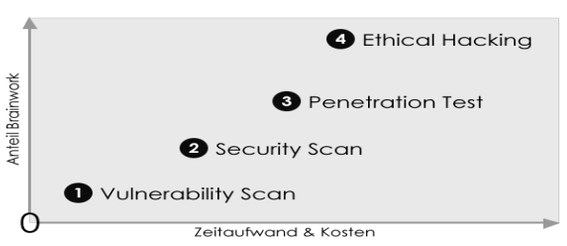
Technische Sicherheitsüberprüfungen – die Nagelprobe

Hacker und Malicious Mobile Code, insbesondere die perfide jüngste Virengeneration, die Hackerviren, bedrohen die IT-Infrastruktur von Unternehmen, Organisationen und Privaten in immer grösserem Ausmass. Neben den klassischen technischen Gegenmassnahmen wie Firewall, Virenscanner, IDS und Co. dienen technische Sicherheitsüberprüfungen den IT-Verantwortlichen zur Aufdeckung und anschliessenden Schliessung von Sicherheitslücken, bevor Unbefugte diese ausnutzen können.

von Christoph Baumgartner

Bei allen technischen Sicherheitsüberprüfungen geht es um die möglichst lückenlose Aufdeckung von Sicherheitslücken mittels eines toolgestützten simulierten «Hackerangriffs». Üblicherweise werden anschliessend technische und/oder organisatorische Massnahmen zur Schliessung gefundener Lücken vorgeschlagen. Der Nutzen liegt einerseits in der Erhöhung des Sicherheitsniveaus, was zu indirekten Kostensenkungen dank Risikominimierung führt. Andererseits fördert die Durchführung einer technischen Sicherheitsüberprüfung bei den am Projekt Beteiligten und deren Vorgesetzten zu einer gesteigerten Security Awareness und dient dem Know-how-Transfer in Richtung Auftraggeber.

Typen und Positionierung



Terminologie angelehnt an:
OSSTMM (Open Source Security Testing Methodology Manual von ISECOM)

Typen und Positionierung

Es gibt verschiedene Typen von technischen Sicherheitsüberprüfungen. Da diese Disziplin noch relativ jung ist, fehlt eine einheitliche Terminologie. In diesem Artikel wird eine an das OSSTMM (Open Source Security Testing Methodology Manual) angelehnte Definition verwendet. Die methodischen Hauptunterscheidungskriterien sind Automatisierungsgrad, Testtiefe und Ausnutzen von Sicherheitslücken.

Prinzipiell kann das Untersuchungsobjekt aus einzelnen oder mehreren Servern, Clients, PDAs, Smartphones, Netzwerkkomponenten und/oder Applikationen bestehen. Man spricht von einem externen Test, wenn das Untersuchungsobjekt aus externer Sicht, beispielsweise via Internet, via Wireless LAN oder via Blue Tooth geprüft wird. Interne Tests erfolgen im LAN oder WAN.

Vulnerability Scans, Security Scans und traditionelle Penetration Tests suchen nach Sicherheitslücken ohne das Untersuchungsobjekt zu modifizieren. Beim Ethical Hacking werden Sicherheitslücken gezielt ausgenutzt und das Untersuchungsobjekt manipuliert oder modifiziert. Ausserdem ist der manuell zu erbringende Anteil an den Projektarbeiten (Planung und Durchführung der eigentlichen Attacke) beim Ethical Hacking massiv höher, weil für den eigentlichen «Hackerangriff» meist nur bedingt Standardtools eingesetzt werden können. Bei komplexen Zielvorgaben müssen vom Tester oftmals massgeschneiderte Tools programmiert werden.

