Souveräne Internet-Dienste: Ein mehrstufiges Unterfangen

Marcel Waldvogel • 9. September 2026



George Becker bei Pexels , PD-ähnlich

Wer seine eigenen Internetdienste souverän anbieten und nutzen will, steht vor mehreren Herausforderungen. Hier ein Überblick über die Stolperfallen und ein paar Rezepte zur Lösung, besonders für souveräne Domainnamen.

Inhalte

- Wieso Digitale Souveränität?
- Abhängigkeiten von Internet-Applikationen
- Wie funktionieren Internet-Domains?
  - Das Domain Name System (DNS)
  - Die Root-Zone
  - Top-Level-Domains
  - Second-Level-Domains
- Souveränität im DNS
  - Auswahl einer souveränen TLD
  - Weitere Souveränitätskriterien
- Weitere Souveränitätsrisiken
- Das Souveräne-Domain-Howto
- Weiterführende Literatur

Wieso Digitale Souveränität?

Donald Trump wirft in seiner zweiten Amtszeit nur so mit Executive Orders um sich, um beispielsweise Strafzölle und Sanktionen zu verhängen oder den Krieg zu erklären. Damit zeigt sich auch für die Öffentlichkeit, was vorher nur zwischen Experten diskutiert wurde: Unsere digitale Abhängigkeit ist sehr hoch, bei Online-Diensten vor allem gegenüber den USA.

Zu den verhängten Sanktionen zählen, in chronologischer Reihenfolge:

1. **2025-05-15: Karim Khan,** der Chefankläger des internationalen Strafgerichtshofs (IStGH; auch International Crimiinal Court, ICC) wird sanktioniert. Bussen oder Gefängnisstrafen drohen allen, die Khan «finanziell, materiell oder technologisch unterstützen». Seine Email- und Bankkonten wurden eingefroren, auch sein dienstliches ICC-Konto bei Microsoft. Bereits im Februar waren Sanktionen gegen das Gericht verhängt worden. Die Open Source Business Alliance (OSBA) betont in der Folge gegenüber Heise, «der US-Präsident könne per Dekret jede Organisation, die von US-Technologie abhängig ist, digital abschalten».
2. **2025-12-23: Gegen die HateAid**-Geschäftsführerinnen, die Gründerin des britischen Global Disinformation Index (GDI) und der Gründer des Center for Counter Digital Hate (CCDH) werden Sanktionen verhängt. Netzpolitik schreibt dazu: «Die USA belegen Menschen mit Sanktionen, weil sie demokratisch legitimierte Gesetze gegen Tech-Konzerne verteidigen.» Zum sanktionierten Personenkreis gehört ebenfalls der ehemalige EU-Kommissar **Thierry Breton**, der sich u. a. mit dem Digital Services Act (DSA) einen Namen machte, zu dessen Ziele es gehört, Verbraucher- und Grundrechte im Internet zu stärken, aber auch grosse Online-Plattformen zu einem Mindestmass und Transparenz und Rechenschaft zu verpflichten.
3. **2026-08-26: Dem italienischen Kollektiv Autistici/Inventati** wird ihre Domain autistici.org gesperrt, die von einer US-Organisation verwaltet wird; ebenfalls ist ihr Bankkonto inzwischen gesperrt und als Folge der Sanktionen haben sie angekündigt, ihren Dienst einzustellen (DNIP berichtete).

> Email- und Cloudkonten sowie ganze Internetdomains von unbescholtenen europäischen Organisationen sind also inzwischen von US-Sanktionen betroffen, oft einfach, weil der US-Präsident gerade ein Zeichen setzen möchte. Wer nicht möchte, dass seine/ihre Digitaldienste – privat oder als Organisation – das gleiche Schicksal erreicht, sollte entsprechende Vorbereitungen tätigen.

Entsprechend bietet dieser Artikel einen Einblick in die Abhängigkeiten von Internet-Applikationen und insbesondere der von ihnen verwendeten Domainnamen. Und wie man diese souveräner aufsetzt.

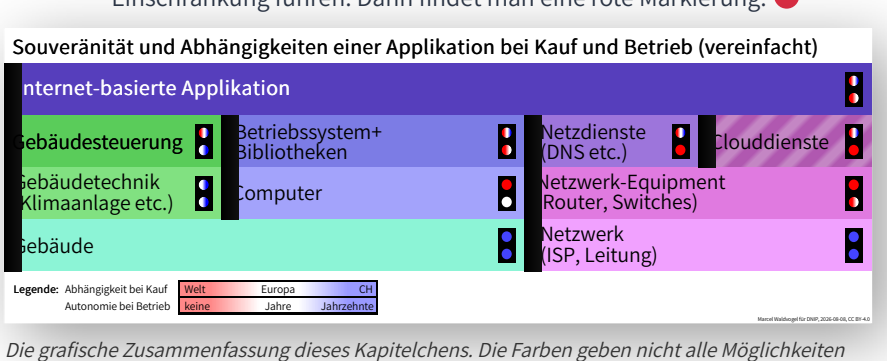
> Inklusive dem Tipp, welche 7 Domains für Schweizer:innen am souveränsten sind, aber auch, welche weiteren rund 100 Internet-Domänen nach einen Satz möglicher europäischen Souveränitätskriterien eine gute Wahl wären. (Die gesamte Domain-Souveränitätsliste ist hier bzw. zum Download.)

