HELPDESK

Sicherheits-tests mit Tief-gang

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

ILLUSTRATION: CW/THÜ

Frage: Wir richten uns nach der Norm ISO 17799. Gibt es dazu eine konforme Anleitung für die Durchführung von technischen Sicherheitsüberprüfungen?

Problem: Gängige Standards wie ISO 17799:2005 empfehlen oder fordern zwar die Durchführung von technischen Sicherheitsüberprüfungen, bieten aber ausser generellen Tipps keine präzise Hilfestellung zu deren Ausführung.

Dies führte dazu, dass Anbieter und Anwender mangels Alternativen eigene Methoden entwickeln mussten. Als logische Folge sind manche Projektergebnisse nicht nachvollziehbar und die Offerten und Schlussberichte verschiedener Anbieter nur schwer oder gar nicht miteinander vergleichbar.

Anforderung: Sicherheitsüberprüfungen sollten Mindestanforderungen erfüllen:

1. Quantifizierbarkeit – Zahlenwerte statt «Bauchgefühl» ermöglichen den Vergleich,
2. Konsistenz und damit die Replizierbarkeit der Ergebnisse,
3. Gültigkeit über das «Jetzt» hinaus – proaktives statt reaktives Handeln,
4. auf der Leistung von Tester statt auf «Brands» basierend,
5. Vollständigkeit und Genauigkeit und
6. Gesetzeskonformität.

Lösung: Das praxisbezogene und international anerkannte «Open Source Security Testing Methodology Manual» (OSSTMM) vom «Institute for Security and Open Methodologies» (ISECOM) ergänzt die Mindestanforderungen mit einem ausgereiften Verhaltenskodex und dem Verantwortlichkeitsprinzip der ausführenden Tester. Der Begriff «Open Source» bezieht sich dabei auf die freie Verfügbarkeit der Methodik und nicht auf den ausschliesslichen Einsatz von Open-Source-Tools. Das OSSTMM wird kontinuierlich weiterentwickelt und besteht aus der Methodologie und den «Security Metrics» (Risk Assessment Values, RAVs). Die Methodologie ist hierarchisch gegliedert. Sich teilweise überlappende «Channels» (Sektionen) decken sämtliche Sichten von der Informations-, System- und Kommunikationssicherheit über die physische Sicherheit bis hin zur Prozesssicherheit ab. Diese Channels sind wiederum in Module gegliedert, welche in Form von verschiedenen Tasks durchlaufen werden müssen. Dem OSSTMM liegen diverse Formularvorschläge bei, welche die Minimalinformationen beinhalten, welche für einen OSSTMM-konformen Test benötigt werden.

«Das OSSTMM ist unter anderem kompatibel mit ITIL, ISO 17799, IT Grundschutzhandbuch und SOX».

Nachdem die ausgefüllten Formulare vorliegen, werden die aufgedeckten Schwachstellen gemäss den OSSTMM-Bewertungskriterien kategorisiert. Anschliessend erfolgt die Berechnung der RAV mittels Formeln, welche neben der Anzahl und den Typen der Schwachstellen auch die Charakteristika des Untersuchungsobjekts berücksichtigen. Die auf Best Practices des Security Testings basierenden RAV beschreiben die zeitbezogene Degradierung des Sicherheitsniveaus des jeweiligen Objekts. Das OSSTMM in der aktuellen Version 2.1 ist bezüglich «Remote Auditing and Testing» kompatibel mit ITIL, ISO 17799, IT Grundschutzhandbuch, SOX, SET Secure Electronic Transaction Compliance Testing Policies and Procedures. Die bereits angekündigten zukünftigen Versionen werden auch für Tests im LAN/WAN ausgelegt sein. Wer sich professionell mit dem OSSTMM beschäftigen möchte, kann das Kursangebot mit anschliessender Zertifizierungsmöglichkeit von ISECOM nutzen: «OSSTMM Professional Security Expert» (OPSE): generelle Kenntnisse der Methodik, «OSSTMM Professional Security Tester» (OPST): Ethical Hacker, «OSSTMM Professional Security Analyst» (OPSA): Analyse und Bewertung von Testergebnissen. Das OSSTMM kann im Internet kostenlos unter http://www.osstmm.org als PDF herunter geladen werden. An gleicher Stelle finden sich auch weitere Informationen zu OSSTMM und ISECOM. Das OSSTMM bietet zumindest eine gute Alternative zu selbst gestrickten Methoden. ■

Der Autor
Christoph Baumgartner ist Senior Consultant bei der sicherheitsspezialistin Oneconsult, Thalwil, www.oneconsult.com.

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch