

Willkommen zur Präsentation

KeyNet Technologieseminar 17. Juni 2005

**KeyNet Technologieseminar**  
**„IT Sicherheitsorganisation“**

**Wolfgang Sidler**  
IT Sicherheitsbeauftragter, Bank Julius Bär

- Mitautor «Sicherheitshandbuch für die Praxis» [www.sihb.ch](http://www.sihb.ch)
- Wirtschaftsinformatiker, Nachdiplom FH Informatiksicicherheit
- Microsoft Certified Systems Engineer (MCSE)

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 1 von 29

Agenda

KeyNet Technologieseminar 17. Juni 2005

1. Ausgangslage / Erkenntnisse
2. Bedrohungen
3. Beobachtungen aus der Praxis
4. Aktuelle Sicherheits-Vorfälle
5. Das Risiko
6. Business-Prozesse
7. IT-Sicherheit / Sicherheitsprozess
8. Die Lösung
9. Nutzen
10. Das Sicherheitshandbuch für die Praxis
11. Fragen

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 2 von 29

## Ausgangslage / Erkenntnisse

KeyNet Technologieseminar 17. Juni 2005

- ▶ 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

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 3 von 29

## Ausgangslage / Erkenntnisse I

KeyNet Technologieseminar 17. Juni 2005

### 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](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 4 von 29

## Ausgangslage / Erkenntnisse II

KeyNet Technologieseminar 17. Juni 2005

### Security: Top-Thema bei Schweizer CIOs

Während mehr in IT-Security investiert wird, werden die Bereiche ERP und IT-Infrastruktur abgebaut.

Bei den Schweizer CIOs ist IT-Security in den kommenden Jahren das wichtigste Thema. Rund 75 Prozent der Unternehmen werden in den nächsten fünf Jahren mehr für IT-Sicherheit ausgeben. In den Bereichen ERP (Enterprise Resource Planning) und IT-Infrastruktur wird hingegen mehrheitlich abgebaut. Dies sind die Resultate der Studie «IT-Trends 2005» von Cappemini. Erstmals wurden für die Erhebung neben 152 deutschen auch 37 österreichische und 21 Schweizer CIOs von Unternehmen mit mehr als 250 Millionen Euro Umsatz befragt. Auf den weiteren Rängen der Prioritätenliste stehen Business Intelligence mit 59 Prozent, gefolgt von ERP (55%) sowie EAI (Enterprise Application Integration) und CRM (Customer Relationship Management) mit jeweils 47 Prozent.

Als zentrales Problem identifizieren die Schweizer CIOs den Geldmangel.

#### Resultat der Studie „IT-Trends 2005“ von Cappemini

- a) Zentrales Problem „Geldmangel“
- b) Dezentrale Organisationen
- c) Fehlende Abstimmung mit Business
- d) Unklare IT-Massnahmen
- e) Zu viele Projekte
- f) Zu wenig Ressourcen

#### Wichtigkeit von IT-Themen bei Schweizer CIOs

Security	100%
Business Intelligence	59%
ERP (Enterprise Resource Planning)	55%
CRM (Customer Relationship Management)	47%
EAI (Enterprise Application Integration)	47%
Marketing/Website	43%
Portale	41%
IT-Infrastruktur	20%

Quelle: Cappemini «IT-Trends 2005»

Quelle: InfoWeek.ch, März 2005

Wolfgang Sidler - www.sidler.ws

Sicherheitshandbuch für die Praxis www.sihb.ch

Seite 5 von 29

## Bedrohungen

KeyNet Technologieseminar 17. Juni 2005

- ▶ **Höhere Gewalt**
  - ▶▶ Feuer, Blitz, Sturm, Überschwemmung, Stromausfall, Krankheit
- ▶ **Menschliches Versagen**
  - ▶▶ Bedienungsfehler, Unwissen, falsches Verhalten, ...
- ▶ **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)
- ▶ **Vorsätzliche Handlungen**
  - ▶▶ Manipulation, Diebstahl, Missbrauch, Spionage, Hacking, Erpressung, Viren, organisierte Kriminalität ...

