Parldigi

Runder Tischer

Kritische IKT-Infrastrukturen – Gibt es politischen Handlungsbedarf bei der Beschaffung?

27. September 2023

Bundeshaus

Begrüssung

Parldigi

Niklaus-Samuel Gugger

Nationalrat und Kernteam Parldigi

Programm

Parldigi

13:15 Uhr *Begrüssung und Einführung ins Thema*
Niklaus-Samuel Gugger, Nationalrat und Mitglied Kernteam Parldigi

Nationale Strategie zum Schutz kritischer Infrastrukturen
Prof. Dr. Matthias Stürmer, Geschäftsleiter Parldigi

Kritische IKT-Infrastrukturen – aktuelle Herausforderungen im Bereich Cybersicherheit
Pascal Lamia, Stv. des Delegierten des Bundes für Cybersicherheit, NCSC

Beschaffungen kritischer IKT-Infrastrukturen aus beschaffungsrechtlicher Optik
Prof. Dr. Rika Koch, Fachgruppe Public Procurement der Berner Fachhochschule

Neue Ansätze bei der IKT-Beschaffung im Kontext der kritischen Infrastrukturen
Raffaello Dolci, Leiter Digital Acceleration Program & Swiss Public Services CISCO

Diskussion aktuelle Herausforderungen und mögliche politische Handlungsfelder

14:40 Uhr *Schlusswort und weiteres Vorgehen*
Niklaus-Samuel Gugger, Nationalrat und Mitglied Kernteam Parldigi

Co-Präsidium und Kernteam von Parldigi

Edith Graf-Litscher
Nationalrätin SP, Thurgau

Franz Grüter
Nationalrat SVP, Luzern

Gerhard Andrey
Nationalrat Grüne, Fribourg

Judith Bellaiche
Nationalrätin GLP, Zürich

Matthias Michel
Ständerat FDP, Zug

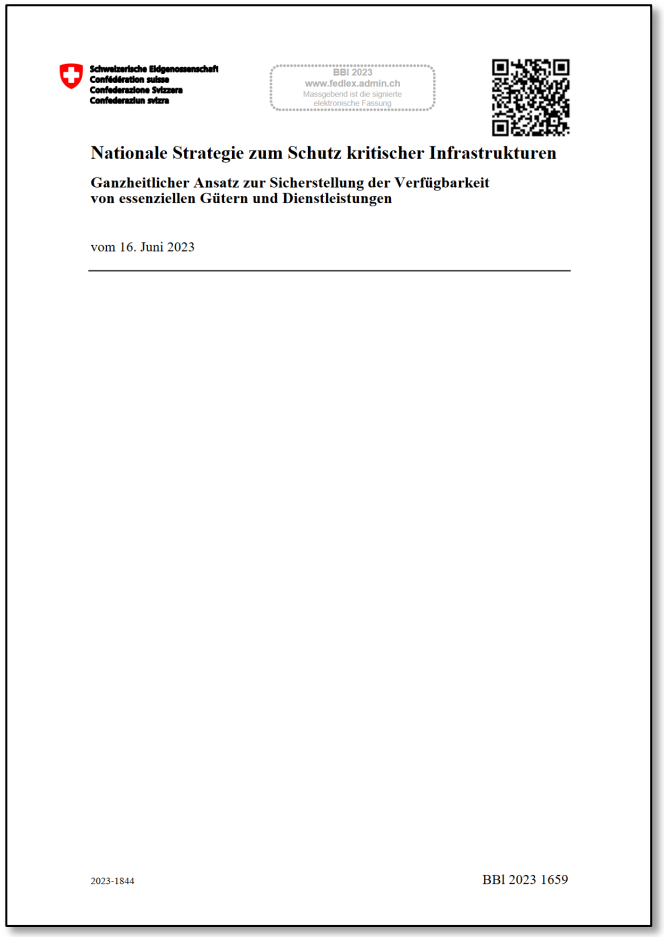
Nik Gugger
Nationalrat EVP, Zürich

Sidney Kamerzin
Nationalrat Mitte, Wallis

Nationale Strategie SKI

Parldigi

- Bundesrat hat am 16. Juni 2023 neue nationale Strategie zum **Schutz kritischer Infrastrukturen (SKI)** genehmigt
- **Unbefristete Gültigkeit** der Strategie SKI
- Zielsetzung ist Erhöhung der **Resilienz**
- **8 Massnahmen** an kritische Sektoren sowie Sektor-übergreifende Massnahmen
- Verzeichnis essenziell wichtige Objekte
- **Keine spezifische** Resilienzkriterien in der **IKT**



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 2023
www.fedlex.admin.ch
Massgebend ist die signierte elektronische Fassung

Nationale Strategie zum Schutz kritischer Infrastrukturen

Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen

vom 16. Juni 2023

2023-1844

BBl 2023 1659

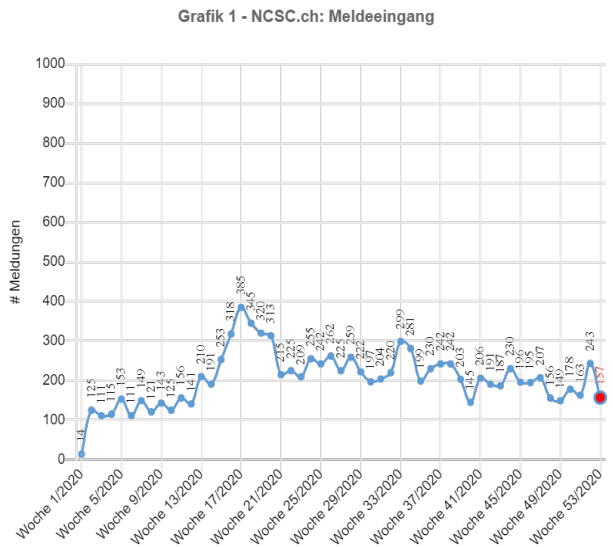
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

