
Buffer Overflow
Basic Authentication
PHP
Encoding Attacks
Session Tampering
LDAP Injection
SDLC
Page Sequencing
Brute Force
Denial of Service
Form Field Manipulation
OS Command Injection
HTTP Response Splitting
SSI Injection
SQL-Injection
Backup File Disclosure
Cross Site Scripting
Extension Manipulation
Format String Attack
Configuration File Disclosure
Content Spoofing
Secure Software
Cookie Poisoning
File Enumeration
Abuse of Functionality
DotNET
Java
Directory Traversal

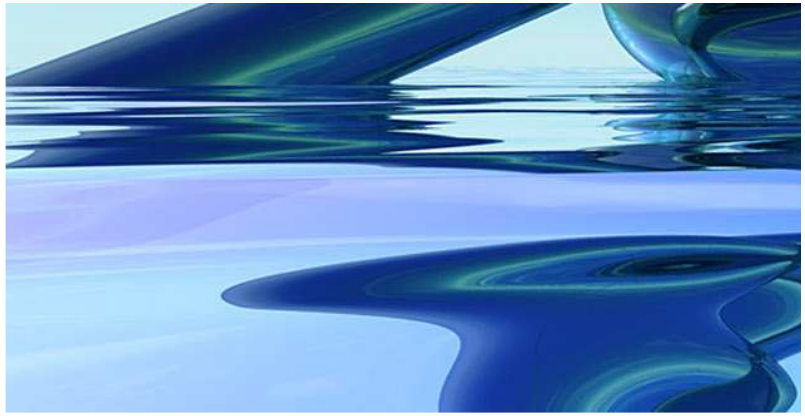
“There is no security on this earth.”

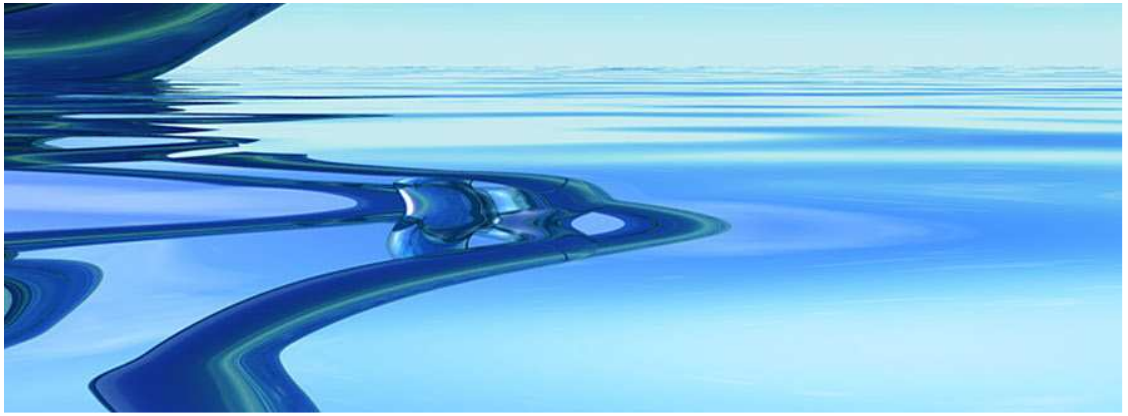
General Douglas MacArthur

“Na und ?”

