

# *REPORT 2019*

of the .ch Registry

**SWITCH**



<b>Management summary – highlights</b>	
Creating security	3
<b>Activity report – operations</b>	
Battling cybercrime	4
Dealing with cases of suspected abuse	5
DNSSEC Day	6
Swiss DNSSEC Pioneer Award	7
Security awareness	8
Swiss Web Security Day	10
Domain pulse	11
Registry operations	12
ISMS Surveillance Audit	13
<b>Activity report – innovations</b>	
Registry Lock	14
DNS Health Check	15
<b>Activity report – statistical indicators</b>	
Domain name inventory 2019	16
Market share of .ch and .li	17
DNSSEC developments	18
DNSSEC validation in Switzerland	20
Dispute resolution	21
Registrar developments	22
Name server performance	23
Cybercrime	24
<b>Activity report – economic indicators</b>	
Economic indicators 2019	25
<b>Activity report – planned developments</b>	
Orientation and goals 2020	26
Planned innovations 2020	28
Growth forecast 2020	29



**Urs Eppenberger**  
Head of Registry, SWITCH  
(photo SWITCH)

# Creating security

By raising awareness and recognising dangers

Companies and private individuals identify strongly with their domain names. It reserves them a place on the internet and secures their identity in the digital world. The price of this identity is secondary, as long as it – like .ch – remains under a certain threshold.

Many internet users require a bundle of email and web hosting. Some will want to protect their brand with all relevant top-level domains. And then others only need one domain name.

Interested parties will find offers tailored to their needs at around 130 registrars. The low price of .ch domain names stimulates the market and enables growth for everyone at well above the European average.

But the other side of the coin is that cybercrime follows the same economic rules. Low prices and an open registration policy also attract criminal enterprise.

Working with law enforcement agencies and registrars, the registry is an important hub in the fight against cybercrime.

SWITCH-CERT, the registry's Computer Emergency Response Team, collects and analyses information from its own sources and from its specialist contacts nationally and internationally. SWITCH-CERT also monitors the usage of secure communications protocols as an indicator of the robustness of the entire system.

One activity that is becoming increasingly important focuses on people as users. Our expert for security awareness on the internet teaches responsible handling of own data as well as a healthy understanding of dangers, in intensive cooperation with committees and associations.

It remains our goal to continuously increase the security and stability of the internet in Switzerland. That's our commitment.

# Battling cybercrime

In 2019, we continued our measures to combat cybercrime.

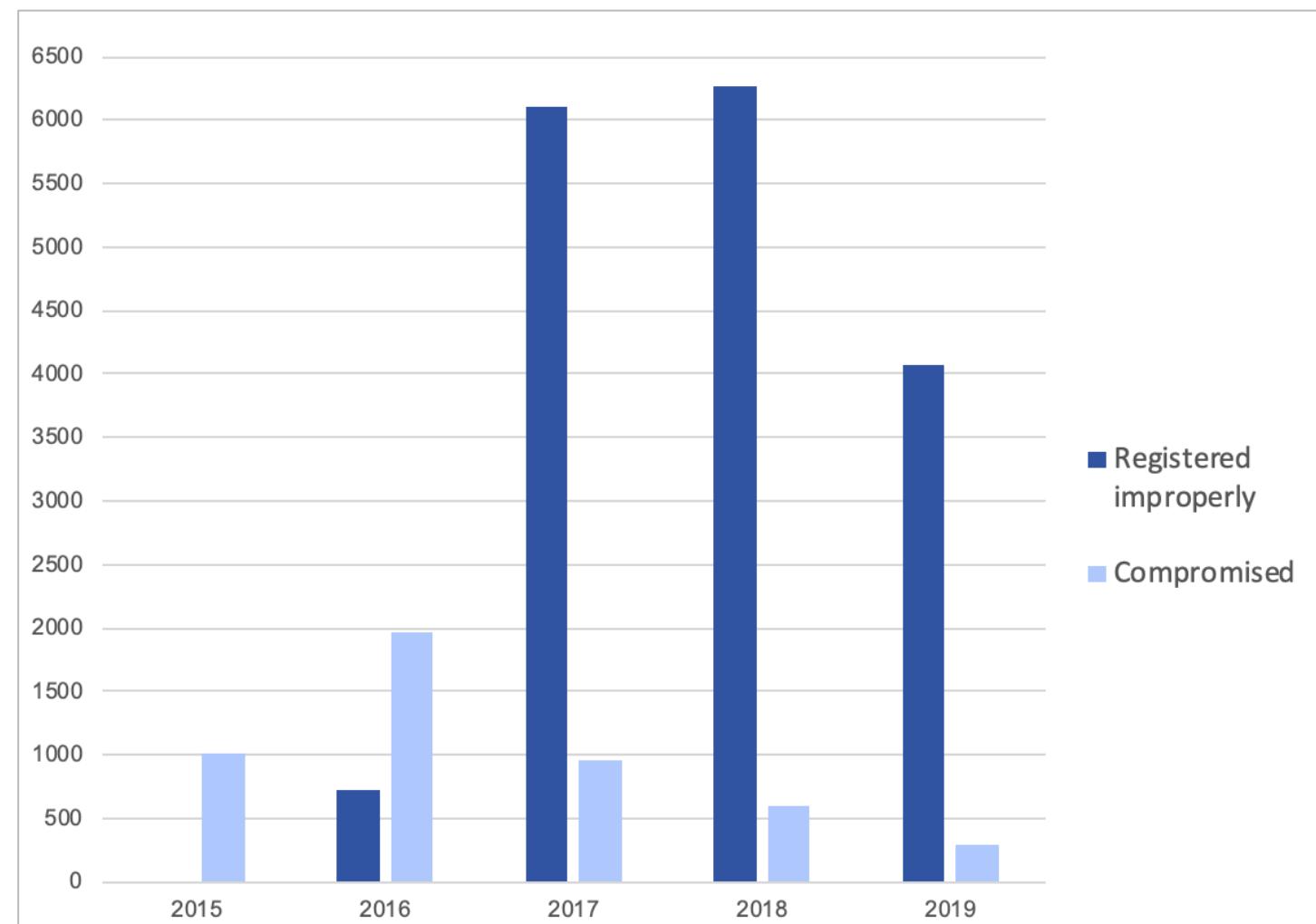
## PHISHING AND FRAUDULENT WEBSHOPS

The number of compromised websites continued to decrease. The number of improperly registered domain names has decreased slightly for the first time after a sharp increase in the past two years. This is largely due to cooperation with the cybercrime division of the Zurich Cantonal Police. The process of identifying improper registrations has been further improved, automated and accelerated.

## DRIVE-BY/MALWARE

The use of drive-by and malware has further declined since the previous year.

Webpage: <https://www.switch.ch/saferinternet>



→ Statistical indicators on the battle against cybercrime can be found on page 24.

# Dealing with cases of suspected abuse

---

## REQUESTS FROM RECOGNISED AUTHORITIES – OID 15.1

In 2019, the two accredited authorities, MELANI and the Zurich Cantonal Police Force, submitted 1,492 requests for immediate blocking of domain names (technical/administrative) under OID Art. 15.1. All but one of these requests related to Art. 15.1a ‘Phishing’.

Requests	Consequences	2019
Not answered	Domain names deleted	1,492
Answered	Domain names reactivated	0
<b>Total</b>		<b>1,492</b>

## ADMINISTRATIVE ASSISTANCE – OID 16.3

At the request of intervening Swiss authorities acting within their areas of responsibility, 2,507 requests were submitted for Swiss correspondence addresses under OID Art. 16.3.