> **Email-Domains** sollten doppelt gut auf Souveränitätsrisiken geprüft werden. Mailadressen sind oft Teil von **Account-Zugangsprüfungen und Wiederherstellungsrozessen** („Magic Link„, Passwort-Reset, …). Der Verlust von Zugang zur Mailadresse kann auch den Verlust von Zugang zum Konto bedeuten, unter welchem man sich beim einem Online-Dienst angemeldet hat. Schlimmer noch: Ein allfälliger neuer Besitzer kann unter Umständen alle damit registrierten Konten übernehmen. **[Neu 2026-09-09]**

Abhängigkeiten von Internet-Applikationen

Jede Applikation, welche über das Internet angeboten wird, läuft auf irgendeinem Computer, meist einem Server in einem Gebäude. Ebenso benötigt es Internetverbindung und (heutzutage) meist auch eine Cloudanbindung. Bei jeder dieser Komponenten haben wir Abhängigkeiten vom Ausland, sowohl bei der Beschaffung als auch dann im Betrieb. Dazu müssen zwei Fragen geklärt werden. In der unteren Grafik sind diese Farben über zwei eingefärbte Kreise innerhalb einer schwarzen «Ampel» repräsentiert:

- Woher stammen die Komponenten, also die Computer, Router, Gebäudetechnik, Glasfasern oder die Gebäude selbst?
  - Am einfachsten ist es, wenn die Komponenten und ihre Vorprodukte lokal hergestellt werden. Diese sind in der folgenden Grafik mit blauen Punkten 🔵 oben markiert.
  - Werden die notwendigen Komponenten und ihre Vorprodukte in benachbarten (üblicherweise befreundeten) Ländern produziert? Oder werden sie von vielen verschiedenen Ländern und Regionen angeboten? Dann dürfte die Beschaffung auch noch relativ einfach sein. Dafür steht eine weisse Markierung ⚪ im oberen der Kreise einer Komponente.
  - Schwieriger wird es, wenn die Komponenten bzw. ihre Vorprodukte nur in wenigen Ländern produziert werden. Am grössten ist die Abhängigkeit, wenn diese Länder auch bereit sind bzw. in Zukunft bereit sein könnten, ihre Schlüsselposition auszuspielen und wir keinen Hebel haben, um ihren Machtspielen etwas entgegenzusetzen (also dass wir etwas haben, was sie unbedingt wollen). Hier wird oben ein roter Punkt gesetzt. 🔴
- Wenn wir die Komponenten gekauft haben, wie abhängig sind wir weiterhin vom Lieferanten bzw. vom Lieferland?
  - Können wir die Komponente über viele Jahre hinweg ohne grössere Einschränkung autonom weiterbetreiben, auch wenn der ursprüngliche Lieferant nicht mehr existiert oder in eine Wirtschaftsbeziehung mit uns treten will/kann? Dann ist der untere Kreis blau 🔵 markiert. Dazu zählen beispielsweise Gebäude, die auf Jahrzehnte ausgelegt sind.
  - Wenn schon nach wenigen Jahren allerdings Ersatzteile oder ein vollständiger Ersatz notwendig ist, ist die Komponente weiss ⚪ markiert. Hierzu gehören beispielsweise Computer, die etliche Jahre durchlaufen können mit minimaler Wartung.
  - Wenn hingegen eine dauerhafte Abhängigkeit besteht, wie beispielsweise bei Onlinediensten oder wenn Software nicht gekauft, sondern nur gemietet ist, kann ein Abbruch einer Wirtschaftsbeziehung in wenigen Sekunden bis wenigen Wochen bereits zu einer grossen Einschränkung führen. Dann findet man eine rote Markierung. 🔴



