

Výroční zpráva 2019

1 Profil sdružení	3	8 Laboratoře CZ.NIC	42	14 Vybrané finanční ukazatele	76
		8.1 ADAM – monitoring a analýza DNS provozu	43	14.1 Hospodářský výsledek po zdanění	77
2 Úvodní slovo předsedy představenstva	5	8.2 BIRD	44	14.2 Rozvaha	78
		8.3 Datovka	44	14.3 Výkaz zisků a ztrát	79
3 Úvodní slovo výkonného ředitele	7	8.4 Knot DNS a Knot Resolver	45	14.4 Vývoj tržeb	79
		8.5 Tablexia	45		
4 Doména .CZ	9	8.6 Turrís	46	15 Seznam dodavatelů	80
4.1 Stav a vývoj počtu registrací	10				
4.2 IDN (Internationalized domain names)	13	9 Vzdělání a osvěta	47	16 Údaje o skutečnostech mezi dnem účetní závěrky a valnou hromadou	82
4.3 Registrátoři	14	9.1 Komunikace s veřejností	48		
4.4 Zkvalitňování dat v registru	17	9.2 Popularizační seriály	49		
		9.3 Výukové středisko Akademie CZ.NIC	49	17 Zpráva auditora	84
5 Infrastruktura	20	9.4 Konference	51		
5.1 Datová centra	21	9.5 Edice CZ.NIC	52	18 Sídlo a kontaktní údaje	87
5.2 Technické řešení správy domén	23				
5.3 Podpora internetové infrastruktury	28	10 Spolupráce a partnerství	54		
5.4 Podpora základní infrastruktury Internetu	31	10.1 Česká republika	55		
		10.2 Zahraničí	57		
6 Bezpečnostní tým CSIRT	32				
6.1 CSIRT.CZ – Národní CERT tým České republiky	33	11 Grantové projekty	60		
6.2 CZ.NIC-CSIRT	37	11.1 Zapojení do projektů evropské spolupráce	61		
		11.2 Zapojení do národních a dalších projektů	63		
7 MojeID	38	12 Struktura sdružení	65		
7.1 Podpora mojeID	39	12.1 Členská základna	66		
7.2 Externí validační místa	40	12.2 Orgány sdružení	70		
7.3 Uživatelé mojeID	40				
7.4 MojeID jako nástroj pro přeshraniční autentizaci v Evropě	41	13 Lidské zdroje	73		
		13.1 Stav a vývoj počtu zaměstnanců	74		
		13.2 Struktura zaměstnanců	75		

1 Profil sdružení

CZ.NIC je zájmové sdružení právnických osob, otevřený a nezávislý subjekt, jehož hlavní činnost představuje správa a zabezpečení provozu registru národní domény nejvyšší úrovně .CZ. Velký význam mají aktivity sdružení v oblasti bezpečnosti, a to jak prostřednictvím Národního bezpečnostního týmu CSIRT.CZ, tak prostřednictvím bezpečnostních projektů, zejména ekosystému výkonného routeru Turris Omnia či modulárního routeru Turris MOX.

Vedle těchto činností se sdružení věnuje výzkumu, vývoji a osvětě v oblasti Internetu, internetových protokolů, síťového provozu a nových technologií obecně. Sdružení CZ.NIC mezi své dlouhodobé cíle řadí podporu a rozvoj internetové komunity jak v České republice, tak v zahraničí.

Sdružení CZ.NIC vzniklo v květnu roku 1998 a hlavním důvodem jeho založení byl růst významu sítě Internet a tím i počtu jeho uživatelů a zájemců o registraci jmen domén v ccTLD .CZ. Ke konci roku 2019 mělo sdružení 116 členů rozdělených do tří komor.

V současnosti představuje sdružení stabilní a důvěryhodný subjekt, který je schopen zajistit spolehlivý chod české národní domény .CZ. Od roku 2013 je sdružení CZ.NIC držitelem certifikace ISO 27001, potvrzující bezpečné nakládání s informacemi včetně nastavení odpovídajících pravidel a postupů.

Pro držitele jmen domén, registrátory, ale i ostatní subjekty využívající Internet při práci i ve volném čase je sdružení spolehlivým partnerem, který nezabezpečuje pouze správu jmen domén, ale rovněž dbá o bezpečnost Internetu a zapojuje se do společensky prospěšných aktivit – ať již v podobě projektů Laboratoří CZ.NIC nebo osvěty.



2 Úvodní slovo předsedy představenstva

Vážené dámy, vážení pánové,

je mi ctí uvést výroční zprávu našeho sdružení za rok 2019.

Podařilo se nám splnit finanční plán i velmi náročný interní plán činností. Jsem hrdý na to, že stejně jako v uplynulých letech česká národní internetová doména i ostatní naše služby fungovaly spolehlivě a dobře sloužily svým uživatelům.

Důležitou událostí uplynulého roku bylo projednání a schválení koncepce sdružení do roku 2024. V jejím úvodu jsme si stanovili, že naším posláním zůstává provozování a rozvoj internetové infrastruktury a obecně prospěšných služeb, zejména domény .CZ, ku prospěchu lokální komunity. Chceme podporovat rozvoj těchto služeb pomocí inovativních projektů, posilovat informovanost o aspektech internetových technologií a zvyšovat úroveň kybernetické bezpečnosti.

Zvýšení velkoobchodní ceny za roční vedení záznamu o jménu domény nemělo zřejmě žádný podstatný vliv na počet registrací. Meziroční růst byl asi půl procenta, což koresponduje s dlouhodobým trendem. Ani na počtu uzavřených registrátorských smluv se tato změna nijak neprojevila, počet registrátorů je stabilně nad čtyřiceti.

Hlavní činností našeho sdružení je správa národní internetové domény. Tato zodpovědnost se projevila mimo jiné tím, že Národní bezpečnostní úřad naše sdružení určil jako provozovatele základní služby podle Zákona o kybernetické bezpečnosti. Již poněkolkáté jsme uspořádali průzkum ohledně zájmu o zavedení možnosti registrace doménových jmen s národními znaky (IDN). Individuální uživatelé ani komerční organizace tomu nejsou nakloněny.

