

THE BEST-RUN BUSINESSES RUN SAP



Secologic

Leitfaden

Applikationspenetrationstest

Version 1.0 – März 2007

Dieses Material wird von der SAP AG zur Informationszwecken zur Verfügung gestellt, ohne Haftung für Fehler oder Auslassungen in dieser Publikation. Des Weiteren übernimmt SAP keine Garantie für die Exaktheit oder Vollständigkeit der Informationen, Texte, Grafiken, Links und sonstigen in dieser Publikation enthaltenen Elementen. Diese Publikation wird ohne jegliche Gewähr, weder ausdrücklich noch stillschweigend, bereitgestellt. Dies gilt u. a., aber nicht ausschließlich, hinsichtlich der Gewährleistung der Marktgängigkeit und der Eignung für einen bestimmten Zweck sowie für die Gewährleistung der Nichtverletzung geltenden Rechts.

SAP haftet nicht für entstandene Schäden. Dies gilt u. a. und uneingeschränkt für konkrete, besondere und mittelbare Schäden oder Folgeschäden, die aus der Nutzung dieser Materialien entstehen können. Diese Einschränkung gilt nicht bei Vorsatz oder grober Fahrlässigkeit.

Die gesetzliche Haftung bei Personenschäden oder Produkthaftung bleibt unberührt. Die Informationen, auf die Sie möglicherweise über die in diesem Material enthaltenen Hotlinks zugreifen, unterliegen nicht dem Einfluss von SAP, und SAP unterstützt nicht die Nutzung von Internetseiten Dritter durch Sie und gibt keinerlei Gewährleistungen oder Zusagen über Internetseiten Dritter ab.

Dieses Material wurde von der SAP mit Unterstützung des Fraunhofer Institut ‚Sichere Informations-Technologie‘ (SIT) im Rahmen des Forschungsprojektes *secologic* erstellt. *Secologic* (Laufzeit 2005 - März 2007) wird gefördert vom Bundesministerium für Wirtschaft und Technologie (BMWi). Wir danken dem BMWi für die Unterstützung des Projektes.

Weitere Informationen zu dem Projekt finden Sie unter www.secologic.de. Bei Fragen und/oder Anregungen zu diesem Dokument wenden Sie sich bitte an Rosemaria Giesecke (rosemaria.giesecke@sap.com).

Inhalt

Überblick.....	2
1 Grundlagen	6
1.1 Was ist ein Penetrationstest?	6
1.2 Testverfahren	9
1.3 Warum Penetrationstests?	10
1.4 Was testen?	11
1.5 Wann testen?	13
1.6 Aufwand und Kosten	13
2 Anbietersauswahl	16
2.1 Können wir das nicht selbst machen?	16
2.2 Fachliche Kriterien	17
2.3 Organisatorische Kriterien	19
2.4 Kompetenznachweise	20
2.5 Rotation	21
3 Vertrag und Informationsaustausch	23
3.1 Vertragliche Regelungen	23
3.2 Technische Informationen	24
3.3 Projektmanagement	26
4 Dokumentation	28
4.1 Testplan	28
4.2 Ergebnisbericht	28
5 Ablauf und Checklisten	30
5.1 Vorbereitung	30
5.2 Anbietersauswahl und Vertrag	31
5.3 Detailplanung und Organisation	32
5.4 Test	34
5.5 Ergebnisse und Projektabschluss	34
Anhang A Beispiel: Testplan	36



Anhang B Beispiel: Ergebnisbericht..... 38
Literatur..... 41

Überblick

Dieser Leitfaden soll kleine und mittelständische Unternehmen dabei unterstützen, Penetrationstests zur Prüfung ihrer IT-Sicherheit einzusetzen. Er enthält Erläuterungen und Handlungsempfehlungen für IT-Verantwortliche, die externe Anbieter mit solchen Tests beauftragen möchten. Die eigentlichen Testverfahren werden nicht im Detail behandelt.

Neben einem kurzen Überblick über Sinn, Zweck, Möglichkeiten und Grenzen von Penetrationstests gibt der Leitfaden Empfehlungen zur Anbieterauswahl, zur Auftragsgestaltung, zum Projektablauf und zur Dokumentation. Checklisten im Anhang fassen diese Empfehlungen zusammen.

1 Grundlagen

Kein Unternehmen kann sich Sicherheitslücken der eigenen Infrastruktur leisten. Jeder Systemausfall und / oder an die Öffentlichkeit gelangte interne Informationen bedeuten einen Wettbewerbsnachteil und damit direkt oder indirekt entgangene Gewinne. Um diese zu vermeiden, werden Sicherheitskonzepte entwickelt, Gefährdungen erkannt und Gegenmaßnahmen implementiert. Viele Gesetzliche Regelungen oder eine interne Sicherheitspolitik fordern regelmäßige IT – Sicherheitsaudits um die Qualität der implementierten Sicherheitsmaßnahmen zu gewährleisten. Der Penetrationstest ist ein wichtiger Bestandteil eines Sicherheitsaudits.

Bevor das Management über einen Penetrationstest entscheidet, muss es notwendige Informationen über die Durchführung von Penetrationstest in der Hand haben. In diesem Dokument werden die wichtigen Informationen über Penetrationstest in kompakter Form beschrieben.

1.1 Was ist ein Penetrationstest?

Penetrationstests werden genutzt um Sicherheitsschwachstellen in IT-Systemen zu identifizieren. Um einen möglichen realen Angriff so gut wie möglich zu simulieren, werden vom Tester dieselben Angriffstechniken angewendet, die ein böswilliger Angreifer einsetzen würde.

Derzeit gibt es zwei offizielle Dokumente, welche die Abläufe bei Penetrationstests beschreiben: das Open Source Security Testing Methodology Manual (OSSTMM), Version 2.2 [3] und die Studie „Durchführungskonzept für Penetrationstests“ [2] vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

In der BSI-Studie werden Penetrationstests wie folgt beschrieben:

„Durch Penetrationstest kann geprüft werden, inwieweit die Sicherheit der IT-Systeme durch Bedrohungen von Hackern, Crackern, etc. gefährdet ist bzw. ob die IT-Sicherheit durch die eingesetzten Sicherheitsmaßnahmen aktuell gewährleistet ist“ [2].

Sicherheits-Audit vs. Penetrationstest

Penetrationstests werden häufig als Sicherheits-Audit bezeichnet, was aber grundlegend falsch ist.

Während Penetrationstests auf die technische Umgebung abzielen und eine Momentaufnahme des IT-Systems darstellen, dienen Sicherheits-Audits der generellen Überprüfung der IT-Infrastruktur. Bei der Durchführung von Sicherheits-Audits werden nicht nur die aktuellen technischen Einstellungen überprüft, sondern auch Ordnungsmäßigkeit, Effizienz, Effektivität etc. genauer betrachtet.

So wird z.B. im Rahmen eines Penetrationstests nicht geprüft, ob bestimmte Daten im Falle eines Hardwareschadens durch regelmäßige Datensicherung wiederherstellbar wären, sondern nur, ob auf diese Daten Zugriff erlangt werden könnte. Dies wird möglicherweise auch im Rahmen eines Sicherheits-Audits bzw. im Rahmen einer IT-Revision geprüft, üblicherweise aber aus einer anderen Perspektive und auch nicht in der technischen Tiefe, die einen Penetrationstest auszeichnet [2].

