IT-SECURITY - Forum #2

Erfolgreiche Umsetzung von IT-Sicherheit

Reto C. Zbinden

Swiss Infosec AG

reto.zbinden@infosec.ch

IT-SECURITY - Forum #2

Übersicht

- Einführung, Definition, Begriffe
- Gesetzliche Anforderungen
- Methoden zur Umsetzung im Unternehmen
- Elemente der Umsetzung / Best Practice
- Tipps
- Fragen zum Vortrag

Warum Aktivitäten in Informationssicherheit?

Bekannte Vorurteile:

- „Es trifft immer nur die Anderen“
- „Es passiert sowieso nichts“
- „Ist viel zu teuer“/ „Bringt nichts ein“

Aber:

- Bekannte Fälle nur die Spitze des Eisbergs
- Einschneidende Schäden oder Beinaheschäden
- Aus Schaden klug werden, kann zu spät sein

IT-SECURITY - Forum #2

Warum Aktivitäten in Informationssicherheit?

Gesetzliche Anforderungen

- Datenschutzgesetz
- Geschäftsbücherverordnung
- Urheberrechte
  - z.B Software-Lizenzen
- Individuelle Geheimhaltungspflichten
  - Arztgeheimnis
  - Fernmeldegeheimnis
  - Bankgeheimnis
- Für Banken: Bestimmungen der Eidg. Bankenkommission (EBK)
  - z.B. Rundschreiben: Outsourcing

Warum Aktivitäten in Informationssicherheit: Basel II

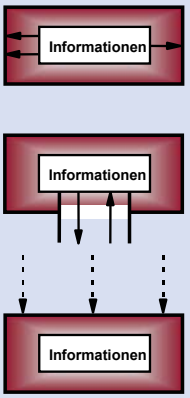
- Basler Ausschuss für Bankenaufsicht
  - 16. Januar 2001: Konsultationspapier
  - Basler Eigenkapitalvereinbarung (Basel II)
  - Endgültige Fassung: Ende 2003, 2006 in Kraft
- Neue Ansätze zur Messung des
  - Kreditrisikos und operationellen Risikos
- Operationelle Risiken
  - „die Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignissen eintreten„
- Hauptursachen
  - Unzureichende Systeme und Kontrollen
  - Komplexe IT-Projekte

Informationssicherheit Definition

- Angemessenes und dauerndes Gewährleisten von:
  - Verfügbarkeit
  - Vertraulichkeit
  - Integrität
- Schutz sämtlicher Informationen ungeachtet:
  - Art ihrer Darstellung
  - Art ihrer Speicherung

Informations- und IT-Sicherheit Definition

- Information
  Zweckbezogenes Wissen, das man beim Handeln in Hinblick auf gesetzte Ziele benötigt
- Vertraulichkeit
  Confidentiality
- Verfügbarkeit
  Availability
- Integrität
  Integrity



Abgrenzung der Begriffe

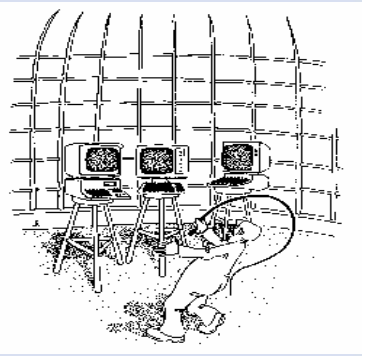
- Informationssicherheit befasst sich mit allen Informationen
- Informatiksicherheit (IT Security) befasst sich mit elektronisch gespeicherten Informationen
- Integrale Sicherheit umfasst alle Aspekte der Sicherheit in einer Unternehmung

