Bundesministerium
Landwirtschaft, Regionen
und Tourismus

AUSTRIAN INSTITUTE OF TECHNOLOGY

CISA – Cyber Incident Situational Awareness

Florian Skopik, AIT

FFG
Forschung wirkt.

KIRAS
Sicherheitsforschung

DAS PROJEKT CISA

- CISA – Cyber Incident Situational Awareness
- 01.11.2015 – 30.04.2018
- Partner: 10+1
  - Inkl. aller Sicherheitsressorts
- Forschungsgegenstand:
  - Die Erarbeitung und Definition des Begriffs „**Situational Awareness**“ für die Cyber-Domäne
  - auf taktischer, operationeller und strategischer Ebene,
  - und die Untersuchung **wie Entscheidungsfindung** auf diesen Ebenen basierend auf einer umfassenden Situational Awareness **unterstützt** wird,
  - und **welche Informationen** dafür aus den vorhandenen technisch-operativen Datenquellen aufbereitet und dargestellt werden müssen.

AUSTRIAN INSTITUTE OF TECHNOLOGY

SBA Research

INFRA PROTECT

Repuco

THALES

T-Systems

Bundeskanzleramt

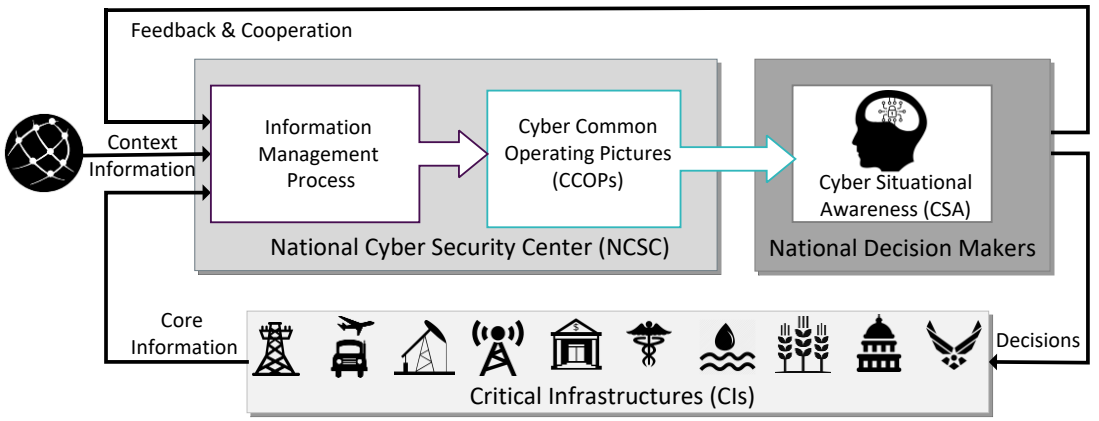
Bundesministerium Landesverteidigung

Bundesministerium Inneres

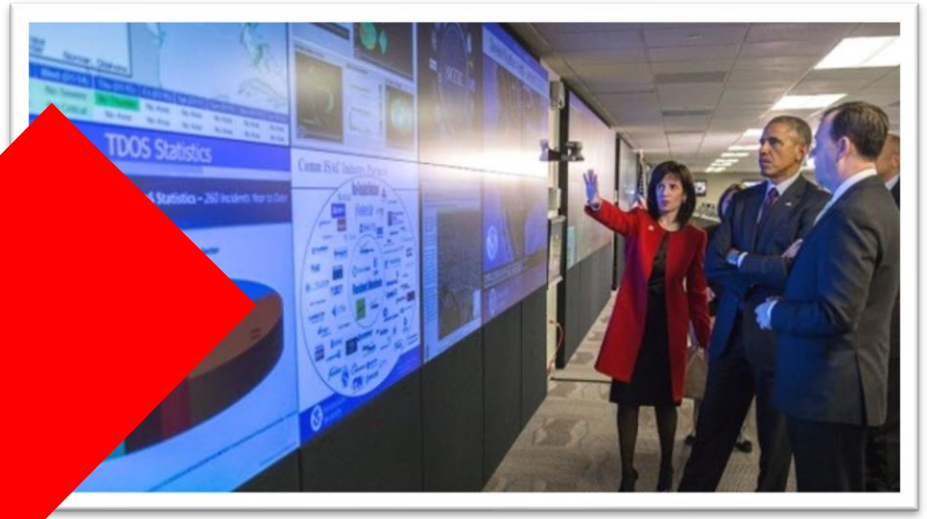
MISSION GOAL

- (staatliche) Cyber-Lagebilder als fundierte **Grundlage zur Entscheidungsfindung**
  - Umgang mit Bedrohungen: Risikobewertung durch Trendanalysen
  - Umgang mit Vorfällen: Bewertung von Handlungsoptionen im konkreten Anlassfall

- CISA ist keine „bottom up magic“!
  - **NICHT**: „Wir sammeln alle Daten, die technisch erhoben werden können und überlegen uns dann, wozu sie genutzt werden können“
  - **SONDERN**: TOP-DOWN Ansatz
    - Dazu später mehr!



CYBER-LAGEBILDER



CYBER LAGEBILDER: INITIALE ERKENNTNISSE

- **DAS EINE** Cyber-Lagebild gibt es nicht!
- Lagebilder sind **immer** Stakeholder- und Aufgabenspezifisch
- **Ebenen-gerecht**
  - Taktisch-Op. Ebene (z.B. Server Admin) benötigt andere Informationen als
  - Operationelle/Business Ebene (z.B. CISO), und wiederum anders darüber auf
  - Strategischer Ebene (z.B. Geschäftsführung)
  - Außerdem: Unterscheidung zwischen Organisationssicht und nationaler Sicht
- **Aufgaben-bezogen**
  - Incident Response auf technischer Ebene
  - Risikoeinschätzung und -linderung
  - Strateg. Infrastrukturentwicklung
  - Strafverfolgung
  - …

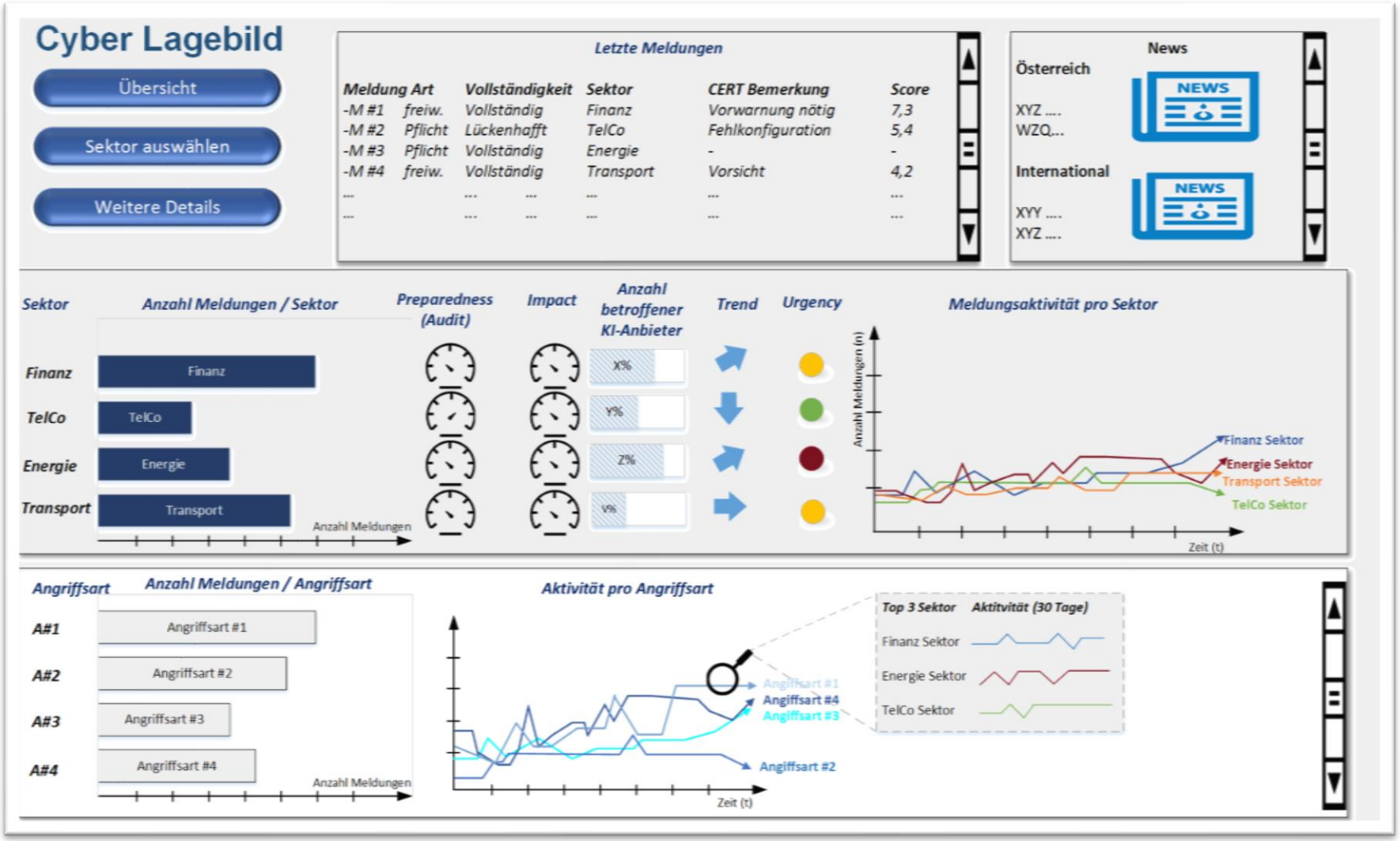
LAGEBILD-ERSTELLUNGSPROZESS

- Informationserhebung nicht als „bottom up“-Magic!
  - Kein „Big Data“, „Large-scale Security Analytics“, …

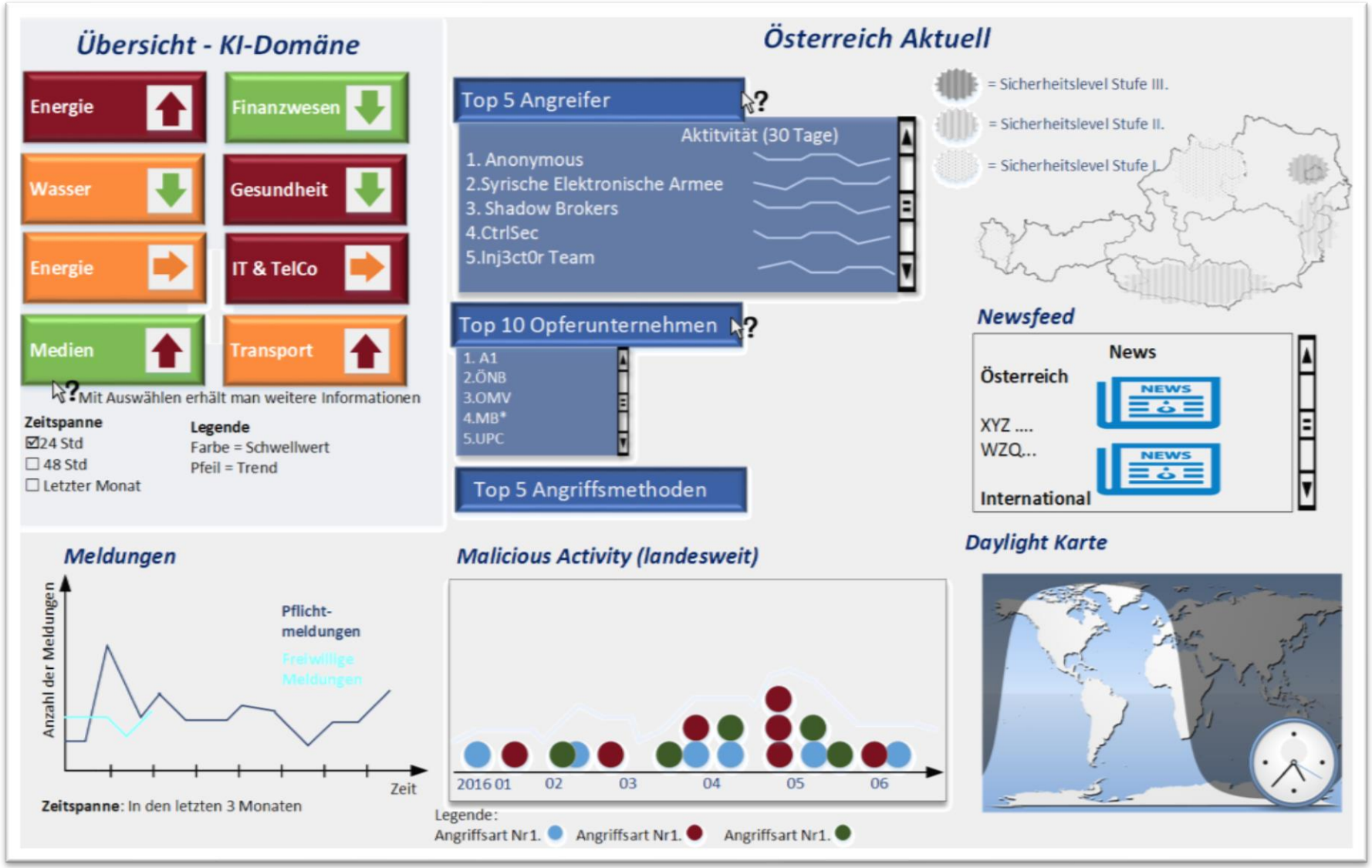
- SONDERN: ein rigider und durchüberlegter **Top-down-Prozess**:
  1. Welche Aktionen bzw. Entscheidungen sollen abgeleitet werden?
  2. Welche Informationen müssen dafür dargestellt werden?
  3. Welche Daten müssen dafür gesammelt werden?
  4. Wie können geeignete Quellen bewertet werden?
  5. Welche Daten einer Organisation können mittels Sensorik nutzbar gemacht werden?

https://www.amazon.de/dp/3662560836/

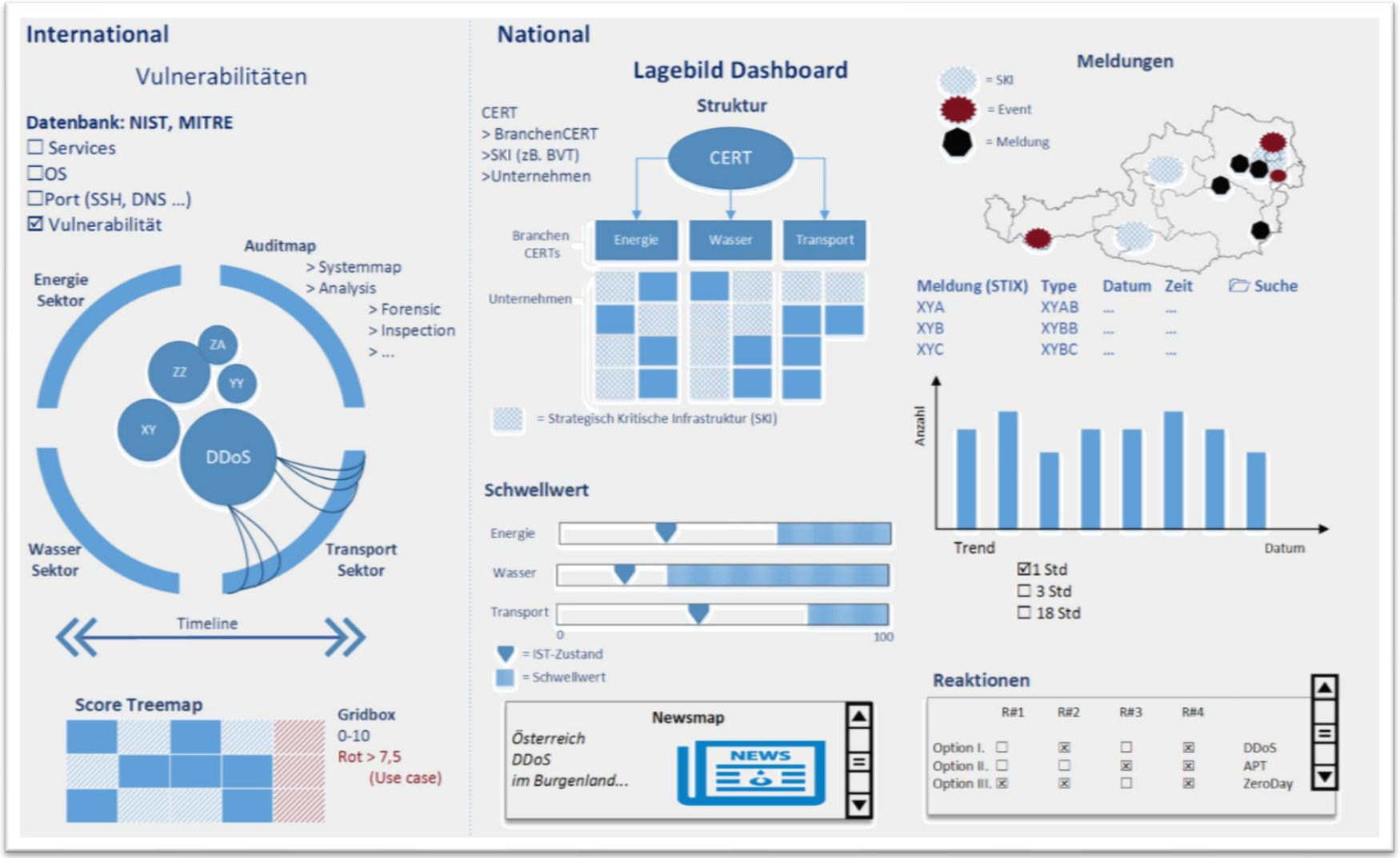
BEISPIEL-LAGEBILDER (1/3)



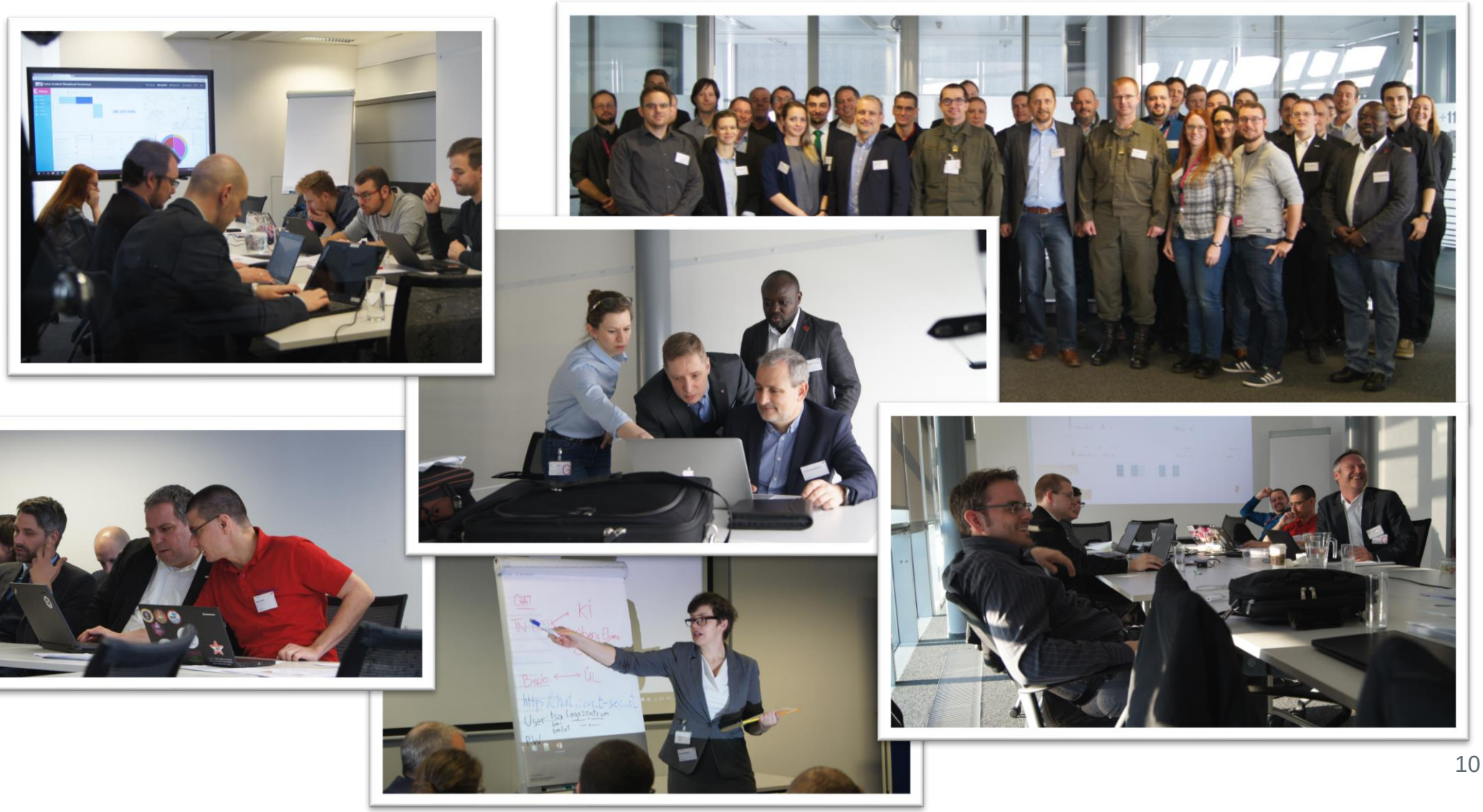
BEISPIEL-LAGEBILDER (2/3)



