Swiss Testing Day

Swiss Testing Day 2009, 18.03.2009

Security Testing mit System

Christoph Baumgartner

CEO OneConsult GmbH & ISECOM Core Team Member

...mit Sicherheit bessere Lösungen

Agenda

Swiss Testing Day

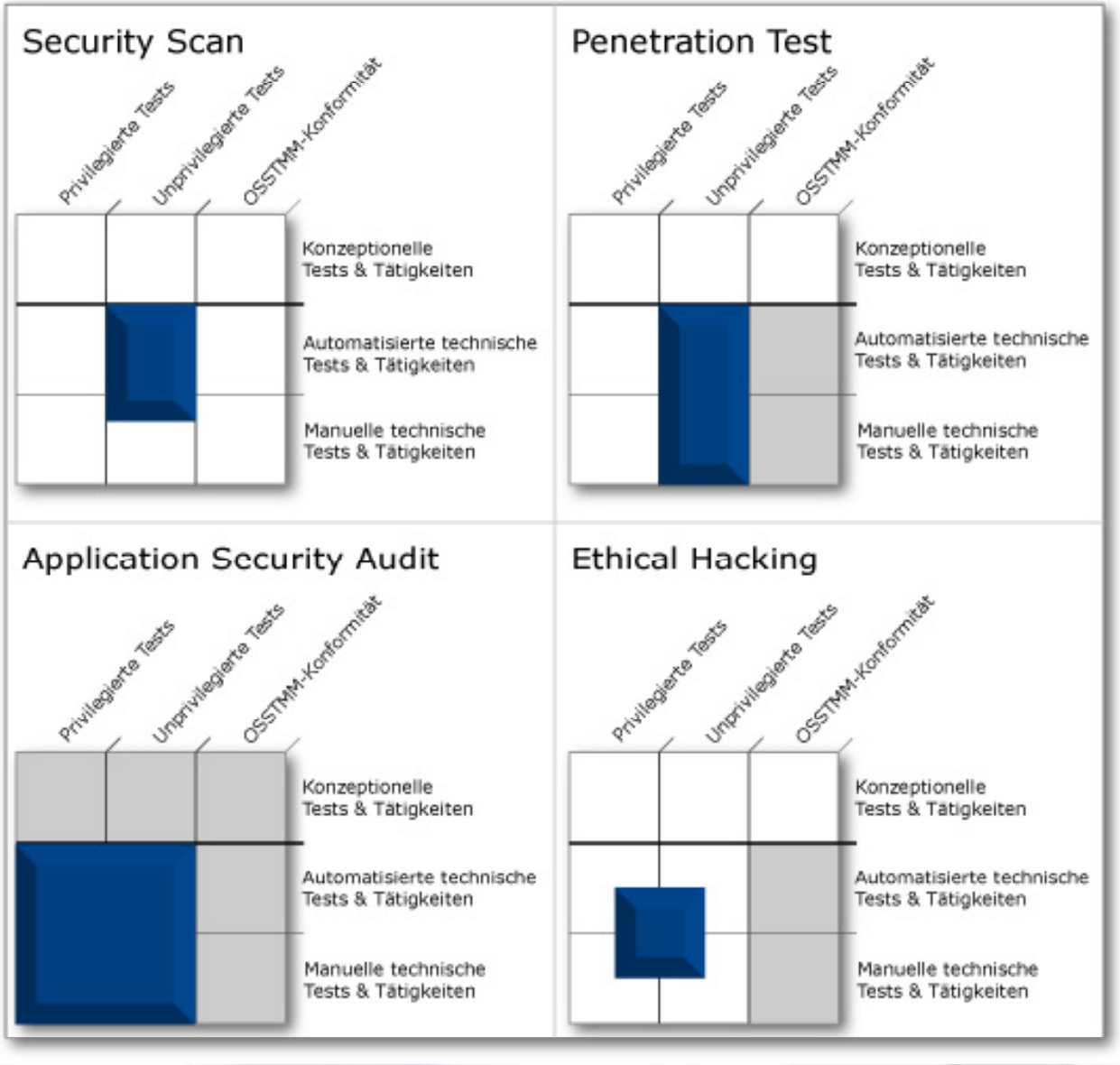
- Testtypen
- OSSTMM
- Aufwandschätzung
- Tipps & Tricks
- Beantwortung von Fragen

Achtung!

