Security Testing nach OSSTMM

Christoph Baumgartner

HIS-Roundtable: Einhalten von Regulationen und Vorgaben (Compliances) in der IT, 19.01.2006

…mit Sicherheit bessere Lösungen

Agenda

- Probleme im Zusammenhang mit technischen Audits
- OSSTMM (Open Source Security Testing Methodology Manual)
- Aufbau
- OSSTMM-Typen von Sicherheitslücken
- Security Metrics (Risk Assessment Value (RAV))
- Zeitabhängige Verschlechterung des Sicherheitsniveaus
- Compliancy
- Zertifizierungsmöglichkeiten
- Nutzen
- Kosten und Aufwand OSSTMM-konformer Security Tests
- Beantwortung von Fragen
- Diverse Beilagen (Typen und Unterscheidungsmerkmale technischer Sicherheitsüberprüfungen)

Probleme im Zusammenhang mit technischen Audits

- **Fach-** und **Sozialkompetenz** der Tester und der am Projekt beteiligten Mitarbeiter
- **Vergleichbarkeit** und **Nachvollziehbar** von
  - Offerten
  - Vorgehen (Sinnhaftigkeit und Vollständigkeit)
  - Resultaten und Dokumentationen
- **Compliancy** zu Gesetzen, Standards und Vorgaben erwünscht, aber:
  - Nur rudimentäre Behandlung von technischen Audits in Standards (z.B. ISO/IEC 27001/17799)
  - Keine Checklisten oder Guidelines verfügbar

OSSTMM

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

  von technischen Sicherheitsüberprüfungen
- **Verhaltenskodex für Tester**

Aufbau

- 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 beinhalten bzw. darstellen)
- Methodologie ist **hierarchisch gegliedert**
  - 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

OSSTMM-Typen von Sicherheitslücken

Typ	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 wie fingerd
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 stehen-den Informationen im vorgegebenen Zeitrahmen nicht identifizieren konnte. Beispiel: nicht erwartete Antwort eines Routers

Security Metrics (Risk Assessment Value (RAV)), 1. Teil

- «Risk Assessment Value» (RAV) stellt **Sicherheits-niveau 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 (Risk Assessment Value (RAV)), 2. Teil

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

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

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

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

	Scope		Loss Controls
Scope	10	Authentication	5
		Non-Repudiation	2
	Operational Security	Confidentiality	2
Visibility	10	Privacy	0
Access	14	Indemnification	1
Trust	1	Integrity	0
Op Sec Δ	-25	Safety	2
Op Sec Total	25	Usability	1
Op Sec % of Scope	97.5	Continuity	2
		Alarm	1
		Loss Controls Δ	1.6
		Loss Controls Total	16
		Loss Controls % of Op Sec	6.4
		Loss Controls % of Scope	16

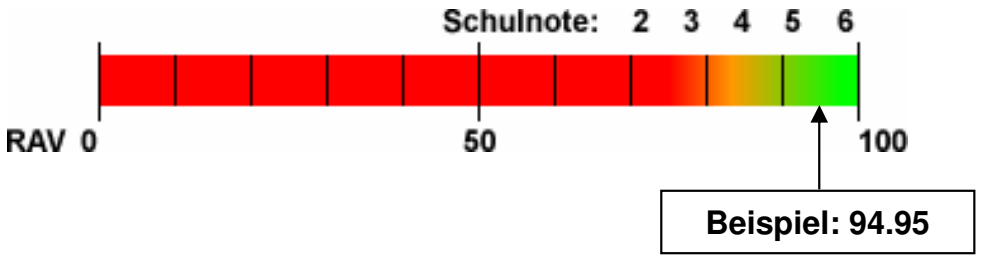
Security Limitations Values

	Verified	Identified
Vulnerability	1.34615385	1.35996055
Weakness	1.33234714	1.34601224
Concern	1.31868204	1.33220699
Exposure	1.30515710	1.31854332
Anomaly	1.29177087	1.30501980