BEISPIEL-LAGEBILDER (3/3)



EVALUIERUNG DES LAGEBILDKONZEPTS UND DER SOFTWARE-PROTOTYPEN



RESULTATE AUS CISA

- Definition von Cyber-Lagebildkonzepten
- Dokumentation der Kommunikations- und Entscheidungsprozesse
- Rechtliche Bewertung in Hinblick auf NISG und DSGVO (Datenquellen, Verarbeitung, Verbreitung)
- Technischer Demonstrator
- Pilotierung und Planspiel
- Wissenschaftlicher Diskurs/Publikationen

- JEDOCH WESENTLICH:

Die Abwicklung des Projekts zum richtigen Zeitpunkt!

- CISA startete am 1.11.2015;
- Projekteinreichung war im Feb 2015;
- Ideenentwicklung Q3+Q4 2014

https://www.amazon.de/dp/3662560836/

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

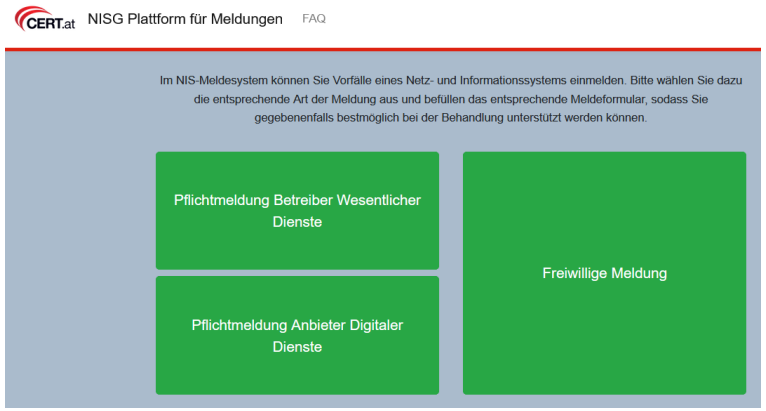
DAS FORSCHUNGSPROJEKT ALS GLASKUGEL

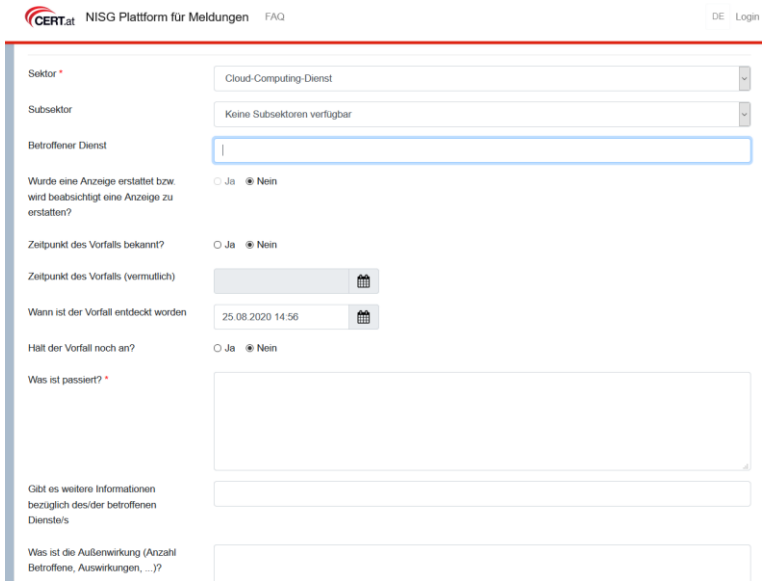
Im Forschungsprojekt entwickelte Ideen im Reality Check

