Security Audits nach OSSTMM

Transparenz und Vergleichbarkeit dank Normenkonformität

SWISS INFOSEC 2006, 25.10.06

Christoph Baumgartner

Agenda

- Herausforderung Security Audit
- Perfect Security
- OSSTMM in a Nutshell
- Aufbau
- Risikotypen
- Security Metrics
- Compliance
- Zertifizierungsmöglichkeiten
- Aufwandschätzung
- Fazit
- Beantwortung von Fragen

Herausforderung Security Audit

- **Fach-** und **Sozialkompetenz** der Tester und der am Projekt beteiligten Mitarbeiter
- **Vergleichbarkeit** und **Nachvollziehbarkeit** von
  - Offerten
  - Vorgehen (Sinnhaftigkeit und Vollständigkeit)
  - Resultaten und Dokumentationen
- **Umsetzbarkeit** und **Zweckmässigkeit** der Massnahmen(vorschläge)
- **Compliance** zu Gesetzen, Standards und Vorgaben erwünscht, aber:
  - Rudimentäre Behandlung von technischen Audits in Standards, Frameworks und Guidelines (ISO/IEC 27001/17799 (inkl. ITIL), COBIT, IT GSHB, etc.)
  - Was sicherzustellen ist, aber nicht wie

Perfect Security: Behauptung

Perfect Security: Nachweis

OSSTMM in a Nutshell

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

  von **technischen Security Audits**
- **Verhaltenskodex** für Tester
- **Compliant** zu **ISO/IEC 17799/27001**, **ITIL**, **GSHB**, **SOX**, etc.
- **Zertifizierungsmöglichkeit** (Personen, Anbieter und Projekte) durch ISECOM

Aufbau 1

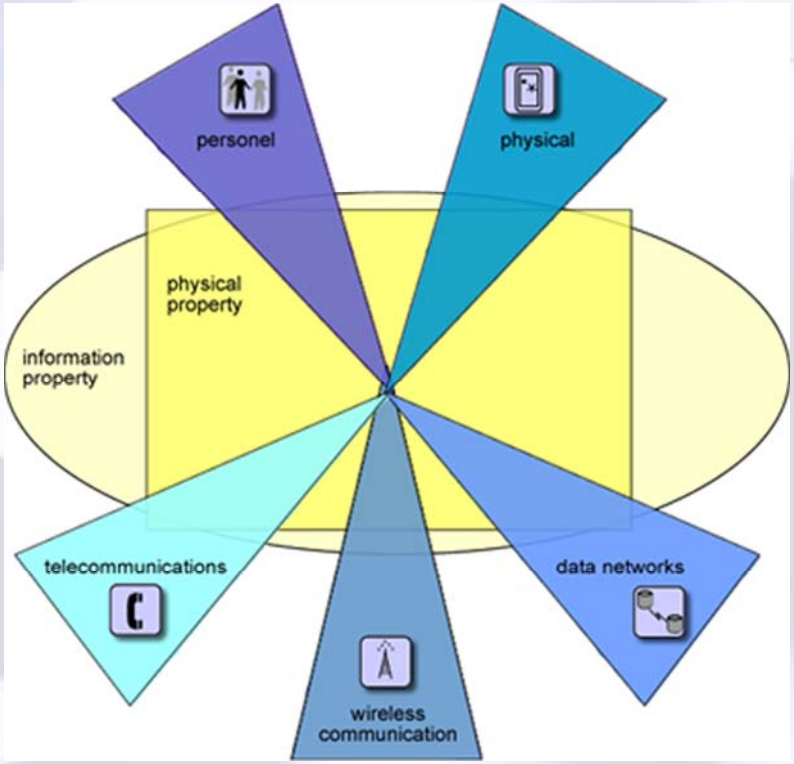
OSSTMM besteht aus

- der **Methodologie**
- den «**Security Metrics**» (Risk Assessment Values, RAVs)
- den **Formularvorschlägen** (welche die Minimalanforderungen an den Informationsgehalt / Dokumentationsgrad eines OSSTMM-konformen Tests definieren bzw. darstellen)

Aufbau 2

Methodologie ist **hierarchisch gegliedert**

- Security Map: Besteht aus sich überlappenden «**Channels**» (Sektionen), welche **sämtliche Sichten** der Informations-, System-, Kommunikations-, Prozesssicherheit und der physischen Sicherheit **abdecken**



- **Channels** sind wiederum **in Module gegliedert**, welche in Form von verschiedenen Tasks durchlaufen werden

