



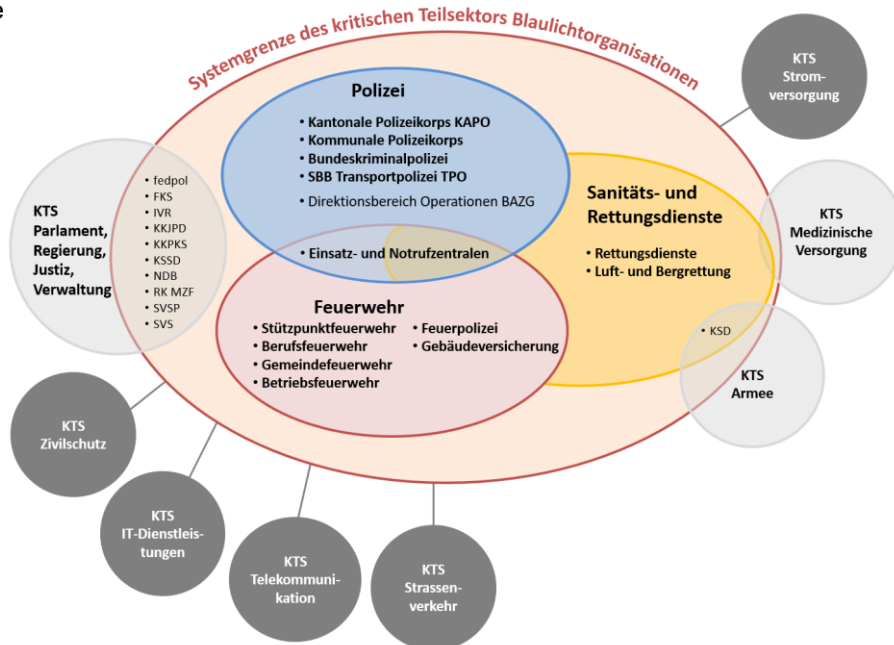
Nationale Strategien Schutz kritischer Infrastrukturen SKI / Cyber NCS

Factsheet zum kritischen Teilsektor Blaulichtorganisationen

Allgemeine Beschreibung und Versorgungsleistungen

Zum kritischen Teilsektor Blaulichtorganisationen gehören Polizei, Feuerwehr sowie die Sanitäts- und Rettungsdienste. Zusammen leisten sie einen essenziellen Beitrag zur Gewährleistung der öffentlichen Sicherheit und zur Gesundheit der Bevölkerung. Dies umfasst lebensrettende Hilfs- und Rettungseinsätze, Ordnungsaufgaben im öffentlichen Raum sowie Leistungen zum Schutz von Leib und Leben, von Eigentums- und Vermögenswerten usw. Konkret sind dies Aufgaben wie das Retten von Menschen und Tieren aus Notlagen oder bei Unfällen, das Löschen von Bränden, das Verhindern oder Eindämmen von Folgeschäden für die Umwelt bei Unfällen und Katastrophen wie auch die polizeiliche Strafverfolgung, das Untersuchen von Straftaten und die Ermittlung sowie die Fahndung und Festnahme von Tatverdächtigen.

Die Blaulichtorganisationen arbeiten aufgrund der teils überschneidenden Aufgabengebiete sehr eng zusammen. Wie in der folgenden Abbildung ersichtlich ist, gibt es aber auch Berührungspunkte mit anderen kritischen Teilsektoren wie z. B. dem Zivilschutz, der Stromversorgung sowie den kommunalen, kantonalen und nationalen Behörden und Führungsorganen. Zudem bestehen Abhängigkeiten zu anderen kritischen Teilsektoren wie z. B. der medizinischen Versorgung oder der Armee



Marktanalyse / Systemstruktur

Um effizient operieren und ausreichend schnell reagieren zu können, ist der Teilsektor geografisch grossflächig über die ganze Schweiz verteilt. Dadurch sind nur wenige Akteure systemrelevant. Bestimmte technische Systeme, wie z. B. das Sicherheitsfunknetz Polycom, werden jedoch zentral betrieben und von allen Organisationen des Teilsektors gemeinsam genutzt.

Die Einsatzorganisationen sind explizit auf die gegenseitige Zusammenarbeit mit wechselnden Partnern ausgerichtet. Ein Beispiel dafür sind die polizeilichen Konkordate. Innerhalb und zwischen den verschiedenen Blaulichtorganisationen besteht somit eine hohe gegenseitige Unterstützungsfähigkeit. Einschränkungen existieren vor allem bei den eingesetzten IKT-Systemen sowie den geltenden rechtlichen Grundlagen (z. B. Polizeigesetzen) in Bezug auf den Datenaustausch.

Die Blaulichtorganisationen sind bei der Erfüllung ihres Auftrags an diverse Gesetze und Richtlinien gebunden, was eine starke regulatorische Einwirkung auf den Teilsektor ermöglicht.

