Security Audits: Licht ins Dunkel

Mindestens jeder zweite ICT-Integrator und viele spezialisierte Anbieter führen technische Security Audits im Angebot. Was gilt es dabei zu beachten?

Von Christoph Baumgartner

IN KÜRZE

- Security-Audits reichen von einem simplen Scan bis zum komplexen Ethical Hack.
- Es wird entweder nach Software-basierten und/oder Design-basierten Lücken gesucht.
- Regelmässige Tests der eigenen ICT schützen präventiv vor möglichen, echten Hacker-Angriffen und fördern die Awareness.

Meldungen von DOS-Attacken, Virenbefall und anderen Security-Zwischenfällen in Unternehmen gehören schon fast zur Tagesordnung. Weil die ICT in fast allen Unternehmen eine vitale Rolle übernommen hat, kommt der Verhinderung derartiger Attacken eine grosse Bedeutung zu. Ein praktikabler und vor allem auch präventiver Ansatz ist die regelmässige Durchführung sogenannter technischer Security Audits.

Was ein Security Audit bringt

Mit einem gründlichen Security Audit werden aber nicht nur Sicherheitslecks aufgedeckt und hoffentlich anschliessend geschlossen, bevor sie von Unberechtigten ausgenutzt werden. Derartige Sicherheitsüberprüfungen dienen auch der Qualitätssicherung und dem Compliance-Nachweis bezüglich gesetzlicher Rahmenbedingungen, Vorgaben und Normen wie beispielsweise Basel II, ISO/IEC 27001, SOX oder BSI-Standard 100-1/4.

Präventiv durchgeführte Security Audits ermöglichen Kosten einzusparen, welche später durch Sicherheitslecks hätten verursacht werden können. Last but not least wird, und das ist kein unwesentlicher Faktor, auch die Security Awareness gefördert, und zwar auf allen Stufen im Unternehmen, einhergehend auch mit einem Know-how-Transfer vom Dienstleister in Richtung Auftraggeber. Der erhält zudem eine Argumentationsgrundlage für zukünftige IT-Security-Projekte und -Aktivitäten.

Security Audit ist nicht Security Audit

Bevor man einen technischen Security Audit bestellt, sollte man sich genau über den Fokus der Sicherheitsüberprüfung im klaren sein. Steht die Suche nach Software-basierten (Betriebssystem und Applikationen) Sicherheitslücken oder die Suche nach Design-basierten (Architektur) Schwachstellen im Mittelpunkt?

So dienen Vulnerability Scans, Security Scans und Penetration Tests primär der Aufdeckung von Software-basierten Sicherheitslücken. Dabei wird während der zur Verfügung stehenden Testzeit systematisch nach möglichst allen Sicherheitslücken im Untersuchungsobjekt gesucht. Das Ethical Hacking dient hauptsächlich der Aufdeckung Design-basierter Mängel – was dazu führt, dass nicht zwangsläufig nach allen Software-basierten Sicherheitslücken gesucht wird. Der Application Security Audit kann abhängig vom Aktivitätsumfang beide Fokusse abdecken.

Black or White?

Vor der Testdurchführung muss vom Auftraggeber auch definiert werden, inwieweit die Mitarbeiter des Auftraggebers über bevorstehende Tests und die Tester über das Untersu-

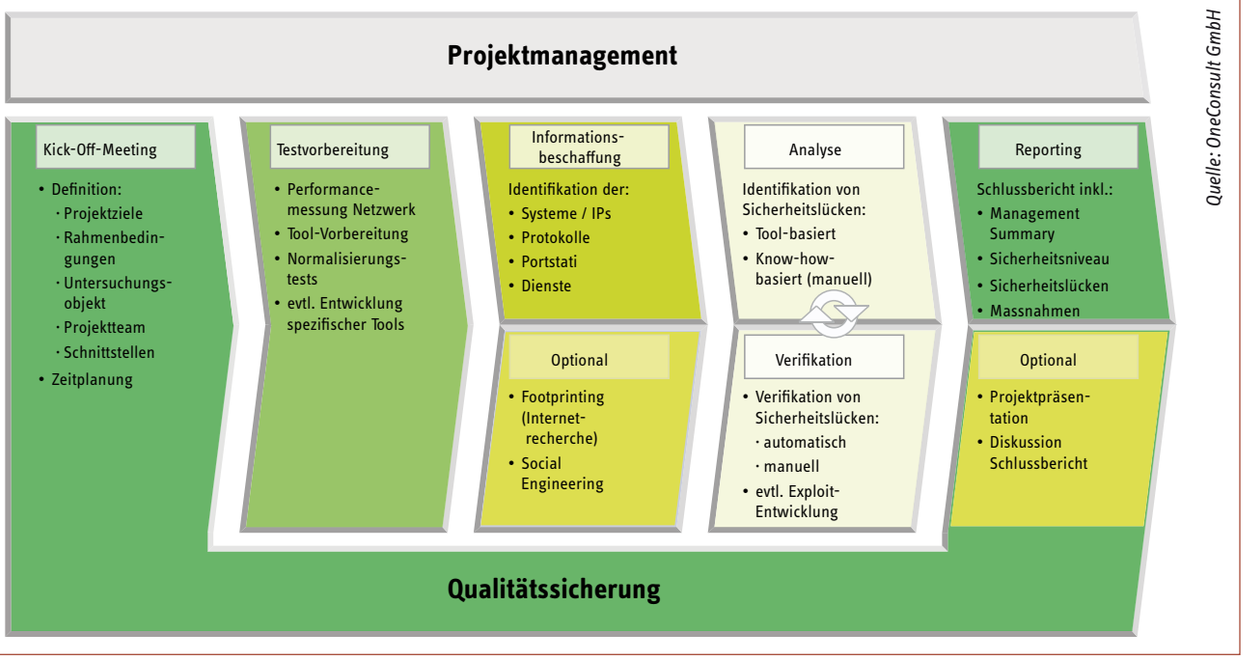
CHARAKTERISTIKA TECHNISCHER SECURITY AUDITS

