Anhang 2 zur EVB Informationssicherheit
SaaS, PaaS, Cloud-Services, RZ-Betrieb

Ausgabe 01.11.2024

4 Präambel

Diese Regelungen gelten ergänzend zu den Ergänzenden Vertragsbedingungen der Deutsche Bahn AG und der mit ihr verbundenen Unternehmen zu Anforderungen an die Informationssicherheit (EVB Informationssicherheit) und regeln den folgenden Anwendungsfall:

- Bezug von ‚as a Service'-Produkten und Cloud-Services
- Rechenzentrums-Betrieb

5 Zusätzliche Anforderungen an die Informationssicherheit

5.1 Erreichbarkeiten

Für die Erreichbarkeit der Ansprechpartner gelten folgende Verfügbarkeits- und Reaktionszeiten, soweit Auftraggeber und Auftragnehmer im Vertrag nicht ausdrücklich etwas anderes vereinbart haben.

	Schutzbedarf	
	Normal	Hoch / sehr hoch
Regelkommunikation		
Reaktionszeit AN auf Anfrage AG	8h, innerhalb Geschäftszeit	4h, innerhalb Geschäftszeit
Notfallkommunikation		
Meldung Informationssicherheitsvorfälle und Schwachstellen	Unverzüglich	Unverzüglich
Reaktionszeit Notfall-SPOC AN	4h innerhalb Geschäftszeiten (9 – 17 h)	1h innerhalb erweiterter Geschäftszeiten gem. SLA

Tabelle 1: Reaktionszeiten

5.2 – entfällt –

5.3 – entfällt –

5.4 Sicherheitsdokumentation

Der Auftragnehmer dokumentiert die Sicherheitseigenschaften des IT- / OT-Produkts derart, dass die Anforderungen des Auftraggebers (z.B. auf Grund des Schutzbedarfs) verifiziert werden können. Die Dokumentation beinhaltet z.B. Angaben zu

- implementierten Mechanismen zum Schutz der verarbeiteten und gespeicherten Daten,
- Archivierungskonzepten,
- verwendeten Komponenten (im Sinne der kleinsten tauschbaren Einheit, auch Netzwerkkomponenten und Komponenten Dritter) inklusive eindeutiger Seriennummern bzw. Indentifikationsmerkmalen,
- Datenflüssen und deren Schutzmechanismen,
- Netzplänen und Schnittstellen,
- Informationen zu Zugriffsmöglichkeiten (auch drahtlos, u.A. offene Ports) und deren Schutzmaßnahmen.

Bei Änderungen am Produkt hält der Auftragnehmer die Dokumentation auf dem aktuellen Stand.

Für OT-Produkte erstellt der Auftragnehmer eine Risikoanalyse gem. IEC62443 und hält diese über die Vertragslaufzeit bzw. bis zum Ende der Gewährleistungsfrist aktuell (soweit nicht vertraglich ab-

weichend vereinbart; es gilt das weiter in der Zukunft liegende Datum). Ergeben sich hieraus Maßnahmen am Produkt, stimmen sich Auftraggeber und Auftragnehmer über Umsetzungsrahmen und Kosten ab.

Auf Aufforderung lässt der Auftragnehmer die Risikoanalyse durch einen unabhängigen Dritten verifizieren. Die Kosten hierfür trägt der Auftraggeber.

5.5 **Untersagung unerwünschter Funktionen**

Der Auftragnehmer gewährleistet, dass die von ihm gelieferten oder für den Auftraggeber betriebenen IT- / OT-Produkte keine unerwünschten Funktionen aufweisen, die die Integrität, Vertraulichkeit und Verfügbarkeit von Software, Hardware oder Daten gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen, z.B. Backdoors oder Funktionalitäten zur Manipulation von Daten oder Ablauflogik.

5.6 – entfällt –

5.7 **Anbindung**

Betreibt der Auftragnehmer IT- / OT-Produkte für den Auftraggeber bzw. stellt ‚as a Service'-Produkte zur Verfügung, gewährleistet er die ausreichend performante, redundante und gesicherte Anbindung seines Rechenzentrums / Netzes an das Rechenzentrum / Netz der DB AG und deren verbundenen Unternehmen. Bei einer Netzkopplung bzw. Schnittstelle zu den Services des Auftragnehmers ist die Brandbreite (Min/Max) in einem OLA / SLA mit dem Auftraggeber abzustimmen und der technische Übergabepunkt zu benennen. Sofern die Anbindung über das Internet erfolgt, muss die Bandbreite der Internetanbindung ausreichend bemessen sein.

