Switch

Report 2023

of the .ch Registry

Table of contents

Switch

We're doing everything we can to secure the future of our digital ecosystem.

Urs Eppenberger
Head of Registry, Switch

Switch

Full steam ahead in the fight against cybercrime

Urs Eppenberger, Head of Registry

Switch's ongoing efforts in the fight against cybercrime have led to the development of 'Domain Abuse 4.0'. The aim of this project is to secure the future of our digital ecosystem, which required a complete rethink of our strategy in our fight against cybercrime. Processes are being optimised and the entire technical infrastructure is being redesigned. A description of the project can be found on page 23.

While law enforcement in Switzerland is fundamentally the responsibility of the competent authorities, Switch also plays a special role. Switch has its own CERT (Computer Emergency Response Team) and offers modern security services to Swiss universities and businesses. By working with other CERTs and working closely with law enforcement authorities, Switch has become an agile entity that is able to single-handedly manage the flood of malware and phishing cases very efficiently and effectively. OFCOM recognised this at an early stage, and created the necessary legal basis and incorporated the relevant mandate in its agreement with Switch.

Switch's fight against cybercrime is like a highly complex machine, bringing together specialists from different disciplines, networking with other players in the field and linking different IT components.

For Swiss users, it is easier than ever before: They secure their domain name with a Registrar and operate their website through a hosting provider. Plus, they receive these services at attractive prices. However, it is largely unknown what efforts are needed in the background to ensure the secure and stable operation of the internet as a whole and of each individual domain name. This requires coordinated and well-established cooperation between hosts, Registrars, Switch and law enforcement authorities.

Anyone involved in fighting cybercrime knows the importance and necessity of this work. That is why we at Switch have decided to step up our efforts. The registration and management of domain names, which is the core task of the registry, is organised so efficiently that we are able to focus all our innovation effort on fighting cybercrime. This means that the highest level of security and stability can still be guaranteed for all internet users.

Switch_

1.

Activity report – operations

Switch

Combating cybercrime

**Compromised websites**

The number of compromised websites used for phishing and malware was almost unchanged from last year.

Improper registration

The number of domain names reported as suspected improper registrations has increased. One reason for this is that Fedpol has sent more requests under Art. 15 as part of its SWITCHoff project.

Website: https://www.saferinternet.ch
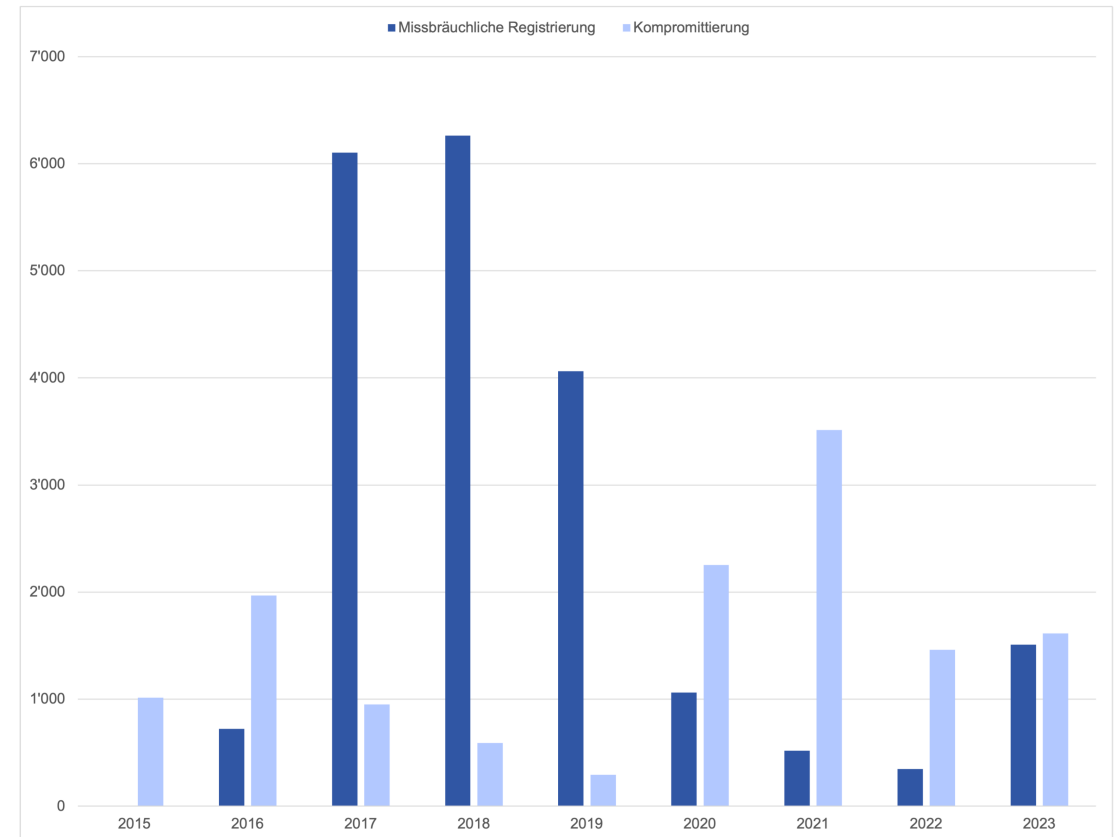
Measures in the event of suspected abuse

Requests from recognised authorities – OID Art. 15.1

In 2023, accredited authorities sent a total of 426 requests under OID Art. 15.1 for immediate blocking (technical/administrative) of domain names related to phishing or malware.

Requests	Consequences	2023
Not answered	Domain name deleted	410
Answered	Domain name reactivated	16
Total		**426**

All authorities recognised by OFCOM are listed on the following website: Recognised authorities

Administrative assistance – OID Art. 16.3

At the request of an intervening Swiss authority acting within its area of responsibility, 1,084 requests were submitted for Swiss correspondence addresses under OID Art. 16.3.

| Requests	Consequences	2023
Not answered	Domain name deleted	964
Answered	Domain name reactivated	120
Total		**1,084**

Security awareness – iBarry and SISA

In collaboration with SISA, Switch continues to help raise awareness among the Swiss population. With its three new information campaigns (fake news, data protection, VPN), iBarry.ch is providing information, guidance and support for anyone who is uncertain or has questions about internet security.

https://checkawebsite.ibarry.ch/en
https://ibarry.ch/en/

In order to optimise the range of services available to the Swiss population and to better position the iBarry platform, SISA once again took part in this year's survey of Swiss internet users.

https://internet-sicherheit.ch
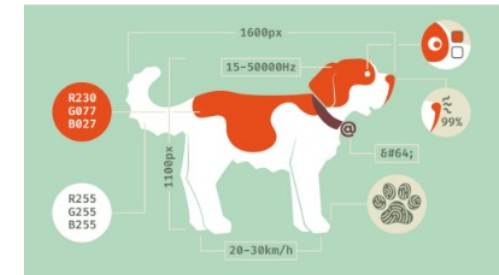
Security Awareness Day

On 26 October 2023, Switch hosted its sixth Swiss Security Awareness Day. This year, iBarry was a partner at the constantly growing conference. Around 120 attendees were able to network with other experts during various breaks in between the exciting presentations.

Once again, the purpose of this year's programme was to increase awareness of security-related issues within the Switch community, while also sharing ideas and encouraging communication and interaction.

All presentations are available online: https://swit.ch/ssad2023-recordings

Security Awareness Adventures

Switch Security Awareness Adventures

'Hack the Hacker – the escape room' was the first of three Switch security awareness adventures, followed by 'Track the Hacker – the scavenger hunt' and 'Piece of Cake – the role play'. The adventures remain extremely popular: In 2023, Switch hosted a total of 40 game-style security training sessions, and even helped three other organisations to set up their own.

Twelve OFCOM employees also successfully hacked the hacker.

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

Security awareness – Podcast

Podcast: Security Awareness Insider

In December 2023, the 38th episode of the 'Security Awareness Insider' (German-language) podcast was released.

In the episode, Katja Dörlemann (Switch) and Marcus Beyer (Swisscom) talk about raising employees' awareness of security issues and new and creative methods, tools, and training approaches, provide insight into the security awareness programmes of companies and organisations, and much more.

Since the podcast first launched, it has been downloaded 17,000 times, with an average of 400 downloads per episode.

Available on Spotify or here:
https://www.securityawarenessinsider.ch
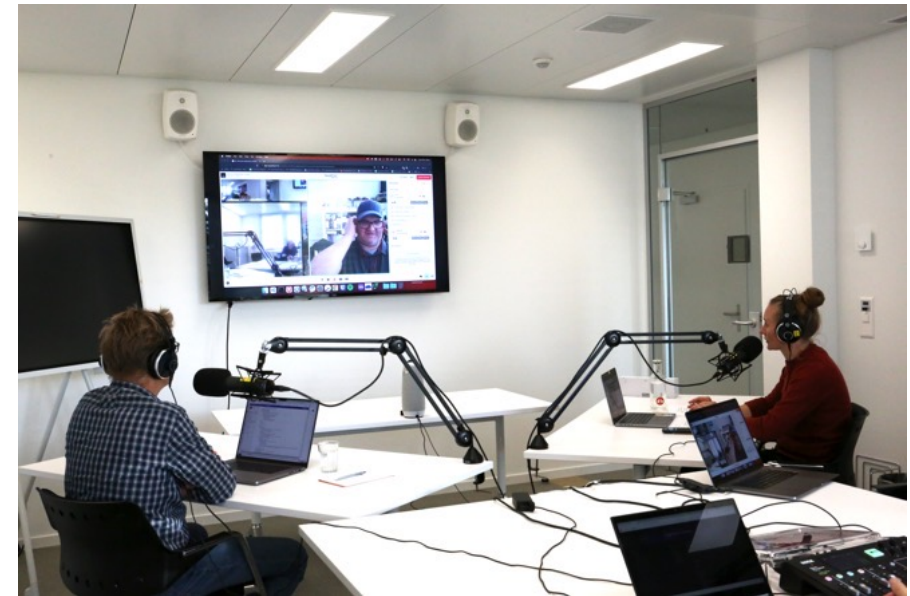
Community – Swiss Web Security Day

On 17 October 2023, Switch, together with SISA and Swico, organised the Swiss Web Security Day in Bern, which ran alongside the LEO event with Swiss law enforcement authorities. The event was a superb success, with 73 participants in attendance from Switzerland and abroad, and very positive feedback.

