Willkommen zur Präsentation

CC Data-Disc Security-Days 26. April 2006

CC Data-Disc Security-Days

„IT-Security, IT-Risk Management und Datenschutz 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

CC Data-Disc Security-Days 26. April 2006

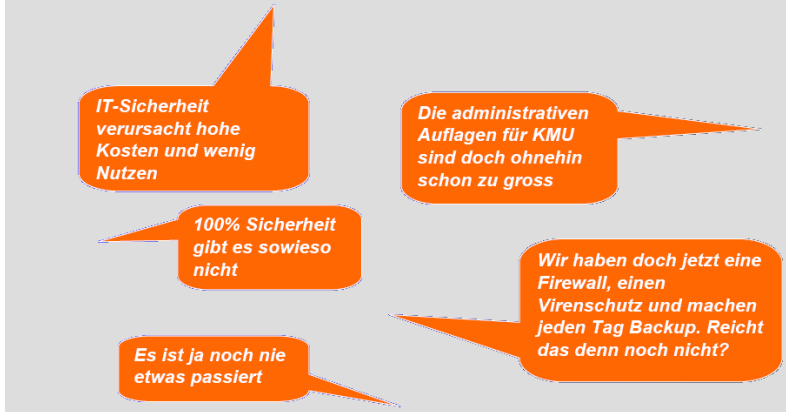
- **Abhängigkeit und Komplexität der Geschäftsprozesse in Bezug auf die IT steigt und das Bewusstsein für diese Abhängigkeit fehlt häufig.**
- **Verantwortlichkeiten sind nicht klar und ignorieren der Risiken.**
- **Die Häufigkeit und die Art der Bedrohungen nehmen stetig zu.**
- **Missverständnisse 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

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

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



Bedrohungen

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 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, Sabotage, Spionage, Hacking, Erpressung, Viren, organisierte Kriminalität, ...

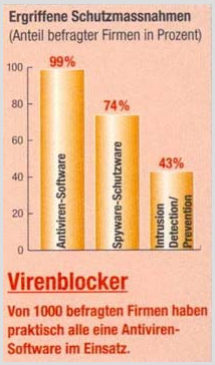
Aktuelle CH-Studien

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

Die Studie zeigt weiter, dass insgesamt 223 Millionen Franken für die IT-Sicherheit ausgegeben wird. Fast alle KMU (98,6%) haben einen Virenschutz, 86 Prozent verfügen über einen Spamschutz und 81,2 Prozent setzen Anti-Spyware-Lösungen ein.

Quelle: Netzreport 2006



Quelle: PWC Studie, März 2006

Quelle: Accenture, April 2006

2005:
5198 neue Sicherheitslücken

Beobachtungen aus der Praxis

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

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

Was ist ein Risiko?

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

R = Wahrscheinlichkeit (Häufigkeit) * Ausmass des Schadenereignisses

$$R = \frac{\text{Assets x Vulnerablilties x Threats}}{\text{Criticality}}$$

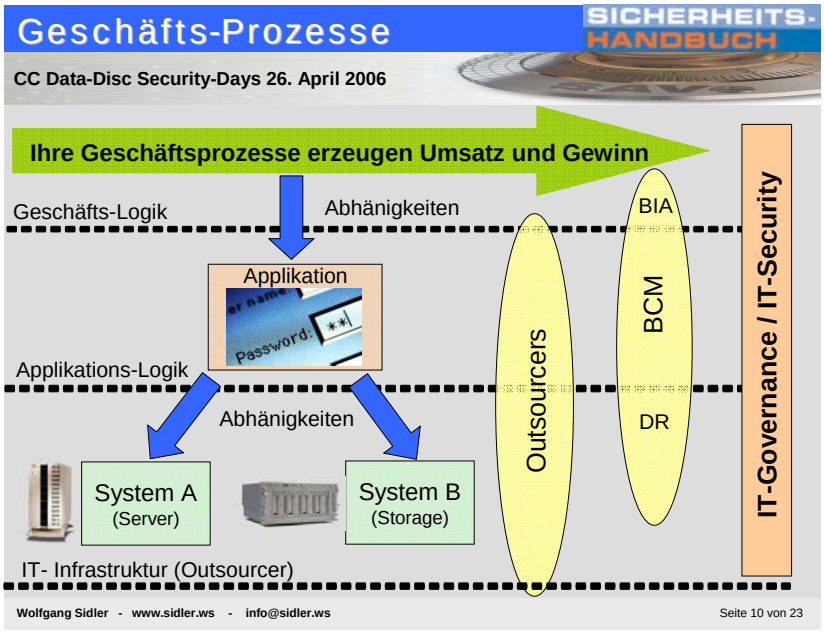
Die wissentliche oder unwissentliche Inkaufnahme eines Verlusts in bestimmter Höhe im Verhältnis zur Eintretenswahrscheinlichkeit.

