CZ.NIC | CZ DOMAIN REGISTRY

Annual Report 2019

1 **Profile of the association**

CZ.NIC is a special-interest association of legal entities, an open and independent organisation whose main activity is the administration of the registry of the top-level national .CZ domain, as well as securing its operation. The association's activities in the field of security are also very important, involving both the Czech National CSIRT.CZ Security Team and other security projects, such as the powerful Turris Omnia router ecosystem and the Turris MOX modular router.

In addition to these activities, the association is dedicated to research, development and education in the field of the internet, internet protocols, network traffic and new technologies in general. The CZ.NIC Association ranks the support and development of the internet community both in the Czech Republic and abroad among its long-term goals.

The CZ.NIC Association was established in May 1998 due to the growing importance of the internet and, thus, the number of its users and those interested in registering domain names in ccTLD .CZ. At the end of 2019, the association had 116 members divided into three chambers.

At present, the association represents a stable and trustworthy entity capable of ensuring the reliable operation of the Czech national domain .CZ. Since 2013, CZ.NIC has been the holder of the ISO 27001 certification, confirming the safe handling of information, including setting appropriate rules and procedures.

For domain name holders, registrars and also other entities that use the internet for their work and leisure time, the association is a reliable partner that not only provides domain name administration but also safeguards internet security and is involved in socially beneficial activities – both in the form of CZ.NIC Labs projects or education.

2 **Foreword from the Chairman of the Board of Directors**

Ladies and Gentlemen,

I am honoured to present the Annual Report of our association for 2019.

We managed to meet the financial plan and the very demanding internal plan of activities. I am proud that, as in previous years, the Czech national internet domain and our other services worked reliably and served their users well.

An important event in the past year was the discussion and approval of the concept of the association until 2024. In its introduction, we stated that our mission remained the operation and development of the internet infrastructure and services of general interest, especially the .CZ domain, for the benefit of the local community. We want to support the development of these services through innovative projects, raise awareness of aspects of internet technologies, and increase the level of cyber security.

The increase in the wholesale price for the annual keeping of the domain name record did not appear to have any significant effect on the number of registrations. Year-on-year growth was about half a percent, which corresponds to the long-term trend. This change did not affect the number of concluded registrar agreements in any way; the number of registrars is stable at over forty.

The main activity of our association is the administration of the national internet domain. This responsibility was reflected, among other things, in the fact that the National Security Authority designated our association as the operator of the basic service under the Cyber Security Act. We have conducted several surveys concerning interest in introducing the possibility of registering domain names with national characters (IDN). Individual users and commercial organisations are not in favour.

In addition to the administration of the national domain, we implement other major projects. I would like to mention at least the operation of the National CSIRT of the Czech Republic, the development of the infrastructure of secure Turris routers, education in cyber security (e.g., collaboration on the successful film V síti (In the Network)), the development of the globally widespread routing daemon Bird, the mojeID authentication technology, the development of the successful authoritative DNS server Knot, and the organisation of seminars and conferences (e.g., IETF 104). For many other projects, especially in the field of cyber security, we managed to obtain funding in the form of grants and subsidies (e.g., the PROKI, Safer Internet, CyberExchange, CEF, Safer Internet or NetMetr projects).

I am glad that as the chairman of the governing body I can look back at the excellent results of our organisation. I would like to thank all our people for this, not only for the enormous amount of work done for the association in the past year, but also for the exceptional commitment they have shown in dealing with the emergency situation caused by this year's viral pandemic. We managed not only to keep our infrastructure and services running smoothly, but also to help other organisations and individuals.

Basic information about the association and its activities in the past year is available on the following pages of this Annual Report. I firmly believe that we will successfully continue pursuing our mission and serving as your reliable and transparent partner.

RNDr. Karel Taft, MBA – Chairman of the Board of Directors

3 **Foreword from the Managing Director**

Ladies and Gentlemen,

2019 was a year when the number of registered domains was not expected to increase again. An increase of just under 7,000 domains is nothing significant, but it is positive news that it is still possible to find interesting domains with the .CZ suffix.

In 2019, we naturally worked hard to increase the quality and security of our registration system. That is why we built a new private hall in the Žižkov Television Tower in Prague and moved all the technology that had been in the common hall there. Naturally, we also worked on improving our DNS Anycast. To improve coverage in Latin America, we opened a new node in Brazil, and another entity interested in the ISP stack, namely CESNET, contacted us.

The share of the DNSSEC technology deployment also increased. As early as the beginning of the year, the registrar Seonet Multimedia announced that it was implementing DNSSEC for all domains under administration. It used a recently implemented automated administration system that does not require EPP to interact with the register. Not only thanks to this event, over 59% of all domains in the register were signed up at the end of the year, which is a very high number in an international comparison. However, the list of news from the world of DNS does not end there. We introduced support for the DNS over TLS and DNS over HTTPS technologies on our open resolvers (ODVR). It will be interesting to see if this trend in DNS traffic encryption takes hold.

The mojeID service also underwent great development. To increase login security, we introduced support for the FIDO2 authentication standard. As a second factor to the password, the user thus has a choice between

OTP, the mojeID Authenticator application and the hardware device supporting FIDO2. Another novelty was the introduction of the possibility to validate accounts using the CzechPOINT public administration assistance network. With regard to the number of contact points of this system, validation is already actually available for all citizens of the Czech Republic. Of course, these changes pursue a clear goal, which is to connect mojeID with state administration systems, specifically with the National Identification Authority (NIA). This connection will be the main goal of the mojeID project in 2020.

Another interesting project is taking shape in the field of security. The national CSIRT.CZ security team that we operate worked to launch a new service for the public. It concerns an offer of penetration tests. In 2019, a successful pilot test of this service took place with the Vysočina Region. I believe that more customers will use this service next year.

Another project focused on security – the Turris project – also announced an expected novelty. By the middle of the year, we managed to distribute all the routers that contributors had ordered in the crowdfunding campaign, and we launched free commercial sales.

In 2019, we also invested considerable effort in education. We continued focusing on young internet users. We produced the film *Maturant* (High-School Graduate), which was presented at the film festival for children and youth in Zlín. The film can be downloaded for non-commercial use free of charge. Another achievement in this area was the series *Marty is Dead*, which was awarded at the Serial Killer Festival.

Finally, I would like to mention one more important thing. In 2019, the validity of the existing concept of the association's activities expired and, therefore, a new concept for the period of 2020–2024 was prepared and subsequently approved.

I firmly believe it is clear from my foreword that the year 2019 can also be considered a successful one, and I would very much like to thank my colleagues for that.
I wish you pleasant reading of this Annual Report.

Mgr. Ondřej Filip, MBA – Managing Director
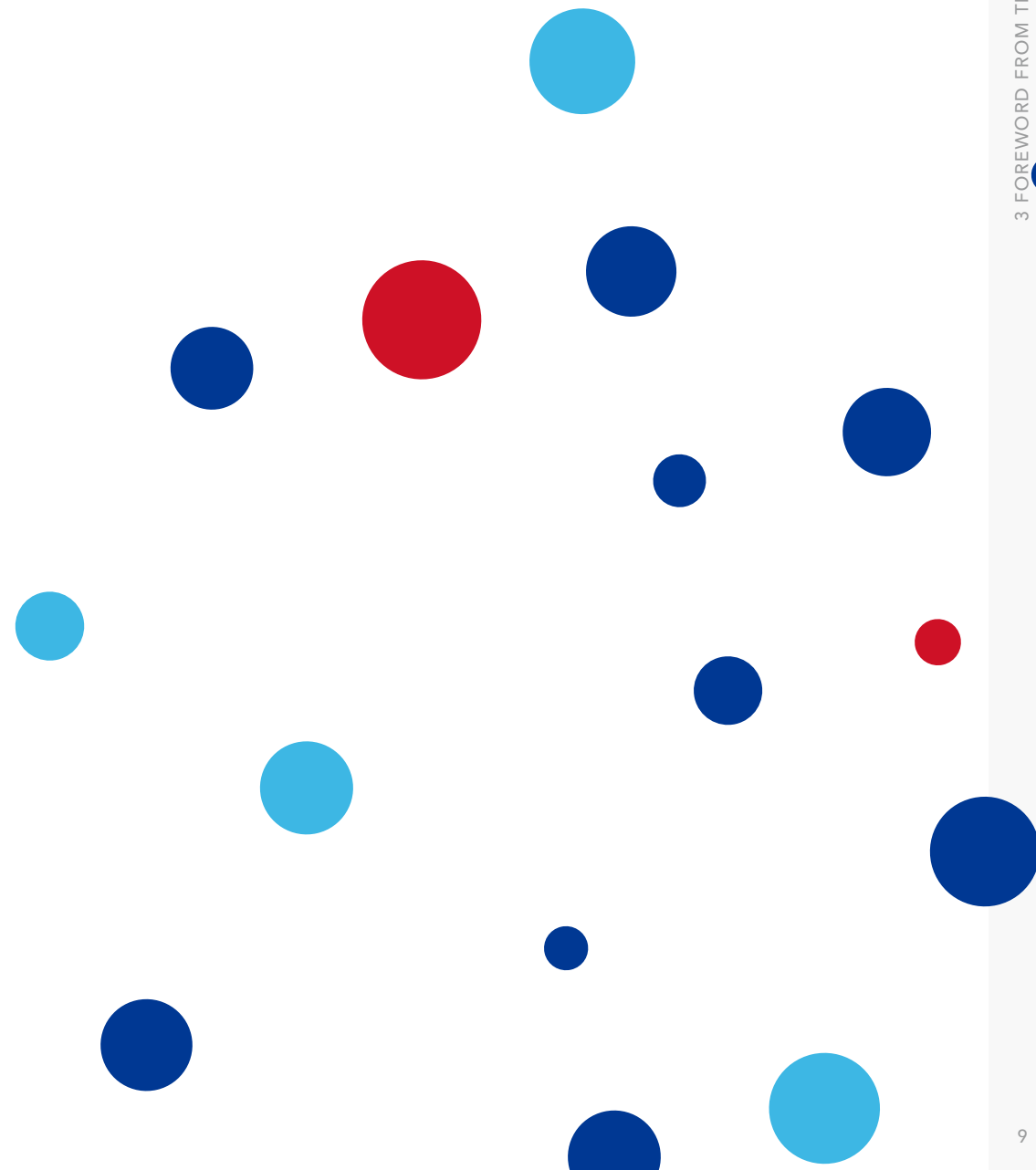
4 **The .CZ domain**

4.1 State and development of registration numbers

In 2019, the total number of domains in the .CZ zone rose by 6,689, which constitutes growth by about 0.5 %. The Czech national domain .CZ, therefore, reflects a trend that is being experienced by almost all national registers: a falling tendency of national domain registrations (ccTLD), caused mostly by market saturation and also partly by new alternatives for domain name registration through new, generic domains (new gTLD).

Total number of registered .CZ domain names in 2019

Month	Total
January	1 326 026
February	1 331 251
March	1 331 839
April	1 329 807
May	1 328 529
June	1 326 021
July	1 324 735
August	1 325 121
September	1 327 551
October	1 329 310
November	1 331 332
December	1 329 289
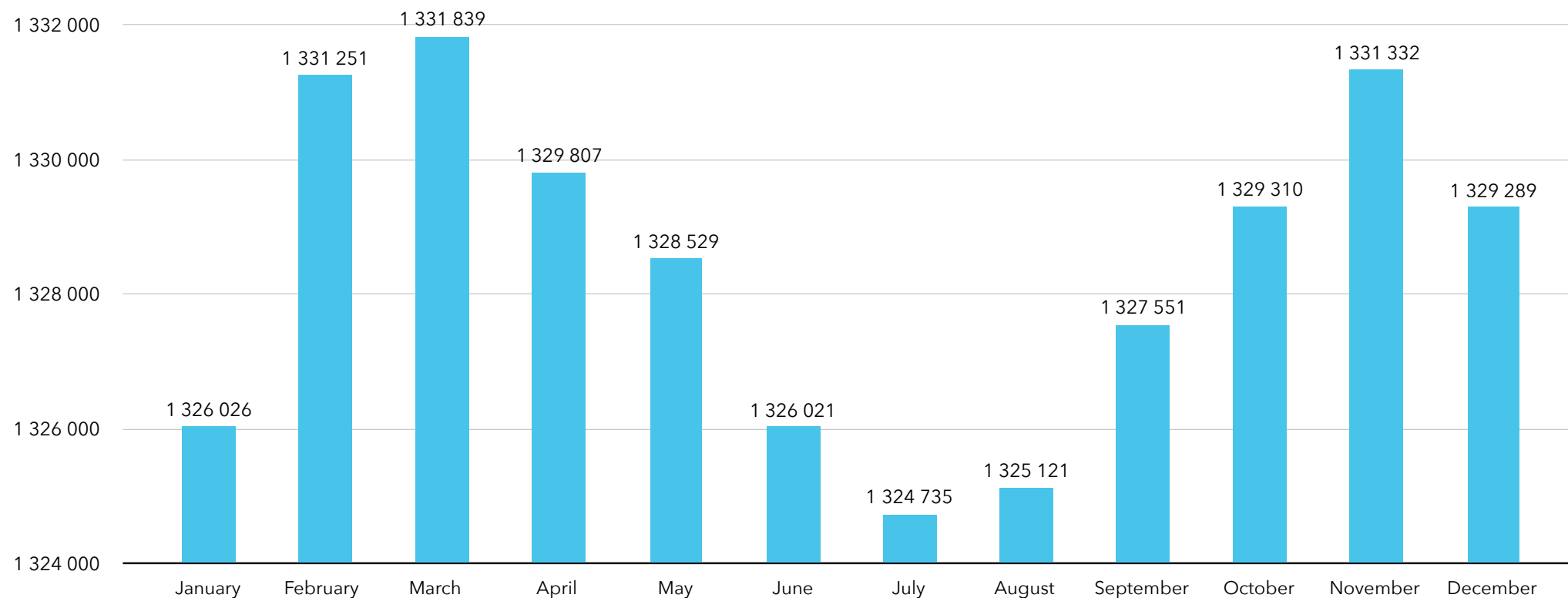
In 2019, an average of 13,886 new domain names were registered every month. Like in the past period, this slight drop in the average number of registrations reflected the trend of global growth in new domains. The following charts show the number of new registrations in 2019 by month and the development of the average rate of new registrations since 2008.

Number of newly registered .CZ domain names in 2019

January	18 111
February	16 768
March	17 089
April	15 032
May	15 279
June	12 879
July	13 032
August	13 817
September	14 560
October	15 201
November	15 300
December	13 269
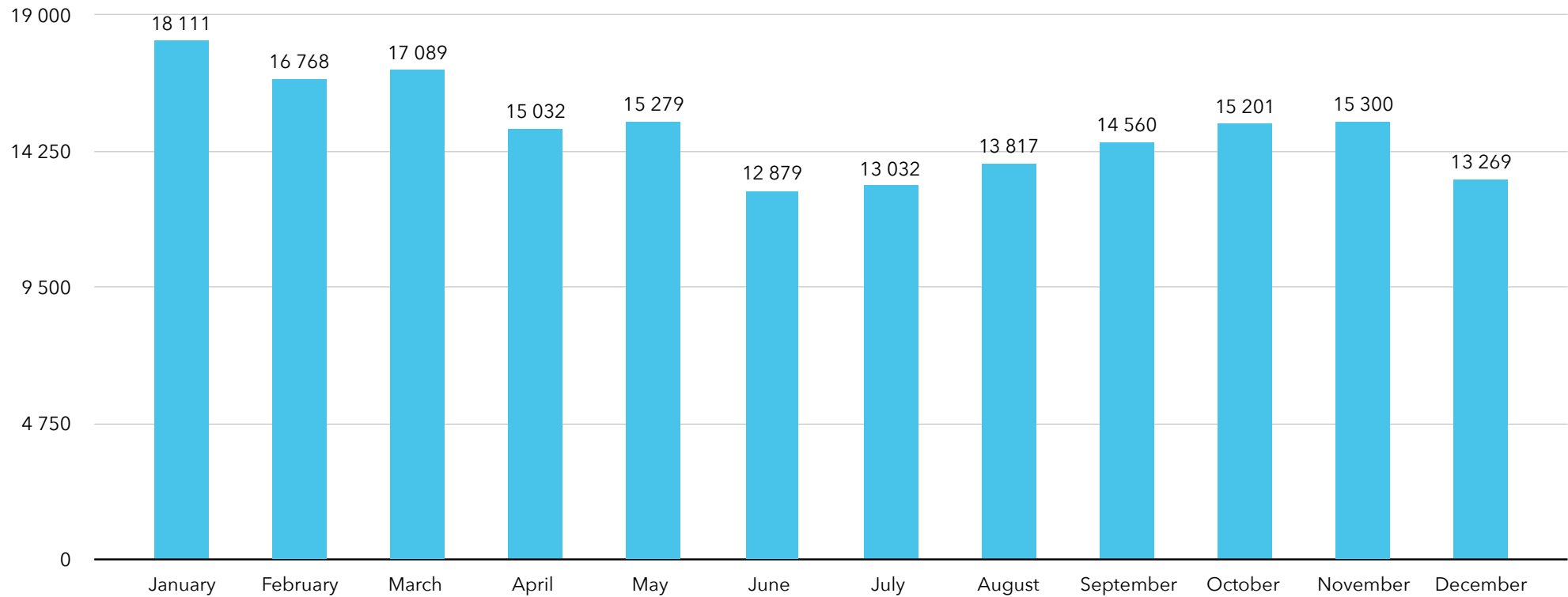
New registrations 2008-2019 (monthly average)

Year	Value
2008	13 866
2009	15 890
2010	17 490
2011	19 490
2012	20 982
2013	20 369
2014	19 842
2015	18 890
2016	18 595
2017	16 889
2018	16 076
2019	13 886
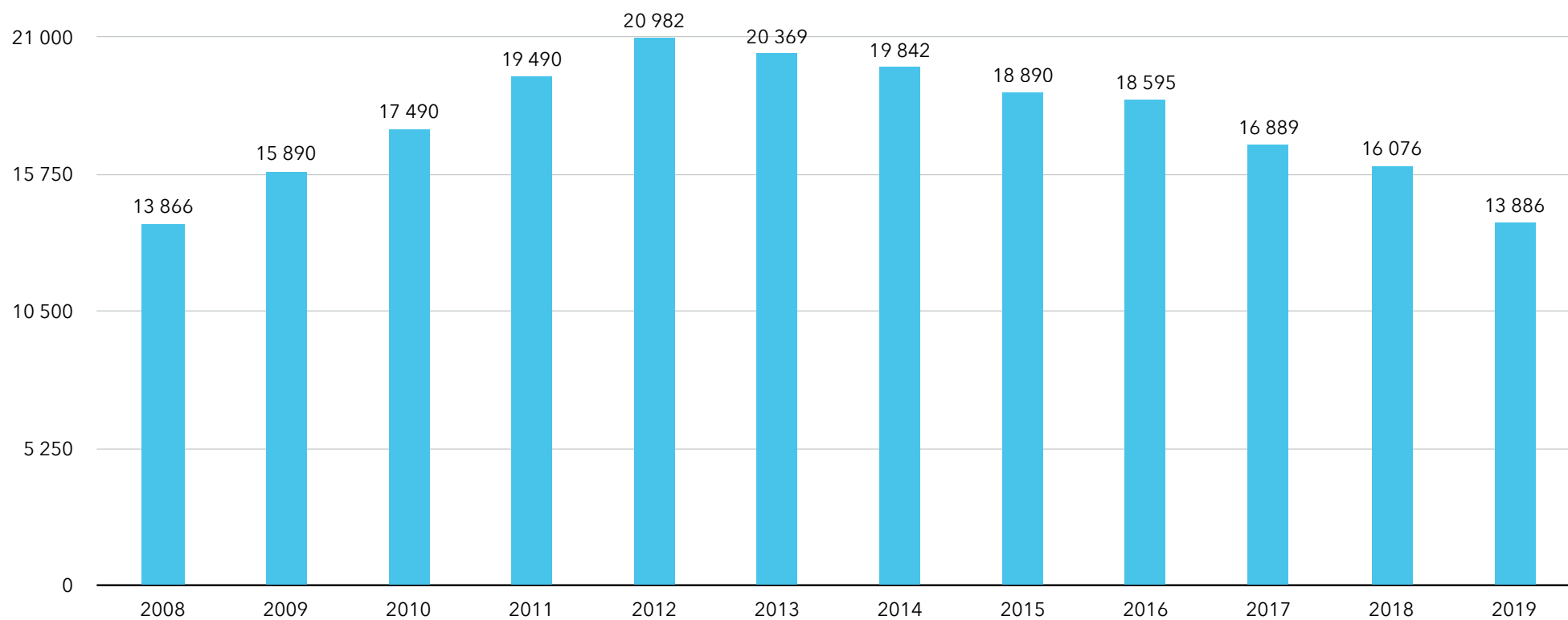
4.2 IDN (Internationalised domain names)

IDN is a system thanks to which domain names can contain characters of national alphabets. In the Czech Republic, it means that .CZ domains may contain characters with Czech diacritics: acute accents and carons.

The CZ.NIC Association is technically prepared for the possible introduction of IDN into our national domain but IDN has not yet been introduced for .CZ domains because the community of internet users in the Czech Republic is not yet interested in the introduction of IDN. CZ.NIC repeatedly organises a public opinion survey once every two to three years to gauge the interest of users. In the autumn of 2019, 88% of respondents from organisations and 64% of regular internet users opposed the introduction of the IDN system. In the first case, it is an increase by two percentage points compared to the last survey in 2016, in the second case the figure is higher by nine percentage points. A total of 1,015 representatives of organisations and 1,206 individual users took part in the survey.

INDIVIDUALS

	2006	2008	2010	2012	2014	2016	2019
absolutely no	23	26	27	27	29	26	31
rather no	32	40	35	40	39	29	33
rather yes	33	25	26	23	23	33	24
absolutely yes	12	9	11	10	9	12	12

● absolutely no ● rather no ● rather yes ● absolutely yes   Values given as percentage.

ORGANIZATIONS

	2006	2008	2010	2012	2014	2016	2019
absolutely no	52	60	63	60	38	60	62
rather no	35	30	28	25	43	26	26
rather yes	10	6	6	10	14	9	8
absolutely yes	4	4	3	5	6	5	4

● absolutely no ● rather no ● rather yes ● absolutely yes   Values given as percentage.

4.3 Registrars

The system of .CZ domain administration is based on a distributed principle in which the registration of domain names is carried out by contractual partners of the CZ.NIC Association – registrars. CZ.NIC acts similarly as a wholesale partner towards them but provides the technical aspects and functionality of the .CZ domain of the highest level.

In 2019, their agreements were terminated by the registrars Sonexo B.V. (as of 30 June 2019) and Economia, a.s. (as of 31 December 2019); at the end of the year, GENERAL REGISTRY ceased to exist by merging with INTERNET CZ, a.s.

