Kontrollierter Einbruch

Penetration Tests erhöhen die Sicherheit

Der Penetration Test ist ein Mittel, um mögliche Fehler in der IT-Infrastruktur zu erkennen und damit die 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.

Autor: Andreas Wisler

Der IT-Alltag ist oft von Hektik und Stress begleitet. Sehr schnell kann es geschehen, meist unabsichtlich, dass eine Härtungsmassnahme nicht umgesetzt wird 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.

Zum Autor

Andreas Wisler (Tel.: 052 320 91 20) Dipl. Ing. FH, CISSP, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. System Hardening rundet das Profil ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.

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 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, 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 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.

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, ein Hacking mit teilweisem oder komplettem Wissen über die interne Infrastruktur (White- oder Grey-Hacking) und können durch netzwerkinterne Tests inklusive Social Engineering erweitert werden.

Die Testphase: 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 erklären 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 über eine Suchmaschine? 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 nichts. Wurde in einem Forum eine Frage platziert, kann diese auch nach Jahren noch abgerufen werden. Ebenfalls sind Namen von Personen, vielleicht sogar mit einer Emailadresse versehen, ideal für die weiteren Angriffe.

Nachdem bereits viele Informationen zur Verfügung stehen, gilt es das Angriffsziel einzuschränken. Ein IP- und Portscan liefert die dazu notwendigen Hinweise. Es soll geklärt werden, welche IP-Adressen antworten und welche offenen Ports, also »Türen« zum System, im Internet ersichtlich sind. Daraus leiten sich die interessanten Ziele ab. Es lohnt sich, trotz grossem Zeitbedarf, alle 65.535 möglichen Ports durchzusehen. 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).

Als weitere Möglichkeit stehen Vulnerability Scanner auf der Liste. 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 (je nach Auftrag) weiterverwertet werden. So können CGI-Skripts (Austausch zwischen Website und User) missbraucht, SQL-Abfragen manipuliert und Schwachstellen in der gefundenen Software ausgenutzt werden. Loginangaben für Webseiten, Mail, FTP und viele weitere Programme können durch Dictionarys (Wörterbücher) oder Brute Force Attacken (»wildes« Durchprobieren) geknackt werden. Dies benötigt aber oft viel Zeit, ausser es werden schwache Passwörter 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. ♦