»|secaron

Software unsicher entwickeln in sieben Schritten

Markus Wutzke, 26.01.2011
wutzke@secaron.de

Vorstellung

Markus Wutzke
Senior Consultant
Secaron AG

- Certified Secure Software Lifecycle Professional (CSSLP^{CM})
- Zertifizierter Auditteamleiter für ISO 27001-Audits auf Basis IT-Grundschutz

Themenfelder

- Aufbau und Auditierung von ISMS nach ISO 27001 bzw. BSI Grundschutz

- Sichere Entwicklungsprozesse

Mein Vortrag – Ihre Möglichkeiten

»|secaron

(ISC)²

Inhalt:
Wie kommt es zu unsicherer Software?
Was kann man dafür/dagegen tun?

Zielpublikum:
IT-Sicherheitsbeauftragte, IT-Leiter, Entwicklungsleiter, Produktverantwortliche, Projektmanager

„Welche Rolle haben Sie?“

Voraussetzungen:
Grundkenntnisse bezüglich der Entwicklung von Software

„Wie läuft das bei Ihnen ab?“

Beteiligen Sie sich!

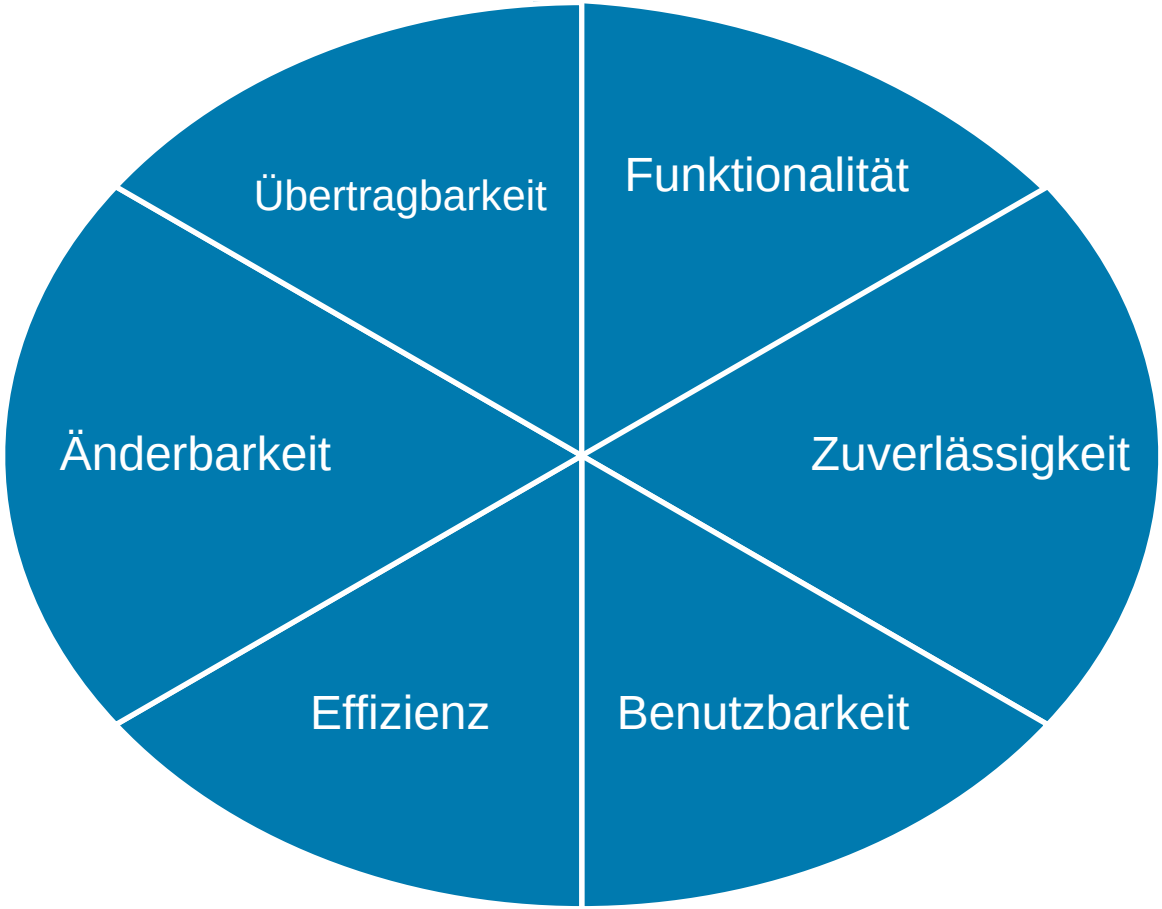
90 Minuten sind lang, wenn nur ich rede ;-)