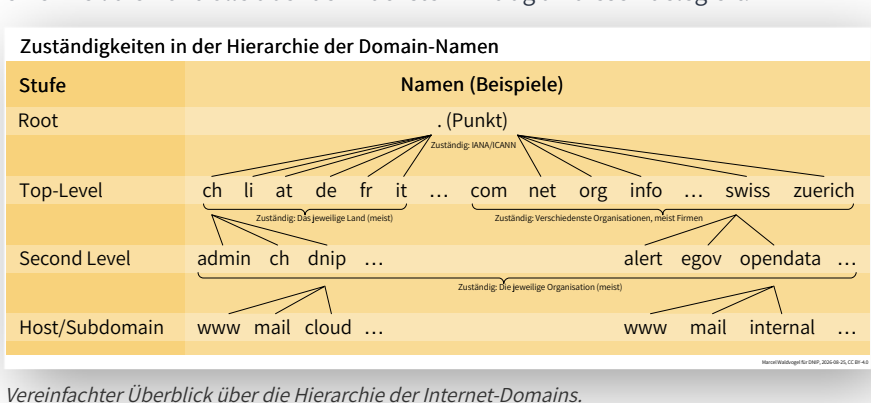
Die grafische Zusammenfassung dieses Kapitelchens. Die Farben geben nicht alle Möglichkeiten an, sondern einen wichtigen Auszug; jeder Nutzer muss die untenstehenden Überlegungen für seinen konkreten Fall selbst anstellen.

Einige Beispiele zum besseren Verständnis:

- Das **Gebäude** lässt sich mit vielen lokalen Materialien bauen; Zement, Sand und Stahl (für Stahlbeton) oder Ton (für Backsteine) werden lokal gefördert und verarbeitet. Ein bestehendes Gebäude lässt sich über Jahrzehnte weiterbetreiben, auch wenn einzelne Rohstoffe mal fehlen. Deshalb zweimal blau, sowohl beim Bau/Kauf als auch beim Betrieb.
- **Gebäudetechnik** wie Klimaanlagen für die Rechnerkühlung wird ebenfalls lokal oder regional gefertigt und hält Jahre bis Jahrzehnte aus. Deshalb zweimal blau/weiss.
- Die **Gebäudesteuerung** enthält schon relativ viel Software und Elektronik, die aus wenigen/fernen Ländern stammt und oft raschere Ersatz-/Updatezyklen braucht oder von Lizenzzahlungen abhängig ist, damit die Software weiter genutzt wird. Moderne Steuerungen hängen oft teilweise oder vollständig von Cloud-Lösungen ab. Deshalb sind je nach Komponente viele Kombinationen der Farben möglich.
- Die **Computer** in den Gebäuden sind beim Kauf sehr stark von wenigen Ländern wie USA oder Fernost abhängig, hier also oben rot. Einmal im Betrieb, laufen die meisten davon aber mehrere Jahre ohne neue Teile des Herstellers, deshalb unten weiss.
- Bei **Betriebssystemen** und Softwarebibliotheken als Grundlage für die Applikationsentwicklung haben wir die Wahl von Optionen aus der ganzen Welt, inklusive Open-Source-Lösungen, die unabhängig von Sanktionen eingebaut werden können. Trotzdem werden viele proprietäre Softwarelösungen zugekauft, bei denen wir dann Abhängigkeiten haben; deshalb ist die obere Ampel hier bunt. Alle Softwarekomponenten benötigen aber regelmässige Updates, insbesondere solche, auf die direkt oder indirekt aus dem Internet zugegriffen werden kann. Deshalb ist unten rot mit etwas weiss.
- Beim **Netzwerk** selbst haben wir einheimische Internetprovider zur Auswahl; viele Schritte der Glasfaserherstellung erfolgen ebenfalls zumindest teilweise in der Schweiz.
- **Netzwerkequipment** wie Router, Firewalls und Switches stammen fast durchgehend aus fernöstlicher Fertigung, zum Teil unter US-Label. Bei vielen Geräten ist regelmässiges Software-Update angesagt, auch wenn es dort Open–Source–Lösungen gibt. Zum Teil ist der Einsatz der Geräte an Lizenzverträge gekoppelt oder die automatische Aktualisierung von Bedrohungslisten notwendig.
- Bei **Cloud-Diensten** sollte es eigentlich offensichtlich sein, dass der Cloudanbieter jederzeit den Hahn zudrehen kann. Doch neben den grossen US- und chinesischen Cloudanbietern gibt es auch verschiedene europäische Angebote sowie die Möglichkeit, Cloud-Technologien auch auf eigener Infrastruktur zum Effizienzgewinn zu nutzen.
- **Netzwerkdienste** gehen jedoch häufig vergessen. Um die geht es in diesem Artikel, insbesondere um Domains, wie beispielsweise DNIP.ch. Auch die Netzwerkdienste können naturgemäss jederzeit abgedreht werden.

Wie funktionieren Internet-Domains?

Internet-Domains und die Namen von Webseiten (z.B. www.dnip.ch), Netzwerkdiensten (mail.dnip.ch) und Rechner (webserver15.dnip.ch) sind hierarchisch aufgebaut, wobei die Wurzel der Hierarchie rechts ist. Also www.dnip.ch ist eigentlich «.» → «ch» → «dnip» → «www», wobei jede Stufe einen Teil die Kontrolle über den nächsten Eintrag an diesen delegiert.