Alfred E. Neumann

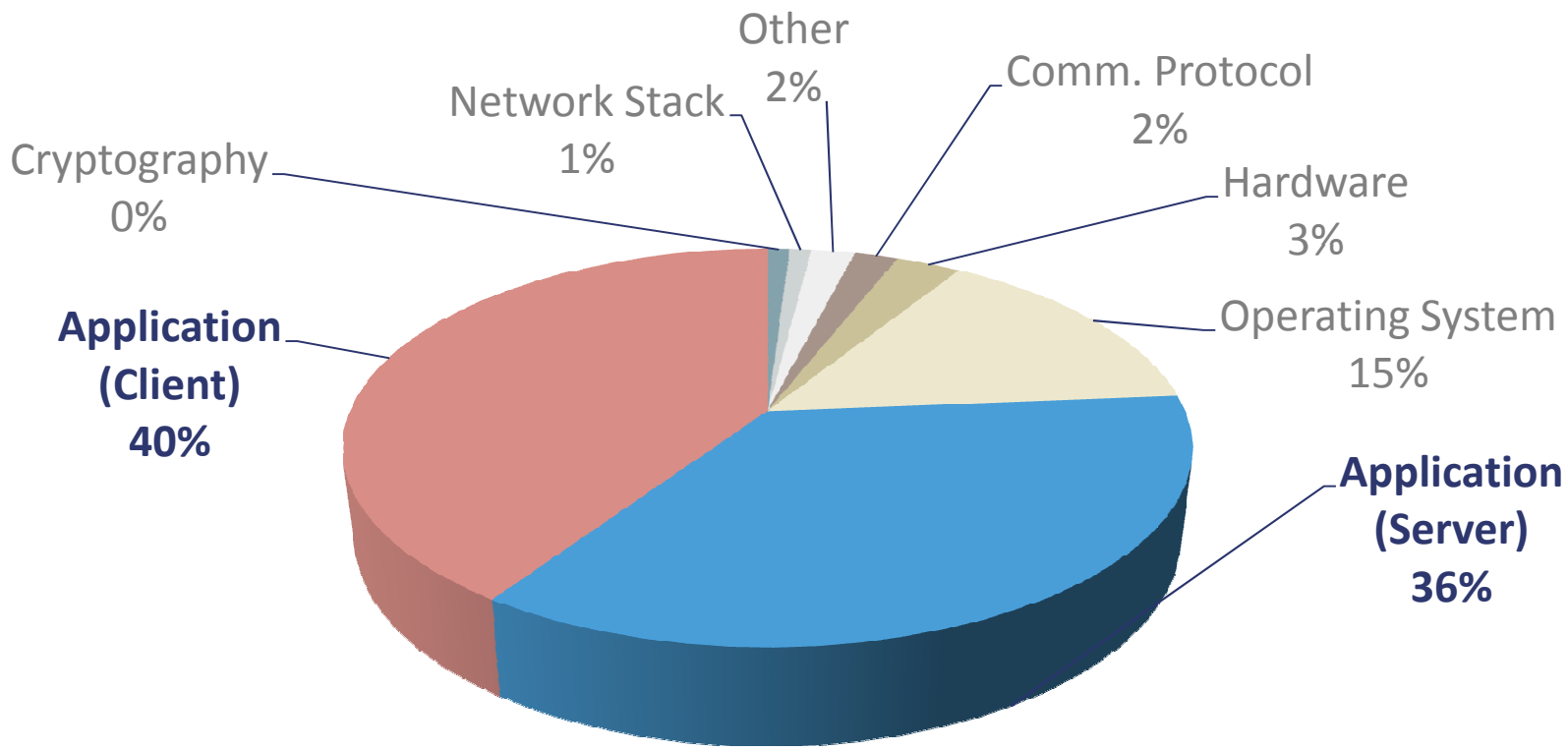
OPTiMA..bit
business information technology





Anwendungen verursachen Unsicherheit

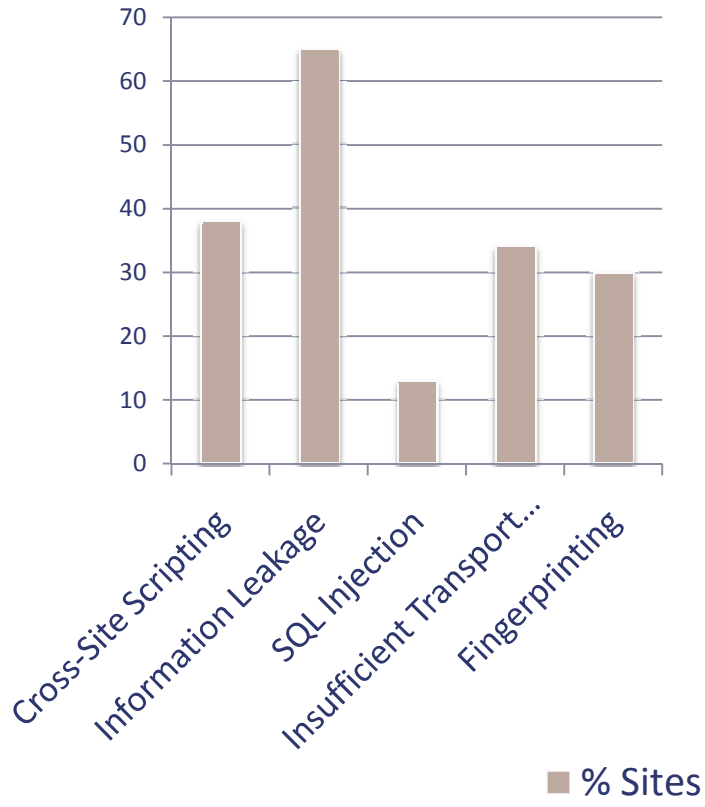
Ca. ¾ aller Schwachstellen stammen aus Anwendungen.



