Universität Ulm

Internet-Dienste

Thema 5: Penetrationstests

Seminararbeit

an der
Fakultät für Mathematik und Wirtschaftswissenschaften
Abteilung Angewandte Informationsverarbeitung

Seminarleiter:	Prof. Dr. Franz Schweiggert
Eingereicht von:	Siegfried Schleker
	Bahnstraße 21
	89278 Nersingen
	Matr.-Nr. 429670
Datum:	02. Juli 2004

Inhaltsverzeichnis

1. IT-Sicherheit und Penetrationstest

Unternehmen, die an öffentliche Netze angeschlossen sind, setzen sich der Gefahr aus, dass fremde Personen über das Internet Zugriff auf unternehmensinterne Daten erhalten. Um diese Gefahr zu minimieren, wurden Penetrationstests entwickelt. Dies ist der „kontrollierte Versuch, von außen in ein bestimmtes Computersystem bzw. Computernetzwerk einzudringen, um Schwachstellen zu identifizieren.“[1] Dabei werden dieselben Techniken verwendet wie bei einem realen Angriff, um einen solchen so gut wie möglich immitieren zu können. Ziel eines Penetrationstests ist die Überprüfung, ob in einem Unternehmen oder einer öffentlichen Einrichtung die IT-Sicherheit gewährleistet ist bzw. ob die eingesetzten Sicherheitssysteme in genügendem Maße vor Angriffen schützen. Falls Schwachstellen gefunden werden, können diese somit behoben und durch einen realen Angriff nicht mehr ausgenutzt werden.
Potentielle Bedrohungen der IT-Sicherheit können in drei Kategorien gegliedert werden:
Zum einen sind dies Angriffe über das Netzwerk mittels Portscanning. Jeder netzwerkfähige Computer besitzt über 65.000 logische Anschlüsse (Ports) über die andere Rechner mit ihm Kontakt aufnehmen können. Ein Abtasten des Rechners, welche und wieviele dieser Ports für Verbindungsaufnahmen geöffnet sind, wird als Portscanning bezeichnet. Falls ein offener Anschluß gefunden wird, kann dies dazu genutzt werden, illegal Zugriff auf diesen Rechner zu nehmen[2].
Eine weitere Gefahrenkategorie wird als Social Engineering bezeichnet. Darunter versteht man die Manipulation von Mitarbeitern, die über spezielle Kenntnisse bzgl. der IT-Sicherheit im Unternehmen verfügen. Dabei wird versucht, diese Leute psychisch unter Druck zu setzen, um an sicherheitsspezifische Daten wie z.B. Passwörter zu gelangen.
Eine dritte Gefahrenquelle ist die Umgehung physischer Sicherheitsmaßnahmen wie z.B. Einbruch oder Diebstahl.

1 BSI (2003), Internetpublikation, S. 4
2 Vgl. Fritsch (2002), Internetpublikation

2. Klassifikation von Penetrationstests

Penetrationstests können nach folgenden Kriterien unterteilt werden:

- Informationsbasis
  Die Informationsbasis beschreibt den Wissensstand zu Beginn des Tests. Hier wird unterschieden in Black-Box-Test und White-Box-Test. Beim Black-Box-Test stehen nur wenig Informationen über das Zielsystem zur Verfügung, d.h. es wird ein Angriff einer außenstehenden Person, die über kein firmeninternes Wissen verfügt, simuliert. Dagegen wird durch einen White-Box-Test der Angriff eines Insiders simuliert, dem die Ziele genau bekannt sind.
- Aggressivität
  Hier wird festgelegt, wie konsequent gefundene Schwachstellen ausgenutzt werden
- Umfang
  Auswahl der Systeme, die getestet werden sollen. Dies hat direkten Einfluß auf den mit dem Test verbundenen Aufwand.
- Vorgehensweise
  In dieser Kategorie wird definiert, wie „sichtbar“ ein Penetrationstest durchgeführt wird.
- Technik
  Bestimmung der Techniken, die beim Testen eingesetzt werden
- Ausgangspunkt
  Festlegung des Angriffspunktes. Dieser kann sich innerhalb oder außerhalb des Netzwerkes bzw. des Gebäudes befinden.

