CISA – Cyber Incident Situational Awareness

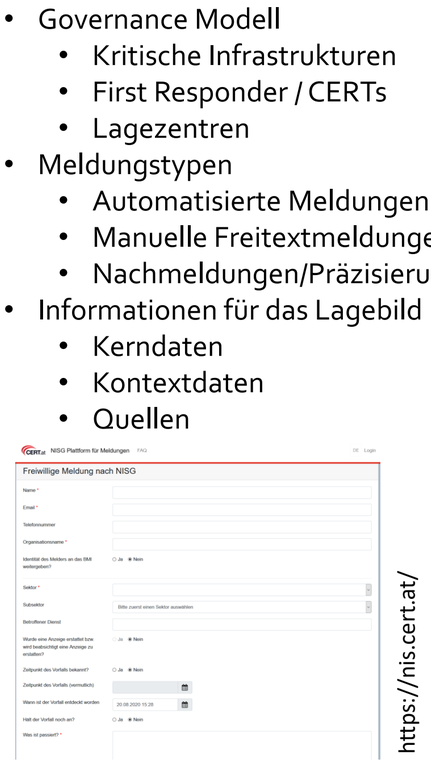
Projektziel

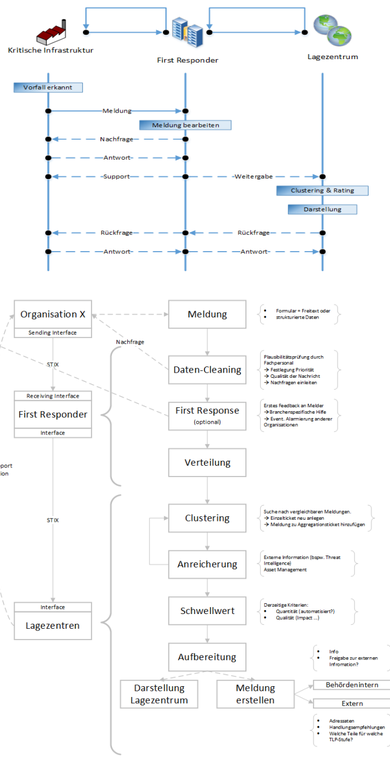
Während technische Lösungen zur Erhebung von Informationen über Cyber-Bedrohungen bereits existieren und auch Prozesse zum Umgang mit Krisensituationen auf staatlicher Ebene vorhanden sind, fehlt ein wichtiges Bindeglied, nämlich die Fragestellung **wie die technischen Informationen aus dem Cyberspace in geeigneter Form aufbereitet und präsentiert werden müssen** – dafür existieren auch international noch keine hinreichend guten Lösungen. Im Projekt CISA soll daher in enger Kooperation mit nationalen Bedarfsträgern der Begriff der Cyber Situational Awareness (**Lageverständnis**) allumfassend (sowohl militärisch als auch zivil) definiert werden, sowie die Erstellungs- und Verwendungsprozesse, unterstützt durch technische Werkzeuge, erarbeitet werden. Durch die Einbindung von österreichischen Rechtsexperten wird die reale Anwendbarkeit der zu erarbeitenden Lösungen sichergestellt. Die erarbeiteten Forschungsergebnisse werden im Rahmen einer Übung (Cyber-Planspiel) evaluiert und bewertet.