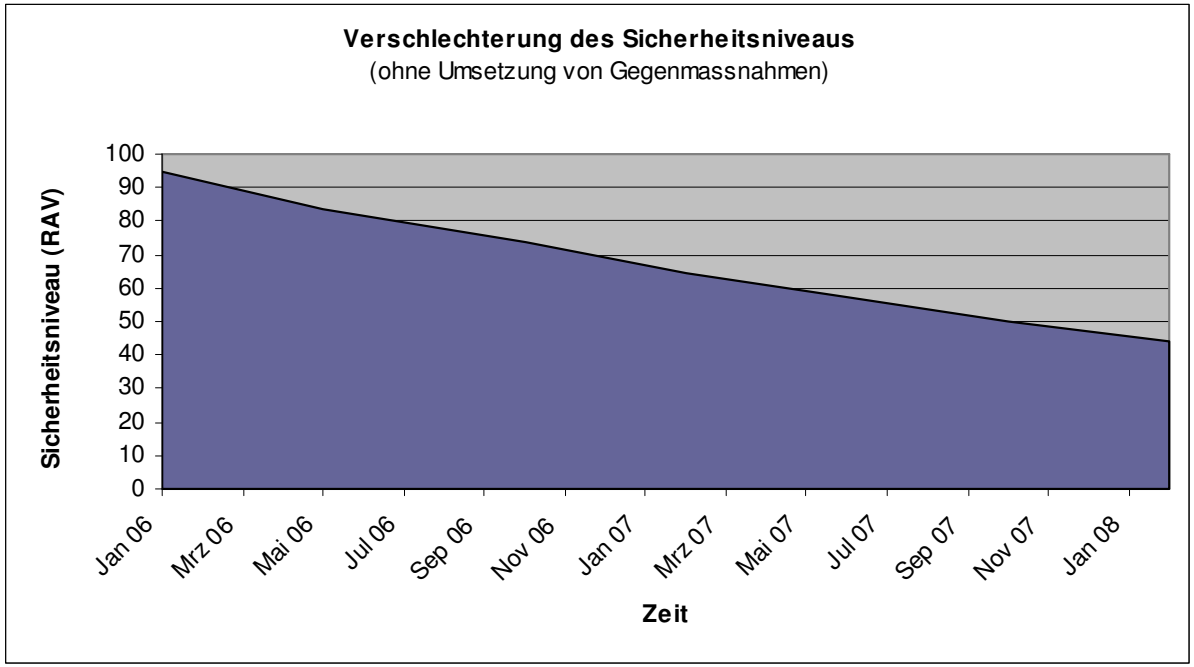
	verified	identified	total
Vulnerabilities	8	0	10.76923077
Weaknesses	7	0	9.32642998
Concerns	8	0	10.54945633
Exposures	10	0	13.05157097
Anomalies	0	0	0
		Security Limitations Δ:	43.69668805
		Security Limitations Total:	4.36966881
		Actual Delta:	-67.09668805
		Actual Security:	99.72230331

RAV Calculation	
Opsec base	99.28571429
LC base	0.457142857
ActSec base	4.369668805
RAV	94.95052271

Nicht Bestandteil des OSSTMM



Zeitabhängige Verschlechterung des Sicherheitsniveaus



Degradation	
Cycle (days)	128
Degradation (%)	12
Date:	19.01.2006

Helper table for degradation	
19.01.2006	94.95052271
27.05.2006	83.55645998
02.10.2006	73.52968478
07.02.2007	64.70612261
15.06.2007	56.94138790
21.10.2007	50.10842135
26.02.2008	44.09541079

Bemerkungen:

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

Compliancy

Kompatibel hinsichtlich der **Durchführung von technischen Sicherheitsüberprüfungen** zu diversen Gesetzen und «Best Practices» (bis Version 2.1 nur für Remote Tests):

- SOX (Sarbanes-Oxley Act)
- 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.

Die komplette Liste kann dem OSSTMM entnommen werden.