Die Methoden des Ethical Hacking lassen sich zwei Kategorien zuordnen. Der direkte Ansatz wird gewählt, wenn das Untersuchungsobjekt Sicherheitslükken aufweist, welche es dem Tester direkt ermögli-

chen, das vordefinierte Ziel zu erreichen. In diese Kategorie fallen alle «Buffer Overflow-», «Brute Force-», «Denial of Service-»Attacken und das «Sniffing». Im Gegensatz dazu wird beim indirekten Ansatz die (un)freiwillige, aktive Hilfe eines «Komplizen», beispielsweise eines normalen PC-Users beim Kunden benötigt. Dieses Vorgehen wird dann gewählt, wenn zur Zielerreichung Systeme genutzt werden müssen, welche vom Tester nicht direkt oder nur mittels grossen Aufwands erreicht und manipuliert werden können. Dabei kommen sogenannte «RATs» (Remote Administration Tools) zum Einsatz. Bei Erfolg lässt sich das infizierte System durch die Firewall hindurch von der zugehörigen Steuerkomponente (der PC des Testers) fernsteuern.

Nutzenoptimierung

Wer das Kosten/Nutzen-Verhältnis optimieren will, sollte die Stärken der verschiedenen Testtypen kombinieren. Vulnerability und Security Scans untersuchen das Untersuchungsobjekt mit Hilfe von spezialisierten Tools voll- oder teilautomatisch. Dank dieser Automatisierung können in relativ kurzer Zeit verschiedenste Tests auf sämtliche Komponenten des Untersuchungsobjekts durchgeführt werden. Leider finden diese Tools in der Regel nur allgemein bekannte Sicherheitslücken und generieren oft Falschmeldungen (vermeintliche Sicherheitslücken). Ausserdem fehlt diesen Tools die Intelligenz, Sicherheitslücken kontextgerecht zu bewerten. Sofern detektierte Sicherheitslücken manuell verifiziert werden, eignen sich diese Tests dennoch gut für einen ersten Überblick bezüglich des generellen Sicherheitsniveaus.

Basierend auf den Ergebnissen des Vulnerability Scans / Security Scans kann anschliessend mittels eines Penetration Tests gezielt nach Sicherheitslücken gesucht werden. Die daraus resultierenden Ergebnisse zeigen vorhandene, mögliche Angriffspunkte im Untersuchungsobjekt auf. Mit anderen Worten: Der Auftraggeber weiss, welche Sicherheitslücken von Hackern in welcher Form ausgenutzt werden könnten, um bestimmte Ziele bzw. Effekte zu erreichen. Dieses mehrstufige Vorgehen stellt sicher, dass monetäre und personelle Ressourcen und Tools optimal eingesetzt werden.

Hauptunterscheidungskriterien

Bezeichnung	1 Vulnerability Scan	2 Security Scan	3 Penetration Test	4 Ethical Hacking
Aufspüren von Sicherheitslücken	voll-auto-matisiert	voll-auto-matisiert	teil-auto-matisiert / manuell	teil-auto-matisiert / manuell
manuelle Verifikation	nein	ja	ja	ja
Einsatz mehrerer Tools zur Plausibilisierung	nein	nein	ja	ja
Ausnützen von Sicherheitslücken	nein	nein	nein	ja
Ansatz	direkt	direkt	direkt	direkt / indirekt
Massnahmenvorschläge	technisch	technisch	technisch / organisatorisch	technisch / organisatorisch

Kosten und Aufwand

Wer eine Sicherheitsüberprüfung in Auftrag geben möchte, sollte im Minimum mit externen Kosten von CHF 5 000.- rechnen. Für diesen Betrag erhält der Kunde einen Security Scan inklusive manueller Verifikation aus externer Sicht, wobei das Untersuchungsobjekt aus ca. 5 Systemen besteht. Eine gründliche und repräsentative Sicherheitsüberprüfung der Klasse Penetration Test inkl. Ethical Hacking kostet zwischen CHF 15 000.- und CHF 30 000.-. Die Anzahl der zu untersuchenden Systeme spielt dabei eine untergeordnete Rolle.

Der Aufwand seitens Auftraggeber beträgt pro Testtag mindestens 30 Minuten. Zusätzlich ist noch mit ca. zwei Stunden für das Kick-off-Meeting und die Dokumentationsbereitstellung zu rechnen. Falls möglich ist aus sicherheitstechnischer Sicht und bezüglich des Know-how-Transfers eine Betreuung des Testers seitens Kunde während der gesamten Dauer der Tests empfehlenswert.