Requests	Consequences	2019
Not answered	Domain names deleted	2,400
Answered	Domain names reactivated	107
<b>Total</b>		<b>2,507</b>

# DNSSEC Day

On 21 November 2019, SWITCH held its DNSSEC Day at PH Zurich. The distinguished panel, moderated by Markus Kummer (ISOC-CH), was composed of the three national councillors Balthasar Glättli (GPS), Marcel Dobler (FDP) and Judith Bellaiche (GLP, Swico), OFCOM director Philipp Metzger, Lorenz Inglin from Swisscom as well as the two speakers Michael Hausding (SWITCH) and Michiel Henneke (SIDN).

To coincide with DNSSEC Day, SWITCH published a webpage on the issue of DNSSEC.

The webpage contains readily comprehensible information on DNSSEC for a broad audience, a flyer with information to download as well as a short awareness video. The aim of this video is to generate more attention and interest in the topic on the website as well as on social media channels.

Webpage: <https://www.switch.ch/dnssec>



*Panel discussion with Markus Kummer, Marcel Dobler, Judith Bellaiche, Balthasar Glättli, Michael Hausding, Lorenz Inglin, Philipp Metzger, Michiel Henneke (l. to r.)*

# Swiss DNSSEC Pioneer Award

The Swiss DNSSEC Pioneer Award is given to organisations and individuals that offer outstanding services related to the implementation and promotion of DNSSEC, and thereby make the Swiss internet safer.

This year's award went to Swisscom and Firestorm.

As Switzerland's largest ISP, Swisscom has activated DNSSEC validation for all its customers, bringing Switzerland to a validation rate of 65%. Firestorm was the first registrar to sign its entire portfolio of .ch domain names.

The award ceremony took place on DNSSEC Day, 21 November 2019.

*SWITCH presents Roger Kunz (left) and Christian Geissler (centre) from Firestorm with the Swiss DNSSEC Pioneer Award 2019*

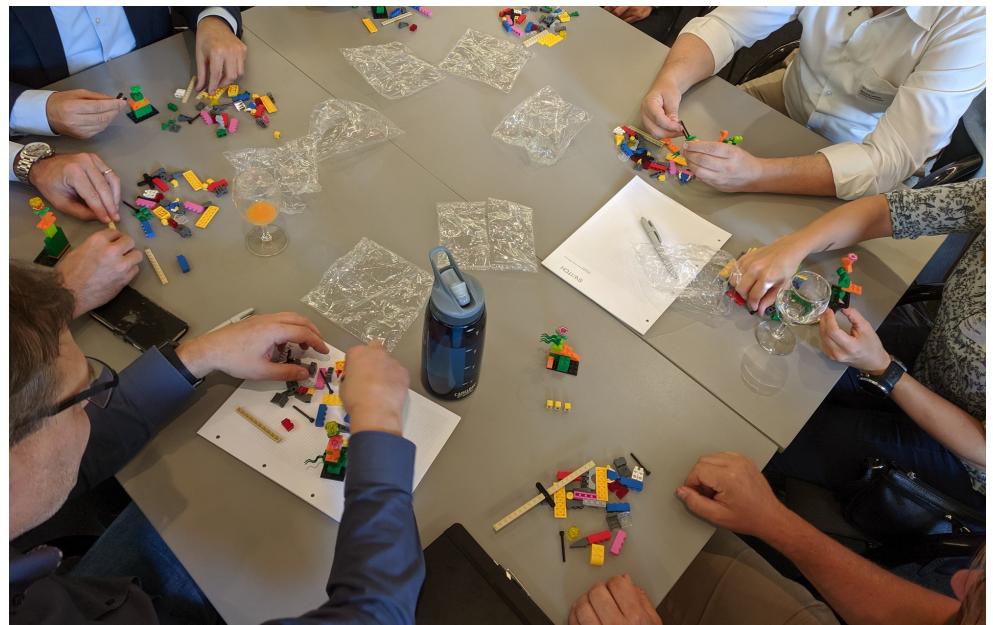


*Martin Wismer from Swisscom also received the Swiss DNSSEC Pioneer Award 2019*

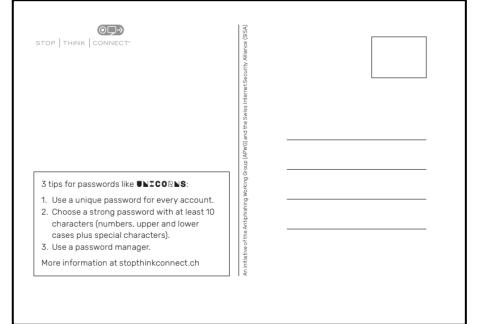
# Security awareness

## SECURITY AWARENESS DAY

On 1 October 2019, SWITCH hosted its second Security Awareness Day in Bern. Once again, the purpose of this year's programme was to heighten awareness for security-related issues in the SWITCH community while also sharing ideas and encouraging communication and interaction. A total of 46 representatives from universities and hosting providers/registrars took part.



*Improving the security awareness concept:  
Lego Serious Play Workshop on Security Awareness Day*



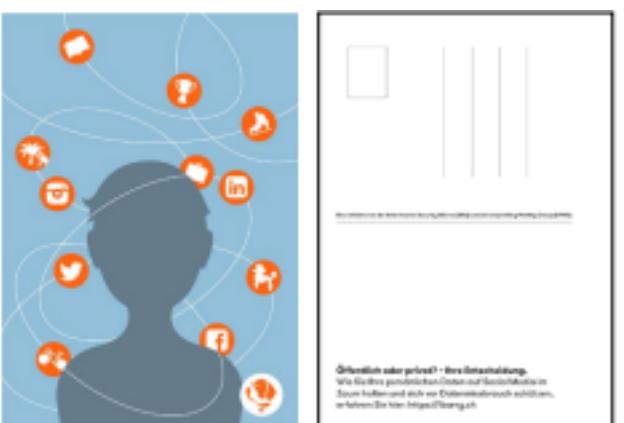
## iBARRY

Since July 2019, SISA has been presenting itself to the Swiss population under the name 'iBarry'.

In cooperation with SISA, SWITCH launched campaigns on internet security as part of World Password Day (May) and European Cybersecurity Month (October).

Postcards and stickers on the topics of password security and data protection in four languages (German, French, Italian, English) were issued, accompanied by readily comprehensible information on [www.ibarry.ch](http://www.ibarry.ch).

Recipients of the stickers and postcards included universities and OFCOM, as well as over 50 registrars.



# Security awareness

## SWITCH EXPERTS – THE STATE OF SECURITY OF THE SWISS INTERNET

On 5 February 2019, SWITCH hosted the ‘SWITCH Experts’ information event. The topic was the state of security of the Swiss internet.

Twelve media representatives from the Zurich region attended the event, including the SRF Tagesschau, NZZ, NZZ Folio, Inside-IT, Netzwoche, Computerworld, Swiss IT Magazine, Finanz & Wirtschaft, AWP Finanznachrichten (Cash), 20 Minuten and nau.ch.

We provided the assembled representatives of the press with an up-to-date picture of where we are in the battle against cybercrime and the state of security of the Swiss internet.

Webpage: [Netzwoche report \(in German\)](#)

## SECURITY HACKATHON

SWITCH-CERT hosted the annual Security Tools Hackathon from 13 to 15 August 2019. This saw 20 participants from universities as well as private companies both domestic and international working on a wide range of security-related projects.

For awareness purposes, a tabletop game was developed which was intended to teach players about secure behaviour on the internet.

On the technical side, the event looked at issues such as enrichment of passive DNS data, clusters of websites for automated detection of fraudulent webshops, and rapid scanning of large networks with the goal of efficiently documenting non-patched servers.

# Swiss Web Security Day

On 30 October 2019, SWITCH organised the third Swiss Web Security Day in collaboration with Swico and SISA. The goal of the meeting was to raise awareness of security issues.

