CZ DOMAIN REGISTRY

2025 **Annual Report**

1 Profile of the Association **3**

2 Foreword **5**

3 .CZ domain **8**
3.1 Status and development of the number of registrations 9
3.2 Publication of the list of domain names removed from the DNS 11
3.3 Registrars 11
3.4 Domain Auction 17

4 Infrastructure **19**
4.1 Data centres 20
4.2 Technical aspects of domain administration 22
4.3 Support for Internet infrastructure 30
4.4 Support for the basic Internet infrastructure 34

5 CSIRT security team **36**
5.1 CSIRT.CZ – National CERT Team of the Czech Republic 37
5.2 CZ.NIC-CSIRT 42

6 MojeID **43**
6.1 Security of the MojeID service 44
6.2 Private sector and public administration partnership services 45
6.3 MojeID users 47
6.4 MojeID as a tool for cross-border authentication in Europe 48

7 Turris **49**
7.1 Software development 50
7.2 Hardware development 50
7.3 Turris OS 50
7.4 Business cooperation 51

8 CZ.NIC Labs **52**
8.1 ADAM 53
8.2 BIRD 54
8.3 Datovka 54
8.4 Knot DNS and Knot Resolver 55
8.5 DNS Patrol 59

9 Education and awareness **61**
9.1 Communication with the public 62
9.2 Popularisation series 63
9.3 CZ.NIC Academy educational centre 63
9.4 Conferences 66
9.5 CZ.NIC Edition 66

10 Cooperation,support and partnership **68**
10.1 Cooperation in the Czech Republic 69
10.2 Social responsibility (supporting third parties and projects) 71
10.3 Cooperation abroad 72

11 Grant projects **75**

12 Structure of the Association **78**
12.1 Members 79
12.2 Bodies of the Association 82

13 Human resources **85**
13.1 Number of employees 86
13.2 Employee structure 88

14 Selected financial indicators **90**
14.1 Balance Sheet 91
14.2 Profit and Loss Statement 92

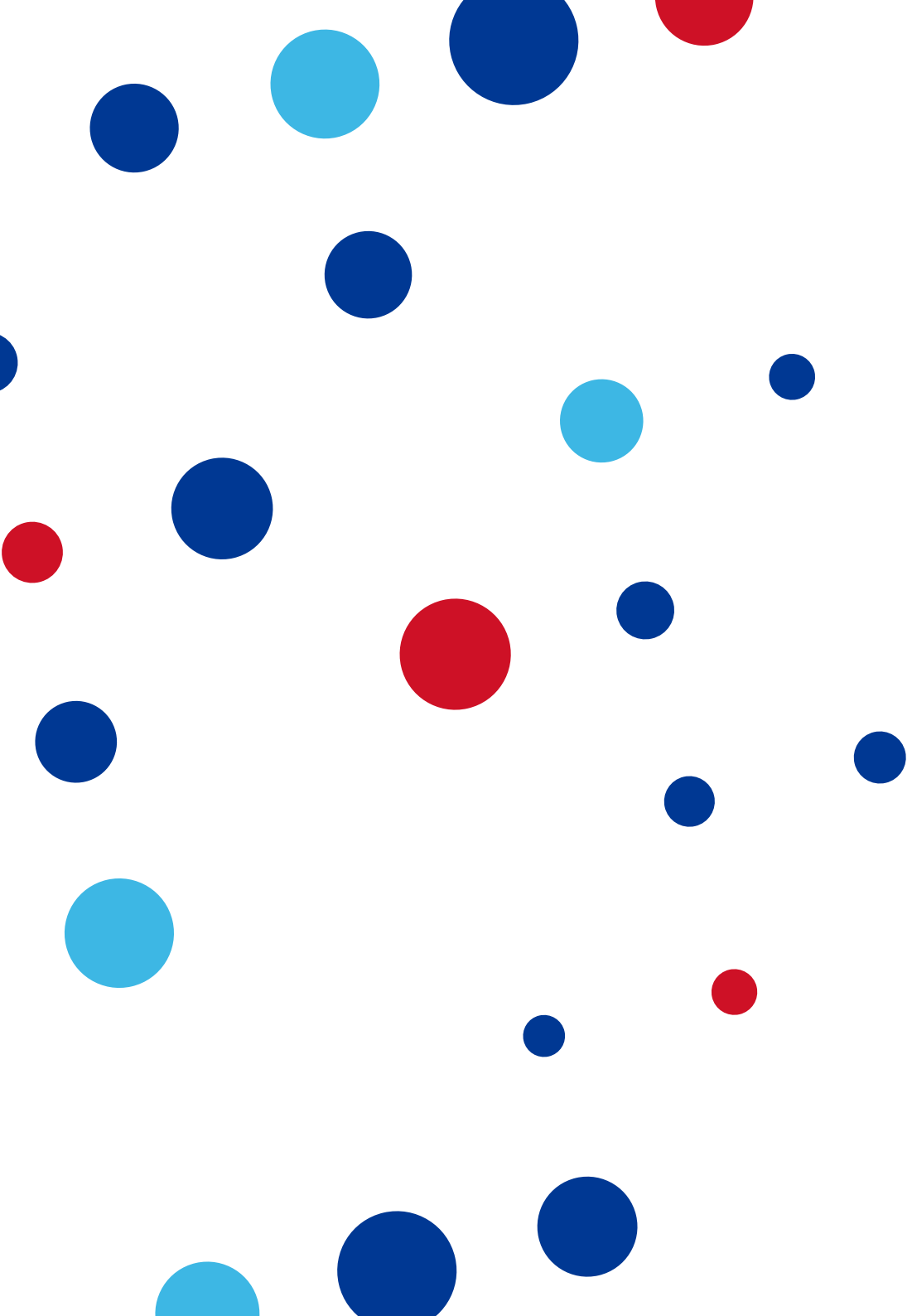
15 List of suppliers **93**

16 Events between the date of the Financial Statements and the General Meeting **95**

17 Auditor's Report **97**

18 Registered officeand contact details **101**

1 Profile of the Association



CZ.NIC is an interest association of legal entities, an open and independent organisation whose main activity is the administration of the register of the national top-level .CZ domain and securing its operation.

Cybersecurity is a key part of its activities, both through the national CSIRT.CZ team and through a number of the Association's own security projects. In addition, the Association is involved in research, development and public awareness-raising in the field of the Internet, network technologies and Internet protocols. It has long supported the development of the online community in the Czech Republic and abroad.

The Association was founded in May 1998 in response to the growing importance of the Internet and the interest in registering domain names under ccTLD .CZ. At the end of 2025, the Association had 117 members divided into three chambers.

CZ.NIC is now a stable and trustworthy organisation ensuring the reliable operation of the Czech national domain, .CZ. Since 2013, it has held ISO 27001 certification, which confirms its high standards of information security and established processes.

For domain holders, registrars and the wider Internet community, the Association is a reliable partner which, in addition to domain administration, actively contributes to Internet security and carries out a range of educational and awareness-raising activities.

2 Foreword

Ladies and Gentlemen,

The 2025 Annual Report describes another year in the development of the CZ.NIC Association. In line with CZ.NIC's new Concept for 2025–2030, we continued operating and developing a trustworthy, secure and stable infrastructure and generally beneficial Internet services (including the .CZ domain) for the benefit of the Internet community.

The .CZ national domain grew by 2% and had 1,515,860 registered domain names at the end of the year. The monthly average for new registrations was 16,254. The Domain Auction service launched in 2024 established itself in 2025 as a transparent way of returning vacated domains to the domain space. Bidders were granted preferential rights to 5,387 domains, and 1,241 individual participants actively took part in domain auctions last year.

CZ.NIC once again significantly strengthened its network infrastructure, i.e. both the second link to the NIX.CZ peering node at the CE Colo site, which has been upgraded to 400 Gbps, and the international connectivity at the DC TOWER site, which has been upgraded to 100 Gbps. The connection to the non-public site has also undergone the same upgrade. We have recently connected our DNS node in Los Angeles to the Equinix peering centre. The very good news is that the total capacity of the DNS infrastructure for the .CZ domain approached 1.5 Tbps at the end of the year and is distributed across twenty-six locations in fifteen countries on six continents.

In 2025, the FRED software administered domains in twelve countries around the world and now includes Venezuela (.VE). However, the most significant expansion in the use of this open-source tool came from the Czech Republic. Following the outcome of a tender procedure, we launched the GOV.CZ domain administration portal in December 2025. For the Association, carrying out this contract entails responsibility for a second domain register with its own domain lifecycle. At the same time, following discussions with registrars at a themed workshop, we began making adjustments to the system in line with the obligations arising from the new Cyber Security Act.

Thanks to the Association's proactive approach, the share of domains secured by DNSSEC technology has exceeded two-thirds – specifically 66.8% of the total number of registered domains. For the first time in history, their total number has exceeded one million. In an international comparison of top-level domains, .CZ ranks among the best-equipped ccTLDs in terms of DNSSEC support.

The CSIRT.CZ security team handled a total of 3,305 incidents in 2025, the highest number since 2008. Preparations for the new Cyber Security Act played a part in that, as even organisations not yet subject to this obligation began to report incidents. Customer activity in the Deny Lists service also had an impact on these figures.

In 2025, we also launched the new Turris Omnia NG routers with Wi-Fi 7 support. We established cooperation with a new partner in Switzerland and expanded our retail network in Italy and Slovenia.

The Association successfully completed the EWC pilot project focusing on the European Digital Identity Wallet. We demonstrated how to initialise a wallet using the MojeID service, verify the domain holder and issue a certificate confirming the holding of the domain. The demonstration took place live at the European Commission's EUDI Wallets Launchpad event in December. MojeID users started enjoying greater convenience at the end of the year when the Association launched a system allowing them to log in (not only to government services) using a QR code.

In 2025, we launched a new service, DNS Patrol, to ensure secure DNS in the networks of large organisations. We have been running it for the Vysočina Region since November 2025; in 2026, it will be extended to cover other organisations within the Rowanet regional network.

The CZ.NIC Academy underwent a major change in 2025, when we moved it to newly reconstructed premises in Vinohradská Street, Prague 3. We expanded our range of educational activities to include four new courses, one of which is the popular e-learning course named "Digital Footprint". It is worth noting that we have built the Wi-Fi infrastructure at our headquarters and at the Academy using Turris MOX routers developed by the Association, and have moved away from a commercially licensed solution.

In 2025, CZ.NIC Edition continued publishing popular specialised publications focusing on the Internet and related technologies. It has recently been expanded to include two new titles: *Programovací jazyk GO* (GO Programming Language) by Pavel Tišnovský and the popular *Kity, bity, neurony* (Kits, Bits, Neurons) by Martin Malý.

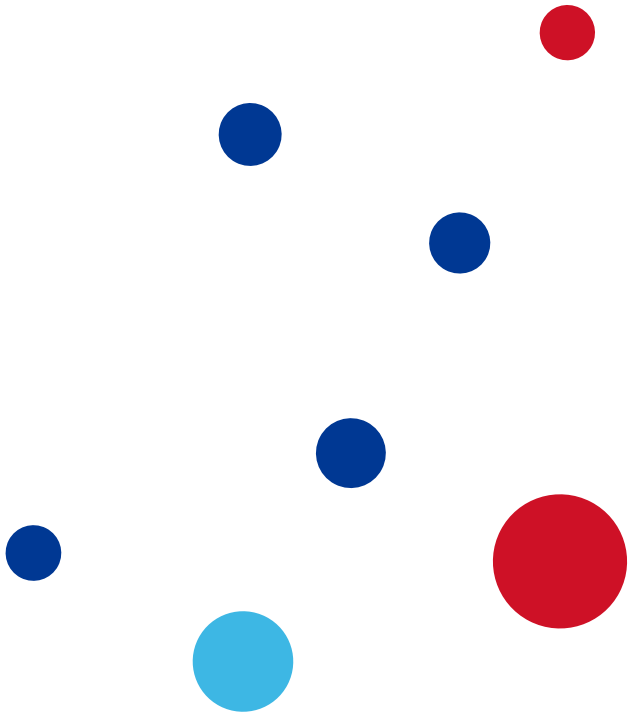
We are delighted that in 2025 we managed to (co-)organise several community events, including the CSNOG community meet-up in Zlín, the LinuxDays 2025 conference and IPv6 Day. In June, we also hosted the ICANN 83 international meeting in Prague.

The Association's financial performance remained stable; more detailed financial indicators can be found in the following sections of this report.

We would like to thank our Association members, partners, colleagues and users of our services for their trust, and we look forward to our continued collaboration, which helps us to do things right.

Yours sincerely,

Ing. Tomáš Košňar – Chair of the Board of Directors
Mgr. Ondřej Filip, MBA – Chief Executive Officer

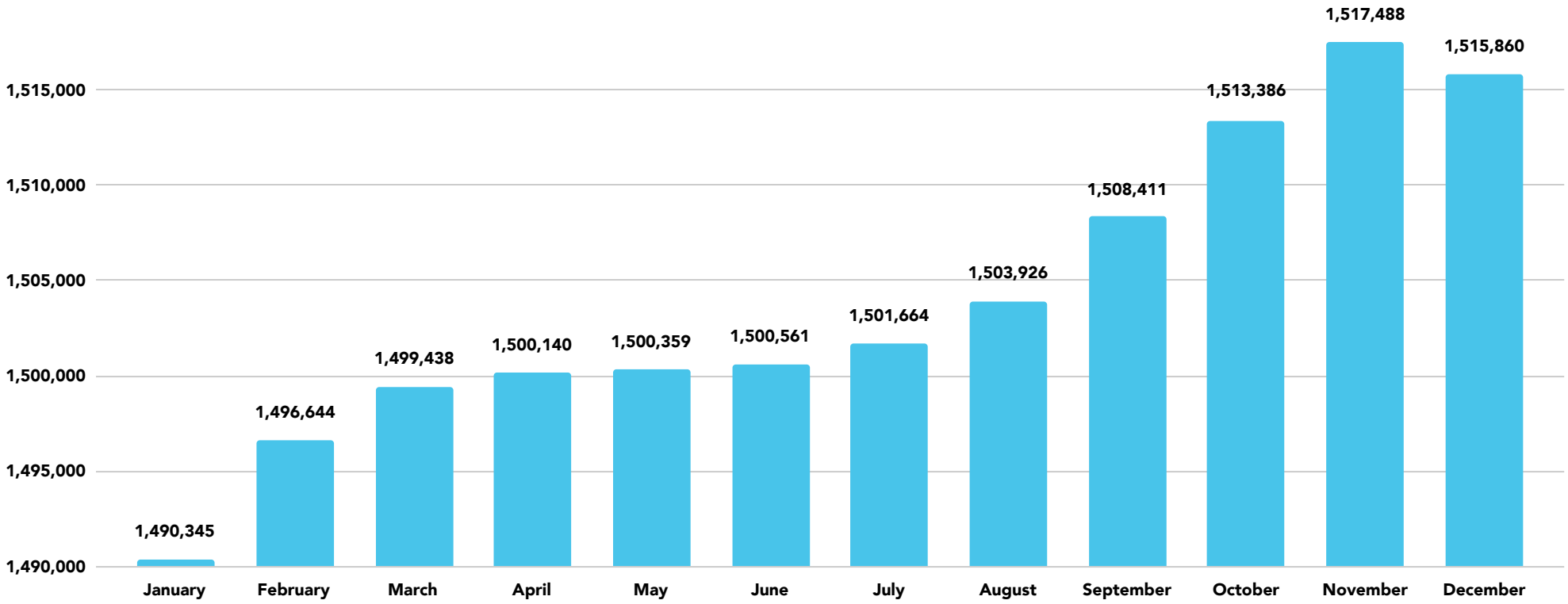


3 .CZ domain

3.1 Status and development of the number of registrations

In 2025, the trend of slight growth in the total number of registered .CZ domains continued, despite a small decline recorded in December of that year. As at 31 December 2025, the total number of domain names stood at **1,515,860**, representing a 2% increase over the previous year.

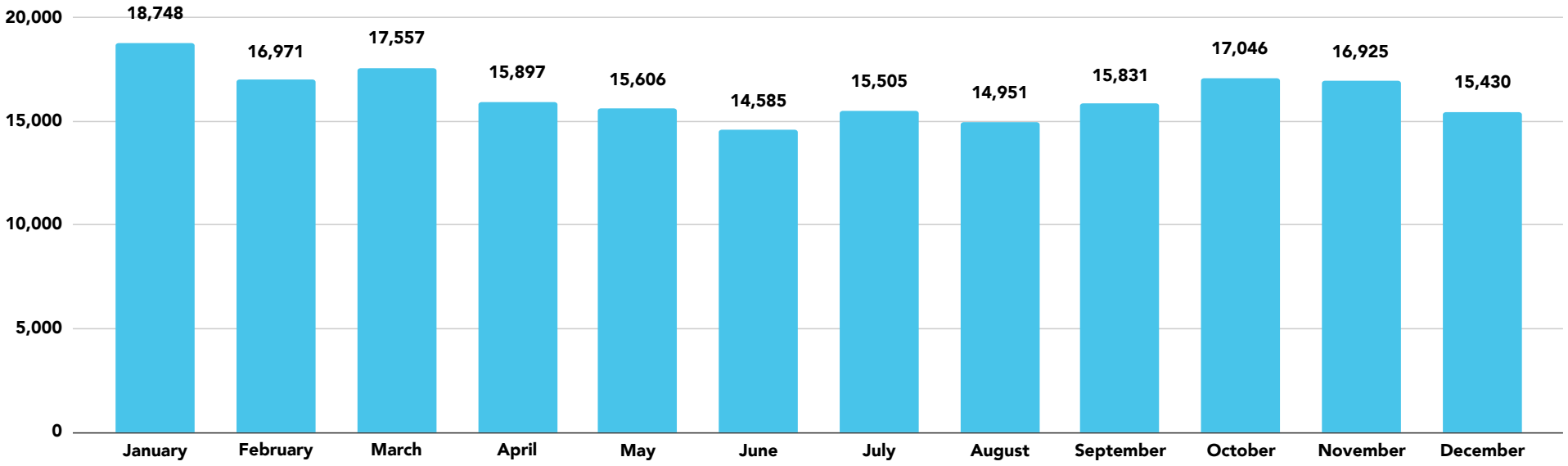
Total number of registered .CZ domain names in 2025



* The data in the chart is always as of the last day of the month; the increase in the number of domain names is calculated from 1 January to 31 December.

In 2025, an average of **16,254 new domain names** were registered every month.

Number of newly registered .CZ domain names in 2025



3.2 Publication of the list of domain names removed from the DNS

The CZ.NIC Association may decide to remove a particular domain name from the .CZ zone for several reasons. The effect of such an intervention is that the services made available through that domain name become unavailable. While the services themselves still physically exist, it is not possible to find them using the corresponding domain name.

This is most often the case if the holder's data is incorrect, incomplete or misleading and despite several requests it has not been corrected. Other reasons may be decisions by public authorities (especially the police, but also the courts) or the application of Article 17 of the Rules of Registration of Domain Names (threat to national or international computer security, most often in connection with the spread of phishing).

To ensure greater transparency, the list of domain names currently removed from the zone is available on the Association's website.

3.3 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 towards them as if they were a wholesale partner, but also provides the technical aspects and functionality of the .CZ top-level domain.

During 2025, the Association established cooperation with three new registrars – BARBERO & Associates Ltd (UK), INWX GmbH and OpusDNS GmbH (both DE).

At the end of 2025, a total of 49 companies, 24 domestic and 25 foreign, had concluded a registrar contract with the Association. This number of entities offers a broad choice for end customers and also supports competition.

3.3.1 Overview of .CZ domain name registrars

List of all accredited registrars as at 31 December 2025

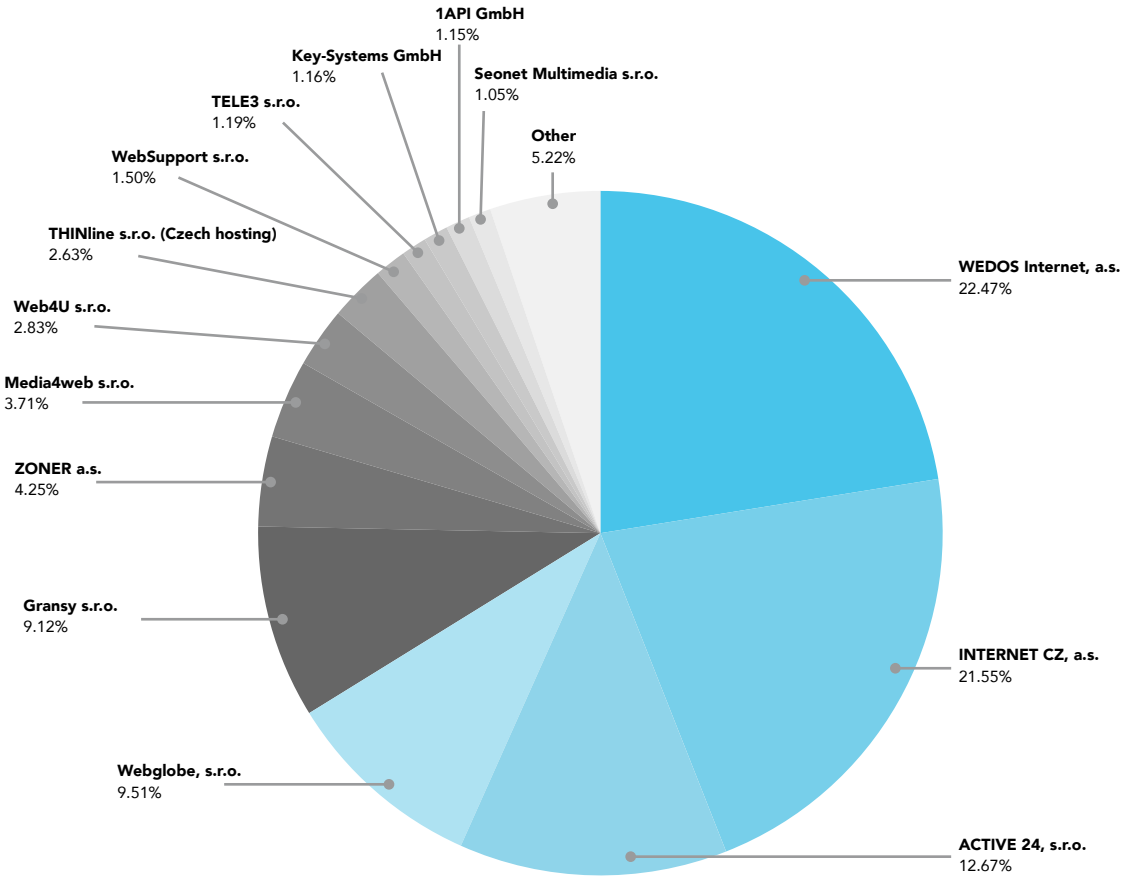
1API GmbH
ACTIVE 24, s.r.o.
AERO Trip PRO s.r.o.
Ascio Technologies inc.
ASPone, s.r.o.
BARBERO & Associates Ltd
COREHUB SL (Sociedad Unipersonal)
Corporation Service Company (Singapore) Pte Ltd
DomainProfi GmbH
Domeneshop AS
Dynadot Inc.
e-BAAN Net s.r.o.
Gandi SAS
Gransy s.r.o.
Hosting Concepts B.V. d/b/a Registrar.eu
Instra Corporation Pty Ltd
INTERNET CZ, a.s.
InterNetX GmbH
INWX GmbH
Key-Systems GmbH
KRAXNET s.r.o.
Lexsynergy Limited
MarkMonitor Inc.
Media4web, s.r.o.
MIRAMO spol. s r.o.
NAMESHIELD SAS
Netim
nexum Trilog a.s.
Nom-IQ Ltd, dba Com Laude
O2 Czech Republic a.s.
ONE.CZ s.r.o.
OpusDNS GmbH
OVH, Sas
PIPNI s.r.o.
ProfiHOSTING s.r.o.
Quantcom, a.s.
Safenames Ltd.
Seonet Multimedia s.r.o.
Seznam.cz, a.s.
TELE3 s.r.o.
THINline s.r.o.
united-domains GmbH
Variomedia AG
Web4U s.r.o.
Webglobe, s.r.o.
WebSupport s.r.o.
WEDOS Internet, a.s.
ZONER a.s.
ZooControl s.r.o.

