

Leistungsbeschreibung (Anlage 1)

Aktenzeichen: 2026-0068

Beratung zur internen IT-Sicherheit im vzbv

27. Mai 2026

Inhalt

I. Vorbemerkung	3
II. Zielsetzung und Aufgabenstellung	3
III. Regelungen zum Personaleinsatz seitens des AN	4
IV. Beschreibung der erbringenden Leistung	4
1. Beratung beim Aufbau einer Informationssicherheitsorganisation und eines Informationssicherheitsmanagementsystems (ISMS) gemäß BSI-Grundschutzstandards.....	4
1.1 Einarbeitung	4
1.2 Beratung bei der Erstellung einer Sicherheitskonzeption	5
2. Daueraufgaben	5
V. Kostenkalkulation	6
VI. Anforderung an das Angebot	6
1. Anforderungen im Rahmen der Zuschlagskriterien	6
1.1 Kurzkonzept zu Abschnitt IV. Punkt 1	7
1.2 Nachweis fachlicher Eignung	7
VII. Service Level Agreement	8
1. Verfügbarkeit	8
2. Definition Störung	8
2.1 Serviceanfragen	8
2.2 Reaktionszeiten	9
2.3 Wiederherstellungszeiten	9
VIII. Zeitplan	9

I. Vorbemerkung

Der Verbraucherzentrale Bundesverband (vzbv) bündelt als Dachverband die Expertise von 16 Verbraucherzentralen und mehr als 30 verbraucherpolitischen Verbänden - darunter über 2.000 Organisationen und sieben Millionen Einzelmitglieder - für einen starken Schutz der Verbraucher:innen in Deutschland. Der vzbv ist die Stimme der Verbraucher:innen – und damit eine entscheidende Kraft in der Politik. Wir wissen, was Verbraucher:innen bewegt und verschaffen ihnen Gehör bei Politik, Wirtschaft und Verwaltung. Strukturelle Missstände decken wir auf, benennen Verbraucherprobleme und entwickeln Lösungen. So tragen wir dazu bei, dass Märkte transparent und gerecht gestaltet werden.

II. Zielsetzung und Aufgabenstellung

Gegenstand des Verfahrens ist die Beauftragung eines externen Dienstleisters für die fachliche Beratung und Unterstützung im Bedarfsfall im Bereich der IT-Sicherheit beim Verbraucherzentrale Bundesverband e.V. (vzbv) ab dem 1. September 2026.

Der vzbv als Auftraggeber (AG) verfügt über eine interne IT-Sicherheitsbeauftragte (IT-SiBe). Der Auftragnehmer (AN) übernimmt somit nicht die Funktion einer/einem IT-SiBe, sondern berät im Bedarfsfall die interne IT-SiBe fachlich bei der Weiterentwicklung, Koordination und Umsetzung der IT-Sicherheitsmaßnahmen.

Die interne IT-SiBe ist im vzbv erste Ansprechpartnerin für alle Fragen und Vorfälle der IT-Sicherheit und gewährleistet den notwendigen Informationsaustausch mit dem externen Auftragnehmer.

Der Auftragnehmer fungiert als externer Ansprechpartner und Berater und arbeitet bei Bedarf eng mit der internen IT-SiBe sowie der zuständigen IT-Abteilung zusammen.

Die Leistungen umfassen im Bedarfsfall insbesondere die fachliche Beratung bei der Weiterentwicklung des Informationssicherheitsmanagementsystems (ISMS), die Bewertung des Sicherheitsniveaus sowie die Begleitung sicherheitsrelevanter Projekte und fundierte Beratung bei Sicherheitsvorfällen.

Darüber hinaus stellt der Auftragnehmer sicher, dass bei Bedarf weiterführende Sicherheitsleistungen aus seinem Unternehmen oder über qualifizierte Partner bereitgestellt werden können, insbesondere Penetrationstests, Schwachstellenmanagement sowie bei der Analyse und Behandlung von Sicherheitsvorfällen (Incident Response), die separat abgerechnet werden.

Zu Beginn der Zusammenarbeit berät der Auftragnehmer die interne IT-SiBe bei der Bewertung des aktuellen Sicherheitsniveaus und bei der Identifikation möglicher Verbesserungsmaßnahmen.