The event took place in Bern with 80 attendees from various industries – web hosting providers, registrars as well as representatives of associations, telcos, banks and authorities. Welcoming the participants was the federal Cybersecurity Delegate Florian Schütz.

The Swiss hosting and security community as well as international guests gave talks on various topics ranging from web security in the (Tor) browser through to self-regulation with the code of conduct for hosting providers.

The Swiss Web Security Day will also be held next year.



Daniel Nussbaumer from the Zurich Cantonal Police and SISA welcomes attendees to the Swiss Web Security Day

# Domain pulse

'Domain pulse' took place on 18 and 19 February 2019 in Bern's townhall. The forum on themes and trends around domain names and the internet has very much established itself as an industry fixture, and the 16th event saw around 250 participants from Switzerland, Germany and Austria take part.

At the heart of the event were issues like internet governance, internet security, digital identities and e-voting in Switzerland. Among the extensive feedback from participants was plenty of praise for the interesting programme, the highly appropriate location as well as the many opportunities to exchange views.



# Registry operations

## AVAILABILITY – STABILITY – SECURITY

The main focal points for the operation of the registry are availability, stability and security for our registrars and their domain name holders.

SWITCH can also look back on a successful year of operations of critical infrastructure for the top-level domain .ch. We have achieved stable operations and high availability throughout the entire year.

The challenges in the area of security remain, and working with our CERT team and through successful collaboration with the authorities we were able to guarantee secure operations.

## SIGNATURE FOR .CH ZONE

The key signing ceremony for the .ch domain took place on 21 October 2019. Further details can be found in the minutes prepared for OFCOM.

## REGISTRY OUTAGE

On 17 May 2019, the registration system went down for 13 minutes. The reason was a software error in the EPP back-end server. Rebooting the system resolved the problem.

On 23 September 2019, the registration system went down for 29 minutes. Following planned maintenance work at the backup location, full redundancy was meant to be re-established. A faulty manipulation unfortunately had an impact on the production system, leading to the outage.

On 26 February 2019, our email provider had problems with forwarding emails for around five hours. This led to delays of up to several hours which affected incoming and outgoing emails. No requests were lost as far as we were informed. Registrars were able to contact us by telephone at all times and there was no negative impact on registry operations.

# ISMS

## Surveillance Audit

An annual audit is performed to verify ISMS certification in accordance with ISO 27001. In 2019, the audit was conducted in the form of a one-day surveillance audit on the premises of SWITCH. The improvements introduced throughout the year were also presented. The audit took a deeper look at individual topics, such as the new Registry Lock security function.

The results from the audit are documented in an audit report: No deficiencies were identified.

One area for improvement was identified: additionally to the standard controls, custom controls can be defined.

### Pflichten der Zertifizierungsstelle

Die Zertifizierungsstelle ist insbesondere verpflichtet ihre Akkreditierung aufrecht zu halten, die Audits zu den vereinbarten Fristen durchzuführen sowie die Unbefangenheit bei den Audits sicher zu stellen. Des Weiteren ist die Zertifizierungsstelle verpflichtet, die Änderungen in den Normanforderungen zu verfolgen und die Einwände und Beschwerden des Auftraggebers oder Dritten innerhalb den angemessenen Fristen zu lösen.

### Bereitstellung des Berichts an Dritte

Dieser Auditbericht trägt die Auditergebnisse zusammen. Der Auditbericht wird dem Kunden in elektronischer Form per E-Mail zugesendet, eine Kopie wird bei LL-C (Certification) aufbewahrt. Der Kunde ist verpflichtet den Dritten nur den vollständigen Auditbericht zukommen zu lassen. Der Inhalt des Auditberichts und dessen Aufzeichnungen, sind vertraulich zu behandeln. An Dritte, mit Ausnahme der Akkreditierungsorgane, kann er nur mit einer Genehmigung der Organisation übergeben werden.

### Report provision to third parties

Dieser Bericht fasst die Ergebnisse der Prüfung zusammen. Der Bericht wird dem Kunden zur Verfügung gestellt, eine Kopie in elektronischer Form wird bei der LL-C (Certification) hinterlegt. Der Kunde ist berechtigt, Dritten nur den vollständigen Bericht vorzulegen. Der Inhalt dieses Berichts und alle Prüfungsunterlagen werden als vertraulich betrachtet. Der Inhalt dieses Berichts und alle Prüfungsunterlagen werden als vertraulich betrachtet. Die Berichte dürfen Dritten nur mit Zustimmung des Kunden vorgelegt werden, ohne diese Genehmigung nur wenn die Akkreditierungsstelle und die Eigentümer privater Systeme dies verlangen.

### Schlussbestimmung

Das Auditziel wurde erreicht. Die Organisation hat nachgewiesen, dass die Anforderungen sowie internen Vorgaben erfüllt worden sind.

**Ich empfehle, unter Berücksichtigung der Auditergebnisse, die Aufrechterhaltung des Zertifikat für die Konformität des Managementsystems und den Normanforderungen ISO 27001 für den Bereich Domain Namen Registrierung**

LL-C (Certification) Peter Erwin

**LL-C (Certification) Czech Republic a.s.**  
Pobřežní 620/3 186 00  
Reg. No. 27118339



**ISO 27001**  
Surveillance Audit Report

LL-C (Certification)

[www.ll-c.info](http://www.ll-c.info)

# Registry Lock

The ‘Registry Lock’ security function announced last year was introduced in November 2019. With this, SWITCH is further consolidating the foundation of internet security in Switzerland.

Registry Lock offers protection against unintended or malicious changes to domain names. If Registry Lock is enabled for a domain name, it can no longer be changed in the normal way, the registrar-registry interface EPP.

In recent years there has been an increasing number of ‘domain hijacking’ cases, in which attacks unlawfully take over domain names and misdirect data traffic to their own servers. Enabling Registry Lock can effectively prevent some of the possible attack variants for domain hijacking.

Registry Lock is primarily designed for domain names of business-critical websites. It protects both the registrars and holders against hijacking and other improper or inadvertent changes to domain names.



Christian Kölle from SWITCH presents the Registry Lock at the Swiss Web Security Day 2019 in Bern