Swiss Testing Day

- Jegliche «**Sicherheitsüberprüfungen**» **ohne** explizite **Genehmigung** des Systemeigners und Systembesitzers **sind strafbar** und können mit Busse und/oder Haft bestraft werden.
- Deutscher «**Hackerparagraph**» **stellt** selbst das **Bereitstellen von Software**, welche für das Hacking missbraucht werden *könnte*, **unter Strafe**.

Typen technischer Audits



Charakteristika

Swiss Testing Day

Merkmal	Security Scan	Penetra-tion Test	Application Security Audit	Ethical Hacking
Suche nach Software (Betriebssystem und Applikationen)-basierten Sicherheitslücken	•	•	•	-
Suche nach Design-basierten Sicherheitslücken	-	-	•	•
Unprivilegierte Tests (ohne Kenntnis gültiger Zugriffsinformationen)	•	•	•	•
Privilegierte Tests (mit Kenntnis gültiger Zugriffsinformationen)	-	-	•	•
Automatisierte Suche nach Sicherheitslücken	•	•	•	•
Manuelle Suche nach Sicherheitslücken	-	•	•	•
Einsatz mehrerer Tools mit ähnlicher Funktionalität	-	•	•	•
Nicht-intrusive Verifikation von Sicherheitslücken	•	•	•	•
Intrusive Verifikation von Sicherheitslücken	-	•	•	•
Gezielte Modifikation des Untersuchungsobjektes (z.B. User Accounts, Datenbankinhalte, Dateisystem, etc.)	-	-	-	•
Technische Massnahmenvorschläge	•	•	•	•
Organisatorische Massnahmenvorschläge	-	•	•	-
Dokumentation	•	•	•	•

• = erfüllt, - = nicht erfüllt

Untersuchungsobjekte

- **Computer-Netzwerke**
  - Externe Netze / DMZ (z.B. Firewall, Web-, FTP-, Mail-, DNS-, Terminalserver und weitere Netzwerkkomponenten) aus externer oder interner Sicht
  - LAN / WAN (z.B. Clients, Server, Peripheriegeräte und Netzwerkkomponenten)
  - Wireless LAN, Bluetooth, Infrarot, GSM, UMTS, etc.
- **Kommunikation** (inkl. VoIP, Fax, Modem und Mobiltelefone, E-mail, etc.)
- **Applikationen** (z.B. n-Tier-Applikationen wie SAP, CRM und Branchenlösungen)
- (kombinierte) **Systeme** (z.B. verteilter Schutz vor Malware)

Nutzen

- **Qualitätssicherung** dank (unabhängiger) IT Security-Analyse
- **Compliancy**-Nachweis bezüglich gesetzlicher Rahmenbedingungen und Vorgaben
- **Prävention** ermöglicht direkte und indirekte Kosteneinsparungen (in der Zukunft)
- **Awareness** Building auf allen Stufen und Know-how Transfer
- **Argumentationsgrundlage** für zukünftige IT Security-Projekte bzw. -Aktivitäten

Problemkreis Security Audit

Swiss Testing Day

- **Fach-** und **Sozialkompetenz** der Tester und anderer am Projekt beteiligter Mitarbeiter
- **Nachvollziehbarkeit** und **Vergleichbarkeit**
- **Umsetzbarkeit** vs. **Zweckmässigkeit**
- **Compliance** zu
  - **Gesetzen**
  - **Standards**
  - (Firmen-)internen **Vorgaben**

OSSTMM in a Nutshell 1

Swiss Testing Day

- Abkürzung von «**Open Source Security Testing Methodology Manual**»
- **Erstausgabe 2000/2001**, entwickelt und kontinuierlich weiterentwickelt unter der Leitung **von ISECOM** (Institute for SECurity and Open Methodologies), http://www.osstmm.org
- **Offene** und **frei verfügbare Methode** zur **Planung**, **Durchführung** und **Dokumentation** (Zielgruppe: IT Spezialisten) von (technischen) **Security Audits**