As of 1 January 2019, NAMESHIELD SAS (France) and Focus IP, Inc (USA) became new registrars.

Hence, by the end of 2019, a total of 43 companies had concluded an Agreement on Cooperation in Domain Registration with the association, of which 27 were domestic and 16 foreign. This number offers a broad choice for the end user and also provides sufficient competition.

4.3.1 .CZ domain name registrar overview

List of all accredited registrars as of 31 December 2019

1API GmbH	MIRAMO spol. s r.o.
ACTIVE 24, s.r.o.	NAMESHIELD SAS
AERO Trip PRO s.r.o.	nexum Trilog a.s.
Ascio Technologies inc.	Com Laude
ASPone, s.r.o.	ONE.CZ s.r.o.
e-BAAN Net s. r. o.	ONEsolution s.r.o.
Economia, a.s.	OVH, Sas
CORE ASSOCIATION	PIPNI s.r.o.
O2 Czech Republic a.s.	Safenames Ltd.
Dial Telecom, a.s.	Seonet Multimedia s.r.o.
Focus IP, Inc.	Seznam.cz, a.s.
Gandi SAS	Stable.cz s.r.o.
Gransy s.r.o.	TELE3 s.r.o.
IGNUM, s.r.o.	TERMS a.s.
Instra Corporation Pty Ltd	united-domains AG
INTERNET CZ, a.s.	Variomedia AG
InterNetX GmbH	Web4U s.r.o.
IP Mirror Pte Ltd	Websupport, s.r.o.
Key-Systems GmbH	WEDOS Internet, a.s.
KRAXNET s.r.o.	ProfiHOSTING s.r.o.
MarkMonitor Inc.	ZONER software, a.s.
Media4Web s.r.o.	

4.3.2 Major domain name registrars

The major registrar, according to the number of administered domains, was the same as last year: INTERNET.CZ, a.s., followed by WEDOS Internet, a.s., ACTIVE 24, s.r.o., Gransy s.r.o. and IGNUM, s.r.o. An overview of registrars with a market share of over 1% is shown in the following chart.

Key-Systems GmbH
1,00 %

Seonet Multimedia s.r.o.
1,27 %

Stable.cz s.r.o.
1,45 %

ONEsolution s.r.o.
1,50 %

TELE3 s.r.o.
2,15 %

Web4U s.r.o.
3,77 %

Media4Web s.r.o
4,11 %

ZONER software, a. s.
5,59 %

IGNUM, s.r.o.
7,67 %

Gransy s.r.o.
8,24 %

ACTIVE 24, s.r.o.
12,97 %

WEDOS Internet, a.s.
19,71 %

INTERNET CZ, a.s.
23,62 %

Other
6,97 %
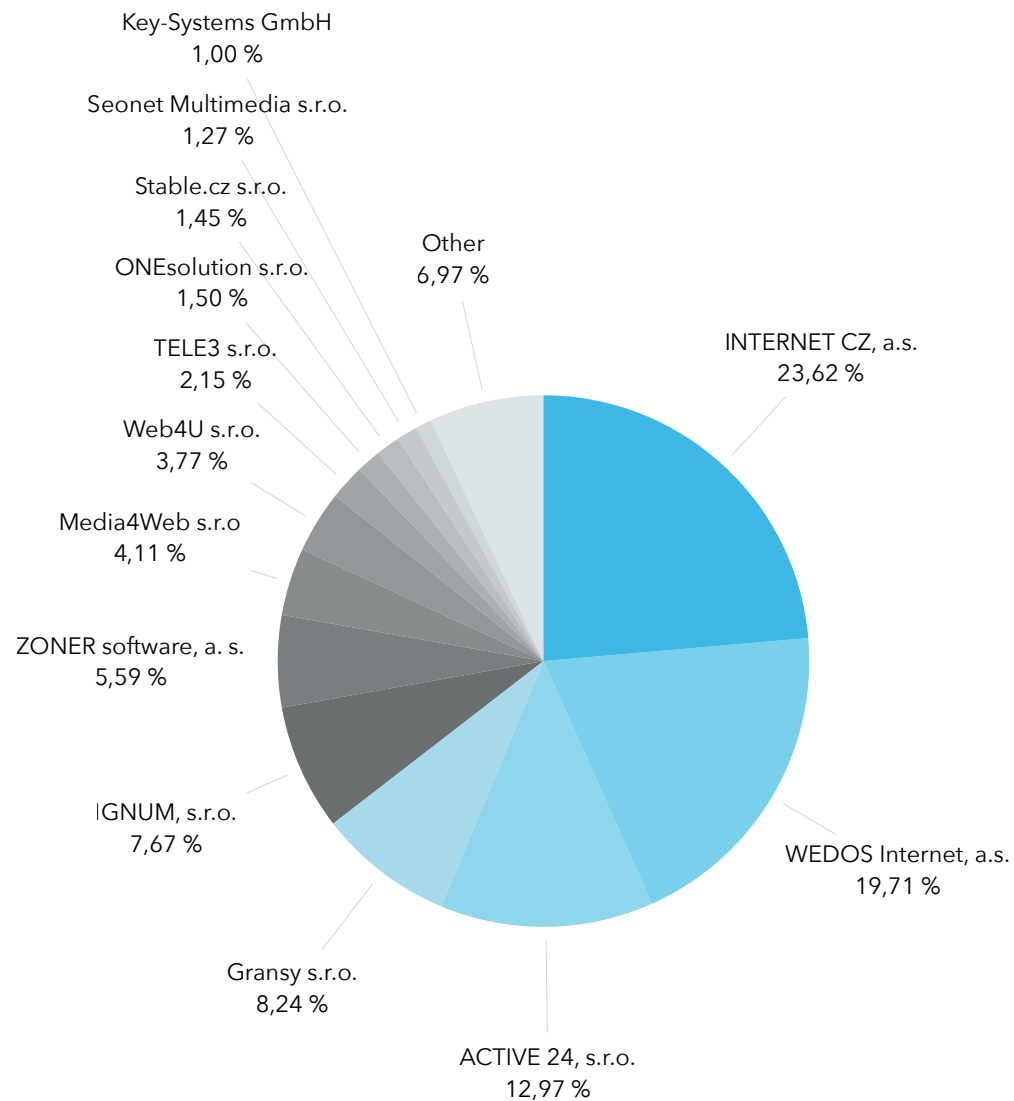
4.3.3 Registrar certification

Launched as early as the middle of 2011, the certification project makes it easier for end users (i.e. parties interested in a new registration, as well as existing domain name holders) to find their way amongst the high number of registrars, particularly regarding portfolio and service quality. The certification method was prepared in collaboration with registrars and APEK (Association for Electronic Commerce).

Registrars who participate in the programme can always receive the "Certified Registrar" logo for one year. From the initial 9 registrars involved in voluntary certification in 2011, the number rose to 12. The end customer can, hence, enjoy the constantly improving quality of services offered. At the end of 2019, nine registrars met the most demanding criteria to receive five stars. There is also no longer a registrar among the certified registrars with only three stars. The service quality of registrars, reflected by the number of stars, is shown in the following table.

	2011	2012	2013	2014	2015	2016	2017	2018	2019
*****	3	6	8	9	10	10	9	9	9
****	3	5	4	3	2	2	3	3	3
***	2	1							
**	1								

4.3.4 Cooperation with registrars – co-marketing scheme

In accordance with its main activities and long-term objectives, the CZ.NIC Association aims to promote and support domain registration under the top-level .CZ domain. Given the distributed administration method of the national domain, the CZ.NIC Association has limited options for addressing potential domain name holders through direct marketing.

This fact gave rise to the co-marketing scheme, which CZ.NIC contributes to registrars' (provided that they have fulfilled the applicable requirements) communication campaigns, promoting domain name registrations in ccTLD .CZ. The amount of the contribution from CZ.NIC depends on the registrar size (the number of registrations and domain name renewals), campaign volume and compliance with other factors, such as the use of mojeID or domain security through DNSSEC, all of which are used by CZ.NIC to motivate the registrars to expand these technologies.

The popularity of the co-marketing scheme, thanks to the .CZ Czech national domain being popular among users and clearly and frequently visible (e.g., on outdoor advertisements), is still high in terms of the number of registrars involved and the volume of funding. In 2019, the scheme included 14 registrars, to which CZ.NIC paid a total of CZK 10,200,000.

4.4 Register data improvement

Quality improvements of data maintained in the domain name holder register continued in 2019 when, as in the previous year, the aim of CZ.NIC was to merge multiple duplicate contacts that have been accumulating in the database over the years. In addition, user data were verified to improve their security and correctness and, hence, make it easier for the association to contact the holder, e.g., when there was a risk that the domain name would be cancelled due to an outstanding payment for the registration renewal fee. Domain name holders were motivated to update and verify their data by receiving a small reward (promotional item of CZ.NIC) and the opportunity to receive more valuable prizes.

4.4.1 Resolving disputes over domain names in ccTLD .CZ

The average duration of a lawsuit before a general court is about 3 years, and only if there are no complications. The association therefore tried to find an alternative way to resolve domain name disputes, one that would be fast, stable and also safe. Therefore, the Alternative Dispute Resolution (ADR) system has been in use since the summer of 2004. Until 2015, it took the form of arbitration, where it was possible to file a dispute concerning the domain name against its holder with the Arbitration Court, which is attached to the Czech Chamber of Commerce and the Agrarian

Chamber of the Czech Republic. The Arbitration Court considered over one hundred disputes during the ten years of existence of this alternative dispute solving method.

However, following a decision by the Supreme Court at the end of 2013, there was a change. In March 2015 a new ADR method was introduced, the basic principles of which are identical to those that have been and continue to be used successfully in disputes over generic TLDs (UDRP) or domain names registered in the .EU top-level domain. The platform where the disputes take place is administered by a trusted entity on the basis of a concluded memorandum. That entity is the Arbitration Court attached to the Czech Chamber of Commerce and the Agrarian Chamber of the Czech Republic, which is one of the three permanent arbitration courts that exist in the Czech Republic. This permanent arbitration court enjoys considerable authority and an indisputable advantage. Especially in the case of domain name disputes, it is one of the few courts to offer online proceedings.

However, the ADR system used since 2015 is not an arbitration process that complies with the arbitration law, a fact that is also reflected in the terminology used. The system is based on contractual arrangements and only a domain name transfer or cancellation (no other claims, such as damage compensation) can be claimed. The decision is not an execution order for the judgment; the ongoing dispute, according to the new ADR system, does not impede lis pendens (i.e., proceedings pending in the same matter) and a resolved dispute does not obstruct decided matters. The same claims can be, therefore, forwarded to a general court during the proceedings or afterwards.

The year 2015, when the new ADR was introduced, was very cautious in terms of use, but the following years show that this method of dispute resolution has been accepted.

Year	Number of disputes initiated in ADR
2015	7
2016	20
2017	22
2018	22
2019	**29**

Of general courts, the Municipal Court in Prague most often decides disputes over domain names, especially in view of the fact that it is a specialised court for, inter alia, competition and intellectual property disputes, which are the most frequently violated rights in the case of domain disputes.

4.4.2 Customer support

24/7 customer support is an integral part in securely operating the .CZ domain. The objective of customer support is to provide the best possible care to domain name holders, particularly in situations where a domain registration is to be cancelled or transferred, or where contact details change. Assistance for mojeID service users and their validation is also an integral part of customer support.

In the relationship with domain holders, customer support is based on a proactive approach, the aim of which is to prevent domain name de-registration or expiry due to obsolete contact details or forgotten payment. Given the distributed .CZ domain administration system, customer support is the only case in which the CZ.NIC Association is in direct contact with domain name holders.

In addition to standard e-mails that are sent to customers automatically by the domain registration system, notifying them, in particular, of the non-

payment of the renewal fee, our customer support manually reviewed more than 250,000 domains prior to removal or contacted almost 130,000 holders at risk of cancelling their domain names by phone (which was discontinued at the end of 2017) or via SMS (the service was introduced gradually in the second half of 2017) .

The following table shows activity trends converted into the monthly average.

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Manual check of domain names before exclusion	-	8,916	15,176	18,586	21,598	20,512	20,894	21,834	21,437	20,867
Manual check of domain names before cancellation	-	4,314	11,061	14,378	16,666	16,041	16,529	16,864	17,000	16,869
Calls to holders (contacts) of domain names scheduled for cancellation	4,263	4,314	4,767	6,690	7,808	7,367	7,826	7,573	790	904
SMS – information about upcoming domain name cancellation	-	-	-	-	-	-	-	8,139*1	8,948	9,859
E-mails sent before exclusion	1,201	1,429	1,708	1,716	1,915	1,718	1,849	3,157	2,826	3,036
Responses to e-mail inquiries	828	1,240	1,746	1,945	2,782	3,015	2,074	2,319	2,080	2,802
Responses to telephone inquiries	561	1,063	1,120	1,242	1,416	1,262	1,227	994	774	702
Requests (validation, blocking…)	145	180	248	315	455	405	701	776	559	363
Chat inquiries	-	-	-	-	-	166*2	132	114	168	262
Manual data accuracy check	-	-	-	-	1,073*3	875	953	1,372	1,628	1,170

The data represent the average number of the given actions per month

*1 monthly average of sent SMS in the second half of 2017

*2 monthly average since April 2015, when the service was launched

*3 monthly average since July 2014, when the practice of manual data checks was introduced
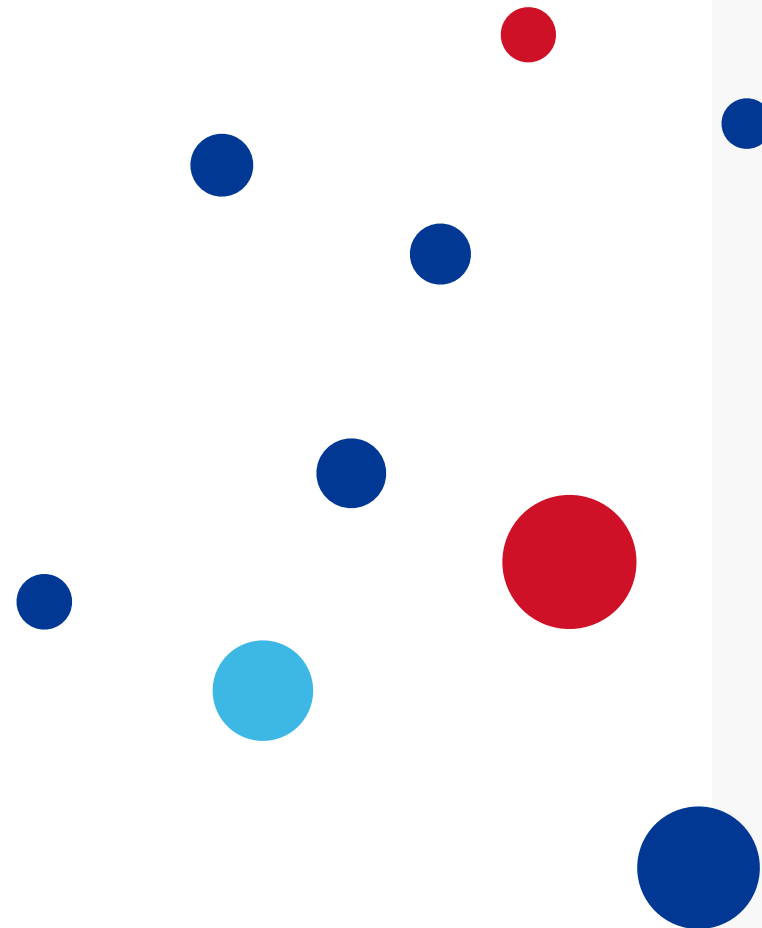
5 **Infrastructure**

5.1 Data centres

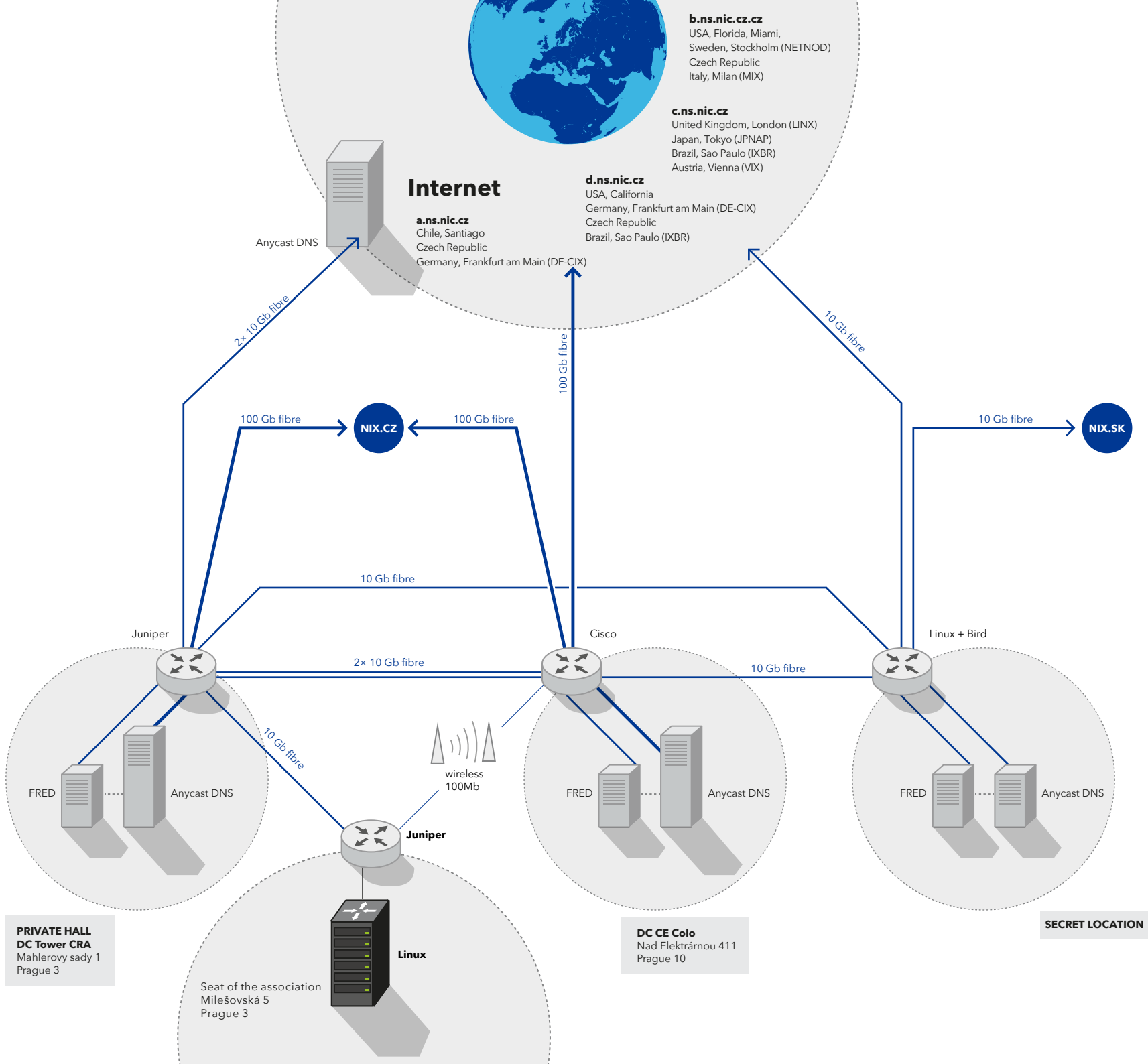The DSDng central register system was designed to be fully redundant. All hardware and software is located in three mutually independent locations:

– The TOWER data centre of České Radiokomunikace in Prague 3,
– The CE Colo data centre in Prague 10,
– A non-public location outside Prague.

All locations have their own internet connection and also a connection to the power grid. The DC TOWER data centre is connected to the distribution network from three independent transformer stations, while the CE Colo data centre and the location outside Prague are supplied from two transformer stations. A back-up power supply is available in all data centres via UPS and possible longer outages are bridged by power from diesel generators.

In 2019, the association built a private data hall in the DC TOWER of České Radiokomunikace and moved all traffic from this location there. This step increased physical security and capacity and ensured an overall modernisation of this part of the infrastructure. At the same time, the association managed to keep the same operating costs in this location, both during the relocation process and in further operations. The association used the relocation for significant upgrades of the network infrastructure. The association provided detailed information about the preparations and the relocation itself through a series of posts on its blog and in a presentation at the conference Internet and Technology 19 (IT19) in November 2019.

b.ns.nic.cz.cz
USA, Florida, Miami,
Sweden, Stockholm (NETNOD)
Czech Republic
Italy, Milan (MIX)

c.ns.nic.cz
United Kingdom, London (LINX)
Japan, Tokyo (JPNAP)
Brazil, Sao Paulo (IXBR)
Austria, Vienna (VIX)

d.ns.nic.cz
USA, California
Germany, Frankfurt am Main (DE-CIX)
Czech Republic
Brazil, Sao Paulo (IXBR)

Internet

a.ns.nic.cz
Chile, Santiago
Czech Republic
Germany, Frankfurt am Main (DE-CIX)

Anycast DNS

2× 10 Gb fibre

100 Gb fibre

10 Gb fibre

100 Gb fibre

NIX.CZ

100 Gb fibre

10 Gb fibre

NIX.SK

10 Gb fibre

Juniper

Cisco

Linux + Bird

2× 10 Gb fibre

10 Gb fibre

10 Gb fibre

FRED

Anycast DNS

wireless
100Mb

FRED

Anycast DNS

FRED

Anycast DNS

Juniper

**PRIVATE HALL
DC Tower CRA**
Mahlerovy sady 1
Prague 3

Linux

Seat of the association
Milešovská 5
Prague 3

DC CE Colo
Nad Elektrárnou 411
Prague 10

SECRET LOCATION

5.2 Technical aspects of domain administration

The infrastructure of the register carefully follows the rules of diversity of hardware equipment so that a possible error of a particular hardware manufacturer affects only a part of the infrastructure and thus minimises the possibility of failure of the central register as a whole. Therefore, technologies from different manufacturers are installed in every location. The same approach is used for authoritative DNS (Domain Name System) software, which we operate on three different systems (KNOT, Bind and NSD).

The actual software of the central register is designed in a way that ensures that any component of the architecture can be replaced by any copy that runs on the server in the other locations, at any time. A critical component is the PostgreSQL database, which is always being replicated to both of the other locations during standard operation. When the primary location is down, traffic can be redirected to the replicated database without any limitation or impact on functionality. Back-up systems are designed and operated in a way as to make it possible for any components to take over the operation of the register within a very short period of time in the event of an outage.

The central registry system is prepared for operation on IPv4 and IPv6 and its current implementation for the .CZ domain (as well as all DNS servers) is operated on these both protocols.

