Willkommen zur Präsentation

IT-Protection Service AG 3. März 2006

IT-Protection Service AG

„Datenschutz und Datensicherheit für KMU“

Wolfgang Sidler

CEO Swiss IT-Markt AG „Der Onlineshop für Unternehmen“

- Mitautor «Sicherheitshandbuch für die Praxis» www.sidler.ws
- Wirtschaftsinformatiker, Nachdiplom FH Informatiksicherheit
- Microsoft Certified Systems Engineer (MCSE), ITIL Certificate

Ausgangslage

IT-Protection Service AG 3. März 2006

- ca. 93% aller Unternehmen in der Schweiz sind KMUs
- Informationen werden nicht genügend gut geschützt
- Abhängigkeit der Geschäftsprozesse in Bezug auf die IT steigt und das Bewusstsein für diese Abhängigkeit fehlt häufig
- Verantwortlichkeiten sind nicht klar
- Fahrlässigkeit und Ignoranz bezüglich der IT-Risiken
- Die Häufigkeit und die Art der Bedrohungen nehmen stetig zu
- Missverständnisse zwischen dem Management und der IT erzeugen Unsicherheit und falsches Verhalten
- Der Druck seitens Gesetzgebung und Best Practice steigt
- Angst vor hohen Kosten, fehlenden Ressourcen und Fachwissen
- Komplexität und Funktionalität werden immer grösser
- Fehlende Unterstützung des Managements
- Das Datenschutzgesetz (DSG) wird unwissentlich verletzt

Ausgangslage I

IT-Protection Service AG 3. März 2006

IT-Sicherheit ist Chefsache – und so sieht‘s der Chef!

IT-Sicherheit verursacht hohe Kosten und wenig Nutzen

Die administrativen Auflagen für KMU sind doch ohnehin schon zu gross

100% Sicherheit gibt es sowieso nicht

Wir haben doch jetzt eine Firewall, einen Virenschutz und machen jeden Tag Backup. Reicht das denn noch nicht?

Es ist ja noch nie etwas passiert

Bedrohungen

IT-Protection Service AG 3. März 2006

- **Höhere Gewalt**
  - Feuer, Blitz, Sturm, Überschwemmung, Stromausfall, Krankheit, …
- **Menschliches Versagen**
  - Bedienungsfehler, Unwissen, falsches Verhalten, …
- **Gesetzliche Mängel**
  - Nicht Einhalten der Gesetze, Reglemente etc. (Compliance)
- **Technisches Versagen**
  - Netzwerkausfall, Software-Fehler, Viren, Disk-Ausfall, …
- **Organisatorische Mängel**
  - Fehlende oder nicht angewendete Weisungen, unzureichende Zutrittskontrollen, falsche Zugriffsrechte, Abgang von Schlüsselpersonen (Know-how-Verlust), Versagen der Prozesse, …
- **Vorsätzliche Handlungen**
  - Manipulation, Diebstahl, Missbrauch, Spionage, Hacking, Erpressung, Viren, organisierte Kriminalität, ...

Beobachtungen aus der Praxis

IT-Protection Service AG 3. März 2006

- Unklare,verteilte und unkontrollierte Kompetenzen
- Mangelhafte Aktualisierung der Zutritts-, Zugriffskontrollen
- Nicht Einhaltung vorhandener Prozesse
- Verletzung des Datenschutzgesetzes
- Fehlende Umsetzung festgelegter Schutzmassnahmen
- Sorglosigkeit und fehlendes Sicherheitsbewusstsein
- Defekte Festplatten, andere Datenträger und Dokumente werden nicht fachgerecht entsorgt
- etc.

Was ist ein Risiko?