FACT OR FICTION (1/6)?
MELDUNGEN AN EIN LAGEZENTRUM

- CISA Ideen **2014**
  - Nationales Lagebild mit Sicherheitsstatus von KIs
  - Kritische Infrastrukturen sollen Sicherheitsvorfälle melden
- Diskussionspunkte im Laufe des Projekts
  - Wie detailliert sollen diese Meldungen sein?
  - Struktur von Meldungen?
  - Personenbezogene Daten?
  - Interpretationsspielräume beim Meldungsempfänger
  - Widerstand der Industrie
  - Zur Meldung verpflichten oder freiwillig? Incentive?
- **FAKTENCHECK:**

☑ Etablierung einer Meldeplattform bei CERT.at
Ende **2018** im Zuge des NIS-G





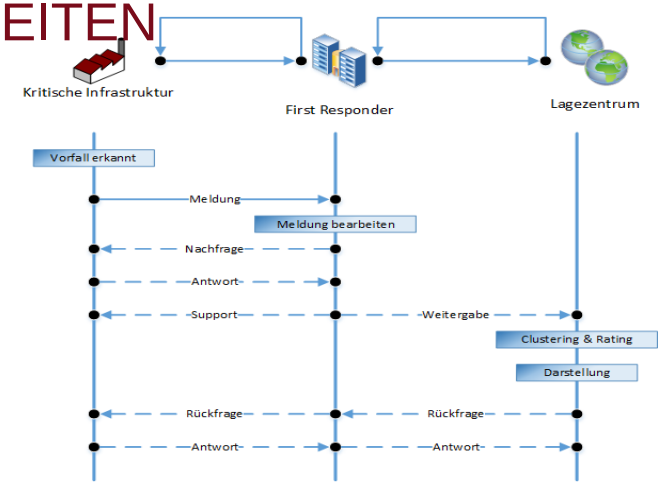
https://nis.cert.at/

FACT OR FICTION (2/6)?

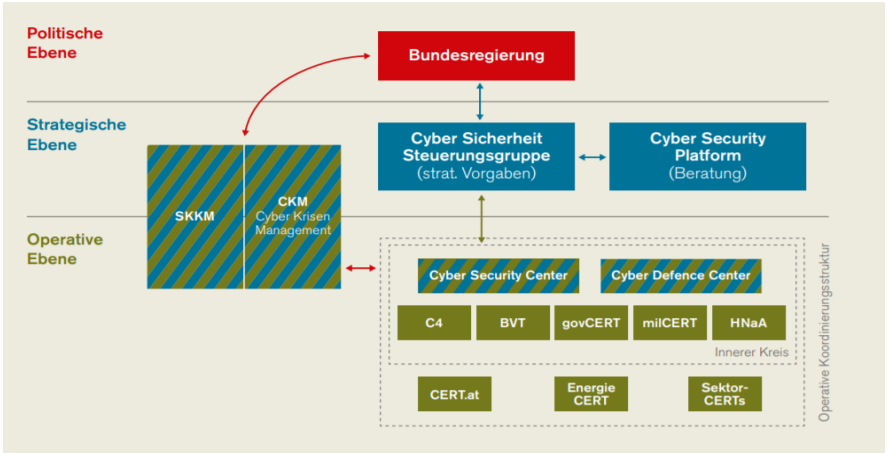
MELDEWEGE, ROLLEN, TRENNUNG DER VERANTWORTLICHKEITEN

- CISA Ideen **2014**
  - Um die Datenqualität zu gewährleisten sollen sog. Sammelstellen (später First Responder) Meldungen entgegennehmen, überprüfen, anreichern und weiterleiten an Lagezentrum
- Diskussionspunkte im Laufe des Projekts
  - Datenmanagement und Duplikate
  - Übergabe zwischen Akteuren?
  - Koordinierungsstrukturen zwischen Bedarfsträgern
- **FAKTENCHECK:**

✓ Etablierung von Branchen-CERTs (AEC **2016**) als Meldestellen (NISG, **2018**).
  - Festlegung der Meldewege **2018** (siehe rechts)



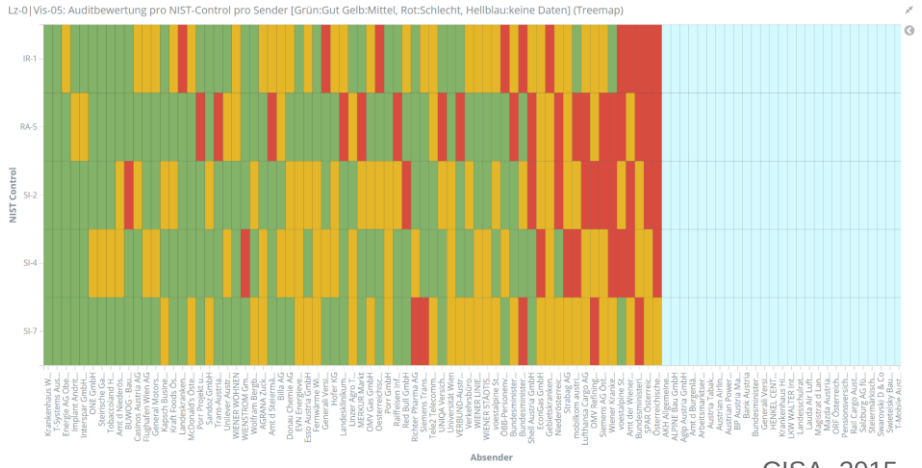
CISA, 2015



https://www.it-businesstalk.at/wp-content/uploads/4_20190411-it-businesstalk-nisg-16x9.pdf

