|  |  |  |
| --- | --- | --- |
| Angebot über: Penetrationstest Blackbox | | |
| Empfänger firmatoken  von Telekom Deutschland GmbH  -nachfolgend Telekom Deutschland genannt- | |  |
| Angebotsnummer: Angebotsdatum: | angebotsnumtoken angebotsdatoken | |

Informationen zum Angebot

|  |  |
| --- | --- |
| An | firmatoken  nachfolgend Auftraggeber genannt  fansprpartnertoken  fanschrifttoken  fortschafttoken |
| Kundennummer | angebotsnumtoken |
| Über | Penetrationstest Blackbox |
| Von | Telekom Deutschland GmbH, Geschäftskunden  aanschrifttoken  aortschafttoken |

|  |  |
| --- | --- |
| Ansprechpartner |  |
| Account Management | acmtoken |
| Telefon | acmtnrtoken |
| E-Mail | acmmailtoken |

|  |  |
| --- | --- |
| Angebotsnummer | angebotsnumtoken |
| Angebotsdatum | angebotsdatoken |

Telekom Deutschland GmbH, Gerichtsstand Bonn

Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Dieses Angebot enthält vertrauliche Informationen von der Telekom und wird unter der Voraussetzung unterbreitet, dass es weder ganz noch teilweise in irgendeiner Form verwendet oder Dritten zugänglich gemacht wird, außer den Mitarbeitern und professionellen Beratern des Kunden zum Zweck der Bewertung dieses Angebots oder zu einem anderen Zweck, sofern dies vorab schriftlich von der Telekom genehmigt wurde.

Inhaltsverzeichnis

1 Management Summary 4

2 Unternehmensporträt 5

3 Fachliche Beschreibung 6

3.1 Blackbox-Penetrationstest 6

3.2 Lieferumfang 7

3.3 Leistungsabgrenzung 7

3.4 Mitwirkung des Auftraggebers 7

3.4.1 Abstimmungsleistungen 7

3.4.2 Zuarbeitungsleistungen Penetrationstest 7

4 Projektabwicklung 9

4.1 Zeitplanung 9

4.2 Ort der Leistungserbringung 9

4.3 Abnahme 9

4.4 Abnahmefrist 9

5 Preise und Konditionen 10

5.1 Preise 10

5.1.1 Preisklausel 10

5.1.2 Rechnungslegung 10

5.1.3 Reisekosten 10

6 Ergänzende Bedingungen 11

6.1 Gültigkeitsdauer 11

6.2 Rechtliche Bedingungen 11

6.3 Garantieausschluss 11

6.4 Haftung 11

6.5 Haftungsausschluss 12

6.6 Nutzungsrechte 12

6.7 Datenschutz 12

6.8 Vertraulichkeit 12

7 Ansprechpartner 13

8 Auftragserteilung 15

# Management Summary

Vernetzte Rechnersysteme und Anwendungen sind insbesondere aufgrund ihrer Verfügbarkeit im Internet einer permanenten Gefährdung ausgesetzt (z. B. durch Hackerangriffe). Diese können zu erheblichen materiellen sowie immateriellen Schäden (z. B. Vertrauens- und Imageverlust) führen. Unter diesen Aspekten ist es daher geboten, die Sicherheit der Systeme und Anwendungen regelmäßig zu prüfen und ggf. Maßnahmen einzuleiten, um mögliche Risiken zu senken.

Die Telekom Deutschland GmbH (im Folgenden Telekom Deutschland oder Auftragnehmer genannt) bietet daher der firmatoken (im Folgenden Auftraggeber genannt) die Durchführung eines Blackbox-Penetrationstests an.

Die Leistungen werden durch die T-Systems Multimedia Solutions GmbH (im Folgenden T-Systems MMS genannt), eine 100%ige Tochter der T-Systems International GmbH, als Subunternehmerin erbracht.

Preis

Der Angebotspreis für die Durchführung des Blackbox-Penetrationstests gemäß Kapitel 3.1 beträgt 4.248,00 €.

