Willkommen zur Präsentation

CA IT-Security Trends 2006 Report 18. Jan. 2006

CA IT Security Trends 2006

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

Wolfgang Sidler

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

Ausgangslage

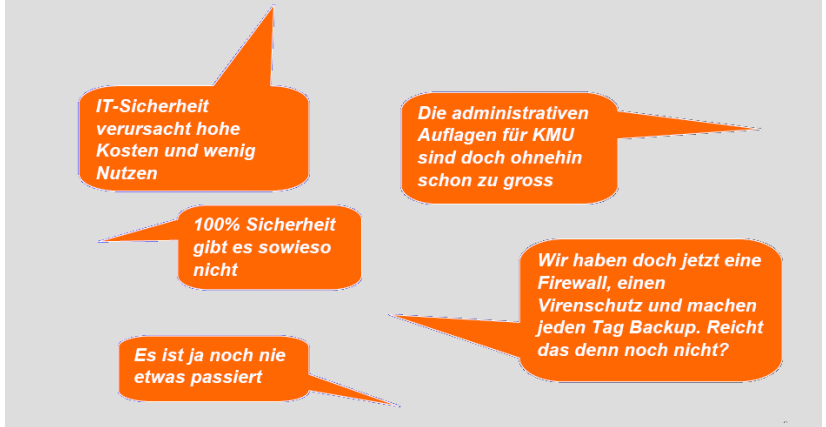
CA IT-Security Trends 2006 Report 18. Jan. 2006

- **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

CA IT-Security Trends 2006 Report 18. Jan. 2006

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



Wolfgang Sidler - www.sidler.ws

Seite 3 von 21

Bedrohungen

CA IT-Security Trends 2006 Report 18. Jan. 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, ...

Wolfgang Sidler - www.sidler.ws

Seite 4 von 21

Beobachtungen aus der Praxis

CA IT-Security Trends 2006 Report 18. Jan. 2006

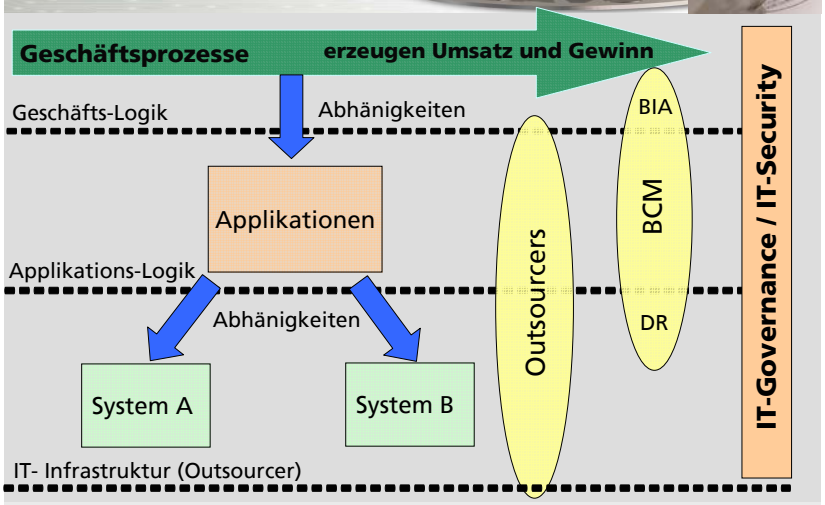
- Unklare,verteilte und unkontrollierte Kompetenzen
- Mangelhafte Aktualisierung der Zutritts-, Zugriffskontrollen
- Nicht Einhaltung vorhandener Prozesse
- Verletzung des Datenschutzgesetzes
- Fehlende Umsetzung festgelegter Schutzmassnahmen
- Sorglosigkeit und fehlendes Sicherheitsbewusstsein
- Defekte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