Untersuchte Prozesse

Im Teilsektor Blaulichtorganisationen wurden insgesamt 19 Prozesse untersucht, die für die Funktionserbringung des Teilsektors als wichtig erachtet werden. Bei vier Prozessen handelt es sich um organisationsübergreifende Prozesse.

Feuerwehr	Polizei und Direktionsbereich Operationen BAZG	Sanitäts- und Rettungswesen
<ul style="list-style-type: none"> - Brand-, Explosions-, ABC-, Naturgefahren-, Rettungs- und Spezialeinsätze - Aufbieten der Angehörigen der Feuerwehr (AdF) sowie von Spezialmitteln 	<ul style="list-style-type: none"> - Polizeiliche Gefahrenabwehr - Polizeiliche Strafverfolgung - Unterstützung bei Grossanlässen - Lenken, Regeln und Überwachen des Verkehrs - Zoll- und Grenzkontrollen 	<ul style="list-style-type: none"> - Primäreinsätze (medizinische Not- und Rettungseinsätze) - Sekundäreinsätze (Transport von Kranken und Verletzten) - Unterstützung bei Grossanlässen
Prozesse, die sämtliche Blaulichtorganisationen betreffen		
<ul style="list-style-type: none"> - Bewältigen von Grosseinsätzen und ausserordentlichen Lagen - Entgegennahme von Notrufen und Einsatzkoordination - Unterhalt der Infrastruktur 		

Relevante Gefährdungen für den kritischen Teilsektor



Cyber-Angriff



Ausfall Telekommunikation



Strommangellage

Hinweis: Die untersuchten Gefährdungen sind für den gesamten Teilsektor relevant. Für einzelne Unternehmen / kritische Infrastrukturobjekte können weitere Risiken relevant sein.

Verwundbarkeiten und Risiken

Die Blaulichtorganisationen weisen eine generell tiefe Verwundbarkeit auf. Dies liegt einerseits an den breit vorhandenen Notstromeinrichtungen und den teils hohen Treibstoffreserven. Andererseits tragen die dezentralen Organisations- und Führungsstrukturen und die Tatsache, dass sich die Blaulichtorganisationen in vielen Bereichen gegenseitig unterstützen können, zur geringen Verwundbarkeit bei.

Die Wahrscheinlichkeit, dass eine allein auftretende Gefährdung zu einer massiven Beeinträchtigung der Blaulichtorganisationen mit gravierenden Konsequenzen für Bevölkerung und Wirtschaft führt, ist - Stand heute - tief. Die oben aufgeführten Gefährdungen können jedoch die Einsatzdisposition und -führung stark erschweren und Verzögerungen bei Schutz- und Rettungseinsätzen zur Folge haben. Aufgrund der hohen Zeitkritikalität können diese Verzögerungen zu erhöhten Personenschäden (Tote und Verletzte) als auch zu erhöhten Schäden im Bereich von Infrastruktur und Umwelt führen. Zudem können selbst geringe Einschränkungen bei Blaulichtorganisationen zu einem Vertrauensverlust von Seiten der Bevölkerung führen.

Ein erfolgreicher Cyber-Angriff auf eine Notruf- bzw. Einsatzleitzentrale kann dazu führen, dass zentrale IT-Systeme (z .B. Einsatzleitsysteme ELS) für einen gewissen Zeitraum nicht mehr zur Verfügung stehen. Dies kann zu massiven Einschränkungen bei der Abwicklung von Notrufen sowie der Koordination von Einsätzen innerhalb und zwischen den Blaulichtorganisationen führen. Aufgrund der teils vorhandenen Inkompatibilität zwischen ELS sowie den rechtlichen Grundlagen (z. B. Polizeigesetzen), die teils keinen Datenaustausch zwischen Kantonen zulassen, sind die Unterstützungsmöglichkeiten zwischen den Kantonen eingeschränkt. Dies wirkt sich insbesondere auf die Entgegennahme von Notrufen sowie die Einsatzdisposition aus. Ein erhöhter Koordinationsaufwand und Zeitverluste insbesondere bei Primäreinsätzen der Sanitäts- und Rettungsdienste können lebensbedrohliche Folgen haben.

Der Ausfall eines grossen, landesweit tätigen Telekomanbieters schränkt die Operationsfähigkeit von Blaulichtorganisation ein. Solche Einschränkungen liegen unter anderem im Bereich der breitbandigen, mobilen Datenkommunikation sowie im Aufbieten von Angehörigen der Feuerwehr. Dies macht aufwändige Umgehungslösungen notwendig und führt zu Einschränkungen und Verzögerungen bei zeitkritischen Dienstleistungen.

