

Willkommen zur Präsentation **SICHERHEITS-
HANDBUCH**

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

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 1 von 23

Ausgangslage **SICHERHEITS-
HANDBUCH**

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.**

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 2 von 23

Ausgangslage I **SICHERHEITS-HANDBUCH**

CC Data-Disc Security-Days 26. April 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

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 3 von 23

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, ...

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 4 von 23

Aktuelle CH-Studien

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

Ergriffene Schutzmassnahmen
(Anteil befragter Firmen in Prozent)

Virenblocker

Von 1000 befragten Firmen haben praktisch alle eine Antiviren-Software im Einsatz.

Quelle: PWC Studie, März 2006

Top-CIO-Themen der nächsten 24 Monate

Befragte wurden 67 CIOs, die jeweils für drei ihrer Top-Prioritäten je drei, zwei und einen Punkt angeben durften. Nicht alle Befragten haben drei Prioritäten genannt. Quelle: Accenture-Barometer

Quelle: Accenture, April 2006

2005:
5198 neue Sicherheitslücken

Wolfgang Sidler - www.sidler.ws - info@sidler.ws
Seite 5 von 23

Beobachtungen aus der Praxis

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.**

Wolfgang Sidler - www.sidler.ws - info@sidler.ws
Seite 6 von 23

Wolfgang Sidler - www.sidler.ws

3

Was ist ein Risiko? **SICHERHEITS-HANDBUCH**

CC Data-Disc Security-Days 26. April 2006

R = Wahrscheinlichkeit (Häufigkeit) * Ausmass des Schadenereignisses

**R = Assets x Vulnerabilities x Threats
Criticality**

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

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 7 von 23

Abstrakte versus konkrete Risiken **SICHERHEITS-HANDBUCH**

CC Data-Disc Security-Days 26. April 2006



Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 8 von 23

Umgang mit Risiken **SICHERHEITS-HANDBUCH**

CC Data-Disc Security-Days 26. April 2006

Sicherheitsdispositiv

Gesamtrisiko

selbst tragen
• Restrisiko

überwälzen
• Versicherung

vermindern
• Krisenstäbe
• Katastrophenplanung
• Ausbildung
• Training

vermeiden
• Gebäude
• Zutrittskontrollen
• Redundanzen
• Personal
• Gewaltentrennung

laufende Überprüfung

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 → **Abhängigkeiten**

Applikations-Logik → **Abhängigkeiten**

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

```
graph TD; IT[IT-Sicherheit] --- A[Schutz der Vertraulichkeit]; IT --- B[Schutz der Integrität]; IT --- C[Schutz der Verfügbarkeit]; IT --- D[Schutz der Verbindlichkeit]; A --- A1[Informationen sollen nur an befugte Personen gelangen]; B --- B1[Unversehrtheit und Korrektheit der Daten]; C --- C1[Daten zur rechten Zeit am rechten Ort]; D --- D1[Der Empfänger hat nachweisbar eine Nachricht erhalten];
```

IT - Sicherheit ist nur 20% Technologie!!!

Recht
Mensch
Organisation
Management

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 11 von 23

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, GebäV)**
- ▶ **Das Unternehmen und deren Management vor Haftungsklagen schützen**
- ▶ **Daten-Missbrauch und -Diebstahl erkennen und verhindern**
- ▶ **Alle Mitarbeiter in Bezug auf Sicherheit sensibilisieren**

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 12 von 23

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 <u>schaft</u> 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.)

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 15 von 23

Die Lösung **SICHERHEITS-HANDBUCH**

CC Data-Disc Security-Days 26. April 2006

hoch

- Fall zu Fall
- in Szenarien denken
- 80/20 Regel

Realistische Sicherheit-Lösung

- ▶ hohe Sicherheit
- ▶ tiefes Risiko
- ▶ hohe Kosten
- ▶ schlechte Bedienbarkeit

Kosten

- ▶ gefährlich
- ▶ hohe Risiken
- ▶ tiefe Kosten
- ▶ gute Bedienbarkeit

Reduktion auf ein akzeptables Restrisiko

Sicherheit

tief

hoch

Bedienbarkeit

hoch

tief

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 16 von 23

Datenschutz Ausgangslage **SICHERHEITS-HANDBUCH**
CC Data-Disc Security-Days 26. April 2006

The diagram consists of three horizontal boxes connected by double-headed blue arrows. The top box (light blue) contains: **• Schutz der Persönlichkeit der Arbeitnehmenden (Arbeitgeber)** and **• Sorgfalts- und Treupflicht (Arbeitnehmer)**. The middle box (medium blue) contains: **• Technologische Entwicklung** and **• Kontrolle und Überwachung**. The bottom box (light blue) contains: **• 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.

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 17 von 23

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!

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 18 von 23

Datenschutz in der Schweiz

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.

«Die Kantone nehmen einen Grossteil der gesetzlichen Aufgaben beim Datenschutz gar nicht wahr.»
BEAT RUDIN, STIFTUNG FÜR DATENSCHUTZ UND INFORMATIONSSICHERHEIT

Kanton	Stellenprozent	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	

Wolfgang Sidler - www.sidler.ws - info@sidler.ws
Seite 19 von 23

Datenschutz weltweit?

CC Data-Disc Security-Days 26. April 2006

Blue - Comprehensive Data Protection Law Enforced
Red - Legislation Pending
Cream - No Law
Quelle: ISF

David Banisar
September 2003

Wolfgang Sidler - www.sidler.ws - info@sidler.ws
Seite 20 von 23

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 StGB¹⁾).

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 21 von 23

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

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 22 von 23

Fragen

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 26. April 2006



Restore? Davon haben Sie nichts gesagt. Sie wollten ein Backup-Programm. Wenn Sie Ihre Daten wiederherstellen wollen, müssen Sie unser Restore-Programm für 199 € kaufen.

Warum ist das so teuer???

Weil da ein Backup-Programm integriert ist.

Wolfgang Sidler - www.sidler.ws - info@sidler.ws

Seite 23 von 23