Sicherheit ist ein Qualitätsmerkmal

»|secaron

(ISC)²®

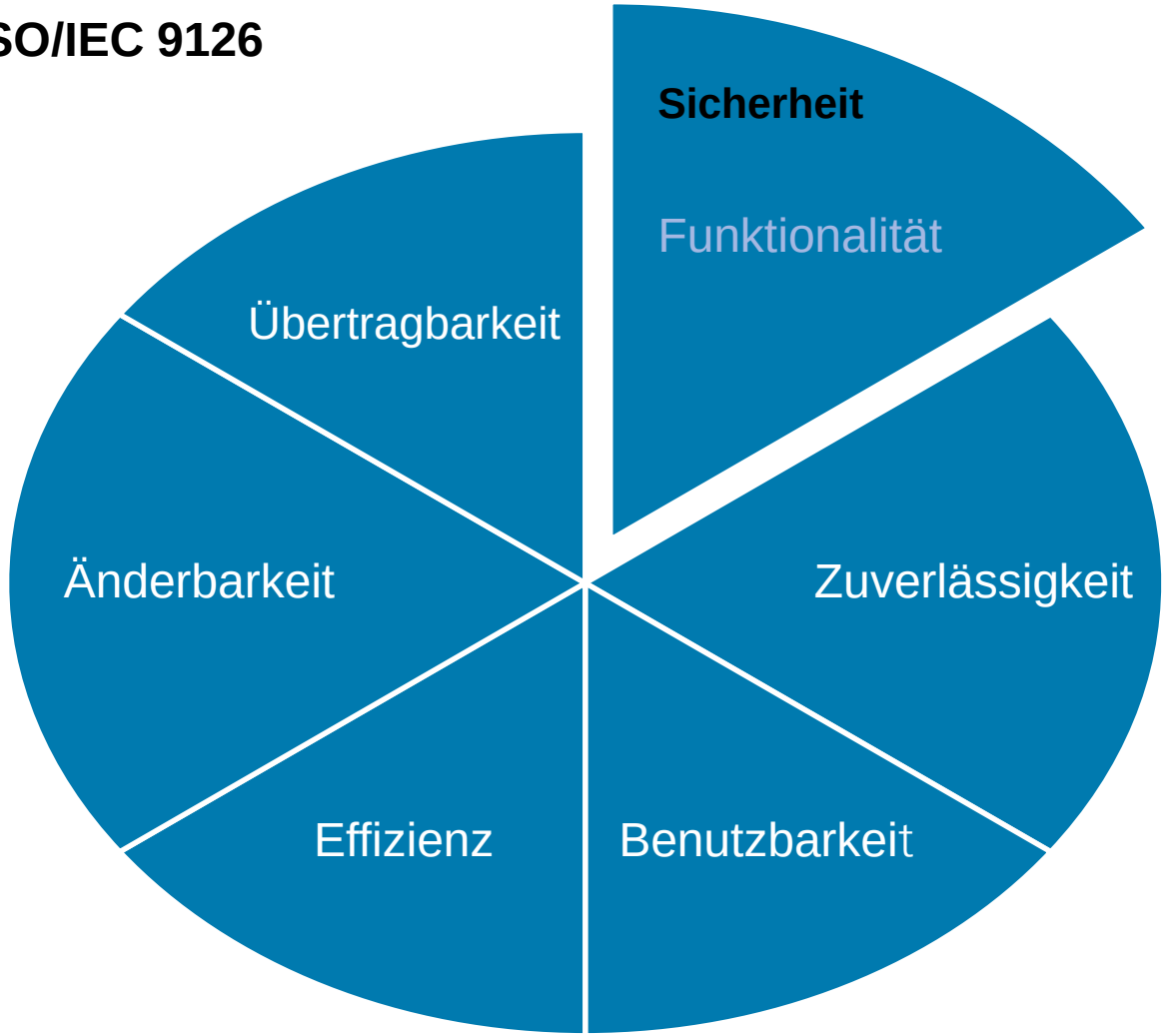
ISO/IEC 9126



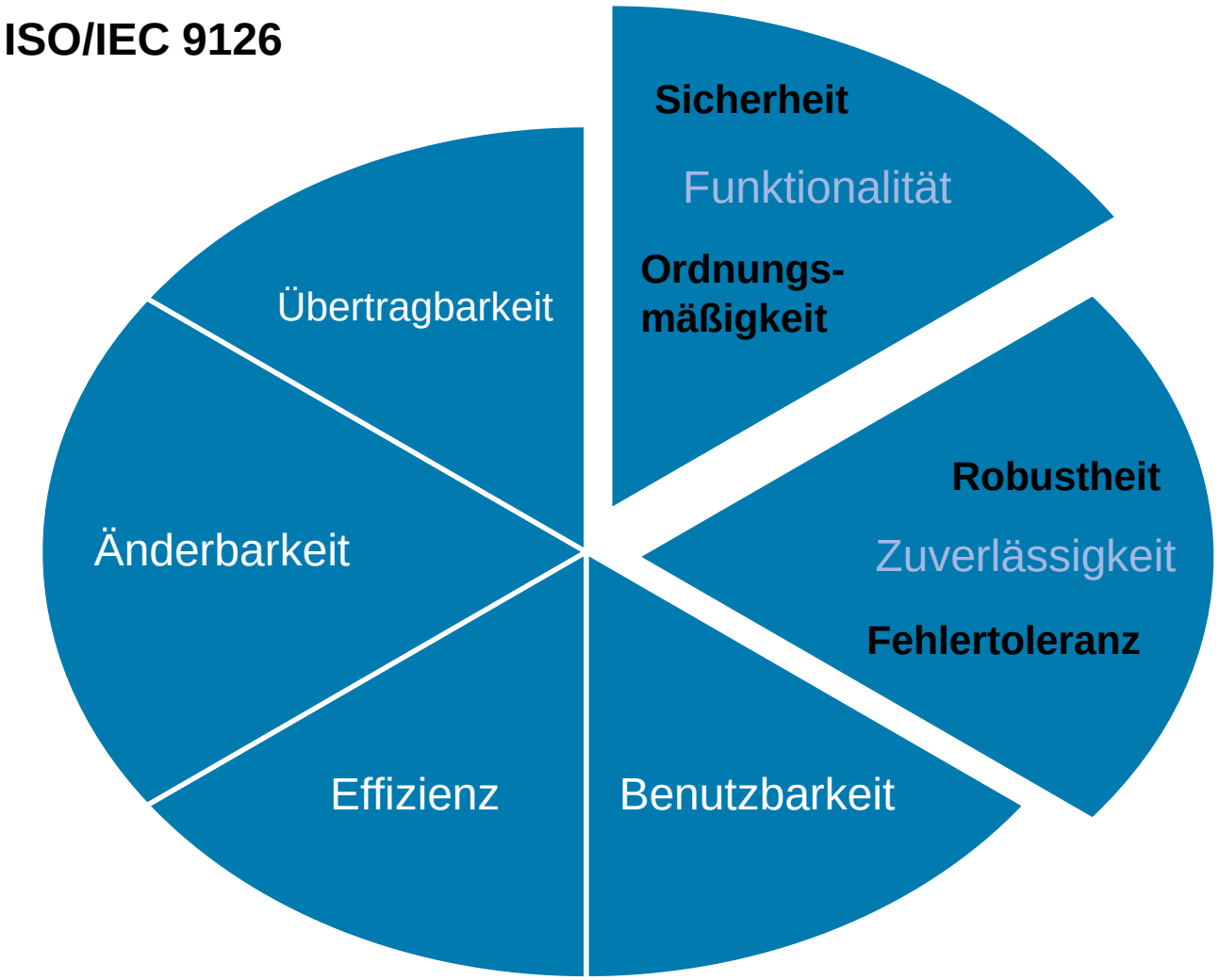
e.security solutions

Sicherheit ist ein Qualitätsmerkmal

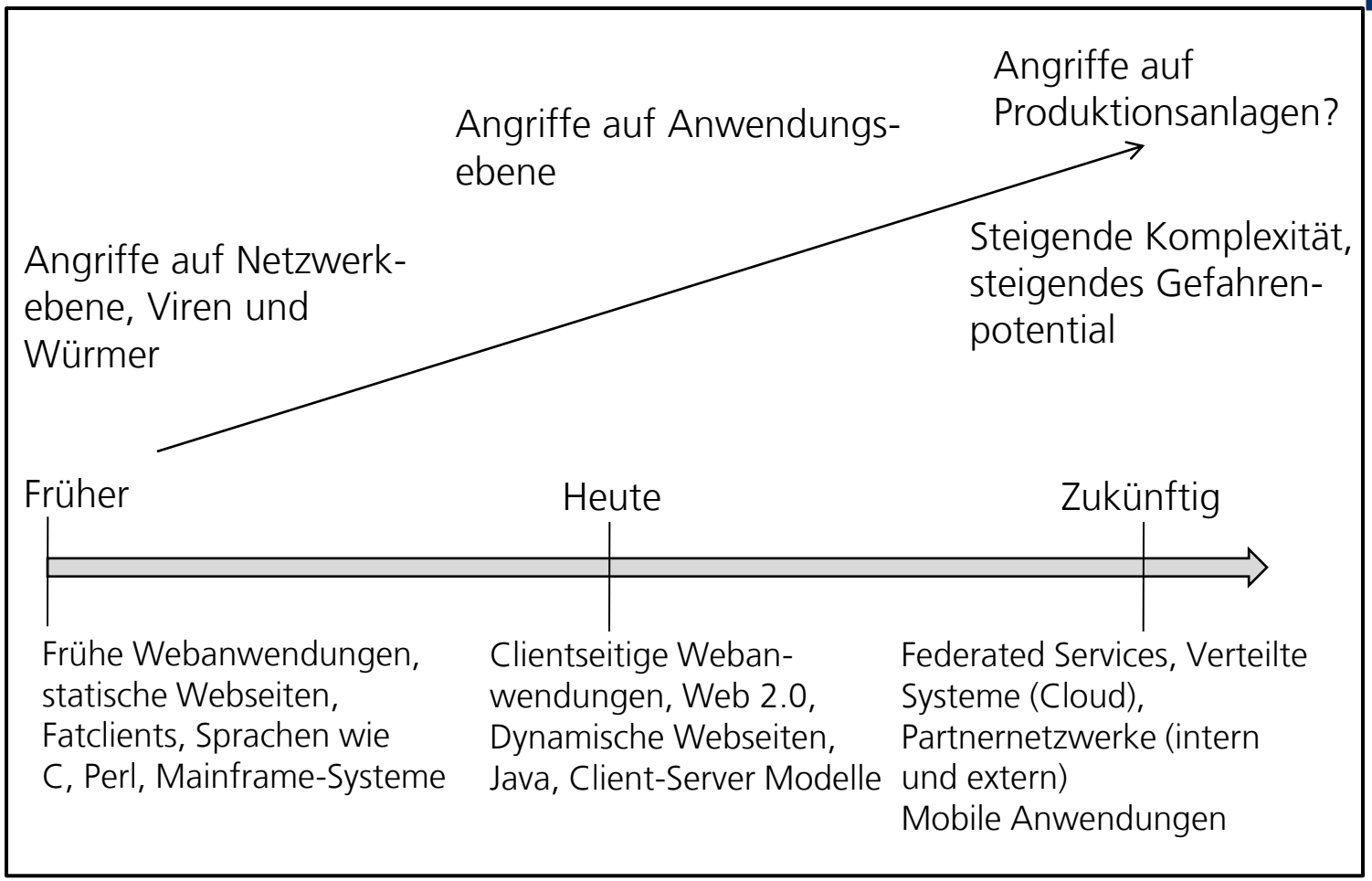
ISO/IEC 9126



Sicherheit ist ein Qualitätsmerkmal



Entwicklung der Anwendungen und Bedrohungen



Vorfälle in 2010

Chaos Computer Club Kongress
http://events.ccc.de/congress/2010/wiki/Hacked

Website Defacement zwischen den Feiertagen

FDP Webshop
Nur heiße Luft von FDP-Chef Guido Westerwelle?

ARD-Homepage:
