Aus der Praxis für die Praxis

Erläuterungen zu Angriffen und Vorgehensweisen im Vorfall-Management am Beispiel eines anonymisierten Szenarios

Initiative für Cyber-Sicherheit Thüringen e.V.

18.10.2023, Pößneck, Auftaktveranstaltung ICST

Szenario

Mögliche Ausgangslage

„Es ist der 23.12.23, in Weimar wird ein Cyber-Angriff auf die **Wasserversorgung**,

in Jena auf die Produktionsanlagen einer AG, welche wichtige Artikel für **kritische Geschäftszweige** produziert,

in Erfurt auf die **Anlagen der Straßenbahn**, und

in Gera auf die **Infrastruktur eines Krankenhauses** verübt“

Was meinen Sie, haben wir die **Kapazitäten**, um den Normalbetrieb möglichst schnell wieder herzustellen? Wenn nein, warum nicht ?

Was müssen wir tun?

Angriffsszenario

Warum ist das angesprochene Szenario realistisch?

Aktuelle Situation

Aus der Praxis für die Praxis - Aktuelle Szenarien

Angriffsarten Allgemein

Vernetzte Wirkweise

- CVEs/ Zero-Day als Türöffner für Angreifer Gruppen

Staging von Angriffen

- Double/Triple Extortion

APT – Advanced Persistance Threat

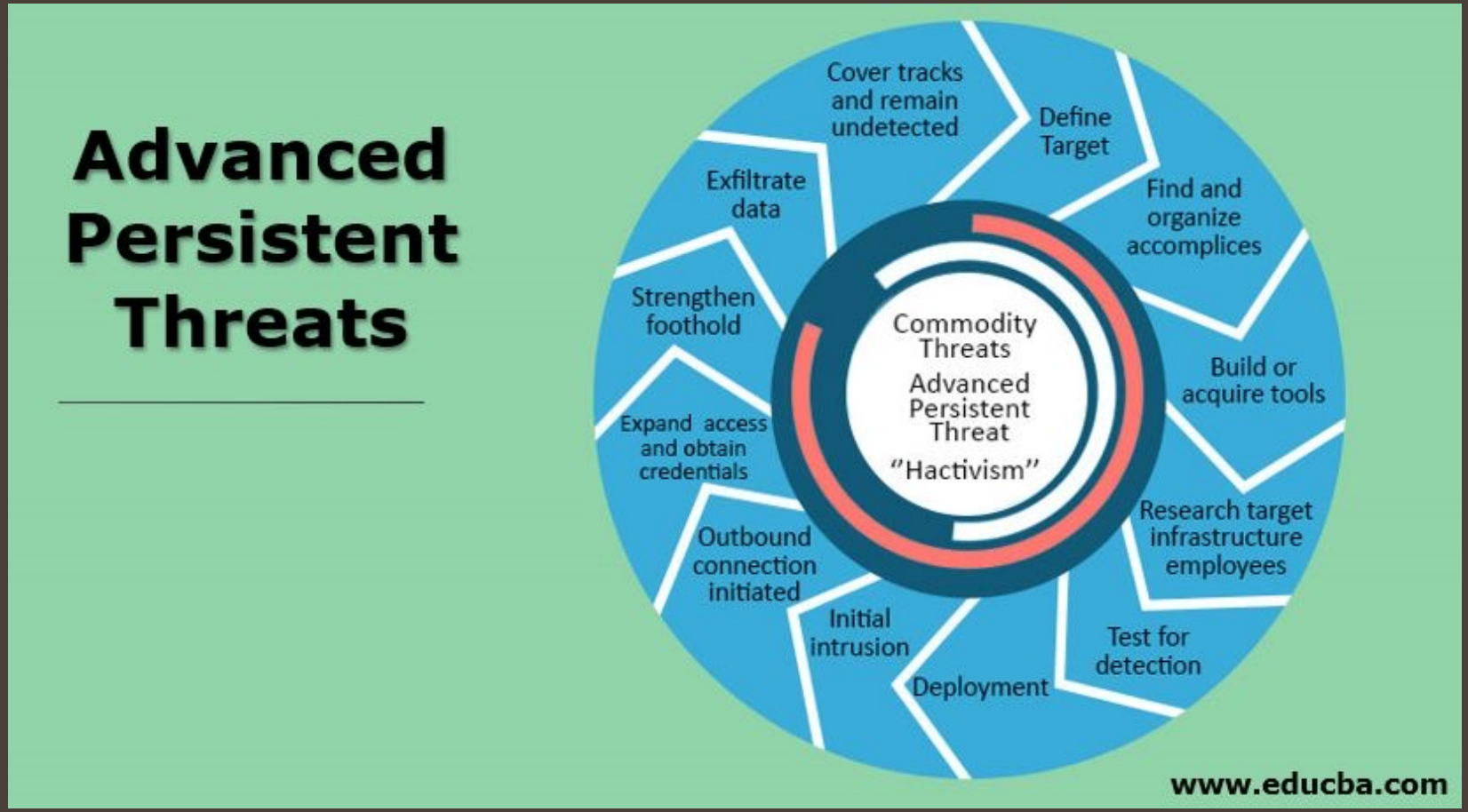
Hacktivismus

- Politische von außen gesteuerte (Bsp. Ukrainekrieg) und
- intrinsische (Bsp. meinungs- und motivationsgesteuert) Angriffe

