Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

Gefahren im Netz und Zusammenarbeiten Private / Bund / Kantone / Städte

Melde- und Analysestelle Informationssicherung MELANI

Agenda

1. Spannungsfeld Und Bedrohungslage
2. Von der Sicherheit zum Risikomanagement
3. Die Rolle von MELANI
4. Schlussfolgerungen

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan Bund ISB
Nachrichtendienst des Bundes NDB

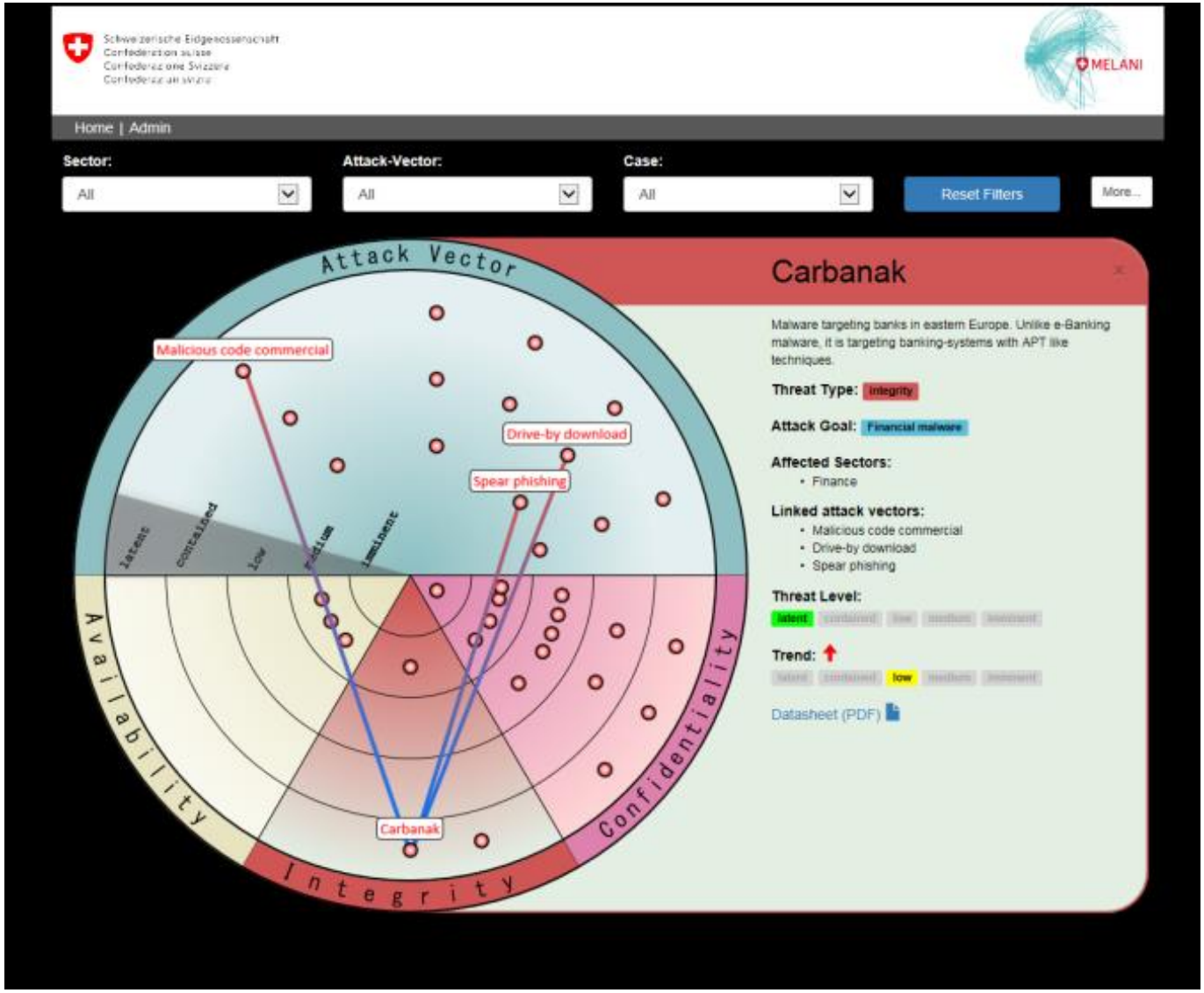
Melde- und Analysestelle Informationssicherung MELANI