IT-SECURITY - Forum #2

Integrale Sicherheit Beschreibung

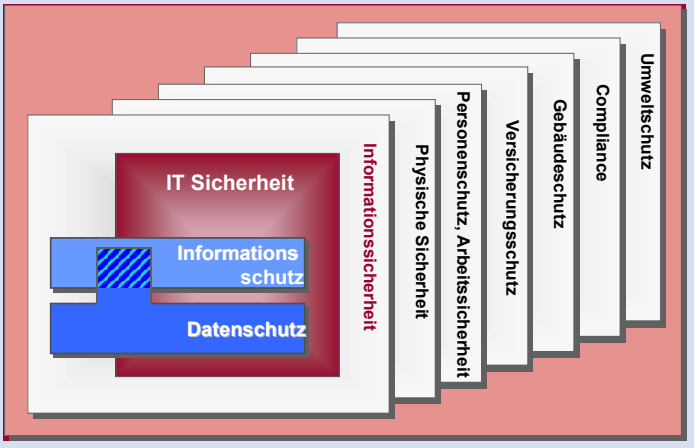
Ein Unternehmen begegnet dem gesamten Bereich Sicherheit konsequent, umfassend, abgestimmt, geplant und effizient in ethisch, wirtschaftlich und rechtlich vertretbarem Rahmen unter Ausnützung bestehender Synergien.

Ziel aller Aktivitäten im Bereich Sicherheit ist es, schädigende Ereignisse für das Unternehmen, seine Mitarbeiter und Partner in Häufigkeit und Auswirkung auf ein Minimum zu reduzieren.



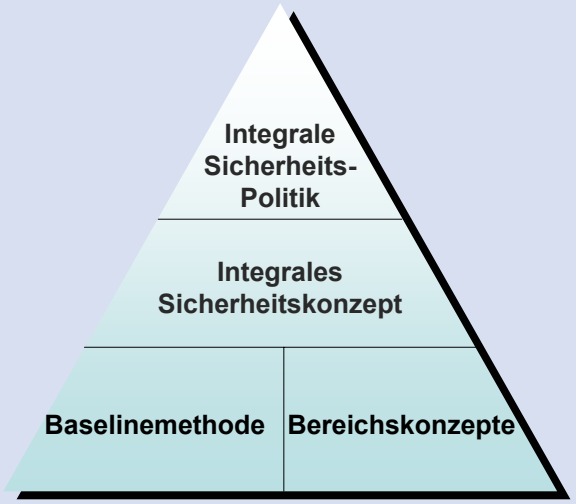
IT-SECURITY - Forum #2

Informationssicherheit als Teil der Integralen Sicherheit



IT-SECURITY - Forum #2

Hierarchie der Dokumente



IT-SECURITY - Forum #2

Sicherheitspolitik

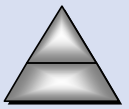
Ziel

- schafft Grundlage auf strategischer Ebene
- legt Grundsätze fest
- bestimmt übergeordnete Sicherheitsziele
- benennt wichtige Sicherheitsfunktionen

Sicherheitspolitik
Grundlagen für alle Massnahmen und Aktivitäten zur Erreichung einer optimalen Sicherheit

IT-SECURITY - Forum #2

Sicherheitskonzept



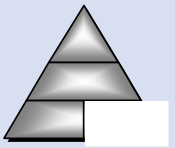
Ziel

- nennt die Ziele in der Informationssicherheit
- legt die nötigen Strategien und Organisationsstrukturen zur Erreichung dieser Ziele fest
- definiert die Funktionen auf operativer Ebene
- legt die Sicherheitsstufen (Klassifizierungen) von Informationen fest

Sicherheitskonzept
Rahmenbedingungen für Sicherheit und notwendige Entscheidungsprozesse

IT-SECURITY - Forum #2

Regelwerk

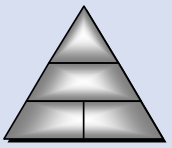


Ziel

- sorgt für einen Grundschutz in der Unternehmung
- enthält generelle und spezielle Massnahmen
  - generell: für alle Schutzobjekte gültig
  - speziell: nur für Schutzobjekte mit höherem Schutzbedarf (klassifizierte Objekte) gültig
- zu jeder Massnahme sind die Zuständigkeiten definiert

Regelwerk
Konkrete Ausformulierung der einzelnen Massnahmen

Bereichskonzepte



Ziel

- Ausführung der Anforderungen in einzelnen wichtigen Themenbereichen
- Beispiele:
  - Zugriffsschutz
  - Datensicherung
  - Datenschutz
  - Notfallvorsorge

Bereichskonzepte
Weiterführende Anforderungen in spezifischen Themenbereichen

Code of Practice Information Security Management

- **ISO/IEC 17799 (BS 7799-1)**
  - International anerkannter Leitfaden für Management der Informationssicherheit
  - umfassende Sammlung von Verfahren („best practices“) der Informationssicherheit
  - Basis für Entwicklung organisationsbezogener Sicherheitsnormen und effektiver Managementpraktiken
- **BS 7799-2**
  - Spezifikation für einzelne Anforderungen zur Definition, Implementierung und Dokumentation eines Informationssicherheits-Managementsystems
  - Grundlage für die Bewertung des Systems.