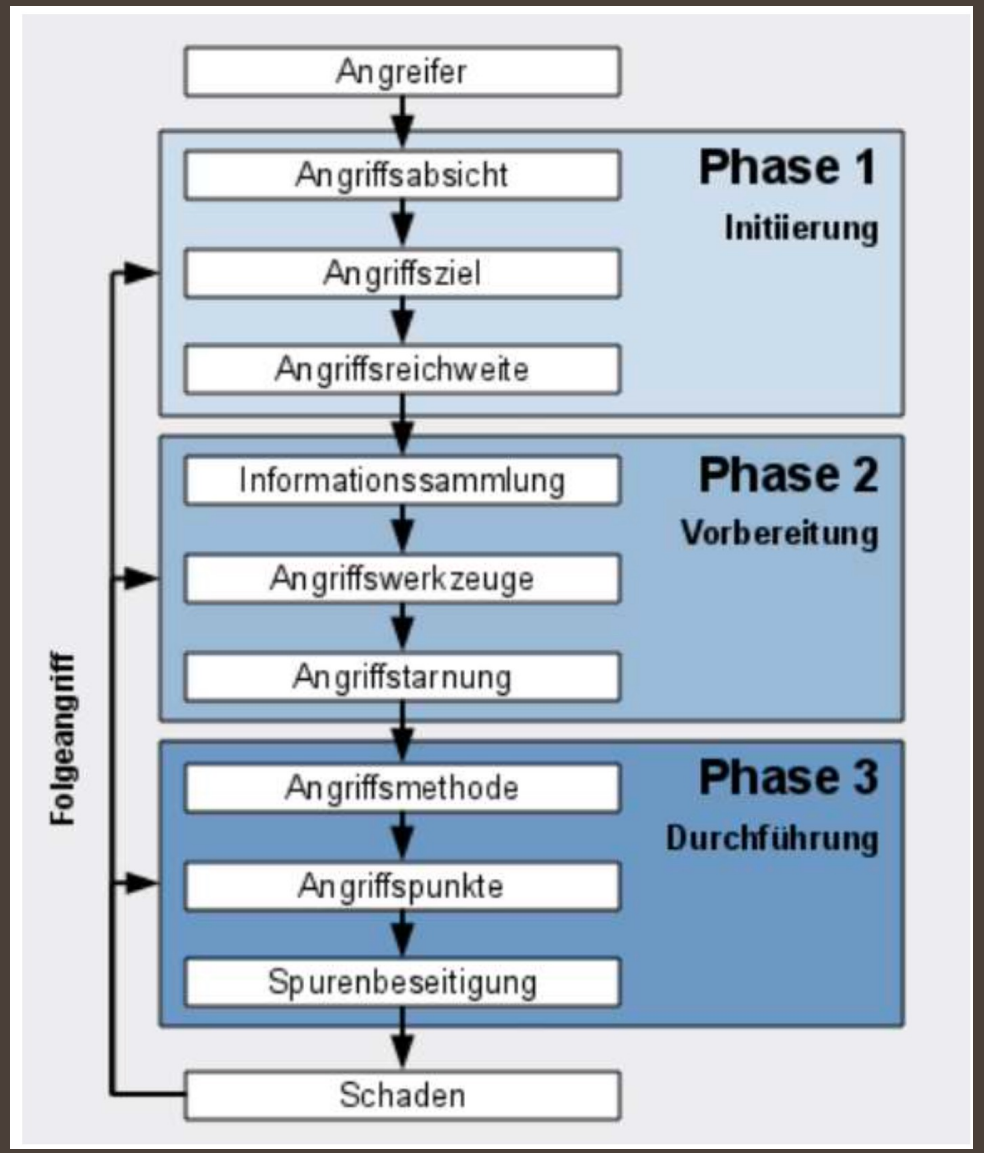
Angriffe Akteure

ICST

APT-Angriffe

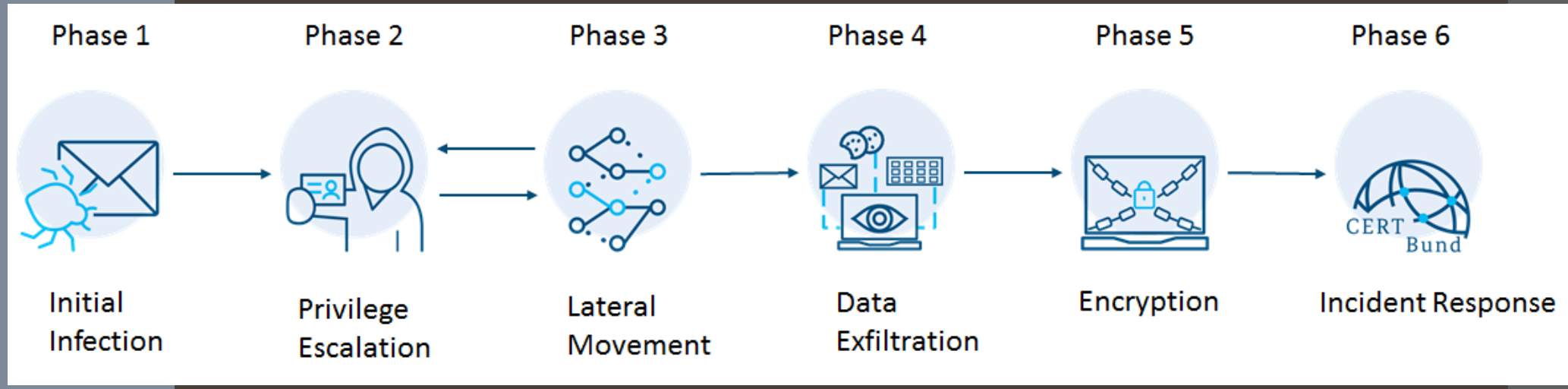


Stufen von Angriffen



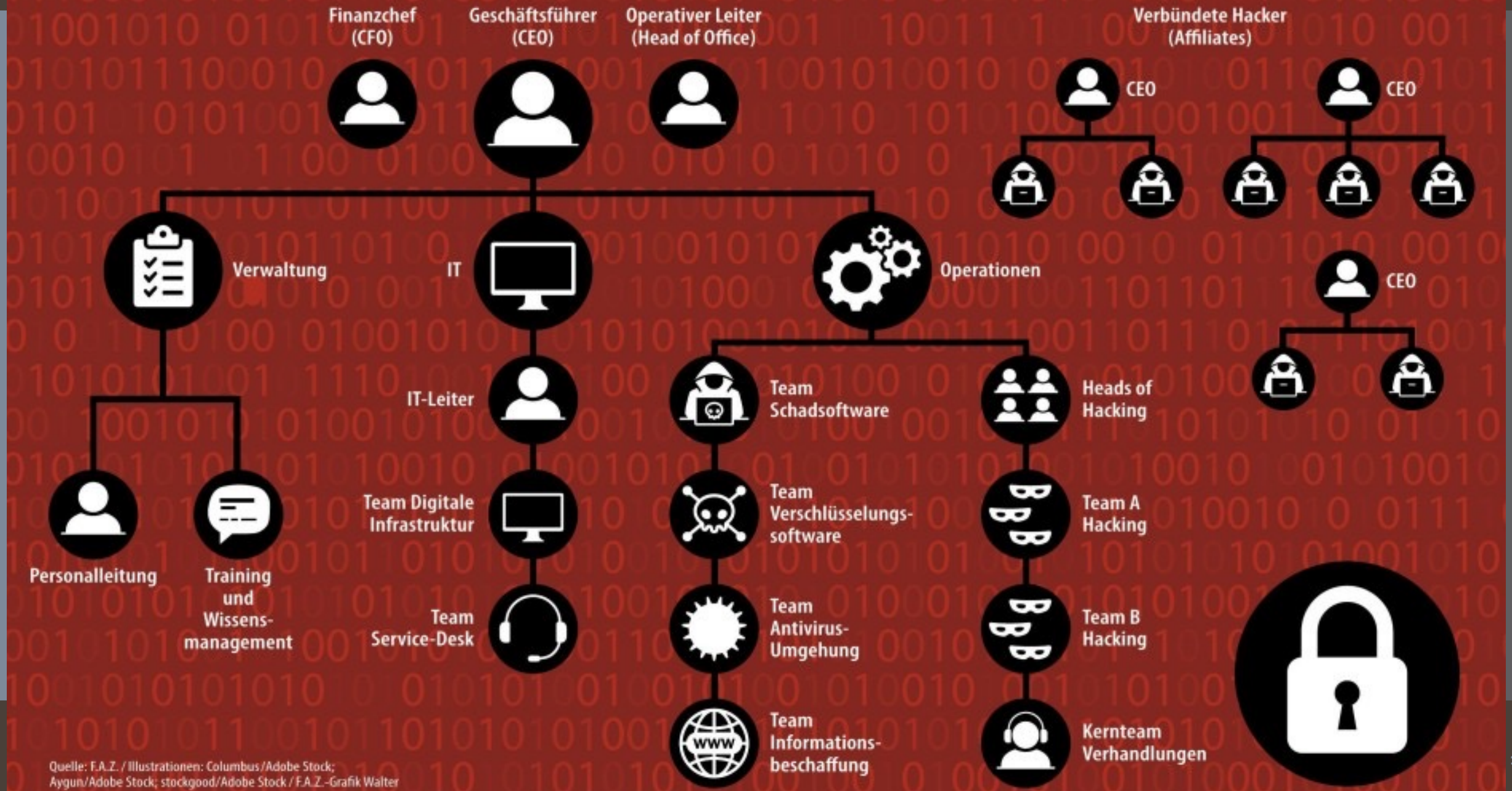
Quelle: BSI-CS 026 / Version 2.0 vom 11.07.2022, BSI- Veröffentlichung zur Cyber- Sicherheit / Register aktueller Cyber-Gefährdungen und –Angriffsformen

Ransomware Kill Chain



Quelle: BSI-CS 026 / Version 2.0 vom 11.07.2022, BSI- Veröffentlichung zur Cyber- Sicherheit / Register aktueller Cyber-Gefährdungen und –Angriffsformen