OSSTMM in a Nutshell 2

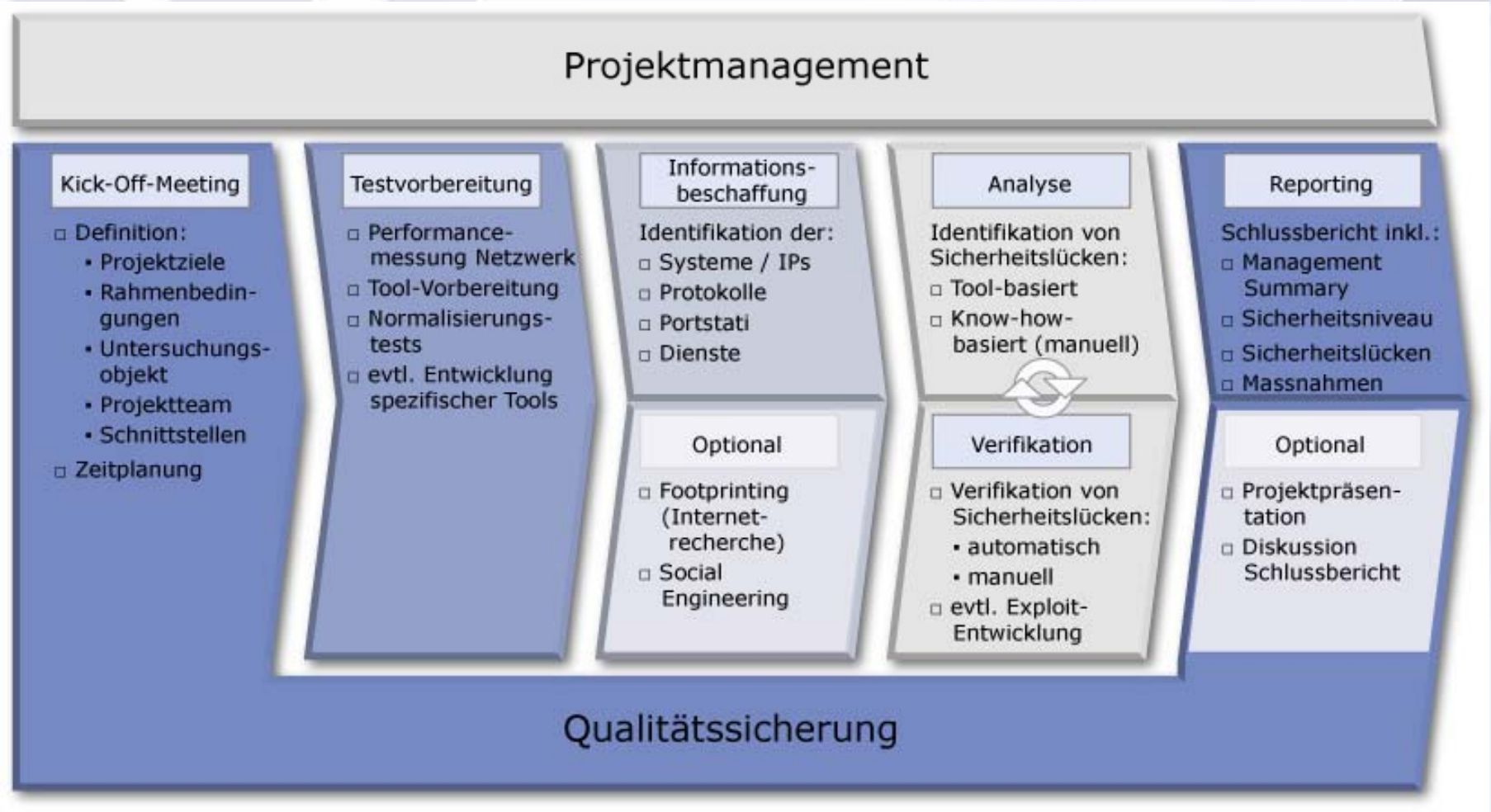
Swiss Testing Day

- **Sicherheitsniveau als Zahlenwert** (Risk Assessment Value)
- **Verhaltenskodex** für Tester (Rules of Engagement)
- **Compliant** zu **ISO/IEC 2700x**, **ITIL**, **BSI Standard 100-1/4** (vom BSI empfohlen), **SOx**, **Basel II**, etc.
- **Zertifizierungsmöglichkeiten**

