Anhang 1 zur EVB Informationssicherheit
Entwicklungsdienstleistungen für DB-spezifische Software, Software-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:

- Entwicklungsdienstleistungen für DB-spezifische Software
- Betriebsführungsleistungen für DB-spezifische Software

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 Ansprechpartner nach Produktionseinführung

Bei individuell entwickelten IT- / OT-Produkten, die vom Auftraggeber im Betrieb geführt werden, sind die vereinbarten Verfügbarkeiten und Reaktionszeiten der Ansprechpartner mindestens 3 Monate nach Einführung aufrecht zu erhalten, falls der Vertrag nichts anderes vorsieht. Für den weiteren erwartbaren und vom Auftragnehmer zu benennenden Lifecycle sind angemessene Verfügbarkeiten und Reaktionszeiten zu gewährleisten.

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

- 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 abweichend 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 Netzwerkarchitektur und -betrieb

Der Auftragnehmer gewährleistet die Integration des von ihm gelieferten IT- / OT-Produkts in die Netzinfrastruktur des DB-Konzerns in Abstimmung mit dem Auftraggeber.

Für spezifisch für den Auftraggeber entwickelte IT- / OT-Produkte gewährleistet der Auftragnehmer, dass die verwendete physische Netzaufteilung einschließlich der Verwendung von Netzwerkkomponenten mit IT-Sicherheitseigenschaften oder äquivalenten Mechanismen entsprechend dem vom Auftraggeber genehmigten Entwurf umgesetzt wurde. Dies schließt drahtlose Netzwerke ein. Vom Auftragnehmer betriebene Netzwerke sind kontinuierlich nach Stand der Technik zu überwachen. Die Nutzung nicht autorisierter Geräteadressen ist mittels angemessener Maßnahmen zu verhindern.

Betreibt der Auftragnehmer IT- / OT-Produkte im Auftrag des Auftraggebers in seinem eigenen Netzwerk, gewährleistet er die Umsetzung von netzwerktechnischen Schutzvorkehrungen nach dem Stand der Technik.

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 Entwicklung und Test

Führt der Auftragnehmer Entwicklungsleistungen spezifisch für den Auftraggeber durch, plant er Entwicklung und Tests in Abstimmung mit dem Auftraggeber und nach dem Stand der Technik. Der Auftraggeber behält sich das Recht auf Einsicht in die Testprotokolle vor.

5.10 Bereitstellung Sicherheitspatches

Sofern der Vertrag die Lieferung oder den Betrieb von IT- / OT-Produkten – auch im Rahmen eines Services – vorsieht, gewährleistet der Auftragnehmer während des von ihm zu benennenden Produktlebenszyklus die Schließung von Sicherheitslücken mittels Patches. Der Auftragnehmer liefert/betreibt ein patchfähiges IT- / OT-Produkt, so dass Änderungen nachträglich vorgenommen werden können, ohne Grundfunktionalitäten zu verändern oder Schutzziele zu gefährden. Der Auftragnehmer gewährleistet, dass eingespielte Patches nach dem Stand der Technik entwickelt, getestet und freigegeben sind, bei Produktionsproblemen zurückgenommen werden können (Revoke) und Änderungen systemseitig protokolliert und dokumentiert werden. Der Patchrhythmus orientiert sich am Stand der Technik.

Bei Betrieb des Produkts im Netz des Auftraggebers stellt der Auftragnehmer eine Bewertung der Patches und einen Terminplan zu deren Bereitstellung zur Verfügung. Security Advisories sollen wenn möglich maschinenlesbar (in Abstimmung mit dem Auftraggeber als Common Security Advisory Framework (CSAF) oder Cyclone DX) bekanntgegeben werden.

Die Dokumentation der Patches beinhaltet die Auswirkungen des Patches auf die betriebliche Risikosituation sowie notwendige Voraussetzungen und Schritte zur Installation, z.B. Versionsabhängigkeiten und eventuelle Leistungsminderungen.

Für aus betrieblichen Gründen nicht installierbare Patches erstellt der Auftragnehmer in Zusammenarbeit mit dem Auftraggeber Anweisungen zu Workarounds und ggf. weiteren Mitigationsmaßnahmen.