3.3.2 Major domain name registrars

The leading registrar in terms of the number of administered domains was WEDOS Internet, a.s., closely followed by INTERNET CZ, a.s., and then ACTIVE 24, s.r.o., Webglobe, s.r.o. and Gransy s.r.o.

Number of domains by registrars

The chart shows registrars with a market share of over 1%.



3.3.3 Certification of registrars

Since 2011, the certification project has made it easier to navigate the large number of registrars, particularly in terms of their portfolio and the quality of the services they offer. The certification methodology was prepared **in cooperation with registrars and the Association of E-commerce (APEK)**.

Registrars that are interested in participating in the programme can receive the *Certified Registrar* logo, always for a period of one year.

By the end of 2025, a total of seven registrars had been certified, with (as in 2024) only one registrar achieving a 5* rating.

Certification of registrars, reflected in the number of awarded stars

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
*****	9	10	10	9	9	9	8	7	7	7	1	**1**
****	3	2	2	3	3	3	3	3	2	2	2	**3**
***											1	**2**
**											1	**1**

In 2024, new criteria and stricter assessment standards were introduced, which is why it is now more difficult to achieve the full mark. The registrars are actively working on improvements to their systems.

3.3.4 Cooperation with registrars

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

It does so as part of the **co-marketing programme**, under which the **CZ.NIC** Association provides funding to registrars for the implementation of communication campaigns aimed at promoting registrations of domain names in ccTLD .CZ. The amount of the contribution depends on the size of the registrar, the scope of the campaign and other factors, such as the use of the MojeID service with a connection to the NIA (which, among other things, increases the accuracy and protection of data in the register) and domain security through DNSSEC, the expansion of which CZ.NIC is trying to promote. In 2025, only registrars who, among other things, had successfully completed the certification programme were eligible to take part in the programme.

In 2025, the programme was revised and renamed the **Benefits Scheme**. In addition to a direct contribution towards the marketing campaign (the terms of which remained the same as in previous years) registrars were given the option to take part in a shared campaign run directly by the Association, or to request a direct payment of part of the contribution. Funding earmarked for the programme has also been increased.

Although most registrars continued contributing to their own campaigns, some of them did in fact take advantage of the newly available options.

A total of eight registrars took part in the programme, and the CZ.NIC Association paid them a total of **CZK 13,861,852.42**.

3.3.5 Resolution of disputes over domain names in ccTLD .CZ

Litigation before a general court, provided that there are no circumstances (such as appellate proceedings) that might prolong its duration, takes approximately 2–3 years. However, even that is a very long time in the fast-moving world of the Internet, which is why we sought an alternative method of dispute resolution that would not only be quicker, but also reliable and widely respected. The Alternative Dispute Resolution (ADR) system was introduced in 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 attached to the Czech Chamber of Commerce and the Agrarian Chamber of the Czech Republic. Over the ten years that this model was in operation, the Arbitration Court heard more than one hundred cases.

Following a decision by the Supreme Court at the end of 2013, there was a change; in March 2015, an ADR system was introduced, the basic principles of which are essentially identical to those that have been successfully used in disputes over generic TLDs (UDRP) or domain names registered in the top-level .EU domain. The platform on which the disputes are handled 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, with the undeniable advantage of the possibility of conducting the entire proceedings online.

However, the ADR system used since 2015 is not an arbitration procedure within the meaning of the arbitration law, which is also reflected in the applied terminology. It is based on a contractual arrangement and can only be used to request the transfer or cancellation of a domain name. Any other claims, such as claims for damage, the surrender of unjust enrichment or appropriate redress, must be brought before a general court. A decision issued within ADR does not constitute an enforceable title, and neither ongoing nor concluded ADR proceedings constitute an obstacle on the grounds of *lis pendens* (pending suit) or *res judicata* (claim preclusion). It is therefore possible to bring the same claim before a general court at any time.

Ten years' experience of using this ADR system shows that it has been accepted and that its popularity remains stable. The fact that there is a domain ADR in ccTLD .CZ also corresponds to Commission Recommendation (EU) 2024/915 of 19 March 2024 on measures to combat counterfeiting and enhance the enforcement of intellectual property rights, which calls on EU-based top-level domain registers to "provide for an ADR procedure in which IP rights can be invoked by: (a) taking into account the international good practices in this area and in particular the relevant recommendations of the World Intellectual Property Organization to ensure that speculative and abusive registrations are prevented as much as possible; (b) complying with uniform procedural rules in line with those set out in the ICANN Uniform Domain Name Dispute Resolution Policy."

Year	Number of disputes initiated in ADR
2015	7
2016	20
2017	22
2018	22
2019	29
2020	29
2021	22
2022	25
2023	33
2024	34
2025	**30**

Among the general courts, the Municipal Court in Prague most often hears disputes over domain names, especially in view of the fact that it is a specialised court for, inter alia, intellectual property and competition disputes, which are the most frequently violated rights in the case of domain disputes. In conclusion, it should be noted that the **majority of claimants (holders of the rights) leave the Arbitration Court attached to the Czech Chamber of Commerce and the Agrarian Chamber of the Czech Republic with their claim being satisfied, and they usually receive the expert's decision within three (3) months of the commencement of the resolution of the dispute.**

3.3.6 Customer support

Customer support available **24/7** is an integral part of .CZ domain operation.

The aim of customer support is to ensure **maximum care for domain name holders**, especially in situations where the domain name is threatened with cancellation, or where a contact change or domain transfer occurs. Assistance for MojeID service users is also an integral part of customer support.

Customer support is based on a proactive approach to domain name holders, the aim of which is to prevent a domain from being removed from the .CZ zone and subsequently cancelled, e.g. due to outdated contact details or the non-payment of fees. Given the distributed .CZ domain administration system, customer support is the only case where CZ.NIC is in direct touch with domain name holders.

In addition to the standard email notifications concerning non-renewal of domain registration for the next period, customer support manually checked roughly 270,000 domains before they were removed from the .CZ zone (i.e. effectively disabled). It also contacted (by phone or text message) more than 200,000 domain holders who were threatened with cancellation.

Development of individual customer support tasks in 2021–2025

	2021	2022	2023	2024	2025
Manual check of domain names before exclusion	18,658	20,544	22,672	22,492	**22,286**
Manual check of domain names before cancellation	15,050	16,160	18,431	18,407	**17,986**
Calls to holders (contacts) of domain names scheduled for cancellation	444 *1	552 *1	413	448	**477**
Text messages – information about upcoming domain name cancellation	9,028	9,510	10,575	11,307	**11,872**
Emails sent before exclusion	2,066	3,633	1,477 *2	1,450 *2	**1,633 *2**
Responses to email inquiries	3,245	2,783	2,762	3,081	**4,069**
Responses to telephone inquiries	1,547	1,393	1,099	1,428	**1,392**
Requests (validation, blocking…)	162	155	182	282	**207**
Chat inquiries	1,295	503	724	371	**244**
Manual data accuracy check	1,188	1,387	1,437	1,085	**1,301**
Manual data accuracy check – detailed for EU	479	542	308	811	**874**
Manual data accuracy check – detailed for other countries	257	439	370	285	**211**

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

*1 Due to restricted office operations during the pandemic, the statistics only take into account part of the calls made.

*2 Only unique email addresses are included in the statistics. If the same email appears in multiple domains, it will only be included once.

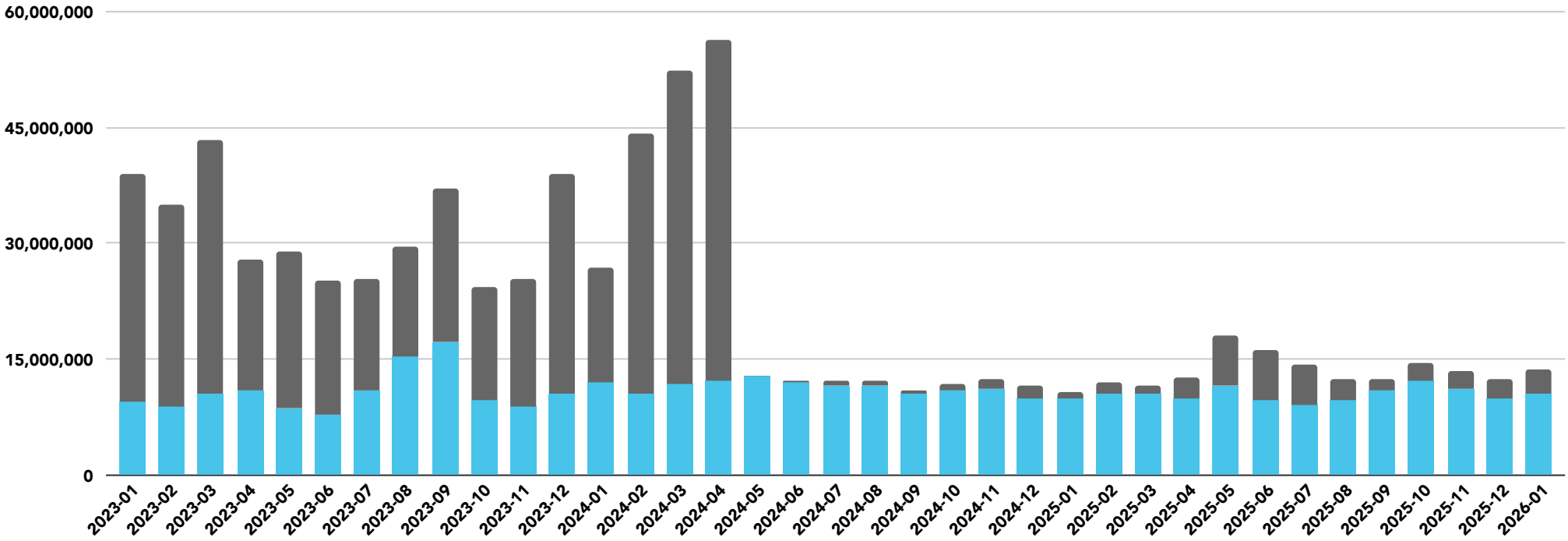
3.4 Domain Auction

The Association has been operating the Domain Auction service since 2024. As part of this service, interested parties can bid for the preferential right to register a domain that has already been deleted (cancelled), thereby allowing it to be returned to the domain space. The winning bidder can exercise the preferential right and register the domain upon payment.

In the past, there were fierce battles over the registration of attractive expired domains, in which, given the technical and administrative restrictions on access to the register, only a limited number of parties were actually able to take part.

For this reason, the CZ.NIC Association has decided to open up the market for deleted domains to everyone and, through its Domain Auction service, offers the opportunity to obtain a preferential right to register. Thanks to Domain Auction, there has been a significant reduction in the number of domain disputes, which has also led to a very significant drop in traffic between registrars and the .CZ domain register via the EPP protocol. The CZ.NIC Association was therefore able to increase the minimum number of free queries to registrars from 25,000 to 100,000 per month with effect from 1 September 2025. The decline in EPP traffic associated with domain disputes and the (as yet) minimal impact of the increase in the minimum number of queries on overall EPP traffic can be seen in the following chart.

EPP traffic trends



In 2025, 5,387 .CZ domains were sold at auction, with the share of domains sold at auction compared to those entering the auctions averaging 3.3%. Of these auctioned domains, 5,051 were subsequently registered, representing almost 94% of successful exercises of preferential rights.

A total of 1,241 different bidders actively took part in the auctions throughout the year. The high number of active bidders is further evidence that the launch of Domain Auctions has helped to level the playing field when it comes to accessing domains released from the register.

The preferential rights auctioned and paid for exceeded CZK 5,500,000 (exclusive of VAT) in the year under review, which means that the time invested in development will pay for itself within a few years.

Public statistics provide detailed information on the progress of Domain Auctions.

4 Infrastructure

4.1 Data centres

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

- the DC TOWER data centre of České Radiokomunikace in Prague 3,
- the CE Colo data centre in Prague 10,
- a non-public site outside of Prague.

All the locations have their own Internet connection and a connection to the electrical 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 site outside of 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.

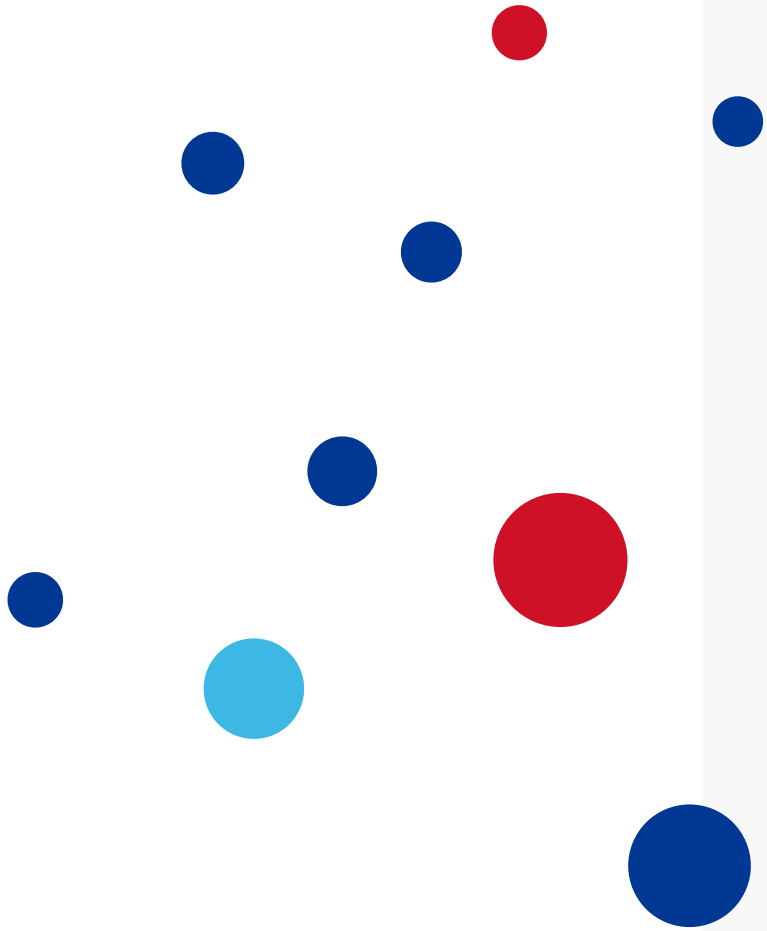
In 2025, changes were implemented at the CE Colo site, which included, among other things, the installation of measures to enhance physical security and improve energy efficiency.

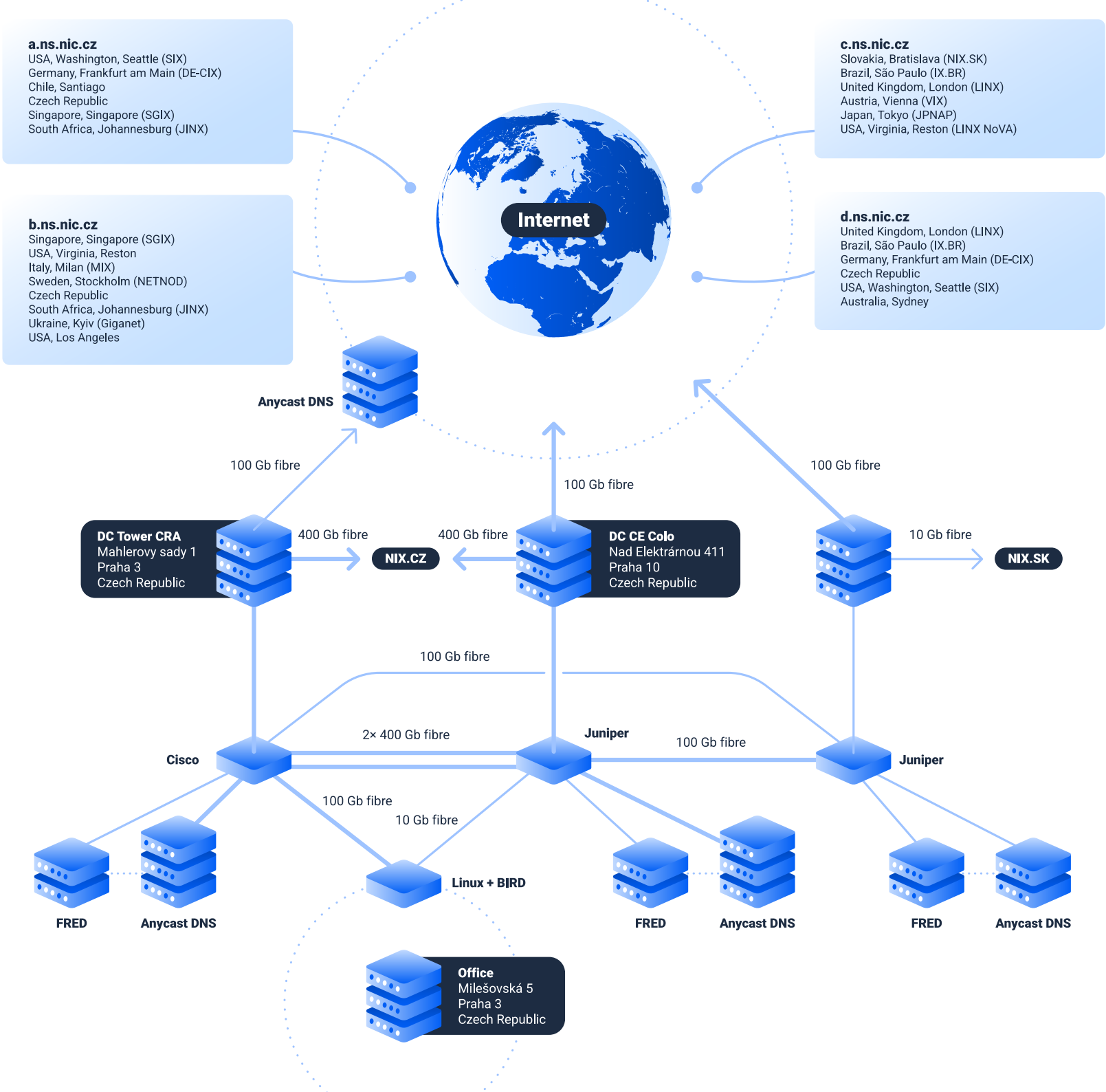
As part of the network infrastructure development, connectivity to the Czech NIX.CZ peering node was significantly strengthened. Following the work carried out at the DC TOWER site in 2024, the backbone network components were upgraded in 2025 and the capacity of the second link to NIX.CZ was also increased at the CE Colo site, namely to 400 Gbps.

In 2025, the Association continued to maintain a 100% pass rate in repeat tests of compliance with the technical requirements of the FENIX project.

In 2025, the server hardware at the DC TOWER site, on which the .CZ register's services run, was upgraded.

As part of the CZ.NIC Academy's relocation, two new dedicated data circuits were installed in 2025 to connect the branch office on Jiřího z Poděbrad Square. At the head office in Milešovská Street, the entire Wi-Fi infrastructure has been upgraded from the original commercial solution, which was subject to licensing restrictions, to a new decentralised system based on small Turris MOX routers developed by the Association.




a.ns.nic.cz
USA, Washington, Seattle (SIX)
Germany, Frankfurt am Main (DE-CIX)
Chile, Santiago
Czech Republic
Singapore, Singapore (SGIX)
South Africa, Johannesburg (JINX)
b.ns.nic.cz
Singapore, Singapore (SGIX)
USA, Virginia, Reston
Italy, Milan (MIX)
Sweden, Stockholm (NETNOD)
Czech Republic
South Africa, Johannesburg (JINX)
Ukraine, Kyiv (Giganet)
USA, Los Angeles
c.ns.nic.cz
Slovakia, Bratislava (NIX.SK)
Brazil, São Paulo (IX.BR)
United Kingdom, London (LINX)
Austria, Vienna (VIX)
Japan, Tokyo (JPNAP)
USA, Virginia, Reston (LINX NoVA)
d.ns.nic.cz
United Kingdom, London (LINX)
Brazil, São Paulo (IX.BR)
Germany, Frankfurt am Main (DE-CIX)
Czech Republic
USA, Washington, Seattle (SIX)
Australia, Sydney
Internet
Anycast DNS
100 Gb fibre
100 Gb fibre
100 Gb fibre
DC Tower CRA
Mahlerovy sady 1
Praha 3
Czech Republic
400 Gb fibre
NIX.CZ
400 Gb fibre
DC CE Colo
Nad Elektrárnou 411
Praha 10
Czech Republic
10 Gb fibre
NIX.SK
100 Gb fibre
2× 400 Gb fibre
Cisco
Juniper
100 Gb fibre
Juniper
100 Gb fibre
10 Gb fibre
FRED
Anycast DNS
Linux + BIRD
FRED
Anycast DNS
FRED
Anycast DNS
Office
Milešovská 5
Praha 3
Czech Republic

4.2 Technical aspects of domain administration

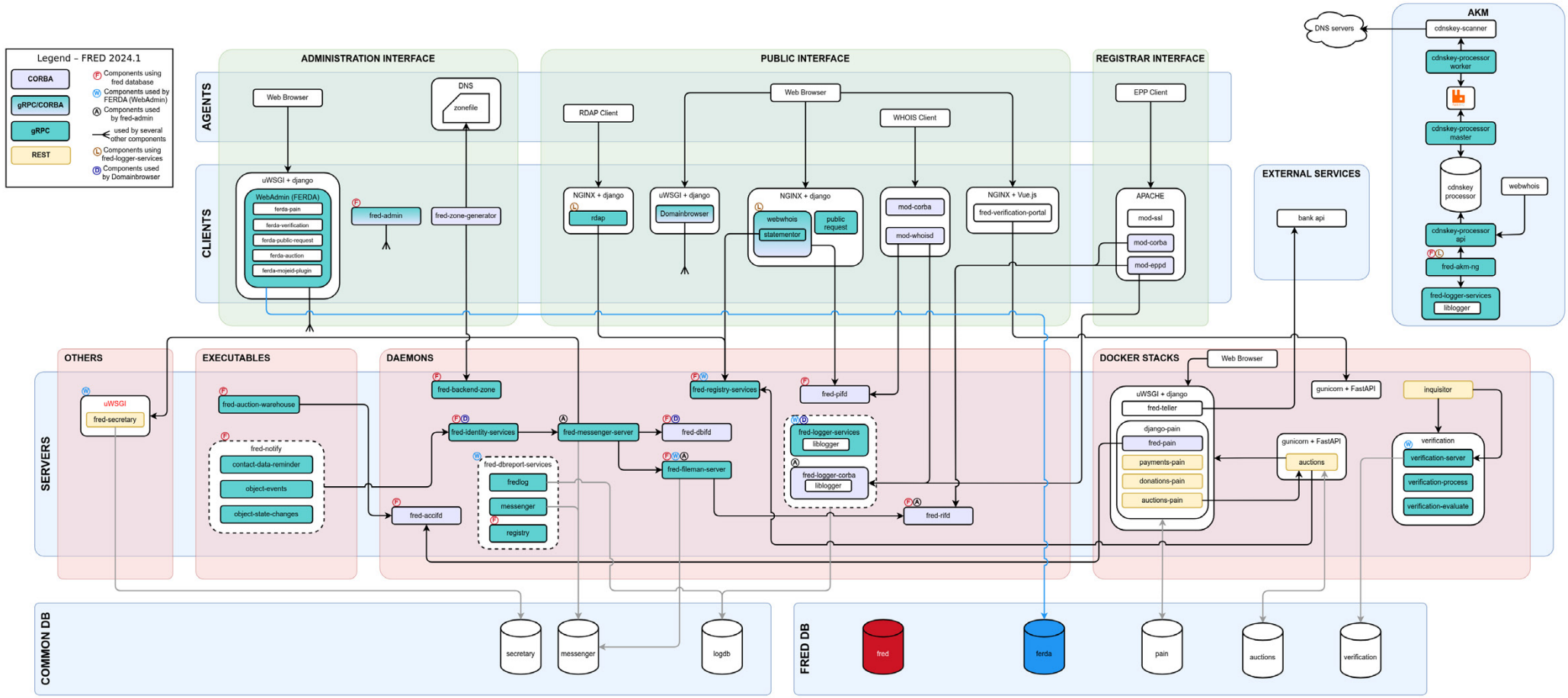
The infrastructure of the register carefully follows the rules of diversity of hardware equipment so that a possible error of a particular hardware manufacturer affects only a part of the infrastructure, thus minimising the possibility of the failure of the central domain register as a whole. Therefore, technologies from different manufacturers are installed at every site. The same approach is used by the Association 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 such a way that they are capable of taking over the operation of any component of the register at very short notice.