Kromě správy národní domény realizujeme další významné projekty. Zmínil bych alespoň provoz Národního CSIRTu České republiky, vývoj infrastruktury bezpečných routerů Turriss, edukaci v oblasti kybernetické bezpečnosti (např. spolupráce na úspěšném filmu V síti), vývoj světově významně rozšířeného routovacího démonu Bird, autentizační technologii MojelD, vývoj úspěšného autoritativního DNS serveru Knot, pořádání seminářů a konferencí (např. IETF 104). Na mnoho dalších projektů, zejména v oblasti kybernetické bezpečnosti, se nám podařilo získat financování formou grantů a dotací (např. projekty PROKI, Safer Internet, CyberExchange, CEF, Safer Internet nebo NetMetr).

Jsem rád, že se jako předseda statutárního orgánu mohu ohlédnout za výbornými výsledky organizace. Děkuji za to všem našim lidem, a to nejen za obrovský kus práce pro sdružení v uplynulém roce, ale i za výjimečné nasazení, které projevili při zvládnutí mimořádné situace vyvolané letošními virovými pandemiemi. Podařilo se nám nejen bezvadně udržet v chodu naši infrastrukturu a služby, ale i pomáhat ostatním organizacím a jednotlivcům.

Zásadní informace o sdružení a jeho činnosti v uplynulém roce jsou Vám k dispozici na dalších stranách této výroční zprávy. Pevně věřím, že budeme úspěšně pokračovat v našem poslání a budeme Vám nadále spolehlivým a transparentním partnerem.

RNDr. Karel Taft, MBA - předseda představenstva



3 Úvodní slovo výkonného ředitele

Vážené dámy, vážení pánové,

rok 2019 byl rokem, kdy se již ani nečekalo, že se opět zvýší počet registrovaných domén. Nárůst o necelých 7 tisíc domén není nic významného, ale jde o pozitivní zprávu, že ještě pořád lze nacházet zajímavé domény s koncovkou .CZ.

V roce 2019 jsme pochopitelně pilně pracovali na zvýšení kvality a zabezpečení našeho registračního systému. Proto jsme vybudovali v Žižkovské televizní věži v Praze zcela nový privátní sál a přesunuli tam veškerou technologii, která byla dosud ve společném sále. Pracovali jsme pochopitelně i na zkvalitnění našeho DNS anycastu. Pro zlepšení pokrytí v Latinské Americe jsme otevřeli nový uzel v Brazílii a přihlásil se nám další zájemce o ISP stack, konkrétně společnost CESNET.

Zvyšoval se i podíl nasazení technologie DNSSEC. Už z kraje roku ohlásil registrátor Seonet Multimedia, že zavádí DNSSEC pro všechny spravované domény. Použil již nedávno implementovaný systém automatické správy, který nevyžaduje EPP interakci s registrem. Nejen díky této události, bylo na konci roku podepsáno přes 59 % všech domén v registru, což je v mezinárodním srovnání skutečně vysoké číslo. Tím ovšem výčet novinek ze světa DNS nekončí. Na našich otevřených resolversch (ODVR) jsme zavedli podporu technologií DNS over TLS a DNS over HTTPS. Bude zajímavé sledovat, zdali se tento trend šifrování DNS provozu uchytí.

Velkým rozvojem procházela i služba mojID. Pro zvýšení bezpečnosti přihlašování jsme zavedli podporu autentizačního standardu FIDO2. Jako druhý faktor k heslu má tedy uživatel na výběr mezi OTP, aplikací mojID Autentikátor a právě hardwarovým prostředkem podporujícím FIDO2.

Další novinkou bylo zavedení možnosti validace účtů pomocí sítě pro asistenci výkonu veřejné správy CzechPOINT. S ohledem na množství kontaktních míst tohoto systému je již validace skutečně dostupná pro všechny občany České republiky. Tyto změny pochopitelně sledují jasný cíl, a tím je propojení mojID se systémy státní správy, konkrétně s Národní identifikační autoritou (NIA). Právě toto propojení bude hlavním cílem projektu mojID v roce 2020.

Další zajímavý projekt se rýsuje v oblasti bezpečnosti. Námi provozovaný národní bezpečnostní tým CSIRT.CZ pracoval na spuštění nové služby pro veřejnost. Jde o nabídku penetračních testů. V roce 2019 proběhl úspěšný pilotní test této služby s Krajem Vysočina. Věřím, že v dalším roce této služby využijí i další zákazníci.

Očekávanou novinku ohlásil i další projekt, který je zaměřen na bezpečnost – projekt Turrus. Do poloviny roku se podařilo rozeslat všechny routery, které si přispěvatelé objednali v crowdfundingové kampani, a zahájili jsme volný komerční prodej.

I v roce 2019 jsme investovali nemalé úsilí do osvěty. Pokračovali jsme v zaměření na mladé uživatele Internetu. Vyprodukovali jsme film Maturant, který byl představen na filmovém festivalu pro děti a mládež ve Zlíně. Film je volně ke stažení k nekomerčnímu užití. A druhým počinem v této oblasti byl seriál Marty is dead, který zvítězil na festivalu Serial Killer.

Na závěr bych rád zmínil ještě jednu důležitou věc. V roce 2019 končila platnost stávající koncepce činnosti sdružení a proto byla připravena a následně schválena [nová koncepce](#) pro období 2020 až 2024.

Pevně věřím, že z mé předmluvy je zřejmé, že i rok 2019 lze pokládat za úspěšný, a velice rád bych za to chtěl poděkovat mým kolegům. Přeji Vám příjemné čtení této výroční zprávy.

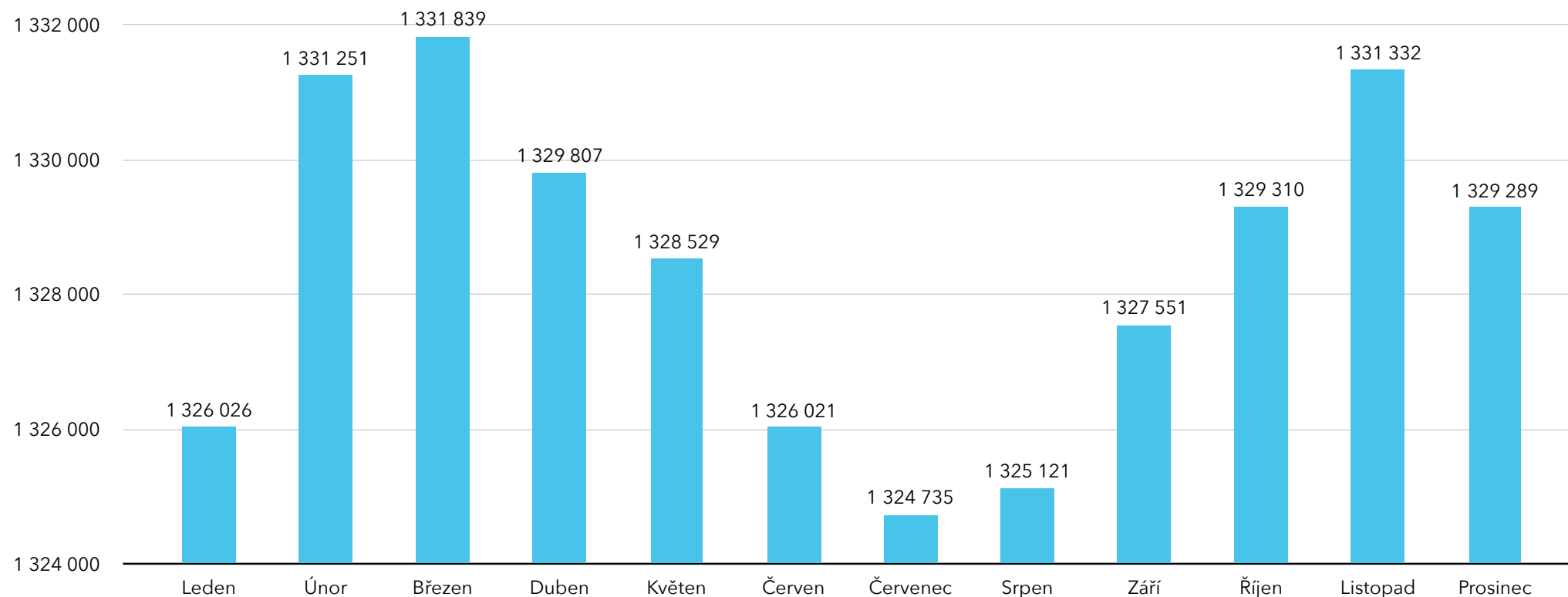
Mgr. Ondřej Filip, MBA - výkonný ředitel

4 Doména .CZ

4.1 Stav a vývoj počtu registrací

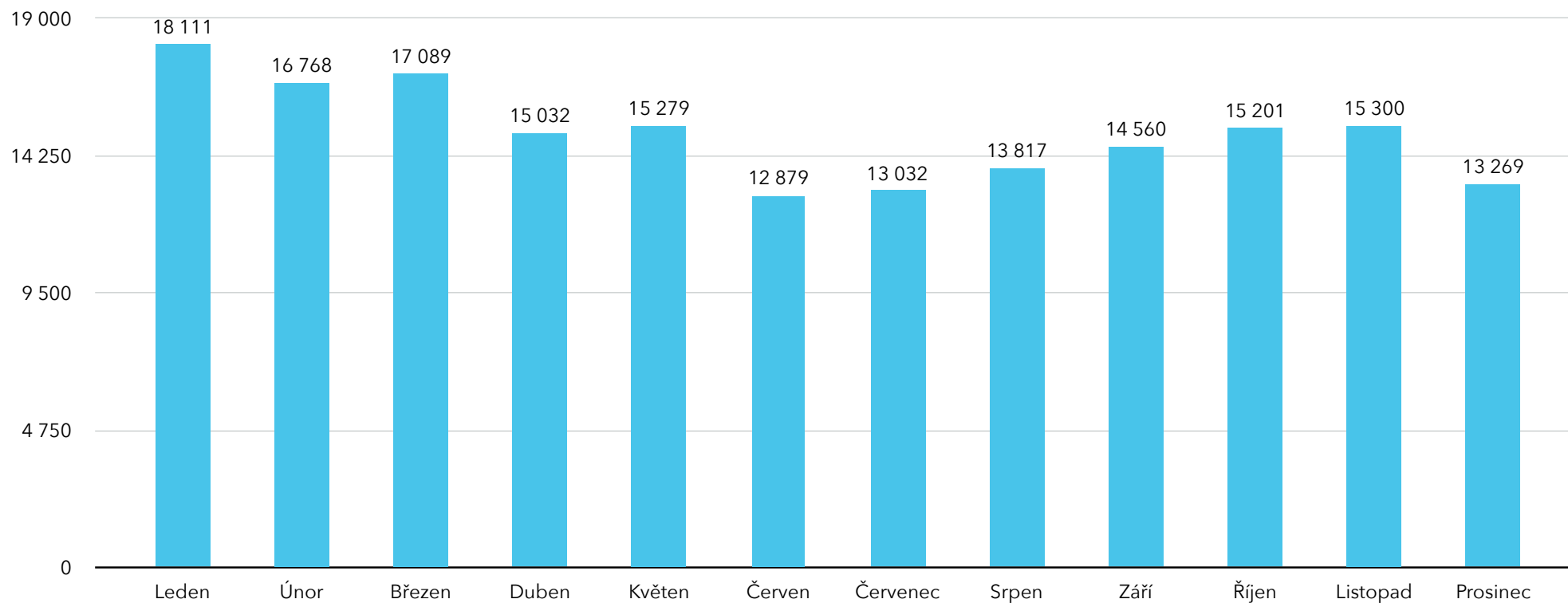
V průběhu roku 2019 se celkový počet domén v zóně .CZ zvýšil o 6 689, což představuje asi 0,5% nárůst. Česká národní doména .CZ tak odráží trend, který zažívají prakticky všechny národní registry, a to klesající tempo registrací národních domén (ccTLD), které je způsobeno především nasycením trhu a částečně též novými alternativami pro registraci jména domény v podobě tzv. nových generických domén (new gTLD).