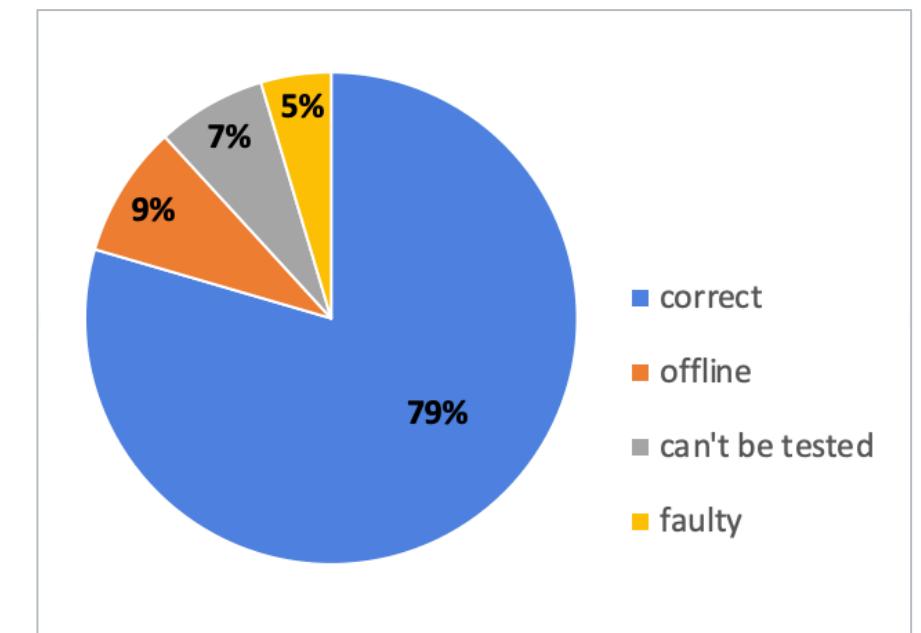
# DNS Health Check

## Checking name-server and DNSSEC configurations

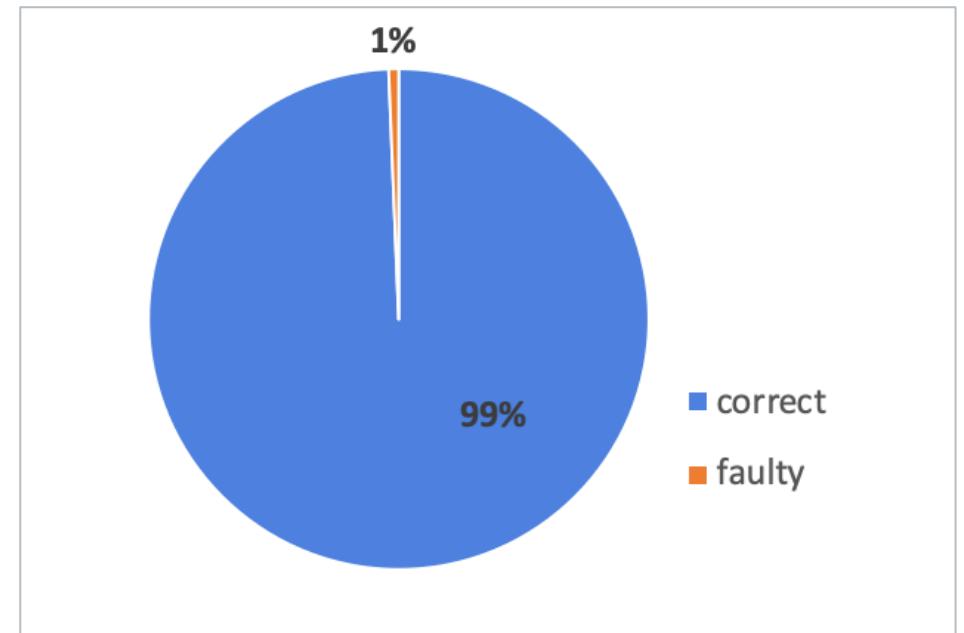
SWITCH assigns domain names, regardless of whether the domain name is merely reserved or whether it can actually be used via assigned name servers. The configuration of the name servers is up to the registrars or hosting providers. The DNS is very stable and will usually even work with a sub-optimal configuration.

To secure and improve the accessibility of .ch and .li domain names, we are introducing a 'DNS Health Check' for name servers as well as DNSSEC-signed domain names. The goal is to detect incorrect configurations and report them to the name server operator as well as the technical contact of a DNSSEC-signed domain name.

With the name server check, we aim to ensure that all name servers assigned to a domain name fulfil selected criteria which are key to accessibility. According to current data, 5% of name servers do not fulfil these criteria. Almost 1% of DNSSEC-signed domain names are incorrect. SWITCH will be introducing notification for operators and technical contacts in stages throughout 2020.



*Name servers of .ch and .li domain names*



*DNSSEC-signed domain names*

# Domain name inventory

## Developments 2019

### DEVELOPMENT OF .CH

The inventory of .ch domain names increased by a good 65,000 within a year.

	2018	2019
New registrations	274,720	299,440
Deletions	227,969	257,897
Reactivations*	23,031	30,373
Domain inventory as at 31/12	2,193,164	2,257,527

### DOMAIN NAME INVENTORY

Development of the domain name inventory for .ch and .li

\* Deleted domain names which were reactivated by the registrar within the 40-day transition period

### DEVELOPMENT OF .LI

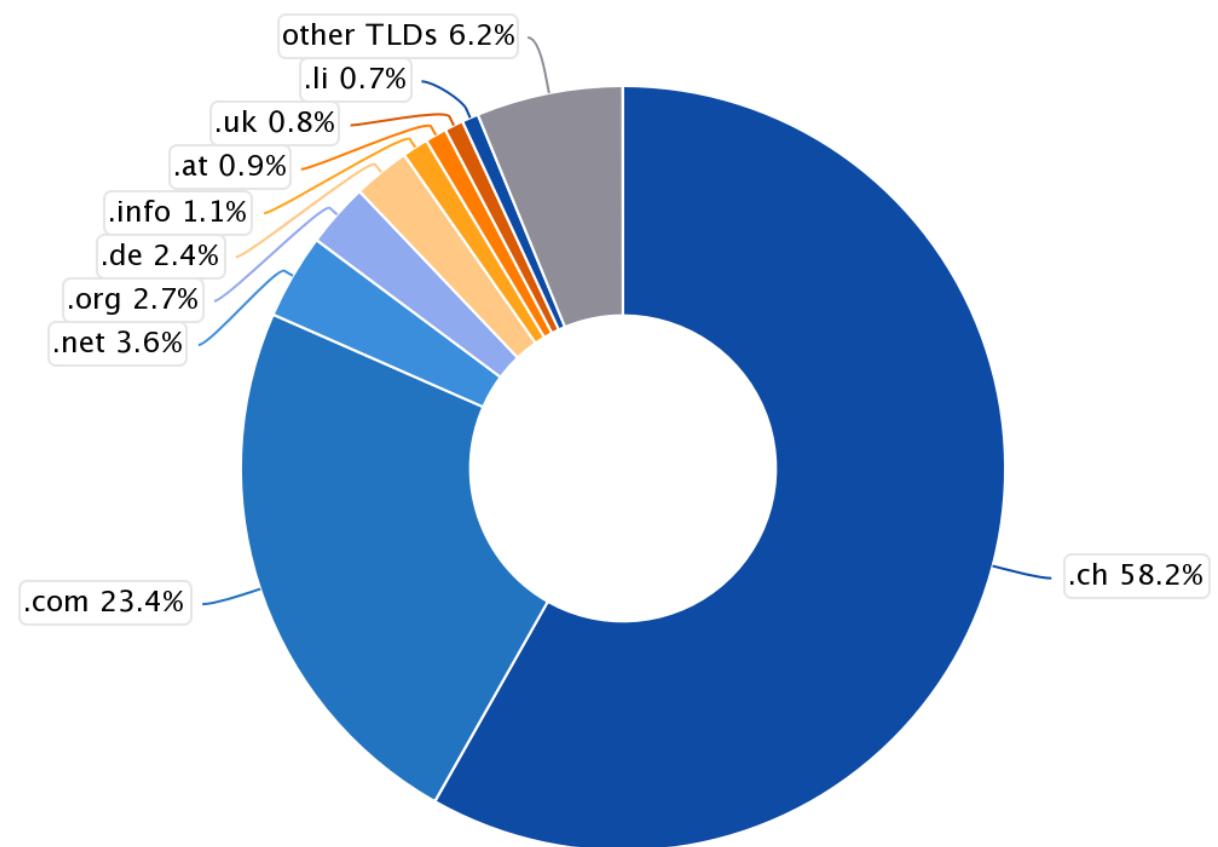
The inventory of .li domain names increased by almost 1,000 within a year.

