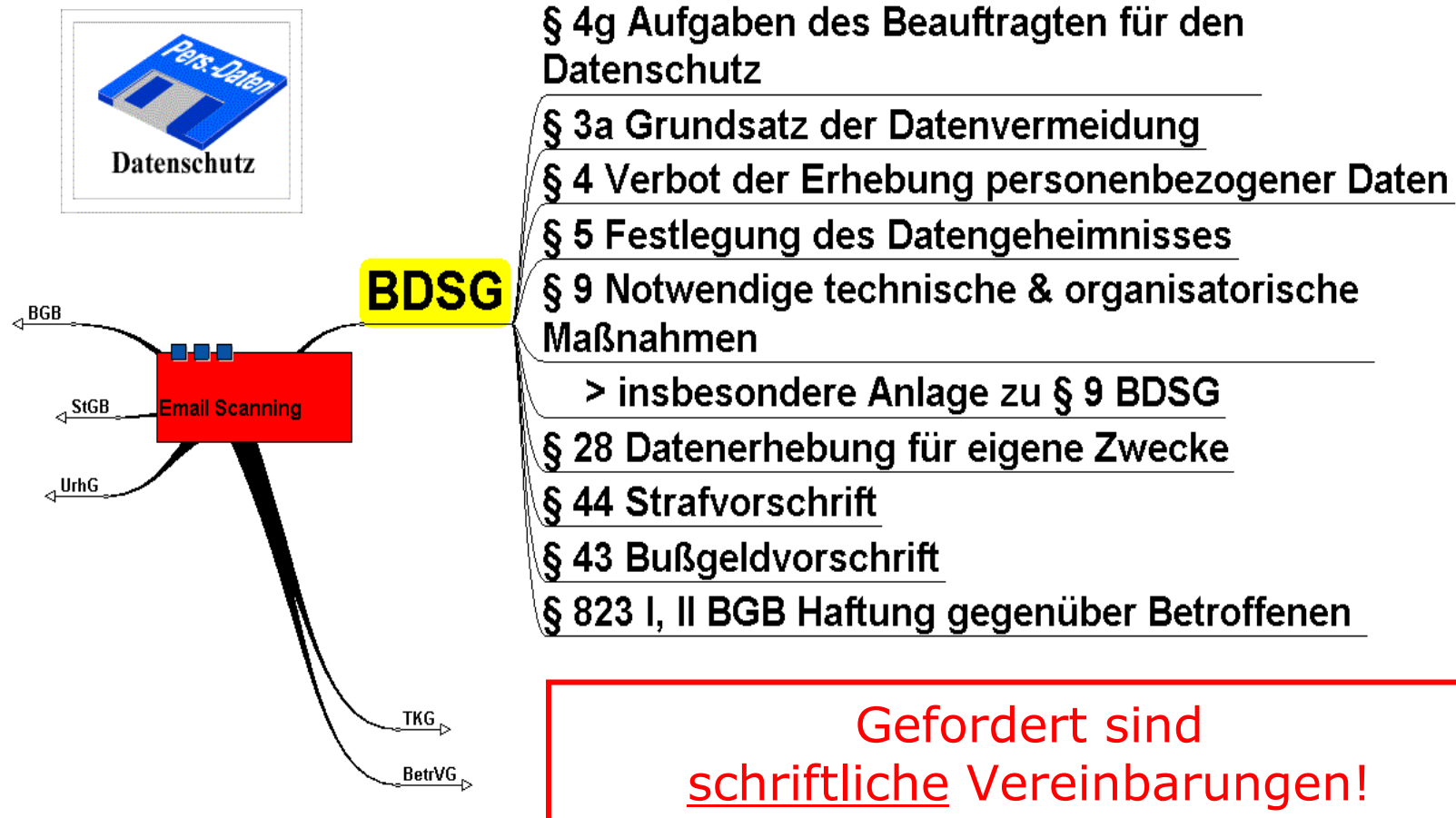
§ 269 StGB Fälschung beweiserheblicher Tatsachen

§ 303a, b StGB Datenveränderung, Computersabotage

§ 270 StGB Täuschung bei Datenverarbeitung



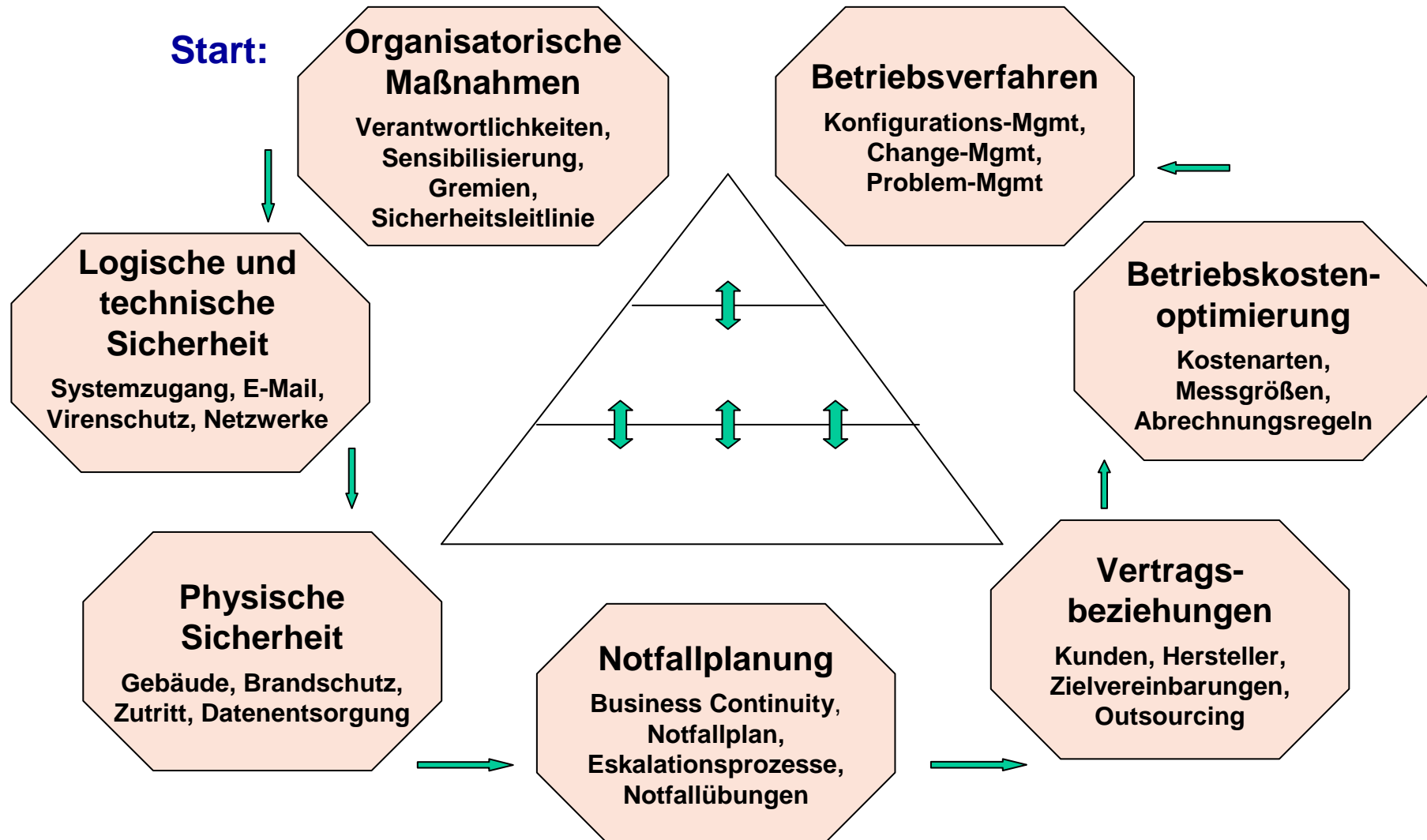
... auf der Suche nach Viren



Welcher Aufwand ist nötig?



