Anhang 2 zu den EVB Informationssicherheit
„SaaS PaaS Cloud Services RZ-Betrieb“

- Ausgabe 01.01.2021 -

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:

- Hosting
- SaaS, PaaS, Cloud Services, RZ-Betrieb
- Ausgelagerter Betrieb von IT-Systemen

5 Zusätzliche Anforderungen an die Informationssicherheit

5.1 Erreichbarkeiten

Während der Vertragslaufzeit gelten folgende Verfügbarkeits- und Reaktionszeiten zur Erreichbarkeit der Ansprechpartner, 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 Incident	Unverzüglich	Unverzüglich
Reaktionszeit SPOC AN	4h innerhalb Geschäftszeiten (9 – 17 h)	1h innerhalb erweiterter Geschäftszeiten gem. SLA
Schwachstellenmeldung	72h	24h

Tabelle 1: Reaktionszeiten

5.2 entfällt

5.3 Verantwortungsübergang

Organisiert der Auftragnehmer die Einführung des Produkts, unterbreitet er dem Auftraggeber einen Vorschlag in Textform für eindeutige Regelungen zum Übergang operativer Verantwortung zwischen Auftragnehmer und Auftraggeber.

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 u.a. Angaben zu Datenflüssen und Sicherheitsmechanismen.

5.5 Designprinzipien

Der Auftragnehmer trägt dafür Sorge, 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, 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 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**
Kommen kryptographische Verfahren zum Einsatz, dokumentiert der Auftragnehmer diese in Abstimmung mit dem Auftraggeber gemäß den Vorgaben der Leistungsbeschreibung. Der Auftragnehmer gewährleistet, dass die verwendeten kryptographischen Verfahren dem vereinbarten Stand der Technik entsprechen.

5.9 entfällt

5.10 **Patchfähigkeit**
Sofern der Vertrag die Lieferung von IT- / OT-Produkten vorsieht, gewährleistet der Auftragnehmer während des Lifecycles die Schließung von Sicherheitslücken mittels Patches. Der Auftragnehmer liefert ein patchfähiges IT- / OT-Produkt, so dass Änderungen nachträglich vorgenommen werden können, ohne Grundfunktionalitäten zu verändern. Der Auftragnehmer gewährleistet, dass eingespielte Patches nach dem jeweils aktuellen Stand der Technik getestet sind, bei Produktionsproblemen zurückgenommen werden können (Revoke) und Änderungen systemseitig protokolliert und dokumentiert werden. Der Patchrhythmus orientiert sich am jeweils aktuellen Stand der Technik.

5.11 entfällt

5.12 entfällt

5.13 entfällt

5.14 **Identitätsmanagement**
Betreibt der Auftragnehmer IT- / OT-Produkte im Auftrag des Auftraggebers, gewährleistet der Auftragnehmer das Management der Identitäten und des Zugriffs auf Daten und Schnittstellen gemäß dem jeweils aktuellen Stand der Technik, soweit im Vertrag nicht etwas anderes vereinbart sein sollte. Jede natürliche Person und jeder technische User bekommt ein separates Nutzerkonto bereitgestellt, es werden nur die minimal notwendigen Rechte vergeben. Auf Verlangen übermittelt der Auftragnehmer dem Auftraggeber die konkrete Leistung betreffende Informationen aus dem Identity Access Management (IAM).

5.15 entfällt

5.16 **Konfigurationsdaten**
Der Auftragnehmer muss die Konfiguration bei jeder Änderung eines Assets dokumentieren und zu jedem Zeitpunkt in der Lage sein, jedes Konfigurationselement zu identifizieren und alle notwendigen Daten zur Konfiguration dieses Elementes bis hin zur Sourcecode Ebene vollständig und maschinenlesbar zu erhalten.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber diese Konfigurationsdaten auf Anfrage zur Verfügung zu stellen. Betreibt der Auftragnehmer Assets im Netz des Auftraggebers, ist die Meldung der Konfigurationsdaten in das Assetmanagement des Auftraggebers verpflichtend.

Für den Fall, dass der Auftragnehmer weder Wartung noch Betrieb leistet, verpflichtet sich der Auftragnehmer, dem Auftraggeber die vollständige Konfiguration der Versionen-/Releases des Produkts und aller Komponenten, Bibliotheken, Firmware, Bios sowie der verwendeten Hardware auf Beschreibungsebene zu übergeben.

Der Auftraggeber kann die Übereignung bzw. Hinterlegung des Sourcecodes bei einer anerkannten Hinterlegungsstelle verlangen; handelt es sich bei der zu erbringenden Leistung um ein Produkt, ist die Hardware-Stückliste des Produkts durch die Informationen über Objektcode und Sourcecode zu ergänzen. Dabei sind insbesondere verwendete Bibliotheken und Schnittstellen aufzuführen.

5.17 entfällt

5.18 **Unterstützung Datenrückführung**

Bei Betriebsführung 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 mit ein. Proprietäre Formate und proprietäre Verschlüsselungstechnologien sind nicht gestattet.

5.19 **Physische Sicherheit**

Der Auftragnehmer muss angemessene Vorkehrungen zur physischen Sicherheit seiner Infrastruktur treffen.

Insbesondere sollen Maßnahmen zum/zur:

- Schutz gegen Feuer und Wasser,
- 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 auch die Zutrittsschutzmaßnahmen für Rechenzentren inklusive Überwachung der kritischen Bereiche, Zutrittsprotokoll, Sicherung gegen Einbruch u.a..

5.20 **Behandlung Sicherheitsvorfälle**

Sieht der Vertrag die Lieferung von IT-/ OT-Produkten vor, ergreift der Auftragnehmer in seinem Kontext präventive Maßnahmen, um die Folgen von Sicherheitsvorfällen zu minimieren (z.B. IDS, IPS, SIEM). Der Auftragnehmer hat ein System etabliert, in dem Sicherheitsvorfälle, die den Auftraggeber betreffen, abgehandelt werden und das den Informationsaustausch mit dem Auftraggeber über den zentralen Ansprechpartner des Auftragnehmers gewährleistet. Die Erstbewertung eines Sicherheitsvorfalles 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.

5.21 **Schwachstellenprüfung**

Der Auftragnehmer verpflichtet sich, seine Produkte und Dienstleistungen während der Laufzeit des Vertrages kontinuierlich auf Schwachstellen zu prüfen, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren.
Die Häufigkeit und Intensität der Schwachstellenüberprüfung müssen sich an der Risikosituation des Auftraggebers orientieren. Hierzu stimmen sich Auftraggeber und Auftragnehmer regelmäßig ab.

5.22 **Integration Schwachstellenmanagement und Event Management**

Für IT- / 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.
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 sind.

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.

❑