



Sichere Webapplikationen mit ISO 27001: Secure Coding Policy

Johannes MARIEL
10. Juni 2011





Bundesrechenzentrum Der IKT-Dienstleister des Bundes



- **Marktführender E-Governmentpartner**
 - Themenführer bei E-Government Projekten in der Verwaltung
 - Unterstützung bei der E-Government-Integration
 - Umsetzung innovativer Referenzprojekte

- **IKT-Dienstleistungszentrum für Verwaltungsmodernisierung und -reform sowie Services für Bürger und Wirtschaft**
 - IKT-Lösungen zum bedarfsgenau besten Qualitäts-/Kostenverhältnis
 - Ausschöpfung aller Produktivitäts- u. Effizienzsteigerungspotenziale
 - Nachhaltige Kosteneinsparungen für den Bund

- **Das IKT-Shared Service Center des Bundes**
 - Shared-Service-Modell steigert Effizienz, Qualität und Serviceorientierung in verbundenen Organisationen
 - Bündelung gleichartiger Prozesse und Aufgaben
 - Entlastung der Behörden durch Auslagerung von IKT-Aufgaben

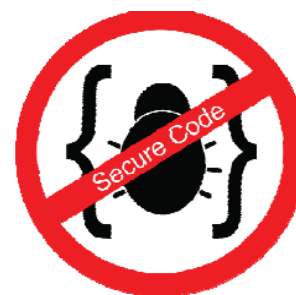
BRZ - Marktführender E-Government Partner in Österreich

IT Service-Provider Ranking*	Platz 4
Infrastrukturbetreuung	an 1.200 Lokationen
Betreute IT-Arbeitsplätze	30.000
Implementierte IT-Lösungen	> 300
Hostleistung	> 7.000Mips
Server in Betrieb	> 1.270
Outputservice (Aussendungen)	> 30 Mio. p.a.

Mitarbeiter SW-Entwicklung/Betreuung ~ 400

* IDC Market Analysis - Austria IT-Services
2008-2012 Forecast and 2007 Vender Share

WARUM Secure Coding?



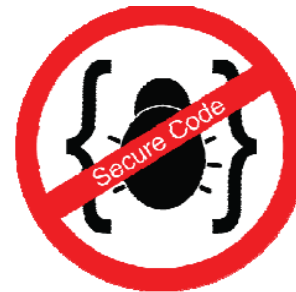
Das Bundesrechenzentrum als IKT-Dienstleister des Bundes

- Immer mehr Verwaltungsanwendungen sind im Internet verfügbar
- Die überwiegende Anzahl der Attacken auf IKT-Systeme erfolgt auf Webanwendungen (51% - IBM-Studie 12/2008)
- Angriffs-Szenarien nutzen eine relativ kleine Anzahl typischer Softwarefehler
- Ein Großteil dieser Fehler ist durch Information, Schulung und Qualitätssicherung leicht vermeidbar

Das Bundesrechenzentrum entwickelt und betreibt Individualanwendungen für die öffentliche Verwaltung

- **Vertrauen unserer Kunden** in die Sicherheit und Qualität der Leistungen des BRZ
- **Vertrauen der Bürger**, die E-Governmentanwendungen nutzen, dass ihre Daten gut geschützt sind
- **Compliance** zu den gesetzlichen Pflichten (zB. DSGVO), den verbindlichen Standards (zB. ISO27001) und vor allem den vertraglichen Verpflichtungen gegenüber unseren Kunden

Secure Coding im Service-Lifecycle



Das Bundesrechenzentrum betreibt ein Informations Sicherheits-Management-System (ISMS) nach ISO 27001

- Riskmanagement zeigt Schwachstellen von unsicherem Code auf (2007)
- Audits bringen konkrete Schwachstellen zutage
- Behebung fördert erste Awareness bei Entwicklern
- Workshops Secure Coding verbessern Skills (2008/2009)
- Standardisierung der Vorgaben = Secure Coding Standards (2008/2009)
- Aufnahme in Standardausbildung für Programmierer (2010)

