Switch

Rechenschaftsbericht 2023

der .ch–Registerbetreiberin

Inhaltsverzeichnis

Wir setzen alles daran, die Zukunft unseres digitalen Ökosystems abzusichern.

Urs Eppenberger
Head of Registry, Switch

Switch

Volle Innovationskraft auf Cybercrime-Bekämpfung

Urs Eppenberger, Head of Registry

Kontinuierliche Bemühungen von Switch bei der Cybercrime-Bekämpfung haben zur Projektierung von «Domain Abuse 4.0» geführt. Das Ziel des Projekts: die Zukunft unseres digitalen Ökosystems abzusichern. Das Fundament unserer Cybercrime-Bekämpfung soll neu gestaltet werden. Die Prozesse werden optimiert und die gesamte technische Infrastruktur wird erneuert. Eine Beschreibung des Projekts findet sich auf Seite 23.

Während die Strafverfolgung in der Schweiz grundsätzlich Aufgabe der zuständigen Behörden ist, nimmt Switch eine Sonderstellung ein. Switch betreibt ein eigenes CERT (Computer Emergency Response Team) und bietet den Schweizer Hochschulen und der Wirtschaft moderne Sicherheitsdienstleistungen an. Durch die Zusammenarbeit mit anderen CERTs und die enge Kooperation mit Strafverfolgungsbehörden wird Switch zu einer agilen und handlungsfähigen Instanz, die in der Lage ist, eigenständig die Flut von Malware- und Phishing-Fällen sehr effizient und effektiv zu bewältigen. Das Bakom hat dies früh erkannt, die nötigen gesetzlichen Grundlagen geschaffen und den entsprechenden Auftrag im Vertrag mit Switch verankert.

Die Bekämpfung von Cybercrime bei Switch gleicht einer hochkomplexen Maschinerie. Es arbeiten Spezialistinnen und Spezialisten aus verschiedenen Fachbereichen zusammen, knüpfen Netzwerke mit anderen Akteuren in diesem Bereich und verbinden unterschiedliche IT-Komponenten miteinander.

Schweizer Nutzerinnen und Nutzer haben es so einfach wie nie zuvor: Sie sichern sich ihren Domain-Namen bei einem Registrar und betreiben ihre Website bei einem Hosting-Provider. Diese Dienstleistungen erhalten sie zu attraktiven Preisen. Es ist jedoch weitgehend unbekannt, welche Anstrengungen im Hintergrund erforderlich sind, um den sicheren und stabilen Betrieb des Internets als Ganzes sowie jedes einzelnen Domain-Namens zu gewährleisten. Dies erfordert eine eingespielte und etablierte Zusammenarbeit zwischen Hostern, Registraren, Switch und den Strafverfolgungsbehörden.

Wer im Bereich der Cybercrime-Bekämpfung tätig ist, weiss um die Bedeutung und Notwendigkeit dieser Arbeit. Deshalb haben wir bei Switch beschlossen, unsere Bemühungen noch zu verstärken. Die Registrierung und Verwaltung der Domain-Namen als Kernaufgabe der Registry ist so effizient organisiert, dass es möglich wird, die gesamte Innovationskraft auf die Bekämpfung von Cybercrime zu richten. Höchste Sicherheit und Stabilität für alle Nutzerinnen und Nutzer des Internets werden somit weiterhin gewährleistet.

1.
Tätigkeitsbericht – Betrieb

Switch

Bekämpfung Cyberkriminalität

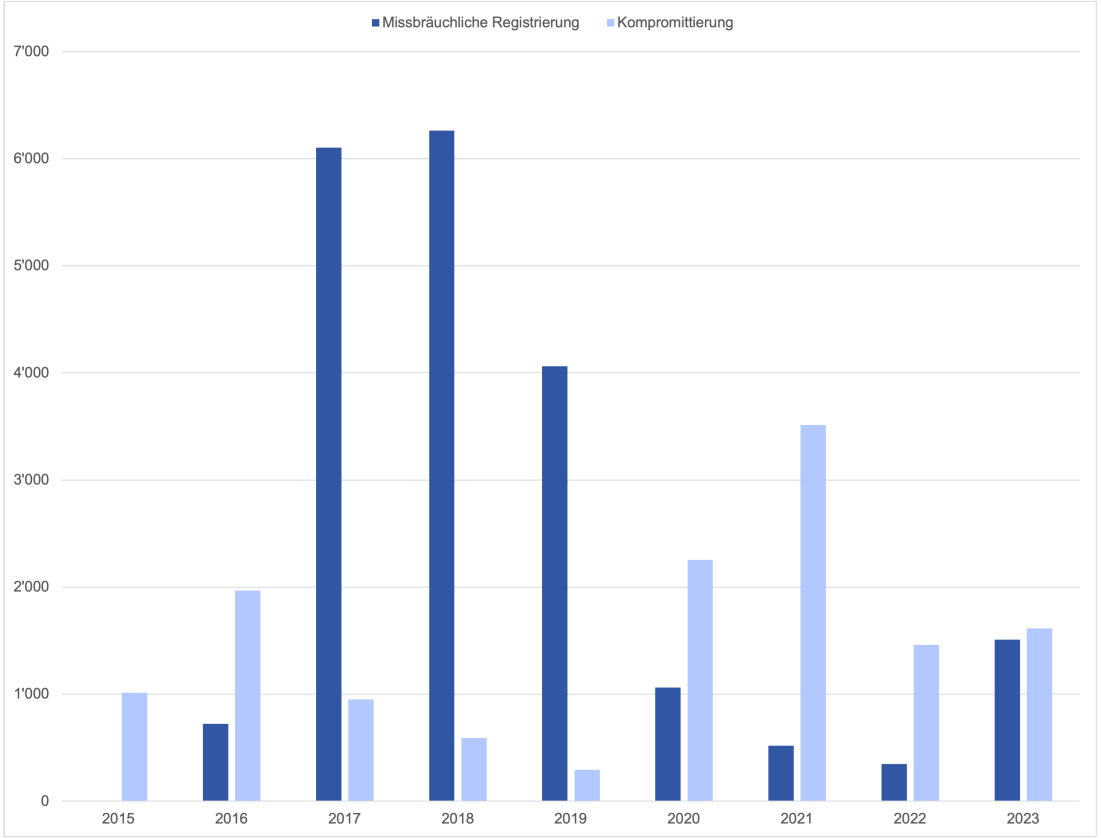
Kompromittierte Webseiten

Die Zahl der kompromittierten Webseiten, die für Phishing und Malware missbraucht wurden, blieb im Vergleich zum Vorjahr in etwa konstant.

Missbräuchliche Registrierung

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

Webseite: https://www.saferinternet.ch



Massnahmen bei Missbrauchsverdacht

Anträge anerkannter Behörden – VID Art. 15.1

Im Jahr 2023 haben die akkreditierten Behörden insgesamt 426 Anfragen gemäss VID Art. 15.1 zur sofortigen Blockierung (technisch/administrativ) von Domain-Namen betreffend Phishing oder Malware gesendet.

Anfragen	Konsequenz	2023
Nicht beantwortet	Domain-Name gelöscht	410
Beantwortet	Domain-Name reaktiviert	16
Total		**426**

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 1’084 Anfragen für eine Schweizer Korrespondenzadresse gemäss VID Art. 16.3 versendet.

Anfragen	Konsequenz	2023
Nicht beantwortet	Domain-Name gelöscht	964
Beantwortet	Domain-Name reaktiviert	120
Total		**1’084**

Security Awareness – iBarry und SISA

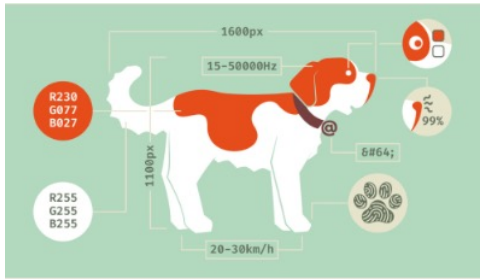
In Zusammenarbeit mit SISA unterstützt Switch die Sensibilisierung der Schweizer Bevölkerung. Mit drei neuen Informationskampagnen (Fake News, Datenschutz, VPN) informiert iBarry.ch und bietet gleichzeitig Orientierung und Unterstützung bei Unsicherheit und Fragen rund um die Internetsicherheit.

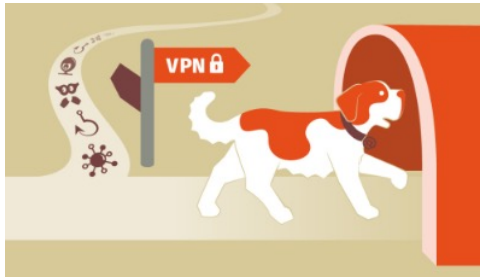
https://checkawebsite.ibarry.ch

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 Bevölkerungsbefragung der Schweizer Internet-Nutzenden mitgewirkt.

https://internet-sicherheit.ch





Security Awareness Day

Am 26. Oktober 2023 veranstaltete Switch zum sechsten Mal den Swiss Security Awareness Day. In diesem Jahr wurde die stetig wachsende Konferenz mit iBarry als Partner durchgeführt. Die rund 120 Teilnehmenden konnten sich zwischen den spannenden Vorträgen in diversen Networking-Pausen mit anderen Expertinnen und Experten vernetzen.

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: https://swit.ch/ssad2023-recordings

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 2023 hat Switch die spielerischen Security-Trainings insgesamt 40-mal durchgeführt und drei Organisationen dabei unterstützt, ihre eigenen aufzubauen.

Auch 12 Mitarbeitende des Bakom haben erfolgreich den Hacker gehackt.

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

Security Awareness – Podcast

Podcast: Security Awareness Insider

Im Dezember 2023 wurde die mittlerweile 38. Folge des Podcasts «Security Awareness Insider» (auf Deutsch) veröffentlicht.

Katja Dörlemann (Switch) und Marcus Beyer (Swisscom) sprechen 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 über 17'000-mal heruntergeladen, pro Folge sind es inzwischen durchschnittlich 400 Downloads.

Verfügbar auf Spotify oder hier:
https://www.securityawarenessinsider.ch

Community – Swiss Web Security Day

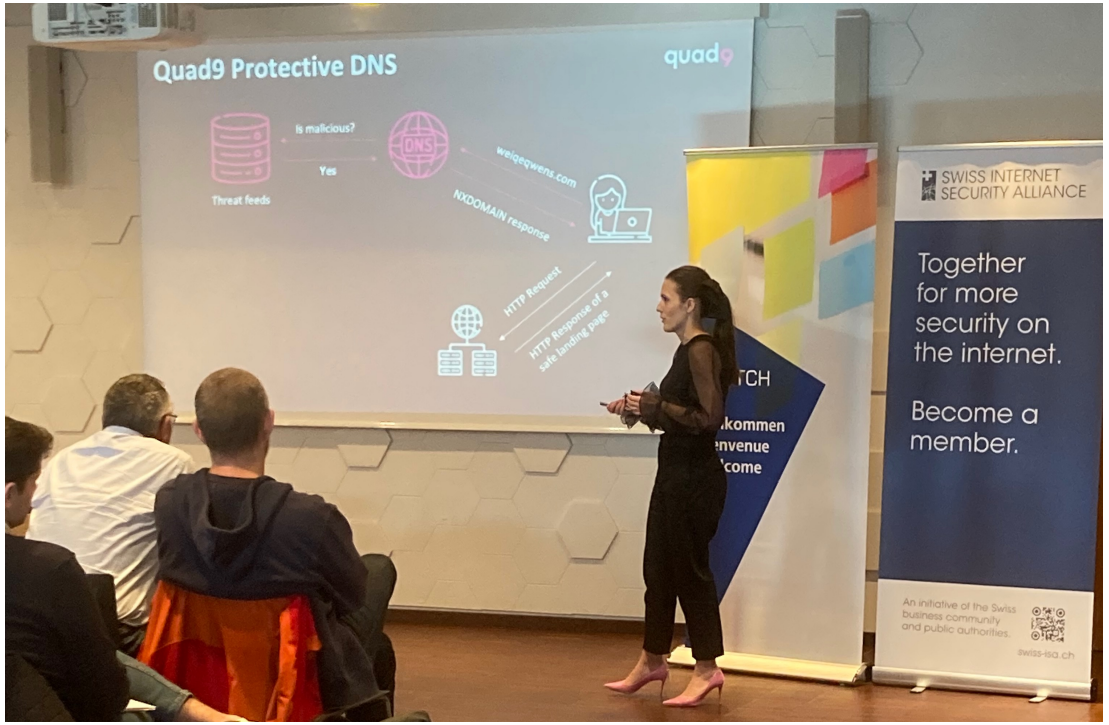
Am 17. Oktober 2023 hat Switch zusammen mit SISA und Swico den Swiss Web Security Day in Bern durchgeführt, parallel zum LEO-Event mit Schweizer Strafverfolgungsbehörden. Mit 73 Teilnehmenden aus der Schweiz und aus dem Ausland war der Anlass ein Erfolg, mit sehr positivem Echo der Teilnehmenden.