Eilmeldung „Die Ursache für den Tod einer Eule im Kölner Dom sei geklärt: Gottes Zorn habe einen Reissack zum Umfallen gebracht, der wiederum die Eule erschlagen habe“.

Vorfälle in 2010

Handelsblatt.de und Zeit.de
Verteilung von Schadcode über Werbebanner

Sensible Daten von 40 Firmen öffentlich im Netz
Die Bewerbungsbögen von rund 40 Firmen für den Wirtschaftspreis Teltow-Fläming 2009 waren durch ein Sicherheitsleck frei zugänglich (Umsatz- und Mitarbeiterzahlen, Ausbildungsplätze, Investitionen, ...)

Datenleck bei Jugendreisen-Veranstalter
Unzureichende Berechtigungsprüfung beim Zugriff auf Reservierungen legen personenbezogene Daten offen

Quelle: http://www.xamit-leistungen.de/sicherheitsvorfaelle/

Iran bestätigt Cyber-Angriff durch Stuxnet
Wurm mit Schadprogramm speziell für SCADA-Systeme von Siemens

Software unsicher entwickeln in sieben Schritten

1. Planen Sie kein Budget für Sicherheit ein
2. Verankern sie keine Sicherheitsaktivitäten in Ihrem Entwicklungsprozess
3. Ermitteln Sie nur funktionale Anforderungen und keine Sicherheitsanforderungen
4. Schulen Sie ihre Entwickler nicht in Sicherheitsthemen
5. Erfinden Sie stets das Rad neu
6. Vermeiden Sie Security-Tests
7. Installieren Sie die Software in einer Standardbetriebsumgebung

