

Concept of a Professional Code of Ethics for Penetration Testers

Penetration Tests have been performed in Germany for about 15 years. This test method in particular has only been established within the last five years. Therefore, this discipline is relatively young. There is no accredited schooling for the profession of a penetration tester and the occupational title is not protected. Furthermore, the penetration test is often seen as quite close to illegal hacking. In anticipation of an imaginable regulation of this profession, there should be a self-declaration in form of a professional code of ethics. This article was originally written in German (Entwurf einer Berufsethik für Penetrationstester) and published in the *Datenschutz und Datensicherheit* 4/2009.

1 The Penetration Test

There is hardly any day on which we do not hear from hacker attacks in our various media and learn about the publication of sensitive personal data or the existence of new security holes. The risk potential increases with the significance of the Internet and the dependence from IT systems grows consistently.

The practice shows that despite good care and even the best quality management from the company's point of view, systems are compromised and data monitored. Reasons for this are often mistakes of administrators or software developers, which cannot be identified by traditional controlling and quality assurance measures.

The penetration test uses an approach which differs from that of the common quality management. The systems of the customer are analyzed from the perspective of an attacker by using special tools and special know-how. Hereby, exactly those problems are uncovered which a real attacker would also detect and exploit. Thus, the customer is put into the position to evaluate the security level of his own systems from a potential threat's eye view and to remedy the detected vulnerabilities in order to operate a secure IT environment. Although approach and procedure of penetration tests differ from traditional measures of common quality management, they should still be considered as a vital part

of it and be integrated into quality management processes.

In contrast to other analyses and quality assurance methods, the penetration test is quick and good value for money and brings forth hard facts free of doubt. The fact that systems are often compromised within the coverage of the penetration test proves the test's right to exist.

2 Particularity of the Profession 'Penetration Tester'

If the profession of a penetration tester has a similar development to those of other testing professions (e.g. inspecting structural engineer, financial auditor, food inspector, etc.), there will be a specialised training in the near future as a precondition for practicing this profession as well as an official examination.

The task of conventional testing professions is to identify anomalies to norms and standards. The analyses therefore happen according to a special scheme (calculation, check list, random sample, etc.). A penetration tester, too, follows certain standards; his work also contains a high amount of creativity – he thus walks on a ground of tension between inspector, consultant and researcher.

3 The Need for a Professional Code of Ethics

Long-established professions like doc-

tors, carpenters, policemen or solicitors do not only have a clearly defined vocational training and a clear occupational image but also a distinct ethical self-conception. While the profession of craftsmen like carpenters have a code of ethics postulating basic values like honesty, a correct way to work or refraining from deceit, doctors and policemen in particular are dependent on a clear professional code of ethics as their professions often cause them to act in a violent way (towards men). Although their acts of violence are situational and necessary, they have to be regulated by a basic code of ethics and kept within a certain limit. In principle, the work of penetration testers is comparable to that of policemen or doctors. The penetration tester also executes a certain form of violence which must be regulated. The violence is not directed against human beings directly but against systems from which man and human living are dependent. These systems need to be attacked specifically in order to obtain reliable information about the security standard of the tested systems. There is often an inconspicuous border between the maximum test optimization and causing damage, which under no means should be crossed. A clearly worded professional codex helps to define and to eventually find this border.

The penetration tester, however, is lacking this ethical self-conception, which has neither been explicitly formulated yet nor agreed on by the industry sector. It is therefore especially essential

as unethically performed penetration tests may have a considerable damage potential.

Furthermore, there are reservations against penetration tests and testers which are uttered over and over again and thus appear in a bad light: .

- Penetration tests are performed by persons being close to a criminal hacker scene.
- Penetration testers act on the verge of legality. It is unavoidable that their work causes conflicts with the data protection law of the Federal Republic of Germany and paragraph §202c StGB¹, which has been existing since 2007 as the so-called ‘Hacking Paragraph’.
- Penetration testers work in an undisciplined way and are not very professional.

In order to countervail these reservations and to establish estimation for penetration testers, which helps to define which acts are justifiable from an ethical point of view, a professional code of ethics is now attempted to be drawn.

4 Viewing Other Professional Codes of Ethics/Codices

Before presenting our own suggestion for a code of ethics for penetration testers, three well-known professional codices should be taken up and considered².

They contain some characteristics which are remarkable and which may serve as good examples for such a codex. As the reasoning of codices already happens by political discussions and forming a consensus in the run-up, the points mentioned just cover their results.

The suggested code of ethics should be the basis for discussion for a valid professional codex for penetration testers which will be similar to codices of other professional guilds and also con-

tain the same points.

4.1 The Hippocratic Oath

Approximately 2400 years ago, the Greek doctor Hippocrates (460 to 370 B.C.) defined the both oldest and best known professional code of ethics, the Hippocratic Oath. Although this oath is not up-to-date anymore, it nevertheless forms the ethical ground for physicians who still obey it – although adapted to today’s conditions. To some degree the situation of doctors in Hippocrates’ time can be compared with the current situation of penetration testers. In the old times there was no guideline for physicians, how they were to practice and treat patients and what they were entitled to and not.

There are points within the Hippocratic Oath which apply in general, for instance, the duty to safeguard one’s own life, to act in a social way and to be philanthropic. Furthermore, the oath contains clauses which can easily be adopted by penetration testers. Clause 3, for instance, says the following: “I will use those dietary regimens which will benefit my patients according to my greatest ability and judgement, and I will do no harm or injustice to them.”³ And clause 8 deals with medical confidentiality: “Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.”

Both of these points of the Hippocratic Oath should also be the basis of the work of a penetration tester, for every act which is performed should be done in favour of the “patient”, i.e. in favour of the computer system to be tested which may be flawed with security weaknesses and in order to remedy them according to the best of abilities (comparable to healing). Moreover, they are bound to professional discretion – in the same way as a doctor – and have to treat confidential data as such. In the same way they also ought to regard security holes in companies as sensitive and worth to be protected keeping them as a secret “as considering all such things to be private” which should not be made known to the public.

Penetration testers often find themselves in a similar situation today as

Hippocrates in his own time. In order to build an ethical fence to their deeds and actions, a professional codex is essential forming the basis for their work.

4.2 BdSI Codex

Besides the assurance to offer expertise and to treat customer data confidential, the codex of the BdSI⁴ (*Federal Association of Independent German Security Consultants and Engineers*) contains some remarkable clauses serving as a role model for setting up a codex for penetration testers.

On the one hand, the BdSI codex determines that security advisors should work financially and ideologically independent: “The members of the BdSI are legally and financially independent. Besides the criterion to be independent from any producers, any kind of dependencies from third parties – which may have some influence on the content of the member’s advisory service – are ruled out. Member companies especially guarantee within the scope of the BdSI independence codex that there are no connections to sects or groups with extremist directions.

Furthermore, the code of ethics contains an interdiction to take any commission fees: “Members of the BdSI and their members of staff are strictly forbidden by the constitution to take commission fees or other comparable advantages.” It is interesting that a number of other codes of ethics do not cover this point at all or only indirectly. Unfortunately it is good practice in the consultants’ line of business to receive high commission fees which are often concealed from end customers. Thus, the independence of consultants is destructed and the customer conceived.

4.3 Professional Principles of the BDU

The code of ethics of the BDU⁵ (Federal Association of German Corporate Consultants) is similar to that of the BdSI and puts its emphasis on professional competence, reliability, independence and confidentiality. It is remarkable, however, that the Professional Principles of the BDU contain a passage in clause 7 which is not in accord with the head-

¹ §202c StGB says that under certain circumstances even the possession of hacker tools may be liable to prosecution. The former German Secretary of Justice, Brigitte Zypries, made clear in the Bundestag printed paper 16/5449 that a good-willed use of hacker tools by IT security experts is not captured by §202c, StGB.

² As this original article was written and published in German, the professional codices to be considered – apart from the Hippocratic Oath – are German codices and therefore refer to German work situations and standards. Nevertheless, the examples taken from these German codices also apply from an international point of view.

³ Wording of clauses taken from a translation of the Hippocratic Oath by Michael North, National Library of Medicine, 2002

⁴ The German name is: *Bundesverband unabhängiger deutscher Sicherheitsberater und – Ingenieure e.V.*

⁵ Abbreviation of: *Bundesverband Deutscher Unternehmensberater BDU e.V.*

ing of the clause, *Fair Competition*. The following wording can be found in the passage: "If professionally and topically necessary, corporate consultants only recommend colleagues whose proficiency level is known to them, therewith and when cooperating they will favour members of the BDU."