Vereinfachter Überblick über die Hierarchie der Internet-Domains.

Das Domain Name System (DNS)

Wenn man eine Anfrage an einen Webserver wie www.DNIP.ch stellen will, muss man zuerst seine IP-Adresse kennen, um dann die richtige Anfrage dorthin zu schicken (und die passende Webseite als Antwort zurückzuerhalten). Wer das genauer verstehen möchte, sei zum einen auf unsere Erklärung verwiesen, wie Internetsperren funktionieren (da wird auch erklärt, was im Normalfall alles funktionieren muss) oder wie das Internet entstanden ist.

Während anfänglich – bis das Internet mehrere tausend Rechner umfasste – diese Übersetzungstabelle von Name zu IP-Adresse noch auf jedem Rechner vorgehalten werden konnte, ist das heute mit über einer Milliarde Hostnamen alleine für Webserver nicht mehr praktikabel. Seit vielen Jahrzehnten ist das Internet also hierarchisch organisiert, so ähnlich wie die Dateien auf dem Computer.

Auf einem Computer würde man auch nicht eine Milliarde Dateien in einen Ordner legen wollen, sondern die gut strukturiert in mehrere Ebenen Unterverzeichnisse legen, jedes mit einer übersichtlichen Grösse. Dafür müsste man sich dann auch vom obersten Verzeichnis in den «ch»-Ordner bewegen und in diesem in den «dnip»-Ordner öffnen, bevor man dort die «www»-Datei fände, also, als ob man die Datei `/ch/dnip/www` öffnen wollte. So ähnlich läuft das auch mit Domainnamen; die verschiedene Ordner sind aber auf verschiedenen Servern, unter unterschiedlichem Management.

Schauen wir uns das Schritt für Schritt an.

> Auch wenn die Übersetzung Namen → IP-Adresse die bekannteste und am meisten genutzte Funktion ist, im DNS sind viele weitere Informationen abgelegt, beispielsweise zu Mail (wer soll Mail für meine Domain senden/empfangen dürfen und wie), zu Sicherheit (wer darf Zertifikate ausstellen, welcher Schlüssel ist gültig und rede ich gerade mit dem richtigen DNS-Server) und mehr. Die Details sind hier nicht relevant, es reicht, wenn wir uns merken, dass ohne DNS im Internet eigentlich nichts mehr laufen würde.

Die Root-Zone

Zuoberst ist die Root-Zone, das Wurzelverzeichnis des DNS, verwaltet von der ICANN, die Internet Corporation for Assigned Names and Numbers, seit 2016 eine Non-Profit-Organisation mit Sitz in Kalifornien. Sie übernimmt die Aufgaben der früheren IANA (Internet Assigned Numbers Authority), und verwaltet beispielsweise die Root-Zone und führt Buch über die Delegationen an die darunterliegenden Länderdomains (wie .ch) und sonstigen Top-Level-Domains (wie .com).

Die meisten Internet-Nutzer:innen wissen nichts von der Root-Zone, die sich vor der Öffentlichkeit hinter technischen und administrativen Kulissen verbirgt. Sie ist aber wichtig, da man nur über eine Abfrage bei der Root-Zone erfahren kann, welche Top-Level-Domains es gibt und wie man sie kontaktiert.

Top-Level-Domains

Bekannt und beliebt sind hingegen die Top-Level-Domains (TLD) wie die Länderdomains .ch und andere bekannte Domains wie .com. Insgesamt gibt es 1595(!) dieser Domains. Etliche dieser 1595 Domains gehören Firmen, die diese Domains reserviert haben, sie aber nicht oder kaum nutzen, wie beispielsweise .ABB (www.abb existiert, scheint aber nicht zu funktionieren) oder .AEG (www.aeg leitet um auf www.aeg.com und von dort weiter auf www.aeg.ch). In vielen Fällen dürfte der Markenschutz das Hauptkriterium gewesen sein.

Betrachten wir aber die Domains, die auch für normale Kund:innen nutzbar sind, am Beispiel von .ch. Die TLD .ch wird von Switch im Auftrag des Bakom verwaltet. .ch gehört damit eigentlich «der Schweiz», auch wenn Switch die für die TLD notwendige Infrastruktur (Server, Datenbanken) betreibt. Switch fungiert als Registry, besitzt also die Datenbank für die .ch-Domains. Kunden wenden sich aber nicht direkt an Switch, wenn sie eine Domain wollen, sondern dafür gibt es rund 180 Firmen, bei denen man eine .ch-Domain bestellen kann.

Rolle	Wer	Erklärung
„Besitzer“	Schweizerische Eidgenossenschaft	
Registry	Switch	Der Betreiber der Infrastruktur (Server, Datenbanken, etc.) und Verwalter der Domainnamen.
Registrar	Ca. 180 verschiedene Firmen im In- und Ausland	Anlaufstellen für die Kunden, welche eine Domain registrieren möchten.

Switch erfüllt drei Rollen gegenüber ICANN, quasi in Personalunion: Sie ist der Landeskontakt («ccTLD Manager»), Ansprechpartner für Verwaltungsfragen («Administrative Contact») und auch Betreiberin der Infrastruktur («Technical Contact»). Dies ist zwar bei vielen «alteingesessenen» Ländern üblich, aber muss nicht unbedingt so sein. .bayern beispielsweise hat als «Sponsoring Organization» (den «Besitzer» der Domain) die Bayern Connect GmbH (mit Sitz in Köln), die Verwaltung erfolgt durch GoDaddy (mit Sitz in den USA) und die Technik wird betrieben durch IronDNS in Dortmund.

Second-Level-Domains

So richtig interessant werden Second-Level-Domains wie beispielsweise DNIP.ch. Für diese haben wir die Domain bei einem der knapp 80 .ch-Registrare bestellt, die ihren Sitz auch in der Schweiz haben (die restlichen gut 100 haben ihren Sitz ausserhalb der Schweiz). In unserem Fall sind die Server, welche auf die Frage «Wo finde ich `www.dnip.ch`?» die korrekte IP-Adresse (aktuell 94.237.81.241) zurückliefern, ebenfalls von unserem Registrar betrieben. Bei grösseren Firmen, komplexeren Setups oder auch Self-Hostern ist das aber oft nicht der Fall, da sind dies eigene Server oder solche von Dritten.

Stufe	„Besitz“	Verwaltung	Technik	Ansprechsperson
`.` (Root)	ICANN	ICANN (früher NTIA, eine US-Behörde)	Verisign	—
`.ch`	Eidgenossenschaft, vertreten durch Switch	Switch	Switch	Unser Registrar
`.dnip.ch`	DNIP	DNIP	Unser Registrar	—
`www.dnip.ch`	DNIIP	DNIP	Unser Webhoster	—

Vereinfachte Rollenaufteilung für die DNS-Stufen zu unserem Webserver (und das Webhosting).

Souveränität im DNS

Während für `.ch` sowohl der Besitzer, als auch die Verwaltung und die für die Technik verantwortliche Organisation ihren Sitz in der Schweiz haben, ist dies für andere TLDs nicht so klar, wie die folgende Tabelle und die Zusammenfassung darunter zeigen.

Typ	TLD	Sitz	Betrieb
Land	`.ch`	CH	CH
	`.de`	DE	DE
	`.li`	**CH**	**CH**
	`.at`	AT	AT
	`.it`	IT	IT
	`.fr`	FR	FR
	`.gi`	GI	GI/**US**
Klassisch	`.com`	US	US
	`.net`	US	US
	`.org`	US	US
	`.info`	US	US
	`.biz`	US	US
Region	`.alsace`	FR	FR
	`.amsterdam`	NL	NL
	`.barcelona`	ES	ES/**CH**
	`.bayern`	DE	**US**/DE
	`.corsica`	FR	FR
	`.eu`	BE	BE
	`.helsinki`	FI	**US**
	`.swiss`	CH	CH
	`.zuerich`	CH	**UK**
Thema	`.art`	UK	UK
	`.cloud`	IT	**CA**
	`.hotels`	NL	**US**
	`.music`	CY	**CA**
	`.rugby`	IE	**US**
	`.voting`	CH	**US**

*Übersicht über einige Domains und die für sie zuständigen Länder. Unerwartete Werte sind **rot fett** markiert. Der Link der TLD zeigt auf die Beschreibung der zuständigen Stellen für die Top-Level-Domains bei der IANA.*
Die gesamte sortier- und durchsuchbare Liste Domain-Souveränität mit allen 1595(!) TLDs kann hier heruntergeladen werden.

- **Land:** Viele der (im Internet) „alteingesessenen“ Länder sind ähnlich aufgestellt wie die Schweiz und damit souverän, beispielsweise unsere 4 grossen Nachbarländer. Bei Kleinstaaten setzt man aber auf Kooperation: Liechtenstein (`.li`) hat ihre Domainverwaltung an die Schweizer Switch delegiert; Gibraltar (`.gi`) macht alles bis auf die Technik selbst.
- **Klassisch:** Die ursprünglichen sogenannten „generischen“ TLDs (gTLD) wie `.com`, `.net` oder `.org` sind alle fest in US-Hand, wie auch Autistici/Inventati kürzlich leidvoll feststellen musste.
- **Region:** Die verschiedenen Regionen sind oft in der Hand von Organisationen, welche auch in den zu dieser Region gehörigen Ländern angesiedelt sind. Ausnahmen sind beispielsweise `.barcelona`, welches technisch von einem internationalen Verein mit Sitz in der Schweiz geleitet wird; oder `.bayern`, welches organisatorisch und technisch in Deutschland (ausserhalb Bayerns) verankert ist, wo die Administration aber über eine US-Firma läuft.
- **Thema:** Hier sind die natürlichen Zuordnungen zu Ländern oft nicht klar, auch wenn Rugby durchaus etwas mit Irland und Voting mit der Schweiz zu tun hat. Für diese Domains gab es offene Ausschreibungen, bei denen Organisation aus aller Welt Vorschläge für TLDs vorschlagen konnten.

Auswahl einer souveränen TLD

Wer aktuell eine TLD sucht, bei der sowohl Sitz, Administration als auch Technikverantwortung in Europa sitzen, kann aus 166 Top-Level-Domains auswählen, rund 10 % der total 1595 TLDs:

Typ	Anzahl	TLDs
Land (ccTLD)	43	.at, .be, .bg, .bv, .ch, .cy, .cz, .de, .dk, .ee, .es, .eu, .fi, .fr, .gf, .gr, .hr, .hu, .ie, .im, .is, .it, .li, .lt, .lu, .lv, .mq, .mt, .nl, .no, .pl, .pm, .pt, .re, .se, .si, .sj, .sk, .tf, .tm, .uk, .wf, .yt
Erweitertes Europa (ccTLD)	15	.aw, .ax, .cw, .gg, .gp, .gs, .io, .je, .mc, .ms, .nc, .pf, .sh, .va, .vg
Nicht-lateinische ccTLD	4	Kyrillisch: Bulgarien (.бг) und EU (.ею); Griechisch: Griechenland (.ελ) und EU (.ευ)
Region	28	.alsace, .amsterdam, .barcelona, .bcn (Barcelona), .berlin, .brussels, .bzh (Bretagne), .cat (Katalonien), .cologne, .corsica, .cymru, .frl (Friesland), .gal (Galicien), .gent, .hamburg, .koeln, .london, .madrid, .paris, .ruhr, .saarland, .scot, .swiss, .tirol, .vlaanderen, .wales, .wien, .zuerich
Thema	12	.art, .bond, .cam, .cfd, .cyou, .eus, .icu, .museum, .one, .sbs, .sport, .tel
Nicht-lateinische Themen	4	Arabisch: .موقع (Site; offline?) und .بازار (Bazaar); Kyrillisch .ОНЛАЙН (Online) und .САЙТ (Site)

*Übersicht über die Domains unter europäischer Kontrolle zum Zeitpunkt der Publikation, wozu hier „Europa“ als EU- und EFTA-Länder sowie UK definiert ist und „Erweitertes Europa“ inklusive Länder und Regionen, welche zumindest teilweise von diesen abhängig sind (auf Basis der „Sovereignty“-Spalte hier). Die französischen Übersee-Départements werden aufgrund ihrer Adresszeile „France“ übrigens zu Frankreich gezählt und **.eu** wird von der IANA/ICANN als länderspezifische Domain geführt, nicht als Region.*
Die Links zeigen auf die Wikipedia-Einträge der Domains, falls vorhanden. Nicht alle TLDs sind für alle Nutzungen verfügbar; 60 TLDs, die mutmasslich nur für die Besitzerfirma selbst nutzbar sind, auch diese sind aber im Gesamtverzeichnis aller 1595 TLDs enthalten.

Obwohl die Zahl von 166 TLDs zuerst gross klingt, ist gut ein Drittel davon Firmendomains, die nur für die dahinter stehende Firma nutzbar ist. Die verbleibende Auswahl ist – abgesehen von den geografischen Domains – recht beschränkt.

Trotzdem gibt es ein paar „hippe“ TLDs darunter, beispielsweise die bei Informatikern beliebige TLD .io, die für die British Indian Ocean Territory gehört, was Grossbritannien demnächst an Mauritius abgeben will und der zugrunde liegende ISO-3166-Ländercode damit erlöschen würde. Es gibt Anzeichen, dass .io aber über die nominelle Übergangsfrist von 5 Jahren hinweg in Betrieb gehalten wird, analog zu .su, welche auch 35 Jahre nach Ende der Sowjetunion noch in Betrieb ist (und davor nur gut ein Jahr aktiv war).

Ebenfalls regional beliebt ist .sh, eigentlich für Sankt Helena und Tristan da Cunha gedacht. Sie ist aufgrund der Abkürzung auch im Kanton Schaffhausen und in Schleswig-Holstein verbreitet. Sowohl .io als auch .sh haben ihren offiziellen Sitz im jeweiligen britischen Überseegebiet, mit Technologie aus UK.