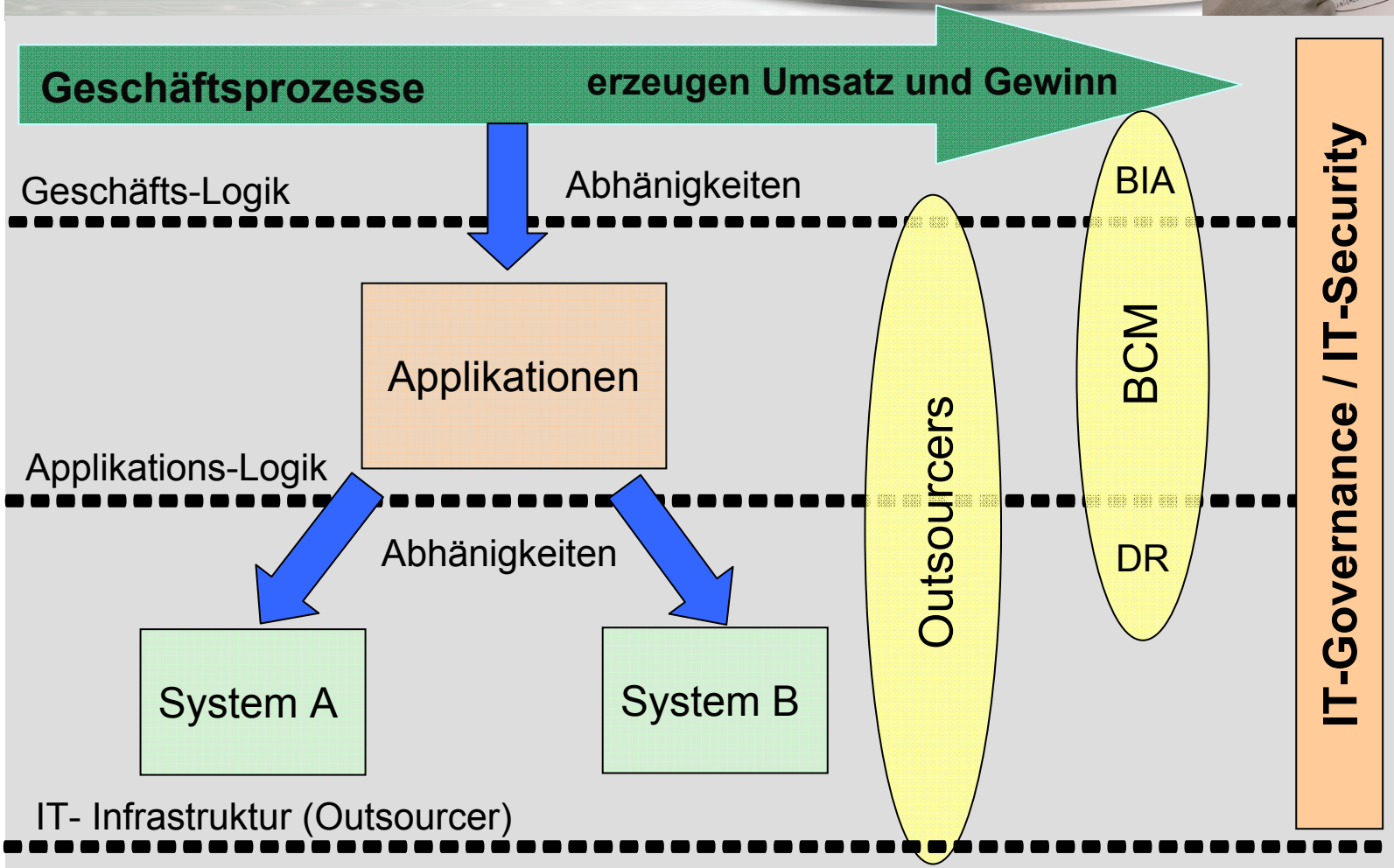
Die wissentliche oder unwissentliche Inkaufnahme eines Verlusts in bestimmter Höhe im Verhältnis zur Eintretenswahrscheinlichkeit

Abstrakte versus konkrete Risiken

Umgang mit Risiken

Geschäfts-Prozesse

IT-Protection Service AG 3. März 2006



Vom OLD Business zum NEW Business Modell

Old Business Modell

- IT und Geschäft getrennt
- Traditionelle Geschäftsmodelle
- Kundenschnittstelle ist Mensch

Geschäftsprozesse

IT

Mitarbeiter Kunden | Organisation | IT

New Business Modell

- Verschmelzung von IT und Geschäft
- Ziele: B2B und B2C
- Wachsende Globalisierung (Internet, EU)
- e-business Modelle
- Kundenschnittstelle ist die IT