Wolfgang Sidler - www.sidler.ws

Seite 5 von 21

Geschäfts-Prozesse

CA IT-Security Trends 2006 Report 18. Jan. 2006



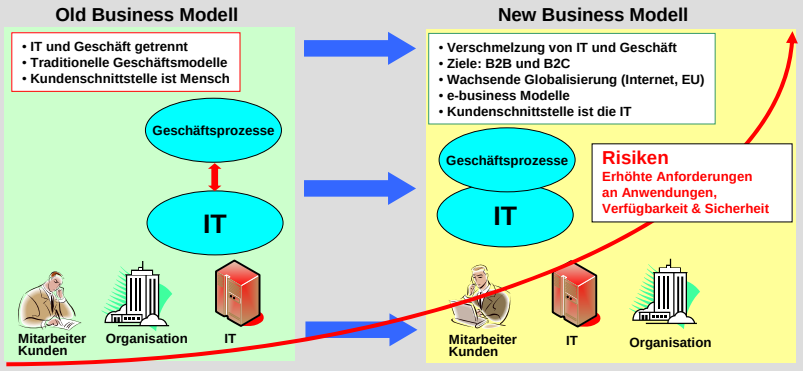
Wolfgang Sidler - www.sidler.ws

Seite 6 von 21

Geschäftsprozess Entwicklung

CA IT-Security Trends 2006 Report 18. Jan. 2006

Vom OLD Business zum NEW Business Modell



Wolfgang Sidler - www.sidler.ws

Seite 7 von 21

IT-Sicherheit

CA IT-Security Trends 2006 Report 18. Jan. 2006

Aufgaben der IT-Sicherheit „Die 4 Pfeiler“

Wolfgang Sidler - www.sidler.ws

Seite 8 von 21

Ziele der IT-Sicherheit

CA IT-Security Trends 2006 Report 18. Jan. 2006

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**

Wolfgang Sidler - www.sidler.ws

Seite 9 von 21

IT-Sicherheits-Prozess I

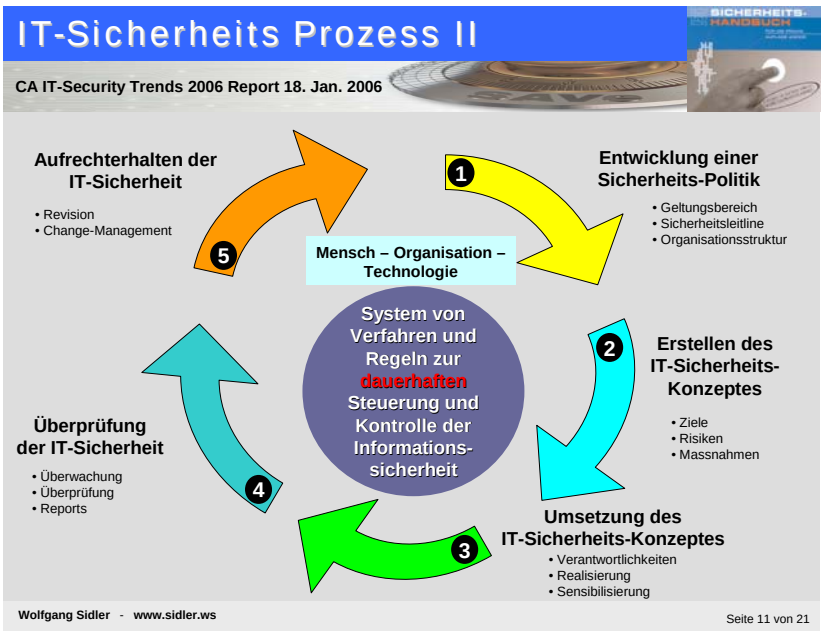
CA IT-Security Trends 2006 Report 18. Jan. 2006