In the morning there were presentations on guidelines for secure mail communication, Medicrime, vulnerability management in Switzerland, threats against Swiss internet users and an update on the revision of the Ordinance on Internet Domains. In the afternoon, there was time for workshops and small group discussions, followed by a drinks reception.

Following years of hybrid events, this year was a purely in-person event in Bern.

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

The Swiss Web Security Day will be held again in 2024:
29 October 2024, Welle 7, Bern.
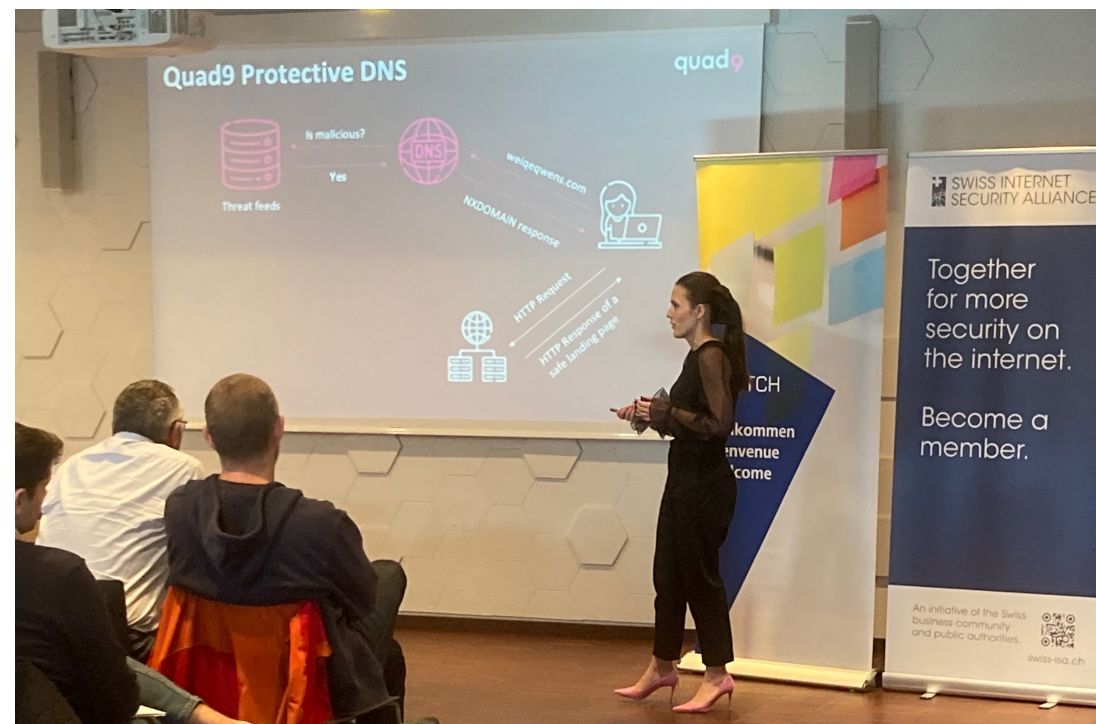
Community – ModSecurity course

ModSecurity is a very popular, powerful open source web application firewall. Web application firewalls are an important building block for the protection of a web application and are therefore of interest to hosts and registrars, as well as to any operator of a web application in general.

In order to offer added value to our community, Switch and world-renowned ModSecurity expert Dr Christian Folini from Netnea organised an introductory course at Switch Zurich on 15 and 16 March 2023. Switch leveraged its strong connections within the community to raise awareness of the course, provided the venue and subsidised tickets for Registrars and Switch customers.

This saw a broad mix of Registrars, hosts and university staff attend in the course in Zurich.

We plan to hold the course again in 2024.

LEO event
Cooperation with law enforcement authorities

Target group

This year, to ramp up cooperation with the authorities, Switch organised its third LEO event. LEO stands for 'law enforcement organisations'.

The law enforcement community met in Bern on 17 October 2023. The LEO event was attended by 63 people, many of whom attended last year and brought along interested colleagues with them. The event is growing each year.

The distribution between the regions was very balanced, with presentations given in national languages and in English. The participants came from the cantonal police forces, the cantonal public prosecutor's offices and the Liechtenstein National Police. Authorities such as Swissmedic, SECO and OFCOM were also represented.
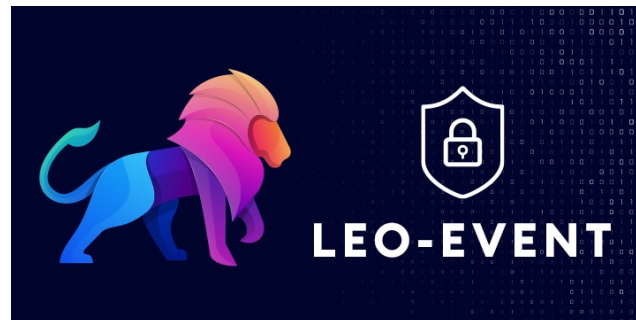
Topics

Various topics were discussed. The core topic was working together in the community to prevent cybercrime. Various cases were presented, which could be solved successfully and efficiently through the cooperation of community partners.

A Finnish case study provided inspiration on how to handle cases that may seem extremely challenging at first. The 'Lessons Learned' on OID requests to Switch and their potential pitfalls were discussed and participants from OFCOM answered questions from the community.

Feedback

The event was a superb success. Participants discussed current developments and projects relating to domain abuse and cybercrime. Processes and interfaces to simplify cooperation were also covered. Exchange between both sides has increased significantly. Participants are looking forward to another event in 2024.

Domain Pulse 2023

At this year's Domain Pulse, industry experts mainly from Switzerland, Germany and Austria came together on 6 and 7 February 2023 to discuss the security and stability of the internet.

Around 250 participants from registries, Registrars, hosts, federal offices and other experts accepted the invitation to Winterthur.

Looking at the topic of 'Critical internet infrastructure: Maintaining sovereignty and protecting against abuse' they explored the challenges facing the internet industry today.

The focus was on the question of how politicians and critical infrastructure operating organisations can maintain sovereignty over the internet in times of international conflict, protect it from attacks and make it more resilient.

The baroque conference hall was a striking backdrop for the many participants and the considerable time set aside for networking was much appreciated.

We look forward to hosting the Domain Pulse event again in 2026.

DNS resilience programme

50%

As of 1 January 2024, almost 50% of all .ch domain names have been signed.

Switch

DNS resilience programme

Resilience for .ch domain names

The DNS resilience programme promotes the introduction and use of open security standards for .ch and .li domain names. The use of these standards is critical for resilience against cyber threats. The programme is based on a financial incentive scheme and will run from 2022 to 2026.

The main objective is to promote the signing of domain names with DNSSEC. For the entire duration of the programme, Registrars will be charged a surcharge for domain names that are not signed or not signed correctly.

The DNSSEC Advisory Board determines which standards should be supported. OFCOM, a representative of the Registrars, and Switch are represented on this committee.

For 2024, the e-mail security technologies DMARC and SPF will be added to the programme. DNSSEC and the implementation of both DMARC and SPF will be decisive for the reimbursement of the additional revenue.

The Advisory Board has already agreed that DANE will be promoted in 2025 and IPv6 in 2026, in addition to DNSSEC. This leaves the Registrars sufficient time to attend the training courses offered by Switch and to plan the technical measures.

Quality control measurements

As with DNSSEC, external monitoring service provider OpenIntel will also be called in to measure the other security technologies. For all .ch and .li domain names with name servers, they check whether the criteria defined by Switch for the programme are met and report this to Switch on a daily basis. In the event of incorrect configurations, Registrars receive error reports from us.

DNS resilience programme

In its second year of operation, we continued to focus on the development of the resilience programme, in addition to operations.

Developments 2023

- Reimbursements for 2022 to eligible Registrars in the form of credit entries (end of January 2023).

- Implementation of DMARC and SPF measurements, which will be relevant in 2024.

- Since September 2023 new error reports for DMARC/SPF have been sent to Registrars. Although the criterion will not be decisive until 2024, this gives Registrars the opportunity to prepare for it.

- Extension of the Dashboard for DMARC/SPF, provided by the external monitoring service provider OpenIntel (see screenshot).

- Continuously providing information to the Registrars, answering their questions, providing support.

- Two new reports that enable interested Registrars to follow the assessment of their domain names.

- Training sessions on DNSSEC and DANE in Zurich and Lausanne in October 2023.

DNS – Anycast locations and zone generation

Anycast locations

Our DNS Anycast hosting partners have added several locations in Switzerland and abroad to which the DNS zone is provided via Anycast in 2023. For example, there has been a point of presence in Geneva since January 2023.

Zone generation

The infrastructure for zone generation and distribution was completely redesigned in 2023. The Hidden Primary Servers, which create the zone and generate the DNSSEC signatures, have been upgraded to new hardware.

Due to the now high proportion of DNSSEC-signed domain names and changes in the requirements resulting from the publication of the .ch zone in 2020, the method used to create DNSSEC signatures for non-existent names has also been changed:
Previous: NSEC3 with opt-out
New: NSEC

ISMS recertification

From 5 to 7 September 2023, the recertification of the information security management system (ISMS) was performed in accordance with ISO 27001:2013.

Over three days, the auditor examined all aspects of the ISMS at Switch in accordance with the requirements for recertification. Switch passed the audit without any deviations or other issues.

The auditor made seven recommendations on how Switch can improve the ISMS. These recommendations feed into the continuous improvement process (CIP) of the ISMS.

The auditor's report includes their positive overall impression and concludes with the following comment: 'There is a strong commitment on the part of the management and a high level of understanding of information security among all employees interviewed. One of Switch's strengths is its continuous improvement and the high level of expertise of its employees at all levels.'

'One of Switch's strengths is its continuous improvement and the high level of expertise of its employees at all levels.'

