Sebastian Schreiber

Entwurf einer Berufsethik für Penetrationstester

Seit ungefähr 15 Jahren werden in Deutschland Penetrationstests durchgeführt. Etabliert hat sich die Prüfmethode allerdings erst in den letzten fünf Jahren. Die Prüfdisziplin ist jung, eine anerkannte Ausbildung zum Beruf des Penetrationstesters existiert nicht und die Berufsbezeichnung ist nicht geschützt. Zudem wird der Penetrationstest oft in die Nähe des illegalen Hackings gerückt. Im Vorgriff einer denkbaren Regulierung des Berufsstandes sollte eine Selbsterklärung in Gestalt einer Berufsethik treten.

1 Der Penetrationstest

Kein Tag vergeht, an dem wir nicht den Medien Informationen über Hackerangriffe entnehmen und von Veröffentlichungen personenbezogener Daten oder von neuen Sicherheitslücken hören. Die Gefährdungssituation nimmt mit der Bedeutung des Internets und der Abhängigkeit von IT-Systemen weiter stetig zu.

Die Praxis zeigt, dass trotz großer Sorgfalt und bestem Qualitätsmanagement seitens der Unternehmen Systeme kompromittiert und Daten ausgespäht werden. Ursachen hierfür sind oft Fehler bei Administratoren oder Softwareentwicklern, die durch eine traditionelle Kontrolle sowie Qualitätssicherungsmaßnahmen nicht identifiziert werden können.

Der Penetrationstest nutzt einen Ansatz, der sich von denen des üblichen Qualitätsmanagements unterscheidet. Die Systeme des Kunden werden unter Anwendung von Spezialwerkzeugen und Spezialwissen aus der Perspektive eines Angreifers untersucht und angegriffen. Hierbei werden exakt die Probleme aufgedeckt, die ein realer Angreifer ebenfalls entdecken und ausnutzen würde. So wird der Kunde in die Lage versetzt, das Sicherheitsniveau seiner Systeme aus einer potentiellen Bedrohungsperspektive heraus einzuschätzen und die detektierten Schwächen zu beheben, um somit eine sichere IT-Landschaft zu betreiben. Auch wenn sich Ansatz und Vorgehensweise bei Penetrationstests von traditionellen Maßnahmen des generellen Qualitätsmanagements unterscheiden, sollten sie dennoch als Teil dessen betrachtet und in Qualitätsmanagementprozesse mit eingebunden werden.

Im Gegensatz zu anderen Prüf- und Qualitätssicherungsmethoden ist der Penetrationstest schnell und preiswert durchführbar und schafft harte, zweifelsfreie Fakten. Die Tatsache, dass im Rahmen von Penetrationstests oft Systeme kompromittiert werden, beweist ihre Daseinsberechtigung.

Dipl.-Inform. Sebastian Schreiber

SySS GmbH, Tübingen, Gründer und Geschäftsführer der SySS GmbH. Expertise bei Penetrationstests, bekannt durch Vorträge und Live Hacking-Präsentationen im In- und Ausland und in den Medien.
E-Mail: sebastian.schreiber@syss.de

2 Besonderheit des Berufs ‚Penetrationstester'

Wenn sich der Beruf des Penetrationstesters ähnlich entwickelt wie der anderer Prüfberufe (z.B. dem des Prüfstatikers, Wirtschaftsprüfers, Lebensmittelkontrolleurs), so wird es in naher Zukunft eine Ausbildung als Voraussetzung zur Ausübung des Berufs sowie eine staatliche Prüfung geben.

Die Aufgabe der klassischen Prüfberufe besteht darin, Abweichungen zu Normen und Standards zu identifizieren. Die Prüfungen laufen daher nach einem speziellen Schema (Kalkulation, Checkliste, Stichprobe,...) ab. Auch ein Penetrationstester folgt gewissen Standards; zugleich umfasst seine Arbeit allerdings einen großen Anteil an Kreativität – er befindet sich also in einem Spannungsverhältnis zwischen Prüfer, Berater und Forscher.