	2018	2019
New registrations	8,812	8,588
Deletions	8,412	8,379
Reactivations*	484	813
Domain inventory as at 31/12	63,473	64,497

# Market share

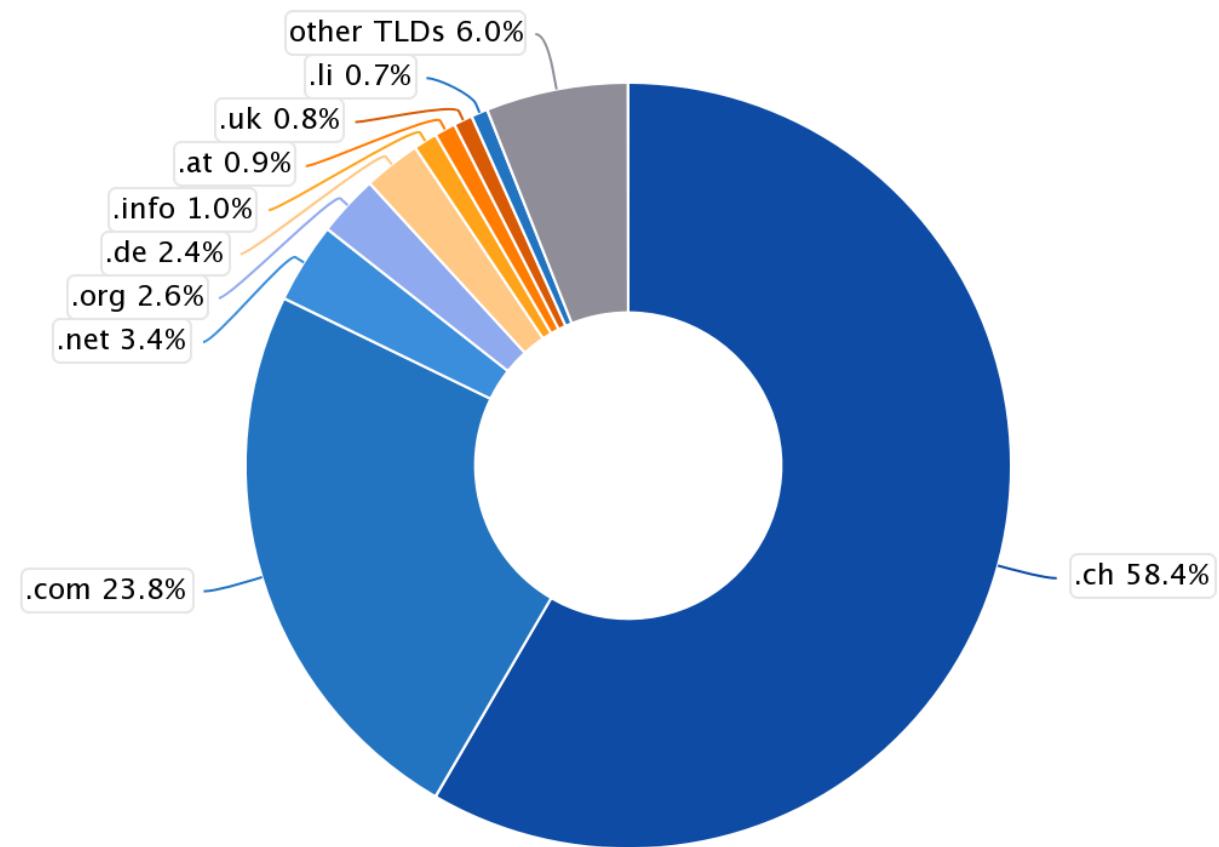
## of .ch and .li among Swiss domain name holders

The market share of the TLD (top-level domain) .ch among holders in Switzerland remained nearly unchanged from January 2019 to January 2020.



**MARKET SHARES JANUARY 2019**  
of various TLDs among domain name  
holders in Switzerland  
Source: CENTR

Little has changed in market share for the old generic TLDs .com/.net/.org; the same is true for .li domain names.



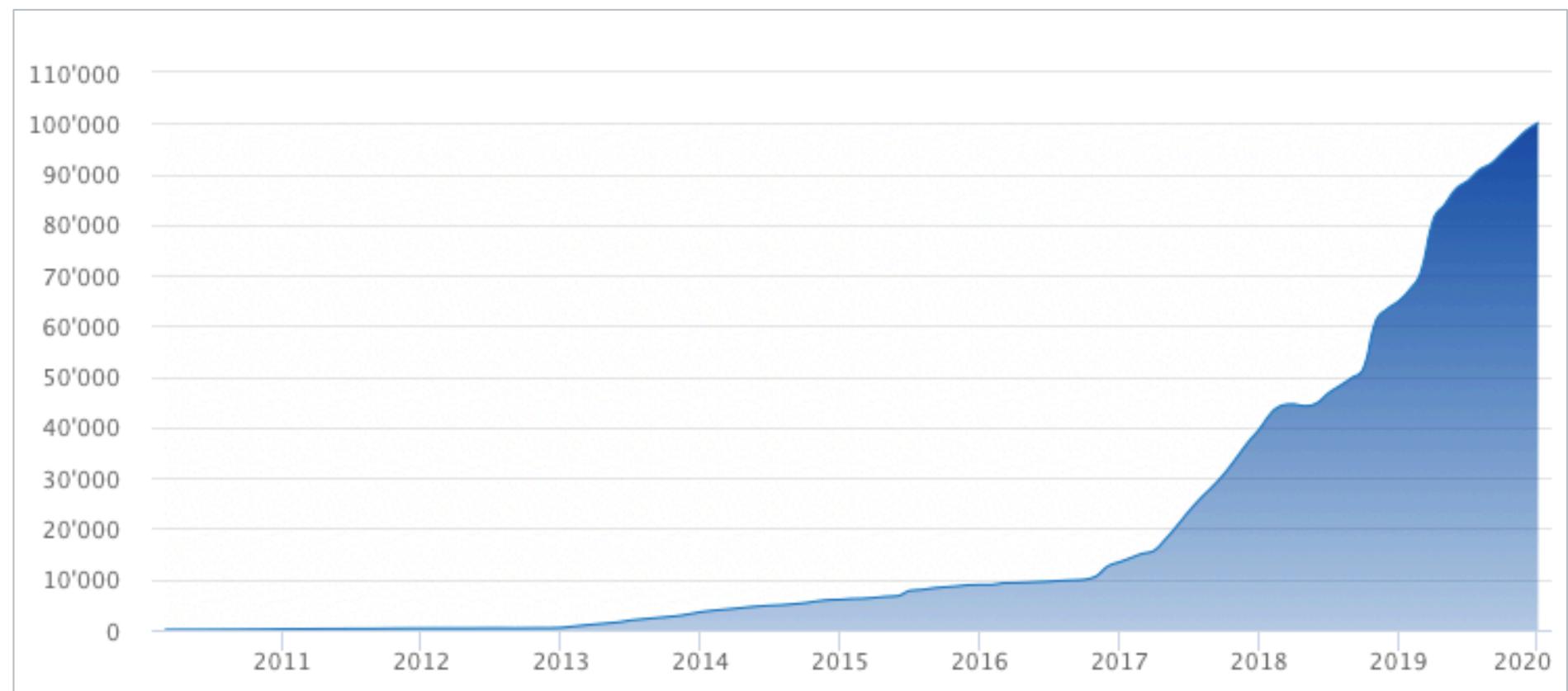
**MARKET SHARES JANUARY 2020**  
of various TLDs among domain name  
holders in Switzerland  
Source: CENTR

# DNSSEC developments

## Number of signed domain names

The introduction of ‘Automated DNSSEC Provisioning’ in 2018 (RFC 8078) has also made the activation of DNSSEC easier for hosting providers that do not also function as recognised registrars.

The number of .ch domain names signed with DNSSEC increased to 100,000 by the close of 2019. This is equivalent to 4.8% of all .ch domain names, compared to 3.0% for the previous year.