Ein Sicherheitsaudit soll nachweisen, dass das angestrebte Sicherheitsniveau erreicht wird. Dazu sind die Sicherheitsmaßnahmen auf Vollständigkeit, Angemessenheit und richtige Umsetzung zu prüfen. Ein Penetrationstest hat im Gegensatz dazu das Ziel, Schwächen im Konzept oder seiner Umsetzung aufzudecken.

Penetrationstests können Bestandteil eines Sicherheits-Audits sein.

Was leisten Penetrationstests?

Penetrationstests können Fehler und unerwartete Wechselwirkungen in der Software oder der Konfiguration eines Systems aufdecken. Wie alle Testverfahren eignen sie sich jedoch nicht dazu, die Fehlerfreiheit nachzuweisen. Nicht zuverlässig aufdecken lassen sich insbesondere bewusst eingebaute und versteckte Hintertüren.

Regelmäßige Penetrationstests sind kein Ersatz für sichere Software oder ein angemessenes Sicherheitsmanagement. Sie unterstützen lediglich die Einführung und den Betrieb sicherer Systeme.

Penetrationstests liefern keine Sicherheitszertifikate. Sie führen auch nicht unmittelbar zu einem umfassenden Sicherheitskonzept; die Ergebnisse können jedoch in ein solches einfließen.

Testumfang

Ein Penetrationstest kann sich auf:

- ein einzelnes System
- eine technische Infrastruktur, z.B. ein Netz
- eine ganze Firma, Niederlassung oder Abteilung beziehen

Im letztgenannten Fall gehören auch zum Beispiel der physische Zugangsschutz und das Verhalten der Mitarbeiter zum Testumfang; Social Engineering ist eine typische und oft erfolgreiche Methode jenseits der Technik. Solche umfassenden Tests bleiben in diesem Leitfaden unberücksichtigt.

Automatisierung

Gut automatisieren lässt sich die Suche nach schlecht gepflegten Systemen. Scanner wie Nessus untersuchen Systeme anhand einer Bibliothek auf bekannte Schwachstellen in verbreiteten Anwendungen und Betriebssystemen. Dazu gehören insbesondere fehlende Patches und einige Konfigurationsmängel.

Soll ein Test über solche grundlegenden Untersuchungen hinausgehen oder weicht das Testziel von den Fähigkeiten solcher Scanner ab, so ist Handarbeit unumgänglich. Zwar steht eine große Zahl von Tools zur Verfügung, sie decken jedoch nur einzelne Aspekte ab und bedürfen der Anpassung oder des gezielten Einsatzes durch erfahrenes Personal. Ihre Ergebnisse müssen interpretiert und gefiltert werden. Automatisch generierte Reports liefern in solchen Fällen kein befriedigendes Ergebnis.

1.2 Testverfahren

Black-Box-Test

Ein Black-Box-Test erfolgt aus der Perspektive eines Angreifers, der zunächst keine Informationen über Interna besitzt. Solche Informationen zu gewinnen ist Bestandteil des Tests.

Effektive Black-Box-Tests erfordern ein gutes Verständnis der Sicherheitsziele und der schutzwürdigen Objekte und Werte. Andernfalls lassen sich die Ergebnisse nur schwer interpretieren, da das Bezugssystem fehlt.

Echte Black-Box-Tests an Produktivsystemen sind riskant: ohne jegliches Wissen über den inneren Aufbau eines Systems oder Netzes kann der Tester schwer entscheiden, welche Methoden mit dem Risiko einer Betriebsstörung oder eines Datenverlusts verbunden sind.

White-Box-Test

Für einen White-Box-Test steht den Testern idealerweise jegliche Information über den Testgegenstand offen, bis hin zu Programmquelltexten, Konfigurationsdateien, interner Dokumentation usw. Die verbreitete Nutzung von Closed-Source-Produkten setzt diesem Ansatz eine natürliche Grenze. Zudem kann ein White-Box-Test aufgrund der großen Informationsfülle leicht ausufern. Ziele und Einzeluntersuchungen müssen deshalb klar priorisiert werden.

White-Box-Tests können auch solche Schwachstellen aufdecken, die ohne Kenntnis der Interna schwer zu finden, bei Kenntnis aber leicht auszunutzen sind. Sie berücksichtigen damit auch die Insider-Perspektive.

Grey-Box-Test

In der Praxis nutzt man meist Mischformen, die als Grey-Box-Test bezeichnet werden. Welche Informationen die Tester nutzen, richtet sich dabei vor allem nach der Ver-

füchtigkeit. Die vorhandene oder angeforderte Dokumentation wird im Test verwendet; fehlt sie oder reicht sie nicht aus, so greifen die Tester zu Black-Box-Verfahren.

Generell empfiehlt es sich für Auftraggeber, den Testern keine verfügbaren Informationen vorzuenthalten. Ihre Verwendung kann den Testern und damit dem Auftraggeber einen Vorsprung vor echten Angreifern verschaffen.

1.3 Warum Penetrationstests?

Es gibt viele Gründe dafür, warum ein Penetrationstest durchgeführt werden sollte. Einige sind im Folgenden beschrieben.

Sorgfaltspflichten

Sorgfaltspflichten des Unternehmens ergeben sich aus einer Reihe von Gesetzen[2]. Beispiele sind:

- Handelsgesetzbuch (HGB)
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Kreditwesengesetz (KWG)
- Verordnungen und Verlautbarungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin)
- Bundesdatenschutzgesetz (BDSG)
- Staatsvertrag für Mediendienste (MDStV)
- Teledienstegesetz (TDG) und Teledienstedatenschutzgesetz (TDDSG)

Teilweise werden auch konkrete organisatorisch-technische Maßnahmen gefordert, etwa für die Verarbeitung personenbezogener Daten. Keines dieser Gesetze fordert unmittelbar Penetrationstests. Die Überprüfung der getroffenen Vorkehrungen ist jedoch Bestandteil der erforderlichen Sorgfalt.

Haftungs- und Imagerisiken

Unzureichende oder unwirksame Sicherheitsvorkehrungen können im Schadensfall zur Haftung, zu Imageschäden sowie zu Eingriffen durch Aufsichtsbehörden führen. Beispielhaft, wenngleich nicht im hiesigen Rechtsraum angesiedelt, ist der Fall der US-Firma Guidance Software [8]. Nach einem Servereinbruch, bei dem die Täter Kunden- und Kreditkartendaten kopierten, wurde die Aufsichtsbehörde FTC aktiv. Die Firma muss nun umfassendes Sicherheitsprogramm umsetzen und zehn Jahre lang unabhängig prüfen lassen.