Weitere Souveränitätskriterien

Zusätzlich zu den Eigenschaften der Domain und ihrer Registry kann auch die Auswahl des **Registrars** relevant werden. Wenn ein Land wie die USA Sanktionen gegen Personen oder Organisationen ausspricht, betreffen die oft Personen und Firmen im Land, welches die Sanktionen ausspricht. Wenn nun ein US-(Wohn-)Sitz oder -Staatsbürgerschaft besteht oder wichtige Abhängigkeiten (z.B. Filialen) bestehen, werden diese Sanktionen mutmasslich greifen.

Für .ch bietet Switch einen Überblick über ihre Registrare an, sortiert in die drei Kategorien Schweiz, Europa und Weitere Länder. Grössere Schweizer Registrare und die meisten der Registrare ausserhalb der Schweiz dürften auch etliche der anderen oben genannten Domains im Angebot haben. Die Switch-Liste dürfte also ein guter Startpunkt für die Suche nach einem Registrar sein.

Ebenfalls zu beachten ist, wer die **DNS-Server** betreibt und in welchem Land bzw. über welchen Dienstleister. Wer sich nicht selbst um die DNS-Server gekümmert hat, dürfte typischerweise die DNS-Server des gewählten Registrars mitnutzten.

Dasselbe gilt für die **Server** selbst, seien das Webserver, Mailserver oder andere Server. Auch hier ist Serverstandort, Betreiberfirma und allfälliger Serverhoster bzw. Cloudprovider in die Souveränitätsüberlegungen einzubeziehen.

Michael Hausding vom Switch-DNS-Team hat dies letztes Jahr an einem Vortrag einiges davon detailliierter betrachtet.

Weitere Souveränitäts-risiken

Auch wenn die ICANN formell selbstverwaltet ist, hat sie ihren Sitz in den USA und untersteht damit US-Rechtsprechung und -Sanktionen. Bisher ist die ICANN nicht auf Anträge von Ländern eingegangen, die weitere Länder als Sanktion aus dem DNS-Root entfernen lassen wollten. Ob die ICANN allerdings Handlungsspielraum hat, wenn die USA ein Land oder eine seiner Registries sanktionieren, darf bezweifelt werden.

Ausgelöst durch verschiedene Kritikpunkte an der ICANN wie die (nicht auf Sanktionen beruhende) Aussetzung von .af-Registrierung während des Afghanistankriegs wurde das Open Root Server Network (ORSN) gegründet. Dieses stellte seinen Betrieb aber 2019 ein, ohne Pläne zur Wiederaufnahme. Auf Basis der ORSN-Erfahrungen könnte – potenziell in Zusammenarbeit mit bestehenden alternativen DNS-Root-Providern – ein Ersatz-Root-DNS-Notbetrieb hochgefahren werden, falls ICANN wichtige Länder oder Registries ausschliessen würde.

Der Aufwand dafür wäre signifikant und würde – auch bedingt durch die Sicherheitserweiterung DNSSEC – an verschiedenen Stellen Konfigurationsänderungen bedingen, wäre aber als Reaktion der Weltgemeinschaft auf eine unverständliche US-Sanktion in diesem Bereich durchaus möglich.

Das Souveräne-Domain-Howto

Folgende Schritte helfen bei der Umsetzung einer souveränen Domain:

1. Auswahl eines vertrauenswürdigen **Registrars** in einem vertrauenswürdigen Land, vorzugsweise dem eigenen (Wohn-)Sitzland. Beispielsweise auf Basis der oben bereits erwähnten Switch-Liste.
2. Über diesen Registrar erfolgt dann die Auswahl einer **souveränen TLD.** Auch hier sollten sowohl die Organisationen als auch ihre Firmensitze vertrauenswürdig sein. Neben 3 Domains in kyrillischer oder arabischer Schrift gibt es 4 öffentlich nutzbare Domains mit vollständigem Schweiz-Sitz, nämlich .ch, .swiss, .li und .sport. Wem diese Domains nicht ausreichen, findet in der obigen Liste rund 100 mehr.
3. Bei vielen Registrars dürften **DNS-Server** im Land ihres Firmensitzes zum Standard gehören, neben weiteren Servern im Ausland zu Redundanz- und Geschwindigkeitszwecken. Wer das aber genau wissen will, soll die Internet-Expertin ihres Vertrauens oder den Registrar selbst fragen.
4. Die eigenen **Mail-, Web- und sonstigen Server** ebenfalls von vertrauenswürdigen Firmen in politisch stabilen Ländern betreiben lassen.

Wem Souveränität wichtig ist, sollte in allen obigen Fällen darauf geachtet werden, dass die genannten Firmen auch ihre Subunternehmer bzw. Rechenzentrums- und Clouddienstleister aus geeigneten Ländern rekrutieren.

