

# Sicherheit wird messbar

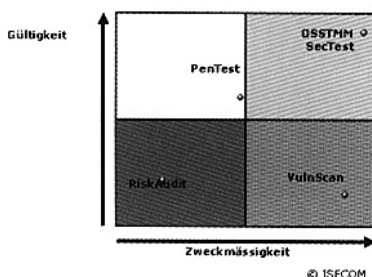
**Für IT-Sicherheitsverantwortliche gehören Sicherheitsaudits heute ebenso zum Standard, um die Wirksamkeit der implementierten Schutzmaßnahmen zu überprüfen, wie ein standardbasiertes IT-Sicherheits-Management, welches den regulatorischen und wirtschaftlichen Anforderungen gerecht wird.**

**Eine nicht hinreichend abgegrenzte Terminologie im weitläufigen Bereich der Sicherheitstests wirft unweigerlich Fragestellungen bei Verantwortlichen für die Beurteilung von Vergleichbarkeit von Angeboten, Transparenz von Leistungen sowie von Leistungsbreite und –tiefe auf. So werden Begrifflichkeiten, wie Penetrationstest, Sicherheitsanalyse/-test, Risikoaudit, Health Check oder Ethical Hacking in beliebiger Kombination mit den Zielobjekten System, Netz, Applikation etc. vermengt.**

## Teststandards

Dieser Zustand formuliert Anforderungen nach einem offenen Standard, der mit dem „Open Source Security Testing Methodology Manual“ (OSSTMM), herausgegeben von dem „Institut for Security and Open Methodologies“ (ISECOM) seit 2001 existiert. Aktuell in der Version 2.2 verfügbar, wird die grundsätzlich überarbeitete Version 3.0 der Testmethode in Kürze veröffentlicht.

Das OSSTMM ist eine offene von vielen hersteller- und technologieunabhängigen Fachleuten überprüfte Methode für Sicherheitstests und -metriken. Es stellt weltweit das einzige Methodenhandbuch für Sicherheitstests dar. Die ganzheitliche Methodik fokussiert stark darauf, exakt welche technischen Details zu testen sind, was bei dem Testprozess von der Vor- bis zur Nachberei-



Graphik 1: Positionierung OSSTMM-Audit

tung zu beachten ist und vor allem wie die Ergebnisse zu bewerten und zu messen sind. Tests für Best Practices, Standards, wie BSI, ISO etc., Regularien und Gesetze werden ständig aktualisiert adoptiert.

Dabei legt das OSSTMM besonderen Wert darauf, gründlich, konsistent, transparent und vor allem reproduzierbar zu testen. So erwirkt die konsequent angewendete Methode einen hohen Return on Invest.

Im Hinblick auf die eingangs aufgezeigte faktische Begriffsverwirrung grenzt

OSSTMM die Tests sinnvoll ab (siehe nebenstehende Grafik).

## Hintergrund

Das OSSTMM definiert IT-Sicherheit als „Business Enabler“ und statuiert damit klar, dass Sicherheit kein Selbstzweck ist. Hierbei referenziert es die IT-Sicherheit stark auf das jeweilig betriebene Geschäftsmodell im Kontext mit deren Abhängigkeit zur EDV. Auf diese Weise werden betriebliche und technische Wahrheit sinnvoll miteinander kombiniert zum Zwecke der zu erhaltenen Kontrolle über die Technologien, welche das Geschäftsmodell unterstützen.

Ein OSSTMM-valider Sicherheitstest ermittelt daher nicht nur die auf technischen Details beruhenden Sicherheitslücken, sondern verdichtet diese im Hinblick auf das Geschäftsmodell und der ihnen begründenden Informationen sowie der sie unterstützenden Technologien. Mittels dieser Methodik kann überprüft werden, ob die jeweilig betriebenen Dienste auch eine geschäftsgerichtete Grundlage haben, wie OSSTMM die „Business Justification“ definiert.

Ein OSSTMM-gültiger Sicherheitstest unterstützt somit den IT-Sicherheitsprozess, in dem er ermöglicht, richtlinien- und geschäftsmodellorientiert vorzugehen, um so die Vorgaben anzupassen.