Termine

Vertragsbeginn: nach Beauftragung

Vertragsende: 1 Monat nach Lieferung Abschlussbericht

# Unternehmensporträt

Telekom Deutschland Geschäftskunden

Die Telekom stärkt die Wettbewerbsfähigkeit ihrer Geschäftskunden mit integrierten Festnetz-, Mobilfunk- und IT-Lösungen aus einer Hand. Im Bereich Geschäftskunden der Telekom Deutschland GmbH bündelt der Konzern Telekom alle Leistungen für kleine, mittlere und große Unternehmen sowie für Freiberufler und Selbstständige. Hier werden in Deutschland rund 2,7 Millionen Geschäftskunden betreut. Die Telekom Deutschland GmbH bietet ihren Geschäftskunden ein integriertes Portfolio aus Festnetz-, Mobilfunk- und IT-Leistungen für das vernetzte Leben und Arbeiten. Entscheidend aus Sicht der Geschäftskunden: Sie haben stets nur einen Ansprechpartner für alle Anforderungen an die Informationstechnik und Telekommunikation. Für die Geschäftskunden sind rund 15 500 Mitarbeiter in Vertrieb, Kundenservice und technischem Service im Einsatz.

Zum Angebotsspektrum für Geschäftskunden gehören:

* Festnetz- und Mobiltelefonie
* IP-Telefonie
* Breitbandige Internetanbindung und mobiles Internet- mit jeweils maßgeschneiderten Tarifen
* Endgeräte und Kommunikationssysteme für Festnetz, Mobilfunk und IT  
  (z.B. Telefonanlagen, iPhone, Google-Phone, BlackBerry, Desktops und Laptops)
* Lösungen für die Standortvernetzung und Sicherheitsarchitektur
* IT-Services wie Hosting und Desktop Services
* Netzzentrierte Informations- und Kommunikationstechnik wie Software as a Service oder Telefonanlagen aus dem Netz
* IT-Anwendungen wie Customer Relationship Management (CRM) und Microsoft Office.

Mit ihrem Angebotsportfolio stärkt die Telekom die Wettbewerbsfähigkeit ihrer Geschäfts-kunden und ermöglicht es ihnen, neue Effizienz- und Wertschöpfungspotenziale zu erschließen. Das standardisierte Leistungsangebot ist modular aufgebaut und lässt sich so exakt auf die Anforderungen des Kunden anpassen - und bei wachsenden Anforderungen flexibel erweitern.

Die Geschäftskunden der Telekom profitieren vor allem von der umfassenden Integration der IT- und Telekommunikationstechnologien. Auf der Basis dieser Integration sind beispielsweise die Vertriebsmitarbeiter eines Unternehmens im Büro und unterwegs stets unter derselben Rufnummer erreichbar. Darüber hinaus können sie von überall auf Informationen im Unternehmensnetz zugreifen. Mit Diensten wie Software as a Service stellt die Telekom klassische Office- und Unternehmensanwendungen auf Mietbasis über das Netz zur Verfügung – und entlastet die Kunden damit von aufwändiger Implementierung, Wartung und Pflege sowie hohen Investitionskosten für Hardware und Lizenzen.

Die Telekom Deutschland GmbH ist in Deutschland auch für ihre Geschäftskunden flächendeckend präsent. Durch die Nähe zu den Kunden bietet die Telekom den Geschäftskunden eine Beratung und Betreuung in hoher Qualität, schnelle Entstörung und ausgeprägte Termintreue. Zusätzlich kann der Telekom Konzern die internationalen Standorte größerer Unternehmen weltweit über ein virtuelles privates Netz auf Basis des Internetprotokolls (IP-VPN) anbinden. Ihre Leistungen können Kunden persönlich, telefonisch, über das Internet oder über externe Vertriebs- und Servicepartner beauftragen.

# Fachliche Beschreibung

## Blackbox-Penetrationstest

Im Rahmen des Penetrationstests werden die Systeme / Anwendungen aus der Position eines potentiellen Angreifers auf vorhandene Schwachstellen überprüft. Damit kann eine Einschätzung des Sicherheitsniveaus gegeben werden.

