Wie helfen Penetration Tests die Sicherheit zu erhöhen?

Der Penetration Test ist ein Mittel, um mögliche Fehler zu erkennen und damit die IT-Sicherheit zu erhöhen. Der richtige Partner und ein strukturiertes Vorgehen sind dabei sehr wichtig, um eine qualifizierte Aussage über den Stand der IT-Mittel zu erhalten und diese in Vergleich setzen zu können. Dieser Beitrag zeigt ein mögliches Vorgehen für ein optimales Ergebnis.

Problemstellen

Der IT-Alltag ist oft von Hektik, Stress und finanziellem Druck begleitet. Sehr schnell kann es geschehen, meist unabsichtlich, dass eine Härtungsmassnahme eines Systems nicht oder eine Testregel in der Firewall vergessen geht. Ebenfalls gehören ständige Änderungen, Erweiterungen und Anforderungen am Netzwerk und IT-Systemen zum täglichen Business. Sollte weiter ein Mitarbeiter die Firma verlassen, geschieht die Übergabe oft nicht optimal. Dass dabei die Dokumentation gerne vernachlässigt wird, zeigen diverse Studien und meine persönliche Erfahrung.

Standards

Im Gegensatz zu IT-Revisionen gibt es im Bereich der Penetration Tests weder gesetzliche Vorgaben noch Richtlinien. Somit sind der Ablauf, die Methodik und die Art der Dokumentation offen. Seit einigen Jahren gibt es Versuche, diesen Missstand zu beheben.

Zu den bekanntesten Verfahren gehört sicherlich das Open Source Security Testing Methodology Manuel OSSTMM (http://www.osstmm.org). Das OSSTMM ist bezüglich technischen Security Audits kompatibel zu gängigen Standards und Weisungen wie ISO/IEC 27001/27002, IT-Grundschutzhandbuch, SOX und Basel II. Aufgrund der Praxisorientierung und der Standardkonformität erfreut es sich international wachsender Beliebtheit.

Das BSI (Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de) hat in einen Leitfaden zur Organisation und Durchführung von Penetration Tests mit dem Titel «Durchführungskonzept für Penetrationstests» erstellt. Zusätzlich werden die rechtlichen Rahmenbedingungen dargestellt, die im Umfeld von Penetrationstests zu beachten sind. Die Studie stellt keine Anleitung zum «Hacken» von Netzen und Systemen dar, daher wurde bewusst auf detaillierte technische Anleitungen und Beschreibung von Werkzeugen, die in Penetrationstests verwendet werden, verzichtet. Im November 2014 wurde dieser Leitfaden durch den Praxis-Leitfaden für IS-Penetrationtests ergänzt.

Weiter sehr empfehlenswert ist der inoffizielle Pentest-Standard unter http://www.pentest-standard.org/. Er zeigt die verschiedenen Schritte und Hintergrundinformationen.

Schritte eines Penetration Tests

Der Ablauf eines Penetration Tests sieht in etwa immer gleich aus: Workshop – Testphase – Bericht – Präsentation.

In einem ersten Workshop werden die Ziele der Tests definiert. Hier muss auch klar die Motivation festgehalten werden, die ein potenzieller Hacker aufwenden

kann. Zudem wird festgehalten, wie weit die beauftragten Tester gehen dürfen. Die Möglichkeiten eines gezielten Angriffs umfassen ein Blackbox-Hacking von aussen (überhaupt keine Informationen über die Zielsysteme), ein Hacking mit teilweisem oder komplettem Wissen über die interne Infrastruktur (White- oder Grey-Hacking) und können durch netzwerkinterne Tests inkl. Social Engineering erweitert werden.

Die Testphase wird anschliessend ausführlich beschrieben. Daher hier nur zwei Bemerkungen. Wichtig ist es, nie das Ziel der Tests aus den Augen zu verlieren. Schnell kann es in der Flut von Informationen geschehen, dass ein falscher Weg eingeschlagen wird. Im Gegensatz steht dazu, dass die Kreativität der Angriffe nicht ausser Acht gelassen werden darf. Ein stures Vorgehen nach Checklisten zeigt oft nicht das ganze Bild.

