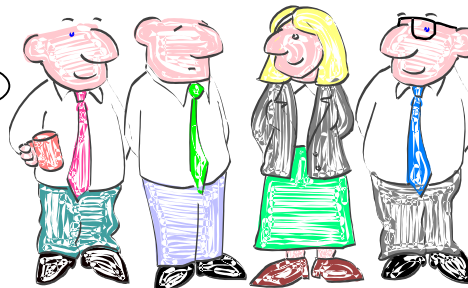


# Quality Point München

## Sicherheit als Qualitätsaspekt



Paul,  
was hat denn  
Sicherheit mit Qualität  
zu tun ?



Nun, ohne Sicherheit kann  
jeder Deine Qualität in Schrott  
verwandeln.

## Qualitätsmerkmal ‚Sicherheit‘ (1)

- **Sicherheit** = Grad, in dem ein Softwaresystem sich vor äußeren und inneren Störungen schützt -> unterteilt in Datenintegrität und Funktionsintegrität
  - **Datenintegrität** = Abwehr aller falschen Eingaben (falsche Eingaben müssten vom System erkannt und abgelehnt werden)
  - **Funktionsintegrität** = Kontrolle aller Funktionsausführungen (eine kontrollierte Funktion ist eine, deren Ergebnisse vom System geprüft werden; falls sich eine Funktion als fehlerhaft erweist, so müsste sich das System vor der Funktion schützen, in dem es die Ergebnisse der Funktion annulliert und die Funktion ausschaltet)

siehe ‚Softwarequalität‘ von H.M.Sneed 1990

## Qualitätsmerkmal ‚Sicherheit‘ (2)

- **Sicherheit** = Abfragen und Ändern von Daten wird ausschließlich durch berechtigte Personen vorgenommen

siehe ‚Management und Optimierung des Testprozesses‘ von Pol, Koonen,  
Spillner 2000

## Qualitätsmerkmal ‚Sicherheit‘ (3)

- **Sicherheit** = Merkmale von Software, die sich auf ihre Eignung beziehen, unberechtigten Zugriff sowohl versehentlich als auch vorsätzlich, auf Programme und Daten zu verhindern

siehe ‚ISO 9126 Qualitätsmerkmale‘

## Qualitätsmerkmal ‚Sicherheit‘ (4)

- **Sicherheit** = ein System ist sicher, wenn es **verlässlich** und **beherrschbar** ist, d.h. Sicherheit hat technische, juristische und organisatorische Komponenten

siehe ‚Sicherheit für Systeme und Netze in Unternehmen‘ von BITKOM 2002

## Qualitätsmerkmal ‚Sicherheit‘ (4-1)

- spezifische Eigenschaften eines **verlässlichen** Systems:
  - **Vertraulichkeit** = Informationen werden vor dem Zugriff vor Dritten geschützt (Zugriff nur für befugte Personen oder Dienste)
  - **Integrität** = Informationen, Systeme und Netze können nicht unbemerkt verändert werden (Veränderung wird offensichtlich)
  - **Verfügbarkeit** = Informationen, Systeme und Netze sind verfügbar, d.h. das System muss bei einem Zugriff in einem definierten Zeitraum antworten bzw. bestimmte Aktionen auslösen

## Qualitätsmerkmal ‚Sicherheit‘ (4-2)

- spezifische Eigenschaften eines **beherrschbaren** Systems:
  - **Authentizität** = Die Identität von Informationen, Systemen, Netzen oder Personen kann zweifelsfrei nachgewiesen werden. Im Sonderfall Pseudonymität und Anonymität = z.B. nur ein Aspekt der Identität (Alter) kann zweifelsfrei nachgewiesen werden bzw. die Identität soll vollständig verborgen bleiben.
  - **Zurechenbarkeit** = Aktion und Informationen können einer auslösenden Instanz (Person oder System) zugerechnet werden. Zurechenbarkeit folgt mitunter aus der Authentizität.
  - **Rechtssicherheit und Revisionsfähigkeit** = Alle für den Rechtsverkehr in Systemen und Netzen verwendeten Informationen und Vorgänge gegenüber Dritten sind beweisbar.
  - **Verbindlichkeit** = abgegebene Willenserklärungen oder Daten in digitaler Form müssen verbindlich sein. Das heißt analog, dass sie vom Sender nicht später abgestritten werden können. Verbindlichkeit ergibt sich aus dem Nachweis der Authentizität, der Zurechenbarkeit und der Integrität von Daten