MERKMAL	SECURITY SCAN	PENETRATION TEST	APPLICATION SECURITY AUDIT	ETHICAL HACKING
Suche nach Software-basierten Sicherheitslücken (während zur Verfügung stehender Testzeit)	■	■	■	□
Suche nach Design-basierten Sicherheitslücken	□	□	■	■
Unprivilegierte Tests (ohne Kenntnis gültiger Zugriffsinformationen)	■	■	■	■
Privilegierte Tests (mit Kenntnis gültiger Zugriffsinformationen)	□	□	■	■
Automatisierte Suche nach Sicherheitslücken	■	■	■	■
Manuelle Suche nach Sicherheitslücken	□	■	■	■
Einsatz mehrerer Tools mit ähnlicher Funktionalität	□	■	■	■
Nichtintrusive Verifikation von Sicherheitslücken	■	■	■	■
Intrusive Verifikation von Sicherheitslücken	□	■	■	■
Gezielte Modifikation des Untersuchungsobjektes (z.B. User Accounts, Datenbankinhalte, Dateisystem etc.)	□	□	□	■
Technische Massnahmenvorschläge	■	■	■	■
Organisatorische Massnahmenvorschläge	□	■	■	□
Dokumentation	■	■	■	■

■ = ja, □ = nein

Quelle: OneConsult GmbH

PROJEKTPHASEN EINES PENETRATION TESTS



Quelle: OneConsult GmbH

chungsobjekt informiert werden. In der Praxis wählt der Auftraggeber meist den «Gray Box»-Ansatz, bei welchem die Tester die wesentlichen Informationen über das Untersuchungsobjekt wie Netzwerkdesign, IP-Adressen, Betriebssysteme, Applikationen und aktive Sicherheitsmechanismen (z.B. Paket-Filter, Intrusion Detection und/oder Prevention-Systeme etc.) erhalten – Informationen, welche die Tester während der Tests eh erlangen würden. Aber es wird keine wertvolle Projektzeit für die Informationsbeschaffung vergeudet.

Möglich wären aber auch folgende Ansätze: Der «Double Blind»-Ansatz, wo weder die Mitarbeiter des Auftraggebers noch die Tester informiert werden, oder das Gegenteil, der «Tandem»- oder «White Box»-Ansatz, wobei beide Parteien über alles informiert sind. Dazwischen angesiedelt ist auch noch eine vierte Lösung, der «Black Box»-Ansatz, bei dem die Tester keinerlei Informationen über das Untersuchungsobjekt erhalten, aber die Mitarbeiter des Auftraggebers informiert sind.

Einfache Testtypen

Für technische Security Audits existieren (noch) keine allgemeingültigen Bezeichnungen und Definitionen, man kann sie aber anhand ihrer typischen Charakteristika beschreiben. Der simpelste Testtyp ist der **Vulnerability Scan,** eine vollautomatisierte, unprivilegierte Sicherheitsüberprüfung, bei welcher man sich voll auf die Zuverlässigkeit des verwendeten Tools verlassen muss, weil keinerlei manuelle Verifikation der vom Tool angezeigten Sicherheitslücken erfolgt. Die Praxis belegt, dass selbst die besten Tools zu Falschmeldungen neigen – somit darf der praktische Nutzen von Vulnerability Scans in Frage gestellt werden.

Der **Security Scan** behebt dieses Manko teilweise. Er ist eine teilautomatisierte, unprivilegierte Sicherheitsüberprüfung aus der Perspektive eines Angreifers mit Skill-Level «Script Kiddie». Im Gegensatz zum Vulnerability Scan werden von den Tools detektierte Sicherheitslücken (zumindest teilweise) manuell verifiziert, um die Anzahl von Falschmeldungen, welche die Resultate massiv verfälschen können, zu minimieren.

Fortgeschrittene Testtypen

Der **Penetration Test** ist eine intensive, technische, unprivilegierte Sicherheitsüberprüfung aus der Perspektive eines Angreifers mit Skill-Level «Hacker/Cracker». Hier kommen

PROJEKTVERGLEICHBARKEIT SICHERSTELLEN

Wer regelmässig technische Security Audits durchführen lässt, tut gut daran, eine Methode zu wählen, die ermöglicht, das Vorgehen, die Durchführung, die Dokumentation und die Ergebnisse der verschiedenen Projektdurchführungen zu vergleichen.