Dabei bedeutet ein Blackbox Penetrationstest den zielgerichteten Versuch, mit den Mitteln eines Angreifers innerhalb einer gegebenen Zeitspanne Lücken in der Sicherheit einer Anwendung oder eines Systems aufzudecken. Im Rahmen des Tests werden Informationen über die Sicherheitsmerkmale auf dem Zielsystem gesammelt und dann versucht, diese Sicherheitsmerkmale zu umgehen, um Zugriff auf das System zu erhalten.

**Ergebnisse:**

* **Analyse** des Sicherheitsniveaus
* **Auffinden** von **Sicherheitslücken**
* **Dokumentation und Beschreibung** der gefundenen Sicherheitslücken sowie der möglichen Angriffsszenarien
* **Empfehlung von Maßnahmen** zur Mitigation oder zum Schließen der Sicherheitslücken

Die Durchführung des Penetrationstests erfolgt in den folgenden Phasen:

**Phase 1: Vorbereitung**

Das Ziel der Vorbereitungsphase ist die Festlegung des Umfangs, der Rahmenbedingungen und des Vorgehens beim Penetrationstest. Folgende Punkte sind hierbei zu berücksichtigen:

* Erläuterung der Testrisiken und Planung von Notfallmaßnahmen
* Auswahl und Erstellung von Testfällen

**Phase 2: Durchführung aktiver Angriffsversuche**

Mit Hilfe eines Schwachstellenscanners werden die Systeme/Anwendungen auf bekannte Schwachstellen untersucht.

Zudem erfolgt die Durchführung von aktiven Angriffsversuchen, indem manuelle Tests basierend auf ausgewählten Testfällen ausgeführt werden. Aus den Ergebnissen des durchgeführten Schwachstellenscans können weitere Angriffsvektoren resultieren, die in manuellen Tests untersucht werden.

**Phase 3: Bewertung der Informationen**

In der letzten Phase des Penetrationstests werden die Ergebnisse bewertet und geeignete Maßnahmen zum Schließen der gefundenen Schwachstellen erarbeitet. Folgende Tätigkeiten werden hierbei durchgeführt:

* Durchführung einer Risikoanalyse und erste Einschätzung des Sicherheitsniveaus
* Definition von geeigneten Maßnahmen zum Schließen oder zur Mitigation der gefundenen Schwachstellen

Im Falle des Blackbox-Penetrationstests übergibt der Auftraggeber lediglich die notwendigsten Informationen (z. B. nur eine IP-Adresse bzw. URL) an den Auftragnehmer. Der Auftragnehmer versucht weitere Informationen mittels passiver Informationsbeschaffung, Portscans etc. aufzubauen. Diese Art von Tests wird angewandt, um die Möglichkeiten eines externen Angreifers möglichst realistisch nachzustellen. Auch die Überprüfung der Funktionsweise von installierten IDS/IPS-Systemen sowie das Reaktionsverhalten und -Geschwindigkeit der eigenen Mitarbeiter kann ein Teilziel eines Black-Box-Tests darstellen.

Es wird davon ausgegangen das ein Angreifer über potentiell unendliche Zeitmittel verfügt. Da dies ein einem Testszenario nicht möglich ist endet der Test nicht nach Erreichen eines bestimmten Testziels, sondern mit Ablauf des Testzeitraumes. Der angebotene Test endet daher nach 4 Werktagen und die Ergebnisse werden in einem Abschlussbericht aufbereitet und ggf. Maßnahmen abgeleitet.

### Testschwerpunkte

Bei einem Blackbox-Test liegen keine detaillierten Informationen zum zu testenden System vor. Fokus des Tests ist die Klärung der Frage: „Was ist für einen Angreifer von außen sichtbar?" Der Test umfasst deshalb u. a. den Scan mit einem Vulnerability Scanner. Aufbauend auf diesen Ergebnissen erfolgen weiterführende manuelle Tests.

Testschwerpunkte sind dabei:

* Bestimmung der Netzwerktopologie
* Durchführung eines Portscans
* Prüfung der Erreichbarkeit von Systemen und Diensten
* Test der Möglichkeiten zur Umgehung von Sicherheitssystemen (z. B. Firewall)
* Test der Möglichkeiten zum nicht autorisierten Zugriff auf Anwendungen und Infrastruktur

Die Ergebnisse werden entsprechend in einem Abschlußbericht aufbereitet und ggf. Maßnahmen abgeleitet. Die Ergebnisse werden mit dem Auftraggeber telefonisch ausgewertet.

