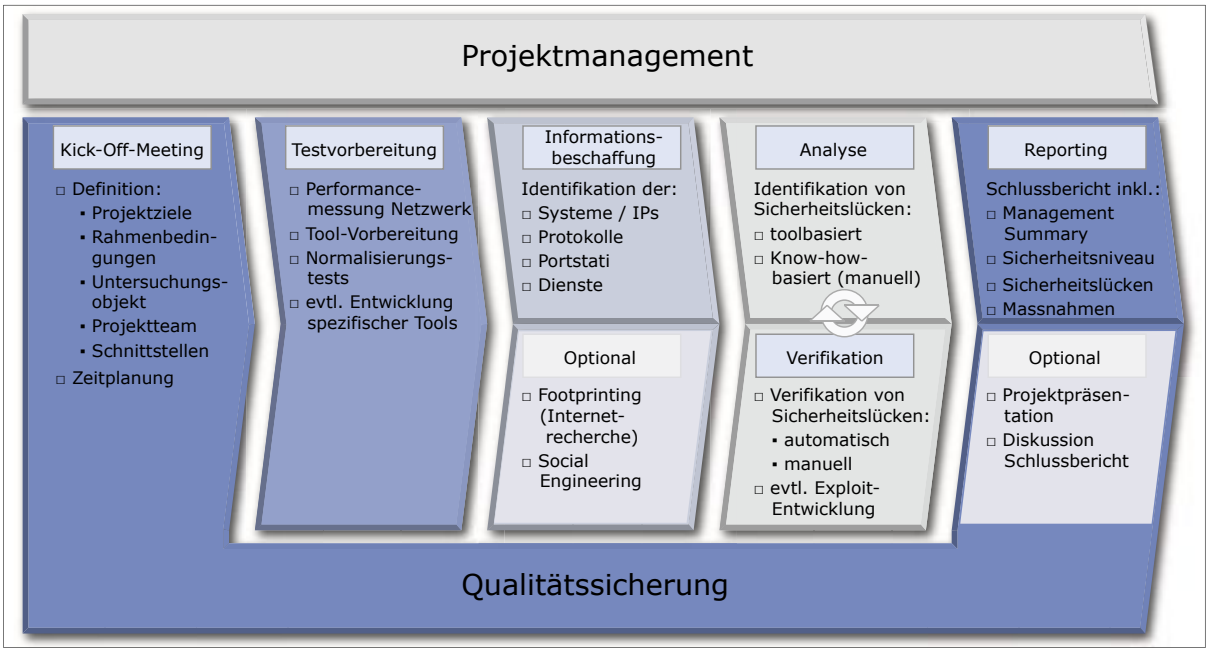
Security Audits: Sicherheitscheck für ICT

Wer die Sicherheit von ICT-Infrastrukturen unter realistischen Bedingungen überprüfen möchte, kommt um technische Security Audits nicht herum. Dieser Artikel bietet eine Übersicht der gängigen Testtypen. VON CHRISTOPH BAUMGARTNER



Stufenplan: Die einzelnen Phasen im Ablauf eines typischen Penetration Testzyklus' von der Planung bis zum Report

Kaum ein Unternehmen mit überregionalem Einzugsgebiet kann es sich leisten, nicht mittels Website im Internet präsent und nicht via E-Mail erreichbar zu sein. Transaktionen, welche noch vor wenigen Jahren zwingend den Besuch eines Ladens oder Bankschalters erforderten, können heute bequem online abgewickelt werden. Generell unterstützt die ICT-Infrastruktur die meisten Geschäftsprozesse und bildet somit die Achillesferse vieler Organisationen. Aus diesem Grund entspricht es den best practices, die ICT-Infrastruktur in regelmässigen Abständen einer technischen Sicherheitsüberprüfung zu unterziehen.

Rechtliche Rahmenbedingungen

Technische Security Audits sind oft nicht von echten Hackerangriffen zu unterscheiden. Hacking ohne explizite vorherige Genehmigung des Systemeigners und -betreibers ist strafbar und kann mit Busse und/oder Haft bestraft werden. In Deutschland wurde die Gesetzeslage kürzlich sogar weiter verschärft: Jetzt steht selbst die Bereitstellung von Tools im Web, welche für das Hacking verwendet werden könnten, unter Strafe. Der anfänglichen Verunsicherung der Security-Tester-Branche folgte die Erkenntnis, dass auch hier die Devise zu gelten scheint: Wo kein Kläger, da kein Richter.