Das frei verfügbare «Open Source Security Testing Methodology Manual» (OSSTMM) ist eine von Fachleuten laufend überprüfte und erweiterte, weltweit anerkannte Methode, welche diese Anforderungen erfüllt und das Sicherheitsniveau des Untersuchungsobjekts in Form eines neutralen Zahlenwerts darstellt.

überall dort Tools zum Einsatz, wo sie den Projektfortschritt fördern, ohne die Qualität der Tests und Ergebnisse negativ zu beeinträchtigen. Im Vergleich zum Security Scan ist der Anteil an Brainwork und manuell zu leistenden Arbeiten wesentlich höher, was sich auf die Projektdauer und den Preis auswirkt.

Beim **Application Security Audit** handelt es sich um eine ganzheitliche Sicherheitsüberprüfung einer Applikation unter Berücksichtigung technischer und/oder organisatorischer Aspekte. Dabei kommen unprivilegierte und privilegierte Tests zum Zug. Beim Application Security Audit werden die Netzwerk-basierten Tests, welche meist auf Qualitätslevel Penetration Test erfolgen, mit weiteren Methoden wie beispielsweise Configuration Review, Code Review, Reverse Engineering oder Gap-Analysen bezüglich in der Dokumentation beschriebener und in der Applikation tatsächlich implementierter Funktionalität kombiniert.

Ethical Hacking bezeichnet den gezielten Auftragshackerangriff aus der Perspektive eines Angreifers mit Skill Level «Hacker/Cracker». Abhängig vom Projektziel kommen verschiedene Ansätze zum Zug: Der «Shoot all»-Ansatz dient zur taktischen Auslotung des Sicherheitsrisikos und der Folgen, falls ein zum Untersuchungsobjekt gehörendes System kompromittiert wird. Dabei werden mittels Exploiting Design-bedingte Sicherheitslücken wie beispielsweise Mängel im Zonenkonzept oder suboptimale Trusts zwischen Systemen ermittelt, indem alle zur Verfügung stehenden Ressourcen des kompromittierten Systems ausgenutzt werden. Dies kann mittels Post-Exploitation-Techniken wie der Installation von Back Doors, der Nutzung von Tools, welche User-/Administratoren-Zugriffsinformationen auslesen, etc. erfolgen. Der Netzwerkverkehr wird analysiert, um aus dem Datenstrom Zugangsinformationen zu extrahieren. Die erlangten Informationen können anschliessend dazu verwendet werden, um von einem System im Netzwerk auf ein anderes – bis zu diesem Zeitpunkt noch als sicher geltendes System – zu springen.

Im Gegensatz dazu wird beim «Capture the Flag»-Ansatz der Härtungsgrad eines spezifischen Systems ermittelt – es wird dabei nur so lange nach Sicherheitslücken auf dem Zielsystem gesucht, bis eine gefunden wird, welche den Tester zum Ziel führt. Vor Projektstart wird eine Flagge (= Datei, Datenbankeintrag, System etc.) definiert, welche es als Erfolgsnachweis innerhalb eines vorgegebenen Zeitfensters zu ergattern gilt. Die dabei eingesetzten Techniken ähneln denen, welche beim «Shoot all»-Ansatz zum Einsatz kommen. Ausserdem werden oftmals Bots genutzt. Da Ethical Hacking sehr realitätsnah ist, eignet es sich sehr gut, die Reaktion des internen Security-Teams zu testen.

Fazit

Die regelmässige Durchführung technischer Security Audits und insbesondere die zeitnahe Umsetzung daraus resultierender Massnahmenvorschläge schützen präventiv vor den unangenehmen Folgen echter Hackerattacken und steigern nebenbei die Security Awareness aller am Projekt beteiligten Mitarbeiter. Doch Qualität hat seinen Preis: Abgesehen vom vollautomatisierten Vulnerability Scan und dem hochautomatisierten Security Scan, mittels welchen Dutzende Systeme pro Tag getestet werden können, sind die anderen Testtypen wesentlich zeitintensiver. So muss beispielsweise für einen Penetration Test von zirka 5 bis 8 Systemen mit externen Projektkosten ab mindestens fünf Personentagessätzen gerechnet werden, wobei die Obergrenze offen ist.

Christoph Baumgartner ist CEO der auf technische Security Audits spezialisierten, international tätigen OneConsult GmbH.

RECHTLICHE ASPEKTE

Technische Security Audits sind oft nicht von echten Hackerangriffen zu unterscheiden. Deshalb sind jegliche Sicherheitsüberprüfungen ohne explizite vorherige Genehmigung des Systemeigners und -betreibers strafbar und können mit Busse und/oder Haft bestraft werden. In Deutschland ist selbst die Bereitstellung von Tools im Web strafbar, welche für das Hacking verwendet werden könnten.