Unter Beachtung der im Einzelnen durchzuführenden Aufgaben wird von einem maximal benötigten Kontingent pro Vertragsjahr von 18 Arbeitstage (AT) à 8 Stunden (= 1,5 AT / Monat) ausgegangen. Die 1,5 AT stellen einen Durchschnittswert für jeden Monat des jeweiligen Kalenderjahres dar. Es besteht kein Anspruch auf Abruf des gesamten Kontingents. Das nicht verbrauchte Kontingent kann in Absprache zwischen AG und AN in das Folgejahr übertragen werden. Der Übertrag über die maximale Vertragslaufzeit ist nicht möglich. Die Abrechnungsmodalitäten sind im Vertrag geregelt.

III. Regelungen zum Personaleinsatz seitens des AN

Es wird erwartet, dass der AN (oder im Falle seiner Verhinderung seine Stellvertretung) dem AG zu festen Zeiten auf regelmäßiger zu vereinbarender Basis (Jour Fixe), mindestens jedoch an einem Termin pro laufenden Kalendermonat, zur Besprechung von Fragestellungen zur Verfügung steht. Besprechungen finden in der Regel digital als TEAMS-Meeting statt. Von Seiten des AG wird dem AN eine Person als Ansprechpartner:in auf fachlicher Ebene und eine Stellvertretung benannt.

Der AN stellt eine angemessene Erreichbarkeit für sicherheitsrelevante Fragestellungen und IT-Sicherheitsvorfälle sicher. Reaktionszeiten werden im Rahmen einer Service Level Vereinbarung (SLA) festgelegt.

Sollte der vom AN benannte Ansprechpartner:in langfristig nicht zur Verfügung stehen oder das Unternehmen verlassen, so hat der AN unverzüglich eine fachlich gleichwertig qualifizierte Ersatzperson zu benennen. Der Wechsel bedarf der vorherigen Zustimmung des AG. Die Qualifikation ist dem AG nachzuweisen.

IV. Beschreibung der erbringenden Leistung

1. Beratung beim Aufbau einer Informationssicherheitsorganisation und eines Informationssicherheitsmanagementsystems (ISMS) gemäß BSI-Grundschutzstandards

1.1 Einarbeitung

Für den Einstieg in die Tätigkeit wird mit einer Einarbeitung gerechnet, in der die interne IT-SiBe und bei Bedarf der Leiter-IT den AN in die wesentlichen Begebenheiten einführen. Dazu gehören u.a. Briefing-Gespräche zum Kennenlernen infrastruktureller Besonderheiten im vzbv und zum Stand der Umsetzung IT-Sicherheit. Die Einarbeitungsphase beinhaltet:

- Einsicht in bisherige Dokumentationen der IT-SiBe
- Einsicht in die Dokumentation der IT-Infrastruktur
- Einsicht in die interne Projektplanung „digitale Transformation“
- Prüfung der vorliegenden Dokumente und Erarbeitung von ersten Verbesserungsvorschlägen

1.2 Beratung bei der Erstellung einer Sicherheitskonzeption

Die Erstellung einer Sicherheitskonzeption muss mindestens mit einer Basis-Absicherung nach BSI-IT-Grundschutz erfolgen und soll bis Ende 2026 abgeschlossen sein.

- Beratung bei der Organisation des Sicherheitsprozesses:
 - Überprüfung der Sicherheitsziele
 - Beratung beim Aufbau der Sicherheitsorganisation
 - Beratung bei der Integration in bestehende Abläufe und Prozesse
 - Beratung bei der der Konzeption und Planung des Sicherheitsprozesses
 - Überprüfung der bestehenden Leitlinie und Richtlinie auf Aktualität und Vollständigkeit
- Beratung bei der Identifikation, Konzeption und Erstellung erforderlicher ergänzender Vorgabedokumenten (z.B. Betriebshandbuch, Notfallhandbuch) sowie Fortschreibung fehlender Richtlinien und Leitlinien:
 - Beratung bei der Durchführung des Sicherheitsprozesses
 - Strukturanalyse
 - Schutzbedarfsfeststellung
 - Modellierung (Ist- und Soll-Zustand ermitteln)
 - IT-Grundschutz-Checks
 - Ableitung und Priorisierung von Maßnahmen in Abstimmung mit dem jeweils zuständigen Serviceverantwortlichen
- Beratung beim Realisierungsplan (Kosten- und Aufwandsabschätzung für die Realisierung von Maßnahmen, Ersatzmaßnahmen, Restrisiko, Umsetzungsreihenfolge, Verantwortlichkeiten, Ressourcenplanung)
- Empfehlungen zur Weiterentwicklung des Sicherheitsniveaus

2. Daueraufgaben

Der AN berät bei Bedarf die interne IT-SiBe bei laufenden Aufgaben der IT-Sicherheit und im Rahmen des vereinbarten Kontigents.

