NIS2 · KRITIS · VSVGV · IT-SIG 2.0

Cybersecurity im öffentlichen Sektor vergaberechtskonform beschaffen

Rechtsrahmen, VS-Stufen, Anforderungsstruktur und typische Fehler
für Behörden und KRITIS-Betreiber

30.000+	4	3	18 Mon.
NIS2-pflichtige Einrichtungen	VS-Stufen im deutschen Recht	Vergabewege UVgO / VgV / VSVgV	typischer Vorlauf VS-VERTRAULICH

it-leistungsverzeichnisse.de · Mai 2026 · Auftraggeber-Perspektive

Die doppelte Herausforderung

Behörden bewegen sich gleichzeitig in zwei regulatorischen Welten

VERGABERECHT

UVgO / VgV / VSVgV

Wettbewerb, Transparenz, Diskriminierungsverbot. Cybersecurity-Leistungen müssen ausgeschrieben werden, sobald Schwellenwerte überschritten werden. Produktneutrale Anforderungen, messbare Kriterien, dokumentierter Vergabevermerk.

- Vergabekammer prüft bei Rüge
- Bieterausschluss nur bei Verhältnismässigkeit

IT-SICHERHEITSRECHT

NIS2 / KRITIS / IT-SiG 2.0

Risikomanagementpflichten, Meldepflichten, Mindeststandards. Die konkret geforderten Massnahmen müssen nachweislich im Leistungsverzeichnis verankert werden. BSI-Mindeststandards sind für Bundesbehörden verbindlich.

- BSI prüft Umsetzungsnachweis
- Verstösse: Bussgelder bis 10 Mio. EUR

Rechtlicher Rahmen im Überblick

Vier Regelwerke, die Cybersecurity-Beschaffung direkt beeinflussen

IT-SIG 2.0 (2021)

IT-Sicherheitsgesetz 2.0

Erweitert KRITIS-Kreis, neue Meldepflichten, Unternehmen im besonderen öffentlichen Interesse (UBI) verpflichtet. Nachweis der Massnahmen im LV erforderlich.

NIS2UMSUCG (2024)

NIS2-Umsetzung

Ca. 30.000 Einrichtungen neu verpflichtet. Risikomanagementmassnahmen nach § 30 BSIG n.F. sind Pflicht. Umfasst viele Behörden und kommunale Unternehmen.

KRITIS-DACHG (2024)

Resilienzpflichten

Physische und digitale Resilienz für kritische Anlagen. Risikoanalysen und Abhilfemassnahmen dokumentationspflichtig. Cybersecurity-Beschaffung als Nachweisgrundlage.

BSI-MINDESTSTANDARDS

Technische Pflichten

Für Bundesbehörden verbindlich, faktisch massgeblich für alle. Cloud-Nutzung, Webdienste, Protokollierung: konkrete Anforderungen, direkt ins LV überführbar.

Aus unserer Erfahrung: Behörden, die den Rechtsrahmen frühzeitig als Anforderungsquelle nutzen, sparen später erheblichen Aufwand. NIS2-Pflichten erst nach Zuschlagserteilung nachzuverhandeln, ist vergaberechtlich problematisch.

VSVgV und VS-Stufen strategisch einsetzen

Die VS-Einstufung ist ein Steuerungsmittel, kein bürokratisches Etikett

VS-STUFE	BEDEUTUNG	GEHEIMSCHUTZ	ÜBERPRÜFUNG	VERGABE
VS-NfD	Nur für den Dienstgebrauch	Ressort-intern	Keine SÜG-Pflicht	UVgO / VgV
VS-VERTRAULICH	Staatliche Interessen gefährdet	BMWK verpflichtend	Ü1 (ca. 3 Mon.)	VSVgV
GEHEIM	Schwere Schäden möglich	BMWK + BfV	Ü2 (6-12 Mon.)	VSVgV
STRENG GEHEIM	Existenzbedrohende Schäden	Mehrere Behörden	Ü3 (ca. 12+ Mon.)	VSVgV

Strategisch: Eine höhere VS-Einstufung begrenzt den Bieterkreis auf Unternehmen mit BMWK-Geheimschutzbetreuung und sicherheitsüberprüftem Personal. Bei hochsensiblen Vorhaben ist das das Ziel. Der Vorlauf muss entsprechend geplant werden: erstmalige Geheimschutzbetreuung dauert 6-18 Monate.