Risikotypen

Risikotyp	Beschreibung
Vulnerability (Verwund-barkeit)	Eine Schwachstelle im Sicherheitsmechanismus, womit privilegierter Zugang zu einer Infrastruktur erlangt werden kann Beispiel: Anfälligkeit auf eine «Buffer Overflow»-Attacke
Weakness (Schwach-stelle)	Eine Schwachstelle in der Plattform, auf welcher der Sicherheitsmechanismus aufbaut Beispiel: Tür-Alarm, der nicht ertönt, wenn die Türe länger geöffnet bleibt
Concern (Bedenken)	Keine direkte Bedrohung, entspricht jedoch nicht den Regeln der «best practices» Beispiel: aktive, nicht benötigte Dienste
Exposure (Informations-abfluss)	Preisgabe von sensitiven Informationen über unsichere Kanäle Beispiel: interne IP Adressen wird im E-Mail Header kommuniziert
Anomaly (Anomalie)	Unbekannte im System, welche der Tester mit den ihm zur Verfügung stehenden Informationen im vorgegebenen Zeitrahmen nicht identifizieren konnte Beispiel: nicht erwartete Antwort eines Routers

Security Metrics: RAV

«**Risk Assessment Value**» (RAV) stellt Sicherheitsniveau des Untersuchungsobjekts als Zahl dar und wird anhand dreier Variablen ermittelt:

- **Operative Sicherheit** (OpSec): bewertet Sichtbarkeit, Vertrauensstellungen und Zugriffspunkte (Interaktions-möglichkeiten)
- **Kontrollausgleich** (Loss Control (LC)): berücksichtigt implementierte Sicherheitsmechanismen und hat positiven Einfluss («Bonuspunkte») auf RAV
- **Aktuelle Sicherheit** (ActSec): detektierte Risiken («Security Limitations») werden hinsichtlich ihres Bedrohungspotentials gewichtet

Security Metrics: RAV-Berechnung (OSSTMM 3.0)

Input:

- Informationen zum Untersuchungsobjekt
- Testergebnisse

$$OpSec_{base} = 100 - \frac{OpSec_{sum}}{(Scope + OpSec_{sum})}$$

$$LC_{base} = Scope \times \frac{LC_{sum} \times 0.1}{(Scope + OpSec_{sum})}$$

$$ActSec_{base} = \frac{ActSec_{sum}}{Scope}$$

$$RAV = OpSec_{base} - \left(\frac{OpSec_{base} \times ActSec_{base}}{100}\right) + \left(\frac{OpSec_{sum}}{Scope + OpSec_{sum}} \times \frac{LC_{base}}{100}\right)$$

Output:

- Sicherheitsniveau als Prozentwert

RAV	97.7609114

	Scope		Loss Controls
Scope	28	Authentication	6
		Non-Repudiation	3
	Operational Security	Confidentiality	0
Visibility	27	Privacy	0
Access	33	Indemnification	1
Trust	19	Integrity	0
Op Sec Δ	-79	Safety	10
Op Sec Total	79	Usability	14
Op Sec % of Scope	97.17857143	Continuity	3
		Alarm	28
		Loss Controls Δ	6.5
		Loss Controls Total	65
		Loss Controls % of Op Sec	8.227848101
		Loss Controls % of Scope	23.21428571