This clause therefore violates the principle of free competition and is critical inasmuch as members of the association are favoured just because of their membership and non-members of the association are implicitly denied to work on the same level and with comparable high ethical standards as their colleagues in the BDU.

5 Our Own Suggestion

In order to counter the prejudices in section 3 – of which some are not entirely ungrounded – the suggestion will be made to word a code of ethics for penetration testers. This code should lay the basis for testers to get out of their original position on the verge of crime and reach the circle of socially responsible professions. Thus, the Hippocratic Oath may be an example for one's own behaviour in relation to weak company networks when it is determined that when doing any work, the strengthening of the system security should be at the forefront. The BdSI codex may be an example when dealing with the question of financial independence and incorruptibility. The critical passage in the professional principles of the BDU is a negative example for contents which should be avoided in professional codes of ethics.

Nevertheless, each one of the three codices serve as a role model for correct working, professionalism and a confidential handling of sensitive customer data.

Relating to the highlighted points in the considered codes, a first concept of a possible professional code of ethics shall be presented:

1) Independence

Companies performing penetration tests only test in enterprises in which they have neither taken part in planning the IT environment nor in the implementation of any security measurements. Furthermore, they also abstain from testing companies they have sold their own software to or want to sell software to. This is the only way to safeguard that

test results are impartial.

2) Prohibition of Commission Fees

Accepting any kind of monetary commissions or other comparable advantages is interdicted.

3) Care

The customer is to be informed about any possible risks which can emanate from the tests.

4) Professionalism and Quality Assurance

All work has to be done in a professional way and to undergo a quality assurance. A penetration tester does his work to the best of his technical knowledge.

5) Liability

Any consents agreed both by contract and orally in counselling interviews are to be adhered to by the members of staff of the company performing penetration tests and are binding.

6) Impartiality, Neutrality and Transparency

Conclusions must be impartial and to be depicted in a comprehensible way.

7) Conflicts of Interests

Conflicts of interests between penetration testers and customers are to be avoided and if so reported and smoothed out.

8) Strict Obedience of Laws

The laws of the country where the penetration test is performed are to be kept strictly even if partial results of a penetration test could in itself be a conflict of interest with the existing legislation. Thus, the discovery of vulnerabilities in certain cases can promote breaches of law. Penetration testers therefore are bound to acquaint themselves with the respective legal situation and to carefully take heed to their work being done within the existing legal boundaries.

9) Respect of Human Beings

Social Engineering attacks are directed at the behaviour of human beings. Therefore they will only – if they happen at all – be performed with prior notice.

10) Quoting Correctly

If knowledge from outside is considered and used during the course of work,

sources and authors have to be indicated to in a correct way.

6 Conclusions

This concept for a profession-related code of ethics for penetration testers presented in this article shall serve as a basis for discussion. The prime goal is to determine and to make known ethical guidelines and to help them find a deeply rooted acceptance within the society. Thus, penetration testers may truly ground their work on them and help customers to have confidence and to be treated in a professional way. Professional ethical guidelines therefore serve as patterns of which the Hippocratic Oath is presumably the best known.

Literature

- [1] Hacker Ethic: http://en.wikipedia.org/wiki/Hacker_ethic
- [2] BdSI codex: <http://www.bdsi-ev.de/kodex.htm>
- [3] Study by the Swiss Information Technology Society „Section Security“, <http://www.iss.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] The German Press Codex: <http://www.presserat.info/pressekodex.html>
- [6] Behavioural Codex Against Corruption: http://www.stmi.bayern.de/imperia/md/content/stmi/service/gesetzundvorschriften/korruptionsriili_verhaltenskodex.pdf
- [7] Snitcher Affair at the German Telecom: <http://www.spiegel.de/wirtschaft/0,1518,k-7343,00.html>
- [8] Codex of the Association of Management Consulting Firms: <http://www.amcf.org/memEthics.asp>
- [9] Professional Basic Principles of the Federal Association of German Corporate Consultants.: http://www.bdu.de/docs/downloads/BDU_Online/Auswahl_von_UB/Berufsgru nds%C3%A4tze_UB_PB.pdf
- [10] North, Michael: *Greek Medicine – the Hippocratic Oath*: http://www.nlm.nih.gov/hmd/greek/greek_oath.html
- [11] Declaration of Geneva by the World Medical Association: <http://www.cirp.org/library/ethics/gen eva/>