Im Allgemeinen setzt sich ein Penetrationstest aus einer Kombination dieser Kriterien zusammen, wobei aber nicht alle Kombinationen sinnvoll sind.

3. Durchführung von Penetrationstests

Unter der Berücksichtigung der Ziele des Auftraggebers und des Aufwandes und unter der Beachtung der rechtlichen Bestimmungen kann ein Penetrationstest in 5 Phasen gegliedert werden. Dabei sollte während der gesammten Prüfung eine ausführliche Dokumentation erstellt werden, um die Nachvollziehbarkeit des Tests zu gewährleisten.

3.1 Vorbereitung

In dieser 1. Phase werden die Ziele des Penetrationstests von Auftragnehmer und Auftraggeber gemeinsam festgelegt. Dadurch ist gewährleistet, daß beide Seiten von denselben Voraussetzungen ausgehen. Ziele können u.a. die Erhöhung der Sicherheit der technischen Systeme sein, die Bestätigung der Sicherheit durch einen externen Dritten oder die Erhöhung der Sicherheit der technischen und organisatorischen Infrastruktur. Dabei sollten die gesetzlichen und vertraglichen Bestimmungen eingehalten werden, um später strafrechtliche und / oder zivilrechtliche Konsequenzen auszuschliessen. Desweiteren müssen die organisatorischen, technischen und personellen Voraussetzungen des Testunternehmens berücksichtigt werden (vgl. Gliederungspunkt 4, Rahmenbedingungen).
Nach der Abstimmung der Ziele erfolgt die Konkretisierung des gewünschten Tests mit Hilfe der unter Gliederungspunkt 3 beschriebenen Klassifikation. Außerdem sollten durch eine Diskussion der auftretenden Risiken nach deren Eintrittswahrscheinlichkeit und Wirkung geeignete Notfallmaßnahmen vorbereitet werden.

3.2 Informationsbeschaffung und -auswertung

Die 2. Phase beinhaltet die Informationsbeschaffung und Informationsauswertung. Sie wird deshalb auch als passiver Penetrationstest bezeichnet. Mit Hilfe von Search-Engines wie Google und durch den Web-Server des Unternehmens können Informationen über die Unternehmensstruktur erlangt werden. Mit weiteren Methoden könne Domain-Namen und IP-Adressbereiche bestimmt werden[3]. Danach erfolgt ein Scan der Zielsysteme auf angebotene Dienste (Portscan). Hierbei werden die zuvor ermittelten IP-Adressbereiche auf wirklich erreichbare Zielsysteme untersucht. Anschließend werden die Ergebnisse des Portscans verwendet, um gezielt nach Schwachstellen zu suchen. Dabei sammeln die Eindringlinge Informationen über die System- und Anwendungssoftware, die auf dem Zielsystem eingesetzt werden. Als Ergebnis erhält man eine detailierte Übersicht über installierte Systeme und potentielle Angriffspunkte.

3.3 Bewertung der Informationen / Risikoanalyse

In der 3. Phase erfolgt eine Bewertung der gewonnenen Informationen nach den Zielen des Test, nach Gefährdungspotential und Aufwand. Für jede Schwachstelle wird eine individuelle Abwägung des Aufwandes mit den Erfolgschancen durchgeführt, um auf diese Art beim

3 Vgl. Weidenhammer (2001), Internetpublikation, S. 4

späteren aktiven Eindringen Prioritäten setzen zu können, da dies mit sehr hohem Zeitaufwand verbunden ist. Die 3. Phase endet mit der Auswahl der Angriffsziele und der Prüfungsschritte.