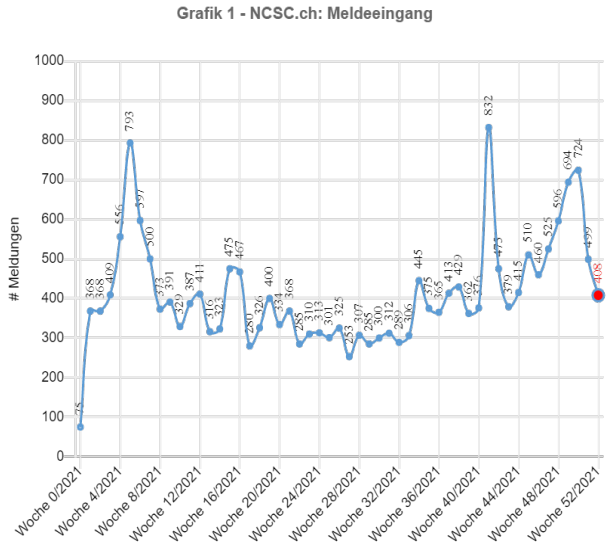
Aktuelle Herausforderungen im Cyberbereich

Pascal Lamia
Stellvertreter des Delegierten des Bundes für Cybersicherheit
Leiter der operativen Cybersicherheit im NCSC

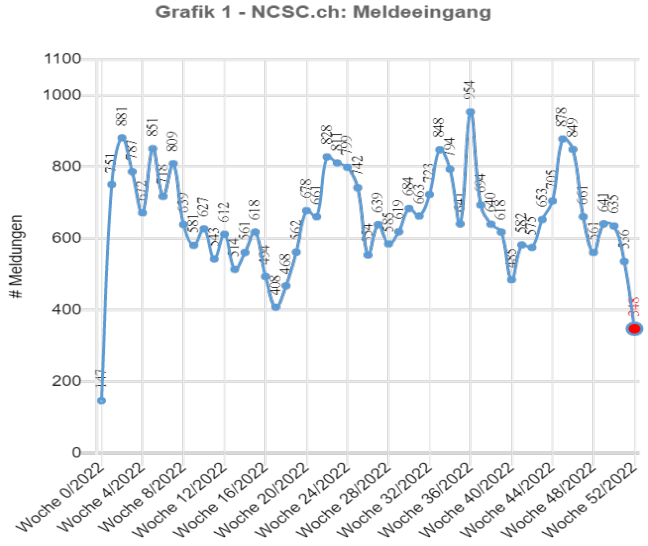
Was wird dem NCSC gemeldet
Meldungen 2020 - heute



2020
10833 Meldungen



2021
21714 Meldungen



2022
34527 Meldungen

Ziele der Meldepflicht

- **Frühwarnung und Übersicht zur Bedrohungslage:** mehr Informationen über Cyberangriffe ermöglichen es dem NCSC andere Organisationen schneller und präziser zu Warnen und eine gute Übersicht zur Bedrohungslage zu erhalten.

- **Rechtssicherheit- und gleichheit:** der freiwillige Informationsaustausch war lange sehr effizient. Er führt allerdings zum Problem des «Freeriding». Alle profitieren von den geteilten Informationen aber nicht alle sind bereit dazu, Informationen über Cyberangriffe zu teilen.

- **Internationaler Kontext:** mit der NIS-Direktive hat die EU 2018 eine Meldepflicht für Cyberangriffe für alle Mitgliedsstaaten eingeführt.

Die Meldepflicht im Informationssicherheitsgesetz (ISG)

- Das ISG ist ein relativ neues Gesetz (Beschluss 18. Dezember 2020), welches bisher ausschliesslich die Informationssicherheit des Bundes und teilweise der Kantone regelt.
- Das ISG tritt per 1. Januar 2024 in Kraft.
- Die Einführung der Meldepflicht wird als Revision des ISG umgesetzt. Das ISG wird so erweitert zu einem Informationssicherheitsgesetz mit Auswirkungen auf kritische Infrastrukturen.

➔ Die Meldepflicht tritt noch nicht am 1. Januar 24 in Kraft. Sie wird separat als Revision des Gesetzes beschlossen.

Wie es nicht sein sollte…

Das NCSC hat die folgende Meldung 41 Tage verspätet erhalten:

«Wir hatten am tt.mm.jjjj eine Ransomware Infektion und haben 0.8BTC bezahlt. Wollen nun eine Strafanzeige aufgeben. Eintrittsvektor vermutlich abcdefg mit vier ungepatchten Lücken und dann Verschlüsselung auf dem ESXi.»

Sie haben den Angreifer gefragt, was sie verbessern könnten.
Antwort:
"Just don't use old systems and update the network devices' firmware to the latest."

Der Schutz der Schweiz vor Cyberrisiken ist eine gemeinsame Aufgabe von Gesellschaft, Wirtschaft und Staat

Offene, ehrliche und transparente Kommunikation

ASR ASSOCIATION SÉCURITÉ RIVIERA

COMMUNE DE MONTREUX

COMMUNIQUE DE PRESSE
Cyberattaque contre la Commune de Montreux

Dans la matinée du dimanche 10 octobre 2021, les services de l'administration communale de Montreux ont constaté une attaque informatique.

Une cellule de crise a immédiatement été mise en place en collaboration avec l'Association Sécurité Riviera et la Police cantonale vaudoise. Les faits ont été portés à la connaissance des autorités pénales.

Une analyse approfondie a démarré avec le support d'experts du Canton et de la Confédération, ainsi que d'un partenaire externe spécialisé pour fournir une réponse adéquate à un tel événement.

Les premières mesures techniques d'urgence ont d'ores et déjà été prises. Une évaluation des impacts pour les différents partenaires ayant recours aux prestations du service informatique montreusien est en cours.

Dans un souci de transparence, la cellule de crise communiquera régulièrement les nouveaux éléments en sa possession via les réseaux sociaux de la Commune de Montreux et de l'ASR, ainsi qu'au moyen du site internet www.montreux.ch.