## Mit OSSTMM wird Sicherheit messbar

Ein wesentlicher Schwerpunkt des Testhandbuches OSSTMM liegt in der Metrik für IT-Sicherheit durch einen „Risk Assessment Value“ (RAV). Der RAV gibt einen Prozentwert als Ergebnis verschiedener Einflussgrößen aus. Diese sind – bezogen auf den Zielbereich (Scope) – die operative Sicherheit (Operational Security – Sicher-

heits-Design), die aktuelle Sicherheitssituation (Actual Security - Sicherheitslücken) und die Schutzmaßnahmen (Loss Controls). Ausgehend von einem Best Practice-basierendem „Perfect Security“-Ansatz definiert der RAV das individuelle Sicherheitsniveau aus dem eine Degradationskurve (siehe nebenstehende Graphik) für die Systemeigenschaften, sicher und angemessen auf unerwartete Ereignisse zu reagieren, abgeleitet wird.

Damit geht einher, dass ein auf technischen Details beruhender OSSTMM-analoger Sicherheitstest kein papierbasiertes und auf Eintrittswahrscheinlichkeiten basierendes Risiko-Audit darstellt. Der RAV beruht auf einer technisch zwingend verifizierten Faktenlage. Der OSSTMM-Standard grenzt sich so deutlich von klassischen Risikoaudit-Alternativen ab und positioniert sich als operativer Sicherheitstest. Gleichzeitig wird so der Vergleichbarkeit von Sicherheitstests genügt.

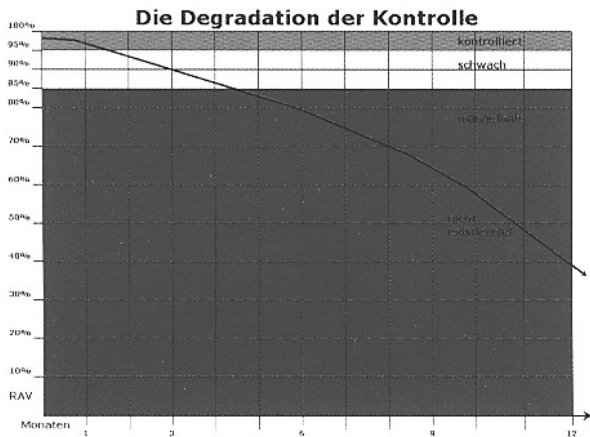
Ferner lässt sich der RAV problemlos in eine Governance-Strategie einbinden.

## Testqualität

Um die vorangestellte hohe Qualität zu sichern, erlegt OSSTMM den Testern ein restriktives Regelwerk, das sogenannte „Rules of Engagement“, auf.

Diese Regeln stellen auf ein Höchstmaß an Ethik und Qualität über den gesamten Testprozess ab, beginnend bei der Vertragsverhandlung über Verhaltensregeln bei der Durchführung bis hin zum Reporting. Gemäß ISECOM muss ein OSSTMM-gültiger Test folgende Qualifikationen zwingend erfüllen:

- quantifizierbar
- konsistent und reproduzierbar
- über den aktuellen Zeitrahmen hinaus begründet



Graphik 2: RAV-Degradation

- basierend auf dem Verdienst des Testers und nicht dem von Produkten oder Marken
- gründlich
- vereinbar mit dem individuellen und lokalen Recht und Datenschutzgesetz

Was bislang für Sicherheitstests fehlte, war ein Checklisten-Handbuch mit klaren Definitionen, wie ein solcher Test durchgeführt werden muss. Darüber hinaus verlangt das OSSTMM, wichtige Sicherheitsaspekte des Unternehmens bezogen auf das zugrundeliegende Geschäftsmodell einzubeziehen. Nur so können Aussagen zur globalen Unternehmenssicherheit getroffen werden.

### Durchführen von OSSTMM-Tests

Dabei verzichtet OSSTMM darauf, Tools für die Tests vorzuschreiben und garantiert mit hin, dass keine kommerziellen Tools zur Vorgabe gemacht werden. Freiheit und Kreativität des Testers bei der Aufdeckung von Lücken und ihrer Verifizierung stehen im Vordergrund. So wendet es sich gegen die alleinige Nutzung von Verwundbarkeits-Scannern, um schnell „Out of the Box“-Aussagen zu treffen. Ohne manuelle Verifizierung erhalten sie laut OSSTMM keine Wertigkeit, was der Erfahrung des hohen Fehleranteils (False-Positives) entspricht. Es regelt, dass der Tester alle identifizierten Lücken manuell verifizieren muss.