3 Bedarf einer Berufsethik

Mit alteingesessenen Berufen wie beispielsweise Ärzten, Zimmermännern, Polizisten oder Notaren geht nicht nur eine definierte Ausbildung und ein klares Berufsbild einher, sondern auch ein ausgeprägtes ethisches Selbstverständnis. Während bei Handwerksberufen wie dem des Zimmermanns die Arbeitsethik vor allem grundlegende Werte wie Ehrlichkeit, eine saubere Arbeitsweise oder das Sich-Fernhalten von Betrug postuliert, sind Ärzte und Polizisten im Besonderen auf eine klare Berufsethik angewiesen, da sie bei der Ausübung ihres Berufes oftmals Gewalt (gegen Menschen) ausüben müssen. Auch wenn diese Gewalt aus der Situation bedingt und notwendig ist, so muss sie durch die zugrunde liegende Ethik in Grenzen gehalten und reguliert werden. Im Prinzip ist die Arbeit von Penetrationstestern der von Polizisten oder Ärzten nicht unähnlich, denn auch ein Penetrationstester wendet eine Art von Gewalt an, die es zu regulieren gilt. Sie richtet sich zwar nicht gegen den Menschen direkt, aber gegen Systeme, von denen der Mensch und menschliche Existenzen abhängig sind. Diese Systeme müssen in einem Penetrationstest gezielt angegriffen werden, um eine verlässliche Aussage über

den Sicherheitsstandard der getesteten Systeme treffen zu können. Dabei gibt es eine oftmals unscheinbare Grenze zwischen maximaler Testoptimierung und Schadensverursachung, welche nicht überschritten werden sollte. Eine klar formulierte Berufsethik hilft, diese Grenze zu definieren und zu finden.

Beim Penetrationstester fehlt jedoch ein ethisches Selbstverständnis. Dieses ist für Penetrationstests noch nicht explizit formuliert und branchenweit abgestimmt worden. Das wäre aber deshalb besonders erforderlich, weil unethisch ausgeführte Penetrationstests ein nicht unerhebliches Schadenspotential hervorrufen können.

Zudem existieren Vorbehalte gegen Penetrationstests und Penetrationstester, die immer wieder geäußert werden und sie in schlechtem Licht zeigen:

- Penetrationstests werden von Personen durchgeführt, die einer kriminellen Hacker-Szene nahe stehen.
- Penetrationstester agieren am Rande der Legalität. Sie kommen durch ihre Arbeit zwangsläufig in Konflikt mit dem Bundesdatenschutzgesetz und dem Paragraphen §202c StGB[1], der als sogenannter Hackerparagraph seit 2007 besteht.
- Penetrationstester arbeiten undiszipliniert und wenig professionell.

Um diesen Vorbehalten entgegenzuwirken und um ein Kalkül für Penetrationstester zu erstellen, anhand dessen schnell festgestellt werden kann, welche Handlungen ethisch gesehen vertretbar sind, wird versucht, eine Berufsethik zu skizzieren.

4 Blick auf andere Berufsethiken/Kodizes

Bevor ein eigener Vorschlag für eine Penetrationstest-Ethik vorgestellt wird, sollen drei bekannte Berufsethiken kurz aufgegriffen und betrachtet werden, da sie ein paar Merkmale enthalten, die bemerkenswert sind und für die Erstellung eines solchen Kodex als Vorbild dienen können. Da die Begründung von Kodizes schon im Vorfeld durch politische Diskussionen und Konsensbildung geschehen, sind die enthaltenen Punkte deren Ergebnisse.

Die vorgeschlagene Ethik soll Diskussionsgrundlage sein für eine für Penetrationstester gültige Berufsethik: Sie wird Kodizes anderer Berufssparten ähneln und auch Punkte umfassen, die in diesen zu finden sind.

4.1 Der Eid des Hippokrates

Der griechische Arzt Hippokrates (460 bis 370 v. Chr) definierte vor etwa 2400 Jahren die sowohl älteste als auch bekannteste Berufsethik, nämlich den nach ihm benannten Eid des Hippokrates. Obwohl dieser Eid nicht mehr zeitgemäß ist, bildet er dennoch die ethische Grundlage der Ärzte, die ihn – angepasst an die heutigen Gegebenheiten – immer noch befolgen. In gewisser Weise lässt sich die Situation der Ärzte damals mit der der Penetrationstester heute vergleichen. Damals gab es auch keinen Leitfaden für Ärzte, wie sie praktizieren und Patienten behandeln sollen und was sie dürfen und nicht dürfen.