ISO 27001 audit report

Switch_

2.
Activity report – innovations

Switch_

Domain Abuse 4.0

Increasing demands

With a strong team of experts and the support of self-developed software solutions, Switch has been combating domain name abuse on the Swiss internet for years. Cybercriminals are becoming more and more cunning, which means that the demands on experts and software solutions are increasing.

Challenge of the current software solution

The codebase of the current software solution for combating cybercrime dates back to 2008, so the solution is based on an outdated IT architecture. It is slow, and maintenance and the ever-increasing challenges of combating domain name abuse are time-consuming.

Modern and future-oriented anti-abuse measures

As part of the Domain Abuse 4.0 project, a new, future-focused software solution is being developed. It is based on state-of-the-art technologies and the latest Switch Cloud infrastructure. The registry development team and the CERT development team are combining their experience and skills to develop a fast, low-maintenance and highly scalable solution. The processes are also being revised, adapted to the new circumstances and our experts are being trained in them. With these measures, Switch continues to be a global leader in the fight against cybercrime.

Domain Abuse 4.0

Facts and figures

- 20 workflows (anti-abuse processes) have been defined on the basis of the OID.

- 14 software components need to be newly developed or further developed.

- 50+ user stories have been written (not yet finalised).

- 16 solution variants have been evaluated.

- 12 people in different positions have worked on the project so far.

2022	2023	2024	2025
Start	**Evaluation**	**Development**	**Operations**
In October 2022, the project started with the definition of the workflows and the IT architecture	From 16 solution variants, an in-house development was selected as the most future-focused solution	The software solution is developed iteratively with regular releases	The new solution should be implemented by the end of 2025

Switch

Establishment of the European TLD ISAC

The European TLD Information Sharing and Analysis Centre (ISAC) was established in 2023 under the umbrella of CENTR.

The European Top Level Domain Information Sharing and Analysis Centre (TLD ISAC) aims to promote the security and resilience of top-level domain registries in Europe through information sharing, collaboration and sharing of best practices.

It brings together operators, security professionals and other stakeholders to exchange information on threats, identify emerging trends and develop proactive measures to prevent and respond to cyber attacks.

Switch, together with other operators of European ccTLDs, is a founding member and active participant in the steering committee, the working group and the threat intelligence sharing group.

The first TLD ISAC conference took place in Brussels on 13 November 2023, with Switch represented by two participants.

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

Web crawler

As part of the fight against cybercrime, Switch developed a new tool at the end of 2023: a web crawler that systematically scans publicly available resources in the .ch and .li zones in order to detect compromised or malicious domain names at an early stage and thus eliminate the threat to internet users.

Our Cyber Threat Intelligence team regularly updates the criteria that help us identify threats so that we can stay up to date and work effectively. We also exchange ideas with authorities and other registries.

If our crawler detects domain names that are phishing or spreading malware, we can block the domain name after notifying the owner and waiting for a period of time.

This way, Switch can make an important contribution to further increasing the security of the .ch and .li zones not only reactively, but also proactively through independent searches.

New data protection act

The new Swiss data protection act entered into force on 1 September 2023. Switch started implementing the new legal requirements at an early stage.

Data protection officer

Switch appointed a new data protection officer on 1 March 2023 and notified the Federal Data Protection and Information Commissioner (FDPIC). Angelo Marchetta holds this position at Switch, and advises and supports Switch in the implementation of data protection regulations and employee training. His responsibilities also include monitoring and coordinating all relevant data protection activities in the company. He is also in charge of setting up a data protection management system (DPMS).

Processing directory

The introduction of the provision on keeping a processing directory replaced the previous obligation to report data collections. Switch has recorded its data processing activities as a registry operator both in the internal processing directory and in the publicly accessible registry, the DataReg.

Data security

As part of the new Swiss data protection act, Switch has implemented adjustments to the notification process for data security breaches. This enables rapid reporting of incidents that are likely to pose a high risk to the privacy or fundamental rights of the data subject.

DPMS

Switch has always attached great importance to the protection of personal data – not just since the implementation of the new Swiss data protection act. In addition to the information security management system (ISMS), over the next few years Switch will develop a data protection management system to ensure that data protection is systematically guaranteed and continuously improved.

Quad9: The role of threat intelligence

Quad9 and Switch are working together to analyse threats to the Swiss internet. This includes:

– Developing and implementing a threat intelligence strategy for Quad9 and for Domain Abuse at Switch.

– Analysing the top threats blocked by Quad9 around the world each month and producing regular reports that are shared with interested parties within the security community and with local government cybersecurity organisations.
Example reports: Q9 Cyber Insights Report, Malawi Report

– Acquiring new threat intelligence partnerships for Quad9.
For example: Phish Report, SISA

– Presentations on topics related to threat data, Quad9 and data protection. Presentations: Swiss Web Security Day, M3AAWG, Women in Cyber

– Creating a 'Quad9 Threat Intelligence Product for Switch CERT'. The aim of this project was to develop a solution for Switch CERT for collecting, aggregating and analysing threat data from Quad9 DNS. The findings were used for the Switch Threat Radar and presented at Swiss Web Security Day.
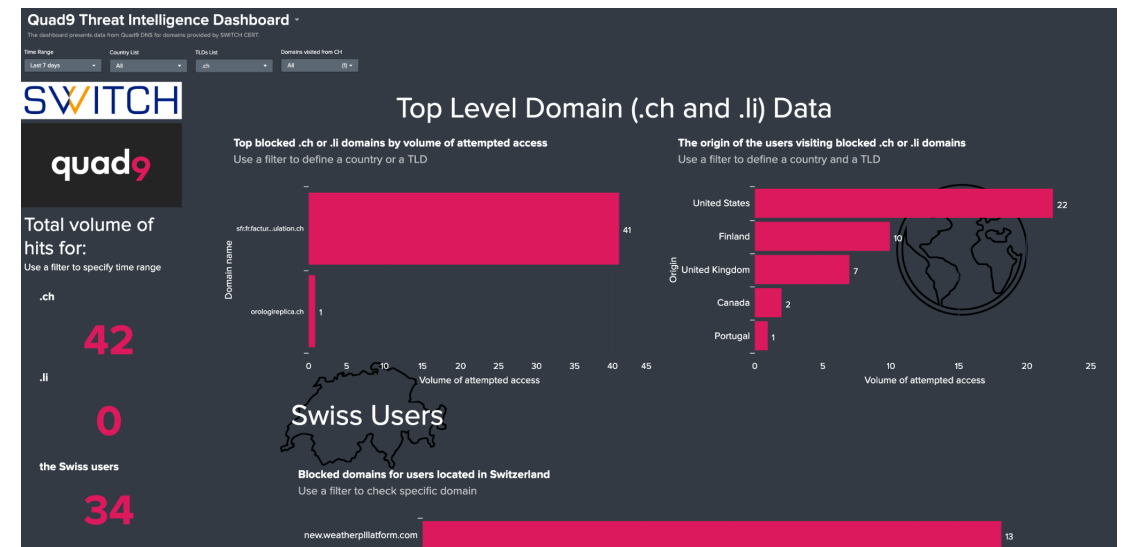
Top threats to the Swiss web

According to data collected by Quad9, the following campaigns were active in 2023 and posed a threat to Swiss internet users:

Fake jQuery domain

The malicious script is injected into legitimate JavaScript files and executes a script from the malicious domain jqueryns[.]com. This redirects you to various fraudulent sites. Vulnerable WordPress websites in particular were affected. More than 8,000 DNS queries were blocked by Quad9 in Switzerland and 47 .ch domain names were affected.

SocGholish WordPress injections

SocGholish is a widespread malware campaign that has been active for several years and is intended to distribute fake browser updates, including to Swiss internet users. Once installed, the fake browser updates infect the victim's computer with various types of malware, including Remote Access Trojans (RATs). In just one month, Quad9 blocked around 1,700 DNS queries from Switzerland.

Phishing targeting Swiss Post

The phishing site targeting Swiss Post was hosted under campaign-image[.]eu. The campaign was active between 20 and 26 April. In Switzerland, more than 870 queries were blocked by Quad9 in a single week in April. More than 24,900 queries have been blocked by Quad9 worldwide.

'ndsw/ndsx' malware

This is another variant of SocGholish malware. All malware variants contain the statement 'if(ndsw===undefined)', hence the name. Its aim is to install the 'fake update' malware on Windows computers. 92 .ch domain names were affected.

Black Hat ad network and Balada injector

This is a major campaign that uses hacked WordPress websites as an inventory platform for ad placements and redirects. The infected websites redirect to fake browser updates and support scams. 37 .ch domain names were affected.

New location in Lausanne

On 2 May 2023, Switch opened a new location in western Switzerland. The foundation has taken over offices for up to 15 employees at the EPFL Innovation Park. Tom Kleiber, Managing Director of Switch, explained the main reason behind the move, "In order to fulfil our national role in the university sector in a better and more credible way, we need a location in western Switzerland. Being close to the community and having direct discussions with the people in it is very important to us."

Martin Vetterli, President of EPFL, had positive things to say about the new location in his speech at the opening ceremony: "The universities in western Switzerland are looking forward to increased collaboration with Switch."

This also means that the registry is closer to Registrars who are based in French-speaking Switzerland. The new location in western Switzerland also offers local talent the opportunity to work on meaningful tasks in their own region, such as the sustainable use of research data, cyber security or digital identities.

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

IPv6 Evangelist

Switch has been working since 1996 to introduce the IPv6 standard, which we believe is essential for the sustainable development of the internet. In addition to the implementation in the university network and the registry, we have also supported related activities of the Swiss internet community. This takes the form of events such as conferences and courses, standardisation work with the Internet Engineering Task Force (IETF) and advising political bodies.

This has enabled us to play our part in making Switzerland one of the countries where IPv6 is well established and is steadily spreading.

These efforts were recognised by the international IPv6 Forum in 2023 when Simon Leinen, a Switch employee for many years, was inducted into the IPv6 Hall of Fame as an IPv6 Evangelist. There are currently only about 100 IPv6 Evangelists in the world.

Registrar customer survey

In November/December 2023, Switch conducted a customer satisfaction survey among all Registrars. 30 of 156 Registrars took part in the survey. The results are therefore considered to be indicative.