- Zusammenarbeit:
 - Ansprechpartner:in für die interne IT-SiBe bei allen Fragen und Vorfällen in der IT-Sicherheit
 - Unterstützung bei der Begleitung von sicherheitsrelevanten Projekten, die deutliche Auswirkungen auf die IT-Sicherheit haben
 - Untersuchung und Dokumentation von Sicherheitsvorfällen
 - Incident Response bei Bedarf
- Bei Bedarf Beratung bei der Steuerung und Koordination des Informationssicherheitsprozesses:
 - hinsichtlich der Weiterentwicklung der Informationssicherheitsorganisation und des ISMS
 - bezüglich der Aufrechterhaltung und Verbesserung der IT-Sicherheit

Leistungsbeschreibung

(Anlage 1) AZ: 2026-0068

- Bei Bedarf Beratung bei der Erarbeitung von Konzepten und Richtlinien:
 - Weiterentwicklung des IT-Sicherheitskonzepts für den laufenden Betrieb
 - Erstellung eines Sicherheitskonzepts
 - Erstellung eines Notfallvorsorgekonzepts
 - Erarbeitung von notwendigen Richtlinien und Regelungen zur IT-Sicherheit entsprechend der Organisationsstruktur
- Bei Bedarf Unterstützung bei der Mitarbeitersensibilisierung:
 - Planung von Schulungs- und Informationsmaßnahmen
 - Planung von Sensibilisierungsmaßnahmen
- Bei Bedarf IT-Unterstützung:
 - Beantwortung von Fragen zu bestehenden IT-Systemen und deren Sicherheitskompatibilität

V. Kostenkalkulation

Bitte kalkulieren Sie Kosten für die Umsetzung der oben genannten Maßnahmen wie folgt:

1. Kalkulieren Sie bitte einen Paketpreis für die unter Abschnitt IV - Beschreibung der erbringenden Leistungen - dargelegten Aufgaben unter Punkt 1. - Beratung beim Aufbau einer Informationssicherheitsorganisation und eines Informationssicherheitsmanagementsystems (ISMS) gemäß BSI-Grundschutzstandards
2. Kalkulieren Sie bitte einen Stundenpreis/ Kosten je Arbeitsstunde für die unter Abschnitt IV - Beschreibung der erbringenden Leistungen - dargelegten Daueraufgaben unter Punkt 2.
3. Abgerechnet werden dürfen ausschließlich Stunden, die durch konkrete Leistungen und Ergebnisse nachweisbar sind. Zeiten ohne nachweisbare Leistungserbringung sind nicht abrechnungsfähig.
4. Zusätzliche sicherheitsrelevante Leistungen wie z.B. Penetrationstests oder spezielle Sicherheitsanalysen können bei Bedarf gesondert beauftragt werden. Es besteht jedoch kein Anspruch auf Beauftragung.

VI. Anforderung an das Angebot

Das Angebot ist vollständig, nachvollziehbar und in deutscher Sprache einzureichen. Die nachfolgenden Anforderungen sind zwingend zu erfüllen. Unvollständige oder nicht aussagekräftige Angebote können vom weiteren Verfahren ausgeschlossen werden.