Am Vormittag gab es Vorträge zu Richtlinien für sichere Mail-Kommunikation, Medicrime, Schwachstellenmanagement in der Schweiz, Threats für Schweizer Internetnutzer sowie ein Update zur Revision der Verordnung über Internet-Domains (VID). Am Nachmittag war Zeit für Workshops und Gespräche in Kleingruppen, gefolgt von einem Apero.

Der Event fand diesmal nicht mehr hybrid, sondern vor Ort in Bern statt.

Webseite: https://swsd2023.events.switch.ch

Der Swiss Web Security Day wird auch im 2024 wieder stattfinden: 29. Oktober 2024, Welle 7, Bern.



Community – ModSecurity-Kurs

ModSecurity ist eine sehr populäre und mächtige Open Source Web Application Firewall. Web Application Firewalls sind wiederum ein wichtiger Baustein zum Schutz einer Web-Applikation und damit für Hoster, Registrare, aber auch generell für jeden Betreiber einer Web-Applikation interessant.

Um hier einen Mehrwert für unsere Community zu bieten, hat Switch zusammen mit dem weltweit renommierten ModSecurity-Experten Dr. Christian Folini von Netnea am 15. und 16. März 2023 einen Einstiegskurs bei Switch in Zürich veranstaltet. Switch nutzte hierbei ihre guten Beziehungen zur Community, um auf den Kurs aufmerksam zu machen, stellte die Räumlichkeiten zur Verfügung und war Sponsor von vergünstigten Tickets für Registrare und Switch-Kunden.

Schliesslich nahm eine bunte Mischung aus Registraren, Hostern und Mitarbeitenden von Hochschulen am Kurs in Zürich teil.

Im Jahr 2024 ist eine weitere Durchführung geplant.

LEO-Event
Zusammenarbeit mit Strafverfolgungsbehörden

Zielgruppe

Um die Zusammenarbeit mit den Behörden zu intensivieren, hat Switch in diesem Jahr zum dritten Mal den LEO-Event organisiert. LEO steht für «Law Enforcement Organizations».

Am 17. Oktober 2023 traf sich die Law Enforcement Community in Bern. Es waren 63 Personen am LEO-Event anwesend. Viele waren bereits im letzten Jahr dabei und brachten ihre interessierten Kollegen mit. Es lässt sich jedes Jahr ein Zuwachs feststellen.

Die Verteilung zwischen den Regionen war sehr ausgeglichen, so wurden Vorträge in den Landessprachen und Englisch gehalten. Die Teilnehmenden kamen von den Kantonspolizeien, den kantonalen Staatsanwaltschaften sowie der Landespolizei Liechtenstein. Auch Behörden wie Swissmedic, Seco und das Bakom waren vertreten.

Themen

Verschiedene Themen wurden besprochen. Schwerpunkt war die Zusammenarbeit in der Community um Cybercrime zu verhindern. So wurden verschiedene Fälle vorgestellt, welche durch die Zusammenarbeit der Partner der Community erfolgreich und effizient gelöst werden konnten.

Es wurde eine finnische Fallstudie vorgestellt, die Inspiration liefert, wie Fälle gelöst werden können, auch wenn sie zu Beginn sehr schwierig erscheinen. Die «Lessons Learned» zu den VID-Anfragen an Switch mit ihren möglichen Fallstricken wurden diskutiert und Teilnehmer des Bakom haben sich den Fragen der Community gestellt.

Resonanz

Der Event verlief sehr erfolgreich. Die Teilnehmenden sprachen über aktuelle Entwicklungen und Projekte im Bereich Domain-Abuse und Cybercrime. Prozesse und Schnittstellen, welche die Zusammenarbeit vereinfachen, wurden diskutiert. Der Austausch in der Zusammenarbeit hat deutlich zugenommen. Die Teilnehmenden wünschen sich eine weitere Veranstaltung im 2024.

Domain pulse 2023

Am diesjährigen Domain pulse trafen sich am 6. und 7. Februar 2023 Branchenfachleute hauptsächlich aus der Schweiz, Deutschland und Österrreich und diskutierten über die Sicherheit und Stabilität des Internets.

Rund 250 Teilnehmende von Registrierungsstellen, Registraren, Hostern, Bundesämtern sowie weitere Expertinnen und Experten folgten der Einladung nach Winterthur.

Unter dem Titel «Kritische Infrastruktur Internet: Hoheit wahren und vor Missbrauch schützen» diskutierten sie über aktuelle Herausforderungen der Internetbranche.

Im Zentrum stand die Frage, wie die Politik und Betreiberorganisationen von kritischen Infrastrukturen in Zeiten internationaler Konflikte die Hoheit über das Internet wahren, es vor Angriffen schützen und ausfallsicherer machen.

Der barocke Konferenzsaal war für viele Teilnehmenden eine Augenweide und die ausgiebige Zeit für Networking wurde sehr geschätzt.

Wir freuen uns darauf, im Jahr 2026 wieder Gastgeberland des Events Domain pulse zu sein.

DNS-Resilienzprogramm

50%

Per 1. Januar 2024 sind bereits fast 50 Prozent aller .ch-Domain-Namen signiert.

DNS-Resilienzprogramm

Widerstandsfähigkeit für .ch-Domain-Namen

Das DNS-Resilienzprogramm fördert die Einführung und Verwendung von offenen Sicherheitsstandards bei .ch- und .li-Domain-Namen. Der Einsatz solcher Standards ist entscheidend für die Widerstandsfähigkeit (Resilienz) gegen Cyber-Bedrohungen. Das Programm basiert auf einem System mit finanziellen Anreizen und läuft von 2022 bis 2026.

Das Hauptziel ist es, das Signieren von Domain-Namen mit DNSSEC zu fördern. Während der ganzen Dauer des Programms wird den Registraren für nicht oder nicht korrekt signierte Domain-Namen beim Preis ein Zuschlag verrechnet.

Das «DNSSEC Advisory Board» legt fest, welche Standards gefördert werden sollen. In diesem Gremium sind das Bakom, eine Vertretung der Registrare und Switch vertreten.

Für das Jahr 2024 werden zusätzlich die E-Mail-Sicherheitstechnologien DMARC und SPF ins Programm aufgenommen. Für die Rückvergütung der Mehreinnahmen ist dann nicht nur DNSSEC massgeblich, sondern auch die Implementation von sowohl DMARC als auch SPF.

Das Advisory Board hat bereits festgelegt, dass im Jahr 2025 DANE und im Jahr 2026 IPv6 zusätzlich zu DNSSEC gefördert werden sollen. Damit bleibt den Registraren ausreichend Zeit, die von Switch angebotenen Weiterbildungen zu besuchen und die technischen Massnahmen einzuplanen.

Messungen zur Qualitätskontrolle

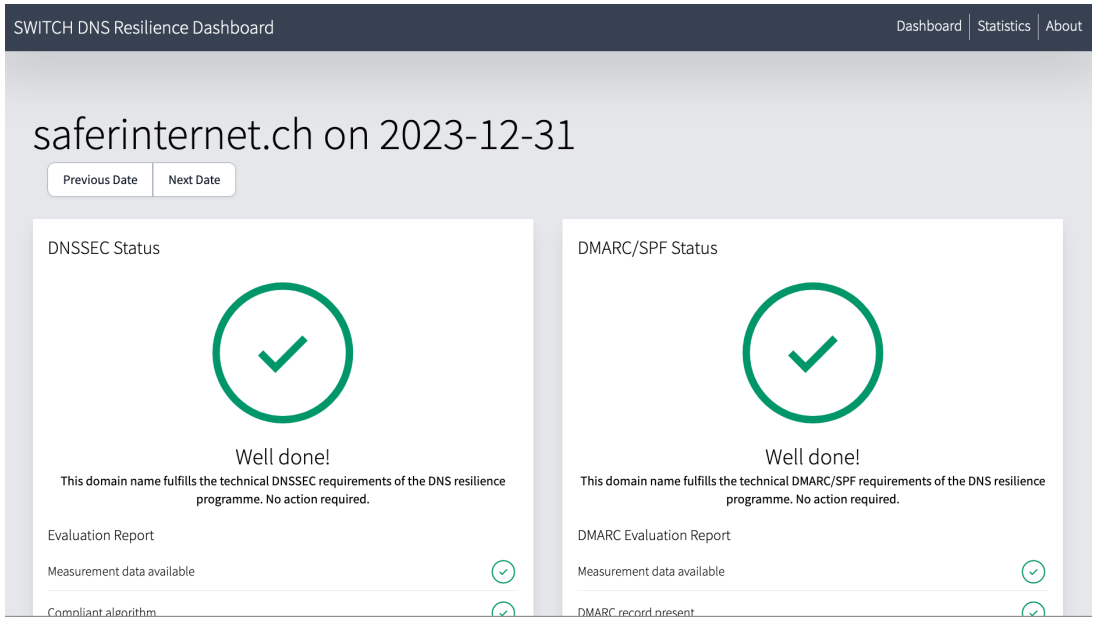
Wie bereits bei DNSSEC wird auch für die Messung der anderen Sicherheitstechnologien der externe Messdienstleister OpenIntel beigezogen. Sie überprüfen bei allen .ch- und .li-Domain-Namen mit Name-Servern, ob die von Switch für das Programm definierten Kriterien erfüllt sind und melden dies täglich an Switch. Bei fehlerhaften Konfigurationen erhalten die Registrare von uns sogenannte Error-Reports.

DNS-Resilienzprogramm

Auch in seinem zweiten Betriebsjahr haben wir uns neben dem Betrieb fortlaufend mit der Weiterentwicklung des Resilienzprogramms beschäftigt.

Entwicklungen 2023

- Rückvergütungen für 2022 an die berechtigten Registrare in Form von Gutschriften (Ende Januar 2023).
- Implementierung der Messungen von DMARC und SPF, die im 2024 relevant sein werden.
- Ab September 2023 Versand der neuen Error-Reports für DMARC/SPF an die Registrare. Obwohl das Kriterium erst im 2024 massgeblich sein wird, haben die Registrare so die Möglichkeit, sich darauf vorzubereiten.
- Erweiterung des Dashboards für DMARC/SPF beim externen Messdienstleister OpenIntel (siehe Sceenshot rechts).
- Fortlaufende Information der Registrare, Beantwortung ihrer Anfragen, Support.
- Zwei neue Reports, die dem interessierten Registrar ermöglichen die Beurteilung seiner Domain-Namen nachzuvollziehen.
- Trainings zu DNSSEC und DANE in Zürich und Lausanne im Oktober 2023.



DNS – Anycast-Standorte und Zonengenerierung

Anycast-Standorte

Unsere DNS Anycast Hosting-Partner haben im 2023 mehrere Standorte im In- und Ausland hinzugefügt, auf welchen die DNS-Zone über Anycast bereitgestellt wird. Beispielsweise gibt es seit Januar 2023 einen Point-of-Presence in Genf.