Key info at a glance

– Among the Registrars, Switch has a reputation for being highly trustworthy, secure, stable, friendly, quality-focused and competent.

– According to the survey participants, Switch offers the best overall service by far compared to all major registries around the world.

– Overall, the Registrars gave Switch a very high average score of 8.7 out of 10 points.
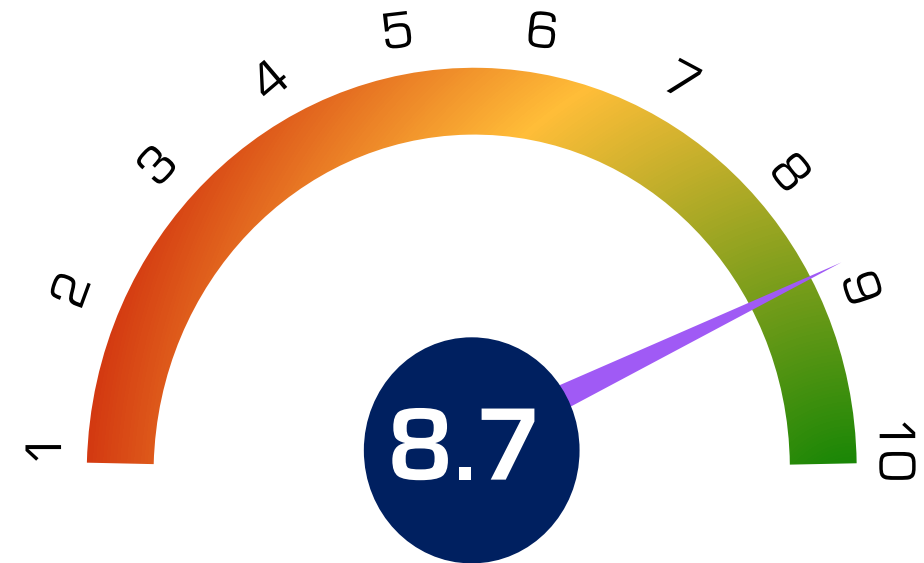
Overall impression of Switch
Question: Considering everything you know about Switch as a registry, what is your overall impression of Switch?
Scale: 1 = very negative; 10 = very positive

3.
Activity report – statistical indicators

Switch

50%

The DNS resilience programme gave DNSSEC the desired breakthrough. Almost 50% of domain names are now signed.

1.6%

Growth of the .ch domain

40,000

Increase of around 40,000 domain names.

Switch_

Domain name inventory – 2023 developments

Development of .ch

The inventory of .ch domain names increased by around 40,000 within a year. This corresponds to an increase of 1.6% compared to the previous year.

	2022	2023
New registrations	281,610	294,195
Deletions	258,724	282,649
Reactivations*	31,097	29,958
Domain inventory as at 31/12	**2,521,444**	**2,562,914**

Development of .li

The inventory of .li domain names has hardly changed in the past year.

	2022	2023
New registrations	10,094	10,658
Deletions	10,178	12,218
Reactivations*	1,823	1,699
Domain inventory as at 31/12	**70,478**	**70,607**

Development of the domain name inventory for .ch and .li
* Deleted domain names that were reactivated by the Registrar within the 40-day transition period.

Information service – statistics 2023

Information service

Switch grants anyone who can credibly demonstrate an overriding legitimate interest free access to the domain name holder's personal data contained in the RDDS database (Whois). These statistics record all requests that were made in the reporting year using the information service's forms. The number of enquiries remained at the same level compared to the previous year.

	Private	Authorities
Information provided	304	135
Information not provided	56	5
General requests *	4	0
Total requests	**364**	**140**

* These are requests about processes, procedures and legal bases.

Simplified access via RDAP for .ch and .li

If an authority or organisation has the appropriate permissions, it can query domain names with personal data via RDAP (Registration Data Access Protocol). The number of authorities increased sharply in 2023, which is also thanks to our improved networking with law enforcement authorities. At the end of 2022, only 5 authorities were using RDAP, compared to 18 by the end of 2023. The cantonal police forces make up the largest proportion.
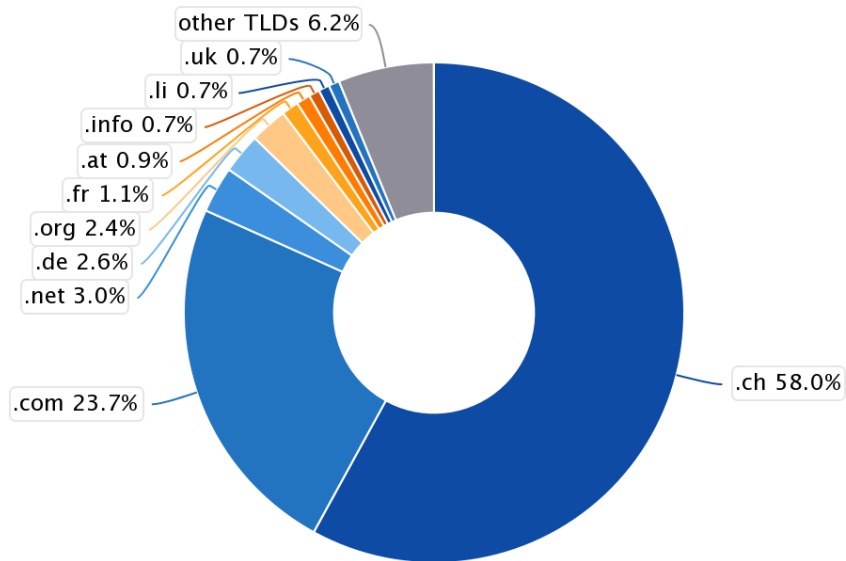
	Requests
Information provided	3,612
Information not provided	309
Total requests	3,921

Market share of .ch and .li with Swiss domain name holders

The market share of the TLD (top-level domain) **.ch** among holders in Switzerland remained nearly unchanged from October 2022 to October 2023.

There was little change in the market share for the generic TLDs **.com/.net/.org**, or for **.li** domain names.

October 2022

Market share of different TLDs among domain name holders in Switzerland. Source: CENTR

other TLDs 6.2%
.uk 0.7%
.li 0.7%
.info 0.7%
.at 0.9%
.fr 1.1%
.org 2.4%
.de 2.6%
.net 3.0%
.com 23.7%
.ch 58.0%

October 2023

Market share of different TLDs among domain name holders in Switzerland. Source: CENTR

other TLDs 5.7%
.swiss 0.5%
.uk 0.5%
.li 0.7%
.info 0.8%
.at 0.9%
.fr 1.2%
.org 2.4%
.de 2.7%
.net 2.9%
.com 23.4%
.ch 58.3%
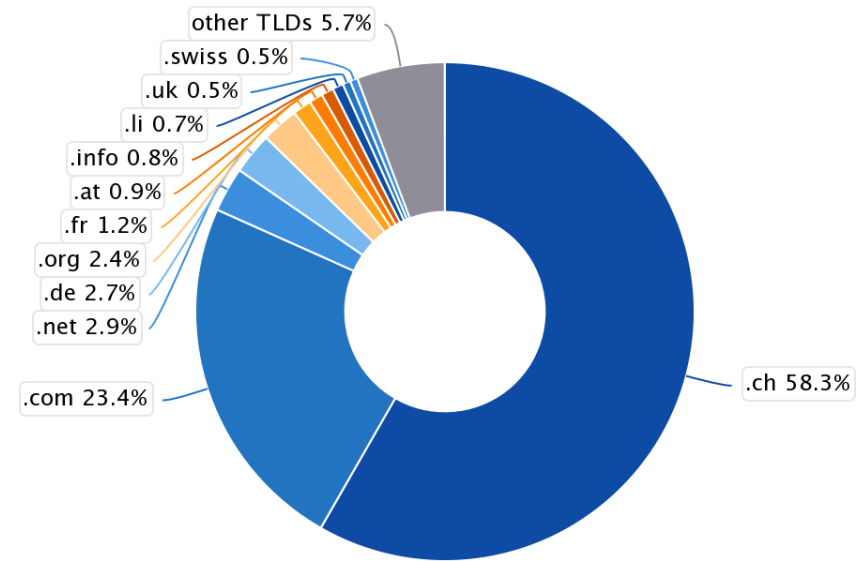
DNS resilience programme – development in figures

DNSSEC

– Percentage of .ch domain names with DNSSEC, as of
1 January 2024: 49.1% (1 January 2023: 44.8%).

– Error rate: The error rate remained more or less constant at a
very low level over the year. Less than 0.25% of all DNSSEC
domain names had errors (2022: less than 0.5%).

DMARC and SPF

– 1 July 2023 (start of measurements by OpenIntel):
2.6% correctly configured.

– 1 January 2024: 4.5% correctly configured. Figures for .ch and
.li domain names, correct configuration of both DMARC and
SPF. Data according to statistics from the external monitoring
service provider.

DNSSEC statistics at Switch

Statistics at OpenIntel

Refund calculation for 2023

– Additional revenue collected from price differentiation:
CHF 1,792,697

– Less fixed compensation for Switch and the external
monitoring service provider for 2023: CHF – 444,907

– Total refund CHF 1,347,790

The refund will be made at the end of February 2024.