Der konkrete Nutzen

Die Durchführung technischer Audits bringt vielfältigen Nutzen. Es folgt eine Auswahl:

- Aufdeckung von Sicherheitslücken (bevor dies Unberechtigte tun) und Nennung geeigneter Gegenmassnahmen
- Qualitätssicherung dank (unabhängiger) IT-Security-Analyse
- Compliance-Nachweis bezüglich gesetzlicher Rahmenbedingungen, Vorgaben und Normen (z.B. ISO/IEC 27001/17799, SOX, IT GSHB)
- Prävention von Störfällen und damit direkte und indirekte Kosteneinsparungen für die Zukunft
- Awareness Building auf allen Stufen
- Know-how-Transfer (vom Dienstleister in Richtung Auftraggeber)
- Argumentationsgrundlage für zukünftige IT-Security-Projekte und -Aktivitäten

Die verschiedenen Testtypen

Das Gebiet der technischen Audits ist eine relativ junge Disziplin. Deshalb gibt es (noch) keine allgemeingültigen Bezeichnungen. Prinzipiell können alle netzwerkbasierten Tests aus Sicht Internet (Remote Tests) oder vor Ort durchgeführt werden. Ausserdem muss vor der Testdurchführung definiert werden, inwieweit die Mitarbeiter des Auftraggebers über bevorstehende Tests und die Tester über das Untersuchungsobjekt informiert werden.

Christoph Baumgartner ist CEO der auf technische Security Audits spezialisierten OneConsult GmbH, www.oneconsult.com

Falls weder die Mitarbeiter des Auftraggebers noch die Tester informiert werden, spricht man vom Double Blind-Ansatz. Das Gegenteil (also volle Information für alle) wird als Tandem- oder White Box-Ansatz bezeichnet. Beim Black Box-Ansatz erhalten die Tester keinerlei Informationen über das Untersuchungsobjekt, aber die Mitarbeiter des Auftraggebers sind informiert. Beim Gray Box-Ansatz werden die Tester nur teilweise informiert.

«Manches Penetration Test-Schnäppchen entpuppt sich als simpler Security Scan»

Christoph Baumgartner

Bevor ein technischer Security Audit geordert wird, sollte sich der Auftraggeber über das Ziel im Klaren sein: Steht die Suche nach Software-basierten Sicherheitslücken (Betriebssystem und Applikationen) oder die Suche nach Design -basierten Schwachstellen (Architektur)im Fokus? So dienen Security Scans und Penetration Tests primär der Aufdeckung von Software-basierten Sicherheitslücken, es wird also systematisch nach möglichst allen Sicherheitslücken gesucht. Das Ethical Hacking dient primär der Aufdeckung Design-basierter Mängel – was dazu führt, dass nicht nach allen Software-basierten Sicherheitslücken gesucht wird. Der Application Security Audit kann abhängig vom Aktivitätsumfang beides abdecken.

Der **Security Scan** ist eine teilautomatisierte, unprivilegierte Sicherheitsüberprüfung aus der Perspektive eines Angreifers mit Skill-Level «Skript Kiddie». Im Gegensatz zum **Vulnerability Scan** werden von den Tools detektierte Sicherheitslücken zumindest teilweise verifiziert, um die Anzahl von Falschmeldungen, welche die Resultate massiv verfälschen können, zu minimieren. Der **Penetration Test** ist der bekannteste Testtyp. Es handelt sich dabei um eine intensive, technische, unprivilegierte Sicherheitsüberprüfung aus der Perspektive eines Angreifers mit Skill-Level «Hacker/Cracker». Auch hier kommen 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 wesentlich höher.

Beim **Application Security Audit** handelt es sich um eine ganzheitliche Sicherheitsüberprüfung einer Applikation unter Berücksichtigung technischer und/oder organisatorischer Aspekte. Dabei werden unprivilegierte und privilegierte Tests durchgeführt.