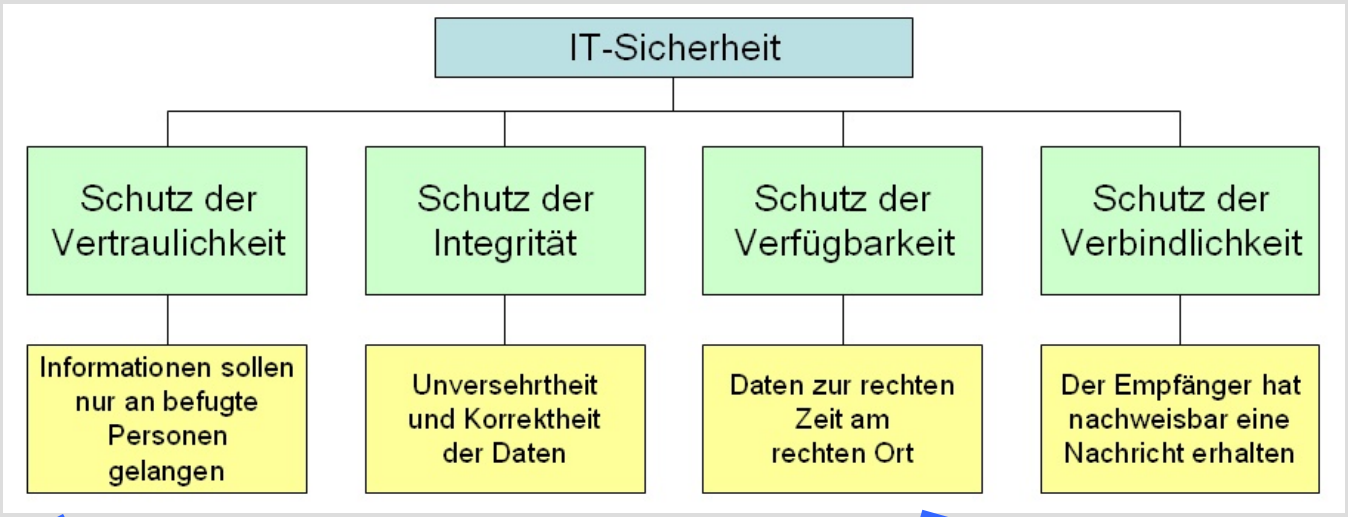
Geschäftsprozesse

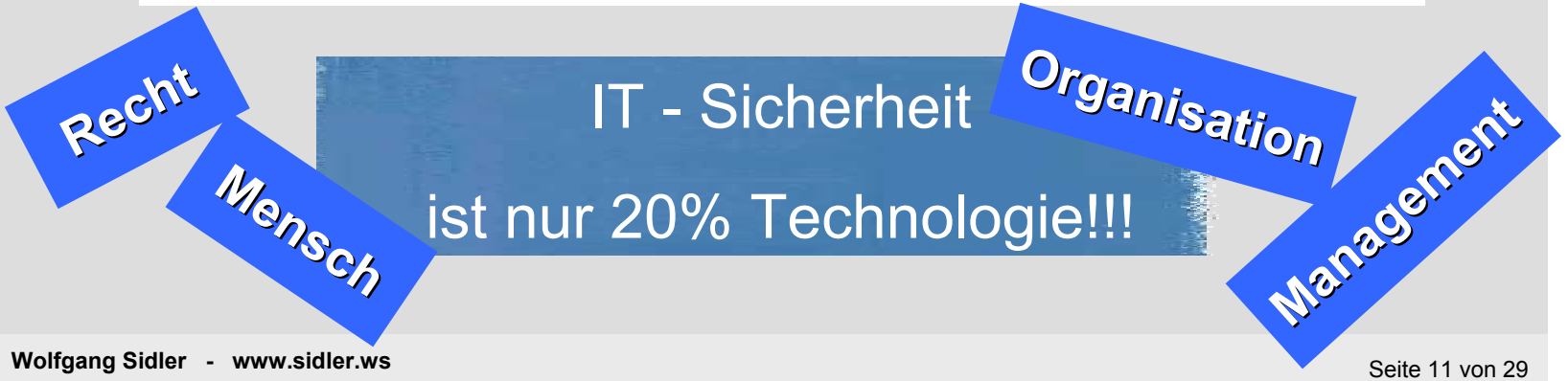
IT

Risiken
Erhöhte Anforderungen an Anwendungen, Verfügbarkeit & Sicherheit

Mitarbeiter Kunden | IT | Organisation

Aufgaben der IT-Sicherheit „Die 4 Pfeiler“





Ziele der IT-Sicherheit

Die Hauptziele einer Sicherheits-Strategie (Organisation)

- **Sicherung der Geschäfts-Prozesse** (BCM und DR)
- **Einhaltung der Gesetze und Verordnungen** (DSG,Basel II, SOX, GebüV)
- **Das Unternehmen und deren Management vor Haftungsklagen schützen**
- **Daten-Missbrauch und –Diebstahl erkennen und verhindern**
- **Alle Mitarbeiter in Bezug auf Sicherheit sensibilisieren**