Percentage of .ch domain names with DNSSEC
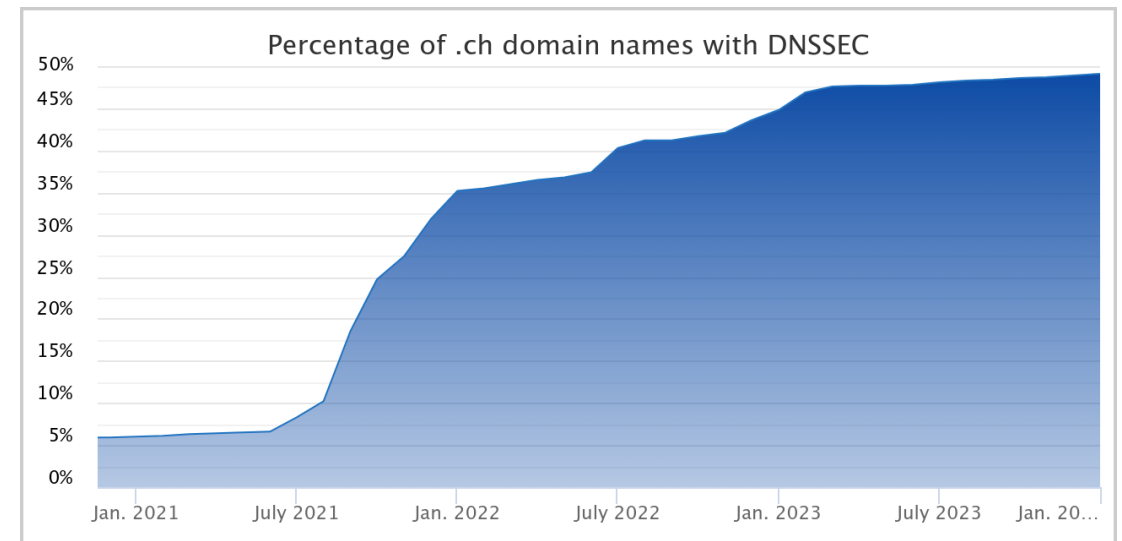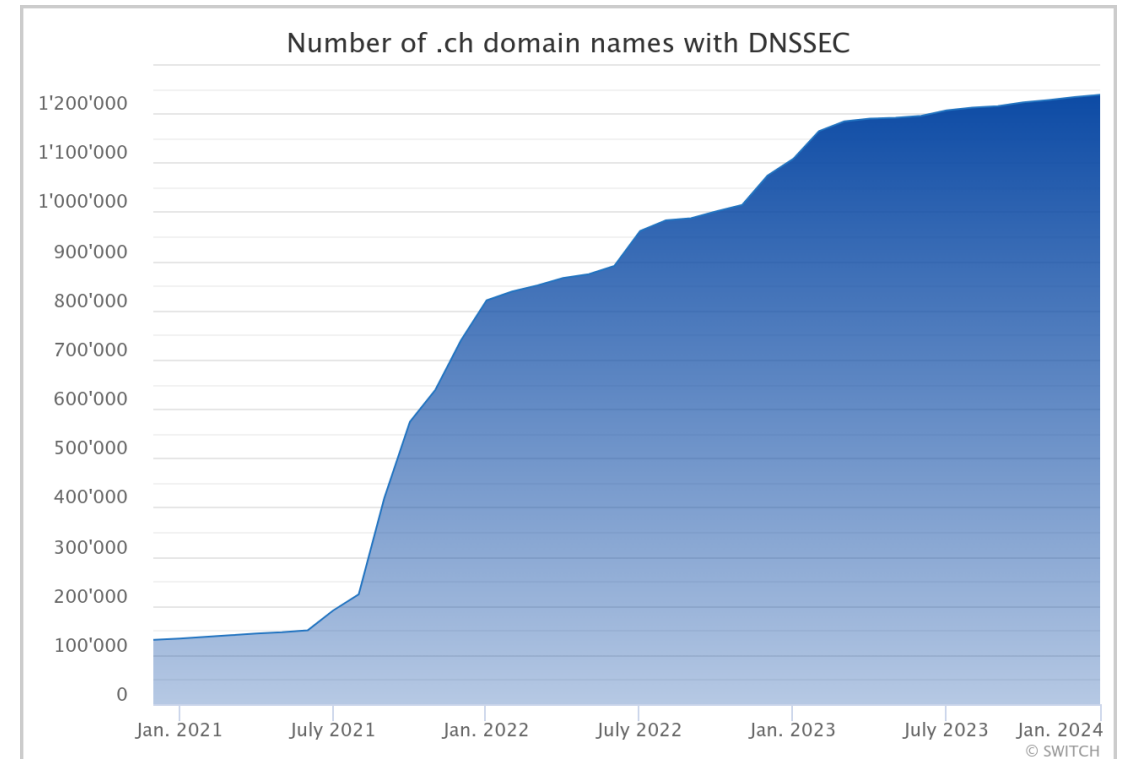
DNSSEC developments
Number of signed domain names

As of the end of 2023, more than 1.2 million .ch domain names have been signed with DNSSEC.

This corresponds to almost 50% of all .ch domain names with name servers, compared with 45% at the end of 2022 and 35% at the end of 2021. The strong growth in 2021 and 2022 was mainly driven by Registrars signing all their clients' domain names as part of the DNS resilience programme. In 2023, this growth slowed down.

The larger Swiss Registrars have now signed as many of their domain names as possible. If the domain names have 'external' name servers, the Registrars have no influence on the signature. For large Registrars abroad, the .ch TLD is only a very small part of their business and the effort of signing is not worth it for them. Growth is therefore expected to slow sharply in the future.

Number of .ch domain names with DNSSEC

1,237,670 .ch domain names signed with DNSSEC as of 1 January 2024

DNSSEC developments
Distribution of DS algorithms

More than 90% of all .ch domain names now use the currently recommended algorithm 13 (ECDSAP256SHA256).

DS records with algorithms 5 and 7, which are no longer considered secure due to their SHA-1 signature, are no longer supported as of February 2023 and have been removed from the zone accordingly.
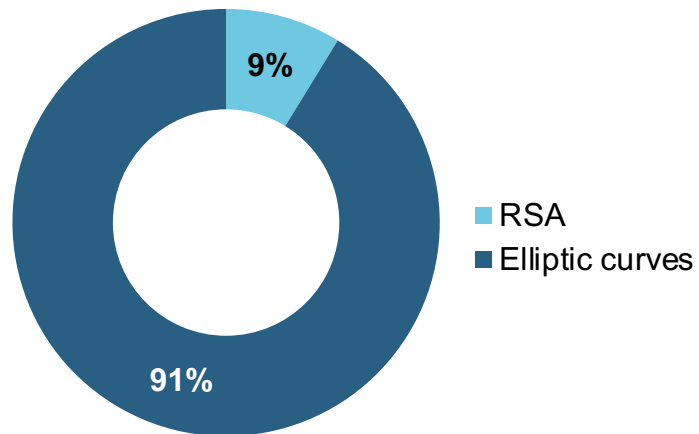
DNSSEC signatures used

DNSSEC algorithm	Number	Percentage
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%

■ RSA
■ Elliptic curves

DNSSEC validation in Switzerland

## DNSSEC validation

In order to protect users from DNS spoofing, not only must the domain names be signed, but these signatures must also be validated by the DNS resolver.

According to APNIC measurements, the DNSSEC validation rate on the resolvers of Swiss ISPs rose to over 70% for the first time last year.

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

DNSSEC validation on Swiss resolvers
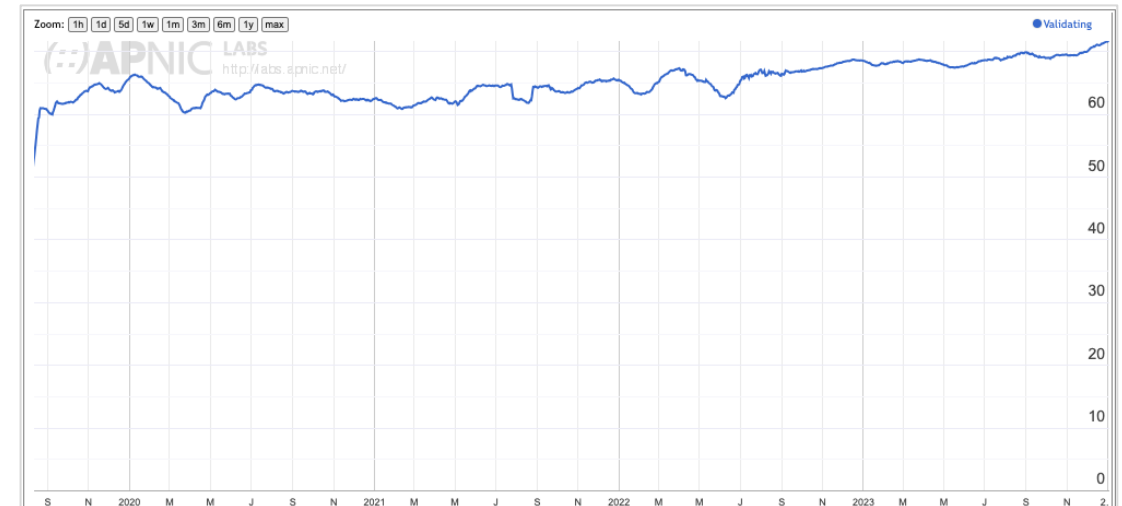
Deferred Delegation – status

Legal basis

With Article 25 of the OID entitled 'General conditions of allocation', OFCOM has established the legal basis that enables a registry to defer activation of a domain name for a fixed period of time and to refrain from entering the name servers in the zone file if there is suspicion that the domain name is being used unlawfully or its purpose is unlawful. This process is referred to as 'deferred delegation'.

Process adjustments

By tightening the rules, we were able to withhold and delete considerably more registrations in 2023.

After the transfer to productive operation, we continue to revise the criteria on a regular basis. In addition, new criteria and verification methods are being researched to better identify improper registrations. The latter always keeps in mind authorised users, who should not be affected.

We keep in contact with other registries for further improvement and to exchange experiences.

We have developed a dashboard that gives us an overview of the current process metrics at all times. The criteria are regularly revised and refined using data analysis. Deferred delegation should as far as possible only aim at improper use; authorised users should not be hindered.

Key figures for Deferred Delegation 2023

|	
Total new registrations	294,195
Domain names deferred	2,751
Domain names deleted	1,956

Deferred Delegation – status

A look back at Deferred Delegation

Since the introduction of Deferred Delegation in early 2022, we have been gradually increasing the number of deferred domain names (blue bars).

This has been achieved by making the criteria increasingly more stringent. By carefully selecting these criteria, the proportion of domain names that were revoked after the holder was not identified was kept stable (orange curve).