The central register 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 both of these protocols.

Among the most significant changes to the FRED system architecture in 2025 were, for example, the completion of the dockerisation of the FRED system's Python modules and a major technological upgrade to the Domain Browser. As part of this, the presentation website was separated from the application and migrated to the Nuxt cluster, which had already proven its worth within the MojeID service's infrastructure.

FRED system software architecture



4.2.1 FRED (Free Registry for ENUM and Domains)

The FRED software for the operation of the central register, developed and operated by the CZ.NIC Association, has been released as an open and free software under the GNU GPLv3+ licence in support of small registers. This way, small and newly-started registers can operate their domains on a system developed for the operation of the Czech domain, which, thanks to its parameters and capacity, is in fact prepared for a much higher number of domains than are currently registered in ccTLD .CZ.

Apart from the Czech Republic, the FRED system performed domain administration in twelve other countries in 2025. It is used to administer the domains of Argentina (.AR), Bosnia and Herzegovina (.BA), Costa Rica (.CR), Albania (.AL), North Macedonia (.MK), Tanzania (.TZ), Angola (.AO), Malawi (.MW), Lesotho (.LS), Macau (.MO), Paraguay (.PY) and Venezuela (.VE), which switched to FRED in 2025. With over 670,000 registered domain names, the deployment in Argentina is the second largest instance of the FRED system.



Countries where FRED is used for domain administration

The CZ.NIC Association offers paid support for the implementation and operation of the FRED system for other TLD administrators. As part of this support, greater attention was paid to administrators from Tanzania and Costa Rica in 2025. In a number of registers, the possibility of implementing the **FRED Global Block** system extension module, developed in 2024 in collaboration with the Brand Safety Alliance, remained a hot topic in 2025. It is used to block domains en masse across registers in order to protect trademarks.

Because of its importance and wide use around the world, the development of the FRED system in 2025 also focused on long-term sustainability and configurability. The Association continued to update the system's oldest components in line with current standards and requirements. Examples include the refactoring of a large portion of the Domain Browser's code, the switch to a new gRPC client for the FERDA web interface, the change of the tool used for signing PDF documents (jsignpdf → pyhanko), and the release of a new EPP client (Eppic 3.1.0).

The FRED system was enhanced with new functionalities in 2025. By far the most significant innovation was the system modifications carried out in connection with the launch of the gov.cz domain administration portal for the Digital and Information Agency. In addition to significant changes to the system's backend, a new interface has been created; it can be used to manage DNS records for domains in the register. A web portal has been created based on the interface; the portal serves as a central tool for public authorities to administer gov.cz domains. In December 2025, the entire solution was brought into operation, which effectively means that CZ.NIC is now responsible for the operation of another domain register, with a different domain lifecycle to boot. Registration of gov.cz domains is subject to approval by the competent staff at the Digital and Information Agency, and the domains are automatically renewed. The project was carried out following a tender procedure in 2024 and serves as confirmation of the Association's role as a reputable partner to the state in its digitalisation efforts.

The development of the Domain Auction system also continued in 2025. We introduced a more intelligent sorting of domains in lists, automatic sending of satisfaction surveys to bidders in specific situations, sending tax documents via email, improvements to tools for customer support operators, and an extension of the deadline for exercising the preferential right to register a domain obtained in an auction from 7 to 14 days.

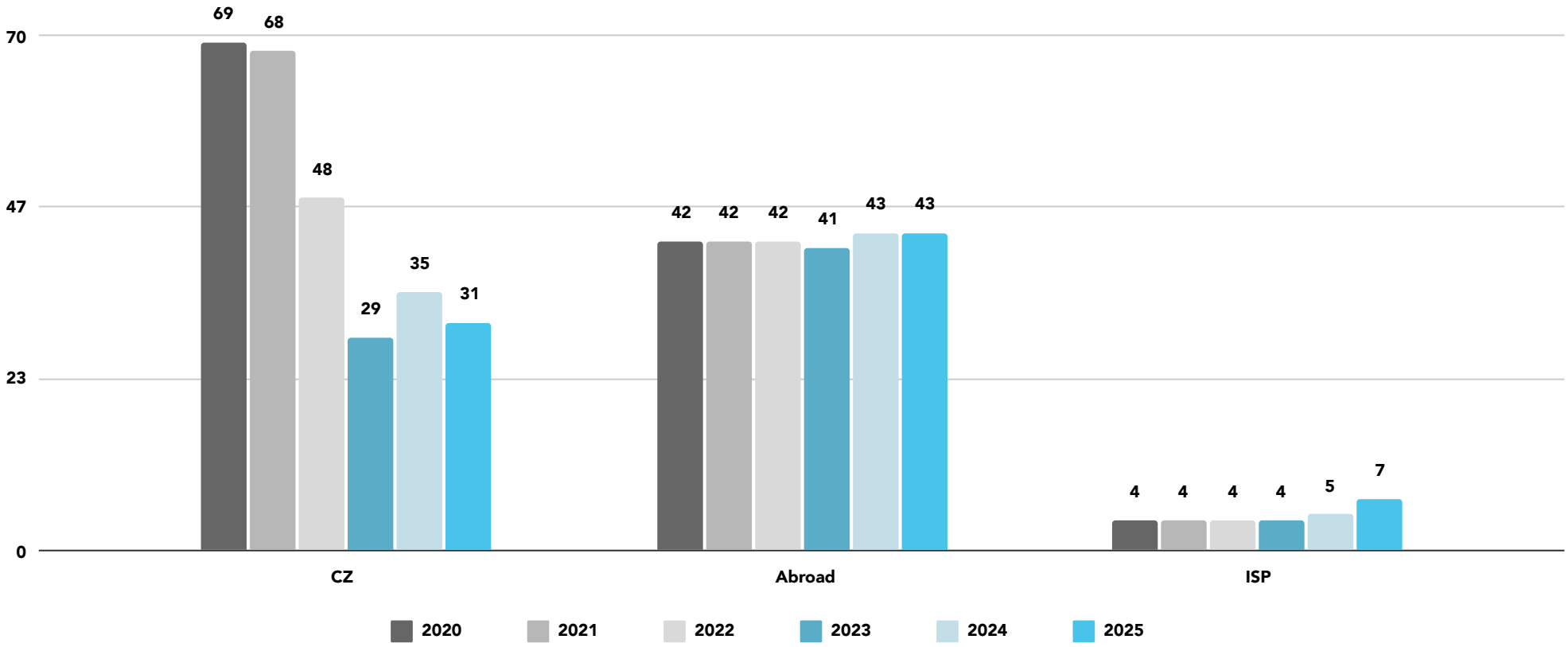
Another fairly significant change introduced in 2025 is the addition of the option to register a contact in the .CZ domain register via the Domain Browser, provided that the user logs in using an EU eID, i.e., via eIDAS. This change was prompted by the need to simplify the process for foreign participants to enter Domain Auctions. The Domain Browser has also been enhanced with the "changes" feature, which clearly informs users about the changes being rolled out in each version.

During 2025, an analysis was also carried out regarding the impact of the transposition of the NIS2 Directive into Czech law, specifically the obligations imposed by the new Cyber Security Act. The main change, the implementation of which began at the end of 2025, was the addition of a telephone number as a mandatory detail to be disclosed by domain holders. The plan was for the roll-out to take place gradually in three stages. At first, it will not be possible to create or edit a contact without a valid telephone number; subsequently, it will not be possible to register a domain for such a contact; and, as a final step, the renewal of a domain held by such a holder will also be prevented. All these steps will be implemented in 2026 and will be accompanied by further activities organised by the Association in collaboration with registrars, which will prevent any negative impact on the operation of .CZ domains.

4.2.2 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 sites in the Czech Republic (mentioned in the "Data centres" section), additional servers are operated in 14 other countries.

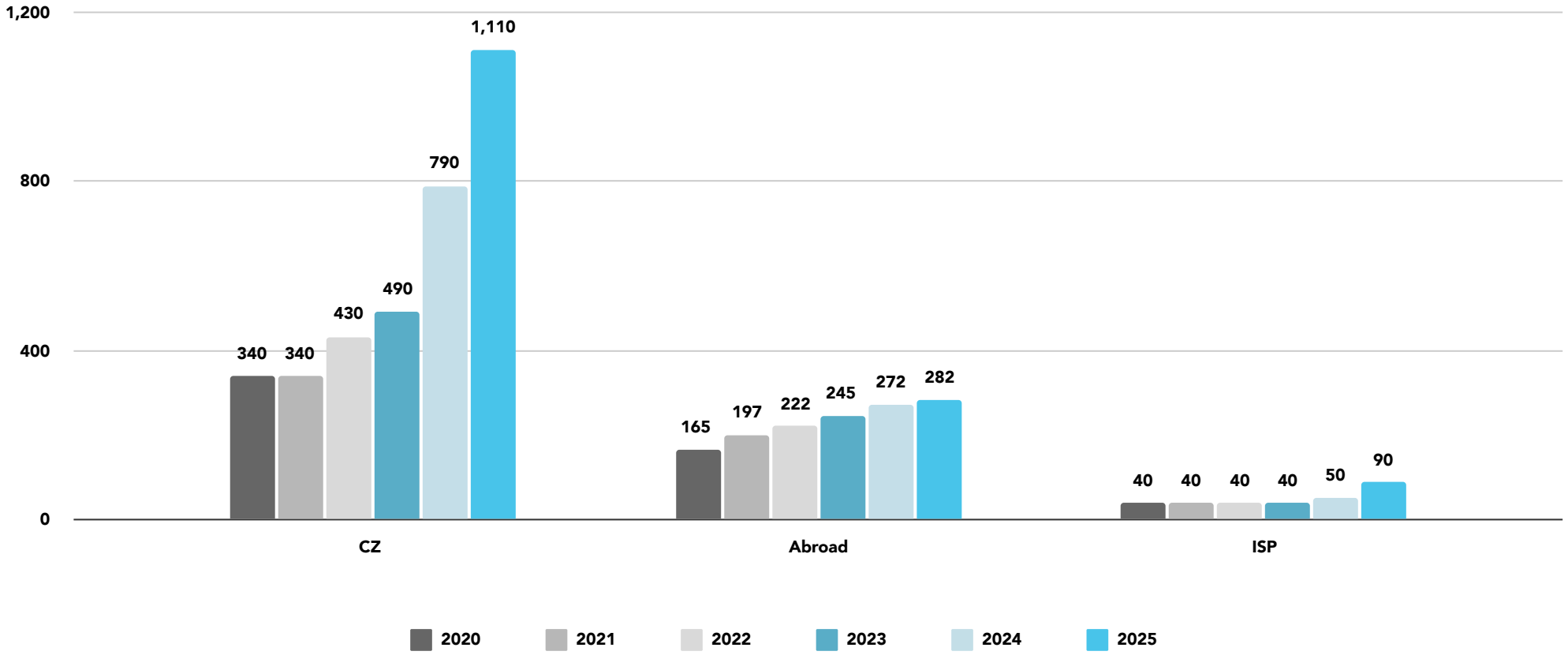
Number of physical .CZ DNS anycast servers





Countries where servers managing records of .CZ domains are located

Data capacity on DNS servers



4.2.3 Strengthening the DNS infrastructure

In 2025, the CZ.NIC Association continued to increase the resilience of the .CZ DNS infrastructure against DoS attacks and to cover the needs of the continuous growth of operations.

A significant step was the upgrade of the backbone network infrastructure and the second link to the Czech NIX.CZ peering centre at the CE Colo site to 400 Gbps. At the DC TOWER site, international connectivity has been upgraded to a full 100 Gbps. The secondary link to the non-public site has also been upgraded to 100 Gbps and, at the same time, relocated in accordance with the requirement to avoid concurrence with the primary circuit. The non-public site therefore has two independent 100 Gbps connections to Prague's data centres.

The DNS site on the west coast of the U.S., in Los Angeles, has recently been connected to the Equinix peering centre.

In total, the capacity of the DNS infrastructure for the .CZ domain grew at the end of 2025 to almost 1.5 Tbps distributed across 26 geographically remote locations in 15 countries on 6 continents. Thanks to the rising use of XDP technology, a significant increase in capacity is being achieved, even with a reduction in the number of physical servers in operation. The available HW power is thus used up to two-thirds more efficiently.

In order to ensure stable operation of the .CZ domain, the Association also performs, in addition to regular hardware renewals and upgrades, periodic maintenance and development of the DNS anycast software equipment. In 2025, a number of SW updates were made to DNS sites and network equipment.

The hidden master and validation servers, where the .CZ zone is generated and defined checks are performed before the zone is distributed from them to all DNS anycast sites, were also updated.

For planning the development of anycast, the Association makes good use of data from the ADAM project, which collects and processes traffic data from all DNS anycast hubs. One of the most important DNS traffic parameters monitored by the ADAM project is RTT (Round-Trip-Time) – the time required for communication between a DNS traffic source and an authoritative DNS server, or its weighted averages related to a specific DNS traffic source, or a geographical or network aggregation of these sources. Thanks to this method, the Association is able to manage the latency of DNS traffic of the .CZ domain in relation to the size of traffic from individual regions of the world effectively.

For major Internet service providers, CZ.NIC operates mirrors of .CZ DNS anycast nodes – 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 event of an attack against the authoritative DNS servers of CZ.NIC.

Their customers will thus not be affected by any attack in any way, and the Internet services in the .CZ domain will remain fully available to them. Another advantage is the acceleration of responses in the provider's network with the ISP DNS stack. The companies that use this service of the CZ.NIC Association are Seznam.cz, Vodafone Czech Republic, CESNET and T-Mobile.

4.2.4 Utilisation of the .CZ DNS infrastructure

On a commercial and non-commercial basis, the Association offers the hosting of secondary DNS servers for operators of foreign TLD registers. From a technical point of view, this involves the sharing of the capacity of DNS servers, which are primarily intended for the .CZ domain, with other entities. This capacity is systematically dimensioned for a load many times higher than the normal operational requirements of the .CZ domain in order to withstand possible attacks, and therefore it is useful and beneficial to also use it partly for other projects.

For this purpose, the Association operates the separate IP anycast "E" and "F" ranges, which are reserved specifically for hosting purposes. Both anycast ranges are designed to ensure low latency anywhere in the world and to offer a high handling capacity while still leaving some sites and capacity reserved only for .CZ TLDs. The hosting service set up in this way offers the possibility of easily using the infrastructure capacity for other entities and, at the same time, maintains significant independence of the operation of the .CZ domain itself.

In 2025, the national TLD .NA (Namibia) domain and several of its SLD subdomains were added to the domains hosted on the Association's DNS anycast.

In addition to hosting for national TLD domains, the Association offers the "VIP Domain" service, which allows hosting of very important Czech SLD domains (second-level domains) on the same DNS anycast, thus helping ensure the security and resilience of the key infrastructure of important services on the Czech Internet. In 2025, the public service broadcaster's main domain, ceskatelevize.cz, was added to the list of VIP domains.

Since 2024, when the Association succeeded in a public tender for the operation of the register of the unified gov.cz government domain, this contract has also included DNS hosting on the anycast for that domain and all its subdomains. The gov.cz domain was technically transferred to the Association's anycast at the end of 2024. In 2025, the gov.cz domain register was launched; this includes the management of DNS records across all subdomains, while DNSSEC management was transferred under the FRED AKM automated register system.

4.3 Support for Internet infrastructure

4.3.1 IPv6 support

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

The long-term goals of the Association include supporting the deployment of the IPv6 technology at all levels, i.e., content, networks and end devices. CZ.NIC also cooperates with registrars, who often provide web hosting, so it can seek support for IPv6 on the side of web, email and DNS servers. In 2024, a new certification programme came into force, under which the accessibility of the main domain, order form and administration

panel for registrar customers over IPv6 was added as a mandatory condition for entry into the certification programme for registrars. The weight of IPv6 support on registrar services in the evaluation criteria was further increased. Based on these rules, IPv6 support on certified registrar services has been added or corrected.

Evaluations under the new certification programme with these criteria will be carried out in the coming years. The Association also participates in promoting IPv6 within state administration. In 2024, these efforts resulted in a government resolution "to restart the deployment of DNSSEC and IPv6 technology in the state administration", which, among other things, sets a deadline for terminating the provision of state administration services on the old IPv4 protocol on 6 June 2032. The Association has also launched a separate website for this purpose, https://konecipv4.cz/.

All services operated by the Association are available in dual-stack mode, i.e., on both IPv4 and IPv6.

In 2025, the share of IPv6 traffic on authoritative DNS servers remains at around one-third.

4.3.2 DNSSEC support

DNSSEC is a DNS extension that increases its security through asymmetric cryptography.

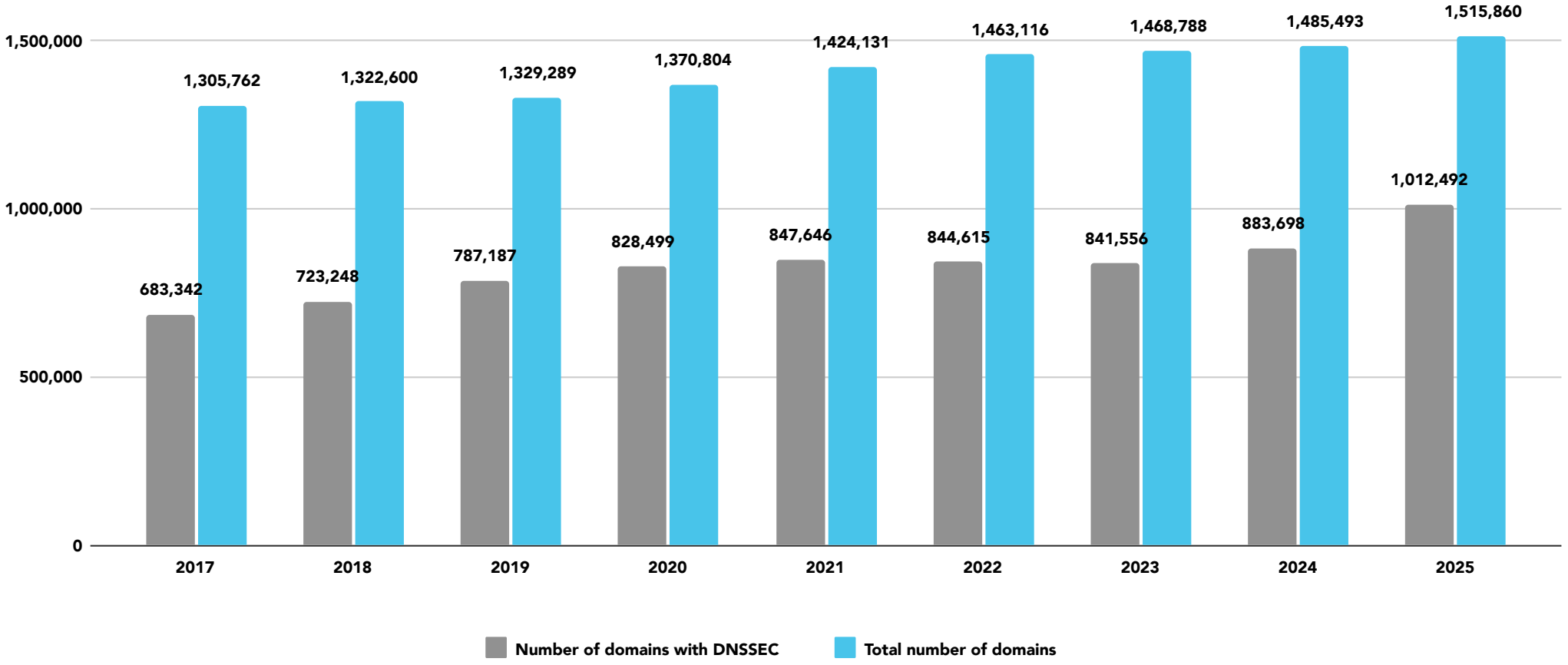
The DNSSEC technology gives users the certainty that the information they obtained from DNS was provided from a correct source that it is complete and that its integrity was not compromised during the transfer. The DNSSEC technology has been available within the Czech national domain .CZ since 2008. The .CZ domain was thus one of the first top-level domains in which this technology could be used.

The absolute number of domains secured by DNSSEC grew until 2020 before subsequently stagnating in the following years. Therefore, the CZ.NIC Association decided in 2023 to significantly increase the weight of the criterion that evaluates the share of secured domains using DNSSEC at individual registrars in the certification programme. In the years that followed, this change was accompanied with more active communication with registrars with the potential to secure larger numbers of domains, and communication of the new version of automated DNSSEC management. All of this led to a reversal of the trend, and by the end of 2025 the share of domains secured using DNSSEC had risen to more than two-thirds (66.8%), with their total number exceeding 1 million for the first time in history. Thanks to its high level of DNSSEC support, the .CZ domain ranks among the very best ccTLDs in the world.

Ondřej Filip, Managing Director of the Association, continues as Cryptographic Officer Trusted Community Representative (TCR) in 2025. He is one of fourteen trusted representatives of this organisation who have access to and actively participate in the hardware security module, the initiation of which is necessary for the root zone signing process. The TCR group was established within the ICANN international organisation in an effort to increase confidence in the process of implementing DNS security using DNSSEC technology at the root zone level.

In addition to registrars, the main Internet service providers in the Czech Republic are also gradually introducing DNSSEC technology. This makes the system fully functional for most regular Internet users.

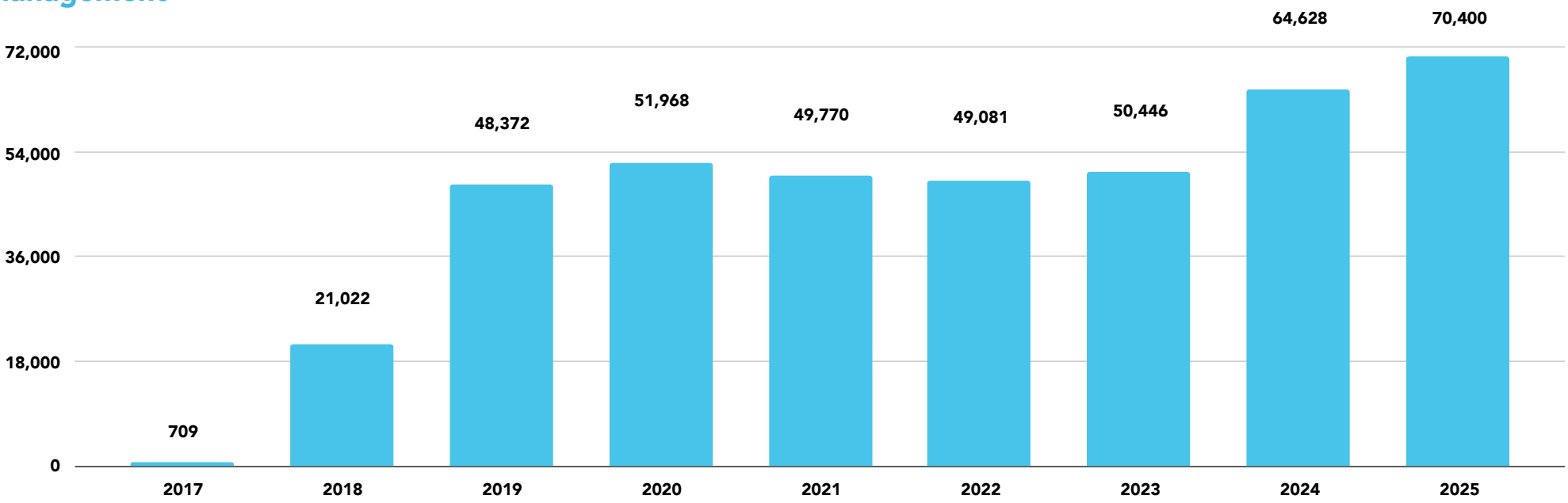
Development of the number of .CZ domains with/without DNSSEC



The high number of DNSSEC for the .CZ domain is aided, among other things, by the support of automated DNSSEC key management, which CZ.NIC introduced in 2017 as the first in the world. This was possible thanks to the introduction of new RFC 7344 and RFC 8078 standards into the FRED domain administration system. These extensions are thus available to all TLD administrators that 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.

Thanks to this mechanism, DNSSEC can also be easily deployed for those domains where it was not previously possible, e.g. for domains whose registrar does not support DNSSEC, or for domains that are administered by someone other than the registrar. The number of domains under automated DNSSEC key management rose again in 2025, as can be seen in the chart below.