Es gibt Punkte aus dem Schwur des Hippokrates, die sehr allgemein gelten, zum Beispiel, die Pflicht, sowohl auf sein eigenes Leben zu achten als auch sozial verträglich und menschenfreundlich zu agieren. Darüber hinaus umfasst der Eid ein paar Punkte, die sich problemlos auf die Arbeit von Penetrationstestern anwenden lassen. Punkt 3 beispielsweise macht folgende Aussage: „Die diätetischen Maßnahmen werde ich treffen zum Nutzen der Leidenden nach meinem Vermögen und Urteil, Schädigung und Unrecht aber von ihnen abwehren."[2] Und Punkt 8 befasst sich mit der ärztlichen Schweigepflicht: „Was immer ich bei der Behandlung (der Patienten) sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, soweit man es nicht ausschwatzen darf, werde ich darüber schweigen, solches als heiliges Geheimnis achtend."

Die Aussagen dieser beiden Punkte des Hippokratischen Eides sollten auch die ethische Basis der Arbeit von Penetrationstestern sein, denn jede Handlung, die vorgenommen wird, sollte dem „Leidenden", sprich dem untersuchten und eventuell mit Sicherheitsschwächen behafteten Computersystem nutzen und nach bestem Vermögen zu deren Behebung (vergleichbar mit der Heilung) dienen. Ferner müssen sie – ebenso wie ein Arzt – eine Schweigepflicht einhalten, also vertraulich mit ihnen anvertrauten Daten umgehen, und sollten die Sicherheitslücken in Unternehmen als sensibel und schützenswert betrachten, „als heiliges Geheimnis achtend", die nicht an die Öffentlichkeit zu tragen sind.

Penetrationstester befinden sich heute daher in einer ähnlichen Situation wie Hippokrates damals. Um ihrem Handeln und Agieren ethische Grenzen zu setzen, bedarf es einer Berufsethik, der die Grundlage ihrer Arbeit bildet

4.2 BdSI-Kodex

Der Kodex des BdSI (*Bundesverband unabhängiger deutscher Sicherheitsberater und -Ingenieure e.V.*) enthält neben der Versicherung, Fachkompetenz zu bieten, mit Kundendaten vertraulich umzugehen und anderen Punkten auch einige Absätze, die beachtenswert sind und ebenso Vorbildcharakter für die Erstellung eines Kodex für Penetrationstester haben.

Zum einen legt der BdSI-Kodex fest, dass Sicherheitsberater finanziell und ideologisch unabhängig arbeiten: „Die BdSI-Mitglieder sind rechtlich und finanziell unabhängig. Neben dem Kriterium der Unabhängigkeit von Herstellern werden zugleich jegliche Abhängigkeiten von Dritten ausgeschlossen, die Einfluss auf Beratungsinhalte des Mitglieds haben könnten. Die Mitgliedsunternehmen garantieren im Rahmen des BdSI-Unabhängigkeitskodex insbesondere auch, dass es keine Verbindungen zu Sekten oder Gruppierungen mit extremistischen Ausrichtungen gibt."[3]

Ferner beinhaltet die Ethik ein Provisionsverbot: „BdSI-Mitgliedern und ihren Mitarbeitern ist die Annahme von Provisionen oder vergleichbaren Vorteilen durch Satzung untersagt." Interessant ist, dass viele andere Ethiken diesen Punkt gar nicht oder nur indirekt abdecken. Leider sind in der Beraterbranche hohe, vor dem Endkunden verheimlichte Provisionen üblich. Dadurch wird die Unabhängigkeit der Berater zerstört und der Kunde getäuscht.

