

1. Geltungsbereich und Begriffsbestimmungen

1.1. Diese Geschäftsbedingungen für Security Services („Besondere Bedingungen“) gelten ergänzend zu den Allgemeinen Geschäftsbedingungen der E&C Testlab GmbH („E&C“) für alle Verträge über Beratungs-, Prüfungs-, Analyse-, Monitoring-, Engineering- oder sonstige Dienstleistungen im Bereich der SECURITY SERVICES mit deren Auftraggeber („Auftraggeber“).

2. Definitionen

2.1. „**PENTESTS**“ (Penetrationstests) bezeichnen eine vereinbarte, kontrollierte Simulation von Angriffen auf Systeme, Anwendungen, Netzwerke oder organisatorische Prozesse des Auftraggebers, um deren Sicherheit zu überprüfen und Schwachstellen zu identifizieren.

2.2. „**ZIELSYSTEME**“ sind die vom Auftraggeber ausdrücklich benannten Produkte, IP-Adressen, Domains, Applikationen oder Infrastrukturelemente, auf die sich der Test bezieht.

2.3. „**ERGEBNISSE**“ sind die im Rahmen der Security Services erstellten Testergebnisse, Reports, Risikoanalysen, Konzepte, Architekturbewertungen, Empfehlungen oder sonstigen Arbeitsergebnisse.

2.4. „**SECURITY SERVICES**“ umfassen sämtliche von E&C angebotenen oder durchgeführten Dienstleistungen im Bereich Cyber-Security, einschließlich, aber nicht beschränkt auf, Penetrationstests, Sicherheitsanalysen, Schwachstellenbewertungen, Risikoanalysen (z. B. TARA), Beratung, Monitoring, Incident Response, Security Engineering sowie die Erstellung von Sicherheits- und Systemkonzepten.

2.5. „**STATEMENT OF WORK (SOW)**“ bezeichnet die zwischen den Parteien schriftlich vereinbarte Leistungsbeschreibung, in der insbesondere Leistungsumfang, Methodik, Zeitplan, Vergütung und sonstige Details des jeweiligen Projekts festgelegt sind.

3. Leistungsgegenstand und Durchführung

3.1. E&C führt die SECURITY SERVICES ausschließlich im Rahmen und Umfang des schriftlich vereinbarten SOWs durch. Änderungen oder Erweiterungen des Leistungsumfangs bedürfen der schriftlichen Zustimmung beider Parteien.

3.2. Der Auftraggeber trägt die Verantwortung für:

- die rechtmäßige Beauftragung des SECURITY SERVICES,
- die Einholung aller erforderlichen Genehmigungen (z. B. von Eigentümern, Hostern oder Providern),
- die Korrektheit und Vollständigkeit der Zieldefinition.

3.3. E&C ist berechtigt, im Rahmen der SECURITY SERVICES technische Handlungen vorzunehmen, die – auch unbeabsichtigt – zu Systembeeinträchtigungen oder Datenverlusten führen können. Der Auftraggeber erkennt an, dass solche Risiken typischerweise mit Sicherheitsprüfungen und technischen Tests verbunden sind.

3.4. Teilergebnisse und Zwischenberichte sind keine verbindlichen Gutachten, sondern dienen der fortlaufenden Kommunikation über den Fortschritt der Leistungserbringung.

3.5. E&C ist berechtigt, zur Erfüllung der vertraglich geschuldeten Leistungen verbundene Unternehmen im Sinne der §§ 15 ff. AktG, externe Dienstleister oder sonstige Dritte als Unterauftragnehmer einzusetzen.

3.6. Leistungen dürfen ganz oder teilweise remote, über VPN, dedizierte Testzugänge oder Internetverbindungen oder von Standorten außerhalb Deutschlands erbracht werden. In diesem Fall gelten die Leistungen gleichwohl als am Sitz der E&C erbracht. E&C bleibt gegenüber dem Auftraggeber für die ordnungsgemäße Erfüllung sämtlicher vertraglicher Pflichten verantwortlich.

4. Mitwirkungspflichten des Auftraggebers

4.1. Der Auftraggeber hat sicherzustellen, dass:

- die zu prüfenden oder zu bearbeitenden Systeme, Prozesse oder Daten in seinem Eigentum stehen oder mit Zustimmung der Berechtigten getestet bzw. bearbeitet werden dürfen;
- bei PENTESTS vor Testbeginn eine schriftliche Freigabeerklärung durch den Auftraggeber sowie die finale, von beiden Parteien bestätigte Testscope-Definition im SOW vorliegt;
- Backups aller relevanten Systeme und Daten vor Beginn der technischen Leistungen erstellt sind;
- alle betroffenen internen Stakeholder (IT, SOC, ggf. Provider) informiert sind;

- während der Durchführung der SECURITY SERVICES ein technischer Ansprechpartner für die E&C erreichbar ist.

4.2. Kommt der Auftraggeber diesen Pflichten nicht nach, kann die E&C die Durchführung der SECURITY SERVICES ganz oder teilweise ablehnen, unterbrechen oder anpassen. Entstandene Mehrkosten und Verzögerungen trägt der Auftraggeber.

4.3. Erkennt der Auftraggeber nachträglich, dass SECURITY SERVICES unzulässig sein könnten, hat er E&C unverzüglich zu informieren.

4.4. Nach Abschluss der SECURITY SERVICES stellt E&C dem Auftraggeber die vereinbarten ERGEBNISSE zur Verfügung. Der Auftraggeber prüft diese innerhalb angemessener Zeit, spätestens jedoch innerhalb von 14 Kalendertagen nach Zugang, und teilt etwaige Rückfragen oder offenkundige Unstimmigkeiten unverzüglich mit. Sofern innerhalb dieser Frist keine Mitteilung erfolgt, gelten die Leistungen als ordnungsgemäß erbracht und abgeschlossen.

5. Ergebnisse und Nutzungsrechte

5.1. Die E&C räumt dem Auftraggeber nach vollständiger Vergütungszahlung das nicht ausschließliche, nicht übertragbare Recht ein, die im Rahmen der SECURITY SERVICES erstellten ERGEBNISSE zeitlich unbeschränkt für eigene betriebliche und interne Zwecke zu nutzen.

5.2. Eine Weitergabe der ERGEBNISSE oder Auszüge daraus an Dritte (z. B. Kunden, Auditoren, Versicherer) bedarf der vorherigen schriftlichen Zustimmung von E&C, soweit nicht gesetzliche oder regulatorische Offenlegungs- oder Nachweispflichten bestehen.

5.3. Veröffentlichungen der ERGEBNISSE, insbesondere in Pressemitteilungen, Marketingunterlagen oder öffentlichen Dokumentationen, sind nur mit ausdrücklicher schriftlicher Freigabe von E&C zulässig.

5.4. Alle Rechte, insbesondere Urheber-, Nutzungs- und Verwertungsrechte an Methoden, Verfahren, Tools, Skripten, Templates, Checklisten oder sonstiges Know-how, das E&C im Rahmen der SECURITY SERVICES einsetzt oder entwickelt, verbleiben ausschließlich bei E&C. Der Auftraggeber erhält hieran keine Rechte, auch wenn entsprechende Elemente in den ERGEBNISSEN enthalten oder beschrieben sind.

5.5. Eine Nutzung der ERGEBNISSE zu kommerziellen oder wettbewerblichen Zwecken, insbesondere zur Erbringung eigener oder fremder Sicherheitsdienstleistungen, zur Schulung Dritter oder zum Weiterverkauf, ist ohne vorherige schriftliche Zustimmung der E&C ausgeschlossen.

6. Vertraulichkeit und Datenschutz

6.1. Beide Parteien verpflichten sich zur strikten Vertraulichkeit sämtlicher im Zusammenhang mit den SECURITY SERVICES erlangten Informationen. Es gelten ergänzend die Geheimhaltungsregelungen der Ziffer 7 der Allgemeinen Geschäftsbedingungen von E&C und gegebenenfalls eine zusätzliche Geheimhaltungsvereinbarung zwischen den Parteien.

6.2. E&C behandelt sämtliche erhaltenen Zugangsdaten, Systeminformationen und ERGEBNISSE vertraulich und verwendet sie ausschließlich zur Vertragserfüllung.

6.3. Soweit im Rahmen der Durchführung der SECURITY SERVICES personenbezogene Daten verarbeitet werden, schließen die Parteien vor Beginn der Arbeiten eine Vereinbarung zur Auftragsverarbeitung (Art. 28 DSGVO).

6.4. E&C darf Unterauftragnehmern die für die Leistungserbringung erforderlichen Informationen, einschließlich vertraulicher Daten des Auftraggebers, offenlegen, soweit dies zur ordnungsgemäßen Vertragserfüllung erforderlich ist. E&C verpflichtet sämtliche Unterauftragnehmer zur Wahrung der Vertraulichkeit mindestens in dem Umfang, der sich aus Ziffer 7 der Allgemeinen Geschäftsbedingungen von E&C und Ziffer 6 dieser Besonderen Bedingungen ergibt.