Development of the number of .CZ domains under the system of automated DNSSEC key management



4.4 Support for the basic Internet infrastructure

Operation of root servers

In 2025, the CZ.NIC Association continued to operate mirrors on the K and L root servers. Therefore, CZ.NIC operates mirrors of two out of the 13 root name servers that are the basis of the domain names system (DNS). This increases not only the security and stability of the root servers on a global scale, but especially their availability in the European region.

Support for emerging registers

In addition to these root servers, the Association's infrastructure is also used to support emerging registers through the operation of secondary name servers for their ccTLD. Malawi, North Macedonia, Tanzania and Guatemala use this option to administer their national domains. Angola has expanded its portfolio of domains hosted on the Association's anycast and moved into commercial cooperation mode. A new partnership was established with the Namibian register in 2025. During the year under review, the Association also operated the infrastructure for the operation of the DNS register of domains of Brazil and the association of Latin American ccTLD LacTLD in its data centres.

Support for the Ukraine register

The military conflict in Ukraine, which has a significant impact on the online world and the operation of the .UA register, continued in 2025. Ukraine faced not only cyber attacks, but also intense missile attacks on its energy infrastructure and problems with staffing the register.

Thus, the Association's support for the Ukrainian register continued. As part of the support, the operation of the previously built DNS stack was replaced by full hosting of the .UA domain on the Association's DNS anycast and the infrastructure for the register itself, which is operated from the Association's data centres in the Czech Republic, was optimised with a focus on increasing redundancy.

Since 2024, the cooperation has also included an element of reciprocity, with the administrator of the Ukrainian register providing hosting and connectivity in Kiev for the Association's DNS server, which was integrated into the global DNS anycast, thus providing services for users of the .CZ domain. The site also handles most of the Ukrainian traffic on the .UA domain, which now uses the DNS anycast services of the Association.

The support of the Association was a pillar for keeping the Ukrainian domain in continuous operation in 2025.

Hosting DNS zones and servers

On the basis of mutual sharing of knowledge and long-term cooperation, the Association also operates a secondary authoritative DNS server for the Czech neutral peering node NIX.CZ.

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

Open DNSSEC Validating Resolvers (ODVR)

Since 2010, the Association has also operated Open DNSSEC Validating Resolvers (ODVR), which are freely available for use as an alternative to DNS resolvers operated by connection providers.

The ODVR service (also because it is operated on the Knot Resolver being developed by the Association) supports encrypted DNS communication using DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT). Since 2020, the option of using this encrypted DNS communication has even been incorporated in the user interface of the Google Chrome browser (from version 87 on Windows and Android OS).

Software upgrades and updates were carried out on the ODVR in 2025.

RIPE Atlas Anchor hosting

The CZ.NIC Association is actively involved in the RIPE Atlas global monitoring network project and supports this project by hosting fixed monitoring points called RIPE Atlas Anchor. In the past, the Association also participated in this project by supplying HW probes of its own production (Turris MOX platform modified for the needs of RIPE Atlas Anchor).

Hosting a public NTP server

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

Operation of the register and DNS services for the unified Government domain gov.cz

In 2024, the Association succeeded in a public tender for the operation of the register and DNS services for the unified Government domain gov.cz and all its subdomains. The cooperation began with the construction of non-public DNS sites for the needs of the State and then the migration of the domain itself to the Association's DNS anycast, which contributes significantly to the stable operation of all public online services of the state. As part of the ongoing cooperation, in 2025 the DNSSEC security for the domain was transferred under the fully automated AKM system within the FRED register, which also handles the regular rotation of signature keys. The main change was the deployment of a newly developed portal to support the domain lifecycle and enable self-service management of DNS record configurations by individual public authorities. A separate infrastructure has been set up for the gov.cz domain register, which is built on top of the FRED system; its architecture is similar to that of the .CZ domain register.

5 CSIRT security team

The growing importance of the Internet and the rising number of its users are accompanied by a rising number of security incidents, such as the misuse of computers, a network element or a network for illegal activities (e.g. spam), copyright infringement, phishing or data interception. The severity of these incidents is also increasing. Dependence on cyberspace and the level of criticality of failure associated with it is also greater, where not only the ordinary user or various private law institutions, but also the infrastructure of the state itself is at risk.

It is therefore necessary to create, formalise and streamline defence against attacks on these entities, and CSIRTs (Computer Security Incident Response Teams) are being created for this very purpose. The CZ.NIC Association has long-term experience with projects in the field of Internet infrastructure, and therefore it is involved in supporting the activities of security teams at the national and academic levels. The Association also runs 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.

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

The CSIRT.CZ security team is the official national security team of the Czech Republic, which is operated in accordance with Act No. 181/2014 Coll. on cybersecurity and the public law contract concluded with the National Security Authority (NSA) on 18 December 2015. As at 1 August 2017, the then newly established National Cyber and Information Security Agency (NÚKIB) took over the position of the NSA and thus became the manager of cybersecurity issues and the national authority in this field.

The main objective of the CSIRT.CZ team is to **resolve incidents** related to **cybersecurity in networks operated in the Czech Republic**.

In addition, it also focuses on **prevention, research and education**. CSIRT.CZ collects and evaluates data on notified incidents and forwards the data to the persons responsible for the operation of the network or service that is the source of the occurrence of the incident in question, and/or provides coordination assistance. In its activities, the team cooperates with a number of entities with which it exchanges information on incidents and their solutions on the basis of mutual trust.

CSIRT.CZ collaboration

In order to effectively carry out its tasks as defined by legislation, the CSIRT.CZ team cooperates with a number of entities at both the national and international level:

- national level – cooperation mainly with NÚKIB (especially the Government CERT team), the Police of the Czech Republic (PCR), CSIRT/CERT teams with different specialisms, Internet service providers (ISP), banks and others,
- international level – the team is part of the CSIRTs Network structure (a network composed of national and governmental CSIRTs/CERTs of the EU Member States) and cooperates actively with the European Network and Information Security Agency (ENISA) and the Europol organisation.

Other international structures of which it is an active member include:

- FIRST, an organisation that connects security teams from around the world and is thus a platform through which the teams involved can effectively respond to security incidents and threats and cooperate to resolve them.
- Trusted Introducer – TI, an organisation established by the European CERT community in 2000 to address common needs and to build a service infrastructure that provides important support to security teams; the organisation certifies security teams according to their proven and tested level.

Projects and activities in 2025

In 2025, the CSIRT.CZ security team continued to participate in the **Safer Internet Centre CR (SIC CZ) project**, which is implemented by the CZ.NIC Association under the name **Bezpečně na netu** (Safe on the Net).

The team was involved in the operation of the STOPonline.cz hotline, which is intended for reporting illegal online content and for awareness-raising and education of both children and parents. The team members also participated in the training activities of the SIC CZ project when needed.

In 2025, the CSIRT.CZ security team focused intensively on preparations to meet the requirements of the new legislation, the new obligations arising from Act No. 264/2025 Coll., and the further development of the Deny Lists service.

5.1.1 Traffic statistics

In 2025, the CSIRT.CZ security team handled a total of 3,305 incidents, the highest number recorded by the team to date since 2008. This meant that the trend seen in the previous year, when there was a 17% year-on-year decrease in the number of reported incidents, did not continue.

The final figures are likely to reflect the intensive debate surrounding the new Cyber Security Act, as a result of which even organisations not yet subject to this obligation have begun to report incidents, in anticipation of its future implementation. The total number of incidents was also influenced by the proactive approach of Deny Lists customers, who shared their findings.

Number of incidents addressed

	2022	2023	2024	2025
Sensor Network*	8,815	8,903	9,682	**6,853**
Phishing	1,485	2,064	1,689	**2,003**
Spam	220	352	260	**483**
Malware	228	163	108	**179**
Information gathering	71	105	99	**126**
Intrusions	39	21	69	**125**
Other	24	35	53	**84**
DOS		12	4	**5**
Total	2,067	2,752	2,282	**3,005**

** Sensor Network is not included in the total number*

In 2025, CSIRT.CZ continued streamlining its incident response procedures. The main motivation was to prepare for the expected increase in the number of reported incidents in connection with the significant

expansion of the range of entities falling within its remit. This included, for example, developing an API for communication with the NÚKIB portal and further automating work with internal tools.

At the same time, an improvement was achieved in the integration between the ticketing tool and the Deny Lists service. The aim was to ensure that only relevant domains verified by the operator were included in the Deny Lists, while minimising the increase in repetitive work. A solution has been proposed which requires no additional action on the part of the operator; it simply expands the range of the options available.

Open-source tools were further developed and maintained throughout the year. The mininterface library, which provides a general-purpose user interface, has surpassed 30,000 downloads and has been deployed in a number of backend scripts as well as in open-source tools where its use is appropriate (e.g. convey and deduplidog). As a result, their code has been simplified, with the part responsible for the user interface being developed centrally. Any improvements made to it are therefore automatically reflected in all programmes that use the library.

Over the past year, the library has gained a stable API and has been enhanced with a number of features, including a web interface that allows full control of programmes via a web browser.

5.1.2 Awareness and educational activities

In 2025, CSIRT.CZ continued running its established training courses on "Security and Privacy on the Internet" and "Forensic Memory Analysis". Two new courses were launched. The first of these, which focuses on the basics of web application penetration testing, provides an overview of the subject with an emphasis on practical skills. The second course is aimed at organisations that are planning to set up an official CSIRT team and are seeking membership in international associations of these teams.

Tailor-made training courses also continued to be delivered, e.g. for staff at the Mikulov Municipal Authority, the Slezská brána (Silesian Gate Region) Association and the National Radiation Protection Institute.

A new training concept has been developed in the form of a "table-top exercise", in which organisations test their procedural readiness to deal with large-scale cyber incidents.

Representatives of CSIRT.CZ have also appeared repeatedly in the media, both public and private. Team members have published papers on the blog covering current topics, which help to raise awareness and provide information, shed light on the context of CSIRT.CZ's activities, and explain its role within the CZ.NIC Association, in the Czech Republic as well as in the context of international cooperation.

CSIRT.CZ has also regularly shared its experiences at specialised forums and conferences, such as TF-CSIRT, C2S2, ICANN, LinuxDays 2025 and Alternativo Security Days.

Other awareness-raising activities that the team has been involved in for a long time include publishing news from the world of security. Active cooperation with the Root.cz server continues through the Postřehy z bezpečnosti (Security Insights) series. This is a regular security review of the past few days. The published information highlights the most interesting events and news.

5.1.3 National and international cooperation

Cooperation at both the national and international level was strengthened in 2025. Close cooperation continued with the Police of the Czech Republic, NÚKIB and other security teams, both within the remit of CSIRT.CZ and beyond.

Alongside standard activities, intensive discussions took place regarding the implementation of the new Cyber Security Act and preparations for the Cyber Europe 2026 exercise.

An important aspect of international cooperation is participation in the CSIRTs Network, which brings together national and government teams from EU Member States. Within that platform, there is regular information sharing, coordination of procedures and cooperation in resolving incidents, particularly in collaboration with the GovCERT.CZ team.

In 2025, Věra Mikušová, a representative of CSIRT.CZ, was elected to chair the Steering Committee of the TF-CSIRT organisation. This appointment recognises both the expertise and the long-standing contribution of CSIRT.CZ within the international community. As part of this role, two international conferences were co-organised, attended by more than 150 teams from across Europe.

The Czech Republic has a total of 73 members within the CSIRT community, of whom 6 are certified, 20 are accredited and 39 are listed. Two further teams are awaiting certification, one team is awaiting accreditation, three teams are awaiting renewal of their basic-level membership, and two brand-new teams would like to join the community. Compared to 2024, the number of member teams again increased.

The Czech Republic has registered a new applicant for membership within the international FIRST organisation. CSIRT.CZ also shared its experience with international partners, such as representatives from Argentina, Azerbaijan and the Western Balkans.

At the same time, CSIRT.CZ continued providing expert support and advice to other organisations in the field of cybersecurity.

5.1.4 Preventive measures and Deny Lists

One of CSIRT.CZ's key roles lies in the area of prevention and public awareness.
Key long-term services provided in this area include the Deny Lists service.

The **Deny Lists commercial product** was launched in 2024. This service was originally intended for free deployment on the Association's ODVR servers; however, it was subsequently transformed into a commercial service, under which the outputs are provided to Internet service providers and other entities in return for payment.

The service essentially involves compiling lists of malicious domains that pose a risk to end users, particularly in connection with phishing, fraudulent online shops or fake investment offers. Through its work, CSIRT.CZ often obtains information about such domains at an early stage of their existence.

In the case of .CZ domains, we can ensure a very rapid response, while for foreign domains the process depends on cooperation with our international partners. The Deny Lists service thus enables Internet service

providers to protect users in the Czech Republic right from the early stages of malicious campaigns.

In addition to the data obtained as part of incident response, the outputs of the PROKI project, which analyses data from other projects run by the Association, such as Turris and honeypots, also constitute a significant source of information.

In 2025, the focus was on the further development of the service. The scope of the domains monitored has been expanded, partly with a view to reaching potential customers in Slovakia. Support for bulk blocking has been added, and the customer portal has been updated to allow users to manage their own lists of domains, including the ability to define exceptions.

The measures implemented led to **a year-on-year increase of almost 484% in the number of malicious domains identified**.

At the same time, the system for detecting malicious domains was further developed. A tool for analysing Certificate Transparency data has been deployed into routine operation, enabling the identification and blocking of malicious domains before they are actively exploited.

The Deny Lists system has also been adapted for use within the DNS Patrol project. In addition to technical cooperation, CSIRT.CZ provided ongoing expert advice on the project.

Penetration and stress testing

Penetration testing was also successfully conducted in 2025. The tests were carried out for both commercial entities and public administration. Two important projects of the Association, DNS Portal and DNS Patrol, also underwent penetration testing.

PROKI (Prediction and Protection from Cyber Incidents)

In 2025, the PROKI system recorded 9,285,478 entries relating to 360,394 unique Czech IP addresses. This was also reflected in the number of reports. A total of 43,047 reports were sent to 832 unique abuse contacts. In addition to its original purpose, PROKI also provides a platform for processing information from various sources, enabling its ultimate use in the Deny Lists project.

In 2025, cooperation also continued with NÚKIB, to which the Association provides information on any issues arising among KII entities.

PROKI statistics	Number
Number of emails sent from PROKI	43,047
Number of unique recipients (abuse contacts) of PROKI reports	832
Number of unique Czech IP addresses that we recorded	360,394

Web scanner

In 2025, a nominal charge was introduced for the service, with the main aim being to make it available to commercial entities that had expressed an interest in it. These are typically small companies that do not make use of services such as comprehensive penetration testing.

Automated testing for schools

As part of internal cooperation on the bezpecnyinternet.cz (Safe Internet) project, a service for automatic testing of web presentations for institutions working with children was launched in 2023. The primary focus is on schools, but other similar entities have also expressed interest in regular testing. We are currently working with 30 entities, who are tested every three (3) months.

5.2 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.

On the basis of the Rules of Registration, 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 a domain name when the server available through the domain name is the control centre of networked hardware distributing harmful content (botnet).

Fighting phishing in .CZ domains in 2025

In 2025, CSIRT.CZ recorded a total of 23 phishing-related incidents, the majority of which were not linked to a .CZ domain.

The long-term downward trend in phishing activity within the .CZ domain, first noted more clearly as early as 2023, continued into 2024 and 2025.

In 2025, 23 phishing domains were taken down, representing a year-on-year decrease of three domains compared with 2024 and a significant decrease of 102 domains compared with 2023.

This development is likely the result of the systematic integration of insights gained from the work of CSIRT.CZ, the ADAM project and the application of the provisions of Article 17.1 of the Rules of Registration of Domain Names in the .CZ zone. Thanks to this combination of tools and procedures, we are able to identify and eliminate phishing domains at an early stage of their existence.

Since 2022, the monitoring of fraudulent domains and the process for removing them have been significantly improved. In many cases, it is now possible to block a malicious domain even before the first report is received from users, sometimes as quickly as 15 minutes after the domain goes live.

Internal security

Within the CZ.NIC Association, the CZ.NIC-CSIRT team also ensures the implementation and fulfilment of the internationally recognised certification of the information security management systems (ISMS) in compliance with the ISO 27001 standard. In 2025, an external recertification audit was carried out; it also included an audit of the new Prague office. Regular technical security tests were also carried out on websites and other systems; CZ.NIC-CSIRT focused on responding to alerts from NÚKIB, preparing and organising KSK ceremonies, improving the security of the CCTV system, and ensuring that the relevant guidelines complied with the new version of the ISO standard. In 2025, the Deny Lists service was also deployed on the internal DNS servers.

6 MojeID

MojeID is a service for electronic authentication that allows Internet users in the Czech Republic to log in to various online services using uniform identification data. It offers users easier access without the need to manage multiple sets of login details, while for service providers it enhances user convenience and enables them to work with verified identity details.

This service has already been operated by the CZ.NIC Association for sixteen years. Since 2020, the MojeID service has also been one of the possible means of communication with state administration authorities thanks to its connection with the National Identification and Authentication Point (NIA). Moreover, in 2021 MojeID was accredited by the Ministry of the Interior at the "high" level of assurance. Therefore, there is currently not any more secure means of electronic identification in the Czech Republic.

Following the redesign of MojeID, which was completed in 2023, the benefits of the service, particularly in the area of onboarding new users, became fully apparent in the following year. A simplified registration process and clearer user guidance have led to a higher success rate in creating accounts and a significant increase in the use of two-factor authentication.

Security remains an important aspect of this service. The convenient, modern and accessible MojeID Klíč mobile app thus remains the most used account security option. At the end of 2025, we introduced a new QR code-based login system, which allows the user to log in quickly and conveniently via the app.

MojeID presentations at professional conferences

Throughout 2025, we presented the MojeID service at several specialised conferences and field-specific events focusing on digital services, security and e-commerce. Among the most significant were, for example, the Czech Online Expo conference in Prague, CyberCon in Brno and Reshoper in Prague.

At these events, we focused, in particular, on presenting the use of MojeID as an authentication service for online services and e-commerce projects. The presentation also included demonstrations of the service's practical applications and new information materials aimed at our partners as well as end users. The aim of taking part was to forge new partnerships and raise awareness of the options for secure login via MojeID.

The growing popularity of the service is also evidenced by the fact that MojeID was repeatedly nominated for the Crystal Magnifier 2025 – Czech Internet Award in the Public Service category.

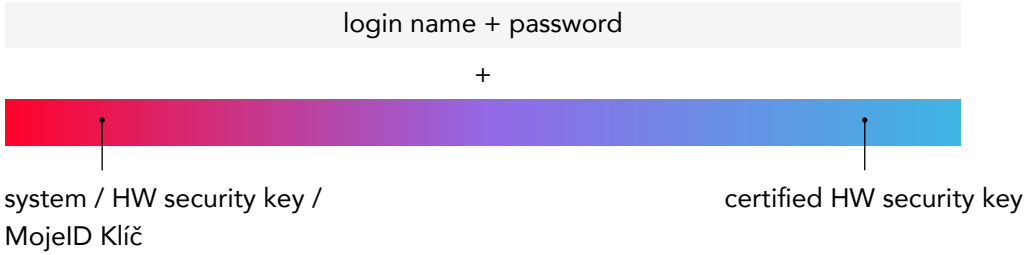
6.1 Security of the MojeID service

The basic features of MojeID include the security and trustworthiness of the entire system and the protection of personal data. The register of user details is protected on the same high level as the .CZ domains register. At each login, the users themselves can define which details from their profile are to be handed over to the provider for whose services the user wants to sign up using MojeID. This gives the user maximum control over their data.

MojeID offers a wide range of login options. A login name and password are the basics. Furthermore, the service provider may determine whether this level of security is sufficient for them or whether the user must provide additional authentication by one of these means:

- the MojeID Klíč* mobile application,
- a system security key (often included with common operating systems, such as Windows 10+ and Android version 7+),
- a hardware security key (a suitable USB/NFC key is a prerequisite for the "high" assurance level).

Options of the level of security of login methods



* The one-time password login options and the legacy MojeID Authenticator app were discontinued during 2022.

6.2 Private sector and public administration partnership services

A key factor in the systematic expansion of the MojeID service is its support from Internet service providers. The growing range of places where MojeID can be used has an impact on attracting new users, for whom it is important to be able to log in to as many services as possible with one name and password, those they use every day and services they may be visiting for the very first time.

In the areas listed below, the Association aims to maintain and consolidate its position, while also expanding into new segments.

6.2.1 Private sector service providers

The partner network of private service providers had a composition in 2025 similar to the previous year. The list of partners can be found in the catalogue on the MojeID website.

In the private sector, MojeID is used by:

- e-shops that are interested in the possibility of verifying the age of the majority of their customers when selling specific goods or services,
- community servers,
- discussion forums,

- news sites,
- servers providing microservices,
- advertising servers and others.

6.2.2 Public administration service providers

In the autumn of 2020, the option of **linking** the MojeID account to the **National Identification and Authentication Point** (NIA) was launched.

Individuals can thus use MojeID to **log in to state administration and local government services**, such as:

- the Citizen's Portal (checking the validity of documents, the number of points in a driver's account, extracts from public registers, etc.),
- the Financial Administration Portal Moje daně (My Taxes) (online filing of personal income tax returns, real estate tax returns and other tax returns),
- ePortal of the Czech Social Security Administration (for example, to view the pension insurance information sheet),
- the client applications of health insurance companies (reports on care provided, insurance premium payers and arrears, applications for contributions from prevention funds, etc.),
- the patient application for eRecept electronic prescriptions,
- the web portals of some regions, cities and municipalities,
- library systems,
- the systems of educational institutions and other entities.

6.2.3 Cooperation and implementation partners

Following the earlier successful integration of Seznam.cz accounts with the MojeID service, further integration of this identity into the portal's services continued in 2025. Users whose identity has been verified via MojeID are marked as "Verified users" on Sbazar.cz, which helps boost the credibility of their profile. During 2025, this labelling was extended to other services on the portal.

In 2025, cooperation was established with the **Smart Forms** system, which uses MojeID as a means of identification. This solution provides a comprehensive tool for municipalities in the preparation and submission of electronic applications. In the locations where the system has been rolled out, public awareness-raising campaigns were also carried out, including support in setting up MojeID accounts.

Further development of MojeID is focusing on library services. Integration into library systems is currently underway in collaboration with Cosmotron. The gradual roll-out of the solution is planned for 2026.

At the same time, integration is underway with the international identity ecosystems **Trinsic** and **Hopae**, which enable digital identities to be linked across services and national borders. These platforms support the use of digital identity in an international context and contribute to the development of interoperable identification solutions.

6.3 MojeID users

The user base is the most valuable asset of the MojeID service. During 2025, the total number of users rose to **1,235,000**, an increase of **116,923** new users in the relevant year.