1. Planen Sie kein Budget für Sicherheit ein

»|secaron

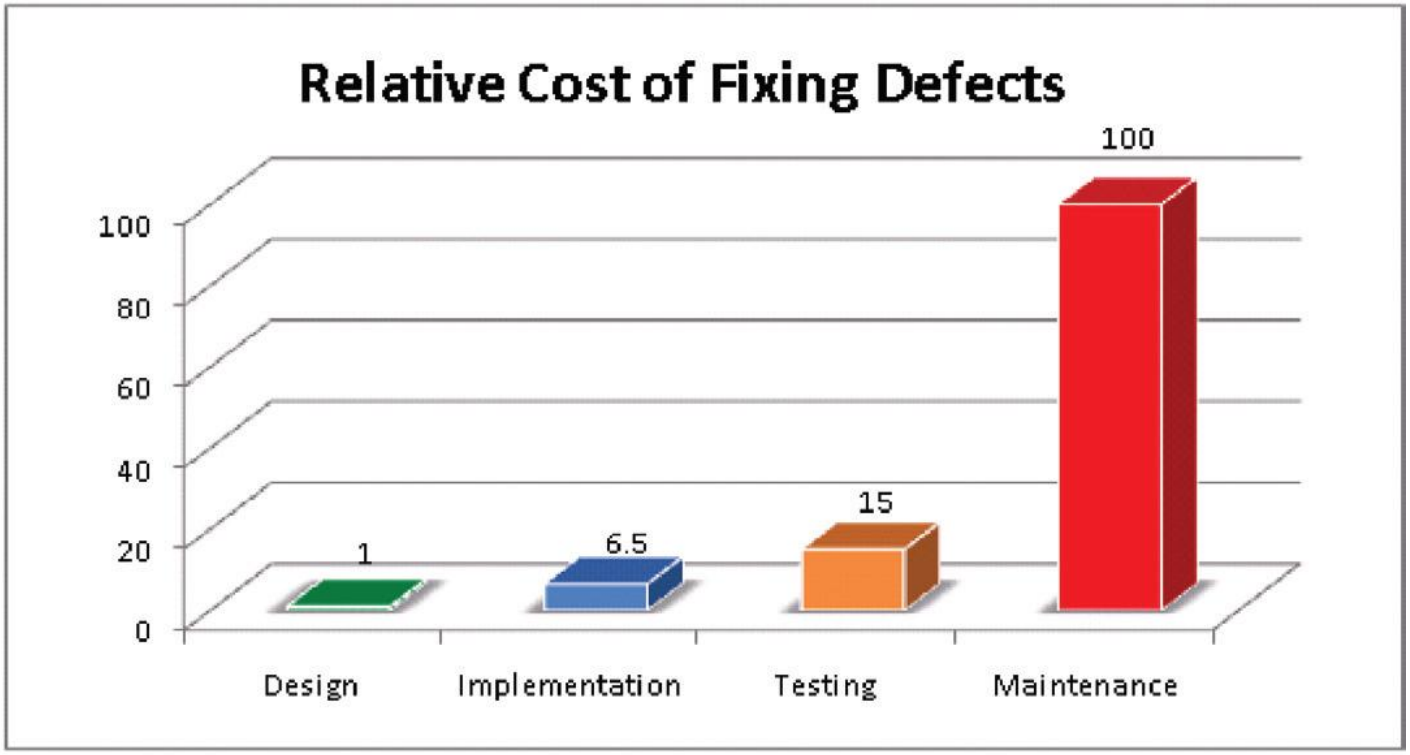
(ISC)²

„Wir machen noch schnell einen Penetrationstest.“

„Wenn etwas passiert, dann fixen wir das schnell.“

„Diese Sicherheitsmaßnahme können wir nicht mehr umsetzen, weil wir damit den Go-Live gefährden.“

Keine Sicherheit kostet auch Geld



Source: Implementing Software Inspections, IBM Systems Sciences Institute

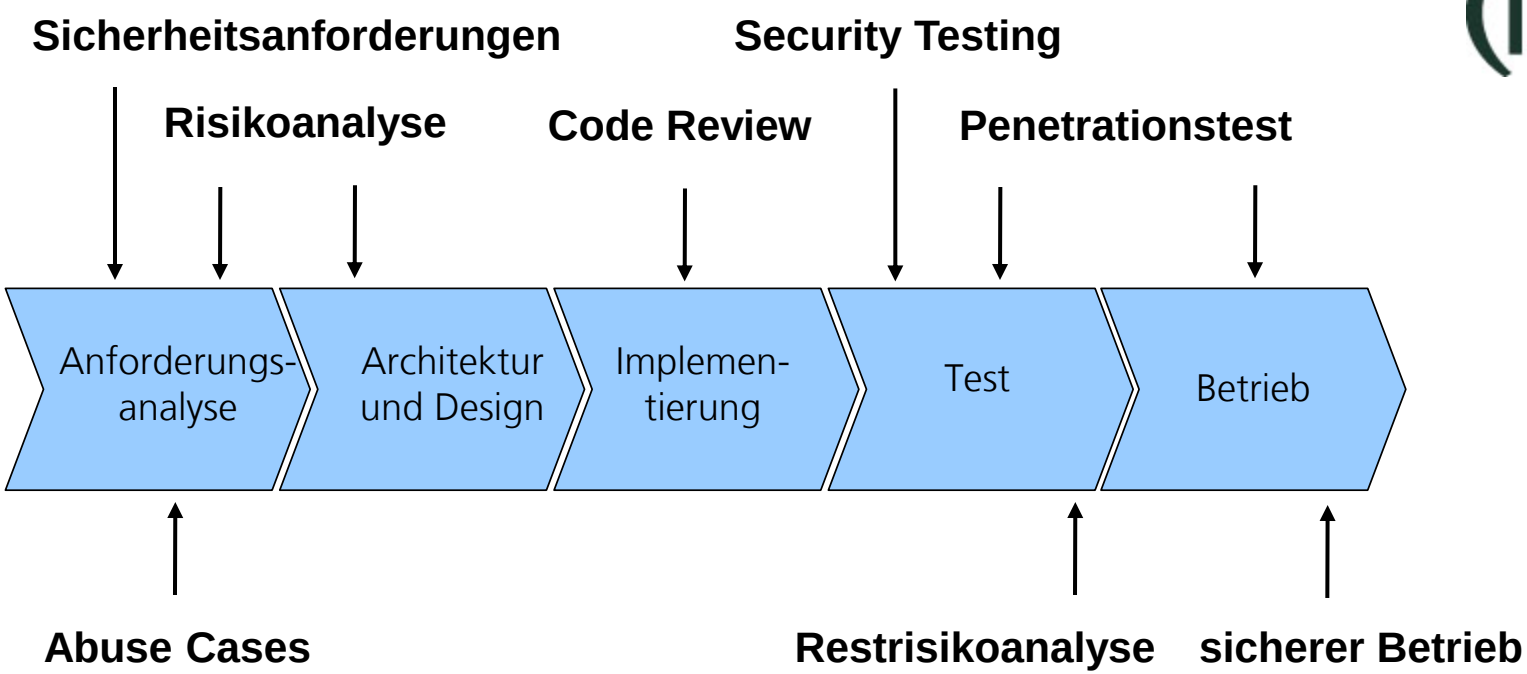
Wie viel Budget brauche ich?

