



OESTERREICHISCHE NATIONALBANK
HAUPTABTEILUNG ANALYSE UND REVISION

Oesterreichische Nationalbank
- Zahlungssystemaufsicht -

Aufsichtsgrundsätze

für

elektronische Zahlungssysteme

Systemrelevante Teilnahme

Teil 2
Betrieb von Infrastruktureinrichtungen
für Zahlungssysteme

Die vorliegenden Aufsichtsgrundsätze für den Betrieb von Infrastruktureinrichtungen für Zahlungssysteme beinhalten die von der OeNB für die Gewährleistung der sicheren Systemteilnahme als erforderlich erachteten Anforderungen und dienen als Evaluierungsmaßstab für die gemäß § 44a Abs. 8 NBG zu erteilenden Auskünfte.

Anforderungen

Rechtliche und finanzielle Sicherheit der Systemteilnahme

- (1) Dem Infrastrukturbetreiber sollen die Rechtsgrundlagen und die Geschäftsbedingungen für die Teilnahme am Zahlungssystem in der jeweils aktuellen Fassung bekannt sein.
- (2) Dem Infrastrukturbetreiber soll die gerichtliche Zuständigkeit bekannt sein.
- (3) Der Infrastrukturbetreiber soll über Geschäftsbedingungen verfügen, aus denen die Bedingungen für den Zugang zu den Infrastruktureinrichtungen klar und eindeutig hervorgehen.
- (4) Der Infrastrukturbetreiber soll die ihn aufgrund der Teilnahme am Zahlungssystem betreffenden haftungsrechtlichen Risiken kennen. Gegebenenfalls bestehende haftungsrechtliche Risiken sollen durch entsprechende Vorkehrungen soweit als möglich abgesichert sein.
- (5) Dem Infrastrukturbetreiber sollen die haftungsrechtlichen Regelungen, die seitens seiner relevanten Vertragspartner ihm gegenüber bestehen, bekannt sein.
- (6) Es sollen klare Regelungen und Vorgehensweisen für die geordnete Beendigung der Teilnahme des Infrastrukturbetreibers am Zahlungssystem sowohl durch den Infrastrukturbetreiber als auch durch den Zahlungssystembetreiber festgelegt sein.
- (7) Der Infrastrukturbetreiber soll die für ihn relevanten datenschutzrechtlichen Bestimmungen in der jeweils aktuellen Fassung kennen und ihre jederzeitige Einhaltung sicherstellen.

Organisatorische Sicherheit der Systemteilnahme

- (1) Der Infrastrukturbetreiber soll über eine transparente und nachvollziehbare Führungs- und Verwaltungsstruktur verfügen.
- (2) Der Infrastrukturbetreiber soll die Vorgaben und Richtlinien des Zahlungssystembetreibers (bzw. der Zahlungssystembetreiber) vollständig und aktuell dokumentiert halten und für ihre jederzeitige Einhaltung sorgen.
- (3) Der Infrastrukturbetreiber soll darüber hinausgehende selbst entwickelte Richtlinien, für die vorzugsweise internationale Standards herangezogen werden sollten, vollständig und aktuell dokumentiert halten und für ihre jederzeitige Einhaltung sorgen.
- (4) Der Infrastrukturbetreiber soll die Einhaltung von (2) und (3) regelmäßig einer internen Überprüfung unterziehen.

- (5) Der Infrastrukturbetreiber soll dem Stand der Technik entsprechende sichere Verfahren für die Bereitstellung von Infrastrukturkomponenten an die Zahlungssysteme beziehungsweise gegebenenfalls an deren Teilnehmer und Endkunden anwenden.
- (6) Der Infrastrukturbetreiber soll sicherstellen, dass ausreichend, ausgebildetes und vertrauenswürdige Personal für den Betrieb sowohl in Normal- als auch in Ausnahmesituationen zur Verfügung steht.
- (7) Der Infrastrukturbetreiber soll geeignete Eskalationsmechanismen für den Fehler- und Katastrophenfall vorsehen, insbesondere sollen geeignete Kommunikationsverfahren mit den servicierten Zahlungssystemen eingerichtet und regelmäßig getestet werden.

Technische Sicherheit der Systemteilnahme

- (1) Vom Infrastrukturbetreiber soll sichergestellt werden, dass zumindest für folgende Bereiche konkrete Richtlinien festgelegt sind:
 - die Gewährleistung der Verfügbarkeit und Betriebssicherheit der Infrastruktur,
 - das Erkennen und die Abwehr von Angriffen auf die Infrastruktur,
 - die Nachprüfbarkeit der Authentizität und Integrität der von den Teilnehmern und Endkunden verwendeten Infrastrukturkomponenten,
 - die Integrität und Vertraulichkeit der Transaktionsdaten und Parameter des servicierten Zahlungssystems,
 - eine zur eindeutigen Nachverfolgung geeignete Aufbewahrungsdauer von Änderungsprotokollen,
 - die korrekte Authentisierung der Teilnehmer und Endkunden, die korrekte Autorisierung der Transaktionen sowie die wirksame Sperre (sofern diese Funktionen über die Infrastruktur ausgeübt werden).Diese Richtlinien können Vorgaben der Zahlungssystembetreiber oder eigene Richtlinien sein.
- (2) Die Richtlinien sollen durch geeignete, dem Stand der Technik entsprechende Einrichtungen und Maßnahmen umgesetzt werden.
- (3) Der Infrastrukturbetreiber soll an Hand einer Risikoanalyse kritische Komponenten und Prozesse identifizieren. Notfallsmaßnahmen sollen für verschiedene Szenarien und entsprechend dieser Klassifizierung verfügbar sein.
- (4) Übungen für Notfallsmaßnahmen sollen in regelmäßigen Abständen durchgeführt werden.
- (5) Wenn mehrere Systeme (Zahlungssysteme oder Systeme für andere Zwecke) ein und dieselbe Infrastruktur benutzen, soll ausgeschlossen werden, dass eine gegenseitige negative Beeinflussung der einzelnen Systeme in Bezug auf die Sicherheit und Verfügbarkeit möglich ist.

- (6) Werden vom Infrastrukturbetreiber Dienste angeboten, welche die jeweiligen Zahlungssysteme integrieren, benutzen oder erweitern (Add-on-Dienste), soll sichergestellt sein, dass dies nachweislich unter Beachtung der Vorgaben der betroffenen Systeme erfolgt.
- (7) Es soll sichergestellt sein, dass die für die Zahlungssysteme relevanten Sicherheitsfunktionen auch in Fällen von Betriebsstörungen oder Fehlbedienungen aufrecht bleiben.

Nachweise

Die Erfüllung der Anforderungen ist auf Verlangen der OeNB an Hand des „Leitfadens zur Erteilung von Auskünften gemäß § 44a Abs. 8 NBG über die zur sicheren Teilnahme getroffenen Vorkehrungen – Teil 2: Betrieb von Infrastruktureinrichtungen für Zahlungssysteme“ binnen der im Aufforderungsschreiben genannten Frist nachzuweisen.

Die Nachweise sind bei wesentlichen Änderungen des Systems bzw. des Systemzuganges unaufgefordert in aktualisierter Form wiedervorzulegen.