Security Service Level Agreement - Teil B

Zusätzliche Maßnahmen für den grundschutzkonformen Betrieb der Online-Service-Infrastruktur Plattform (OSI)

für

Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung des Landes SH
ZIT SH
Niemannsweg 220

24106 Kiel

nachfolgend Auftraggeber

Stand: 29.06.2021

Inhaltsverzeichnis

1. Einleitung

Gegenstand

Gegenstand des Security Service Level Agreements (SSLA) Teil B ist die Festlegung von zusätzlichen Sicherheitsmaßnahmen, die über den im SSLA Teil A vereinbarten Maßnahmenumfang hinausgehen.

Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Leistungsumfang und -beschreibung (Kapitel 2): Inhaltliche Beschreibung der vom Auftragnehmer bereitgestellten Leistungen.

Auflistung der ergänzenden Sicherheitsmaßnahmen (Kapitel 3**)**: Liste der zusätzlichen Sicherheitsmaßnahmen einschl. Kurzbeschreibung.

2. Leistungsumfang und -beschreibung

Der Auftragnehmer verpflichtet sich, die unter Kapitel 3 **‚Zusätzliche Sicherheitsmaßnahmen**‘ aufgeführten zusätzlichen Sicherheitsmaßnahmen zusätzlich zu den im SSLA Teil A vereinbarten Maßnahmen umzusetzen.

Die Umsetzung, Dokumentation und regelmäßige Überprüfung dieser Maßnahmen erfolgt durch den Auftragnehmer. Die im SSLA Teil A festgelegten Rahmenbedingungen (Dokumentation, Leistungserbringung, Leistungsvoraussetzungen, etc.) gelten analog.

Der Auftragnehmer kann auf die Mitwirkung des Auftraggebers oder von diesem beauftragten Dritten angewiesen sein. Dies ist beispielsweise der Fall, wenn Maßnahmen nicht oder nicht vollständig im Verantwortungsbereich des Auftragnehmers liegen oder Maßnahmen durch den Auftragnehmer alleine nicht umgesetzt werden können. Die erforderliche Mitwirkung ist durch den Auftraggeber sicherzustellen.

3. Zusätzliche Sicherheitsmaßnahmen

3.1 Maßnahmen zur Systemüberwachung, Systemlastmessung und Alarmierung

Begründung:

Diese Maßnahme verringert die Eintrittswahrscheinlichkeit der Gefahren G 0.14, G0.19, G 0.22, G 0.23, G 0.25, G 0.27, G 0.28, G 0.38, G 0.39, G 0.46, G 0.47.

Umsetzung:

Mithilfe o. g. Maßnahmen können u.a. Performanceprobleme als auch andere Risiken von intern und extern frühzeitig erkannt und rechtzeitig darauf reagieren werden. Mögliche schädigende Ereignissen können somit abgemildert oder gänzlich vermieden werden.

3.2 Erarbeitung einer sicheren Verfahrensarchitektur

Begründung:

Diese Maßnahme wirkt gegen die Gefährdungen G 0.14, G 0.19, G 0.23, G 0.27, G 0.46

Umsetzung:

Eine sichere Verfahrensinfrastruktur, getragen u.a. durch ALGs, minimiert Risiken wie SQL-Injection, etc..

3.3 Verschlüsselung der Datenübermittlung über das Internet

Begründung:

Die Nutzung der TLS-Verschlüsselung verringert die Eintrittswahrscheinlichkeit und die Auswirkungen von G 0.14, G 0.15, G 0.19, G 0.23, G 0.38, G 0.46.

Umsetzung:

Diese Maßnahme beschreibt die Absicherung des Datentransfers und den Zugriff auf Daten außerhalb der Anwendung. Für den verschlüsselten Filetransfer stehen einige Techniken zur Verfügung, die auch Mechanismen zur Verifikation der Kommunikationspartner bieten. Weiterhin werden Kommunikationspartner mit HTTPS-Verschlüsselung, Kleopatra-Verschlüsselung oder über VPN beliefert.

3.4 3-Tier System

Begründung:

Diese Maßnahme wirkt gegen die Gefährdung G 0.19 (Offenlegung schützenswerter Informationen).

Umsetzung:

Eine strikte Trennung von Eingabe- / Presentationlayer – Applicationlayer – Datalayer steigert den Schutz gespeicherter Informationen und die Stabilität der Systeme.

3.5 Erstellung und Umsetzung eines Redundanzkonzeptes

Begründung:

Diese Maßnahme verringert die Eintrittswahrscheinlichkeit und die Auswirkungen von G 0.25.

Umsetzung:

Die Erarbeitung und Umsetzung eines Redundanzkonzepts erhöht und gewährleistet die Verfügbarkeit der Onlineservices, die OSI als Plattform und Environment-System benötigen.
OSI wurde redundant aufgebaut.

3.6 Verifikation von Nutzereingaben

Begründung:

Diese Maßnahme verringert die Eintrittswahrscheinlichkeit von G 0.46.

Umsetzung:

Wo es Services erfordern, werden durch Nutzer eingegebene Daten u.a. auf Integrität, Plausibilität geprüft.

3.7 Test- und Deployment Konzept

Begründung:

Diese Maßnahme verringert die Eintrittswahrscheinlichkeit von G 0.28.

Umsetzung:

Für OSI ist eine Testumgebung aufgebaut, auf der Server und Applications getestet und festgestellte Mängel behoben werden, bevor diese auf dem Production-System deployed werden.

3.8 AV-Konzept

Begründung:

Diese Maßnahme verringert die Eintrittswahrscheinlichkeit von G 0.39.

Umsetzung:

Der AV-Scan ist über die Basisdiente abgedeckt.

3.9 Authentifizierungskonzept

Begründung:

Diese Maßnahme verringert die Eintrittswahrscheinlichkeit von G 0.23 und G 0.38.

Umsetzung:

Die Erarbeitung und Implementierung einer Authentifizierung, die an den Anforderungen orientiert ist, die sich aus der Art, den Umfang und der Sensitivität der zu verarbeitenden Daten ergibt, minimiert Risiken und Schadensmöglichkeiten.

4. Mitwirkungen

Der Auftraggeber stellt dem Auftragnehmer eine aussagekräftige Beschreibung der zusätzlichen Maßnahmen bereit, die vom Auftragnehmer umzusetzenden sind. Der Auftraggeber unterstützt bei der Klärung von Fragen bzgl. der entsprechenden Maßnahmen die sich im Rahmen der Umsetzung ergeben. Sofern Maßnahmen kooperativ umgesetzt werden müssen, unterstützt der Auftraggeber den Auftragnehmer bei der Maßnahmenumsetzung.

Es gelten ferner die im SSLA Teil A genannten Mitwirkungspflichten.