Interreg AUSTRIA-HUNGARY Co-funded by the European Union

Trendig Plus
AN INTEGRATED BORDER REGION

Arbeitsblatt Datenschutzrecht und Risikomanagement

Bitte beschreiben Sie Ihr Produkt/Service, insbesondere in Hinblick auf IoT /smarte Aspekte.

1. *Produktbeschreibung, Internetfähigkeit (IoT, smarte Anwendungen):*

_____

_____

2. *Welche personenbezogenen Daten fallen bei der Verwendung des Produkts an?*

_____

_____

_____

3. *Was müssen Sie beachten, um Ihr Produkt/Service datenschutzkonform zu designen, zu produzieren bzw. eine datenschutzkonforme Verwendung sicherzustellen? (Stichworte: Privacy by design / by default)*

_____

_____

_____

4. *Welche Risiken für die Rechte und Freiheiten natürlicher Personen könnte dieses Produkt/Service mit sich bringen? Führen Sie ein Risiko Assessment durch, das folgende Teile enthält:*

4.1 Risikoidentifikation – finden Sie möglichst viele Risiken.
4.2 Risikoanalyse – Analysieren Sie die drei aus Ihrer Sicht wichtigsten Risiken.
4.3 Risikobewertung – Bewerten Sie diese drei wichtigsten Risiken.
4.4 Beschreiben Sie Maßnahmen zur Risikominimierung dieser drei Risiken.

_____

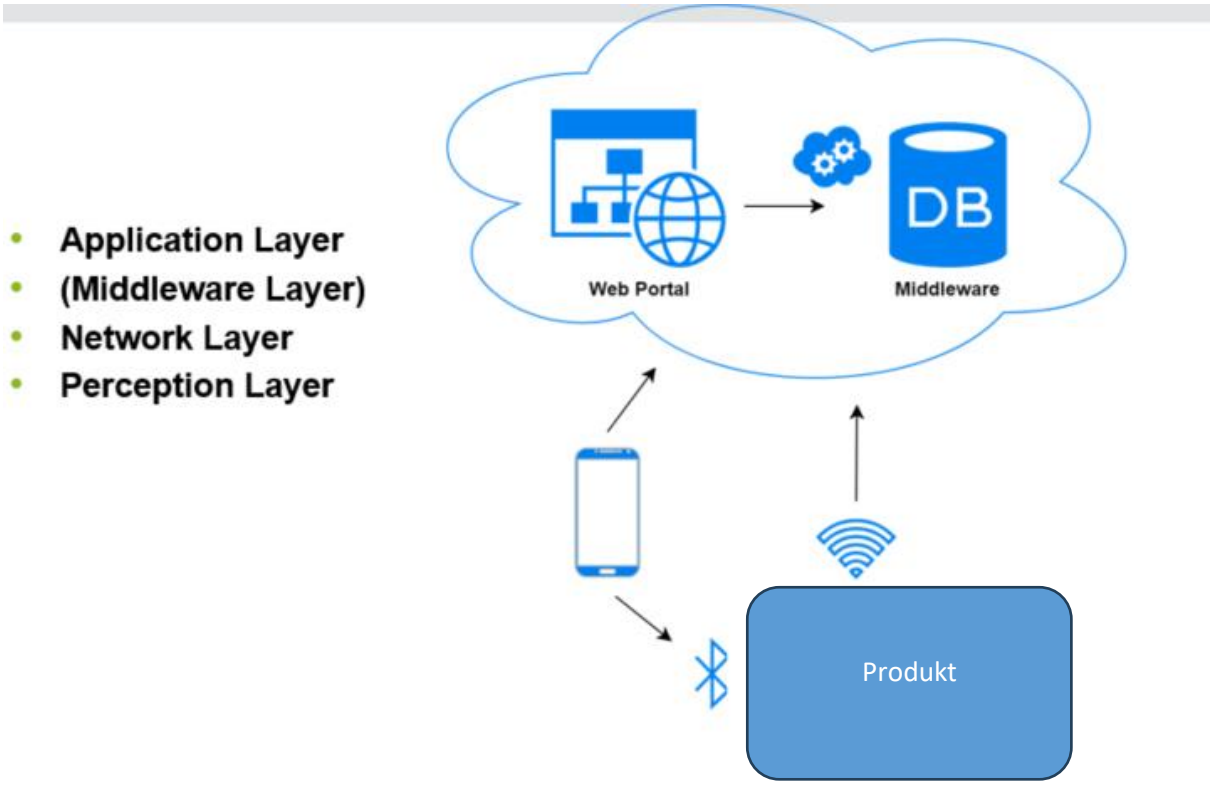
_____

_____

Sabine Proßnegg, FHJ, April 2025

Hilfstabellen:

