Servicebeschreibung Penetration-Tests & Phishing-Simulationen

Allgemeine Grundlagen und Geltungsbereich

1. Für sämtliche Rechtsgeschäfte im Zusammenhang mit Penetration-Tests und Phishing-Simulationen zwischen dem Auftraggeber und dem Auftragnehmer (Unternehmensberater) – im Folgenden wird nur die Bezeichnung Auftragnehmer verwendet - gilt ausschließlich diese Servicebeschreibung. Maßgeblich ist jeweils die zum Zeitpunkt des Vertragsabschlusses gültige Fassung.

2. Auftraggeber kann nur ein Unternehmer im Sinne des § 1 des Österreichischen Konsumentenschutzgesetzes (KSchG) sein.

3. Diese Servicebeschreibung gilt auch für alle künftigen Vertragsbeziehungen im Zusammenhang mit Penetration-Tests und Phishing-Simulationen, somit auch dann, wenn bei Zusatzverträgen darauf nicht ausdrücklich hingewiesen wird.

4. Entgegenstehende Allgemeine Geschäftsbedingungen des Auftraggebers sind ungültig, es sei denn, diese werden vom Auftragnehmer ausdrücklich schriftlich anerkannt.

5. Für den Fall, dass einzelne Bestimmungen dieser Servicebeschreibung unwirksam sein und/oder werden sollten, berührt dies die Wirksamkeit der verbleibenden Bestimmungen und der unter ihrer Zugrundelegung geschlossenen Verträge nicht. Die unwirksame ist durch eine wirksame Bestimmung, die ihr dem Sinn und wirtschaftlichen Zweck nach am nächsten kommt, zu ersetzen.

Ziel und Umfang von Penetration-Tests

6. Das Ziel von Penetration-Tests ist die Identifizierung von technischen Risiken und Schwachstellen der Zielsysteme.

7. Im Zuge der Durchführung von Penetration-Tests werden keine Maßnahmen durchgeführt, die die Nichtverfügbarkeit der Zielsysteme zum Zweck haben (Denial of Service, Distributed Denial of Service), es sei denn im Angebot ist explizit eine derartige Dienstleistung angeboten.

8. Der Umfang des konkreten Penetration-Tests wird im Einzelfall vertraglich vereinbart und ist zeitlich limitiert (“Time Box”). Der Auftragnehmer sichert nicht zu, sämtliche vorhandene Sicherheitslücken auch tatsächlich aufzudecken. Dies ist bedingt durch die limitierten zeitlichen Ressourcen und den eingeschränkten Kenntnisstand der Penetration-Tester zu IT-Infrastruktur, Software, Quellcode, Benutzer, etc. Die Offenlegung von Systeminterna, die Bereitstellung von Test-Benutzern und die umfassende Kooperation des Auftraggebers mit dem Auftragnehmer erhöhen die Effizienz des Penetration-Tests.

9. Der Auftraggeber stellt dem Auftragnehmer spätestens drei Werktage vor Beginn der Dienstleistung schriftlich (z. B. per E-Mail) die Liste der Zielsysteme (“Scope”; IP-Adressen, Domains, Subdomains, Standorte, E-Mail-Adressen, etc.) zur Verfügung. Mit der Übermittlung des Scopes geht die implizite Erlaubnis des Auftraggebers für die Durchführung intrusiver Penetration-Tests einher (“Permission to Attack”). Der Auftraggeber garantiert die Befugnis zu haben, die genannten Zielsysteme intrusiv attackieren zu lassen.

Ziel und Umfang von Phishing-Simulationen

10. Das Ziel von Phishing-Simulationen ist die Schaffung und Erhebung des Security-Bewusstseins der seitens des Auftraggebers definierten Zielgruppe.

11. Der Umfang und die genaue Ausgestaltung der Phishing-Simulation wird im Einvernehmen zwischen Auftraggeber und Auftragnehmer vereinbart.

12. Der Auftraggeber stellt dem Auftragnehmer spätestens drei Werktage vor Beginn der Dienstleistung schriftlich (z. B. per E-Mail) die Liste der E-Mail-Adressen der Empfänger (“Scope”) zur Verfügung. Mit der Übermittlung des Scopes geht die implizite Erlaubnis des Auftraggebers für die Durchführung von Phishing-Simulationen einher (“Permission to Attack”). Der Auftraggeber garantiert die Befugnis zu haben, Phishing-Simulationen mit dem übermittelten Scope durchführen zu lassen.