- Implementierung von Sicherheitsfunktionalitäten
  (Authentisierung, Autorisierung, Eingabevalidierungen, ...)
  - Spezifikation
  - Implementierung
  - Test
  - Wartung
  - Betriebskosten

- Durchführung von spezifischen Sicherheitsaktivitäten

Generischer Entwicklungsprozess

Ansatzpunkte für mehr Sicherheit



3. Ermitteln Sie nur funktionale Anforderungen und keine Sicherheitsanforderungen

Use Case:
„Bewerber können sich über das Portal der Personalabteilung für offene Stellen bewerben.“

Wie wenig Sicherheit brauche ich?

»|secaron

(ISC)²®

Abuse Case:
„Ein Bewerber darf keine Bewerbungen von anderen einsehen.“

manager magazin

Suche

Home Unternehmen Finanzen Technologie Karriere Lifesty

Home > Technologie

04.09.2008

drucken verschicken bookmarken

Datenklau

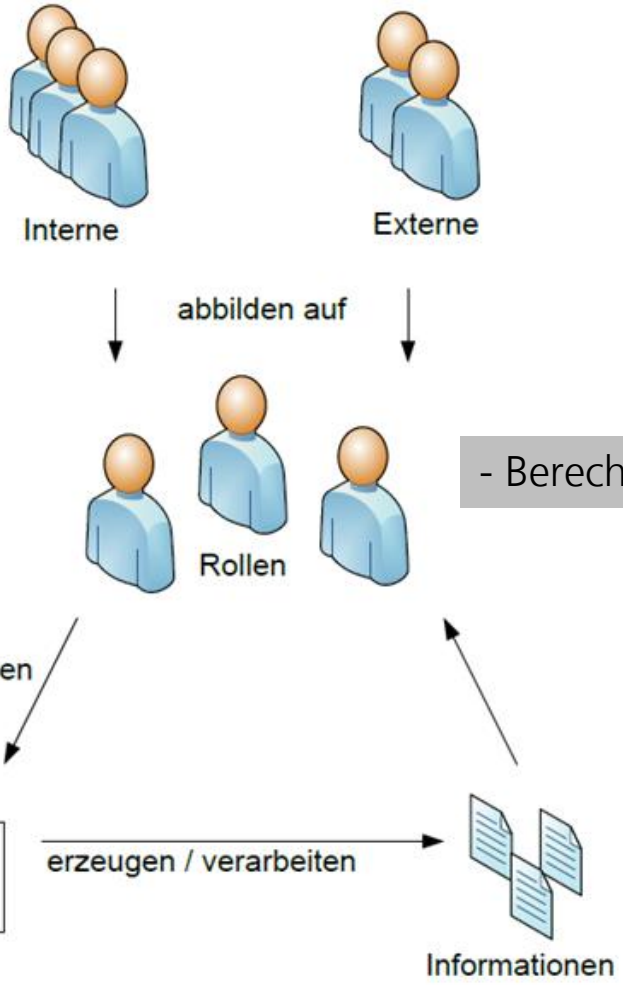
Zehntausende PwC-Bewerber betroffen

Nach Telekom und Bertelsmann ist offenbar auch PwC Opfer von Datendiebstahl geworden. Viele tausend Bewerber des Unternehmens könnten in Gefahr geraten sein, online Geld von Zahlungskonten zu verlieren. PwC hat Strafanzeige erstattet.

Frankfurt am Main - Nach einem Hackerangriff auf eine Datenbank hat die Wirtschaftsprüfungsgesellschaft PricewaterhouseCoopers (PwC)

Welche Sicherheitsrichtlinien meines Unternehmens bzw. welche gesetzlichen Anforderungen muss ich einhalten?

Fachliche Anforderungsanalyse



Zugriffswege:

- Internet
- Intranet
- Extranet

- Berechtigungen

- Schutzbedarf
- Aufbewahrungsfristen
- Datensicherung

- Nachvollziehbarkeit

4. Schulen Sie ihre Entwickler nicht bezüglich Sicherheitsthemen

»|secaron

(ISC)²

Session Management

SQL Injection

Vulnerabilities

Cross Site Scripting (XSS)

Parameter Tampering

Input validation

Authentication enforcer

Buffer Overflows

Threat modeling

Harvesting

Cross Site Request Forgery (CSRF)

Malicious File Execution

Brute Force Attack

Risk analysis

Exception handling

Was muss ich wissen?

60% der Angriffe in 2009 über das Internet zielten auf Webapplikationen ab.

80% davon waren erfolgreich durch
- SQL Injection
- Cross-Site-Scripting (XSS)

Beide Angriffe sind seit langem bekannt.
(vgl. SANS Top 25, OWASP Top 10)

Schulungsangebote

»|secaron

Zertifizierungen

(ISC)²

- (ISC)²
  Certified Secure Software Lifecycle Professional

- ISSECO®
  Certified Professional for Secure Software Engineering

Informationsquellen

- SANS Top 25

- Open Web Application Security Project (OWASP)

- Leitfaden sichere Entwicklung (DsiN e.V.)

