Service description penetration tests & phishing simulations

General principles and scope of application

1. All legal transactions in connection with penetration tests and phishing simulations between the Client and the Contractor (Management Consultant) - hereinafter referred to only as the Contractor - shall be governed exclusively by this Service Description. The version valid at the time the contract is concluded shall apply.

2. The Client may only be an entrepreneur within the meaning of § 1 of the Austrian Consumer Protection Act (KSchG).

3. This service description also applies to all future contractual relationships in connection with penetration tests and phishing simulations, even if no express reference is made to this in additional contracts.

4. Conflicting general terms and conditions of the Client are invalid unless they are expressly recognized by the Contractor in writing.

5. In the event that individual provisions of this service description are and/or become invalid, this shall not affect the validity of the remaining provisions and the contracts concluded on the basis thereof. The invalid provision shall be replaced by a valid provision that comes as close as possible to the meaning and economic purpose of the invalid provision.

Aim and scope of penetration tests

6. The aim of penetration tests is to identify technical risks and vulnerabilities in the target systems.

7. In the course of carrying out penetration tests, no measures are carried out with the aim of making the target systems unavailable (denial of service, distributed denial of service), unless such a service is explicitly offered in the offer.

8. The scope of the specific penetration test is contractually agreed on a case-by-case basis and is limited in time ("time box"). The Contractor does not guarantee that all existing security vulnerabilities will actually be uncovered. This is due to the limited time resources available and the penetration testers' limited knowledge of IT infrastructure, software,

source code, users, etc. The disclosure of system internals, the provision of test users and the comprehensive cooperation of the client with the contractor increase the efficiency of the penetration test.

9. The Client shall provide the Contractor with the list of target systems ("scope"; IP addresses, domains, subdomains, locations, e-mail addresses, etc.) in writing (e.g. by e-mail) no later than three working days before the start of the service. The transmission of the scope is accompanied by the client's implicit permission to carry out intrusive penetration tests ("Permission to Attack"). The client guarantees to have the authorization to have the named target systems intrusively attacked.

Aim and scope of phishing simulations

10. The aim of phishing simulations is to create and raise the security awareness of the target group defined by the client.

11. The scope and exact design of the phishing simulation shall be agreed between the client and the contractor.

12. The Client shall provide the Contractor with the list of e-mail addresses of the recipients ("scope") in writing (e.g. by e-mail) no later than three working days before the start of the service. The transmission of the scope is accompanied by the Client's implicit permission to carry out phishing simulations ("Permission to Attack"). The client guarantees to have the authorization to carry out phishing simulations with the transmitted scope.

13. The client shall ensure that all technical measures to block unwanted emails (SPAM protection, phishing prevention, anti-virus systems, mail security solutions, etc.) are deactivated for the sender addresses to be specified by the client during the execution period. Otherwise, the delivery of the phishing simulation to the recipients and thus the successful execution of the service cannot be guaranteed.

Duty of the client to provide information and cooperate

14. The performance period shall be agreed between the Contractor and the Client. The lead time between the conclusion of the contract and the start of the performance period may be up to twelve weeks.

15. The client shall ensure that all documents, accesses, user accounts, authorizations and operating resources necessary for the performance and execution of the service are submitted to the contractor at least three working days before the start of the service, even without a special request from the contractor.

16. The Client shall ensure that the organizational framework conditions allow for work that is as undisturbed as possible and conducive to the rapid progress of the service process

during the performance of the service.

17. The client shall ensure that all necessary bodies (if applicable, its employees, the established employee representative body (works council), etc.) are informed of the contractor's activities before they begin.

Confidentiality / data protection

18. The Contractor undertakes to maintain absolute confidentiality about all business matters of which it becomes aware, in particular business and trade secrets as well as any information it receives about the nature, scope of operations and practical activities of the Client.

19. Furthermore, the Contractor undertakes to maintain confidentiality vis-à-vis third parties regarding all information and circumstances that it has received in connection with the performance of the commissioned service.

20. The Contractor shall be released from the duty of confidentiality vis-à-vis any assistants and representatives it uses. However, he must impose the duty of confidentiality on them in full and shall be liable for their breach of the duty of confidentiality as for his own breach.

21. If security vulnerabilities are identified in third-party components (e.g. software or hardware) in the course of the service, the Contractor is entitled to inform the manufacturer, apply for CVE (Common Vulnerabilities and Exposures) numbers and publish them as part of a responsible disclosure process. Publication takes place taking into account the remediation status and risk of the client.

22. The duty of confidentiality extends indefinitely beyond the end of this contractual relationship. Exceptions exist in the case of statutory obligations to testify.

23. The Contractor is entitled to process personal data entrusted to it within the scope of the purpose of the contractual relationship. The Client warrants to the Contractor that all legal measures have been taken for this purpose.

Liability / compensation for damages

24. The performance of penetration tests may affect the integrity and availability of the target systems and/or connected systems. The Client shall ensure that the integrity and availability can be restored at any time during the execution of the penetration tests (e.g. via data backups, etc.). The Contractor shall not be liable for interruptions, failures and/or data losses, even if these were caused by the Contractor.