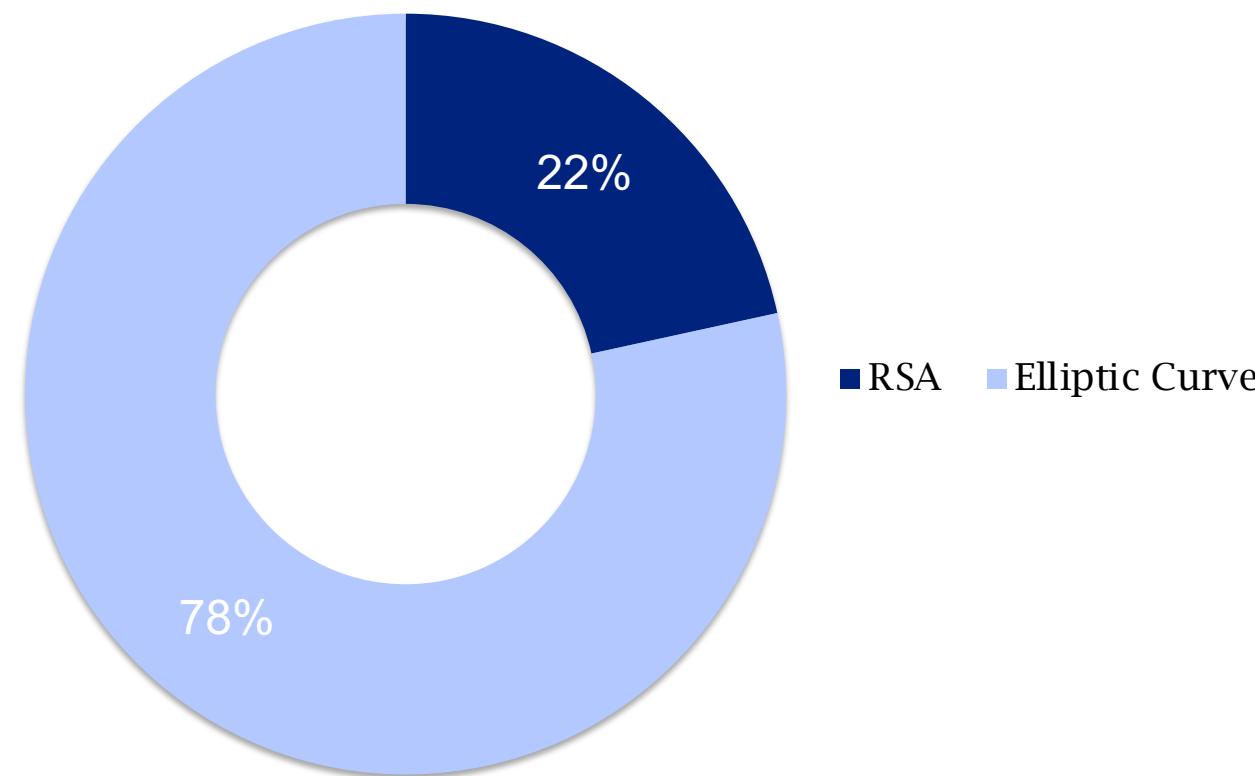
**DNSSEC**

*Number of .ch domain names  
signed with DNSSEC*

# DNSSEC developments

## Distribution of DS algorithms

Almost 80% of the .ch domain names signed with DNSSEC use modern ECDSA signatures (elliptic curve). The percentage increased by 10% compared to the previous year, with 22% being traditional RSA signatures.



Percentage of DNSSEC algorithms

DNSSEC algorithm	Number	Percentage
5 – RSASHA1	218	0.22%
7 – RSASHA1-NSEC3-SHA1	10,669	10.60 %
8 – RSASHA256	10,781	10.71%
10 – RSASHA512	65	0.06 %
13 – ECDSAP256SHA256	78,930	78.39 %
14 – ECDSAP384SHA384	23	0.02 %
15 – ED25519	7	0.01 %
16 – ED448	1	0.00 %

DNSSEC signatures used

# DNSSEC validation

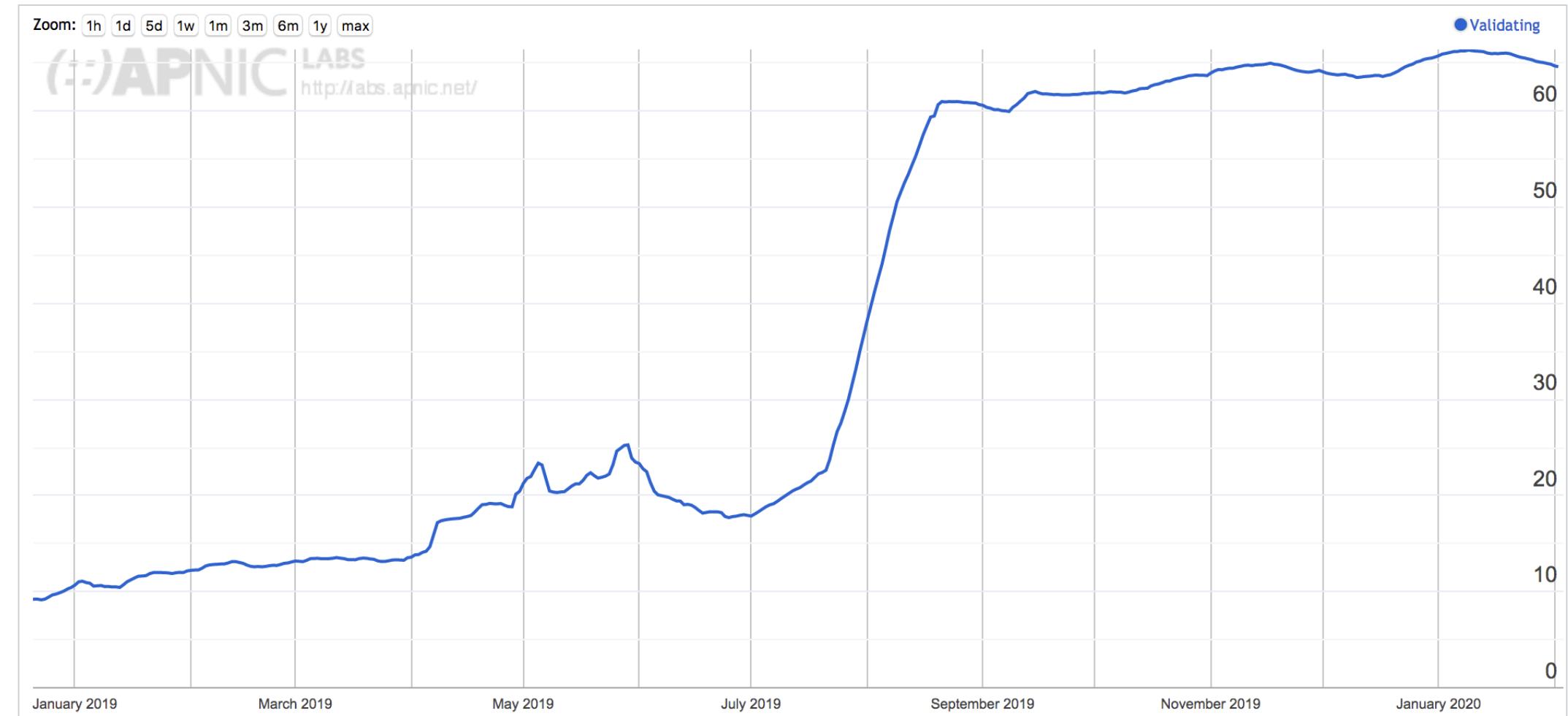
---

## in Switzerland

### DNSSEC VALIDATION AT 65%

According to APNIC measurements, the validation of DNSSEC on resolvers of Swiss ISPs currently lies at around 65%. The reason for this leap is that Swisscom activated DNSSEC validation on all its resolvers in mid-2019. SWITCH was in constant contact with Swisscom, and advised and supported DNS operators.