Clarens, le 10 octobre 2021

Pour toutes demandes complémentaires :
- ASR : Dounya Schürmann-Kabouya, Chargée de communication 076 501 45 99 – communication@securiviera.ch

Der Bundesrat › WBF › SECO

Einkaufskorb

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Staatssekretariat für Wirtschaft

Wirtschaftslage & Wirtschaftspolitik | Aussenwirtschaft & Wirtschaftliche Zusammenarbeit | Arbeit | Standortförderung | Werbe- und Geschäftsmethoden | Publikationen & Dienstleistungen | Das SE

SECO - Staatssekretariat für Wirtschaft › Das SECO › Medienmitteilungen › Medienmitteilungen 2021 - SECO › Cyberangriff auf E

‹ Das SECO

Medienmitteilungen

- Medienmitteilungen 2023 - SECO
- Medienmitteilungen 2022 - SECO
- Medienmitteilungen 2021 - SECO
- Medienmitteilungen 2020 - SECO
- Medienmitteilungen 2019 - SECO
- Medienmitteilungen 2018 - SECO
- Medienmitteilungen 2017 - SECO
- Medienmitteilungen 2016 - SECO
- Medienmitteilungen 2015 - SECO
- Medienmitteilungen 2014 - SECO
- Medienmitteilungen 2013 - SECO

‹ Zurück zur Übersicht

Cyberangriff auf EasyGov

Bern, 21.10.2021 - Kriminellen Hackern ist es mutmasslich gelungen, eine Liste mit Namen von bis zu 130'000 Unternehmen zu entwenden, welche über die Plattform EasyGov im Jahr 2020 einen Covid-19-Kredit beantragt hatten. Weitere Daten ausser den Firmennamen wurden nach heutiger Erkenntnis nicht gestohlen. Das SECO, als Betreiberin von Easy-Gov, hat Sofortmassnahmen ergriffen und eine Untersuchung eingeleitet.

Über die Web-Plattform www.easygov.swiss gelang es im August 2021 kriminellen Hackern mittels einer automatisierten Abfrage, mutmasslich eine Liste mit Namen von bis zu 130'000 Unternehmen zu stehlen. Diese Unternehmen hatten im Jahr 2020, auf dem Höhepunkt der pandemiebedingten Wirtschaftskrise, einen Covid-19-Kredit beantragt.

Nicht betroffen sind jene Firmen, welche den Kredit schon vollständig zurückbezahlt haben, sowie alle vertraulichen Unternehmensdaten wie Bankverbindung, IBAN-Nummer, Kontaktpersonen, etc. Der Kreditbetrag als Teil der angegriffenen Datensammlung wurde von den Hackern nicht abgegriffen. Die Daten der auf EasyGov registrierten Unternehmen sind ebenfalls nicht betroffen.

"Der Cyberangriff hat uns insgesamt weit über 1 Million Franken gekostet"

Von Reto Vogt, 20. September 2023 um 16:39

SECURITY PLAY UNICO DATA RANSOMWARE IT-DIENSTLEISTER CYBERANGRIFF

Vince Lehmann, CEO von Unico Data

Der IT-Dienstleister Unico Data wurde Ende Mai Opfer eines Ransomware-Angriffs. Im Interview blickt CEO Vince Lehmann zurück und spricht über Kosten, Versicherungen und Kundenreaktionen.

Unico Data, IT-Dienstleister aus dem bernischen Münsingen, wurde Ende Mai von der Ransomware-Bande Play angegriffen. Es war einschneidend: Alle Dienstleistungen des Unternehmens und zahlreiche Kunden waren offline. Vier Monate nach dem Angriff gibt CEO Vince Lehmann im Interview transparent Auskunft darüber, wie sein Unternehmen die Situation bewältigte, inwiefern ihm dabei Versicherungen halfen und welche Ratschläge er anderen Unternehmen geben würde.

Besten Dank für Ihre Aufmerksamkeit

Pascal Lamia
Stv. des Delegierten des Bundes für Cybersicherheit
Leiter der operativen Cybersicherheit

Schwarztorstrasse 59
3003 Bern
pascal.lamia@gs-efd.admin.ch
www.ncsc.admin.ch

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Kritische IKT-Infrastrukturen: Perspektive öffentliches Beschaffungsrecht

«Runder Tisch zu Öffentliche Beschaffungen kritischer IKT-Infrastrukturen» am 27.09.2023

Prof. Dr. Rika Koch, Berner Fachhochschule BFH, Fachgruppe Public Procurement

«Strategie zum Schutz kritischer Infrastrukturen 2023»

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 2023
www.fedlex.admin.ch
Massgebend ist die signierte elektronische Fassung

Nationale Strategie zum Schutz kritischer Infrastrukturen

Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen

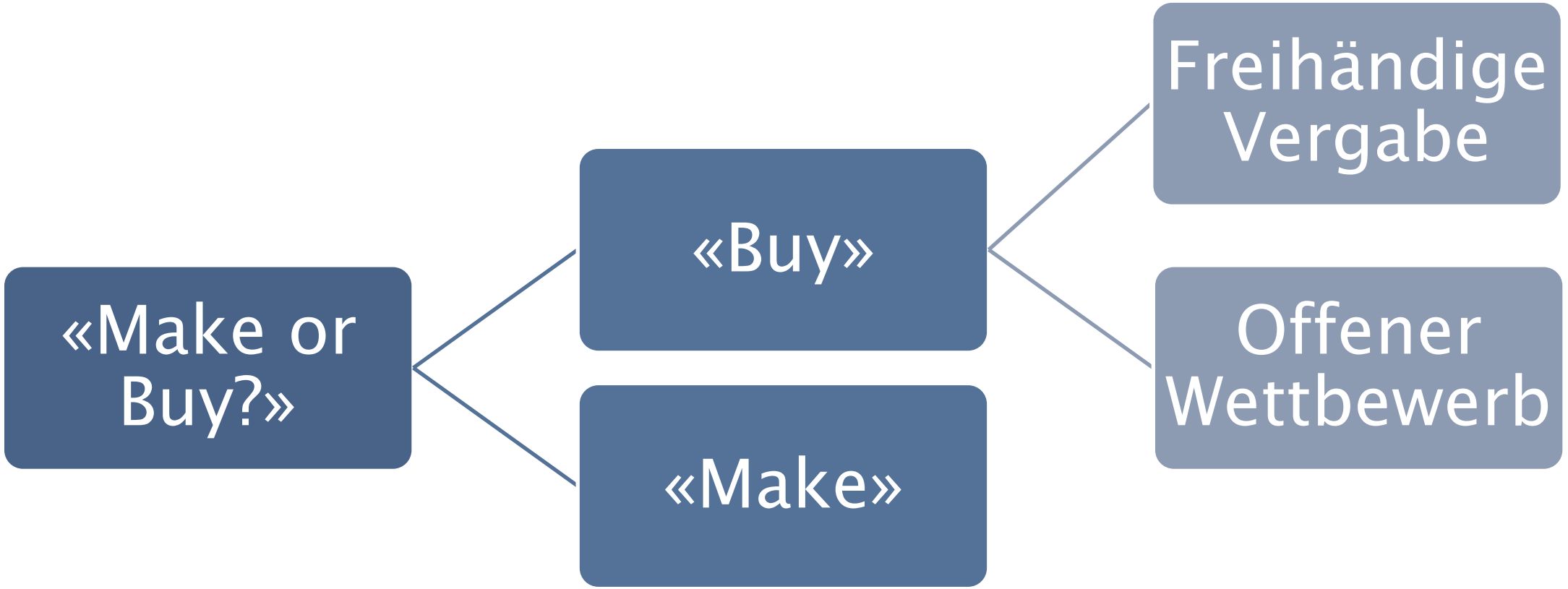
vom 16. Juni 2023

Ja klar, aber wie?

S. 9: *Zu prüfende Massnahmen [für den Schutz kritischer Infrastrukturen] können folgende Bereiche umfassen:*

- *Wahl eines **besonders sicheren Anbieters** bei Beschaffungsvorhaben.*

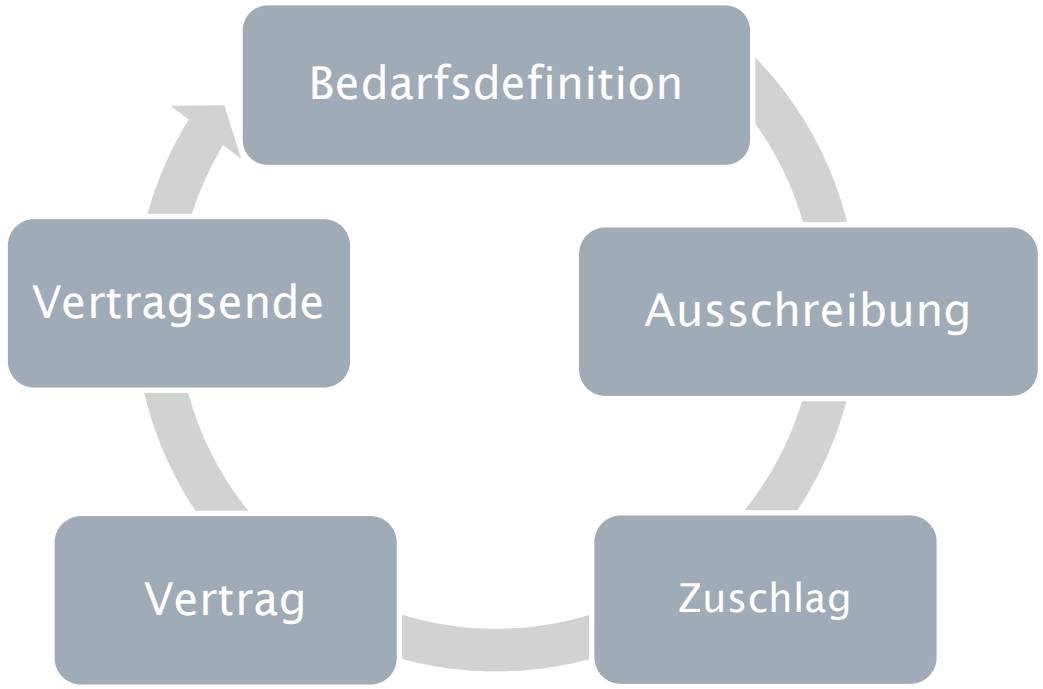
Kritische Infrastrukturen und öffentliche Beschaffung



Öffentliches Beschaffungsrecht als Problem oder als Lösung?

Herausforderungen bei einer öffentlichen Beschaffung (Auswahl):

1. Starre Regeln (innovationshemmend?)
2. Offener Wettbewerb, Gleichbehandlung ausländischer Anbieter
3. Preis (Preisdiktat)

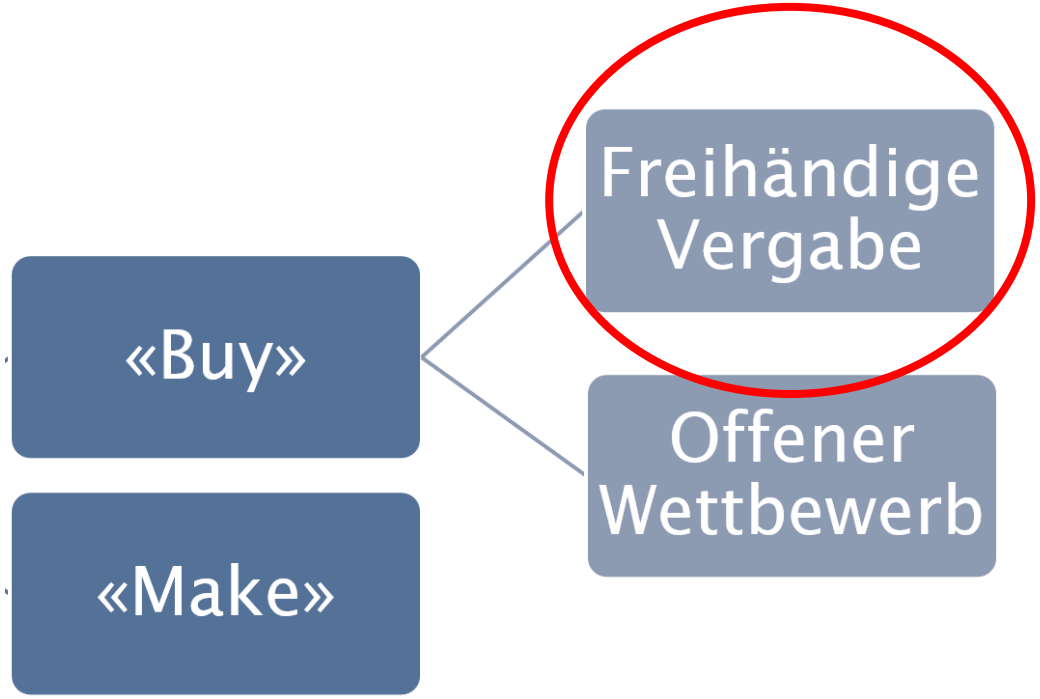


Freihändige Vergabe als Ausnahme

→ Direkte Vergabe an einen Anbieter ohne Wettbewerb

Ausnahmetatbestand: Art. 10 Abs. 4 lit. A BöB/IVöB

*Wenn dies für den **Schutz und die Aufrechterhaltung der äusseren und inneren Sicherheit** oder der **öffentlichen Ordnung** als **erforderlich erachtet** wird.*



Freihändige Vergabe als Ausnahme

→ Direkte Vergabe an einen Anbieter ohne Wettbewerb

Ausnahmetatbestand: Art. 10 Abs. 4 lit. a BöB/IVöB

*Wenn dies für den **Schutz und die Aufrechterhaltung der äusseren und inneren Sicherheit** oder der **öffentlichen Ordnung** als **erforderlich erachtet** wird.*

1. *«Äussere und innere Sicherheit»: Rüstungsgüter, aber auch andere (militärischen oder zivile) Leistungen, die sicherheitskritisch sind.*
2. *«Öffentliche Ordnung»: ?? (siehe Art. III WTO/GPA, «public morals»), aber nur wenn dies gem. WTO/GPA nicht zu «willkürlicher Diskriminierung» oder «verstecktem Protektionismus» führt.*
3. *«Als erforderlich erachtet»: «Weichgespülte» Verhältnismässigkeitsprüfung mit subjektiver Komponente.*

Freihändige Vergabe als Lösung?

Herausforderungen

1. Starre Regeln (innovationshemmend?)
2. Offener Wettbewerb, Gleichbehandlung ausl. Anbieter
3. Preis (Preisdiktat)

Lösung?

1. Keine Regeln, Abweichungen vom Pflichtenheft möglich
2. Kein Wettbewerb, Bevorzugung nationaler Anbieter möglich
3. Preis spielt keine Rolle

→ Nur möglich, wenn zum **Schutz der Sicherheit** oder aus **Gründen der öffentlichen Ordnung** «als erforderlich erachtet».

Offener Wettbewerb

Art. 18

1. *Im offenen Verfahren schreibt die Auftraggeberin den Auftrag öffentlich aus.*
2. *Alle Anbieterinnen können ein Angebot einreichen.*

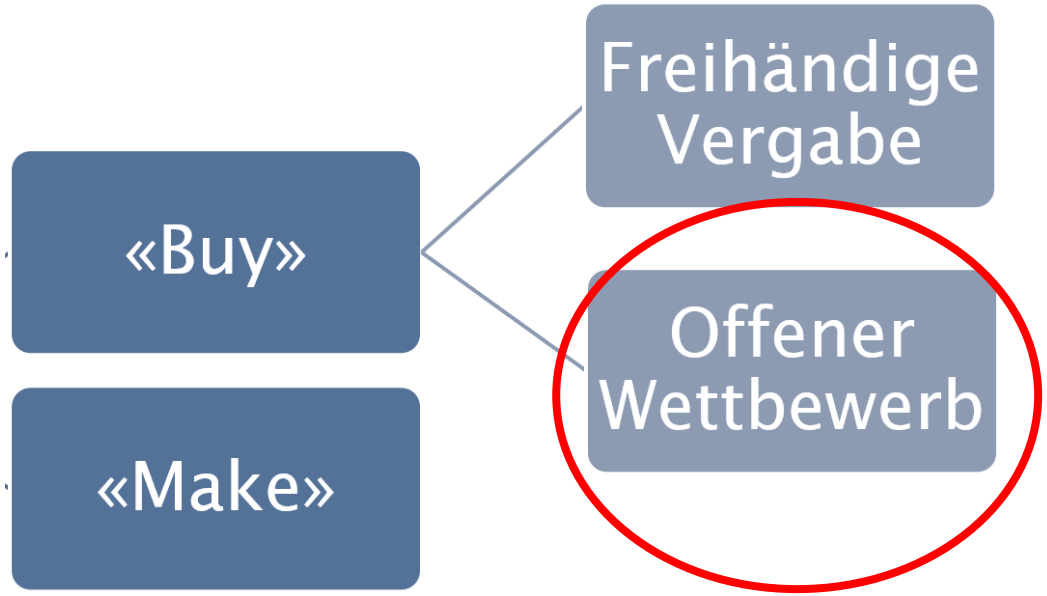
Art. 2

1. *Dieses Gesetz bezweckt den (…) nachhaltigen Einsatz der öffentlichen Mittel.*

Art. 41

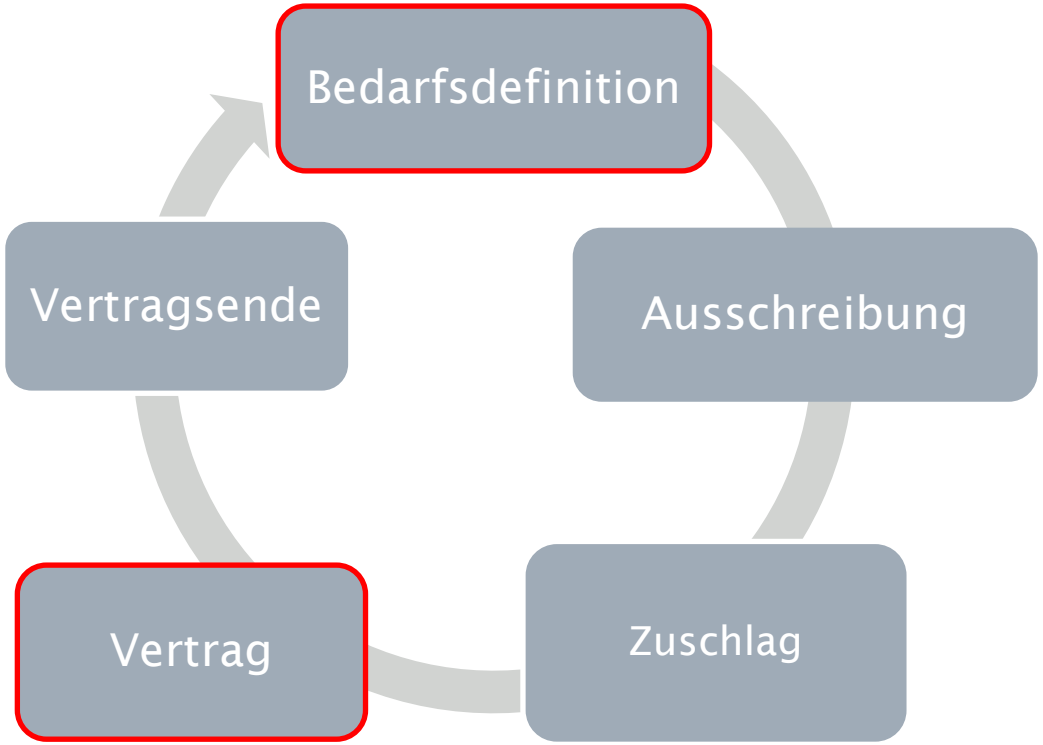
*Das **vorteilhafteste** Angebot erhält den Zuschlag.*

→ Qualitäts- statt Preiswettbewerb unter dem revidierten Beschaffungsrecht!



Implementierung sicherheitsrelevanter Kriterien im Beschaffungsprozess

Sicherheitsrelevante Kriterien müssen zwingend in der Ausschreibung eingefordert und vertraglich durchgesetzt werden!



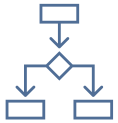
Beschaffungskriterien in Bezug auf IT-Sicherheit

Zum Beispiel:

Gesetzliche Grundlage Datenbearbeitung

Umsetzung der technischen Massnahme (Verschlüsselung etc.)

Einwilligung in mögliche Audits



Meldepflichten (Datenleaks, Cybervorfälle etc.)

Art und Umfang der Datenbearbeitung, und Verzeichnis (RoPA)

Schweizer Recht/ Gerichtstandort Schweiz

Datenlöschung!

Georedundanz

Managementsystem Cybersicherheit (z.B. ISO 27001)

Schnittstellen-management

Ausschreibung im offenen Wettbewerb als Lösung wenn…

Herausforderungen

1. Starre Regeln (Innovationshemmend?)
2. Offener Wettbewerb, Gleichbehandlung ausländische Anbieter
3. Preis

Lösung

1. Neue Flexibilitätsinstrumente im BöB 2021 nutzen für mehr Innovation
2. Wettbewerb kann zu höherer Qualität führen→ Kriterien IT-Sicherheit einfordern (in der Ausschreibung)
3. Kein Preisdiktat sondern **Qualitätswettbewerb** («vorteilhaftestes Angebot»)

Fragen?

Vielen Dank!

Rika Koch
Rika.koch@bfh.ch

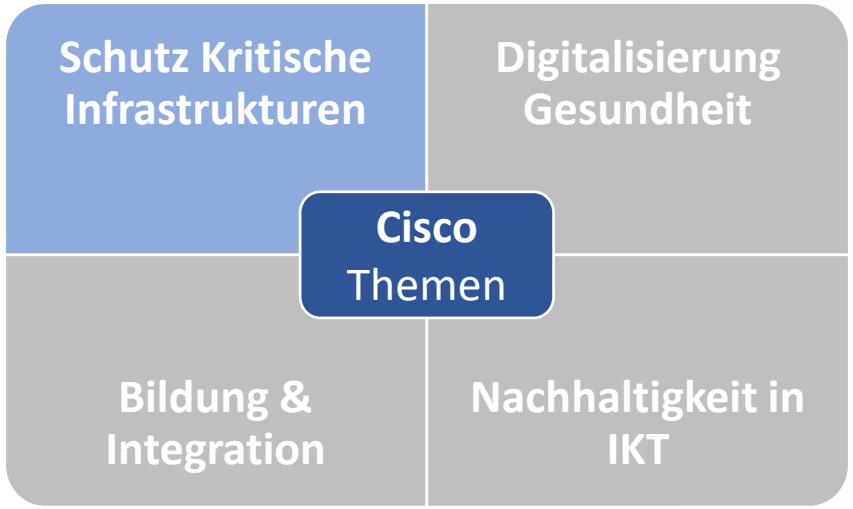
https://www.bfh.ch/de/forschung/forschungsbereiche/public-sector-transformation/public-procurement/

Sicherung kritische Infrastrukturen

Raffaello Dolci, Direktor des CISCO Digital Acceleration Program

Create value for the country, its economy and citizens

SCHUTZ KRITISCHER INFRASTRUKTUREN – EIN KERN-THEMA FÜR CISCO



Cisco's CDA Fokus-Themen

Überbrückung der digitalen Kluft, Chancengleichheit, diskriminierungs-freier Zugang zu Dienstleistungen

Schutz der Schweizer Bevölkerung, des öffentlichen Dienstes und der Wirtschaft vor Cyberrisiken

Die Exzellenz der Schweiz in Bildung, Forschung und Innovation weiterentwickeln

Aufwertung, um neue Jobs und digitale Wachstumschancen zu generieren

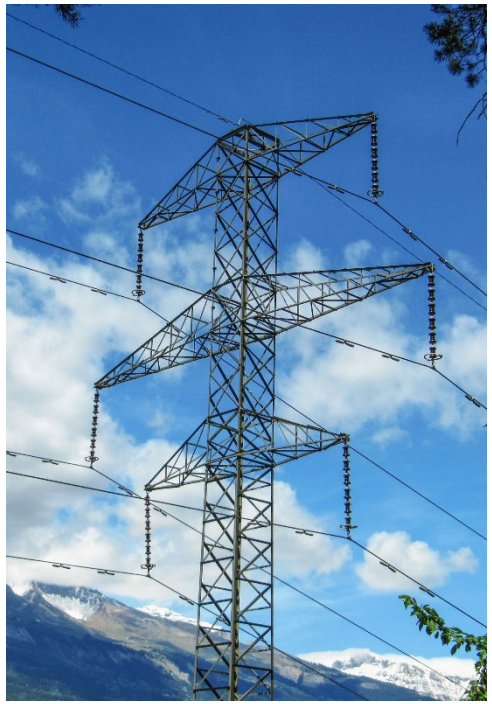
Sicherung der nationalen kritischen Infrastrukturen, senken der Betriebskosten und verbessern der Kundenerfahrung

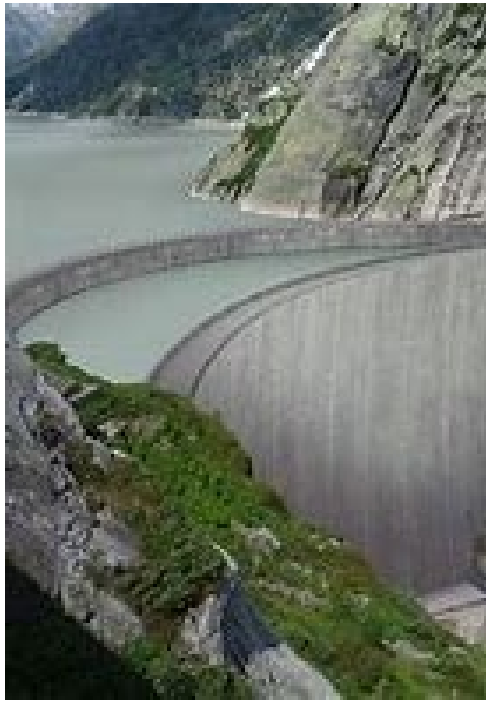
Den hohen Standard der Schweizer Gesundheitsversorgung aufrechter-halten und weiterentwickeln

KRITISCHE INFRASTRUKTUREN SIND BESONDERS SCHÜTZENSWERT

- **Kritische Infrastrukturen (KI)** sind speziell – KI sind Prozesse, **Systeme und Anlagen**, die für das **Funktionieren der Wirtschaft** sowie für die **Lebensqualität** der Schweizer Bevölkerung **von wesentlicher Bedeutung** sind.

- Deshalb sind im Kontext von KI **zusätzliche Kriterien bei Ausschreibungen erforderlich**, um diese besser zu schützen.





HERAUSFORDERUNG AUSSCHREIBUNG

- **CISCO** betreibt **ICT-Lösungen in** der **Schweiz** und im **Ausland**.
- Wir stellen fest, **Bietenden** sind **nicht immer im Klaren**, dass bei KI **zusätzliche** & besondere **Aspekte** zu berücksichtigen sind.
- Sobald öffentliche Ausschreibung läuft, wird **Auftrag an externe Beratende** vergeben, die zwar über technologische Kompetenzen, aber nicht immer über System-Verständnis verfügen.
- Erfahrung zeigt, dieselben Organisationen betrauen dieselben Beratenden mit Mandaten. RfP beschreibt oft Funktionalitäten, die den Beratenden selbst bekannt sind (**Cyber-EMPA** zum **Validieren RfP**-Dokumente und Auswahlkriterien zur Stärkung Systemkompetenz).

- Regeln sind so streng geworden, dass **Kosten für Vorbereitung** bei **Ausschreibung explodieren**.
- Vor 10 Jahren erstreckten sich **Ausschreibungen** über einen Zeitraum von 5 Jahren, der um 3 Jahre verlängert werden konnte. **Heute** werden öffentliche Aufträge **für 10 bis 15 Jahre vergeben**, um zu vermeiden, dass zu oft Ausschreibungen durchgeführt werden müssen.
- Bei der **Vergabe** öffentlicher Auftrag: **Zu grosses Gewicht auf Preis-/Leistung**, was zu Situationen führt, in denen man evtl. gezwungen ist, mit Lieferanten/Dienstleister zusammenzuarbeiten, welche die eigene Strategie nicht unbedingt unterstützen.
- **Ausserbetriebnahme** oder Migration der **IKT-Lösung** am Ende ihres Lebenszyklus ist fast nie Gegenstand von Ausschreibungen.

ENTSCHEIDENDE FAKTOREN AUSSCHREIBUNG

Transparenz

- **Transparenz technische Eigenschaften**: Betrifft das System und seine Komponenten.
- **Lieferantentransparenz**: finanzielle oder geografische Abhängigkeit, Informationen zu Lieferketten, finanzielle Stabilität und Transparenz, Aktionäre, usw.
- **Transparenz** über den **gesamten Lebenszyklus**: Upstream, bei Installation, Betrieb und Demontage/ Stilllegung – Know-how, Schulungen, Übungen und langfristiges Engagement vor Ort.

Resilienz (Widerstandsfähigkeit)

- Resilienz in **Prozess, Betrieb und System**
- Resilienz der **Gesamtarchitektur** – Sicherheit einzelner Elemente garantiert nicht Sicherheit des Gesamtsystems.

Insbesondere im Kontext der **Abhängigkeit von ausländischen Lieferanten und Produkten** ist die Betrachtung des gesamten Systems – und nicht nur einzelner Elemente – unerlässlich.

- Resilienz durch **Regenerationsfähigkeit im Krisenfall** – Gute Vorbereitung, Einsatz etablierter Technologien sowie lokales Know-how und Ressourcen, die im Krisenfall abgerufen werden können als Voraussetzung. Dadurch möglich, Abhängigkeiten IKT von Lieferanten zu reduzieren.
- Resilienz dank **intelligenter Abbaukapazität** – Systeme erforderlich, die im Krisenfall Speicherung kritischer Daten auf Servern in der Schweiz gewährleistet oder sicherstellen, das Gesamtsystem weiterhin funktioniert trotz Energieknappheit.

KRITISCHE INFRASTRUKTUREN – ENTSCHEIDENDE FAKTOREN AUSSCHREIBUNG

- > Sicherheit muss von Anschaffungsentscheid bis Ende Lebenszyklus gewährleistet sein.
- > Es gibt keine hundertprozentige Sicherheit. Schweiz ist in diesem Bereich auf Importe angewiesen.
- > Neue Kriterien für Transparenz & Resilienz beim Erwerb KI IKT können höhere Sicherheit bieten.
- > Folgen eines IK-Ausfalls für Wirtschaft und Gesellschaft dürfen nicht vernachlässigt werden.