# Praktikabilität und Relevanz der Definitionen für den konkreten Fall (1)

- Eingrenzen des zu sichernden Objektraums
  - komplette IT-Landschaft der Firma
  - einzelne Anwendungen oder Anwendungsgruppen
  - einzelne Funktionen oder Funktionsgruppen
  - einzelne Daten oder Datenkonglomerate

## Praktikabilität und Relevanz der Definitionen für den konkreten Fall (2)

- Beschreibung der Minimalanforderungen an Sicherheit , z.B.
  - Sicherheit des lesenden und verändernden Zugriffs auf Daten
  - Sicherheit vor Datenverlust und/oder Verfälschung
  - Sicherheit gegen vorsätzliche und unbefugte Veränderung der Anwendungen und sonstigen Programme

## konstruktive Maßnahmen für das Qualitätsmerkmal 'Sicherheit'

- Zugriffsschutz durch zentrales oder anwendungsspezifisches Berechtigungssystem (Passwörter, biometrische Merkmale, Hardwaresicherungen (Dongles, Chipkarten usw.))
- aktive Maßnahmen gegen Datenverlust und/oder Verfälschung wie Protokollierung, Historisierung, Datierung, 4-Augen-Prinzip, Statuskonzepte ,
- Verschlüsselung von ein- und ausgehenden Daten (vor/nach der Anwendung bzw. gespeichert und in der Anwendung), Parametern bei Programm-/Klassen-/Komponenten- und sonstigen Aufrufen, globalen Daten einer Anwendung ,
- Sicherung gegen Codeänderungen und Einbinden fremder Unterprogramme

## statischer Test des Qualitätsmerkmals ‚Sicherheit‘

- anhand einer Checkliste zu folgenden Punkten
  - Verarbeitungsorganisation (u.a. Verarbeitung vertraulicher Daten in gesonderten Verfahren ?)
  - Benutzerorganisation (u.a. Trennung von Funktionen, Befugnissen und Verantwortlichkeiten, need-to-do und need-to-know, Einteilung von Dokumenten in Vertrauensklassen, Vorhandensein von Verfahrensbeschreibungen für Zugriffsschutz)
  - technische Systemarchitektur (u.a. optimale Ausnutzung der Möglichkeiten zur Zugangsbeschränkung, kein Durchbruch des Zugriffsschutzes durch DB-Abfragesprachen, Einschränkungen für Passwortgebrauch)
  - Dateninfrastruktur (u.a. Dateien verschlüsselt, Verschlüsselung von Daten, die über das Netz gehen)
  - Produktionsumgebung (verschiedene Identifizierungen für Produktions- und Entwicklungs- bzw. Testumgebungen)

# dynamischer Test

- intuitiver Test der Zugriffsmöglichkeiten (like a hacker)
- semantischer Test (Testfälle gemäß Sicherheitsanforderungen)
  - Zugriffsmöglichkeiten anhand Anwenderprofilen
  - Überprüfung von Datenverschlüsselungen
  - Überprüfung des Passwortschutzes
  - Überprüfung der Protokollierungen
  - Überprüfung von Datierungen, des Schreibens von Änderungsinformationen usw.
  - Überprüfung der Auswertbarkeit von Protokollierungsinformationen (wer, wie und in welcher Form, Einhaltung Datenschutz usw.)

# Probleme und Konflikte

- Sicherheit versus
  - Handhabbarkeit/Benutzerfreundlichkeit (z.B. bei Verschlüsselung)
  - Performance
  - einfache und vertrauensvolle Kommunikation im Team, in der Firma usw.
  - Kosten von Sicherheitssoftware und sonstigen Maßnahmen
- Tools werden es schon richten
  - Firewall
  - Antivirensoftware
  - Zugriffsrechte
  - Verschlüsselungssoftware
- Sicherheitspolitik und Sicherheitsmanagement sind viel zuviel Bürokratie

## Es gibt mehr Interessenten als man denkt



und mehr Möglichkeiten als die Schulweisheit sich träumen lässt