Kritische Erfolgsfaktoren

- Leitlinien, Ziele und Massnahmen spiegeln die Geschäftsziele Ihrer Unternehmung
- Die Umsetzung des Sicherheitskonzeptes entspricht Ihrer Firmenkultur bzw. Branche (Best Practice)
- Sichtbare Unterstützung und Verbindlichkeit durch die Geschäftsleitung (die Verantwortung kann nicht delegiert werden!)
- Effektives „Marketing“ der IT-Sicherheit innerhalb der Firma „Sicherheitsbewusstsein – Kultur“ fördern (Awareness-Kampagne)
- Ein klares Verständnis für Sicherheitsanforderungen, Risikobewertung und Risikobehandlung (Restrisiken kennen)
- Messbare Überprüfung der erreichten IT-Sicherheit (ROSI)

IT-Sicherheits Prozess II

IT-Protection Service AG 3. März 2006

Mensch – Organisation – Technologie

System von Verfahren und Regeln zur dauerhaften Steuerung und Kontrolle der Informations-sicherheit

1

Entwicklung einer Sicherheits-Politik

- Geltungsbereich
- Sicherheitsleitline
- Organisationsstruktur

2

Erstellen des IT-Sicherheits-Konzeptes

- Ziele
- Risiken
- Massnahmen

3

Umsetzung des IT-Sicherheits-Konzeptes

- Verantwortlichkeiten
- Realisierung
- Sensibilisierung

4

Überprüfung der IT-Sicherheit

- Überwachung
- Überprüfung
- Reports

5

Aufrechterhalten der IT-Sicherheit

- Revision
- Change-Management

IT-Sicherheits-Grundsätze

IT-Protection Service AG 3. März 2006

Management-Grundsätze von Malik

- Ausrichtung auf Resultate
- Beitrag ans Ganze
- Konzentration auf Weniges
- Stärken nutzen
- Vertrauen
- Konstruktives Denken

Quelle: Malik, Management 2005, Band 1

Security-Grundsätze von W.Sidler

- Vermeiden von Risiken
- Gesamtheitlichkeit
- lieber 5 als 30 umgesetzte Sicherheitsmassnahmen
- Kernkompetenzen nutzen Security = outsourcen
- Sicherheit schafft Vertrauen
- In Szenarien denken