13. Der Auftraggeber sorgt dafür, dass sämtliche technische Maßnahmen zur Blockade unerwünschter E-Mails (SPAM-Schutz, Phishing-Prevention, Anti-Viren-Systeme, Mail-Security-Lösungen, etc) während des Durchführungszeitraums für die vonseiten des Auftraggebers zu nennenden Absenderadressen deaktiviert sind. Andernfalls kann die Zustellung der Phishing-Simulation an die Empfänger und damit die erfolgreiche Durchführung der Dienstleistung nicht gewährleistet werden.

Aufklärungs- und Mitwirkungspflichten des Auftraggebers

14. Der Leistungszeitraum wird im Einvernehmen zwischen Auftragnehmer und Auftraggeber vereinbart. Die Vorlaufzeit zwischen Zustandekommen des Vertrages und

Beginn des Leistungszeitraums kann bis zu zwölf Wochen betragen.

15. Der Auftraggeber sorgt dafür, dass dem Auftragnehmer auch ohne dessen besondere Aufforderung alle für die Erfüllung und Ausführung der Dienstleistung notwendigen Unterlagen, Zugänge, Benutzerkonten, Berechtigungen und Betriebsmittel spätestens drei Werktage vor Beginn der Dienstleistung vorgelegt werden.

16. Der Auftraggeber sorgt dafür, dass die organisatorischen Rahmenbedingungen bei Erfüllung der Dienstleistung ein möglichst ungestörtes, dem raschen Fortgang des Dienstleistungsprozesses förderliches Arbeiten erlauben.

17. Der Auftraggeber sorgt dafür, dass alle notwendigen Stellen (ggf. seine Mitarbeiter, die eingerichtete Arbeitnehmervertretung (Betriebsrat), etc.) bereits vor Beginn der Tätigkeit des Auftragnehmers von dieser informiert werden.

Geheimhaltung / Datenschutz

18. Der Auftragnehmer verpflichtet sich zu unbedingtem Stillschweigen über alle ihm zur Kenntnis gelangenden geschäftlichen Angelegenheiten, insbesondere Geschäfts- und Betriebsgeheimnisse sowie jedwede Information, die er über Art, Betriebsumfang und praktische Tätigkeit des Auftraggebers erhält.

19. Weiters verpflichtet sich der Auftragnehmer, über sämtliche Informationen und Umstände, die ihm im Zusammenhang mit der Erfüllung der beauftragten Dienstleistung zugegangen sind, Dritten gegenüber Stillschweigen zu bewahren.

20. Der Auftragnehmer ist von der Schweigepflicht gegenüber allfälligen Gehilfen und Stellvertretern, denen er sich bedient, entbunden. Er hat die Schweigepflicht aber auf diese vollständig zu überbinden und haftet für deren Verstoß gegen die Verschwiegenheitsverpflichtung wie für einen eigenen Verstoß.

21. Sollten im Zuge der Dienstleistung Sicherheitslücken in Komponenten (z. B. Software oder Hardware) von Drittanbietern identifiziert werden, ist der Auftragnehmer berechtigt, den Hersteller darüber zu informieren, CVE-(Common Vulnerabilities and Exposures-)Nummern zu beantragen und im Rahmen eines Responsible Disclosure-Prozesses zu veröffentlichen. Eine Veröffentlichung erfolgt unter Berücksichtigung des Behebungsstatus und Risikos des Auftraggebers.

22. Die Schweigepflicht reicht unbegrenzt auch über das Ende dieses Vertragsverhältnisses hinaus. Ausnahmen bestehen im Falle gesetzlich vorgesehener Aussageverpflichtungen.

23. Der Auftragnehmer ist berechtigt, ihm anvertraute personenbezogene Daten im Rahmen der Zweckbestimmung des Vertragsverhältnisses zu verarbeiten. Der

Auftraggeber leistet dem Auftragnehmer Gewähr, dass hiefür sämtliche gesetzliche Maßnahmen getroffen worden sind.

Haftung / Schadenersatz

24. Die Durchführung von Penetration-Tests kann die Integrität und Verfügbarkeit der Zielsysteme und/oder verbundener Systeme beeinträchtigen. Der Auftraggeber sorgt dafür, dass die Integrität und Verfügbarkeit während der Durchführung der Penetration-Tests jederzeit wiederhergestellt werden können (z. B. über Datensicherungen, etc.). Der Auftragnehmer haftet nicht für Unterbrechungen, Ausfälle und/oder Datenverluste, auch wenn diese von ihm herbeigeführt wurden.