Zonengenerierung

Die Infrastruktur für die Zonengenerierung und -Verteilung wurde im 2023 rundum erneuert. Die «Hidden Primary Server», welche die Zone erstellen und die DNSSEC-Signaturen generieren, haben neue Hardware erhalten.

Wegen des mittlerweile hohen Anteils an DNSSEC-signierten Domain-Namen und geänderten Anforderungen aufgrund der Veröffentlichung der .CH-Zone im 2020 wurde ausserdem die Methode geändert, mit der die DNSSEC-Signaturen für nicht existierende Namen erstellt werden:
Bisher: «NSEC3 mit Opt-Out»
Neu: «NSEC»

ISMS Rezertifizierung

Vom 5. bis 7. September 2023 fand die Rezertifizierung des Informationssicherheits-Managementsystem ISMS nach ISO 27001:2013 statt.

Über drei Tage verschaffte sich der Auditor einen Einblick in alle Aspekte des ISMS bei Switch gemäss den Vorgaben für eine Rezertifizierung. Switch bestand den Audit erfolgreich ohne Abweichungen oder Feststellungen.

Der Auditor hielt sieben Empfehlungen fest, wie Switch das ISMS konkret verbessern kann. Diese Empfehlungen fliessen in den kontinuierlichen Verbesserungsprozess KVP des ISMS ein.

Im Bericht des Auditors ist der positive Gesamteindruck festgehalten, abgeschlossen mit folgender Bemerkung: «Es besteht ein grosses Commitment seitens der Geschäftsleitung und ein hohes Verständnis bezüglich Informationssicherheit bei allen interviewten Mitarbeitenden. Eine Stärke von Switch ist die kontinuierliche Verbesserung und die hohen Fachkenntnisse der Mitarbeitenden auf allen Stufen.»

SV Cert.

IAF

SNAS
Reg. No. 661/R-141

ZERTIFIKAT

Nr. 860-ISMS-23

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 1.4 vom 14.10.2021	05/12/2017	09/10/2023	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: Jégého 220/19, Bratislava
Mestská Cast Ružinov 821 08 – SLOVAKIA
Info & Contact: svcertification.com – info@svgroupcert.ch

«Eine Stärke von Switch ist die kontinuierliche Verbesserung und die hohen Fachkenntnisse der Mitarbeitenden auf allen Stufen.»

ISO 27001 Audit-Bericht

2.
Tätigkeitsbericht – Neuheiten

Switch

Domain Abuse 4.0

Steigende Anforderungen

Mit einem schlagkräftigen Experten-Team und der Unterstützung durch selbstentwickelte Softwarelösungen bekämpft Switch seit Jahren den Domain-Namen-Missbrauch im Schweizer Internet. Die Cyberkriminellen werden immer gerissener und damit steigen die Anforderungen an die Experten sowie an die Softwarelösungen.

Herausforderung der heutigen Softwarelösung

Die Codebasis der heutigen Softwarelösung zur Bekämpfung von Cyberkriminalität geht zurück bis ins Jahr 2008. Die Lösung basiert auf einer veralteten IT-Architektur. Sie ist langsam, aufwendig in der Wartung und den stetig zunehmenden Herausforderungen in der Missbrauchsbekämpfung von Domain-Namen nicht mehr gewachsen.

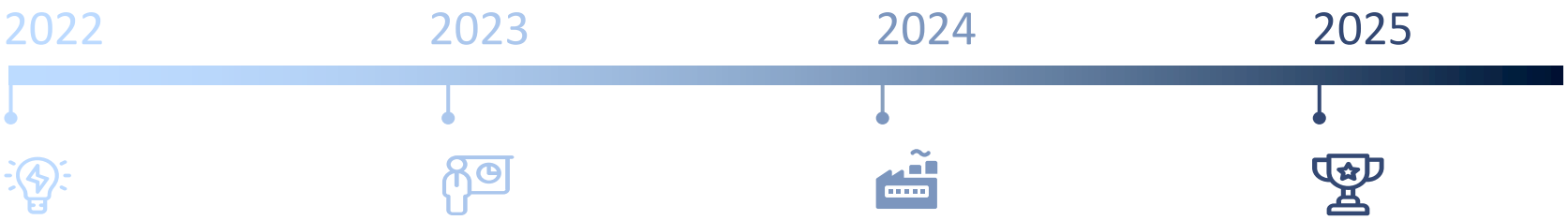
Moderne und zukunftsträchtige Missbrauchsbekämpfung

Im Rahmen des Projektes «Domain Abuse 4.0» wird eine neue zukunftsweisende Softwarelösung entwickelt. Sie basiert auf modernsten Technologien und der neusten Switch-Infrastruktur «Switch Cloud». Das Entwicklungsteam der Registry und das Entwicklungsteam des CERT bündeln ihre Erfahrungen und Fertigkeiten, um eine schnelle, wartungsarme und hochskalierbare Lösung zu entwickeln. 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.

Domain Abuse 4.0

Zahlen und Fakten

- 20 Workflows (Prozesse gegen Missbrauch) wurden anhand der VID definiert.
- 14 Software-Komponenten müssen neu oder weiterentwickelt werden.
- 50+ User Stories wurden geschrieben (noch nicht abschliessend).
- 16 Lösungsvarianten wurden evaluiert.
- 12 Personen in verschiedenen Positionen arbeiteten bisher am Projekt.



Start
Im Oktober 2022 begann das Projekt mit der Definition der Workflows und der IT-Architektur

Evaluation
Aus 16 Lösungs-varianten wurde eine Eigenentwicklung als zukunftsweisendste Lösung ausgewählt

Entwicklung
Die Softwarelösung wird iterativ mit regelmässigen Releases entwickelt

Betrieb
Bis Ende 2025 soll die neue Lösung implementiert sein

Gründung des European TLD ISAC

Unter dem Dach von CENTR wurde im 2023 das Europäische TLD Information Sharing and Analysis Centr (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.

Die erste TLD ISAC Konferenz fand am 13. November 2023 in Brüssel statt, Switch war mit zwei Teilnehmern vertreten.

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

EUROPEAN TLD ISAC

Web-Crawler

Im Rahmen der Bekämpfung von Cyberkriminalität wurde gegen Ende des Jahres 2023 bei Switch ein neues Tool entwickelt: ein Web-Crawler, der öffentlich zugängliche Ressourcen in der .ch- und .li-Zone systematisch untersucht, um kompromittierte oder böswillige Domain-Namen frühzeitig zu entdecken und damit die Gefahr für Internetnutzende zu bannen.

Damit wir immer auf dem neuesten Stand sind und wirksame Arbeit leisten können, aktualisiert unser Cyber Threat Intelligence Team regelmässig die Kriterien, die uns bei der Erkennung der Gefahren helfen. Ebenso tauschen wir uns rege mit Behörden und anderen Registries aus.

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.

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.

Neues Datenschutzgesetz

Am 1. September 2023 trat das neue Datenschutzgesetz der Schweiz in Kraft. Switch hat frühzeitig mit der Umsetzung der neuen gesetzlichen Vorgaben begonnen.

Datenschutzberater

Switch hat am 1. März 2023 einen neuen Datenschutzberater ernannt und dies dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet. Angelo Marchetta übt diese Funktion für Switch aus und berät und unterstützt Switch bei der Anwendung der Datenschutzvorschriften und der Schulung der Mitarbeitenden. Zu seinen Aufgaben gehören auch die Überwachung und Koordination aller relevanten Datenschutzaktivitäten im Unternehmen. Darüber hinaus ist er mit dem Aufbau eines Datenschutzmanagementsystems (DSMS) betraut.

Bearbeitungsverzeichnisse

Die Einführung der Bestimmung zur Führung eines Bearbeitungsverzeichnisses ersetzte die bisherige Meldepflicht von Datensammlungen. Switch hat ihre Datenbearbeitungsaktivitäten als Registerbetreiberin einerseits im internen Bearbeitungsverzeichnis erfasst, andererseits im öffentlich zugänglichen Register, dem DataReg, registriert.

Datensicherheit

Im Rahmen des neuen Datenschutzgesetzes hat Switch Anpassungen im Meldungsprozess von Datensicherheitsverletzungen implementiert. Dies ermöglicht eine rasche Meldung von Vorfällen, welche voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person darstellen.

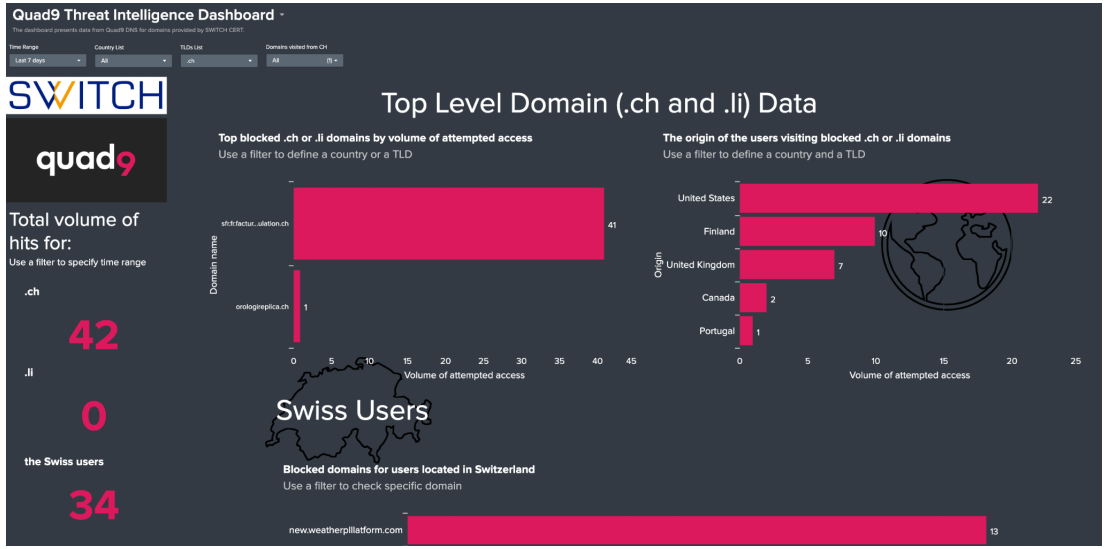
DSMS

Nicht erst seit der Umsetzung des neuen Datenschutzgesetzes legt Switch hohen Wert auf den Schutz von Personendaten. Zusätzlich zum Informationssicherheits-Managementsystem ISMS entwickelt Switch über die nächsten Jahre ein Managementsystem für Datenschutz, um die systematische Gewährleistung und kontinuierliche Verbesserung des Datenschutzes sicherzustellen.

Quad9: die Rolle von Threat Intelligence

Quad9 und Switch arbeiten zusammen bei der Analyse von Bedrohungen für das Schweizer Internet. 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: Q9 Cyber Insights Report, Malawi Report
- Akquirieren neuer Threat-Intelligence-Partnerschaften für Quad9. Beispiele: Phish Report, SISA
- Vorträge zu Themen im Zusammenhang mit Bedrohungsdaten, Quad9 und Datenschutz. Vorträge: Swiss Web Security Day, M3AAWG, Women in Cyber
- 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. Die Erkenntnisse wurden für den Switch Threat Radar verwendet und am Swiss Web Security Day präsentiert.



Top-Bedrohungen für das Schweizer Web

Aufgrund der von Quad9 erhobenen Daten waren 2023 folgende Kampagnen in Gang und eine Gefahr für Schweizer Internetnutzende:

Fake jQuery Domain

Die Infektion wird in legitime Javascript-Dateien injiziert und führt ein Skript von der bösartigen Domain jqueryns[.]com aus. Diese leitet auf diverse Betrugsseiten weiter. Befallen wurden hier vor allem verwundbare WordPress-Webseiten. Mehr als 8000 DNS-Anfragen wurden von Quad9 in der Schweiz blockiert und 47 .ch-Domain-Namen waren betroffen.