- ñ Feststellung Ihres IT – Sicherheitsniveaus
- ñ Feststellung der Schutzbedürftigkeit
- ñ Ganzheitliche Betrachtung der IT-Sicherheit
- ñ Bearbeitung der Einzelthemen auf hoher Ebene
- ñ Bewertung des Erfüllungsgrades aller Kriterien
- ñ Durchführung von vertiefenden Audits möglich
(z.B. System-Audit, TK-Anlagen-Audit u.a.)
- ñ Erstellung eines priorisierten Maßnahmenplans

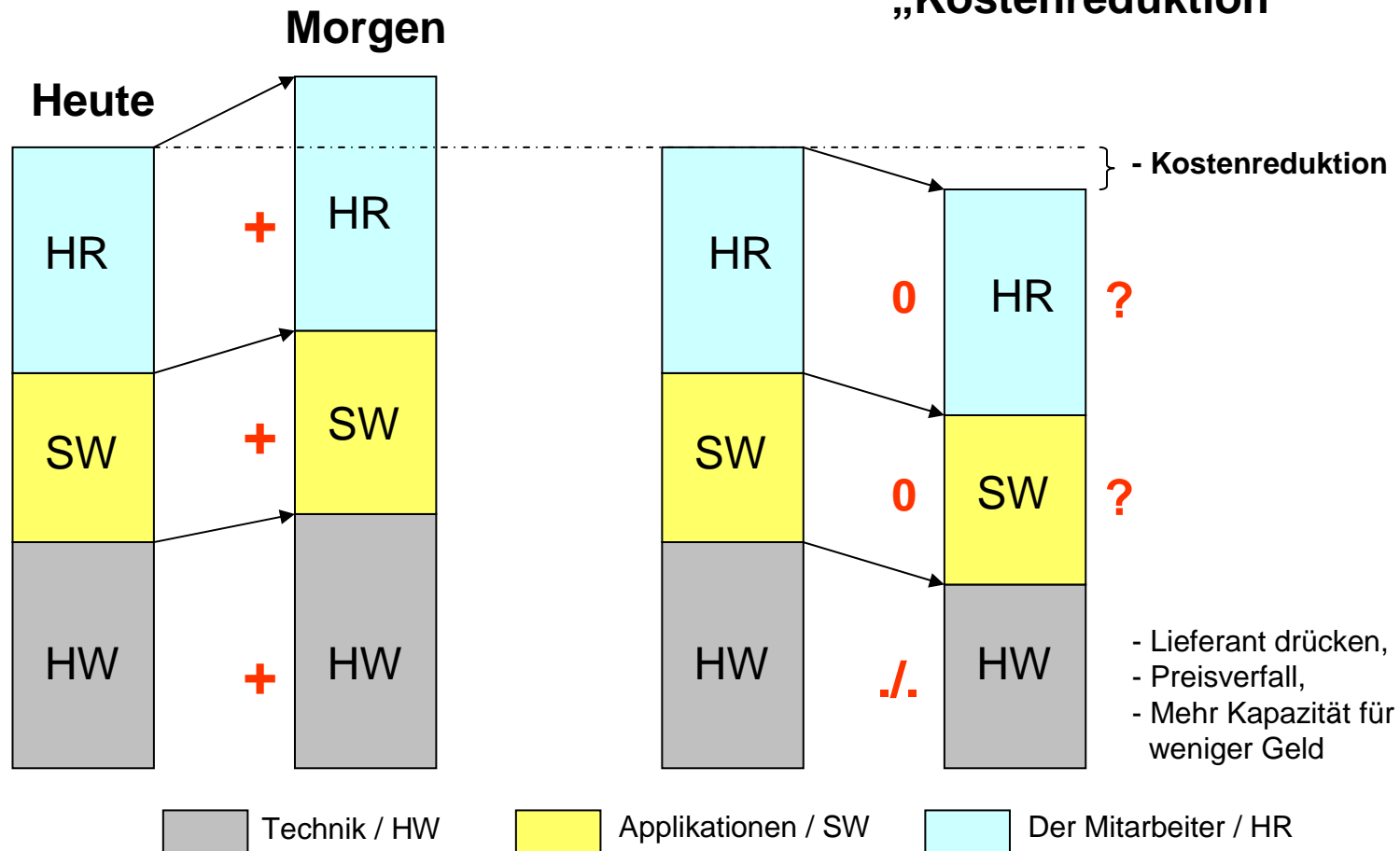


- 👤 **Standortbestimmung, wo befinde ich mich heute**
- 👤 **Erste Aussage über meine Schutzbedürftigkeiten**
- 👤 **Bestandsaufnahme für die Versicherung (Betriebshaftpflicht, u.a.)**
- 👤 **Bestandsaufnahme für Trainingsmaßnahmen**
- 👤 **Ausgangspapier (Start) für mein IT Sicherheitsmanagement**
