Willkommen zur Präsentation

CC Data-Disc Security-Days 28. April 2006

CC Data-Disc Security-Days

„Das Zusammenspiel von IT-Security, IT-Risk Management und IT-Governance“

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 28. April 2006

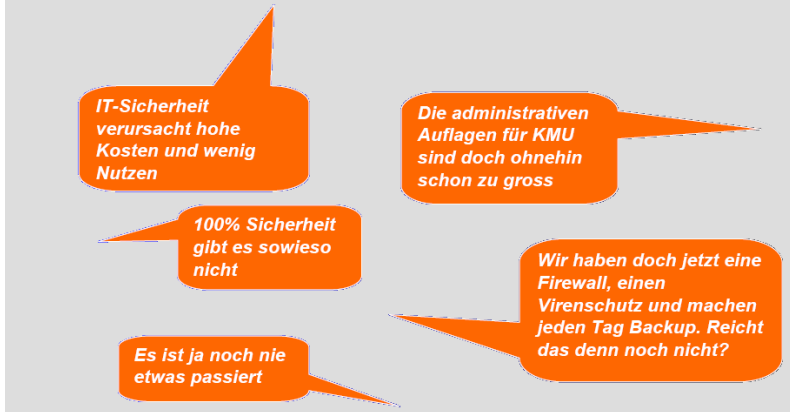
- **Abhängigkeit und Komplexität der Geschäftsprozesse in Bezug auf die IT steigt und das Bewusstsein für diese Abhängigkeit fehlt häufig.**
- **Verantwortlichkeiten sind nicht klar und ignorieren der Risiken.**
- **Die Häufigkeit und die Art der Bedrohungen nehmen stetig zu.**
- **Missverständnisse 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 28. April 2006

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



Bedrohungen

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. 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, ...

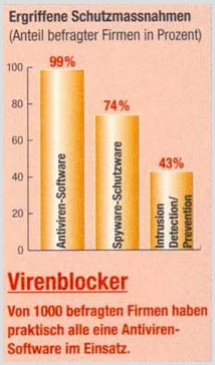
Aktuelle CH-Studien

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. 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 28. 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 28. April 2006

R = Wahrscheinlichkeit (Häufigkeit) * Ausmass des Schadenereignisses

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

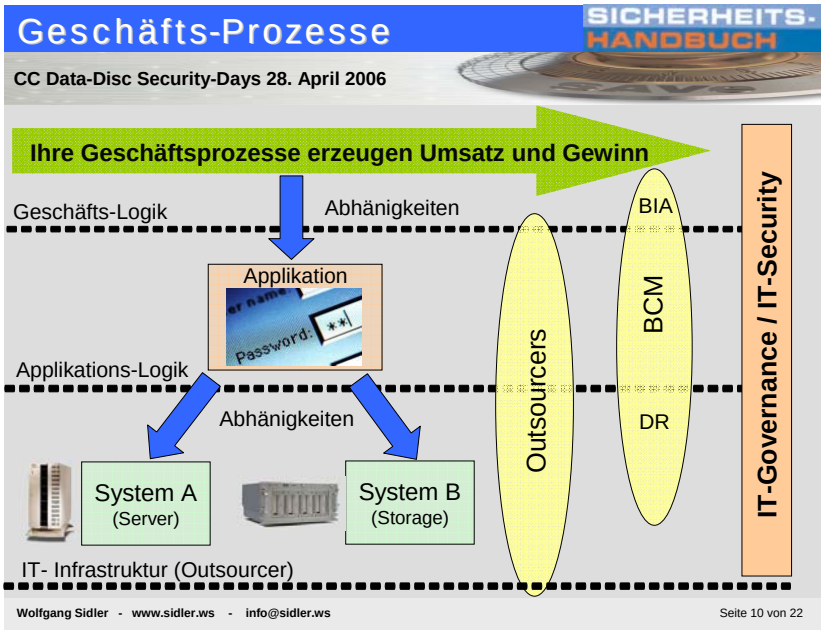
Die wissentliche oder unwissentliche Inkaufnahme eines Verlusts in bestimmter Höhe im Verhältnis zur Eintretenswahrscheinlichkeit.