WordPress SocGholish Injections

SocGholish ist eine weit verbreitete, mehrjährige Malware-Kampagne, die darauf abzielt, gefälschte Browser-Updates zu verteilen, auch an Schweizer Internetnutzende. Einmal installiert, infizieren die gefälschten Browser-Updates den Computer des Opfers mit verschiedenen Arten von Malware, darunter auch Remote-Access-Trojaner (RATs). In einem Monat wurden von Quad9 ca. 1700 DNS-Anfragen aus der Schweiz blockiert.

Phishing gegen die Schweizerische Post

Die Phishingseite gegen die Schweizerische Post war unter campaign-image[.]eu gehostet. Die Kampagne war zwischen dem 20. und 26. April aktiv. In der Schweiz wurden im April in einer Woche mehr als 870 Abfragen durch Quad9 blockiert. Weltweit wurden mehr als 24'900 Abfragen durch Quad9 blockiert.

Malware «ndsw/ndsx»

Hierbei handelt es sich um eine weitere Variante der SocGholish-Malware. Alle Malware-Varianten enthalten die Anweisung «if(ndsw===undefined)», daher der Name. Das Ziel ist die Installation der sogenannten «Fake Update» Malware auf Windows-Computern. 92 .ch-Domain-Namen waren betroffen.

Black Hat Ad Network und Balada Injector

Dies ist eine massive Kampagne, die gehackte WordPress-Webseiten als Inventarplattform für Anzeigenplatzierungen und Weiterleitungen nutzt. Die infizierten Webseiten leiten zu gefälschten Browser-Updates und Support-Betrug weiter. 37 .ch-Domain-Namen waren betroffen.

Neuer Standort in Lausanne

Am 2. Mai 2023 hat Switch neue Räumlichkeiten in der Westschweiz bezogen. Im EPFL Innovation Park übernimmt die Stiftung Büros für bis zu 15 Mitarbeitende. Den primären Treiber für diesen Schritt erklärt Tom Kleiber, Geschäftsführer von Switch, wie folgt: «Um unsere nationale Rolle im Hochschulsektor besser und glaubwürdiger wahrnehmen zu können, benötigen wir einen Standort in der Westschweiz. Die Nähe zur Community und der direkte Austausch mit ihr sind uns sehr wichtig.»

In seiner Ansprache an der Eröffnungsfeier äusserte sich Martin Vetterli, Präsident der EPFL, positiv zum neuen Standort: «Die Hochschulen in der Westschweiz freuen sich auf die verstärkte Zusammenarbeit mit Switch.»

Auch die Registrierungsstelle ist damit näher bei denjenigen Registraren, die in der Westschweiz ihren Schwerpunkt haben. Zudem bietet der neue Standort in der Westschweiz lokalen Talenten die Chance, sich in der Region für sinnstiftende Aufgaben wie die nachhaltige Nutzung von Forschungsdaten, Cybersicherheit oder digitale Identitäten einzusetzen.

Martin Vetterli, EPFL; Tom Kleiber, Switch; Claudia Lienert, Switch; Alexandre Gachet, Stiftungsrat Switch

IPv6 Evangelist

Switch setzt sich seit 1996 für die Einführung des IPv6-Standards ein, den wir als essenziell für die nachhaltige Entwicklung des Internets ansehen. Neben der Implementierung im Hochschulnetz und bei der Registry haben wir auch diesbezügliche Aktivitäten der Schweizer Internet-Community unterstützt. Dies in Form von Veranstaltungen wie Konferenzen und Kursen, Standardisierungsarbeiten in der Internet Engineering Task Force (IETF) und durch Beratung politischer Gremien.

Damit konnten wir unseren Teil dazu beitragen, dass die Schweiz seit vielen Jahren zu den Ländern gehört, in denen IPv6 gut etabliert ist und sich stetig weiter verbreitet.

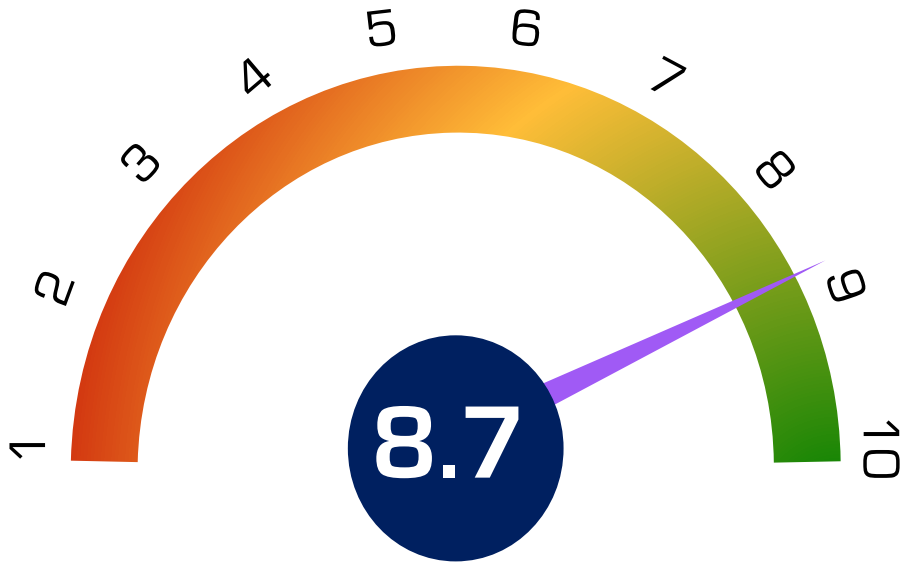
Diese Anstrengungen wurden 2023 vom internationalen IPv6 Forum gewürdigt, indem Simon Leinen, langjähriger Switch-Mitarbeiter, als «IPv6 Evangelist» in die IPv6 Hall of Fame aufgenommen wurde. Aktuell gibt es weltweit nur um die 100 «IPv6 Evangelists».

Kundenumfrage Registrare

Im November/Dezember 2023 führte Switch bei allen Registraren eine Kundenzufriedenheitsumfrage durch. 30 von 156 Registraren nahmen an der Befragung teil. Die Ergebnisse sind daher als indikativ zu bewerten.

Das Wichtigste in Kürze

- Switch geniesst bei den Registraren einen Ruf, der von höchster Vertrauenswürdigkeit, Sicherheit, Stabilität, Sympathie, Qualitätsbewusstsein und Kompetenz geprägt ist.
- Im Vergleich zu allen grossen Registries weltweit erbringt Switch nach Ansicht der Befragungsteilnehmenden die mit Abstand beste Gesamtleistung.
- Der Gesamteindruck, den die Registrare von Switch haben, ist mit 8.7 von maximal 10 Punkten auf einem sehr hohen Niveau.



Gesamteindruck von Switch
Fragestellung: Wenn Sie alles in Betracht ziehen, was Sie über Switch als Registry wissen, welchen Gesamteindruck haben Sie dann von Switch?
Skala: 1 = ausgesprochen negativ; 10 = ausgesprochen positiv

3.

Tätigkeitsbericht – Statistische Kennzahlen

Switch

50%

Das DNS-Resilienzprogramm gab DNSSEC den gewünschten Durchbruch. Mittlerweile sind fast 50 Prozent der Domain-Namen signiert.

1.6%

Wachstum der .ch-Domain

40'000

Zuwachs von rund 40'000 Domain-Namen.

Domain-Namen-Bestand – Entwicklung 2023

Entwicklung .ch

Innerhalb eines Jahres hat sich der Bestand von .ch-Domain-Namen um gut 40’000 vergrössert. Dies entspricht einer Zunahme von 1.6 Prozent gegenüber dem Vorjahr.

	2022	2023
Neuregistrierungen	281’610	294’195
Löschungen	258’724	282’649
Reaktivierungen*	31’097	29’958
Domain-Bestand per 31.12.	**2’521’444**	**2’562’914**

Entwicklung .li

Innerhalb eines Jahres hat sich der Bestand von .li-Domain-Namen kaum verändert.

	2022	2023
Neuregistrierungen	10’094	10’658
Löschungen	10’178	12’218
Reaktivierungen*	1’823	1’699
Domain-Bestand per 31.12.	**70’478**	**70’607**

Entwicklung des Domain-Namen-Bestandes bei .ch und .li
* Gelöschte Domain-Namen, die vom Registrar innerhalb der Übergangsfrist von 40 Tagen wieder reaktiviert wurden.

Auskunftsdienst – Statistik 2023

Auskunftsdienst

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 blieben im Vergleich zum Vorjahr im selben Rahmen.

	Privat	Behörden
Auskunft erteilt	304	135
Auskunft nicht erteilt	56	5
Generelle Anfragen *	4	0
Total Anfragen	**364**	**140**

* 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 2023 stark zugenommen, was auch auf unsere bessere Vernetzung mit den Strafverfolgungsbehörden zurückzuführen ist. Per Ende 2022 nutzten erst 5 Behörden RDAP, Ende 2023 waren es schon 18 Behörden. Den grössten Anteil machen die Kantonspolizeien aus.

	Anfragen
Auskunft erteilt	3’612
Auskunft nicht erteilt	309
Total Anfragen	3’921

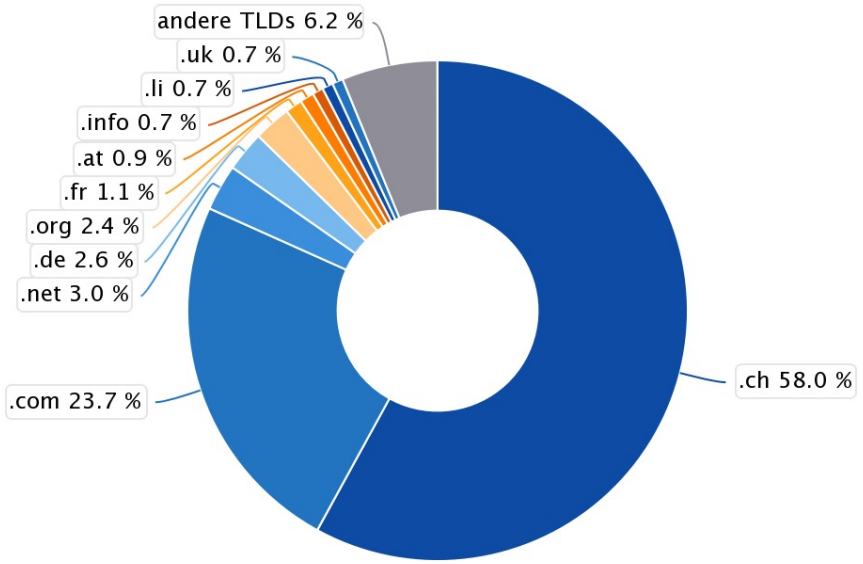
Marktanteil von .ch und .li bei Schweizer Halterinnen und Haltern von Domain-Namen

Der Marktanteil der TLD (Top-Level Domain) **.ch** bei Halterinnen und Haltern aus der Schweiz blieb vom Oktober 2022 bis Oktober 2023 praktisch unverändert.