Webanwendungen: besonders gefährdet

Web-Anwendungen sind bevorzugte Ziele für die Cybermafia

- Die Anzahl und die Aggressivität der Angriffe auf Anwendungen steigt stetig.
- Die Angreifer sind professionelle Verbrecher: Die „Cybermafia“.
- Web-Anwendungen sind beliebte Ziele, weil sie oft Schwächen vorweisen, die einfach auszunutzen sind.



OPTIMA..bit
business information technology gmbh

Sicherer Software Development Lifecycle

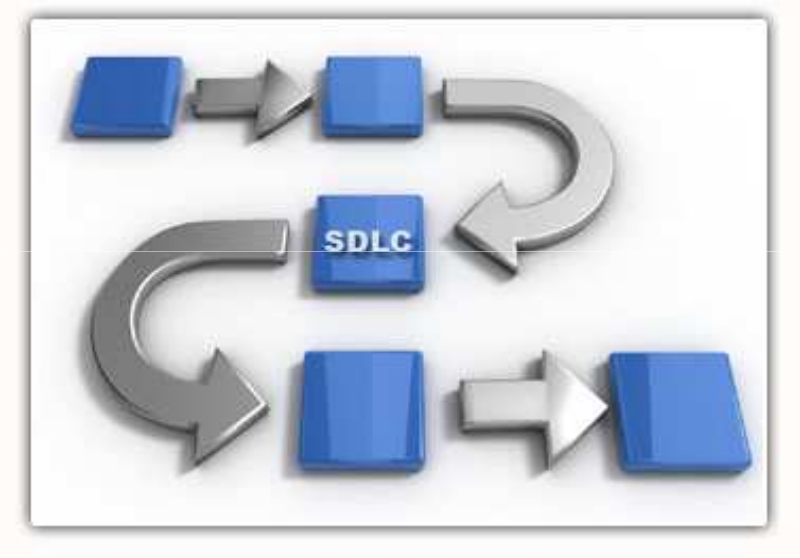
Weg von Punktmaßnahmen hin zur strategische Planung

Seit ca. 5 Jahren gibt es ein großes Interesse an den sicheren SDLC

Leider sind Standards und (publizierte) Erfahrung noch Mangelware

Viele offene Fragen, z.B:

- **Welche Maßnahmen gehören dazu?**
- **Prozess- oder Maturity-Modell?**
- **Anwendbarkeit?**



OPTIMA..bit
business information technology gmbh

Die Historie des sicheren SDLCs

Seit ca. 2000 wird es versucht, ein passendes Modell zu finden

Name	Jahr	Merkmale
TSP-Secure	?	Fokus auf “defect removal”, eigenständige Teams
CMMI	2002	Für allgemeine Entwicklung, kein Fokus auf Sicherheit, Reifegradmodell
CLASP	2005	Lose Sammlung von Prozesserweiterungen, Tools, Vulnerabilitykategorien etc.
Microsoft SDL (Prozess)	2004	Prozess, sehr stark integriert, speziell auf Microsoft-ähnliche Organisationen angepasst
Touchpoints	2006	Prozesserweiterungen ähnlich CLASP aber strukturierter
OpenSAMM (Software Assurance Maturity Model)	2008	Reifegradmodell, inkrementell, anpassbar, basiert auf Expertenmeinung, detailliert
BSI-MM (Build Security In Maturity Model)	2009	Reifegradmodell, inkrementell, anpassbar, basiert auf Studie, wenig Detail-Informationen

Prozess- vs. ReifegradModelle

Nur ein Reifegradmodell kann erfolg haben

Softwareentwicklung ist vielfältig und jedes Unternehmen hat seine eigene Prozesse und Verfahren dazu.

