Switch

Rechenschaftsbericht 2024

der Registerbetreiberin für die ccTLDs .ch und .li

Inhaltsverzeichnis

Die Kostendeckung der kritischen Infrastruktur DNS kann nicht mehr ausschliesslich über das Mengenwachstum erfolgen.

Urs Eppenberger
Head of Registry, Switch

Editorial

Urs Eppenberger, Head of Registry

Die Domain-Namen-Welt befindet sich in einer Konsolidierungsphase. Vor allem die Registry-Betreiber erhoffen sich von der nächsten Einführungsrunde von Toplevel-Domain-Namen im 2026 einen neuen Schub. Davon dürfte das Mengengerüst der .ch-Domain-Namen aber kaum beeinflusst werden.

Die Corona-Zeit hat einen Digitalisierungsschub gebracht. Diese Phase ist klar vorbei, jetzt konsolidieren private Halter ihre gehorteten Domain-Namen. Das führt zu einem kleineren Wachstum total und zu tieferen Umsätzen bei den Registraren. Werbemassnahmen der Webhoster und Registrare könnten bei Unternehmen das Bewusstsein stärken, dass ein individueller Webauftritt mit eigenem Domain-Namen deren Marke stärkt und ihre Angebote unter eigener Kontrolle positioniert. Wenn Firmen hingegen den Weg wählen, ihre Produkte oder Dienstleistungen über die grossen Verkaufsplattformen anzubieten, benötigen sie weder eine eigene Website noch einen Domain-Namen. Die Verkaufsplattformen haben durch ihre Grösse und globale Reichweite einen Vorteil. Es ist schwer abzuschätzen, welcher Verkaufskanal gewinnt.

Die Diskussion über Wachstum oder Stagnation ist für die Registrare und die Registrierungsstelle relevant, da es um die Deckung der Kosten geht, die durch die Teuerung, durch steigende Anforderungen an die Resilienz der Infrastruktur und durch die Compliance-Vorgaben verursacht werden. Die Kostendeckung kann nicht mehr ausschliesslich über das Mengenwachstum erfolgen.

Die 2.6 Millionen registrierten Domain-Namen, die Name-Server und die Resolver der Internet Service Provider bilden eine relevante Infrastruktur für die Schweizer Wirtschaft und für die Bevölkerung. Diese gilt es zu pflegen und zu schützen. Vorgaben dazu finden sich in der nationalen Cyberstrategie und im Fernmeldegesetz. Die technischen Fähigkeiten sind bei der Registrierungsstelle und den Registraren vorhanden. In Abstimmung mit den involvierten Behörden werden wir die effizientesten Massnahmen zur Sicherung und Weiterentwicklung dieser Infrastruktur finden und umsetzen.

1.
Tätigkeitsbericht – Betrieb

Switch

Bekämpfung Cyberkriminalität

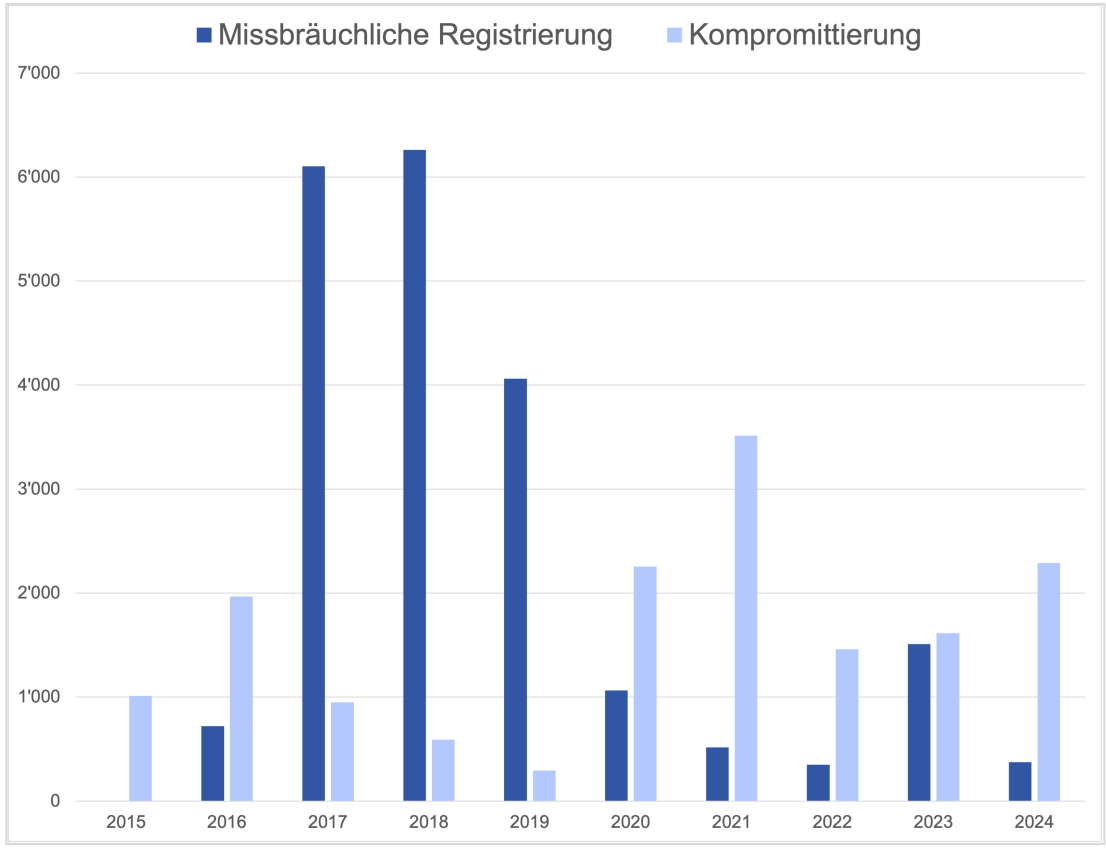
Kompromittierte Webseiten

Die Zahl der kompromittierten Webseiten, die für Phishing und Malware missbraucht wurden, stieg im Vergleich zum Vorjahr an. Ein Grossteil davon wurde mit dem eigens entwickelten Crawler für die .ch-Zone gefunden.

Missbräuchliche Registrierung

Die Zahl der Domain-Namen, bei denen der Verdacht auf eine missbräuchliche Registrierung gemeldet wurde, hat abgenommen. Ein Grund dafür ist, dass das Fedpol weniger Anfragen nach Art. 15 VID via ihr Projekt «SWITCHoff» gesendet hat. Die Anzahl der Anfragen nach Art. 16 VID ist ebenfalls zurückgegangen.

Webseite: https://www.saferinternet.ch



Massnahmen bei Missbrauchsverdacht

Anträge anerkannter Behörden – VID Art. 15.1

Im Jahr 2024 haben die akkreditierten Behörden insgesamt 66 Anfragen gemäss VID Art. 15.1 zur sofortigen Blockierung (technisch/administrativ) von Domain-Namen betreffend Phishing gesendet. Es gab keine Fälle betreffend Malware.

Anfragen	Konsequenz	2024
Nicht beantwortet	Domain-Name gelöscht	65
Beantwortet	Domain-Name reaktiviert	1
Total		**66**

Alle vom Bakom anerkannten Behörden sind auf folgender Webseite aufgelistet: Anerkannte Behörden

Amtshilfe – VID Art. 16.3

Auf Verlangen einer im Rahmen ihrer Zuständigkeit intervenierenden Schweizer Behörde wurden 310 Anfragen für eine Schweizer Korrespondenzadresse gemäss VID Art. 16.3 versendet.

Anfragen	Konsequenz	2024
Nicht beantwortet	Domain-Name gelöscht	246
Beantwortet	Domain-Name reaktiviert	64
Total		**310**

Security Awareness – iBarry und SISA

In Zusammenarbeit mit SISA unterstützt Switch die Sensibilisierung der Schweizer Bevölkerung. Mit drei neuen Informationskampagnen (Passkeys, neues Datenschutzgesetz, Deepfakes) informiert iBarry.ch und bietet gleichzeitig Orientierung und Unterstützung bei Unsicherheit und Fragen rund um die Internetsicherheit.

https://checkawebsite.ibarry.ch

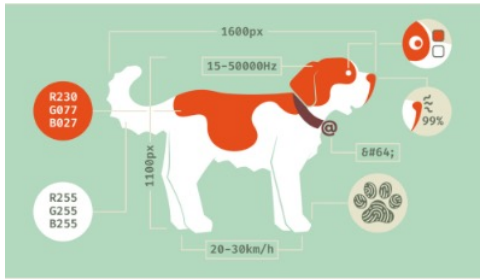
https://ibarry.ch

Um das Angebot für die Schweizer Bevölkerung zu optimieren und die Plattform iBarry besser zu positionieren, hat SISA wieder an der diesjährigen Befragung der Schweizer Internet-Nutzerinnen und -Nutzer mitgewirkt.

https://cyberstudie.ch

Die iBarry-Community wird seit diesem Jahr mit einem Newsletter mit aktuellen Informationen versorgt.

→ Hier registrieren



Security Awareness – SISA Jubiläum

Die Swiss Internet Security Alliance (SISA) hat sich auch in diesem Jahr zum Ziel gesetzt, wichtige Akteure der Schweizer Internetsicherheit zu vernetzen und die Schweizer Bevölkerung zu schützen.

Seit Mitte des Jahres können die Mitglieder über den bestehenden SISA Phishing Feed zusätzlich Cryptofraud-URLs beziehen. NEDIK sammelt und teilt diese Daten zusammen mit Mute Group.

Neue Mitglieder und Partner im 2024:

NEDIK

CLUSIS 1989

Zürcher Hochschule für Angewandte Wissenschaften
zh aw

SBB CFF FFS

cyon

ISC2 CHAPTER

Die SISA feiert ihr 10-Jahr-Jubiläum

Die Swiss Internet Security Alliance wurde 2014 von namhaften Vertretern der Wirtschaft ins Leben gerufen. Ihre Vision ist es, die Schweiz zum sichersten Internet-Land der Welt zu machen.

Der fast vollständige Vorstand der SISA (v.l.): Simon Seebeck (Die Mobiliar), SISA-Präsidentin Katja Dörlemann (Switch), Rita Frei (Sunrise), Marcus Beyer (Swisscom). Nicht auf dem Foto: Fabian Ilg (Schweizerische Kriminalprävention). Foto: Netzmedien

Security Awareness Day

Am 24. Oktober 2024 veranstaltete Switch zum siebten Mal den Swiss Security Awareness Day. In diesem Jahr wurde die stetig wachsende Konferenz wieder mit iBarry.ch als Partner durchgeführt. Die rund 130 Teilnehmenden konnten sich zwischen den spannenden Vorträgen in diversen Networking-Pausen mit anderen Expertinnen und Experten vernetzen.

Zum ersten Mal wurde auch zu Workshops eingeladen, um Hands-on-Erfahrung zu vermitteln.

Das Programm zielte auch diesmal darauf ab, das Verständnis für das Thema Security Awareness in der Switch-Community und darüber hinaus zu schärfen, gleichzeitig neue Ideen zu vermitteln sowie den Austausch anzuregen.

Alle Vorträge sind online.

Security Awareness Adventures

The Switch Security Awareness Adventures

«Hack The Hacker – der Escape Room» war das erste von drei Security Awareness Adventures von Switch, gefolgt von «Track The Hacker – die Schnitzeljagd» und «Piece of Cake – das Rollenspiel». Nach wie vor erfreuen sich die Abenteuer grosser Beliebtheit.

Im Jahr 2024 hat Switch die spielerischen Security-Trainings insgesamt 77-mal durchgeführt, was gegenüber 2023 (40 Durchführungen) fast eine Verdopplung ist, und auf diversen Konferenzen die Expertise über Training Games geteilt.

Webseite: https://swit.ch/security-awareness-adventures

Security Awareness – Podcast

Podcast: Security Awareness Insider

Im Dezember 2024 wurde die mittlerweile 50. Folge des Podcast «Security Awareness Insider» (auf Deutsch) veröffentlicht.

In diesem Podcast sprechen Katja Dörlemann (Switch) und Marcus Beyer (Swisscom) über die Sensibilisierung der Mitarbeitenden für Sicherheitsthemen, neue und kreative Wege, Tools und Trainingsansätze, sie vermitteln Einsicht in Security-Awareness-Programme von Firmen und Organisationen und vieles mehr.

Seit Beginn wurde der Podcast bereits knapp 25’000 mal heruntergeladen, pro Folge sind es inzwischen durchschnittlich 450 Downloads.

Verfügbar überall, wo es Podcasts gibt, oder hier: https://www.securityawarenessinsider.ch

Swiss Web Security Day

Am 29. Oktober 2024 hat Switch zusammen mit SISA und Swico den Swiss Web Security Day in Bern durchgeführt, parallel zum LEO-Event mit Schweizer Strafverfolgungsbehörden. Mit 79 Teilnehmenden aus der Schweiz und aus dem nahen Ausland war der Anlass ein Erfolg, mit sehr positivem Echo der Teilnehmenden.

Am Vormittag gab es einen Vortrag zu Cryptoinvestment-Fraud von der Zentralstelle Cybercrime Bayern. Ein zweiter Vortrag behandelte das Thema «Internet-wide deployment of Post Quantum Cryptography for security protocols».

Am Nachmittag gab es unter anderem Vorträge zum Thema DNS Abuse sowie die Präsentation eines Rechtstreites, bei dem die Selbstregulierung der Schweizer Hosting-Branche (Swico Code of Conduct Domainnamen) bestätigt wurde.

Der Event fand wie letztes Jahr ausschliesslich vor Ort in Bern statt.

Katja Dörlemann, SISA-Präsidentin, Urs Eppenberger, Head of Registry Switch, Claudius Röllin, Vertreter von Swico IG Hosting. Foto: Netzmedien

LEO-Event
Zusammenarbeit mit Strafverfolgungsbehörden

Zielgruppe

Um die Behörden im Kampf gegen Cybercrime weiter zu unterstützen, hat Switch in diesem Jahr zum vierten Mal den LEO-Event organisiert. LEO steht für «Law Enforcement Organizations».

Am 29. Oktober 2024 traf sich die Law Enforcement Community in Bern mit dem Fokus, die Gemeinschaft zu stärken und den Aufbau von Partnerschaften mit privatwirtschaftlichen CERTs zu fördern. Diese Zusammenarbeit ist bei der Bekämpfung der Cyberkriminalität entscheidend.

Daher wurde nicht nur die LEO-Community (59 Personen) eingeladen, sondern auch Vertreter der Schweizer CERTs (CH-CERT, 40 Personen). Viele Teilnehmende waren bereits im letzten Jahr dabei und brachten ihre interessierten Kollegen mit.

Die Verteilung zwischen den Regionen war sehr ausgeglichen. Die Teilnehmenden kamen von den Polizeien, den Staatsanwaltschaften sowie der Landespolizei Liechtenstein. Auch Behörden wie Swissmedic, Seco, Finma und das Bakom waren vertreten.

Themen

Verschiedene Themen wurden besprochen. Die Teilnehmenden sprachen über aktuelle Entwicklungen und Projekte im Bereich Domain-Abuse und Cybercrime. Prozesse und Schnittstellen, welche die Zusammenarbeit vereinfachen, wurden diskutiert.

Schwerpunkt war die Zusammenarbeit mit den relevanten Stakeholdern über die Community hinaus, um Cybercrime zu verhindern. So wurden verschiedene Fälle vorgestellt, welche durch diese Kooperation erfolgreich und effizient gelöst werden konnten.

Resonanz

Der Event verlief sehr erfolgreich. Der Austausch in der Zusammenarbeit hat deutlich zugenommen. Es lässt sich jedes Jahr ein grosses Interesse feststellen. Die Teilnehmenden wünschen sich eine weitere Veranstaltung im Jahr 2025. Wir werden uns vermehrt auf konkrete Beispiele fokussieren, um diese interdisziplinäre Kooperation zu fördern.

Betrieb Registry

Unterbruch des Registrierungssystems

Am 19. Januar 2024 ereignete sich ein Unterbruch des Registrierungssystems. Zwischen 07:50 und 08:39 Uhr war die EPP-Schnittstelle für die Registrare nicht verfügbar. Durch eine Umschaltung auf das Standby-System konnte der Unterbruch behoben werden.

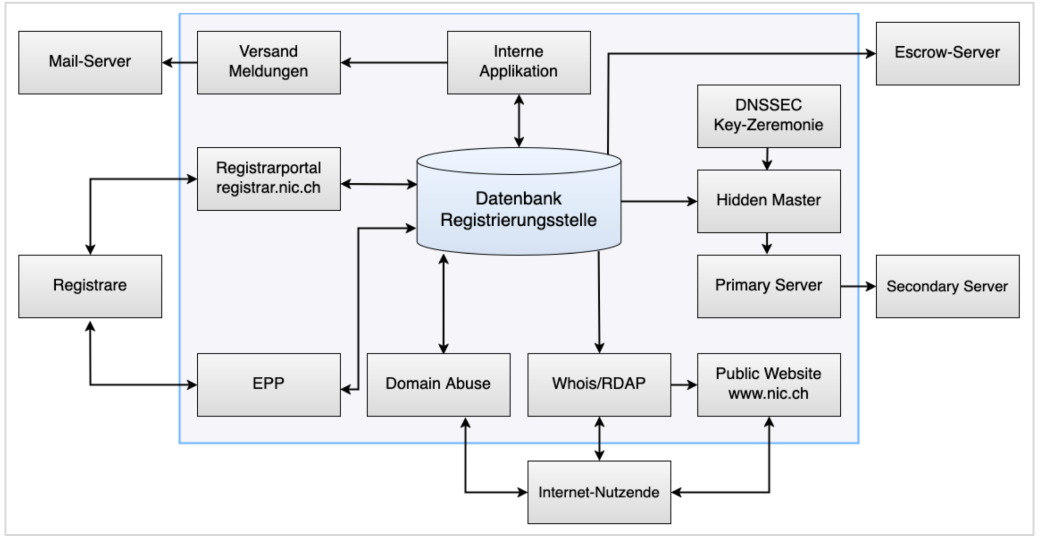
Die Störung wurde durch eine Fehlmanipulation während einer geplanten Standardwartung an der unterliegenden Serverplattform in Lausanne verursacht. Da die zentrale Datenbank von der Fehlmanipulation betroffen war, war eine automatische Umschaltung auf das Standby-System in Zürich nicht möglich.

Nach einer Ausfallzeit von 49 Minuten war die Registrierungsanwendung in Zürich ohne Datenverlust wieder in Betrieb. Die Name-Server waren vom Ausfall nicht betroffen und das Zonenfile war stets aktuell.

Ausfall des Registration Data Directory Service (RDDS)

Ein Softwarefehler beim Whois-Server führte zu übermässig grossen Logeinträgen wegen fehlerhaften Verbindungen/Clients und damit zu einer vollen Harddisk. Dies wiederum führte zum Stillstand des Servers, auf dem die Dienste whois.nic.ch und rdap.nic.ch bereitgestellt werden. Die Verwaltung und Zuteilung von Domain-Namen war jederzeit möglich und von dieser Störung nicht tangiert.

Systemübersicht und Scope der Registrierungsstelle



European TLD ISAC

Unter dem Dach von CENTR wurde im 2023 das Europäische TLD Information Sharing and Analysis Center (ISAC) gegründet.

Das europäische Zentrum für Informationsaustausch und Analysen von Top Level Domains (European Top Level Domain Information Sharing and Analysis Center, TLD ISAC) hat zum Ziel, die Sicherheit und Resilienz von Top-Level-Domain-Registrierungsstellen in Europa durch Informationsaustausch, Zusammenarbeit und Teilen bewährter Praktiken zu fördern.

Es bringt die Betreiber, Sicherheitsfachleute und andere Interessengruppen zusammen, um Informationen über Bedrohungen auszutauschen, neue Trends zu identifizieren und proaktive Massnahmen zur Verhinderung und zur Abwehr von Cyberangriffen zu entwickeln.

Switch ist, zusammen mit anderen Betreibern von europäischen ccTLDs, Gründungsmitglied und aktive Teilnehmerin im Steuerungsauschuss, der Arbeitsgruppe und der Threat Intelligence Sharing Gruppe.

Webseite: https://www.tld-isac.eu

Alle CENTR-Mitglieder wurden aufgefordert, ihre Einschätzung zu Risiken, der Handhabung und möglichen Folgen abzugeben. Auch Switch hat sich daran beteiligt. Die Resultate wurden konsolidiert und in einem Bericht (Threat Landscape Analysis) zusammengefasst. Die daraus resultierenden Top-10-Risiken hat Switch mit ihrer eigenen Risiko-Landkarte abgeglichen. Zwei fehlende und plausible Risiken wurden in die Switch-eigene Risikoverwaltung aufgenommen.

Missbrauch im globalen Vergleich

Einstellung der DAAR-Reports von ICANN

Switch hat freiwillig am DAAR-Projekt von ICANN teilgenommen und erhielt dadurch einen individualisierten Bericht betreffend Domain-Abuse für .ch und .li. ICANN hat die Reports im Q1 2024 eingestellt.

ICANN hat ein Nachfolgeprojekt namens Domain Metrica lanciert, vorerst für gTLDs. Die Teilnahme von ccTLDs ist noch nicht möglich, wir verfolgen die Entwicklungen jedoch aufmerksam.

Öffentliche Netbeacon-Reports

Switch beteiligt sich an den Messungen des Netbeacon Institute.

Im Oktober 2024 belegt die .ch-Zone den 5. Rang unter den sichersten ccTLDs mit einem Mengengerüst von mehr als 1 Million Domain-Namen.

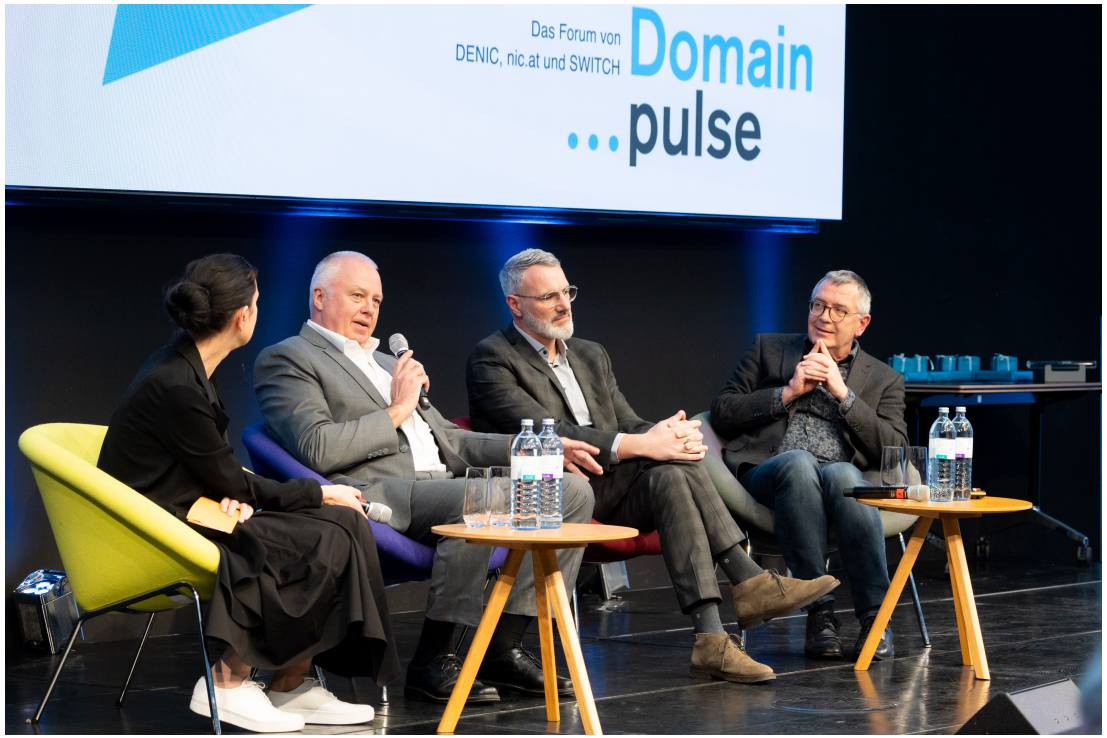
TLD	Observed Maliciously Registered Domains Per 100,000 DUM	Observed Maliciously Registered Domains	Observed DUM
nl	0.23	14	5,970,658
uk	0.28	28	9,870,870
it	0.37	12	3,222,803
at	0.41	6	1,457,415
ch	0.43	11	2,588,005
dk	0.46	6	1,317,284
ca	0.48	16	3,322,327
be	0.49	8	1,639,348
de	0.60	102	17,071,778
jp	0.64	11	1,713,367

Quelle: https://netbeacon.org/wp-content/uploads/2024/12/MAP-Report-December-2024-.pdf

Domain pulse 2024

Vom 23. bis 24. Februar 2024 fand der Domain pulse in Wien statt.

Unter dem Motto «Vienna Calling: Domain pulse 2024» wurden Möglichkeiten, Grenzen und Auswirkungen der technischen Fortschritte sowie der damit verbundenen Regulierungen (NIS2) und Herausforderungen beleuchtet. Ein weiterer Schwerpunkt waren die Sicherheit und Updates aus der Domain-Branche.



Panel mit Richard Wein (Geschäftsführer nic.at), Andreas Musielak (Vorstand DENIC) und Urs Eppenberger (Head of Registry Switch).

DNS-Resilienzprogramm

50.4%

Per 1. Januar 2025 sind 50.4 Prozent aller .ch-Domain-Namen signiert.

DNS-Resilienzprogramm

Widerstandsfähigkeit für .ch-Domain-Namen

Mit dem DNS-Resilienzprogramm unterstützt Switch die Einführung und Verbreitung offener Sicherheitsstandards bei .ch- und .li-Domain-Namen. Diese Standards spielen eine Schlüsselrolle, um die Widerstandsfähigkeit (Resilienz) gegenüber Cyber-Bedrohungen zu erhöhen. Das Programm, das auf finanzielle Anreize setzt, läuft von 2022 bis 2026.

Das Hauptziel ist es, das Signieren von Domain-Namen mit DNSSEC zu fördern. Für Domain-Namen, die nicht oder fehlerhaft signiert sind, wird während der Programmlaufzeit ein Preiszuschlag erhoben.

Die Entscheidung, welche Sicherheitsstandards gefördert werden, trifft das «DNSSEC Advisory Board». Dieses Gremium besteht aus Vertretern des Bakom, der Registrare und von Switch.

Für das Jahr 2024 wurde das Programm um die E-Mail-Sicherheitsstandards DMARC und SPF erweitert. Dies bedeutet: Die Rückvergütung der Mehreinnahmen basiert im Jahr 2024 nicht nur auf DNSSEC, sondern zusätzlich auch auf der erfolgreichen Implementation von DMARC und SPF.

Das Advisory Board hat bereits festgelegt, dass (zusätzlich zu DNSSEC) im Jahr 2025 DANE und im Jahr 2026 IPv6 gefördert werden sollen.

Messungen zur Qualitätskontrolle

Die Überprüfung der korrekten Implementierung der Sicherheitsstandards erfolgt in Zusammenarbeit mit dem externen Dienstleister OpenIntel. Für sämtliche .ch- und .li-Domain-Namen mit Name-Servern wird täglich geprüft, ob die vom Programm vorgegebenen Kriterien erfüllt werden. Die Ergebnisse dieser Prüfungen werden an Switch übermittelt. Registrare mit fehlerhaften Konfigurationen erhalten Error-Reports, um die Probleme zu beheben.

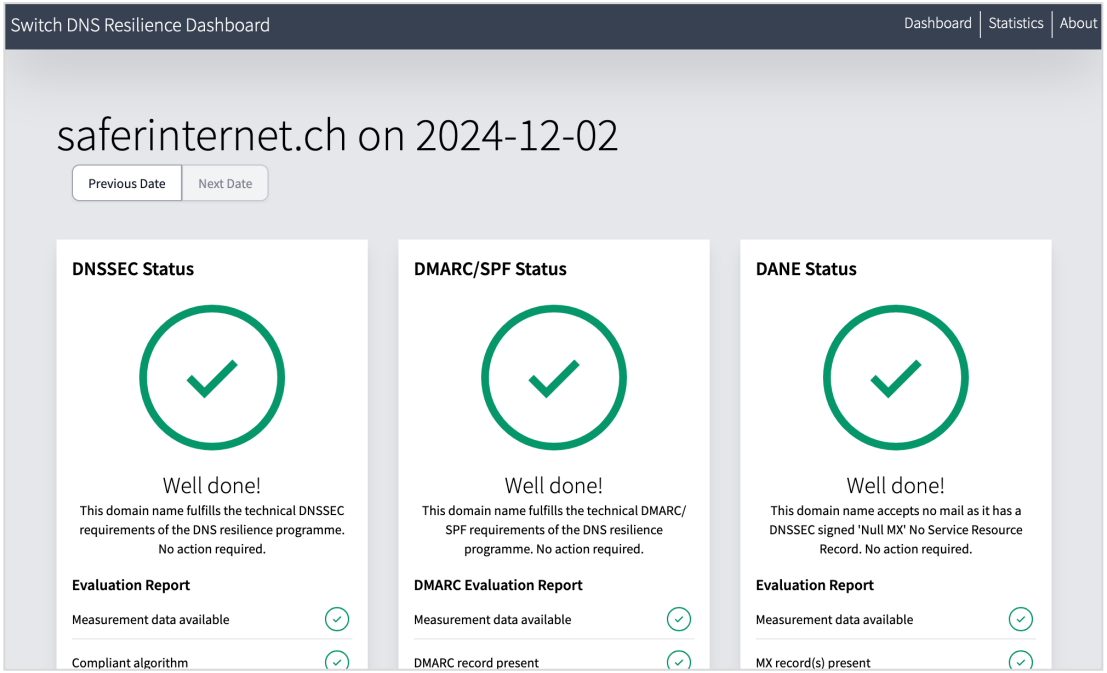
DNS-Resilienzprogramm

Auch im dritten Betriebsjahr haben wir uns neben dem Betrieb fortlaufend mit der Weiterentwicklung des Resilienzprogramms beschäftigt.

Entwicklungen 2024

- Zunahme bei der Implementation von DMARC/SPF.
- Fortlaufende Messungen bei DMARC/SPF, Versand der entsprechenden Error-Reports.
- Rückvergütungen für 2023 an die berechtigten Registrare in Form von Gutschriften (Ende Februar 2024).
- Implementierung der Messungen von DANE, dieses Kriterium wird im 2025 relevant sein.
- Seit September 2024 Versand der Error-Reports für DANE an die Registrare. Das gibt ihnen die Möglichkeit, sich auf 2025 vorzubereiten.
- Erweiterung des Dashboards für DANE beim externen Messdienstleister OpenIntel (siehe Sceenshot unten mit Resultat für den Domain-Namen saferinternet.ch).
- Fortlaufende Information der Registrare, Beantwortung ihrer Anfragen, Support.

Zahlen zum Resilienzprogramm sind auf Seite 40 zu finden.



DNS – Anycast-Standorte und Zonengenerierung

Anycast-Standorte

Mit unseren Anycast-Hostingpartnern wird die DNS-Zone weltweit auf über einhundert Standorte verteilt. Diese werden laufend den aktuellen Gegebenheiten angepasst. Seit Ende 2024 gibt es beispielweise einen neuen Knotenpunkt in Klagenfurt.

Zonengenerierung

Seit dem Wechsel der DNSSEC-Konfiguration von NSEC3 auf NSEC im Jahr 2023 wurden an der Art der Zonengenerierung keine Änderungen mehr vorgenommen.

ISO 27001 Audit mit benachbarten Registries

Der DACH-Audit findet dreimal im Jahr statt, jeweils bei einer der drei teilnehmenden Registries (DENIC, nic.at und Switch) und unter rotierender Auditführung. Im Anschluss des Audits findet jeweils ein Austausch zu den Best Practices statt.

Der erste Termin war Ende April in Frankfurt bei DENIC (denic.de). Während dreier Tage wurden DENIC und ihre Tochter, die Denic Services, auditiert. Die Leitung hatte nic.at.

Anfangs Juli traf sich die Auditgruppe bei Switch. Auditiert wurde Switch unter der Leitung des CISO der DENIC, mit der Unterstützung von ISOs aus Deutschland und der österreichischen nic.at.

Die Audit-Ergebnisse fliessen in den kontinuierlichen Verbesserungsprozess ein und werden in einem der nachfolgenden DACH-Audits durch die Auditoren überprüft.

Unter der Leitung von Switch fand vom 24. bis 26. September 2024 ein internes Audit nach ISO 27001:2022 bei der österreichischen Registrierungsstelle nic.at statt. Mit dabei waren auch Vertreter der deutschen Registrierungsstelle DENIC.

Obschon es sich um einen freundschaftlichen internen Audit handelte, wurden die gleichen strengen Ansätze wie bei einem regulären externen Audit angewendet. nic.at bestätigte den hohen Reifegrad der letzten Jahre und bewies mit kontinuierlichen Verbesserungen, dass sie ihren hohen Ansprüchen an die Normkonformität gerecht werden können.

Nach dem Audit vertiefte sich die Runde in Diskussionen rund um Normanforderungen und die Möglichkeiten, diese mit technischen und organisatorischen Massnahmen möglichst effizient und konform umzusetzen.

ISMS – ISO 27001 Surveillance Audit

Am 5. September fand der formelle ISO 27001 Surveillance Audit in den Räumlichkeiten der CSCS (Swiss National Supercomputing Centre) in Lugano statt.

Geprüft wurden bereits verschiedene Controls aus der neuen ISO 27001:2022 Norm – so unter anderem Threat Intelligence. Switch konnte hier mit ihrer langjährigen CERT-Betriebserfahrung den Auditor restlos überzeugen. Weitere Themen waren unter anderem Security Architecture Governance und Procurement.

Das Zertifikat wurde noch nach der 2013er-Norm ausgestellt.

Fazit des Auditors: «Für Switch ist Informationssicherheit ein wichtiges Asset. Auffallend sind die hohen Fachkenntnisse und das Bewusstsein für Informationssicherheit bei allen interviewten Mitarbeitenden.»

SV Cert.

IAF

SNAS
Reg. No. 661/R-141

ZERTIFIKAT

Nr. 860-ISMS-23

Rev.1

Hiermit wird bestätigt, dass das Managementsystem der

SWITCH

Werdstrasse 2 - 8021 - Zürich (Zürich, Switzerland)

Geschäftsstellen:
Werdstrasse 2 - 8021 - Zürich (Zürich, Switzerland)

die Anforderungen der Norm für das Information Security Management Systems

ISO/IEC 27001:2013

für folgenden anwendungsbereich erfüllt:

Domain Namen Registrierung

SOA Ausführung	Erstausgabedatum	Datum der Änderung	Ablaufdatum des Zertifikats
Version 1.7 vom 17.07.2024	05/12/2017	13/09/2024	05/12/2026

SV Cert. Group

Für die Zertifizierungsstelle
SV Certification Sro

(Gaetano Spera CEO SV CERT.)

Die Gültigkeit des Zertifikats unterliegt einer regelmäßigen jährlichen Überwachung und einer vollständigen Überprüfung des Systems alle drei Jahre.
Die Verwendung und Gültigkeit dieses Zertifikats unterliegen der Einhaltung der Zertifizierungsbestimmungen der SV Certification Sro.

SV CERTIFICATION Sro, HQ: Karadžičova 8A Bratislava
Mestská Casť Ružinov 821 08 – SLOVAKIA
Info & Contact: svcertification.com – info@svgroupcert.ch

«Für Switch ist Informationssicherheit ein wichtiges Asset. Auffallend sind die hohen Fachkenntnisse und das Bewusstsein für Informationssicherheit bei allen interviewten Mitarbeitenden.»

ISO 27001 Audit-Bericht

2.
Tätigkeitsbericht – Neuheiten

Switch

Domain Abuse 4.0

Moderne und zukunftsträchtige Missbrauchsbekämpfung

Wie im Jahresbericht 2023 erwähnt, ist die heutige Softwarelösung zur Bekämpfung von Cyberkriminalität den stetig zunehmenden Herausforderungen bei der Bekämpfung des Domain-Namen-Missbrauchs nicht mehr gewachsen.

Im Rahmen des Projektes «Domain Abuse 4.0» wird daher eine neue zukunftsweisende Softwarelösung entwickelt, basierend auf modernsten Technologien. Das Projektteam entwickelt eine schnelle, wartungsarme und hochskalierbare Lösung. Auch die Prozesse werden überarbeitet, an die neuen Begebenheiten angepasst und unsere Experten darin geschult. Mit diesen Massnahmen behält Switch weiterhin eine weltweit führende Rolle in der Bekämpfung von Cyberkriminalität.

Ein grosser Meilenstein ist erreicht

2024 implementierten das CERT und die Registry in gemeinsamer Arbeit die zentralen Komponenten der neuen Softwarelösung. Darin wurden erste Workflows (Prozesse gegen Missbrauch) umgesetzt und getestet.

Pünktlich auf Ende des Jahres haben wir die erste produktive Version der neuen Softwarelösung in Betrieb genommen. Seit Januar 2025 können wir nun die neue Software verwenden, um Identifikationsanfragen nach Art. 29 und 30 VID an den Halter eines Domain-Namens zu senden, wenn wir einen begründeten Verdacht auf falsche Halterangaben haben.

Domain Abuse 4.0

Ausblick 2025

Dank des Erfolges im Jahr 2024 sind wir gut aufgestellt, um bis Ende 2025 die restlichen Workflows zu implementieren und unsere alte Softwarelösung in ihren wohlverdienten Ruhestand zu entlassen.

Auf der rechten Seite sind die wichtigsten Workflows und Softwarekomponenten aufgeführt, die pro Quartal 2025 zur Implementierung geplant sind und danach schrittweise in den Betrieb überführt werden.

Ausblick 2026

Es werden fortlaufend allfällige neue Workflows und Funktionalitäten implementiert. Eine angedachte Funktionalität wird eine technische Schnittstelle zu den Behörden sein. Mit dieser Schnittstelle können Behörden unsere Softwarelösung an ihre Systeme anbinden und uns Anfragen automatisiert zusenden.