Quelle: W.Sidler 2006

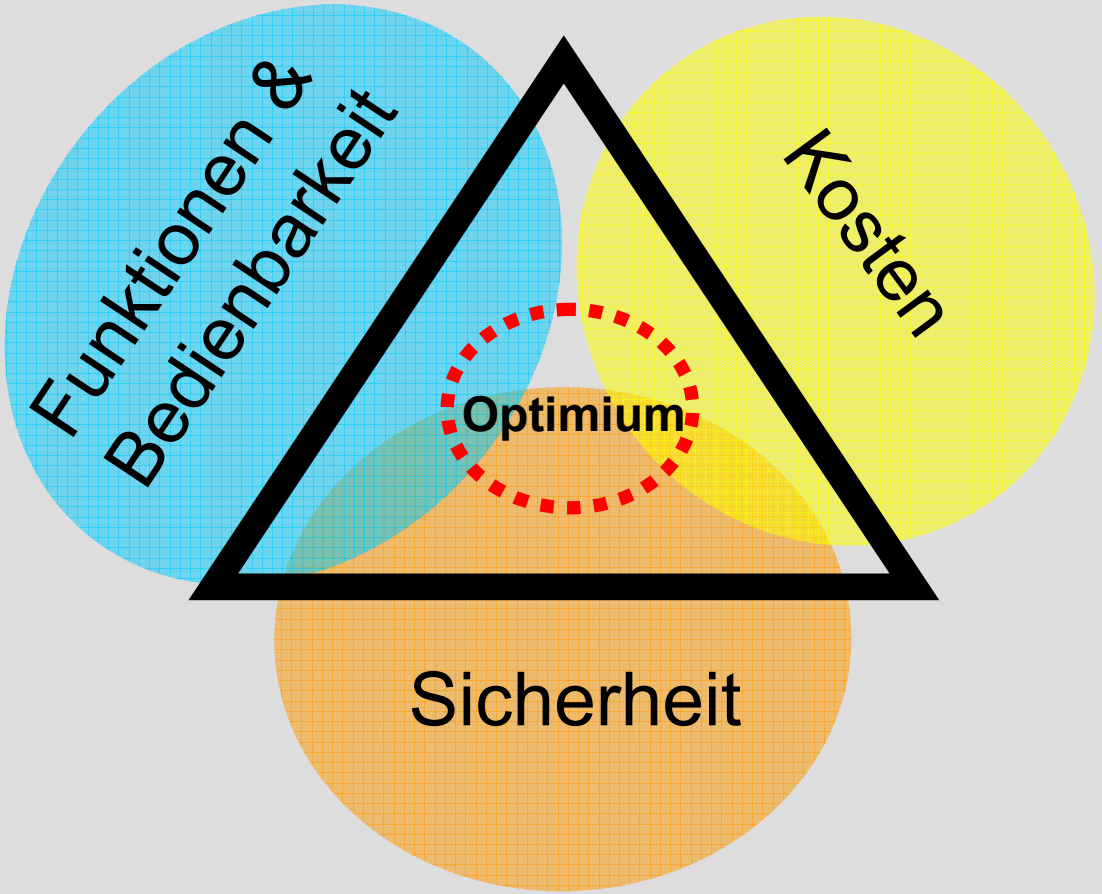
Die goldenen Sicherheits-Grundregeln

IT-Protection Service AG 3. März 2006

- Erstellen Sie ein Pflichtenheft/Sicherheitspolitik für IT-Verantwortliche!
- Sichern Sie Ihre Daten regelmässig mit Backups!
- Halten Sie Ihr Antivirus-Programm aktuell!
- Schützen Sie Ihren Internetzugang mit einer Firewall! (URL- und SPAM-Filter)
- Aktualisieren Sie Ihre Software regelmässig (Updates)!
- Verwenden Sie starke Passwörter!
- Schützen Sie Ihre mobilen Geräte! (Notebook, PDA, Natel, Smartphones)
- Machen Sie Ihre IT-Benutzerrichtlinien bekannt! (Awareness)
- Schützen Sie die Umgebung Ihrer IT-Infrastruktur! (physische Sicherheit)
- Ordnen Sie Ihre Dokumente und Datenträger! (Data-Owner, Klassifizierung etc.)
- Verwenden Sie eine sichere Wireless Lösung!
- Clear Desk Policy (alles unter Verschluss!)
- Erstellen Sie einen Notfallplanung / Disaster Recovery!
- Archivieren Sie alle geschäftlich relevanten Daten, Dokumente etc.
- Einhaltung der Gesetze und Verordnungen!
- Geschäftsprozesse und deren Abhängigkeiten kennen (Risiko-Analyse)
- Sicherheit ist Chef-Sache, eine Management-Aufgabe
- Sicherheit muss gelebt werden (Sicherheitskultur)