25. Der Auftragnehmer haftet dem Auftraggeber für Schäden – ausgenommen für Personenschäden - nur im Falle groben Verschuldens (Vorsatz oder grobe Fahrlässigkeit). Dies gilt sinngemäß auch für Schäden, die auf vom Auftragnehmer beigezogene Dritte zurückgehen.

26. Die Haftung für Folgeschäden, entgangenen Gewinn, ausgebliebene Einsparungen, sowie Schäden aus Ansprüchen Dritter ist ausgeschlossen. Der Auftraggeber hält den Auftragnehmer hinsichtlich sämtlicher von Dritter Seite erhobener Ansprüche in vollem Umfang schad- und klaglos.

27. Schadenersatzansprüche des Auftraggebers können nur innerhalb von sechs Monaten ab Kenntnis von Schaden und Schädiger, spätestens aber innerhalb von drei Jahren nach dem anspruchsbegründenden Ereignis gerichtlich geltend gemacht werden.

28. Der Auftraggeber hat jeweils den Beweis zu erbringen, dass der Schaden auf ein Verschulden des Auftragnehmers zurückzuführen ist.

29. Sofern der Auftragnehmer die beauftragte Dienstleistung unter Zuhilfenahme Dritter erbringt und in diesem Zusammenhang Gewährleistungs- und/oder Haftungsansprüche gegenüber diesen Dritten entstehen, tritt der Auftragnehmer diese Ansprüche an den Auftraggeber ab. Der Auftraggeber wird sich in diesem Fall vorrangig an diese Dritten halten.

Berichterstattung

30. Den Schlussbericht erhält der Auftraggeber spätestens vier Wochen nach Abschluss des Auftrages. Der Schlussbericht wird elektronisch in verschlüsselter Form übermittelt. Die zum Öffnen benötigten Zugangsdaten (z. B. Passwort) werden über einen zweiten Kanal (z. B. Signal Messenger, SMS) übermittelt.

31. Der Auftragnehmer ist bei der Erbringung der beauftragten Dienstleistung weisungsfrei, handelt nach eigenem Gutdünken und in eigener Verantwortung. Er ist an

keinen bestimmten Arbeitsort und keine bestimmte Arbeitszeit gebunden.

32. Muss die Leistungserbringung auf Verlangen des Auftraggebers außerhalb der gewöhnlichen Arbeitszeit (Arbeitstage Montag bis Freitag zwischen 08.00 und 18.00 Uhr MEZ) durchgeführt werden, so wird für Sonntage und Feiertage ein Zuschlag von 100%, für Samstage sowie montags bis freitags zwischen 18.00 und 08.00 Uhr MEZ ein Zuschlag von 50% in Rechnung gestellt.

33. Wird die Leistung durch den Auftragnehmer in einer Betriebsstätte des Auftraggebers durchgeführt, so stellt der Auftraggeber kostenlos eine geeignete Arbeitsumgebung zur Verfügung. Diese Arbeitsumgebung umfasst eine dem Stand der Technik entsprechende Büroinfrastruktur inklusive Internetzugang und entspricht der jeweils lokal gültigen Arbeitsstättenverordnung.

Stellvertretung

34. Der Auftragnehmer ist berechtigt, die ihm obliegenden Aufgaben ganz oder teilweise durch Dritte erbringen zu lassen. Die Bezahlung des Dritten erfolgt ausschließlich durch den Auftragnehmer selbst. Es entsteht kein wie immer geartetes direktes Vertragsverhältnis zwischen dem Dritten und dem Auftraggeber.

Honorar

35. Dem Auftragnehmer steht für die von ihm erbrachten Leistungen (inklusive Reise- und Wartezeiten) ein Honorar gemäß der einzelvertraglichen Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer zu. Der Auftragnehmer ist berechtigt, dem Arbeitsfortschritt entsprechend Zwischenabrechnungen zu legen. Das Honorar ist 30 Tage ab Rechnungsdatum zur Zahlung fällig, soweit sich aus Rechnung oder Auftragsbestätigung kein anderes Zahlungsziel ergibt.