25. The Contractor shall only be liable to the Client for damages - with the exception of personal injury - in the event of gross negligence (intent or gross negligence). This shall also apply mutatis mutandis to damage attributable to third parties engaged by the Contractor.

26. Liability for consequential damages, loss of profit, loss of savings and damages from third-party claims is excluded. The Client shall fully indemnify and hold the Contractor harmless with regard to all claims asserted by third parties.

27. Claims for damages by the Client can only be asserted in court within six months of becoming aware of the damage and the damaging party, but at the latest within three years of the event giving rise to the claim.

28. The Client must provide proof that the damage is attributable to the Contractor's fault.

29. If the Contractor provides the commissioned service with the assistance of third parties and warranty and/or liability claims arise against these third parties in this context, the Contractor shall assign these claims to the Client. In this case, the Client shall give priority to these third parties.

Reporting

30. The client shall receive the final report no later than four weeks after completion of the order. The final report is transmitted electronically in encrypted form. The access data required to open it (e.g. password) is transmitted via a second channel (e.g. Signal Messenger, SMS).

31. The Contractor is not bound by instructions when providing the commissioned service and acts at its own discretion and under its own responsibility. He is not bound to a specific place of work or specific working hours.

32. If, at the request of the Client, the service must be provided outside normal working hours (working days Monday to Friday between 08.00 and 18.00 CET), a surcharge of 100% shall be charged for Sundays and public holidays and a surcharge of 50% for Saturdays and Mondays to Fridays between 18.00 and 08.00 CET.

33. If the service is performed by the Contractor at the Client's premises, the Client shall provide a suitable working environment free of charge. This working environment shall include a state-of-the-art office infrastructure including Internet access and shall comply with the applicable local workplace regulations.

Substitution

34. The Contractor shall be entitled to have the tasks incumbent upon it performed in whole or in part by third parties. Payment of the third party shall be made exclusively by the Contractor itself. No direct contractual relationship of any kind shall arise between the third party and the client.

Fee

35. The Contractor shall be entitled to a fee for the services provided by it (including travel and waiting times) in accordance with the individual contractual agreement between the Client and the Contractor. The Contractor shall be entitled to submit interim invoices in accordance with the progress of the work. The fee is due for payment 30 days from the invoice date, unless the invoice or order confirmation specifies a different payment term.

36. All payments arising from the contract shall be made in EURO.

37. In the event of late payment, default interest of 9% and reminder fees of EUR 20.00 per reminder shall be due even without a reminder.

38. The Contractor shall issue an invoice with all legally required features.

39. Any cash outlays, expenses, travel costs, etc. incurred shall be additionally reimbursed by the Client on presentation of an invoice by the Contractor.

40. The services rendered shall be invoiced according to actual expenditure.

41. The Contractor shall be free to charge a flat rate of 80% of the estimated fee for projects and/or project sections canceled or postponed by the Client at short notice (less than 14 days before agreed execution).

Electronic invoicing

42. The Contractor is also entitled to send invoices to the Client in electronic form. The Client expressly agrees to the Contractor sending invoices in electronic form.

Duration of the contract

43. This contract shall generally end with the completion of the project and the corresponding invoicing.

44. Notwithstanding this, the contract may be terminated by either party at any time for good cause without notice. Good cause shall be deemed to exist in particular

- if a contracting party breaches material contractual obligations, or
- if a contracting party is in default of payment, or

- if there are justified concerns regarding the creditworthiness of a contracting party for which insolvency proceedings have not been opened and this party neither makes advance payments at the request of the contractor nor provides suitable security before the contractor performs and the poor financial circumstances of the other contracting party were not known when the contract was concluded.

Mediation

45. In the event of disputes arising from this contract that cannot be settled amicably, the contracting parties agree by mutual consent to use registered mediators (Austrian Civil Mediation Act) specializing in commercial mediation from the list of the Austrian Ministry of Justice to settle the conflict out of court. If no agreement can be reached on the selection of business mediators or on the content of the mediation, legal action will be initiated at the earliest one month after the failure of the negotiations.

46. In the event that mediation does not take place or is terminated, Austrian substantive law shall apply in any legal proceedings initiated, to the exclusion of the conflict of law rules of private international law and the UN Convention on Contracts for the International Sale of Goods.

47. All necessary expenses incurred as a result of prior mediation, in particular also those for legal advisors consulted, can be claimed as "pre-litigation costs" in court or arbitration proceedings as agreed.

Final provisions

48. The contracting parties confirm that they have provided all information in the contract conscientiously and truthfully and undertake to notify each other immediately of any changes.

49. Amendments to the contract and these GTC must be made in writing; the same applies to any waiver of this formal requirement. Verbal collateral agreements do not exist.

50. This contract shall be governed by Austrian substantive law to the exclusion of the conflict of law rules of private international law and the UN Convention on Contracts for the International Sale of Goods. The place of performance is the location of the Contractor's professional establishment. The courts in Vienna (Austria) shall have exclusive jurisdiction for disputes.

This service description was machine-translated to English and shall be governed exclusively by the German language version; the translation into English is for illustrative purposes only.

As of November 27, 2023