Webpage: <https://stats.labs.apnic.net/dnssec/CH>



**DNSSEC validation  
on Swiss resolvers**

# Dispute resolution

---

Since 2004, SWITCH has been using the dispute resolution service of WIPO (World Intellectual Property Organization). WIPO operates a dispute resolution service accredited by ICANN for over 70 other registries.

In 2019, the experts passed down decisions on nine .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	2018	2019
Transfer to applicant	10	7
Complaint rejected	1	2
<b>Number of proceedings</b>	<b>11</b>	<b>9</b>

	Domain names
Transfer to applicant	novaflair.ch investmentgroup.ch wilier.ch brunobischofberger.ch kulikseidler.ch raiffeisen.ch arcelormittal-construction.ch
Complaint rejected	scx.ch nailcode.ch

# Registrar developments

With the announcement of domain name migration from SWITCH to the registrars, the number of registrars leapt from 83 to 100 in 2015. An increasing number of hosting and email providers were aiming to become registrars so that they could manage their customers' domain names themselves in the future.

This trend has slowed a little, and SWITCH had 104 active registrars by the end of 2016. There were only three additional registrars in 2017. In 2018, considerably more registrars than expected were added; by the end of the year, we recorded 122 registrars.

By the end of 2019, the registry counted 131 registrars.

The market is working and the potential domain name holders have a wide range of providers from which to choose.



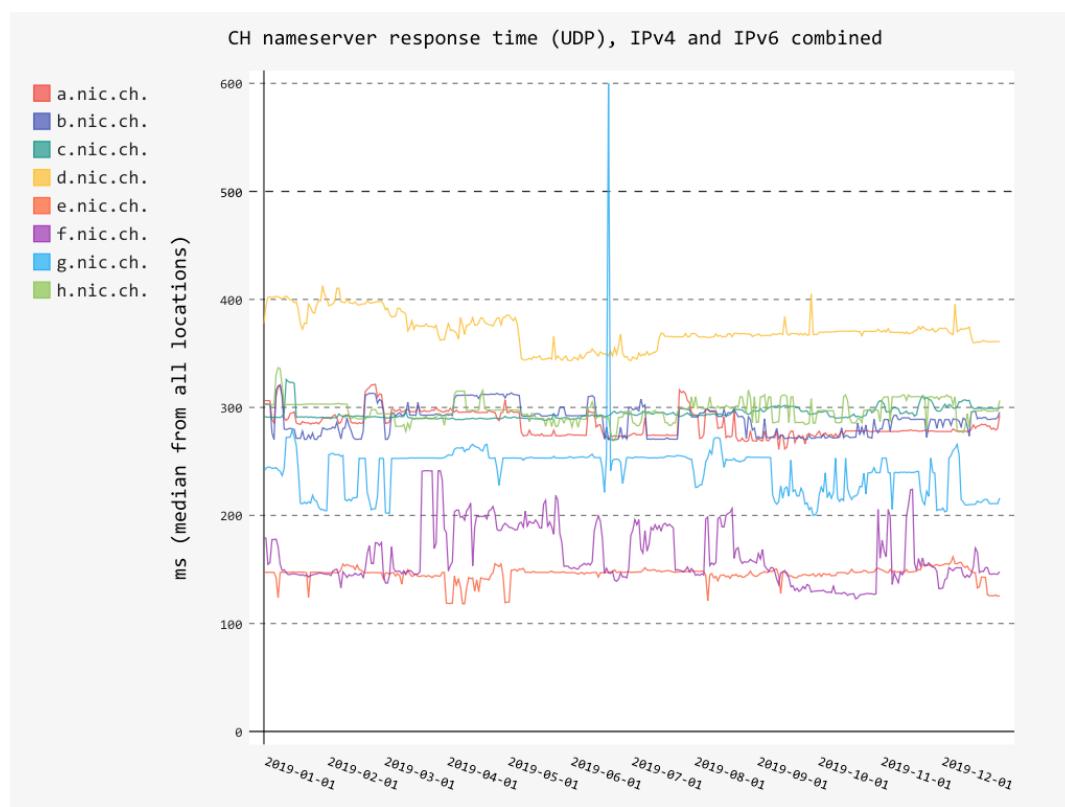
**INVENTORY DEVELOPMENT**  
By the end of 2019, the registry had 131 active registrars

# Performance

---

## of the name servers

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 1500 ms (TCP).



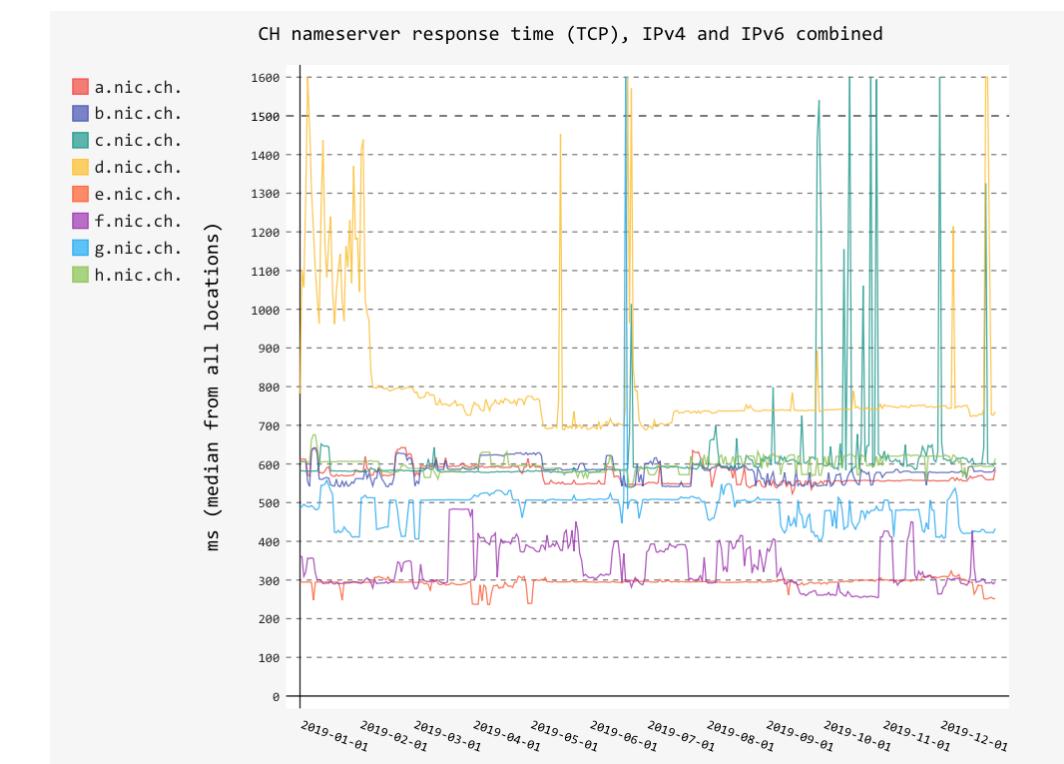
### UDP RESPONSE TIMES

Combined response times of IPv4 and IPv6

In 2019, this requirement was met in each instance. The measurements were carried out by RIPE and are available to the public at <https://atlas.ripe.net/dnsmon/group/ch>.