In 2019, a new web application (FERDA) was put into operation for the administration of data in the register, which will increase the efficiency

of the helpdesk in the future and will also be an attractive part of the FRED system for users abroad. This new web application brought with it a whole set of technological innovations, which will gradually be expanded in other modules of the FRED system. For example, we use the gRPC framework for remote procedure calls, replacing the use of the CORBA interface, the Vue.js JavaScript framework and other modern JavaScript tools, such as Webpack and Babel. The search for partial matches was optimised using database trigram indexes.

The behaviour of the register system was also adjusted according to the requirements of registrars in 2019. The possibility of monthly invoicing of a share of the fee for connection to the register was implemented (an annual period is also possible), a tool for merging registrars was developed and tested in operation, and providing information on changes in contact details was introduced for all designated domain registrars to which that contact is linked.

The change in legislation in the course of 2019 required a change in the method of calculating VAT. The association also optimised the process of deleting domains in the case of contacts with incorrect data outside the EU and adjusted the process of administrative blocking of domain names and contacts in the case of litigation, criminal and distraint proceedings and the like. In the test environment, the preparation of anonymised data was automated, monitoring of test environments was introduced, including periodic checking of software package versions, and smoke tests (i.e., basic test scenarios) were improved.

A strength of the FRED system is its technical documentation. In 2019, it was further expanded. A procedure for editing web whois templates and PDF document templates was described. Manual (man) pages for command line tools (fred-admin) were created for administrators and the basis for technical and implementation documentation for the new FERDA web interface was prepared.

5.2.1 FRED (Free Registry for ENUM and Domains)

The software, developed for the central registry and operated by CZ.NIC, was made available as open and free software as part of our support of smaller registries. In 2019, FRED licences were transferred to GNU GPLv3+. This way, smaller and newly-started registers can operate their domains on the system, which is designed for the Czech domain environment and prepared (thanks to its parameters and capacity) for a much higher number of domain names than currently registered in ccTLD .CZ.

Besides the Czech Republic, this system was controlling the domain administration in ten more countries in 2019. It is used to administer the domains of Argentina (.AR), Costa Rica (.CR), Albania (.AL), North Macedonia (.MK), Tanzania (.TZ), Angola (.IT.AO and .CO.AO), Malawi (.MW), Lesotho (.LS) and Macao (.MO). The deployment in Argentina, with over 500,000 domains, is the second-largest instance of FRED.

The CZ.NIC Association offers support for the implementation and operation of the FRED system for other TLDs.

Countries where FRED is used for domain administration

5.2.2 Authoritative DNS server system for .CZ

The .CZ domain management servers are operated by CZ.NIC in several locations around the world. In addition to the three locations in the Czech Republic (referred to in Chapter 5.1 Data centres), they include Sweden (Stockholm), Austria (Vienna), the United Kingdom (London), Germany (Frankfurt am Main), Chile (Santiago de Chile), the United States (Redwood City and Culpeper), Japan (Tokyo) and, since 2019, also Brazil (Sao Paolo) and Italy (Milan).

5.2.3 Authoritative DNS server system for .CZ

In 2019, the CZ.NIC Association continued increasing the resilience of the .CZ DNS infrastructure against DoS attacks and covering the needs for the continuous growth of normal operations. Specifically, the upgrade of the existing DNS node in Germany was completed, and then new nodes were installed in completely new locations, specifically in Brazil and Italy. In total, the DNS infrastructure for the .CZ domain at the end of 2019 had the capacity of 100+ physical servers and a connection capacity of 400+ Gbps distributed in 17 geographically remote locations of ten countries on four continents.

In 2019, the association also significantly improved the processing and evaluation of operating parameters from the DNS Anycast thanks to the ADAM project. Thanks to this, the association will be able to better manage its development in the future. As soon as 2020, upgrades and

installations of other foreign locations of the .CZ DNS infrastructure will be carried out in accordance with the outputs of this project.

For major internet service providers, CZ.NIC operates mirrors of .CZ Anycast DNS nodes, called ISP DNS Stacks, in the networks of those providers. The main advantage of this service is the full availability of services in the .CZ domain in the case of an attack against DNS servers of CZ.NIC. Customers of companies with the ISP DNS Stack will not be affected by any attack and the internet services in the .CZ domain will remain fully available to them. Another advantage is the acceleration of their responses in the provider's network with the ISP DNS Stack. The first companies to join the CZ.NIC Association in this activity are Seznam. cz and Vodafone Czech Republic. At the end of 2019, a contract was concluded for the operation of another such DNS mirror in the CESNET network.

Change in number of queries vs evaluated RTT by region

For DNS traffic captured on 1-14 May 2019 and 1-14 October 2019
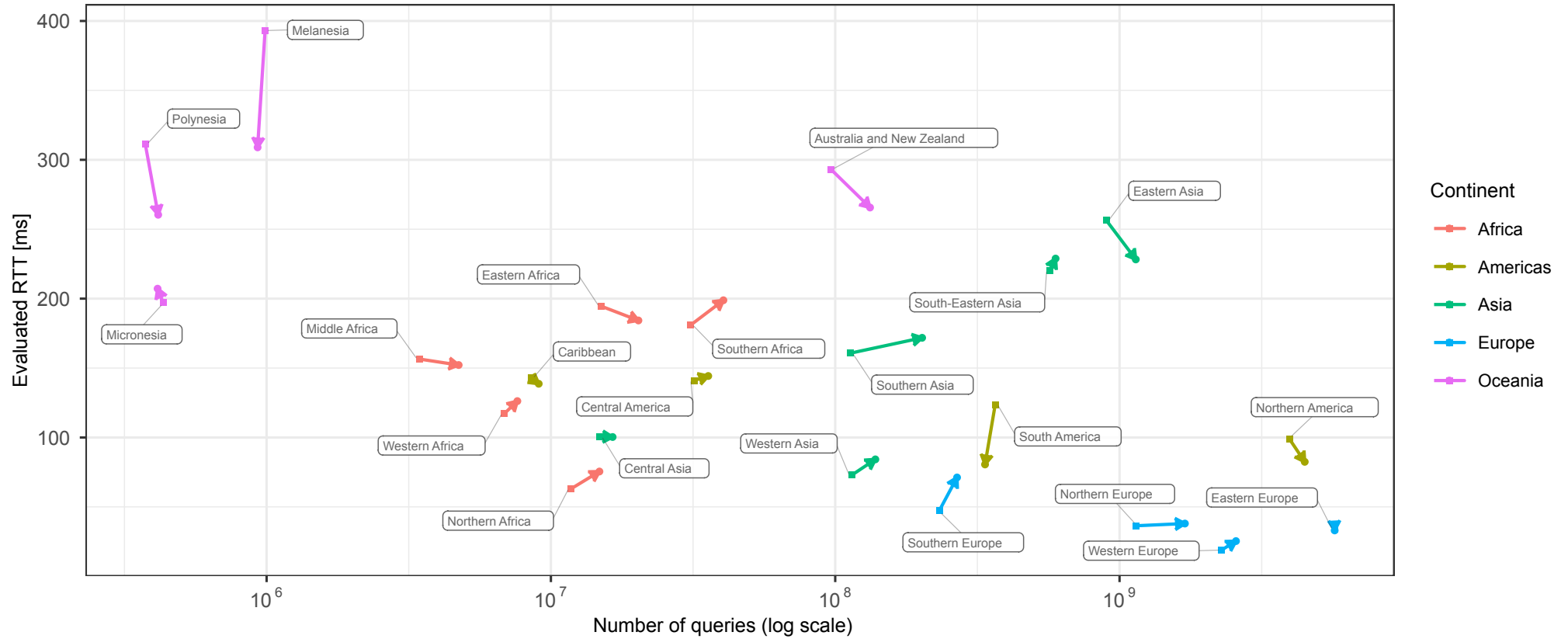
Example of evaluating DNS traffic of a .CZ domain in the world according to RTT

*RTT (round-trip-time) is the time required for communication between the source of DNS traffic and the authoritative DNS server.

5.2.4 Utilisation of .CZ DNS infrastructure

In 2018, the CZ.NIC Association agreed on commercial cooperation with the Canadian organisation CIRA (Canadian Internet Registration Authority), consisting in the operation of part of the secondary DNS servers of the .CA domain. This cooperation continued successfully in 2019. The Canadian register counts more than 2.8 million domains and is, therefore, approximately twice the size of its Czech counterpart. From a technical point of view, it shares the capacity of DNS servers that are primarily intended for the .CZ domain with another entity. Due to significant upgrades in recent years, this capacity is dimensioned many times higher than the real utilisation and therefore it is useful and beneficial to use it for other projects as well.
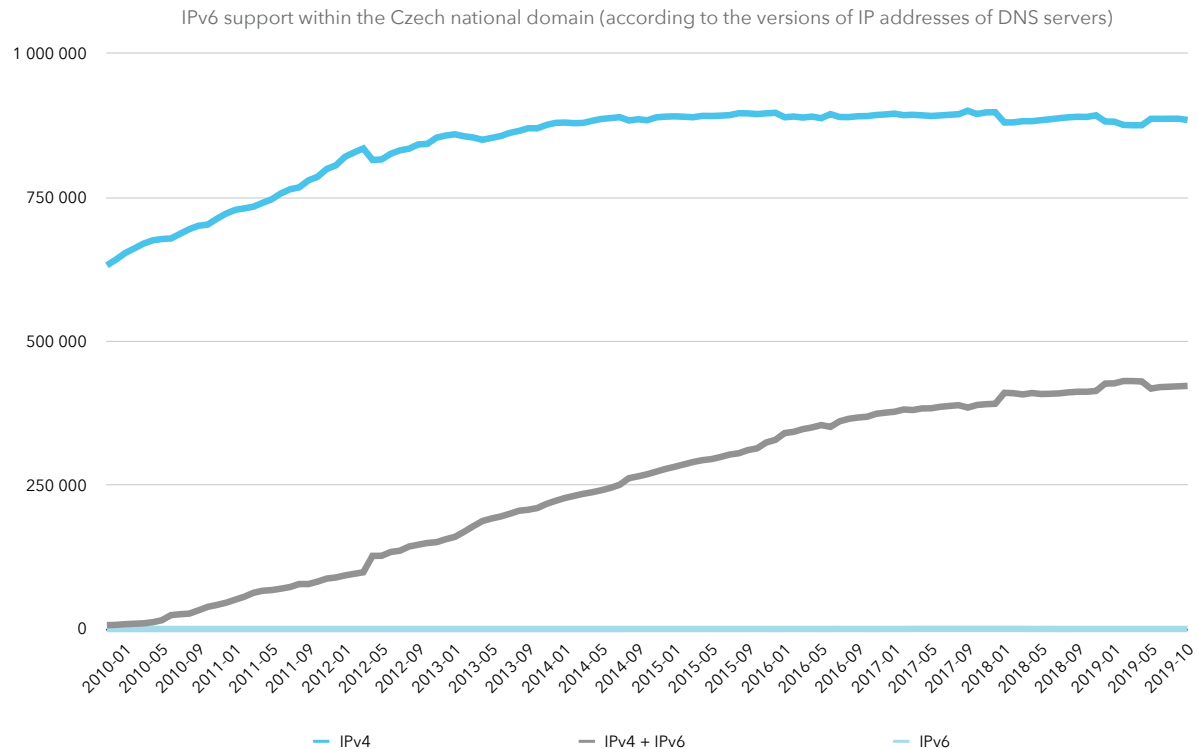
5.3 Support for internet infrastructure

5.3.1 IPv6 support

IP addresses are the basic building blocks of the internet. Without IP addresses, it is not possible to connect to the global network, which also prevents mutual recognition and interconnecting computers. The current space of IP addresses of the version 4 (IPv4) internet protocol has essentially been exhausted. The new, version IPv6 internet protocol is the response to the lack of IPv4 addresses, as it offers a much bigger bank of addresses and also new options.

The long-term goals of the association include supporting the deployment of this technology at all levels, i.e. content, networks and end devices. CZ.NIC also cooperates with registrars that often provide webhosting, so it can seek support for IPv6 on the side of web, e-mail and DNS servers. The association also participates in promoting IPv6 in state administration.

Thanks to these activities, IPv6 has been enjoying growing support in the Czech Republic and, according to independent surveys our country, belongs among the world powers in IPv6 introduction.

IPv6 support within the Czech national domain (according to the versions of IP addresses of DNS servers)


IPv4   IPv4 + IPv6   IPv6

5.3.2 DNSSEC support

DNSSEC is an extension of the domain name system (DNS), which increases its security. The DNSSEC technology gives the users the certainty that the information they obtained from DNS was provided from a correct source, that it is complete and that its integrity was not compromised during the transfer. The DNSSEC technology has been available since 2008 within the Czech national domain .CZ. The number of such secured domains has grown steadily since then, and cooperation with registrars also contributes to this. At the end of 2019, the DNSSEC support rate for .CZ exceeded 59%. With its share of signed domains, the Czech Republic clearly ranks among world leaders. Last November, the international IANA organisation appointed the managing director of the association, Ondřej Filip, to the prestigious group of Trusted Community Representatives (TCR). This group was formed on the basis of efforts to increase the security of the DNS system using DNSSEC technology. Besides support from registrars, DNSSEC has been gradually introduced among main internet connectivity providers in the Czech Republic, which has made this system fully functional for the majority of standard internet users.

The high support for DNSSEC for the .CZ domain is, among other things, aided by the support of the DNSSEC key automation management, which CZ.NIC introduced in 2017 as the first in the world. This was made possible by introducing support for the new RFC 7344 and RFC 8078 standards in the FRED domain administration system. These standards are thus available to all TLD administrators who use the FRED system. Administrators of authoritative DNS servers will then be assisted in the implementation of this simplification via KNOT DNS, which is also compatible with these standards. DNSSEC can now be easily deployed for those domains where it was not previously possible (e.g., for domains that the DNSSEC registrar does not support), or for domains that are administered by someone other than the registrar. However, this technology is also interesting for registrars.

Development of the number of .CZ domains with / without DNSSEC

without DNSSEC   with DNSSEC
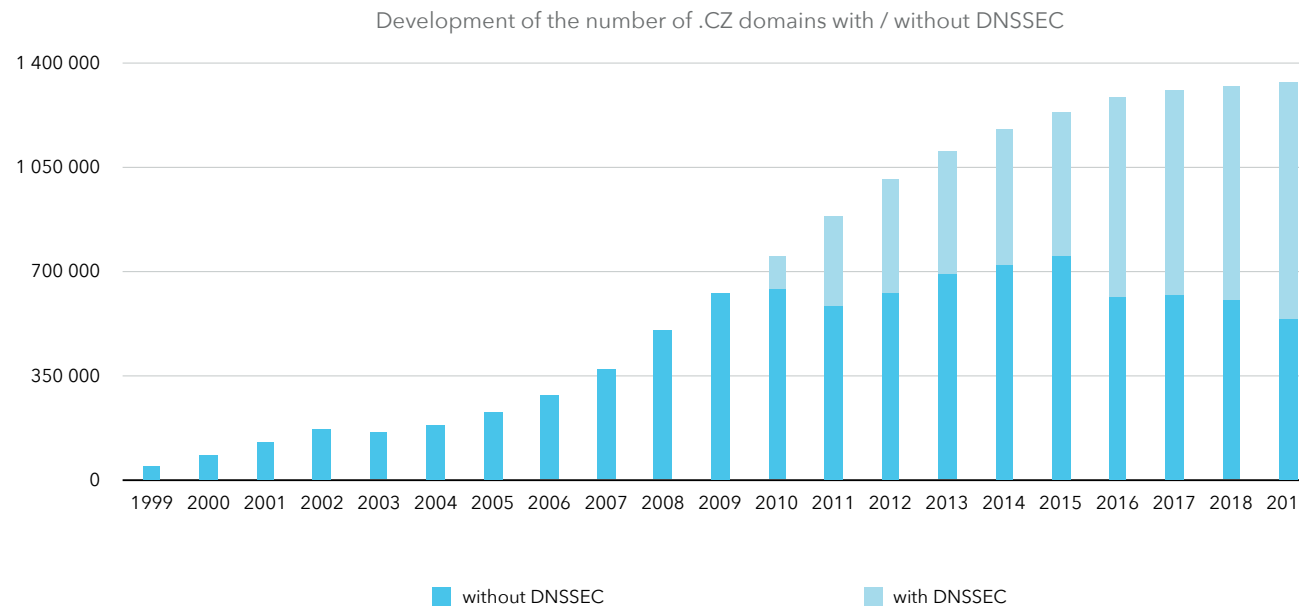
Development of the number of domains under the system of DNSSEC key automation management
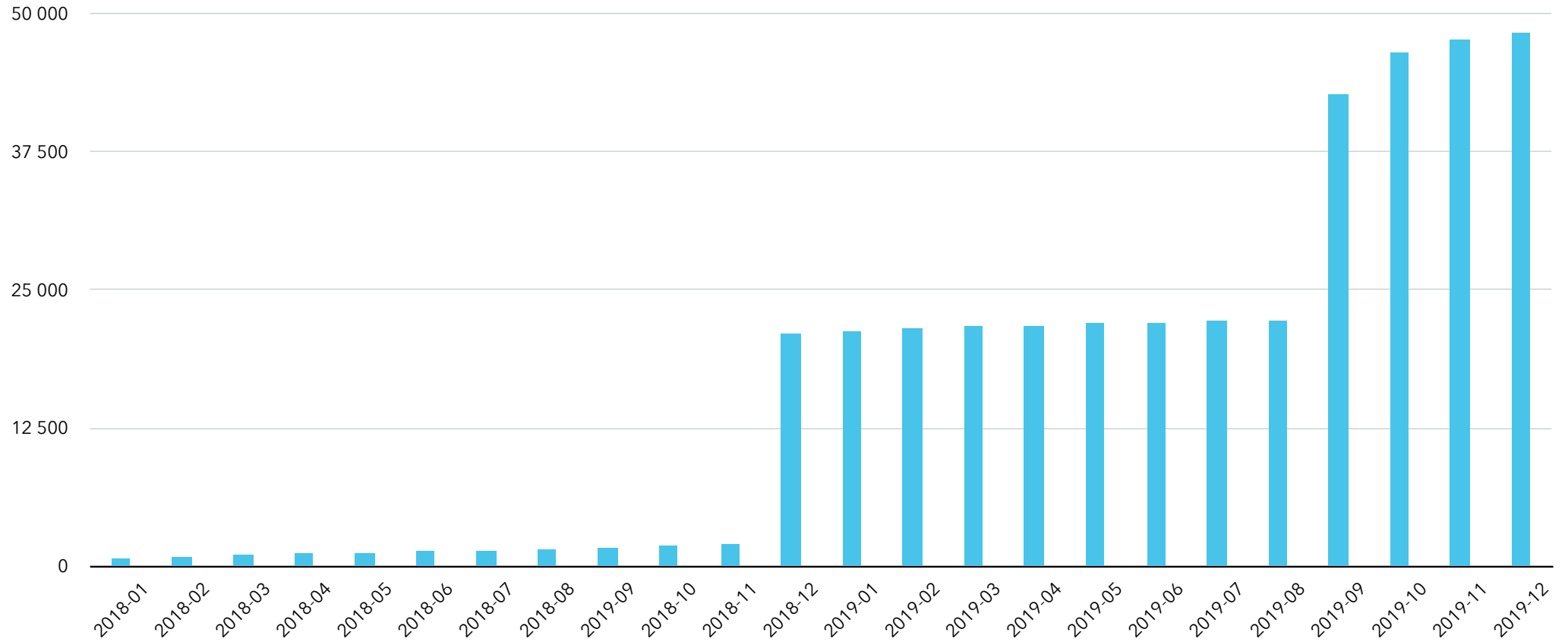
5.4 Support for basic internet infrastructure

The CZ.NIC Association continued to operate mirrors on root servers F, K and L. Therefore, CZ.NIC runs mirrors on three of a total of thirteen root name servers that are the basis of the Internet Domain Names System (DNS). Their operation improves, not only the security and stability of the root server system on a global scale, but also their availability in the European region. In 2019, the association actively assisted in the upgrade of the L root server infrastructure.

Besides these root servers, the association uses its infrastructure to support growing registers through secondary name servers for their ccTLD. Angola, Tanzania and North Macedonia and, since 2019 also Malawi, are using this option for the administration of their national domains. In 2019, the association also began operating in its data centres the infrastructure for the operation of the DNS register of Brazil's domains and the association of Latin American ccTLD LacTLD.

Another form of support aimed at the local internet community is hosting servers of some non-profit organisations – such as the Jeden svět na školách (One World in Schools) project server of the People in Need organisation, or operating a server with a mirror of popular Linux distributions – Ubuntu, Debian, Fedora, etc.

Since 2010, the association has also operated Open DNSSEC Validating Resolvers (ODVR), which are freely available instead of the standard DNS resolvers offered by connection providers. In 2019, a new infrastructure of this service was installed and is now running on the association-developed KNOT Resolver. Thanks to this, ODVR also supports DNS communication encrypted using DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT).

By installing a dedicated anycast infrastructure for ODVR, it was separated from the anycast infrastructure for the .CZ domain (from the point of view of sharing hardware as well as IP addresses), thus increasing the security of both services. In the course of 2019, the association intensively communicated the need for users to switch to this new infrastructure; at the end of 2019, most of the traffic was handled from it and the association was able to plan the shutdown of the original infrastructure in 2020.

CZ.NIC is also actively involved in the RIPE Atlas Global Monitoring Network project. As one of the first organisations to support this project, the association hosted fixed monitoring points called the RIPE Atlas Anchor.

One of the key operating conditions of many computer systems is correct time synchronisation. Systems connected to the internet for this purpose use the NTP Internet Protocol. CZ.NIC hosts a public top-level NTP server (stratum 1) controlled by GPS and fitted with a high-quality oscillator of the OCXO DHQ type.

6 The CSIRT security team

The growing importance of the internet and the rising number of its users are connected with a growing number of security incidents (misuse of PC, a network element or network for an illegal purpose, e.g., spam, copyright breach, phishing, tapping of data), and the severity has been growing as well. This creates an acute need for creating efficient protection against these attacks and giving it a formal shape. CSIRT teams (Computer Security Incident Response Teams) are created for this purpose. CZ.NIC, an entity with long experience with internet infrastructure projects, engages security teams on the national and academic levels. The association also has its own CZ.NIC-CSIRT team responsible for dealing with incidents within AS25192, as well as incidents that affect the name servers for the .CZ domain and 0.2.4.e164.arpa.

An example of the recognition of CZ.NIC activities in the field of cyber security and projects on which CZ.NIC has been working for many years is that, on the occasion of the 20th IS2 – Information Security Summit, the managing director of the association, Ondřej Filip, received an award for contribution in the field of cyber security in the Czech Republic and entered the Cybersecurity Hall of Fame.