Workflows und Komponenten, die 2025 implementiert werden

Q1 2025

- Registrierungen für rein missbräuchliche Zwecke
- Feed Reader (Empfang von Missbrauchsmeldungen)

Q2 2025

- Kompromittierte Webseiten (Phishing und Malware)
- Anbindung an saferinternet.ch

Q3 2025

- Blockierungsanfragen von Behörden nach Art. 15 VID
- Automatisiertes Reporting

Q4 2025

- Korrespondenzadressenanfragen von Behörden nach Art. 16 VID

Q1 2026 laufende Weiterentwicklung

Reliability Engineering

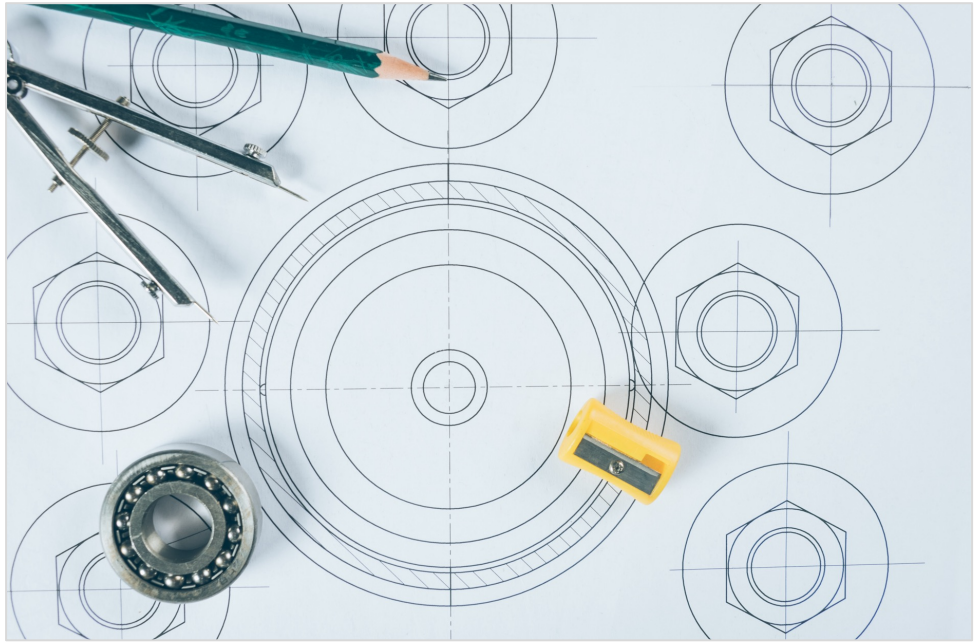
Da IT-Systeme immer komplexer werden und immer stärker in unser Leben integriert sind, ändert sich auch der Betrieb.

Um die Informationssicherheit zu ergänzen, führt Switch das Konzept des «Reliability Engineering» ein, zusammen mit einer speziellen ITSM- und Reliability-Coach-Rolle, damit Teams stabile und zuverlässige Dienste bereitstellen können.

Wir konzentrieren uns auf automatisierte und skalierbare Methoden zur Verwaltung von Verfügbarkeit, Kapazitätsleistung, Incident- und Change-Management.

Es wurden neue Prozesse und Richtlinien für das Incident-Management, das Change-Management und die Überwachung entwickelt sowie 15 Fachschulungen durchgeführt, unter anderem für Mitglieder des Infrastruktur- und des Senior-Management-Teams.

«Hope is not a strategy. Luck is not a factor. Fear is not an option.» James Cameron



Integration ISMS – DSMS

ISMS (ISO 27001) und DSMS (ISO 27701) weisen grosse Überschneidungen auf.

Einerseits verwenden sie dasselbe Managementsystem von ISO, andererseits ist das DSMS lediglich eine Ergänzung zum ISMS. Deshalb haben die beiden dafür zuständigen Boards beschlossen, die beiden Konzepte zusammenzulegen.

Das neue Konstrukt nennt sich nun «Integriertes Management-System» oder kurz IMS. Ein Zertifizierung nach ISO 27701 strebt Switch im Moment nicht an.

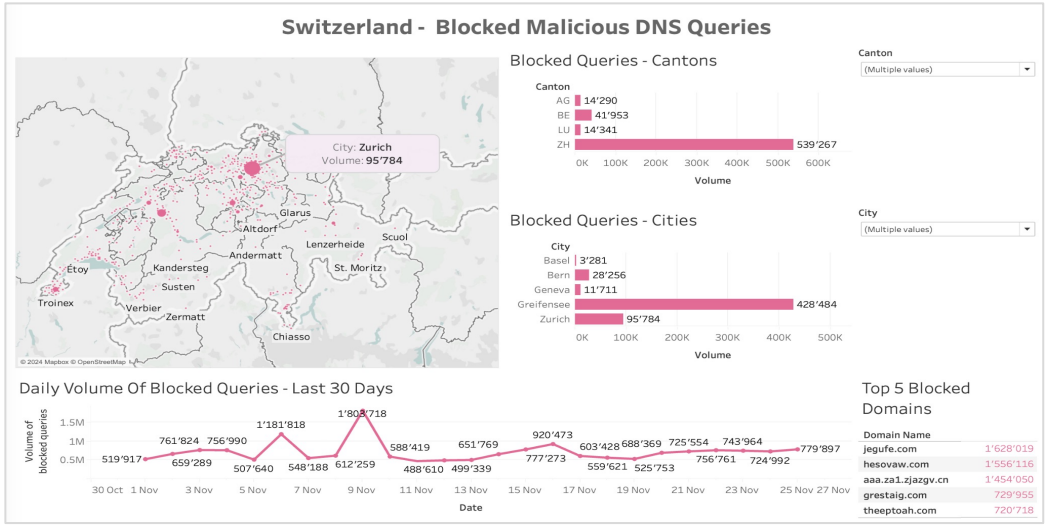
Die Zusammenführung hilft jedoch Doppelspurigkeit in der Dokumentation zu vermeiden. Es vereinfacht auch die Schulung der Mitarbeitenden, da alle erforderlichen Informationen nun an einer Stelle zu finden sind.

ISMS: Information Security Management System
DSMS: Data Protection Management Systems

Quad9: die Rolle von Threat Intelligence

Quad9 und Switch arbeiten bei der Analyse von Bedrohungen für das Schweizer Internet zusammen. Dies umfasst unter anderem:

- Entwicklung und Umsetzung einer Threat-Intelligence-Strategie für Quad9 und für Domain Abuse bei Switch.
- Analysen der monatlichen Top-Bedrohungen, die von Quad9 weltweit blockiert werden sowie Erstellung regelmässiger Berichte, die sowohl an die interessierte Sicherheits-Gemeinschaft als auch an lokale staatliche Cybersicherheitsorganisationen weitergegeben werden. Beispiele für Berichte: Security Awareness Blogpost for Christmas Shopping Season, Trends H1 2024: Cyber Insights und Blog-Artikel für AFRINIC
- Akquirieren neuer Threat-Intelligence-Partnerschaften für Quad9. Im 2024 hat Quad9 12 neue Partnerschaften geschlossen, darunter mit einem neuen Partner in der Schweiz, ThreatCat.
  Eine Liste der Partnerschaften findet man hier.
- Die Erstellung eines «Quad9 Threat Intelligence Product für Switch CERT». Ziel dieses Projekts war es, eine Lösung für Switch CERT zu entwickeln, um Bedrohungsdaten von Quad9 DNS zu sammeln, zu aggregieren und zu analysieren.
- Erstellung eines Proof of Concept Dashboards für die Schweizer Regierung. Das Dashboard zeigt die wichtigsten Bedrohungen, die von Quad9 auf nationaler Ebene blockiert wurden:



- Wie das Eidgenössische Departement für auswärtige Angelegenheiten EDA mitteilte, wurde Quad9 zum schützenden DNS-Resolver für NGOs und IGOs, die in der Schweiz ansässig sind.

Top-Bedrohungen für das Schweizer Web

Aufgrund der von Quad9 erhobenen Daten waren 2024 folgende Kampagnen in Gang und eine Gefahr für Schweizer Internetnutzende:

SocGolish-Kampagnen

Eine weit verbreitete, jahrelange Malware-Kampagne, die darauf abzielt, gefälschte Browser-Updates an ahnungslose Internetnutzende zu verteilen. Einmal installiert, infizieren die gefälschten Browser-Updates den Computer des Opfers mit verschiedenen Arten von Malware, darunter auch Remote-Access-Trojaner (RATs).

In dieser speziellen Kampagne wurde blacksaltys.com verwendet. Mehr als 123’000 Anfragen wurden durch Quad9 in der Schweiz und mehr als 7 Millionen weltweit blockiert.

Phishing SBB

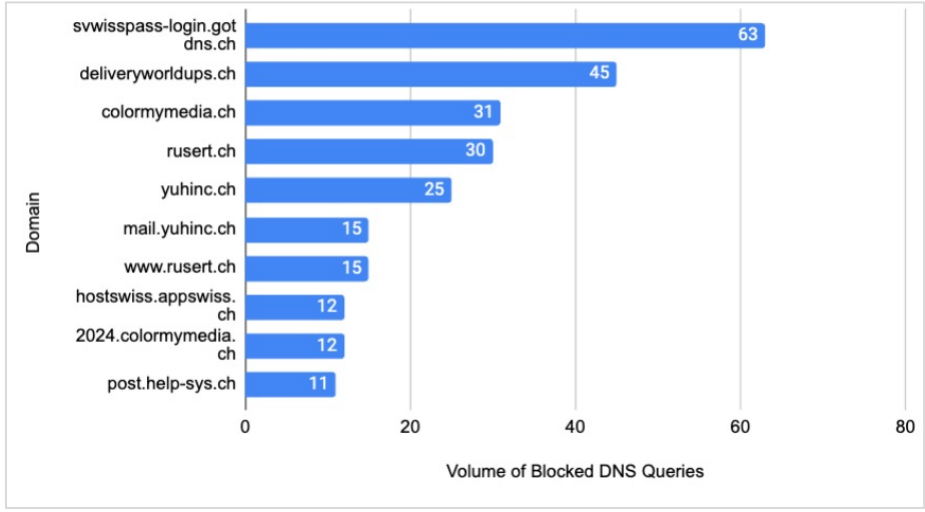
Phishing-Kampagne, welche die Opfer dazu brachte, ihre SwissPass-Daten einzugeben.

Verwendet wurde der Domain-Name divinedownload.com. Quad9 blockierte mehr als 2280 DNS-Anfragen von Schweizer Internet-Nutzenden.

Phishing Schweizer Post

Phishing-Kampagne gegen die Schweizer Post, bei der die Opfer dazu gebracht wurden, ihre Anmeldedaten anzugeben. Bei dieser Kampagne wurde der Domain-Name espace-login.net verwendet. Quad9 blockierte mehr als 2340 DNS-Anfragen von Schweizer Internet-Nutzenden.

Die am häufigsten blockierten infizierten .ch-Domain-Namen, die von Switch CERT an Quad9 übermittelt wurden, betrafen die Kampagne gegen SwissPass-Benutzer und Kampagnen gegen Zusteller (UPS, Deutsche Post) sowie Webmail-Dienste.



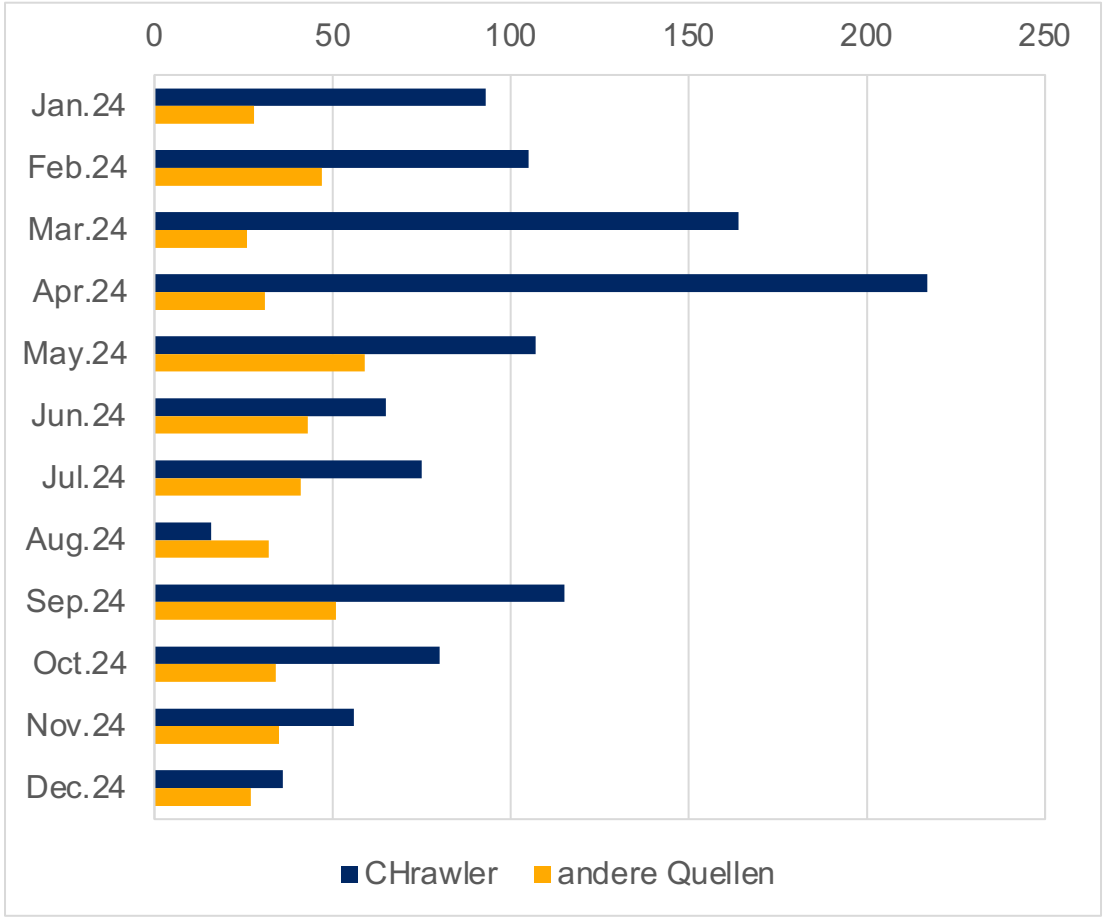
Web-Crawler

Mit unserem Web-Crawler (CHrawler), der Anfang 2024 in Betrieb genommen wurde, untersuchen wir regelmässig und systematisch öffentlich zugängliche Ressourcen in der .ch- und .li-Zone, um kompromittierte oder böswillige Domain-Namen frühzeitig zu entdecken und damit die Gefahr für Internetnutzende zu bannen. Wenn wir mit unserem Crawler Domain-Namen entdecken, die Phishing betreiben oder Malware verbreiten, können wir den Domain-Namen nach Benachrichtigung des Halters und einer Wartezeit blockieren.

Nach knapp einem Jahr Betrieb zeigt sich, dass wir regelmässig eine erhebliche Anzahl an infizierten Domain-Namen finden können, dies gerade auch im Vergleich zu den uns sonst gemeldeten Zahlen, siehe hierzu die Statistik rechts. Insgesamt konnten wir so im Jahr 2024 rund 1200 infizierte Domain-Namen entdecken.

Somit kann Switch nicht nur reaktiv, sondern auch proaktiv durch eigenständige Suche einen wichtigen Beitrag dazu leisten, die Sicherheit der .ch- und .li-Zone noch weiter zu steigern. Darüber hinaus sammeln wir wichtige Erkenntnisse darüber, welche Kampagnen und Bedrohungen im Schweizer Web derzeit aktiv sind. Siehe auch «Top-Bedrohungen für das Schweizer Web» auf Seite 32.

Verarbeitete .ch Malware-Domains 2024



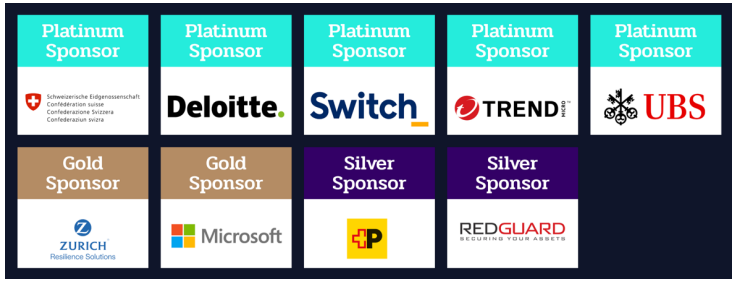
Women in Cyber Switzerland

Trotz des in den letzten Jahren zu beobachtenden Wachstums im Bereich Cyber ist bei näherer Betrachtung festzustellen, dass Frauen bei den Beschäftigten weltweit immer noch unterrepräsentiert sind. Dies geschieht vor dem Hintergrund eines wachsenden Fachkräftemangels im Cyberbereich. Um den Unternehmen zu helfen, diese Lücke zu schliessen, ist es wichtig, mehr Frauen für den Cyberbereich zu begeistern und ihnen gleiche Chancen zu bieten.

«Women in Cyber Switzerland» engagiert sich für mehr Diversität mit der Organisation des jährlichen «Women in Cyber« Days und lokalen Networking Events sowie einem Mentoringprogramm.

Switch unterstützt die Initiative seit 2019 und ist aktives Vorstandsmitglied. Im März fand bei Switch in Zürich das erste lokale Networking Event statt.

https://women-in-cyber.ch



NextGen Hero

Jungtalente gewinnen NextGen Hero Award

Bei der Preisverleihung der Digital Economy Awards am 14. November 2024 wurden im Zürcher Hallenstadion Unternehmen, Organisationen und Persönlichkeiten in verschiedenen Kategorien für ihre einzigartigen Beiträge zu Gunsten der digitalen Transformation der Schweiz ausgezeichnet.

In der Kategorie «NextGen Hero», die in Zusammenarbeit mit Switch stattfindet, wählte das anwesende Publikum zwei junge Talente für ihre herausragende Kreativität und Innovationskraft: Selina Pfyffer und David Cleres.

Wer sind diese aufstrebenden Stars und welche Ziele verfolgen sie? Im Interview berichten sie von ihren Visionen und wie sie den digitalen Fortschritt der Schweiz mitgestalten.

Die fünfte Ausgabe der Digital Economy Awards brachte hunderte Fachleute der Schweizer ICT-Szene zusammen, um die herausragendsten Talente und ihre Innovationen zu feiern. In sechs Preiskategorien nahmen die Besten der Besten einen Award entgegen.

Übergabe des Digital Economy Awards 2024 in der Kategorie «NextGen Hero». V.l.n.r.: Tom Kleiber, Switch; Claudia Lienert, Switch; David Cleres, GirlsCodeToo; Selina Pfyffer, SeasonCell; Monika Schär, Moderation. Foto: Switch

3.

Tätigkeitsbericht – Statistische Kennzahlen

Switch

Domain-Namen-Bestand – Entwicklung 2024

Entwicklung .ch

Innerhalb eines Jahres hat sich der Bestand von .ch-Domain-Namen um gut 6’000 vergrössert.

	2023	2024
Neuregistrierungen	294’195	279’916
Löschungen	282’649	303’361
Reaktivierungen*	29’958	29’948
Domain-Bestand per 31.12.	**2’562’914**	**2’568’952**

Entwicklung .li

Innerhalb eines Jahres hat sich der Bestand von .li-Domain-Namen um gut 1’000 Domain-Namen verkleinert.

	2023	2024
Neuregistrierungen	10’658	9’495
Löschungen	12’218	11’608
Reaktivierungen*	1’699	1’285
Domain-Bestand per 31.12.	**70’607**	**69’774**

* Gelöschte Domain-Namen, die vom Registrar innerhalb der Übergangsfrist von 40 Tagen wieder reaktiviert wurden.

Auskunftsdienst – Statistik 2024

Auskunftsdienst Zahlen

Switch gewährt jeder Person, die ein überwiegendes legitimes Interesse glaubhaft macht, kostenlos Zugang zu den in der RDDS-Datenbank (Whois) enthaltenen Personendaten der Halterin oder des Halters des betreffenden Domain-Namens. Diese Statistik erfasst alle Anfragen im Berichtsjahr, welche über die Formulare des Auskunftsdienstes gestellt wurden. Die Anzahl der Anfragen von Privaten blieb im Vergleich zum Vorjahr im selben Rahmen.

	Privat	Behörden
Auskunft erteilt	309	73
Auskunft nicht erteilt	54	5
Generelle Anfragen *	6	0
Total Anfragen	**369**	**78**

* Hierbei handelt es sich um Anfragen zu Prozessen, Vorgehen und zu rechtlichen Grundlagen.

Vereinfachter Zugang über RDAP für .ch und .li

Wenn eine Behörde oder Organisation die entsprechenden Berechtigungen hat, kann sie via RDAP (Registration Data Access Protocol) Domain-Namen mit Personendaten abfragen. Die Anzahl der Behörden hat im 2024 weiter zugenommen, was auch auf unsere bessere Vernetzung mit den Strafverfolgungsbehörden zurückzuführen ist. Per Ende 2022 nutzten erst 5 Behörden RDAP, Ende 2024 waren es 17 Behörden. Den grössten Anteil machen die Kantonspolizeien aus.

	Anfragen
Auskunft erteilt	4’203
Auskunft nicht erteilt	368
Total Anfragen	**4’571**

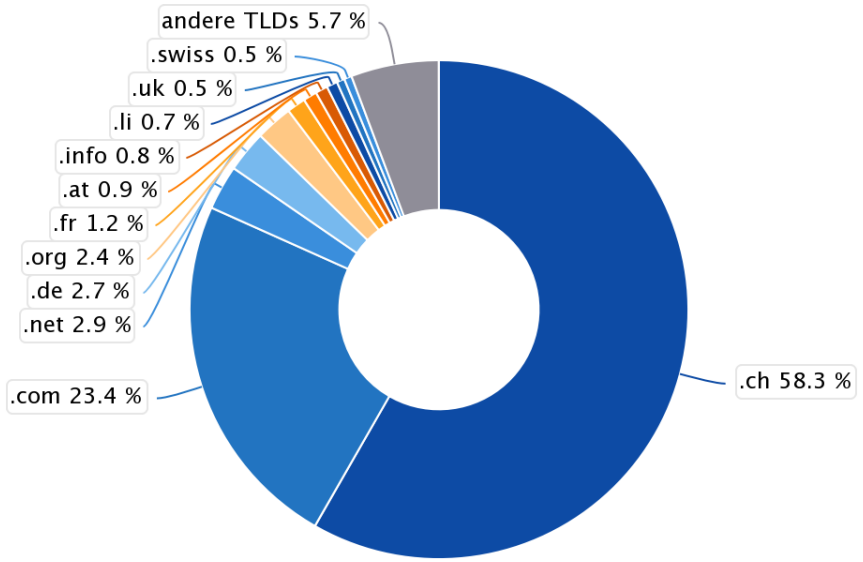
Marktanteil von .ch und .li bei Schweizer Halterinnen und Haltern von Domain-Namen

Der Marktanteil der TLD (Top-Level Domain) **.ch** bei Halterinnen und Haltern aus der Schweiz blieb vom Oktober 2023 bis Oktober 2024 praktisch unverändert.

Beim Marktanteil der generischen TLDs **.com/.net/.org** hat sich wenig verändert, ebenso bei **.li**-Domain-Namen.

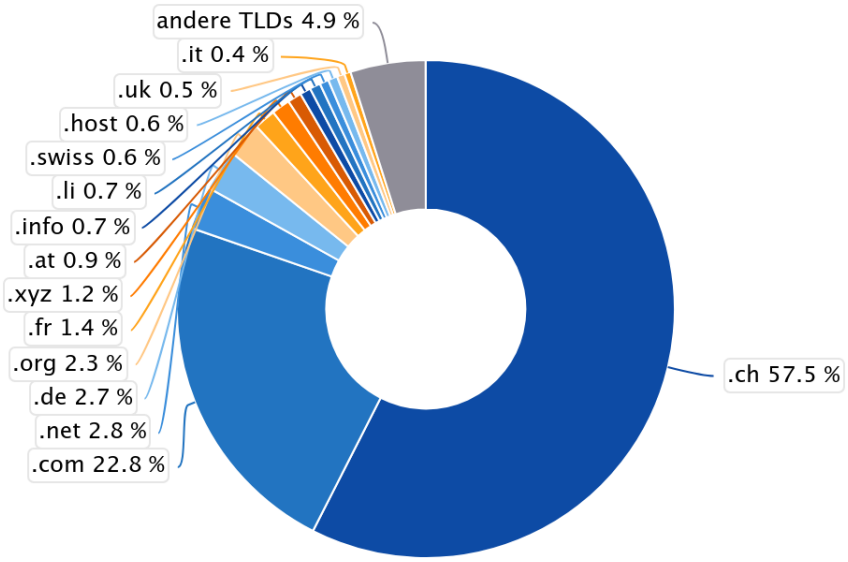
Oktober 2023

Marktanteil verschiedener TLDs bei Domain-Namen-Halterinnen und Haltern in der Schweiz. Quelle: CENTR



Oktober 2024

Marktanteil verschiedener TLDs bei Domain-Namen-Halterinnen und Haltern in der Schweiz. Quelle: CENTR



DNS-Resilienzprogramm – Entwicklung in Zahlen

DNSSEC

- Anteil DNSSEC bei .ch-Domain-Namen, Stand 1. Januar 2025: 50.4% (1. Januar 2024: 49,1%).
- Fehlerquote: Die Fehlerquote ist übers Jahr konstant auf sehr tiefem Niveau geblieben. Durchschnittliche Fehlerquote aller DNSSEC-Domain-Namen: 0.17%, wie schon im Jahr 2023.

DMARC und SPF

- 1. Januar 2025: 20.1% korrekt konfiguriert (1. Januar 2024: 4.5%). Zahlen für .ch und .li Domain-Namen, korrekte Konfiguration sowohl von DMARC als auch von SPF. Angaben gemäss Statistik des externen Messdienstleisters.