Aufgrund des Umstandes, dass dem Tester ein sehr hohes technisches Niveau mit großem Erfahrungsschatz für einen OSSTMM-Test abverlangt wird, existieren mit dem OSSTMM Professional Security Tester (OPST) und dem Analysten (OPSA) entsprechende Zertifizierungen mit akademischer Akkreditierung.

Im Zusammenspiel mit OPST und OPSA werden solide Aussagen über Problembe-

reiche und Sicherheitslücken getroffen, die das OSSTMM wie folgt einteilt:

- Verwundbarkeiten (Vulnerability)
- Schwachstellen (Weakness)
- Bedenken (Concerns)
- Informationslücken (Exposures)
- Anomalien (Anomaly)

### Reporting

Nachfolgend ein paar Beispiele, welche Unternehmens-Sicherheitsaspekte das OSSTMM umfasst:

- Informationssicherheit
- Prozess-Sicherheit
- Internet Technologie Sicherheit
- Wireless Security
- physikalische Sicherheit

Ein wesentlicher Schwerpunkt in dem Reporting mit ergänzenden Workshops ist der Know How-Transfer vom Tester an den Kunden.

### Fazit

Die Anwendung der ISECOM „Risk Assessment Values“ ermöglicht, mittels vordefinierter Testintervalle das Problem der Testzyklen leicht zu lösen. Durch Anwendung des ISECOM „Business Security Testing & Analysis Workbook“ kombiniert mit den OSSTMM-Formularen und -Checklisten, können Tests jedes Mal auf dieselbe Art durchgeführt werden, unabhängig wer testet. Die OSSTMM-Formulare und Checklisten dienen gleichzeitig als Grundgerüst für die Berichte und sind für Unternehmen eine große Hilfe, um die Berichtskonsistenz über Jahre hinweg sicherzustellen.

Heiko Rudolph, adMERITia  
Nicolas Mayencourt, Dreamlab Technologies AG  
Halle 7, Stand A47



Schon über 1 Mio. mal im Einsatz!

### GDD - Merkblatt Neues Bundesdatenschutz-Gesetz

Erstinformation für Mitarbeiter in Betrieb und Verwaltung  
21. Auflage 2006  
broschiert – 21 x 21 cm – 20 Seiten  
ISBN 978 3 89577 228 3  
Kostenloses Muster auf Anfrage

- Allgemein einführende Erstinformation
- Ideal für jeden neu eingestellten Mitarbeiter
- Grundlagen, Bedeutung und Notwendigkeit des Datenschutzes
- Erklärt Rechte und Pflichten
- Geeignet für Wirtschaft und Verwaltung
- Kurz und knapp auf 20 Seiten
- Durch anschauliche Grafiken aufgelockert

### Staffelpreise in Euro ab:

20	Expl.	64,-	50	Expl.	130,-
100	Expl.	220,-	200	Expl.	360,-
500	Expl.	775,-	1000	Expl.	1.450,-



Über 1/2 Mio. mal verkauft

### GDD - Datenschutz-Mitarbeiterinformation zur Datenschutz-Unterweisung am Arbeitsplatz

12. Auflage 2006  
broschiert – DIN A4 – 30 Seiten  
ISBN 978 3 89577 227 6  
Kostenloses Muster auf Anfrage

- Ausführliche Datenschutzunterweisung auf 27 DIN A4 Seiten
- Für Mitarbeiter, die auf das DS-Geheimnis zu verpflichten sind und mit personenbezogenen Daten umgehen
- Erläutert Grundregeln, Aufbau und Schutzbereich des BDSG
- Auch als Grundlage für Schulungen und die Erstellung einer betrieblichen Datenschutzrichtlinie geeignet

### Staffelpreise in Euro ab:

20	Expl.	72,-	50	Expl.	160,-
100	Expl.	260,-	200	Expl.	480,-
500	Expl.	1.000,-	1000	Expl.	1.850,-



Tel. 02234 / 96610-0 · Fax 02234 / 96610-9  
www.datakontext.com  
bestellung@datakontext.com