5. Erfinden Sie stets das Rad neu.

Quelle: Stanley Wagon, Macalester College
http://www.stanwagon.com/

Wiederholung von Fehlern vermeiden
Aufwand reduzieren

- Wiederverwendung und Standardisierung
- Best Practices / Security Design Patterns
- Bewährte Frameworks und –methoden
- Musterlösungen

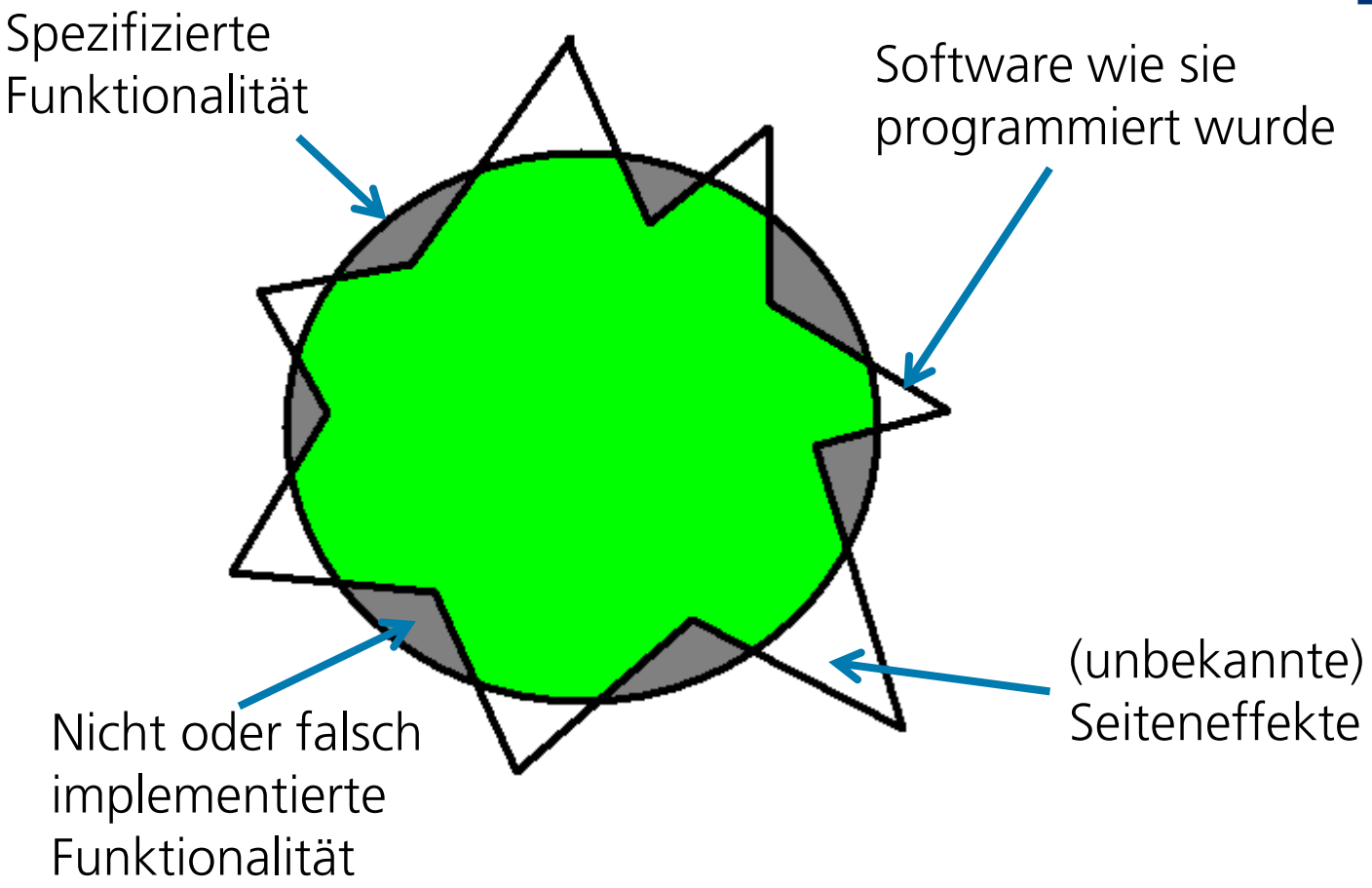
Sichere Architektur vs. Sichere Programmierung

- Umsetzung der Sicherheitsanforderungen durch angemessene Sicherheitsmaßnahmen
- Eine sichere Architektur kann durch Programmierfehler unsicher werden.
- Eine Software ohne Programmierfehler kann Schwächen durch die Architektur aufweisen

  Fehlerfreie *telnet* Implementierung ist trotzdem aufgrund der unverschlüsselten Übertragung angreifbar.

6. Vermeiden Sie Security-Tests

Die Wahrheit über Software



Was sollte ich prüfen/testen?