Spannungsfeld und Bedrohungslage

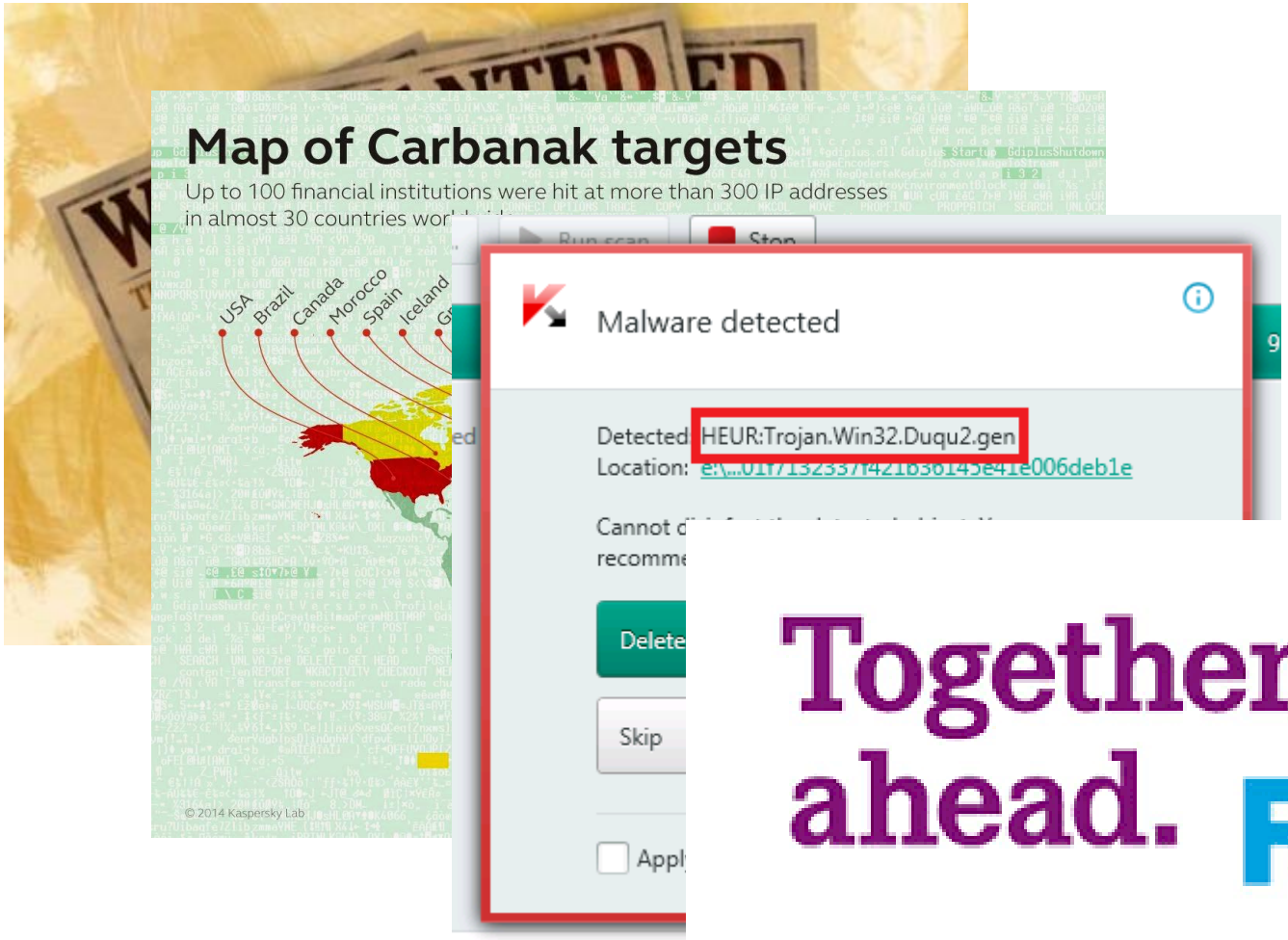
Generelle Betrachtungen

- Zunahme der Bedeutung der Informationstechnologie für Geschäftsprozesse und Finanztransaktionen
- Zunahme der Teilnehmer an diesen Prozessen, zunehmende Vernetzung
- Zugang zu immer mehr wertvoller Information wird möglich
- Zunahme der Möglichkeiten für Betrug, Spionage, Erpressung, Sabotage