Kritische Erfolgsfaktoren

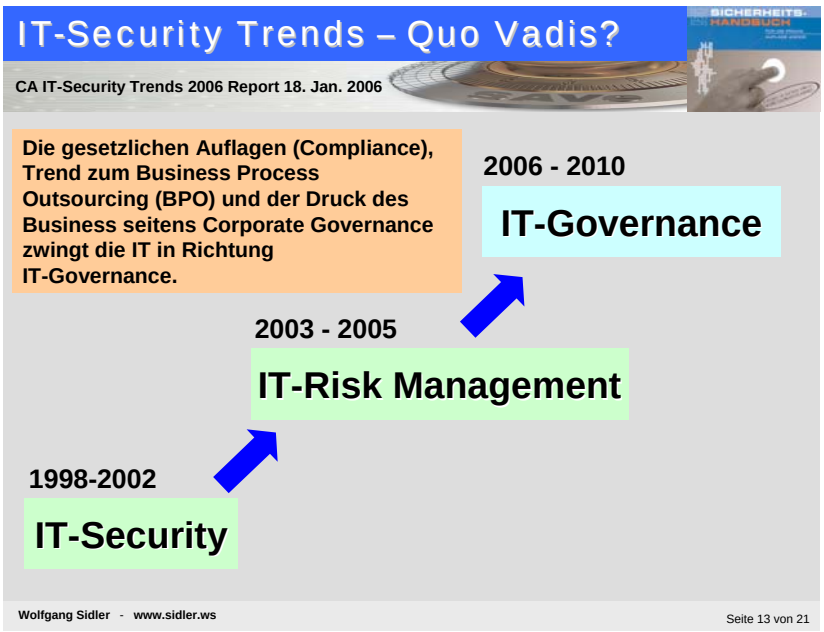
- **Leitlinien, Ziele und Massnahmen spiegeln die Geschäftsziele Ihrer Unternehmung**
- **Die Umsetzung des Sicherheitskonzeptes entspricht Ihrer Firmenkultur bzw. Branche (Best Practice)**
- **Sichtbare Unterstützung und Verbindlichkeit durch die Geschäftsleitung (die Verantwortung kann nicht delegiert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