Wolfgang Sidler - www.sidler.ws

Sicherheitshandbuch für die Praxis www.sihb.ch

Seite 6 von 29

## Beobachtungen aus der Praxis

KeyNet Technologieseminar 17. Juni 2005

- ▶ Unklare, verteilte und unkontrollierte Kompetenzen
- ▶ Mangelhafte Aktualisierung der Zutritts-, Zugriffskontrollen
- ▶ Unzureichende Nutzung bzw. Auswertung vorhandener Überwachungsfunktionen
- ▶ Fehlende Umsetzung festgelegter Schutzmassnahmen
- ▶ Sorglosigkeit und fehlendes Sicherheitsbewusstsein
- ▶ Defekte Festplatten, andere Datenträger und Dokumente werden nicht fachgerecht entsorgt
- ▶ etc.

Wolfgang Sidler - www.sidler.ws      Sicherheitshandbuch für die Praxis www.sihb.ch      Seite 7 von 29

## Aktuelle Sicherheits-Vorfälle

KeyNet Technologieseminar 17. Juni 2005

**PostFinance** Alles rund ums Geld.  
Jugend | Auszubildende | Privatkunden | Geschäftskunden | Vereine

E-Banking  
E-Trading  
Events  
Dossiers  
Wir über uns

Suche  OK

### Vorsicht! Gefälschte E-Mails mit Absender PostFinance

In der Nacht auf Sonntag 5. Juni 2005 sind E-Mails mit gefälschten Absenderadressen und dem möglichen Betreff "PostFinance Member", "PostFinance Security Information" oder "PostFinance Online Service" in Umlauf gesetzt worden.



Wer im E-Mail auf den gefälschten Link klickt, wird auf eine Internetseite gelenkt, welche den Originalseiten sehr stark gleicht. Vorsicht! In einem gefälschten Popup werden die Kunden aufgefordert, ihre Sicherheitsnummern einzugeben. Geben Sie keine Daten ein!

**PostFinance wird Sie niemals mittels E-Mail zur Bekanntgabe Ihres Passwortes oder Ihrer Sicherheitsnummern auffordern. Weder PostFinance noch yellownet verwenden "Login-Halls".**

Tippen Sie für das Login die Internetadresse [www.postfinance.ch](http://www.postfinance.ch) ein und benutzen Sie die dort vorhandenen Links.

**Antworten Sie nie auf E-Mails mit der Aufforderung zur Bekanntgabe Ihres Passwortes oder Ihrer Sicherheitsnummern und klicken Sie nie auf dort vorhandene Links.**

Sollten Sie aufgrund solcher E-Mails bereits vertrauliche Daten weitergegeben haben, bitten wir Sie, sich **sofort** mit unserer Hotline in Verbindung zu setzen.

Hotline yellownet:  
0048 888 488 (Normaltarif)  
E-Mail: [yellownet@postfinance.ch](mailto:yellownet@postfinance.ch)



## Aktuelle Sicherheits-Vorfälle II

KeyNet Technologieseminar 17. Juni 2005

**„R b o t“ in der Migros: Schadenssumme unklar**

Der Computerwurm „R b o t“ legte im Migros-Hochhaus am Zürcher Limmatplatz rund **2000 PCs** lahm. Der Wurm hatte jegliche E-Mail-Kommunikation verunmöglicht und deshalb gingen viele Angestellte wegen der Computerpanne nach Hause.

Die Migros-Mitarbeitenden erfuhren über die hausinterne Lautsprecheranlage vom unangenehmen Besucher.

„R b o t“ ermöglicht Dritten den Zugriff auf den Computer, unter Umständen kann der Wurm auch Dateien verändern oder gar löschen. **Nach 35 Stunden** intensivster Arbeit gelang es die ersten Computer wieder in Betrieb zu nehmen. Über die Schadenssumme liegen bisher keine genauen Zahlen vor.