6.1 CSIRT.CZ – National CERT Team of the Czech Republic

The CSIRT.CZ security team is the official national security team of the Czech Republic and is operated in accordance with Act No. 181/2014 Coll. on cyber security, and the public contract concluded on 18

December 2015 with the National Security Authority (NSA). As of 1 August 2017, the newly established National Cyber and Information Security Authority (NÚKIB) took over the position of the NSA and thus became the manager of cyber security issues and the national authority for this area. The mission of the CSIRT.CZ team is to deal with incidents connected with cybersecurity in networks operated in the Czech Republic.

The team collects and evaluates information on reported incidents and forwards such incidents to persons responsible for the network or services being the source of the incident and/or provides help with coordination. In its activities, the team cooperates with entities at the national level (in particular the NÚKIB, the Police of the Czech Republic (PCR), academic CSIRT, internet providers (ISPs), banks and others) as well as at the international level (national CSIRTs of other states, the European Network and Information Security Agency (ENISA), EUROPOL and others), with which the team exchanges information on individual incidents and their solutions based on mutual trust.

CSIRT.CZ also participates in a number of grant projects, including PROKI (Prediction and Protection against Cyber Incidents), which is supported by the Security Research of the Czech Republic in 2015-2020.

In 2019, there was further development in the PROKI project. A complete upgrade of the used open source products was performed, which brought, for example, greater possibilities for securing the data used in the project.

A new addition to the project is access to the outputs of daily large-scale scans performed by the Shodan service, mediated by the Austrian CERT team for the entire Czech Republic. Although the nature of these data is different from those processed by the PROKI system, the data from Shodan can provide an interesting context for the interpretation of data

from PROKI. They include not only vulnerable and faulty services but also the overall state of the network – for example, what service is running on a particular device.

The involvement of data from the Shodan service made it possible to test a new way to analyse data, where by comparing the Shodan service information and the information in PROKI, it was possible to identify IP cameras that were compromised and were being exploited by attackers for further attacks.

The same principle was used in 2019 in cooperation with the community, when CSIRT.CZ, based on the received list of Industrial Control Systems (ICS) devices allocated to IP addresses in the Czech Republic, made a comparison with information in the PROKI system allowing the identification of those ICS devices which most likely had already been compromised and could therefore pose a significant security risk. The operators of these devices were warned of the potential risks.

The team also continued to cooperate on the SIC CZ project (Safer Internet Centre, which is implemented by the CZ.NIC Association under the "Bezpečně na netu" ("Safe on the Net") brand), more precisely on the operation of the STOPonline.cz hotline, which is intended for reporting illegal online content, and was involved in the education and training of children and parents. Another project in which CSIRT.CZ successfully participated in 2019 is the Cyber Exchange project. Its essence is the technical and administrative exchange of experts across the national and governmental security teams of the EU Member States involved in the project. For example, the project created an open-source envelope library, which allows programmers to use comprehensive support for PGP and S/MIME standards when working in Python or Bash. During 2019, the project called Support for the Development of Cyber Security Capacities in the Czech Republic, which supported further deepening of national and international cooperation, as well as extended education and training

of CSIRT.CZ team members, was completed. As part of this project, for example, we published the regular educational series, "Observations in Security," on the Root.cz server.

6.1.1 Traffic statistics

In 2019, CSIRT.CZ handled 954 security incidents. At the same time, the number of responses related to the resolution of those incidents increased again. A total of 13,883 e-mails were sent, i.e., 3,821 more compared to the previous year. Up to dozens of e-mails sent can be associated with a single incident due to the complexity of the attacks (botnets, vulnerable devices, compromised accounts, etc.).

The open-source Convey tool was developed by CZ.NIC security experts as early as 2016 to automate communication regarding security incidents involving multiple parties. In 2019, the Convey utility was enriched with additional features that allow team members to work much more efficiently. These include, for example, learning how to work with LACNIC quotas or the ability to convert specific values across 50 data types. At the same time, the installation of this tool was simplified. Thanks to its publication on GitLab, it can now be used by all security teams in the community and beyond.

In 2018, the "csirt.cz-boost" browser add-on was created to speed up work with internally used applications – especially OTRS. In 2019, this add-on was enhanced to automatically determine the language of the response template based on the recipient's domain, display a small preview of the problem page, or automatically recalculate the metadata required to resolve specific incidents.

Number of incidents addressed

	2012	2013	2014	2015	2016	2017	2018	2019
Sensor Network*	3,924	2,121	2,380	3,771	9,944	13,858	18,435	14,911
Phishing	159	175	368	367	363	409	518	483
Spam	43	73	159	108	290	121	144	128
Malware	20	45	117	240	104	99	135	85
Other	14	75	102	264	181	200	58	85
Trojan	5	12	56	90	79	94	0	0
Probe	12	26	86	42	13	26	171	141
DOS	68	72	32	37	12	14	7	16
Botnet	8	15	0	4	71	29	20	4
Virus	0	0	0	0	0	0	0	0
Portscan	1	3	2	5	6	13	16	3
Pharming	0	0	18	3	2	3	10	9
Total	330	496	940	1,160	1,121	1,008	1,079	954

* Sensor Network is not included in the total number

The incident resolution process also includes the distribution of information in the case of vulnerable systems.

The statistics of individual types of incidents are still dominated by phishing, followed by the incident type referred to as Probe. This type of incident includes, among others, brute force attacks on user accounts, i.e., attempts to crack the password on targeted machines. This is a type of attack where the attacker, after finding out the login information, can misuse the attacked machine to their advantage and commit other attacks in cyberspace. These practices are currently very popular among attackers. Spam ranks third in statistics.

6.1.2 Awareness and educational activities

Throughout 2019, members of the CSIRT.CZ team spoke at various conferences and participated in expert groups (Internet and Technology, CSIRT.CZ Working Group, Safe Internet, TF-CSIRT, Police Academy of the Czech Republic, Safe Internet Festival (FBI19), Addressing Electronic Violence and Cybercrime , Ministry of Industry and Trade of the Czech Republic). The team members also commented on current events in the media when necessary.

In addition, a new training called "Introduction to forensic memory analysis" was prepared in 2019 and successfully premiered in December. In total, CSIRT.CZ implemented four runs of the Security and Privacy on the internet training and two specialised trainings for the Police of the Czech Republic. Furthermore, it organised one training for employees of Nestlé Česko s.r.o., one specialised training for the State Office for Nuclear Safety and one for the Czech National Bank.

Other publishing activities included the publication of awareness-related and educational articles. Specifically, these were twenty-four episodes of the series *Postřehy z bezpečnosti* (Perceptions of Security) on the Root.cz server and a number of thematic contributions on blog.nic.cz. According to current topics and the situation in the field of cyber security, articles were also published in the print media: it is worth mentioning articles in the IT Systems magazine on the security of the MQTT protocol or on risk modelling in CVSS. CSIRT.CZ also continued publishing manuals for administrators and users on its own website.

In 2019, CSIRT.CZ, in cooperation with the CZ.NIC Academy, also organised training for security teams in the Czech Republic by foreign lecturers from the ENISA agency (Mobile forensics, Memory forensics).

6.1.3 National and international cooperation

The strategic partner in the field of national cooperation is NÚKIB and the Government Team of the Czech Republic, i.e., GovCERT (Government CERT). CSIRT.CZ cooperates with these entities, for example, in the field of legislation, cyber exercises, formulation of common positions within the CSIRT Network and other projects. National and Governmental CERTs meet several times a year on various occasions, providing a sufficient scope for regular information provisions on the work of individual teams and their possible coordination. In addition, both organisations regularly participate in meetings within the TF-CSIRT or CSIRT Network.

To successfully resolve incidents, it is important to maintain contacts with Czech internet providers. CSIRT.CZ Working Group meetings are important because they aim, precisely, to improve communication and cooperation at the national level. An unwritten rule was that in the first half of the year, the association organised a "large" CSIRT.CZ Working Group, to which all those interested in cyber security issues were invited. There is always great interest in this meeting. In 2019, the Working Group addressed topics such as sensitive data and vulnerabilities on the Czech web, the NERD and PROKI systems, the DANE protocol for secure mail transport, DNS firewall and more. The participation of representatives of Military Intelligence, who came to discuss with members of the working

group on the draft amendment to the Military Intelligence Act, was also very valuable.

National and international cooperation also includes support for teams wishing to join TF-CSIRT and FIRST. For some types of membership, this includes the so-called on-site visit, which involves checking the functionality and compliance with requirements for applicants who want to join these organisations.

In 2019, CSIRT.CZ participated in international exercises, such as Locked Shields (technical exercises organised by NATO), Cybersecurity Summer BootCamp, CyberSOPex 2019 and selected SANS Institute trainings.

6.1.4 Preventive activities

The year 2019 was again dedicated to the area of prevention, especially the continuation of information extraction from operated honeypots and the development of the PROKI project, where we managed to achieve the aforementioned significant qualitative shift in analysis thanks to the inclusion of data from the Shodan service.

In 2019, information related to the vulnerability of CVE-2019-11510 in Pulse Secure VPN, allowing a potential attacker to access users' private keys and passwords, was distributed. For this reason, the association asked Bad Packets LLC, which identified the vulnerability, to provide a list of vulnerable servers that it diagnosed in the Czech Republic. A notice was sent to those entities.

6.1.5 Web scanner

The web scanner is one of the preventive security services that was launched in 2013. This service is intended for website providers and administrators, whom it helps to reveal the potential vulnerability of their internet presentations. The service is intended, primarily, for non-profit organisations and public administration. A vulnerability analysis is performed in two phases.

First, with the use of automatic tools and then in a manual website test by a senior tester who evaluates, among other things, the vulnerabilities he/she found in the entire website and offers corresponding solutions. At the end, the party that ordered the test is sent a final report containing detected vulnerabilities, their classification based on the gravity level and also proposals for possible solutions. In analysing potential vulnerabilities, the service is based on its own measurements, the security team's experience and on a list of the general, top 10 most serious security risks according to the Open Web Application Security Project (OWASP).

In total, 38 domains were tested in 2019 on the basis of 19 orders, of which six were domains of major entities and two as part of the Safer Internet Centre project.

6.1.6 Penetration testing

In 2019, CSIRT.CZ launched pilot operation of a new commercial penetration testing service. The first party interested in using this service was the Vysočina Region. More than 20 domains were tested. Also on the basis of positive feedback from the client, a decision was made to start providing the service in full during 2020.

6.2 CZ.NIC-CSIRT

The CZ.NIC-CSIRT team is responsible for handling incidents that affect name servers for the .CZ domain, 0.2.4.e164.arpa and AS 25192. Based on the Registration Rules, CZ.NIC is entitled to cancel the delegation of a domain name if it is used in such a way that national or international computer security is threatened. This can happen, for example, by distributing harmful content (viruses, malware) or by faking the content of another service (phishing) through the domain name or services available through it. The CZ.NIC-CSIRT team can also cancel the domain name when the server, available through the domain name, is the control centre of networked hardware distributing the malign content (botnet).

Activities of CZ.NIC-CSIRT in 2019

CZ.NIC-CSIRT operates its own system used for searching websites with .CZ (MDM) domains that have been attacked. In the CZ.NIC Association, the CZ.NIC-CSIRT team implements internationally accepted information security management systems (ISMS) in compliance with the ISO 27001 standard. An external audit took place in 2019 to confirm that CZ.NIC continues to meet all requirements of that standard. In connection with the designation of the .CZ domain register as a basic service, in 2019 CZ.NIC-CSIRT focused on mapping the statutory requirements for basic service operators, amending internal guidelines and preparing documents for the technical department, which implements some of the requirements.

7 **MojeID**

MojeID is a unique service that enables internet users in the Czech Republic to use uniform identification data to log in to various internet services. This service, operated by the CZ.NIC Association, was put into operation in 2010, and has thus been serving its users for the tenth year in a row.

If an internet user uses mojeID, they do not have to create a separate account for each new service and go through a lengthy registration process. Instead, they enter their registration data only once into mojeID, where this data is verified and then used to sign up for internet services. Operators implementing mojeID will not only increase their users' comfort in using their service but will also get verified information about their visitors, to whom they can subsequently provide additional benefits.

The mojeID service is based on the OpenID standard, extended with unique features that other OpenID services do not have – e.g. user identity data transfer with every user login and user validation on multiple levels in different ways.

In the development of this service, emphasis was placed on the security and trustworthiness of the entire system, as well as on the protection of personal data. The register of user details is protected on the same high level as the .CZ domain register. Users, themselves, can define which details from their profiles can be provided to the given provider for whose services the user wants to sign up using mojeID. This gives the user full control over their data. The user also knows what data they provided to what entity and when.

The service is constantly evolving and responding to the current needs of its users. In recent years, for example, it introduced a public profile that allows mojeID to serve as an internet calling card, the possibility of directly opening mojeID and prepopulating data directly from Facebook, LinkedIn and Google user accounts, and a complete redesign of websites.

The year 2019 was focused on increasing user convenience and safety. Users must now authorise via SMS when changing their password, and they can now also use a security key with the FIDO 2 standard for authentication. To increase the convenience of account validation, a new free option for validating the mojeID account was introduced by providing consent to transfer data to a third party at Czech POINT sites.

7.1 Support of mojeID

A key factor in the systematic expansion of the mojeID service is its support by internet service providers. The growing number of sites where mojeID can be applied has had an impact on attracting new users, for whom it is important to be able to sign in to as many services as possible with a single username and password – whether they use them on a daily basis or those (e.g. online stores) they visited for the first time – and mojeID has saved them time in registering and provided control over the information they provide.

In relation to service providers, in addition to seeking to penetrate new segments, the focus is on maintaining or consolidating positions in existing areas, such as e-shops that are interested in verifying the maturity of their customers for specific goods or services, community servers, web presentations of cities and municipalities, citizen portals or library systems.

In 2019, there was significantly greater interest in the mojeID service on the part of developers for cities and municipalities. These are mainly so-called citizen portals. Cooperation with Datron and Vera developers has been ongoing for years. There are also a number of individual

implementations by smaller developers. MojeID is currently clearly perceived as a means of authenticating and identifying internet users.

7.2 External validation points

The expansion of the network of validation points, which is a means to facilitate the user's validation process, i.e., the highest level of validation in the mojeID service, continued in 2019. New validation points were opened mainly in towns and villages in connection with the Citizen Portals – Bílovice nad Svitavou, Lysá nad Labem, Turnov and Kraslice.

In 2019, the agenda of validation points was extended to verify the contact upon its transfer from the central register (i.e., the register for registration of domain names in ccTLD .CZ) to the identity register (i.e., to the mojeID service) with the change of data. So far, this verification could only be performed in the form of an authenticated signature.

Systematic work with existing validation points and their employees is also a significant aspect of the operation of the network of external validators. In 2019, the recertification of validators was launched in the form of an updated training course. During the first months after the launch, almost 60% of the validation points were recertified.

7.3 Users of mojeID

The user base is the most valuable asset of the mojeID service. Without an increasing number of users, it would be difficult to attract more and more important service providers and make the service known among the general public. During 2019, the mojeID user base grew by 53,584 new users to a total of 663,286 users.

The trend of an increasing share of validated users continued to rise, reaching a total of 26,219 at the end of the year. This result is attributable to two main factors – the continuing interest in validation, in relation to the Účtenkovka state lottery, and the new possibility to validate the mojeID account via the data box information system or at Czech POINTs.

Account security level of mojeID

Year	Validated contact	Identified contact	Partially identified contact	Users total
2010	163	2,168	1,324	3,655
2011	680	17,218	24,369	42,267
2012	1,760	75,513	86,218	163,491
2013	3,324	143,364	144,376	291,064
2014	5,920	207,242	211,409	424,571
2015	8,280	249,649	241,270	499,199
2016	10,446	273,334	257,650	541,430
2017	18,378	293,503	283,133	595,014
2018	23,233	308,764	301,806	633,803
2019	**26,290**	**344,738**	**318,547**	**663,285**

7.4 MojeID as a tool of cross-border authentication in Europe

In 2019, CZ.NIC also actively participated in the Czech Republic's involvement in building an infrastructure for cross-border electronic identification, as defined by the eIDAS Regulation. This regulation builds on the work under the STORK (Secure idenTity acrOss boRders linKed) pilot project, which our association participated in with the Ministry of the Interior of the Czech Republic. Throughout 2019, the CZ.NIC Association operated a gateway that was created within the framework of the STORK project and which allowed logging into the services of the European Commission using mojeID.
This gateway will be completely replaced in the future by an official eIDAS node for the Czech Republic.

In 2019, the CZ.NIC Association also operated, on the basis of an agreement with the National Registers Authority, a node in the production operation of eIDAS, enabling the use of login means announced by other EU Member States for Czech online services and the middleware component required for login with the German electronic identity card. Germany remained the only Member State that notified its electronic identification means and met the relevant technical specifications throughout the year. During the year, work also began on launching the second component of the eIDAS node, which will enable Czech electronic identity card holders to use them for foreign online services. As part of

contractual performance, active involvement of the association's staff in the functioning of the platforms that were established by the European Commission, namely eIDAS Cooperation Group and eIDAS Technical SubGroup, continued throughout the year.

These initiatives are based on the concept of the association's activities, including, in particular, cooperation with the state in the area of eGovernment expansion. The association will also continue working on the initiatives in 2020.

8 CZ.NIC Labs

The CZ.NIC Labs are an organisationally separate research and development centre that focuses primarily on innovative projects for the benefit of the Czech and global internet community. The projects focus, mainly, on infrastructure protocols and services, DNS traffic monitoring and network security. Some of the projects deliberately support major trends in today's digital society, such as open data, eGovernment, open source software and support for disadvantaged users. The CZ.NIC Labs are represented in all regional branches of the association, i.e., not only in Prague, but also in Brno, České Budějovice and Plzeň, and therefore they make intensive use of tools for distributed software development and other means for remote cooperation (video conferencing, discussion forums, etc.). The CZ.NIC Labs and employees working on their projects have a very good reputation abroad. This is also confirmed by the fact that Maciej Andziński, research and development programmer, received the R&D Working Group Champion Award. The award is given every two years by the CENTR organisation, which brings together European and other domain registers.

Brief summary of 2019 activities

In 2019, the CZ.NIC Labs focused primarily on further development of existing projects. Key projects are:

– The ADAM system for monitoring and analysis of services provided by the association,
– Multiprotocol routing daemon BIRD,
– Pair of DNS servers – authoritative Knot DNS and recursive Knot Resolver,
– Tablexia educational application for children with dyslexia and other learning difficulties,
– Turris router for end home and SOHO network security.

8.1 ADAM – monitoring and analysis of DNS traffic

An important prerequisite for the reliable operation of DNS servers in the .CZ domain, domain register and other services provided by the association is, among other things, systematic and detailed monitoring of real DNS traffic and its immediate and additional analysis. These procedures can detect potential technical problems or network attacks to which the DNS infrastructure is permanently exposed in a timely manner, but also effectively plan further development of the infrastructure and services.

The ADAM (Advanced DNS Analytics and Monitoring) project aims to develop tools for effective and robust collection and processing of data on DNS transactions, to improve and expand the methods of their analysis, and to develop appropriate user interfaces and reporting methods.

In 2019, the first version of the DNS probe was completed in cooperation with FIT BUT Brno. It is a software tool for high-speed processing of DNS traffic in real time, generation of selected output data in C-DNS or Parquet format and their subsequent storage on disk or sending to a remote collection point. The DNS probe will be gradually deployed to all DNS servers that are administered by the association and will replace current inefficient procedures.

Another software tool developed in 2019 is the DNS crawler. Its task is to obtain and verify selected data from DNS for a given list of domain names, but also to obtain information from the web and mail server of each domain. The DNS crawler architecture allows the user to communicate with multiple domains simultaneously (even from multiple cooperating computers), thus enabling data processing from a large number of domains in a relatively short time. For the year 2020, the DNS crawler will be used to regularly scan the entire .CZ zone with the aim of early detection of configuration and security issues.

In the area of publishing the outputs of the ADAM project to various groups of recipients (internally for the purposes of the association, to registrars and members or to the general public), an application programming interface such as REST API was designed and implemented to enable the user to obtain various data and statistics in machine-readable form suitable for further processing. Additional data items are added to the interface on an ongoing basis.

8.2 BIRD

The routing daemon for dynamic IP protocol routing is designed for Linux and BSD. The project began at the Faculty of Mathematics and Physics of Charles University, and the CZ.NIC Labs are participating in its further development. It is currently the most used route server software in peering centres in the world. According to a survey conducted by EURO-IX, more than two-thirds use it.

In 2019, five new versions 2.0.x and four older versions 1.6.x were released. The main task of working on this software in 2019 was to stabilise the new 2.0.x branch so that it could be deployed in a production environment.

This was completely successful and users are already routinely migrating to this series. No new features are added to versions 1.6.x. Another important innovation will be a change in the architecture to support multithreading, which will be a task in 2020.

8.3 Datovka

The Datovka project is developing a multiplatform application for efficient operation of data boxes in the ISDS system. The application is available as open source software for Windows, macOS and Linux desktop operating systems, as well as for both major Android and iOS mobile platforms.

In 2019, users were offered mobile key login support in both desktop and mobile applications. Configuration files were simplified in both applications – configurations that do not directly affect user accounts are stored in separate databases.

Modifications were made to the desktop application to allow the application to work in an isolated environment (sandbox). It is now possible to change the login name of existing accounts on the desktop in the event new user login information has been generated for the data box.

The mobile application added the ability to work with files in iCloud on iOS devices. Similar to the ISDS web portal, it is possible to create text attachments of data messages in PDF format in the mobile Datovka. Support for backing up stored data as well as restoring them from backup was also added.

8.4 Knot DNS and Knot Resolver

Knot DNS is a software implementation of an authoritative DNS server. Its main goals include achieving high performance in processing DNS queries and efficient administration of large TLD zones, including advanced automation of DNSSEC signing. After ten years of development, not only were the main goals of the project achieved, but the project also gained recognition in the DNS community and among users.

In 2019, great attention was paid to performance optimisations when signing DNSSEC. Thanks to this, Knot DNS was successfully deployed by DENIC (the administrator of the German .de domain) to sign the German zone, which made it possible to significantly reduce the delay between the modification of the zone and its promotion to public DNS servers. Knot DNS was also successfully deployed by DK Hostmaster to sign the Danish zone.
Based on ongoing communication with other European national domain administrators, it can be expected that further significant deployments will be added in the future.

The Knot Resolver project is developing an independent implementation of a recursive DNS resolver. In 2016, it was deployed as the default resolver for Turris Omnia routers. It underwent another major deployment in 2018, namely on the public resolver Cloudflare at IP address 1.1.1.1. In the same year, protection against Random Subdomain attacks using the so-called aggressive DNSSEC cache was added.

In 2019, experimental support for the DoH protocol was added and optimisation was performed to improve throughput. Knot Resolver was given further deployment indirectly when Whalebone based its own DNS solution on it. As a result, in early 2020, Knot Resolver is used by more than a hundred ISP and telecommunications operators.