- 👤 **Bestandsaufnahme zum Ratinggespräch nach Basel II**
- 👤 **Bestandsaufnahme für den WP zur Jahresabschlussprüfung**
- 👤 **Qualitätsaussage (B2B und B2C):**
 - „Ich bin ein verlässlicher Partner für eine langfristige Zusammenarbeit“.
 - „Ich arbeite aktiv an der Sicherheit meines Unternehmens“.
 - „Die Sicherheit meines Unternehmens und die störungsfreie Zusammenarbeit mit meinen Partnern stehen für mich als Unternehmer im Vordergrund.“

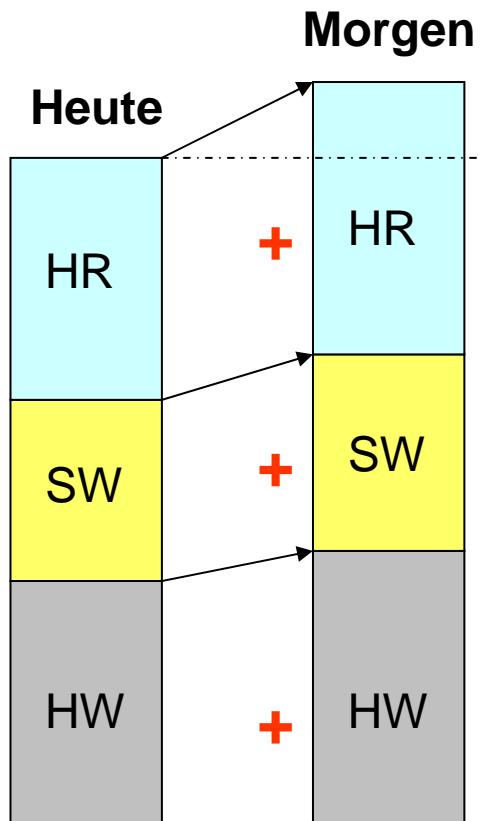
Traditioneller Blick

Wunsch der Geschäftsleitung

„Kostenreduktion“

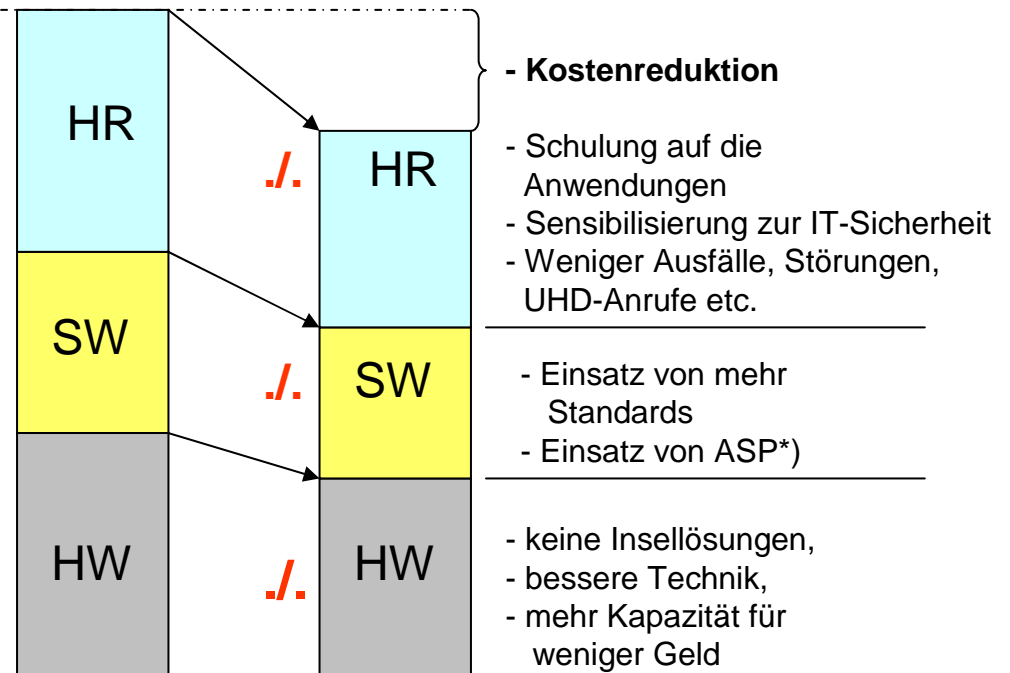


Traditioneller Blick




Ausblick

„Kostenreduktion und Erhöhung der Qualität“!!!