Quelle: ComputerWorld 9.3.2005

**Daten gekidnappt**

Ein neuartiger Trojaner schleicht sich auf PCs und verschlüsselt dort Daten. Will der User die Daten wieder entschlüsseln, wird er mittels einem Text-File aufgefordert, für das Passwort 200 Dollar Lösegeld bezahlen. Der Schädling verbreitet sich via Mail und über manipulierte Sites, die Verbreitung ist noch gering.

Quelle: InfoWeek 30.5.2005

**IBM-Lenovo-Deal in Gefahr**

Der Verkauf von IBMs PC-Bereich an Lenovo könnte unter Umständen platzen. Dies, da bei den US-Behörden Bedenken wegen der Gefährdung der nationalen Sicherheit bestehen. So fürchtet man, dass Angestellte von Lenovo in den US-amerikanischen IBM-Fabriken zur Industriespionage eingesetzt werden und geheime Informationen über Aufträge der US-Regierung in Erfahrung bringen könnten.

Quelle: InfoWeek 7.2.2005

Wolfgang Sidler - www.sidler.ws      Sicherheitshandbuch für die Praxis www.sihb.ch      Seite 9 von 29

## Aktuelle Sicherheits-Vorfälle III

KeyNet Technologieseminar 17. Juni 2005

**Festplatte mit geheimen Polizeidaten versteigert**

Eine Computer-Festplatte mit geheimen Daten der brandenburgischen Polizei ist laut Nachrichtenmagazin "Spiegel" über das **Internet-Auktionshaus ebay** versteigert worden. Ein Potsdamer Student habe die Festplatte, ohne etwas über den brisanten Inhalt zu wissen, Anfang März für knapp 20 Euro erworben, schreibt das Blatt in seiner neuesten Ausgabe. Die Sprecherin des Potsdamer Innenministeriums, Dorothee Stacke, bestätigte den Bericht am Samstag zunächst nicht.

Minister Jörg Schönbohm (CDU) habe aber umgehend eine Überprüfung veranlasst, inwieweit hier möglicherweise ein Versagen von Fremdfirmen vorliege oder kriminelle Energie im Spiel sei, sagte Stacke der Nachrichtenagentur dpa. Der gebrauchte Datenträger mit 20 Gigabyte Speicher enthält laut "Spiegel" **interne Alarmpläne für "besondere Lagen" wie Geiselnahmen oder Entführungen, Namenslisten für die Besetzung von Krisenstäben, Einsatzbefehle und -analysen sowie so genannte Landeslagebilder, in denen die sicherheitspolitische Situation dargestellt wird.**

Solche Landeslagebilder seien als "Verschlussache - Nur für den Dienstgebrauch" deklariert und stünden normalerweise nur der Spitze des Landeskriminalamtes, der Polizeiführung und dem Stab um Innenminister Schönbohm zur Verfügung. **Bis Ende 2004 seien nicht mehr gebrauchte Festplatten des Innenressorts zerschreddert worden, erläuterte Ministeriumssprecherin Stacke. Seit Anfang dieses Jahres würden die Datenträger nach einem lizenziertem Verfahren des Bundesamtes für Sicherheit in der Datenverarbeitung durch Fremdfirmen "irreparabel gelöscht".** (dpa)

Quelle: c't Heise 2. April 2005

Wolfgang Sidler - www.sidler.ws      Sicherheitshandbuch für die Praxis www.sihb.ch      Seite 10 von 29

## Aktuelle Sicherheits-Vorfälle IV

KeyNet Technologieseminar 17. Juni 2005




### Organisierte Kriminalität

#### Vergleich von Verbrechen in der realen Welt und im Internet

Ständliche Online-Verbrechen dieser Debatte stellen den organisierten Kriminalität eine Herausforderung dar.