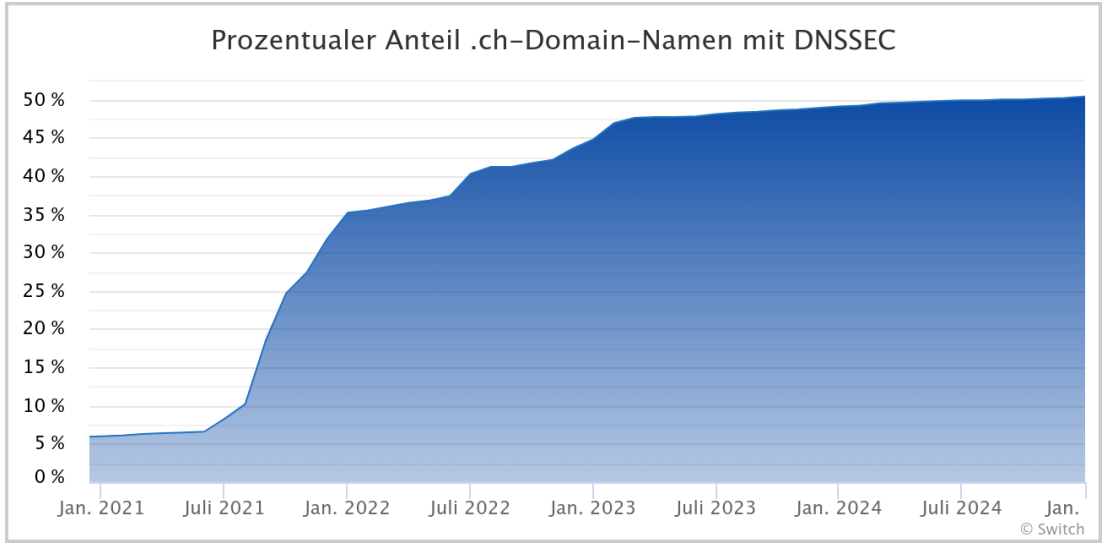
Statistik DNSSEC bei Switch

Statistik bei OpenIntel

Berechnung der Rückvergütung für das Jahr 2024

- Gesammelte Mehreinnahmen aus Preisdifferenzierung: CHF 1'569'687
- Abzüglich fixer Kompensation für Switch und den externen Messdienstleister 2024: CHF – 444'907
- Total Rückvergütung CHF 1'124'780

Die Rückvergütungen erfolgen Ende Februar 2025.

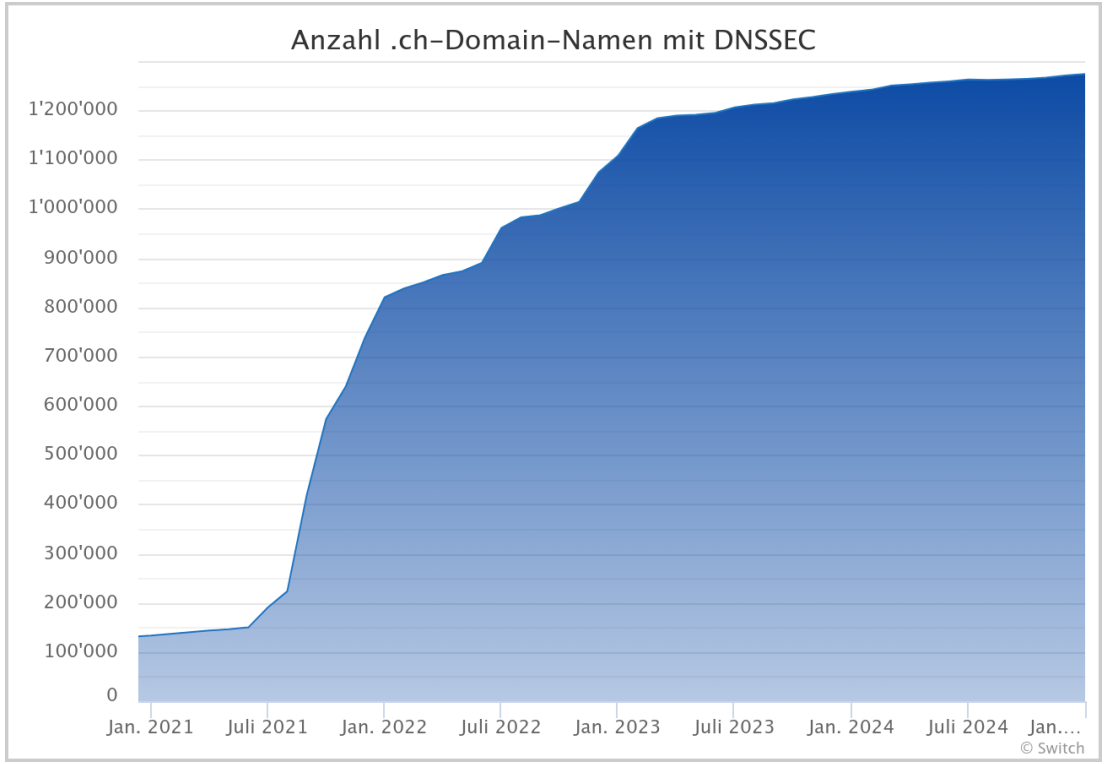


Entwicklung DNSSEC
Anzahl signierter Domain-Namen

Ende 2024 sind über 1.27 Millionen .ch-Domain-Namen mit DNSSEC signiert.

Dies entspricht einem Anteil von 50.4 Prozent aller .ch-Domain-Namen mit Name-Servern, gegenüber 45 Prozent Ende 2022 und 35 Prozent Ende 2021. Die starke Zunahme in den Jahren 2021 und 2022 wurde hauptsächlich von Registraren getrieben, welche im Zuge des DNS-Resilienzprogramms alle Domain-Namen ihrer Kunden signiert haben. In den folgenden Jahren hat sich dieses Wachstum verlangsamt.

Die grösseren Schweizer Registrare haben mittlerweile ihre Domain-Namen soweit möglich signiert. Wenn die Domain-Namen «fremde» Name-Server haben, haben die Registrare keinen Einfluss auf die Signierung. Für die grossen Registrare im Ausland macht die TLD .ch nur einen sehr kleinen Teil ihres Business aus und der Aufwand der Signierung lohnt sich für sie eher nicht. Daher ist für die Zukunft nur noch mit wenig Zuwachs zu rechnen.

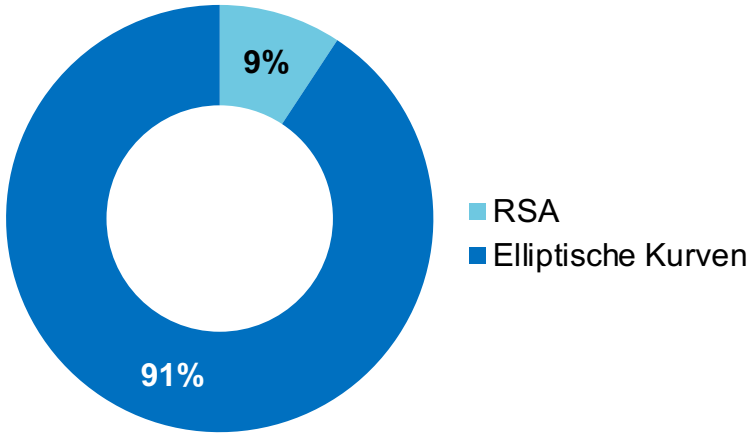


1'273'817 mit DNSSEC signierte .ch-Domain-Namen am 1. Januar 2025

Entwicklung DNSSEC
Verteilung DS-Algorithmen

Weiterhin verwenden über 90 Prozent aller .ch-Domain-Namen den aktuell empfohlenen Algorithmus 13 (ECDSAP256SHA256).

Ein leichter Anstieg ist bei der Signierung mittels Edwards-Curves (EdDSA-Algorithmen 15 und 16) zu verzeichnen. Diese werden von älteren Betriebssystemen nicht oder nur teilweise unterstützt und sind daher bisher nur beschränkt empfohlen.



Verwendete DNSSEC-Signaturen

DNSSEC-Algorithmus	Anzahl	Anteil
8 – RSASHA256	11’806	9.27 %
10 – RSASHA512	86	0.01 %
13 – ECDSAP256SHA256	1’153’418	90.55 %
14 – ECDSAP384SHA384	150	0.01 %
15 – Ed25519	1’929	0.15 %
16 – Ed448	123	0.01 %

DNSSEC-Validierung in der Schweiz

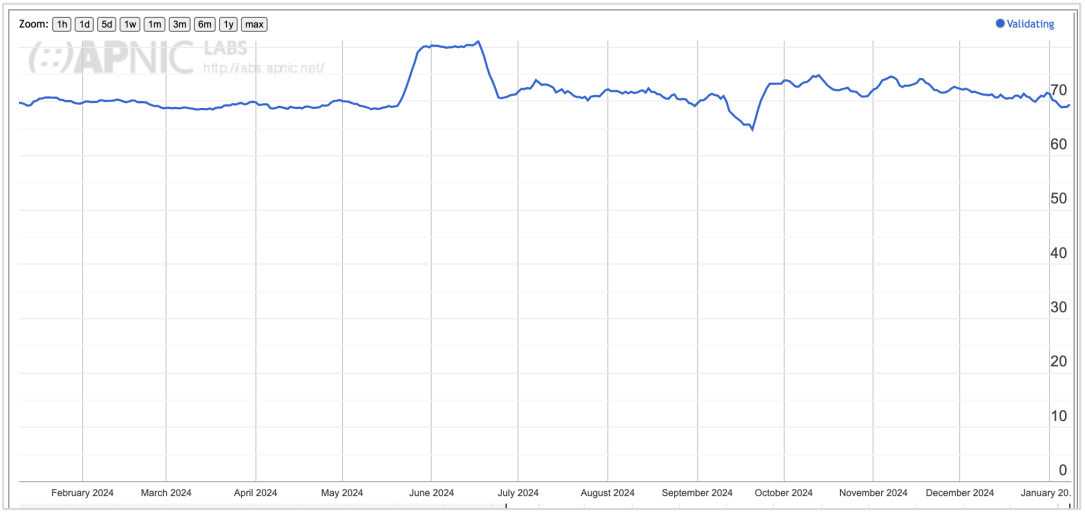
DNSSEC-Validierung

Damit Nutzende vor DNS-Spoofing geschützt sind, müssen einerseits die Domain-Namen signiert sein, andererseits müssen diese Signaturen vom DNS-Resolver validiert werden.

Nach Messungen von APNIC lag die DNSSEC-Validierungsrate auf den Resolvern der Schweizer ISPs im letzten Jahr konstant bei ca. 70%.

Webseite: https://stats.labs.apnic.net/dnssec/CH

DNSSEC-Validierung auf Schweizer Resolvern

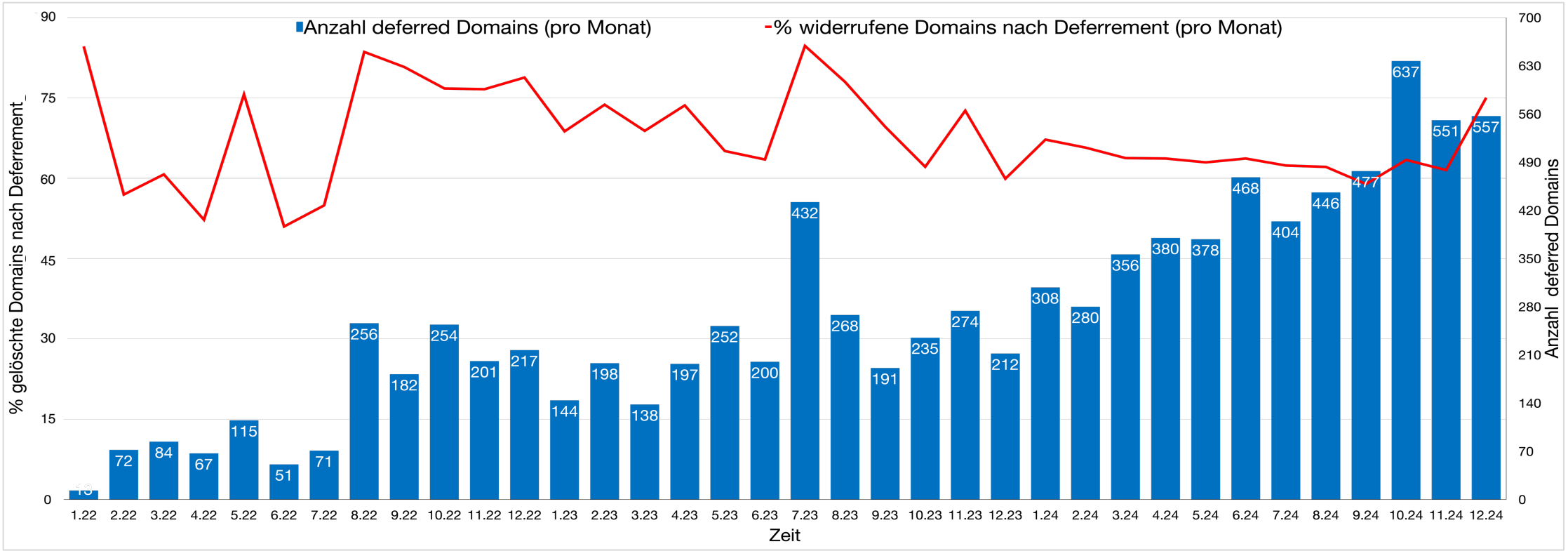


Deferred Delegation

Deferred Delegation im zeitlichen Rückblick

Im letzten Jahr haben wir die Anzahl an Registrationen, welche «deferred» wurden, durch weitere Regelverschärfungen nochmal erheblich gesteigert, ungefähr um den Faktor zwei.