Sicherheitsmanagement

Zum Sicherheitsmanagement gehört neben der Festlegung von Zielen, Maßnahme, Verantwortlichkeiten usw. auch deren Prüfung. Penetrationstests bieten eine Prüfmöglichkeit, die sich auf die Effektivität der getroffenen Vorkehrungen konzentriert. Der Einsatz externer Tester verringert die Gefahr von Betriebsblindheit; die Testmethode geht von der Sicht eines Angreifers aus, der sich nicht um formale Prozesse und Dokumente kümmert, sondern ein Ziel verfolgt.

Industriestandards und individuelle Verträge

Individuelle Verträge mit Kunden und Partnern sowie Industriestandards können ebenfalls Penetrationstests fordern oder nahelegen. Ein Beispiel ist der *Payment Card Industry Data Security Standard (PCI-DSS)*, zu dessen Einhaltung Kreditkartenunternehmen alle Händler verpflichten, die Kartenzahlungen annehmen möchten. Er sieht regelmäßige Penetrationstests ausdrücklich vor.

1.4 Was testen?

Besondere Aufmerksamkeit verdienen naturgemäß Systeme und Anwendungen mit hohem Schutzbedarf:

- Von außen erreichbare Anwendungen, z.B. auf öffentlichen Websites an Schnittstellen zu anderen Unternehmen
- Sicherheitskomponenten, z.B. Firewalls

- Geschäftskritische Anwendungen, z.B. Dokumentenmanagement- und ERP-Systeme
- Anwendungen, die besonders gefährdete Daten verarbeiten, z.B. Kunden- oder Kreditkartendaten
- Hilfskomponenten solcher Anwendungen, z.B. Datenbanksysteme, insbesondere wenn sie von mehreren Anwendungen genutzt werden

Weniger verbreitet sind Penetrationstests für einzelne Arbeitsplatzsysteme. Sie können dennoch sinnvoll sein, wenn Arbeitsplätze zu den oben genannten Systemen gehören, ein firmenweites Standard-Setup geprüft werden soll oder besondere Sicherheitsanforderungen bestehen.

Testmöglichkeiten

Allgemeine Standardsoftware, z.B. Betriebssysteme, lässt sich aus Anwendersicht nur sehr beschränkt testen. Der Schwerpunkt liegt hier zwangsläufig auf der individuellen Konfiguration und Härtung und anderen Ergebnissen des Sicherheitsprozesses.

Standardsoftware für Unternehmensanwendungen, etwa ERP- und ECM-Systeme, wird in der Regel für den Einsatz individuell angepasst und erweitert sowie mit anderen Systemen integriert. Ein Penetrationstest sollte hier neben der individuellen Konfiguration auch alle unternehmensspezifischen Erweiterungen und Besonderheiten berücksichtigen.

Individualsoftware gestattet prinzipiell tiefgehende Untersuchungen bis hin zu Quellcode-Reviews. Eine wirtschaftliche Grenze setzt jedoch der erforderliche Aufwand. Sinnvoll ist es, die Qualitätssicherung primär den Entwicklern zu überlassen, deren Erfolg jedoch durch Penetrationstests zu prüfen und zu überwachen. Penetrationstests sollten in diesem Fall Teil eines Gesamtkonzepts zur Entwicklung eines sicheren Systems sein, dessen Beschreibung jedoch den Rahmen dieses Leitfadens sprengen würde.

1.5 Wann testen?

Penetrationstests eignen sich als Methode vor allem zur Untersuchung fertiger Anwendungen, d.h. aus Anwendersicht für die Einführung und den Betrieb einer Anwendung.

In der Einführungsphase liefern Tests Hinweise auf erforderliche Maßnahmen zur Härtung und Sicherung des Systems. Häufig sind sie schlecht dokumentiert, so dass der Anwender zwangsläufig zur Selbsthilfe greifen muss, um sein Sicherheitskonzept zu vervollständigen. Mehr noch als für Standardsoftware gilt dies für individuelle Erweiterungen und Anpassungen. Ebenfalls bereits in der Einführungsphase kann das spezifische Einsatzszenario und das Zusammenspiel mit anderen Systemen in der Umgebung auf Sicherheitsmängel untersucht werden.

Während des Betriebs dienen Penetrationstests dazu, die Erhaltung des anfangs geschaffenen Sicherheitsniveaus zu prüfen. Anwendungssysteme degenerieren im Laufe der Zeit durch Eingriffe der Administratoren und Nutzer, Änderungen in ihrer IT-Umgebung (z.B. Netztopologie und –komponenten), das Einspielen oder Unterlassen von Patches und andere Faktoren. Auch kommen zuweilen neue Bedrohungen, Risiken und Angriffsarten hinzu, die bei der Einführung noch nicht bekannt waren.

Größere Modifikationen oder Migrationen sollten wie die Neueinführung behandelt werden.

1.6 Aufwand und Kosten

Eine allgemeingültige Aufwandsschätzung ist schwer zu geben. Welcher Aufwand sinnvoll ist, hängt von mehreren Faktoren ab:

Komplexität des Systems und Testabdeckung

Sie ergibt sich aus der Zahl der beteiligten Hosts, der Softwarekomponenten und der Schnittstellen zur Umgebung etc. Mit steigender Komplexität erhöht sich der Aufwand. Durch Beschränkung auf einzelne Aspekte, Schnittstellen und

Funktionen lässt sich der Aufwand unter Umständen reduzieren, allerdings auf Kosten der Ergebnisqualität.

Spezifikation des Testziels

Je genauer das Ziel eingegrenzt werden kann, desto geringer ist der Testaufwand. Dabei besteht andererseits die Gefahr, wichtige Fragen bereits bei der Zieldefinition unbemerkt auszuschließen.

Dokumentation des Testgegenstands

Liegt den Testern geeignete, vollständige Dokumentation des Testgegenstands vor, so müssen sie weniger Informationen selbst erarbeiten. Andererseits kann dieses Erarbeiten aber wertvoll sein, wenn das Testziel unscharf definiert ist und gänzlich unbekannte Angriffsmöglichkeiten gefunden werden sollen.

Prüftiefe

Je gründlicher die angestrebte Untersuchung, desto höher ist der Aufwand. Zu unterscheiden ist insbesondere zwischen Tests, die lediglich Versäumnisse im Betrieb – schwache Passworte, vergessene Patches usw. – identifizieren sollen, und solchen, deren Ziel das Finden unbekannter Softwarefehler ist. Gründliche Softwaretests sind aufwändiger, während sich Tests auf typische Betriebsprobleme zum Teil automatisieren lassen. Vollständige Automatisierung ist unseriös.

Vorhandenes Sicherheitsniveau

Ist das Ausgangsniveau hoch, so können sich Tester lange mit einer Anwendung beschäftigen, ohne nennenswerte Probleme zu finden. Bei geringem Sicherheitsniveau hingegen liefert bereits ein flüchtiger Test beachtliche Ergebnisse.

Randbedingungen

Die Kosten erhöhen sich, wenn Tests etwa nur vor Ort in einem Rechenzentrum oder nur während bestimmter Zeiten – häufig nachts oder am Wochenende – ausgeführt werden können. Neben den direkten Kosten können auch indirekte entstehen, etwa für die Begleitung durch einen Systemadministrator oder zusätzliche Bereitschaftsdienste.

