Quelle: iStockphoto

Sicherheit erhöhen

Penetration Tests sind ein Mittel, um Fehlerquellen zu erkennen und die IT-Sicherheit zu erhöhen. Ein strukturiertes Vorgehen ist dabei wichtig, um eine qualifizierte Aussage über den Stand der IT-Mittel zu erhalten.

ANDREAS WISLER

Der IT-Alltag ist oft von Hektik und Stress begleitet. Sehr schnell kann es geschehen, meist unabsichtlich, dass eine Härtungsmassnahme nicht oder eine Testregel in der Firewall vergessen geht. Ebenfalls gehören ständige Änderungen und Erweiterungen am Netzwerk zum täglichen Business. Sollte dann ein Mitarbeiter zusätzlich die Firma verlassen, geschieht die Übergabe oft nicht optimal. Dass dabei die Dokumentation gerne vernachlässigt wird, zeigen diverse Studien. Nicht vergessen werden dürfen die regelmässigen Änderungen an Systemen und an der Software durch Patches und Updates. Aus diesen Gründen lautete bereits 1993 der Usenet-Ausspruch von Dan Farmer und Wietse Venema: «Improving the security of your site by breaking into it».

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 technischer 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 Zusammenarbeit mit BDO und Ernst & Young 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 Penetration Tests 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.

Vom US-amerikanischen National Institute of Standards and Technology (NIST) wurde der «Technical Guide to Information Security Testing» erstellt und befindet sich seit November 2007 im Draft-Status. Vom EC-Council steht zudem die Möglichkeit zur Verfügung, sich als Ethical Hacker zertifizieren zu lassen.

Schritte eines Penetration Tests

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

Workshop

In einem ersten Workshop werden die Ziele der Tests definiert. Hier muss auch klar die Motivation festgehalten werden, die ein potentieller Hacker aufwenden kann. Zudem wird festgehalten, wie weit die beauftragten «Hacker» gehen dürfen. Die Möglichkeiten eines gezielten Angriffs umfassen ein Blackbox-Hacking von Aussen, ein Hacking mit teilweisem oder komplettem Wissen über die interne Infrastruktur (White- oder Grey-Hakking) und können durch netzwerkinterne Tests inkl. Social Engineering erweitert

werden. Wichtig hier sind die rechtlichen Spielregeln und die Vertraulichkeitsvereinbarung.

Testphase

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.

Bericht

Der Bericht zeigt 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.

Präsentation

Die Präsentation ist analog aufgebaut. Da Penetration Tests oft von der Geschäftsleitung in Auftrag gegeben werden, sollte dies für die Präsentation beachtet und entsprechend umgesetzt werden. Es hilft nichts, Ergebnisse schön zu malen, sondern nüchtern und ohne Bewertung wiederzugeben. Es liegt im Ermessen und dem notwendigen Fingerspitzengefühl des Prüfers, mit dieser Situation umzugehen. Schlussendlich geht es immer darum, die Verbesserung der IT-Sicherheit voranzutreiben.


Quelle: shutterstock

Die Fülle an gewonnenen Informationen sollte in einem Audit zur Behebung der Schwachstellen genutzt werden.

Die Werkzeuge

An dieser Stelle ist es nicht möglich, auf alle zur Verfügung stehenden Werkzeuge einzugehen. Praktisch für jeden möglichen und unmöglichen Zweck steht ein Programm oder Tool bereit. Täglich stossen neue dazu. Bei der Beschreibung des Vorgehens wird jeweils auf ein Programm hingewiesen, viele davon stammen aus der Open Source-Szene. An dieser Stelle erwähnenswert sind sicherlich die so genannten Exploit Frameworks. Sie beinhalten eine Sammlung von diversen Werkzeugen unter einer einheitlichen Oberfläche, meistens direkt bootbar von einer Standalone-CD-ROM. Eines davon ist das Metasploit Framework (http://www.metasploit.com/), welches kostenlos verfügbar ist.

Flinke Finger, Know-how und die richtigen Tools: mehr braucht es oftmals nicht, um in ein System eindringen zu können.


