Zusatzbedingungen für Penetrationstests

Fassung / Version 2 vom / of 22.01.2020

1. Allgemeine Grundlagen / Geltungsbereich

1.1 Für alle Aufträge des Auftraggebers an den Auftragnehmer (Unternehmensberater), die einen Penetrations-Test umfassen, gelten insoweit diese Zusatzbedingungen für Penetrations-Tests. Subsidiär gelten die Allgemeinen Geschäftsbedingungen des Auftragnehmers (Unternehmensberaters).

2. Penetrations-Test

2.1 Ein Penetrations-Test ist der kontrollierte Versuch, von außen in ein Computersystem einzudringen, um Schwachstellen des Systems zu erkennen. Dabei werden Techniken angewandt, die auch bei einem echten Angriff auf das System Verwendung finden würden. Das Ziel des Penetrations-Tests liegt darin Schwachstellen zu erkennen, um diese korrigieren zu können.

2.2 Der Penetrations-Test erfolgt ausschließlich aus bestimmten IPv4 und IPv6-Adressbereichen, sodass der Auftraggeber zwischen dem Penetrations-Test und realen Angriffen unterscheiden kann.

2.3 Das Erkennen sozialer Risiken wie etwa Schädigung durch untreue Mitarbeiter ist nicht Gegenstand des Penetrations-Tests. Der Auftragnehmer (Unternehmensberater) wird beim Penetrations-Test auch keine Mitarbeiter zu unethischem Verhalten anstiften.

2.4 Ein Penetrations-Test umfasst nicht die Überprüfung auf IT-Compliance (wie Einhaltung von Richtlinien und von Prozessbeschreibungen).

2.5 Wegen unvermeidlicher Beschränkung der zeitlichen und finanziellen Ressourcen, ist bei einem Penetrations-Test nicht gewährleistet, dass im Rahmen der Tests sämtliche Risiken aufgedeckt werden.

2.6 Der Auftraggeber wird dem Auftragnehmer (Unternehmensberater) etwaige erforderliche Informationen zur Verfügung stellen. Welche Informationen notwendig sind, wird der Auftragnehmer (Unternehmensberater) vor Beginn des Penetrations-Tests bekannt geben.

3. Art des Penetrations-Tests

3.1 Der Penetrations-Test wird in der Regel passiv-scannend erfolgen. Es wird keine absichtliche Störung oder Zerstörung des Computersystems erfolgen. Von diesem Umfang kann mittels ausdrücklicher Vereinbarung abgewichen werden.

3.2 Der Penetrations-Test wird durch technische Methoden über den Internet-Zugang, LAN-Zugang und WLAN-Zugang erfolgen.

risk on mind® GmbH
Prinz Eugenstraße 45/8
2301 Groß Enzersdorf
Österreich

+43 (664) 353 99 22
office@riskonmind.at
www.riskonmind.at

IBAN AT25 1200 0100 2613 2638
BIC BKAUATWW
UID ATU74086589
FN 506108 b

3.3 Der Penetrations-Test wird nur bei ausdrücklicher Beauftragung den Versuch umfassen, durch Manipulation der Systeme oder von Mitarbeitern des Auftraggebers in das Computersystem einzudringen (Social Hacking).

4. Computersystem

4.1 Der Auftraggeber bestätigt, dass das Computersystem sein eigenes ist und dass er das Recht hat, einen Penetrations-Test auf das Computersystem zu erlauben.

4.2 Bei Standardsoftware wird der Auftragnehmer (Unternehmensberater) die Penetrations-Test-Regeln des jeweiligen Softwareunternehmens (etwa die 'Penetration Testing Rules of Engagement' der Microsoft Cloud) einhalten.

4.3 Der Auftraggeber erklärt, dass er alle erforderlichen Zustimmungen Dritter (wie Lizenzgeber, IT-Dienstleister, Provider, Hoster, Mitarbeiter, Betriebsrat, Datenschutzbeauftragte) eingeholt hat.

4.4 Wenn der Auftragnehmer (Unternehmensberater) wegen des Penetrationstest von Dritten in Anspruch genommen wird, so wird der Auftraggeber den Auftragnehmer (Unternehmensberater) unterstützen und schad- und klaglos halten.

4.5 Der Auftraggeber erteilt seine ausdrückliche Einwilligung, dass beim Penetrations-Test Handlungen gesetzt werden, welche ohne Zustimmung verboten wären, etwa als:
- Widerrechtlicher Zugriff auf ein Computersystem (§ 118a StGB);
- Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB);
- Missbräuchliches Abfangen von Daten (§ 119a StGB);
- Auskundschaften eines Geschäfts- oder Betriebsgeheimnisses (§ 119a StGB);
- Datenbeschädigung (§ 126a StGB);
- Funktionsstörung eines Computersystems (§ 126b StGB);
- Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB).

5. Prüfungsumfang und Werkzeuge

5.1 Der Umfang des zu prüfenden Computersystems und die eingesetzten Werkzeuge ergeben sich aus der getroffenen Vereinbarung.

5.2 Der Auftragnehmer (Unternehmensberater) ist jedoch berechtigt, auf das gesamte Computersystem des Auftraggebers zuzugreifen. Wenn es Systemteile gibt, auf die der Auftragnehmer (Unternehmensberater) nicht zugreifen darf, muß der Auftraggeber diese schriftlich bekanntgeben.

6. Back-Up

6.1 Dem Auftraggeber ist bekannt, dass durch Penetrations-Tests Schäden an bestehenden Systemen auftreten können, die nur durch das Einspielen von Back-Ups und allenfalls zusätzliche Nachbearbeitungen des Auftraggebers behoben werden können.

6.2 Der Auftraggeber ist daher verpflichtet, das gesamte Computersystem und damit in Verbindung stehende Daten vor Beginn des Penetrations-Tests durch ein Back-Up und andere notwendige Sicherheitsmaßnahmen zu sichern und zu verifizieren, dass ihn der Back-Up Vorgang und die anderen Sicherheitsmaßnahmen in die Lage versetzt, das Computersystem wieder in den Vortest-Zustand zu versetzen.

6.3 Der Auftraggeber verzichtet auf alle Schadenersatzansprüche aus Schäden, die im Zuge des Penetrations-Tests entstehen.

7. Daten

7.1 Der Auftragnehmer (Unternehmensberater) verpflichtet sich, alle gewonnen Informationen des Auftraggebers auch über die Dauer der geschäftlichen Beziehung hinaus streng vertraulich zu behandeln und darüber Stillschweigen zu wahren.

7.2 Sollte der Auftragnehmer (Unternehmensberater) während des Penetrations-Tests auf personenbezogene Daten zugreifen müssen, werden diese soweit wie möglich anonymisiert werden.

7.3 Nach Beendigung des Auftrags wird der Auftragnehmer (Unternehmensberater) alle gewonnenen Informationen löschen.

7.4 Der Auftragnehmer (Unternehmensberater) wird mit den eingesetzten Mitarbeitern Vertraulichkeitsvereinbarungen abschließen und wird die Vertraulichkeitsvereinbarungen dem Auftraggeber auf Verlangen vorweisen.

8. Rechtswahl und Gerichtsstand

8.1 Auf diesen Vertrag ist materielles österreichisches Recht unter Ausschluss der Verweisungsnormen des internationalen Privatrechts anwendbar. Erfüllungsort ist der Ort der beruflichen Niederlassung des Auftragnehmers (Unternehmensberaters).

8.2 Für Streitigkeiten ist das Gericht am Unternehmensort des Auftragnehmers (Unternehmensberaters) zuständig.