4.3 Berufsgrundsätze des BDU

Die Ethik des BDU (*Bundesverband Deutscher Unternehmensberater BDU e.V*) ist der des BdSI ähnlich und legt in gleichem

1 §202c StGB sagt aus, dass unter gewissen Umständen bereits der Besitz von Hackertools strafbar sei. Allerdings hat Justizministerin Brigitte Zypries in der Bundestags-Drucksache 16/5449 klargestellt, dass der gutwillige Umgang mit Hackertools durch IT-Sicherheitsexperten nicht von §202c, StGB erfasst werde.

2 Alle zitierten Punkte sind entnommen aus: Lichtenthaeler, 1984, S.19-21 [10],

3 sieheBdSI-Kodex [2]

Maße Wert auf fachliche Kompetenz, Seriosität, Unabhängigkeit und Vertraulichkeit. Bemerkenswert jedoch ist, dass die Berufsgrundsätze des BDU in Punkt 7 einen Passus enthalten, der sich nicht mit der dem Punkt zugeordneten Überschrift *Fairer Wettbewerb* in Einklang bringen lässt. So steht im mittleren Abschnitt des Grundsatzpunktes 7: „Unternehmensberater empfehlen bei sachlich-fachlicher Notwendigkeit nur solche Kollegen, deren Leistungsstand ihnen bekannt ist, dabei und bei Kooperationen bevorzugen sie BDU-Mitglieder."[4]

Dieser Passus verstößt gegen das Prinzip des freien Wettbewerbs und ist insofern bedenklich, da Verbandsmitglieder aufgrund ihrer Mitgliedschaft bevorzugt behandelt werden und Nichtverbandsmitgliedern implizit abgesprochen wird, auf demselben Niveau und mit vergleichbaren hohen ethischen Standards wie ihre Kollegen im BDU zu arbeiten.

5 Eigener Vorschlag

Um den – teilweise nicht unbegründeten – Vorurteilen in Kapitel 3 entgegenzutreten, wird der Versuch unternommen, eine Penetrationstest-Ethik zu formulieren. Diese soll eine Grundlage schaffen, um Penetrationstester von ihrer Position am Rande der Kriminalität in den Kreis sozial-verantwortlicher Berufe zu holen. So kann der Hippokratische Eid ein Beispiel sein für das eigene Verhalten in Bezug auf schwache Firmennetzwerke, wenn festgelegt wird, dass bei allen Arbeiten die Stärkung der Systemsicherheit im Vordergrund stehen soll, und der BdSI-Kodex bei der Frage der finanziellen Unabhängigkeit und der Unbestechlichkeit. Der kritische Passus in den Berufsgrundsätzen des BDU ist ein Negativ-Beispiel dafür, welche Inhalte in Berufsethiken vermieden werden sollten.

Dennoch dient jeder der drei Kodizes wiederum als Vorbild für korrektes Arbeiten, Professionalität und dem vertraulichen Umgang mit sensiblen Kundendaten.

Unter Bezugnahme auf die hervorgehobenen Punkte in den betrachteten Berufsethiken soll nun ein erster Entwurf einer möglichen Berufsethik für Penetrationstester dargelegt werden:

- **Unabhängigkeit**

Penetrationstests durchführende Firmen testen nur in solchen Unternehmen, in denen sie weder bei der Konzipierung der IT-Umgebung noch der Einrichtung von Sicherheitsmaßnahmen beteiligt gewesen sind und an die sie auch keine eigene Software verkauft haben oder verkaufen wollen. Nur so kann sichergestellt werden, dass die Ergebnisse des Tests objektiv sind.

- **Vertraulichkeit**

Sowohl die Identität der beauftragenden Firma als auch jegliche Einblicke in interne Netzwerke, Strukturen sowie in jegliche Daten, ebenso auch die, die dem Penetrationstester zur Verfügung gestellt werden, sind absolut vertraulich zu behandeln.

- **Provisionsverbot**

Die Annahme von Provisionen oder vergleichbaren Vorteilen ist untersagt.

- **Vorsicht**

Der Kunde ist über mögliche Risiken in Kenntnis zu setzen, die bei den Prüfungen erstehen können.

- **Professionalität und Qualitätsmanagement**

Die Arbeit hat professionell zu erfolgen und ist einem Qualitätsmanagement zu unterziehen. Dabei leistet der Penetrationstester seine Arbeit nach bestem handwerklichem Wissen und ethischem Gewissen.

