CISO-Checkliste für die NRZ-Integration

Diese Checkliste fasst die wichtigsten Sicherheitsanforderungen und -empfehlungen aus der NRZ-Integrationsdokumentation zusammen. Sie dient als praxisorientiertes Werkzeug für CISOs zur Bewertung, Planung und Überwachung der Sicherheitsmaßnahmen in den verschiedenen Integrationsszenarien.

---

1. Governance, Risk & Compliance (GRC)

Checkpunkt	Status (Offen / In Prüfung / Erfüllt)	Anmerkungen
1.1 DSGVO-Konformität sichergestellt?		AV-Vertrag (Art. 28 DSGVO) für RZ-Szenarien (3 & 4) vorhanden und geprüft?
1.2 Zero-Trust-Prinzipien angewendet?		Wird jede Transaktion explizit verifiziert, unabhängig vom Ursprung?
1.3 Compliance-Anforderungen erfüllt?		Sind branchenspezifische Standards (ISO 27001, SOC 2, etc.) für das gewählte Szenario abgedeckt?
1.4 Incident-Response-Plan vorhanden?		Ist der Prozess für Sicherheitsvorfälle definiert, kommuniziert und getestet?
1.5 Regelmäßige Sicherheitsaudits geplant?		Sind interne und externe Audits (inkl. Penetrationstests) fest im Jahresplan verankert?

---

2. Identitäts- und Zugriffsmanagement (IAM)

Checkpunkt	Status (Offen / In Prüfung / Erfüllt)	Anmerkungen
2.1 Starke Authentifizierung implementiert?		Wird durchgehend OAuth 2.0 für APIs und MFA für kritische Systemzugriffe verwendet?
2.2 Prinzip der minimalen Rechte (Least Privilege) umgesetzt?		Erhalten Benutzer und Systeme nur die Berechtigungen, die für ihre Aufgabe zwingend notwendig sind?
2.3 Zugriffskontrolle feingranular genug?		Werden Scopes (grob) und Claims (fein) zur präzisen Steuerung von API-Zugriffen genutzt?
2.4 Single Sign-On (SSO) integriert?		Ist die Anbindung an bestehende Identity-Provider (z.B. Azure AD) via OpenID Connect erfolgt?
2.5 Regelmäßige Access Reviews durchgeführt?		Werden Benutzerberechtigungen periodisch überprüft und veraltete Zugriffe entzogen?

3. Netzwerksicherheit

Checkpunkt	Status (Offen / In Prüfung / Erfüllt)	Anmerkungen
3.1 Netzwerksegmentierung vorhanden?		Ist das Netzwerk in isolierte Segmente unterteilt, um laterale Bewegungen zu verhindern (besonders im RZ)?
3.2 API Gateway als zentraler Schutzpunkt im Einsatz?		Werden alle API-Anfragen über ein Gateway geleitet, das Sicherheitsrichtlinien (Rate Limiting, etc.) durchsetzt?
3.3 Perimeter-Sicherheit ausreichend?		Sind Firewalls, IDS/IPS und DDoS-Schutzmechanismen für alle externen Schnittstellen aktiv?
3.4 VPN-Zugänge abgesichert?		Erfolgt der externe Zugriff ausschließlich über VPN-Verbindungen mit starker Authentifizierung?
3.5 Unnötige Ports geschlossen?		Sind nur die explizit benötigten Ports (z.B. 443 für HTTPS) geöffnet und alle anderen blockiert?

---

4. Datensicherheit und Verschlüsselung

Checkpunkt	Status (Offen / In Prüfung / Erfüllt)	Anmerkungen
4.1 Verschlüsselung “in Transit” durchgesetzt?		Wird ausnahmslos TLS 1.2 oder höher für die gesamte Datenübertragung verwendet?
4.2 Verschlüsselung “at Rest” implementiert?		Werden sensible Daten im Ruhezustand (Datenbanken, Backups) mit AES-256 verschlüsselt?
4.3 Sicheres Schlüsselmanagement (KMS) vorhanden?		Werden Verschlüsselungsschlüssel sicher in einem dedizierten System verwaltet und regelmäßig rotiert?
4.4 Data Loss Prevention (DLP) konfiguriert?		Sind Maßnahmen aktiv, die den unbefugten Abfluss sensibler Daten verhindern?
4.5 Backup- und Recovery-Strategie getestet?		Werden Backups regelmäßig erstellt, sicher aufbewahrt und die Wiederherstellungsprozesse getestet?

5. Anwendungs- und Endpoint-Sicherheit

Checkpunkt	Status (Offen / In Prüfung / Erfüllt)	Anmerkungen
5.1 Schwachstellenmanagement-Prozess etabliert?		Gibt es einen proaktiven Prozess für das Scannen, Bewerten und Patchen von Schwachstellen?
5.2 Endpoint Protection (EPP/EDR) im Einsatz?		Sind alle Endgeräte (Clients, Server) mit modernen Schutzlösungen ausgestattet?
5.3 Security Awareness Trainings obligatorisch?		Werden alle Mitarbeiter regelmäßig zu Themen wie Phishing und Social Engineering geschult?
5.4 Sichere Softwareentwicklung (SSDLC) praktiziert?		Werden Sicherheitsaspekte bereits im Entwicklungsprozess berücksichtigt (z.B. durch Code-Analysen)?
5.5 Schutz vor API-spezifischen Bedrohungen?		Sind Maßnahmen gegen die OWASP API Security Top 10 (z.B. Broken Object Level Authorization) implementiert?

6. Monitoring und Logging

Checkpunkt	Status (Offen / In Prüfung / Erfüllt)	Anmerkungen
6.1 Umfassende Audit-Protokollierung aktiv?		Werden alle sicherheitsrelevanten Ereignisse (Zugriffe, Änderungen) manipulationssicher protokolliert?
6.2 Zentrale Log-Aggregation (SIEM) vorhanden?		Werden alle Logs in einem zentralen SIEM-System gesammelt und korreliert?
6.3 Echtzeit-Monitoring und Alarmierung eingerichtet?		Gibt es automatisierte Alarme bei verdächtigen Aktivitäten oder dem Überschreiten von Schwellenwerten?
6.4 Log-Aufbewahrungsrichtlinien definiert?		Sind die Aufbewahrungsfristen für Log-Daten gemäß den Compliance-Anforderungen festgelegt?
6.5 Regelmäßige Überprüfung der Monitoring-Regeln?		Werden die Regeln und Schwellenwerte im Monitoring-System periodisch auf ihre Wirksamkeit überprüft?

7. Szenario-spezifische Sicherheitsanforderungen

7.1 Szenarien 1 & 2 (Kundenseitige API)

Checkpunkt	Status (Offen / In Prüfung / Erfüllt)	Anmerkungen
7.1.1 Firewall-Konfiguration für Port 3050 abgesichert?		Ist der Zugriff auf Port 3050 auf autorisierte IP-Adressen beschränkt (IP-Whitelisting)?
7.1.2 Rollenbasierte Zugriffskontrolle (RBAC) implementiert?		Sind für Szenario 2 (Schreibzugriff) granulare Berechtigungen je nach Benutzerrolle definiert?
7.1.3 Umfassende Audit-Protokollierung für Schreibvorgänge?		Werden alle Datenänderungen mit Zeitstempel, Benutzer und geändertem Datensatz protokolliert?
7.1.4 API-Infrastruktur redundant ausgelegt?		Ist die kundenseitige API-Infrastruktur gegen Ausfälle abgesichert (Load Balancer, Failover)?
7.1.5 Netzwerkbandbreite ausreichend dimensioniert?		Wurde die VPN-Kapazität für den gesamten API-Verkehr geprüft und ggf. erweitert?

7.2 Szenarien 3 & 4 (Rechenzentrum-gehostete API)

Checkpunkt	Status (Offen / In Prüfung / Erfüllt)	Anmerkungen
7.2.1 SLA mit RZ-Provider vertraglich fixiert?		Sind Verfügbarkeit (99,9%), Reaktionszeiten und Pönalen bei Nichteinhaltung klar definiert?
7.2.2 Mandantentrennung auf allen Ebenen sichergestellt?		Ist die strikte Isolation zwischen Mandanten (Datenbank, Applikation, Netzwerk) verifiziert?
7.2.3 Zertifizierungen des RZ-Providers geprüft?		Liegen aktuelle ISO 27001-Zertifikate und Audit-Berichte vor?
7.2.4 Zugriff auf Monitoring-Dashboard gewährt?		Haben Sie als Kunde Zugriff auf Echtzeit-Metriken (Verfügbarkeit, Latenz, Fehlerraten)?
7.2.5 Incident-Response-Kommunikation definiert?		Ist der Eskalationspfad bei Sicherheitsvorfällen klar dokumentiert und getestet?

7.3 Szenario 5 (XCare XChange Tool)

Checkpunkt	Status (Offen / In Prüfung / Erfüllt)	Anmerkungen
7.3.1 Endpoint-Sicherheit auf Client-Systemen gewährleistet?		Sind alle Geräte, auf denen das XChange Tool läuft, mit aktueller EPP/EDR-Software ausgestattet?
7.3.2 Schulung der Anwender zu sicheren Praktiken erfolgt?		Wurden die Nutzer in der korrekten und sicheren Handhabung des Tools geschult?
7.3.3 Datenvalidierung vor Import implementiert?		Gibt es automatisierte Prüfungen, die fehlerhafte oder bösartige Daten vor dem Import erkennen?
7.3.4 Zugriff auf Terminal Server eingeschränkt?		Ist der Remote-Desktop-Zugriff auf autorisierte Benutzer beschränkt und wird er überwacht?
7.3.5 Regelmäßige Überprüfung der Datenqualität?		Werden die manuell übertragenen Daten stichprobenartig auf Fehler und Inkonsistenzen geprüft?

---

8. Risikobewertung und Priorisierung

Nutzen Sie die folgende Matrix, um die Sicherheitsrisiken Ihres gewählten Szenarios zu bewerten und Maßnahmen zu priorisieren.

Risiko	Eintrittswahrscheinlichkeit (Niedrig / Mittel / Hoch)	Auswirkung (Niedrig / Mittel / Hoch)	Risikostufe	Maßnahmen
Unbefugter Datenbankzugriff (Szenarien 1 & 2)				IP-Whitelisting, MFA, Audit-Logs
API-Missbrauch (DDoS, Brute Force)				Rate Limiting, API Gateway, WAF
Datenleck durch Fehlkonfiguration				Automatisierte Config-Checks, IaC
Insider-Bedrohung				RBAC, Audit-Logs, User Behavior Analytics
Phishing/Social Engineering (Szenario 5)				Security Awareness Training, MFA
Ausfall des RZ-Providers (Szenarien 3 & 4)				SLA, Backup-Provider, Disaster Recovery
Compliance-Verletzung (DSGVO)				AV-Vertrag, TOMs, regelmäßige Audits

Legende Risikostufe:

- **Niedrig × Niedrig = Gering** (Akzeptabel, Monitoring)
- **Niedrig × Mittel / Mittel × Niedrig = Mittel** (Maßnahmen planen)
- **Mittel × Mittel / Hoch × Niedrig = Erhöht** (Maßnahmen zeitnah umsetzen)
- **Hoch × Mittel / Mittel × Hoch = Hoch** (Sofortige Maßnahmen erforderlich)

- **Hoch × Hoch = Kritisch** (Höchste Priorität, ggf. Projekt-Stopp)

---

9. Kontinuierliche Verbesserung

Aktivität	Frequenz	Verantwortlich	Nächster Termin
Überprüfung dieser Checkliste	Quartalsweise	CISO	
Penetrationstests	Jährlich	Externer Dienstleister	
Vulnerability Scans	Monatlich	IT-Sicherheitsteam	
Security Awareness Training	Halbjährlich	HR & IT-Sicherheit	
Incident-Response-Übung	Jährlich	CISO & IT-Leitung	
Compliance-Audit	Jährlich	Interner Audit / Externer Auditor	
Review der Zugriffsberechtigungen	Quartalsweise	IAM-Team	

---

10. Empfehlungen und Best Practices

10.1 Defense-in-Depth-Strategie

Verlassen Sie sich niemals auf eine einzelne Sicherheitsmaßnahme. Implementieren Sie mehrere Schutzschichten, sodass der Ausfall einer Schicht nicht zum Totalversagen führt. Kombinieren Sie Elemente aus allen drei Sicherheitsdomänen (API, Rechenzentrum, Büroumgebung).

10.2 Zero-Trust-Architektur

Vertrauen Sie keiner Verbindung implizit, auch nicht innerhalb des eigenen Netzwerks. Jede Transaktion muss explizit authentifiziert und autorisiert werden. Dies ist besonders relevant für Szenario 4 (Managed API im RZ), das diesem Prinzip am nächsten kommt.

10.3 Automatisierung und Orchestrierung

Automatisieren Sie Sicherheitsprozesse, wo immer möglich. Automatisierte Schwachstellen-Scans, Patch-Management und Security-Orchestration-Tools (SOAR) reduzieren menschliche Fehler und beschleunigen die Reaktionszeiten.

10.4 Transparenz und Kommunikation

Stellen Sie sicher, dass alle Stakeholder (IT, RZ, Management, Endanwender) ein gemeinsames Verständnis der Sicherheitsanforderungen haben. Regelmäßige Sicherheitsberichte an das Management schaffen Transparenz und sichern die notwendige Unterstützung.

10.5 Lessons Learned und Post-Mortems

Führen Sie nach jedem Sicherheitsvorfall (oder Beinahe-Vorfall) eine strukturierte Analyse durch. Dokumentieren Sie die Erkenntnisse und leiten Sie konkrete Verbesserungsmaßnahmen ab, um zukünftige Vorfälle zu verhindern.

---

11. Kontakte und Eskalation

Rolle	Name	Kontakt	Verfügbarkeit
CISO			
IT-Sicherheitsleiter			
RZ-Provider (Security Contact)			
Incident-Response-Team			24/7
Externer Sicherheitsberater			Nach Vereinbarung

Dokumentenversion: 1.0 **Letzte Aktualisierung:** 30. Januar 2026 **Nächste geplante Überprüfung:** April 2026

Diese Checkliste ist ein lebendes Dokument und sollte regelmäßig an neue Bedrohungen, Technologien und organisatorische Veränderungen angepasst werden.