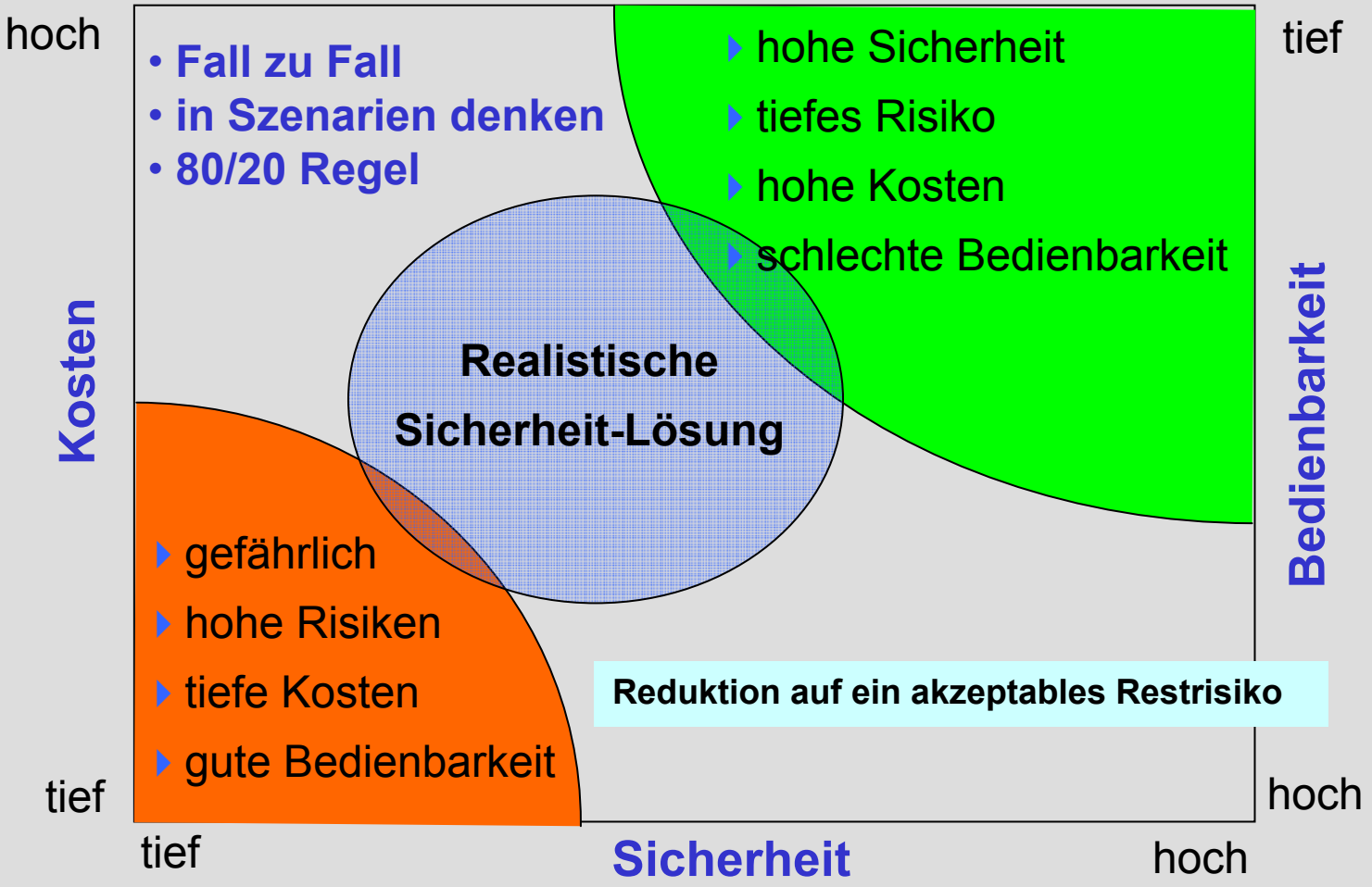
Die Lösung

IT-Protection Service AG 3. März 2006



Die Lösung I

IT-Protection Service AG 3. März 2006



Datenschutz Ausgangslage

IT-Protection Service AG 3. März 2006

- **Schutz der Persönlichkeit der Arbeitnehmenden (Arbeitgeber)**
- **Sorgfalts- und Treupflicht (Arbeitnehmer)**

- **Technologische Entwicklung**
- **Kontrolle und Überwachung**

- **Datenschutzrechtliche Rahmenbedingungen**

OR: Art. 328b
Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind.
Im Übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz.

Datenschutz Rahmenbedingungen

IT-Protection Service AG 3. März 2006

- **Rechtmässigkeit (Rechtsgrundlage)**
  - Datenbeschaffung, Treu und Glauben, Rechtfertigungsgrund, Einwilligung
- **Verhältnismässigkeit**
  - Geeignet und erforderlich (vor, während, nach dem Anstellungsverhältnis)
- **Zweckgebundenheit**
  - Verwendung von Personaldaten
- **Transparenz**
- **Integrität**
  - Korrektheit und Vollständigkeit der Daten

Ziel:
Rechtskonformer und sicherer Umgang mit Personendaten!

Respektierung der Personen!

Datenschutz Beispiele

IT-Protection Service AG 3. März 2006

- **E-Mail Überwachung**
- **Internet Benutzung**
- **Video Überwachung**
- **Telefon Überwachung (Fixnet und Mobile)**
- **Daten Speicherung (Archiv)**
- **Datenspuren (GSM, Kreditkarten etc.)**
- **Daten-Transfer ins Ausland (EU und nicht EU)**
- **Neue Technologien und Trends wie:**
  - Voice over IP
  - Outsourcing / Offshoring
  - Blackberry, Smartphones etc.