FACT OR FICTION (3/6)?
ZENTRALE SAMMLUNG VON AUDITDATEN

- CISA Ideen **2014**
  - Zur Interpretation von Vorfalls-Meldungen werden Kontextdaten benötigt. Eine zentrale Ablage von Audit-Daten von Organisationen wäre sehr hilfreich. Wie etablieren?
- Diskussionspunkte im Laufe des Projekts
  - Politisch durchsetzbar?
  - Technisch sinnvoll?
  - Nach welchen Normen/Standards?
  - Mgl. Beiträge zu einem Lagebild?
- **FAKTENCHECK:**

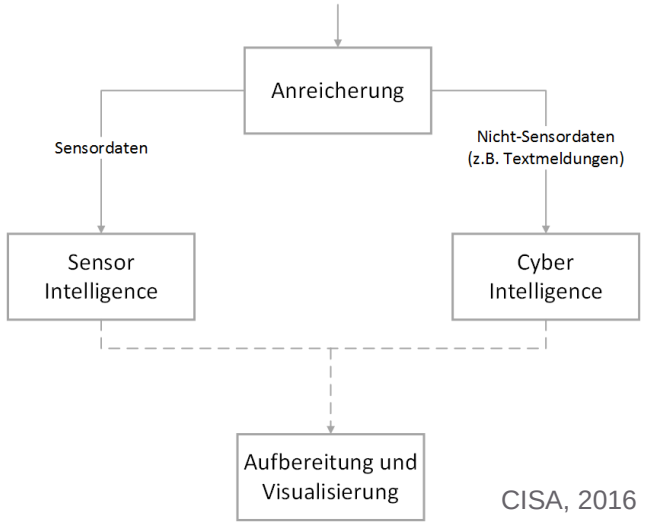


CISA, 2015

Qualifizierte Stellen werden ernannt, welche Betreiber wesentlicher Dienste nach einem eigens definierten Standard auditieren (QuaSteV **2019**). Die Ergebnisberichte sind dem CSC zu übermitteln.

FACT OR FICTION (4/6)?
CYBER SECURITY SENSORNETZ

- CISA Ideen **2014**
  - Zur effizienten Meldung sollen automatisierte Systeme zum Einsatz kommen, bspsweise periodische Scanner, die Infos über Sicherheitsstatus einer Org. liefern
- Diskussionspunkte im Laufe des Projekts
  - Politisch durchsetzbar?
  - Technisch sinnvoll?
  - Mgl. Beiträge zu einem Lagebild?
- **FAKTENCHECK:**
  - Ausschreibung im BVT „Sensornetz-Hauptreferent“ (**2020**) als vorbereitende Maßnahme



CISA, 2016

Hinweise Screenreader

Sensornetz-Hauptreferent/in Referat II/BVT/5.2

Im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung, Referat II/BVT/5.2 (Technik/APT Competence Center), gelangen gemäß den Bestimmungen des Ausschreibungsgesetzes 1989 zwei Funktionen mit der Bezeichnung „Hauptreferent/in Sensornetz“ (A1/2 bzw. v1/2) ehestmöglich zur Besetzung.

Bundesministerium Inneres

Grunddaten

Wertigkeit/Einstufung:	A1/2 bzw v1/2	**Beschäftigungsausmaß:**	Vollzeit
Dienststelle:	BM f. Inneres	**Beginn der Tätigkeit:**	ehestmöglich
Dienstort:	Wien	**Ende der Bewerbungsfrist:**	24.08.2020
Vertragsart:	Unbefristet	**Monatsentgelt/bezug mindestens:**	A1/2 € 2.903,30 brutto bzw. v1/2 € 3.422,90 brutto
Befristung:		**Referenzcode:**	BMI-20-0532

Aufgaben und Tätigkeiten

Erfordernisse

https://bund.jobboerse.gv.at/sap/bc/jobs/#/details/005056816B0F1EEAB693E2C0FC6813ED

FACT OR FICTION (5/6)?

