Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

Cyberrisiken: Bedrohungslage und Herausforderungen

Melde- und Analysestelle Informationssicherung MELANI

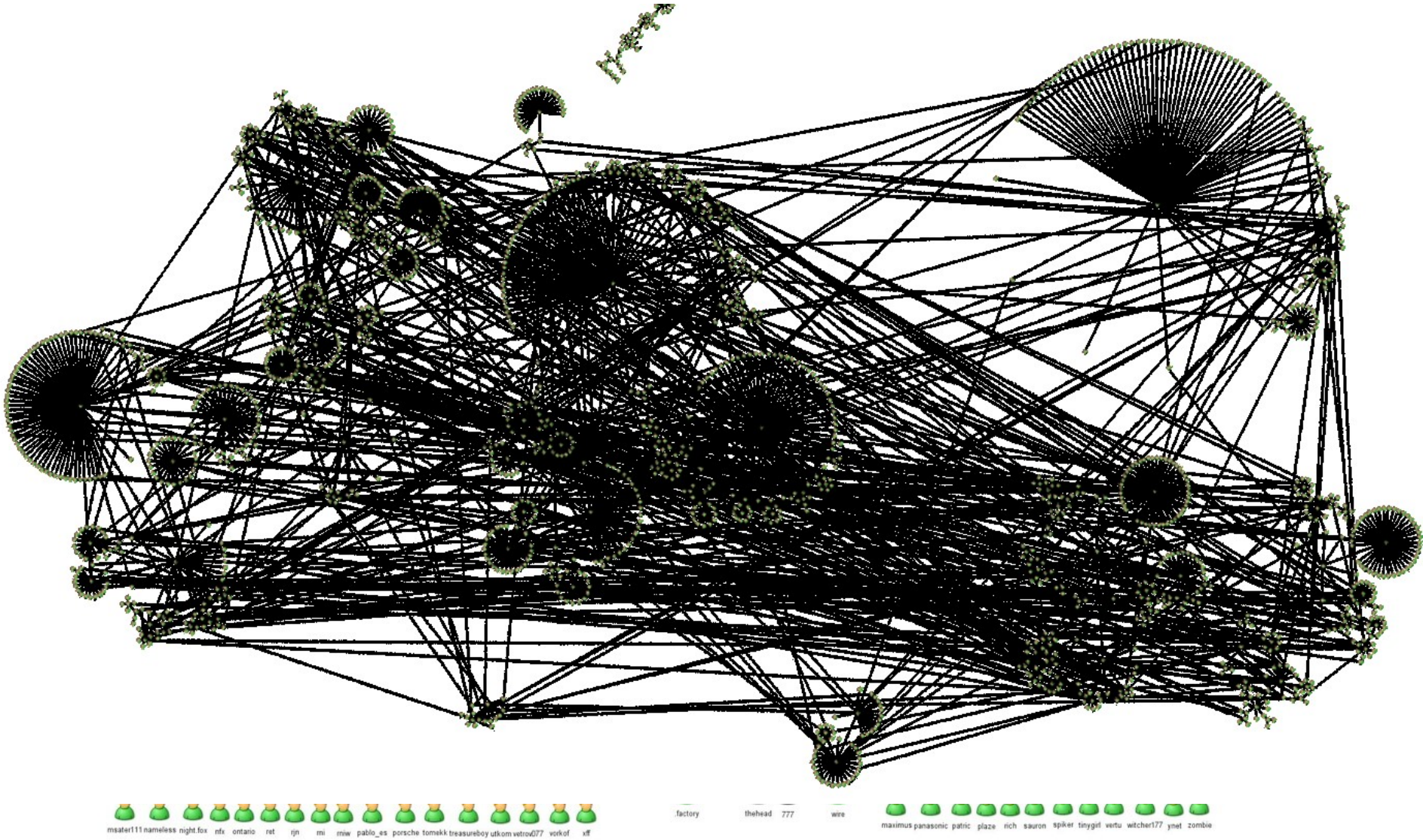
Tag der Schweizer Qualität, 7. Mai 2019

Die Situation Heute

Das Spannungsfeld

- 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

Die Akteure dahinter



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

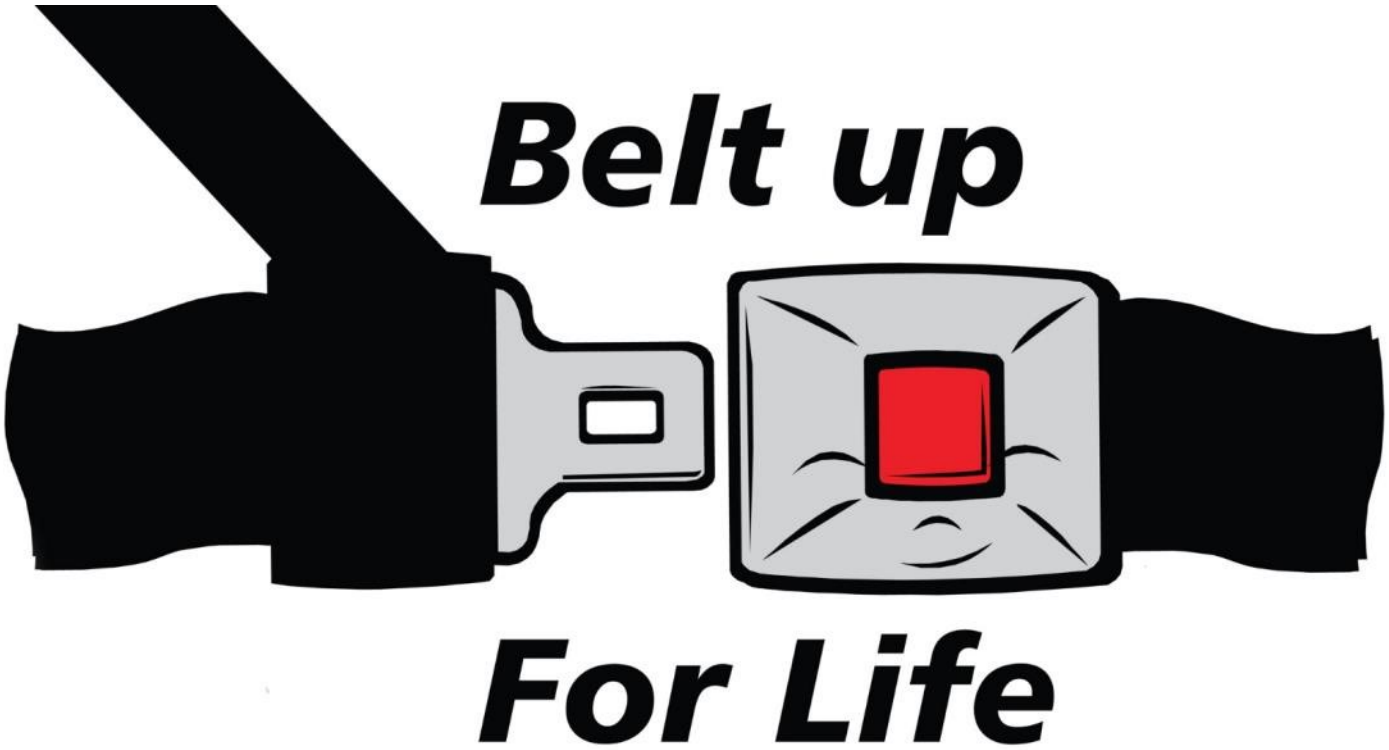
Informatiksteuerungsorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI

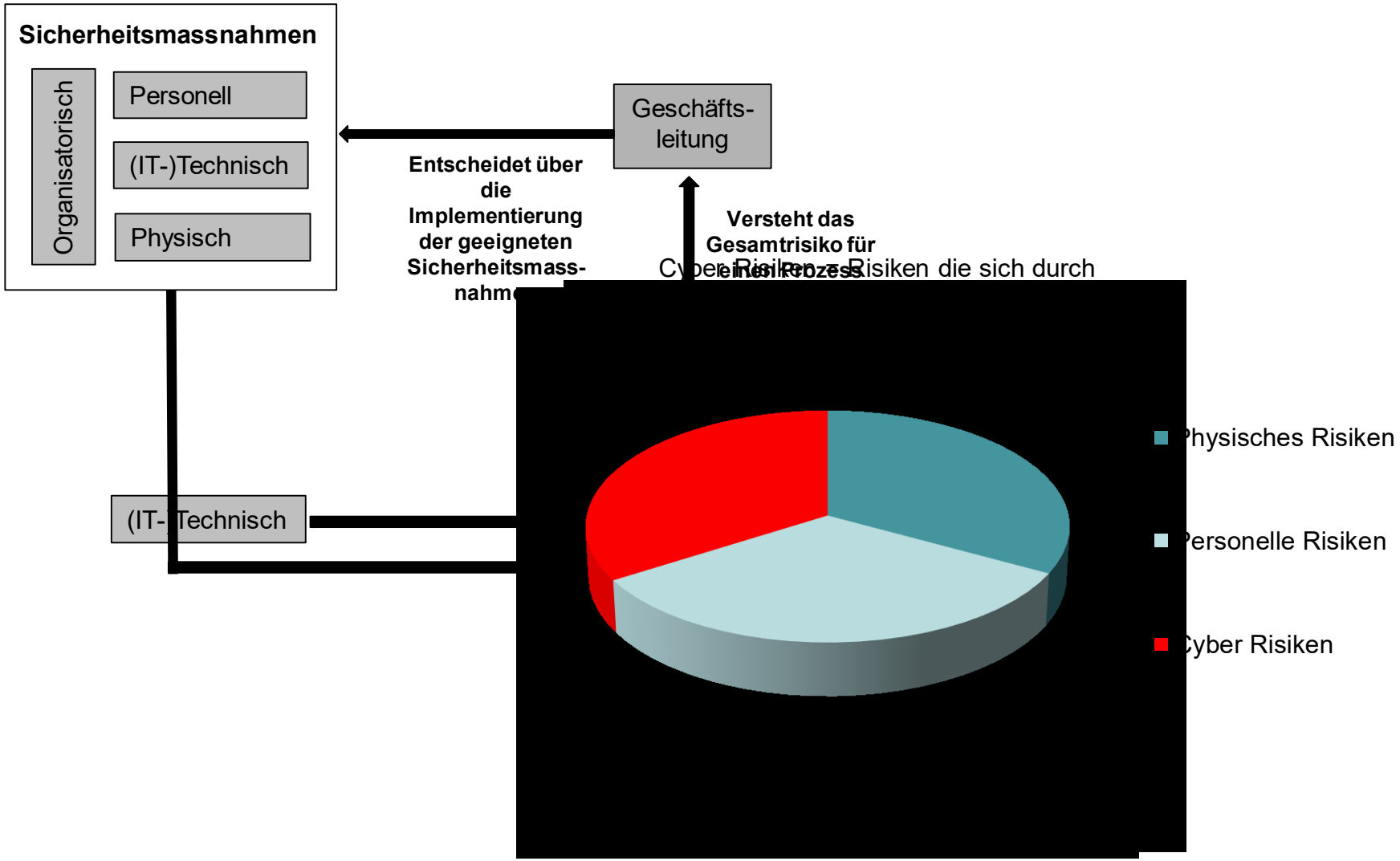
Von der Sicherheit zum Risiko

Sicherheit vs. Risiko

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



Cyber Risiken im Gesamtkontext



Cyber Risiken im Gesamtkontext

- Informationssicherheit ist nicht gleich IT-Sicherheit. Nur ein integraler, Risikomanagement basierter Prozess kann zu einem besseren Informationsschutz führen.
- Risikomanagement ist Aufgabe der Geschäftsleitung. Fragen Sie die richtigen Fragen und vertrauen sie nicht auf eine rein technische Lösung. Diese mag als Sicherheitsmassnahme Sinn machen, aber sie sind nur Teil des Risikomanagements.
- Prinzipiell gilt: Chancen sind zu ergreifen, aber die inhärenten Risiken zu erkennen (Datenschutz, Komponentensicherheit, Abhängigkeiten etc…)
- Es empfiehlt sich Risiken früh genug zu erkennen und beispielsweise Industriestandards anzustreben. Ansonsten reguliert jemand anders früher oder später.

Im Zentrum stehen die Daten

- Wer hat Zugriff auf was? Und wie werden diese Mitarbeiter genau ausgewählt und überprüft?
- 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? (Soziale Medien ➔ Social Engineering)

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

Fragen?