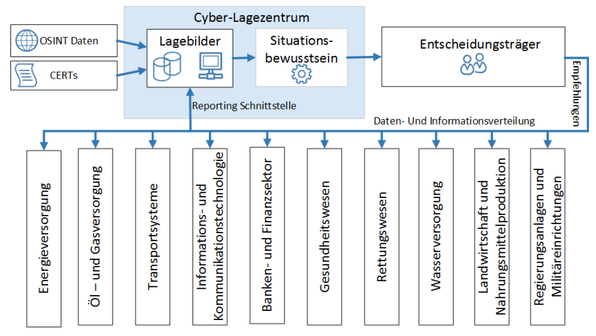
Projektlaufzeit: 01.11.2015 – 30.4.2018

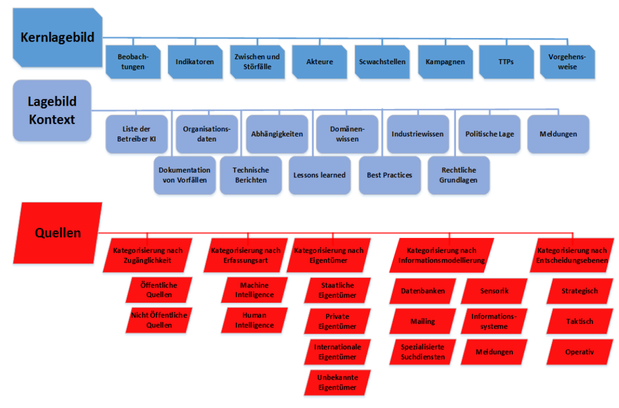
Meldungstypen, Meldewege, Sammelstellen und Lagezentren: Struktur und Daten

- Governance Modell
  - Kritische Infrastrukturen
  - First Responder / CERTs
  - Lagezentren
- Meldungstypen
  - Automatisierte Meldungen
  - Manuelle Freitextmeldungen
  - Nachmeldungen/Präzisierungen
- Informationen für das Lagebild
  - Kerndaten
  - Kontextdaten
  - Quellen



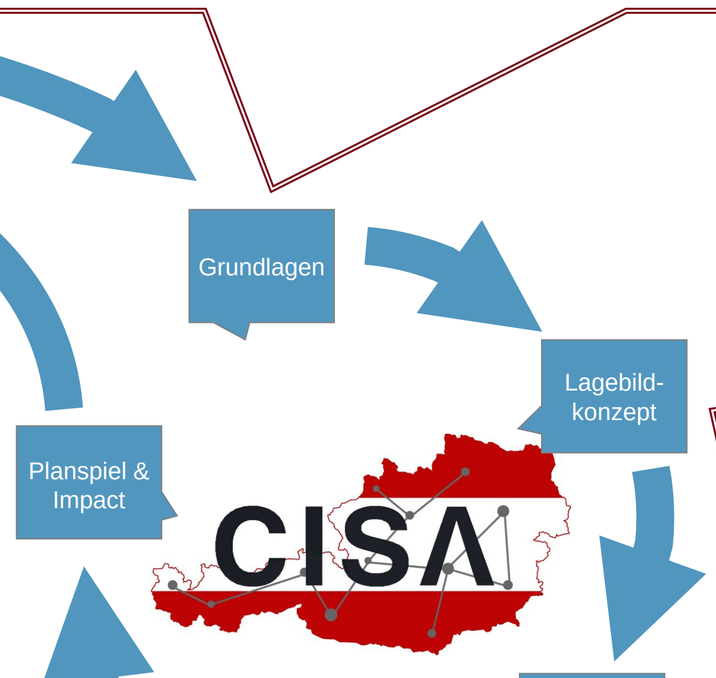






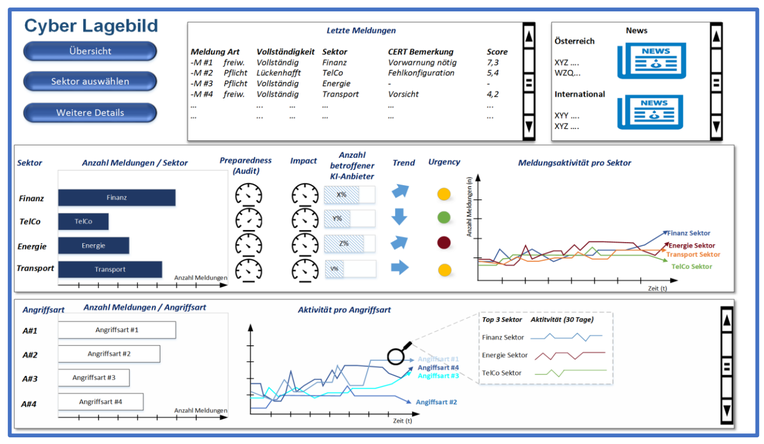
IMPACT

- Prototypische **Implementierung eines Systems** als Vorläufer zu real eingesetzten Meldeplattformen
- Evaluierung eines **Demonstrators** im Zuge eines **Planspiels** mit allen nationalen Security-Stakeholdern
- Erarbeitung von **Konzepte**n und Entwurf von Methoden als **Vorläufer zum NISG**
- **Referenzwerk zum Thema Cyber-Lagebild** im deutschsprachigen Raum