Die Integrität von Sicherheits-Patches und Updates muss durch einen kryptographischen Mechanismus prüfbar sein.

5.11 Patch-Management

Bei Betrieb eines IT- / OT-Produkts im Netzwerk der DB verpflichtet sich der Auftragnehmer, während der Vertragslaufzeit alle Änderungen von Hard- und Softwareständen bzw. Konfigurationen in Abstimmung mit dem Auftraggeber über dessen Patch-Management zu steuern und zu kontrollieren. Änderungen sind im Konfigurationsmanagement zu erfassen.

Terminvorgaben zur Installation der Patches (durch Hersteller oder Auftraggeber) sind nachprüfbar einzuhalten und der Installationsstatus aller anwendbaren Patches transparent zu halten. Der Härtungszustand des Systems ist nach Installation der Patches wiederherzustellen und zu gewährleisten.

5.12 Vorbereitung der Inbetriebnahme / Härtung

Sofern der Vertrag die Lieferung von IT- / OT-Produkts vorsieht, gewährleistet der Auftragnehmer, dass diese vor Produktionseinführung frei von Bestandteilen und Funktionen sind, die zur Erfüllung der vertraglichen Aufgaben nicht zwingend notwendig sind. Der Produkt-/ Serviceübergabe ist eine entsprechende Bestätigung beizulegen. Installationsprinzipien, Schritte zur Härtung und zum Schutz der Schnittstellen, Konfigurationsanweisungen sowie zur Installation notwendige Werkzeuge und Programmesind zu dokumentieren und dem Auftraggeber bereitzustellen.
Der Auftragnehmer stellt dem Auftraggeber alle Administrationszugänge für den Fall der eigenständigen Inbetriebnahme und Betrieb der Systeme zur Verfügung. Ebenfalls ist die Dokumentation für die Administration zu übergeben.

Nicht benötigte Anwendungen, Dienste, Konten und Funktionen sind bei Auslieferung deaktiviert, ungenutzte Ports und Schnittstellen gesperrt.

Zum Betrieb des Produkts notwendige Zertifikate und deren Management werden mit dem Auftraggeber abgestimmt. Die Verwendung selbst signierter Zertifikate ist untersagt.
Der Auftragnehmer prüft Installations- und weitere benötigte Datenträger vor Auslieferung auf Freiheit von Schadsoftware und bestätigt dies dem Auftraggeber. Für diese Zwecke genutzte Datenträger dürfen nicht anderweitig zum Einsatz kommen.

5.13 **Passwörter**

Fest im Sourcecode verankerte Passwörter sind unzulässig. Der Auftragnehmer händigt dem Auftraggeber eine vollständige Liste der systemseitig angelegten Passwörter aus. Diese müssen zufällig generiert sein. Sofern der Vertrag die Implementierung von IT- / OT-Systemen vorsieht, verpflichtet sich der Auftragnehmer, Standardpasswörter vor Produktivsetzung zu ändern. Alle verwendeten Passwörter müssen vereinbarten Komplexitätskriterien genügen und zentral rücksetzbar sein. Die Komplexität, die Änderbarkeit und die Gültigkeitsdauer müssen technisch sichergestellt werden und dem Stand der Technik entsprechen.

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.

Betreibt der Auftragnehmer IT- / OT-Produkte oder Netzwerkkomponenten im Auftrag des Auftraggebers, gelten folgende Anforderungen: Jede natürliche Person und jeder technische User bekommt für die Dauer seiner Tätigkeit ein separates Nutzerkonto bereitgestellt. Bei Beendigung der Tätigkeit ist das Konto zu deaktivieren und nach einem zu vereinbarenden Zeitraum zu löschen. Bei Auslieferung angelegte User werden in der Datenbank dokumentiert. 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). Ein Zugriff auf das IT- / OT-Produkt unter Umgehung des IAM ist technisch auszuschließen.

Für Fernwartungszugriffe ist bevorzugt das DB-Fernwartungssystem zu nutzen, Details sind zwischen AG und AN abzustimmen.