Celkový počet registrovaných jmen domén .CZ v roce 2019

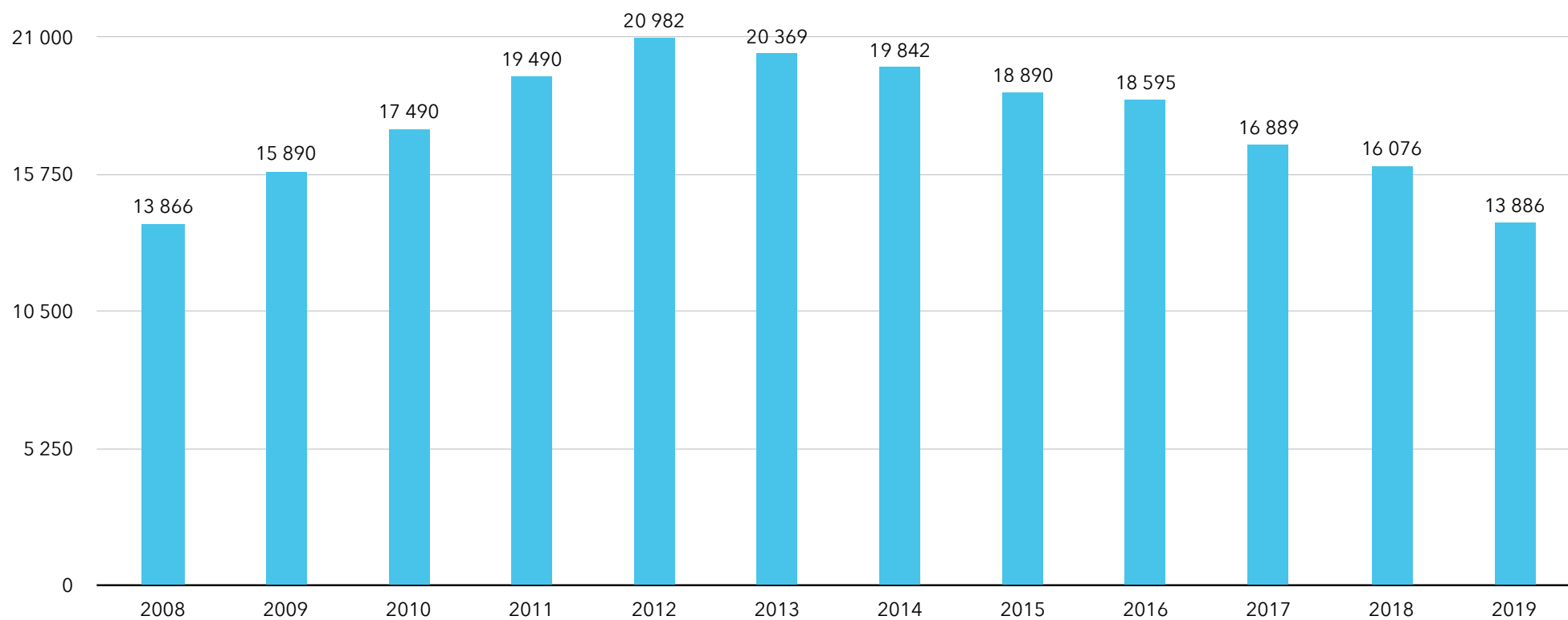


V roce 2019 bylo každý měsíc zaregistrováno průměrně 13 886 nových jmen domén. Mírné snížení průměrného počtu registrací odráželo, podobně jako v minulém období, trend celkového přírůstku nových domén. Následující grafy zobrazují počet nových registrací v roce 2019 po měsících a vývoj průměrného počtu nových registrací od roku 2008.

Počet nově registrovaných jmen domén .CZ v roce 2019



Nové registrace 2008-2019 (průměr za měsíc)

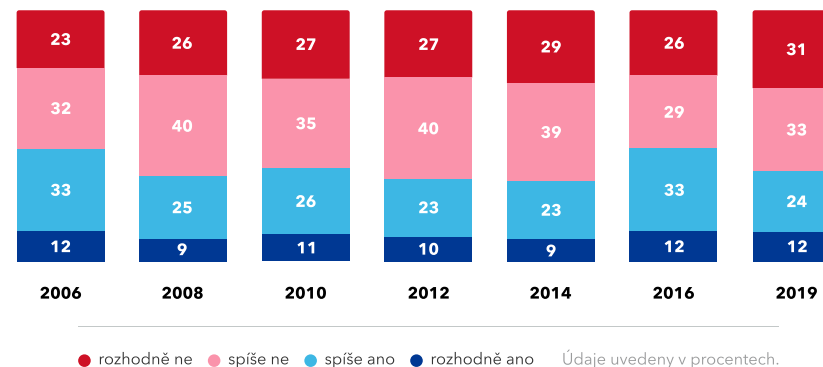


4.2 IDN (Internationalized domain names)

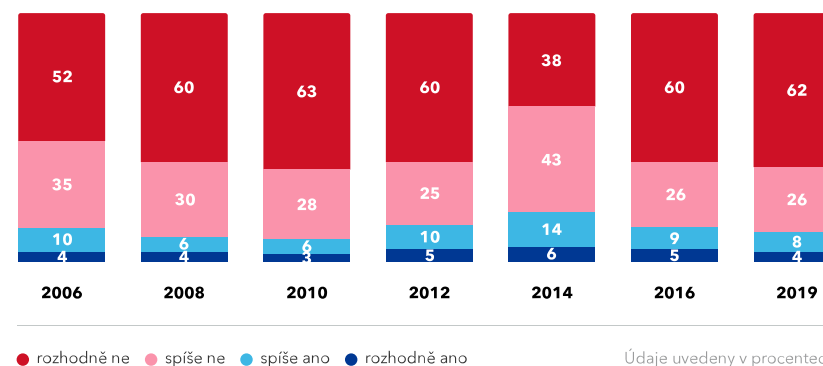
IDN je systém, díky němuž mohou doménová jména obsahovat znaky národních abeced. V České republice by to tedy znamenalo, že by domény .CZ mohly obsahovat znaky s českou diakritikou, tedy s háčky a čárkami.