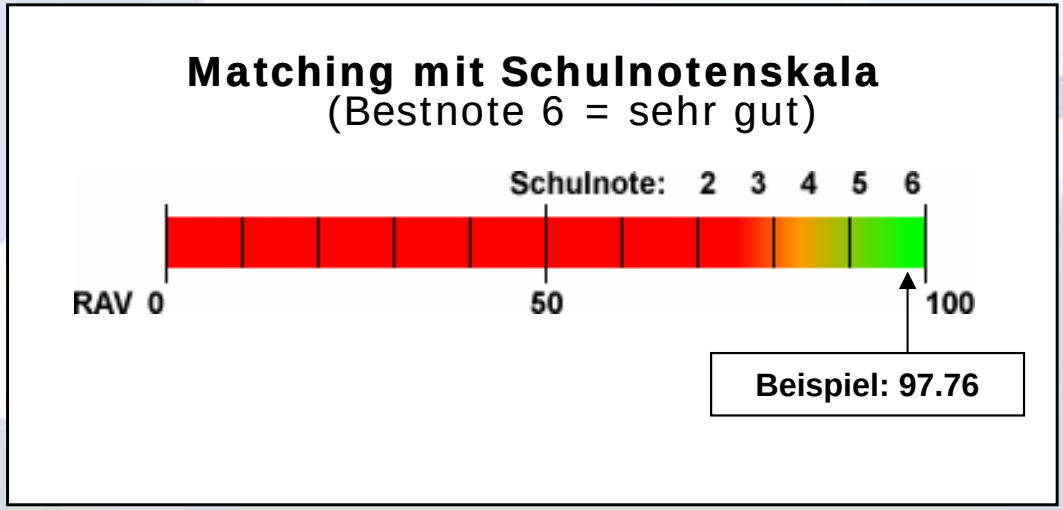
Security Limitations Values

	Verified	Identified
Vulnerability	1.15053763	1.16237705
Weakness	1.13869822	1.15041580
Concern	1.12698063	1.13857764
Exposure	1.11538362	1.12686129
Anomaly	1.10390595	1.11526552

	verified	identified	total
Vulnerabilities	3	0	3.451612903
Weaknesses	8	0	9.109585739
Concerns	3	0	3.380941896
Exposures	22	0	24.53843973
Anomalies	2	0	2.207811908
		Security Limitations Δ:	42.68839218
		Security Limitations Total:	1.52458543
		Actual Delta:	-115.18839218
		Actual Security:	99.25975415

RAV-Beurteilung

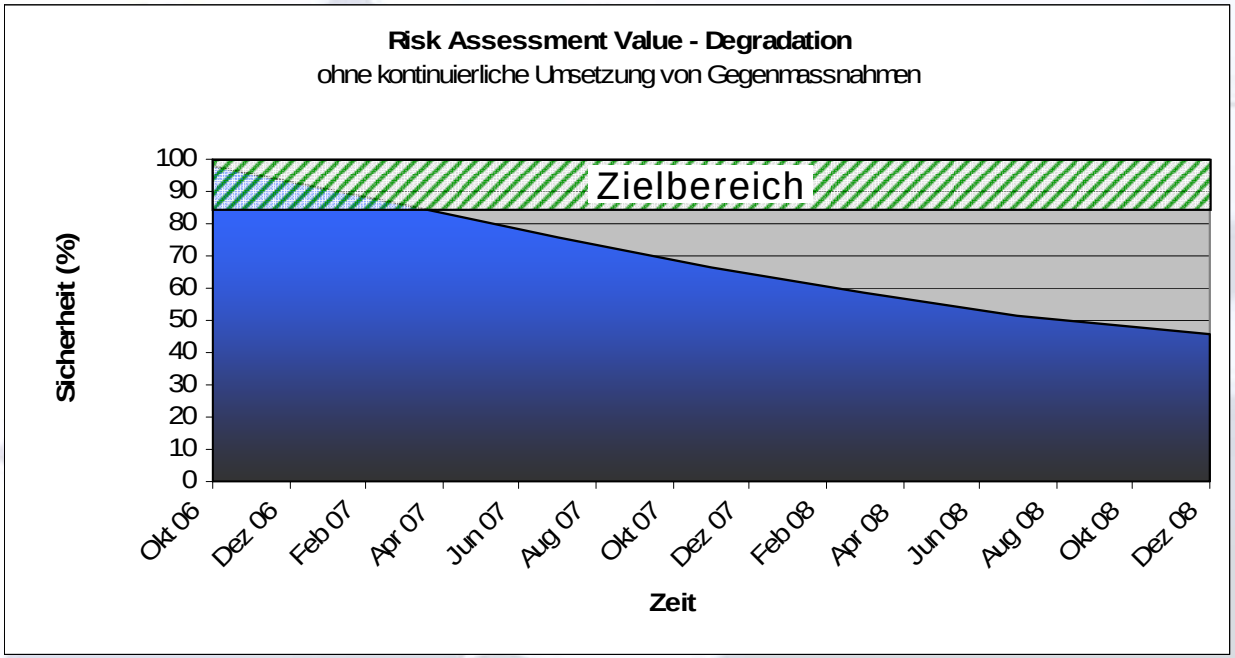
Dieses Matching mit der Schulnotenskala **ist nicht Bestandteil des OSSTMM**, sondern wird von OneConsult zur Veranschaulichung angewendet.



Faustregel für Remote-Tests:

- RAV zwischen 90 und 95 = gut
- RAV über 95 = sehr gut (➡ Zielbereich für Unternehmen/Organisationen mit hohem Schutzbedarf)

Verschlechterung des Sicherheitsniveaus



Degradation	
Cycle (days)	128
Degradation (%)	12
Date:	25.10.2006

Helper table for degradation	
25.10.2006	97.76091140
02.03.2007	86.02960203
08.07.2007	75.70604978
13.11.2007	66.62132381
20.03.2008	58.62676495
26.07.2008	51.59155316
01.12.2008	45.40056678

Bemerkungen:

- Laufend werden
  - neue Schwachstellen entdeckt und neue Angriffsmethoden entwickelt
  - Um-Systeme verändert
  - Konfigurationen modifiziert
- Falls keine Massnahmen (z.B. Security Patching) umgesetzt werden, verschlechtert sich das Sicherheitsniveau im Lauf der Zeit

Compliance

Kompatibel hinsichtlich der **Durchführung von technischen Security Audits** mit diversen Gesetzen und «Best Practices» (bis OSSTMM Version 2.x nur für Remote Tests):

- SOX (Sarbanes-Oxley Act) 302/404
- Basel II
- ISO/IEC 17799 (Code of Practice)
- IT GSHB (BSI IT Grundschutzhandbuch)
- ITIL (IT Information Library)
- SET (Secure Electronic Transactions)
- FISCAM (Federal Information System Control Audit Manual)
- etc.

Zertifizierungsmöglichkeiten

Offizielle ISECOM-Zertifizierungen nach OSSTMM:

- Personenbezogen
  - OPSE (OSSTMM Professional Security Expert): belegt, dass der/die Zertifizierte genaue theoretische Kenntnisse des OSSTMMs (wie, warum und wann das OSSTMM angewandt wird) und bezüglich Projektplanung hat
  - OPST (OSSTMM Professional Security Tester): belegt, dass der/die Zertifizierte über die nötigen Fähigkeiten verfügt, um als professioneller Security Tester nach OSSTMM zu arbeiten
  - OPSA (OSSTMM Professional Security Analyst): belegt, dass der/die Zertifizierte über die nötigen Fähigkeiten verfügt, Testresultate richtig zu interpretieren, den RAV zu berechnen und Testerteams zu koordinieren
- Anbieterbezogen: «ISECOM Licensed Auditor» (mehrere Level): von ISECOM regelmässig überprüfte Qualität http://www.isecom.org/auditors.shtml
- Projektbezogen (Review durch ISECOM)

Aufwandschätzung

Diese Aufwandschätzung bezieht sich auf das reine OSSTMM-konforme Remote-Testing der Qualitätsstufe **Penetration Test** (via max. 15 Hops und Breitbandanschluss), **exkl. Dokumentationsaufwand**!

Typ (aus Sicht Tester)	**Beispiele**	**Aufwandschätzung** (pro System)
Einfaches System	▫ DNS-Server ▫ Router ▫ Switch	2 - 4 h
Mittel-komplexes System	▫ Web-Server ▫ Mail-Server ▫ DB-Server	4 - 8 h
Hoch-komplexes System	▫ Firewall ▫ IDS ▫ VPN-Gateway	6 - 12 h

Fazit

- Anforderungsgerechte Beurteilung des Sicherheitsniveaus
- Quantifizierbarkeit – Zahlenwerte statt «Bauchgefühl» ermöglichen den Vergleich
- Konsistenz – Replizierbarkeit der Ergebnisse
- Gültigkeit über das «Jetzt» hinaus – proaktives statt reaktives Handeln
- Basierend auf Leistung von Tester bzw. Analyst statt auf «Brands» oder Tools
- Vollständigkeit und Genauigkeit
- Gesetzes- und Standardkonformität
- Zertifizierungsmöglichkeit (Personen und Projekt)

Echte Alternative zu «Methoden Marke Eigenbau»

Besten Dank...

...für Ihre Aufmerksamkeit!

Christoph Baumgartner
lic. oec. publ., OPST
CEO

info@oneconsult.com
+41 79 421 20 01

OneConsult®
IT Security & Strategic Consulting

Hauptsitz:

OneConsult GmbH
Zürcherstrasse 73
8800 Thalwil
Schweiz

http://www.oneconsult.com
info@oneconsult.com
Tel. +41 43 443 52 52
Fax +41 43 443 52 62

Filiale Bern:

OneConsult GmbH
Aarstrasse 98
3005 Bern
Schweiz

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

Vertretung Deutschland:

Vertretung der OneConsult GmbH
in Deutschland
Parkstraße 2
89231 Neu-Ulm
Deutschland

http://www.oneconsult.com
info-de@oneconsult.com
Tel. +49 731 977 191 70
Fax +49 731 977 191 99