 Technik / HW

 Applikationen / SW

 Der Mitarbeiter / HR

ASP*) = Applikation Service Provider



Es kann sein, dass sich mit einer Wünschelrute alle möglichen Dinge aufspüren lassen.

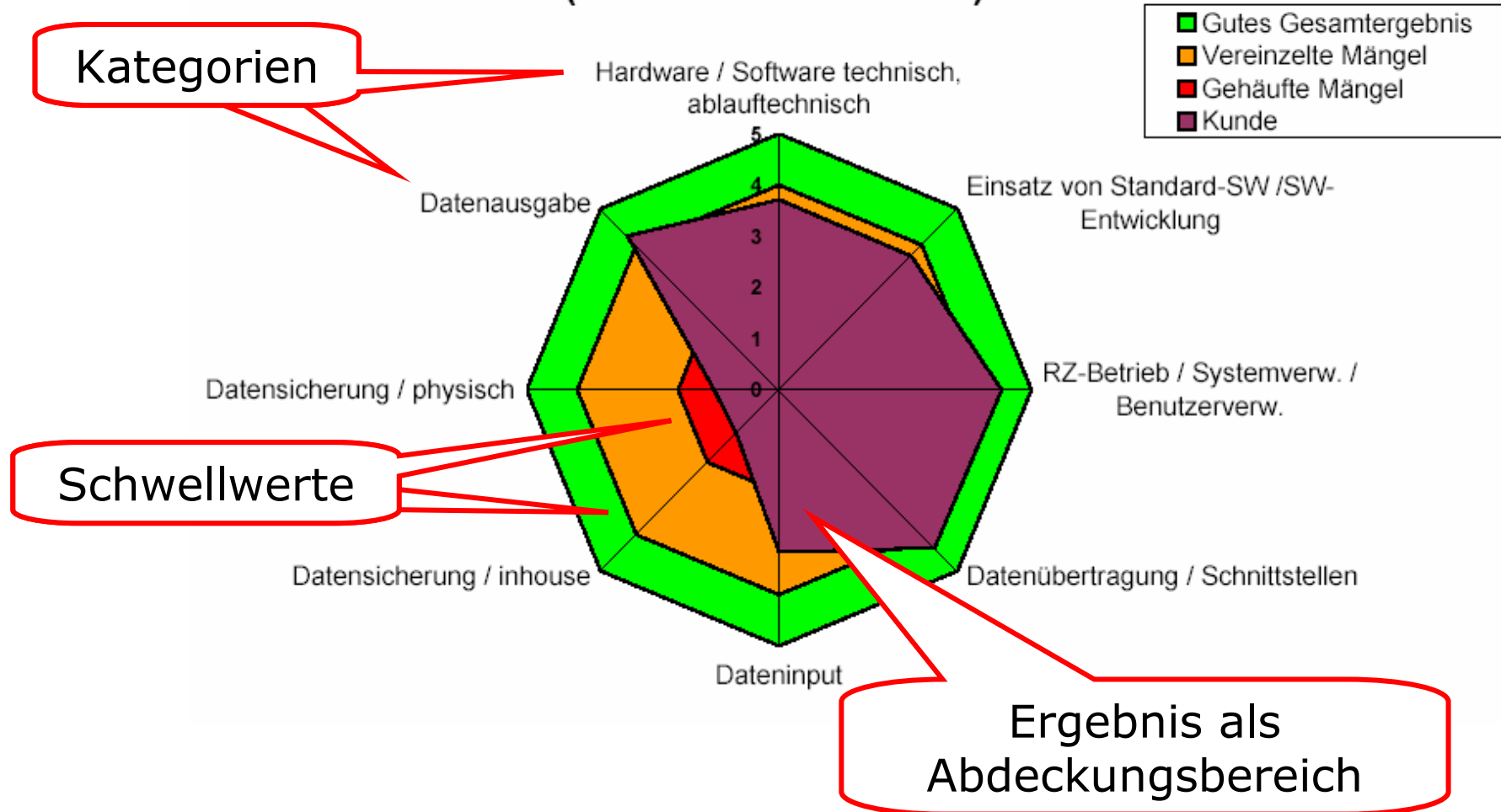
Für Ihre Schutzbedürftigkeit gehen Sie bitte mit methodisch abgesicherten Verfahren vor!

