> # *One-Pager für den CISO*
>
> ***NRZ-Integration: Risiko minimieren, Kontrolle maximieren***

Was ist das?

Wir etablieren eine zentrale, sichere **API-Schnittstelle** als einzigen Zugangspunkt zum NRZ-System. Anstatt direkten, unkontrollierten Datenbankzugriff zu gewähren, wird jede Anfrage über eine gemanagte und überwachte API abgewickelt. Unsere klare Empfehlung ist **Szenario 4: Eine im Rechenzentrum gehostete API mit vollem Lese- und Schreibzugriff**.

Warum ist das für Sie relevant?

Dieses Modell ermöglicht die Umsetzung einer **Zero-Trust-Architektur**. Sie verlagern die Sicherheitsverantwortung von vielen unkontrollierbaren Endpunkten beim Kunden in eine einzige, von Experten betriebene und nach **ISO 27001 zertifizierte** Umgebung. Dies reduziert die Angriffsfläche drastisch und erhöht die Transparenz.

Sicherheitsrisiko	Traditioneller Ansatz (DB-Zugriff)	Empfohlene Lösung (Managed API)
Angriffsfläche	Breit (Jeder Client mit DB-Port-Zugriff)	**Minimal** (Nur ein HTTPS-Endpunkt)
Daten-Exfiltration	Schwer zu kontrollieren	**Kontrolliert** (Jeder Zugriff wird geloggt)
Compliance (DSGVO)	Geteilte Verantwortung, schwer nachweisbar	**Zentral nachweisbar** (AV-Vertrag mit RZ)
Sicherheits-Updates	Abhängig vom Kunden	**Zentral & Garantiert** (Patch-Management im RZ)

Ihre Vorteile auf einen Blick

1. **Maximale Kontrolle & Sichtbarkeit:** Kein direkter Datenbankzugriff von außen. Jeder einzelne Datenzugriff wird über die API **authentifiziert, autorisiert und protokolliert**.
2. **Reduzierte Komplexität & Angriffsfläche:** Sie müssen nicht die Sicherheitslage dutzender Kundenumgebungen prüfen, sondern nur die des **zertifizierten Rechenzentrums**.
3. **Garantierte Compliance:** Die Datenverarbeitung findet ausschließlich in einem **EU-Rechenzentrum** statt. Ein Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO regelt alle Pflichten klar.

Checkliste der implementierten Kernanforderungen

- [x] **Zero-Trust-Ansatz:** Jede Transaktion wird verifiziert.
- [x] **Verschlüsselung:** TLS 1.2+ in Transit, AES-256 at Rest.
- [x] **Starke Authentifizierung:** OAuth 2.0 Standard.
- [x] **Netzwerkisolation:** Keine offenen Datenbank-Ports nach außen.
- [x] **Umfassendes Auditing:** Lückenlose Logs aller Zugriffe für Ihr SIEM.

Fazit: Szenario 4 ist aus Sicherheitssicht die überlegene Lösung. Es bietet Ihnen die Werkzeuge für eine lückenlose Governance, vereinfacht den Nachweis der Compliance und setzt moderne Sicherheitsprinzipien wie Zero Trust konsequent um.