Sdružení CZ.NIC je na případné zavedení IDN do naší národní domény technicky připraveno, IDN však pro domény .CZ dosud nezavedlo, protože komunita uživatelů Internetu v České republice zatím o zavedení IDN nejeví zájem. CZ.NIC pořádá opakovaně jednou za dva až tři roky průzkum veřejného mínění, kde zájem uživatelů zjišťuje. Na podzim roku 2019 se proti zavedení systému IDN vyjádřilo 88 procent respondentů z řad organizací a 64 procent oslovených běžných uživatelů Internetu. V prvním případě jde o nárůst o dva procentní body oproti poslednímu dotazování v roce 2016, v tom druhém je údaj vyšší o devět procentních bodů. Průzkumu se zúčastnilo celkem 1015 zástupců organizací a 1206 individuálních uživatelů.

JEDNOTLIVCI



ORGANIZACE



4.3 Registrátoři

Systém správy domén .CZ je založen na tzv. distribuovaném principu, kdy registraci jména domény provádějí smluvní partneři sdružení CZ.NIC – registrátoři. CZ.NIC vůči nim vystupuje podobně jako velkoobchodní partner, zároveň však zajišťuje technickou stránku fungování domény nejvyššího řádu .CZ.

V roce 2019 smlouvu ukončili registrátoři Sonexo B.V. (k 30. 6. 2019) a Economia, a. s. (k 31. 12. 2019), ke konci roku společnost GENERAL REGISTRY zanikla fúzí s INTERNET CZ, a. s.

Novými registrátory k 1. 1. 2019 se staly společnosti NAMESHIELD SAS (Francie) a Focus IP, Inc (USA).

Na konci roku 2019 tedy mělo Smlouvu o spolupráci při registraci domén se sdružením uzavřeno celkem 43 společností, z toho 27 tuzemských a 16 zahraničních. Tento počet nabízí široké možnosti volby pro koncového zákazníka a rovněž zajišťuje dostatečnou hospodářskou soutěž.

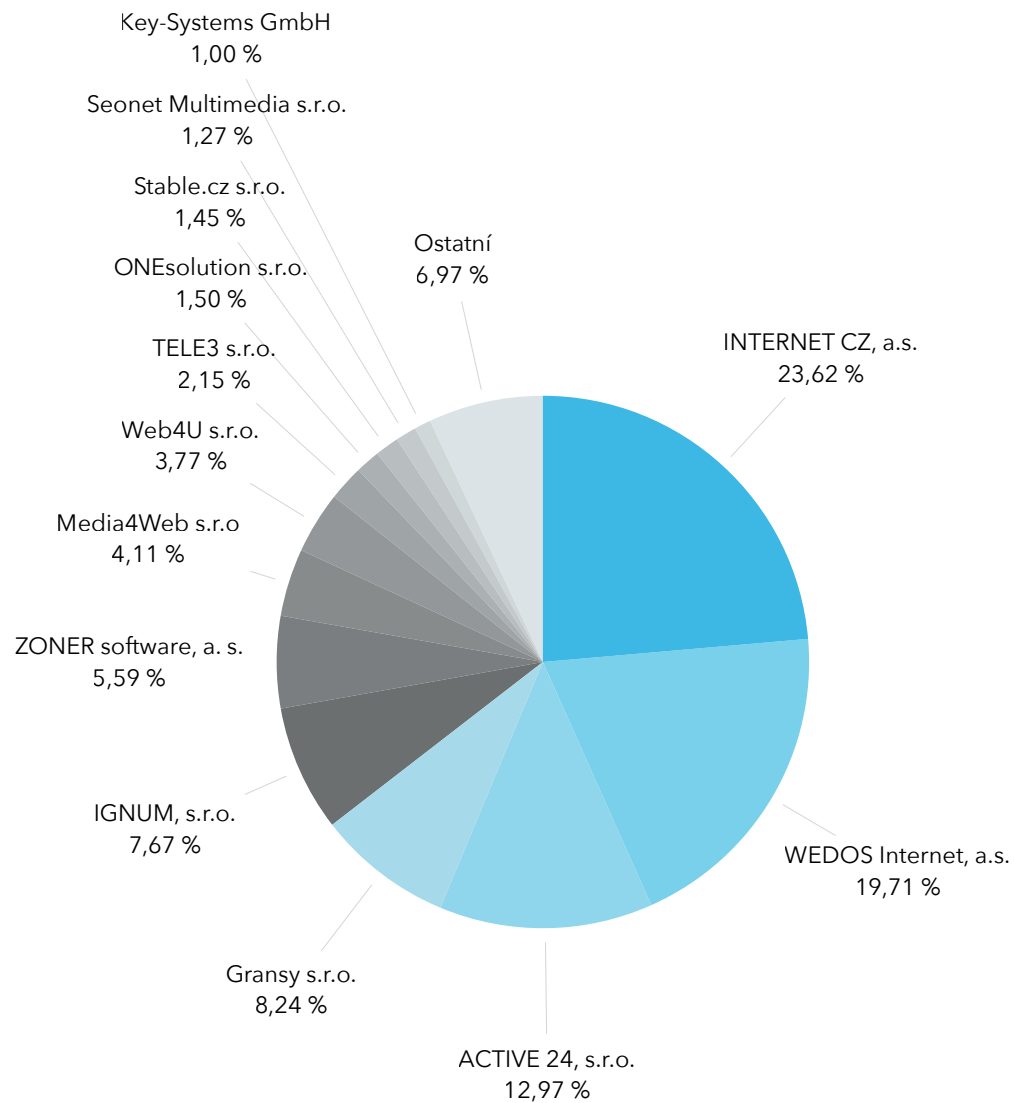
4.3.1 Přehled registrátorů jmen domén .CZ

Seznam všech akreditovaných registrátorů k 31. 12. 2019

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

4.3.2 Nejvýznamnější registrátoři jmen domén

Nejvýznamnějším registrátorem dle počtu spravovaných domén byla stejně jako v loňském roce společnost INTERNET.CZ, a. s., následovaná WEDOS Internet, a. s., ACTIVE 24, s. r. o., Gransy s. r. o. a IGNUM, s. r. o. Přehled registrátorů s tržním podílem nad 1 % je znázorněn v následujícím grafu.



