



Nationale Strategien Schutz kritischer Infrastrukturen SKI / Cyber NCS

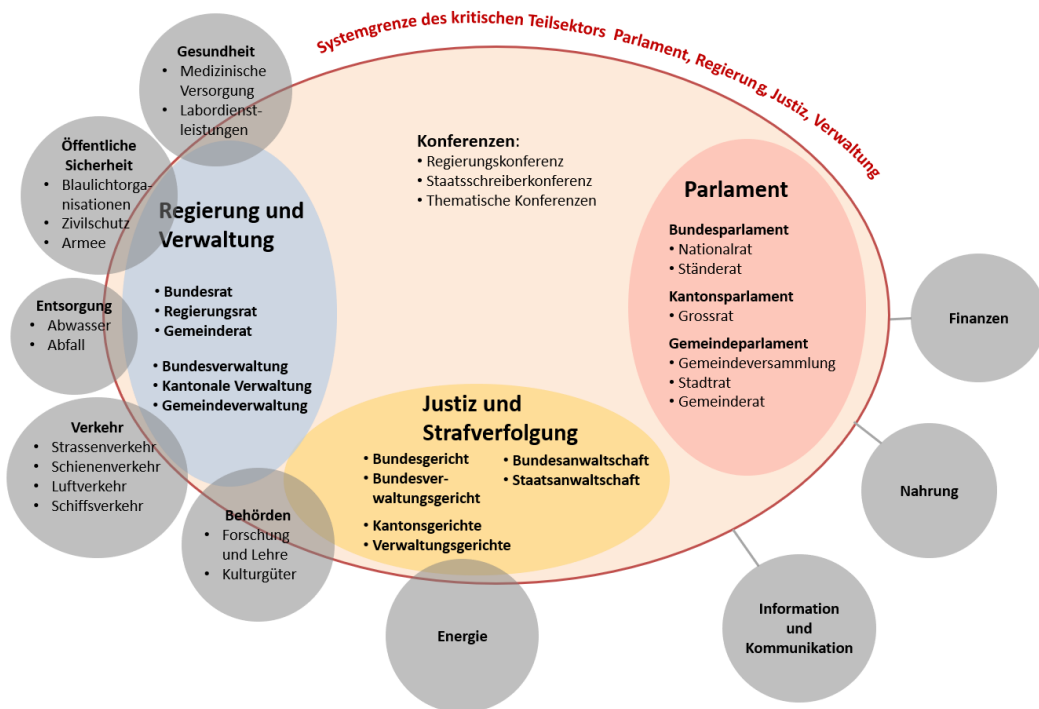
Factsheet zum kritischen Teilsektor Parlament, Regierung, Justiz, Verwaltung

Allgemeine Beschreibung und Versorgungsleistungen

Der Teilsektor Parlament, Regierung, Justiz, Verwaltung erbringt eine Vielzahl von wichtigen Dienstleistungen für die Bevölkerung und die Wirtschaft. Diese Dienstleistungen umfassen Gesetzgebung, Rechtsprechung und deren Vollzug sowie staatliche Verwaltungsleistungen, wie das Erteilen von Bewilligungen und deren Kontrolle. Bei den meisten dieser Dienstleistungen führen kurzfristige Störungen oder Ausfälle von einigen Stunden bis Tagen nicht zu gravierenden Schäden für Bevölkerung und Wirtschaft.

Zeitkritisch sind vor allem Prozesse in der Zollabwicklung des internationalen Handelswarenverkehrs, beim Betrieb von häufig genutzten Verzeichnissen und Registern (polizeiliche Datenbanken, Grundbücher, Wahlregister u. v. a.) und im Rahmen des Schutzes der Bevölkerung bei Gefahr (Information, Warnung und Alarmierung der Bevölkerung).

Die Behörden erbringen auch für alle anderen kritischen Sektoren relevante Leistungen. Aufgaben, die andere Teilsektoren direkt betreffen, z. B. die Aufsichtstätigkeit über Stauanlagen im Teilsektor Stromversorgung, werden jedoch direkt dort analysiert.



Marktanalyse / Systemstruktur

Der Teilsektor Parlament, Regierung, Justiz, Verwaltung hat eine dezentrale Struktur mit den Teilbereichen Exekutive, Legislative und Judikative sowie den drei Ebenen Bund, Kantone und Gemeinden. Innerhalb dieser Bereiche besteht der Teilsektor aus einzelnen systemrelevanten Akteuren, die in ihrem Verantwortungsbereich spezifische Aufgaben übernehmen. Diese Akteure können sich nur eingeschränkt gegenseitig unterstützen. Die Konsequenzen von Ausfällen sind jedoch räumlich begrenzt und, da viele Aufgaben zeitlich verschiebbar sind, meistens nicht zeitkritisch.