Abstrakte versus konkrete Risiken

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

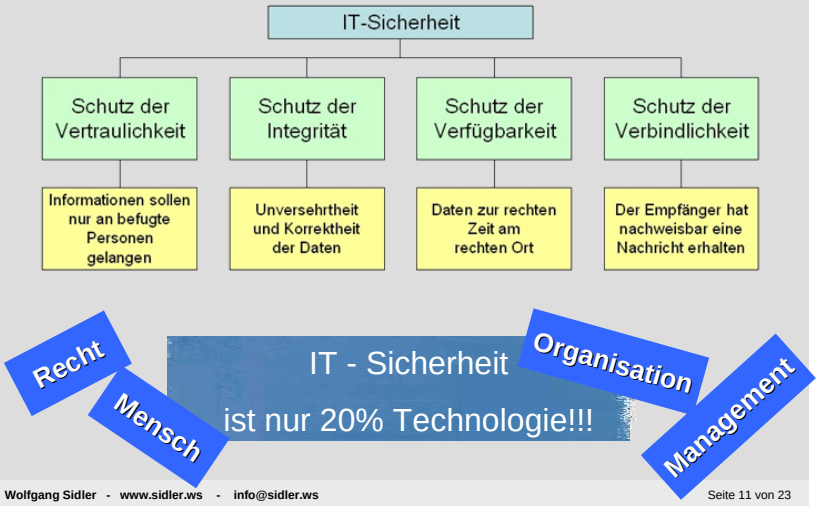

Umgang mit Risiken
SICHERHEITS-HANDBUCH
CC Data-Disc Security-Days 26. April 2006
Sicherheitsdispositiv
laufende Überprüfung
Gesamtrisiko
vermeiden
• Gebäude
• Zutrittskontrollen
• Redundanzen
• Personal
• Gewaltentrennung
vermindern
• Krisenstäbe
• Katastrophenplanung
• Ausbildung
• Training
überwälzen
• Versicherung
selbst tragen
• Restrisiko
Operationelles Risiko – das Risiko von Verlusten infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignissen.
Quelle: Geschäftsbericht 2005 der Credit Suisse Group
Wolfgang Sidler - www.sidler.ws - info@sidler.ws
Seite 9 von 23


Geschäfts-Prozesse
SICHERHEITS-HANDBUCH
CC Data-Disc Security-Days 26. April 2006
Ihre Geschäftsprozesse erzeugen Umsatz und Gewinn
Geschäfts-Logik
Abhänigkeiten
Applikation
Password:
Applikations-Logik
Abhänigkeiten
System A
(Server)
System B
(Storage)
IT- Infrastruktur (Outsourcer)
Outsourcers
BIA
BCM
DR
IT-Governance / IT-Security
Wolfgang Sidler - www.sidler.ws - info@sidler.ws
Seite 10 von 23

Was ist IT-Sicherheit?

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006



Ziele der IT-Sicherheit

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

- **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**

IT-Sicherheits-Prozess

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

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 (Security Audit)

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 13 von 23

IT-Sicherheits-Grundsätze

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

Management-Grundsätze von Prof. Malik	Security-Grundsätze von W.Sidler
Ausrichtung auf Resultate	Vermeiden von Risiken
Beitrag ans Ganze	Gesamtheitlichkeit
Konzentration auf Weniges	lieber 5 als 30 umgesetzte Sicherheitsmassnahmen
Stärken nutzen	Kernkompetenzen nutzen Security = outsourcen
Vertrauen	Sicherheit schafft Vertrauen
Konstruktives Denken	In Szenarien denken