## Lieferumfang

Die Erstellung des unter Kapitel 3.1 beschriebenen Werkes beinhaltet den nachfolgend beschriebenen Liefergegenstand:

* Abschlussbericht über den durchgeführten Blackbox-Penetrationstest

Darüber hinausgehende Details werden zu Projektbeginn zwischen dem Auftraggeber und dem Auftragnehmer einvernehmlich schriftlich festgelegt.

## Leistungsabgrenzung

Folgende Leistungen sind insbesondere nicht im Angebot inbegriffen:

* Test von weiteren, nicht genannten Systemen und Anwendungen
* Koordinierung und Recherche von Verantwortlichkeiten
* Maßnahmencontrolling / Koordinierung der Maßnahmenumsetzung
* Behebung der Schwachstellen oder Optimierung von Sicherheitsmaßnahmen
* Tiefergehende Ausnutzung der Schwachstellen und Exploitation
* Rechtsberatung insbesondere auf dem Gebiet von Datenschutz- und Datensicherheit

## Mitwirkung des Auftraggebers

Die Mitwirkungspflichten stellen Hauptleistungspflichten des Vertrages dar.

Grundlagen der Tests sind folgende Dokumente und technische Voraussetzungen, welche seitens des Auftraggebers rechtzeitig zur Verfügung zu stellen sind:

### Abstimmungsleistungen

Der Auftraggeber steht für Fragen, die während der Durchführung des Penetrationstests anfallen, zur Verfügung.

### Zuarbeitungsleistungen Penetrationstest

Die Information über die zu analysierende Umgebung ist Grundlage für die Durchführung des Penetrationstests sowie die Bewertung der Maßnahmenumsetzung. Grundlage hierfür sind folgende Informationen, welche seitens des Auftraggebers rechtzeitig zur Verfügung zu stellen sind:

* URL und IP-Adresse
* Liste Ansprechpartner zu Organisations- und Betriebsfragen im Kontext der Testdurchführung
* Bereitstellung eines Testfensters zur Testdurchführung
* Firewallfreischaltung zu eventueller Testumgebung (falls erforderlich)
* Informationen über Durchführung Penetrationstet an Drittparteien (wie z. B. Hoster)
* Bereitstellung eines Arbeitsplatzes (falls Vor-Ort Test notwendig ist)

Für diese Tätigkeiten anfallende Kosten sind vom Auftraggeber zu tragen.

Werden die Mitwirkungsleistungen nicht termingerecht erbracht, kann das zu Verzögerungen bei der Leistungserbringung oder zu Einschränkungen im Leistungsumfang führen, die der Auftragnehmer nicht zu vertreten hat.

# Projektabwicklung

## Zeitplanung

Vertragsbeginn: nach Beauftragung

Testbeginn: nach Beauftragung und Vereinbarung

Lieferung Abschlussbericht 1 Woche nach Testbeginn

Vertragsende: 1 Monat nach Testbeginn

Die detaillierte Zeitplanung wird zu Projektbeginn zwischen dem Auftraggeber und dem Auftragnehmer einvernehmlich festgelegt.

Die Termine gelten vorbehaltlich der vollständigen, sachlich richtigen und termingerechten Erfüllung der unter Kapitel 3.4 aufgeführten Mitwirkungspflichten.

## Ort der Leistungserbringung

Der Ort der Leistungserbringung ist Dresden.

## Abnahme

Dem Auftraggeber wird der Abschlussbericht des Penetrationstests zur Abnahme vorgelegt. Der Auftraggeber unterzeichnet nach Bereitstellung des Werkes zur Abnahme ein Abnahmeprotokoll.

Das Abnahmeprotokoll bestätigt die angeforderten, angebotenen und in Rechnung zu stellenden Leistungen und setzt die Verjährungsfrist für Sach- und Rechtsmängel in Gang.

## Abnahmefrist

Die Abnahmefrist beträgt 14 Kalendertage und beginnt mit dem Zeitpunkt der Zusendung des vollständigen Lieferumfangs durch den Auftragnehmer.