3.4 Aktive Angriffsversuche

In der 4. Phase wird das Zielsystem anhand der zuvor bestimmten Prioritäten aktiv angegriffen. Diese Phase beinhaltet das größte Risiko des gesammten Tests und sollte daher äußerst sorgfältig durchgeführt werden. Hier sollten die in der 1. Phase getroffenen Notfallmaßnahmen besonders beachtet werden. Ziel des aktiven Angreifens ist es, festzustellen, ob die zuvor identifizierten Schwachstellen tatsächliche Risiken darstellen.

3.5 Abschlussanalyse

In der 5. und letzten Phase wird der Abschlussbericht fertiggestellt. Dieser dokumentiert neben dem Prüfungsauftrag und den Prüfungsergebnissen auch das weitere Vorgehen, wie die gefundenen Risiken behoben werden können und damit die IT-Sicherheit verbessert werden kann. Hierzu werden die Schwachstellen nach deren potentiellen Gefahren bewertet und Maßnahmen zu deren Kompensation eingeleitet. Besonders wichtig ist, wie oben bereits erwähnt, die Nachvollziehbarkeit des Test, um rechtliche Konsequenzen zu vermeiden.

4. Rahmenbedingungen

Zu Beginn des Penetrationstests sollten Überlegungen angestellt werden, inwiefern folgende Voraussetzungen erfüllt sind, um den Test durchführen zu können.

4.1 Organisatorische Voraussetzungen

Wer ist direkt oder indirekt vom Penetrationstest betroffen? Neben den Systemen des zu testenden Unternehmens sind oftmals auch die Systeme des Providers betroffen. Denial-of-Service-Tests (DoS-Tests) können durch Übermittlung überlanger Zeichenketten eine Unterbindung von Diensten verursachen (Buffer Overflow), weshalb der Provider auf jeden Fall über den Test in Kenntnis gesetzt werden sollte.
Sind die haftungsrechtlichen Risiken angemessen berücksichtigt? Der Auftragnehmer sollte eine Haftpflichtversicherung in ausreichender Höhe abschließen, um sich gegen

Schadensersatzforderungen Dritter abzusichern. Obwohl der Test sehr sorgfältig durchgeführt wird, können Schäden nicht gänzlich ausgeschlossen werden.
Auch der Durchführungszeitpunkt bzw. -zeitraum sollte überlegt gewählt werden, da der Penetrationstest zu einer Beeinträchtigung wichtiger Systeme führen und den Geschäftsbetrieb stören kann. Dies kann jedoch nur innerhalb eines White-Box-Tests berücksichtigt werden. Bei einem Black-Box-Test stehen diese Informationen nicht zur Verfügung.
Außerdem sollten Überlegungen bezüglich Notfallmaßnahmen bei einem Systemausfall oder bei einem sonstigen Notfall getroffen werden. Diesbezüglich sollte zumindest festgelegt werden, welche Personen wann zu benachrichtigen sind.
Desweiteren sollte überdacht werden, welche Mitarbeiter des Auftraggebers vom Test betroffen sind. Je größer der Umfang des Penetrationstests, desto mehr Mitarbeiter müssen miteinbezogen werden. Überlegungen dieser Art sind v.a. bei Tests mit Social-Engineering-Techniken wichtig. Hier ist zu klären, welche Mitarbeiter in welchem Maß „getestet“ werden dürfen.
Ein weiterer wichtiger Punkt ist der Aufwand sowohl für den Auftraggeber als auch für das Testunternehmen. Ersterer muß mit Unregelmäßigkeiten im Geschäftsbetrieb und einer Beeinträchtigung der IT-Systeme rechnen. Deshalb sollte vor dem Test eine Datensicherung vorgenommen werden und der Test durch einen eigenen Mitarbeiter überwacht werden. Letzterer sollte die Zielsetzung und den Umfang des Test berücksichtigen, um entscheiden zu können, welche Ressourcen zur Verfügung stehen müssen.

