Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Strassen ASTRA
Office fédéral des routes OFROU
Ufficio federale delle strade USTRA

ASTRA Fachtagung - Journée technique OFROU
BSA: Von der Strategie zur Anwendung - EES: De la stratégie à l‘utilisation

Richtlinie 13030 IT-Sicherheit Leit- und Steuersysteme der Betriebs- und Sicherheits-ausrüstungen

21. Januar 2020

Autor: Felix Roth

Inhalte

1. Wieso gibt es diese Richtlinie ?
2. Zweck der Richtlinie
3. Inhalte der Richtlinie
4. Anwendung der Richtlinie in der Praxis
5. Beispiel

1. Wieso gibt es diese Richtlinie 13030?

- BSA werden immer mehr vernetzt
- Anteil IT steigt, IT und BSA nähern sich immer mehr an
- Durchgängige IP-Netze anstelle Feldbusse
- Instrumente und Methoden für die Entwicklung und Betrieb von IT Systemen sind allgemein bekannt und zugänglich

⇒ Gefahren aufgrund Fahrlässigkeit oder Böswilligkeit nehmen zu

⇒ Risiken werden zunehmend unakzeptabler

⇒ Eintrittswahrscheinlich und/oder Ausmass müssen gesenkt werden

2. Zweck der Richtlinie 13030 und Abgrenzungen

- Soll vor Manipulation der BSA schützen:
  - Steuern von BSA
  - Lahmlegen von BSA
  - Verändern oder Diebstahl von Daten
  - Unbeabsichtigte Manipulationen

- Die Richtlinie ist <u>kein</u> IT-Security Konzept
  - Sie definiert jedoch welche Schutzmassnahmen getroffen werden müssen.
  - Die projektspezifische Definitionen und Umsetzung der Massnahmen müssen jeweils erarbeitet werden.