8.5 Tablexia

Tablexia is a modern educational application for children with dyslexia at the second level of elementary school. It is intended for use both in schools as a supplement to standard teaching and in pedagogical and psychological counselling centres, and other counselling facilities for pupils with learning difficulties.
It is available for free in Google Play and the App Store, and a desktop version can be found on the project website.

In 2019, the association joined the Safer Internet project. Within this cooperation, attention was paid to the development of two new games focused on the training of spatial orientation and memory. These areas were chosen because the excessive use of applications and mobile devices affects cognitive abilities and, in particular, attention, memory, concentration and spatial orientation.

This created the games called Archiv (Archive), where the main goal of the detective is to remember and correctly assign items to the numbers marking the items, and Na stopě (Following the Trail), where the detective must get their bearings in the city and track down the thief before the thief disappears. At the end of 2019, the games were ready for release and testing with children. Attention training is planned for 2020.

During the year, minor bugs in the desktop version of the application were resolved and some graphic modifications were also made, especially in connection with the situation where players manage to achieve all trophies and all detective ranks. Animation was created for these cases and a completely new environment was designed.

8.6 Turris

The beginning of 2019 in the Turris project was marked by the completion of a new modular secure network device, Turris MOX. During the first half of 2019, all Turris MOX devices intended for the first customers – supporters of the crowdfunding campaign – were distributed. In the second half of the year, the device was put up for retail sale in the Czech Republic and abroad.

Following the campaign, some new features were also developed for the Turris OS, i.e., the easy possibility of installing Nextcloud and the related support for multiple disks and the ability to boot over a network and administer multiple routers from one place.

At the same time, as a result of the successful sale, stocks of the Turris Omnia routers began to run low. Production of another series began in the autumn of 2019. The new routers received FCC certification and can therefore be sold in the USA, which should lead to an increase in

awareness of the Turris project and to the expansion of the data collection network to new locations in 2020.

The development of the Turris OS – a system that drives Turris devices – also progressed significantly. After initial testing, the version of the system Turris OS 4.0 built on the new version of OpenWRT was deployed on the Turris MOX as well as on the newly manufactured Turris Omnia routers. Thanks to a change in the development model of new versions of the Turris OS during 2019, CZ.NIC made a significant contribution to the open-source project OpenWrt and brought the Turris OS developed by the association closer to a more upstream project. At the same time, work began on a plan to automatically migrate older devices to the new system without compromising user configuration.

Other interesting features that are definitely worth mentioning include cooperation with RIPE, where we managed to integrate software from the RIPE Atlas project. Any Turris router can thus be easily turned into a probe and contribute to global statistics on the state of the internet.

The web interface for controlling the router also underwent major changes, especially below the surface. Future changes should facilitate further expansion and at the same time unify the look across functions. Users have been given a new version available for testing. It includes new features as well as a redesigned look and feel for greater user comfort.

The new data collection system has also made great progress. It is now offered as part of Turris OS 4.0 and higher, and during the year it was supplemented with a number of new minipots – attacker traps. It was also further promoted and received interest from users. As part of the project, the website view.sentinel.turris.cz was launched, containing global statistics on attacks and providing unique insight into internet security. At the same time, the defence part – a dynamic firewall – was made available to the professional public for private use and protection of their

own servers. Next year, we plan to implement additional attacker traps, allow users to access statistics only from their devices, and provide better control over the services operated directly on the router.
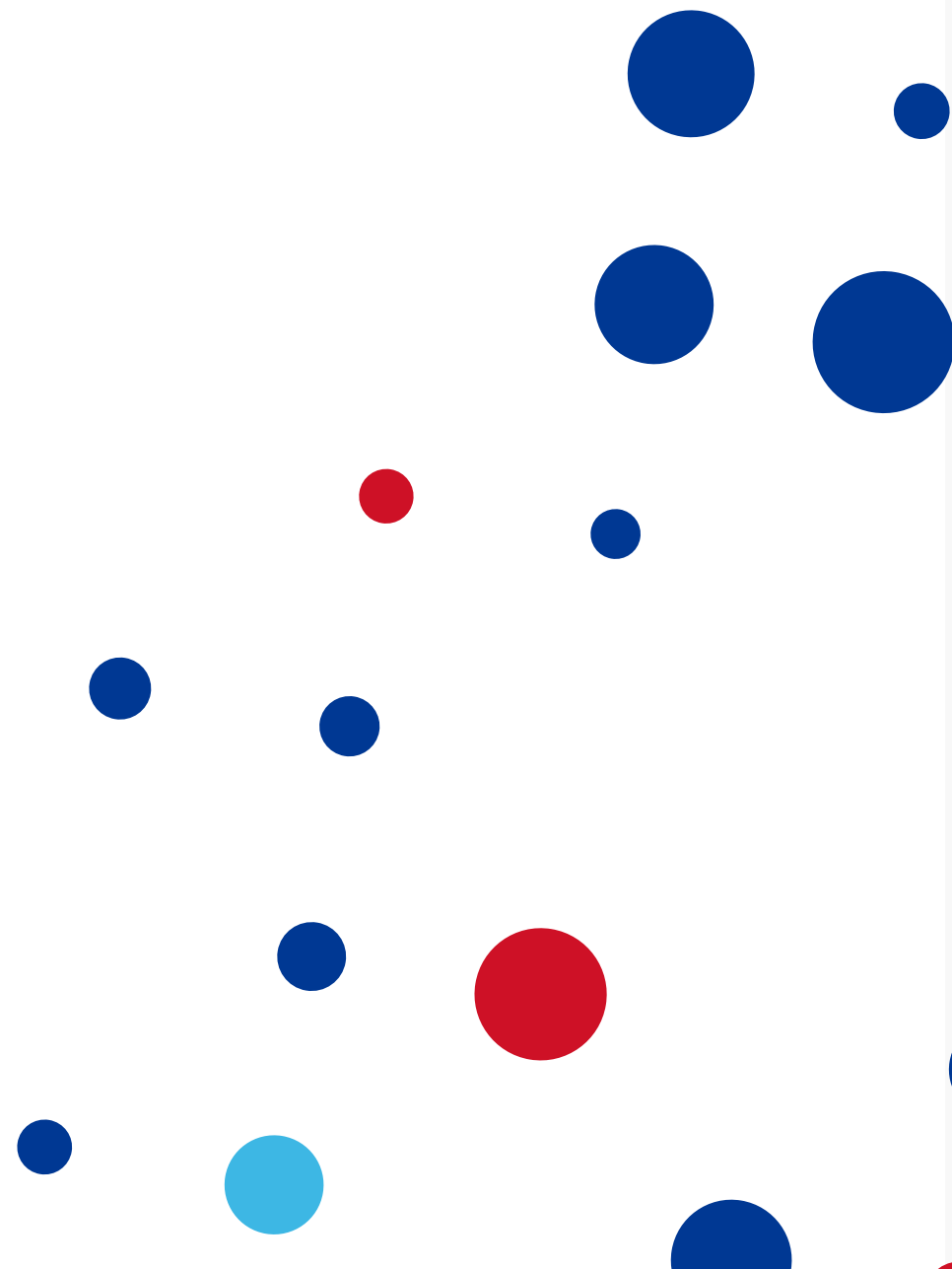
9 Education and awareness

9.1 Communication with the public

In 2019, the already established and proven cooperation with public and private media continued. Newspapers, radio and television stations and major media servers dealing with the internet and technologies thus provided news about the CZ.NIC Association.

The association issued 14 press releases and 20 press announcements, the recipients of which were professional journalists as well as journalists from the media aimed at the general public or specific groups of recipients. CZ.NIC publishes these releases in the News section at www. nic.cz. The News section is also part of the information website of the association's education centre (CZ.NIC Academy), the CSIRT.CZ security team and selected projects of the CZ.NIC Labs.

The communication mainly covered topics related to the basic activities of the association, its key projects and activities, and also topics related to the activities of the association, such as cyber security, personal data protection and education and awareness in the field of the internet and internet technologies.

As in previous years, press releases appeared mainly in technically-oriented media. The most frequent portals were Root.cz and Lupa.cz. In printed form, these were mainly the *Securityworld* and *IT Systems* magazines. Topics related to the online safety of children on the internet were then presented in the *Řízení školy* (School Management) magazine.

In 2019, CZ.NIC employees published more than 60 original articles. Ondřej Filip, managing director of the CZ.NIC Association, as well as other employees, were guests on television and radio programmes,

mainly on Czech Television, Czech Radio and Frekvence 1. The audience was interested in topics related to security in cyberspace, mobile internet and the Czech national domain.

For administrators of the Czech national domain, accounts on social networks – Facebook, Twitter and Google+ (only until April 2019) and newly also LinkedIn – are an integral part of communication with the public. Supporters are informed, in regular contributions, about the activities of the association, events and current happenings in individual projects. The most watched account was the Twitter account, which had 4,297 followers at the end of the year, 9% more compared to 2018. This was followed by the Facebook account, where the association had 2,984 fans. A new measure was the revival of the LinkedIn account – 1,040 people signed up to follow it.

An important part of communication is also the NIC-NEWS newsletter, through which messages are sent to subscribers to the e-mail conference of the same name, and the online CZ.NIC Employee Blog. 47 contributions were published on the blog in 2019 thanks to activities of association employees. The blog serves as the official communication channel of the association, so it is used by journalists from various media.

	Outputs in media		Social networks (fans)	
	Papers	Blog	Facebook	Twitter
2012	21	97	900	630
2013	29	95	1,100	1,000
2014	38	84	1,500	1,750
2015	57	82	1,800	2,370
2016	57	59	2,600	3,088
2017	73	49	2,826	3,573
2018	56	55	2,905	3,942
2019	**63**	**47**	**2,984**	**4,297**

Internal communication is provided primarily by the IN newsletter, which CZ.NIC employees usually receive once or twice in 14 days.

9.2 Popularisation series

The *Jak na Internet* (How to Use the Internet) series is the association's largest educational activity, which is focused on the general public. With its 125 episodes broadcast on Czech Television channels in 2012–2019, it reached a total of 225 million views. In addition to the public service media, the series is also used in local cable television. The popularity of the series is also evidenced by the repeatedly positive results in awareness surveys among the internet public. More than a quarter (25–35 %) of internet users know the programme.

Jak na Internet is no longer just a television series. The YouTube channel that presents the online version of each episode has had approximately half a million total views. The video content can also be found in the entertainment portals of RegioJet buses and trains and on the

Methodological Portal of RVP.cz for teachers. Expanding texts published on the website jaknainternet.cz also gained popularity, as evidenced, among other things, by the fact that they are widely cited in graduation theses (see Theses.cz). The series is also published in a comic book version.

In the past, the CZ.NIC Association also made it possible to create several co-production programmes of Czech Television for children and youth. These included two seasons of the series Nauč tetu na netu (Teach Your Aunt to Use the Internet) and selected episodes from the series Lovci záhad (Hunters of Mysteries). The original series *Nebojte se Internetu* (Don't Be Afraid of the Internet) (nebojteseinternetu.cz) is targeted at seniors. All of the aforementioned video materials were also available online in 2019 and systematically used by organisations that focus on educating the selected risk groups – children and seniors.

9.3 The CZ.NIC Academy educational centre

In 2019, the CZ.NIC Academy expanded its portfolio of courses with three new ones: Sphinx for Documentarians, Cyberbullying and Other High-Risk Phenomena on the Internet, and Forensic Analysis. In addition to these full-time courses, the Academy, in cooperation with NÚKIB, also created a new electronic course, Digital Footprint, for primary school pupils, the aim of which is to protect children from the risks they face in cyberspace.

In 2019, the CZ.NIC Academy provided its rooms, not only for internal training and meetings of the association's employees, but also to other organisations and groups, such as ENISA, the Central Bohemia Education Institute and PyLadies. In the summer, in cooperation with Prague 3, a weeklong children's cyber camp took place at the Academy. The CZ.NIC Academy not only offers rooms but it also provides support for other educational activities. In 2019, it was mainly the SOČ (Secondary-School Specialised Activities) competition.

Development of the number of students in the CZ.NIC Academy

Standard courses   Customized courses   Courses and lectures for schools
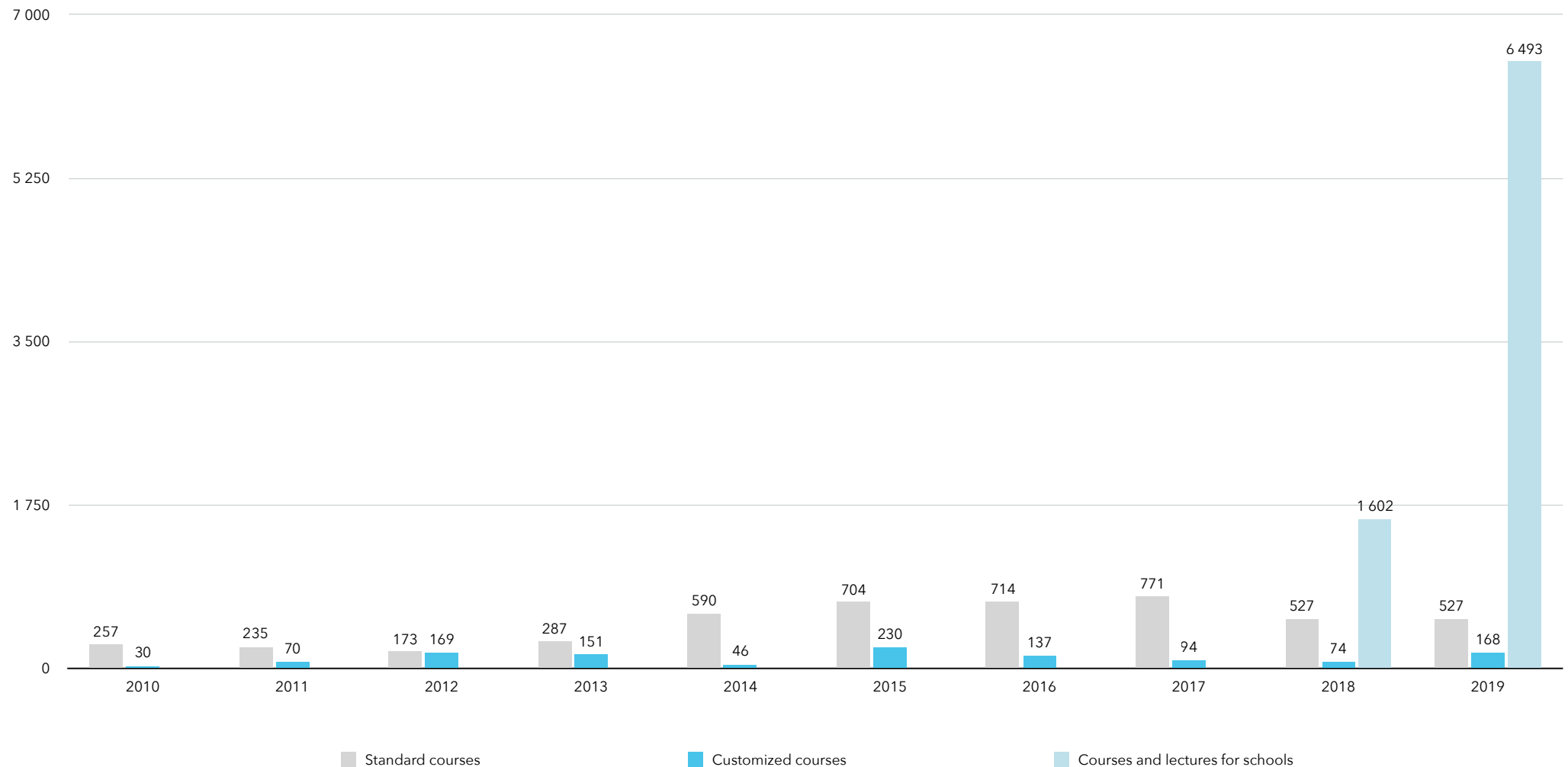
List of professional courses conducted at the CZ.NIC Academy in 2019

Name	Number of courses	Number of students
3D printing	1	7
Ansible – Introduction to Mass Automation	6	88
Internet Security and Privacy	3	28
Security of Mobile Applications	1	8
Security of Web Applications	1	5
Barrier-Free Digital Design for Beginners	2	18
DNSSEC – Securing DNS	4	46
Software Documentation Using Sphinx	1	3
Git – Universal Versioning System	2	25
Advanced IPv6	1	14
Cyberbullying and Other High-Risk Phenomena on the Internet	2	19
The eIDAS Regulation in a Clear Way	2	16
Advanced Networking in Linux	6	90
DNS Principles and Administration	3	35
The BGP Routing Protocol	2	28
Technical Writers' Exchange of Experience Workshop	1	20
Turris in Practice	2	23
Introduction to Forensic Memory Analysis	1	10
Introduction to Linux	3	29
Advanced Vim	1	15

List of customised courses offered at the CZ.NIC Academy in 2019

Name	Number of courses	Number of students
Safe Behaviour on the Internet	1	30

Name	Number of courses	Number of students
Cyberbullying and Other High-Risk Phenomena on the Internet	8	60
Illegal Online Content	3	78

List of courses and lectures for schools held in 2019

Name	Number of courses	Number of students
(Not) Safe mobile phone	62	1,310
Discussion with the Book "ONLINE ZOO"	82	1,813
Digital Footprint	29	594
Functioning of the Internet	58	1,235
Cyberbullying	34	1,034
Illegal Online Content	18	507

Total number of courses organised by the CZ.NIC Academy in 2019

Course type	Organised in total	Total students
Professional courses	45	527
Customised courses	12	168
Schools	283	6,493
Total	**340**	**7,188**

9.4 Conferences

CZ.NIC organised the traditional Internet and Technology conference on 14 and 15 November 2019 (19). The latest edition of the conference

offered contributions that brought news from the world of domains and the association's key projects. Presentations on topics related to DNS and internet security were also included.

In 2019, CZ.NIC presented itself at a number of events and professional conferences in the Czech Republic and abroad. The domestic ones included InstallFest, Linux Days, Openalt, MakerFaire, Kam kráčejí komunikační sítě (Where Communication Networks Are Going), Safe Internet Festival (FBI), Internet 2020 and a seminar on IPv6. As regards foreign events, the association attended, for example, OpenCamp, FOSDEM and Peering Days.

In 2019, the CZ.NIC, NIX.CZ and CESNET associations organised a community meeting of CSNOG 2019 (Czech and Slovak Network Operators Group). The main goal of this event was the mutual exchange of experience between internet access providers, telecommunications network operators, domain registrars, computer network operators and technical enthusiasts, as well as discussions on current topics and sharing solutions leading to the development of internet networks in the Czech and Slovak republics. The meeting took place on 28 and 29 May 2019 in Brno and was attended by 130 people.

In accordance with its strategy, the CZ.NIC Association, together with its partner CISCO, hosted an international meeting of internet experts, scientists and engineers, IETF 104. A total of 1,233 participants gathered in Prague between March 23 and 29.

9.5 CZ.NIC Edition

Publishing specialised and popular publications on topics related to the internet and its technologies is already a traditional educational activity of the association. Printed and electronic books are published by CZ.NIC Edice. Electronic versions of books are available for free download at knihy.nic.cz, as well as in the content distributor network (Palmknihy, Wooky, eReading, Municipal Library of Prague and newly in the Flexibooks network) in PDF or e-reader formats (EPUB and MOBI). Printed books are now also available in the Kosmas, Euromedia Group and Pemic Books distribution networks and in the IKAR network in Slovakia, opening the door for the Edice titles to hundreds of bookstore counters and e-shops in the Czech Republic and Slovakia.

Cooperation in the distribution of electronic books through the BookPort portal, operated by Grada, was newly established. In the distribution of printed books, the association focused on other specialised sales channels. The first achievements include, for example, HW Kitchen as the distributor of EduShield and the book entitled *Hradla, volty, jednočipy* (Gates, Volts, Single Chips). The second is the Prague Zoo, which supported the distribution of the *Online ZOO* book and colouring book. Addressing these smaller but field-specific sales channels will continue in 2020.

In 2019, Edice was expanded by three additional printed titles and an audio book, which expanded the offer to 23 specialised and popular science titles. The first title, *Porty, bajty, osmibity* (Ports, Bytes, 8-Bits) by the proven author Martin Malý is a free continuation of his publication from last year, *Hradla, volty, jednočipy* (Gates, Volts, Single Chips). The author describes the construction of more complex circuits. On the example of three detailed constructions, the reader will learn the basic principles of the operation of 8-bit computers. The second title is the fourth updated

edition of the highly popular publication *IPv6 – Internetový protokol*, version 6 by the experienced university teacher Pavel Satrapa. The third book, *Kryptografie okolo nás* (Cryptography Around Us) by Karel Burda, describes the use of cryptography in everyday life. The book explains the characteristics of selected cryptographic functions, such as encryption, hashing and the like.

A completely new achievement in the Edice is the first published audio book, *Online ZOO*, which builds on the previously published book of the same name. The spoken word can thus easily make the basics of safe behaviour on the internet accessible to even the youngest audience.