Die Secure Coding Standards folgen den Standards und Best Practices

- ISO 27001 (Informationssicherheit)
- ISO 20000 (IT-Service Management)
- Sicherheitsrichtlinie der BRZ Gruppe
- Internationale Communities (OWASP)

Secure Coding folgt dem Lebenszyklus eines Services

- Anforderungen (Schutzbedarf des Services)
- Projektplanung berücksichtigt „Sicheren Code“
- Servicearchitekturen berücksichtigen die Vorgaben der BRZ-Sicherheitsarchitektur
- Entwickler beachten die Vorgaben der Secure Coding Standards
- Abnahmen prüfen die Sicherheit des Codes des neuen Services vor der Betriebsübergabe

Secure Coding folgt dem Lebenszyklus eines Services

- Regelmäßig durchgeführte Risikoanalysen halten die Anforderungen aktuell bei
 - Änderungen der Bedrohungen von außen
 - Änderungen des Services
- Audits prüfen die Wirksamkeit der Code-Sicherheitsmaßnahmen
- Je nach Schutzbedarf werden weitere Maßnahmen ergänzt (z.B.: Applikations-Firewalls)

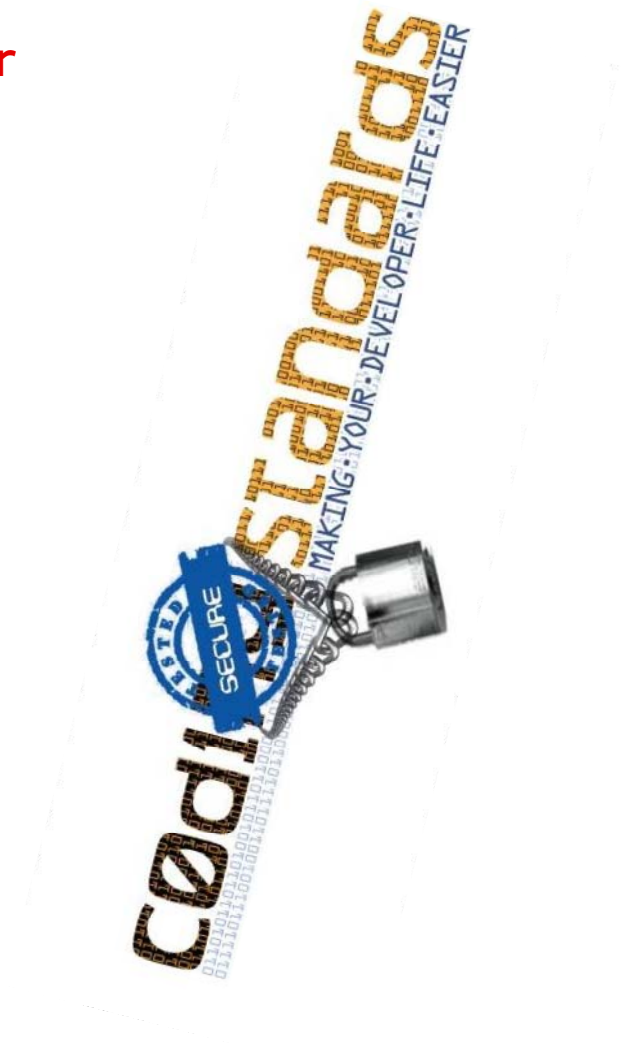
10 Grundsätze zum sicheren Programmieren

- **R01:** Input- und Outputvalidierung
- **R02:** Verwenden von Prepared Statements
- **R03:** Verwenden von http-only-Cookies
- **R04:** geringstmögliche Rechte auf Datenbank und Betriebssystem
- **R05:** MIME-Types bei Upload beschränken
- **R06:** Passwörter verschlüsselt Speichern
- **R07:** Aufstellen von Passwort-Policies
- **R08:** Korrekte Fehlermeldungen
- **R09:** Dynamische Ausgaben HTML escapen
- **R10:** Vermeiden von HTML-Kommentaren