Quelle: Malik, Management 2005, Band 1

Quelle: W.Sidler 2006

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 14 von 23

Die Sicherheits-Grundregeln

SICHERHEITS-HANDBUCH

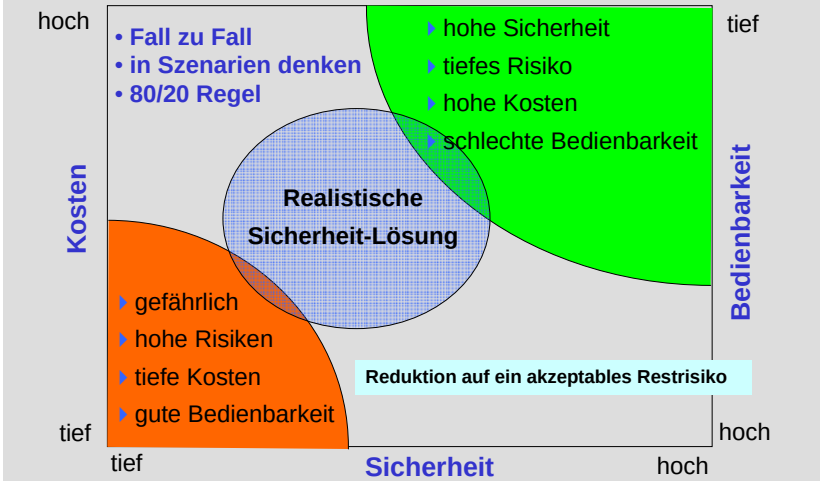
CC Data-Disc Security-Days 26. April 2006

- Erstellen Sie ein Pflichtenheft/Sicherheitspolitik für IT-Verantwortliche!
- Datensicherung
- Virenschutz
- Firewall! (URL- und SPAM-Filter)
- Software-Update
- 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.)

Die Lösung

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006



Datenschutz Ausgangslage

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 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.

DSG Rahmenbedingungen

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 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 in der Schweiz

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

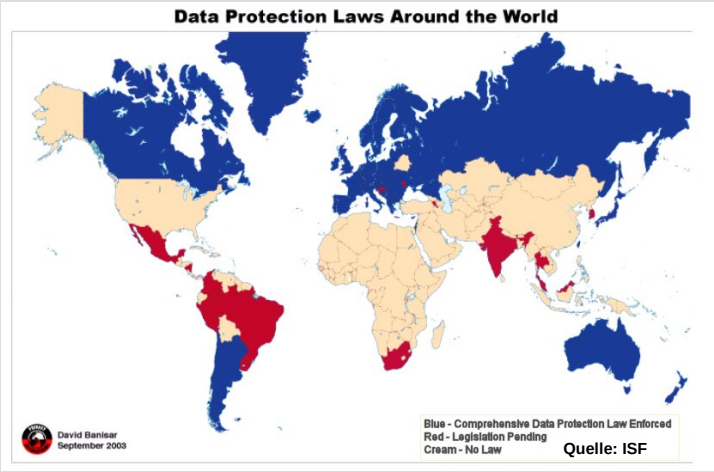
<< Die Kantone nehmen einen Grossteil der gesetzlichen Aufgaben beim Datenschutz gar nicht wahr >>, sagt Beat Rudin, Geschäftsführer der Stiftung für Datenschutz und Informationssicherheit.

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?

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006



Archivierung

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

Die Buchführungsvorschriften (GebüV 24.4.2002) verpflichten die Unternehmen, alle Geschäftsdokumente aufzubewahren, die zum Verständnis und zum Nachweis der Vermögenslage und des Geschäftsergebnisses erforderlich sind.

Aufbewahrungsform
Gemäss Art. 957ff OR müssen nur die Bilanz und die Erfolgsrechnung im Original aufbewahrt werden. Die Bücher, die Belege und die Geschäftskorrespondenz dürfen hingegen schriftlich, elektronisch oder in vergleichbarer Weise geführt werden.

Die **Integrität** und **Verfügbarkeit** der aufbewahrungspflichtigen Dokumente ist während der gesamten Aufbewahrungsdauer (10 Jahre) sicherzustellen.

Ihr Nutzen: Kosteneinsparungen, Prozessoptimierung und das vereinfachte Suchen und Finden von Dokumenten

Der Mangel an Beweisen kann im Streitfall zum Verlust eines Gerichtsprozesses führen *(Art. 325 StGB[11]).*

Ihr Nutzen

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006

- **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.)**
- **Sichere Kommunikation und eindeutige Identifikation**
- **Wettbewerbsvorteil**
- **Reduziert das Risiko einer Geschäftsunterbrechung erheblich (hohe Verfügbarkeit)**
- **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**

Fragen

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006