4.3.3 Certifikace registrátorů

Projekt certifikace, který byl spuštěn již v polovině roku 2011, má za cíl usnadnit koncovým uživatelům (tedy jak zájemcům o novou registraci, tak i stávajícím držitelům jmen domén) orientaci ve vysokém počtu registrátorů, a to především z pohledu portfolia a kvality služeb, které nabízejí. Metodika certifikace byla vypracována ve spolupráci s registrátory a Asociací pro elektronickou komerci (APEK).

Registrátoři, kteří mají zájem se programu účastnit, mohou vždy na jeden rok získat logo „certifikovaný registrátor“. Z počátečních 9 registrátorů zapojených do dobrovolné certifikace v roce 2011 jejich počet stoupl na 12. Z pohledu koncového zákazníka je potěšující především neustále se zlepšující kvalita nabízených služeb. Na konci roku 2019 splňovalo nejnáročnější kritéria pro udělení pěti hvězdiček 9 registrátorů. Mezi certifikovanými registrátory se již zároveň nevyskytuje žádný, který by měl pouze tři hvězdičky. Kvalita služeb registrátorů promítnutá do počtu udělených hvězdiček je znázorněna v následující tabulce.

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

4.3.4 Spolupráce s registrátory - co-marketingový program

Zájmem sdružení CZ.NIC je, v souladu s jeho hlavní činností a dlouhodobým cílem, propagovat a podporovat registraci domén pod doménou nejvyšší úrovně .CZ. Vzhledem k distribuovanému způsobu správy národní domény má však sdružení CZ.NIC omezené možnosti, jak oslovit potenciální držitele jmen domén přímo cílenou marketingovou akcí.

Tato skutečnost stála u zrodu tzv. co-marketingového programu, v rámci kterého CZ.NIC přispívá registrátorům v případě splnění předepsaných podmínek na realizaci komunikačních kampaní zaměřených na podporu registrací jmen domén v ccTLD .CZ. Výše příspěvku CZ.NIC je závislá na velikosti registrátora (na počtu registrací a prodloužení jmen domén), objemu kampaně a splnění dalších faktorů, jako je využívání mojeID či zabezpečení domén prostřednictvím DNSSEC, kterými se CZ.NIC snaží registrátory motivovat k rozšiřování těchto technologií.

Oblíbenost co-marketingového programu, díky kterému je česká národní doména .CZ mezi uživateli populární a dobře a často viditelná např. na venkovních reklamních plochách, je stále vysoká, a to jak z pohledu počtu zapojených registrátorů, tak objemu využitých finančních prostředků. V roce 2019 se programu účastnilo 14 registrátorů, kterým sdružení CZ.NIC vyplatilo celkem 10 200 000 Kč.

4.4 Zkvalitňování dat v registru

Zkvalitňování dat vedených v registru držitelů jmen domén pokračovalo i v roce 2019, kdy se sdružení CZ.NIC stejně jako v roce předešlém zaměřilo jak na slučování vícenásobných duplicitních kontaktů, které se v databázi v průběhu let nashromáždily, tak i na ověřování dat uživatelů za účelem zvýšení jejich bezpečnosti, správnosti, a tedy i snadnějšího kontaktování ze strany sdružení například v okamžiku, kdy hrozí zrušení jména domény z důvodu neuhrazení poplatku za prodloužení registrace. K aktualizaci a ověření svých údajů byli držitelé jmen domén motivováni získáním drobné odměny ve formě propagačního předmětu sdružení CZ.NIC a možností obdržet hodnotnější ceny.

4.4.1 Řešení sporů o jména domén v ccTLD .CZ

Průměrná doba trvání soudního sporu u obecného soudu činí zhruba 3 roky, a to jen pokud nenastanou nějaké komplikace. Sdružení se proto snažilo pro řešení sporů o jména domén najít alternativní možnost, jak spory řešit, a to takovou, která bude rychlá, stabilní a zároveň důvěryhodná. Proto již od léta 2004 fungoval systém alternativního řešení sporů (ADR). Ten měl až do roku 2015 podobu rozhodčího řízení, kdy bylo možné spor týkající se jména domény proti jeho držiteli vést u Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky. Za desetileté trvání tohoto alternativního

způsobu řešení sporů byla Rozhodčím soudem projednávána více než stovka sporů.

Na základě rozhodnutí Nejvyššího soudu z konce roku 2013 však došlo ke změně a od března 2015 byl zaveden nový způsob ADR, jehož základní principy jsou shodné s těmi, které byly a nadále jsou úspěšně využívány v případech sporů o generické TLD (UDRP) či o jména domén registrovaná v doméně nejvyšší úrovně .EU. Platforma, kde spory probíhají, je na základě uzavřeného memoranda stále spravována důvěryhodným subjektem. Tím je Rozhodčí soud při Hospodářské komoře České republiky a Agrární komoře České republiky, což je jeden ze tří stálých rozhodčích soudů, které v České republice existují. Tento stálý rozhodčí soud požívá značné autority, přičemž nespornou výhodou, zejména v případě sporů o jména domén, je skutečnost, že jako jeden z mála nabízí řízení on-line.

