

# Sicherheitsanforderungen an den Auftragnehmer für Erbringung von Dienstleistungen im TK-Umfeld des WDR

## Einleitung

Sprachliche Regelung „MUSS“ und ähnliche Begriffe wie „müssen“, „müssten“, etc. beschreiben Aspekte, die zwingend erforderlich sind.

„SOLL“ bzw. „sollen“, „sollten“, etc. beschreibt Aspekte, die ebenfalls zu betrachten und umzusetzen sind.

## 1. Technische und organisatorische Schutzmaßnahmen

Es MÜSSEN kryptographische Verfahren nach Stand der Technik (z. B. BSI TR-02102) verwendet werden; unsichere/abgekündigte Verfahren DÜRFEN NICHT eingesetzt werden.

Datenkommunikation MUSS durchgängig verschlüsselt werden (z. B. TLS 1.2/1.3; Perfect Forward Secrecy); Klartext-Protokolle DÜRFEN NICHT verwendet werden.

Ruhende Daten MUSS der Auftragnehmer verschlüsselt speichern; Schlüssel MÜSSEN vor unbefugter Nutzung geschützt sein.

Erläuterung: Geeignete Verfahren sind z. B. Volume-/Filesystem-Verschlüsselung mit gesichertem Recovery-Prozess.

Die Verwendung von Entschlüsselungs-Keys SOLLTE nachvollziehbar dokumentiert werden (Zweck, Zeitraum, verantwortliche Rolle).

## 2. Identitäts- & Berechtigungsmanagement

Es MUSS eine Identitäts- und Berechtigungsverwaltung existieren, die Benutzer- und Administrationskonten strikt trennt.

Das Prinzip der minimalen Rechte (Least Privilege) MUSS umgesetzt und regelmäßig rezertifiziert werden (z. B. quartalsweise Access-Reviews).

Die Verbindung zur Erbringung von Dienstleistungen MUSS durch eine sichere Authentisierung geschützt werden; schwache Verfahren DÜRFEN NICHT verwendet werden.

Für privilegierte/administrative Zugänge MUSS Multi-Faktor-Authentisierung (MFA) eingesetzt werden.

Passwörter MÜSSEN Komplexität, Historie und Mindestlänge erfüllen; Default-Kennungen MÜSSEN deaktiviert/geändert werden.

Die Übertragung von Passwörtern MUSS ausschließlich über sichere, aktuelle Verfahren erfolgen (z. B. TLS 1.2/1.3).

Erläuterung: Unsichere Protokolle (z. B. HTTP, Telnet, FTP) DÜRFEN NICHT zur Verbindung mit dem Netz des Abrufberechtigten eingesetzt werden.

### **3. Patch-, Schwachstellen- und Schadsoftware-Management**

Neue Schwachstellenmeldungen MUSS der Auftragnehmer kontinuierlich beobachten und bewerten (Threat Intelligence/Advisories).

Ein strukturiertes Patchmanagement auf den zur Erbringung der Dienstleistung eingesetzten Systeme MUSS etabliert sein (Test, Rollout, Backout-Plan, Nachweis).

Sicherheitskritische Updates MÜSSEN auf den zur Erbringung der Dienstleistung eingesetzten Systeme unverzüglich eingespielt werden; Notfall-Patching MUSS organisatorisch/technisch möglich sein.

Ein aktueller Schutz nach Stand der Technik vor Schadsoftware MUSS auf den zur Erbringung der Dienstleistung eingesetzten Systeme betrieben werden (EDR/AV, On-Access/On-Demand, heuristische Verfahren).

### **4. Protokollierung, Monitoring und Incident Response**

Sicherheitsrelevante Ereignisse auf den zur Erbringung der Dienstleistung eingesetzten Systeme MÜSSEN vollständig, nachvollziehbar und manipulationsgeschützt protokolliert werden.

Sicherheitsvorfälle, die die Dienstleistung betreffen, MÜSSEN unverzüglich gemeldet werden (inkl. Erstbewertung, Auswirkungen, Sofortmaßnahmen).

Der Zugriff auf Protokolldaten MUSS auf autorisierte Rollen beschränkt werden; Logs MÜSSEN vor unbefugter Einsichtnahme geschützt werden.

Der Auftragnehmer MUSS eine zeitnahe Reaktion auf Angriffe bzw. Sicherheitsvorfälle gewährleisten (Detection-Containment-Eradication-Recovery).

### **5. Sichere Löschung**

Nach Vertragsende MÜSSEN sämtliche WDR-Daten vollständig und nachweisbar gelöscht werden (inkl. Replikate, Backups nach Frist).

### **6. Subunternehmerregelungen**

Subunternehmer MÜSSEN die gleichen Sicherheitsanforderungen erfüllen wie der Auftragnehmer selbst; dies MUSS vertraglich fixiert werden.