CISA Lagebildkonzept

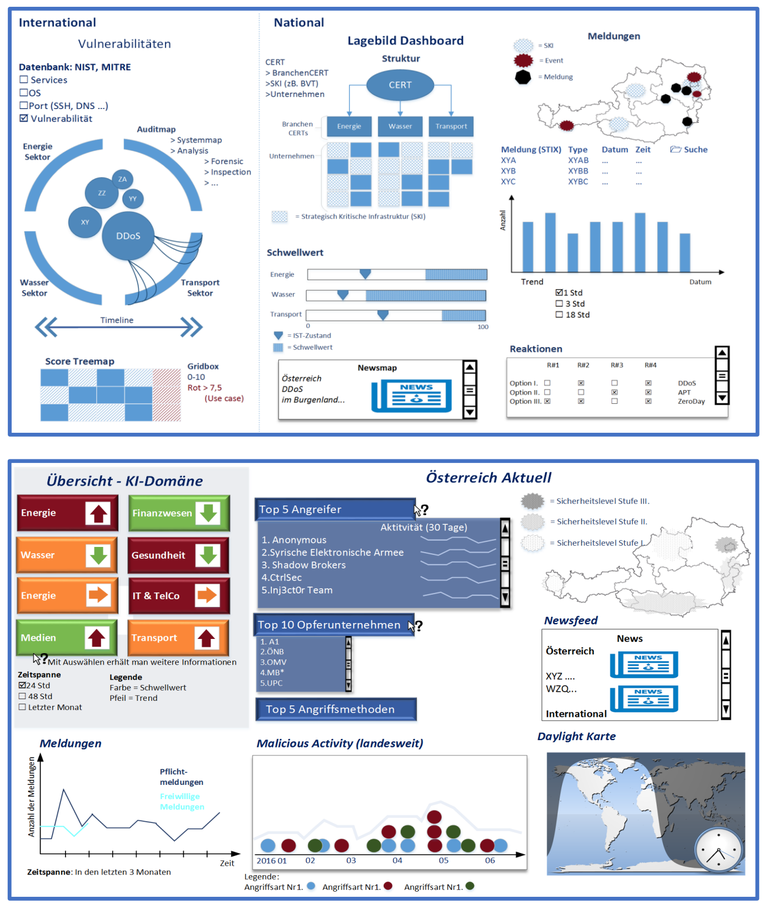
- Umfangreiche Literaturstudie
  - Modelle der Situational Awareness
  - Lagebild-Modelle außerhalb der Cyber-Domäne
  - Cyber-Lagebildkonzepte der jüngeren Vergangenheit
- Erstellung von Stakeholder-spez. Mockups im Zuge von Workshops (siehe Ausschnitte unten)
  - Fokus auf unterschiedliche Ebenen (taktisch, operativ, strategisch)
  - Individuell für unterschiedliche Stakeholder (militärisch, zivil, staatlich, privat)
  - Angepasst für Rollen und deren Verantwortlichkeiten
- **Forschungsfrage: Wie sollen Informationen aufbereitet werden ohne Entscheidungen vorwegzunehmen?**



Einklang mit der geltenden Rechtsordnung und den gesellschaftlichen Wertvorstellungen

Implementierung der Lagebild-Tools

- Web-basiertes System auf Basis von Kibana
- Individuelle Visualisierungsmöglichkeiten auf einem homogenen Datensatz nach Stakeholder-Anforderungen



Gefördert/finanziert durch das Sicherheitsforschungs-Förderungsprogramm KIRAS des Bundesministeriums für Landwirtschaft, Regionen und Tourismus (BMLRT).

Kontakt
Dr. Dr. Florian Skopik
E-Mail: florian.skopik@ait.ac.at
Web: https://www.ait.ac.at/cyber-security/