Abrechnungsmodelle

Für die Abrechnung mit dem Auftragnehmer sind zwei Modelle typisch: nach Hosts oder nach Arbeitsaufwand. Handelt es sich um gut spezifizierte, weitgehend standardisierte Tests in der Betriebsphase, die vielfach zu wiederholen sind, so bietet sich die Abrechnung nach Anzahl der Hosts an. Bei solchen Tests steigt der Aufwand im Wesentlichen linear mit der Anzahl der getesteten Systeme.

Für nicht standardisierbare explorative Tests, für komplexe Systeme, bei hohem Ausgangsniveau oder großer Prüftiefe eignen sich Festpreise oder auch die Abrechnung nach Aufwand mit vereinbarter Obergrenze. Gegebenenfalls sind dann anhand von Zwischenergebnissen Prioritäten festzulegen bzw. Auslassungen zu dokumentieren.

Alternativ kann man sich bei komplizierteren Tests auch an Preismodellen für die agile Softwareentwicklung orientieren, etwa am *agilen Festpreis* [9]. Solche Modelle eignen sich für Situationen, in denen Flexibilität nötig und keine vollständige Planung vor Beginn möglich ist. An die Stelle der Anforderungen in einem Entwicklungsprojekt können beim Penetrationstest die zu testenden Systemkomponenten, Funktionen oder Testziele treten.

2 Anbieterauswahl

2.1 Können wir das nicht selbst machen?

Testen sollten ein System nicht diejenigen, die es entworfen, implementiert oder konfiguriert haben. Dennoch stellt sich die Frage, ob eine Firma ihre Anwendungen und Systeme nicht selbst testen kann und soll.

Interne Tester

Einige große Organisationen oder Behörden besitzen eigenes Personal für die Durchführung von Penetrationstests. Sind viele Systeme häufig zu testen, so ist dies kostengünstiger als Aufträge an externe Anbieter. Allerdings ist der anfängliche Aufwand für den Aufbau einer solchen Abteilung hoch, und der Kostenvorteil schwindet, wenn die Mitarbeiter nicht ausgelastet sind.

Von Nachteil sind dabei die Gefahr der Betriebsblindheit sowie die Beschränkung auf die eigene Fachkompetenz. Zudem fehlt eigenen, weisungsgebundenen Mitarbeitern zumindest formell die Unabhängigkeit. Zur Überprüfung des Sicherheitsmanagements können sie daher nur eingeschränkt, zur Erfüllung formeller Prüfpflichten überhaupt nicht eingesetzt werden.

Externe Tester

Werden externe Tester beauftragt, so fallen Kosten nur für ausgeführte Arbeiten an und lassen sich über Projektbudgets gut steuern. Auswahlkriterien, Anforderungen und Einsatz der Dienstleister sollten explizit geregelt werden. Naheliegend ist, dies im Rahmen des ohnehin erforderlichen Sicherheitsmanagements zu tun und entsprechende Regeln in Handbücher und Verfahrensanweisungen aufzunehmen. Empfehlungen hierfür gibt dieser Leitfaden. Dazu gehören auch Maßnahmen zum Schutz des Auftraggebers, etwa vor Verletzungen der Vertraulichkeit.

Aus fachlicher Sicht bieten externe Tester die Möglichkeit, auf ein breiteres Spektrum an Erfahrungen und Kompetenzen zuzugreifen.

2.2 Fachliche Kriterien

Know-How der Prüfer

Die beteiligten Mitarbeiter, die den Penetrationstest durchführen werden, müssen nachweislich (z.B. tätigkeitsbezogener Lebenslauf, Zertifikate etc.) dafür qualifiziert sein. Neben der formellen Qualifikation müssen sie vor allem über nachgewiesene praktische Erfahrung verfügen.

Daneben gehört zum Know-How gute Kenntnis der im System verwendeten Standardkomponenten und Plattformen, z.B. Betriebssysteme, Netztechnologien und -protokolle etc.

Risikobewertung und Lösungsvorschläge

Werden Schwachstellen gefunden, müssen die Tester in der Lage sein, die daraus resultierenden Risiken zu bewerten und Lösungen vorzuschlagen. Der Anbieter sollte darlegen können, nach welchen Kriterien die Bewertung erfolgen wird. Unkommentierte Listen von Schwachstellen sind nicht hilfreich.

Testmethoden

Der Anbieter sollte darlegen können, welche Werkzeuge er wozu einzusetzen gedenkt. Für gut spezifizierte und standardisierte Tests in der Betriebsphase gehören dazu (teil)automatische Scanner etc. In anderen Situationen ist Vorsicht geboten, wenn Anbieter zu stark auf Automatisierung und überhaupt auf einzelne Werkzeuge setzen.

Bei Tests an Produktivsystemen ist die Risikominimierung ein weiterer Aspekt. Der Dienstleister sollte darlegen können, wie er das Risiko von Störungen und Schäden durch den Test begrenzt, und Informationen zur Risikobewertung selbständig vom Auftraggeber erfragen.

Musterberichte

Musterberichte können Aufschluss geben über die Qualität der gelieferten Dokumentation, die Testmethoden, die Art der Risikobewertung und andere Details. Zu beachten ist jedoch, dass Musterberichte aufgrund von Geheimhaltungspflichten kaum je ein reales Projektergebnis vollständig abbilden können.

Referenzen

Erklärt ein Anbieter, er könne aufgrund von Geheimhaltungspflichten keine konkreten Referenzen liefern, so kann man ihn bitten, Kontaktpersonen bei einzelnen Kunden zu nennen und sich dort erkundigen. Ist der Anbieter dazu nicht in der Lage, so verfügt er wahrscheinlich nicht über Referenzen.

Unabhängigkeit von Herstellern

Die Anbieter sollten nicht durch Provisionen oder Verträge an bestimmte Lieferanten gebunden sein. Dies verletzt die Neutralität bei den Lösungsvorschlägen. Dies lässt sich jedoch kaum direkt prüfen. Praktikabler ist die Maßgabe, in Projektberichten auf Produkt- und Serviceempfehlungen zu verzichten und lediglich konzeptionelle Möglichkeiten zur Beseitigung einer Schwachstelle zu diskutieren.

Schwer zu bewerten sind Verflechtungen mit den Herstellern der zu testenden Systeme oder ihrer Komponenten. Sie können einerseits zu Interessenkonflikten führen, andererseits jedoch tiefere Technologiekenntnisse mit sich bringen. Nicht akzeptabel sind in jedem Falle Abhängigkeiten, die die Offenlegung von Ergebnissen gegenüber dem Auftraggeber behindern.

Hackerqualitäten

Sollen komplexe Systeme auf Softwareschwachstellen getestet werden, so genügen Toolsammlungen und oberflächliches Wissen nicht. Für solche Tests empfiehlt es sich, Anbieter auszuwählen, die analytische Fähigkeiten nachweisen können, etwa durch entsprechende Veröffentlichungen.

2.3 Organisatorische Kriterien

Unternehmensgröße

Der Anbieter sollte den vorgesehenen Test mit eigenen Mitarbeitern, d.h. ohne Unterauftragnehmer, bewältigen und die vorgesehenen Mitarbeiter nennen können. Eine Ausnahme sind Vertriebspartnerschaften, wenn die Rollen klar zwischen Vertrieb und Ausführung getrennt sind.