Abstrakte versus konkrete Risiken

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. April 2006

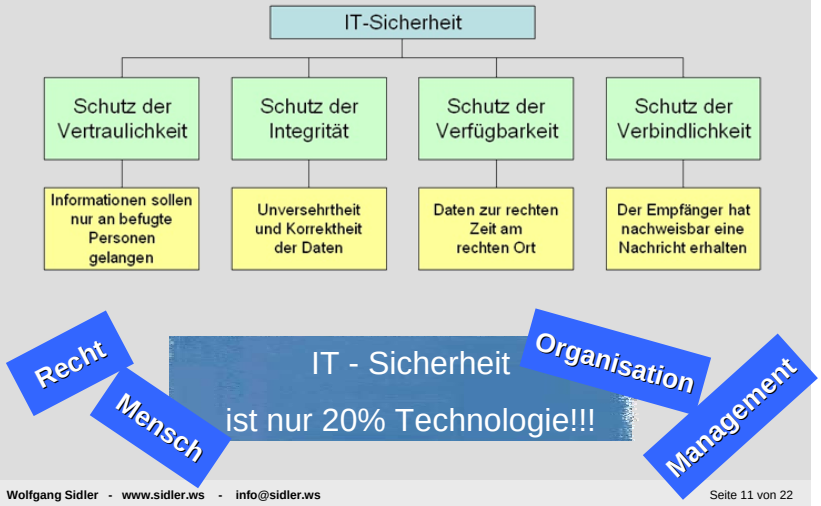

Umgang mit Risiken
SICHERHEITS-HANDBUCH
CC Data-Disc Security-Days 28. April 2006
Sicherheitsdispositiv
laufende Überprüfung
Gesamtrisiko
vermeiden
• Gebäude
• Zutrittskontrollen
• Redundanzen
• Personal
• Gewaltentrennung
vermindern
• Krisenstäbe
• Katastrophenplanung
• Ausbildung
• Training
überwälzen
• 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 22


Geschäfts-Prozesse
SICHERHEITS-HANDBUCH
CC Data-Disc Security-Days 28. 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 22

Was ist IT-Sicherheit?

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. April 2006



Ziele der IT-Sicherheit

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. 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 28. 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)

IT-Sicherheits-Grundsätze

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. 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

Die Sicherheits-Grundregeln

SICHERHEITS-HANDBUCH

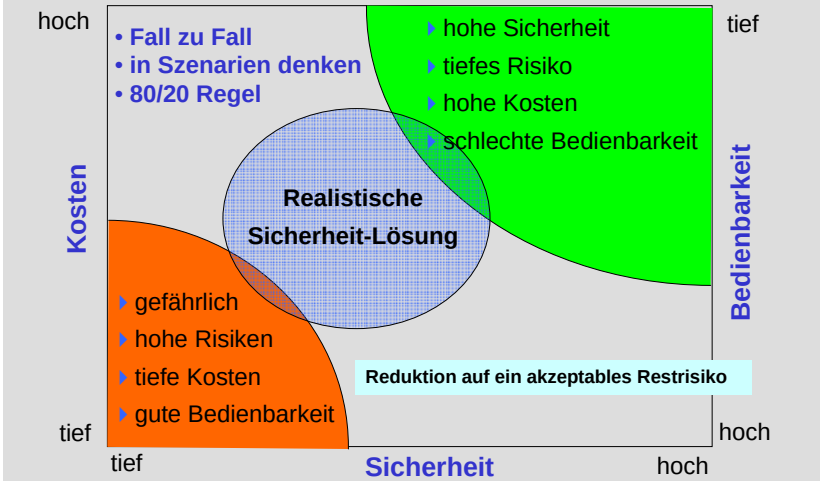
CC Data-Disc Security-Days 28. April 2006

- 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 28. April 2006



IT-Security – Quo Vadis?

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. April 2006

Die gesetzlichen Auflagen (Compliance), Trend zum Business Process Outsourcing (BPO) und der Druck des Business seitens Corporate Governance zwingt die IT in Richtung IT-Governance.

2006 - 2010

IT-Governance

2003 - 2005

IT-Risk Management

1998-2002

IT-Security

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 17 von 22

Was ist IT-Governance?

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. April 2006

- Der Begriff IT-Governance bezeichnet die Organisation, Steuerung und Kontrolle der IT eines Unternehmens durch die Unternehmensführung zur konsequenten Ausrichtung der IT-Prozesse an der Unternehmensstrategie.

oder auf den Punkt gebracht:

- „IT-Governance ist die effiziente und effektive Steuerung und Kontrolle der IT“

Wolfgang Sidler - www.sidler.ws - info@sidler.ws Seite 18 von 22

Ziele von IT-Governance?

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. April 2006

- Fortwährende Ausrichtung der IT an den Unternehmenszielen und Prozessen
- Unterstützung des Unternehmens bei der Erreichung der Geschäftsziele
- Verantwortungsvolle und nachhaltiger Einsatz der IT-Ressourcen
- IT-Risiken minimieren und optimal managen

„Die Umsetzung von gesetzlichen Auflagen in der IT ist nicht nur ein Aufwandsposten, sondern bietet auch eine Optimierungschance!“

„33 Prozent der IT-Abteilungen in Europa können gesetzliche und interne Vorgaben nicht fristgemäss einhalten“

Quelle: Compuware, April 2006

IT-Governance in der Praxis

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. April 2006

- Aufbau einer IT-Risk Management Organisation
- Etablieren eines guten Business-IT Alignement
- Definition von Security Policies & Standards
- Durchführen von Control Reviews (Audits), monitoring
- Planen von IT-Security / IT-Risk Awareness Events

Unterstützende Projekte:

- Identity- und Access Management Projekt
- Data Preservation Projekt (Umgang mit sensiblen Daten, Datenklassifizierung)
- IT-Security / IT-Risk Management Cockpit (MIS), führen eines Risk Kataloges
- Umsetzung der Security Policies & Standards

„IT wird in vielen Unternehmen immer noch eher als Kostenblock denn als strategische Komponente betrachtet“

Ihr Nutzen

SICHERHEITS-HANDBUCH

CC Data-Disc Security-Days 28. 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 28. April 2006

Quelle: LA Times, Sept. 2005