Quelle: iStockphoto

Quelle: iStockphoto

Frei erhältliche Hacker-Tools gibt es zuhauf. Und mit etwas Geduld ist das schwächste Glied rasch aufgefunden. Acces granted!

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 Suchmaschine (z.B. Google). Auch Seiten zur Stellensuche sind eine gute Quelle. Sucht die Firma zum Beispiel nach Oracle Spezialisten, wird vermutlich auch Oracle als Datenbanklösung eingesetzt. Das Internet vergisst dabei nichts. Wurde in einem Forum eine Frage platziert, kann diese auch nach Jahren noch abgerufen werden. Ebenfalls sind Namen von Personen, evtl. sogar mit einer E-Mail-Adresse 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? Ist dies der Fall, sind auf einen Blick alle Anlaufstellen der Firma bekannt. Interessant sicherlich A-Einträge zu Web- und Mailservern. Der MX-Eintrag zeigt, welchen Weg die E-Mails ins Unternehmen nehmen. Ein SPF (Sender Policy Framework) zeigt zusätzlich, ob Mails via andere Wege ins Internet gelangen (zum Beispiel im Falle eines Backup-Mailservers). Ein Tool zur einfachen Informationssuche bildet SamSpade, welches Funktionen zu WHOIS, Ping, Traceroute und DNS in einer grafischen Oberfläche bietet. Alles ist zwar auch von der Kommandozeile möglich, aber mit diesem Tool geht es doch etwas einfacher.

IP- und Portscan

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 «Standardports» (d.h. Ports, die bekannt sind, oft unter 1024). Die Erfahrung zeigt, dass sich viele spannende Ports auch oberhalb der 50 000er Grenze befinden. Es lohnt sich, trotz grossem Zeitbedarf, alle 65 535 möglichen Ports durchzusehen. Gleichzeitig mit dem offenen Port sollte die Header-Information ausgelesen werden. Viele Systeme sind sehr auskunftsfreudig und teilen mit, wer sie sind und vor allem in welcher Version sie vorliegen. Eine erneute Suche im Internet 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 (genannt Exploits).

Zu den gängigsten Scan-Programmen gehört sicherlich NMap (http://www.nmap.org), welches auch unbemerkt IP- und Portscans durchführen kann. Ein Aufruf könnte zum Beispiel «nmap –sS –O –p1-65535 <IP>» lauten. Damit wird der Test im Stealth Scan Modus durchgeführt (d.h. der TCP-Verbindungsaufbau wird nicht komplett durchgeführt und somit evtl. auf der angegriffenen Seite auch nicht geloggt), mit –O wird zusätzlich versucht, das Betriebssystem herauszufinden. Der letzte Parameter sagt aus, dass alle 65 535 Ports durchgescannt werden.

Vulnerabilität

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. Eines dieser Programme ist Nessus, welches im Client-/Server-Prinzip funktioniert. Dabei wird der Server auf einem Unix-System installiert. Der Client kann via SSL eine Verbindung darauf aufbauen und die entsprechenden Routinen starten. Mit diesen Plugins lassen sich diverse Sicherheitslücken des Betriebssystems bzw. der Dienste, die auf dem zu scannenden Host laufen, finden. Wichtig: bei allen Programmen kann es zu Fehlalarmen kommen. Eine manuelle Nachkontrolle ist daher zwingend notwendig.

Fülle von Informationen

Nach diesen Tests stehen sehr viele Informationen zur Verfügung, die es, je nach Auftrag, gilt, weiter auszuwerten. So können CGI-Skripts missbraucht, SQL-Abfragen manipuliert und Schwachstellen in der gefundenen Software ausgenutzt werden. Login-Angaben für Webseiten, Mail, FTP, VNC, RDP und viele weitere Programme können durch Dictionaries (Wörterbücher) oder Brute Force-Attakken («wildes» Durchprobieren) geknackt werden. Hier benötigt es aber oft viel Zeit, ausser es werden schwache Passworte verwendet.

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.

Der Autor: Andreas Wisler ist Sicherheitsspezialist und Mitglied der Geschäftsleitung der GO OUT Production GmbH.