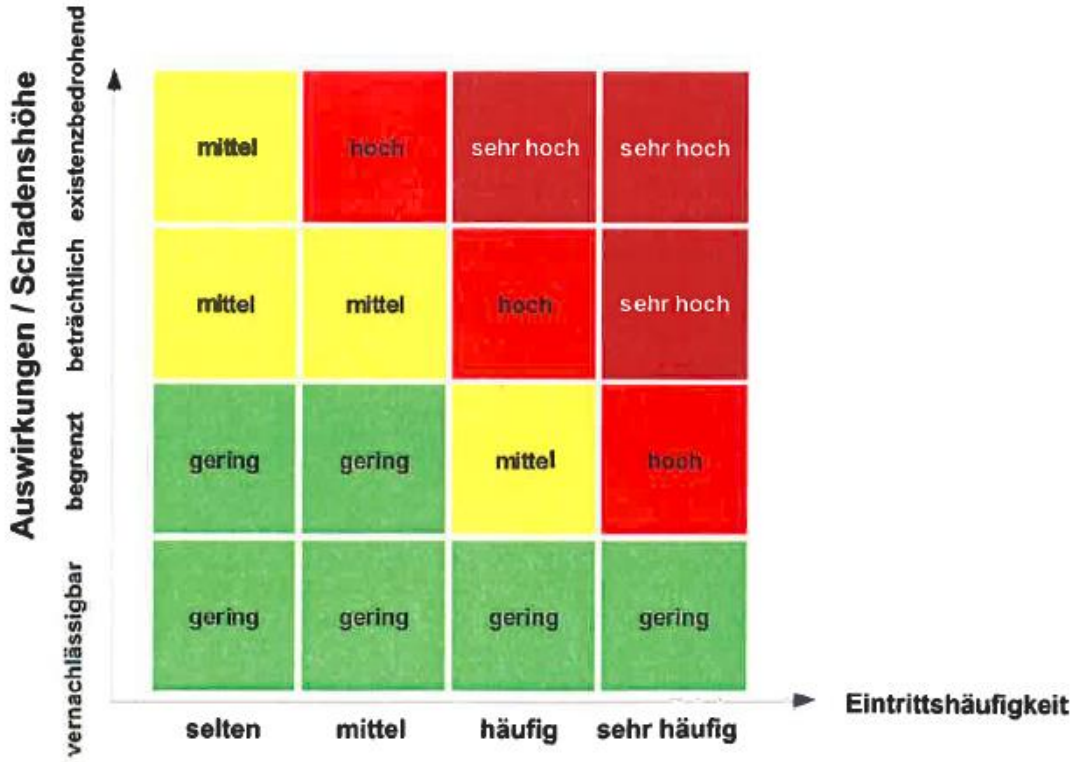
Die IoT Architektur ist wie folgt:



Eintritts-häufigkeit	Beschreibung
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Schadens-höhe	Schadensauswirkungen
vernachläs-sigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar
beträchtlich	Die Schadensauswirkungen können beträchtlich sein
existenz-bedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen

Die Risiken werden nach folgendem Schema klassifiziert



Anhang Elementare Gefährdungen nach BSI Standard 200-3

- G 0.1 Feuer
- G 0.2 Ungünstige klimatische Bedingungen
- G 0.3 Wasser
- G 0.4 Verschmutzung, Staub, Korrosion
- G 0.5 Naturkatastrophen
- G 0.6 Katastrophen im Umfeld
- G 0.7 Großereignisse im Umfeld
- G 0.8 Ausfall oder Störung der Stromversorgung
- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.10 Ausfall oder Störung von Versorgungsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistern
- G 0.12 Elektromagnetische Störstrahlung
- G 0.13 Abfangen kompromittierender Strahlung
- G 0.14 Ausspähen von Informationen / Spionage
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.24 Zerstörung von Geräten oder Datenträgern
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.33 Personalausfall
- G 0.34 Anschlag
- G 0.35 Nötigung, Erpressung oder Korruption
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.39 Schadprogramme
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.41 Sabotage
- G 0.42 Social Engineering
- G 0.43 Einspielen von Nachrichten
- G 0.44 Unbefugtes Eindringen in Räumlichkeiten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen