

IT-SECURITY-HELPDESK

Securitytester: Schulung nach OSSTMM

Warum lohnt es sich, Sicherheitstester nach dem Open Source Security Testing Methodology Manual auszubilden?

Sicherheitstests in der IT-Security sind inzwischen sehr verbreitet. Viele Firmen haben erkannt, dass zyklisch wiederkehrende Audits unersetzbar geworden sind. Allerdings stehen viele Kunden dabei vor dem Problem, dass die Qualifikation von Auditoren nur schwer nachvollziehbar ist. Zudem arbeiten Sicherheitstester oft nach unterschiedlichen Methoden, was dazu führt, dass die Sicherheitstests faktisch nicht vergleichbar sind.

Als Lösung empfiehlt es sich daher, Auditoren zu wählen, die nach dem OSSTMM (Open Source Security Testing Methodology Manual) arbeiten. Dieses stellt eine standardisierte Methode für die Durchführung von Sicherheitstests zur Verfügung. Das OSSTMM baut auf folgenden Begriffen auf: Ziel, Untersuchungsobjekt, Quantität, zu untersuchende Themen (Channels) und Perspektive (Vektor). Die Channels umfassen alle möglichen Technolo-

gien wie physische Sicherheit, Personensicherheit, Wireless-Sicherheit, Kommunikationssicherheit und Sicherheit von Datennetzwerken. Dabei werden die Channels in Sektionen, Module und Tasks unterteilt, nach denen dann ein Tester arbeitet.

Das OSSTMM sagt aber nur, was getestet werden soll. Wie dies geschieht, bleibt den Auditoren überlassen. Das OSSTMM beinhaltet Security Metrics, die sogenannten RAV (Risk Assessment Values), um die Sicherheit schlussendlich als mathematisch repräsentative Prozentzahl auszuweisen. Dabei werden Verwundbarkeiten als Limitationen ausgewiesen, die operative Sicherheit repräsentiert aktive IP-Adressen, offene Ports und Trusts und Bonuspunkte können als Loss Controls (Kontrollausgleich) berücksichtigt werden. Überdies sind auch ethische Richtlinien und Verhaltensregeln im OSSTMM enthalten.

Das OSSTMM bietet im Wesentlichen zwei Berufsbilder: Den OPST (OSSTMM Professi-

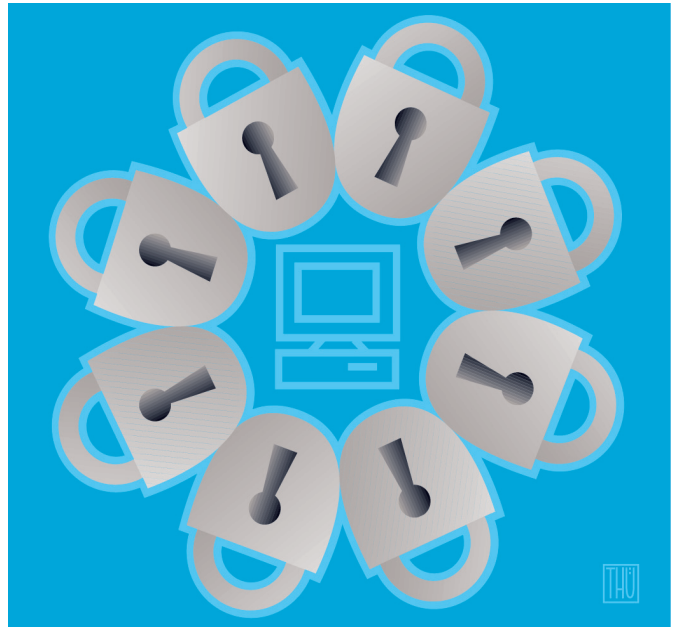
onal Security Tester) und den OPSA (OSSTMM Professional Security Analyst), welche sicherstellen, dass der Audit und die resultierenden Ergebnisse den Vorgaben der Methodik entsprechen. Das OSSTMM stellt insbesondere die Vergleichbarkeit von Audits sicher, weil die Tester immer gleich vorgehen. Damit sorgt es für ein verlässliches Trending, da die Entwicklung der Sicherheit über die Zeit verfolgt und analysiert werden kann.

Das Berufsbild des OPST (OSSTMM Professional Security Tester) stellt sicher, dass der Tester beim Audit nicht auf Brands von Produkten beruht, sondern Sicherheitstests genau nach OSSTMM durchführen kann. Dabei wird Wert darauf gelegt, dass der Tester versteht, was er testet – und nicht blindlings mit unangebrachten Tools wild drauf los schießt. Ethik wird gross geschrieben, auch diesbezüglich wird ein OPST intensiv geschult. Die Schulung beinhaltet keine Toolsammlung, da der Tester mit seinem Verständnis von Technik und Sicherheit in der Lage sein soll, das entsprechend ideal geeignete Tool selbst zu wählen.

Der OPSA (OSSTMM Professional Security Analyst) ist für die korrekte Durchführung der RAV-Berechnung verantwort-

lich. Dabei stellt er sicher, dass der Tester verlässliche Resultate liefert (Vier-Augen-Prinzip) und dass der Test OSSTMM-konform durchgeführt wurde. So muss unter anderem ausgewiesen werden, was nicht getestet wurde. Auch dies macht Audits vergleichbarer. Der OPSA ist zudem verantwortlich, dass die Analyse des Untersuchungsobjektes korrekt durchgeführt wird und die empfohlenen Massnahmen dem Kunden auch eine Verbesserung der Sicherheit bringen.

Es ist also im Sinne von Kunden im Sicherheitsbereich, wenn die Auditoren nach OSSTMM ausgebildet und zertifiziert werden. Das BSI Deutschland (Bundesamt für Sicherheit in der Informationstechnik) empfiehlt das OSSTMM gar für die Durchführung von Sicherheitstests. Die Sicherheitsberaterin OneConsult GmbH ist als ISECOM Licensed Auditor (ILA), Gold Level und ISECOM Partner (akkreditierter Schulungsanbieter) bevollmächtigt, Schulungen in der Schweiz, Deutschland und Österreich von OPST und OPSA durchzuführen. ■



THU



Der Autor
Martin Rutishauser
ist Director Training
& Research und
OSSTMM-Trainer
bei OneConsult,
Thalwil.
oneconsult.com.

Jede Woche beantworten Sicherheitsexperten Ihre Leserfragen:

Haben Sie Fragen rund ums Thema IT-Sicherheit?

Schreiben Sie uns:
it-security@computerworld.ch



Archiv aller Helpdeskartikel:
www.computerworld.ch