**UNICAST** a.nic.ch (CH), b.nic.ch (CH), c.nic.ch (USA), d.nic.ch (BR), h.nic.ch (CH)

**ANYCAST** e.nic.ch, f.nic.ch, g.nic.ch



### TCP RESPONSE TIMES

Combined response times of IPv4 and IPv6

# Cybercrime

## QUANTITATIVE

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

	# malware cases	# phishing cases
Reports received	6,008	6,703
Suspicion confirmed	131	1,736
Number of blocked domain names	41	1,597
Reason for lifting block: - Statutory period expired	11	18
- Lifted after block	0	0
Revoked domain names	21	868

**NUMBER OF MALWARE AND PHISHING CASES 2019**  
quantitative view

## QUALITATIVE

The time spent on cases was:

	Duration		
Duration of temporary blocking according to OID Art. 15.1,2,3 max. blocking time 30 days (720 hours)	Min. time	0.2 h	
	Average	86.05 h	
	Max. time	260.25 h	
Response time from SWITCH following notification			Average
Time until removal of threat after notifying the holders			Average
			38.37 h

**NUMBER OF MALWARE AND PHISHING CASES 2019**  
qualitative view

# *Economic indicators*

---

The Foundation Council session on 4 June 2020 will pass the SWITCH foundation's 2019 Annual Report, along with the balance sheet and income statement. Dispatch and publication will be on 5 June 2020.

No figures will be published at this point. Instead, interested parties will be referred to the comprehensive documents of the 2019 SWITCH Annual Report.

# Orientation and goals 2020

1/2

## COLLABORATION WITH RECOGNISED BODIES

Currently there are already five bodies recognised by OFCOM who can demand blockage of domain names:

- fedpol
- MELANI
- Zug Police
- Bern Cantonal Police
- Zurich Cantonal Police

This is a highly positive development, because it means cybercrime can be fought with increasing resources. For SWITCH there is a consistent increase in costs for training these authorities and the efficient, joint configuration of processes. Regular meetings are held to clarify mutual understanding of roles, tasks and competencies, resulting in a highly constructive and effective collaboration.

The removal of personal data about the domain name holder from the public Whois service means that this service becomes useless for recognised bodies. SWITCH has therefore developed a service based on RDAP. The recognised bodies have protected access to personal registry data through this protocol.

## SECURITY-AWARENESS MEASURES

The ‘Hack the Hacker’ escape room developed by SWITCH-CERT was a complete success. Gamification, an experiential approach that combines training and fun, has a lasting impact. A mobile version of the escape room enables other groups in Switzerland as well as employees of neighbouring registries to conduct this informative course.

We are continuing this success and are currently developing our sequel, ‘Track the Hacker’, based on the idea of a ‘Foxtrail’, or scavenger hunt.

The Security Awareness division of SWITCH will be increased by one person in 2020. We are convinced that we can achieve more with internet users when we join together and coordinate campaigns with committees and associations.

The Swiss Web Security Day is aimed at registrars, ISPs and hosting providers. Through specialist talks, we can increase awareness, contributing to a more secure, more stable internet in Switzerland. Another instalment of this day of action is planned for 2020.

# Orientation and goals 2020

2/2

## MODERNISATION OF THE SERVER INFRASTRUCTURE

The IT services of the registry are based on a cloud architecture. The infrastructure is established redundantly at the two sites, Zurich and Lausanne. In parallel, SWITCH is operating a modern cloud infrastructure. It is also located in these two cities, but in different computing centres. SWITCH already provides Swiss universities with computing and storage services, with data locations in Switzerland and data sovereignty held by the respective university. Throughout 2020 and 2021, the individual modules of the registry application will be migrated to this new infrastructure. The contractually agreed availability must be maintained at all times.

The central database runs on separate infrastructure, also at the two above-mentioned locations. These servers will also be replaced in 2020. The preparatory work for this was already under way in 2019. The migration is planned for mid-2020.

## PREPARATION FOR THE NEW OID

The new Ordinance on Internet Domains (OID) will bring changes in the following key areas:

- Change to Whois service
- Information service
- Deferred delegation

The change to the Whois service is not a major technical undertaking.

The processes for the information service could, depending on the final draft of the OID, prove to be labour-intensive, if the experience of neighbouring registries is anything to go by. Here, SWITCH will be looking for utmost efficiency of solutions.

Deferred delegation (delayed usage of domain names) will be an effective tool in the battle against cybercrime. Figures from the Danish registry bear this out. We will be working with this registry as well as with EURid to exchange experience. The implementation will begin in the second half of 2020 and is likely to last until the end of 2021, as the complete software infrastructure for battling cybercrime will also be updated during this time.

# *Planned innovations 2020*

---

## **PUBLIC NAME SERVER TEST**

In 2019, SWITCH developed a name server test for internal usage. If we receive a report of maloperation, we can use the test to get to the bottom of things and carry out targeted troubleshooting.

In the course of 2020, we will make this test publicly accessible. In the first phase, we will be concentrating on specialist users. In 2019, we carried out two meetings with DNS experts. We will continue these meetings and use them for training purposes.

Based on a cost-benefit analysis that is still to be carried out, we will decide whether we will make the name server test known and accessible to the general public.

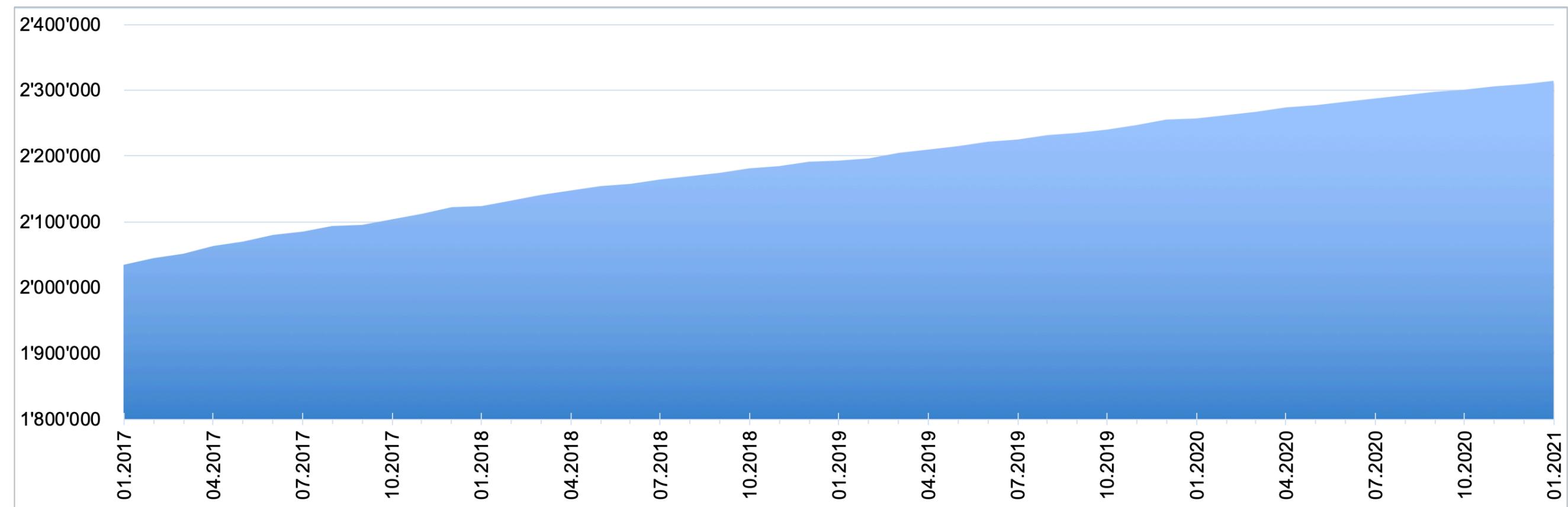
In 2020, the focus is on rebuilding the internal infrastructure (see previous chapter). There are no further outwardly visible changes planned.

# Growth forecast 2020

## .ch domain names

SWITCH is forecasting growth of almost 3% for 2020. This represents an average increase of around 5,000 domain names per month.

**GROWTH FORECAST**  
.ch domain name inventory 2020





*Working for a better digital world*



SWITCH  
Werdstrasse 2  
PO Box  
CH-8021 Zurich

Phone +41 44 268 15 15  
[www.switch.ch](http://www.switch.ch)  
[info@switch.ch](mailto:info@switch.ch)