Ethical Hacking ist ein gezielter Auftragshackerangriff aus der Perspektive eines Angreifers mit Skill Level «Hacker/Cracker». Je nach Projektziel kommen verschiedene Ansätze zum Zug: Der Shoot all-Ansatz soll das Sicherheitsrisiko und deren Folgen ermitteln, falls ein zum Untersuchungsobjekt gehörendes System kompromittiert wird. Dabei werden mittels Exploiting Design-bedingte Sicherheitslücken ermittelt – beispielsweise suboptimale Trusts zwischen Systemen oder Mängel im Zonenkonzept – 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 werden anschliessend verwendet, um von einem System im Netzwerk auf ein anderes, bis zu diesem Zeitpunkt noch als sicher geltendes System, zu springen.

Der Capture-the-flag-Ansatz dient dazu, die Wahrscheinlichkeit einer erfolgreichen Kompromittierung eines Systems zu ermitteln. Obwohl das Ziel üblicherweise darin besteht, eine spezifische und kritische Komponente zu testen, eignet sich dieser Ansatz auch hervorragend, um die Reaktion des internen Security-Teams im Falle einer Attacke zu testen. Vor Projektstart wird eine Flagge (Daten, E-Mail, System, etc.) definiert, welche es innerhalb eines vorgegebenen Zeitfensters zu ergattern gilt. Die dabei zum Einsatz kommenden Techniken ähneln denen, die beim Shoot-all-Ansatz zum Einsatz kommen. Zudem werden oftmals Bots genutzt. Dieser Ansatz kommt nahe an eine echte Hackerattacke heran.

Merkmale technischer Security Audits

Merkmal	Security Scan	Penetration Test	App. Security Audit	Ethical Hacking
Suche nach Software-basierten Sicherheitslücken	⊕	⊕	⊕	⊖
Suche nach Design-basierten Sicherheitslücken	⊖	⊖	⊕	⊕
Unprivilegierte Tests (ohne Kenntnis der Zugriffsinf.)	⊕	⊕	⊕	⊕
Privilegierte Tests (mit Kenntnis der Zugriffsinf.)	⊖	⊖	⊕	⊕
Automatisierte Suche nach Sicherheitslücken	⊕	⊕	⊕	⊕
Manuelle Suche nach Sicherheitslücken	⊖	⊕	⊕	⊕
Einsatz mehrerer Tools mit ähnlicher Funktionalität	⊖	⊕	⊕	⊕
Nicht-intrusive Verifikation von Sicherheitslücken	⊕	⊕	⊕	⊕
Intrusive Verifikation von Sicherheitslücken	⊖	⊕	⊕	⊕
Gezielte Modifikationen (Accounts, Dateisystem, etc.)	⊖	⊖	⊖	⊕
Technische Massnahmenvorschläge	⊕	⊕	⊕	⊕
Organisatorische Massnahmenvorschläge	⊖	⊕	⊕	⊖
Dokumentation	⊕	⊕	⊕	⊕

Legende: ⊕ = erfüllt ⊖ nicht erfüllt

Methode, Aufwand und Kosten

Wer regelmässig technische Security Audits durchführen lässt, tut gut daran, eine Methode zu wählen, die es möglich macht, das Vorgehen, die Durchführung und die Dokumentation der verschiedenen Projekte 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.

Abgesehen vom hochautomatisierten Security Scan, mittels dem Dutzende Systeme pro Tag getestet werden können, sind die anderen Testtypen wesentlich zeitintensiver. So muss für einen Penetration Test mit externen Projektkosten ab mindestens fünf Personentagessätzen gerechnet werden, wobei die Obergrenze offen ist. Der seitens Auftraggeber zu veranschlagende Zeitaufwand beträgt im Minimum 30 Minuten pro Testtag. Allerdings vergibt der Auftraggeber dann die Chance des Know-how-Transfers in Richtung Mitarbeiter des Auftraggebers.

Fazit: Der Aufwand macht sich bezahlt

Die regelmässige und sorgfältige Durchführung technischer Security Audits und die zeitnahe Umsetzung der daraus resultierenden Massnahmenvorschläge schützen präventiv vor den unangenehmen Folgen echter Hackerattacken und steigern das Sicherheitsbewusstsein der am Projekt beteiligten Mitarbeiter. ■