- Die Kriminalität im Internet ist nicht in Einklang mit der realen Welt zu bringen, um das Verbrechen bekämpfen zu können.
- Die Verbrechen können noch über Ländergrenzen hinweg begangen werden, in dem Internet ist weltweit ohne Grenzen als Verbrechen in Deutschland, Italien, Spanien oder in anderen Ländern begangen.
- Mittele von Computern können die Verbrechen aufbewahrt, sich leichter verbreiten und sind schwerer zu verfolgen. Die Ermittlung und Verfolgung werden dadurch erschwert.

#### Bankrott

Bankrott ist ein Verbrechen. Ein Bankrott ist ein Verbrechen, das durch einen Zahlungsstopp...

#### Bankrott

Bankrott ist ein Verbrechen. Ein Bankrott ist ein Verbrechen, das durch einen Zahlungsstopp...

#### Bankrott

Bankrott ist ein Verbrechen. Ein Bankrott ist ein Verbrechen, das durch einen Zahlungsstopp...

#### Bankrott

Bankrott ist ein Verbrechen. Ein Bankrott ist ein Verbrechen, das durch einen Zahlungsstopp...

#### Bankrott

Bankrott ist ein Verbrechen. Ein Bankrott ist ein Verbrechen, das durch einen Zahlungsstopp...

#### Bankrott

Bankrott ist ein Verbrechen. Ein Bankrott ist ein Verbrechen, das durch einen Zahlungsstopp...


Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)

Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)

Seite 11 von 29

## Das Risiko

KeyNet Technologieseminar 17. Juni 2005



### Was ist ein Risiko?

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

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)

Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)

Seite 12 von 29

## Das Risiko I

KeyNet Technologieseminar 17. Juni 2005



### Abstrakte versus konkrete Risiken



Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 13 von 29

## Die Risiko II

KeyNet Technologieseminar 17. Juni 2005



### Abstrakte versus konkrete Risiken



Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 14 von 29

### Die Risiko III

KeyNet Technologieseminar 17. Juni 2005

## Umgang mit Risiken

Sicherheitsdispositiv

Gesamtrisiko

laufende Überprüfung

The diagram illustrates a risk management process. It starts with 'Gesamtrisiko' (Total Risk) and branches into four strategies: 'vermeiden' (avoid), 'vermindern' (reduce), 'überwälzen' (transfer), and 'selbst tragen' (self-insure). 'vermeiden' includes 'Gebäude', 'Zutrittskontrollen', 'Redundanzen', 'Personal', and 'Gewaltentrennung'. 'vermindern' includes 'Krisenstäbe', 'Katastrophenplanung', 'Ausbildung', and 'Training'. 'überwälzen' includes 'Versicherung'. 'selbst tragen' includes 'Restrisiko'. A 'Sicherheitsdispositiv' (Safety Device) is shown as a large grey arrow pointing towards the strategies. A 'laufende Überprüfung' (ongoing review) arrow points back to the 'Gesamtrisiko'.

- vermeiden
  - Gebäude
  - Zutrittskontrollen
  - Redundanzen
  - Personal
  - Gewaltentrennung
- vermindern
  - Krisenstäbe
  - Katastrophenplanung
  - Ausbildung
  - Training
- überwälzen
  - Versicherung
- selbst tragen
  - Restrisiko

Wolfgang Sidler - www.sidler.ws      Sicherheitshandbuch für die Praxis www.sihb.ch      Seite 15 von 29

### Business-Prozesse

KeyNet Technologieseminar 17. Juni 2005

## Abhängigkeiten „Business – IT“

The diagram shows the dependencies between Business and IT. A green arrow labeled 'Geschäftsprozess' (Business Process) points to a cylinder labeled 'Daten / Information' (Data / Information). From 'Daten / Information', a blue arrow points to a yellow trapezoid labeled 'Applikation' (Application), which then points to a red cube labeled 'System'. To the left, a blue box labeled 'Sicherheits-Anforderungen' (Security Requirements) with a cyan triangle labeled 'GL' above it, points to the 'Applikation'. The requirements listed are 'Vertraulichkeit' (Confidentiality), 'Verfügbarkeit' (Availability), and 'Integrität' (Integrity). To the right, a yellow arrow labeled 'Vorbereitung' (Preparation) points downwards.