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

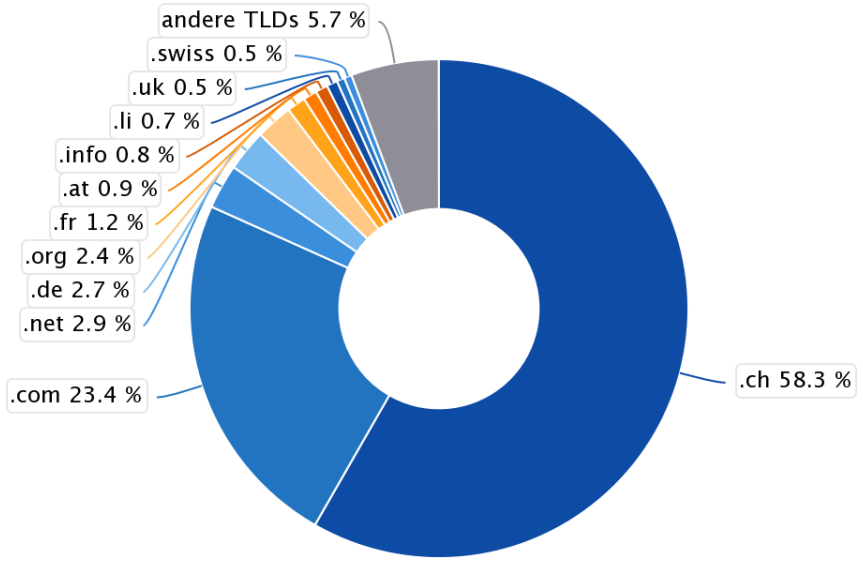
Oktober 2022

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



Oktober 2023

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



DNS-Resilienzprogramm – Entwicklung in Zahlen

DNSSEC

- DNSSEC bei .ch-Domain-Namen, Stand 1. Januar 2024: 49,1% (1. Januar 2023: 44.8%).
- Fehlerquote: Die Fehlerquote ist übers Jahr mehr oder weniger konstant auf sehr tiefem Niveau geblieben. Weniger als 0.25 Prozent aller DNSSEC-Domain-Namen wiesen Fehler auf (2022: weniger als 0.5%).

DMARC und SPF

- 1. Juli 2023 (Beginn der Messungen bei OpenIntel): 2.6% korrekt konfiguriert.
- 1. Januar 2024: 4.5% korrekt konfiguriert. Zahlen für .ch- und .li-Domain-Namen, korrekte Konfiguration sowohl von DMARC als auch von SPF. Angaben gemäss Statistik des externen Messdienstleisters.

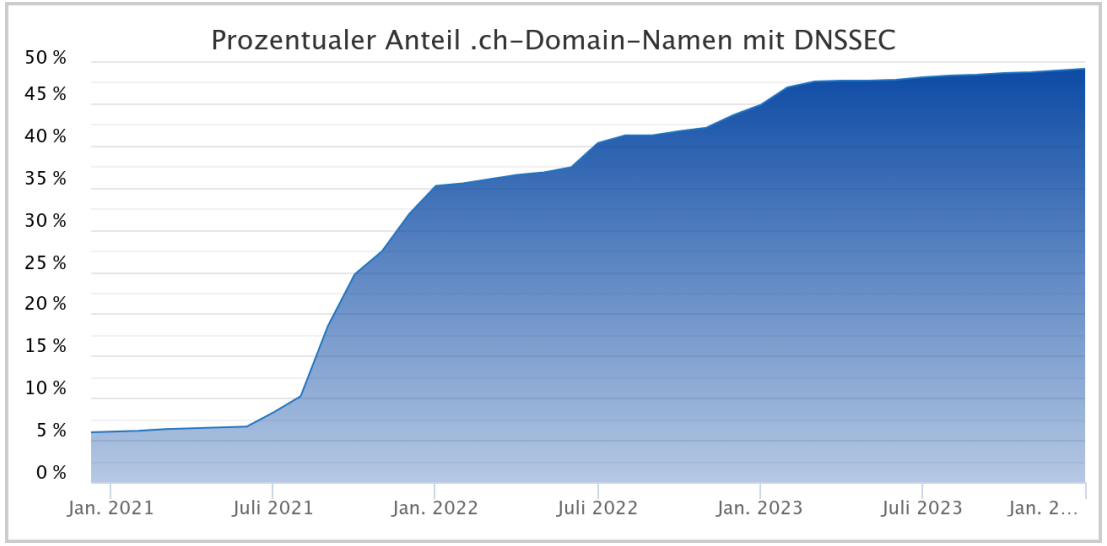
Statistik DNSSEC bei Switch

Statistik bei OpenIntel

Berechnung der Rückvergütung für das Jahr 2023

- Gesammelte Mehreinnahmen aus Preisdifferenzierung: CHF 1'792'697
- Abzüglich fixe Kompensation für Switch und den externen Messdienstleister 2023: CHF – 444'907
- Total Rückvergütung CHF 1'347'790

Die Rückvergütungen erfolgen Ende Februar 2024.



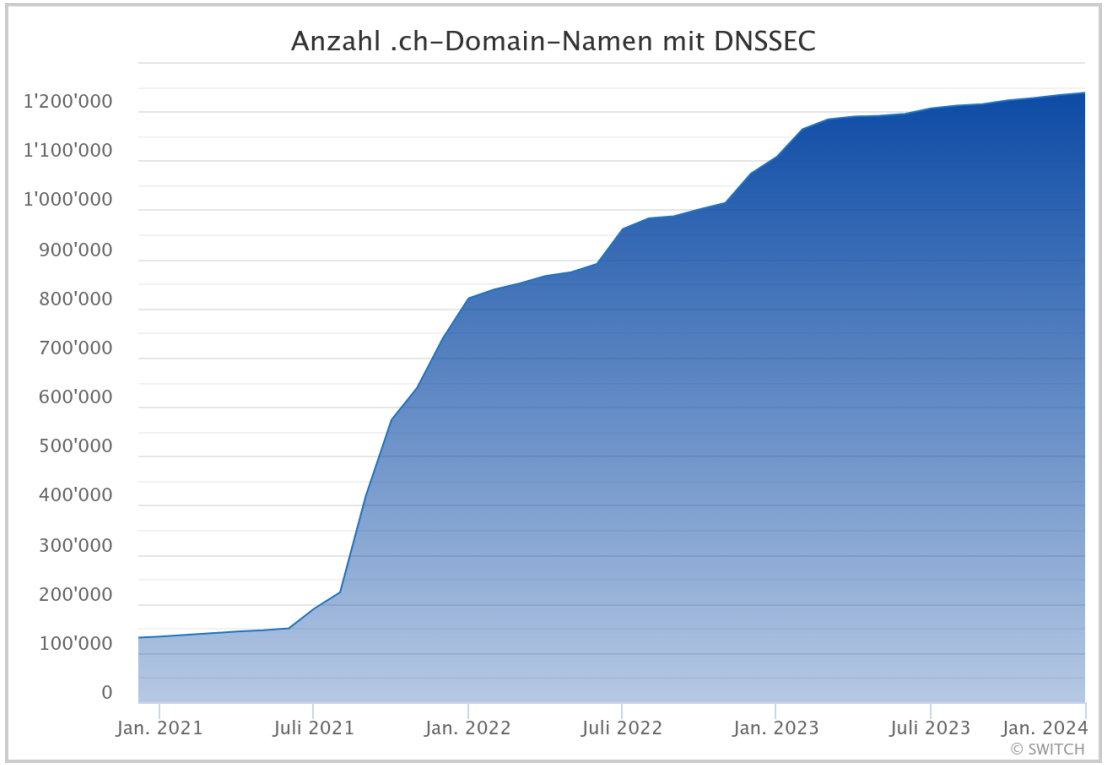
Entwicklung DNSSEC
Anzahl signierter Domain-Namen

Ende 2023 sind über 1.2 Millionen .ch-Domain-Namen mit DNSSEC signiert.

Dies entspricht einem Anteil von fast 50 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. Im Jahr 2023 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 mit einem stark verlangsamten Zuwachs zu rechnen.

Anzahl .ch-Domain-Namen mit DNSSEC

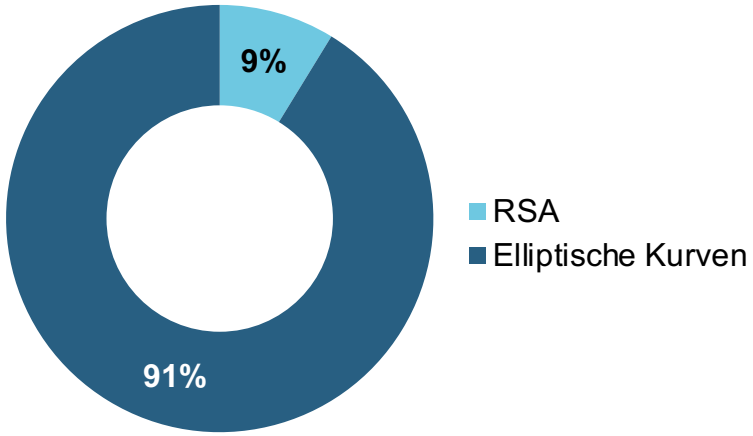


1’237'670 mit DNSSEC signierte .ch Domain-Namen am 1. Januar 2024

Entwicklung DNSSEC
Verteilung DS-Algorithmen

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

DS Records mit Algorithmen 5 und 7, die aufgrund ihrer SHA-1-Signatur nicht mehr als sicher gelten, werden seit Februar 2023 nicht mehr unterstützt und wurden entsprechend aus der Zone entfernt.



Verwendete DNSSEC-Signaturen

DNSSEC-Algorithmus	Anzahl	Anteil
5 – RSASHA1	0	0.00 %
7 – RSASHA1-NSEC3-SHA1	0	0.00 %
8 – RSASHA256	111’923	9.04 %
10 – RSASHA512	59	0.00 %
13 – ECDSAP256SHA256	1’225’464	90.93 %
14 – ECDSAP384SHA384	142	0.01 %
15 – ED25519	42	0.00 %
16 – ED448	90	0.00 %

DNSSEC-Validierung in der Schweiz

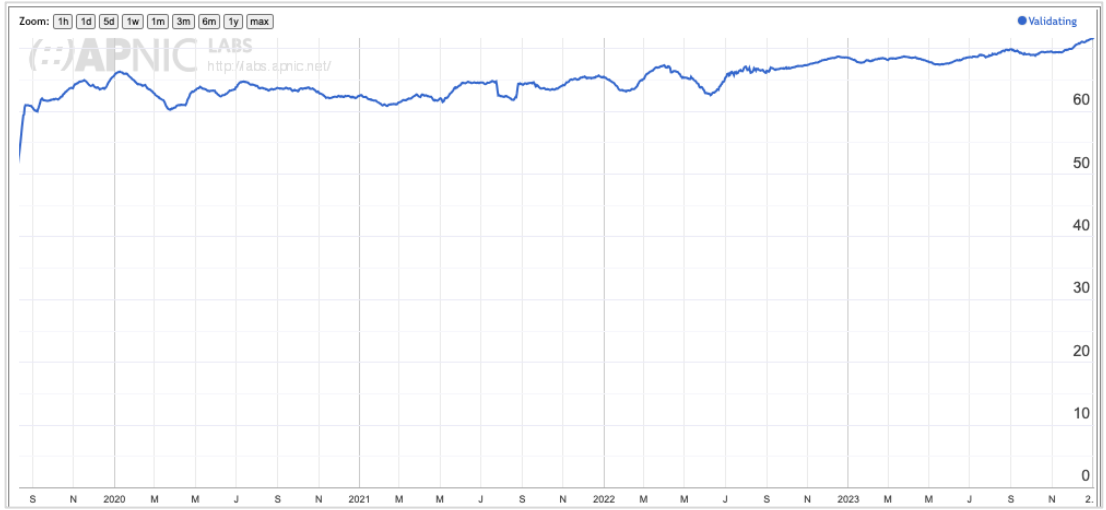
DNSSEC-Validierung

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

Nach Messungen von APNIC ist die DNSSEC-Validierungsrate auf den Resolvern der Schweizer ISPs im letzten Jahr erstmals auf über 70% angestiegen.

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

DNSSEC-Validierung auf Schweizer Resolvern



Deferred Delegation – Status

Gesetzliche Grundlage

Das Bakom hat mit dem Artikel 25 der VID, «Allgemeine Zuteilungsvoraussetzungen», die gesetzliche Grundlage geschaffen, die es der Registry ermöglicht, bei einem Verdacht auf unrechtmässige Nutzung oder Zweck eines Domain-Namens diesen vorerst nicht zu aktivieren und die Name-Server nicht ins Zonenfile einzutragen. Dieser Prozess wird als «Deferred Delegation» (aufgeschobene Delegation) bezeichnet.