Development of the sale of titles in CZ.NIC Edice

In 2019, a total of 3,229 printed books were sold in CZ.NIC Edice, which represents an increase of 230% compared to 2018.
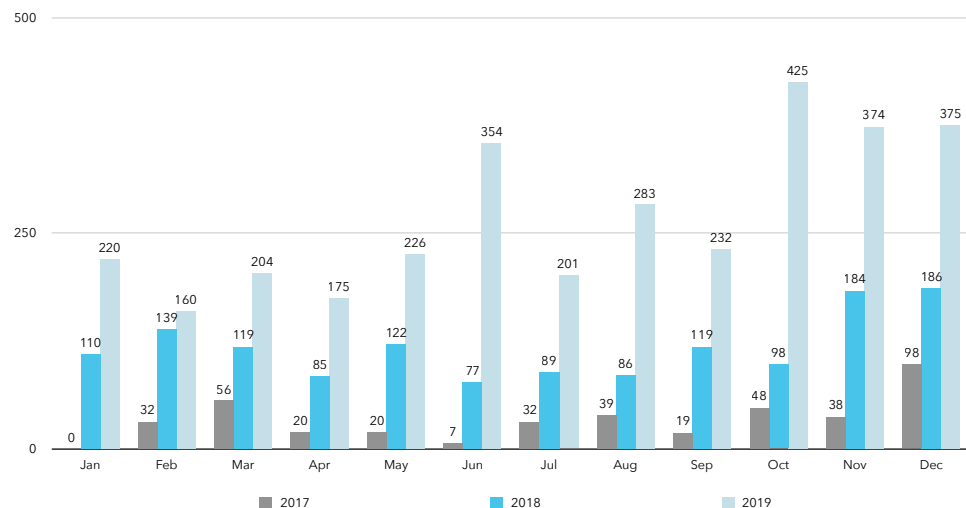
Overview of book sales by distributor
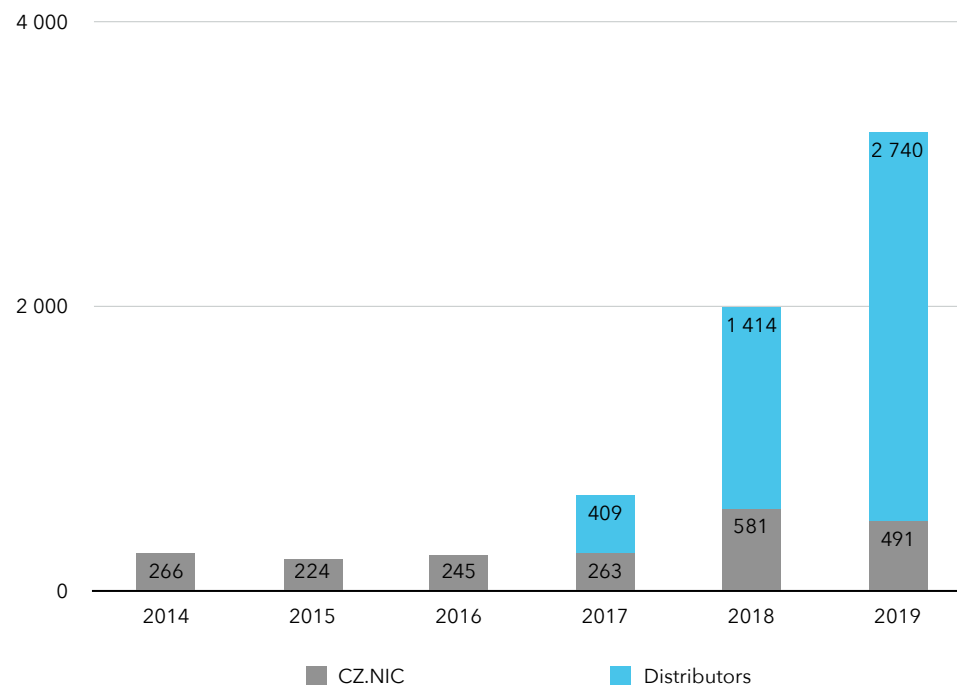
10 **Cooperation and partnerships**

56

Connecting tens of millions of users across continents, the internet is clearly the most important communication tool today. We can often hear that the internet has no borders and does not fall under the authority of any government. This does not mean, however, that the internet is not controlled and has no rules. However, unlike many other industries, the rules are often created by an internet community (including the employees of CZ.NIC) representing a large family of fans and supporters of this global network.

To ensure that no efforts of any member or organisation are in vain, mutual cooperation is essential, both at the national and international level.

Cooperation with our domestic partners helps find the most acceptable system for national domain administration for the Czech user. At the same time, it contributes, mostly thanks to the projects of our Labs, to the expansion of new technologies and the development of the information society.

International cooperation helps, not only follow world trends, but also – thanks to active participation of the association's employees – contributes to their creation and shaping that affects our everyday lives.

Thanks to their high level of expertise, the representatives of the association, both management and other staff, are welcome guests at domestic and international expert forums.

10.1 Czech Republic

Thanks to the importance of the implemented activities, CZ.NIC is the natural partner of both public administration and interest associations operating in the internet domain.

10.1.1 Cooperation with public administration

The importance of the domain name administration system and related internet infrastructure is comparable to that of other critical infrastructures, for example in the energy and transport sectors. As the administrator of the national .CZ domain, the CZ.NIC Association, considers the protection of this infrastructure its duty and a moral obligation to the Czech Republic. It establishes cooperation with a number of state authorities, such as the National Cyber and Information Security Agency (NÚKIB), the Czech Telecommunication Office (CTO), the Ministry of the Interior of the Czech Republic and the Ministry of Industry and Trade of the Czech Republic.

Cooperation with the Czech state in the field of critical infrastructure was intensified in 2017 with the launch of the project entitled "Securing DNS Servers in the Czech Republic". It is being implemented within the framework of the Programme of Security Research for the Needs of the State in 2016–2019.

The representatives of the CZ.NIC Association from the "Development Projects" department made significant contributions to the implementation of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the so-called eIDAS Regulation). In connection with the operation of the national eIDAS node mentioned in Chapter 7.4, our colleague, Jaromír Talíř, as the representative of the Czech Republic, regularly attended meetings of the eIDAS Technical SubGroup, which defines the technical standards of cross-border authentication. Another of his colleagues worked in expert groups of the European Commission and at the Ministry of the Interior.

The position of a trustworthy and reliable public administration partner was also confirmed by the CZ.NIC Association as part of the Safer Internet Centre project (see the Chapter "Grant projects"), as it took over the operation of the Police Cybercrime Reporting Line and further deepened cooperation with regions, especially via the project Regions for Safer Internet.

Furthermore, the association cooperates with the Police of the Czech Republic, enforcement authorities, courts and authorities according to the statutory authorisation, i.e. with the Office for Personal Data Protection, trade and tax offices, the Czech Trade Inspection Authority, the Customs Administration, etc.

10.1.2 Cooperation with the non-profit sector and social responsibility

Člověk v tísni (People in Need)

Other social activities of the CZ.NIC Association include the support of the Člověk v tísni (People in Need) Foundation, in particular its Jeden svět na školách (One World in Schools) educational project, which offers schools documentary films and accompanying methodological aids to teach current topics of the contemporary world and modern history.

Our state, our data (OSF Foundation)

Our state, our data is a project of the OSF Foundation. The CZ.NIC Association is a long-term partner of the project, whose main objectives are to promote the principles and standards of open data, as well as to promote, teach and coordinate activities and experts in this field. Part of this partnership included participation at the 4th Annual Open Data Expo in 2019, where the association participated with presentations focused on Open Data and Turris. Representatives of the association sat on the expert panels of the competition Společně otevíráme data (Together We Open Data), which for the seventh time in a row awarded the best public applications in the categories Transparency, Participation, Data in Everyday Life, Open Source and Solution App Using Open Data for Socially Beneficial Services. Support was also given to meet-ups, meetings and building of the Česko.Digital platform – a community of top developers, designers and product specialists who want to help the state and non-governmental organisations in their free time and thus make the Czech Republic a better place to live.

Helping animals

The CZ.NIC association has been contributing in the long term to the Prague and Zlín Zoos to the breeding of the Australian cassowary, whose original home is New Guinea and Australia.

10.1.3 Membership in professional and interest organisations

Czech Television – Déčko

In 2019, the association was represented in "Déčkolegium", an informal board of advisors providing expert advice, feedback and opinions on the programmes and content of the popular Czech children's channel Déčko. It also helps to acquaint parents with media issues.

NIX.CZ

The largest Czech Internet Exchange Point (IXP) covers domestic and foreign internet service providers for the interconnection of their networks. The NIX. CZ Association is the largest IXP in the Czech Republic and one of the most important in the world. The CZ.NIC association is a member of NIX.CZ and actively contributes to its activities primarily through the FENIX project. NIX. CZ is also a notable user of products of the CZ.NIC Labs, particularly BIRD.

Involvement in the FENIX project

CZ.NIC helped establish the FENIX node on the platform of the biggest Czech peering node NIX.CZ in 2013. Its aim is to secure the availability of internet services among entities involved in this activity in the case of massive DoS attacks. The FENIX project is intended for businesses providing connectivity for major connectivity and content providers who need to secure their operation also in the most critical situations.

Any entity that meets the entry terms can join the FENIX project. These terms resonate with what the CZ.NIC Association has been promoting for a long time, especially with the development of a trustworthy, secure and stable internet infrastructure and services of general interest. To join the FENIX project, the applicant must for example run its CERT/CSIRT team, support IPv6 and DNSSEC, have the response rate limiting implemented and use BCP-38 source address filtering in its network.

10.2 Other countries

Thanks to the activities of the association on the international internet scene or interested foreign organisations are increasingly selecting CZ.NIC as a partner for cooperation and the Czech Republic as the venue for their meetings. The CZ.NIC Association welcomes this fact, as the representatives of the local internet community gain in this manner easier access to interesting topics, as well as to leading experts from the world of the internet.

10.2.1 Membership in professional and interest organisations

APWG (Anti-Phishing Working Group)

A global coalition of private companies, state institutions and security forces focused on the global fight against cybercrime, especially spam.

CENTR (Council of European National Top Level Domain Registries)

A non-profit organisation that associates top-level national and generic domain name administrators. It primarily targets European registers, but members also include representatives of more remote regions – e.g., Canada and Japan. The CZ.NIC association has been a member since 2001 and has been regularly involved in individual working group meetings. In 2019, the head of the CENTR Technical Working Group was Jaromír Talíř.

DNS-OARC (The Domain Name System Operations, Analysis and Research Centre)

A trusted platform where key stakeholders meet and share their experience with DNS operation, analyses and research, so that they can coordinate their work as efficiently as possible, particularly in the field of security. Jaromír Talíř, already the third representative of the Czech Republic and the CZ.NIC Association, was a member of the DNS-OARC

Board of Directors in 2019 and will continue in that post in 2020 based on the election of the General Meeting.

EURid (The European Registry of Internet Domain Names)

An association, which, under the authority of the European Commission, administers the .EU top-level domain. CZ.NIC is an associate member and has a representative in the board.

EuroISPA (European Internet Services Providers Associations)

The European Internet Services Providers Association is the largest organisation, bringing together more than 2,300 organisations around the world. The main objective of EuroISPA, of which CZ.NIC has been a member since 2008, is to represent ISPs within the legislative processes of the European Union and facilitate the exchange of experience between individual internet service providers.

CSIRT Network

A CSIRT team interest group, which acts as a contact point for obliged entities identified in the NIS Directive (Directive of the European Parliament and of the Council concerning measures for a high common level of security of networks and information systems across the union). The group primarily deals with technical issues related to the implementation of this agenda. In 2019, the CSIRT.CZ team actively participated in most of the meetings, where, for example, the outputs of the Melicertes project, which was deployed in CSIRT.CZ as part of the CEF project, were addressed.

FIRST (Forum of Incident Response and Security Teams)

The first international organisation that associates security teams. It has around 400 members, and the American and European teams are represented to a significant degree. It is the only organisation that provides membership to teams from around the world and also covers product teams. The team became member of the FIRST organisation in 2015.

ICANN (Internet Corporation for Assigned Names and Numbers)

An international non-profit organisation founded in 1998, the main task of which is not only to administer and assign generic top-level domain names (gTLDs) and top-level national domain names (ccTLDs) but also IP addresses. The CZ.NIC association, as a national domain administrator, sends its representatives to regular meetings and its experts actively participate in activities of the working groups. Ondřej Filip, managing director of CZ.NIC, is a member of the prestigious Security & Stability Advisory Committee (SSAC) within ICANN.

IETF (Internet Engineering Task Force)

An organisation founded in 1986 directly linked to the birth of the internet. It includes an international community of leading experts, network architects and representatives of the commercial sphere. The IETF approves and enforces internet standards, the RFC documents that govern most internet traffic, and our employees are actively involved in some of them. Meetings of members of this organisation have also taken place several times, thanks to the cooperation of the CZ.NIC Association in Prague.

The CZ.NIC Labs' employees participate in the IETF, mainly in the DNSOP (DNS operation) activities, NETCONF (network device configuration) and NETMOD (configuration and status data modelling) working groups. Ladislav Lhotka, Head of the CZ.NIC Labs, is the author or co-author of six RFC standards. In March 2019, a new internet standard, RFC 8528, was issued. It defines an optional extension of the YANG language for modelling configuration and status data. Ladislav Lhotka is also signed under this standard.

INHOPE (International Association of Internet Hotlines)

INHOPE is an international association of over 50 hotlines aimed at combating and eliminating illegal online content, mainly child pornography. The main benefits of INHOPE membership include access to the ICCAM database (derived from "I see Child Abuse Material") and the possibility of effective cooperation with other countries and institutions, particularly Interpol, in removing illegal content. The CZ.NIC Association with the STOPonline.cz line operated by it became an associate member in June 2017. In 2018, as part of the implementation of the Safer Internet Centre project, the association received full membership in that prestigious association, and a year later received a special financial reward as recognition for a high number of processed reports.

RIPE NCC (Réseaux IP Européens Network Coordination Centre)

An independent non-profit organisation that supports internet infrastructure. Its core activities include the RIR operation (Regional Internet Registry), which allocates internet resources and related services (such as IP addresses) to its members. The CZ.NIC association, as one of the members, attends not only regular meetings, but also participates in

other thematic meetings and trainings organised by this organisation. In 2019, Ondřej Filip, managing director of the CZ.NIC Association, became a member of the board of directors of this organisation.

TF-CSIRT

TF-CSIRT is an organisation that brings together security teams mainly from Europe. The CSIRT.CZ team has the highest possible level of membership in this organisation – certified. CZ.NIC-CSIRT is its accredited member.
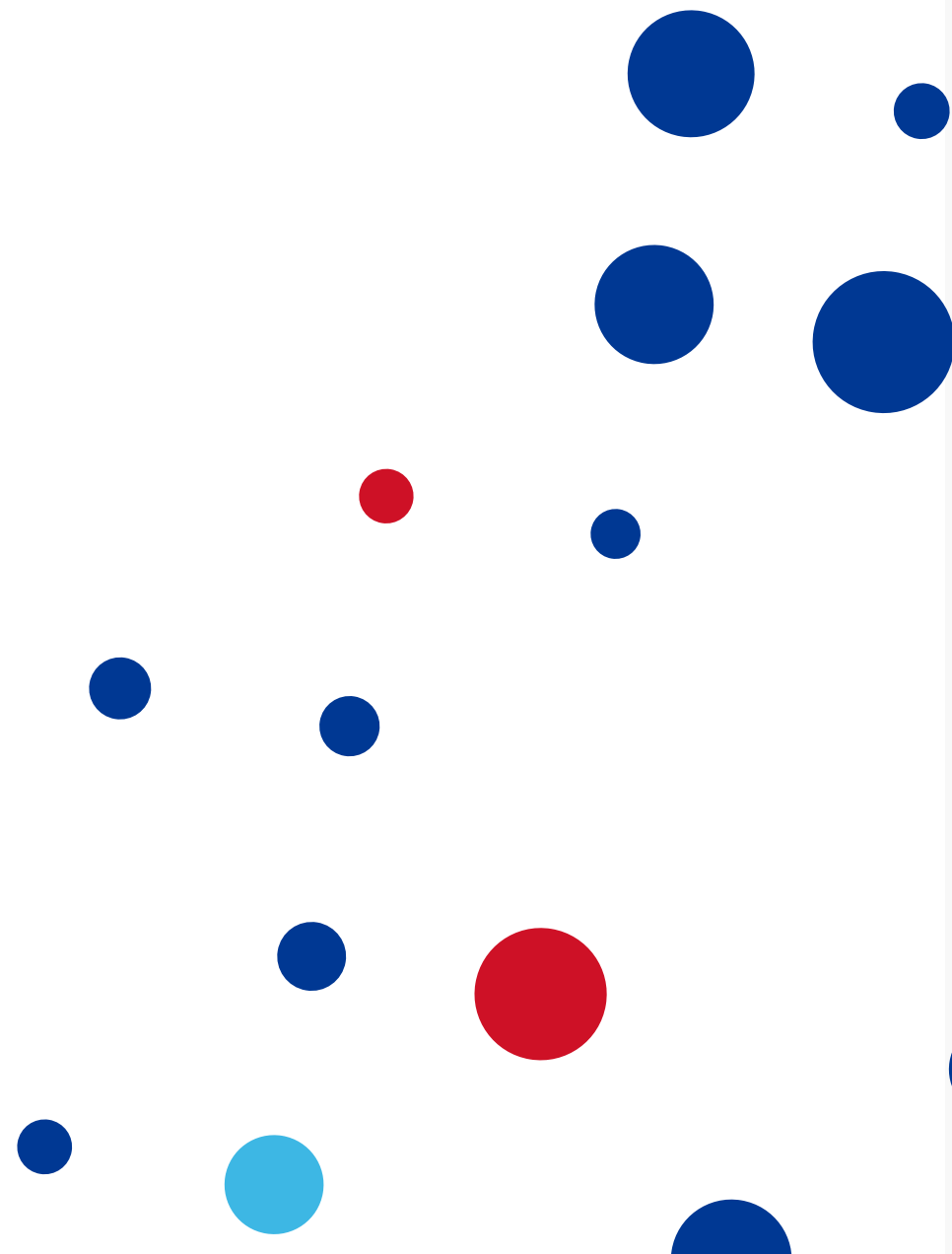
11 **Grant projects**

In line with its long-term objective of developing internet technologies and the information society, and the medium-term concept of the association for the years 2016–2019, the CZ.NIC Association was actively involved in a number of grant projects.

Grant projects represent a very important source of funding for the association. The projects also support the development and training of CZ.NIC employees and enable them to participate in unique projects that often help determine the future direction of the information society; the projects make a significant contribution to the development of the CSIRT. CZ security team.

Thanks to European projects, the association is also significantly involved in building infrastructure intended primarily for cross-border electronic services of the public administration. Projects implemented at the national level significantly contribute to the development of the Turris project, and the implementation of these projects also helps to strengthen the position of the association as a trustworthy partner of the state.

11.1 Involvement in European cooperation projects

In February 2019, the CZ.NIC Association joined the implementation of the new SPARTA project. During 2019, the European Commission also approved a new RegeID project, the implementation of which will take place in 2020–2021.

The following projects were implemented with the support of the European Commission in 2019.

CyberExchange

The CZ.NIC Association is the coordinator of the international CyberExchange project, which responds to increasing threats in the area of cyber security and the resulting necessity of cross-border cooperation in the fight against them. A total of eleven national and government security teams from the Czech Republic, Croatia, Latvia, Luxembourg, Malta, Poland, Austria, Romania, Greece and Slovakia are involved in the project.

Representatives of these teams participate in internships during the project, in which they have the opportunity to exchange experience and strengthen their professional capacities. The project also supports technical internships, where it focuses on supporting the deployment of software tools that have been developed by individual teams to serve the wider security community and the fight against cyber threats in other countries. This project will suitably complement the MeliCERTes platform, which is said to be one of the building blocks of cross-border digital infrastructure services.

In 2019, a total of fourteen exchange internships took place, two of which were also attended by CSIRT.CZ. Thanks to these two exchanges, the Zone Monitor application was designed and tested. The application draws on a list of newly added certificates and monitors whether there is any domain suspected of phishing. The Envelope library, which abstracts the internal structure of the e-mail object and thus significantly simplifies work with sending e-mails and encryption with GPG and S/MIME technologies, was also released.

CZ.PEPS (Czech Pan European Proxy Services)

The objective of the CZ.PEPS project, which took place in 2016–2019, was, primarily, the implementation and operation of national infrastructure (the so-called eIDAS node) for cross-border recognition of electronic identification in Europe in accordance with Regulation No 910/2014 of the European Parliament and of the Council (eIDAS). The issue of eIDAS node operation is described in more detail in Chapter 7.4.

SIC CZ (Safer Internet Centre)

Since 2019, the CZ.NIC Association has taken over the coordination of national activities aimed at improving online safety of children and prevention in the Czech Republic, and with the new project "Bezpečně na netu" (Safe on the Net), it follows the Saferinternet.cz project, which ended in December 2018. From the beginning, the Safety Line has also been involved in the new project, which, thanks to this partnership, has increased its capacity to focus on cases related primarily to cyberbullying, sexting or luring to dangerous meetings. As a national centre, we want to contribute mainly to ensuring that individual projects within the Czech Republic do not emerge as competitive; on the contrary, we want to connect these individual activities, so we maintain a dialogue with many partners or state representatives.

In addition to educational courses for schoolchildren, who are the most important target group, seminars are held for the professional public, teachers, parents or the state administration. By the end of 2019, 318 educational events were held at 180 locations in the Czech Republic. These include a visit to fifteen children's homes. Two conferences were organised. The first was held at the Zlín Film Festival for Children and Youth in May, where a Youth Panel and an Advisory Board took place at the same time. A seminar was also held in the Senate of the Parliament of the Czech Republic.

In cooperation with the internet television MALL.TV, the successful series *#Martyisdead* (mall.tv/martyisdead) , inspired by real cases of cyberbullying, was filmed. The series won the award for the best web series in Central and Eastern Europe at the Serial Killer Festival and currently boasts hundreds of thousands of views. A short film by director Braňo Holiček, *Maturant* (High-School Graduate), was also made. It deals with the topics of addiction, truth and lies on the internet. At the same time, a methodology for working with this film in schools was developed. It is also worth mentioning the summer campaign dedicated to dangerous challenges in the online environment (online challenge). For the youngest children, the association develops the Austrian project ONLINE ZOO, for which a colouring book and an audiobook were created.

One of the successful services is the STOPonline.cz line, which is intended for reporting illegal content, especially child abuse, inappropriate child nudity and cybergrooming. The line is operated on the basis of a memorandum with the National Headquarters against Organised Crime and the Police of the Czech Republic. In 2019, it received a total of 3,224 reports, which is 800 cases more compared to the previous year. An even more significant increase was recorded in the number of cases uploaded to the ICCAM international database, where the number of reported sites increased from 371 in 2018 to 640 incidents uploaded in 2019. This increase was caused both by the increasing awareness of STOPonline's work and by the analytical activities of STOPonline operators themselves.

In addition to cyberbullying, the project also focuses on the safe use of mobile devices and applications. For this reason, three new games were created for the Tablexia application focusing on the training of attention, spatial orientation and memory. It is these cognitive functions that are most often affected by excessive use of mobile devices and applications.

Strengthening cybersecurity capacities in the Czech Republic

The project implemented in 2017–2019 primarily focused on strengthening the knowledge and technical capacities of the national CSIRT.CZ security team and its role based on the European Information and Network Security Directive (NIS Directive). During the implementation of the project, we managed to create and implement a tool called "Routing hijack monitoring", which facilitates the fight against cyber attacks. The national CSIRT.CZ security team also managed to obtain the highest status (certified) at TF-CSIRT. The project also included support for the establishment of security teams in the Czech Republic and their internationalisation within TF-CSIRT.

The project consortium also included the Czech neutral interconnection node NIX.CZ, which in cooperation with the CZ.NIC Association developed the FENIX project within the project.

THREAT-ARREST

The THREAT-ARREST scientific project, implemented as part of the prestigious European Horizon 2020 programme, aims to develop an advanced training platform, including emulation, simulation and gaming and visualisation capabilities serving different types of stakeholders. It aims to prepare and develop expertise in the field of protecting high-risk cyber systems and organisations, including the ability to face advanced, known and new cyber attacks.

In order to achieve this goal, the project plans primarily to develop the so-called CTTP (Cyber Threat and Training Preparation) platform, designed to train defence against cyber attacks and improve the protection of selected systems.

