Teil C Anlage 5 EVB-IT Vertrag Anlage 5_13: Zusätzliche Anforderungen für Dienstleistercluster „DL02 (IKT-) Softwareentwicklung"

Die folgenden Dienstleistungen sind dem Dienstleistercluster DL02 zugeordnet

- IKT-Entwicklung
- Softwareentwicklung

1 Einleitung

Folgende Anforderungen gelten für externe Softwareentwicklungen, die außerhalb der ILB stattfinden.

2 Generelle Sicherheitsthemen

2.1 Softwareentwicklung

1. Physische und logische Trennung: Entwicklungs-, Test- und Produktionsumgebungen sind physisch und/oder logisch voneinander zu trennen, um unbefugte Zugriffe und ungewollte Interaktionen zwischen den Umgebungen zu verhindern.
2. Zugangskontrolle: Der Zugang zu den jeweiligen Umgebungen ist strikt zu regeln. Nur autorisierte Personen dürfen Zugriff auf die Entwicklungs- und Testumgebungen haben. Der Zugang zur Produktionsumgebung ist auf ein Minimum zu beschränken.
3. Daten- und Konfigurationsmanagement: Es ist sicherzustellen, dass in den Entwicklungs- und Testumgebungen keine echten Produktionsdaten verwendet werden. Testdaten müssen anonymisiert, pseudonymisiert, randomisiert oder synthetisch erzeugt werden, um Datenschutzverletzungen zu vermeiden. Die Integrität und Vertraulichkeit von Daten in Nichtproduktionsunternehmen sind zu schützen.
4. In Ausnahmefällen können für bestimmte Verfahren Produktionsdaten für Testanlässe, über einen begrenzten Zeitraum und nach Genehmigung der ILB, gespeichert werden. Die folgenden Anforderungen sind zum Schutz betrieblicher Daten bei deren Nutzung für Prüfzwecke anzuwenden:
   - Wenn auf produktionsnahen Testsystemen produktionsnahe Daten zur Verfügung gestellt werden, sind die Berechtigungen wie im Produktivsystem zu vergeben.
   - Es hat jedes Mal eine separate Berechtigung zu erfolgen, wenn Betriebsinformationen in eine Testumgebung kopiert werden.
   - Nach Abschluss der Überprüfung sind die Betriebsinformationen aus der Testumgebung zu löschen.
   - Das Kopieren und die Verwendung von Betriebsinformationen ist zu protokollieren, sodass ein Prüfpfad existiert.
5. IT-Changemanagement: Änderungen an Systemen und Anwendungen dürfen nur nach erfolgreicher Prüfung in der Testumgebung und einer formalen Genehmigung in die Produktionsumgebung überführt werden. Ein Dokumentationsprozess ist erforderlich, um die Nachverfolgbarkeit von Änderungen sicherzustellen.
6. Sicherheitsmaßnahmen: Sicherheitsmaßnahmen, die in der Produktionsumgebung implementiert sind, müssen auch in Entwicklungs- und Testumgebungen berücksichtigt werden, um eine konsistente Sicherheitsarchitektur zu gewährleisten.
7. Überwachung und Protokollierung: Alle Zugriffe und Änderungen in den Umgebungen sind zu überwachen und zu protokollieren, um die Einhaltung der Sicherheitsrichtlinien und -verfahren zu gewährleisten.
8. Es sind Maßnahmen zu treffen, die das Risiko einer unbeabsichtigten Veränderung oder einer vorsätzlichen Manipulation der IKT-Systeme während der Entwicklung, Wartung und Einführung in die Produktionsumgebung mindern.