Wolfgang Sidler - www.sidler.ws      Sicherheitshandbuch für die Praxis www.sihb.ch      Seite 16 von 29



## Business-Prozesse I

KeyNet Technologieseminar 17. Juni 2005

### Vom OLD Business zum NEW Business Modell

**Old Business Modell**

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

**New Business Modell**

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

**Risiken**  
Erhöhte Anforderungen an Anwendungen, Verfügbarkeit & Sicherheit

Wolfgang Sidler - www.sidler.ws      Sicherheitshandbuch für die Praxis www.sihb.ch      Seite 17 von 29

## IT-Sicherheit

KeyNet Technologieseminar 17. Juni 2005

### Aufgaben der IT-Sicherheit „Die 4 Pfeiler“



```

graph TD
    A[IT-Sicherheit] --> B[Schutz der Vertraulichkeit]
    A --> C[Schutz der Integrität]
    A --> D[Schutz der Verfügbarkeit]
    A --> E[Schutz der Verbindlichkeit]
    B --- B1[Informationen sollen nur an befugte Personen gelangen]
    C --- C1[Unversehrtheit und Korrektheit der Daten]
    D --- D1[Daten zur rechten Zeit am rechten Ort]
    E --- E1[Der Empfänger hat nachweisbar eine Nachricht erhalten]
    
```

Wolfgang Sidler - www.sidler.ws      Sicherheitshandbuch für die Praxis www.sihb.ch      Seite 18 von 29

## IT-Sicherheit I

KeyNet Technologieseminar 17. Juni 2005





### Die Hauptziele einer Sicherheits-Strategie (Organisation)

- ▶ **Sicherung der Geschäfts-Prozesse** (BCM und DR)
- ▶ **Einhaltung der Gesetze und Verordnungen** (Basel II, SOX, GebäV)
- ▶ **Das Unternehmen und deren Management vor Haftungsklagen schützen**
- ▶ **Daten-Missbrauch und –Diebstahl erkennen und verhindern**