Rechtlicher Exkurs und Empfehlungen

Jegliche Ausführung von «Sicherheitsüberprüfungen» ohne die ausdrückliche Genehmigung des Eigentümers und des Betreibers des Untersuchungsobjekts ist strafbar. Wie bei allen Projekten sollten Projektauftrag (inkl. Projektteam, Untersuchungsobjekt, Ziele, Methodik, Zeitfenster, Form und Granularität der Dokumentation etc.) und sämtliche Eventualitäten vertraglich zwischen Auftraggeber und Tester festgehalten werden. Falls beim Ethical Hacking der indirekte Ansatz gewählt wird, sollte der «Komplize» vor

(Fortsetzung Seite 55)

Werkzeugen zum Beispiel für die Bereiche Service Management, IT Security und Qualitätsmanagement auf.

Für eine stark vereinfachte Darstellung siehe Bild 3. Es ist möglich, diese Matrix, bis auf die Ebene der 318 Aktivitäten zu verfeinern, doch muss an dieser Stelle aus Platzgründen darauf verzichtet werden. Die entsprechende Gegenüberstellung ist jedoch sehr aufschlussreich und erlaubt auf der (tiefsten) Aktivitätenebene verschiedene Betrachtungsweisen. Dies ist bei Assessments von grossem Vorteil.

Zusammenfassung

COBIT ist sehr umfassend und deckt wie kein anderes Framework die Prozesse und Aktivitäten in der IT ab. Es eignet sich daher insbesondere zur Umsetzung einer IT Governance, d.h. die optimale Unterordnung und den Einsatz der IT zur Unterstützung der Geschäftsanforderungen.

Spezielle Werkzeuge wie ITIL, ISO 17799, GSHB, ISF, Six Sigma, EFQM können dabei auf ihrem Spezialgebiet weiter in die Tiefe gehen.

COBIT	Service Management	Security	Qualitäts-Management	Aufgabenbereiche (Beispiele)
Planung & Organisation	**Prozesse**: Planning & Control IT Services Operation Financial Management Change Management SW Lifecycle Support Problem Management	**Prozesse**: Security Requirements Security Policy Grundschutz **Werkzeuge**: ISO 17799 ISO 15408 (CC) BSI GSHB ISF	**Prozesse**: Qualitätsmanagement **Werkzeuge**: ISO 9000 EFQM TQM Six Sigma	Strategische IT-Planung Business-IT-Alignment Projektmanagement Sorbanes-Oxley Riskmanagement Tests und Training Qualitätsmanagement
Beschaffung & Implementation	Capacity Management Release Management **Werkzeuge**: ITIL CMM			Spezifikation & Evaluation SW Entwicklung Betriebsmanuals Training Manuals Abnahmetests
Betrieb & Unterstützung				Outsourcing SLA Management SLA Reviews Security Management Business Continuation Impact Analyse TCO Analysen Security Management ITIL Kernprozesse
Überwachung				Audits und Revision

Bild 3: Überlappungsbereiche COBIT

Eine mögliche Vorgehensweise wäre daher im Rahmen eines umfassenden Assessments (z.B. im Bereich IT-Security), mittels COBIT breitflächig eine Schwachstellenanalyse zu beginnen und bei «Problemzonen» unterstützend weitere Werkzeuge beizuziehen. □

Wolfgang Mahr, BBA, ist Senior Consultant bei Intercai (Schweiz) AG in 8304 Wallisellen.

(Fortsetzung von Seite 53)

der Durchführung des «Hackerangriffs» namentlich genannt und vor den rechtlichen Folgen seiner Tat - wie Verstoss gegen die geltende Security Policy - geschützt werden. Oft ist es sinnvoll, wenn ein Mitglied des Managements den «Komplizen» mimt. □

Christoph Baumgartner, lic. oec. publ., ist Geschäftsführer und Senior Consultant der One-Consult GmbH, Thalwil,
baumgartner@oneconsult.com.