One striking feature is the high number of deferred domain names in July 2023. This is in part due to one holder who had registered a large number of domain names but did not provide any identification.
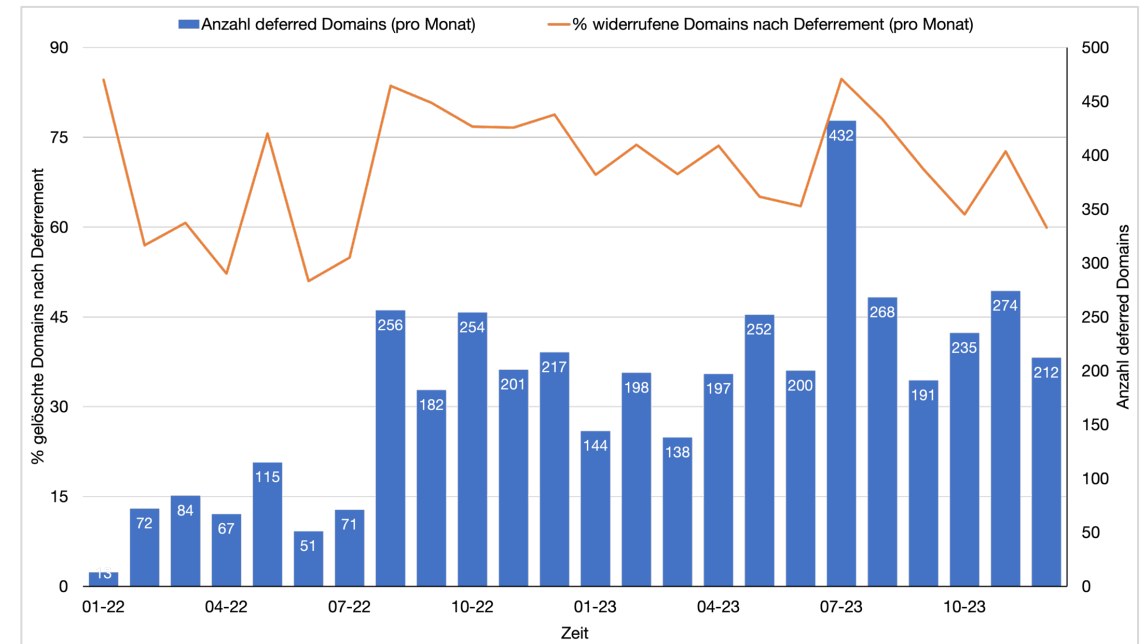
Dispute resolution

OFCOM has tasked Switch with providing an affordable dispute resolution service. Since 2004, Switch has been using the WIPO (World Intellectual Property Organization) dispute resolution service. WIPO operates an ICANN-accredited dispute resolution service for over 70 other registries.

In 2023, the experts made decisions on 16 .ch domain names. The expert decision is the final step in the process. A somewhat smaller number of cases are closed, for example, during arbitration or because proceedings are abandoned.

WIPO decision	2022	2023
Transfer to applicant	15	11
Complaint rejected	2	5
Number of decisions	**17**	**16**

WIPO decisions (as of February 2024)

|	Domain names
Transfer to applicant	diadora.ch immoswisslife.ch albi-keramik.ch albikeramik.ch migrosbankswitzerland.ch naturoflooring.ch dallmayer.ch tmhinternational.ch solidea.ch nortonabrasives.ch dermagora.ch
Complaint rejected	rockantenne.ch cheeze.ch schluessel-luzern.ch imageskincare.ch zoskinhealth.ch

Registrar developments

In 2018, considerably more Registrars than expected were added; by the end of the year, we recorded 122 Registrars.

In 2019, the number of Registrars rose to 131, and the registry had 137 Registrars at the end of 2020. In 2021, the number of Registrars increased by nine to a total of 146.

In 2022, 11 Registrars first signed a test contract for access to the test system. We switched these Registrars to the productive system once they had successfully completed the test phase and passed the test course. The total number of recognised Registrars therefore increased to 157.

In 2023 we were only able to give 1 more Registrar access to the productive system, increasing the number to 158.
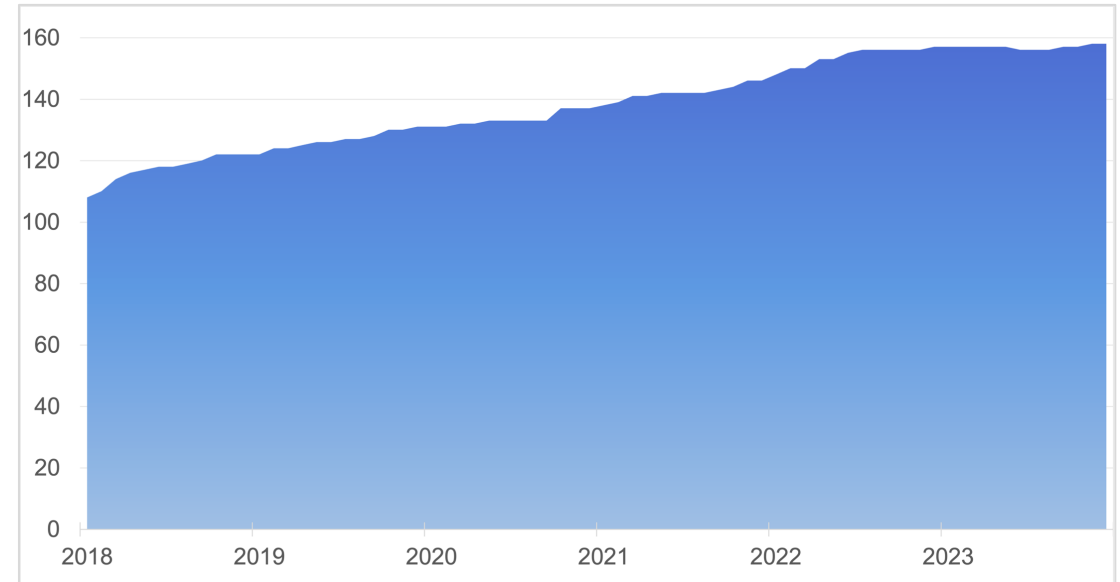
Name server performance

In terms of DNS performance measurement, Switch relies on the response time requirements for DNS queries stipulated by the ICANN Agreement: queries in the CH zone must be answered by at least one logical name server within 500 ms (UDP) or 1,500 ms (TCP).

In 2023, this requirement was met in each instance.

The measurements were carried out by RIPE and are publicly available.
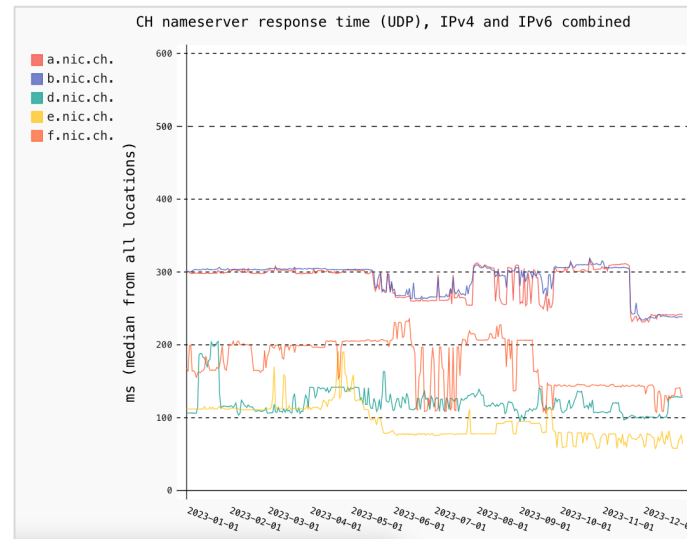https://atlas.ripe.net/dnsmon/group/ch

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

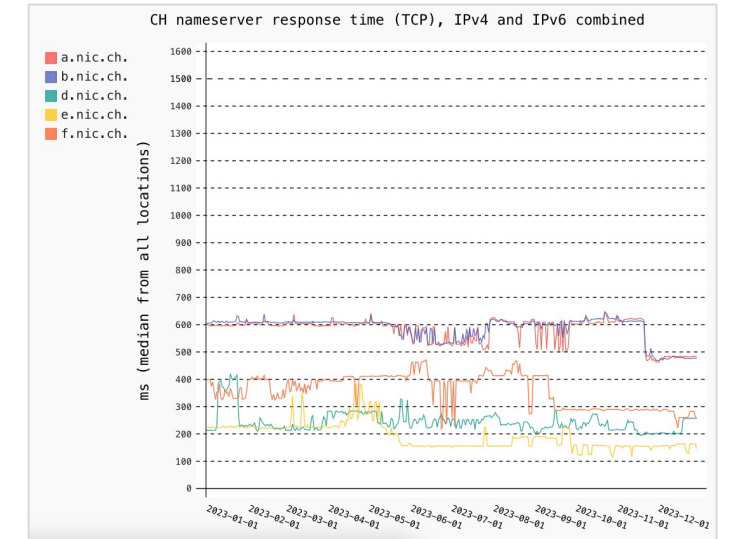**Anycast:** d.nic.ch, e.nic.ch, f.nic.ch

UDP response times
Combined response times
of IPv4 and IPv6

TCP response times
Combined response times
of IPv4 and IPv6

Cybercrime

Quantitative

In the reporting year, we captured and processed the following cases:

Number of malware and phishing cases 2023 quantitative view

	# malware cases	# phishing cases
Reports received	1,242	942
Suspicion confirmed	505	643
Number of blocked domain names	187	475
Reason for lifting block:		
- Statutory period expired	37	17
- Eliminated after block	119	34
- In progress on the cut-off date	4	12
Revoked domain names	27	419

Qualitative

The time spent on cases was:

Number of malware and phishing cases 2023 qualitative view

		Duration
Duration of blocking according to OID Art. 15 (1), (2), (3) max. blocking time 30 days (720 hours)	Min. time	0.50 h
	Average	103.32 h
	Max. time	160.05 h
Response time from Switch following notification	Average	8.15 h
Time until removal of threat after notifying the holders	Average	104.27 h

DNS Health Report

The DNS Health Report checks the accessibility of name servers and .ch and .li domain names. In the event of technical problems, Switch informs the operator and makes recommendations for resolving them. As such, the DNS Health Report improves the reliability of the internet in Switzerland. What is being checked:

- Name servers: The function of the name servers is being checked for compliance with the DNS standards.
- Domain names: It checks whether DNSSEC-signed domain names can be resolved using a validating recursive resolver.