SPARTA (Horizon 2020)

In 2019, the CZ.NIC Association, together with the Brno University of Technology and the CESNET Association, joined another project implemented within the Horizon 2020 programme – SPARTA, which brought together 44 organisations focused on science and research, technological innovation and social sciences. This community aims to review the current way in which cyber security research is conducted in Europe. The collaboration will develop and share solutions to help security experts prevent cybercrime and increase cyber security.

11.2 Engagement in national and other projects

In addition to European projects, the CZ.NIC Association also participates in national projects, especially within the framework of Czech security research.

Ludus

In October 2019, a three-year project supported by the Technology Agency of the Czech Republic under the Epsilon programme ended. The CZ.NIC Association cooperated on it with the Czech Technical University in Prague. The project used scientific knowledge specifically in the field of machine learning and the application of game theory to increase collaborative defence against internet attacks. Within the project, a game-theoretical model was created, which, based on network interaction, allows the creation of filtering rules for the protection of routers.

Furthermore, an overall security metric was introduced in order to detect attacks and measure the level of security of individual devices. The Turris router network was used as the infrastructure for testing and demonstrating this system.

## Prediction and Protection from Cyber Incidents (PROKI)

The aim of the project, aided within the security research of the Czech Republic between 2015-2020, is mainly the development of a system that addresses the analysis of information on cyber incidents from a wide range of sources. The evaluation of this information is made by the national CSIRT.CZ security team, operated by the CZ.NIC Association pursuant to Act No. 181/2014 Coll. on cyber security. When developed, the system will then enable the sharing of information on cyber threats among key players, especially national and government CERT/CSIRTs and major ISPs.

Building and testing Cyber Threat Intelligence (CTI)

The project is aided by the Ministry of the Interior of the Czech Republic within the Programme of Security Research for the Needs of the State 2016–2021. It focuses on strengthening the protection of critical information infrastructure and other important information systems and networks. By building an effective system for detecting, identifying and predicting cyber threats and evaluating cyber security incidents (the so-called Cyber Threat Intelligence), it seeks to reduce the damage caused by cybercrime.

The project also includes the distribution and placement of more than 800 hardware probes based on Turris routers, which will function as

devices for data collection and protection against cyber attacks in the environment of selected public administration entities.
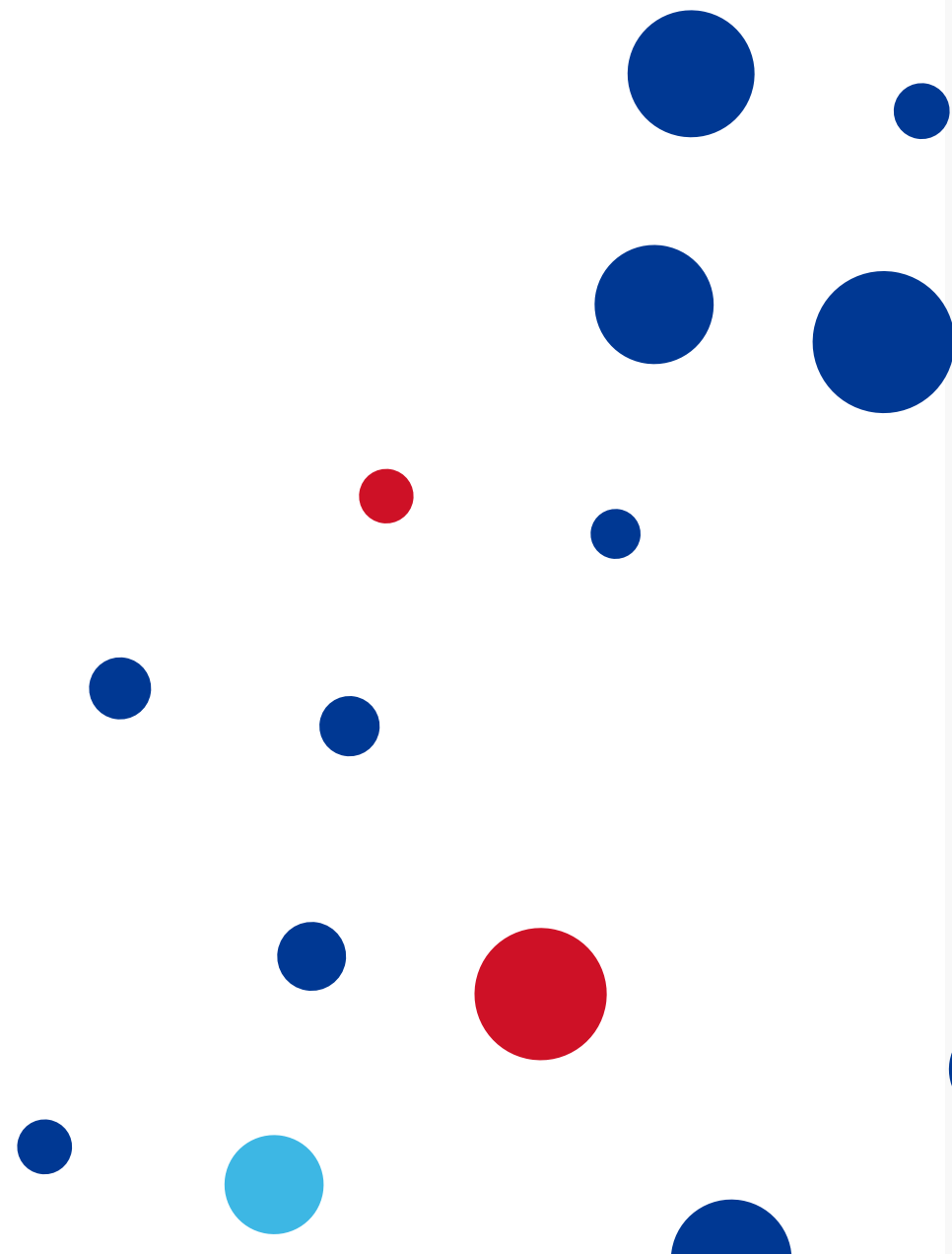
12 **Association structure**

12.1 Members

The member base of the association is made up of a number of entities, which are significantly involved in the functioning of the Czech internet. Among its members are representatives of internet and telecommunications service providers, domain name registrars, publishers of internet and print media, e-commerce businesses and companies for whom the internet and domain names are an important communication tool.

The CZ.NIC association is one of the places where these representatives can meet and so influence the future direction of the Czech internet. The wide range of members' business activities and their involvement in the activities of the association, either through participation in general meetings, working groups and seminars, in e-mail conferences or directly in the bodies of the association, enriches and expands the knowledge portfolio of the association, makes its management more effective and responds to the constant development that is so typical of the internet.

Membership conditions

Any legal entity that fulfils the general membership requirements, including the location of a registered office or an organisational unit in the territory of one of the Member States of the European Union, the holding of at least one domain name in ccTLD .CZ and payment of the membership entry fee, can become a member of the association.

The association members are divided into three chambers – the Chamber of Domain Name Holders, the ISP Chamber and the Chamber of Registrars. The statutes govern the special conditions of the membership in the individual chambers. The chamber arrangement brings benefits to the members of the association, who can easily formulate and defend their opinions and interests, together, with other similarly oriented entities. The chamber arrangement also streamlines the course and the meetings of the association bodies, in particular, the Collegium and the General Meeting.
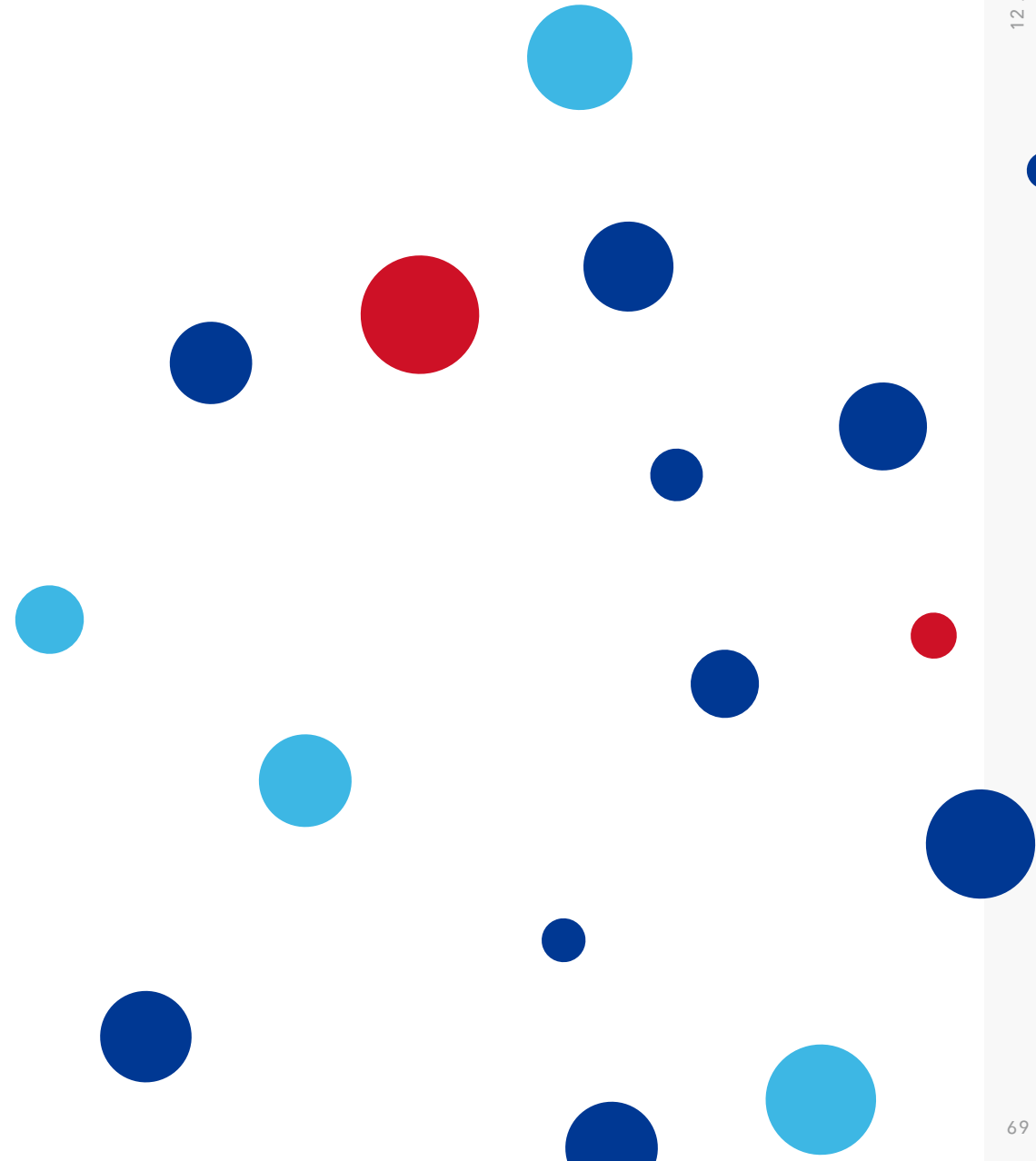
12.1.1 Number of members by chamber

As of 31 December 2019, the CZ.NIC Association had a total of 116 members. Three new members were added to the Chamber of Domain Name Holders, one member joined the ISP Chamber, and two members left the Chamber of Registrars.

Member division according to chambers

Chamber of Domain Name Holders	62 %
ISP Chamber	23%
Chamber of Registrars	15 %

Development of the number of members by chamber

Year	Chamber of Domain Name Holders	ISP Chamber	Chamber of Registrars	Total
2005	19	10	9	**38**
2006	27	8	11	**46**
2007	27	14	11	**52**
2008	30	15	12	**57**
2009	32	17	14	**63**
2010	37	21	19	**77**
2011	50	24	20	**94**
2012	61	27	18	**106**
2013	65	27	19	**111**
2014	69	24	20	**113**
2015	72	23	20	**115**
2016	67	25	20	**112**
2017	71	26	18	**115**
2018	69	26	19	**114**
2019	**72**	**27**	**17**	**116**

12.1.2 Overview of members by chamber

Overview of chamber members as of 31 December 2019.

Chamber of Domain Name Holders (business name, company identification number)

ABRATICA s.r.o.	26108534
ACOMWARE s.r.o.	25047965
ADAPTIVITY s.r.o.	24156027
AdminIT s.r.o.	27864901
Advio Network, s.r.o.	28565673
Adytia Innovation OÜ	14498430
AKREDIT, spol. s r.o.	25797387
ALEF NULA, a.s.	61858579
ALENSA, s.r.o.	27179681
AliaWeb, spol. s r.o.	26117363
Asociace pro elektronickou komerci, z.s.	68684797
AUDITEL, s.r.o.	26775034
CD PROFESIONAL security agency, s.r.o.	25712713
CISCO SYSTEMS (Czech Republic) s.r.o.	63979462
ComSource s.r.o.	29059291
Com-Sys TRADE spol. s r.o.	16188781
CQK HOLDING a.s.	28405579
CYBERSALES a.s.	26199653
Datahost s.r.o.	26390973
DELL Computer, spol. s.r.o.	45272808
ECOMOLE LTD.	9526615
ekolo.cz s.r.o.	27141659

EXPLORER, a.s.	26726653
Fortion Networks, s.r.o.	26397994
Greenlux s.r.o.	28608747
Holubová advokáti s.r.o.	24686727
H17 Networks, s.r.o.	27374041
ICZ a.s.	25145444
igloonet, s.r.o.	27713482
I. H. P. společnost s ručením omezeným	48117846
INBES, spol. s r.o.	14502593
Intell. Net s. r. o.	27971546
Internet Info, s.r.o.	25648071
Internet Mall, a.s.	26204967
i - registry s.r.o.	28451082
Klíč, spol. s r.o.	28129377
Laurián s.r.o.	29018919
MAFRA, a.s.	45313351
Mailkit s. r. o.	26449901
MARIAS s.r.o.	26136139
MASANTA s.r.o.	25730533
MEDIA FACTORY Czech Republic a.s.	26288311
Michal Krsek & partneři s.r.o.	27418570
MITE Infonet s.r.o.	25660292
Moonlake Web Services, s.r.o.	29249911
Neutral czFree eXchange, z.s.p.o.	75093201
NEW MEDIA GROUP s.r.o.	26124611
Nux s.r.o.	27234631
Občanské sdružení Ubuntu pro Českou republiku	22674608
Orego finance s.r.o.	24718955
Panificium, s.r.o.	4526767
PharoCom s.r.o.	25172131
Prague Business Office s.r.o.	27143481
Pražský Účetní Servis s.r.o.	26740575
Q3, s.r.o.	26226073

Qrator Labs CZ s.r.o.	3620174
Seznam.cz, a.s.	26168685
Skymia s. r. o.	28238613
Software602 a.s.	63078236
Socha, spol. s.r.o.	48291153
SuperNetwork s.r.o.	25492063
SVBsoft, s.r.o.	28523644
Tech Ware spol. s.r.o.	14891107
TIKWI s.r.o.	28917651
Trustica s.r.o.	26514362
Unie vydavatelů, z.s. (Czech Publishers Association)	15887081
ÚVT, s.r.o.	25701118
Vema, a.s.	26226511
VIZUS.CZ s.r.o.	27155315
VOLNÝ, a.s.	63080150
Vymáhání a odkup pohledávek s.r.o.	27566510
Webarium, s.r.o.	26089602
Webnames s.r.o.	44848692
1X s.r.o.	44632142

Faster CZ spol. s.r.o.	60722266
FreeTel, s.r.o.	24737887
INTERNEXT 2000, s.r.o.	25352288
IPEX a.s.	45021295
ISP Alliance a.s.	28205812
JHComp s.r.o.	26051362
LAM plus s.r.o.	25129619
Mach3net s.r.o.	27344860
Master Internet, s.r.o.	26277557
NetArt Group s.r.o.	27612694
Pe3ny Net s.r.o.	27252183
PODA a.s.	25816179
STARNET, s.r.o.	26041561
T-Mobile Czech Republic a.s.	64949681
ÚVT Internet s.r.o.	24288705
VIVO CONNECTION, spol. s r.o.	26900696
VSHosting s.r.o.	61505455
2 connect a.s.	29007542

ISP Chamber (business name, company identification number)

ABAK, spol. s.r.o., CZE ABAK, GmbH GER ABAK, Co.Ltd. ENG	40763153
CASABLANCA INT s.r.o.	25079832
CentroNet, a.s.	26165473
CESNET, z.s.p.o.	63839172
COOLHOUSING s.r.o.	14893983
ČD - Telematika a.s.	61459445
České Radiokomunikace a.s.	24738875
Dragon Internet a.s.	27237800
Družstvo EUROSIGNAL	26461129

Chamber of Registrars (business name, company identification number)

ACTIVE 24, s.r.o.	25115804
Dial Telecom, a.s.	28175492
e-BAAN Net s.r.o.	26867257
IGNUM, s.r.o.	26159708
INTERNET CZ, a.s.	26043319
KRAXNET s.r.o.	26460335
Media4web, s.r.o.	26735903
ONE.CZ s.r.o.	25503651
ONEsolution s.r.o.	27710335
O2 Czech Republic a.s.	60193336

Seonet Multimedia s.r.o.	27522041
Seznam.cz, a.s.	26168685
Stable.cz s.r.o.	28741048
TELE3 s.r.o.	26096960
TERMS a.s.	14499037
Web4U s.r.o.	26058774
ZONER software, a.s.	49437381
Web4U s.r.o.	26058774
ZONER software, a.s.	49437381

12.2 Association bodies

12.2.1 General Meeting

The supreme body of the association is the General Meeting, in which all members are members of the association. They are divided into three chambers – the Chamber of Registrars, the ISP Chamber and the Chamber of Domain Name Holders. Each association member has the right to participate in the General Meeting and promote its ideas, and provide opinions and comments.

12.2.2 Collegium

The Collegium is a body of the association, consisting of members elected by the individual chambers of the General Meeting and/or by other persons. The powers of the Collegium include, for example, approving the association's concept and budget, approving agreements between the association and the state, and electing and removing members of the Board of Directors and Supervisory Board. The Collegium has a total of 21 members, of which 18 members are elected by the individual chambers of the General Meeting. Public administration authorities nominate three members. Members of the Collegium are elected to serve three-year terms.

Members of the Collegium elected by the General Meeting in the period from 1 January 2019 to 18 December 2019

Chamber of Domain Name Holders
– Marek Antoš
– Dan Ohnesorg
– Jan Redl
– Karel Taft
– Pavel Tvrdík
– David Vorlíček

ISP Chamber
– Ondřej Filip
– Tomáš Košňar
– Jiří Kysela
– Vlastimil Pečínka
– Zbyněk Pospíchal
– Milan Švácha

Chamber of Registrars
– Tomáš Fiala
– Martin Kukačka
– Stanislav Kysela

- Erich Syrovátka
- Petr Šmída
- Jaroslav Štětina

Members of the Collegium elected by the General Meeting in the period from 19 December 2019 to 31 December 2019

Chamber of Domain Name Holders

- Marek Antoš
- Bedřich Košata
- Dan Ohnesorg
- Jan Redl
- Karel Taft
- Pavel Tvrdík

ISP Chamber

- Ondřej Filip
- Tomáš Košňar
- Jiří Kysela
- Vlastimil Pečínka
- Zbyněk Pospíchal
- Milan Švácha

Chamber of Registrars

- Tomáš Fiala
- Martin Kukačka
- Stanislav Kysela
- Erich Syrovátka
- Petr Šmída
- Jaroslav Štětina

Collegium members nominated by state authorities:

- Zina Bumbálková, Ministry of Industry and Trade of the Czech Republic
- Marie Moravcová, Czech Chamber of Commerce
- Jiří Peterka, Czech Telecommunication Office

12.2.3 Board of Directors

The Board of Directors is a governing body that manages the association's activities and acts in its name.

Members of the board of directors in the period from 1 January to 31 December 2019

- Karel Taft (born in 1971), Chairman of the Board of Directors
- Marek Antoš (born in 1979), Deputy Chairman of the Board of Directors
- Tomáš Košňar (born in 1965), member
- Martin Kukačka (born in 1980), member
- Jiří Kysela (born in 1955), member

12.2.4 Supervisory Board

The association's control body, which supervises the performance of the Board of Directors and the implementation of the association activities.

Members of the supervisory board in the period from 1 January to 31 December 2019

– Jan Redl, Chairman of the Supervisory Board

– Ilona Filípková, member

– Vlastimil Pečínka, member

12.2.5 Management

– Ondřej Filip, Chief Executive Officer

– Martin Peterka, Chief Operating Officer and Deputy Managing Director

– Tomáš Fuňka, Chief Financial Officer

– Zdeněk Brůna, Chief Technical Officer

– Ladislav Lhotka, Head of Research Team (CZ.NIC Labs)

– Michal Hrušecký, Head of the Hardware Development Department

– Jaromír Talíř, Technical Partner

– Ondřej Písek, Marketing Director

– Vilém Sládek, PR Manager

13 **Human resources**

The association's strength lies in its professionally competent and qualified employees, who are essential for achieving its mission and further development. For many employees it is possible to say, without exaggeration, that they are leading experts in the field who have both domestic and international reputations. To strengthen individual competencies, all employees are continuously educated, both in the field of foreign languages, so-called soft skills, and in professional knowledge, so that they can achieve the highest possible professional and personal qualities and contribute with their knowledge and skills to further development of the association and thus also the Czech internet.

# 13.1 State and development of the number of employees

In 2019, the number of employees of the association increased slightly. A major piece of news is that a chief financial officer was hired. The development and security teams were strengthened and a new separate HW Development Department was detached from the Labs.

| Department	Status			
	Number of employees (as of 31 December 2018)	Number of FTEs (as of 31 December 2018)	Number of employees (as of 31 December 2019)	Number of FTEs (as of 31 December 2019)
Management	7	7.000	8	8.000
Marketing/PR	8	7.500	8	7.750
Academy	2	2.000	2	2.000
Development	20	18.200	22	19.275
Network Administration	12	10.875	10	8.875
CZ.NIC Labs	50	42.250	27	24.100
Legal	2	1.625	2	1.750
Secretariat	2	2.000	2	2.000
HR	1	0.800	1	1.000
Customer Support	11	10.800	11	10.800
CSIRT	9	8.550	10	9.000
HW Development Department	0	0.000	25	20.750
EU Projects	3	3.000	3	3.000
Total	**127**	**114.600**	**131**	**118.300**

13.2 Employee structure

Employee structure by education

Most association employees have a university degree. The CZ.NIC Association also provides the opportunity to acquire professional experience to fresh university graduates, for whom it is trying to build suitable conditions and assigns them to its branches in Brno, České Budějovice and Plzeň. Thanks to this, we managed to maintain, and even slightly increase, the share of university-educated employees.