Untersuchte Prozesse

Im Rahmen der Risiko- und Verwundbarkeitsanalyse wurden 13 Prozesse näher untersucht, die entweder für die Funktionsfähigkeit der Behörden wichtig sind oder bereits kurzfristig eine wichtige Bedeutung für die Bevölkerung und die Wirtschaft haben:

| Parlament (Legislative) | Regierung und Verwaltung (Exekutive) | Justiz (Judikative) |
|--|--|--|
| Kernprozesse | Kernprozesse | Kernprozesse |
| <ul style="list-style-type: none"> – Erlassen von Gesetzen – Parlamentarische Beschlussfassung | <ul style="list-style-type: none"> – Allg. Verwaltungsdienstleistungen – Aufgaben zur Wahrung der inneren Sicherheit – Betrieb von Verzeichnissen und Registern – Schützen der Bevölkerung, Wirtschaft und Umwelt bei Gefahr – Sicherstellen politischer Rechte – Zollabwicklung | <ul style="list-style-type: none"> – Rechtsprechung – Strafverfolgung |
| Supportprozesse | Supportprozesse | Supportprozesse |
| <ul style="list-style-type: none"> – Unterstützungsleistungen der Parlamentsdienste | <ul style="list-style-type: none"> – Unterhalt Infrastruktur, inkl. IKT-Systeme | <ul style="list-style-type: none"> – Unterstützungsleistungen der Gerichtsdienste |

Relevante Gefährdungen für den kritischen Teilsektor



Cyber-Angriff



Ausfall Stromversorgung



Ausfall IKT



Konventioneller Anschlag

Hinweis: Die untersuchten Gefährdungen sind für den gesamten Teilsektor relevant. Für einzelne kritische Infrastrukture Objekte können weitere Risiken relevant sein.

Verwundbarkeiten und Risiken

Die grössten Verwundbarkeiten der untersuchten Prozesse liegen im Bereich von IKT-Systemen, die von Bund, Kantonen und Gemeinden gemeinsam genutzt werden. Diese sind stark abhängig vom Funktionieren der öffentlichen Telekommunikationsnetze und der eigenen Versorgung mit Elektrizität. Im Rahmen der Risikoanalyse wurden verschiedene Szenarien wie Cyber-Angriffe auf IKT-Systeme der Behörden (z. B. Datenbanken und Register), ein überregionaler Stromausfall, ein Ausfall eines zentralen IKT-Leistungserbringers sowie ein Anschlag auf eine bedeutende Einrichtung der Behörden untersucht.

Die Analyse zeigt, dass solche Ereignisse direkte wirtschaftliche und gesellschaftliche Schäden verursachen, z. B. können eine grosse Zahl von Aufgaben ohne Registerauszüge nicht abgewickelt werden. Gravierend können auch indirekte Folgeschäden aus solchen Ereignissen sein. Langanhaltende Ausfälle staatlicher Systeme oder Einrichtungen können zu einem Vertrauensverlust der Bevölkerung in die Behörden führen und die Reputation der Schweiz beeinträchtigen (mit Folgen für den Wirtschaftsstandort und den Tourismus).

Der Teilsektor Parlament, Regierung, Justiz, Verwaltung kann insgesamt als vergleichsweise resilient eingestuft werden. Diverse Projekte und Programme im Bereich der Stromversorgungs- und IKT-Resilienz befinden sich derzeit in Planung oder Umsetzung und werden zur weiteren Stärkung dieser Resilienz beitragen. Beispiele dafür sind der Rechenzentrumverbund oder das sichere Datenverbundnetz (SDVN). Es ist aber davon auszugehen, dass die bestehende Resilienz des Teilsektors aufgrund der weiter voranschreitenden Vernetzung von IKT-Systemen ohne begleitende Massnahmen in Zukunft abnehmen wird.

Resilienzmassnahmen

Verbesserung des Informationsaustausches

- Die Zusammenarbeit zwischen allen Ebenen (Bund, Kantone, Gemeinden) in den Bereichen Cyber-Risiken und IKT-Abhängigkeiten soll intensiviert werden.

Kommunikation im Ereignisfall

- Prüfung von Redundanzen im Bereich der Kommunikation mit den Schweizer Vertretungen im Ausland.
- Überprüfung der Information und Kommunikation während Ereignissen.
- Prüfung einer Nutzung respektive Anbindung an das sichere Datenverbundnetz SDVN.

Interdependenzen des Teilsektors Parlament, Regierung, Justiz, Verwaltung



Weitere Informationen zu SKI und NCS online unter:

www.infraprotection.ch

www.ncsc.admin.ch