- Auftreten neuer Akteure (z.B. Organisierte Kriminalität, Staaten)
- Anpassung der Motive und Methoden bestehender Akteure: kommerzieller Gewinn, Know-how Transfer, politische Motive

Bedrohungslage



Ein paar Beispiele



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

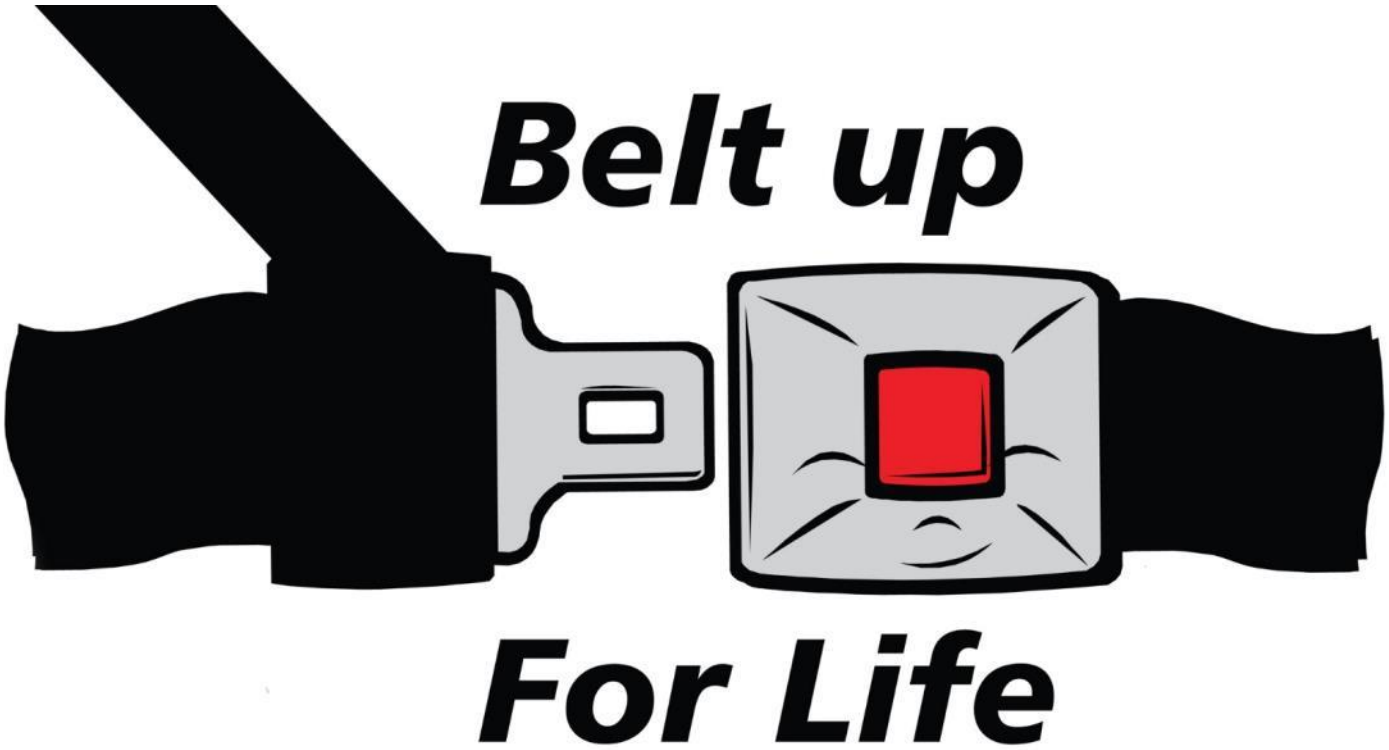
Informatiksteuerungsorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

Von der Sicherheit zum Risikomanagement

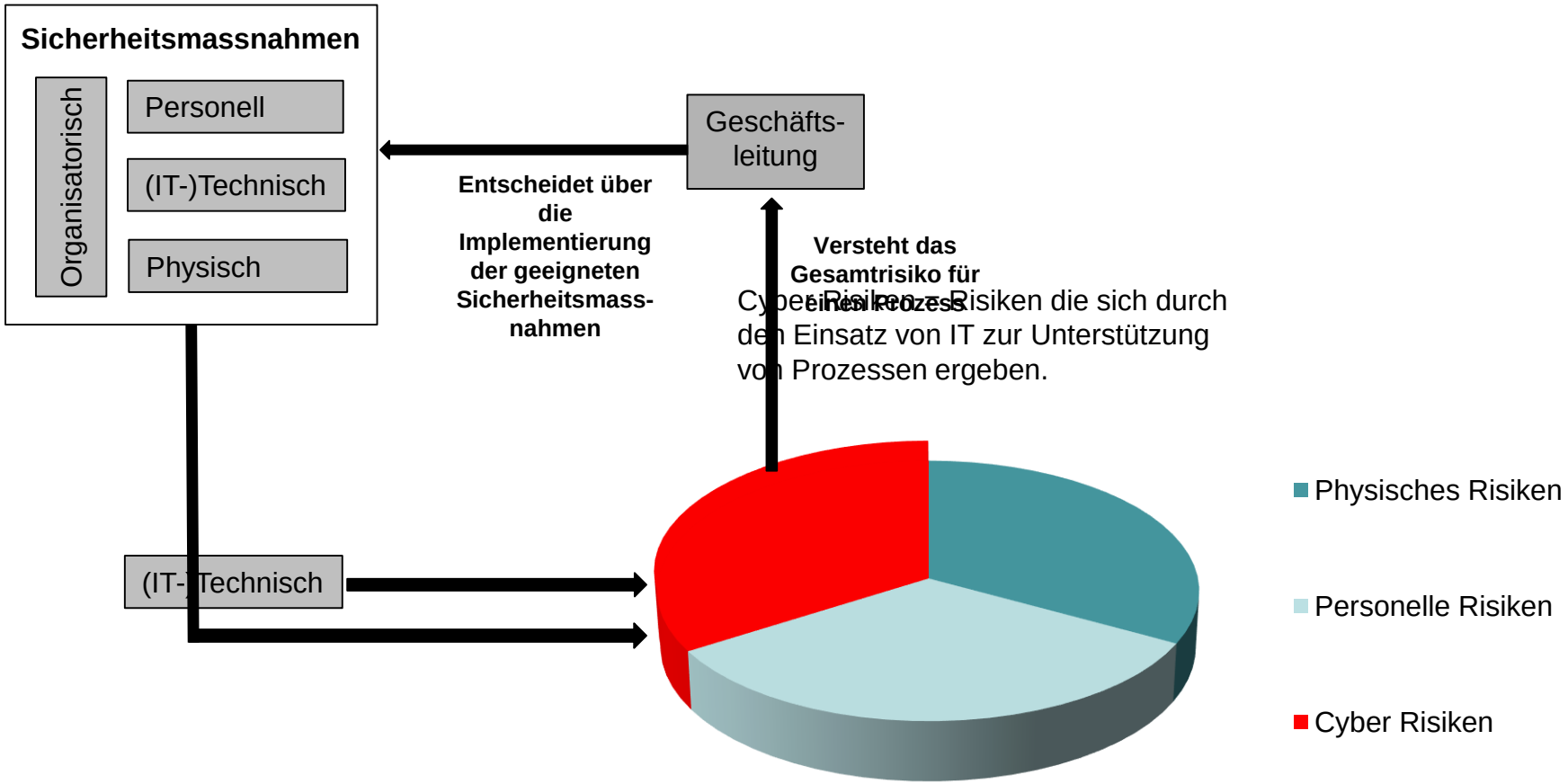
Sicherheit vs. Risiko

“Seat belts reduce serious crash-related injuries and deaths by about half.”
(National Highway Traffic Safety Administration)