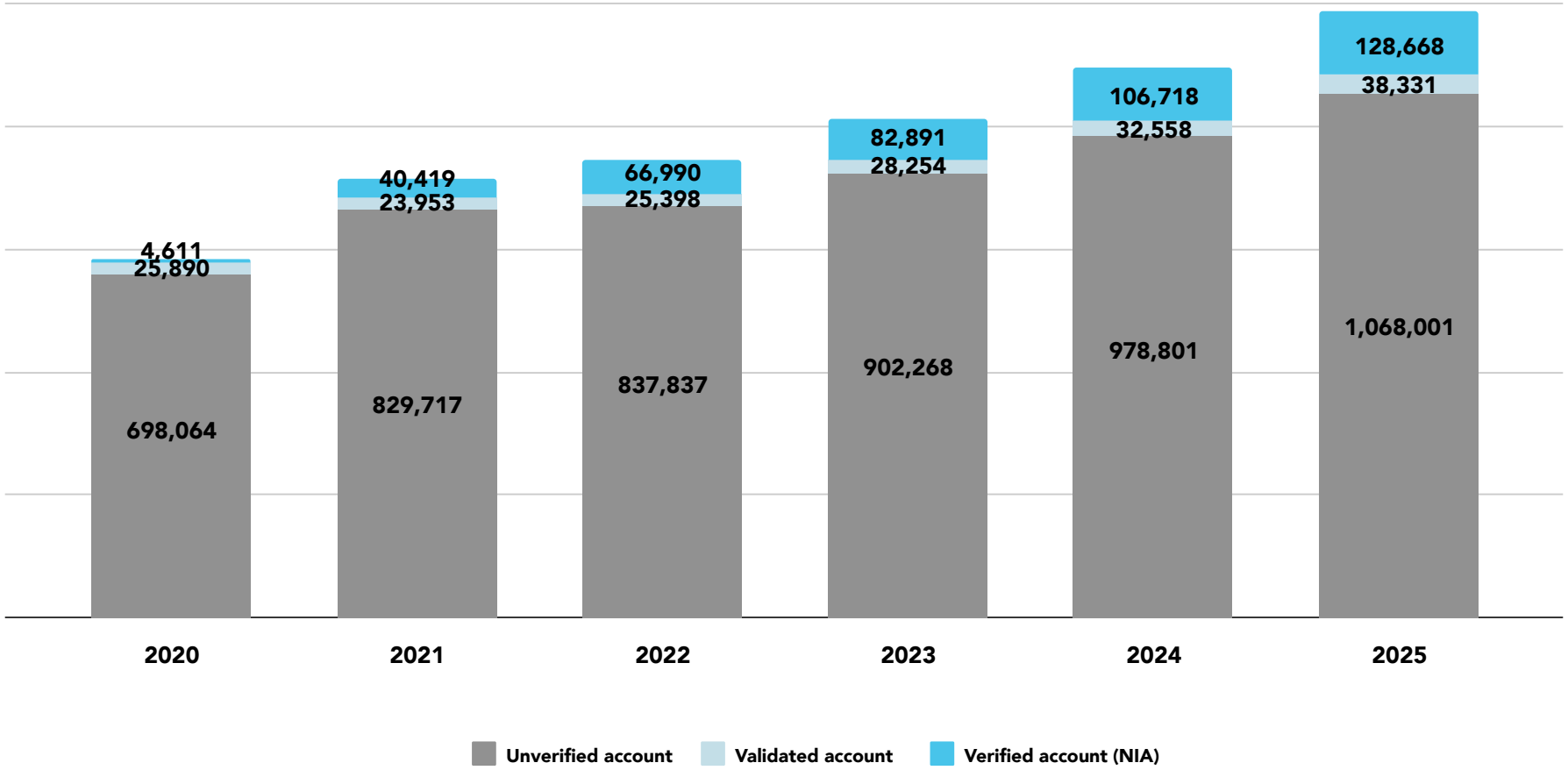
In 2025, efforts continued to increase the number of users connected to the National Identification and Authentication Point (NIA).

As at 1 January 2026, a total of **128,668** accounts were connected, representing an increase of **21,950** accounts compared to the end of 2024.

The number of validated accounts reached **38,331** by the end of 2025.

The chart below shows the level of user identity authentication.

Structure of MojeID accounts by authentication level



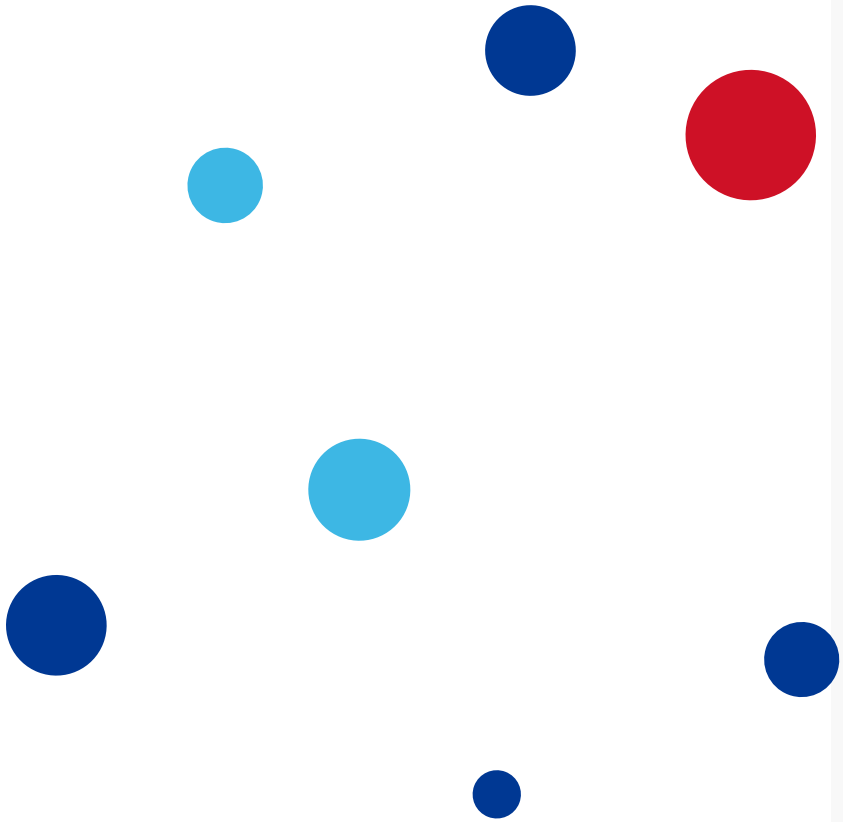
6.4 MojeID as a tool for cross-border authentication in Europe

Also in the previous year, the CZ.NIC Association actively participated in the Czech Republic's involvement in building an infrastructure for cross-border electronic identification pursuant to the eIDAS Regulation. The Regulation follows on from the STORK pilot project, in which the Association took part. As an output of this project, the Association operated a gateway for cross-border authentication that used MojeID as the only means of authentication.

The gateway was gradually replaced by the official eIDAS node for the Czech Republic, operated by the Association on the basis of a contract with the Digital and Information Agency. This node also includes a middleware component necessary for logging in with the German electronic identity card. The Association has repeatedly been successful in the tender procedure for the operation of this system.

Since July 2022, when the MojeID notification process was completed in accordance with the requirements of the eIDAS Regulation, MojeID users have been able to access public services not only in the Czech Republic, but also in the other 29 EEA countries. MojeID is the only non-state means that can be used in this way across borders.

The Association is actively monitoring the ongoing revision of the eIDAS Regulation, which is to come up with a revolutionary wallet concept for the European Digital Identity. In order to pilot the entire ecosystem around this wallet, the European Commission announced large-scale pilot projects, which were officially launched in April 2023. One of these projects involves the EWC (EUDI Wallet Consortium; note: EU Digital Identity Wallet Consortium), of which the Association is a member. In 2025, the Association successfully completed this pilot project by demonstrating how to initialise a wallet via the MojeID service, verify the identity of a domain holder using the wallet, log in to the Domain Browser using the wallet, and issue a domain holding certificate to the wallet. This result was also demonstrated live as part of the European Commission's first major event, the EUDI Wallets Launchpad, in December 2025.



7 Turris

Turris network devices have been developed by the CZ.NIC Association since 2013. They are built on an open-source, Linux-based system and offer automatic updates throughout their lifecycle, a distributed adaptive firewall and other advanced security features.

The year 2025 was marked by the launch of the new generation of the Turris Omnia NG router. The main focus of activities was on completing its development, production and launch. At the same time, production and deliveries were underway for an overseas order placed during the previous year; we also managed to secure a sufficient quantity of the devices for retail sale.

7.1 Software development

The main priority was to integrate support for the new router into Turris OS, including hardware support and the development of a new application to display basic information on the screen.

The development also included a new recovery mode, allowing the device to be reset directly via the screen and a button. Commissioning and testing software was developed for the production process. All the modifications were carried out on the new version of the Turris OS 9.0 system.

7.2 Hardware development

In the first half of the year, the Turris Omnia NG prototype was successfully completed and tested, including the selection of a Wi-Fi 7 module and the procurement of all components.

In the second half of the year, production of the devices under a previous overseas order took place, and production of the Turris Omnia NG and Omnia NG Wired models was subsequently launched straight away.

7.3 Turris OS

As well as supporting new hardware, development of the system continued for existing devices. A new port redirection feature was introduced in the reForis web interface.

Work began on redesigning the Pakoň service interface, with completion scheduled for next year. A significant part of the year was devoted to preparing for and testing the migration to OpenWrt 24.10, which was successfully completed and rolled out for all Turris devices, including Turris 1.0, by the end of the year.

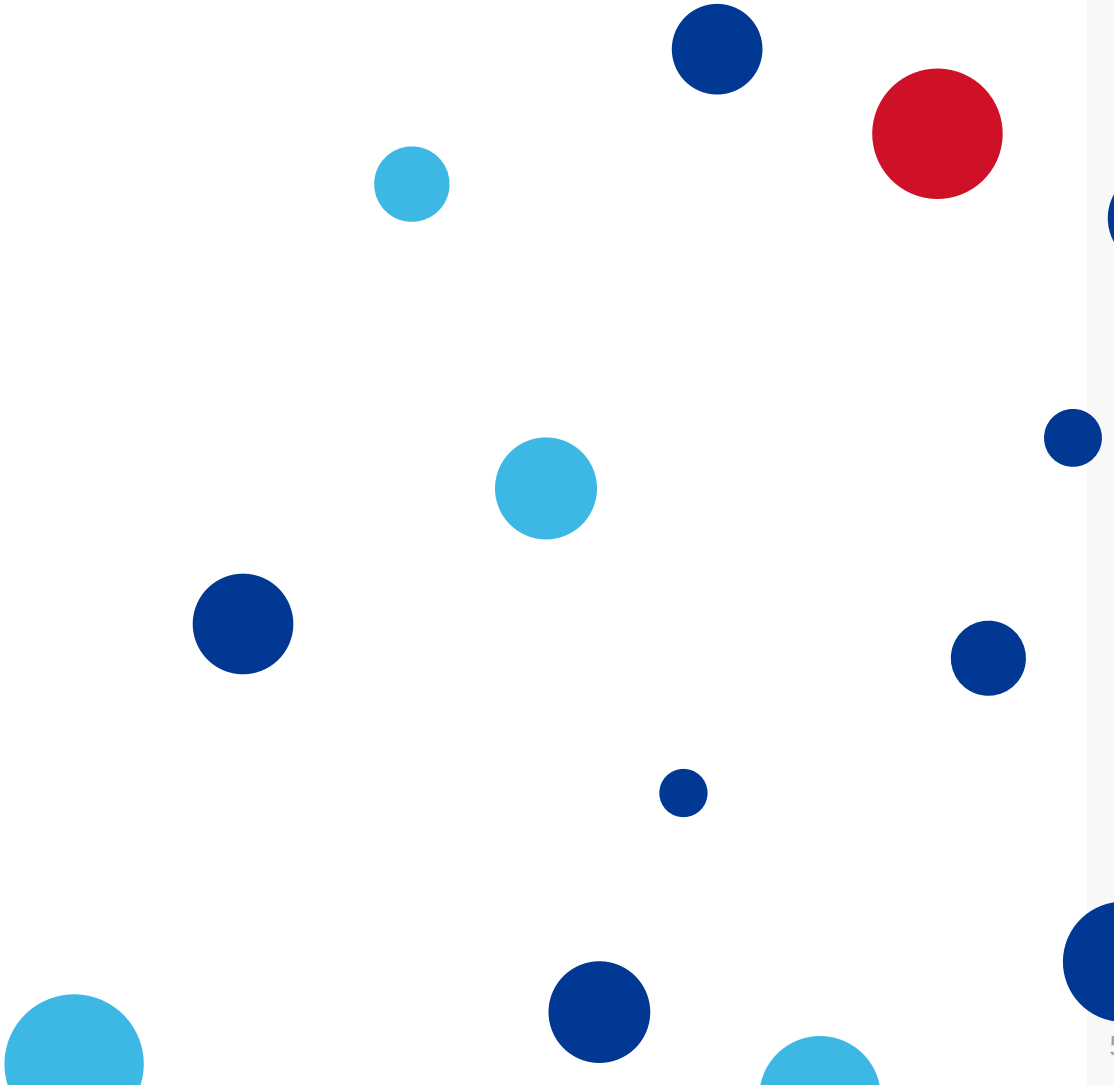
7.4 Business cooperation

The main objective of our business activities was to launch the new generation of Turris Omnia NG routers on the market. These devices are equipped with Wi-Fi 7 technology and 10 Gbps ports. A total of twenty thousand units were delivered to our existing overseas customer.

We established cooperation with a new partner in Switzerland and expanded our retail network in Italy and Slovenia. Turris products are now also available on eBay and are once again available on Amazon, while distribution in the Czech Republic and Slovakia has also been increased.

The Police of the Czech Republic have joined the ranks of our new customers; as part of the National Recovery project, routers have also been supplied to the Universidad Carlos III de Madrid and the IMDEA Networks Institute.

Accessories for the new generation of devices (Rack Mount) have been added to the range. Turris Omnia NG routers have also been successfully showcased at a number of trade events and conferences, where they have attracted considerable interest.



8 CZ.NIC Labs

The CZ.NIC Labs Department is dedicated to research and development of innovative projects for the benefit of both the Czech and global Internet communities. The projects focus mainly on infrastructure protocols and services, network security, traffic monitoring, analyses and DNS statistics. In addition, applications for the general public are being developed. CZ.NIC Labs currently have workplaces in all branches of the Association.

In 2025, CZ.NIC Labs worked on the following main projects:

- ADAM – system for statistical analyses, monitoring and data display,
- BIRD – a multiprotocol routing daemon,
- Datovka – a desktop and mobile application for using data boxes,
- DNS Patrol – a secure DNS system for organisations,
- DNS Knot – an authoritative DNS server,
- Knot Resolver – a recursive DNS server.

8.1 ADAM

The ADAM (Advanced DNS Analytics and Monitoring) project is designed to systematically monitor and conduct in-depth analysis of DNS traffic, which is a critical component of modern Internet infrastructure; its stability and security are essential to the functioning of the vast majority of digital services. The main objective of the ADAM project is to develop and operate tools for the widespread collection, storage and comprehensive processing of data from DNS servers. The team also focuses on refining and expanding analytical methods and on developing user interfaces and reporting procedures.

This activity not only enables the early detection of technical anomalies and cyber attacks to which the infrastructure is constantly exposed, but also provides the data required for planning the expansion of network capacity. The data collection system, built using our proprietary DNS Probe software, is fully operational and utilises the C-DNS format (RFC 8616) to efficiently transfer transaction information from both authoritative and recursive servers to a central repository.

In 2025, the ADAM project moved towards proactive defence using machine learning techniques, particularly through our collaboration on the DNS Patrol project, where it focused its efforts on developing and deploying advanced methods for detecting malicious domains in the Czech cyberspace.

The ADAM project continued to develop both internal and specialised dashboards for customers of the VIP Domain and anycast services, which are used to monitor service availability and quality in real time. The ADAM team's analytical work in 2025 yielded valuable insights into the behaviour of the Czech domain market.

Outputs of the ADAM project intended for the public are available on the CZ.NIC Association's statistics website.

8.2 BIRD

Designed for Linux and BSD, BIRD is a software daemon for dynamic routing of traffic on computer networks. The project originally began at the Faculty of Mathematics and Physics of Charles University, and CZ.NIC Labs are participating in its further development. It is currently the most used software on route servers within peering centres in the world. According to a survey by EURO-IX, more than two-thirds of these centres use it and are also regular customers of the BIRD Support programme. Data centres and CDNs are a rapidly growing user group.

The BIRD project maintains two branches: the single-threaded BIRD 2 and the multi-threaded BIRD 3. New features are generally available in both versions, provided that technical differences between their architectures do not prevent this. The concept of LTS (long-term support) versions has been introduced; these are BIRD 2.17.x and BIRD 3.1.x, which are expected to receive updates for at least three years.

Development in 2025 was characterised by the stabilisation of a number of subsystems, internal refactoring and the resolution of technical debt. In particular, significant progress was made in the implementation of EVPN in BGP and in the stability and performance of the BIRD 3 series.

In addition, the BGP protocol gained support for the link-local next-hop format option and significant improvements to dynamic instances. The filter language has also been improved. In the BIRD 3 series, the OSPF, RIP and Babel protocols have been given their own threads.

In the second half of 2025, experts from the BIRD team taught the course NSWI184 "Computer Network Management" at the Faculty of Mathematics and Physics, Charles University. During the course, we used the EduHawk network simulator, which we developed ourselves, and a number of suggestions for its further development emerged. We have created new training materials which we can now use repeatedly during customer training sessions as part of the BIRD Support programme.

Towards the end of 2025, a prototype of the DebugPack tool was developed; it is designed to deliver crash dumps in their entirety, including the necessary system context. Although we do our best to prevent crashes from occurring in the first place, this tool will significantly reduce the time between the delivery of a crash dump and its analysis in the future.

8.3 Datovka

Datovka is a project that develops applications and a library for communication with the Information System for Data Boxes (ISDS). We provide the desktop application and library to users of Windows, macOS and GNU/Linux operating systems. The mobile app is available for devices running Android and iOS.

In 2025, we made changes to both the light and dark themes of the user interface and the icon set in the desktop version of Datovka, with the aim of making it clearer and improving the contrast of the controls. We added a feature to display news items following an update to a newer version of the app. Other minor improvements include a clearer selection with enhanced features for changing the location of data stored in the data box. On Linux, Datovka can use the desktop environment's functionality (via XDG) to compose an email in the preferred email client. At start-up, while the main window is not yet active, we can alert the user to errors during application initialisation. We have added features to the status bar that alert users if a serious error occurs when accessing saved data, and we have included a tool for recovering data from a corrupted database and rebuilding it.

The mobile app has changed significantly over the last four years of development. There has been a major change to the user interface; with its wide range of features, it is becoming increasingly similar to a desktop application. This is due to the increasing performance of available mobile devices. Increasing the storage capacity allows us to store more data on the mobile device itself. In the mobile app, we have begun the process of gradually transitioning to the same database format as in the desktop application. The structure of the stored data of data messages within the desktop and mobile apps is almost identical. We have recently added features to the desktop and mobile apps that allow data to be transferred between them.

The most significant development in 2025 was the addition of functions for re-timestamping data messages, following the launch of this feature in the ISDS API. Functions for processing archived data messages have been added to both the desktop and mobile versions of the Datovka app, along with features for selecting messages for re-timestamping, monitoring the expiry of time stamps, and processing archived time stamps.

8.4 Knot DNS and Knot Resolver

8.4.1 Knot DNS

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. The project has already gained recognition in the DNS community and among users, whose number is constantly growing.

A new version of Knot DNS, version 3.5, was released in 2025. This version introduces support for a database backend for zone data. For reasons of performance, scalability and replicability, the Redis database – or, alternatively, Valkey – was chosen.

It is now possible to configure the server so that the publication of a zone must be preceded by a user-defined external content check of the zone. The check can be carried out using any script, which will then confirm to the server whether it may proceed or whether the update should be blocked. The contents of the zone to be checked can be obtained in both full and differential formats.

To facilitate migration between different key stores, or to enable the separate storage of DNSSEC KSK (HSM – high security with lower performance) and ZSK (PEM – standard security with higher performance) keys, support has been added for configuring multiple key stores for a single signing policy.

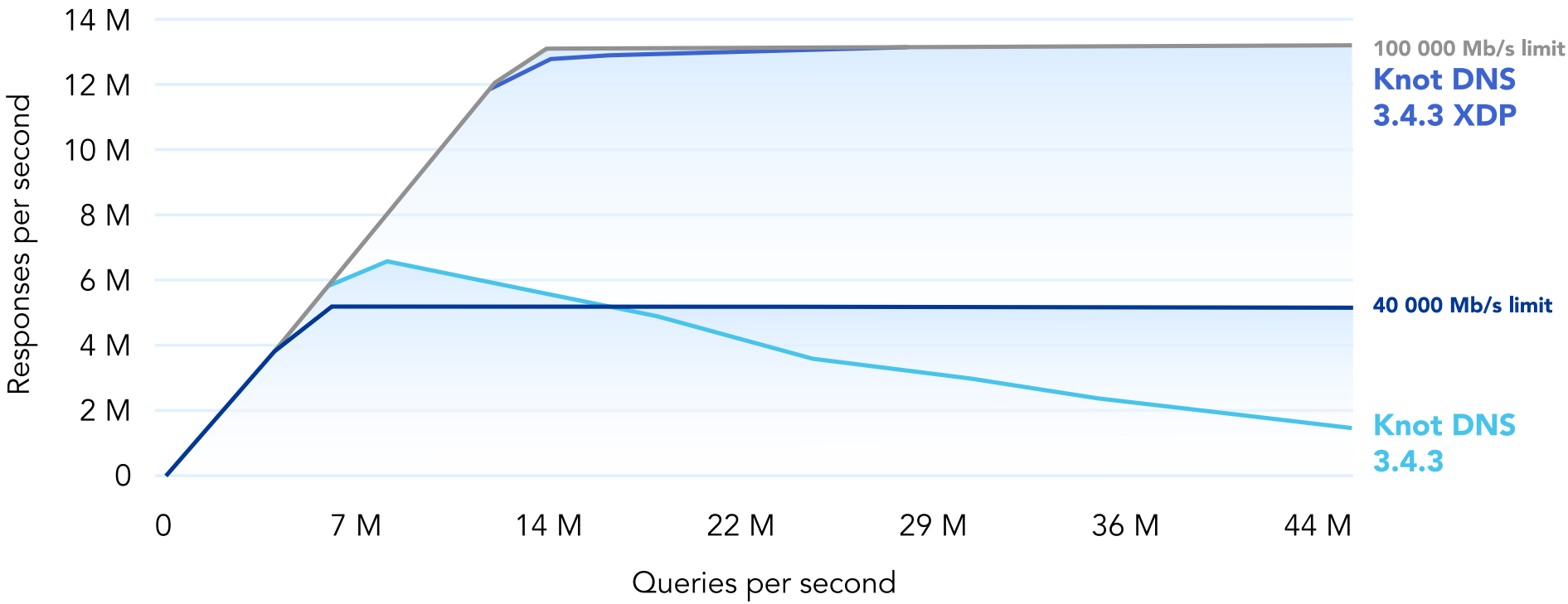
Support for multiple control sockets has been implemented for deployments involving frequent access to the control interface. This makes it possible to dedicate one socket to passive monitoring and another to active server management, without monitoring being hindered by more resource-intensive operations.

Authentication of a remote server via the encrypted QUIC and TLS protocols has been expanded to include validation of the hostname in the certificate.

The processing of changes to configured zones has been optimised to make it more efficient to add or remove zones via the control interface or using catalogue zones.

As part of ongoing performance monitoring of query response times (https://www.knot-dns.cz/benchmark-100G/), we have successfully deployed Intel E810 and Nvidia/Mellanox ConnectX-6 Dx 100GbE network interface controllers in XDP mode. In the case of larger responses, it was possible to approach (for the TLD zone with negative responses) or reach (for the root zone) the line capacity:

Speed of response

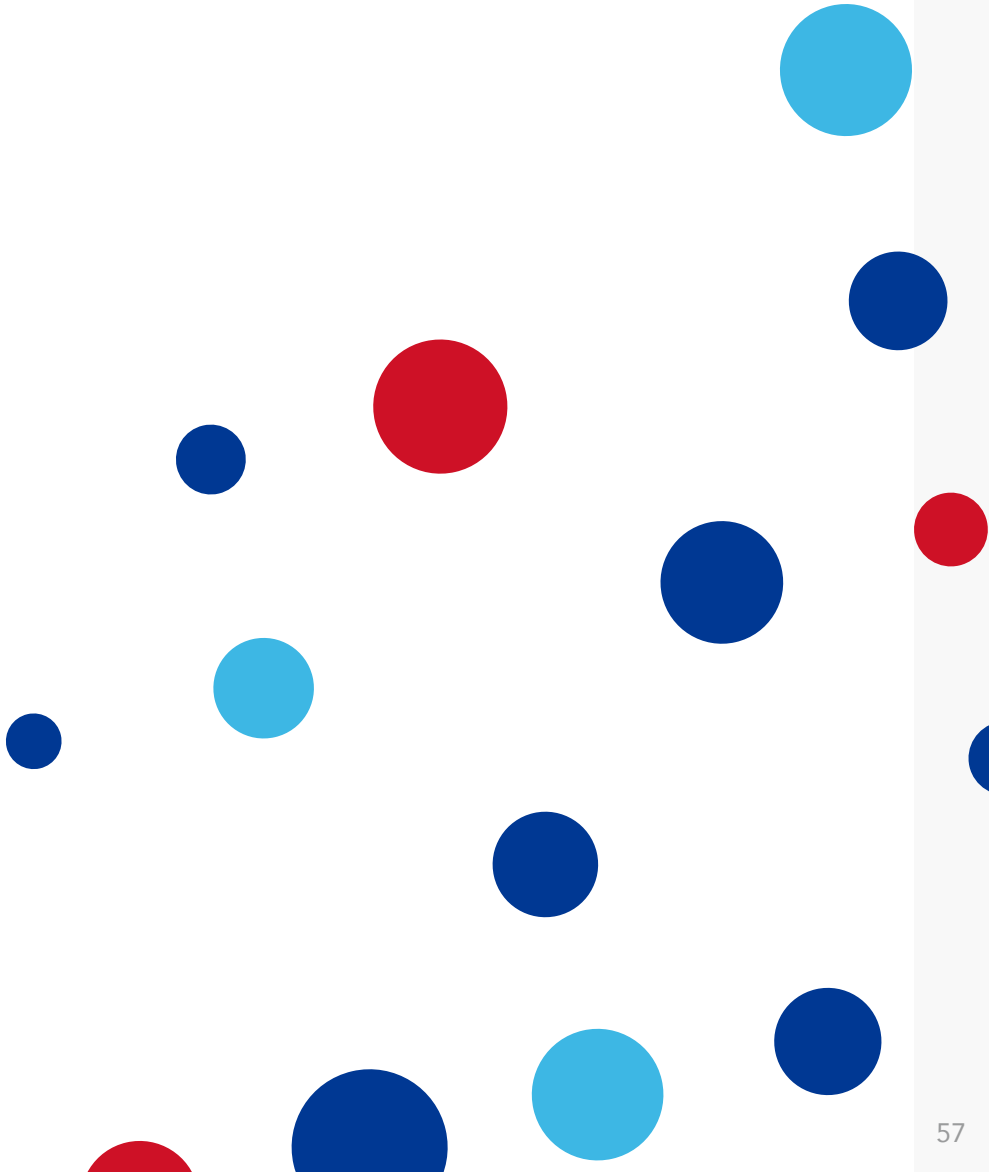


8.4.2 Knot Resolver

Knot Resolver is a recursive DNS resolver, pioneering technologies that improve performance, security and user privacy. It is deployed on our public resolver ODVR and used as the system resolver on Turris routers. It is also used by some Internet service providers and as a key technology in the DNS4EU project, where public resolvers were launched in 2025.