Systém ADR užívaný od roku 2015 však není rozhodčím řízením ve smyslu zákona o rozhodčím řízení, čemuž odpovídá také používaná terminologie. Je založen na smluvním ujednání a je v něm možné nárokovat si pouze převod jména domény či jeho zrušení, nikoliv další nároky, např. náhradu škody. Vydané rozhodnutí není exekučním titulem pro výkon rozhodnutí, probíhající spor v novém systému ADR nepředstavuje překážku litispendence (tedy probíhajícího řízení ve stejné věci) a spor ukončený nepředstavuje překážku věci rozhodnuté. S těmiž nároky se tedy lze v průběhu řízení či po jeho ukončení obrátit na obecný soud.

Rok 2015, kdy bylo nové ADR zavedeno, byl z hlediska užívání velmi opatrný, ale následující roky ukazují, že byl tento způsob řešení sporů akceptován.

Rok	Počet sporů zahájených v systému ADR
2015	7
2016	20
2017	22
2018	22
2019	29

Z obecných soudů rozhoduje spory o jména domén nejčastěji Městský soud v Praze, a to především s ohledem na skutečnost že je specializovaným soudem mj. pro spory ve věcech hospodářské soutěže a duševního vlastnictví, což jsou v případě tzv. doménových sporů nejčastěji porušovaná práva.

Kromě standardních e-mailů, které jsou zákazníkům zasílány automatizovaně systémem registrace domén, a které upozorňují zejména na neuhrazení poplatku za prodloužení registrace na další období, bylo naší zákaznickou podporou například manuálně zkontrolováno více než 250 000 domén před vyřazením nebo bylo kontaktováno telefonicky (od této činnosti bylo na konci roku 2017 ustoupeno) či prostřednictvím SMS (služba zavedena postupně v druhé polovině roku 2017) téměř 130 000 držitelů, kterým hrozilo zrušení jména domény.

4.4.2 Zákaznická podpora

Nedílnou součástí zabezpečení provozu domény .CZ představuje zákaznická podpora, která funguje v nepřetržitém režimu 24/7. Cílem zákaznické podpory je především zajištění maximální péče o držitele jmen domén, a to zejména v situaci, kdy by mělo dojít ke zrušení jména domény, případně kdy dochází ke změně kontaktu či převodu jména domény. Nedílnou součástí zákaznické podpory je rovněž asistence uživatelům služby mojID a jejich validace.

Ve vztahu k držitelům jmen domén je zákaznická podpora založena na proaktivním přístupu, jehož cílem je vyloučit možné vyřazení jména domény a její propadnutí například z důvodu zastaralého kontaktu nebo opomenutí platby. Vzhledem k distribuovanému systému správy domény .CZ představuje zákaznická podpora jediný případ, kdy je sdružení CZ.NIC v přímém kontaktu s držiteli jmen domén.

Vývoj jednotlivých úkonů přepočtený na měsíční průměr je znázorněn v tabulce.

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Manuální kontrola jmen domén před vyřazením	-	8 916	15 176	18 586	21 598	20 512	20 894	21 834	21 437	20 867
Manuální kontrola jmen domén před zrušením	-	4 314	11 061	14 378	16 666	16 041	16 529	16 864	17 000	16 869
Obvolané kontakty jmen domén ke zrušení	4 263	4 314	4 767	6 690	7 808	7 367	7 826	7 573	790	904
SMS - informace o blížícím se zrušení jména domény	-	-	-	-	-	-	-	8 139*1	8 948	9 859
E-maily odesílané před vyřazením	1 201	1 429	1 708	1 716	1 915	1 718	1 849	3 157	2 826	3 036
Reakce na e-mailové dotazy	828	1 240	1 746	1 945	2 782	3 015	2 074	2 319	2 080	2 802
Reakce na telefonické dotazy	561	1 063	1 120	1 242	1 416	1 262	1 227	994	774	702
Žádosti (validace, blokace...)	145	180	248	315	455	405	701	776	559	363
Dotazy na chatu	-	-	-	-	-	166*2	132	114	168	262
Manuální kontrola správnosti údajů	-	-	-	-	1073*3	875	953	1372	1628	1170

Údaje představují průměrný počet daných úkonů za měsíc

*1 měsíční průměr odeslaných SMS v druhé polovině roku 2017

*2 měsíční průměr od dubna 2015, kdy byla tato služba spuštěna

*3 měsíční průměr od července 2014, kdy byla zavedena praxe manuální kontroly údajů