Prozess-Anpassungen

Durch die Verschärfung der Regeln konnten wir im 2023 erheblich mehr Registrationen zurückhalten und auch löschen.

Nach der Überführung in den produktiven Betrieb überarbeiten wir die Kriterien auch weiterhin regelmässig. Darüber hinaus werden neue Kriterien und Überprüfungsmethoden erforscht, um missbräuchliche Registrationen noch besser zu erkennen. Letzteres immer im Hinblick auf berechtigte Nutzer, welche nicht behindert werden sollen.

Zur weiteren Verbesserung und zum Austausch von Erfahrungen sind wir mit anderen Registries in Kontakt.

Wir haben ein Dashboard entwickelt, mit welchem wir jederzeit einen Überblick über die aktuellen Metriken des Prozesses erhalten. Durch Datenanalyse werden die Kriterien regelmässig überarbeitet und nachgeschärft. Deferred Delegation soll möglichst nur auf missbräuchliche Nutzung zielen, berechtigte Nutzer sollen nicht behindert werden.

Kennzahlen Deferred Delegation 2023

Neuregistrierungen insgesamt	294’195
Domain-Namen deferred	2’751
Domain-Namen gelöscht	1'956

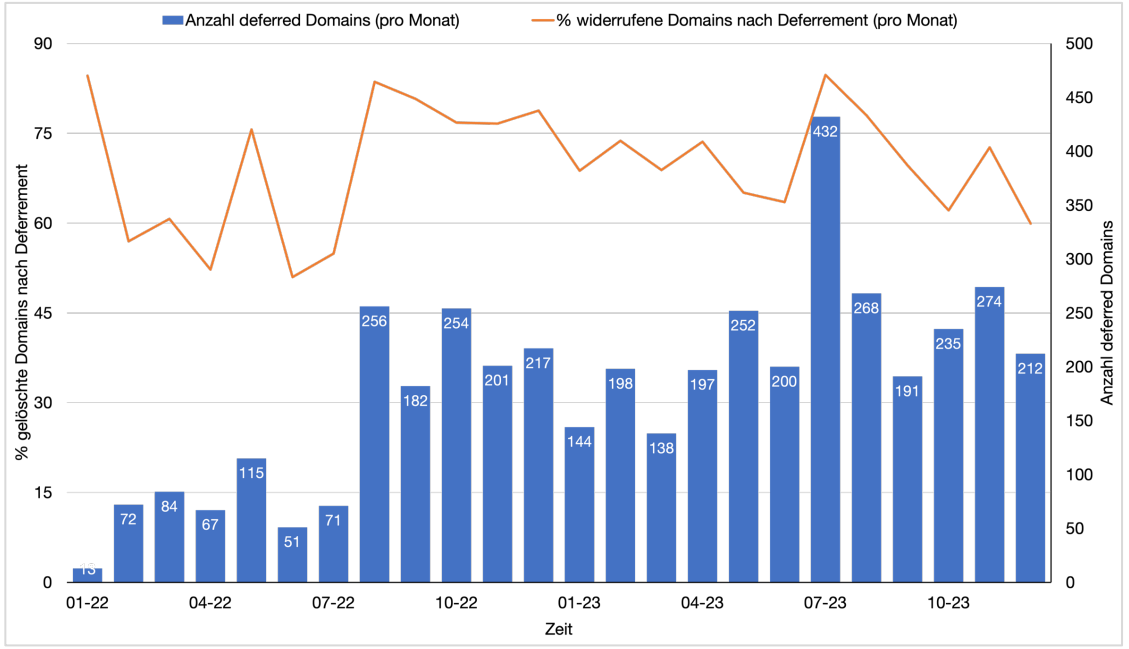
Deferred Delegation – Status

Deferred Delegation im zeitlichen Rückblick

Seit der Einführung von Deferred Delegation Anfang 2022 haben wir die Anzahl der «deferred» Domain-Namen langsam gesteigert (blaue Balken).

Dies wurde mit einer zunehmenden Verschärfung der Kriterien erreicht. Durch eine sorgfältige Auswahl dieser Kriterien konnte gleichzeitig der Anteil von Domain-Namen, die nach ausbleibender Identifikation des Halters widerrufen wurden, stabil gehalten werden (orange Kurve).

Auffallend ist eine hohe Anzahl «deferred» Domain-Namen im Juli 2023. Ein Teil davon ist auf einen Halter zurückzuführen, der eine grosse Anzahl an Domain-Namen registriert hatte, aber keine Identifikation nachlieferte.



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 2023 haben die Experten für 16 .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	**2022**	**2023**
Auf Gesuchsteller übertragen	15	11
Klage abgewiesen	2	5
Anzahl Entscheide	**17**	**16**

Entscheide der WIPO (Stand Februar 2024)

	Domain-Namen
Auf Gesuchsteller übertragen	diadora.ch immoswisslife.ch albi-keramik.ch albikeramik.ch migrosbankswitzerland.ch naturoflooring.ch dallmayer.ch tmhinternational.ch solidea.ch nortonabrasives.ch dermagora.ch
Klage abgewiesen	rockantenne.ch cheeze.ch schluessel-luzern.ch imageskincare.ch zoskinhealth.ch

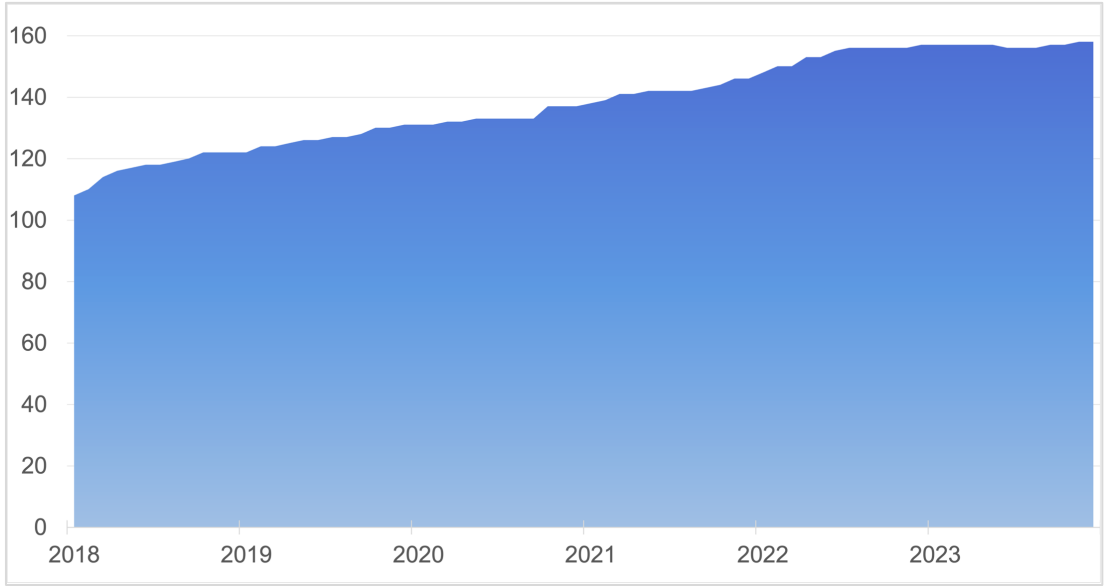
Entwicklung Registrare

Im Jahr 2018 kamen erheblich mehr Registrare als erwartet hinzu, so dass wir per Ende des Jahres 122 Registrare verzeichneten.

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.



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.

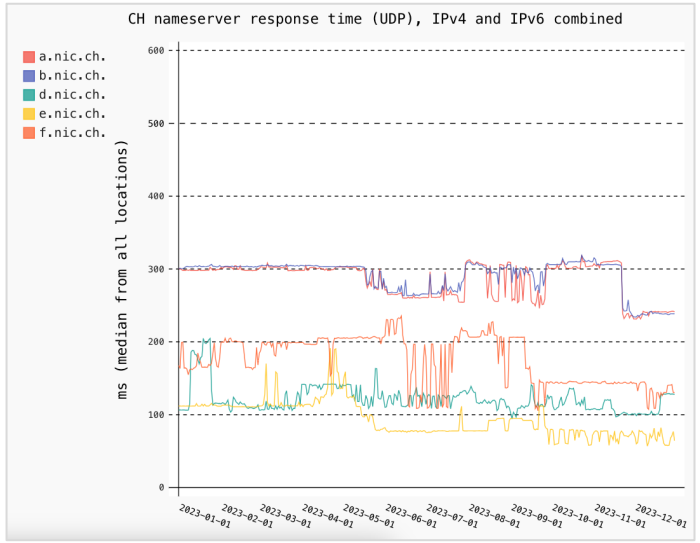
Diese Anforderung wurde 2023 jederzeit erfüllt.

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

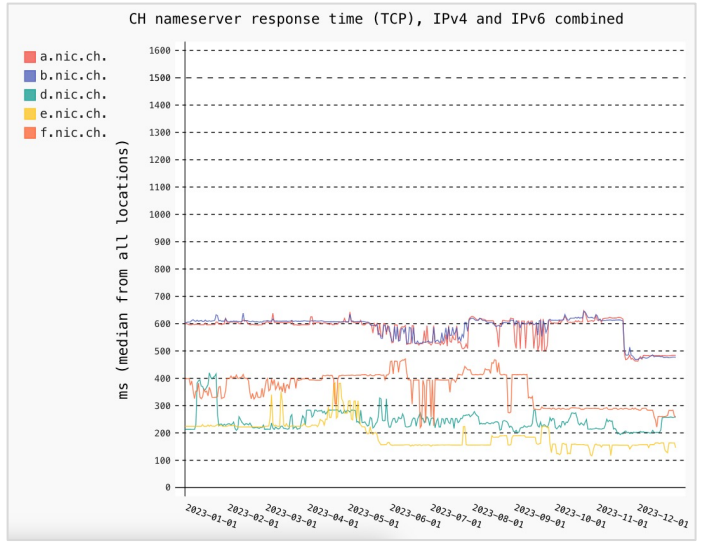
Unicast: a.nic.ch (CH), b.nic.ch (CH),

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

Quantitativ

Im Berichtsjahr wurden folgende Fälle erfasst und behandelt:

Anzahl Malware- und Phishing-Fälle 2023 quantitative Betrachtung

	# Malware-Fälle	# Phishing-Fälle
Eingegangene Meldungen	**1’242**	**942**
Verdacht bestätigt	**505**	**643**
Anzahl blockierte Domain-Namen	**187**	**475**
Begründung für die Aufhebung der Blockierung: - Gesetzliche Dauer ist überschritten - Behoben nach Blockierung - In Bearbeitung am Stichtag	 **37** **119** **4**	 **17** **34** **12**
Widerrufene Domain-Namen	**27**	**419**

Qualitativ

Für die Fälle wurde folgende Zeit aufgewendet:

Anzahl Malware- und Phishing-Fälle 2023 qualitative Betrachtung

	Dauer	
Dauer der Blockierung gemäss VID Art. 15 Abs. 1, 2, 3 max. Blockierungszeit 30 Tage (720h)	Mindestdauer Durchschnitt Höchstdauer	**0.50 h** **103.32 h** **160.05 h**
Reaktionszeiten von Switch nach Meldung	Durchschnitt	**8.15 h**
Zeit bis zur Beseitigung der Bedrohung nach Bekanntgabe an Halter:in	Durchschnitt	**104.27 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.

