BSI OH-SZA V1.1 · KRITIS · IT-SIG 2.0

Systeme zur Angriffserkennung vergaberechtskonform ausschreiben

Alle 217 BSI-Anforderungen im Überblick, kritische Einschätzung zur Orientierungshilfe und Praxiserkenntnisse aus realen KRITIS-Vergabeprojekten.

217	129	6	Stufe 3
BSI-Anforderungen	MUSS-Anforderungen	Kategorien	gesetzliches Minimum

IT-Leistungsverzeichnis.DE | it-leistungsverzeichnis.de

Seit Mai 2023
gesetzlich verpflichtend

KRITIS-Betreiber müssen nach **§8a Abs. 1a BSIG** angemessene Systeme zur Angriffserkennung einsetzen und die Umsetzung gegenüber dem BSI alle zwei Jahre nachweisen.

Das BSI prüft dabei keine Produktlisten, sondern die tatsächliche Erkennungsfähigkeit der Organisation — dokumentiert anhand der 217 Anforderungen der OH-SzA v1.1.

Mit **NIS2** und dem **KRITIS-Dachgesetz** wird der Betreiberkreis erheblich ausgeweitet: Viele Unternehmen, die bisher nicht als KRITIS galten, werden vergleichbare Anforderungen erfüllen müssen.

IT-SiG 2.0 seit 2021 | SzA-Pflicht seit Mai 2023 | NIS2 in Umsetzung

§8A ABS. 1A BSIG — GESETZESPFLICHT

KRITIS-Betreiber sind verpflichtet, **Systeme zur Angriffserkennung** einzusetzen und die Umsetzung gegenüber dem BSI **alle zwei Jahre** nachzuweisen. Erstmals prüfbar seit 1. Mai 2023.

UMSETZUNGSGRADMODELL: 6 STUFEN (0–5)

Stufe 3 = gesetzliches Minimum: alle 129 MUSS-Anforderungen erfüllt.
Stufe 4 = nach erstem Prüfzyklus verpflichtend: zusätzlich relevante SOLL-Anforderungen.
Stufe 5 = vollständige Umsetzung inkl. aller KANN-Anforderungen.

AUSBLICK: NIS2 / KRITIS-DACHG

Erhebliche Ausweitung des Betreiberkreises auf weitere Sektoren und kleinere Unternehmen. Vergleichbare SzA-Melde- und Nachweispflichten gelten künftig für deutlich mehr Organisationen — auch unterhalb der bisherigen KRITIS-Schwellenwerte.

Was ist ein System zur Angriffserkennung?

Kein Produkt, das man kauft, sondern das Zusammenspiel dreier gleichrangiger Elemente. Das BSI prüft alle drei.

Werkzeuge

- SIEM, NDR, EDR zur Angriffserkennung
- Logsources: Netz, Endpoint, Cloud, OT
- Detektionsregeln nach MITRE ATT&CK
- Anomalieerkennung und Korrelation
- Speicherfristen und Normalisierung

Prozesse

- Dokumentierte Betriebsabläufe alle Phasen
- Alarmbearbeitung und Triage-Workflows
- Eskalationspfade und Meldeketten §8b
- Incident-Response-Playbooks
- Regelmäßige Revisionen und Tests

Spezialisten

- Qualifizierte Analysten (Tier 1/2/3)
- 24/7-Betrieb und Rufbereitschaft
- Threat-Intelligence-Kapazität
- Nachgewiesene Qualifikationen
- Klare Rollenverteilung IT/SOC/Security

Vergabe-Konsequenz: Das LV muss alle drei Dimensionen mit messbaren Kriterien abdecken. Wer nur Technologie ausschreibt, beschafft kein BSI-konformes SzA und riskiert ein negatives Prüfergebnis.

217 Anforderungen in 6 Kategorien

Die BSI Orientierungshilfe OH-SzA v1.1 (November 2024) strukturiert alle Anforderungen in drei Verbindlichkeitsstufen. Das LV muss darauf aufbauen:

MUSS: 129 | SOLL: 82 | KANN: 6

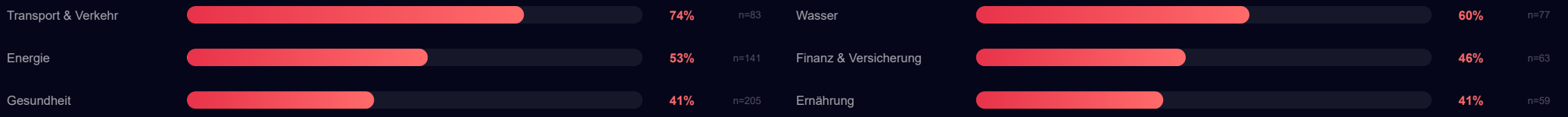
Stufe 3 (gesetzliches Minimum): alle 129 MUSS erfüllt.
Stufe 4 (nach erstem Prüfzyklus): zusätzlich relevante SOLL-Anforderungen.
Vergabe-Konsequenz: Ein LV, das nur Produkte benennt statt Anforderungen prüfbar zu formulieren, schafft keine Vertragsgrundlage für den BSI-Nachweis.