Typische Struktur einer Schadsoftware-Erpresserbande



Quelle: F.A.Z. / Illustrationen: Columbus/Adobe Stock; Aygun/Adobe Stock; stockgood/Adobe Stock / F.A.Z.-Grafik Walter

Statistik/Erfahrungswerte

Aktion

Best Practice neu aufgesetzt – Basisschutz hört nicht beim IT-Notfallplan auf

„Vor allem die Vorbereitung ist der Schlüssel zum Erfolg“

Alexander Graham Bell

Befähigung zur Reaktion

Die häufigsten Probleme

- Ressourcen,
- Wägen in Sicherheit,
- übereilter Aktionismus,
- BIA/SBF - Kennen Sie Ihre Institution?
- Unzweckmäßige Backups/Backupstrategien
- Notfallübungen!
- Anomalie Erkennung fehlt – Logging reicht nicht!
- Interne und Externe Kommunikation – Fallback auf allen Ebenen

Profitieren

Rolle der ICST in Bezug auf CSN /CHW und weitere Lösungsansätze

Vorbeugen Und Informieren

Ransomware Kill-Chain

botfrei.de

abuse.ch

nomoreransom.org

ITDaily

Register aktueller Cybergefährdungen BSI

Lessons Learned

Verständnis und Toleranz schaffen

Voneinander Lernen

Von Erfahrungsschätzen profitieren

Vernetzen

Prävention

Informationslage aktuell halten

Über Compliance hinweg denken