Erfolgt eine Netzanbindung primär über Luftschnittstelle (z.B. Mobil-, Richtfunk) ist der Auftragnehmer verpflichtet, sich mit dem Auftraggeber vor Inbetriebnahme abzustimmen, inwieweit der Dienst im Falle eines Verlustes der Verfügbarkeit über alternative Anbindungen (z.B. kabelgebunden oder über alternative Dienstleister) abgerufen werden kann, um die Geschäftsprozesse des Auftraggebers unter Beachtung der Anforderungen an die Informationssicherheit aufrecht zu erhalten.

5.8 **Kryptographie**

Im IT/OT-Produkt verarbeitete und gespeicherte Informationen sind in Abstimmung mit dem Auftraggeber durch kryptographische Verfahren zu schützen, insbesondere Zugriffs- und Konfigurationsdaten. Der Auftragnehmer dokumentiert diese in Abstimmung mit dem Auftraggeber. Der Auftragnehmer gewährleistet, dass die verwendeten kryptographischen Verfahren und Maßnahmen zur Schlüsselverwaltung dem Stand der Technik entsprechen.

5.9 – entfällt –

5.10 – entfällt –

5.11 – entfällt –

5.12 – entfällt –

5.13 – entfällt –

5.14 **Identitätsmanagement**

Der Auftragnehmer gewährleistet und dokumentiert für sein IT- / OT-Produkt das Management der Identitäten und die von diesen erfolgenden Zugriffe auf Daten und Schnittstellen gemäß dem Stand der Technik, soweit im Vertrag nicht etwas anderes vereinbart sein sollte. Die Verwaltung und Dokumentation von Nutzern und Rechten erfolgt in einer zentralen, integrierten Datenbank.

5.15 – gestrichen –

5.16 – entfällt –

5.17 – entfällt –

5.18 Unterstützung Datenrückführung

Bei Betriebsführung oder bei Bereitstellung von ‚as a Service'-Produkten durch den Auftragnehmer sichert dieser dem Auftraggeber Unterstützung bei der Rückholung von Daten und / oder Anwendungen bei Beendigung des Vertrags zu. Die Unterstützung schließt gegebenenfalls eine entsprechend dimensionierte technische Schnittstelle zu einem vom Auftraggeber definierten System sowie Datenrückführung in einem portierbaren, maschinell verarbeitbaren Format mit ein. Proprietäre Formate und proprietäre Verschlüsselungstechnologien sind nicht gestattet.

5.19 Physische Sicherheit

Der Auftragnehmer muss angemessene Vorkehrungen zur physischen Sicherheit seiner Assets und / oder Infrastruktur treffen.

Insbesondere sollen Maßnahmen zum/zur:

- Schutz gegen Feuer und Wasser,
- Schutz vor Einbruch und Vandalismus,
- Schutz vor bzw. Vermeidung von extremen Temperaturen,
- adäquaten Energieversorgung implementiert sein.

Der Auftragnehmer gewährleistet, dass der Zutritt zu Bereichen mit Informationen oder Systemen auf den autorisierten Personenkreis beschränkt wird.

Dazu gehören z.B. Zutrittsschutzmaßnahmen für Rechenzentren inklusive Überwachung der kritischen Bereiche, Zutrittsprotokoll, Sicherung gegen Einbruch u.a..

5.20 Behandlung von Informationssicherheitsvorfällen

Der Auftragnehmer hat ein System etabliert, in dem Informationssicherheitsvorfälle, die den Auftraggeber betreffen, abgehandelt werden und das den Informationsaustausch mit dem Auftraggeber über den zentralen Ansprechpartner des Auftragnehmers gewährleistet.

Die Erstbewertung eines Informationssicherheitsvorfalls erfolgt im Rahmen der Meldung durch den Auftragnehmer im Rahmen der vereinbarten Reaktionszeiten (siehe 5.1). Etwaige Folgeaktivitäten sind durch ein Incident Response Team beim Auftragnehmer abzubilden. Bei Outsourcing dieser Tätigkeiten beim Auftragnehmer ist der Auftraggeber zu informieren.