Bei als Service bezogenen Leistungen hält der Auftragnehmer über die Vertragslaufzeit ein die hier beschriebenen Anforderungen erfüllendes Identitätsmanagement zur Nutzung durch den Auftraggeber aufrecht.

5.15 – gestrichen –

5.16 **Asset und Konfigurationsmanagement**

Der Auftragnehmer verpflichtet sich, dem Auftraggeber vollständige Konfigurationsdaten inklusive aller Komponenten (im Sinne der kleinsten tauschbaren Einheit), Bibliotheken, Firmware, Bios und verwendeter Hardware zur Verfügung zu stellen.

Der Auftragnehmer muss die Konfiguration bei jeder Änderung eines Assets prüfen, dokumentieren und die aktualisierte Version dem Auftraggeber zur Verfügung stellen. Er muss zu jedem Zeitpunkt in der Lage sein, jedes Konfigurationselement zu identifizieren und alle not-wendigen Konfigurationsdaten dieses Elementes bis hin zur Sourcecode Ebene vollständig und maschinenlesbar zu erhalten.

Wenn vorhanden, stellt der Auftragnehmer diese Informationen in Form einer Software Bill of Materials (SBOM) im SPDX- oder Cyclone-DX-Format (nach Abstimmung mit dem AG) bzw. einer Hardware Bill of Material (HBOM) zur Verfügung.

Der Auftraggeber kann die Übereignung bzw. Hinterlegung des Sourcecodes bei einer anerkannten Hinterlegungsstelle verlangen.

5.17 **End of Service Life**

Sofern der Vertrag die Lieferung von IT- / OT-Produkten vorsieht, verpflichtet sich der Auftragnehmer, Ablösestrategien bei absehbarem End of Service Life fachlich und technisch zu berücksichtigen und dem Auftraggeber entsprechende Informationen zu den betroffenen Assets zur Verfügung zu stellen.

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 Sicherheitsanalysen

Betreibt der Auftragnehmer Systeme im Netz des Auftraggebers, stimmen sich Auftragnehmer und Auftraggeber zu Form und Inhalt der aktiven und passiven Sicherheitsanalysen (z.B. Penetrationstests, Monitoring, Netzwerkscans) vor deren Durchführung ab.

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 Fernzugriff

Verwendete Fernzugriffslösungen entsprechen dem vereinbarten Stand der Technik.

Der Auftragnehmer stellt u.a. folgende Informationen zur Verfügung und hält diese über die Vertragslaufzeit aktuell:

- Zweck und konkrete Ausführung,
- Standorte und Identitäten,
- Vorgehen zu Installation, Konfiguration, Betrieb und Beendigung.

Verbindungen sind einzeln vom Auftraggeber zu genehmigen. Es gelten die vereinbarten Regelungen zu Verschlüsselung und Authentifizierung.

5.30 Schutz vor Schadsoftware

Der Auftragnehmer stellt dem Auftraggeber ein Konzept zum Schutz des IT-/OT-Systems gegen Schadsoftware zur Verfügung. Betreibt der AN das System im Auftrag des AG, verantwortet er in Abstimmung mit dem AG dessen Umsetzung.

Das Konzept beinhaltet u.a.:

- Dokumentation zur Installation, Betrieb und Aktualisierung der Schutzlösung,
- Anforderungen zum Monitoring des Betriebsstatus inklusive Aktualität der Definitionsdateien (Signaturen),
- mögliche Workarounds bis zur Bereitstellung einer Aktualisierung des Schutzmechanismus,
- Nachweis der korrekten Funktion des Schutzmechanismus,
- Zeiten bis zur Bereitstellung aktualisierter Definitionsdateien.

5.31 Außerbetriebsetzung

Der Auftragnehmer stellt dem Auftraggeber ein Konzept zur Außerbetriebsetzung des IT-/OT-Produkts zur Verfügung. Dies beinhaltet insbesondere die notwendigen Schritte zur Löschung der gespeicherten Daten, kryptographischem Material und Gerätekonfigurationen.