1. Anforderungen im Rahmen der Zuschlagskriterien

1.1 Kurzkonzept zu Abschnitt IV. Punkt 1

Mit dem Angebot ist ein Kurzkonzept für die in Abschnitt IV - Beschreibung der zu erbringenden Leistungen - dargelegte Aufgabe unter Punkt 1. - Beratung beim Aufbau einer Informationssicherheitsorganisation und eines Informationssicherheitsmanagementsystems (ISMS) gemäß BSI-Grundsatzstandards - einzureichen. Es soll dargelegt werden, wie der Auftragnehmer die interne IT-SiBe bei der Bewertung des aktuellen Sicherheitsniveaus und bei der Identifikation möglicher Verbesserungsmaßnahmen beraten wird. Das Kurzkonzept muss folgende Inhalte darstellen:

- methodisches Vorgehen
- geplante Einbindung der internen IT-SiBe
- grobe Zeit- und Meilensteinplanung bis zum Abschluss der Aufgabe im Dezember 2026

Der Umfang des Kurzkonzepts darf vier DIN-A4-Seiten, Schriftgröße 12, Aptos oder vergleichbare Schrift wie Arial nicht überschreiten.

Mit dem Angebot ist zusätzlich der Prozess darzulegen, wie der Auftragnehmer bei Sicherheitsvorfällen beim Auftragnehmer vorgeht und wie er zu erreichen ist.

1.2 Nachweis fachlicher Eignung

Das auftragsnehmende Unternehmen muss praktische Erfahrungen im Aufbau, Betrieb und der Weiterentwicklung von ISMS nach BSI-Grundsatz oder ISO27001 nachweisen können.

Das Angebot muss nachweisbare Erfahrungen des/r vorgesehenen Berater/ in und der Stellvertretung im Bereich der IT-Sicherheit enthalten, insbesondere sind Erfahrungen in der Beratung im Bereich ISMS nachzuweisen.

Mit dem Angebot ist der für den Auftrag vorgesehene Berater: in und dessen Stellvertretung namentlich zu benennen. Für diese Personen sind ein je Lebenslauf sowie jeweils Nachweise über Qualifikationen, Zertifizierungen und die einschlägige Berufserfahrung einzureichen. Deutsche und englische Sprachkompetenz werden vorausgesetzt.

Die zwei benannten Personen müssen über Berufserfahrung im Bereich der Informationssicherheit verfügen, insbesondere sind für jede der beiden Personen praktische Erfahrungen nachzuweisen in:

- Aufbau oder Betreuung eines ISMS nach ISO 27001 oder BSI -Grundsatz
- Umsetzung des BSI-Grundsatzes
- Durchführung von Risikoanalysen (nach ISO-27005 oder BSI-Methodik)
- Erstellung und Pflege von Richtlinien & Sicherheitskonzepten
- Behandlung von Sicherheitsvorfällen / Incident Response
- Grundlegendes Verständnis IT-Architekturen, Netzwerken oder Cloud-Umgebungen (gewünscht)
- Grundkenntnisse im Schwachstellenmanagement (gewünscht)

Es sind drei überprüfbare Referenzen mit vergleichbarer Aufgabenstellung (mit Angabe zur Art der ausgeführten Arbeiten, Auftragsvolumen/Rechnungswert, Leistungszeit und Auftraggeber) vorzulegen, die von dem/r für den Auftrag vorgesehene/n Berater: in durchgeführt wurden. Die

Referenzen müssen aus laufenden oder abgeschlossenen Projekten stammen. Im Falle von abgelaufenen Projekten, dürfen diese nicht vor dem Jahr 2022 abgeschlossen worden sein.

Die zwei benannten Personen erbringen die Leistungen selbst. Ein Wechsel ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zulässig. Studierende, Praktikanten oder andere nicht gleichwertig qualifizierte Personen dürfen nicht als Ersatz eingesetzt werden.

VII. Service Level Agreement

1. Verfügbarkeit

Der AG erwartet und fordert eine Verfügbarkeit des Dienstes **werktags** (Montag – Freitag) von **08:00 – 17:00 Uhr**.

Für kritische Störungen ist die Annahme von Störungsmeldungen **P1** und **P2** auch außerhalb der Servicezeiten sicherzustellen.

2. Definition Störung

Die Klassifizierung der Störungen wird wie folgt eingestuft:

- **Kritisch (P1)**

Sicherheitsvorfall mit erheblichem Risiko z.B Angriff, Datenabfluss, Systemausfall, Malwareinfektion etc.