Weiterführende Literatur

- Root Zone Database, IANA
  Alle Top-Level-Domains mit Informationen, jeweils als einzelne Webseite
- Marcel Waldvogel: Domains for Digital Sovereignty, 2026-09-05.
  Vollständige Liste der IANA-Domain-Informationen in einem Tabellendokument; Snapshot mit Stand vom 2026-08-09.
- Marcel Waldvogel: TLD Sovereignty Source Code, Codeberg
  Der Quellcode, mit dem diese Liste (v)erarbeitet wurde.
- Michael Hausding: The DNS as National Critical Infrastructure in an Era of Geopolitical Tensions, Swiss Cyber Storm 2025
- Dorottya Zsiboracs: Reflecting on the Internet community's response to the Ukraine invasion two years on: ICANN's refusal to disconnect Russia from the global Internet was the right decision made at a difficult time, DNS Research Foundation, 2024-03-04.
- Natalie Campbell, Carl Gahnberg: Internet Impact Brief: Impact of Ukraine's Requests to Block Russia's Access to the Internet, Internet Society, 2022-03-19
- Theo van der Sluijs: Lecktest **(neu 2026-10-07)**
  Teste die Abhängigkeiten und Datenabflüsse deiner Domain (oder einer fremden Domain). Mit Tipps zur Verbesserung.

dnip.ch mit Deiner Spende unterstützen

Wir wollen, dass unsere Inhalte frei verfügbar sind, weil wir es wichtig finden, dass möglichst viele Menschen in unserem Land die politischen Dimensionen der Digitalisierung erkennen und verstehen können.

Damit das möglich ist, sind wir auf deine Unterstützung angewiesen. Jeder Beitrag und sei er noch so klein, hilft uns, unsere Aufgabe wahrzunehmen.

CHF 5	CHF 10	CHF 20
CHF 25	CHF 50	CHF 75
CHF 100	CHF 150	CHF 200
CHF 250	CHF 500	CHF 1'000
Anderer		

SPENDEN »

2 Kommentare

David sagt: 6. Oktober 2026 um 17:21 Uhr

Ein sehr interessanter Artikel, vielen Dank! Was ich noch gerne etwas genauer wüsste: Welche genauen Unterschiede gibt es zwischen der .ch und der .swiss Domain? Ist die .swiss Domain genauso souverän, wie die .ch Domain, oder gibt es dort kleine/versteckte Unterschiede (in Grafik 2 ist sie unter Firmen/Organisationen gelistet)?

Antworten

↪ **Marcel Waldvogel** sagt: 6. Oktober 2026 um 21:07 Uhr

Was Souveränität betrifft, sind beide ziemlich vergleichbar, alles in Schweizer Hand. .ch vollständig in den Händen der Switch-Stiftung (agierend im Auftrag des Bundes), .swiss beim Bakom bzw. beim Schweizer CORE-Verein. Letzterer hat etwas mehr Auslandsexposition, ich würde die beiden aber als ziemlich gleichwertig ansehen.

Was die Nutzung betrifft, gibt es allerdings Unterschiede: Eine .ch-Domain bekommt fast jeder, .swiss nur mit klarem Schweiz-Bezug.

Das „Zuständig: Verschiedenste Organisationen, Firmen" bezieht sich darauf, dass diese TLDs nicht offiziell Ländern zugeordnet sind. Der Unterschied dürfte bezüglich Souveränität auch vernachlässigbar sein.

In dieser Tabelle kannst du dir übrigens die Details aller 1500+ TLDs anschauen und direkt vergleichen.

Antworten

Schreibe einen Kommentar

Deine E-Mail-Adresse wird nicht veröffentlicht. Erforderliche Felder sind mit * markiert

Kommentar *

Name *

E-Mail-Adresse *

Website

Name, E-Mail-Adresse und Website in diesem Browser für meinen nächsten Kommentar speichern.

Ja, ich möchte die neuen Blogbeiträge via E-Mail abonnieren. Ich kann mich jederzeit wieder aus der Liste austragen.

KOMMENTAR ABSCHICKEN

‹ DNIP-Briefing #88: Kleine Schritte …

Vogt am Freitag: Überfahren ›

Weitere Beiträge



Vogt am Freitag: Volkskostenrechnung

Reto Vogt · 30. Oktober 2026

127 Millionen Franken wird ein IT-Projekt der Migrationsbehörden teurer als geplant. Kolumnist Reto Vogt sagt: Das ist kein Einzelfall. Und

Weiterlesen »



DNIP-Briefing #85: Mit Sicherheit für die Katz?

Die Redaktion · 27. Oktober 2026

Die Redaktion präsentiert jeden Dienstag die Geschichten, die sie bewegt, aufgerüttelt oder zum Nachdenken angeregt hat. Heute mit allem ausser

Weiterlesen »

Newsletter abonnieren

… und auf dem neusten Stand bleiben

E-Mail

SENDEN

Wenn nicht anders gekennzeichnet, stehen alle durch Mitglieder der dnip-Redaktion erstellten Inhalte dieser Website unter der Lizenz Creative Commons Namensnennung 4.0 International (CC BY 4.0).