Beratungsgebiete

Anbieter sollten neben Penetrationstests auch andere Aspekte der IT-Sicherheit bearbeiten, etwa Audits, die Erstellung von Sicherheitskonzepten oder Produkttests. Abgesehen von der erweiterten Kompetenz des Anbieters erleichtert dies gegebenenfalls die Weiterarbeit anhand der Testergebnisse, sofern daran Interesse besteht.

Haftpflichtversicherung

Da Penetrationstest das Risiko von Betriebsstörungen mit sich bringen, sollte die Haftung nicht nur formell vertraglich geregelt werden. Der Anbieter sollte über eine Haftpflichtversicherung mit ausreichender Deckungssumme verfügen und dies nachweisen können.

Flexibilität

Der Anbieter muss sich flexibel auf die Randbedingungen einstellen können. Das gilt besonders für Tests, die nur zu bestimmten Zeiten (Wartungsfenster) oder nur vor Ort ausgeführt werden können. Für Aufträge, die unverzüglich und vor Ort durchgeführt werden müssen, ist es aus logistischen Gründen hilfreich, dass der Dienstleister seine Niederlassung in der Region hat.

Vertraulichkeit

Der Dienstleister muss bereit und in der Lage sein, Testergebnisse und ihm zugängliche Informationen vertraulich zu behandeln. Neben der vertraglichen Verpflichtung erfordert das ein angemessenes Sicherheitsmanagement seitens des Anbieters.

Ein Penetrationstest kann Schwachstellen in verwendeten Produkten aufdecken. Die Meldung solcher Schwachstellen an den Hersteller und eventuell auch an die Öffentlichkeit im Rahmen der *Responsible Disclosure* ist üblich und sinnvoll. Sie sollte jedoch nur in Abstimmung zwischen Auftraggeber und Tester erfolgen.

2.4 Kompetenznachweise

Zertifikate und andere Kompetenznachweise des Anbieters können bei der Auswahl helfen.

Zertifikate für Penetrationstester

Für Penetrationstester gibt es ein breites Angebot an Schulungen, die zum Teil mit einem (kommerziellen) Zertifikat abgeschlossen werden. Beispiele sind:

- Certified Ethical Hacker
- Certified Penetration Testing Professional
- Certified Penetration Testing Specialist
- Certified Security Testing Associate
- Licensed Penetration Tester

Die Aussagekraft solcher Zertifikate ist beschränkt. Sie bestätigen in der Regel nur den erfolgreichen Abschluss einer Schulung.

Andere Personenzertifikate

Wertvoller sind Zertifikate, die umfassende Kenntnisse und Erfahrungen auf dem Gebiet der IT-Sicherheit bescheinigen und die von mehreren Anbietern unter dem Dach einer Trägerorganisation ausgestellt werden. Beispiele sind:

- TeleTrust Information Security Professional (TISP) des deutschen TeleTrust e.V.
- Certified Information Systems Security Professional (CISSP®) von (ISC)²

Qualitätsstandards

Standards zur Qualitätssicherung (z.B. ISO 9000) und darauf basierende Zertifikate sind zu unspezifisch und geben keine Auskunft über die Kompetenzen und Erfahrungen des Anbieters oder seiner Mitarbeiter. Etwas spezifischer ist der Standard ISO 17025 *General requirements for the competence of testing and calibration laboratories*. Diesen Standard müssen zum Beispiel die beim BSI akkreditierten Prüflabors für IT-Sicherheit umsetzen. Auch er konzentriert sich jedoch vor allem auf die begleitenden Vorkehrungen und Prozesse.

Sicherheitsmanagement

Aufgrund der erforderlichen Vertraulichkeit sind Nachweise des Anbieters über sein Sicherheitsmanagement sinnvoll. Die einschlägigen Standards sind BS 7799, ISO 17799 und ISO 27001.

Für den Umgang mit Projektinformationen können auch spezifische Maßnahmen vereinbart werden. Typisch sind:

- Personenbezogene Vertraulichkeitserklärungen
- Festlegung von Kommunikationswegen und -mitteln
- Verschlüsselung der E-Mail-Kommunikation
- Regelungen zur Aufbewahrung bzw. Vernichtung von Ergebnissen und anderen Informationen nach Projektabschluss

2.5 Rotation

Es empfiehlt sich Penetrationstest in einen kontinuierlichen Prozess der Qualitätssicherung einzugliedern. Deshalb genügt es nicht, sie für jede Anwendung nur einmalig durchzuführen.

Bei wiederholten Tests kann die Anbieterrotation sinnvoll sein: aus einer Menge vorher ausgewählter Anbieter wird in jedem Zyklus ein anderer beauftragt. Da Penetrationstests zwangsläufig unvollständig sind, lässt sich auf diese Weise die Testabdeckung erhöhen.

Gegen die Rotation spricht andererseits, dass gute Kenntnis der zu testenden Systeme die Suche nach Schwachstellen erleichtern kann. Wichtig ist dies vor allem bei komplexen Anwendungen und unspezifischem Testziel.

Für kleinere Unternehmen kann die Rotation schwer umzusetzen sein. Ist der Dienstleister groß genug, kann man jedoch in diesem Fall zumindest das Personal tauschen.

3 Vertrag und Informationsaustausch

Neben den üblichen Vereinbarungen bei der Projektvergabe sind für Penetrationstests einige spezifische Regelungen zu treffen und Informationen auszutauschen. Das betrifft sowohl die Vertragsgestaltung als auch die Technik und Projektmanagement.

3.1 Vertragliche Regelungen

Den Auftraggeber treffen vor allem Informationspflichten. Er muss seinem Dienstleister klar mitteilen,

- Was das Ziel des Penetrationstests ist und welche Ergebnisse erwartet werden. Exakte Abnahmekriterien werden sich allerdings kaum formulieren lassen, da das zukünftige Testergebnis naturgemäß unbestimmt ist.
- Welche Methoden zulässig sind und welche nicht. Häufig wird etwa Social Engineering ausgeschlossen, um den Test auf technische Aspekte zu beschränken.
- An welchen Systemen Tests vorgenommen werden dürfen. Der Klarheit halber empfiehlt sich eine Positiv-Liste der erlaubten Systeme oder Netze.
- Ob es sich um Produktiv- oder Testumgebungen handelt und welche Risiken mit Ausfällen oder Schäden verbunden sind. Dabei sind auch mögliche Wechselwirkungen und Abhängigkeiten zu berücksichtigen, wenn etwa zentrale Komponenten der Unternehmens-IT getestet werden sollen.
- Ob die getesteten Systeme oder die damit verarbeiteten Daten besonderen gesetzlichen Regelungen unterliegen. Dazu gehören zum Beispiel die Verarbeitung personenbezogener Daten sowie Telekommunikationssysteme. Verpflichtungen des Betreibers müssen explizit an den Auftragnehmer weitergegeben werden.
- Welche Betriebsvereinbarungen ggf. zu beachten sind, sofern die Rechte der Mitarbeiter vom Test berührt werden.