Wie bei einer solchen Steigerung zu erwarten, ist auch der Anteil von Domain-Namen, welche nach positiver Identifikation des Halters wieder freigegeben wurden, etwas gestiegen. Durch ein behutsames und iteratives Erweitern der Kriterien ist dies allerdings im Vergleich zu den «deferrten» Domain-Namen in viel geringerem Masse geschehen.



Streitbeilegungsfälle

Switch hat vom Bakom den Auftrag, einen kostengünstigen Streitbeilegungsdienst anzubieten. Dazu nutzt Switch seit 2004 den Streitbeilegungsdienst der WIPO (World Intellectual Property Organization). Die WIPO betreibt einen von ICANN akkreditierten Streitbeilegungsdienst für über 70 weitere Registries.

Im Jahr 2024 haben die Experten für 13 .ch-Domain-Namen Entscheide gefällt. Der Expertenentscheid ist der letzte Schritt im Verfahren. Eine etwas kleinere Zahl von Fällen wird bereits vorher beendigt, zum Beispiel während des Schlichtungsversuchs oder durch Abbruch des Verfahrens.

Entscheid WIPO	**2023**	**2024**
Auf Gesuchsteller übertragen	11	10
Klage abgewiesen	5	3
Anzahl Entscheide	**16**	**13**

Entscheide der WIPO (Stand 17. Februar 2025)

	Domain-Namen
Auf Gesuchsteller übertragen	girlscancode.ch axashop.ch salonmoulinrouge.ch veka-fenster.ch vekafenster.ch floqast.ch elfbar.ch aqara.ch giezemon.ch universalgeneve.ch
Klage abgewiesen	carify.ch johntaylor.ch meinl.ch

Entwicklung Registrare

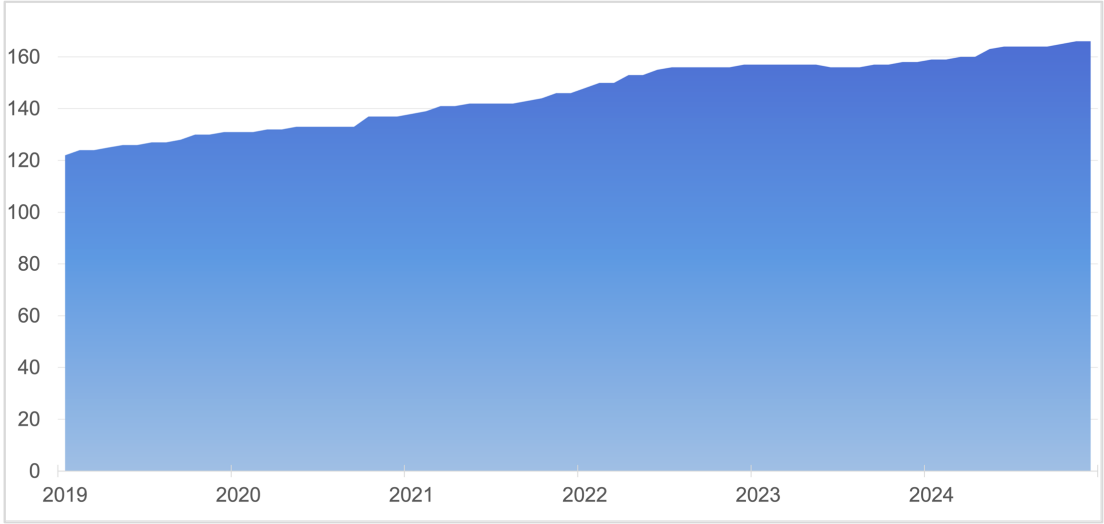
2019 stieg die Anzahl der Registrare auf 131 und per Ende 2020 zählte die Registry 137 Registrare. Im Jahr 2021 stieg die Anzahl um 9 Registrare auf ein Total von 146.

Im 2022 haben 11 Registrare zuerst einen Testvertrag für den Zugang zum Testsystem unterzeichnet. Nach erfolgreicher Testphase und dem Bestehen des Testparcours konnten wir diese Registrare produktiv schalten. Die Gesamtzahl der anerkannten Registrare stieg somit auf 157.

Im Jahr 2023 konnten wir nur einem weiteren Registrar Zugang zum produktiven System geben und die Anzahl stieg auf 158.

2024 kamen 7 Registrare hinzu, was per Ende Jahr ein Total von 165 ergab.

Die in den Jahre 2023 und 2024 acht neu hinzugekommenen Registrare haben zusammen ein Portfolio von 8’500 Domain-Namen, wobei einer davon gut 7’500 Domain-Namen verwaltet.



Performance der Name-Server

Switch stützt sich für die Anforderungen an die DNS-Performance-Messungen bezüglich Antwortzeiten von DNS-Anfragen auf das ICANN-Agreement: Anfragen an die CH-Zone müssen von mindestens einem logischen Name-Server innert 500 ms (UDP) bzw. 1500 ms (TCP) beantwortet werden.

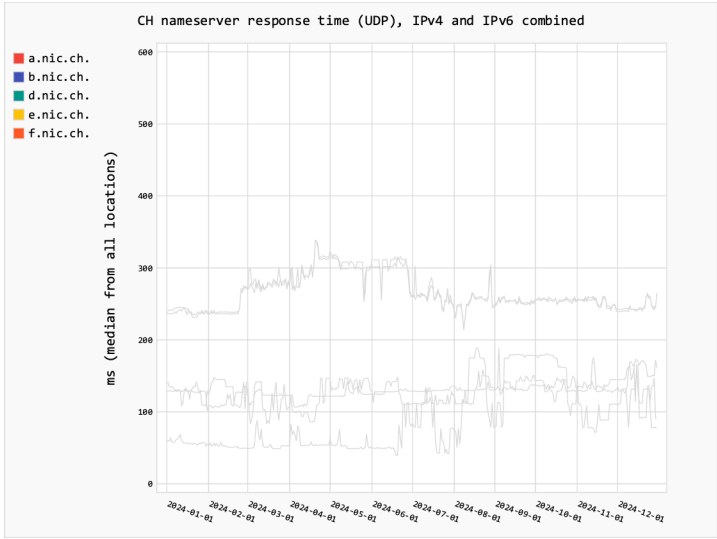
Diese Anforderung wurde 2024 jederzeit erfüllt.

Die Messungen werden von RIPE durchgeführt und sind öffentlich einsehbar.
https://atlas.ripe.net/dnsmon/group/ch

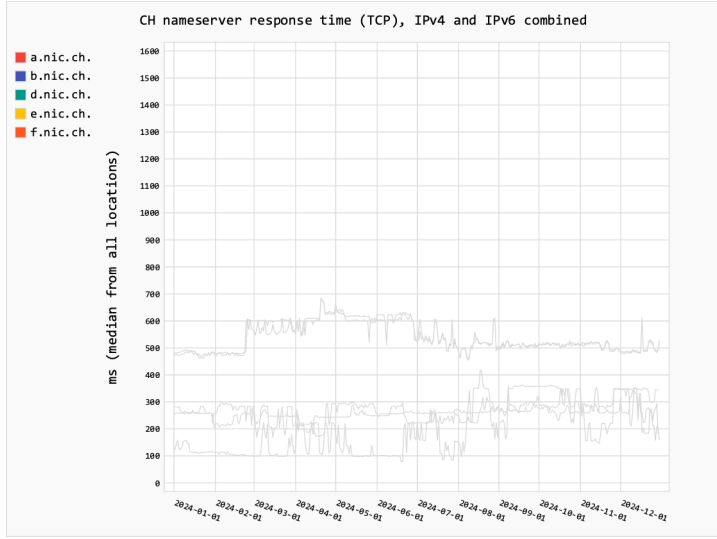
Unicast: a.nic.ch (CH), b.nic.ch (CH)

Anycast: d.nic.ch, e.nic.ch, f.nic.ch

UDP-Antwortzeiten
kombinierte Anwortzeiten
von IPv4 und IPv6



TCP-Antwortzeiten
kombinierte Anwortzeiten
von IPv4 und IPv6



Cyberkriminalität 2024

Quantitativ

Im Berichtsjahr wurden folgende Fälle erfasst und behandelt:

Anzahl Malware- und Phishing-Fälle 2024 quantitative Betrachtung

	# Malware-Fälle	# Phishing-Fälle
Eingegangene Meldungen	**1’730**	**451**
Verdacht bestätigt	**1’392**	**239**
Anzahl blockierte Domain-Namen	**656**	**115**
Begründung für die Aufhebung der Blockierung: - Gesetzliche Dauer ist überschritten - Behoben nach Blockierung - In Bearbeitung am Stichtag	 **83** **402** **3**	 **2** **15** **3**
Widerrufene Domain-Namen	**170**	**95**

Qualitativ

Für die Fälle wurde folgende Zeit aufgewendet:

Anzahl Malware- und Phishing-Fälle 2024 qualitative Betrachtung

	Dauer	
Dauer der Blockierung gemäss VID Art. 15 Abs. 1, 2, 3 max. Blockierungszeit 30 Tage (720h)	Mindestdauer Durchschnitt Höchstdauer	**0.22 h** **103.74 h** **166.92 h**
Reaktionszeiten von Switch nach Meldung	Durchschnitt	**5.13 h**
Zeit bis zur Beseitigung der Bedrohung nach Bekanntgabe an Halter:in	Durchschnitt	**86.8 h**

DNS Health Report

Der DNS Health Report prüft die Erreichbarkeit von Name-Servern und Domain-Namen unter .ch und .li. Bei technischen Problemen informiert Switch die Betreiber und gibt Empfehlungen zur Behebung ab. Damit verbessert der DNS Health Report die Zuverlässigkeit des Schweizer Internets. Was wird geprüft:

- Name-Server: Die Funktion der Name-Server wird auf ihre Übereinstimmung mit den DNS-Standards geprüft.
- Domain-Namen: Es wird geprüft, ob DNSSEC-signierte Domain-Namen über einen validierenden rekursiven Resolver aufgelöst werden können.

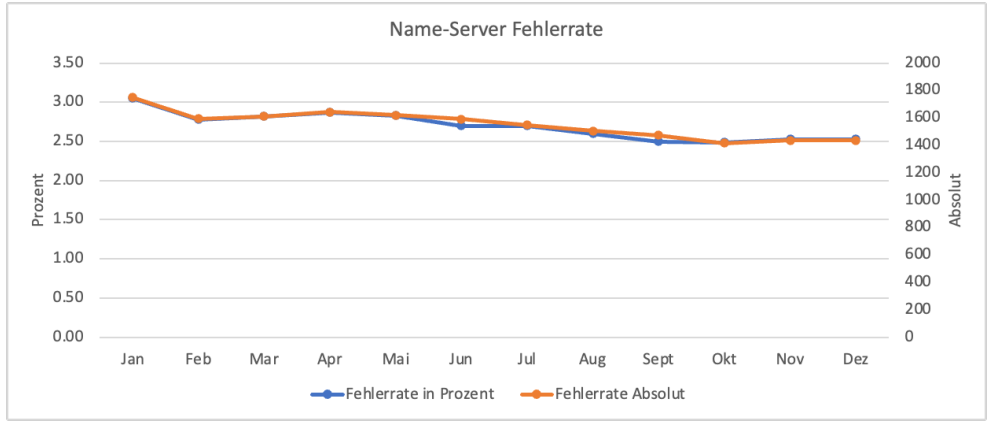
Name-Server-Report

Die Fehlerrate der Erreichbarkeitsmessung von Name-Servern nimmt seit Messbeginn nur leicht aber dafür stetig ab. Die wahrscheinlichste Ursache sind Software-Updates.