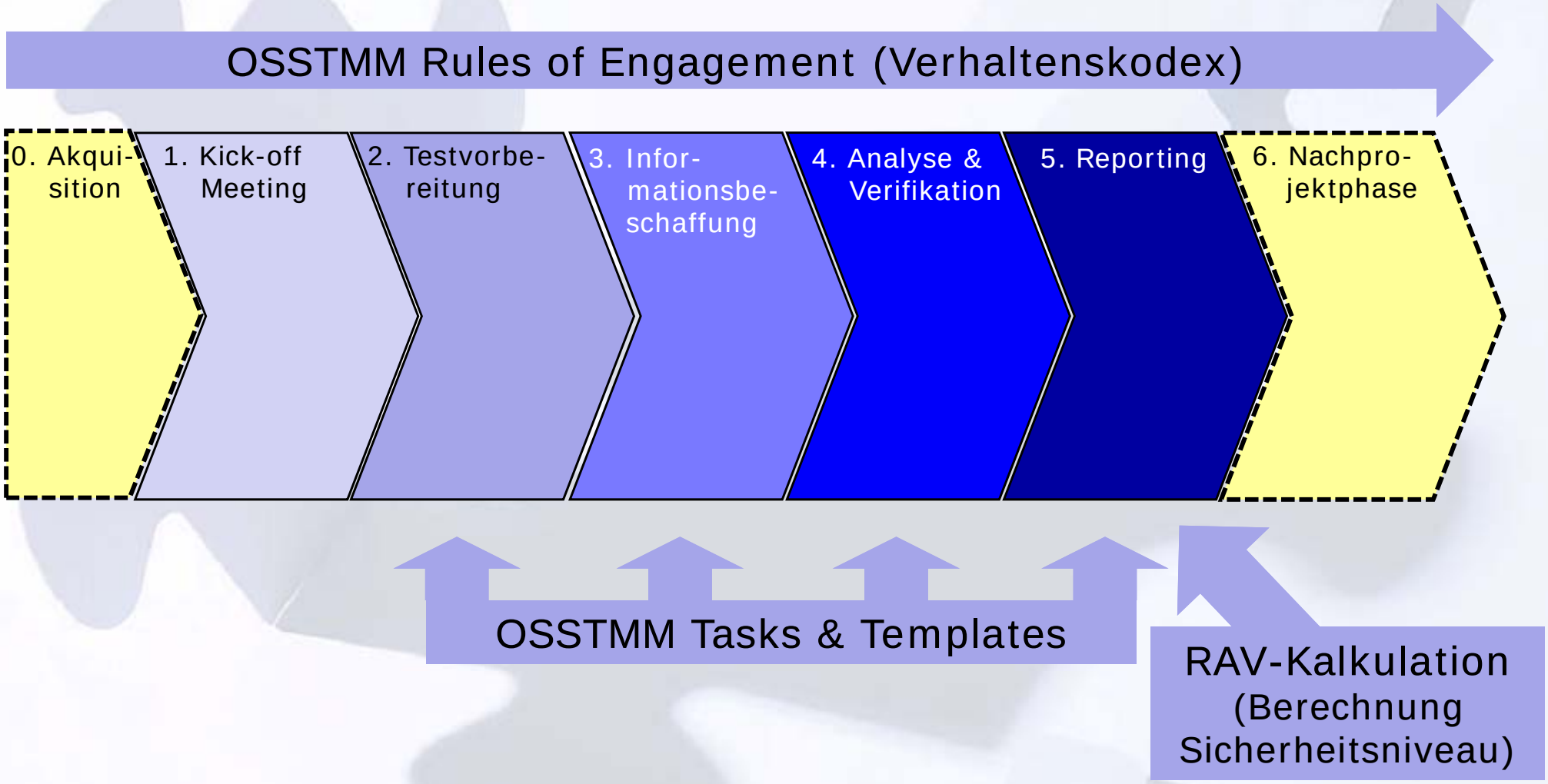
Projektphasen: Penetration Test

Swiss Testing Day

Intensive technische Sicherheitsüberprüfung (Perspektive Angreifer-Skill Level: «Hacker/Cracker»)



OSSTMM-Projektphasen-Abdeckung



Risk Assessment Value (RAV)

Swiss Testing Day

- Sicherheitsniveau als Zahlenwert
- Mathematische Herleitung
- Herleitung nicht umkehrbar

Voraussetzung für

- Nachvollziehbarkeit
- Vergleichbarkeit
- Trendanalysen

OPSEC	
Visibility	7
Access	7
Trust	4

Class A	CONTROLS	Missing
Authentication	13	5
Indemnification	0	18
Resistance	13	5
Subjugation	0	18
Continuity	4	14
Class B		
Non-Repudiation	0	18
Confidentiality	3	15
Privacy	3	15
Integrity	3	15
Alarm	3	15

	LIMITATIONS	Total
Vulnerabilities	1	3.19312
Weaknesses	2	5.78419
Concerns	17	50.69861
Exposures	6	11.07059
Anomalies	1	2.82607

CALCULATION WORKSHEET	
Porosity	18
Total Controls	42
Class A Controls	30
Class B Controls	12
Whole Coverage	23.33%
True Coverage	23.33%
True Coverage A	16.67%
True Coverage B	6.67%
Missing Controls	138
Missing Controls A	60
Missing Controls B	78
Coverage Missing	76.67%
Total # Limitations	27
Limitations Value	73.57258781