Other
2 %

Secondary schools
29 %

Universities
69 %
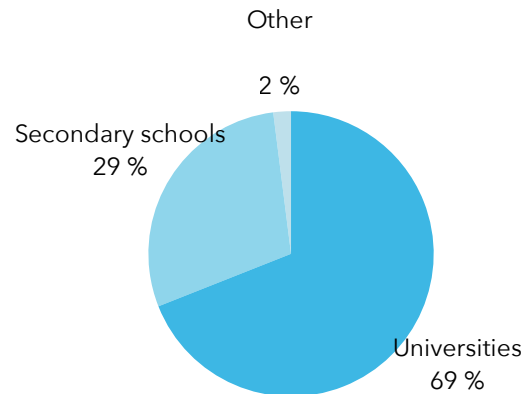
Employee structure by age

The average age of association employees is 35 years. In terms of age structure, employees aged 25–34 predominate.

24 years old or less
7 %

45 years old or more
11 %

35-44 years old
34 %

25-34 years old
48 %
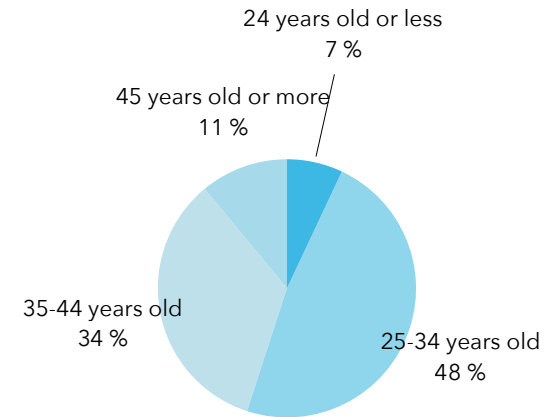
Employee structure by gender

In recruiting new employees, CZ.NIC encourages equal opportunities and the involvement of women. In 2019, the association again managed to increase the number of employed women. This is certainly, partly due to the possibility of working part-time, which allows employees to combine their work and parental responsibilities. Due to the structure of graduates in the technical branches of higher education institutions, however, the proportion of men still prevails, as in other technology companies.

Females
27 %

Males
73 %
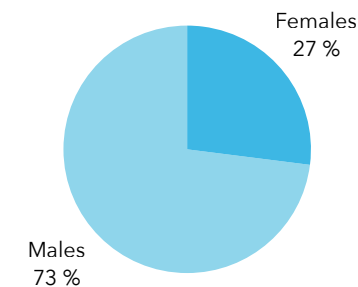
14 **Selected financial indicators**

14.1 Profit or loss after tax

	2011	2012	2013	2014	2015	2016	2017	2018	2019
Income	136,998	141,912	222,736	199,898	197,704	210,708	305,718	260,683	259,016
Expenses	104,370	125,352	209,127	186,092	211,703	189,057	295,442	254,950	238,349
Profit or loss after tax	32,628	16,560	13,609	13,806	13,999	21,650	10,276	5,733	20,667

In CZK '000

14.2 Balance sheet

	2011	2012	2013	2014	2015	2016	2017	2018	2019
Total assets	361,566	387,674	405,154	431,392	449,278	491,643	503,747	534,656	**569,478**
Fixed assets	8,781	63,840	77,095	101,406	89,398	84,611	85,885	89,103	**89,001**
Intangible assets	0	300	249	331	281	1,914	659	1,438	**1,333**
Tangible assets	8,781	63,540	76,846	101,075	89,117	82,697	85,226	87,665	**87,668**
Current assets	351,125	322,087	326,095	327,745	358,842	406,080	416,699	444,082	**479,202**
Inventory	278	189	277	453	798	14,340	20,829	40,435	**41,045**
Long-term receivables	1,379	1,335	59	59	58	58	304	258	**264**
Short-term receivables	12,180	10,676	18,540	22,100	4,948	6,282	16,870	8,602	**10,161**
Financial assets	337,288	309,887	307,219	305,133	353,038	385,400	378,696	394,787	**427,732**
Other assets	1,660	1,747	1,964	2,241	1,038	952	1,163	1,471	**1,275**
Total liabilities	352,036	387,674	405,154	431,392	449,278	491,643	503,747	534,656	**569,478**
Equity	243,795	261,094	274,591	288,397	302,395	324,045	332,308	338,039	**358,705**
Funds from profit	44,597	44,597	93,784	107,393	121,198	135,197	156,847	167,121	**172,853**
Profit or loss from previous years	166,570	199,937	167,198	167,198	167,198	167,198	165,185	165,185	**165,185**
Profit or loss for accounting period	32,628	16,560	13,609	13,806	13,999	21,650	10,276	5,733	**20,667**
External sources	15,988	17,684	27,479	22,497	32,140	48,059	53,906	67,723	**68,862**
Reserves	9,530	884	1,832	1,662	2,662	2,359	3,064	6,454	**8,691**
Long-term payables		241	304	235	1,344	617	8,571	9,990	**23**
Short-term payables	15,988	16,559	25,343	20,600	28,134	45,083	42,271	51,279	**60,148**
Other liabilities	92,253	108,896	103,084	120,498	114,743	119,539	117,533	128,894	**141,911**

In CZK '000

14.3 Profit and loss account

	2011	2012	2013	2014	2015	2016	2017	2018	2019
Performance and sales	127,135	134,030	142,295	155,134	167,480	195,269	196,746	189,797	213,574
Of which earnings and sales	127,133	134,144	138,755	150,880	166,318	194,897	196,746	189,797	213,574
Own work capitalised	0	0	3,379	4,044	797	153	0	0	0
Performance consumption and costs	44,440	70,414	67,042	66,335	64,701	73,668	75,970	67,523	70,268
Added value	82,693	63,616	75,253	88,799	102,779	121,754	120,776	122,274	143,306
Staff costs	39,227	43,328	57,245	66,541	72,930	85,706	98,706	111,018	117,380
Depreciation of assets	6,145	4,183	4,922	13,296	15,552	16,807	16,524	12,747	17,104
Clearance of reserves	533	313	1,020	-137	1,020	-124	393	2,256	3,683
Other operating income	1,208	1,082	2,290	2,029	1,800	1,884	12,184	13,304	13,813
Other operating expenses	351	626	916	1,432	994	1,789	1,865	1,701	1,322
Operating profit or loss	37,795	16,245	13,442	9,664	14,259	19,450	15,472	8,807	17,548
Other financial income	8,435	6,724	78,118	42,736	40,943	13,555	96,788	57,582	30,343
Other financial expenses	4,623	685	74,915	38,254	39,428	11,731	100,810	58,233	25,590
Profit or loss from financial operations	3,812	6,039	3,203	4,482	1,515	1,824	-4,022	-651	6,039
Profit or loss from ordinary activities	41,607	22,284	16,645	14,146	15,774	21,274	11,450	8,156	23,587
Income tax	8,979	5,724	3,036	340	1,775	-376	1,174	2,423	2,920
Profit or loss after tax	32,628	16,560	13,609	13,806	13,999	21,650	10,276	5,733	20,667

In CZK '000

14.4 Revenue development

	2011	2012	2013	2014	2015	2016	2017	2018	2019
Revenue	127,133	134,144	138,755	150,880	166,318	194,897	196,746	189,797	213,574

In CZK '000

15 **List of suppliers**

List of suppliers according to Article 45.4 of the Statutes:

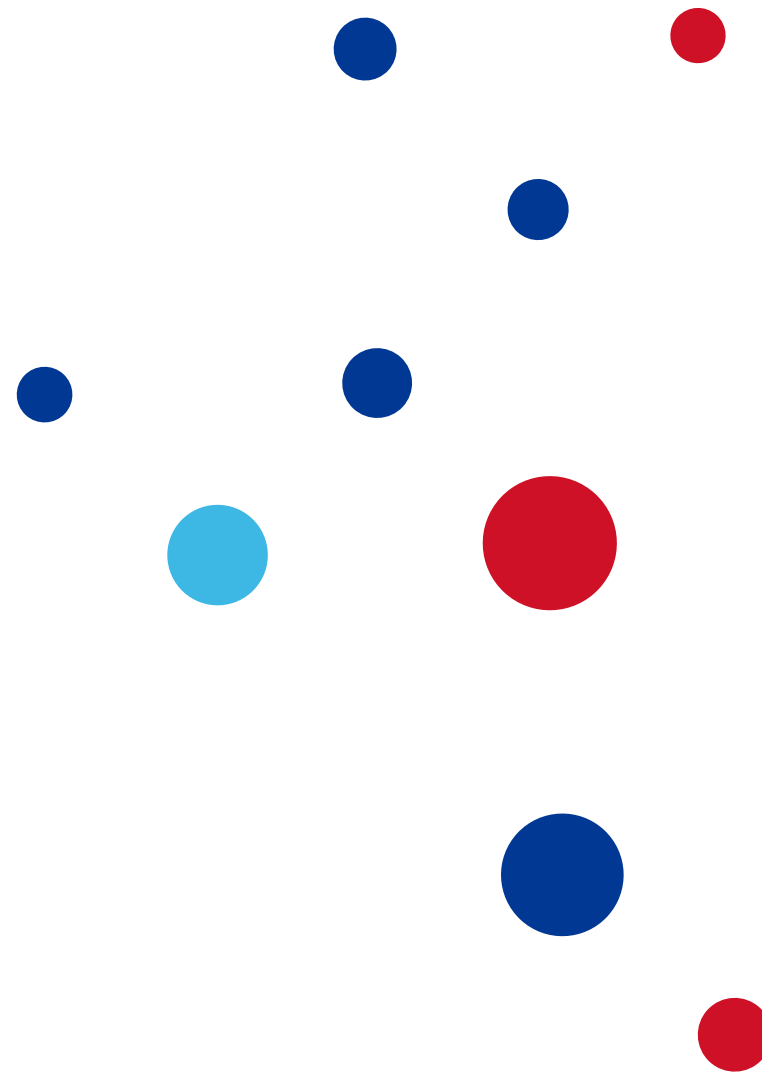|		
České Radiokomunikace a.s.	Company ID No.: 24738875	CZK 5,656,598.40
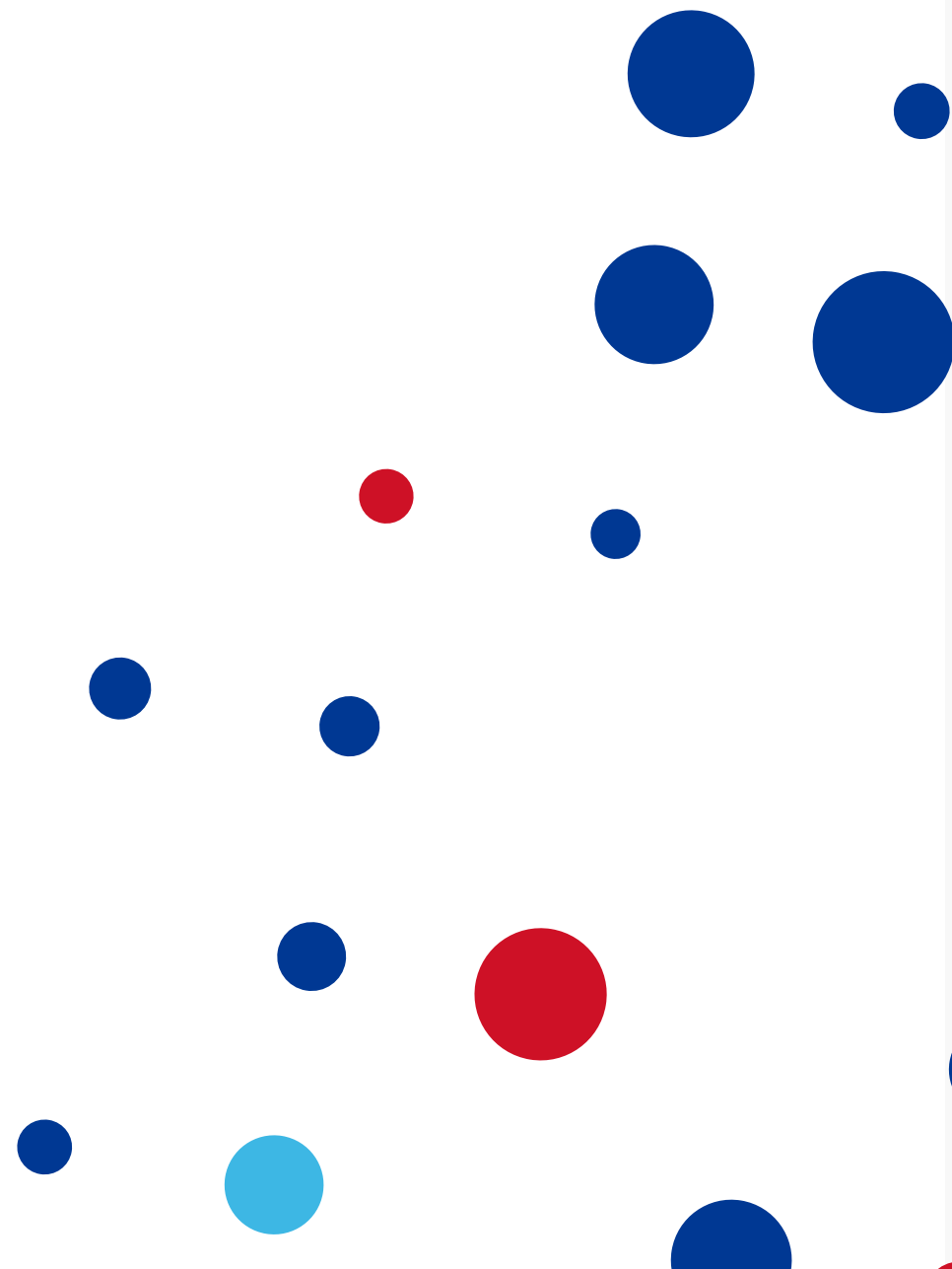
16 **Data on facts between the date of the financial statements and the General Meeting**

No events occurred in the given time that had an impact on the data presented in the financial statements for 2019.

17 **Auditor's report**

ADU.CZ
AUDIT . DANĚ . ÚČETNICTVÍ

TEL: +420 383 371 000
E-MAIL: INFO@ADU.CZ
WWW.ADU.CZ

ZPRÁVA NEZÁVISLÉHO AUDITORA

pro členy zájmového sdružení právnických osob

Výrok auditora

Provedli jsme audit přiložené účetní závěrky zájmového sdružení právnických osob CZ.NIC (dále jen „CZ.NIC") sestavené na základě českých účetních předpisů, která se skládá z rozvahy k 31.12.2019, výkazu zisku a ztráty, za rok končící 31.12.2019, přehledu o změnách vlastního kapitálu, přehledu o peněžních tocích a přílohy této účetní závěrky, která obsahuje popis použitých podstatných účetních metod a další vysvětlující informace. Údaje o CZ.NIC jsou uvedeny v části 1 přílohy této účetní závěrky.

Podle našeho názoru účetní závěrka podává věrný a poctivý obraz aktiv a pasiv zájmového sdružení právnických osob CZ.NIC k 31.12.2019 a nákladů a výnosů a výsledku jejího hospodaření za rok končící 31.12.2019 v souladu s českými účetními předpisy.

Základ pro výrok

Audit jsme provedli v souladu se zákonem o auditorech a standardy Komory auditorů České republiky pro audit, kterými jsou mezinárodní standardy pro audit (ISA) případně doplněné a upravené souvisejícími aplikačními doložkami. Naše odpovědnost stanovená těmito předpisy je podrobněji popsána v oddílu Odpovědnost auditora za audit účetní závěrky. V souladu se zákonem o auditorech a Etickým kodexem přijatým Komorou auditorů České republiky jsme na CZ.NIC nezávislí a splnili jsme i další etické povinnosti vyplývající z uvedených předpisů. Domníváme se, že důkazní informace, které jsme shromáždili, poskytují dostatečný a vhodný základ pro vyjádření našeho výroku.

ADU.CZ

Ostatní informace uvedené ve výroční zprávě

Ostatními informacemi jsou v souladu s § 2 písm. b) zákona o auditorech informace uvedené ve výroční zprávě mimo účetní závěrku a naši zprávu auditora. Za ostatní informace odpovídá představenstvo CZ.NIC.

Náš výrok k účetní závěrce se k ostatním informacím nevztahuje. Přesto je však součástí našich povinností souvisejících s auditem účetní závěrky seznámení se s ostatními informacemi a posouzení, zda ostatní informace nejsou ve významném (materiálním) nesouladu s účetní závěrkou či s našimi znalostmi o účetní jednotce získanými během provádění auditu nebo zda se jinak tyto informace nejeví jako významně (materiálně) nesprávné. Také posuzujeme, zda ostatní informace byly ve všech významných (materiálních) ohledech vypracovány v souladu s příslušnými právními předpisy. Tímto posouzením se rozumí, zda ostatní informace splňují požadavky právních předpisů na formální náležitosti a postup vypracování ostatních informací v kontextu významnosti (materiality), tj. zda případné nedodržení uvedených požadavků by bylo způsobilé ovlivnit úsudek činěný na základě ostatních informací.

Na základě provedených postupů, do míry, již dokážeme posoudit, uvádíme, že

- ostatní informace, které popisují skutečnosti, jež jsou též předmětem zobrazení v účetní závěrce, jsou ve všech významných (materiálních) ohledech v souladu s účetní závěrkou a

- ostatní informace byly vypracovány v souladu s právními předpisy.

Dále jsme povinni uvést, zda na základě poznatků a povědomí o CZ.NIC, k nimž jsme dospěli při provádění auditu, ostatní informace neobsahují významné (materiální) věcné nesprávnosti. V rámci uvedených postupů jsme v obdržených ostatních informacích žádné významné (materiální) věcné nesprávnosti nezjistili.

Odpovědnost představenstva CZ.NIC za účetní závěrku

Představenstvo CZ.NIC odpovídá za sestavení účetní závěrky podávající věrný a poctivý obraz v souladu s českými účetními předpisy a za takový vnitřní kontrolní systém, který považuje za nezbytný pro sestavení účetní závěrky tak, aby neobsahovala významné (materiální) nesprávnosti způsobené podvodem nebo chybou.

Při sestavování účetní závěrky je představenstvo CZ.NIC povinno posoudit, zda je CZ.NIC schopno nepřetržitě trvat, a pokud je to relevantní, popsat v příloze účetní závěrky záležitosti týkající se jejího nepřetržitého trvání a použití předpokladu nepřetržitého trvání při sestavení účetní závěrky, s výjimkou případů, kdy představenstvo CZ.NIC plánuje zrušení CZ.NIC nebo ukončení její činnosti, resp. kdy nemá jinou reálnou možnost než tak učinit.

Odpovědnost auditora za audit účetní závěrky

Naším cílem je získat přiměřenou jistotu, že účetní závěrka jako celek neobsahuje významnou (materiální) nesprávnost způsobenou podvodem nebo chybou a vydat zprávu auditora obsahující náš výrok. Přiměřená míra jistoty je velká míra jistoty, nicméně není zárukou, že audit provedený v souladu s výše uvedenými předpisy ve všech případech v účetní závěrce odhalí případnou existující významnou (materiální) nesprávnost. Nesprávnosti mohou vznikat v důsledku podvodů nebo chyb a považují se za významné (materiální), pokud lze reálně předpokládat, že by jednotlivě nebo v souhrnu mohly ovlivnit ekonomická rozhodnutí, která uživatelé účetní závěrky na jejím základě přijmou.

Při provádění auditu v souladu s výše uvedenými předpisy je naší povinností uplatňovat během celého auditu odborný úsudek a zachovávat profesní skepticismus. Dále je naší povinností:

- Identifikovat a vyhodnotit rizika významné (materiální) nesprávnosti účetní závěrky způsobené podvodem nebo chybou, navrhnout a provést auditorské postupy reagující na tato rizika a získat dostatečné a vhodné důkazní informace, abychom na jejich základě mohli vyjádřit výrok. Riziko, že neodhalíme významnou (materiální) nesprávnost, k níž došlo v důsledku podvodu, je větší než riziko neodhalení významné (materiální) nesprávnosti způsobené chybou, protože součástí podvodu mohou být tajné dohody (koluze), falšování, úmyslná opomenutí, nepravdivá prohlášení nebo obcházení vnitřních kontrol.

- Seznámit se s vnitřním kontrolním systémem CZ.NIC relevantním pro audit v takovém rozsahu, abychom mohli navrhnout auditorské postupy vhodné s ohledem na dané okolnosti, nikoli abychom mohli vyjádřit názor na účinnost jejího vnitřního kontrolního systému.

- Posoudit vhodnost použitých účetních pravidel, přiměřenost provedených účetních odhadů a informace, které v této souvislosti představenstvo CZ.NIC uvedlo v příloze účetní závěrky.

- Posoudit vhodnost použití předpokladu nepřetržitého trvání při sestavení účetní závěrky představenstvem a to, zda s ohledem na shromážděné důkazní informace existuje významná (materiální) nejistota vyplývající z událostí nebo podmínek, které mohou významně zpochybnit schopnost CZ.NIC nepřetržitě trvat. Jestliže dojdeme k závěru, že taková významná (materiální) nejistota existuje, je naší povinností upozornit v naší zprávě na informace uvedené v této souvislosti v příloze účetní závěrky, a pokud tyto informace nejsou dostatečné, vyjádřit modifikovaný výrok. Naše závěry týkající se schopnosti CZ.NIC nepřetržitě trvat vycházejí z důkazních informací, které jsme získali do data naší zprávy. Nicméně budoucí události nebo podmínky mohou vést k tomu, že CZ.NIC ztratí schopnost nepřetržitě trvat.

- Vyhodnotit celkovou prezentaci, členění a obsah účetní závěrky, včetně přílohy, a dále to, zda účetní závěrka zobrazuje podkladové transakce a události způsobem, který vede k věrnému zobrazení.

Naší povinností je informovat představenstvo CZ.NIC mimo jiné o plánovaném rozsahu a načasování auditu a o významných zjištěních, která jsme v jeho průběhu učinili, včetně zjištěných významných nedostatků ve vnitřním kontrolním systému.

Ve Strakonicích, dne 16. června 2020

ADU.CZ s.r.o.
Zámostí 68, 387 06 Malenice
oprávnění Komory auditorů České republiky číslo 368
za auditorskou společnost vypracovala Ing. Simona Pacáková, auditor
auditorské oprávnění Komory auditorů České republiky číslo 1825

Digitálně podepsal Ing.
SIMONA PACÁKOVÁ
Datum: 2020.06.16
11:51:25 +02'00'

18 **Seat and contact details**

CZ.NIC, z.s.p.o.

Milešovská 1136/5
130 00 Prague 3

Company ID No.: 67985726
Tax ID No.: CZ67985726
Phone: +420 222 745 111
Fax: +420 222 745 112
www.nic.cz

The association is registered in the association register kept by
the Municipal Court in Prague, under file number L 58624.

CZ.NIC – 24-hour customer support

Phone: +420 222 745 111
Phone: +420 731 657 660
E-mail: podpora@nic.cz