Datenschutz in der Schweiz

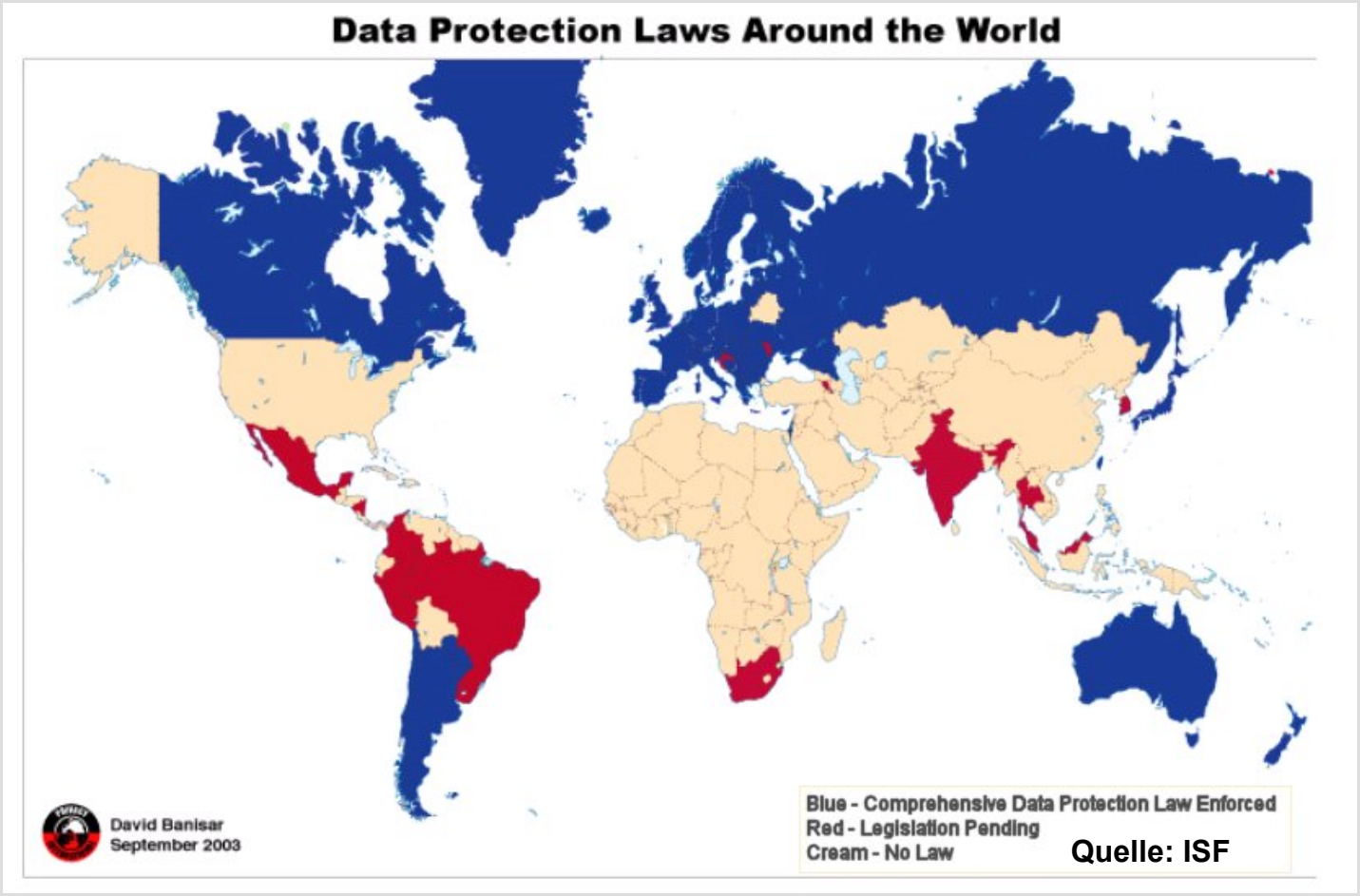
IT-Protection Service AG 3. März 2006

<< Die Kantone nehmen einen Grossteil der gesetzlichen Aufgaben beim Datenschutz gar nicht wahr >>, sagt Beat Rudin, Geschäftsführer der Stiftung für Datenschutz und Informationssicherheit.

Kanton	Stellenprozente	Bemerkung
BL, BS, BE, FR, GR, SO, TI, ZH und **ZG**	50 – 520%	In FR existiert eine Datenschutzkommission.
AR, AI, SH und UR	freiberuflich tätige Anwälte mit max. 10%	
GL, OW, SG, TG und VD	weniger als 10%	Stabsstellen der Staatskanzlei, Rechtsdienstes etc.
AG, GE, JU, NE, NW, SZ und VS	nur Datenschutzkommissionen organisiert im Milizsystem	

Datenschutz weltweit?

