

Aufbau eines Sicherheitskonzeptes

Felix Widmer
TCG Tan Consulting Group GmbH
Hanflaenderstrasse 3
CH-8640 Rapperswil SG

Voice +41 (0)55 214 41 56
Fax +41 (0)55 214 41 57
Mobile +41 (0)79 336 56 76
E-Mail felix.widmer@tan-group.ch
Web www.tan-group.ch

Aufbau eines Sicherheitskonzeptes

- **Code of Practice for Information Security Management**
 - **Britischer Sicherheitsstandard (BS7799).**
 - **In Europa anerkannt.**
 - **Allgemein anerkannte Sicherheitsanforderungen.**
 - **Soll als ISO-Norm festgelegt werden.**
 - **Zielorientiert.**
 - **Geeignet für den konzeptionellen Rahmen.**

- **IT-Grundschutzhandbuch BSI**
 - **Umsetzungshilfe auf der Ausführungsebene.**
 - **Allgemein anerkannte Sicherheitsmassnahmen.**



Code of Practice: Überblick

Sicherheitspolitik

Rechner- und Netzverwaltung

Sicherheitsorganisation

Systemzugriffskontrolle

Inventar & Klassifikation

Systementwicklung & -wartung

Personelle Sicherheit

Geschäftskontinuitätsplanung

Physische Sicherheit

Erfüllung der Verpflichtungen



Sicherheitspolitik

o Ziel

- Richtungsweisung und Unterstützung durch das Management für die Informationssicherheit.
- Die Geschäftsführung muss mit einem **Sicherheitsleitbild** eine klare Richtung setzen.

o Inhalt

- Sicherheitsleitbild.

Sicherheitsorganisation

o Ziel

- Management von Informationssicherheit innerhalb des Unternehmens.
- Benennen der verantwortlichen Stellen und Gremien.
- Fördern der interdisziplinären Vorgehensweise (-> integrale Sicherheit).

o Inhalt

- Management-Forum für Informationssicherheit.
- Koordination der Informationssicherheit.
- Zuordnung der Verantwortlichkeiten.
- Genehmigungsprozess für Informatikmittel.



Inventar & Klassifikation

o Ziel

- Aufbauen und Erhalten geeigneter Schutzvorrichtungen für die IT-Systeme und Daten.
- Jedes IT-System und jeder Datenbestand hat einen „Eigentümer“.

o Inhalt

- Inventar der Anlagen und Bestände.
- Klassifizierung der Informationen (-> Schutzbedarf).

Personelle Sicherheit

o Ziel

- Reduzieren der Risiken durch menschlichen Irrtum, Diebstahl, Betrug oder Missbrauch der IT-Einrichtungen.
- Angemessene Ausbildung der Mitarbeiter im Gebrauch der IT-Systeme unter Berücksichtigung der Sicherheitsanforderungen.

o Inhalt

- Sicherheit bei der Personalanstellung / -freistellung.
- Stellenbeschreibungen / Pflichtenhefte.
- Vertraulichkeitsvereinbarung.
- Verhalten bei Sicherheitsvorfällen.
- Disziplinarprozess.



Physische Sicherheit

o Ziel

- Schützen der IT-Ressourcen und Informationen vor Umwelteinflüssen.
- Schützen der IT-Ressourcen und Informationen vor Zerstörungen und gegen Diebstahl.

o Inhalt

- Physische Sicherheitszonen & Zutrittskontrollen.
- Clear desk and clear screen policy.
- Brandschutz.
- Verkabelung.
- Entsorgung.

Rechner- & Netzverwaltung

o Ziel

- Gewährleisten des korrekten und sicheren Betriebs von Rechner- und Netzeinrichtungen.
- Einschränken des Risikos von Systemausfällen durch Vorausplanung der notwendigen Kapazitäten.

o Inhalt

- Dokumentierte Betriebsverfahren.
- Pflichten- / Funktionentrennung.
- Trennung von Entwicklungs- und Betriebsanlagen.
- Ressourcenplanung.
- Sicherheitskontrollen für Netze.



Systemzugriffskontrolle

o Ziel

- Verhindern unberechtigter Zugriffe auf Systeme und Informationen.
- Einschränken der Zugriffe auf die Geschäftsanforderungen.

o Inhalt

- Dokumentierte Vorschriften für die Zugriffskontrolle.
- Verwaltung der Benutzer Accounts.
- Berechtigungsprüfungen im Netz.
- Isolierung sensibler Systeme.
- Überwachung der Systemzugriffe und Systemnutzung.



Systementwicklung & -wartung

o Ziel

- Rechtzeitige Ermittlung der Sicherheitsanforderungen bei der Entwicklung / Beschaffung neuer Systeme.
- Verhindern von Verlust oder Missbrauch von Benutzerdaten in Anwendungssystemen.

o Inhalt

- Sicherheit in Anwendungssystemen.
- Kontrolle von in Betrieb befindlicher Software.
- Änderungsüberwachungsverfahren.
- Technische Revision von Betriebssystemänderungen.



Geschäftskontinuitätsplanung

o Ziel

- Aufrechterhalten der kritischen Geschäftsprozesse.
- Schaden verhindern, begrenzen, beseitigen.

o Inhalt

- Planungsprozess.
- Schutzbedarfsfeststellung.
- Notfallhandbuch.
- Notfalltests und Aktualisierung.



Erfüllung der Verpflichtungen

o Ziel

- Einhalten jeglicher Gesetze und Regelungen.
- Regelmässige Überprüfung der Sicherheit.

o Inhalt

- Lizenzenkontrolle.
- Datenschutz.
- Sicherheitsüberprüfungen.
- Systemrevisionen.