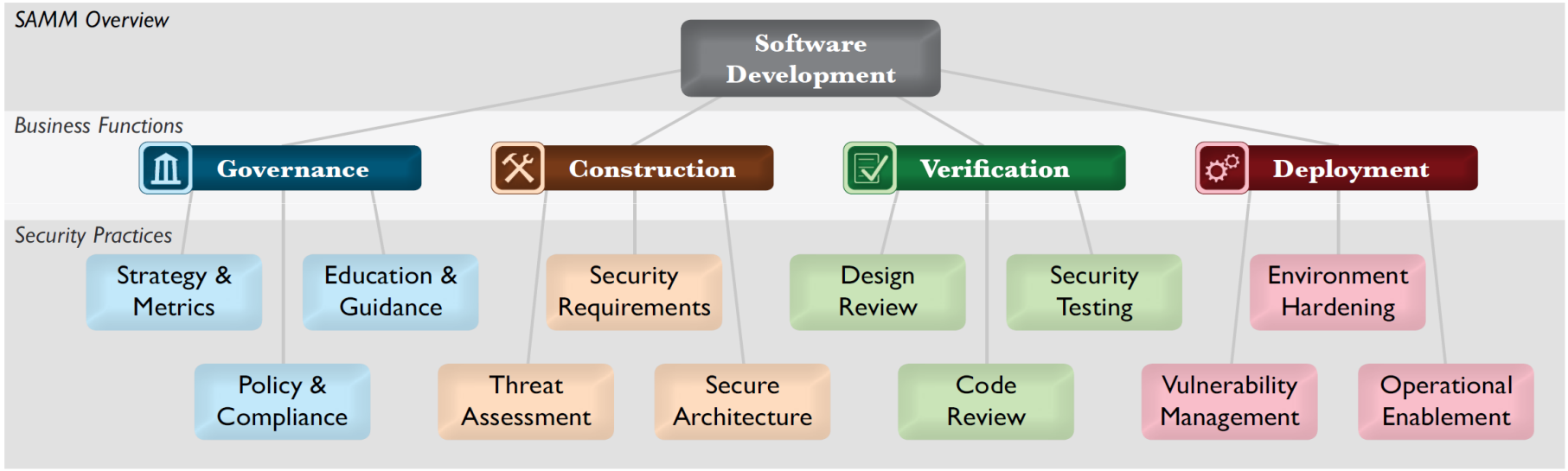
Es ist prinzipiell nicht möglich, ein starres Prozessmodell für Sicherheit aufzuzwingen.

Nur ein Reifegradmodell, welches auf eine höhere Ebene agiert, kann die Vielfalt und die Verwandlung der Softwareentwicklung abdecken.

