Incident-Response-Anbieter: Bewertungsmatrix

Strukturierter Vergleich von IR-Dienstleistern · IT-Leistungsverzeichnisse.DE

Anbieter vergleichbar machen, bevor der Ernstfall eintritt

Diese Matrix hilft Ihnen, mehrere Incident-Response-Dienstleister nach denselben Kriterien zu bewerten und das Ergebnis nachvollziehbar zu dokumentieren. Sie eignet sich als Wertungsraster für einen Angebotsvergleich oder als Anlage zu einer Ausschreibung.

1. Gewichten

Legen Sie je Kriterium die Gewichtung fest (1 = nice-to-have, 2 = wichtig, 3 = Muss).

2. Bewerten

Bewerten Sie jeden Anbieter je Kriterium von 0 (nicht erfüllt) bis 3 (übertrifft).

3. Auswerten

Ergebnis je Anbieter = Summe aus Bewertung × Gewichtung. Muss-Kriterien mit 0 schließen aus.

Bewertung: 0 = nicht erfüllt · 1 = teilweise · 2 = erfüllt · 3 = übertrifft. **Gewichtung (G):** 1 = nice-to-have · 2 = wichtig · 3 = Muss.
Hinweis: Eine BSI-APT-Qualifizierung ist ein starkes Qualitätssignal, ersetzt aber nicht die Prüfung der konkreten Verfügbarkeit und Reaktionszeit im Ernstfall.

Die Kriterien sind in fünf Gruppen gegliedert: A Reaktion & Erreichbarkeit, B Forensik & Analyse, C Team & Qualifikation, D Qualität/Sicherheit/Compliance, E Sprache/Region/Vertrag. Ergänzen Sie eigene Kriterien nach Bedarf.

Bewertungsmatrix (Teil 1 von 2)

Kriterium	G	Anbieter A	Anbieter B	Anbieter C	Notiz
A · Reaktion & Erreichbarkeit					
Erreichbarkeit rund um die Uhr (24/7/365), dedizierte Notfall-Hotline					
Garantierte Reaktionszeit bis zur qualifizierten Erstanalyse					
Garantierte Vor-Ort-Zeit (DACH), falls erforderlich					
Definierte Eskalations- und Kommunikationswege bei IT-Ausfall					
B · Forensik- & Analysefähigkeiten					
Host-Forensik, Netzwerk-Forensik, Malware-Analyse (nachgewiesen)					
Abdeckung der eigenen Umgebung: Cloud, OT/ICS, mobile Geräte					
Herstellerunabhängig, Einbindung vorhandener EDR-/SIEM-Tools					
Unterstützung von Eindämmung über Bereinigung bis Wiederanlauf					
C · Team & Qualifikation					
Teamgröße und Verfügbarkeit in der DACH-Region (parallele Vorfälle)					
Qualifikationsnachweise der Analysten (Forensik-Zertifikate, CVs)					
Referenzen aus vergleichbaren Branchen und Vorfalltypen					

Bewertungsmatrix (Teil 2 von 2)

Kriterium	G	Anbieter A	Anbieter B	Anbieter C	Notiz
D · Qualität, Sicherheit & Compliance					
Qualifizierter APT-Response-Dienstleister beim BSI (§ 3 BSIG)					
ISO/IEC 27001; geregelte Vertraulichkeit und Geheimnisschutz					
Datenschutz: Auftragsverarbeitung Art. 28 DSGVO, Datenhaltung EU					
E · Sprache, Region & Vertrag					
Deutschsprachiger Service, Vertragspartner/Sitz in der EU					
Service-Level mit messbaren Zusagen und Berichtswesen					
Retainer-Modell, Stundenkontingent (Verfall vs. umwandelbar)					
Klare Übergabe an den Regelbetrieb, Lessons-Learned					
Ergebnis					
Gewichtetes Gesamtergebnis (Summe Bewertung × G)		—	—	—	

Quellen (Auswahl): BSI, Qualifizierte APT-Response-Dienstleister im Sinne § 3 BSIG · NIST SP 800-61 Rev. 3 (2025) · ENISA, Incident management · BSI IT-Grundschutz DER.2.1 Behandlung von Sicherheitsvorfällen. Diese Matrix ist eine inhaltsneutrale Arbeitshilfe und ersetzt keine Rechtsberatung. Mehr unter it-leistungsverzeichnisse.de