

Leistungsbeschreibung Beratungsleistung Informationssicherheit ÖPNV

Einführung von Systemen zur Angriffserkennung

1 Leistungsgegenstand

Der Auftragnehmer erbringt Beratungs- und Unterstützungsleistungen mit Schwerpunkt auf Systeme zur Angriffserkennung im IT-/OT-Umfeld des betrieblich-technischen Bereiches der HOCHBAHN.

1.1 Einarbeitung

- Aufbau und Struktur des ISMS
- Richtlinien und Prozesse im Kontext der Systeme zur Angriffserkennung
- Aufbau und Struktur der betrieblich-technischen IT-/OT Systemlandschaften
- organisatorische Strukturen der HOCHBAHN-Technik
- Verantwortlichkeiten und Prozesse der HOCHBAHN-Technik
- informationssicherheitstechnische Besonderheiten der Abteilung Zugsicherungs- und Kommunikationsanlagen
- bestehende Umsetzung der Systeme zur Angriffserkennung

1.2 Strategische/organisatorische Unterstützung für den Aufbau von Systemen zur Angriffserkennung

- Umsetzung und Etablierung der Anforderungen aus der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ des BSI
- Integration der Systeme zur Angriffserkennung in bestehende ISMS-Strukturen
- Entwicklung und Bewertung von KPIs zur Messung der Wirksamkeit der Systeme zur Angriffserkennung
- Unterstützung bei Aufbau und Weiterentwicklung von:
 - Protokollierungs- und Logging-Konzepten
 - Use Cases auf Basis von Angriffsszenarien
 - Alarmierungs- und Reaktionsprozesse
 - Security Operations Center (SOC) Strukturen
 - Vorfallsmanagementprozesse gemäß ISO 27035
 - SLA/OLA für Security-Prozesse
 - Management-Präsentationen und Schulungsunterlagen

1.3 Operative/technische Unterstützung für den Aufbau von Systemen zur Angriffserkennung

- Unterstützung bei der Toolbewertung und -integration (SIEM, EDR, IDS)
- Unterstützung beim technischen Aufbau/ der Weiterentwicklung von:
 - Protokollierungsinfrastruktur
 - Detektionsmechanismen
 - Monitoring
 - Use Case-Management (Erkennungsregeln)
 - Angriffserkennung durch Security Information and Event Management (SIEM)

1.4 Erstellung und Qualitätssicherung von Richtlinien und Prozessen

- Erstellung und Weiterentwicklung audit- und prüfungssicherer Informationssicherheitsrichtlinien
- Unterstützung bei der (Weiter-)Entwicklung von Informationssicherheitsprozessen
- Qualitätssicherung der Richtlinien und Prozesse

2 Anforderungen an den Auftragnehmer

2.1 Anforderungen an das Unternehmen

- Nachweisbare Kompetenz und Erfahrung in der Beratung von Kunden im KRITIS-Umfeld bezogen auf die Themen im Leistungsgegenstand
- Zertifizierung der für den Auftraggeber relevanten Unternehmensbereiche in ISO 27001 o.ä.

2.2 Fachliche Anforderungen an die eingesetzte Person

- Nachweisbare fundierte Kenntnisse in:
 - BSIG und BSI-KritisV
 - BSI Orientierungshilfe Systeme zur Angriffserkennung
 - BSI-Standards (200-X) und Methoden, auch mit RUN und GAI
 - VDV-Schrift 440 und VDV-Mitteilung 4400
- Nachweisbare Kompetenz in der Vorbereitung zur Erbringung von Nachweisen gemäß § 39 BSIG hinsichtlich SzA
- Nachweisbare mehrjährige praktische Erfahrung in:
 - KRITIS-Umfeld im ÖPNV
 - ÖPNV-Branchenkenntnisse
 - SIEM-Lösungen (z. B. Splunk, Sentinel, QRadar etc.), technisch und organisatorisch
 - SOC-Betriebsmodelle
 - OT-Systeme im Umfeld von Zugsicherungs- und Kommunikationsanlagen
 - Erbringung von Nachweisen gegenüber dem BSI
 - Erstellung von Informationssicherheitsrichtlinien im IT- und OT-Bereich
 - Erstellung von Informationssicherheitsprozessen im IT- und OT-Bereich
 - Erstellung revisionssicherer Dokumentation
 - Durchführung von Reifegradanalysen im IT- und OT-Bereich im ÖPNV
- Persönliche Anforderungen
 - sehr gute Deutschkenntnisse (C2)
 - hohe Kommunikations- und Moderationsfähigkeit
 - ausgeprägte Beraterkompetenz und die Fähigkeit, Themen im Unternehmen proaktiv voranzutreiben
 - Möglichkeit, voraussichtlich 2 Personentage pro Quartal vor Ort in Hamburg zu sein

Die Nachweise sind in Form von persönlichen Zertifikaten und individuellen Kundenreferenzen zu erbringen, die dem Angebot beizufügen sind.

3 Zeitlicher Rahmen und Umfang

Die Leistungserbringung erfolgt ab Zuschlagserteilung und endet unter Berücksichtigung möglicher Verlängerungen um zweimal 2 Jahre voraussichtlich im Jahr 2034.

Der Auftraggeber prognostiziert, dass eine Verfügbarkeit der Spezialisten von durchschnittlich insgesamt 1 Personentag in der Woche (Montag bis Freitag) erforderlich sein wird. Davon voraussichtlich durchschnittlich 2 Personentage pro Quartal vor Ort in Hamburg beim Auftraggeber. Ein Personentag entspricht 8 Stunden.

Als prognostiziertes Gesamtvolumen wird ein Bedarf von ca. 350 Personentagen (8 Stunden) geschätzt. Ein Anspruch auf Abruf besteht nicht.