

## HELPDESK

# RAV: Security-niveau als Zahlenwert

Unser CIO behauptet, dass es einen Standard gibt, mit dem sich das Sicherheitsniveau als Zahlenwert wiedergeben lässt. Stimmt das?

Die Antwort ist «Ja». Denn bei der im «Open Source Security Testing Methodology Manual» (OSSTMM) beschriebenen Methode handelt es sich «lediglich» um einen de-facto-Standard. Dies, weil das OSSTMM (noch) nicht von einem offiziellen Standardisierungsgremium abgesegnet wurde. Der Rest der Aussage ihres CIO stimmt allerdings.

**Aufbau des OSSTMM:** Das von der ISECOM entwickelte OSSTMM ist kostenlos und kann auf <http://www.osstmm.org> heruntergeladen werden.

OSSTMM besteht grob gesehen aus drei Teilen. Im ersten Teil wird dabei die eigentliche Methodik für die Planung, Durchführung und Dokumentation von Security Audits beschrieben. Den zweiten Teil bilden die Berechnungen des angetroffenen Sicherheitsniveaus (Security Metrics). Der dritte Teil besteht aus den Formularvorschlägen für die Informationserfassung und

-auswertung während der Tests. Diese Formularvorschläge stellen, zusammen mit dem Action Log des Testers und dem Mit-

**«Ein RAV-Wert von mehr als 90 Prozent belegt, dass eine Firma ihre IT im Griff hat.»**

schnitt des Netzwerkverkehrs, die Minimalanforderungen an einen OSSTMM-konformen Report dar.

**Security Metrics:** Das OSSTMM kennt folgende fünf Risikokategorien: Vulnerability (Verwundbarkeiten), Weakness (Schwachstellen), Concern (Verstoss gegen «Best Practices»), Exposure (Informationsabflüsse) und Anomaly (nicht erklärbares Phänomene).

Der Begriff «Risk Assessment Value» (RAV) wird im OSSTMM für die Darstellung des Sicherheitsniveaus des Untersuchungsobjekts als Zahlenwert verwendet. Dieser Wert wird anhand von Formeln berechnet, welche



ILLUSTRATION: OW/THU

folgende Eingangsvariablen verwenden:

**Operative Sicherheit (OpSec):** Diese Variable bewertet die Sichtbarkeit. Wie viele Systeme sind sichtbar?

**Vertrauensstellungen:** Wie viele Systeme/Dienste vertrauen einander ohne vorherige Authentisierung?

**Zugriffspunkte:** Wie viele Dienste sind ansprechbar, wie viele Interaktionsmöglichkeiten existieren?

**Kontrollausgleich (Loss Control):** Dieser Wert berücksichtigt implementierte Sicherheitsmechanismen wie beispielsweise Verschlüsselung, Authentisierungsmechanismen, Redundanzen, Versicherungsdeckung etcetera im positiven Sinn, indem damit Pluspunkte gesammelt werden können.

**Aktuelle Sicherheit (ActSec):** Detektierte Risiken werden hinsichtlich ihres Bedrohungspotenzials gewichtet.

Sobald diese Informationen vorliegen, kann die Berechnung des RAVs mittels Taschenrechner oder des von der ISECOM bereitgestellten Spreadsheets erfolgen. Der resultierende RAV gibt das Sicherheitsniveau als neutralen Zahlenwert wieder. Dieser bewegt sich zwischen 0 und 100 Prozent – je höher

desto besser. Unternehmen und Organisationen, welche ihre IT im Griff haben, erzielen folgende RAVs nach der derzeit gültigen RAV-Formel: Industrieunternehmen zwischen 90 und 95 Prozent Organisationen im Finanzsektor oder im militärischen Bereich kamen auf Werte zwischen 95 und knapp 99 Prozent.

Ein RAV von 100 Prozent ist in der Realität nicht erreichbar. Bei der RAV-Kalkulationsformel von OSSTMM V3 liegen die Werte bei gleicher Anzahl Sicherheitslücken 15 bis 20 Prozent tiefer, weil dabei beispielsweise bereits die Sichtbarkeit von Systemen bestraft wird – selbst wenn diese Systeme optimal gehärtet sind.

**Fazit:** Der RAV des OSSTMM bietet Vergleichbarkeit und Nachvollziehbarkeit der Resultate. Sicherheitsverantwortliche können die zu erzielenden RAV-Schwellwerte anhand der Sensitivität der von den entsprechenden Systemen gehaltenen Daten definieren. Dies ermöglicht ein proaktives IT Risk Management und Controlling: Fakten statt reines Bauchgefühl. ■

 **Archiv aller Helpdeskartikel:**  
[www.computerworld.ch](http://www.computerworld.ch)



**Der Autor**  
Christoph Baumgartner ist CEO der Sicherheitsberaterin Oneconsult, Thalwil.  
[www.oneconsult.com](http://www.oneconsult.com)

**Jede Woche beantworten Sicherheitsexperten Ihre Leserfragen:**

**Haben Sie Fragen rund ums Thema IT-Sicherheit?**

**Schreiben Sie uns:**  
[it-security@computerworld.ch](mailto:it-security@computerworld.ch)