Der Bericht und die Präsentation zeigen das Vorgehen, die eingesetzten Tools sowie die Erkenntnisse aus den Ergebnissen. Sollten Schwachstellen ersichtlich sein, sind diese mit Massnahmen zu versehen und in einer Prioritätenliste festzuhalten. Soweit möglich sind Zusammenhänge aufzuzeigen und in einem gesamtheitlichen Bild darzustellen.

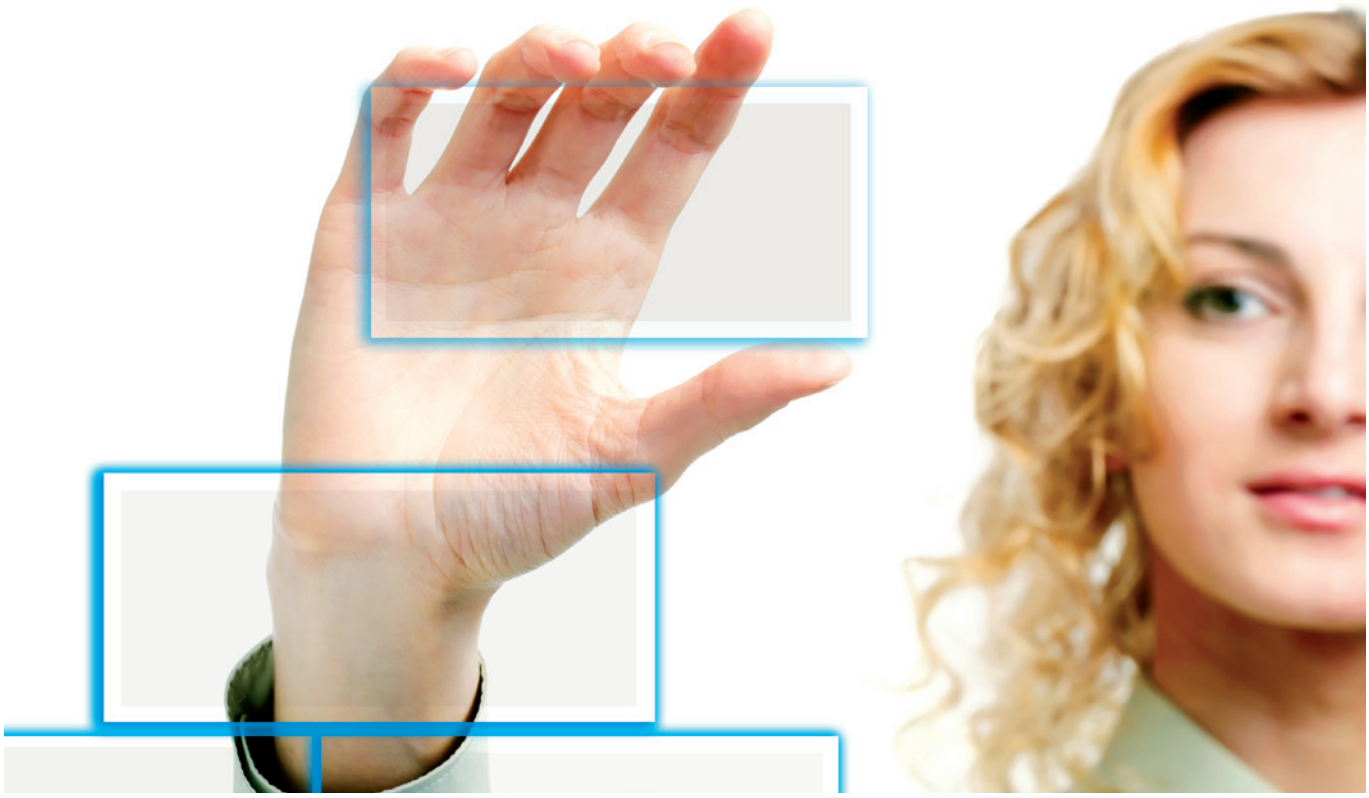
Der Penetration Test

Der erste Schritt des Penetration Tests umfasst die Informationssuche. Welche Informationen sind im Internet verfügbar, sei dies auf der Homepage des Unternehmens oder via eine Suchmaschine wie zum Beispiel von Google? Auch Seiten zur Stellensuche sind eine gute Quelle. Sucht die Firma zum Beispiel nach Oracle-Spezialisten, wird vermutlich auch Oracle als Datenbanklösung eingesetzt. Auch spannend sind so genannte Success Stories, in denen ein Lieferant ausführlich beschreibt, welche Lösung er bei der zu untersuchenden Firma platziert hat. Das Internet vergisst dabei nichts. Wurde zum Beispiel in einem Forum eine (technische) Frage platziert, kann diese auch nach Jahren noch abgerufen werden. Ebenfalls sind Namen von Personen, eventuell sogar mit einer E-Mailadresse versehen, ideal für die weiteren Angriffe.