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 19 von 29

## IT-Sicherheits-Prozess I

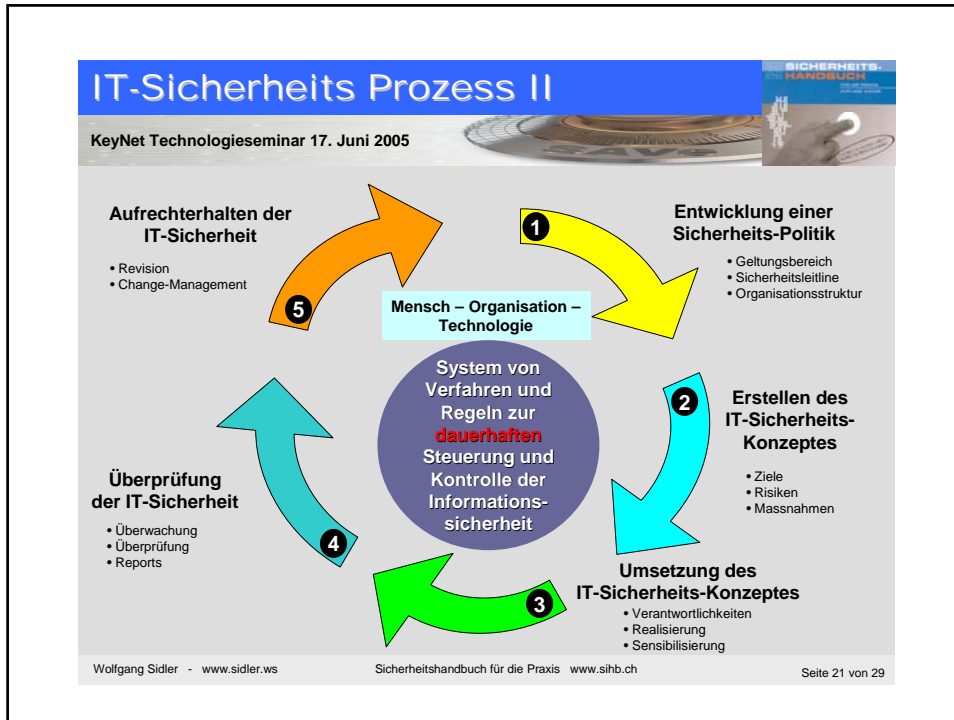
KeyNet Technologieseminar 17. Juni 2005



### 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 delegiert werden!)**
- ▶ **Effektives „Marketing“ der IT-Sicherheit innerhalb der Firma „Sicherheitsbewusstsein – Kultur“**
- ▶ **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](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 20 von 29



### Die Lösung I

KeyNet Technologieseminar 17. Juni 2005

**Information Security  
ist nur 20% Technologie!!!**

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 22 von 29

## Die Lösung II

KeyNet Technologieseminar 17. Juni 2005

### Die goldenen Sicherheits-Grundregeln

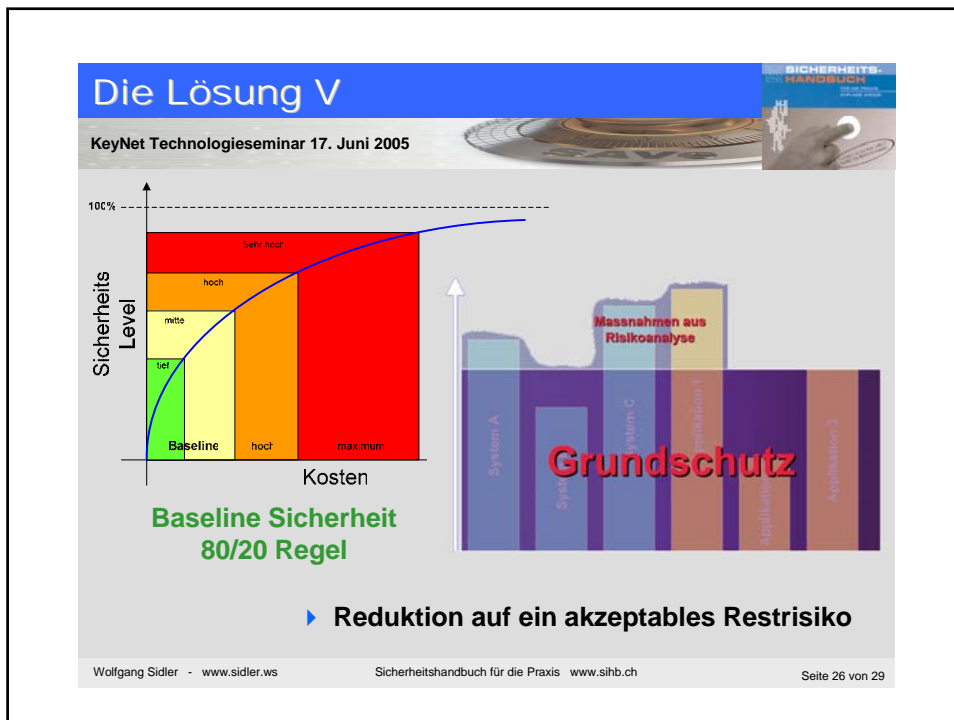
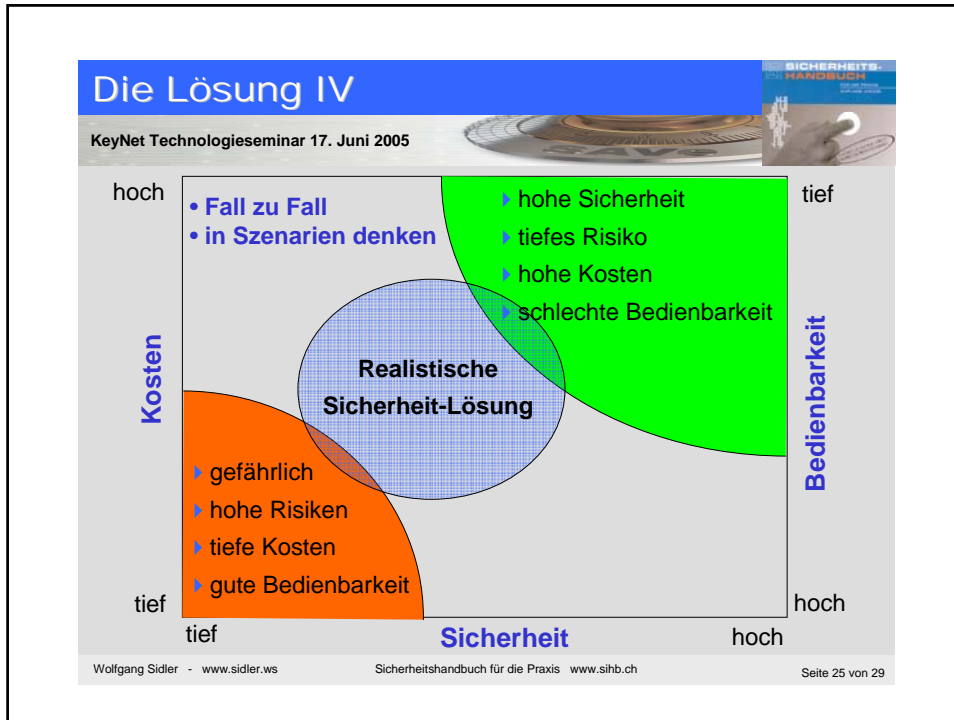
- ▶ Backup
- ▶ Passwörter und deren Umgang (2 Factor Authentication)
- ▶ Richtlinien und Sensibilisierung (Sicherheitspolitik)
- ▶ Schutz vor Viren / Malware
- ▶ Sichere Internet Anbindung (Firewall, IDS/IPS, URL-Filter, Spam-Filter etc.)
- ▶ Software aktualisieren (Change-Management)
- ▶ Sicherer Umgang mit Notebooks, PDA, Smartphone, Memory Stick
- ▶ Sichere Wireless Lösung
- ▶ Clear Desk Policy (alles unter Verschluss!)
- ▶ Physische Sicherheit, Arbeitsplatzsicherheit (EKAS)
- ▶ Notfallplanung / Disaster Recovery
- ▶ Archivierung