- Erstmals 1995 durch BSI UK veröffentlicht (BS 7799)
- Neuauflage 1999 durch BSI UK
- Übernahme als ISO 17799 im Jahre 2000 (nur Teil 1)

IT-Grundschutzhandbuch

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Ziel: „geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmassnahmen um ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann“
- Hilfsmittel für die Erstellung von Sicherheitskonzepten für IT-Systeme
- Massnahmenempfehlungen für mittleren Schutzbedarf
- Aufwändige komplexe Analysen von Bedrohungen und Eintrittswahrscheinlichkeiten entfallen
- Lediglich Abgleich von Massnahmen-Soll mit Massnahmen-Ist

Cobit: Control Objectives for Information and related Technology

- Version 3, 2000
- ISACA: Information Systems Audit and Control Association seit 1993
- IT-Prozess
  - Unterstützte Geschäftsziele
  - Kontrollziele (sieben Geschäftsanforderungen)
- Geschäftsanforderungen
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit,
  - Effektivität (Wirksamkeit)
  - Effizienz (Wirtschaftlichkeit)
  - Compliance (Einhaltung rechtlicher Erfordernisse)
  - Zuverlässigkeit (Ordnungsmässigkeit der Berichterstattung).

Best Practices

- Best Practices
  - Weshalb eigentlich?
- Customizing sehr wichtig
  - Lösungen sind sehr individuell
  - Anforderungen sind sehr unterschiedlich
- Was, aber nicht das Wie
  - Wie: Unzahl de facto-Standards/Muster
- Customizing des Was
  - Individuelle Zielsetzungen, Prioritäten
  - Individuelle Fassung/Konkretisierung
- Zertifizierung
  - Aussagekraft (ISO 9000)
  - Materielle (!) Aussagen zur Sicherheit

Organisation

- Delegierter für Sicherheit
  - Mitglied der Geschäftsleitung
- Fachgremium
  - Fachbeauftragte der Sicherheitsteilbereiche
- Fachbeauftragter für Informationssicherheit (Information Security Officer, ISO)
  - unabhängige Stabsstelle
  - Wenn möglich: kein MA der IT-Abteilung
  - Aufgaben
    - Beratung der Geschäftsleitung in Fachfragen
    - Entwicklung von Vorgehensplänen
    - Anlaufstelle für alle Mitarbeitenden

Awareness

Faktor Mensch ist entscheidend:

- Risikobewusstsein der Mitarbeiter
- Hauptursachen für Schäden im IT-Bereich
  - Nachlässigkeit
  - unzureichende Akzeptanz von Sicherheits-massnahmen
  - mangelnde Kenntnisse
- Mitarbeiter müssen Sinn in Massnahmen erkennen
  - Schulungen, Workshops
  - Erinnerungsmassnahmen: Merkblätter usw.
  - klare, verständliche Regeln

Praktische Hinweise

- Sicherheitskonzepte schrittweise einführen
- realistische Fallbeispiele vorstellen
- Bekenntnis des Managements zur Sicherheit
- Verbesserungen, nicht Fehler betonen
- Regelverstösse thematisieren
- glaubhaftes GL-Mitglied als Mentor
- Mit Angst vorsichtig umgehen
- wiederholt an zentrale Sicherheitsziele erinnern
- Sicherheitsaufgaben dezentralisieren
- Mitarbeiter respektieren und einbeziehen

Vorgehen im Unternehmen Organisation/Konzeption

- Entwickeln Sie eine Strategie
- Setzen Sie diese Strategie um
  - Formulieren Sie eine Politik/Konzept
  - Erarbeiten Sie Minimal-Anforderungen
  - Erarbeiten Sie in wichtigen Bereichen eigentliche Konzepte (Zugriffschutz, Datensicherung)
- Definieren Sie zusätzliche Massnahmen
- Wählen Sie wo nötig Produkte aus
- Sensibilisieren Sie Ihre Mitarbeiter