Weitere Informationen liefern WHOIS und DNS. Was sind für Angaben zu den IP-Adressen festgehalten? Verfügt das Unternehmen über weitere IP-Adressen? Welche Informationen stehen in den DNS-Einträgen? Kann gar ein kompletter Zonentransfer ausgeführt werden?

Nachdem bereits viele Informationen zur Verfügung stehen, gilt es das Angriffsziel einzuschränken. Ein IP- und Portscan liefert die dazu notwendigen Informationen. Es soll geklärt werden, welche IP-Adressen antworten und welche offenen Ports im Internet ersichtlich sind. Daraus leiten sich die «interessanten» Ziele ab. In der Regel antworten die «Standard-Ports» (d. h. Ports, die bekannt sind, oft unter 1024, beispielsweise Port 80 für HTTP). Die Erfahrung zeigt, dass sich viele spannende Ports auch oberhalb der 50'000-Grenze befinden. Es lohnt sich, trotz grossem Zeitbedarf, alle 65'535 möglichen Ports durchzusehen. Gleichzeitig mit dem offenen Port sollte die entsprechende Header-Information ausgelesen werden. Viele Systeme sind sehr auskunftsfreudig und teilen mit, wer sie sind und vor allem in welcher Version sie vorliegen. Eine Schwachstellen-Suche in öffentlichen Vulnerability-Datenbanken zeigt, ob sich das antwortende Programm auf dem aktuellsten Softwarestand befindet oder nicht. Falls nicht, sind vermutlich bereits Tools im Internet verfügbar, die gegen diese Schwachstelle eingesetzt werden können (so genannte Exploits).

Als weitere Möglichkeit stehen Vulnerability-Scanner auf der Liste. Diese verursachen jedoch einen grossen «Lärm». Je nachdem ob alle Personen der zu untersuchenden Firma Bescheid wissen,



können diese bereits zu einem frühen Zeitpunkt eingesetzt werden. Sie dienen dazu, nebst den bereits erwähnten Ports, auch Informationen zum Betriebssystem, Banner (Antworten auf Anfragen), Kontrolle von bekannten Sicherheitslücken, Verbesserungsvorschlägen und automatisch generierten Berichten zu erstellen.

Nach diesen Tests stehen sehr viele Informationen zur Verfügung, die es je nach Auftrag gilt, weiter zu verwerten. So können CGI-Skripts missbraucht, SQL-Abfragen manipuliert und Schwachstellen in der gefundenen Software ausgenutzt werden. Loginangaben für Webseiten, E-Mail, FTP, VNC, RDP und vielen weiteren Programmen können durch Dictionary (d.h. durch Wörterbücher) oder Brute Force (dem «wilden» Durchprobieren) Attacken geknackt werden. Hier benötigt es aber oft viel Zeit, ausser es werden schwache Passworte verwendet.

Andreas Wisler (CISSP, CISA, ISO 22301 + 27001 Lead-Auditor) ist Geschäftsführer und Senior-Security-Auditor bei der goSecurity GmbH, welche IT-Sicherheitsüberprüfungen und -beratungen durchführt. Weiter unterrichtet er unter anderem an der Fachhochschule Nordwestschweiz FHNW IT-Sicherheitsthemen.

Zusammenfassung

Diese Tests sind in der Regel nicht in einem Tag durchzuführen. Zu vielfältig sind die möglichen Angriffsflächen. Neben der Definition der eigenen Sicherheitsbedürfnisse gehört zu einem funktionierenden Sicherheits-Regelkreis das kritische Hinterfragen, ob die definierten Ziele mit den getroffenen Massnahmen erreicht wurden. Der Penetration Test liefert dabei eine unparteiische Drittmeinung. Das strukturiere Vorgehen hilft, mögliche Schwachstellen zu erkennen und geeignete Massnahmen zur Behebung zu treffen.