- **Verbindlichkeit**

Vertraglich zugesicherte und in Beratungsgesprächen mündlich getroffene Zusagen sind von den Mitarbeitern der Penetrationstests durchführenden Firma verbindlich einzuhalten.

- **Objektivität, Neutralität und Transparenz**

Schlussfolgerungen müssen objektiv sein und sind nachvollziehbar darzustellen.

- **Interessenskonflikte**

Interessenskonflikte zwischen Penetrationstestern und Kunden sind zu vermeiden und gegebenenfalls anzuzeigen und auszuräumen.

- **Striktes Legalitätsprinzip**

Die Gesetze der von Penetrationstests betroffenen Länder sind strikt einzuhalten, auch wenn Teilergebnisse eines Penetrationstests selbst einen Interessenskonflikt mit der vorgefundenen Gesetzgebung darstellen könnten. So kann die Aufdeckung von Schwachstellen in bestimmten Fällen Verstöße gegen bestehendes Recht begünstigen. Penetrationstester sind daher verpflichtet, sich mit der jeweiligen Gesetzeslage vertraut zu machen und sorgfältig darauf zu achten, dass ihre Arbeit innerhalb der vorgegebenen Gesetzesgrenzen abläuft.

- **Respekt vor Menschen**

Social Engineering-Attacken sind Angriffe gegen das Verhalten von Menschen – diese werden, sofern sie überhaupt durchgeführt werden, ausschließlich angekündigt durchgeführt.

- **Korrektes Zitieren**

Wird fremdes Wissen bei der Arbeit herangezogen und verwertet, so sind die Quellen/ Urheber korrekt auszuweisen.

6 Fazit

Der hier vorgelegte Vorschlag für eine berufsbezogene Ethik von Penetrationstestern soll als Grundlage zur Diskussion dienen. Das Ziel ist es, ethische Richtlinien festzulegen, bekannt zu machen und zu einer allgemeinen, in der Gesellschaft verankerten Anerkennung zu verhelfen, sodass Penetrationstester auch wirklich ihre Arbeit darauf aufbauen und Kunden sich verlassen können, seriös behandelt zu werden. Als Vorbild dienen berufsethische Grundsätze anderer Branchen, unter denen der Hippokratische Eid wohl der bekannteste ist.

Literatur

[1] Hackerethik, http://de.wikipedia.org/wiki/Hackerethik

[2] BdSI Kodex, http://www.bdsi-ev.de/kodex.htm

[3] Studie der Schweizerischen Informatikgesellschaft Fachgruppe Security, http://www.isss.ch/events/ft1999.11.30/Tiger.pdf (S. 53f.)

[4] Gröndahl, Boris: *The Script Kiddies Are Not Alright*, http://www.heise.de/tp/r4/artikel/9/9266/1.html

[5] Der deutsche Pressekodex, http://www.presserat.info/pressekodex.html

[6] Verhaltenskodex gegen Korruption, http://www.stmi.bayern.de/imperia/md/content/stmi/service/gesetzeundvorschriften/korruptionsrili_verhaltenskodex.pdf

[7] Spitzelaffaire bei der Deutschen Telekom http://www.spiegel.de/wirtschaft/0,1518,k-7343,00.html

[8] Kodex der Association of Management Consulting Firms, http://www.amcf.org/memEthics.asp

[9] Berufsgrundsätze des Bundesverband Deutscher Unternehmensberater BDU e.V., http://www.bdu.de/docs/downloads/BDU_Online/Auswahl_von_UB/Berufsgrunds%C3%A4tze_UB_PB.pdf

[10] Lichtenthaeler, Charles: *Der Eid des Hippokrates*, Deutscher Ärzte-Verlag, Köln, 1984, http://de.wikipedia.org/wiki/Eid_des_Hippokrates

[11] Genfer Deklaration des Weltärztebunds („Genfer Gelöbnis"), http://www.bundesaerztekammer.de/downloads/Genf.pdf

4 Siehe Berufsgrundsätze des BDU [9]