9. Es sind die erforderlichen Tests bei der Entwicklung, vor der Freigabe für den Produktivbetrieb sowie im Zuge des Patch- und Änderungsmanagements durchzuführen und zu dokumentieren.
10. Der Dienstleister muss sicherstellen, dass der Quellcode in einem Versionssystem verwaltetet wird und er vor unbefugtem Zugriff geschützt ist.
11. Software-Änderungen sind in der Programm-Source-Datei wie folgt zu dokumentieren:
    - Die letzte Änderung ist immer in der Dokumentationsreihenfolge als Erstes aufzuführen
    - Änderungsdatum
    - Angefordert von
    - Änderungsgrund
    - Änderungsbeschreibung (angemessen aussagekräftig)
12. Alle auftretenden Fehler oder Normabweichungen sind per Logging-Mechanismus zu protokollieren.
13. Verwendete Codierungssprachen und Entwicklungstools weisen ggf. Schwachstellen auf und erfordern Maßnahmen zur „Härtung“. Diese müssen vom Dienstleister identifiziert, vereinbart und befolgt werden.
14. Um eine gute Wartbarkeit und Lesbarkeit zu gewährleisten, müssen die Programme folgende Eigenschaften besitzen:
    - Zu Programmbeginn muss zusätzlich zur definierten Dokumentation eine Auflistung der beteiligten Ressourcen und externen Schnittstellen vorliegen.
    - Redundante Codestellen sind zu vermeiden, stattdessen sind diese als Funktion auszulagern.
    - Wiederkehrende Funktionen sind in separaten Klassen auszulagern, um deren Wiederverwendbarkeit zu gewährleisten.
    - Festcodierte Parameter sollten vermieden werden. Diese sind in Konfigurationsdateien oder (SQL-)Datenspeicher auszulagern.
    - Keine Codierung von Benutzerdaten und/oder Kennwörtern.
15. Der Dienstleister stellt sicher, dass eine Quellcodeprüfung stattfindet. Identifizierte Schwachstellen und Anomalien im Quellcode sind priorisiert zu beheben. Nach der Umsetzung der Maßnahmen sollte eine erneute Überprüfung durchgeführt werden, um die Wirksamkeit der Behebungsmaßnahmen sicherzustellen.

2.2 Kontrollrecht

ab Schutzbedarf „hoch“

1. Der Dienstleister informiert den Auftraggeber unverzüglich, mindestens in Textform, über wesentliche Feststellungen bei vertragserheblichen Audits, sowie bei vertragsrelevanten entzogenen Zertifikaten und Testaten.
2. Der Dienstleister hat bei Bekanntwerden von unzureichend erfüllten Sicherheitsanforderungen, zum Beispiel aufgrund von allgemeiner Risikoidentifizierung, veränderter Gefährdungs- oder Gesetzeslage, Nachbesserungen zu vollziehen.
3. Der Dienstleister verpflichtet sich, berechtigten Beschäftigten der ILB oder von der ILB beauftragten Prüfern zur Überprüfung der Entwicklungsprozesse und Maßnahmen.

2.3 IKT-Vorfallmanagement

1. Der Dienstleister etabliert einen internen Prozess zur Identifizierung, Eindämmung, Beseitigung und Bewertung von Sicherheitsvorfällen.
2. Über eine geeignete Meldekette ist sicherzustellen, dass alle erforderlichen Stellen schnellstmöglich in die Behandlung der Sicherheitsvorfälle geeignet eingebunden werden. Die relevanten Rollen sind in einer Kommunikations- und Eskalationsmatrix zu dokumentieren.
3. Alle relevanten Ereignisse, Entscheidungen und Handlungen sind nachvollziehbar zu dokumentieren.
4. Im Nachgang ist zu allen Sicherheitsvorfällen eine Ursachenanalyse zu erstellen. Etwaige Maßnahmen zur Vermeidung zukünftiger Sicherheitsvorfälle oder Verbesserung der Sicherheitsvorfallbehandlung sind nachzuhalten.
5. Durch regelmäßige Übungen stellt der Dienstleister sicher, dass die etablierten Maßnahmen zur Sicherheitsvorfallbehandlung den Erwartungen entsprechend funktionieren.
6. Der Dienstleister informiert die ILB umgehend, sobald potenzielle Sicherheitsvorfälle gemeldet werden, die die Informationssicherheit der ILB beinträchtigen könnten und stellt der ILB alle relevanten Unterlagen zur Verfügung.
7. Der Dienstleister hat standardisierte Protokolle und Berichte zur Meldung von Sicherheitsvorfällen zu etablieren.
8. Für Erst-, Folge- und Erledigungsmeldungen zu Informationssicherheitsvorfällen gelten folgende formalen Anforderungen:
   - Kurzbeschreibung
   - Betroffener Service
   - Bearbeitungsstatus
   - Detailbeschreibung
   - Betroffenes Schutzziel
   - Ursachenbeschreibung
   - Eingeleitete Sofortmaßnahmen
   - Lessons Learned

2.4 Personalsicherheit

1. Der Dienstleister verpflichtet seine Mitarbeitende zur Einhaltung der Vertraulichkeitspflichten und zur Bewahrung etwaiger Geschäftsgeheimnisse während und nach der Durchführung von Aufgaben für die ILB.
2. Der Dienstleister muss einen Ansprechpartner benennen, der für alle Fragen der Einbindung bei der ILB aussagefähig ist und bei Bedarf Aktionen zur Sicherstellung der sicheren Einbindung initiieren kann.
3. Die Beschäftigten des Dienstleisters müssen schriftlich verpflichtet werden, einschlägige Gesetze, Vorschriften sowie die Regelungen der ILB einzuhalten.

ab Schutzbedarf „hoch“

4. Der Dienstleister stellt sicher, dass die Beschäftigten geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit unterrichtet wurden.
5. Der Dienstleister stellt sicher, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird.