7. Gewährleistung

7.1. E&C erbringt ihre Leistungen nach dem Stand der Technik und mit branchenüblicher Sorgfalt.

7.2. Die ERGEBNISSE basieren auf den zum Zeitpunkt der Leistungserbringung verfügbaren Informationen und spiegeln den Sicherheitszustand zum Untersuchungszeitpunkt wider. Spätere Änderungen an Systemen, Prozessen oder Rahmenbedingungen können zu abweichenden Bewertungen führen.

7.3. Soweit im Rahmen der SECURITY SERVICES werkvertragliche Leistungen geschuldet sind, leistet E&C Gewähr für Sachmängel nach Maßgabe der folgenden Bestimmungen:

- Voraussetzung für Mängelansprüche ist, dass der Auftraggeber den Mangel unverzüglich, spätestens jedoch innerhalb von vierzehn (14) Tagen, schriftlich rügt und E&C Gelegenheit zur Nacherfüllung gibt.
- Die Gewährleistungsfrist beträgt zwölf (12) Monate ab Abnahme;
- E&C ist berechtigt, den Mangel nach eigener Wahl zu beseitigen oder eine mangelfreie Leistung erneut zu erbringen.
- Weitergehende Ansprüche bestehen nur, wenn der Mangel die vertragsgemäße Nutzung der Leistung erheblich beeinträchtigt.

7.4. Für Beratungs-, Analyse-, Prüf- und sonstige Dienstleistungen gilt keine Gewährleistung im Rechtssinne; es gelten ausschließlich die Haftungsregelungen nach Ziffer 8 dieser Besonderen Bedingungen.

8. Haftung

8.1. Der Auftraggeber erkennt an, dass im Rahmen der SECURITY SERVICES, insbesondere bei technischen Tests oder Analysen, trotz größter Sorgfalt Systemausfälle, Datenverluste, Fehlfunktionen oder Performancebeeinträchtigungen auftreten können.

8.2. Für Schäden an ZIELSYSTEMEN, die im Rahmen ausdrücklich beauftragter PENTESTS entstehen, haftet E&C nicht, soweit nicht Vorsatz oder grobe Fahrlässigkeit vorliegen und die betreffenden Handlungen im vereinbarten Testumfang durchgeführt wurden.

8.3. E&C haftet nur für Schäden, die auf vorsätzliches oder grob fahrlässiges Verhalten zurückzuführen sind. Eine Haftung für entgangenen Gewinn, Produktionsausfall, Datenverlust oder mittelbare Schäden ist ausgeschlossen, es sei denn, E&C hat diese grob fahrlässig oder vorsätzlich verursacht.

Bei einfacher Fahrlässigkeit haftet E&C nur bei Verletzung solcher wesentlichen Vertragspflichten (Kardinalpflichten), deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf. In diesem Fall ist die Haftung auf den vorhersehbaren, vertragstypischen Schaden begrenzt, höchstens jedoch auf:

- bei Einzelaufträgen: den Betrag der vereinbarten Vergütung des jeweiligen SOW, maximal jedoch das Zweifache dieser Vergütung.
- bei Dauerschuldverhältnissen: vereinbarte Jahresvergütung (ohne Steuern) des Vertragsjahres, in dem das den Schaden auslösende Ereignis eingetreten ist.

8.4. Unberührt bleiben Ansprüche wegen Verletzung von Leben, Körper oder Gesundheit sowie zwingende Haftung nach dem Produkthaftungsgesetz.

9. Vergütung und Leistungszeit

9.1. Es gelten die Zahlungsbedingungen gemäß den Allgemeinen Geschäftsbedingungen von E&C in ihrer aktuellen Fassung.

9.2. Leistungstermine und Fristen ergeben sich aus dem jeweiligen SOW. Verzögerungen infolge nicht oder nicht rechtzeitig erfüllter Mitwirkungspflichten des Auftraggebers (vgl. Ziffer 4 dieser Besonderen Bedingungen) verlängern die Leistungszeiten entsprechend. E&C ist berechtigt, daraus entstehende Mehrkosten gesondert in Rechnung zu stellen.

9.3. Verlangt der Auftraggeber Änderungen oder Erweiterungen des Leistungsumfangs nach Vertragsschluss, sog. change request, wird E&C ein angepasstes Angebot vorlegen. Bis zur schriftlichen Annahme bleibt das ursprüngliche SOW maßgeblich.

10. Schlussbestimmungen

10.1. Im Falle von Widersprüchen zwischen diesen besonderen Bedingungen, dem SOW und den Allgemeinen Geschäftsbedingungen der E&C gilt folgende Rangfolge: (1) SOW, (2) Besondere Bedingungen, (3) Allgemeine Geschäftsbedingungen der E&C.