Pflichtpositionen im Leistungsverzeichnis

Anforderungen nach Lösungstyp strukturieren, nicht nach Produktname

EDR / XDR
Endpunktschutz
Agent-Deployment auf 99 % aller Systeme, MITRE ATT&CK-Detektionsregeln, automatische Isolierung, SIEM-Integration

SIEM / Log-Management
Zentrale Protokollierung
Log-Sammlung aller Systeme, Speicherfrist min. 90 Tage, Korrelationsregeln, Alarmierung, DSGVO-konforme Speicherung

NDR
Netzwerkerkennung
Passive Netzwerkanalyse, laterale Bewegungen erkennen, OT/ICS-Protokolle, Retention der Flow-Daten

SOC-as-a-Service / MDR
Managed Detection
24/7-Überwachung, SLA Reaktionszeiten, Eskalationsprozess zur eigenen IT, Incident-Response-Berichte

Penetrationstest
Angriffssimulation
Scope-Definition, OSSTMM/PTES-Methodik, CVSS-Bewertung, Nachtest nach Behebung, Vertraulichkeitsvereinbarung

Schwachstellen-Management
Kontinuierliche Analyse
Asset-Discovery, Scan-Frequenz definiert, CVSS-Priorisierung, Patch-Tracking, Schnittstelle Ticketsystem

Sicherheitsüberprüfungen nach SÜG

Ü3

Mit Sicherheitsermittlungen

STRENG GEHEIM · ca. 12+ Monate

Alle Massnahmen aus Ü2 plus: Befragung mindestens einer Referenzperson und weiterer Auskunftspersonen, aktive Ermittlungen im persönlichen Umfeld. Auch bei hoher Anzahl GEHEIM-VS oder Nachrichtendiensten. Im zivilen IT-Bereich die Ausnahme.

Ü1

Einfache Überprüfung

VS-VERTRAULICH · ca. 3-6 Monate

Person selbst. Abfragen bei Verfassungsschutz, BKA, Bundespolizei, Bundeszentralregister, Staatsanwaltschaft, Gewerbezentralregister, Meldedaten. Seit SÜG-Novelle 2024 auch Social-Media-Recherche. Kein Einbezug des Umfelds.

Ü2

Erweiterte Überprüfung

GEHEIM · ca. 6-12 Monate

Alle Massnahmen aus Ü1 plus: Polizeidienststellen aller Wohnsitze der letzten 5 Jahre, Identitätsprüfung, Einbezug von Ehe-/Lebenspartnern. Keine Referenzbefragung. Bieter mit abgeschlossener Ü2 haben klaren Marktvorteil.

Im LV: Bieter erklären

nur die Bereitschaft zur Überprüfung, keine abgeschlossene Überprüfung ist Voraussetzung. Abgeschlossene Ü2/ Ü3 darf als Zuschlagskriterium gewertet werden. Einen höheren Grad als sachlich erforderlich zu fordern ist vergaberechtlich problematisch.

Typische Fehler bei Cybersecurity-Ausschreibungen

Diese sechs Fehler begegnen uns in der Praxis immer wieder

1

Zu allgemeine Anforderungen

"State-of-the-art-Schutz" ist nicht prüfbar. Anforderungen immer mit messbarem Kriterium verbinden.

2

Betriebskosten fehlen im Preisblatt

Lizenz-, Betriebs- und Wartungskosten müssen separat abgefragt werden, nicht nur Implementierung.

3

DSGVO-Anforderungen fehlen

SIEM und EDR verarbeiten personenbezogene Daten. AVV, EU-Rechenzentrum und Löschfristen ins LV.

4

Kein Proof of Concept vorgesehen

Ohne PoC oder Testphase kauft man die Katze im Sack. Technische Präsentation als Zuschlagskriterium ist zulässig.

5

Produktspezifische Anforderungen

Herstellernamen oder zu enge Spezifikationen verletzen das Wettbewerbsgebot. Immer "oder gleichwertig" ergänzen.

6

BSI-Meldepflichten nicht verankert

24h-Meldepflicht bei KRITIS/NIS2 muss vertraglich festgeschrieben sein, inklusive Fristen und Eskalationspfad.

Wie wir helfen

Von der Anforderungsstruktur bis zum Zuschlag

MUSTER-LEISTUNGSVERZEICHNISSE

Fertige LV-Vorlagen

EDR/XDR, SIEM, NDR und SOC-Leistungen als anpassbare Vorlage, direkt ausschreibungsreif.

/produkte/it-leistungsverzeichnis

VERGABE-ARCHIV

12.000+ Ausschreibungen

Reale IT-Sicherheitsausschreibungen mit Vergabeunterlagen als Referenz und Benchmarking.

/produkte/vergabe-archiv

IT-AUSSCHREIBUNGSBERATUNG

Begleitung von A bis Z

Von der Markterkundung über das LV bis zur Angebotswertung: unabhängige Beratung ohne Herstellerbindung.

/leistungen/ausschreibungsmanagement

Ihr Ansprechpartner
info@it-leistungsverzeichnisse.de · 06124 6059217