Detaillierte Vorgaben können auch nach Vertragsabschluss mitgeteilt werden. In diesem Fall sollte zumindest die Verantwortlichkeit sowie die Art und Weise der Übermittlung im Vertrag geregelt sein.

Der Dienstleister muss die Einhaltung solcher Vorgaben zusichern. Weitere wichtige Zusicherungen sind:

- Vertraulichkeit der Testergebnisse und aller im Verlauf des Tests bekanntgewordenen Informationen. Das gilt zunächst auch für Informationen über Schwachstellen in verwendeten IT-Produkten; die Meldung an den Hersteller sollte nur gemeinsam mit dem Auftraggeber erfolgen.
- Ausführung von Tests nur nach Absprache mit dem Auftraggeber. Dazu kann ein Testplan dienen, wie er im folgenden Abschnitt beschrieben ist.
- Vorhandensein einer geeigneten Haftpflichtversicherung.
- Sofortige Information des Auftraggebers, falls kritische Schwachstellen in Produktivsystemen gefunden werden.

3.2 Technische Informationen

Zieldefinition

Ein Penetrationstest sucht nach Möglichkeiten, Sicherheitsziele zu verletzen. Aus diesen Zielen leiten sich die einzelnen Tests ab, deshalb müssen die Tester sie kennen. Mitgeteilt werden können entweder die Sicherheitsziele selbst („die Firewall soll jeglichen Datenverkehr zwischen X und Y unterbinden“) oder zu versuchende Verletzungen („Zugriff auf Datei Z ohne vorherige Kenntnis eines berechtigten Benutzeraccounts“).

Ohne klare Zieldefinition erhält der Test einen stark explorativen Charakter. Zum Testergebnis gehört in diesem Fall eine Einschätzung, welche Schutzzielverletzungen aufgrund der Ergebnisse möglich sind.

Ausgangsbedingungen

Ebenfalls festzulegen sind die angenommenen Ausgangsbedingungen, zum Beispiel „Zugriff von außen über das Internet“ oder „physischer Zugriff auf einen Ethernet-Anschluss im Gebäude.“

Basisinformationen über Zielsysteme

Über die Zielsysteme sollten die Tester wenigstens erfahren:

- DNS-Namen und IP-Adressen der zu testenden Systeme
- Netztopologie
- Betriebssystem
- Anwendungen auf den Zielsystemen
- Einbettung in die Infrastruktur, z.B. Single Sign-on, Fileserver etc.

Weitere Informationen

Weitere verfügbare Informationen und Dokumentation über die Zielsysteme sollten den Testern ebenfalls zur Verfügung gestellt werden. Die zuweilen geäußerte Vorstellung, ein erzwungener Black-Box-Test sei realistischer und deshalb wertvoller, ist Unsinn. Tatsächlich liefert er lediglich schlechtere Ergebnisse bei gleichem Aufwand.

Nicht unbedingt erforderlich sind hingegen Systeminterna wie Konfigurationsdateien und Programmquellcode, sofern sie nicht ausdrücklich im Rahmen des Tests analysiert werden sollen.

Zugangsmöglichkeiten

Rechtzeitig zu klären ist auch, auf welchem Wege die Tester Zugang zu den Zielsystemen erhalten. Einige Varianten sind:

- Zugriff über das Internet ohne besondere Vorkehrungen. Das ist die Perspektive eines Angreifers von außen. Im Test gewonnene Informationen können bei der Übertragung ungeschützt bleiben.

- Zugriff über das Internet mit einem VPN-Tunnel. Übermittelte Daten sind dabei geschützt.
- Zugang zum Netz vor Ort, Tester bringen ihre eigene Hardware mit.
- Zugang vor Ort mit Hardware des Auftraggebers. Diese Variante empfiehlt sich nicht, da sie den Vorbereitungsaufwand erhöht, aber kaum zusätzliche Sicherheit gibt.
- Zugang über einen Stellvertreter, d.h. ein Systemadministrator führt Tests nach Vorgaben der Tester aus. Auch diese Variante ist nicht zu empfehlen, da sie umständlich und fehleranfällig ist.

Abhängig von Testziel und Testgegenstand kann es sinnvoll sein, den Testern zusätzliche Beobachtungsmöglichkeiten zu verschaffen. So lässt sich etwa eine Firewall am effektivsten testen, wenn der Netzverkehr in allen angeschlossenen Netzen beobachtet werden kann. Beim Test von Anwendungen können auch Beobachtungsmöglichkeiten auf Betriebssystemebene der Server sowie der Zugang zu Logfiles sinnvoll sein.

3.3 Projektmanagement

Zeitplanung

Stehen die Zielsysteme nur zeitweise für Tests zur Verfügung, so sind die Testzeiten rechtzeitig zu vereinbaren.

Ansprechpartner

Der Auftraggeber muss Ansprechpartner auf verschiedenen Ebenen benennen:

- Den Projektleiter oder Ansprechpartner im Management
- Einen technischen Ansprechpartner für Fragen rund um das zu testende System
- Einen Notfallkontakt und dessen Bereitschaftszeiten für den Fall, dass Tests zu Störungen führen.



Umgekehrt sollte auch der Auftragnehmer einen Ansprechpartner für Notfälle nennen, der zu den Testzeiten zur Verfügung steht.

4 Dokumentation

Der Dienstleister sollte mindestens zwei Dokumente liefern, einen Testplan zur Vorbereitung und einen Ergebnisbericht.

4.1 Testplan

Der Testplan dient der Vorbereitung des Tests, der Abstimmung mit dem Auftraggeber und der Information der einzelnen Tester. Er sollte mindestens enthalten:

- Die in Abschnitt 3 genannten Informationen, auch wenn sie bereits im Vertrag vereinbart sind
- Die vorgesehenen Tests und sonstige Eingriffe (z.B. Beobachtung des Netzverkehrs). Bei Tests ohne klar definiertes Ziel oder in komplexen Systemen wird sich jedoch kein vollständiger Plan aufstellen lassen, da Beobachtungen und Zwischenergebnisse neue Tests motivieren können.
- Mögliche Störeinflüsse auf den Testablauf, z.B. durch Intrusion-Prevention-Systeme
- Absehbare Risiken und Nebenwirkungen sowie Gegenmaßnahmen

Anhang A zeigt ein Beispiel für einen solchen Testplan.

4.2 Ergebnisbericht

Die im Penetrationstest erarbeiteten Ergebnisse sollen vom Dienstleister im Abschlussbericht in ausführlicher und strukturierter Art beschrieben werden. Neben dem Testplan sollte die Erstellung eines Abschlussberichts vertraglich gefordert werden. Die Resultate sind von allen Beteiligten zu überprüfen.