1. Einhaltung von Programmierrichtlinien
   Einsatz von statischen Analyse-Tools (Code Scanner)

2. Testabdeckung (Code Coverage)

3. Testfälle für ermittelte Sicherheitsanforderungen und Abuse Cases

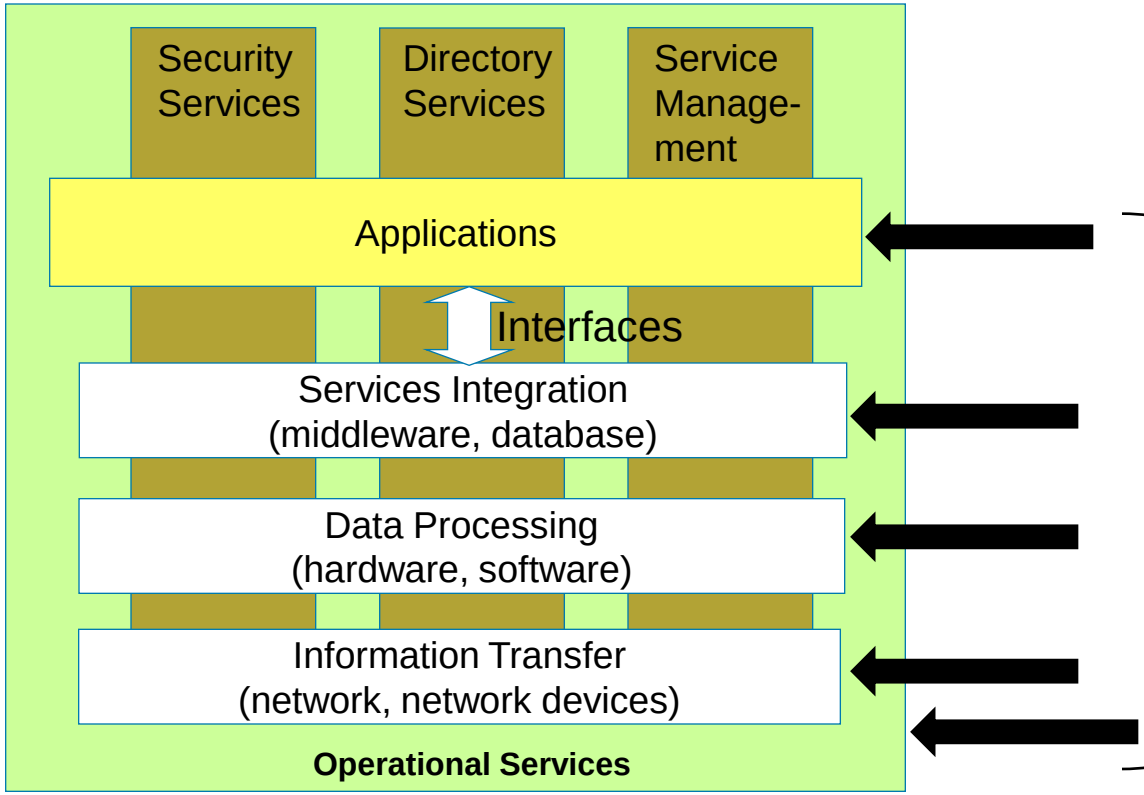
4. Security Scanner, um typische Fehler zu finden

5. Manuelle Penetrationtests, um das nicht Offensichtliche zu finden, auch Design Fehler.

7. Installieren Sie die Software in einer Standardbetriebsumgebung

Quelle: Unbekannt

Ganzheitliche Risikoanalyse



Betriebsrelevante Aspekte

- Anforderungen an Betriebsumgebung
  z.B. Clusterumgebung bei hoher Verfügbarkeit
  Härtung der Serverlandschaft
  Monitoring

- Sichere Konfiguration
  z.B. nur sichere kryptographische SSL-Verfahren
  Ändern von Default-Passwörtern

- Proaktive Logauswertung

- Reaktionen auf Sicherheitsvorfälle

- Definition und Einhaltung von Service Levels

Wenn Sie noch mehr wissen wollen...

Heute, 14:30 – 15:30

Lucas von Stockhausen:

Sichere Software bereits während der Entwicklung - Wie können BSIMM und OpenSAMM hierbei helfen?

Vorgehensweisen zur Implementierung eines sicheren Entwicklungszyklus

BSIMM

»|secaron

(ISC)²

Build Security In Maturity Model

The Software Security Framework (SSF)			
Governance	**Intelligence**	**SSDL Touchpoints**	**Deployment**
Strategie und Metriken	Angriffsmodelle	Architekturanalysen	Penetration Testing
Compliance und Policy	Security Features und Design	Code Review	Software Environment
Training	Standards und Requirements	Security Testing	Configuration Management and Vulnerability Management

http://bsimm.com/

Zusammenfassung

1. Klares Management Commitment
2. Integration der Sicherheit in den Entwicklungsprozess
3. Ganzheitliche Sicht von Anfang an
4. Schulung der Mitarbeiter
5. Wiederverwendung bewährter Lösungen

Kontakt

Secaron AG
Ludwigstr. 45
D-85399 Hallbergmoos
Tel. +49 811- 9594 - 402
Fax +49 811- 9594 - 220
www.secaron.de
Ansprechpartner:
Markus Wutzke
E-Mail: wutzke@secaron.de