6 KATEGORIEN DER OH-SZA V1.1

Übergreifende Anforderungen Governance, Verantwortlichkeiten, Dokumentation	5 MUSS
Planung der Protokollierung Logsources, Speicherfristen, Datenschutz	26 MUSS · 24 SOLL
Umsetzung der Protokollierung Normalisierung, Vollständigkeit, Integrität	19 MUSS · 13 SOLL
Planung der Detektion Detektionsregeln, MITRE ATT&CK, Anomalieerkennung	24 MUSS · 18 SOLL
Umsetzung der Detektion Alarmqualität, False-Positive-Rate, Tuning	11 MUSS · 16 SOLL · 6 KANN
Reaktion Incident Response, Eskalation, Meldewege §8b	44 Anforderungen

Compliance-Stand nach Sektor — Stand 31.12.2025

Anteil KRITIS-Betreiber ohne BSI-Konformität (Umsetzungsgrad < Stufe 3) · Quelle: BSI KRITIS-in-Zahlen



Einordnung: Mehr als zwei Jahre nach der gesetzlichen Frist (1. Mai 2023) erfüllen in den meisten Sektoren 40 bis 74 Prozent der KRITIS-Betreiber die Mindestanforderungen nicht. Im Sektor Transport & Verkehr sind drei von vier Betreibern unterhalb Stufe 3. Stufe 3 ist kein Best-Practice-Ziel, sondern gesetzliches Minimum.

Typische Fehler bei SzA-Ausschreibungen

Häufige Schwachstellen aus realen Vergabeverfahren, die bei der BSI-Prüfung zu negativen Ergebnissen führen.

01 Produkt statt Leistung ausschreiben
LV benennt Produktnamen statt messbarer Erkennungsleistung. Das BSI prüft organisatorische Fähigkeiten, nicht installierte Hersteller-Software.

02 OT/IoT-Netz nicht im Scope
Medizingeräte, SCADA-Systeme und ICS-Protokolle (Modbus, OPC UA) fehlen im LV. Versteckte Lücken, die Auditoren direkt beanstanden.

03 Kein Detektionsqualitäts-SLA
Keine maximale False-Positive-Rate, kein MTTD vereinbart. Teams werden von hunderten täglichen Alerts überflutet, kritische Ereignisse gehen unter.

04 Deployment-Architektur unklar
On-Premises ausgeschrieben, SCADA teilweise cloud-hosted. Günstigster Bieter hat keinen Cloud-Connector, Vertragslücke nach Zuschlag.

05 Reaktion nicht ausgeschrieben
BSI-Kategorie 6 (44 Anforderungen) fehlt komplett im LV. Keine Vertragsgrundlage für Eskalationspfade, Meldewege §8b und Incident-Response.

06 Verantwortlichkeiten ungeklärt
Rollen zwischen IT-Betrieb, Security-Team und SOC nicht definiert. Nach Zuschlag: niemand ist zuständig, wenn dezentrale Systeme keine Logs liefern.

Wie wir Vergabestellen unterstützen

Drei Leistungen von der ersten Bedarfsaufnahme bis zur rechtssicheren Zuschlagsempfehlung.

01 MUSTER-LEISTUNGSVERZEICHNIS

Direkt einsetzbare LV-Vorlagen

- Fertige Muster-LVs für NDR, SIEM, EDR, SzA
- Entwickelt aus realen KRITIS-Projekten
- Abgestimmt auf BSI OH-SzA v1.1
- Eignungs- und Zuschlagskriterien enthalten
- Sofort im eigenen Vergabeverfahren nutzbar

it-leistungsverzeichnis.de/produkte

02 VERGABE-ARCHIV

Reale Ausschreibungen durchsuchen

- LVs aus abgeschlossenen SzA-Verfahren
- Leistungsbeschreibungen und Bewertungsmatrizen
- NDR-, SIEM- und SOC-Ausschreibungen
- Direkt durchsuchbar und als Download
- Laufend aktualisiert mit neuen Verfahren

it-leistungsverzeichnis.de/produkte/vergabe-archiv

03 IT-AUSSCHREIBUNGSMANAGEMENT

Individuelle Vergabeberatung

- Strukturierte Bedarfsaufnahme in Workshops
- LV-Erstellung und Bieterdialog
- Angebotsprüfung und -auswertung
- Zuschlagsempfehlung mit Begründung
- Vergaberechtskonforme Dokumentation

it-leistungsverzeichnis.de/leistungen

NÄCHSTER SCHRITT

SzA-Ausschreibung professionell vorbereiten

BSI-konforme Leistungsverzeichnisse, reale Vergabeunterlagen und projektbegleitende Beratung für KRITIS-Betreiber und öffentliche Auftraggeber.

MUSTER-LVS
it-leistungsverzeichnis.de/produkte
NDR, SIEM, EDR, SzA — sofort einsetzbar

VERGABE-ARCHIV
/produkte/vergabe-archiv
Reale SzA-Ausschreibungsunterlagen

BERATUNG ANFRAGEN
/leistungen/ausschreibungsmanagement-it-vergabe
IT-Ausschreibungsmanagement