Ein Beispiel

Cyber Risiken im Gesamtkontext

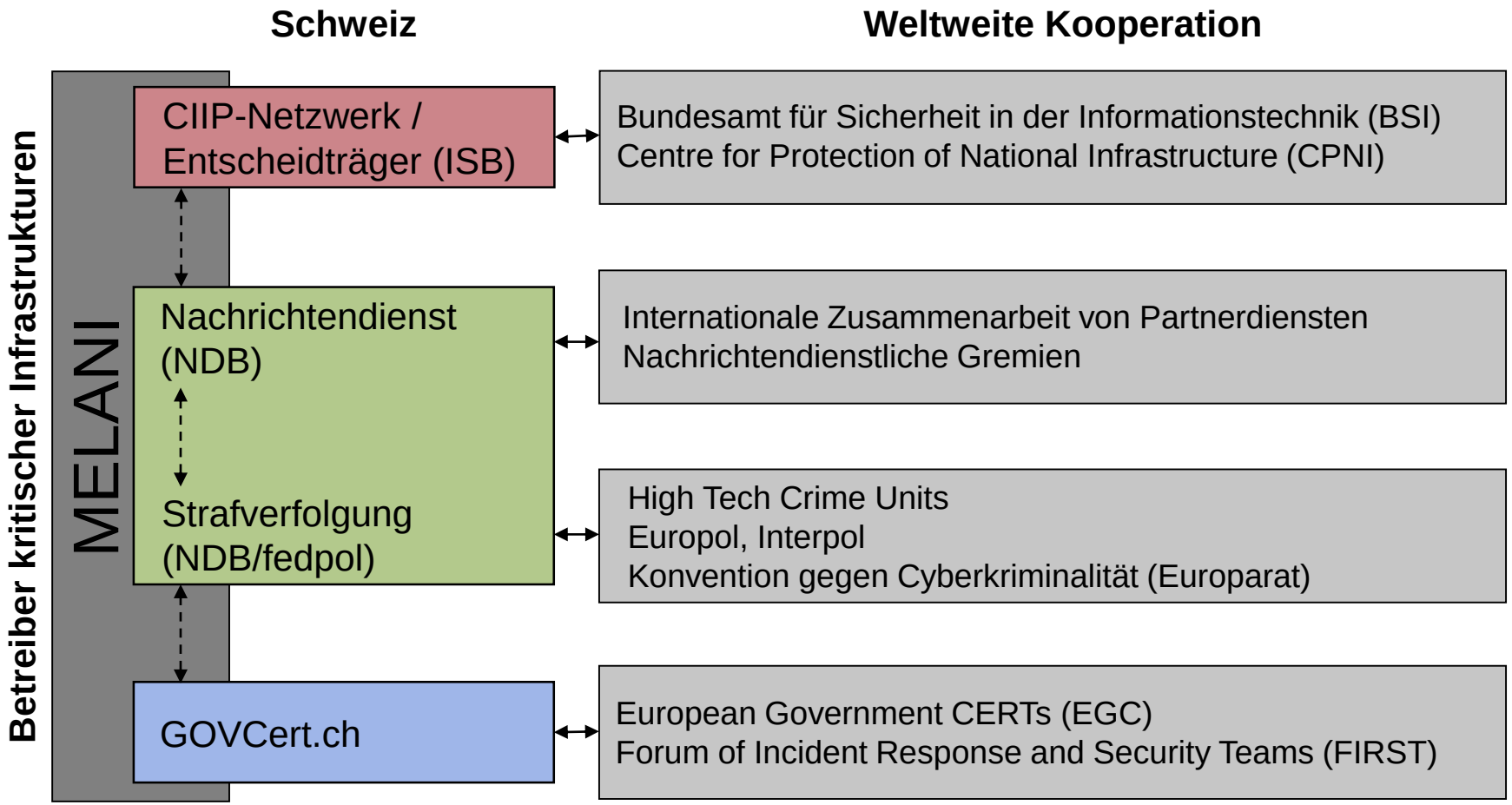


Die Rolle von MELANI

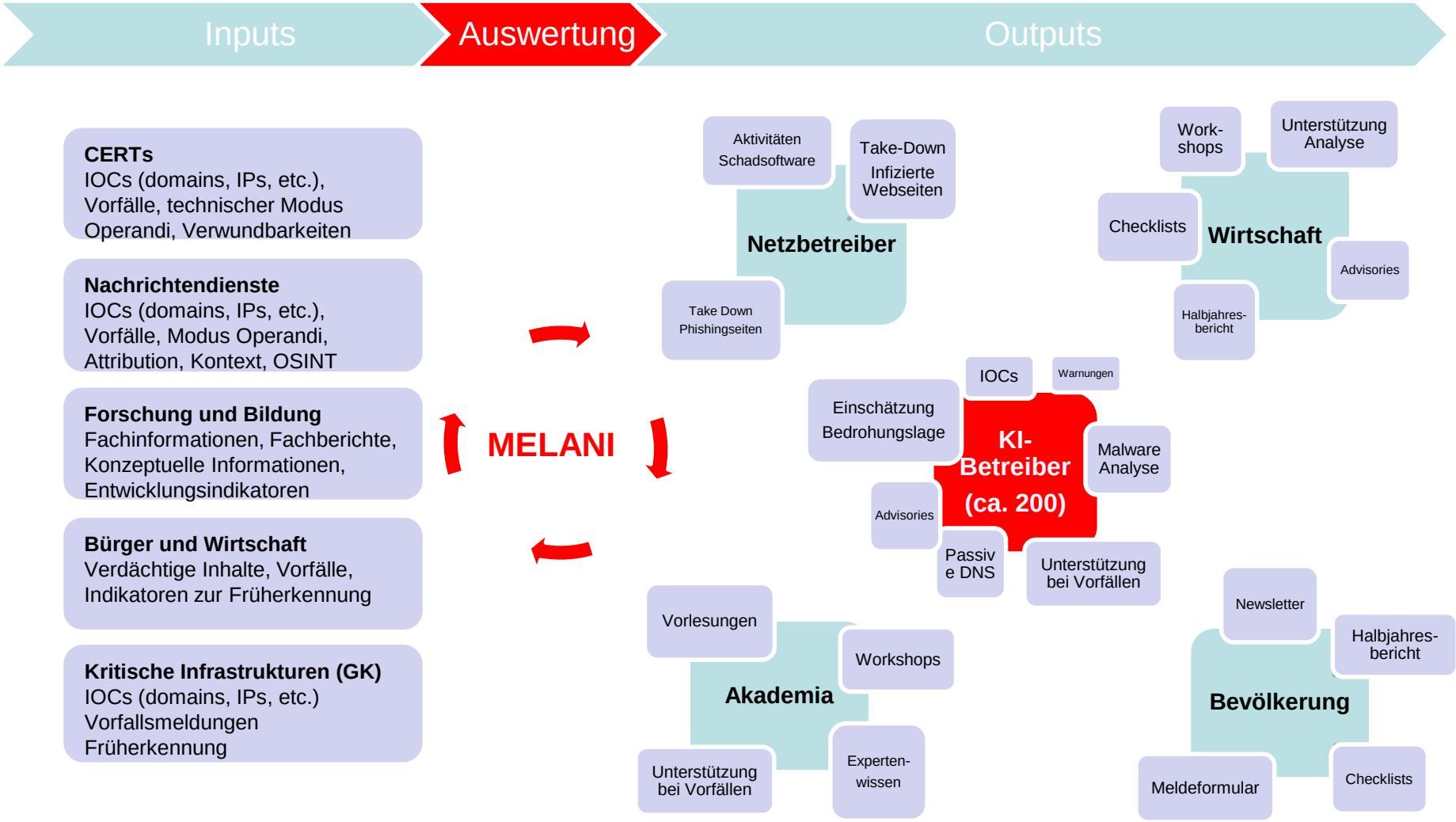
MELANI Auftrag

- MELANI unterstützt subsidiär den Informationssicherungsprozess innerhalb der kritischen Infrastrukturen. Sie tut dies im Rahmen eines Public Private Partnership (PPP).
- MELANI bedient sich dabei in erster Linie technischer und nicht technischer Informationen aus dem öffentlichen oder nicht-öffentlichen Raum und macht diese den kritischen Infrastrukturen zugänglich, in Form von Einschätzungen zur Bedrohungslage, Warnhinweisen und vorfallsspezifischen Informationen.
- Bei Vorfällen nimmt MELANI eine Einschätzung vor, unterstützt und koordiniert nötigenfalls die Massnahmen
- Präventionsarbeit zu Gunsten von KMU und Bürgern