- **Audit in Form von Präsentinterviews**
- **Direkte Erfassung der Antworten und Abstimmung mit den fachspezifischen Interviewpartnern**
- **Sicherstellung der Qualität durch methodische Vorgehensweise**
- **Rücksprache in Zweifelsfällen**
- **Auswertung / Bewertung**
 - **durch das Audit-Team allein oder**
 - **mit dem IT-Sicherheitsbeauftragten**
 - **mit dem Betriebsrat**

1	Hardware / Software technisch, ablauftechnisch	Gewicht Vorgabe	Gewicht Kunde	Erfüllungsgrad aus Kundensicht	Zuständiger Interview- Partner (Kunde)	Erhebungs- datum	Kommentar
1.001	Liegt eine aktuelle Dokumentation im Sinne eines umfassenden Katasters vor?	5,0	4,0	10			
1.002	Ist dokumentiert: auf welchen Rechnern laufen welche DV-Verfahren?	5,0	4,0	10			
1.003	Ist dokumentiert: in welcher Betriebsart diese Rechner betrieben werden?	5,0	4,0	10			
1.004	Sind die Rechnertypen erfasst?	5,0	4,0	10			
1.005	Sind Zuständigkeiten für die Technik / Instandsetzung / Wartung geregelt?	5,0	4,0	10			
1.006	Ist die Aufrechterhaltung des technischen Betriebes gewährleistet?	5,0	4,0	10			
1.007	Existiert eine Netzwerkübersicht in graphischer/verbaler Form?	5,0	4,0	10			
1.008	Ist die Netzwerkübersicht mit einer Konfigurationsübersicht gekoppelt?	5,0	4,0	10			
1.009	Liegt die Bestimmung kritischer Mengengerüste/Ressourcenbedarf vor?	5,0	4,0	10			
1.010	Ist dokumentiert, unter welchen Plattformen welche DV-Verfahren ablaufen?	5,0	4,0	10			