Insource	Outsource
Formal	Agile
Build	Buy

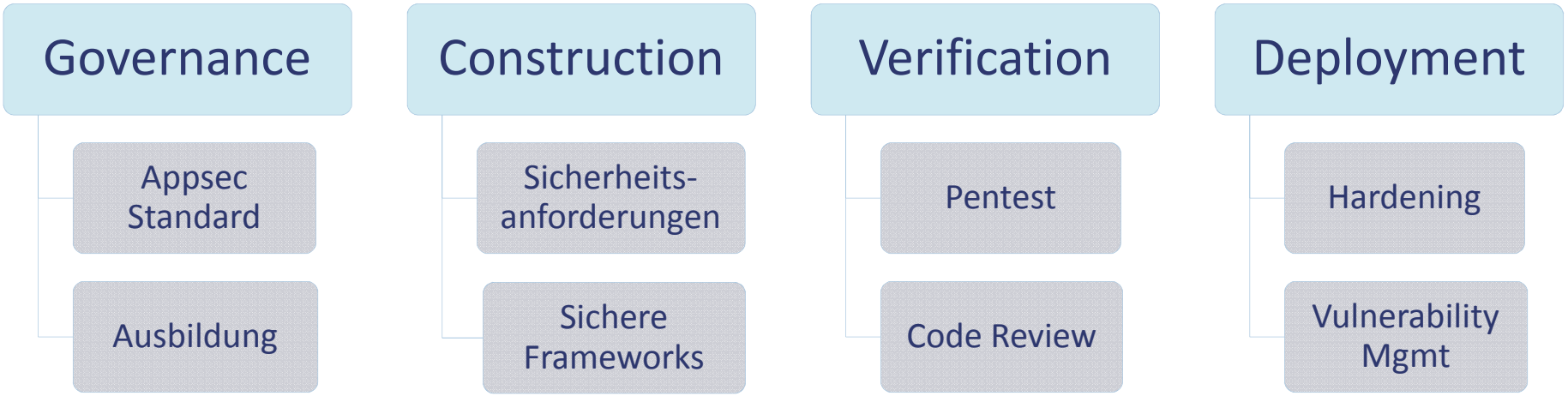
OpenSAMM Overview

4 Geschäftsbereiche, 12 Bereiche der Sicherheitspraktiken



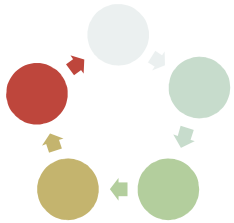
Wichtige Teile eines Secure SDLC

Diese Aktivitäten sichern eine Basislinie für sichere Webapps



Benchmarking with OpenSAMM

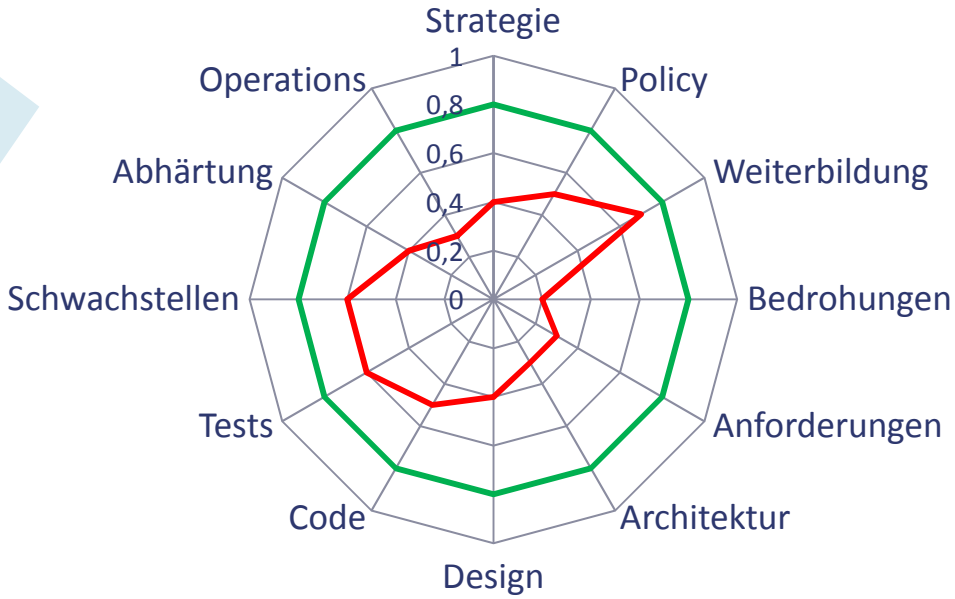
Basierend auf Befragungen (Workshop) zu den Themen