2.5 Berechtigungsmanagement

1. In Abstimmung mit der ILB muss geklärt werden, welche Berechtigungen durch den Dienstleister und welche durch die ILB vergeben werden. Für alle Berechtigungen, die der Dienstleister selbst vergibt, muss dieser ein Berechtigungskonzept auf der Basis von Rollen erstellen. Für jede Rolle sind die erforderlichen Rechte, eine kurze Beschreibung und etwaige Ausschlüsse mit anderen Rollen zu dokumentieren. Es dürfen nur Berechtigungen auf der Basis dieser Berechtigungskonzepte vergeben werden.
2. Jede durch den Dienstleister vergebene Berechtigung ist zu dokumentieren.
3. Das Berechtigungskonzept des Dienstleisters sowie die vergebenen Berechtigungen sind halbjährlich vom Dienstleister zu prüfen.

ab Schutzbedarf „hoch“

4. Für besonders schutzbedürftige Informationen erfolgt eine Vergabe einer Berechtigung nur nach Freigabe durch die ILB.
5. Die Gültigkeit der Berechtigungen ist monatlich vom Dienstleister zu prüfen.

2.6 Mandantentrennung

1. Der Dienstleister muss durch Mandantentrennung sicherstellen, dass die Daten und Verarbeitungskontexte der ILB ausreichend sicher von anderen Mandanten getrennt sind.
2. Der Dienstleister hat dies in einem Mandantentrennungskonzept zu dokumentieren.
3. Das Mandantentrennungskonzept muss zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterscheiden und darlegen, mit welchen Mechanismen der Dienstleister diese trennt.

ab Schutzbedarf „hoch“

4. Die Dienste für die ILB werden auf gesonderten Instanzen bereitgestellt. Der Netzverkehr wird durch eine geeignete Netzsegmentierung von anderen Kunden getrennt.

2.7 Ordnungsgemäße IT-Administration

1. Der IT-Betrieb des Dienstleisters erfolgt auf der Basis von dokumentierten IT-Betriebsprozessen. Alle Entscheidungen und Handlungen im Rahmen dieser Prozesse müssen nachvollziehbar dokumentiert werden.
2. Alle Änderungen an den Anwendungen, IT-Systemen und Kommunikationsverbindungen, die Einfluss auf die Bereitstellung der Dienst für die ILB haben könnten, sind im Rahmen eines Änderungsmanagements (Change-Managements) zu planen, zu testen, freizugeben und umzusetzen. Für jede Änderung müssen geeignete Maßnahmen zur Wiederherstellung des vorigen Zustands dokumentiert werden (Fallback-Lösung). Alle Störungen und sonstigen Vorfälle müssen im Rahmen eines Vorfalls-Management (Incident Management) dokumentiert, bewertet und behandelt werden.

ab Schutzbedarf „hoch“

3. Der Dienstleister etabliert einen Betriebsprozess zu langfristigen Lösungen von Problemen (Problem Management).
4. Die Dokumentation der einzelnen IT-Prozesse erfolgt in geeigneten Softwarelösungen (z. B. Ticket-Systemen).
5. Die IT-Komponenten werden in einer CMDB verwaltet.

2.8 Schwachstellenmanagement

1. Der Dienstleister stellt für alle Komponenten, die für die Bereitstellung der Dienste für die ILB notwendig sind, sicher, dass Quellen zur Beschaffung von Informationen über Schwachstellen dokumentiert sind (z. B. Herstellerseiten, CERTs, Newsletter, Nachrichtenseiten etc.) und regelmäßig bzw. anlassbezogen in Bezug auf Schwachstellen ausgewertet werden.
2. Alle gemeldeten Schwachstellen werden durch den Dienstleister dokumentiert und im Hinblick auf ihre potenziellen Auswirkungen bewertet. Der Dienstleister leitet bei Bedarf Gegenmaßnahmen ein.
3. Der Dienstleister informiert die ILB umgehend über die gemeldeten Schwachstellen und seine Einschätzung über die Auswirkungen.

ab Schutzbedarf „hoch“

4. Der Dienstleister führt mindestens einmal monatlich automatisierte Schwachstellenscans gegen die für die Bereitstellung der Dienste der ILB notwendigen IT-Systeme und Anwendungen durch.
5. Der Dienstleister führt mindestens einmal jährlich einen Penetrationstest gegen die für die Bereitstellung der Dienste der ILB notwendigen IT-Systeme und Anwendungen in Abstimmung mit der ILB durch.