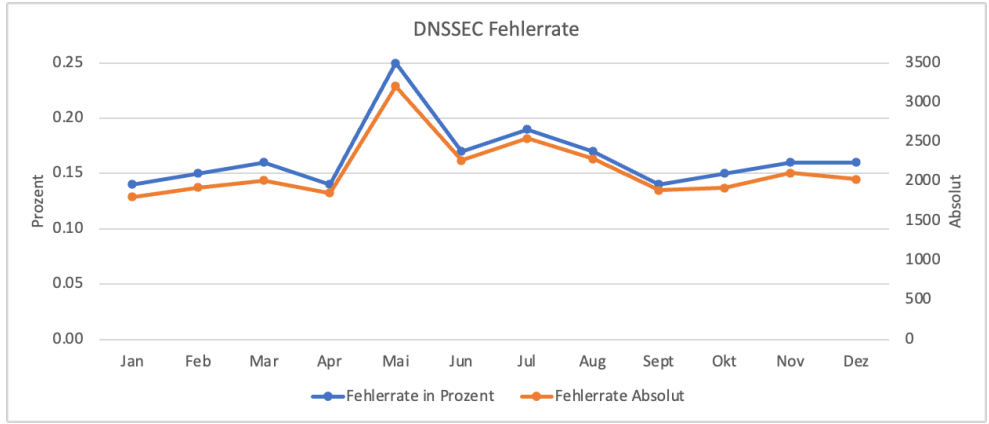
Domain-Namen-Report

Die Fehlerrate der Erreichbarkeitsmessung von DNSSEC-Domain-Namen hat ein Plateau erreicht. Die meisten fehlerhaften Domain-Namen sind geparkte Domain-Namen, bei denen die Motivation klein ist, die Fehler zu korrigieren.

Fehlerrate der Erreichbarkeitsmessung von Name-Servern



Fehlerrate der Erreichbarkeitsmessung von Domain-Namen



4.

Tätigkeitsbericht – Wirtschaftliche Kennzahlen

Switch

Wirtschaftliche Kennzahlen

An der Stiftungsratssitzung vom 12. Juni 2025 wird der Geschäftsbericht 2024 der Stiftung Switch zusammen mit der Bilanz und Erfolgsrechnung verabschiedet. Die Veröffentlichung findet ab dem 13. Juni 2025 statt.

An dieser Stelle werden keine Zahlen publiziert, sondern es wird auf die ausführlichen Unterlagen des Geschäftsberichts 2024 von Switch verwiesen.

5.
Tätigkeitsbericht – Entwicklungen

Switch

Rückblick 2024

DNS-Resilienzprogramm

Die Preisdifferenzierung für korrekt mit DNSSEC signierte Domain-Namen wurde auch 2024 weitergeführt. Die finanziellen Anreize des Programms fördern die kryptographische Sicherung des Domain-Namen-Systems sowie die Einführung von weiteren sicheren Protokollen. Im Jahr 2024 waren das die E-Mail-Sicherheitsstandards DMARC und SPF. Die Messungen und das Feedback an die Registrare konnten reibungslos durchgeführt werden. Mehr auf Seite 21

Web-Crawler für die Registry

Der neue Web-Crawler wurde bereits Anfang 2024 erfolgreich in Betrieb genommen. Diese neue Leistung der Registrierungsstelle wurde erforderlich, weil keine Meldungen mehr vom NCSC kamen, da deren Crawler eingestellt wurde. Den eindrücklichen Leistungsausweis des Crawlers und der darauf folgenden Domain-Abuse-Prozesse zeigt die Statistik auf Seite 33.

Domain Abuse 4.0

Für das Projekt hatten wir eine Laufzeit von zwei Jahren veranschlagt, mit dem Ziel, Ende 2025 fertig zu sein. Der Fortschritt im Jahr 2024 war sehr zufriedenstellend. Damit können wir auch den Termin für die Fertigstellung einhalten.

Die Rahmenbedingungen aus dem Vertrag mit dem BAKOM legen klar fest, dass Daten im Rahmen der Cybercrime-Bekämpfung auf Switch-Systemen verarbeitet werden müssen. Intensive Abklärungen mit möglichen Software-Anbietern für Teile der Applikation zeigten, dass nur eine Eigenentwicklung diese Anforderung erfüllen kann. Das interne Entwicklungsteam wurde für die Dauer der Umsetzung durch zwei externe Fachkräfte verstärkt.

Weitere Details zum Verlauf des Projektes befinden sich auf Seite 27.

ISMS ISO 27001:2022

Die Umstellung des internen ISMS nach der neuen ISO-Norm war für 2024 eingeplant, musste jedoch umpriorisiert werden.

Geplante Neuheiten 2025

DNS-Resilienzprogramm: IPv6-Messungen

Im Jahr 2026 wird das Kriterium für die Rückvergütung IPv6 bei Name-Servern sein. Damit soll die Resilienz weiter erhöht werden. Switch bereitet die Mess-Infrastruktur entsprechend vor. Ebenfalls wird das Dashboard ergänzt, damit Registrare und Hoster prüfen können, ob sie die Konfiguration gemäss den Empfehlungen von Switch korrekt umgesetzt haben.

Domain Abuse 4.0

Ein Grossteil der Entwicklungskapazität der Registrierungsstelle fokussiert sich auf die Fertigstellung der neuen Infrastruktur zur Bekämpfung von Cyberkriminalität. Darin inbegriffen ist auch die Schulung der Fachleute, die schrittweise neue Werkzeuge erhalten. Der grobe Projektplan dazu ist auf Seite 28 zu finden.

Datenbank-Upgrade

Im 2. Quartal 2025 wird die Datenbank PostgreSQL von Version 13 auf Version 16 migriert. Damit wird das Herzstück der Registrierungsanwendung erneuert. Eine sorgfältige Vorbereitung ist eine wichtige Voraussetzung. Ebenso stützen wir uns auf externe Datenbank-Experten.

ISMS ISO 27001:2022

Der zweitägige Audit gemäss der 2022er-Norm findet am 10. und 11. September 2025 statt. Bis dahin müssen alle Dokumente und Prozesse des Informationssicherheits-Managementsystems ISMS angepasst sein.

Geplante Neuheiten 2025

Deferred Delegation und Machine Learning

Ob ein Domain-Name bei der Neuregistrierung in den Deferred-Delegation-Prozess kommt oder nicht, entscheiden Regeln, die nach bestimmten Mustern (Patterns) suchen und danach eine Gewichtung dieser Resultate vornehmen. Dies kann für jeden Fall transparent nachvollzogen werden.

Switch entwickelt einen neuen Algorithmus, der Machine Learning nutzt. Die Patterns sind nach wie vor zentral. Die Gewichtung wird jedoch dynamischer. Das System wird mit Domain-Namen trainiert, die als missbräuchlich bestätigt sind oder die länger ohne Missbrauch registriert sind. Die Registrierungsstellen von Belgien und den Niederlanden setzen bereits ein solches Werkzeug ein und teilen ihre Erfahrung.

Ein Wechsel auf dieses neue System wird voraussichtlich nicht 2025 stattfinden. Es geht zunächst um den Wissensaufbau und die Verifizierung des Konzeptes.

Domain-Scanner für CDS

Im Jahr 2025 ist geplant, die Infrastruktur für das automatische Management der DNSSEC-DS-Records zu erneuern. Der Scanner, welcher täglich die ganze Zone nach CDS-Records (RFC8078) durchsucht, wird dank eines verbesserten Suchalgorithmus effizienter. CDS-Records werden damit schneller gefunden und verarbeitet. Zusätzlich werden vorbereitende Arbeiten durchgeführt, um zukünftig einen Suchlauf für einzelne Domain-Namen zu einem beliebigen Zeitpunkt anzustossen, so dass nicht auf den nächsten täglichen Suchlauf gewartet werden muss.

Mit der erneuerten Scan-Infrastruktur werden die Grundlagen geschaffen, um zukünftig neben den DNSSEC-Daten auch CSYNC-Records (RFC7344) zu verarbeiten, welche die automatisierte Verwaltung der Name-Server-Informationen ermöglichen.

RPP – RESTful Provisioning Protocol

Von EPP zu RPP

Das Extensible Provisioning Protocol (EPP) wurde 2009 standardisiert und hat die Kommunikation zwischen den Registrierungsstellen und den Registraren vereinfacht. Vor der Einführung von EPP hatten die verschiedenen Registries keine einheitlichen Schnittstellen für die Registrierung und Verwaltung von Domain-Namen.

Obwohl EPP der Branche immer noch gute Dienste leistet, wecken die Fortschritte bei Entwicklungs- und Integrationswerkzeugen sowie bei betrieblichen Abläufen und eingesetzten Technologien den Wunsch nach einem neuen Provisioning-Protokoll.

Wie könnte ein modernes Protokoll aussehen?

Ein naheliegender Ansatz ist es, die REST-Architektur und das JSON-Datenaustauschformat zu verwenden. Ein solches Design kann die Vorteile einer zustandslosen Architektur und weit verbreiteter Lösungen wie OpenAPI, Test- und Codegenerierungswerkzeuge sowie API-Gateways, Autorisierungsserver, Lastverteiler usw. nutzen.

Die REST-Architektur soll eine einfachere Integration zwischen Registrierungsstellen und Registraren ermöglichen. Die erfolgreiche Einführung von RDAP hat die Nützlichkeit dieser Art von Architektur gezeigt. Integration und Effizienz können gesteigert werden, ohne die Standardisierung aufzugeben.

Das neue Protokoll soll RPP (RESTful Provisioning Protocol) heissen.

- Es soll als moderne Ergänzung zu EPP dienen.
- Bei der IETF (Internet Engineering Task Force) befindet sich eine neue Arbeitsgruppe zu RPP im Aufbau.
- Ziel dieser Arbeitsgruppe ist die Spezifikation und Standardisierung von RPP.
- Switch verfolgt die aktuelle Entwicklung und bringt seine Expertise bezüglich EPP und REST ein.

Artikel über RPP bei DENIC

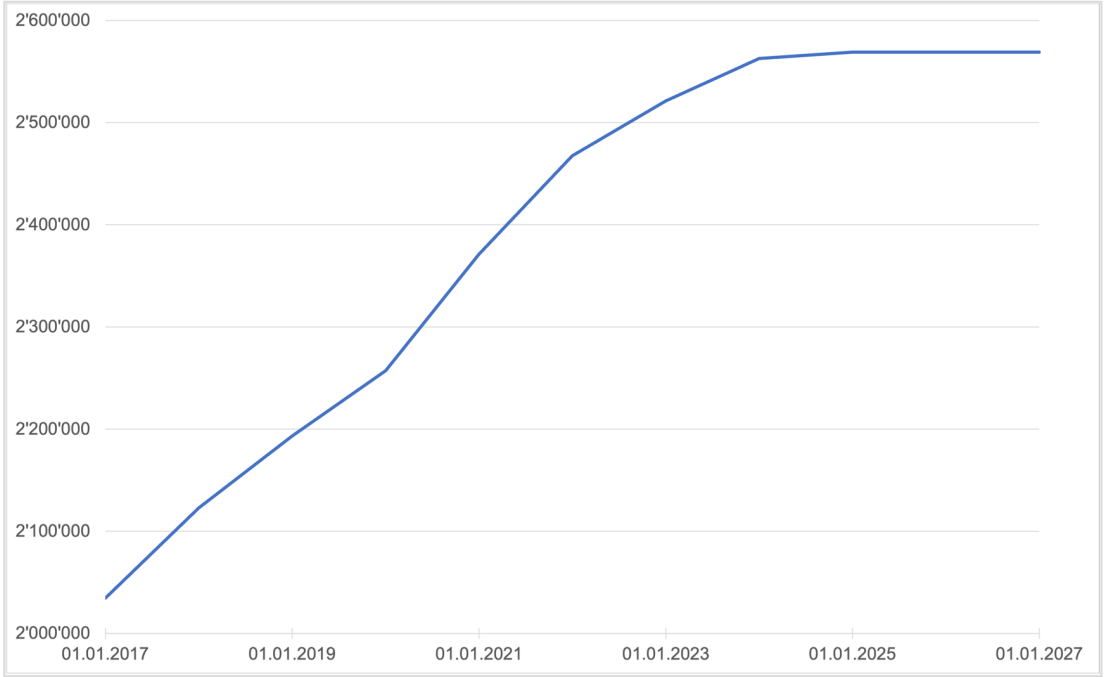
Wachstumsprognose .ch-Domain-Namen

Die Jahre 2018 und 2019 zeigten eine Zunahme, die von Jahr zu Jahr etwas tiefer ausfiel. Im Jahr 2020 führten der pandemiebedingte Digitalisierungsschub und die Marketing-Initiativen der Web-Hoster zu einer erhöhten Nachfrage und damit zu einem Wachstum von 4.8 Prozent. Die Zunahme verringerte sich bereits 2021 auf 3.9 Prozent, lag aber immer noch höher als vor der Pandemie.

Für 2022 verzeichnete die Registrierungsstelle noch ein Wachstum von 2.1 Prozent. Der Digitalisierungsschub dauerte also zwei Jahre und brachte einen unerwarteten Zuwachs von rund 100’000 Domain-Namen.

Im Jahr 2023 lag der Zuwachs bei gut 40’000 Domain-Namen. Dies entspricht 1.6 Prozent und erreicht unsere Prognose von 1.8 Prozent nicht.

Für 2024 hatten wir noch ein Wachstum von 6’000 Domain-Namen. Unsere Prognose für das Jahr 2025 geht von einem Null-Wachstum aus.



Switch
Werdstrasse 2
Postfach
CH-8021 Zürich

Telefon +41 44 268 15 15
www.switch.ch
info@switch.ch

Switch