Sicherer SDLC nach OpenSAMM

Workshop

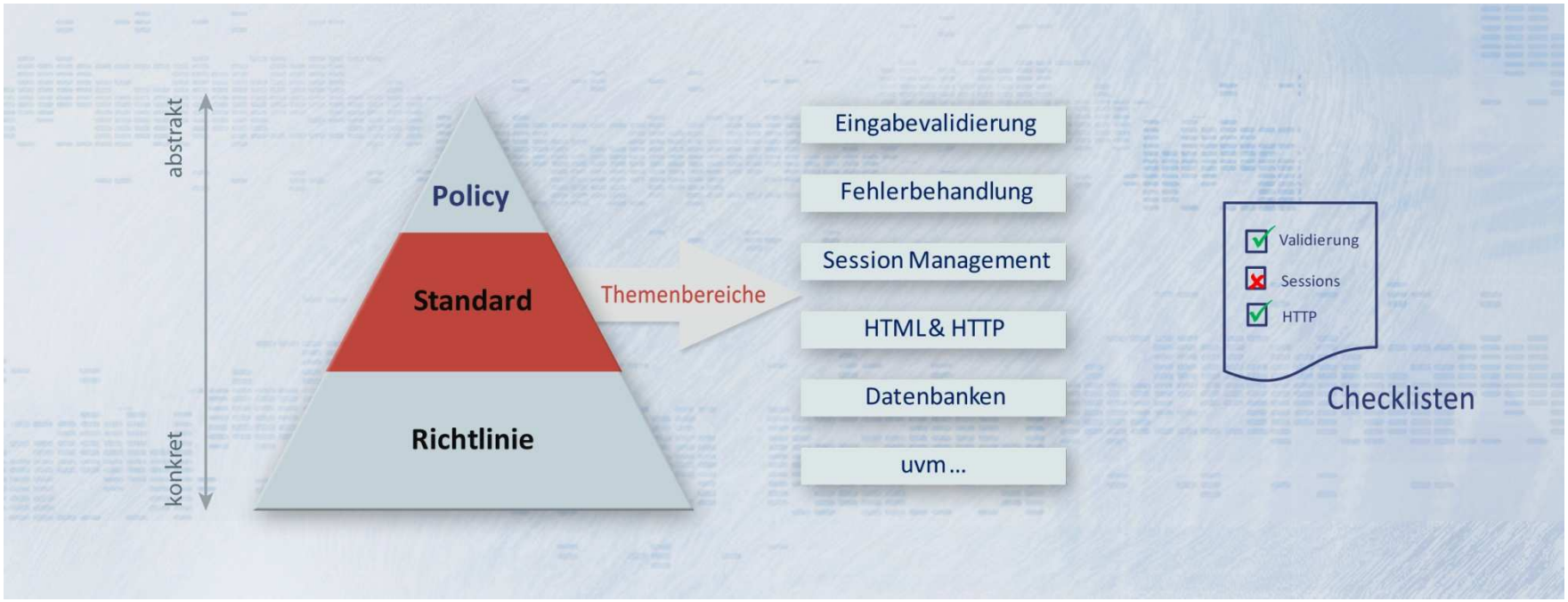
Aktueller Stand eines Unternehmens



OPTIMA..bit
business information technology gmbh

Application Security Standards

Standards regeln die Vorgaben für sichere Entwicklung



Standards und Granularität

Die richtige Bilanz ist wichtig

Zu abstrakt:

```
Systems must be protected
according to §2.4.3 of
ISO/IEC 27002 ...
```

Zu konkret:

```
Do not use
HttpRequest.isUserInRole("adm
in") in an Internet facing
servlet under JDK 1.4
```

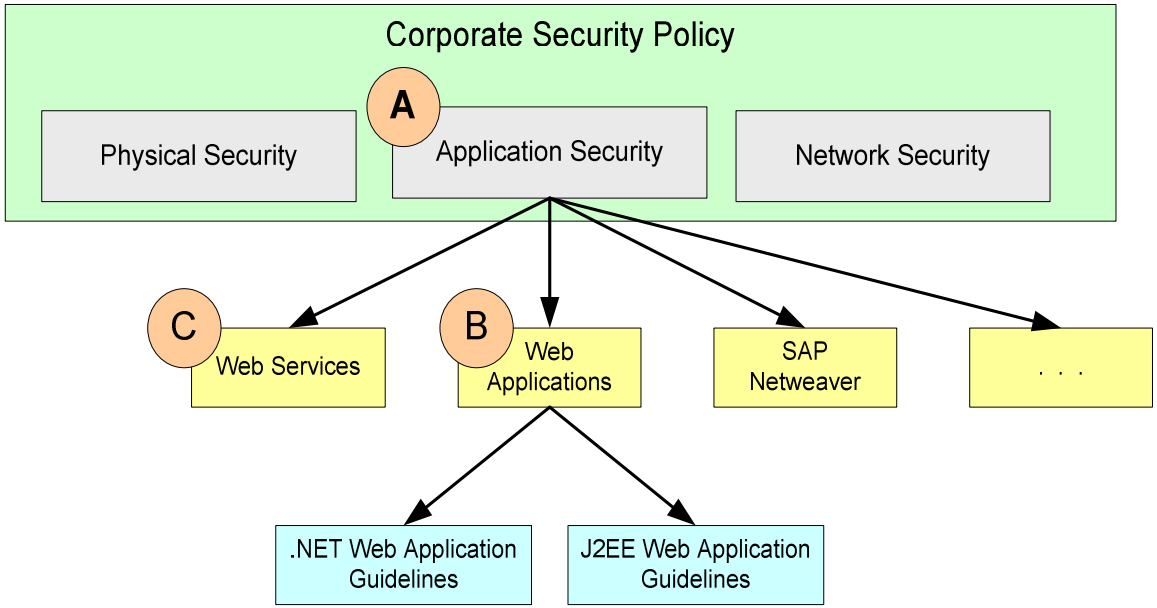
Out of Scope (eher Betrieb):

```
Tomcat must be configured to
deny use of the invoker servlet
```