- ▶ Einhaltung der Gesetze und Verordnungen
- ▶ Geschäftsprozesse und deren Abhängigkeiten kennen (Risiko-Analyse)
- ▶ Sicherheit ist Chef-Sache, eine Management-Aufgabe
- ▶ Sicherheit muss gelebt werden

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 23 von 29

## Die Lösung III

KeyNet Technologieseminar 17. Juni 2005

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 24 von 29



**Nutzen**

KeyNet Technologieseminar 17. Juni 2005

**Was für einen Nutzen erhalten Sie?**

- ▶ Positive Audits (interne und externe Revision)
- ▶ Bessere Kreditwürdigkeit
- ▶ Kundenvertrauen, Zertifizierung, erhöhte Kunden-Privacy
- ▶ 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

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 27 von 29

**Das Sicherheitshandbuch für die Praxis**

KeyNet Technologieseminar 17. Juni 2005

**Das neue Standardwerk der IT-Sicherheit**

Umfang:	A4-Ordner mit 337 Seiten
Auflage:	Version 4
ISBN:	3-9521208-3-9
Preis:	CHF 248.-
Bestellung unter:	<a href="http://www.sihb.ch">www.sihb.ch</a>




Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 28 von 29

Fragen

KeyNet Technologieseminar 17. Juni 2005

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



Carl G. Jung

Wolfgang Sidler - [www.sidler.ws](http://www.sidler.ws)      Sicherheitshandbuch für die Praxis [www.sihb.ch](http://www.sihb.ch)      Seite 29 von 29