2.9 Patchmanagement

1. Der Dienstleister etabliert einen Prozess zur Ermittlung von Updates für alle eingesetzten Anwendungen, Betriebssysteme und Firmwares. Er bewertet alle gemeldeten Updates im Hinblick auf etwaige Auswirkungen auf die Sicherheit und den Betrieb der Dienste für die ILB. Auf Basis dieser Einstufung entscheidet er, wie diese Updates eingespielt werden sollen.
2. Alle Patches sind im Rahmen des Änderungsmanagements auf getrennten Systemen umfassend zu testen, bevor sie auf Produktivsystemen aufgespielt werden.
3. Im Falle unmittelbarer Gefahren für die betroffenen Anwendungen, Betriebssysteme und Firmwares ist ein Verfahren für ein sicheres beschleunigtes Einspielen der Patches zu definieren.

2.10 Systemhärtung

1. Alle IT-Systeme müssen so konfiguriert werden, dass keine nicht benötigten Dienste oder Anwendungen laufen.

2.11 Schutz vor Schadprogrammen

1. Der Dienstleister stellt auf allen Systemen, bei denen es eine realistische Chance für einen Befall durch Schadsoftware gibt oder die Daten mit verwundbaren Systemen austauschen, einen Schutz vor Schadsoftware sicher. Dieser Schutz bietet Virenschutz auf allen Systemen, die angreifbar für Schadsoftware sind oder Daten mit angreifbaren Systemen austauschen.
2. Jede Datei, die auf dieses System übertragen wird, muss durch einen On-Access-Scanner sofort untersucht werden.
3. Zusätzlich sind regelmäßig bzw. mindestens wöchentlich Scans aller gespeicherten Daten durchzuführen.
4. Die Muster für die Schadprogrammerkennung sind nach den Vorgaben des Herstellers zu aktualisieren.

ab Schutzbedarf „hoch“

5. Der für die ILB relevante Netzverkehr muss auf Schadsoftware hin untersucht werden.
6. Alle Meldungen über erkannte Schadsoftware auf IT-Systemen und Anwendungen, die für die Entwicklung bzw. Bereitstellung der ILB-Software benötigt werden, sind an die ILB zu übermitteln.

2.12 Kryptokonzept

1. Der Dienstleister stellt mindestens einmal jährlich oder ggf. bei neuen Erkenntnissen zu den kryptografischen Verfahren sicher, dass die verwendeten Verfahren und Schlüssellängen den offiziellen Empfehlungen gemäß BSI TR-02102-1 entsprechen.
2. Alle eingesetzten kryptografischen Verfahren, die nicht den offiziellen Empfehlungen entsprechen sind an die ILB zu melden.
3. Der Dienstleister stellt sicher, dass die Vorgaben zur sicheren Erzeugung, Übermittlung, Speicherung, Wechsel und Vernichtung von kryptografischen Schlüsseln definiert und umgesetzt werden.

2.13 Löschung und Vernichtung

1. Es muss festgelegt werden, wie alle Informationen, Daten und ggf. Hardware der ILB vom Dienstleister zurückgegeben werden.
2. Im Falle einer Beendigung des Vertrages muss der Dienstleister sicherstellen, dass alle Daten der ILB vernichtet oder an die ILB zurückgegeben werden. Hierbei sind gesetzliche Vorgaben zur Aufbewahrung von Daten zu beachten.

ab Schutzbedarf „hoch“

3. Alle Datenträger, die Daten der ILB enthalten und nicht mehr benötigt werden oder defekt sind, sind durch den Dienstleister angemessen zu vernichten. Die ILB erhält entsprechende Nachweise der Vernichtung.

2.14 Physische Sicherheit

1. Der Dienstleister stellt durch Zutrittsbeschränkungen sicher, dass keine Unbefugten Zutritt zu den IT-Systemen, worauf Daten der ILB verarbeitet bzw. gespeichert werden, erhalten können.

2.15 Berücksichtigung der Gefährdungs- und Gesetzeslage

ab Schutzbedarf „hoch“

1. Die vereinbarten Sicherheitsanforderungen müssen bei Änderung der Gefährdungslage für die Technik sowie bei Änderung der Gesetzeslage für die erbrachte Dienstleistung durch den Dienstleister nachgebessert werden.