Ein Abschlussbericht sollte in der Regel enthalten:

- Executive Summary
- Identifikation des getesteten Systems

- Testziele und zugrundeliegende Annahmen
- Testprotokoll:
 - Eine Aufstellung der ausgeführten Tests sowie ggf. nicht ausgeführter Tests (z.B. wegen Budgetbegrenzung oder aus technischen Gründen)
 - Detaillierte, nachvollziehbare Darstellung zumindest jener Tests, deren Ergebnisse auf Schwachstellen hindeuten. Dazu ist eine genaue Beschreibung der Testausführung und der dabei gemachten Beobachtungen nötig, etwa durch genaue Befehlsfolgen, Inhalte von Datenpaketen etc. Sensible Informationen wie z.B. Passworte wollten jedoch unkenntlich gemacht werden, soweit sie zum Verständnis nicht erforderlich sind.
 - Ebenso dokumentiert werden sollten auch Beobachtungen, die die Tester ohne spezifischen Test gemacht haben, sowie Zufallsfunde.
 - Informationen zur Umgebung und den Zielsystemen, soweit sie zum Verständnis erforderlich sind, etwa die Zuordnung von Namen und Adressen, die im Testprotokoll auftauchen.
- Interpretation der Testergebnisse. Dazu gehört zum einen die Bewertung der einzelnen Schwachstellen hinsichtlich ihrer Schwere, der Voraussetzungen für die Ausnutzung sowie des möglichen Gewinns eines Angreifers. Zum anderen ist ggf. zu zeigen, wie ein Angreifer einzelne Schwachstellen miteinander kombinieren kann, um ein Ziel zu erreichen. Weiterhin gehört zur Interpretation die Einschätzung, ob es sich bei den Schwachstellen um isolierte Einzelfehler oder um Anzeichen für systematische Probleme handelt.
- Handlungsempfehlungen

Anhang B skizziert ein Beispiel.

5 Ablauf und Checklisten

Dieser Abschnitt fasst die Empfehlungen noch einmal entlang eines Ablaufplans in Checklisten zusammen.

5.1 Vorbereitung

Die Vorbereitung obliegt dem Auftraggeber. Sie schafft die Grundlagen für die Auswahl und Beauftragung eines Dienstleisters.

Testziel festlegen

- Welche Systeme sollen getestet werden?
- Welche Sicherheitseigenschaften soll der Test prüfen oder ermitteln?
 - Einhaltung einer detaillierten Vorgabe
 - Qualitätsprüfung bei neuen Systemen
 - Wirksamkeit des Sicherheitsmanagements
 - Beseitigung früher gefundener Mängel
 - Andere

Randbedingungen festlegen

- Welches Budget steht zur Verfügung?
- Welche Einschränkungen sind zu beachten?
 - Zeitlich, z.B. Wartungsfenster
 - Örtlich, z.B. Zugang nur vor Ort möglich
 - Technisch, z.B. Abhängigkeiten zwischen Systemen
 - Organisatorisch, z.B. Betriebsvereinbarungen
- Welche Dokumentation liegt vor?

- zum System
- zum Sicherheitskonzept
- ggf. Ergebnisse früherer Tests

5.2 Anbieterauswahl und Vertrag

Vorbereitung

- Gibt es bereits Erfahrungen mit Anbietern?
- Von wem wurde dasselbe System früher bereits getestet?
- Gibt es interne Richtlinien zur Anbieterauswahl oder eine Liste bevorzugter Anbieter?
- Gibt es Tester innerhalb des Unternehmens? Sind sie geeignet?

Anbietercheck

- Verfügt der Anbieter über geeignetes Know-How?
 - Relevante Systeme, Plattformen, Technologien
 - Penetrationstests
 - IT-Sicherheit insgesamt
- Kann der Anbieter seine Arbeitsweise erläutern und demonstrieren?
 - Musterberichte
 - Skizzierung der Vorgehensweise und Testmethoden
- Hat der Anbieter aussagekräftige Referenzen? Ist er unabhängig von Herstellern?
- Kann der Anbieter seine Kompetenz nachweisen?
 - Qualifiziertes Personal
 - Projekterfahrung

- Ist der Anbieter bereit und in der Lage, die Vertraulichkeit zu gewährleisten?
 - vertragliche Zusicherung
 - Sicherheitsmanagement
 - projektspezifische Vereinbarungen

Grobplanung

Die Grobplanung erfolgt bereits in Zusammenarbeit mit dem zuvor ausgewählten Anbieter. Im Wesentlichen sind hier die projektüblichen Details zu klären.

Vertrag

- Ziel des Tests
- Umgebung: Produktiv- oder Testsysteme?
- ggf. Einschränkungen
 - unzulässige Methoden
 - zu beachtende Regelungen (betrieblich, gesetzlich)
- Zielsysteme (Positivliste)
- Bekannte Risiken und Regelungen zur Vermeidung
- Vertraulichkeitsvereinbarung
- Haftung und Versicherung
- Regelungen zu:
 - Testplanung und Freigabe
 - Gegenseitigen Informationspflichten

5.3 Detailplanung und Organisation

Die Detailplanung erfolgt zu Beginn des Projekts unter Federführung des Dienstleisters. Der Auftraggeber überwacht die Planung, liefert Informationen zu und erteilt die Freigabe für geplante Tests.

Informationsbedarf

- Detaillierte Zieldefinition
- Angenommene Ausgangsbedingungen
- Basisinformationen über Zielsysteme
 - Adressen
 - Netztopologie
 - Betriebssysteme
 - Anwendungen
 - Infrastrukturumgebung
- Verfügbare Dokumentation
- Zugangsmöglichkeiten

Testplan

- Zielsysteme
- Vereinbarte Grenzen
- Geplante Tests, zumindest als Skizze
 - Methode
 - Ziel
 - Risiken
- Sonstige Eingriffe, z.B. zur Beobachtung
- Risikoabschätzung und Gegenmaßnahmen
 - Störung des Tests
 - Störungen an Systemen
- Genaue Zeitplanung, falls hier Einschränkungen bestehen

Organisation

- Notfallplanung
- Ansprechpartner und deren Verfügbarkeit
- Zugänge für Tester
 - zu IT-Systemen
 - ggf. zu Räumlichkeiten
- Dokumentation aller Vorkehrungen, die später rückgängig gemacht werden müssen, insbesondere
 - Zugangsberechtigungen
 - Änderungen an der IT-Infrastruktur

5.4 Test

Den Test führt der Auftragnehmer in eigener Verantwortung aus. Der Auftraggeber muss lediglich sicherstellen, dass die benannten Ansprechpartner verfügbar sind und die vereinbarten Zugangsmöglichkeiten bestehen. Soweit die Einbindung der Administratoren nicht dem Testziel widerspricht, sollten sie zur Beobachtung der betroffenen Systeme auf ungewöhnliche Vorgänge angehalten werden.