Name server report

The error rate for the name server accessibility measurement has decreased only slightly but steadily since the beginning of the measurement. This trend is very satisfactory.
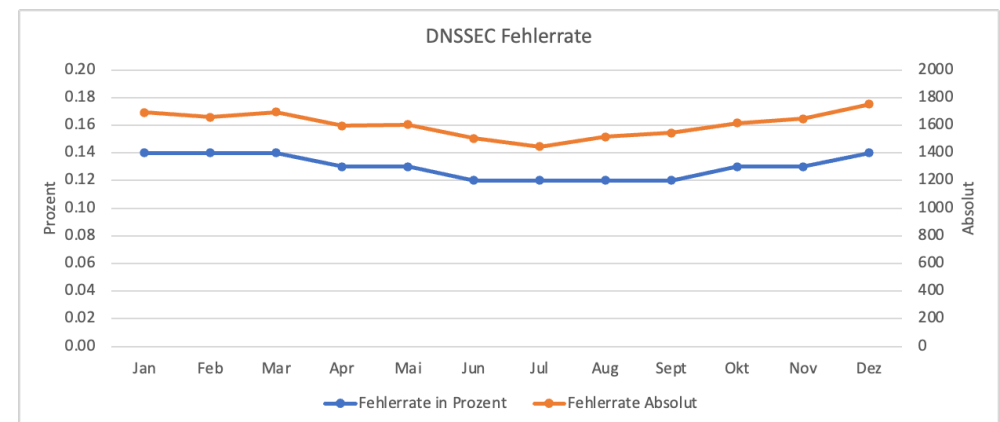
Domain name report

The error rate for the domain name accessibility measurement has plateaued. Most faulty domain names are parked domain names, where there is little motivation to correct the errors.

Error rate for name server accessibility measurement

Name-Server Fehlerrate
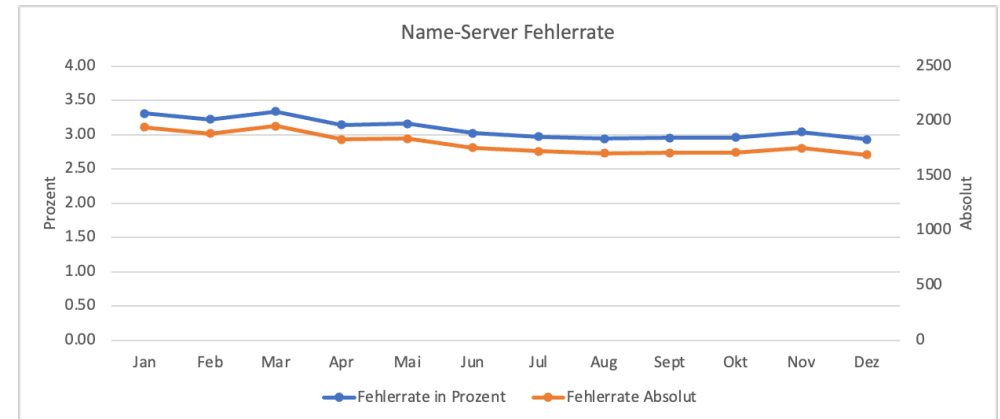
Error rate for domain name accessibility measurement

DNSSEC Fehlerrate

DAAR .ch
ICANN Domain Abuse Activity Reporting

With the publication of the .ch zone, Switch is taking part in ICANN's DAAR (Domain Abuse Activity Reporting) project. The project compares reports of suspected abuse in different TLDs.

The programme and the reports for ccTLDs are still at the beta stage. However, the figure already allows us to compare .ch and other ccTLDs and gTLDs.

What is being measured?

The proportion of .ch domain names (as %) identified as a security threat compared to the average number of domain names in other TLD zones. Detailed information is available from ICANN: https://www.icann.org/octo-ssr/daar

Analysis of .ch

The DAAR report reveals that domain name abuse is low for the .ch ccTLD compared to the average for all TLDs. This confirms the effectiveness of the ongoing measures aimed at combating cybercrime and the effective cooperative relationship with Swiss authorities and international organisations.

DAAR .li
ICANN Domain Abuse Activity Reporting

With the publication of the .li zone, Switch is taking part in ICANN's DAAR (Domain Abuse Activity Reporting) project. The project compares reports of suspected abuse in different TLDs.

The programme and the reports for ccTLDs are still at the beta stage. However, the graphic already allows us to compare .li and other ccTLDs and gTLDs.
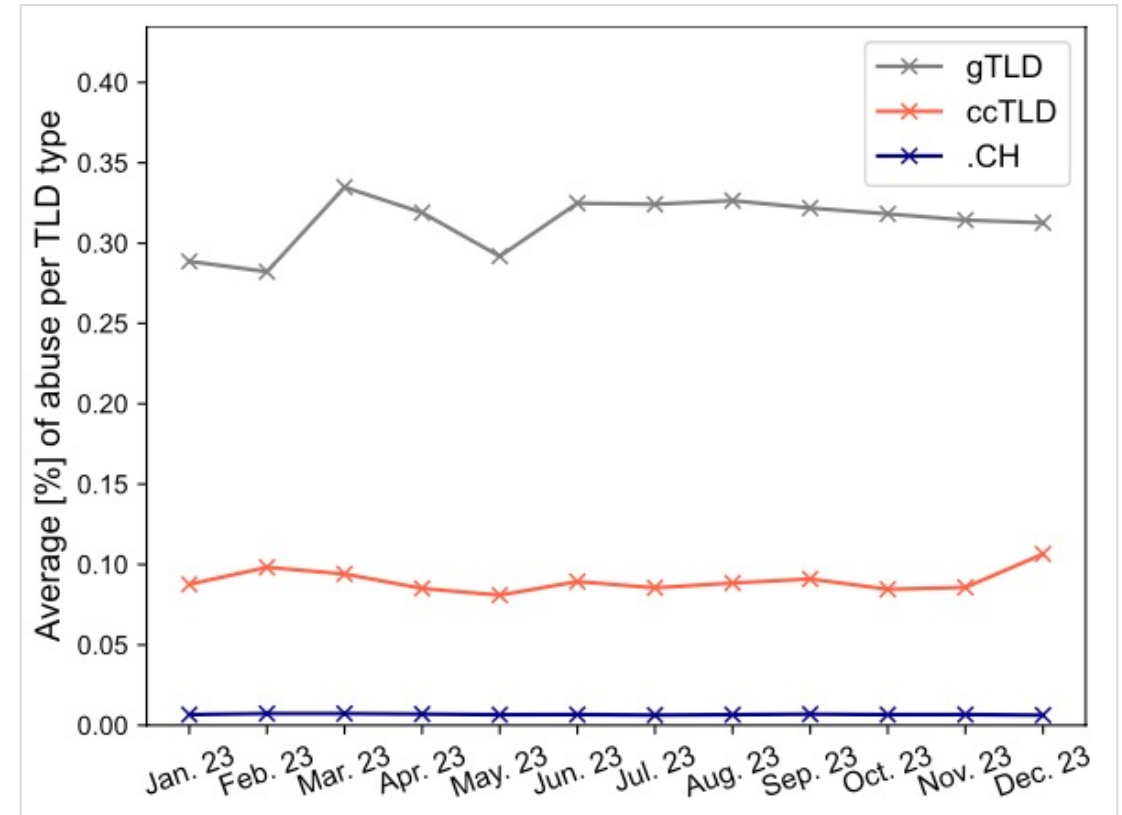
What is being measured?

The proportion of .li domain names (as %) identified as a security threat compared to the average number of domain names in other TLD zones. Detailed information is available from ICANN: https://www.icann.org/octo-ssr/daar

Analysis of .li

The DAAR report reveals that domain name abuse in the .li ccTLD has been eliminated except for nearly two dozen domain names. This low value can only be maintained if the cooperative relationship between the registry and the authorities remains as effective.
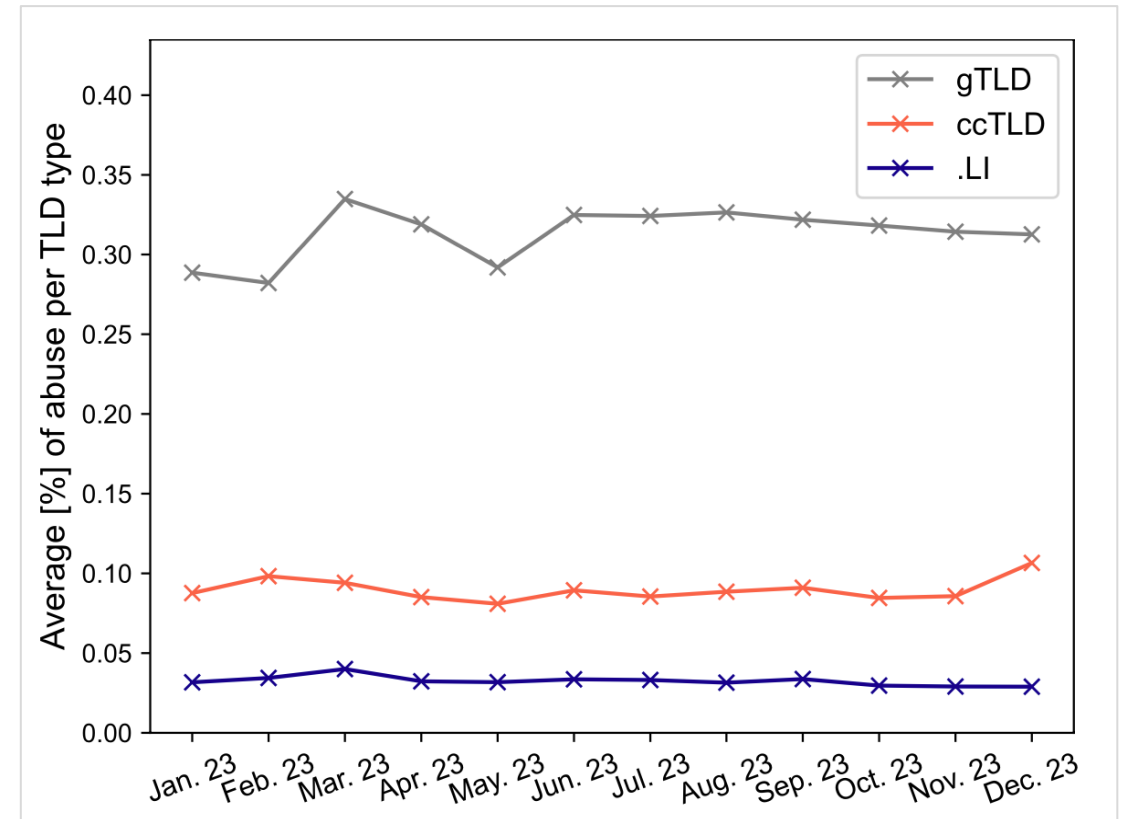
4.
Activity report – economic indicators

Switch_

Economic indicators

The Switch foundation's 2023 annual report will be approved along with the balance sheet and income statement at the Foundation Council session on 13 June 2024. Publication will take place from 14 June 2024.