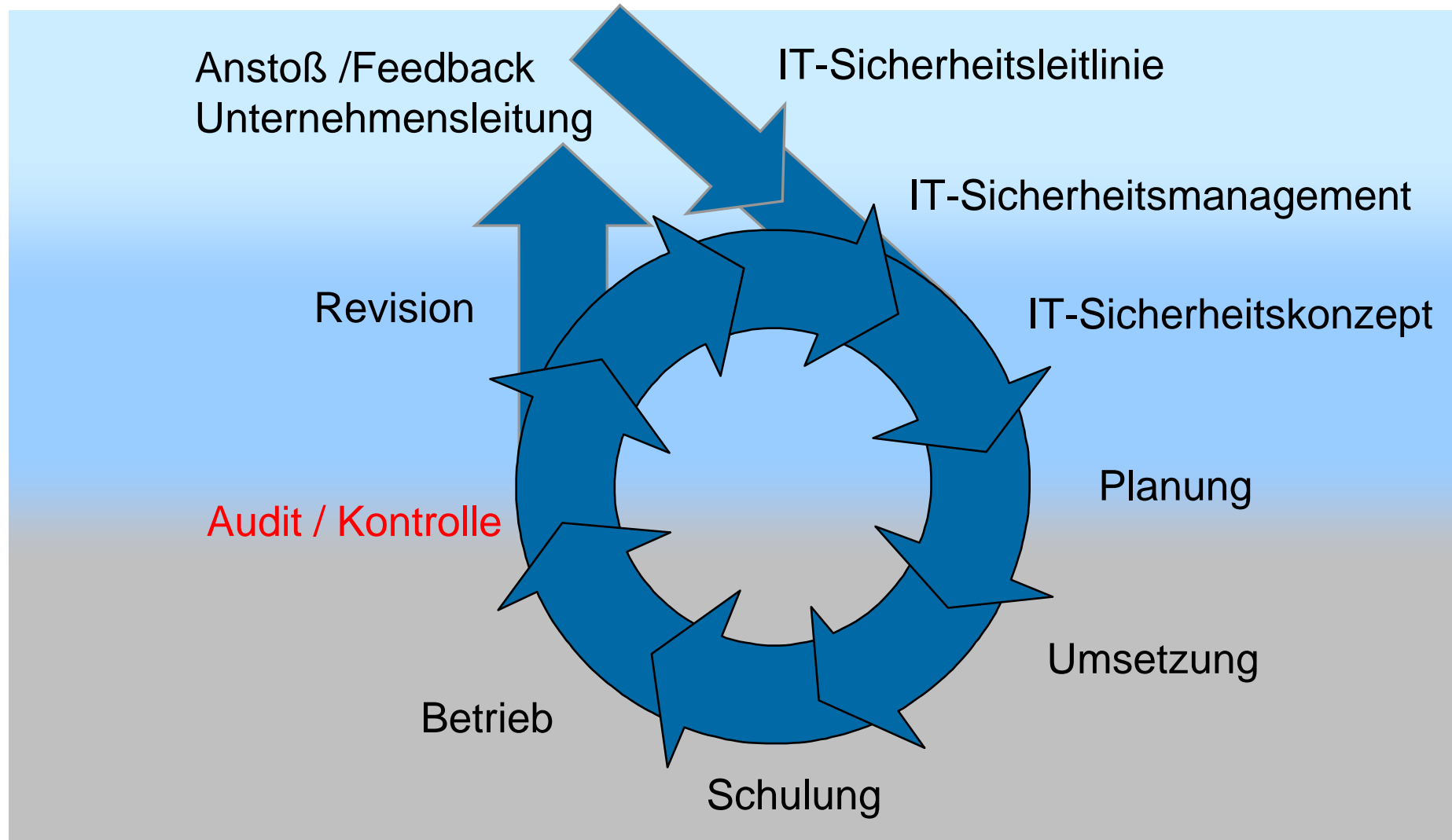
Insgesamt = 24 Kategorien mit über 350 Fragen

Ergebnisse der Checklisten IT-Sicherheit (Teil 1 - Kundensicht)



- **Kundenbesuch zur Sensibilisierung des Themas „Der sichere IT-Betrieb“ (alle Mitarbeiter)**
- **Terminabsprachen für die Vorbereitung zum Audit**
- **Ist-Aufnahme / der Audit vor Ort**
- **Ergebnisbericht für Sie**
- **Empfehlenswert & separat:
Erstellung eines Maßnahmenkataloges zur Beseitigung der Schwachstellen
(mit einem Dienstleister Ihres Vertrauens)**

- **Basis sind die in den Checklisten festgehaltene**
- **Schwachstellen und festgestellten Risiken**
- **Ableitung & Dokumentation konkreter Maßnahmen**
- **Priorisierung der Maßnahmen nach abgeschätztem Nutzen für Ihre Sicherheit (hoch, mittel, niedrig)**
- **Definition des Aufwands (hoch, mittel, niedrig)**
- **Der Ausführende (eigenes Personal oder Dienstleister) und der Status werden festgelegt.**



- **Machen Sie IT-Sicherheit zur Chefsache**
- **Holen Sie professionelle Beratung**
- **Bestellen Sie Verantwortliche für die IT-Sicherheit**
- **Erstellen Sie betriebsinterne Richtlinien für Ihre IT-Sicherheit (ISP = IT-Security Policy)**
- **Schulen / sensibilisieren Sie Ihre Mitarbeiter**
- **Erstellen Sie Notfallpläne für den K-Fall**

Dringend !!!

SOCIUS ñ PRIMUS



**Wer das Thema nicht bewusst als
Führungsaufgabe wahrnimmt,
hat keine Chance zur
Gegenwehr!**

Welche Fragen sind offen geblieben?



Hans - J. Grusewski

Beim Strohhouse 31
20097 Hamburg

Phone: +49 (0) 700 4455-1111

Fax: +49 (0) 700 4455-8888

Mobile: +49 (0) 172 6446 155

Mailto: Hans.Grusewski@Socius-Primus.de

<http://www.socius-primus.de>