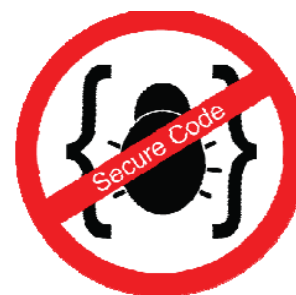
Die „Bibel“ zu Secure Coding

Der Langtext zu den 10 Geboten steht in der Bibel, hier in den „BRZ Secure Coding Standards V 1.0“

- Basisinformation im Intranet
- BRZ Secure Coding Standards V 1.0 für die wesentlichen Plattformen Java und dot.net
- SC-Community trifft sich im BRZ-Wiki mit aktuellen Infos
- Links und News werden vom System Security Engineer Secure Coding ebenso bearbeitet wie neue Erkenntnisse



GENUG Secure Coding?

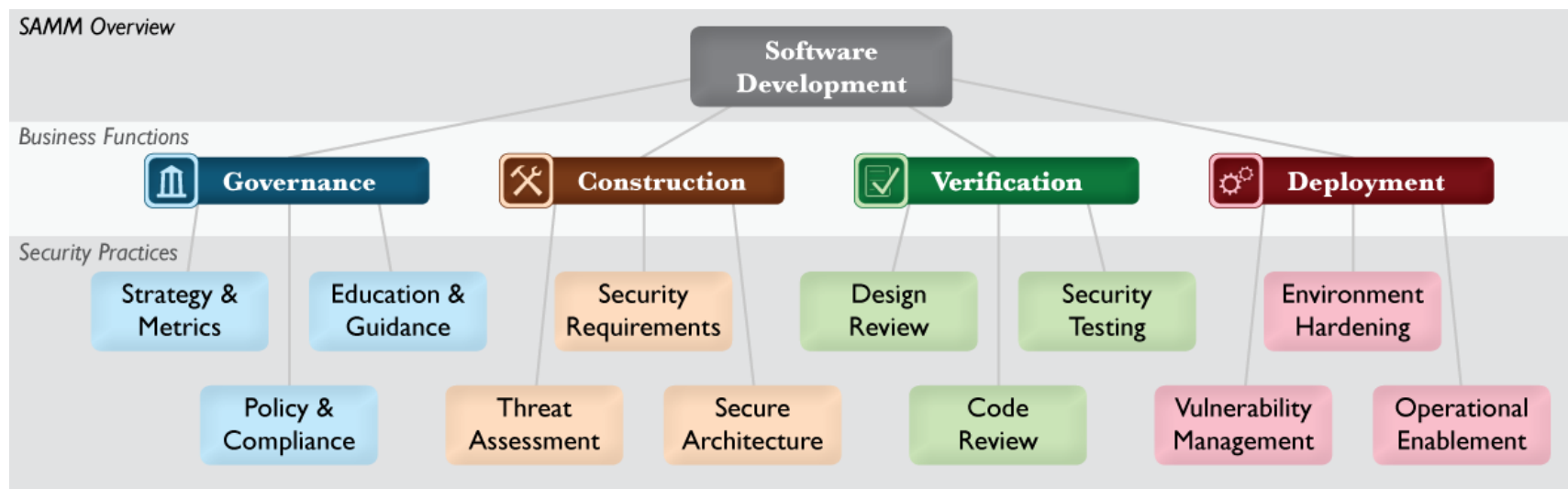


Die Frage nach „Wieviel Security muss/kann/soll man in die Anwendungsentwicklung investieren“ kann mit SAMM beantwortet werden

- SAMM = Software Assurance Maturity Model (Quelle:OWASP)
- beschreibt den SW-Entwicklungszyklus aus der Sicht von Security
- definiert in vier Dimensionen die wesentlichen Maßnahmen
- unterstützt die Evaluierung der Durchdringung der Organisation aus der Sicht von Secure Coding
- eignet sich als Grundlage für die Argumentation gezielter Investitionen für Secure Coding
- bietet wiederholbare Messkriterien, die Fortschritte nachweisen
- konkretisiert die Risiken -> Input für RiskMgmt-Systeme