Out of Scope (eher Security)

```
Logfiles must be monitored for
attacks.
```

Erweiterbare Struktur ist flexibel



Primary Policies

Secondary Policies

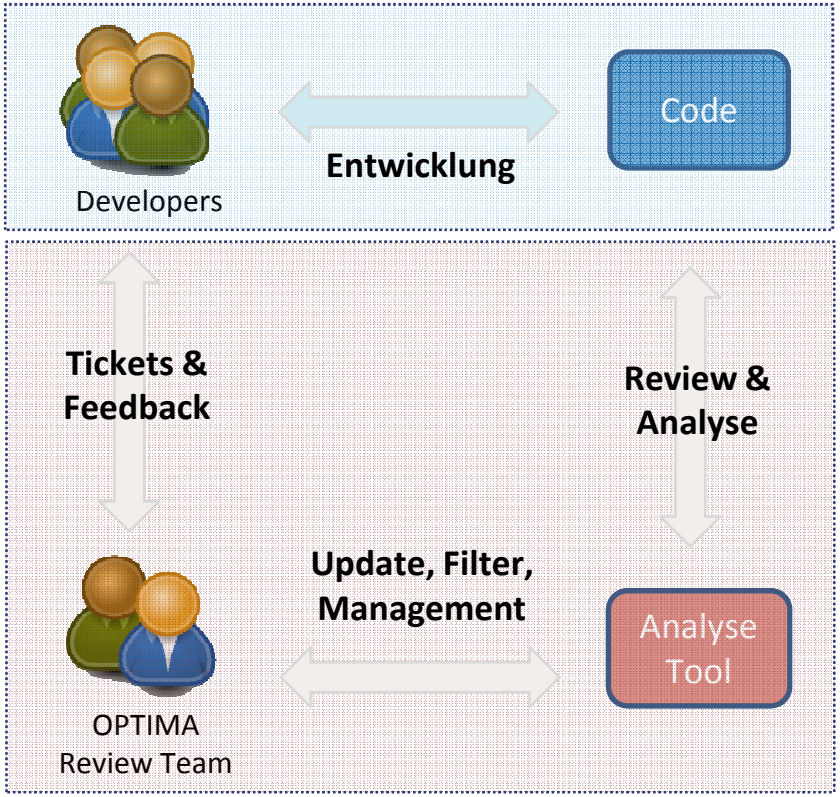
Guidelines

OPTIMA..bit
business information technology gmbh

Managed Code Services

Ihr Code wird auf Qualität und Sicherheit von Experten geprüft

- Managed Code Services sorgen für sichere Anwendungen und erhöhte Code-Qualität.
- Entwickler werden entlastet und unterstutzt.
- Reviews vor Ort oder per Remote
- Metriken für Qualität?
- Bereinigung von False Positives?