36. Alle Zahlungen, die aus dem Vertrag heraus entstehen, werden in EURO geleistet.

37. Bei Zahlungsverzug werden auch ohne Mahnung Verzugszinsen in der Höhe von 9%, sowie Mahnspesen in der Höhe von EURO 20,00 pro Mahnung fällig.

38. Der Auftragnehmer wird jeweils eine Rechnung mit allen gesetzlich erforderlichen Merkmalen ausstellen.

39. Anfallende Barauslagen, Spesen, Reisekosten, etc. sind gegen Rechnungslegung des Auftragnehmers vom Auftraggeber zusätzlich zu ersetzen.

40. Die Verrechnung der erbrachten Leistungen erfolgt nach tatsächlichem Aufwand.

41. Dem Auftragnehmer steht es frei, kurzfristig (weniger als 14 Tage vor vereinbarter Durchführung) durch den Auftraggeber abgesagte oder verschobene Projekte und/oder Projektabschnitte pauschal mit 80% des veranschlagten Honorars zu verrechnen.

Elektronische Rechnungslegung

42. Der Auftragnehmer ist berechtigt, dem Auftraggeber Rechnungen auch in elektronischer Form zu übermitteln. Der Auftraggeber erklärt sich mit der Zusendung von Rechnungen in elektronischer Form durch den Auftragnehmer ausdrücklich einverstanden.

Dauer des Vertrages

43. Dieser Vertrag endet grundsätzlich mit dem Abschluss des Projekts und der entsprechenden Rechnungslegung.

44. Der Vertrag kann dessen ungeachtet jederzeit aus wichtigen Gründen von jeder Seite ohne Einhaltung einer Kündigungsfrist gelöst werden. Als wichtiger Grund ist insbesondere anzusehen,

- wenn eine Vertragspartei wesentliche Vertragsverpflichtungen verletzt, oder
- wenn eine Vertragspartei in Zahlungsverzug gerät, oder
- wenn berechtigte Bedenken hinsichtlich der Bonität einer Vertragspartei, über die kein Insolvenzverfahren eröffnet ist, bestehen und diese auf Begehren des Auftragnehmers weder Vorauszahlungen leistet noch vor Leistung des Auftragnehmers eine taugliche Sicherheit leistet und die schlechten Vermögensverhältnisse der anderen Vertragspartei bei Vertragsabschluss nicht bekannt waren.

Mediation

45. Für den Fall von Streitigkeiten aus diesem Vertrag, die nicht einvernehmlich geregelt werden können, vereinbaren die Vertragsparteien einvernehmlich zur außergerichtlichen Beilegung des Konfliktes eingetragene Mediatoren (Österreichisches ZivMediatG) mit dem Schwerpunkt WirtschaftsMediation aus der Liste des Österreichischen Justizministeriums beizuziehen. Sollte über die Auswahl der WirtschaftsMediatoren oder inhaltlich kein Einvernehmen hergestellt werden können, werden frühestens ein Monat ab Scheitern der Verhandlungen rechtliche Schritte eingeleitet.

46. Im Falle einer nicht zustande gekommenen oder abgebrochenen Mediation, gilt in einem allfällig eingeleiteten Gerichtsverfahren materielles österreichisches Recht unter

Ausschluss der Verweisungsnormen des internationalen Privatrechts sowie des UN-Kaufrechts.

47. Sämtliche aufgrund einer vorherigen Mediation angelaufenen notwendigen Aufwendungen, insbesondere auch jene für beigezogene Rechtsberater, können vereinbarungsgemäß in einem Gerichts- oder Schiedsgerichtsverfahren als „vorprozessuale Kosten“ geltend gemacht werden.

Schlussbestimmungen

48. Die Vertragsparteien bestätigen, alle Angaben im Vertrag gewissenhaft und wahrheitsgetreu gemacht zu haben und verpflichten sich, allfällige Änderungen wechselseitig umgehend bekannt zu geben.

49. Änderungen des Vertrages und dieser AGB bedürfen der Schriftform; ebenso ein Abgehen von dieser Formerfordernis. Mündliche Nebenabreden bestehen nicht.

50. Auf diesen Vertrag ist materielles österreichisches Recht unter Ausschluss der Verweisungsnormen des internationalen Privatrechts sowie des UN-Kaufrechts anwendbar. Erfüllungsort ist der Ort der beruflichen Niederlassung des Auftragnehmers. Für Streitigkeiten sind ausschließlich die Gerichte in Wien (Österreich) zuständig.

Stand: 27. November 2023