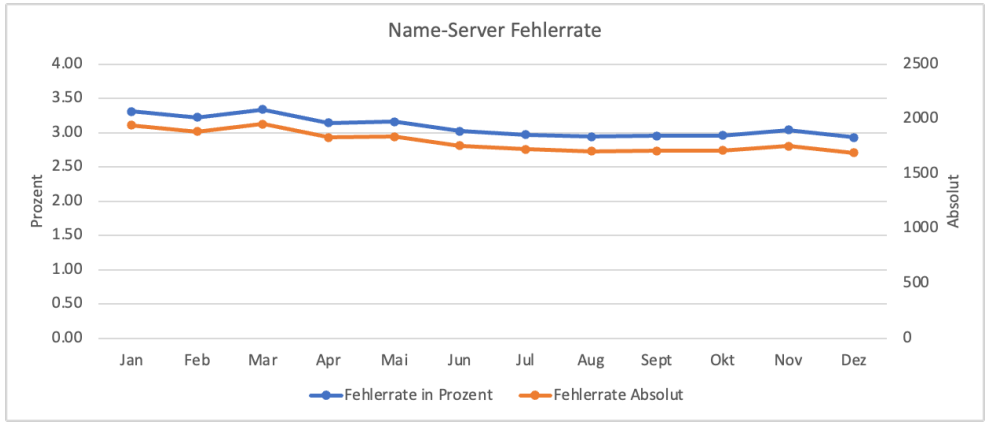
Name-Server-Report

Die Fehlerrate der Erreichbarkeitsmessung von Name-Servern nimmt seit Messbeginn nur leicht aber dafür stetig ab. Eine sehr zufriedenstellende Tendenz.

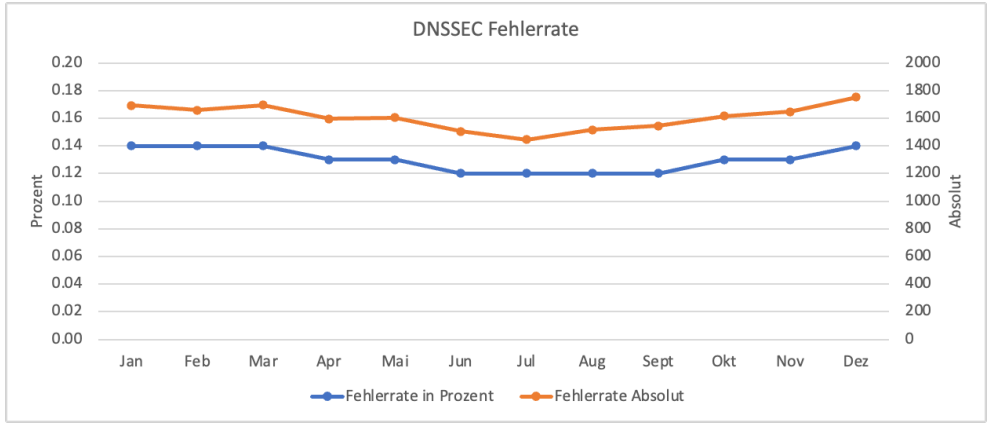
Domain-Namen-Report

Die Fehlerrate der Erreichbarkeitsmessung von 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



DAAR .ch
ICANN Domain Abuse Activity Reporting

Mit der Veröffentlichung der .ch-Zone nimmt Switch am DAAR-Projekt (Domain Abuse Activity Reporting) von ICANN teil. Das Projekt vergleicht Meldungen von Missbrauchsverdacht bei verschiedenen TLDs.

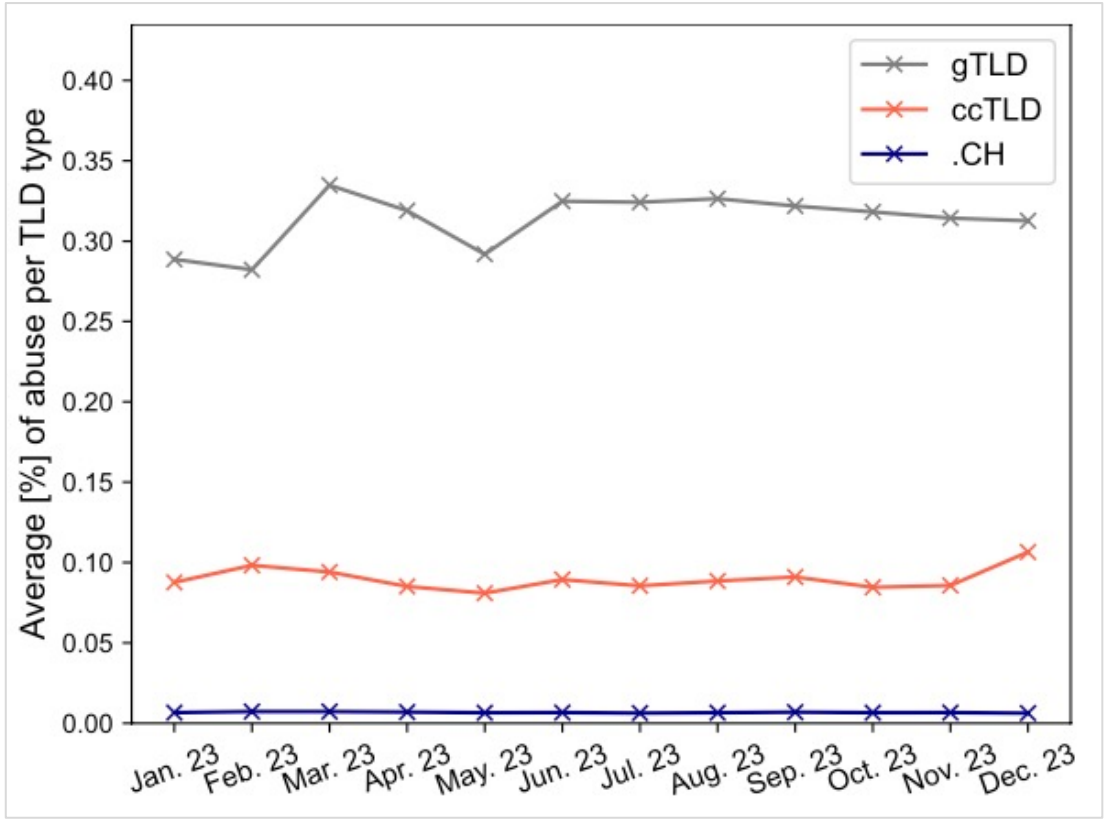
Das Programm und die Reports für ccTLDs sind noch im Beta-Status. Die Grafik ermöglicht jedoch bereits einen Vergleich von .ch mit anderen ccTLDs und gTLDs.

Was wird gemessen?

Anteil der .ch-Domain-Namen in Prozent, die als Sicherheitsbedrohung identifiziert wurden, im Vergleich zur durchschnittlichen Anzahl der Domain-Namen in anderen TLD-Zonen.
Detaillierte Informationen gibt es bei ICANN:
https://www.icann.org/octo-ssr/daar

Analyse von .ch

Der DAAR-Report zeigt, dass der Missbrauch von Domain-Namen bei der ccTLD .ch gering ist, verglichen mit dem Durchschnitt aller TLDs. Dies ist eine Bestätigung für die Effektivität der andauernden Massnahmen zur Bekämpfung von Cybercrime und die funktionierende Zusammenarbeit mit Schweizer Behörden und internationalen Organisationen.



DAAR .li
ICANN Domain Abuse Activity Reporting

Mit der Veröffentlichung der .li-Zone nimmt Switch am DAAR-Projekt (Domain Abuse Activity Reporting) von ICANN teil. Das Projekt vergleicht Meldungen von Missbrauchsverdacht bei verschiedenen TLDs.

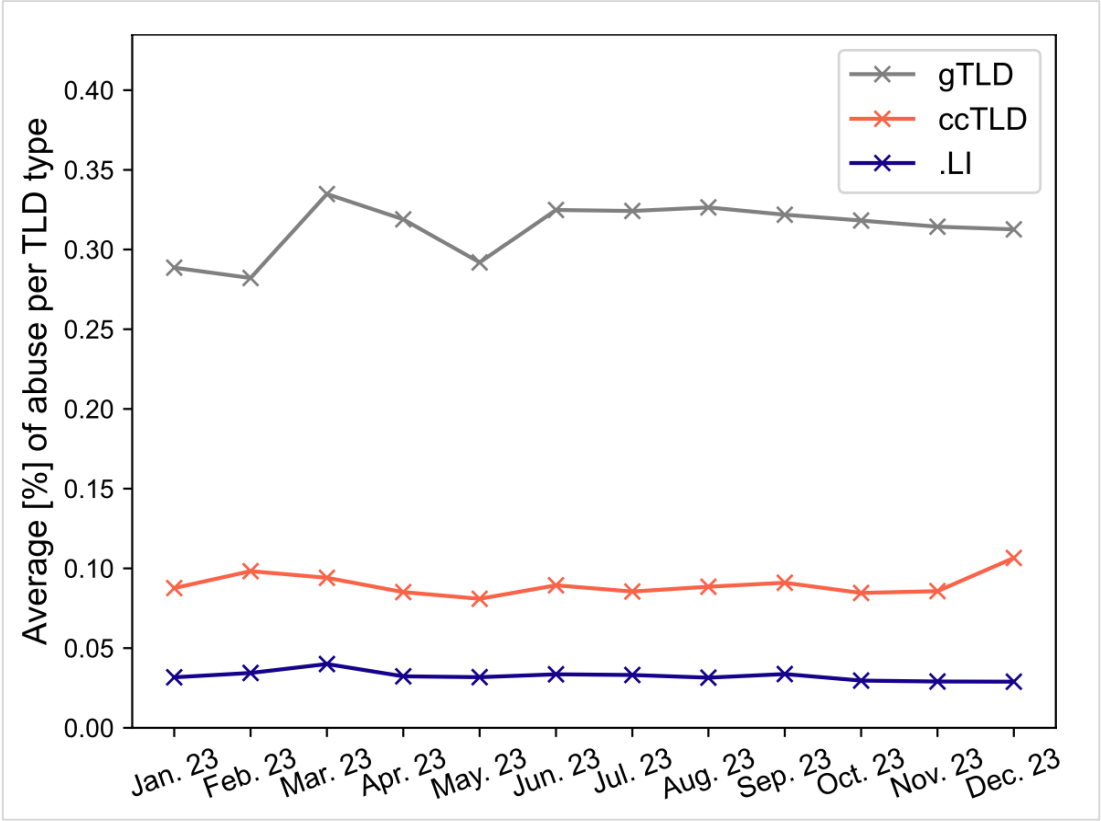
Das Programm und die Reports für ccTLDs sind noch im Beta-Status. Die Grafik ermöglicht jedoch bereits einen Vergleich von .li mit anderen ccTLDs und gTLDs.

Was wird gemessen?

Anteil der .li-Domain-Namen in Prozent, die als Sicherheitsbedrohung identifiziert wurden, im Vergleich zur durchschnittlichen Anzahl der Domain-Namen in anderen TLD-Zonen.
Detaillierte Informationen gibt es bei ICANN:
https://www.icann.org/octo-ssr/daar

Analyse von .li

Der DAAR-Report zeigt, dass der Missbrauch von Domain-Namen bei der ccTLD .li bis auf knapp zwei Dutzend Domain-Namen eliminiert werden konnte. Diesen tiefen Wert kann man nur halten, wenn die Zusammenarbeit zwischen der Registrierungsstelle und den Behörden weiterhin so gut funktioniert.



4.

Tätigkeitsbericht – Wirtschaftliche Kennzahlen

Switch

Wirtschaftliche Kennzahlen

An der Stiftungsratssitzung vom 13. Juni 2024 wird der Geschäftsbericht 2023 der Stiftung Switch zusammen mit der Bilanz und Erfolgsrechnung verabschiedet. Die Veröffentlichung findet ab dem 14. Juni 2024 statt.

An dieser Stelle werden keine Zahlen publiziert, sondern es wird auf die ausführlichen Unterlagen des Geschäftsberichts 2023 von Switch verwiesen.

5.
Tätigkeitsbericht – Entwicklungen

Switch

Rückblick 2023

Wechsel des DNSSEC-Algorithmus

Initial wurde für die Signierung des Zonenfiles der NSEC3-Algorithmus (mit opt-out) gewählt. Dieser Mechanismus verhinderte das sogenannte «Zone Walking» und erschwerte damit eine automatische Auflistung aller Domain-Namen mit der typischen Folge von Spamwellen.