No figures will be published at this point. Instead, interested parties will be referred to the comprehensive documents of the 2023 Switch Annual Report.

5.

Activity report – developments

Switch

Looking back at 2023

Change of DNSSEC algorithm

Initially, the NSEC3 algorithm (with opt-out) was selected for signing the zone file. This mechanism prevented 'zone walking' and thus made it difficult to automatically list all domain names – with the typical consequence of spam waves.

In the meantime, the zone file is public. The high signing rate of 50% requires more efficient methods, which is achieved by switching to the NSEC algorithm. Changing security parameters in the DNS requires detailed technical clarifications in advance. The operators of the name servers and resolvers are involved, the technical community of ICANN and DNS-OARC was also consulted. This gave the green light for the change. The change on 10 November 2023 did not affect the functioning of the name servers or resolvers. The zone file is slightly larger after the change, but the name servers and resolvers require fewer computing resources.

European TLD ISAC

The European TLD ISAC (Information Sharing and Analysis Centre) was launched in February 2023. The development phase is being supported by CENTR and seven ccTLD registries. Switch has representatives on the Board and has delegated an employee to develop the collaboration processes. The focus should be on the exchange of threat intelligence, which is why registries with a CERT and an ISMS are involved. It is expected to take two years to establish the core processes and expand to all ccTLD registries in the EU. The European TLD ISAC is financed entirely by the participating registries.

Looking back at 2023

Increased e-mail security

As part of the DNS resilience programme, it was determined together with OFCOM and the Registrars that the implementation of DMARC and SPF would be the criterion for refund in 2024. With this in mind, Switch set up the measurement infrastructure and a dashboard for manual verification of the measurement criteria in 2023.

DANE has been defined as the criterion for 2025. Switch offered training courses on this topic in Lausanne and Zurich in October 2023.

As a result, Switch's internal e-mail infrastructure has also been reorganised so that all three security protocols can be used for sending and for verification on receipt.

RDAP web front end for authorities

The web frontend to the RDDS database (Whois) is now in operation. Every user at an authority signs a contract for use, and Switch manages the rights of use. So far, only a few smaller authorities are using this convenient method of access, but this is exactly the type of authority for which the web frontend is designed.

Strategic outlook and goals

All our confirmed upcoming projects are outlined under 'Planned innovations 2024'. The Domain Abuse 4.0 project, which we have already explored earlier, will be our main focus for 2024. This section will cover two focus areas that are more strategic.

Location of infrastructure

Over the last five to eight years, large organisations have been shifting their IT infrastructure to hyperscalers in the cloud to consolidate infrastructure and save costs. The move by SMEs came slightly later, in part due to pressure from software providers such as Microsoft, who no longer guarantee the on-premise operation of their software in the long term.

Switch's IT infrastructure is spread over several locations, which are connected by a self-operated fibre-optic infrastructure. This ensures maximum control over all layers of the IT components.

Working with a Swiss cloud provider means that Switch is able to build new computing and storage components in professional data centres. These data centres offer a higher level of reliability and access control than the previous locations in universities. These data centres are also connected to the 'Switch LAN' fibre-optic network.

In the course of 2024 and 2025, the registry's software components will be converted to a new architecture and operated at the new locations. This solution gives Switch full governance over the infrastructure and the stored data and the infrastructure is still located in Switzerland. These are important preconditions for the operation of a critical infrastructure and for data processing in the midst of the fight against cybercrime.

Strategic outlook and goals

DNS resilience programme in 2027 and beyond

The DNS resilience programme is part of the renewal agreement with OFCOM for 2022 to 2026. The DNSSEC Advisory Board determines which security protocols should be promoted by the resilience programme. OFCOM, Swico IG Hosting and Switch each has one representative on the Board. The criteria are determined two years in advance. This enables Switch to offer training and prepare the measurement infrastructure, and gives Registrars sufficient time to plan the technical work for any changes before the measurements begin.

A potential extension of the programme beyond 2026 and what this could look like will be discussed in 2024. The current programme already provides important guidance and experience on this, but it is still advisable to bring the relevant parties together to discuss it.

Planned innovations 2024

DNS resilience programme: DANE measurements

DANE was established as the criterion for the 2025 refunds, and Switch is expanding the measurement infrastructure accordingly. The dashboard will also be extended to allow Registrars and hosts to check whether they have implemented the configuration correctly according to Switch's recommendations.

The criterion for 2026 will be IPv6. There will be no specific training for this.

Domain Abuse 4.0

The Domain Abuse 4.0 project secures the future of the registry's fight against cybercrime. A description of the project can be found on page 23.

ISMS ISO 27001:2022

Previously, ISO 27001:2013 was the standard used for auditing the registry. The revised 2022 version of the standard takes into account a broader range of topics geared towards technological and social requirements.

Switch intends to adapt all relevant processes and documentation for certification to the new version by autumn 2024. Switch benefits from the fact that many of the new requirements stipulated by the standard have already been in place for years, for example, threat intelligence through CERT or its own security solutions such as the DNS firewall. The independent certification demonstrates that Switch has successfully and effectively implemented an information security management system. This ensures that Switch also fulfils its tasks for the operation of critical infrastructures and for the protection of personal data in line with the DSG and ISG.

Planned innovations 2024

Web crawler for the registry

To combat malware and phishing, the registry relies on notifications from specialist bodies. Until the end of 2023, the NCSC operated a web crawler that queried the web servers in the .ch zone individually and analysed the responses for suspicious patterns. In the event of suspected malware and phishing, the NCSC reported the information to Switch. We used our tools to investigate the sites and, if the suspicions were confirmed, triggered the appropriate processes to either remove the web pages or remove the malicious code.

Following the discontinuation of the NCSC crawler, the registry was lacking an important tool in the fight against cybercrime. This led Switch to develop its own crawler for the .ch and .li zones in late autumn. Switch has the necessary commercial and information sources for the patterns, without which the crawler would be useless.

Commissioning is planned as soon as possible, ideally as early as January or February 2024.
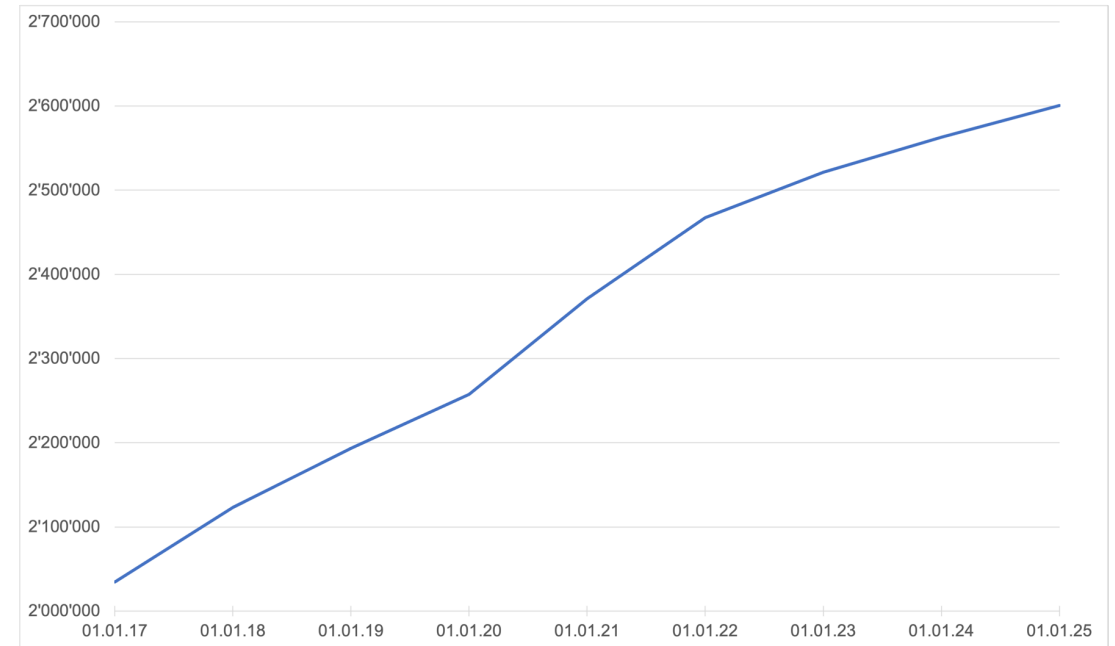
Growth forecast for .ch domain names

2018 and 2019 showed a slightly smaller increase year-on-year. In 2020, the pandemic-related surge in digitalisation and the marketing initiatives of web hosting companies led to increased demand and growth of 4.8%. The increase had already fallen to 3.9% in 2021, but was still higher than before the pandemic.

In 2022, the registry recorded growth of 2.1%. The surge in digitalisation lasted two years and resulted in an unexpected increase of around 100,000 domain names.

In 2023, the growth was just over 40,000 domain names. This corresponds to 1.6%, which falls short of our forecast of 1.8%.

Globally we are seeing market saturation and slowed growth in domain names. Our forecast for 2024 projects an increase of 1.45%.

Switch_