Eventuelle Mängel sind dem Auftragnehmer unverzüglich schriftlich anzuzeigen. Festgestellte Mängel sind zu beschreiben und die Gründe einer etwaigen Abnahmeverweigerung aufzuführen.

Erfolgt innerhalb der angegebenen Frist weder eine Mängelanzeige, noch eine schriftliche Abnahme der Leistung durch den Auftraggeber, so gilt die Leistung als abgenommen.

# Preise und Konditionen

## Preise

Der Angebotspreis für die Durchführung des Blackbox-Penetrationstests gemäß Kapitel 3.1 beträgt 4.248,00 €.

### Preisklausel

Alle Preise dieses Angebotes sind in Euro angegeben und verstehen sich zuzüglich der zum Zeitpunkt der Lieferung und Leistung gesetzlich gültigen Mehrwertsteuer.

### Rechnungslegung

Die Leistungen werden nach der Abnahme anhand des vom Auftraggeber unterzeichneten Abnahmeprotokolls in Rechnung gestellt.

### Reisekosten

Die oben genannten Preise verstehen sich exklusive Reisekosten. Anfallende Reisen werden nach Aufwand zusätzlich in Rechnung gestellt. Reisezeiten werden zum Stundensatz i. H. v. 60,00 € / h abgerechnet.

Aktuell geht die Telekom Deutschland davon aus, dass keine Reisekosten für die Durchführung des Penetrationstests anfallen werden.

# Ergänzende Bedingungen

## Gültigkeitsdauer

Die Angaben in diesem Angebot sind unter dem Vorbehalt der Regelung in Ziffer 6 bis zum abldattoken gültig.

## Rechtliche Bedingungen

Es gelten die Vertragsbestandteile in nachstehender Reihenfolge:

1. Dieses Angebot mit seinen Anlagen
2. Allgemeinen Geschäftsbedingungen Werk- und Dienstleistungen der Telekom Deutschland GmbH vom 21.08.2017

Diese sind Bestandteil dieses Angebotes und als Anlage beigefügt.

Bei Widersprüchen zwischen Regelungen dieses Angebotes und Regelungen der genannten Allgemeinen Geschäftsbedingungen haben die Regelungen dieses Angebotes Vorrang.

## Garantieausschluss

Die Telekom Deutschland übernimmt keine Garantie für eine bestimmte Eigenschaft der Leistung. Technische Daten, Spezifikationen und Leistungsangaben in diesem Angebot und den dazugehörigen Dokumenten dienen alleine der Leistungsbeschreibung. Etwaige Herstellergarantien werden nicht von der Telekom Deutschland übernommen.

## Haftung

Die Parteien haben darüber Einvernehmen erzielt, dass der Auftragnehmer für von ihm fahrlässig verursachte Sach- und sonstige Schäden gleich aus welchem Rechtsgrund wie folgt haftet:

* Bei Vereinbarung einer Einmalvergütung ist die Haftung bei Sach- und sonstigen Schäden dabei auf 10% des Netto-Auftragsvolumens pro Schadensereignis begrenzt.
* Bei Vereinbarung einer wiederkehrenden Vergütung ist die Haftung bei Sach- und sonstige Schäden dabei auf 10% des Netto-Jahresentgelts pro Schadensereignis begrenzt.
* Der Auftragnehmer haftet für alle Schäden aus diesem Vertragsverhältnis bis zu einem Höchstbetrag von 50% des Netto-Auftragsvolumens.

Der Auftragnehmer haftet nicht für Produktionsausfall, Betriebsunterbrechung und entgangenen Gewinn, Verlust von Informationen und Daten sowie sonstige entfernte Mangelfolgeschäden. Weitergehende Schadensersatzansprüche, gleich aus welchem Rechtsgrund, sind ausgeschlossen, soweit nicht wegen Vorsatzes zwingend gehaftet wird.

Soweit die Haftung nach diesen Bedingungen ausgeschlossen ist, gilt dies auch für die persönliche Haftung der Organe des Auftragnehmers, der Angestellten, Arbeitnehmer, Mitarbeiter, Vertreter und Unterauftragnehmer des Auftragnehmers.