Diskussion

Pascal Lamia
Nationales Zentrum für Cybersicherheit (NCSC)

Rika Koch
Berner Fachhochschule

Raffaello Dolci
CISCO

Moderation: **Matthias Stürmer,** Parldigi

Verabschiedung

Parldigi

Niklaus-Samuel Gugger

Nationalrat und Kernteam Parldigi

Nächster Parldigi-Anlass

Parldigi

Mittwoch, 20. Dezember 2023 von 13.15 bis 14.45 Uhr im Bundeshaus:

Was ist «vertrauenswürdige Cybersecurity» und wie kann diese gewährleistet werden?

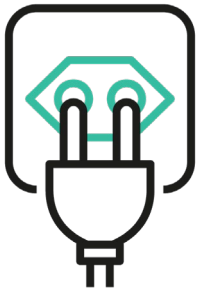
Anlass in Zusammenarbeit mit **SNF NFP77-Projekt** «Mit Ethik und Recht das Vertrauen in die Cybersicherheit fördern» (PD Dr. Markus Christen, Digital Society Initiative, Universität Zürich)

Kernthemen von Parldigi

Parldigi

Open Source Software

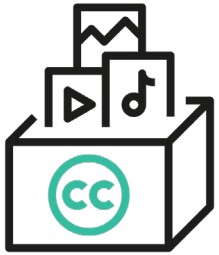
Open Access



Open Standards

Open Government

Open Data



Open Content

Open Internet

Partner und Träger von Parldigi

Parldigi

Adfinis

camptocamp

CH Open
Source | Business | Community

cubetech

nts

digitalswitzerland

PUZZLE ITC
changing IT for the better

redhat

snowflake

SUSE

WIKIMEDIA
CH

Mitgliedschaft beim Verein Parldigi

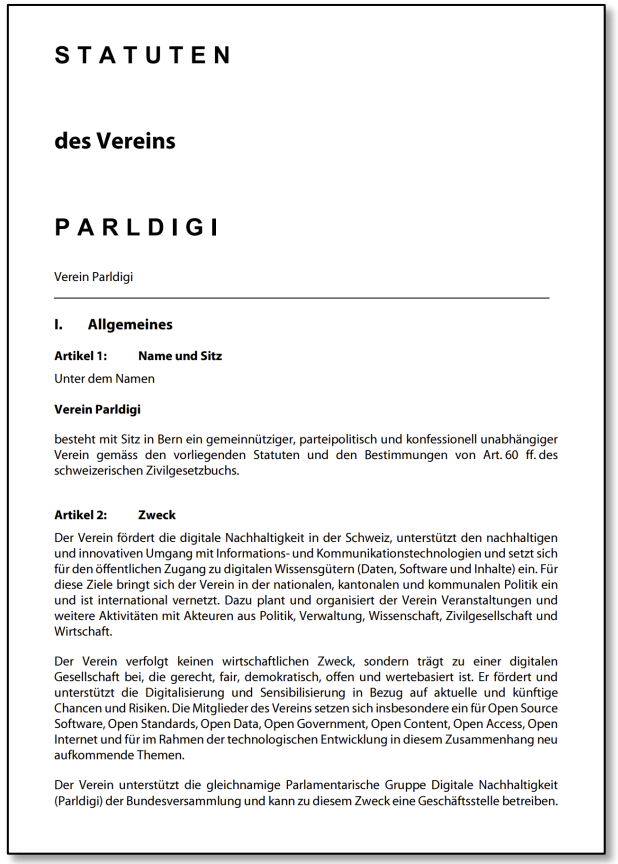
Parldigi

Verein Parldigi gegründet im Dezember 2021

Arten der Mitgliedschaft:

1. **Juristische Personen:** Firmen, Verbände, Behörden etc.
2. **Natürliche Personen:** aktuelle und ehemalige Politiker*innen aus allen föderalen Ebenen (gewählte Amtsträger*innen)
3. **Gäste:** Einzelpersonen

Weitere Infos und Anmeldung auf
www.parldigi.ch/de/ueber-parldigi/verein/



STATUTEN

des Vereins

PARLDIGI

Verein Parldigi

I. Allgemeines

Artikel 1: Name und Sitz

Unter dem Namen

Verein Parldigi

besteht mit Sitz in Bern ein gemeinnütziger, parteipolitisch und konfessionell unabhängiger Verein gemäss den vorliegenden Statuten und den Bestimmungen von Art. 60 ff. des schweizerischen Zivilgesetzbuchs.

Artikel 2: Zweck

Der Verein fördert die digitale Nachhaltigkeit in der Schweiz, unterstützt den nachhaltigen und innovativen Umgang mit Informations- und Kommunikationstechnologien und setzt sich für den öffentlichen Zugang zu digitalen Wissensgütern (Daten, Software und Inhalte) ein. Für diese Ziele bringt sich der Verein in der nationalen, kantonalen und kommunalen Politik ein und ist international vernetzt. Dazu plant und organisiert der Verein Veranstaltungen und weitere Aktivitäten mit Akteuren aus Politik, Verwaltung, Wissenschaft, Zivilgesellschaft und Wirtschaft.

Der Verein verfolgt keinen wirtschaftlichen Zweck, sondern trägt zu einer digitalen Gesellschaft bei, die gerecht, fair, demokratisch, offen und wertebasiert ist. Er fördert und unterstützt die Digitalisierung und Sensibilisierung in Bezug auf aktuelle und künftige Chancen und Risiken. Die Mitglieder des Vereins setzen sich insbesondere ein für Open Source Software, Open Standards, Open Data, Open Government, Open Content, Open Access, Open Internet und für im Rahmen der technologischen Entwicklung in diesem Zusammenhang neu aufkommende Themen.

Der Verein unterstützt die gleichnamige Parlamentarische Gruppe Digitale Nachhaltigkeit (Parldigi) der Bundesversammlung und kann zu diesem Zweck eine Geschäftsstelle betreiben.