Sieht der Vertrag die Lieferung von IT-/ OT-Produkten vor, ergreift der Auftragnehmer in seinem Kontext präventive Maßnahmen, um die Folgen von Informationssicherheitsvorfällen zu minimieren. Hierzu gehört z.B. die Sicherstellung der Freiheit von Schadsoftware bei Inbetriebnahme des IT- / OT Systems.

5.21 Schwachstellenprüfung

Der Auftragnehmer verpflichtet sich, seine Produkte und Dienstleistungen während deren definiertem Lebenszyklus kontinuierlich auf Schwachstellen zu prüfen, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren.

Die Häufigkeit, Intensität und Methoden der Schwachstellenüberprüfung müssen sich an der Risikosituation des Auftraggebers orientieren. Hierzu stimmen sich Auftraggeber und Auftragnehmer regelmäßig ab. Ohne eine solche Vereinbarung orientieren sich die genannten Aktivitäten am Stand der Technik.

5.22 Integration Schwachstellenmanagement und Event-Management

Für IT- und OT-Produkte, die sich in einer Netzwerkinfrastruktur der DB befinden oder Informationen dorthin einspeisen, unterstützt der Auftragnehmer den Auftraggeber bei der Integration in das Schwachstellenmanagementsystem sowie das Event Management System des Auftraggebers.

Hierzu werden sicherheitsrelevante Ereignisse innerhalb des Systems protokolliert, zu eventuellen Untersuchungszwecken archiviert und in einem abgestimmten Format zur Verfügung gestellt. Details (u.A. Art der Meldungen, Mengengerüste, Robustheit) sind in der Leistungsbeschreibung definiert.

Zusätzlich empfiehlt der Auftragnehmer Werkzeuge zur Sicherheitsanalyse bzw. weist auf nachteilige Auswirkungen bestimmter Werkzeuge hin.

5.23 **Meldung von Schwachstellen**

Sind vom Auftragnehmer bereitgestellte oder von diesem betriebene IT- / OT-Produkte von Schwachstellen betroffen, ist der Auftragnehmer verpflichtet, diese dem Auftraggeber unverzüglich und auf sicherem Wege zu melden. Die Einordnung der Ergebnisse erfolgt möglichst nach dem Common Vulnerability Scoring System oder auf Basis von Bewertungen des Bundesamtes für Sicherheit in der Informationstechnik.

Inhalt der Meldung ist insbesondere:

- Genaue Bezeichnung des Produktes (soweit zutreffend Angaben insbesondere zu Bauform, Teilsystem, Komponente, Herstellerbezeichnung, Release, Produkt- und / oder Chargennummer von überlassener Software, Firmware, Treiber, BIOS und Hardware).
- Detaillierte Beschreibung der Schwachstelle einschließlich deren Ausnutzbarkeit.
- Erstbewertung aus Sicht des Auftragnehmers und Empfehlung von konkreten Gegenmaßnahmen zur Schwachstellenbehandlung unter Berücksichtigung der ggf. einschlägigen Vorgaben zur sicherheitstechnischen Zulassung und Freigabe.
- Anzahl und dokumentierte Einbauorte (mit Nennung der technischen Anlage einschließlich Raum und Schrankplatz) der betroffenen Produkte, sofern Informationen beim Auftragnehmer vorhanden und insbesondere bei 'as a Service'-Leistungen relevant sind.

Die Meldepflicht umfasst außerdem Folgemeldungen, sofern eine Schwachstellenbehandlung nicht in den vereinbarten Behandlungsfristen abgearbeitet werden kann.

5.24 **Beseitigung von Schwachstellen**

Die Zeiten zur Neutralisierung von Schwachstellen (z.B. durch einen Workaround) sowie zur finalen Lösung der Schwachstelle orientieren sich am jeweils aktuellen Stand der Technik, soweit im Vertrag nicht anders vereinbart.

5.25 – entfällt –

5.26 **Referenzzeit**

Die IT/OT-Produkte des Auftragnehmers nutzen eine allgemein akzeptierte Zeitquelle. Der AN benennt diese in der Produktdokumentation und stimmt sie auf Anfrage mit dem Auftraggeber ab.

5.27 **Schnittstellen**

Über Datenaustausch- und Eingabeschnittstellen empfangene Daten sind automatisiert auf ihre Plausibilität hin zu prüfen und ggf. abzuweisen. Details und insbesondere Abweichungen hiervon sind in der Leistungsbeschreibung geregelt.

5.28 – entfällt –

5.29 – entfällt –

5.30 – entfällt –

5.31 – entfällt –