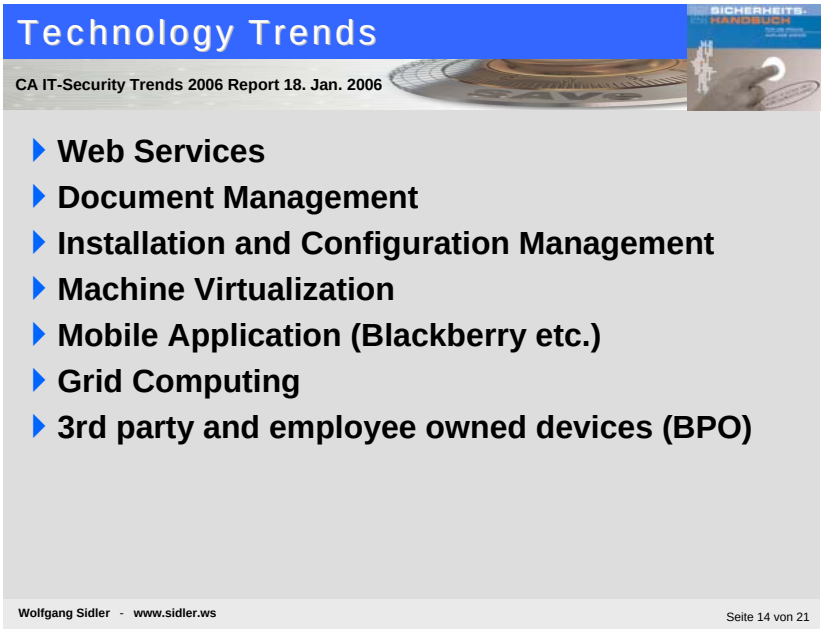
Wolfgang Sidler - www.sidler.ws

Seite 10 von 21


IT-Sicherheits Prozess II
CA IT-Security Trends 2006 Report 18. Jan. 2006
Aufrechterhalten der IT-Sicherheit
• Revision
• Change-Management
Entwicklung einer Sicherheits-Politik
• Geltungsbereich
• Sicherheitsleitline
• Organisationsstruktur
Mensch – Organisation – Technologie
System von Verfahren und Regeln zur dauerhaften Steuerung und Kontrolle der Informations-sicherheit
Erstellen des IT-Sicherheits-Konzeptes
• Ziele
• Risiken
• Massnahmen
Überprüfung der IT-Sicherheit
• Überwachung
• Überprüfung
• Reports
Umsetzung des IT-Sicherheits-Konzeptes
• Verantwortlichkeiten
• Realisierung
• Sensibilisierung
1
2
3
4
5
Wolfgang Sidler - www.sidler.ws
Seite 11 von 21


IT-Risk Management
CA IT-Security Trends 2006 Report 18. Jan. 2006
Umgang mit Risiken
Sicherheitsdispositiv
laufende Überprüfung
Gesamtrisiko
vermeiden
• Gebäude
• Zutrittskontrollen
• Redundanzen
• Personal
• Gewaltentrennung
vermindern
• Krisenstäbe
• Katastrophenplanung
• Ausbildung
• Training
überwälzen
• Versicherung
selbst tragen
• Restrisiko
Wolfgang Sidler - www.sidler.ws
Seite 12 von 21


IT-Security Trends – Quo Vadis?
CA IT-Security Trends 2006 Report 18. Jan. 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
Seite 13 von 21


Technology Trends
CA IT-Security Trends 2006 Report 18. Jan. 2006
Web Services
Document Management
Installation and Configuration Management
Machine Virtualization
Mobile Application (Blackberry etc.)
Grid Computing
3rd party and employee owned devices (BPO)
Wolfgang Sidler - www.sidler.ws
Seite 14 von 21

IT-Risk Trends

CA IT-Security Trends 2006 Report 18. Jan. 2006

- Enterprise single sign-on
- Role Based Access Control (RBAC)
- Network access control
- Smart Cards
- Complex IT-Systems
- Operational Risk (Basel II, SOX)
- Vulnerability Management
- Expand the network perimeter (BPO)
- Organized Crime
- Centralized User Provisioning

Wolfgang Sidler - www.sidler.ws Seite 15 von 21

Was ist IT-Governance?

CA IT-Security Trends 2006 Report 18. Jan. 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 Seite 16 von 21

Ziele von IT-Governance?

CA IT-Security Trends 2006 Report 18. Jan. 2006

- **Fortwährende Ausrichtung der IT an den Unternehmenszielen und –Prozessen**
- **Unterstützung des Unternehmens bei der Erreichung der Geschäftsziele**
- **Verantwortungsvolle und nachhaltiger Einsatz der IT-Resourcen (Mitarbeiter, Systeme, finanzielle Mittel)**
- **IT-Risiken minimieren und optimal managen**

Wolfgang Sidler - www.sidler.ws

Seite 17 von 21

IT-Governance in der Praxis

CA IT-Security Trends 2006 Report 18. Jan. 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 IT-Security / IT-Risk Awareness Events**

Unterstützende Projekte:

- **Identity- und Access Management Projekte**
- **Data Preservation Projekte**
- **IT-Security / IT-Risk Management Cockpit (MIS), führen eines Risk Kataloges**
- **Umsetzung der Security Policies & Standards**

Wolfgang Sidler - www.sidler.ws

Seite 18 von 21

Nutzen

CA IT-Security Trends 2006 Report 18. Jan. 2006

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 „Sicherheits- und Risiko-Bewusstsein“ 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

Seite 19 von 21

Das Sicherheitshandbuch für die Praxis

CA IT-Security Trends 2006 Report 18. Jan. 2006

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

Wolfgang Sidler - www.sidler.ws

Seite 20 von 21

Fragen

CA IT-Security Trends 2006 Report 18. Jan. 2006

Quelle: LA Times, Sept. 2005