4.2 Personelle Voraussetzungen

Da ein Penetrationstest schlecht standardisierbar ist, sollte er nur von Mitarbeitern durchgeführt werden, die über eine langjährige Erfahrung auf diesem Gebiet verfügen. In diesem Zusammenhang werden Kenntnisse über das auf dem Zielsystem installierte Betriebssystem benötigt, um den Test möglichst schnell durchführen zu können. Desweiteren sind Kenntnisse über TCP/IP von Bedeutung, da sich für die Abwicklung des Datenverkehrs im Internet dieses Protokoll durchgesetzt hat. Außerdem sollten die Tester über Programmierkenntnisse verfügen, um Schwachstellen ausnutzen zu können, und sich mit Firewalls auskennen, da in vielen Systemen solche Schutzmechanismen eingesetzt werden. Ein wichtiger Punkt ist auch oder v.a. die Kreativität der einzelnen Mitarbeiter, da der Verlauf eines Penetrationstests nicht nach einem vorgefertigten Muster geschieht.

4.3 Technische Voraussetzungen

Ein Zugang zu öffentlichen Netzen ist unabdingbar, da die meisten Angriffe über das Internet durchgeführt werden. Außerdem sollte das Testunternehmen über die geeigneten Tools verfügen, die für den Testvorgang notwendig sind (z.B. Schwachstellenscanner) und über ein lokales Netzwerk, auf dem diese Tools vor dem realen Einsatz getestet werden können

5. Rechtliche Überlegungen

Bezüglich der rechtlichen Überlegungen kann man folgende drei Fälle unterscheiden:

- rechtliche Überlegungen, die ein Unternehmen oder eine Behörde veranlassen können, einen Penetrationstest durchzuführen
- rechtliche Vorschriften, die der Auftragnehmer während der Testphase beachten sollte
- rechtliche Gesichtspunkte, die der Vertragsgestaltung zugrunde liegen

Es existiert keine Verpflichtung, einen Penetrationstest durchzuführen, jedoch gibt es verbindliche Vorschriften, die indirekt eine Prüfung der IT-Sicherheit erforderlich machen. Diese Vorschriften betreffen die Verfügbarkeit steuerrechtlich und handelsrechtlich relevanter Daten, den Umgang mit personenbezogenen Daten und die Einrichtung und Ausgestaltung eines internen Kontrollsystems.

5.1 Rechtliche Vorschriften als Motivation für einen Penetrationstest

Hier sind Gesetze zu beachten, die alle Unternehmen und öffentliche Einrichtungen betreffen. Dazu gehört das Bundesdatenschutzgesetz (BDSG), das den Umgang mit personenbezogenen Daten regelt. Außerdem schreibt das Handelsgesetzbuch (HGB) vor, Bücher nach den Grundsätzen ordnungsmässiger Buchführung (GoB) bzw. nach den Grundsätzen ordnungsmässiger DV-gestützter Buchführungssysteme (GoBS) zu führen. Desweiteren sind je nach Branchenzugehörigkeit noch spezielle Gesetzestexte zu beachten, wie z.B. das Kreditwesengesetz (KWG) und die Verordnungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin) für Finanzdienstleistungsunternehmen.

5.2 Rechtliche Vorschriften für den Auftragnehmer während der Prüfungsphase

Im Strafgesetzbuch (StGB) sind Tatbestände, die in diesem Fall von Belang sind, nur lückenhaft geregelt, und oftmals ergeben sich zusätzlich Beweisschwierigkeiten. Die Tatbestände beziehen sich v.a. auf die Verletzung des persönlichen Lebens- und Geheimbereichs, Betrug und Untreue, Urkundenfälschung und Sachbeschädigung. Die wichtigsten Straftatbestände sind die folgenden:

§ 202a Abs. 1 (1) StGB [Ausspähen von Daten]: „Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."
Dieser Paragraph regelt den Schutz aller gespeicherten und im Übermittlungsstadium befindlichen Daten. Die Tathandlung ist das Verschaffen der Daten.