IT-Protection Service AG 3. März 2006



Datenschutz EU Übersicht

IT-Protection Service AG 3. März 2006

- *Data Protection Directive (1995):* **Welches das Framework für staatliche Rechte und harmonisierte zugelassene Standards für Datenschutz sicherstellt.**

- *Telecommunications Privacy Directive (1997):* **Welches spezifische Schutzvorkehrungen im Bereich Telekommunikation, digitales Fernsehen und mobile Netzwerke (GSM etc.) bewegliche Netze und andere Nachrichtentechniksysteme gewährleistet.**

- *Privacy and Electronic Communications Directive (2003):* **Welches spezifische Anforderungen für die Privatsphäre der modernen Technologien, wie mobile Telefone, Internet und E-Mail liefert.**

Datenschutz Schweiz Übersicht

IT-Protection Service AG 3. März 2006

Persönliche Informationen müssen:

- **müssen sicher und legal gehalten (gespeichert) werden**
- **dürfen nur legal beschafft werden**
- **dürfen nur für den vorbestimmten Verwendungszweck benutzt werden**
- **Die Verwendung muss angemessen, sachbezogen und darf nicht übermässig (Verhältnismässigkeit) eingesetzt werden.**
- **müssen genau und aktuell sein**
- **müssen erreichbar für den Besitzer sein**
- **müssen sicher gespeichert werden (CIA)**
- **müssen nach dem Gebrauch unwiderruflich zerstört werden**
- **dürfen nicht in ein anderes Land mit tieferem Datenschutz transferiert werden.**

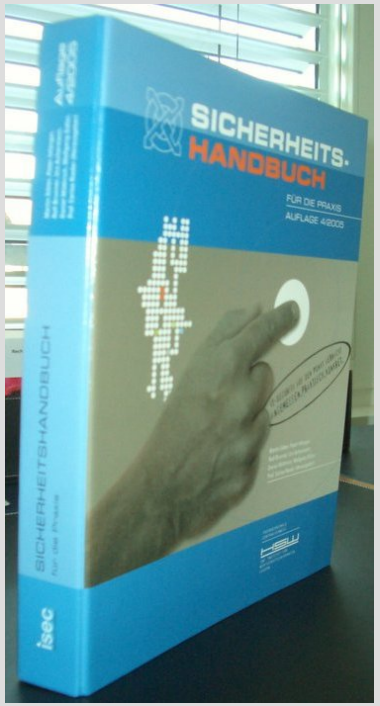
Ihr Nutzen

Was für einen Nutzen erhalten Sie?

- Positive Audits (interne und externe Revision)
- Bessere Kreditwürdigkeit (Basel II)
- Erhöhtes Kundenvertrauen, Zertifizierung für bessere Kunden-Privacy (GoodPriv@cy, ISO17799)
- einhalten aller Gesetze (Datenschutz etc.)
- Wettbewerbsvorteil
- Reduziert das Risiko einer Geschäftsunterbrechung erheblich
- Transparenz in Bezug auf den Umgang mit der Sicherheit (Sicherheits-Kultur)
- Fördert das „Sicherheitsbewusstsein“ der Mitarbeiter
- Ein klares Verständnis für Sicherheitsanforderungen, Risikobewertung und Risikobehandlung
- Steigert die Möglichkeit neue Geschäfts-Felder sicher und schneller anzugehen

Das neue Schweizer Standardwerk der IT-Sicherheit

Umfang:	A4-Ordner mit 337 Seiten
Auflage:	Version 4
ISBN:	3-9521208-3-9
Preis:	CHF 248.-
Bestellung unter:	www.sidler.ws



www.swiss-IT-markt.ch

IT-Protection Service AG 3. März 2006

Besuchen Sie uns ab dem 1. April auf unserem „Onlineshop für Unternehmen“.

- **SwissCASH** Bonus-System
- Tagesaktuelle Preise und hohe Verfügbarkeit
- Über 15‘000 IT-Artikel
- Einfaches Finden von Produkten
- Online-Verkaufberater – eine Neuheit!
- Schnelle und zuverlässige Lieferung

Fragen

«Es ist eine verbreitete Illusion zu glauben, dass das, was wir heute wissen, alles ist, was wir je zu wissen vermögen»

Carl G. Jung