5.5 Ergebnisse und Projektabschluss

Testbericht

Der Testbericht enthält:

- Die technischen Details aus dem Testplan
- Eine Aufstellung ausgeführter bzw. nicht ausgeführter Tests
- Für gefundene Schwachstellen:
 - Eine nachvollziehbare Beschreibung des Tests
 - die gemachten Beobachtungen

- die Kombinierbarkeit mit anderen Schwachstellen
- Eine Liste der Testergebnisse und Beobachtungen mit Einschätzung
 - des möglichen Gewinns bei Ausnutzung
 - der Voraussetzungen für die Ausnutzung
 - der Schwere insgesamt
 - Einzelfehler oder systematisches Problem?
- Gesamteinschätzung und Handlungsempfehlungen

Projektabschluss: Clean-up

- Zugangsberechtigungen entziehen
- Für den Test gemachte Änderungen rückgängig machen
- ggf. Nebenwirkungen der Tests beseitigen, z.B. erzeugte Dateien

Anhang A Beispiel: Testplan

Szenario: Am Applikationsserver *ServerX* soll ein Portscan durchgeführt werden.

Zielsystem

Applikationsserver *ServerX* mit folgenden Daten:

DNS-Name	ServerX.beispiel.test
IP-Adresse	192.168.1.10
Subnetmaske	255.255.255.0

Vereinbarte Grenzen

Keine Denial-of-Service-Versuche, kein Social Engineering

Art des Tests

Portscan auf System X. Alle TCP- und UDP-Ports von 1 bis 65535 werden angesprochen und die Reaktionen des Systems erfasst.

Methode

Für den Test werden folgende Methoden verwendet:

- TCP SYN (Half Open)
- TCP FIN
- UDP Scan

Werkzeuge

Nmap und / oder Netcat werden eingesetzt.

Erwartete Ergebnisse

- Aufdeckung aller offenen, geschlossenen und gefilterten Ports
- Identifizierung der aktiven Dienste
- Feststellung, ob die Firewalls oder IDS Systeme auf solche Tests reagieren.

Absehbare Risiken

Der Test kann:

- das Zielsystem so stören, dass Anwendungen oder das Gesamtsystem neu gestartet werden müssen
- IDS-Alerts auslösen

Testzeit

2. April 2007 zwischen 16 und 24 Uhr

Notfallplanung

Systemadministratoren überwachen während des Testzeitraums den Betrieb. Bei Störungen wird der Test abgebrochen und die Ursache untersucht.

Kontakt

Systemadministrator: Herr Müller, mueller@beispiel.test, Tel.: 555-12345

Testleiterin: Frau Meier, meier@penetrations.test, Tel.: 555-54321

Anhang B Beispiel: Ergebnisbericht

Ein Portscan wurde auf System ServerX durchgeführt, dazu liefert der Dienstleister die Informationen wie in folgendem Beispiel beschrieben:

Zusammenfassung

Auf dem Zielsystem ServerX (192.168.1.10) wurden drei unnötige Dienste gefunden, die deaktiviert oder durch die Softwarefirewall des Hosts blockiert werden sollten. Diese Dienste sind in der nachstehenden Tabelle aufgelistet:

Port Nr.	Dienst	Gewichtung
1234	abc	Bedingt kritisch
3008	HTTP	Kritisch
5678	xyz	Bedingt kritisch

Ziel und Umfang

Siehe Anhang A (Testplan)

Testprotokoll

Der Test wurde am 02.04.07 durchgeführt. Ein detailliertes Protokoll des Tests befindet sich im Anhang „DEF“.

TCP-SYN-Scan mit Nmap

TCP-SYN-Scan von einem Host im lokalen Netz (192.168.1.23). Ergebnis:

```
# nmap -sS -O -p 1-65535 192.168.1.10  
  
Interesting ports on ServerX.muster.url.com (192.168.1.10):
```

```
(The 1659 ports scanned but not shown below are in state: closed)

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
1234/tcp  open  xyz
3008/tcp  open  http        Microsoft IIS 5.0
5678/tcp  open  abc

Device type: general purpose server

Running: Microsoft Windows NT/2K/XP

OS details: Microsoft Windows 2000 Server RC1+ through final release

Service Info: OSs: Windows, Windows 2000 Server
```

Tabelle XXX

Die fett markierte Zeilen in der Tabelle XXX zeigen, dass auf dem ServerX drei Dienste („xyz“ auf Port 1234, „http“ auf Port 3008 und „abc“ auf Port 5678). Keiner dieser Dienste ist zur Nutzung der Anwendung *Foo* erforderlich. Der Webserver auf Port 3008 dient der Systemadministration. Die Dienste „abc“, und „xyz“ sind interne Schnittstellen zu Komponenten der Anwendung, die ausschließlich von localhost (127.0.0.1) aus genutzt werden. Schwachstellen sind nicht öffentlich bekannt; die unnötige Zugriffsmöglichkeit stellt jedoch ein Risiko dar.

Weitere Untersuchung mit Nessus

(...)

Auswertung

Der Webserver (IIS 5.0) auf Port 3008 ist eine kritische Schwachstelle. Die eingesetzte Version hat bekannte Fehler, die zum Eindringen in den Host ausgenutzt werden können. Zudem unterliegt der Server als Hilfskomponente der Anwendung *Foo* nicht der Pflege durch die Systemadministratoren. Nur diese Version des Webserver wird nach Aussage des Herstellers unterstützt.

Für die Dienste abc und xyz sind keine unmittelbaren Schwachstellen bekannt. Jedoch besteht das Risiko, dass solche Schwachstellen in Zukunft gemeldet und ausgenutzt werden.

Empfehlungen

Soweit eine Deaktivierung nicht möglich ist, sollte der Zugriff auf die genannten Ports mittels der Softwarefirewall auf dem Host verhindert werden. Alternativ können die Dienste so konfiguriert werden, dass sie lediglich Verbindungen von 127.0.0.1 (abc und xyz) bzw. von ausgewählten Arbeitsplätzen (HTTP) entgegennehmen.

Anhang XYZ: Erklärung zur Gewichtung

Eine Erklärung zur Gefährdungsskala.

Literatur

- [1] *Leitfaden IT-Sicherheit*, Bundesamt für Sicherheit in der Informationstechnik (BSI) 2004, URL: <http://www.bsi-bund.de>
- [2] *Studie - Durchführungskonzept für Penetrationstests*, Bundesamt für Sicherheit in der Informationstechnik (BSI), URL: <http://www.bsi-bund.de>
- [3] *OSSTMM – Open Source Security Testing Methodology Manual*, Peter Herzog. URL: <http://www.isecom.org/osstmm>
- [4] *Akkreditierung von Prüfstellen beim BSI*, <http://www.bsi.bund.de/zertifiz/akkred/index.html>
- [5] *Auswahl externer IT-Sicherheitsberater*, Kes, 2004, <http://www.kes.info>
- [6] *Information Systems Security Assessment Framework (ISSAF)*, Penetration Testing Draft 0.2.1.B, Open Information Security Group (OISSG), URL: <http://www.oissg.org/>
- [7] *NIST SP 800-42: Guideline on Network Security Testing*, URL: <http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf>
- [8] Heise.de: *Nach Datenschutzpanne: Hersteller zehn Jahre im Visier der FTC*, URL: <http://www.heise.de/newsticker/meldung/81196>
- [9] Bernd Oestereich: *Der agile Festpreis und andere Preis- und Vertragsmodelle*, Objekt-Spektrum, 01/2006, Seite 30, URL: http://www.oose.de/Der_agile_Festpreis_Objekt_Spektrum_01_2006_4_Seite_Seite_30.htm