SAMM Übersicht

Ausgangsbasis sind die Prozesselemente, die eine Organisation im Software-Entwicklungsprozess abbildet (Business Functions)



Jeder Business Function sind drei Security Practises zugeordnet, die alle relevanten Software Security Aufgaben abdecken und jede bildet einen „Silo“, der Verbesserungen erfährt

Jede Security Practice wird nach einer dreistufigen Skala bewertet; gleichzeitig können Risiko bei Untererfüllung, Ziele für Verbesserungen und Nachweis für die Erfüllung objektiv dokumentiert werden

- (Stufe 0 – Startpunkt, keine Aktivitäten erkennbar)
- **Stufe 1** – Grundsätzliches Verständnis besteht, adhoc-Maßnahmen werden gesetzt
- **Stufe 2** – Gezielte Vorgangsweise bei der Umsetzung mit Verbesserung von Wirksamkeit und Wirtschaftlichkeit
- **Stufe 3** – Umfassende Beherrschung der Praxis im angemessenen Umfang

Ein SAMM-Assessment bietet folgende Ergebnisse:

1. GAP-Analyse über den gesamten Prozess
2. Aussagen über Risiken durch fehlende Maßnahmen
3. Planungsgrundlage für iterative Verbesserung
4. Nachweis von Verbesserungen
5. Nachvollziehbare und wiederholbare Messung von Kennzahlen

Wen betrifft Secure Coding im BRZ?



Geht mich das was an?



Sicherheit und damit auch Sicherer Code ist ein Qualitätsmerkmal der Services des BRZ

Daher gibt's auch mehrere Zielgruppen

- Entwickler
 - Verantwortlich für Software (-module)
 - direkte techn. Anwendung von Secure Coding
- Architekten
 - Verantwortlich für Service- und Domainarchitektur
 - definiert Sicherheitsvorgaben nach Sicherheits-Architektur
- Führungskräfte
 - Verantwortlich Prozesse und Ergebnisse
 - Zielvorgaben, -kontrolle und Kommunikation

Informationsangebot

- Ansprechpartner
 - Security System Engineer

- Informationsquellen
 - BRZ Secure Coding Standards V 1.0

 - BRZ Secure Coding Wiki

 - BRZ Sicherheitsarchitektur

Fachwissen – Erfahrung – Verantwortung

Ausbildungsangebote

- Trainings und Workshops
 - Fortsetzung der plattformspezifischen Workshops für Entwickler
 - Aufnahme der SC-Ausbildung in Karrierepfad SW-Entwickler
 - Aufnahme der Ausbildungsmodule Secure Coding und Sicherheitsarchitektur in die Karrierepfade Architekt

- Informationsquellen
 - Vorstellung bei Mitarbeiter-Info-Veranstaltung
 - gezielte Themenpräsentationen bei FK-Meetings

Einer der größten Irrtümer von Sicherheitsverantwortlichen ist der Irrglaube, dass Policies befolgt werden, weil der Chef sie unterschrieben hat

Awareness für Entwickler

- Audits zeigen praxisnahe Schwachstellen auf
- Workshops und Ausbildung steigern das Know-How zur Vermeidung oder Behebung
- Selektive Zielgruppeninformationen fördern die umfassende Akzeptanz
- Solide und aktuelle Informationen, die nur einen Mausklick entfernt sind, werden auch verwendet

**Sobald die Leute drüber reden,
ist es ein Thema.**

**Aber wie bringt man es soweit, dass über ein so trockenes Thema
geredet wird?**

Wir haben es so versucht:



**WAS
wollen sie noch wissen?**

**Sichere Webapplikationen
mit ISO 27001:
Secure Coding Policy**

Johannes MARIEL
10. Juni 2011