IT-SECURITY

OSSTMM – Ein kritischer Blick in den Spiegel

Das Open Source Security Testing Methodology Manual (OSSTMM) ist ein Defakto-Standard zur Durchführung technischer Audits. Doch wie gut ist es wirklich?

Wer regelmässig technische Audits durchführen lässt, muss Angebote, Methoden und Resultate vergleichen können – vor allem, wenn er sie von unterschiedlichen Anbietern durchführen lässt. Nur so sind aussagekräftige Trendanalysen und Audit Trails möglich. Genau diese Transparenz verspricht das von der ISECOM erstmals 2001 veröffentlichte und kontinuierlich weiterentwickelte «Open Source Security Testing Methodology Manual» (OSSTMM).

Im Gegensatz zu gängigen ISO/IEC-Standards positioniert sich das OSSTMM als konkrete Anweisung, was wie getestet und dokumentiert werden soll, ohne den Einsatz konkreter Tools vorzuschreiben. Das frei verfügbare OSSTMM umfasst verschiedene Komponenten: Die «Rules of Engagement» sind der Verhaltenskodex, an welchen sich die Auditoren halten müssen. Es handelt sich dabei um Regeln, welche sämtliche Phasen von der Akquisition über das eigentliche Projekt bis nach Abschluss abdecken. Sie schützen insbesondere die Interessen der Auftraggeber.

Die eigentliche Methode gliedert sich in fünf Channels, die sämtliche Aspekte der Informationssicherheit behandeln und aus einzelnen Modulen bestehen, welche wiederum in Form von Tasks zu durchlaufen sind. Selbstverständlich gehört ein aussagekräftiger Schlussbericht zu jedem OSSTMM-konformen Projekt.

Kritik an der Präzision

Die bisher aufgeführten Bestandteile des OSSTMM werden von Sicherheitsspezialisten nicht ernsthaft in Frage gestellt. Anders verhält es sich mit der Spreadsheet-basierten mathematischen Herleitung des Sicherheitsniveaus, dem sogenannten «Risk Assessment Value» (RAV).

Zur Berechnung werden verschiedene Eingabewerte, beispielsweise die Sichtbarkeit des Untersuchungsobjekts, ansprechbare Dienste, detektierte Sicherheitslücken oder Sicherheitsmassnahmen wie Verschlüsselung, Authentisierung, Redundanz, etc. berücksichtigt. Die Idee dahinter ist bestechend: Der RAV lässt sich unabhängig von der Grösse des Untersuchungsobjekts berechnen und gefahrlos mit anderen RAVs vergleichen, weil er keinerlei Rückschlüsse auf die tatsächlichen Sicherheitslücken erlaubt. Kritisiert wird teilweise die suggerierte Präzision: Der RAV werde zwar auf zig Kommastellen berechnet, der Tester habe aber viel Interpretationsspielraum beim Ausfüllen des Spreadsheets.

Dem ist entgegenzuhalten, dass das OSSTMM in Kürze in Version 3 erhältlich sein wird und mit jeder Version der Interpretationsspielraum der Tester konsequent weiter eingeschränkt wird – dies um die Vergleichbarkeit weiter zu verbessern. Neben der Überarbeitung der RAV-Kalkulation wird voraussichtlich im OSSTMM Version 3 eine Methode zur Erhebung des organisatorischen Reifegrades der zu überprüfenden Organisation eingeführt – und als notwendige Bedingung für die OSSTMM-Konformität gefordert. Der Nachteil dieser Bestrebungen liegt im steigenden Komplexitätsgrad des OSSTMMs. Dies bringt neben dem Problem, dass manche Auftraggeber nicht bereit sind, mehr für die OSSTMM-Konformität zu bezahlen als bisher, auch den Nachteil, dass es schlicht nicht mehr möglich ist, das OSSTMM kurz querzulesen und anschliessend OSSTMM-konform zu testen.

«Beim Audit müssen die Ergebnisse vergleichbar sein.»

Lizenzierte Partner

Die Wissensvermittlungslücke schliessen die «ISECOM Partner», welche als akkreditierte Schulungsunternehmen verschiedene spezialisierte Zertifizierungskurse (OPST, OPSA, OPSE und OWSE) nach OSSTMM anbieten. Unternehmen, welche eine bestimmte Anzahl an OPSx-zertifizierten Mitarbeitern beschäftigen, können sich im Sinne der Qualitätssicherung als «ISECOM Licensed Auditor» (ILA) auf verschiedenen Leveln akkreditieren lassen.

Fazit: Schlüssige Methode

Das OSSTMM bietet eine schlüssige Methode, technische Audits zu standardisieren. Es ist seit mehr als sieben Jahren verfügbar und bestehende Schwächen werden konsequent behoben. Wem das OSSTMM als Gesamtpaket nicht zusagt, der kann zumindest einzelne Teile davon nutzen. Das OSSTMM kann hier heruntergeladen werden: www.osstmm.org ■

Mehr zur IT-Security:
www.computerworld.ch

DER AUTOR

Christoph Baumgartner ist Mitglied des ISECOM-Core-Teams und CEO der OneConsult GmbH. **www.oneconsult.com**