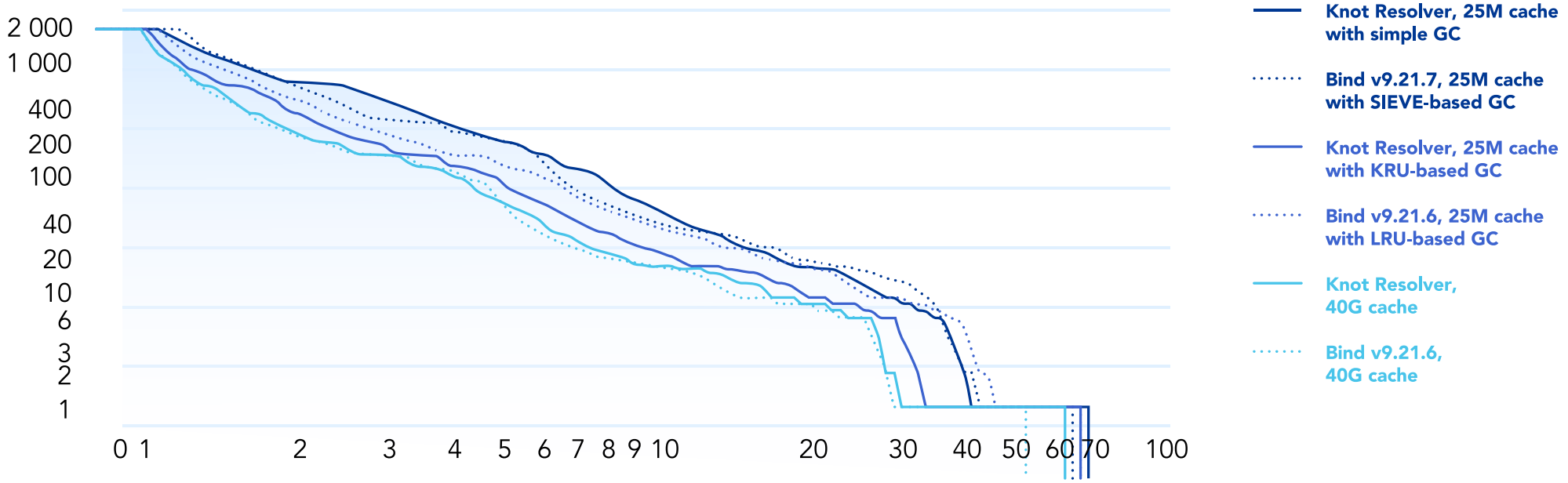
In 2025, development focused mainly on the usability of version 6. The move to version 6 is the most significant change in the project's entire history, spanning roughly a decade; after years of work, it was finally officially declared stable with the release of version 6.1.0. Other notable changes include, for example, a significant improvement to cache management (shown in the image) and the return of support for systems such as FreeBSD and macOS.

In 2025, modifications were made to Knot Resolver, specifically to meet the requirements of the DNS Patrol project. These modifications include, for example, a module for detecting DNS tunnelling using a neural network, the transmission of information regarding the user identifier, the rule applied and other data, as well as the ability to audit blocking rules.



A chart showing the response latency of resolvers configured in various ways when processing a test set of queries. For example, the point [10 ms, 20%] indicates that, for 20% of queries, the response took at least 10 ms. You can read more about this type of chart on the linked blog.

Response latency



8.5 DNS Patrol

In 2025, a new service called DNS Patrol was developed and subsequently launched. It is a service providing a secure DNS system. The service works by analysing DNS traffic in real time. Threats and malicious domains are blocked in accordance with the configured rules. The system administration is carried out via a web interface by an IT administrator or security manager. Client applications for Windows and mobile apps for iOS and Android are available for users accessing the system from outside their home network.

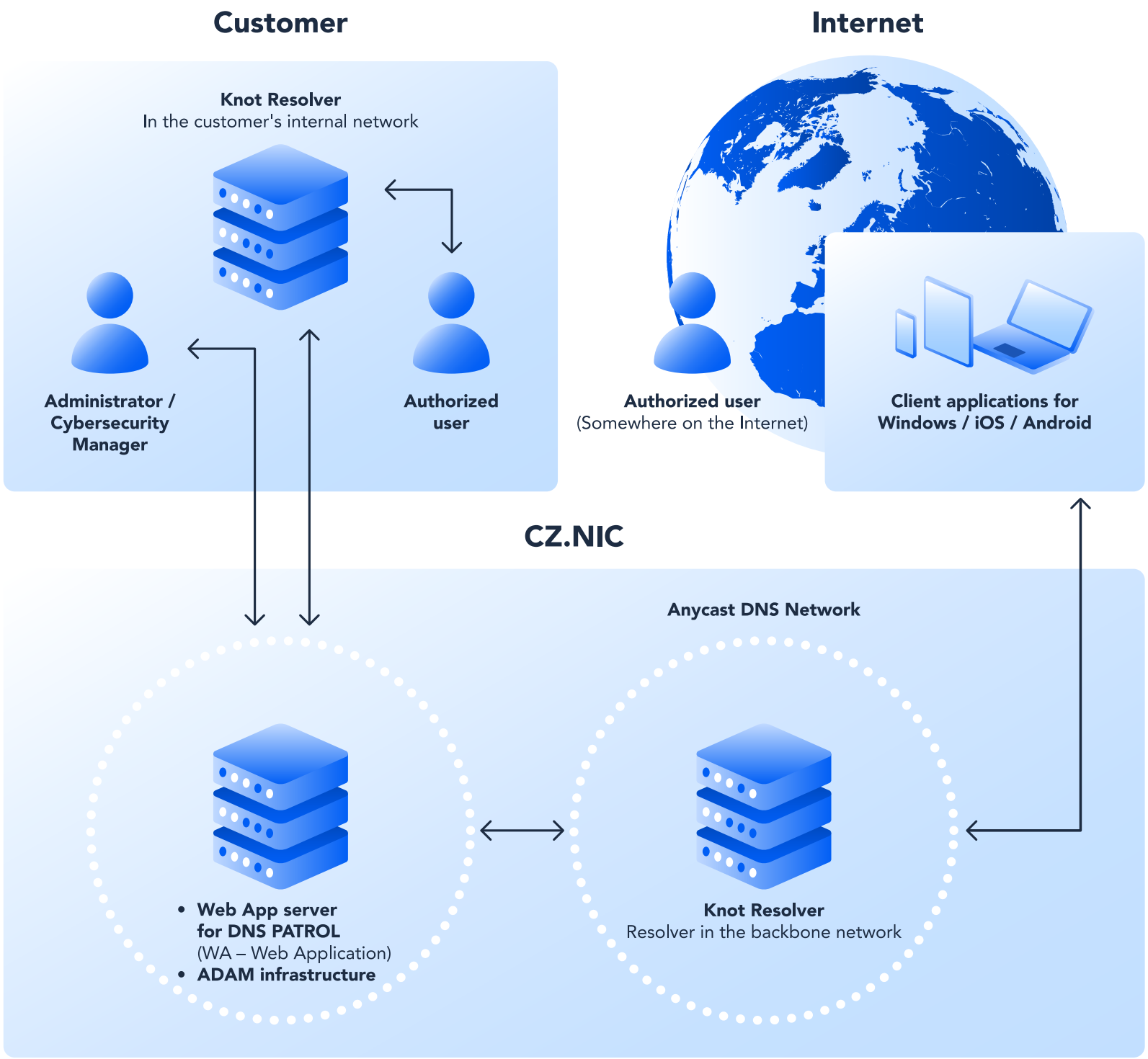
The system was developed in collaboration with the Vysočina Region on a contract basis. It has been in operation in the production environment of the Vysočina Regional Authority since November 2025 and will be gradually rolled out to other subordinate organisations connected to the Rowanet regional network in 2026.

DNS Patrol has been designed to be modular and, in general, in such a way that it can also be used by other users. The entire system is available as open source under an open licence. The paid services include updates to data sources (blacklists), ongoing improvements to detection modules, technical support and operational monitoring. At present, the system is being optimised primarily for the needs of end-user organisations, rather than for Internet service providers (ISPs) or the general public.

DNS Patrol is an add-on that combines existing CZ.NIC projects. At the heart of the system is Knot Resolver, which provides DNS services in the organisation's internal network or via CZ.NIC's anycast infrastructure for users accessing the service from outside the home network. The ADAM project is used for the storage, processing and analysis of logs. CZ.NIC CSIRT is also a source of data for blacklists (via the Deny Lists service).

The newly developed components are the system's backend and the web frontend for managing it. The ClickHouse technology is being deployed to speed up the processing of stored data, while the Kafka platform is used for communication between individual components. The web interface allows us to define different security policies for individual user groups. The multi-tenant approach supports the independent management of subordinate organisations as well as the adoption of policies from the parent layer. MojeID and, more generally, the OIDC interface are used to log in to the system.

The security policy allows operations to be blocked, permitted or audited, separately for each module. In addition to blacklists, whitelists are also used to prevent false detections and resolve false-positive cases. The modules represent different types of threats, each of which can be activated individually. These typically include statutory blacklists (in the Czech Republic, e.g. gambling, medicines and dietary supplements), phishing and targeted phishing, DGA, social media platforms by type (e.g. TikTok), adult websites, fake e-shops and suspicious domains. Some modules are implemented as real-time detectors, such as the detection of DNS tunnelling using a neural network. The web interface also allows users to search the data easily using the query builder and to view statistics according to selected criteria.


Customer
Internet
Knot Resolver
In the customer's internal network
Administrator / Cybersecurity Manager
Authorized user
Authorized user
(Somewhere on the Internet)
Client applications for Windows / iOS / Android
CZ.NIC
Anycast DNS Network
• Web App server for DNS PATROL
(WA – Web Application)
• ADAM infrastructure
Knot Resolver
Resolver in the backbone network

9 Education and awareness

9.1 Communication with the public

The basic pillar of the media communication of the Czech national domain administrator, the CZ.NIC Association, is continuous, regular and systematic cooperation with public and private media. Newspapers, radio and television stations and major media servers dealing with the Internet and technologies thus provided news about the CZ.NIC Association.

In total, the Association published:

- 17 press releases,
- 19 press communications,

which were given to both professional journalists and journalists from media focusing on the general public or specific target groups. 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 educational centre (CZ.NIC Academy), the CSIRT.CZ security team and selected projects of the Association.

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 cybersecurity, personal data protection and education and awareness-raising in the field of the Internet and Internet technologies.

As in previous years, press releases appeared mainly in technically-oriented media. The most common examples were the Root.cz, Lupa.cz and Data Security Management portals. Other online media outlets include the Podnikatel.cz and Novinky.cz servers. The topic of children's online safety was covered, for example, by the lifestyle magazine *Moje psychologie* and the specialised journal *Učitelské noviny*.

CZ.NIC Association employees published 71 authored papers in 2025. Ondřej Filip, Managing Director of the CZ.NIC Association, and other employees were guests on television and radio programmes, mainly on Czech Television, FTV Prima, TV NOVA and Czech Radio. Topics related to cybersecurity, network infrastructure, the Czech national domain and the protection of children online were of interest.

Social media

For administrators of the Czech national domain, accounts on social media (Facebook, X, LinkedIn and, most recently, Bluesky) are an integral part of communications with the public. Supporters are informed, in regular contributions, about the activities of the association, events and current happenings in individual projects. The most followed account of the Association is the one on the X network, followed by the others:

- 6,074
- 3,652
- 2,902
- 113

Other communication channels

Another important part of communication is the NIC-NEWS newsletter, through which messages are sent to subscribers to the email conference of the same name, and the online CZ.NIC Employee Blog. A total of

65 contributions were published in 2025, thanks to the activities of the Association's employees. The blog plays the role of the Association's official communication channel, so it is used by journalists with different focuses.

	Media outputs		Social media (fans)	
	Original papers	Blog	Facebook	X
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
2020	64	50	3,156	4,605
2021	71	56	3,215	5,049
2022	60	67	3,506	5,812
2023	66	72	3,539	5,969
2024	61	65	3,611	6,081
2025	**71**	**65**	**3,652**	**6,074**

Internal communication is provided primarily by the **IN Newsletter**, which CZ.NIC employees usually receive once every two weeks.

9.2 Popularisation series

The CZ.NIC Association supports education as well as the production of popular television programmes.

In the past, series such as *Nauč tetu na netu* (Teach Your Auntie the Internet), *Lovci záhad* (Mystery Hunters) (selected episodes), *Nebojte se Internetu* (Don't Be Afraid of the Internet), *Alenka v říši GIFů* (Alice in GIF Land) and the first and second seasons of *Datová Lhota* were produced in co-production with Czech Television; collaboration on another season of *Datová Lhota* is still ongoing.

We should not forget about our own series, *Jak na Internet* (How to Use the Internet), and the documentary *Caught in the Net*, which won the Czech Lion Award (2021), and the series #martyisdead, which won the International Emmy Award (2020). The Association supported the creation of both projects.

9.3 CZ.NIC Academy educational centre

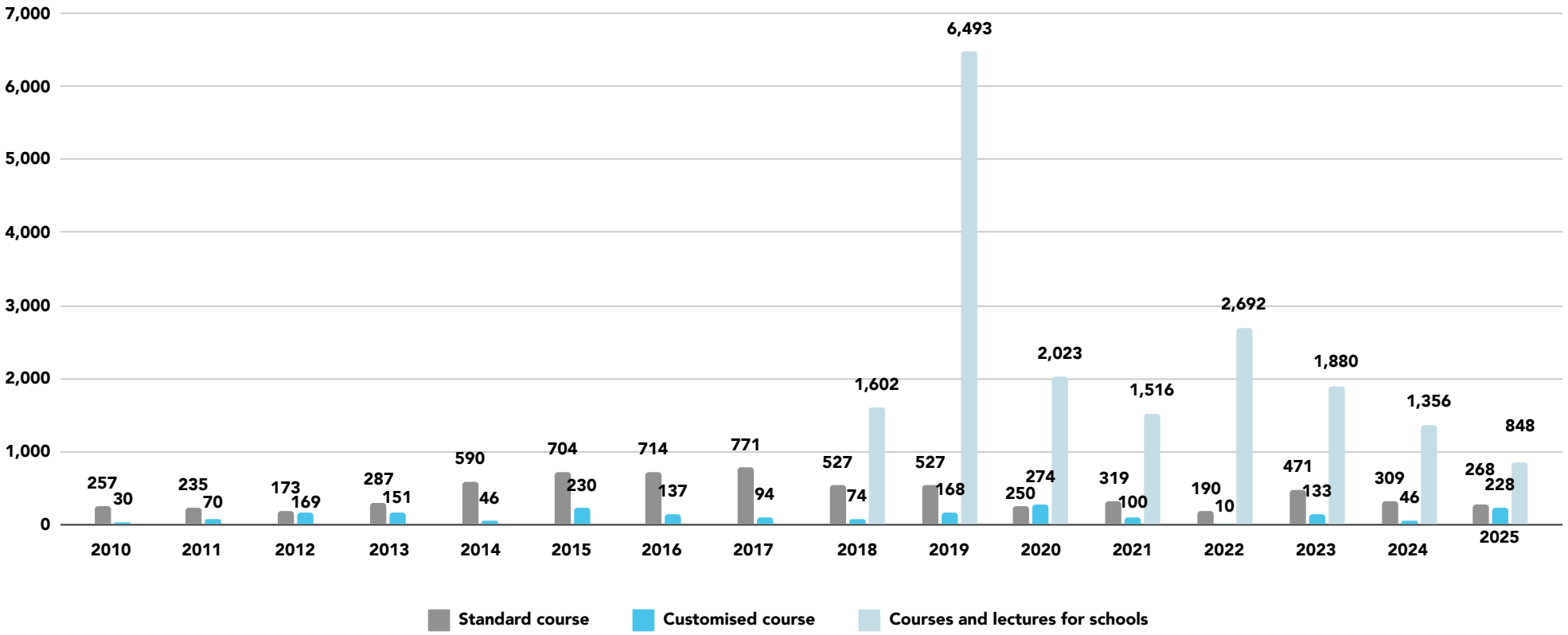
In 2025, the CZ.NIC Academy expanded its offer of educational activities to include four new courses:

- Basics of Web Application Penetration Testing,
- Unsafe Rust in the Linux World,
- A Guide to the Functioning of CSIRT Teams,
- Digital Footprint (e-learning).

From January to October, the CZ.NIC Academy operated from temporary premises in the SUDOP building in Prague 3. During October, it moved into the newly refurbished premises in the Kooperativa insurance company building in Vinohradská Street, also in Prague 3.

In 2025, the CZ.NIC Academy made its premises available not only for in-person courses, but also as a venue for other professional and community events. These included both internal activities, such as a company hackathon, and external events, including seminars for members, the CyberLadies initiative and training organised by RIPE.

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



List of courses and lectures for schools held in 2025

Name	Number of courses	Number of participants
Current Issues in Cybersecurity 2025	1	30
Safe Internet	14	269
Safe Internet – for parents and teachers	1	20
Safe Cyberspace – The Most Common Cyber Attacks and Scams	1	28
Digital Footprint	6	161
E-parenting	2	43
One Share, A Hundred Headaches	5	158
Cyberbullying: A Guide for Parents and Teachers	1	10
On-line Zoo	3	45
Online Content Beyond the Edge	2	64
Follow the Animals to the On-line Zoo	1	20

List of professional courses offered at the CZ.NIC Academy in 2025

Name	Number of courses	Number of participants
Ansible – Mass Automation and Server Management	2	12
DNSSEC – Securing DNS	1	12
Domain Guru	1	9
Git – Universal Versioning System	3	28
Containers (not only) with Docker	2	27
Kubernetes – Container Orchestration	2	23
New Cyber Security Act under NIS2	1	12
DNS Principles and Administration	2	20
A Guide to the Functioning of CSIRT Teams	1	15
Python Formally	2	13
Rust for Beginners	1	12
Introduction to Forensic Memory Analysis	2	22
Introduction to Linux	2	14
Basics of Web Application Penetration Testing	3	33
The Accessibility Act in Practice	2	16

List of tailor-made courses conducted at the CZ.NIC Academy in 2025

Name	Number of courses	Number of participants
Cybersecurity	4	183
Cyberbullying	1	45

Total number of all courses taught at the CZ.NIC Academy in 2025

Course type	Total number of courses	Total number of participants
Professional courses	27	268
Tailor-made courses	5	228
Schools	37	848
Total	**69**	**1,344**

9.4 Conferences

The traditional conference of the CZ.NIC Association, known as Internet and Technology, was held together with the community event LinuxDays 2025. It took place at the Faculty of Information Technology, Czech Technical University in Dejvice, on 4 and 5 October. The conference offered talks that provided information about news from the world of domains and key projects of the Association, as well as presentations on topics related to DNS and Internet security.

In 2025, the CZ.NIC Association presented itself at a number of events and professional conferences in the Czech Republic and abroad. Domestic events included OpenAlt, InstallFest, the Zlín Film Festival, Internet in Telč and the Public Administration Hackathon. As part of its international activities, the Association has, for example, taken part in events organised by DNS OARC, CENTR, ICANN, RIPE NCC and Euro-IX.

In 2025, the CZ.NIC, NIX.CZ and CESNET associations organised another annual meeting of the CSNOG (Czech and Slovak Network Operators Group) community. The main objective of that event was to exchange experience, discuss current topics and share solutions leading to the development of Internet networks in the Czech and Slovak Republics. The meeting took place at Tomáš Baťa University in Zlín on 21–22 January and was attended by 220 participants, mainly from the Czech Republic and Slovakia.

In line with its strategy, the Association hosted an international meeting from 9 to 12 June, bringing together participants from governments, the private sector and the academic community – ICANN 83.

9.5 CZ.NIC Edition

Releasing professional and popularising publications focused on the Internet and related technologies is a long-standing part of the Association's educational activities. The books in **CZ.NIC Edition** are published both in printed and electronic form.

Printed books are offered by the book distribution networks **Kosmas, Euromedia Group and Pemic Books**, and in the **IKAR** network in Slovakia.

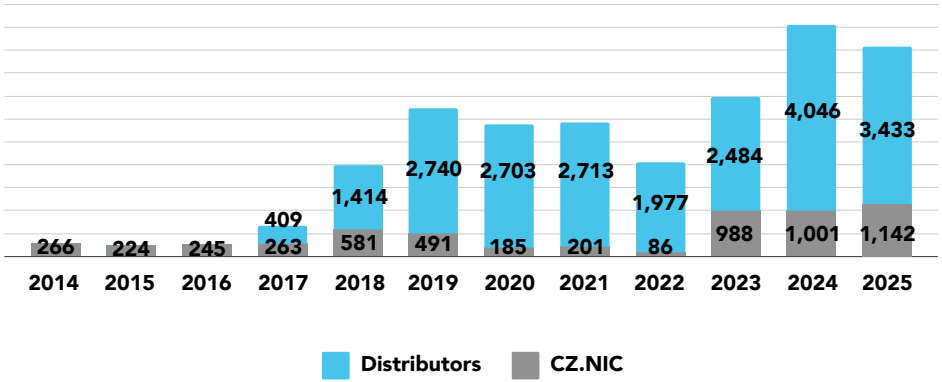
In the year under review, the e-book sector expanded to include the Czech distributor **bookUP**, which handles the sale of our titles via the Luxor e-shop.