- **Hoch (P2)**

Betriebsbehinderte Störung mit erheblichen Einschränkungen

- **Mittel (P3)**

eingeschränkte Funktionalität ohne kritische Einschränkungen

- **Niedrig (P4)**

geringfügige Störung ohne wesentliche Auswirkungen

2.1 Serviceanfragen

Serviceanfragen sind keine Störungen im Sinne dieses Service Level Agreements. Dazu zählen insbesondere allgemeine Anfragen zur IT-Sicherheit, Beratungsleistungen sowie Unterstützungs- oder Änderungswünsche ohne direkte Störungsbezug.

Die Bearbeitung erfolgt innerhalb der vereinbarten Servicezeiten und wird in Abstimmung mit dem Auftraggeber priorisiert.

Für Serviceanfragen gelten keine festen Reaktions- oder Wiederherstellungszeiten wie bei Störungen. Bei Bedarf können jedoch individuelle Bearbeitungszeiten vereinbart werden.

2.2 Reaktionszeiten

- Die Reaktionszeit der Stufe „**kritisch (P1)** Kritisch- Sicherheitsvorfall“ beträgt **30 Minuten** innerhalb der vereinbarten Servicezeiten nach Eingang der Störungsmeldung beim AN. Stellt der AG einen Kritisch- Sicherheitsvorfall fest, muss die Möglichkeit bestehen, diesen Fehler per Direktanruf einer kostenfreien Helpdesk Nummer zu melden. Das daraus folgende Ticket muss der Kategorie „Kritisch“ (oder vergleichbar) zugewiesen werden.
- Die Reaktionszeit der Stufe „**Hoch (P2)** Hoch-Störung“ beträgt **1 Stunde** innerhalb der vereinbarten Servicezeiten nach Eingang der Störungsmeldung beim AN. Stellt der AG einen „Hoch- Störung“ fest, muss die Möglichkeit bestehen, diesen Fehler per Direktanruf einer kostenfreien Helpdesk Nummer zu melden. Kostenfrei bedeutet hier, dass die Kosten für den Anruf der Servicehotline, die Kosten für einen Standardanruf in das deutsche Festnetz nicht überschreiten dürfen. Das daraus folgende Ticket muss der Kategorie „Hoch“ (oder vergleichbar) zugewiesen werden.
- Die Reaktionszeit der Stufe „**Mittel (P3)**“ beträgt **4 Stunden** innerhalb der vereinbarten Servicezeiten.
- Die Reaktionszeit der Stufe „**Niedrig (P4)**“ beträgt **1 Arbeitstag** innerhalb der vereinbarten Servicezeiten.

Die Meldung eines ersten Zwischenergebnisses erfolgt innerhalb von **60 Minuten** nach Störungsmeldung telefonisch und per E-Mail an eine vom AG noch zu benennende, zentrale Rufnummer und E-Mail-Adresse.

2.3 Wiederherstellungszeiten

Eine auftretende Störung ist gemäß den Mängelklassen wie folgt zu beseitigen:

- **Kritische Störungen (P1)** sind innerhalb von **8 Stunden** zu beheben oder durch geeignete Maßnahmen so zu stabilisieren, dass der Betrieb schnellstmöglich wieder hergestellt werden kann.
- **Betriebsverhindernde Störung (P2)** sind innerhalb von **2 Arbeitstagen** zu beheben.
- **Störungen mittlere Priorität (P3)** sind innerhalb von **3 Arbeitstagen** zu beheben.
- **Geringfügige Störungen(P4)** sind innerhalb von **5 Arbeitstagen** zu beheben.

Werden die vereinbarten Reaktions- und Wiederherstellungszeiten nicht eingehalten, erfolgt eine Eskalation an die benannten Ansprechpartner des Auftragnehmers.

VIII. Zeitplan

Der Beginn der beratenden Tätigkeit, zur IT-Sicherheit im vzbv, durch den AN, soll nach erfolgreicher Zuschlagserteilung, spätestens aber zum 1. September 2026, erfolgen; die Vertragslaufzeit ist auf vier Jahre befristet.

Leistungsbeschreibung

(Anlage 1) AZ: 2026-0068

Optional kann die Laufzeit durch den AG zweimal um je ein Jahr verlängert werden. Diese Option kann einseitig vom AG bis drei Monate vor Ende der Vertragslaufzeit schriftlich gezogen werden. Es besteht kein Anspruch des AN auf Wahrnehmung der Verlängerungsoption