Zertifizierungsmöglichkeiten

Zertifizierungen, welche (unabhängig voneinander) die Listung als **offizielle OSSTMM Auditoren** auf der OSSTMM/ISECOM-Website ermöglichen:

- OPSE (**OSSTMM Professional Security Expert**): belegt, dass der/die Zertifizierte genaue theoretische Kenntnisse des OSSTMMs hat (wie, warum und wann das OSSTMM angewandt wird)

- 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 und Testerteams zu koordinieren

Nutzen

- **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»
- **Vollständigkeit** und **Genauigkeit**
- **Gesetzes-** und **Standardkonformität**
- **Zertifizierungsmöglichkeit** (Tester und Projekt)

Kosten und Aufwand OSSTMM-konformer Security Tests

- Externe Kosten (seriöse Durchführung, Qualitätslevel «Penetration Test»):
  - Minimum: CHF 8`000
  - Maximum: offen
  - Durchschnitt: CHF 15`000 – 30`000
- Zeitaufwand seitens Auftraggeber bzw. Betreuer:
  - Minimum: 30 Minuten pro Testtag
  - Besser: Bereitschaftsdienst Kontaktperson und Systemadministratoren während der Durchführung aller Tests
  - Optional: gemeinsame Arbeit mit Auftragnehmer
  - Zusätzlich: Umsetzung Massnahmen

Beantwortung von Fragen

Besten Dank für Ihr Interesse!
Gerne beantworte ich Ihre Fragen:

Christoph Baumgartner

lic. oec. publ., OPST
CEO / Senior Consultant

info@oneconsult.com
+41 (0)79 421 20 01

OneConsult GmbH
Zürcherstrasse 73
8800 Thalwil
Schweiz

http://www.oneconsult.com
info@oneconsult.com
Tel. +41 (0)43 443 52 52
Fax +41 (0)43 443 52 62

…mit Sicherheit bessere Lösungen

Beilage: Definitionen Angreifertypen

- Ein **User** ist ein Anwender, welcher über das nötige Wissen verfügt, um die **Informatikmittel funktionsgerecht zu nutzen**.
- Als «**Skript Kiddie**» wird eine Person bezeichnet, welche über (relativ) **wenig Computer- und Netzwerkfachwissen** verfügt, aber unbedarft (vollautomatisierte) **Hackertools einsetzt**.
- Ein «**Hacker**»/«**Cracker**» **bricht ohne Erlaubnis** des Systemeigners meist via Computernetze **in Computersysteme ein** oder knackt das Lizenzsystem von Computerprogrammen. Dafür umgeht er bewusst Sicherheitsmechanismen. Die Beweggründe sind Ehrgeiz, möglicher finanzieller Profit, Geltungssucht, Idealismus oder Zerstörungswille.
- Ein «**Ethical Hacker**» ist ein Computer- und Netzwerkspezialist, welcher **im Auftrag des Systemeigners** nach **Systemverwundbarkeiten sucht**, welche ein «Hacker»/«Cracker» ausnutzen könnte.
- Ein «**Social Engineer**» versucht mittels Ausnutzens menschlicher Schwächen an vertrauliche Daten zu gelangen.

Beilage: Typen technischer Sicherheitsüberprüfungen

Bemerkungen:

- Terminologie angelehnt an ISECOM - OSSTMM (Open Source Security Testing Methodology Manual).
- Der **Application Security Audit** kann je nach Auftrag sowohl technische als auch konzeptionell/organisatorische Elemente beinhalten.

Beilage: Merkmale technischer Sicherheitsüberprüfungen

Merkmal	1 Vulnerability Scan	2 Security Scan	3 Penetration Test	4 Ethical Hacking
Aufspüren von Sicherheitslücken	voll-auto-matisiert	voll-auto-matisiert	teil-auto-matisiert / manuell	teil-auto-matisiert / manuell
Einsatz mehrerer Tools mit ähnlicher Funktionalität	nein	nein	ja	ja
manuelle Verifikation von vermeintlichen Sicherheits-lücken	nein	ja	ja	ja
Ausnützen von Sicherheitslücken	nein	nein	ja	ja
Modifikation des Untersuchungsobjekts	nein	nein	nein	ja
Ansatz	direkt	direkt	direkt	direkt / indirekt
Typ(en) der empfohlenen Massnahmen	technisch	technisch	technisch / organisatorisch	technisch / organisatorisch