CZ.NIC Edition has recently been expanded to include two new titles:

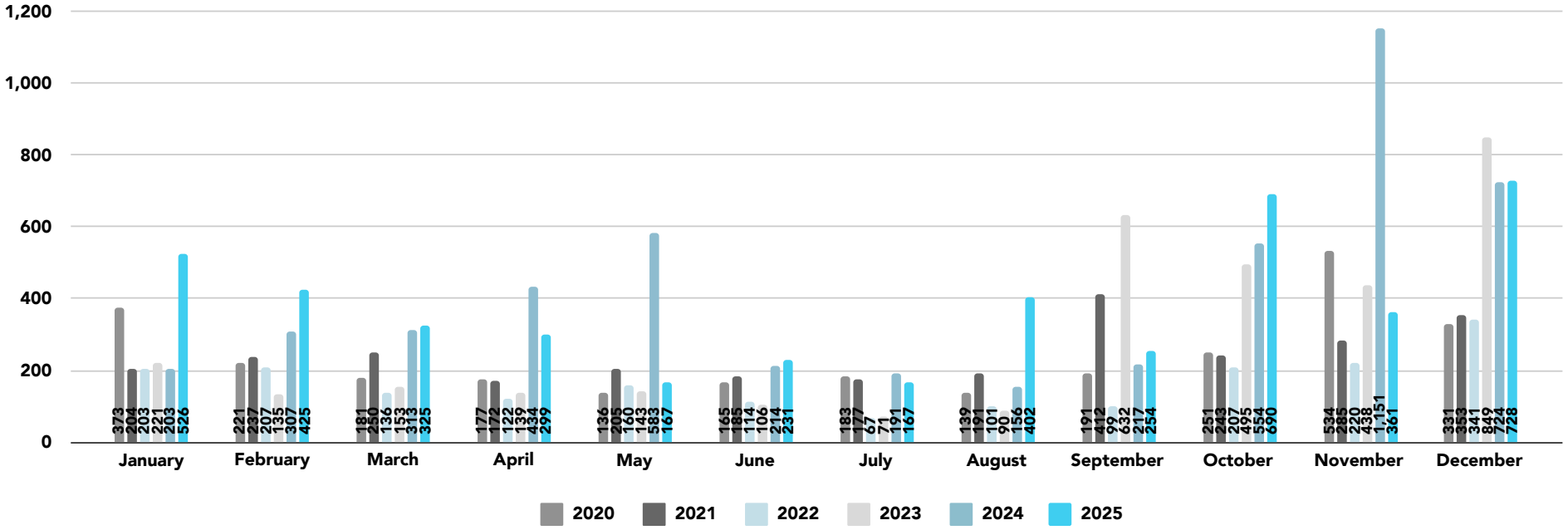
- *Programovací jazyk GO* (The GO Programming Language) by: Pavel Tišnovský
- *Kity, bity, neurony* (Kits, Bits, Neurons) by: Martin Malý

In 2025, a total of **4,575** printed books and **820** e-books were sold.

Overview of book sales by channel



Development of the sale of titles in the CZ.NIC Edition



10 **Cooperation, support and partnership**

Connecting tens of millions of users across all continents, the Internet is clearly the most important communication tool today. We 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 sectors, the rules are often created by the Internet community, which also includes employees of the CZ.NIC Association.

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

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

International cooperation not only facilitates the tracking of global trends, the participation of the Association's employees also contributes to their creation, which 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 Cooperation in the Czech Republic

The CZ.NIC Association has long been rated as a key partner to the public administration and to professional and interest groups and organisations operating in the field of the Internet, providing expert knowledge in the area of Internet governance.

10.1.1 Cooperation with public administration

Domain name administration and the associated Internet infrastructure are a key part of the critical infrastructure of the State. For the CZ.NIC Association, protecting this infrastructure is one of its primary tasks, and ensuring its efficient and secure operation is a fundamental prerequisite for the development of digital services (including eGovernment) not only in the Czech Republic.

Within the framework of the growing cooperation with the public administration, the Association continuously communicates with a number of state authorities, such as the Czech Telecommunication Office (CTO), the National Cyber and Information Security Agency (NÚKIB), the Ministry of the Interior of the Czech Republic and the Police of the Czech Republic.

Under a public-law contract, the CZ.NIC Association operates the National CSIRT (*Computer Security Incident Response Team*) of the Czech Republic on behalf of NÚKIB.

As the state has not yet implemented the so-called "European wallet", the MojeID service, operated by the CZ.NIC Association, continued to significantly facilitate access to public services for Czech citizens in 2025, not only in the Czech Republic but also, thanks to European notification, in other EU Member States. MojeID continues to cement its position as the most versatile tool for electronic identification in the Czech Republic.

At the same time, the CZ.NIC Association continues managing the national eIDAS node on behalf of the Digital and Information Agency.

The Safer Internet Centre CR (SIC CZ) project, whose importance is constantly growing thanks to its indisputable role in protecting young users, and which operates in close cooperation with the state administration, represents a significant initiative by the CZ.NIC Association. A key component is the **STOPonline.cz** service, whose team focuses on reporting and tackling harmful content on the Internet (particularly child pornography), thereby helping to create a safer online environment for children and young people.

The CZ.NIC Association has been actively involved in debates on legislative proposals affecting the digital environment, both at the national and European level. Representatives of the Association have cooperated closely with a number of key institutions, including the Ministry of Industry and Trade of the Czech Republic, the Police of the Czech Republic, judicial and distraint authorities, as well as with other authorities commissioned by law, such as the Office for Personal Data Protection, trade licensing authorities, tax authorities and the Customs Administration.

10.1.2 Cooperation with the non-profit sector

Člověk v tísni (People in Need)

The Association supports, in particular, the educational project of the humanitarian and educational organisation Člověk v tísni (People in Need) entitled **One World**. It offers schools documentary films and accompanying methodological aids for teaching current topics of the contemporary world and modern history.

Faculty of Mathematics and Physics, Charles University

In the years 2021–2026, the Association continues to be a partner of the Faculty of Mathematics and Physics of Charles University. Both entities cooperate particularly in the field of research, development and education, as they are connected by a number of topics related to the Internet and Internet networks, as well as by key projects of the Association, such as the BIRD routing daemon and the Knot DNS authoritative DNS server. As part of this cooperation, the CZ.NIC Association regularly supports the Kasiopea programming competition, intended primarily for secondary-school students.

Whistleblowing

The CZ.NIC Association has introduced an internal whistleblowing system to enable the safe reporting of potential unlawful conduct. It thus promotes the timely resolution of complaints and emphasises transparency and ethical conduct. Further information is available on the Association's website.

10.1.3 Membership in professional and interest organisations

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 also utilises technology from the CZ.NIC Labs, in particular the BIRD routing daemon.

Involvement in the FENIX project

The FENIX project, established in 2013, enhances the resilience of Internet infrastructure against large-scale DoS attacks and helps to ensure the availability of services even in crisis situations. Entities and organisations that meet the specified technical and security requirements may take part.

10.2 Social responsibility (supporting third parties and projects)

The CZ.NIC Association is fully aware of the necessity of environmental protection and the importance of sustainable development. It strictly complies with environmental standards and regulations in accordance with applicable legislation and internal policies. At the same time, we continue to actively seek out opportunities to minimise the negative environmental impact of our activities.

For us, digitalisation and technological transformation are key tools for putting these principles into practice. Modern technology enables us to reduce paper consumption, optimise energy use and make more efficient use of resources. Our priority is to carry out all our activities with a focus on environmental sustainability.

Energy management

Several years ago, thermostatic heads were installed at the Association's headquarters, enabling the temperature in individual rooms to be controlled remotely depending on the season or the day of the week. This modernisation has made the heating of the offices more efficient and has demonstrably helped reduce natural gas consumption.

We are also seeing a drop in electricity consumption. This trend is also driven by the regular replacement of hardware with more energy-efficient

equipment, as well as the adoption of working from home, which reduces energy consumption in offices.

Waste management

The CZ.NIC Association has long strived to minimise waste production and promoted a culture of responsible waste management. We encourage our staff to prevent waste and recycle. Recycling bins are available on every floor of our headquarters.

All electrical waste is sent for environmentally sound disposal in accordance with the law. We arrange waste collection and reporting through an external contractor, which enables us to regularly monitor the composition of the waste, assess its volume, and plan our next steps in this area. As a manufacturer of Turris routers, we are also fully involved in the collective electrical equipment take-back scheme.

Going paperless

CZ.NIC's long-term objective is to digitalise its administrative processes, not only to reduce waste but also to improve efficiency. Thanks to its systematic approach, the Association is succeeding in reducing both paper consumption and the share of paper in waste. The main measures include the electronic conclusion of contracts, the digitalisation of invoicing and changes to the processes for verifying domain holders' details. Flexible working arrangements also help to reduce energy consumption.

Promoting eco-friendly travel

We actively encourage our staff to use sustainable modes of transport. Our workplaces are easily accessible by public transport and are equipped with facilities for cyclists. We also regularly take part in the "Cycle to Work" campaign.

When it comes to business travel, we prioritise efficiency and minimising our environmental impact. Where appropriate, face-to-face meetings are replaced by online meetings or conference calls. We also make use of the option to participate remotely in professional events, which allows us to play a full part without having to travel.

Helping animals

The CZ.NIC Association has been contributing to the breeding of the southern cassowary at the zoos in Prague, Jihlava and Zlín on a long-term basis.

10.3 Cooperation abroad

10.3.1 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 phishing.

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 distant 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. The CENTR Technical Working Group has been headed for a long time by Jaromír Talíř, a technical partner of the Association.

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.

EURid (The European Registry of Internet Domain Names)

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

EuroISPA (European Internet Services Providers Association)

The European Internet Services Providers Association is the largest organisation, bringing together more than 3,300 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

An interest group of CSIRT teams that acts as a contact point for the 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 network and information systems across the Union). The group primarily deals with technical issues related to the implementation of this agenda.

FIRST (Forum of Incident Response and Security Teams)

The first international organisation associating security teams. It has over 800 teams in more than 100 countries around the world, with significant representation of American and European teams. It is the only organisation that provides membership to teams from around the world and also covers product teams. The CSIRT.CZ team became a member of the FIRST organisation as early as 2015.

ICANN (Internet Corporation for Assigned Names and Numbers)

An international non-profit organisation founded in 1998, the main task of which is to administer and assign not only generic top-level domain names (gTLDs) and national top-level 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 the activities of the working groups.

IETF (Internet Engineering Task Force)

Founded in 1986, the organisation is closely linked to the emergence of the Internet and brings together an international community of experts, architects and representatives from the commercial sector. Key Internet standards (RFCs) are developed and approved within the IETF, with CZ.NIC staff also contributing to this work. They are particularly active in the DNSOP, NETCONF and NETMOD working groups. One notable figure is Ladislav Lhotka (a former member of the CZ.NIC management team), the first Czech lead author of an RFC (RFC 6110) and co-author of the more recent standards, RFC 9108 and RFC 9130. IETF meetings have also been held in Prague on several occasions.

INHOPE (International Association of Internet Hotlines)

INHOPE is an international association of more than 55 hotlines dedicated to combating illegal online content, particularly child abuse material. Membership enables data to be shared via the ICCAM system and facilitates effective cooperation with international partners and organisations, including Interpol.

The CZ.NIC Association, through its STOPonline.cz helpline, became an associate member in 2017 and subsequently gained full membership as part of the Safer Internet Centre CR (SIC CZ) project.

Europol (European Union Agency for Law Enforcement Cooperation)

Europol is an organisation dedicated to preventing and combating organised crime. The organisation falls under the European Union and seeks to improve cooperation between Member States, in particular through police and judicial consultancy and its awareness-raising and educational activities.

RIPE NCC (Réseaux IP Européens Network Coordination Centre)

RIPE NCC (Réseaux IP Européens Network Coordination Centre) is an independent, non-profit organisation that supports the development of Internet infrastructure. It operates a regional Internet register (RIR) that manages and allocates Internet resources, in particular IP addresses.

As a member, the CZ.NIC Association takes part in regular meetings, as well as professional activities and training courses. Since May 2025, Ondřej Filip, the Managing Director, has been Chair of the Board of Directors of the organisation.

TF-CSIRT

TF-CSIRT is an organisation that brings together security teams, predominantly from Europe. The CSIRT.CZ team has the highest possible level of membership in this organisation – certified. CZ.NIC-CSIRT is an accredited member.

In 2025, our colleague Věra Mikušová was elected to chair the TF-CSIRT Steering Committee.

11 Grant projects

The CZ.NIC Association has long been involved in European projects focused on the development of digital infrastructure, electronic identity and a safer online environment. In 2025, we focused primarily on areas relating to digital identity, technology services and promoting the safe and responsible use of the Internet.

Over the past year, we have led one national consortium and participated in two international consortia co-funded by the EU's Connecting Europe Facility (CEF) and Digital Europe Programme (DEP).
These initiatives focus on the development of key digital services, infrastructure and security solutions across Europe.

In 2025, we took part in the following projects co-financed from the EU budget:

EU Digital Identity Wallet Consortium (EWC; project no. 101102744)

The EU Digital Identity Wallet Consortium (EWC) project focused on pilot testing the European Digital Identity (EUDI Wallet), a digital wallet designed to enable secure identity verification across the European Union. CZ.NIC became involved in the project as part of its activities in the field of electronic identity and domain administration. The consortium comprised 41 partners from across Europe.

At the beginning of 2025, a four-month extension to the implementation period was approved, with the aim of completing the work in progress and bringing the pilot phase to a close. The final activities focused on finalising the implementation specifications, aligning the solution with the current version of the Architectural Reference Framework, and completing the pilot scenarios in the areas of travel, payment services and the identification of legal entities.

Final testing confirmed the technical consistency and cross-border interoperability of the solution. A set of implementation specifications (RFCs), verified via an interoperability testing environment, confirmed that the system functioned correctly in a multi-provider environment. The project was successfully completed in 2025.

DNS4EU and European DNS Shield (DNS4EU; project no. 101095329)

The DNS4EU project aimed to establish a European DNS resolver infrastructure with the aim of strengthening the European Union's digital sovereignty and offering a secure alternative to public DNS services operated outside the EU. The project built on CZ.NIC's long-standing technological activities in the field of DNS, with the Association providing a key technological component via its DNS resolver.

Throughout 2025, CZ.NIC focused primarily on the further development and optimisation of the resolver, including improving its performance and stability, supporting modern network technologies, and developing functions for filtering DNS traffic. The final phase also included the completion of a DNS standards compliance report, summarising the relevant standards for DNS resolvers and confirming their implementation in the DNS4EU solution.

The final phase of the project culminated in December 2025 with testing on commonly used platforms, operating systems and applications, with the aim of verifying the current status of the solution at the end of the project implementation. The project was completed on 31 December 2025.

Safer Internet Centre CR (SIC CZ; project no. 101158518)

The Safer Internet Centre CR (SIC CZ) focuses on the safety of children and young people online and on developing their digital skills. Since 2019, CZ.NIC has been managing and administering the project, as well as overseeing its European communications and international cooperation within the Insafe and INHOPE networks. The project is being carried out in collaboration with the organisations Člověk v tísni (People in Need) (One World in Schools), the Child Helpline and the Children's Crisis Centre. In addition to technology projects focusing on infrastructure and digital services, CZ.NIC has also been working for many years through SIC CZ to promote the safe and responsible use of the Internet.

The year 2025 saw several significant works, including the national study "Czech Pupils in the Online World", carried out in collaboration with Palacký University in Olomouc, in which 53,119 respondents took part (of whom 42,772 were pupils and students aged 13–17), and the prevention campaign "Don't Leave a Digital Footprint for Your Children", prepared in collaboration with the Police of the Czech Republic and recognised at the National Crime Prevention Days. The partners' activities made a significant contribution to engagement with schools, parents and the professional community, including 131 school visits and 40 other educational activities.

The project also focused on public and specialised events. As part of the 65th Zlín Film Festival, it organised a two-day programme comprising a conference entitled "Journalism in the Digital Age", expert panel discussions and film-related activities for schools focusing on media literacy and online safety. Safer Internet Day 2025 focused on the topic of digital footprints and responsible online sharing, including the impact of artificial intelligence on digital safety. The project also significantly boosted its media presence and became a respected source for the media; 579 media appearances were recorded during the year.

The activities also included the development of online and offline awareness-raising tools. Communication with young audiences took place, among other things, via the Instagram account No_Net_Drama, which complements the main web platform bezpecnyinternet.cz (17,615 unique visitors; 2,926,000 views in 2025). As part of the project, 12 new awareness-raising materials were produced, bringing the total number of available resources to 25 publications, with an estimated reach of nearly 30,000 people.

Last but not least, SIC CZ also includes the STOPonline.cz hotline, operated in collaboration with the national CSIRT.CZ team, which links the project's preventative and awareness-raising activities with practical solutions to harmful content on the Internet. In 2025, the hotline received 6,073 reports, representing a year-on-year increase of approximately 70% compared to 2024.

12 Structure of the Association

12.1 Members

The member base of the Association is made up of a number of entities heavily **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 which the Internet and domain names are an important communication tool.

The CZ.NIC Association is one of the places these representatives can meet and thus influence the future direction of the Czech Internet. Further expansion of the Association's knowledge portfolio, streamlining its management and the ability to respond to the constant development of the Internet allow a wide range of business activities of members and their involvement in the Association, either by attending General Meetings, working groups and seminars, email conferences or by directly working on the Association's bodies.

Membership conditions

A legal entity that meets the following general terms and conditions for membership can become a member of the Association:

- location of the seat or organisational unit in the territory of an EU Member State,
- holding at least one domain name in ccTLD CZ,
- payment of the entrance membership fee.

The members of the Association are divided into three chambers:

- Chamber of Domain Name Holders,
- ISP Chamber,
- Chamber of Registrars.

The respective Statutes govern the special conditions of 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 at 31 December 2025, the CZ.NIC Association had a total of **117 members**.

Development of the number of members by chamber

Chamber/ year	ISP	Registrars	Domain name holders	Total
2008	15	11	31	**57**
2009	17	14	32	**63**
2010	19	19	37	**75**
2011	23	17	49	**89**
2012	27	18	61	**106**
2013	27	19	65	**111**
2014	24	20	69	**113**
2015	23	20	72	**115**
2016	25	20	67	**112**
2017	26	18	71	**115**
2018	26	19	69	**114**
2019	27	17	72	**116**
2020	27	17	75	**119**
2021	29	16	75	**120**
2022	28	16	77	**121**
2023	28	16	76	**120**
2024	27	16	74	**117**
2025	**27**	**16**	**74**	**117**

Division of members by chamber

ISP	23.1%
Registrars	13.7%
Domain name holders	63.2%

12.1.2 Overview of members by chamber

Overview of members of individual chambers as at 31 December 2025

Chamber of Domain Name Holders (business name, Company ID No.)

ABRATICA s.r.o.	26108534
ACOMWARE s.r.o.	25047965
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
Allegro Retail a.s.	8553866
Asociace pro elektronickou komerci, z.s. (Association of E-commerce)	68684797
AUDITEL, s.r.o.	26775034
CD PROFESIONAL security agency, s.r.o.	25712713
CISCO SYSTEMS (Czech Republic) s.r.o.	63979462
.CO.CZ s.r.o.	14364786
COMGUARD a.s.	28215176

ComSource s.r.o.	29059291
Com-Sys TRADE spol. s.r.o.	16188781
CQK HOLDING a.s.	28405579
CYBERSALES a.s.	26199653
Česká unie vydavatelů, z.s. (Czech Publishers Association)	15887081
Datahost s.r.o.	26390973
DELL Computer, spol. s r.o.	45272808
Designers & Developers s.r.o.	7424434
ECOMOLE LTD.	9526615
ekolo.cz s.r.o.	27141659
Fortion Networks, s.r.o.	26397994
Gordian Investments s.r.o.	24159778
Greenlux s.r.o.	28608747
Holubová advokáti s.r.o.	24686727
ICZ a.s.	25145444
igloonet, s.r.o.	27713482
I. H. P. společnost s ručením omezeným	48117846
IMAGIX one s.r.o.	22018930
INBES, spol. s r.o.	14502593
Intell. Net s.r.o.	27971546
Internet Info, s.r.o.	25648071
IoT Way s.r.o.	14363810
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
MEASUREMENT PRAHA, s.r.o.	4404971
MEDIA FACTORY Czech Republic a.s.	26288311
Michal Krsek & partneři s.r.o.	27418570
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
Orego finance s.r.o.	24718955
PharoCom s.r.o.	25172131
Prague Business Office s.r.o.	27143481
Pražský Účetní Servis s.r.o.	26740575
Qrator Labs CZ s.r.o.	3620174
Seyfor, a.s.	1572377
SH.cz s.r.o.	25492063
Skymia s.r.o.	28238613
Software602 a.s.	63078236
Socha, spol. s r.o.	48291153
SVBsoft, s.r.o.	28523644
TechLabs s.r.o.	8618445
TIKWI s.r.o.	28917651
Trustica s.r.o.	26514362
ÚVT, s.r.o.	25701118
Vedea s.r.o.	28913876
VIZUS.CZ s.r.o.	27155315
VOLNÝ, a.s.	63080150
Webarium, s.r.o.	26089602
Webnames s.r.o.	44848692
Web security s.r.o.	6927351
Ztracené kobylky, z.s.	22753001
1X s.r.o.	44632142

ISP Chamber (business name, Company ID No.)

ABAK, spol. s r.o., CZE ABAK, GmbH GER ABAK, Co.Ltd. ENG	40763153
Casablanca INT a.s.	9070931
CESNET, z.s.p.o.	63839172

COOLHOUSING s.r.o.	14893983
ČD – Telematika a. s.	61459445
České Radiokomunikace a.s.	24738875
ČEZNET s.r.o.	26378191
Dragon Internet a.s.	27237800
Družstvo EUROSIGNAL	26461129
Faster CZ spol. s r.o.	60722266
FreeTel, s.r.o.	24737887
H17 Networks, s.r.o.	27374041
IPEX a.s.	45021295
JHComp s.r.o.	26051362
LAM plus s.r.o.	25129619
Mach3net s.r.o.	27344860
MasterDC s.r.o.	26277557
NetArt Group s.r.o.	27612694
NetX Networks a.s.	8544603
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

Chamber of Registrars (business name, Company ID No.)

ACTIVE 24, s.r.o.	25115804
ASPone, s.r.o.	28274326
e-BAAN Net s.r.o.	26867257
INTERNET CZ, a.s.	26043319
KRAXNET s.r.o.	26460335
Media4web, s.r.o.	26735903
ONE.CZ s.r.o.	25503651
O2 Czech Republic a.s.	60193336
Quantcom, a.s.	28175492
Seonet Multimedia s.r.o.	27522041
Seznam.cz, a.s.	26168685
TELE3 s.r.o.	26096960
Webglobe, s.r.o.	26159708
Web4U s.r.o.	17311501
ZONER a.s.	49437381
ZooControl s.r.o.	5766656

12.2 Bodies of the Association

12.2.1 General Meeting

The supreme body of the Association is the General Meeting, i.e. all 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 member of the Association has the right to attend the General Meeting and voice their ideas, 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 of office.