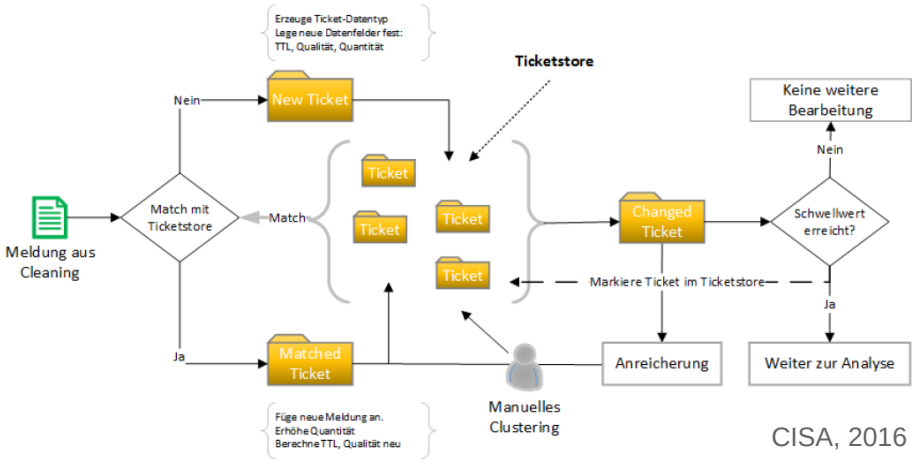
RECHTLICHE ASPEKTE: BEFUGNISSE UND ERMÄCHTIGUNGEN

- CISA Ideen **2014**
  - Organisationen benötigen ggf. eine Verpflichtung zur Meldung,
  - staatliche Stellen benötigen spez. Ermächtigungen zur Verarbeitung der Daten
- Diskussionspunkte im Laufe des Projekts
  - Wie weit realisierbar?
  - Wie weit sinnvoll?
  - Eingriff des Staates in Privatwirtschaft
  - Kompatibilität zu bestehenden Rechtsnormen
- **FAKTENCHECK:**
  - NIS-RL (**2016**), NIS-G (**2018**), QuaSteV (**2019**).
  - Aktuelle Gesetze wesentlich mitgestaltet durch ehem. CISA Projektmitarbeiter

FACT OR FICTION (6/6)?

TECHNISCHE PLATTFORMEN / AUTOMATISIERUNG

- CISA Ideen **2014**
  - Eine neuartige Plattform wird entwickelt, insb. neuartige Übertragungsprotokolle, Speicher- und Anreicherungsmechanismen, Anonymisierungsmechanismen, Verteilte Datenplattformen
- Diskussionspunkte im Laufe des Projekts
  - Wie Meldungen entgegennehmen und speichern?
  - Automatisierte Verarbeitung nach Meldungseingang?
  - Clustering & Korrelation von Meldungen?
  - Aufbau einer „Knowledge Base“?
  - Datenhoheit?
- **FAKTENCHECK:**



CISA, 2016

Noch(?) Fiktion: In der Realität (**2018+**) werden bisher(?) weit einfachere Lösungen eingesetzt als im Projekt antizipiert.

FACT OR FICTION

PROJEKTBEWERTUNG NACH 5 JAHREN

- CISA Fakten Check:
  - Meldungen an ein Lagezentrum ☑
  - Meldewege, Rollen, Trennung der Verantwortlichkeiten ☑
  - Zentrale Sammlung von Auditdaten ☑
  - Cyber Security Sensornetz ☑
  - Rechtliche Aspekte: Befugnisse und Ermächtigungen ☑
  - Technische Plattformen / Automatisierung ☒
- Diskussion neuer Ideen („Was wäre wenn …“) im Rahmen eines Forschungsprojekts ist von unschätzbarem Wert: Im Forschungsprojekt ist alles erlaubt
  - Auch zu erforschen wie es *nicht* geht und wie es *nicht* funktioniert kann wertvolle Einblicke bringen („sanity check“ im Expertenkreis)!
- **CISA war seiner Zeit voraus – Genauso wie es Forschungsprojekte sein sollten!!**

BESTEN DANK FÜR IHRE AUFMERKSAMKEIT!

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Jegliche Anregungen und Anfragen richten Sie bitte gerne an:

Dr. Dr. Florian Skopik
Thematic Coordinator Cyber Security

AIT Austrian Institute of Technology GmbH
Center for Digital Safety & Security
Giefinggasse 4 | 1210 Wien | Austria
M +43 664 8251495 | **florian.skopik@ait.ac.at**

https://www.amazon.de/dp/3662560836/

PROJEKTPORTFOLIO UND PROJEKTÜBERGREIFENDE SYNERGIEEFFEKTE

- AIT Projekte mit Fokus „National Cyber Security“
  - CAIS – Cyber Attack Information System, 2011 – 2013
  - CIIS – Cyber Incident Information Sharing, 2013 – 2016
  - CISA – Cyber Incident Situational Awareness, 2015 -2018
  - ACCSA – Austrian Cyber Crisis Activities, 2017 – 2019
  - APT-CC – Aufbau eines APT-Competence Centers in Österreich, 2018 – 2020
  - CADSP – Cyber Attack Decision and Support Platform, 2019 – 2022 (FORTE)
- Enge Kooperation mit nationalen Sicherheitsinitiativen
  - CSP – Cyber Sicherheit Plattform
  - KSÖ Sicherheitstagung/Enquete/Planspiel
  - IKT Sicherheitskonferenz des AbwA (BMLV)
- Strategische Kooperationen mit nat. Behörden und CERTs
- Kooperationen „beyond Austria“ → EU H2020