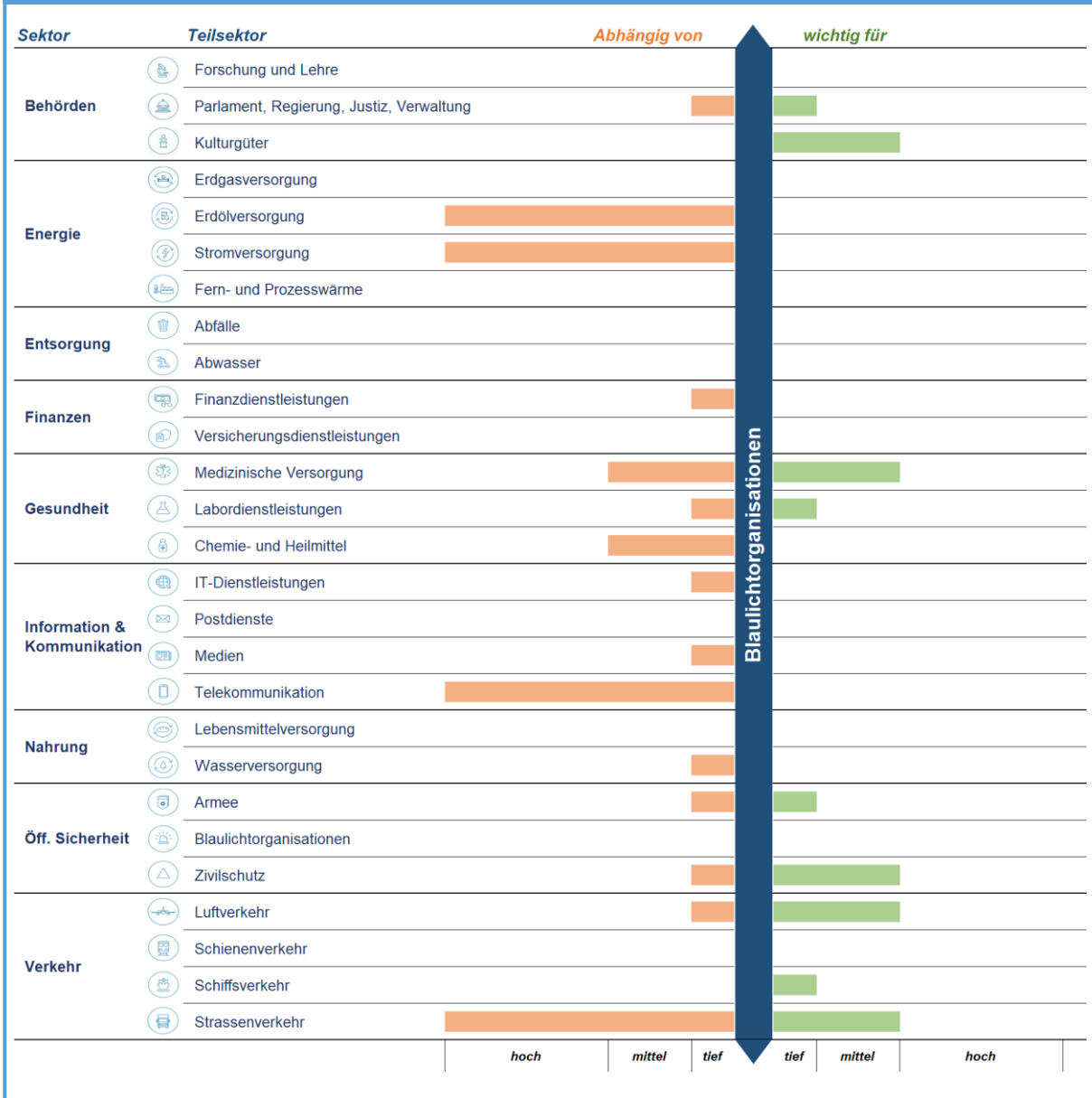
Eine länger dauernde Strommangellage führt zu kommunikationsbedingten Einschränkungen innerhalb der Blaulichtorganisationen und zu einer notwendigen Priorisierung von Tätigkeiten.

Massnahmen zur Verbesserung der Resilienz

Auf Basis der Verwundbarkeit und Risiken werden Massnahmen zur Förderung der Resilienz des Teilssektors Blaublichtorganisationen abgeleitet. Diese bewegen sich in folgenden Bereichen:

- **IKT-Minimalstandard spezifisch für die Blaublichtorganisationen:** Standard zur Förderung der IKT-Widerstandsfähigkeit von Blaublichtorg. (insbesondere von Notruf-/Einsatzleitzentralen).
- **Evaluation einer flächendeckenden Einführung autarker Alarmierungsmittel:** Reduzierung der Abhängigkeit von öff. Telekommunikationsanbietern bei der Alarmierung von Einsatzkräften.
- **Konzept zum selbständigen Einrücken bei einem Ausfall der Kommunikationssysteme:** Entwicklung und Einführung von Standardverhalten von sich nicht im Dienst befindenden Einsatzkräften bei einem Stromausfall und/oder einem Ausfall sämtlicher Kommunikationssysteme.

Interdependenzen des Teilssektors Blaublichtorganisationen



Weitere Informationen zu SKI und NCS online unter:

www.infraprotection.ch

www.ncsc.admin.ch