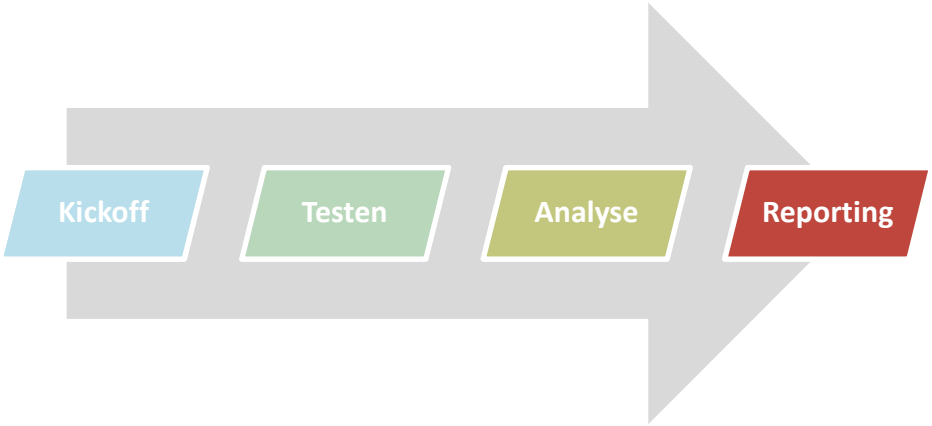


OPTIMA..bit
business information technology gmbh

Penetrationstest

Penetrationstest muss regelmäßig und strukturiert sein

- Strukturierter Penetrationstest nach OWASP Standards und BSI Kriterien.
- Aktuelle Schwachstellen werden erkannt (regelmäßiges Forschen)
- Mit Tools und manuell per Expertenhand.
- Nachvollziehbare und klare Kriterien für Schwere, Eintrittswahrscheinlichkeit, usw.

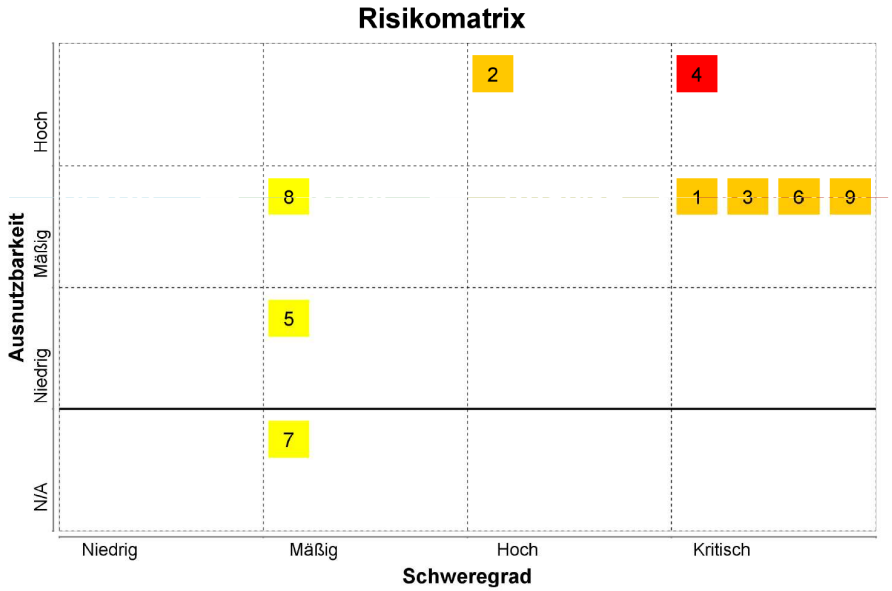


Penetrationstest einer Webanwendung

Qualität ist entscheidend --- Gute Tests brauchen auch Zeit

Ein hochwertiger Pentest:

- ist strukturiert nach OWASP Standards und BSI Kriterien.
- erkennt aktuelle Schwachstellen.
- baut primär auf manueller Expertentest (Tools auch wichtig)
- ausführlich dokumentiert mit nachvollziehbare Risikobewertungen.



OPTIMA..bit
business information technology gmbh

Über

OPTIMbit

GmbH

OPTIMA..bit
business information technology

Fokus

IT-Sicherheit für Anwendungen & Infrastrukturen

Kunden

Unternehmen ab ca. 500 Mitarbeitern

Credo

Herstellerneutrale Beratung von höchster Qualität

Kontakt

OPTIMAbit GmbH
Dr. Bruce Sams
Marktplatz 2
85375 Neufahrn

Tel.: +49 8165/65095
Fax +49 8165/65096

bruce.sams@optimabit.com
www.optimabit.com

OPTIMA..bit
business information technology gmbh

Vielen Dank

für Ihre Aufmerksamkeit

OPTIMA..bit
business information technology