Vulnerability	3.19312460
Weakness	2.89209460
Concern	2.98227123
Exposure	1.84509804
Anomaly	2.82607480

	RAV TOTALS
OPSEC	10.59836953
CONTROLS	6.88685652
LIMITATIONS	14.95194934
Δ	-18.66346236

RAV	81.16158668

Compliance des OSSTMM

Swiss Testing Day

- **SOx** (Sarbanes-Oxley Act) 302/404
- **Basel II**
- **ISO/IEC 2700x**
- **BSI Standard 100-1/4** (ehemals BSI IT Grundschutzhandbuch): Explizit vom Bundesamt für Sicherheit in der Informationstechnik BSI für die Durchführung technischer Audits empfohlen
- **ITIL** (IT Information Library)
- **SET** (Secure Electronic Transactions)
- **FISCAM** (Federal Information System Control Audit Manual)
- etc.

OSSTMM-Fazit

Swiss Testing Day

- **Quantifizierbarkeit – Zahlenwerte** statt «Bauchgefühl»
- **Konsistenz – Replizierbarkeit der Ergebnisse**
- basierend **auf Leistung von Tester** und Analyst anstelle von «Brands» oder Tools
- **Vollständigkeit** und **Genauigkeit**
- **Gesetzes-** und **Standardkonformität**
- **Zertifizierungsmöglichkeiten**

➡ **OSSTMM: der De-facto-Standard für technische Security Audits**

Aufwandschätzung

Swiss Testing Day

Testtyp	Durch-führung	OSSTMM-konform	Aufwandschätzung in Personentagen (PT)	
			Tests	Dokumen-tation
Security Scan DMZ	Remote (=via Internet)	Nein	10-15 Systeme pro PT	
Security Scan LAN	Vor-Ort	Nein	25-50 Systeme pro PT	0.5 x Test-aufwand (Mind. 2 PT)
Penetration Test DMZ oder LAN	Remote oder Vor-Ort	Nein	0.5 PT x Anzahl Systeme	
		Ja	0.6 PT x Anzahl Systeme	
Web Application Security Audit (inkl. privilegierte Tests, aber ohne Code Review)	Remote	Ja	Mind. 3 PT pro Applikation	

Tipps & Tricks

- Genaue **Projektplanung** = klare Aufträge und Rahmenbedingungen
- **Vorlaufzeit**: Mindestens 3 Arbeitstage zwischen Kick-Off Meeting und Testbeginn einkalkulieren
- «**Moving Targets**» verhindern
- **Tools** vom Auftraggeber **absegnen** lassen
- **Source IP-Adressen** bei Remote Tests **bekanntgeben**
- **Tägliche Kommunikation** mit Auftraggeber
- **Wissenstransfer** in Richtung Auftraggeber anstreben
- Nach Möglichkeit **Patchphasen** und allfällige **Nachkontrollen einkalkulieren**

→ **Teamwork** mit dem Team des Auftraggebers = **gegenseitiges Vertrauensverhältnis**

Fragen?

Swiss Testing Day

Christoph Baumgartner

MSc UZH, OPST
CEO

baumgartner@oneconsult.com

+41 43 377 22 22

OneConsult®
IT Security & Strategic Consulting

Schweiz

Hauptsitz:

OneConsult GmbH
Schützenstrasse 1
8800 Thalwil
Schweiz

www.oneconsult.com
info@oneconsult.com
Tel. +41 43 377 22 22
Fax +41 43 377 22 77

Office Bern:

OneConsult GmbH
Aarstrasse 98
3005 Bern
Schweiz

www.oneconsult.com
info@oneconsult.com
Tel. +41 31 318 25 25
Fax +41 31 318 25 35

Deutschland

OneConsult Deutschland GmbH
Parkstraße 2
89231 Neu-Ulm
Deutschland

www.oneconsult.de
info@oneconsult.de
Tel. +49 731 977 191 70
Fax +49 731 977 191 99

Frankreich

Succursale de OneConsult GmbH
Immeuble Le Danica B
21 avenue Georges Pompidou
69486 Lyon cedex 03
France

www.oneconsult.fr
info@oneconsult.fr
Tel. +33 4 72 91 30 31
Fax +33 4 72 91 30 30

Österreich

Niederlassung der
OneConsult GmbH
Twin Tower
Wienerbergstraße 11/12A
1100 Wien
Österreich

www.oneconsult.at
info@oneconsult.at
Tel. +43 1 99460 64 69
Fax +43 1 99460 50 00