Members of the Collegium elected by the General Meeting

Chamber of Domain Name Holders

- Antoš Marek
- Gruntorád Jan
- Košata Bedřich (re-elected for a further term of office from 21 December 2025)
- Ohnesorg Dan (re-elected for a further term of office from 21 December 2025)
- Redl Jan
- Taft Karel

ISP Chamber

- Dragon Tomáš
- Košňar Tomáš
- Pečínka Vlastimil (re-elected for another term in office from 21 December 2025)
- Pospíchal Zbyněk (re-elected for another term in office from 21 December 2025)
- Procházka Marcel
- Švácha Milan

Chamber of Registrars

- Behro Milan (elected from 21 December 2025)
- Filípková Ilona
- Kukačka Martin
- Kysela Stanislav (re-elected for another term in office from 21 December 2025)
- Pohořelická Martina
- Polanský Lukáš (until 20 December 2025)
- Syrovátka Erich

Members of the Collegium nominated by state administration authorities

- Bumbálková Zina, Ministry of Industry and Trade of the Czech Republic
- Schäfer Lenka, Czech Chamber of Commerce
- Peterka Jiří, Czech Telecommunication Office (until 6/2025)
- Vrbík Marek, Czech Telecommunication Office (from 6/2025)

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

1 January 2025 – 30 June 2025

- Taft Karel, Chair of the Board of Directors
- Antoš Marek, Vice-Chair of the Board of Directors
- Filípková Ilona, Member
- Košňar Tomáš, Member
- Kukačka Martin, Member

1 July 2025 – 31 December 2025

- Košňar Tomáš, Chair of the Board of Directors
- Antoš Marek, Vice-Chair of the Board of Directors
- Filípková Ilona, Member
- Kukačka Martin, Member
- Taft Karel, Member

12.2.4 Supervisory Board

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

Members of the Supervisory Board 2025

- Redl Jan, Chair of the Supervisory Board
- Gruntorád Jan, Member
- Pečínka Vlastimil, Member

12.2.5 Management

Overview of the members of the management as at 31 December 2025

- Filip Ondřej, Chief Executive Officer
- Peterka Martin, Chief Operating Officer and Deputy Managing Director
- Brůna Zdeněk, Chief Technical Officer
- Fuňka Tomáš, Chief Financial Officer
- Hála Tomáš, Chief Information Office
- Hatlapa Tomasz, Chief Marketing Officer (from 2/2025)
- Hrušecký Michal, Head of the Hardware Development Department
- Chmelová Kateřina, Chief Sales Officer
- Chomyn Josef, Head of the Research Team (CZ.NIC Labs)
- Novák Jaromír, Partner for Relations with the Public Administration
- Písek Ondřej, Chief Marketing Officer (until 2/2025)
- Sládek Vilém, Chief Communications Officer
- Talíř Jaromír, Technical Fellow

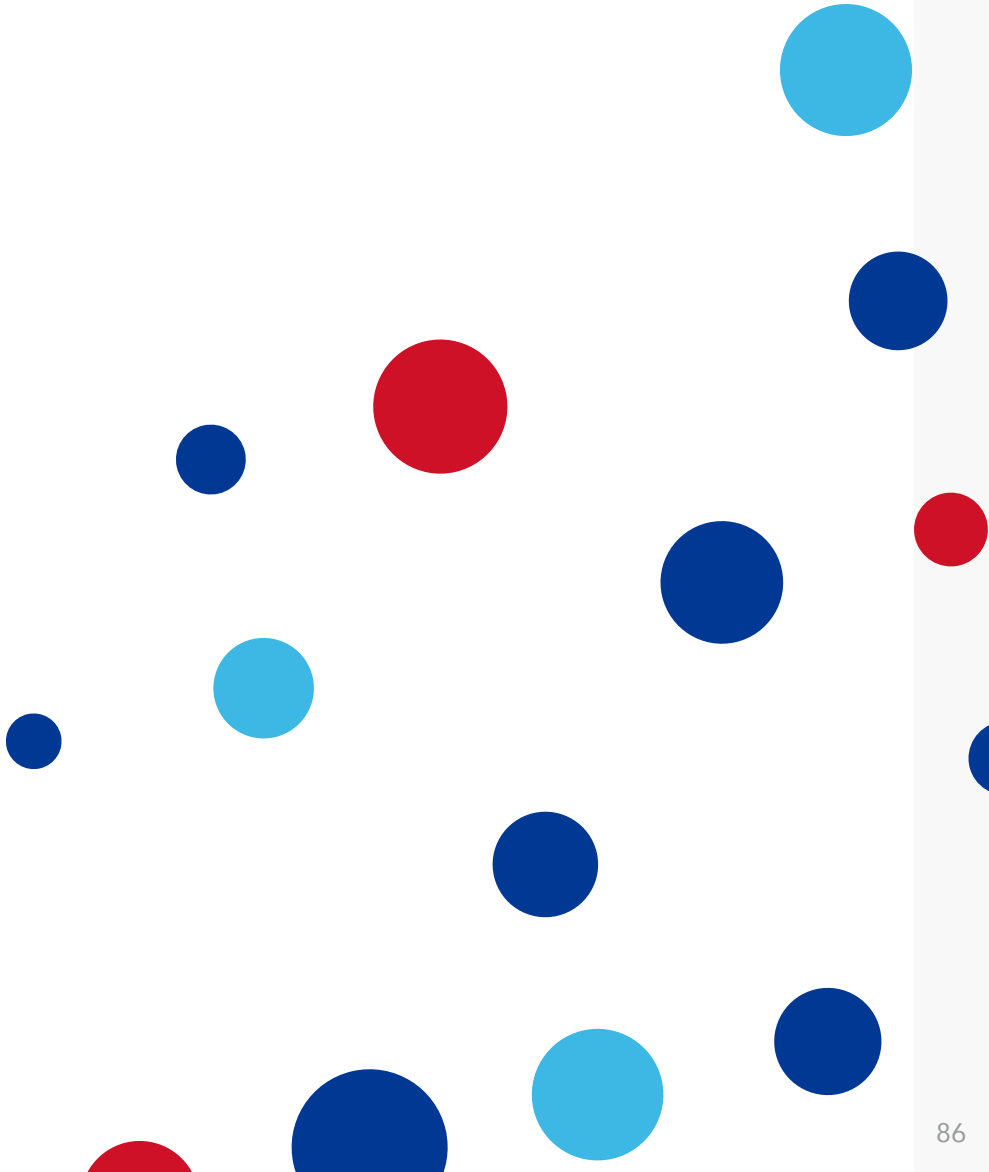
13 **Human resources**

The Association's strength lies in its professionally competent and qualified employees, who are essential for achieving its mission and further development. It is no exaggeration to say that many of our employees are leading experts in their fields, with both a Czech and international reputation.

To strengthen individual competencies, all employees are continuously educated in the fields of foreign languages, so-called soft skills and professional knowledge, so that they can achieve the highest possible professional and personal qualities and contribute with their knowledge and skills to the further development of the Association and thus also the Czech Internet.

13.1 Number of employees

In 2025, the number of employees of the Association again increased. The Hardware Development Department saw the biggest increase in staff, but we also welcomed new colleagues to the development and laboratory teams. As well as employing experienced professionals, the Association also nurtures new talent; as a result, many of its departments employ university and secondary-school students working part-time or under agreements to perform work.



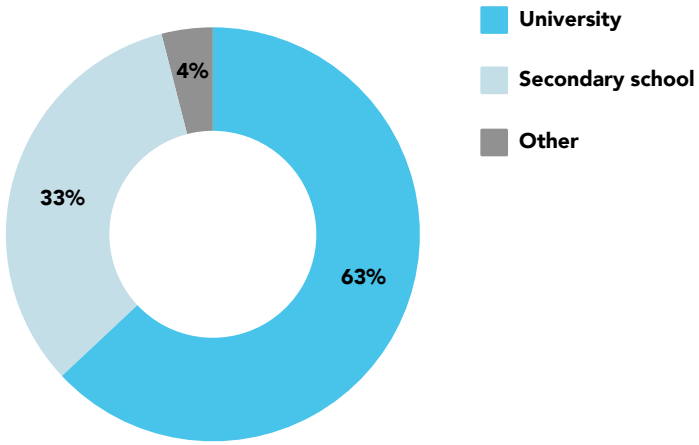
Status and development of the number of employees

Department	Number of employees (as at 31 December 2024)	Number of FTEs (as at 31 December 2024)	Number of employees (as at 31 December 2025)	Number of FTEs (as at 31 December 2025)
Management	12	11.60	12	11.60
Marketing/PR	7	5.60	8	6.40
Sales	3	3.00	4	3.00
Academy	1	1.00	1	0.80
Development	30	25.23	33	27.53
Network Administration	13	12.50	13	12.80
CZ.NIC Labs	26	17.90	29	24.10
Legal	2	1.75	2	1.75
Secretariat	2	2.00	2	2.00
HR	1	0.88	1	0.88
Customer Support	11	11.00	11	11.00
CSIRT	15	12.20	14	12.50
HW Development Department	17	11.38	20	13.80
EU Projects	5	2.75	5	3.25
Total	**145**	**118.78**	**155**	**131.40**

13.2 Employee structure

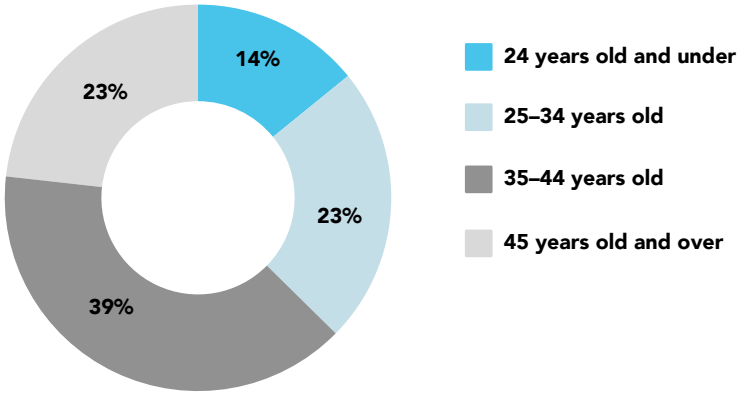
Employee structure by education

Most Association employees have a university degree. The CZ.NIC Association offers recent university graduates the opportunity to gain professional experience, creating suitable conditions for them, including the chance to work at its branches in Brno, České Budějovice and Plzeň. At the same time, the Association has an open door for talented secondary school and university students.



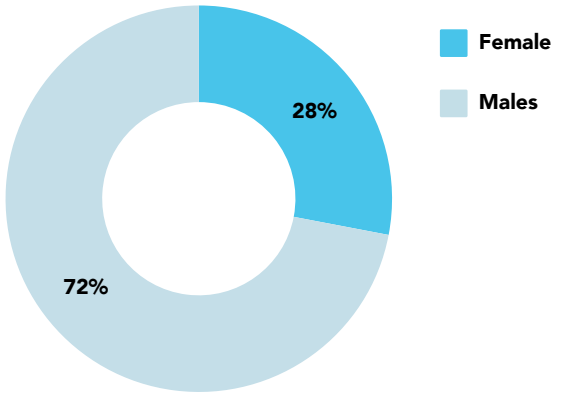
Employee structure by age

The average age of the Association's employees is 38 years. In terms of age structure, employees aged 35–44 predominate.



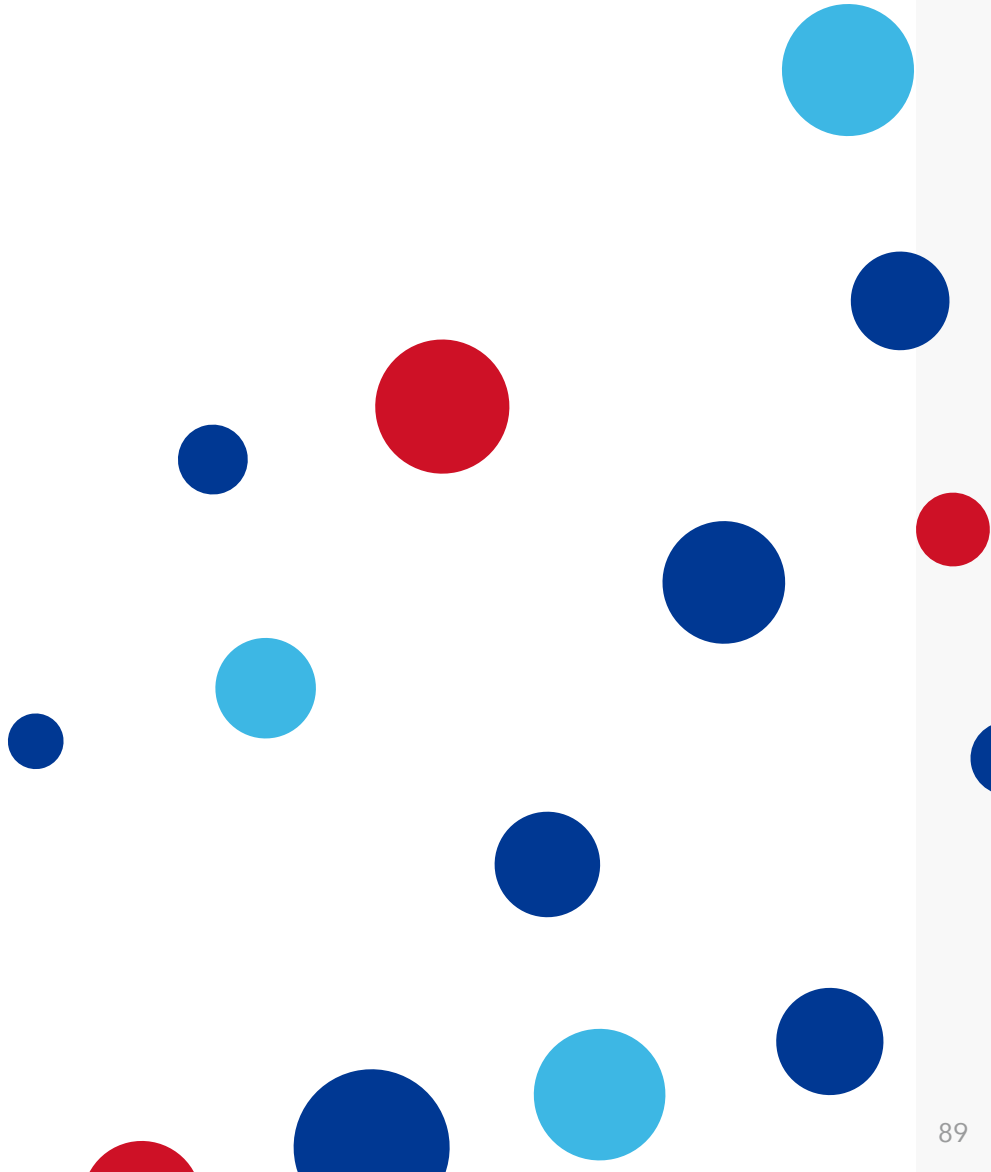
Employee structure by gender

In recruiting new employees, CZ.NIC encourages equal opportunities and the involvement of women. Among other things, it offers the possibility of working part-time, which allows employees to combine their work and parental responsibilities. As a result, the number of women in the Association is steadily increasing. Due to the structure of graduates in the technical branches of higher education institutions, however, the share of men still prevails, as in other technology companies.



Benefits

The CZ.NIC Association also offers its employees a range of benefits, such as flexible working hours, the option to work from home, extra leave, annual bonuses, a cafeteria, a meal allowance, discounts on Turris products and team-building events.



14 Selected financial indicators

14.1 Balance Sheet

	2019	2020	2021	2022	2023	2024	2025
Total assets	569,478	602,667	633,438	653,028	700,871	750,126	**800,506**
Fixed assets	89,001	80,579	75,682	81,573	75,734	69,524	**73,005**
Intangible fixed assets	1,333	931	253	845	149	53	**39**
Tangible fixed assets	87,668	79,648	75,429	80,728	75,585	69,471	**72,966**
Long-term investments	0	0	0	0	0	0	**0**
Current assets	479,202	521,033	556,449	569,256	623,231	674,300	**722,531**
Inventories	41,045	49,591	57,000	71,762	40,563	17,539	**52,380**
Receivables	10,425	14,560	24,348	34,393	19,288	48,217	**77,378**
Short-term investments	194,885	206,593	208,510	204,559	231,211	236,063	**256,436**
Cash	232,847	250,289	266,591	258,542	332,169	372,481	**336,337**
Accrual of assets	1,275	1,055	1,307	2,199	1,906	6,302	**4,970**

Total liabilities	569,478	602,667	633,438	653,028	700,871	750,126	**800,506**
Equity	358,705	382,368	403,553	415,460	451,583	484,733	**517,888**
Registered capital and capital funds	0	0	0	0	0	0	**0**
Funds from profit	172,853	193,520	217,183	236,983	249,912	285,013	**318,163**
Profit/loss of previous years	165,185	165,185	165,185	165,548	165,548	166,570	**166,570**
Profit/loss for the current fiscal period	20,667	23,663	21,185	12,929	36,123	33,150	**33,155**
External sources	68,862	72,841	79,128	82,402	92,086	98,753	**98,656**
Provisions	8,691	14,512	14,671	18,227	20,343	15,562	**14,781**
Payables	60,171	58,329	64,457	64,175	71,743	83,191	**83,875**
Accrual of liabilities	141,911	147,458	150,757	155,166	157,202	166,640	**183,962**

In CZK '000

14.2 Profit and Loss Statement

	2019	2020	2021	2022	2023	2024	2025
Revenue from the sale of products and services	193,364	207,631	220,532	231,276	231,283	237,971	**281,932**
Sales of goods	20,210	24,522	54,530	50,954	48,156	52,374	**112,081**
Other operating income	13,813	11,657	9,878	4,277	7,049	6,840	**8,558**
Production consumption	70,268	65,827	94,937	93,216	93,383	96,266	**154,041**
Change in inventories of the Association's own operations	82	256	445	341	74	12	**-399**
Own work capitalised	0	0	0	0	0	0	**0**
Personnel costs	117,380	129,418	144,066	150,897	167,653	178,687	**198,756**
Adjusting values in the operational area	17,104	14,393	12,924	12,211	11,937	11,894	**7,566**
Other operating expenses	5,005	7,663	2,865	11,338	5,340	2,159	**4,776**
Operating profit/loss	17,548	26,253	29,703	18,504	8,101	8,167	**37,831**
Interest income and similar income	1,286	920	279	4,616	11,864	12,086	**6,333**
Other financial income	30,343	24,606	43,495	70,838	120,978	67,961	**69,068**
Other financial expenses	25,590	22,578	47,976	73,855	96,773	47,008	**73,909**
Financial profit/loss	6,039	2,948	-4,202	1,599	36,069	33,039	**1,492**
Profit before tax	23,587	29,201	25,501	16,404	44,170	41,206	**39,323**
Income tax	2,920	5,538	4,316	3,475	8,047	8,056	**6,168**
Profit after tax	20,667	23,663	21,185	12,929	36,123	33,150	**33,155**

In CZK '000

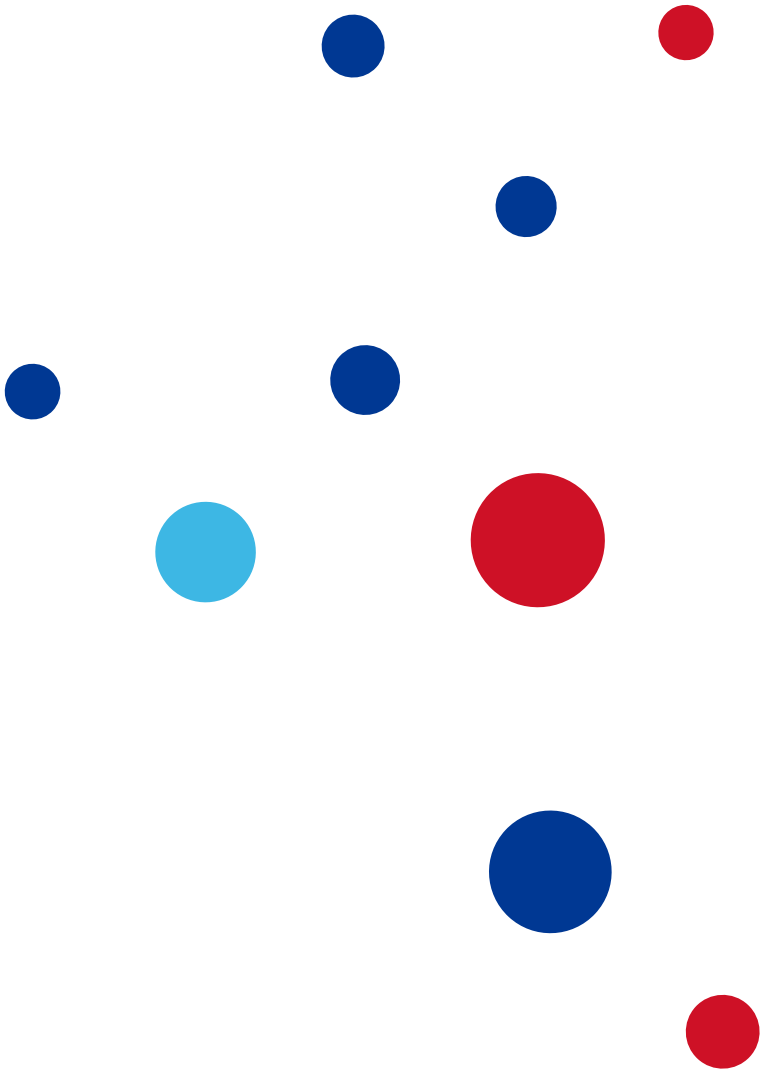
15 List of suppliers

List of suppliers according to Article 45.4 of the Statutes:

Supplier	VAT No.	Amount in CZK
Quectel Wireless Solutions Co., Ltd.		**5,137,856.00**
CODICO GmbH	ATU69769903	**26,485,876.00**
AVNET EUROPE BV	BE0464298616	**17,486,686.00**
ECOM s.r.o.	CZ15041042	**6,986,290.00**
EMKO Case a.s.	CZ25558030	**8,980,518.00**
Morelli electronics s.r.o.	CZ01565842	**10,231,511.00**

16 Events between the date of the Financial Statements and the General Meeting

No events occurred in the given time period having an impact on the data presented in the Financial Statements for 2025.



17 Auditor's Report

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

Účetní závěrka

a

Zpráva nezávislého auditora

za rok končící 31. prosince 2025

Auditor
interexpert BOHEMIA spol. s r.o.

INTEREXPERT BOHEMIA, spol. s r.o., Mikulandská 2, Praha 1, 110 00, Tel:+420 224 933 658, Fax:+420 224 934 101
e-mail: secretary@interexpert.cz www.interexpert.cz

Obsah:

Zpráva nezávislého auditora

Účetní výkazy:

- Rozvaha
- Výkaz zisku a ztráty
- Přehled o peněžních tocích
- Přehled o změnách vlastního kapitálu

Příloha účetní závěrky

Výroční zpráva ve zkrácené formě (str. 1 až 15 z celkového počtu str. 111)

Zpráva nezávislého auditora

Účetní jednotka:	**CZ.NIC, z.s.p.o.**
Sídlo:	Milešovská 1136/5, 130 00 Praha 3 - Vinohrady
Právní forma:	Zájmové sdružení právnických osob (dále jen „Sdružení“)
Identifikační číslo:	679 85 726
Rozvahový den:	31.12.2025
Účetní období:	01.01.2025 – 31.12.2025
Účel činnosti:	Sdružení zejména a) provozuje a rozvíjí doménu nejvyšší úrovně ccTLD CZ; b) provozuje a rozvíjí důvěryhodnou, bezpečnou a stabilní informační a komunikační infrastrukturu, včetně vývoje a podpory rozvoje internetových služeb, a to především prostřednictvím inovativních projektů s otevřeným zdrojovým kódem; c) šíří a podporuje výuku, vzdělávání, osvětu a diskusi o aspektech internetových technologií; d) zabývá se zvyšováním úrovně kybernetické bezpečnosti.

Výrok auditora

Provedli jsme audit přiložené účetní závěrky výše uvedené účetní jednotky sestavené na základě českých účetních předpisů, která se skládá z rozvahy k 31.12.2025, výkazu zisku a ztráty za období 01.01.2025 - 31.12.2025, přehledu o peněžních tocích, přehledu o změnách vlastního kapitálu a přílohy této účetní závěrky včetně významných (materiálních) informací o použitých účetních metodách. Údaje o účetní jednotce jsou uvedeny v příloze této účetní závěrky.

Podle našeho názoru účetní závěrka podává věrný a poctivý obraz aktiv a pasiv účetní jednotky k 31.12.2025 a nákladů a výnosů a výsledku jejího hospodaření za rok končící 31.12.2025 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 účetní jednotce 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.

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 Sdružení.

Náš výrok k účetní závěrce se k ostatním informacím nevztahuje. Přesto je však součástí našich povinností souvisejících s ověřením 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 ověřování účetní závěrky 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, jež dokážeme posoudit, uvádíme, že

- ostatní informace, které posuzují 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 o povědomí o Sdružení, k nimž jsme dospěli při provádění auditu, ostatní informace neobsahují významné (materiální) věcné nesprávnosti. V rámci uvedených postupů jsme v obdržených ostatních informací žádné významné (materiální) věcné nesprávnosti nezjistili.

Odpovědnost statutárního orgánu účetní jednotky za účetní závěrku

Představenstvo účetní jednotky 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 účetní jednotky povinno posoudit, zda je účetní jednotka schopna nepřetržitě trvat, a pokud je to relevantní, popsat v příloze účetní závěrky záležitosti týkající se jeho nepřetržitého trvání a použití předpokladu nepřetržitého trvání při sestavení účetní závěrky, s výjimkou případů, kdy představenstvo plánuje zrušení účetní jednotky 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 účetní jednotky 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 účetní jednotky 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 účetní jednotky 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 účetní jednotky nepřetržitě trvat vycházejí z důkazních informací, které jsme získali do data naší zprávy. Nicméně budoucí události nebo podmínky mohou vést k tomu, že účetní jednotka 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 a dozorčí radu 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.

INTEREXPERT BOHEMIA, spol. s r.o.
Mikulandská 2, 110 00 Praha 1
Oprávnění KA ČR č. 267

Ing. Emil Bušek, jednatel a auditor
Oprávnění KA ČR č. 1325

Datum:	02-06-2026
Podpis auditora:	

18 **Registered office and contact details**

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

Milešovská 1136/5
130 00 Praha 3

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

The Association is incorporated in the Register of Associations maintained by the Municipal Court in Prague, File No. L 58624.

CZ.NIC – 24-hour customer support

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