In der Zwischenzeit ist das Zonenfile öffentlich. Die mit 50% hohe Signierungsrate verlangt effizientere Methoden. Dies wird mit dem Umstieg auf den NSEC-Algorithmus erreicht. Der Wechsel von Sicherheitsparametern im DNS bedingt sorgfältige technische Abklärungen im Vorfeld. Die Betreiber der Name-Server und der Resolver sind involviert. Ebenfalls wurde die technische Fach-Community von ICANN und DNS-OARC konsultiert. Damit konnte für die Umstellung grünes Licht gegeben werden. Die Umstellung vom 10. November 2023 führte zu keinerlei Beeinträchtigung der Name-Server- oder Resolver-Funktionen. Das Zonenfile ist nach dem Wechsel leicht grösser, im Gegenzug benötigen die Name-Server und Resolver weniger Rechen-Ressourcen.

European TLD ISAC

Im Februar 2023 startete das European TLD ISAC (Information Sharing and Analysis Center). Die Aufbauphase wird von CENTR und sieben ccTLD-Registries unterstützt. Switch ist im Board vertreten und stellt einen Mitarbeitenden für die Erarbeitung der Zusammenarbeitsprozesse. Der Fokus soll auf dem Austausch von Threat Intelligence liegen, deshalb sind vor allem Registries mit einem CERT und einem ISMS hier aktiv. Für den Aufbau der Kernprozesse und für die Erweiterung auf alle ccTLD-Registries der EU ist ein Zeitraum von zwei Jahren vorgesehen. Finanziert wird das European TLD ISAC vollständig von den beteiligten Registries.

Rückblick 2023

Erhöhung der E-Mail-Sicherheit

Im DNS-Resilienzprogramm wurde zusammen mit dem Bakom und den Registraren festgelegt, dass im 2024 die Implementation von DMARC und SPF als Kriterium für die Rückvergütung gilt. In diesem Zusammenhang hat Switch im Jahr 2023 die Mess-Infrastruktur und ein Dashboard zur manuellen Verifizierung der Messkriterien aufgebaut.

Für 2025 wurde DANE als Kriterium definiert. Zu diesem Thema hat Switch im Oktober 2023 Schulungen in Lausanne und Zürich angeboten.

Konsequenterweise wurde auch die interne E-Mail-Infrastruktur von Switch so umgestellt, dass alle drei Sicherheitsprotokolle für das Senden und für die Verifikation beim Empfang genutzt werden können.

RDAP Web-Frontend für Behörden

Das Web-Frontend zur RDDS-Datenbank (Whois) ist in Betrieb. Jeder Nutzende bei einer Behörde unterzeichnet einen Vertrag für die Benutzung. Die Verwaltung der Nutzungsrechte macht Switch. Bisher nutzen erst wenige kleinere Behörden diesen komfortablen Zugang, doch genau für solche Behörden ist das Web-Frontend gedacht.

Strategischer Ausblick und Ziele

Einzelne fest eingeplante Projekte werden unter «Geplante Neuheiten 2024» vorgestellt. Ebenfalls an anderer Stelle vorgestellt ist das Projekt Domain Abuse 4.0, das im 2024 den Hauptfokus hat. An dieser Stelle geht es um zwei Ausrichtungen, die eher strategischer Natur sind.

Ort der Infrastruktur

In den letzten fünf bis acht Jahren haben zuerst grosse Organisationen mit ihrer IT-Infrastruktur zu Hyperscalern in die Cloud gewechselt, um Infrastruktur zu konsolidieren und Kosten zu sparen. Dem sind etwas später die KMU gefolgt, dies auch unter Druck von Software-Anbietern wie Microsoft, die den On-Premise-Betrieb ihrer Software nicht mehr langfristig garantieren.

Die IT-Infrastruktur von Switch ist auf mehrere Standorte verteilt. Verbunden sind diese durch eine selbst betriebene Glasfaser-Infrastruktur. Das sichert eine maximale Kontrolle über alle Layer der IT-Komponenten.

Eine Zusammenarbeit mit einem Schweizer Cloud-Anbieter eröffnet Switch die Möglichkeit, neue Computer- und Storage-Komponenten in professionellen Rechenzentren aufzubauen. Hier ist ein höherer Level von Ausfallsicherheit und Zugangskontrolle gegeben als an den bisherigen von den Hochschulen angebotenen Standorten. Auch diese Rechenzentren sind mit dem Glasfaser-Netzwerk «Switch LAN» erschlossen.

Im Laufe von 2024 und 2025 werden die Software-Komponenten der Registrierungsstelle auf eine neue Architektur umgestellt und an den neuen Standorten betrieben. Die Governance über Infrastruktur und über die gespeicherten Daten liegt ganz bei Switch und der Standort der Infrastruktur bleibt in der Schweiz. Das sind wichtige Randbedingungen für das Betreiben einer kritischen Infrastruktur und für die Datenbearbeitung im Rahmen der Bekämpfung von Cybercrime.

Strategischer Ausblick und Ziele

DNS-Resilienzprogramm 2027+

Das DNS-Resilienzprogramm ist Teil des Verlängerungsvertrages 2022 bis 2026 mit dem Bakom. Welche Sicherheitsprotokolle durch das Resilienzprogramm gefördert werden sollen, wird im DNSSEC Advisory Board bestimmt. Dieses ist durch je eine delegierte Person des Bakom, der IG Hosting von Swico und von Switch zusammengesetzt. Jeweils mit zwei Jahren Vorlauf werden die Kriterien bestimmt. So kann Switch Schulungen anbieten und die Mess-Infrastruktur vorbereiten. Die Registrare haben genügend Zeit für die Einplanung der technischen Arbeiten für allfällige Umstellungen, bevor die Messungen beginnen.

Über eine allfällige Fortführung des Programms nach 2026 und über die Art und Weise sollte im Jahr 2024 diskutiert werden. Das laufende Programm liefert dazu bereits wichtige Hinweise und Erfahrungen. Es empfiehlt sich, für diese Diskussion die involvierten Parteien an einen Tisch zu bringen.

Geplante Neuheiten 2024

DNS-Resilienzprogramm: DANE-Messungen

Als Kriterium für die Rückvergütungen 2025 wurde DANE als Sicherheitsprotokoll festgelegt. Switch erweitert die Mess-Infrastruktur entsprechend. Ebenfalls wird das Dashboard ergänzt, damit Registrare und Hoster prüfen können, ob sie die Konfiguration gemäss den Empfehlungen von Switch korrekt umgesetzt haben.

Das Kriterium für 2026 wird IPv6 sein. Dafür sind keine spezifischen Schulungen vorgesehen.

Domain Abuse 4.0

Das Projekt «Domain Abuse 4.0» sichert die Zukunft der Cybercrime-Bekämpfung der Registrierungsstelle. Eine Beschreibung des Projekts ist auf Seite 23 zu finden.

ISMS ISO27001:2022

Bisher war ISO 27001:2013 die Norm, gemäss derer die Registrierungsstelle auditiert wurde. Die überarbeitete Norm in der 2022er-Version berücksichtigt ein breiteres und den technologischen und gesellschaftlichen Anforderungen angepasstes Themenfeld.

Switch beabsichtigt, bis zum Herbst 2024 alle relevanten Prozesse und Dokumentationen für eine Zertifizierung nach der neuen Version anzupassen. Dabei kommt Switch zugute, dass bereits viele der von der Norm neu geforderten Themen seit Jahren erfolgreich im Einsatz sind: zum Beispiel Threat Intelligence durch das CERT oder eigene Sicherheitslösungen wie die DNS-Firewall. Die unabhängige Zertifizierung bescheinigt, dass Switch erfolgreich und wirksam ein Informationssicherheits-Managementsystem implementiert hat. Damit ist sichergestellt, dass Switch ihre Aufgaben für den Betrieb kritischer Infrastrukturen und für den Schutz von personenbezogenen Daten auch nach DSG und ISG erfüllt.

Geplante Neuheiten 2024

Web-Crawler für die Registry

Für die Bekämpfung von Malware und Phishing ist die Registrierungsstelle auf Meldungen von Fachstellen angewiesen. Bis Ende 2023 hat das NCSC einen Web-Crawler betrieben. Dieser fragte die Webserver der .ch Zone einzeln ab und untersuchte die Antworten auf verdächtige Patterns. Bei Verdacht auf Malware und Phishing meldete das NCSC die Hinweise an Switch. Wir untersuchten die Seiten mit unseren Werkzeugen und lösten bei einem bestätigten Verdacht die entsprechenden Prozesse aus, um die Webseiten entweder vom Netz zu nehmen oder den Schadcode entfernen zu lassen.

Mit dem Wegfall des NCSC-Crawlers fehlt der Registry ein wichtiger Input für die Bekämpfung von Cybercrime. Deshalb hat Switch bereits im Spätherbst einen eigenen Crawler für die .ch- und .li-Zone entwickelt. Switch hat die nötigen kommerziellen und informellen Quellen für die Patterns, ohne die der Crawler nutzlos wäre.

Die Inbetriebnahme ist so bald wie möglich vorgesehen, idealerweise bereits im Januar oder Februar 2024.

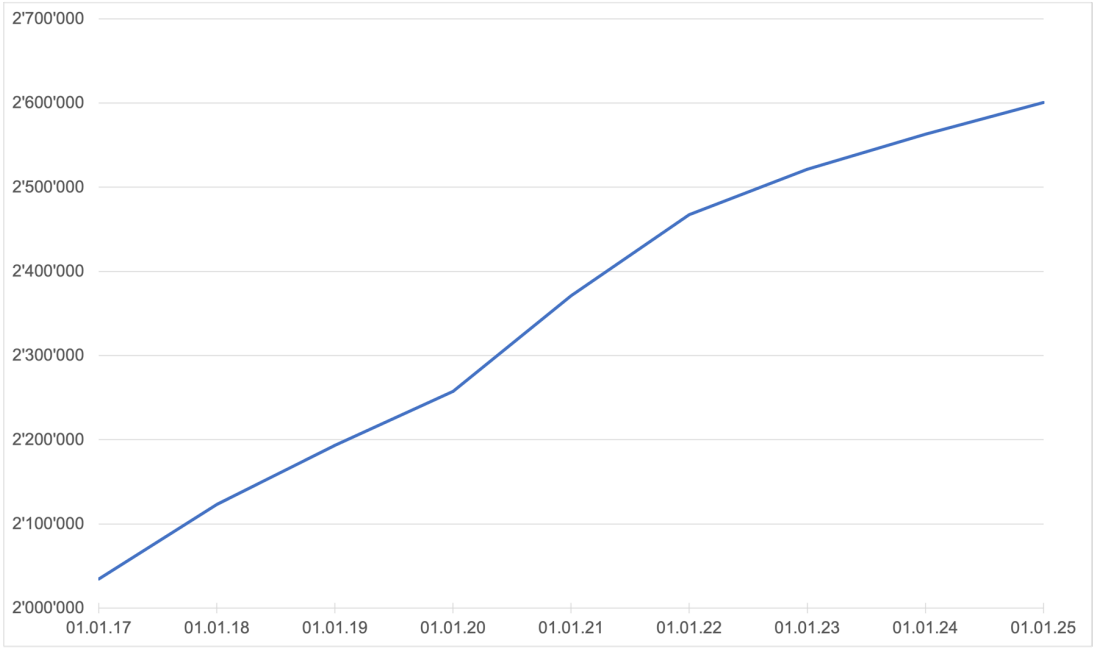
Wachstumsprognose .ch-Domain-Namen

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.

Wir beobachten eine Sättigung des Marktes und ein global gedämpftes Wachstum bei Domain-Namen. Unsere Prognose für 2024 rechnet mit einer Zunahme von 1.45 Prozent.



Switch
Werdstrasse 2
Postfach
CH-8021 Zürich

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

Switch