  (→ Offener Kundenkreis)

Organisation von MELANI: Kooperationspartner



Das Sicherheitsdispositiv Schweiz



Schlussfolgerungen

Im Fokus stehen Daten und Prozesse

- Wer hat Zugriff auf was? Und wie werden diese Mitarbeiter genau ausgewählt, überprüft und allenfalls überwacht?
- Existieren Klassifizierungen? Wo sind unterschiedlich klassifizierte Daten gespeichert? Und wer hat die Verantwortung dafür? (Cloud-Services)
- Welche Kanäle werden gebraucht, um welche Daten zu senden oder um sie verfügbar zu machen?
- Welche Daten werden öffentlich oder intern publiziert? (Facebook: Social Engineering)

Das Schutzbedürfnis der Information diktiert das entsprechende Schutzniveau. Dieses soll unter Einbezug und Austarieren aller Risikofaktoren erreicht werden.

Schlussfolgerungen

- Prinzipiell gilt: Wenn ein Markt oder Wille existiert, wird Information gestohlen. Aber, es braucht einen Business-Case dazu.

- Informationssicherheit ist nicht gleich IT-Sicherheit. Nur ein integraler, Risikomanagement basierter Ansatz kann zu einem besseren Informationsschutz führen.

- Risikomanagement ist Aufgabe der Geschäftsleitung. Die gute Nachricht ist, auf dieser Ebene gibt es nur Geschäftsrisiken und kein “Cyber”. Die schlechte Nachricht ist, es müssen die richtigen Entscheidgrundlagen eingefordert und Fragen gestellt werden. Am Ende lässt sich Verantwortung nicht delegieren.

- Risiken sind nie Null. Sind die Abhängigkeiten bekannt und welche Prozesse geschäftskritisch sind und gibt es dazu ein Plan B wie in BCP?

Fragen?