§ 263a StGB [Computerbetrug]: „Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft."
Dieser Paragraph bezieht sich auf die Manipulation eines Datenverarbeitungsvorgangs mit der Absicht einer rechtswidrigen Vermögensbeschaffung. Voraussetzung ist allerdings eine vorätzliche Handlung.

§ 268 Abs. 1 StGB [Fälschung technischer Aufzeichnungen]: „Wer zur Täuschung im Rechtsverkehr 1.) eine unechte technische Aufzeichnung herstellt oder eine technische Aufzeichnung verfälscht oder 2.) eine unechte oder verfälschte technische Aufzeichnung gebraucht wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft."
In diesem Fall ist die Tathandlung die Herstellung einer unechten technischen Aufzeichnung, die Verfälschung einer technischen Aufzeichnung und jewils deren Gebrauch.

§ 303a Abs. 1 StGB [Datenveränderung]: „Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit

Geldstrafe bestraft.“

§ 303b StGB [Computersabotage]: „Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch dass er 1.) eine Tat nach § 303a begeht oder 2.) eine Datenverarbeitungsanlage oder einen Datenträger zerstört, unbrauchbar macht beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.“

Weitere Vorschriften macht das Zugangskontrolldiensteschutzgesetz (ZKDSG). Hierzu gehört z.B. der Angriff auf einen passwortgeschützten WWW- oder FTP-Server. Außerdem ist das Telekommunikationsgesetz (TKG) zu beachten, das das Abhören des Netzwerkverkehrs untersagt, falls dies nicht explizit erlaubt wurde. Desweiteren gesteht das Betriebsverfassungsgesetz (BetrVG) dem Betriebsrat, ein Informationsrecht zu, jedoch keine Entscheidungsbefugnis.

5.3 Rechtliche Gesichtspunkte bei der Vertragsgestaltung

Bei einem Penetrationstest handelt es sich i.A. Um einen Dienstleistungsvertrag, nicht um einen Werkvertrag, d.h. es wird eine Leistung vereinbart, aber kein bestimmter wirtschaftlicher Erfolg. Der Vertrag sollte v.a. die folgenden Punkte beinhalten:

- Zielsetzung des Penetrationstests (Erhöhung der IT-Sicherheits, Bestätigung der Sicherheit durch einen externen Dritten, ...)
- Art des Penetrationstest (Klassifikation nach Aggressivität, Umfang, Vorgehensweise, Technik, Ausgangspunkt)
- eingesetzte und ausgeschlossene Techniken

6. Zusammenfassung

Abschließend lässt sich sagen, dass ein Penetrationstest aufgrund der fortwährenden Entwicklung neuer Angriffstechniken zwar lediglich eine zeitlich begrenzte IT-Sicherheit gewährleistet, jedoch jedem Unternehmen zu empfehlen ist, da das Risiko eines unberechtigten Zugriffs auf interne Daten beträchtlich gesenkt wird. Je schützenswerter die Daten sind, über die das Unternehmen verfügt, desto öfter sollte ein Penetrationstest durchgeführt werden.

Außerdem kann ein Penetrationstest nicht die üblichen Sicherheitsvorkehrungen wie z.B. Datensicherung ersetzen. Er ist vielmehr eine Erweiterung des im Unternehmen bereits bestehenden Sicherungskonzepts.

7. Literaturverzeichnis

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI): Durchführungskonzept für Penetrationstests (2003), Internetpublikation, http://www.bsi.de/literat/studien/pentest/penetrationstests.pdf

FRITSCH, JÖRG: Fangfragen (2002), Internetpublikation, http://www.heise.de/ix/artikel/2002/11/048

WEIDENHAMMER, DETLEF: Penetrationstests: Einbruch auf Bestellung, Internetpublikation, http://www.computerwoche.de/index.cfm?type=detail&artid=29387&category=158&Pageid=255