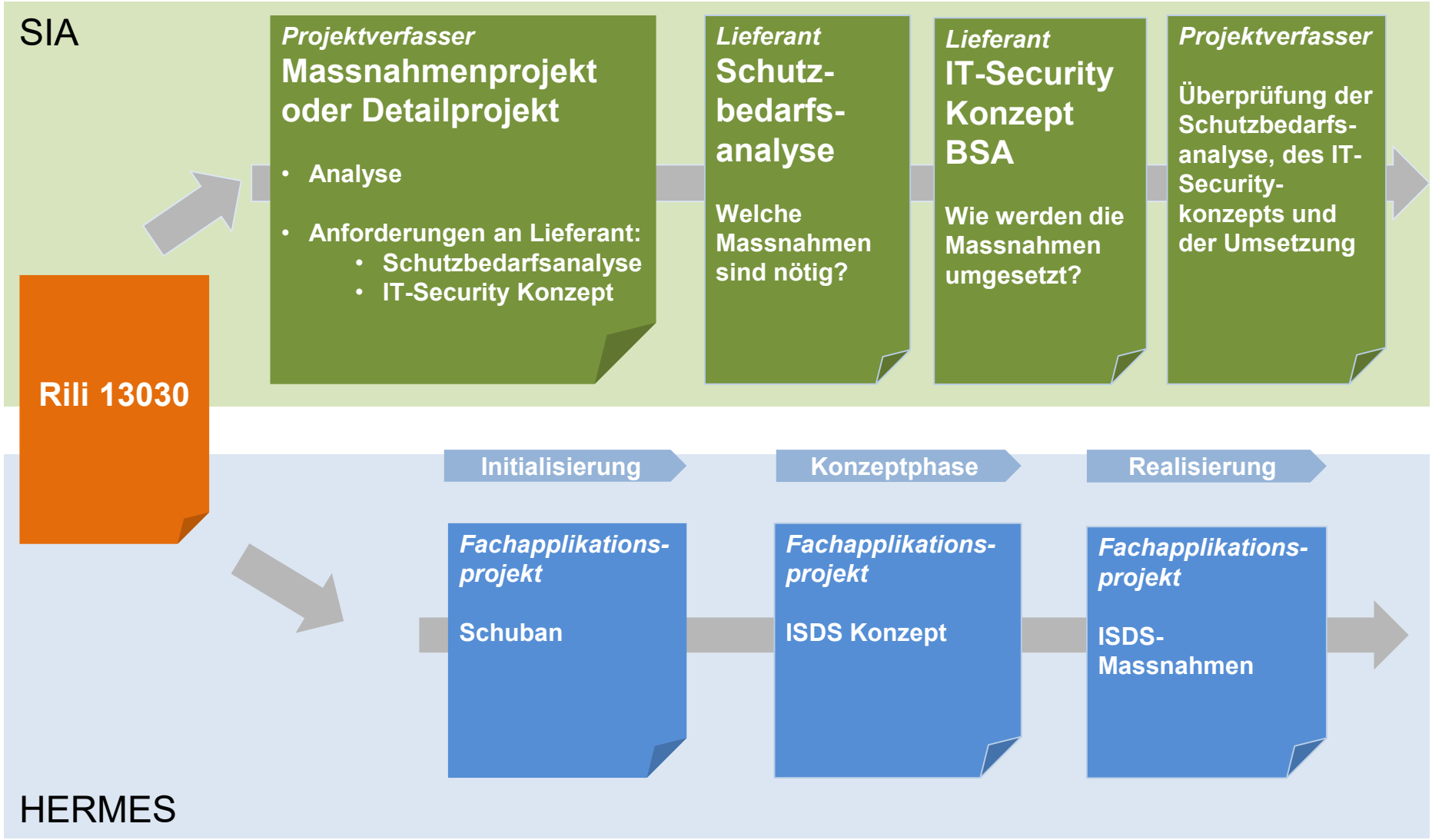
3. Inhalte der Richtlinie 13030

Inhalte der Richtlinie

- Vorgehen in der Anwendung der Richtlinie
- Grundschutz sowie Methode zur Bestimmung des spezifischen Schutzes
- Anforderungen an Zugriffserlaubnis und den Datenschutz
- Passwortverwaltung
- Logischer Aufbau des Netzwerks (z.B. Zonierung)
- Spezifische Massnahmen für eine bestimmte Ausrüstung (mit Beispielen)

=> Projektspezifisches IT-Sicherheits-Konzept erstellt durch das Projekt

4. Anwendung der Rili 13030 in der Praxis



4. Anwendung der Richtlinie in der Praxis

Inhalt Schutzbedarfsanalyse

Vertraulichkeit	Sollen Personendaten nach der Datenschutzgesetzgebung bearbeitet werden?
	Sollen klassifizierte Informationen bearbeitet werden? Wenn ja, welche Klassierungen sind betroffen (intern, vertraulich, geheim)?
	Sollen Informationen oder Daten bearbeitet werden, die aus einem sonstigen Grund (z.B. Amtsgeheimnis geschützt werden müssen? Wenn ja, wie hoch sind die Schutzanforderungen?
Verfügbarkeit	Max zulässige Ausfalldauer? z.B. 2 Stunden, 1 Tag…
	Servicezeiten? 7x24?
	ITSCM / BCM notwendig?
Integrität	Muss die Echtheit, Korrektheit und/oder Unversehrtheit der Daten gewährleistet werden können?
Nachvollzieh-barkeit	Müssen bestimmte Arbeitsvorgänge nachgewiesen werden können?

* IT Service Continuity Management / Business Continuity Management

4. Anwendung der Richtlinie in der Praxis

Inhalt eines IT Security Konzept BSA

- Sicherheitsrelevante Systembeschreibung
  - Ansprechpartner / Verantwortlichkeiten
  - Beschreibung des Gesamtsystems
  - Beschreibung der zu bearbeitenden Daten
  - Architekturskizze / Kommunikationsmatrix
  - Beschreibung der zugrundeliegenden Technik
- Risikoanalyse
- Notfallkonzept
- Einhaltung / Überprüfung der Schutzmassnahmen
- Test / Abnahme der Informationssicherheitsfunktionen

4. Anwendung der Richtlinie in der Praxis

Leitfaden zur Anwendung der Rili 13030

- Ein Leitfaden ist in Planung und wird 2020 erarbeitet
- Er wird helfen die Richtlinie projektspezifisch anzuwenden
- Vorlagen für die Lieferobjekte werden im Leitfaden ebenfalls enthalten sein.

5. Beispiel UeLS

Ebene	Umsetzung UeLS
Physische Zugriffe	Zentralenräume, Zutrittssystem, Schliesskonzepte
Logische Ebene	Umsetzung eIAM Nutzerverwaltung Authentisierung Keine Shared Accounts Passwörter gemäss WIsB Kontrollierter Remote Access über DMZ
Netzwerk Zonierung	Zonierung gemäss Kap.8.2 der Rili
Organisation	Die Aktivitäten der Operatoren und Remote Access werden nachvollziehbar geloggt. Change Management Prozesse werden angewendet.

Was wir nicht wollen….

Besten Dank für Ihre Aufmerksamkeit

Fragen?