Die benannten Haftungsbegrenzungen gelten nicht bei Schäden auf Grund Verletzung von Leben, Körper und Gesundheit.

Sämtliche vertraglichen Schadensersatzansprüche verjähren mit Ablauf eines Jahres nach Beginn der gesetzlichen Verjährungsfrist.

## Haftungsausschluss

Nachfolgende Einflüsse, deren Ursache außerhalb des Zuständigkeitsbereichs des Auftragnehmers liegen, sowie die nachfolgenden Zustände, führen zeitlich begrenzt und nur für den zutreffenden Fall zum Haftungsausschluss bzw. stellen keine Vertragspflichtverletzung des Auftragnehmers dar:

* zum Zeitpunkt der Datenerfassung keine Onlinequellen bzw. zu erfassende Daten zur Verfügung stehen
* Höhere Gewalt einschließlich Krieg, Bürgerkrieg, Streik, Aussperrung, Katastrophen,
* Störungen durch Fehler in der Kundenapplikation bzw. zugehöriger Softwarekomponenten,
* Störungen durch unsachgemäße Eingriffe des Auftraggebers bzw. eines vom Auftraggeber autorisierten Dritten,
* Ausfälle im Internet und dessen Zugängen, die durch Viren, Würmer o. ä. Angriffe verursacht werden, insbesondere auch die Zeiten die zur Beseitigung dieser Angriffe notwendig sind,
* Nichtverfügbarkeiten aufgrund von angekündigten Wartungsarbeiten in den vereinbarten Wartungsfenstern gelten nicht als Einschränkung der Verfügbarkeit und nicht als Ausfallzeit,
* Störungen in Einrichtungen der Telekommunikationsversorger, der Energieversorger oder der vom Auftraggeber beigestellten Komponenten,
* Störungen durch ein nicht abgenommenes System (nicht in den Regelbetrieb überführt).

## Nutzungsrechte

Die Telekom Deutschland räumt dem Auftraggeber für individuell erstellte Teile nach vollständiger Bezahlung der vertraglich geschuldeten Gesamtvergütung ein nicht ausschließliches, zeitlich unbegrenztes, nicht übertragbares Nutzungsrecht auf die vertragliche Leistung ein.

## Datenschutz

Verarbeitet der Auftragnehmer personenbezogene Daten für den Auftraggeber, so verpflichten sich Auftraggeber und Auftragnehmer zum Abschluss einer Vereinbarung zur Verarbeitung personenbezogener Daten.

## Vertraulichkeit

Dieses Angebot enthält vertrauliche Informationen von uns und wird unter der Voraussetzung unterbreitet, dass es weder ganz noch teilweise in irgendeiner Form verwendet oder Dritten zugänglich gemacht wird, außer den Mitarbeitern und professionellen Beratern des Auftraggebers zum Zweck der Bewertung dieses Angebotes oder zu einem anderen Zweck, sofern dies vorab schriftlich von uns genehmigt wurde.

# Ansprechpartner

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ansprechpartner | Funktion | E-Mail | | Telefon |
| acmtoken | Account Manager | acmmailtoken | acmtnrtoken | |
|  | Solution Sales Manager Security |  |  | |
|  | Projektleitung T-Systems MMS |  |  | |

Telekom Deutschland GmbH

aortschafttoken

|  |  |  |  |
| --- | --- | --- | --- |
| Name: | acmtoken | Name: | i.A. |
| Funktion: | Account Manager | Funktion: |  |
| Ort: | aortschafttoken | Ort: |  |
| Datum: | angebotsdatoken | Datum: |  |
| Unterschrift: |  | Unterschrift: |  |

# Auftragserteilung

|  |  |
| --- | --- |
|  |  |

firmatoken

fanschrifttoken

fortschafttoken

|  |  |
| --- | --- |
| Angebotstitel | Penetrationstest Blackbox |
| Angebotsnummer | angebotsnumtoken |

Wir erteilen hiermit den Auftrag gemäß dem o.g. Angebot.

Die für diesen Auftrag geltenden Allgemeinen Geschäftsbedingungen Werk - und Dienstleistungen der Telekom Deutschland GmbH haben wir zur Kenntnis genommen.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_