5 Infrastruktura

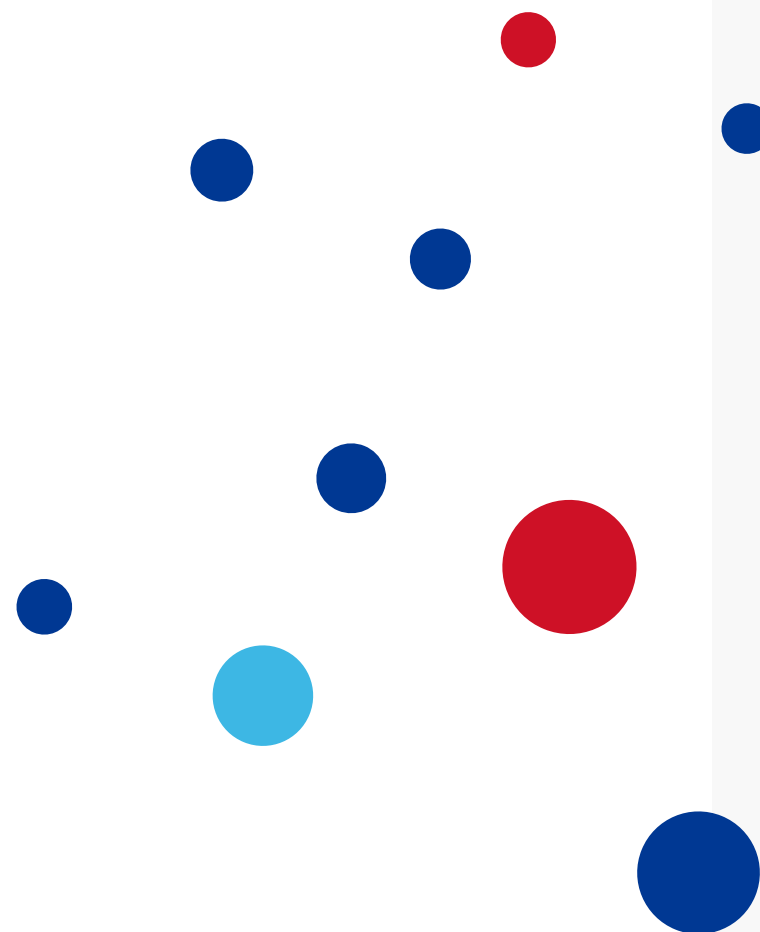
5.1 Datová centra

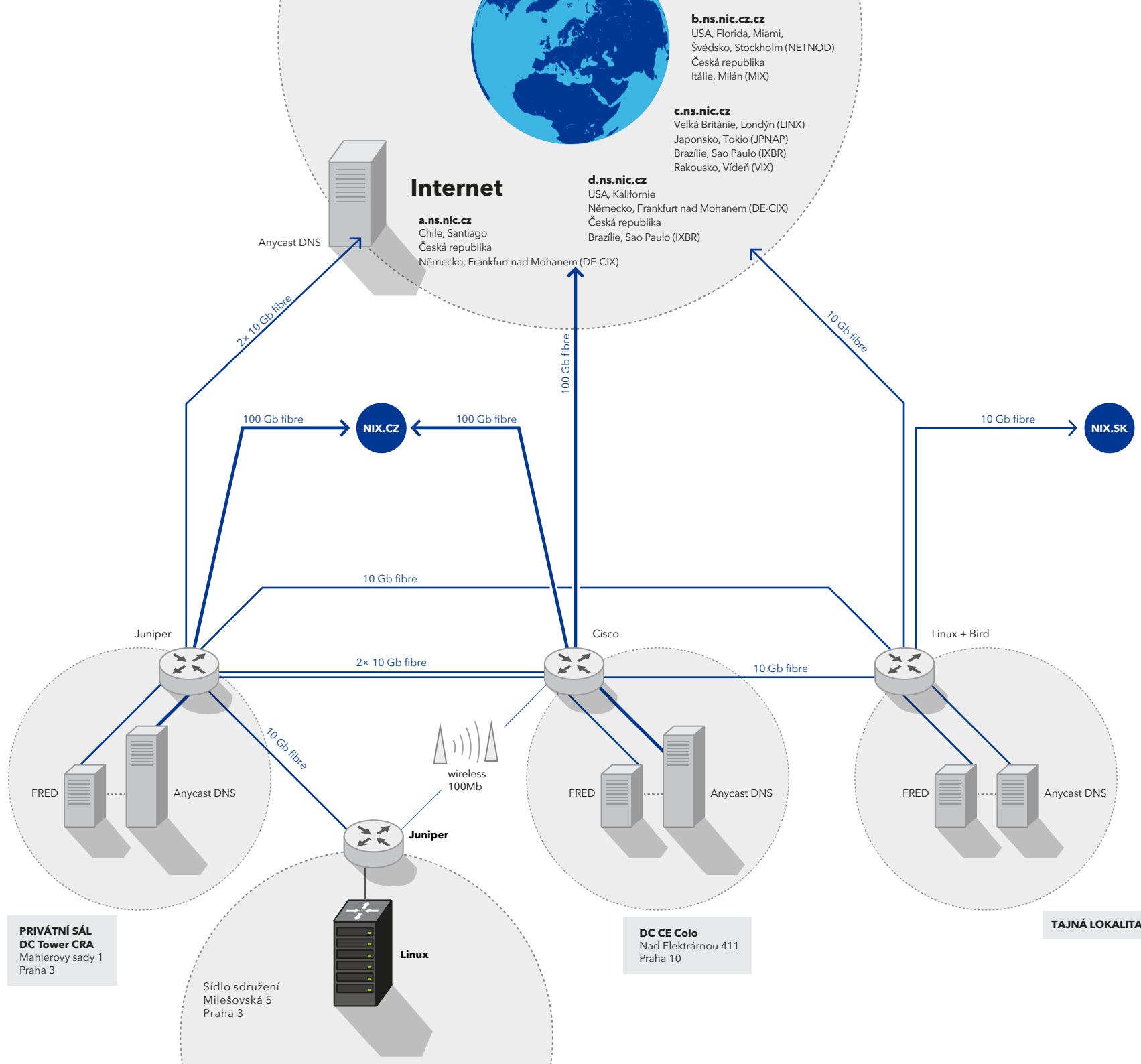
Systém centrálního registru DSDng byl navržen jako plně redundantní. Veškerý hardware i software je umístěn ve třech vzájemně nezávislých lokalitách:

- datovém centru TOWER Českých Radiokomunikací v Praze 3,
- datovém centru CE Colo v Praze 10,
- neveřejné mimopražské lokalitě.

Všechny lokality mají svoje vlastní připojení k síti Internet, ale i k elektrické rozvodné síti. Datové Centrum DC TOWER je do rozvodné sítě připojeno ze tří nezávislých trafostanic, datové centrum CE Colo a mimopražská lokalita pak ze dvou. Ve všech datových centrech je dostupné zálohované napájení pomocí UPS a krytí případných delších výpadků elektrického proudu pomocí dieselových generátorů.

V roce 2019 sdružení vybuodovalo privátní datový sál v DC TOWER Českých Radiokomunikací a přesunulo do něj veškerý provoz z této lokality. Tímto krokem došlo ke zvýšení fyzické bezpečnosti, navýšení kapacity a celkové modernizaci této části infrastruktury. Zároveň se sdružení podařilo udržet v této lokalitě stejné provozní náklady, a to jak v průběhu stěhování, ale i v dalším provozu. Sdružení stěhování využilo pro významné upgrady síťové infrastruktury. O přípravách a samotném stěhování sdružení detailně informovalo pomocí [série příspěvků](#) na svém blogu a v rámci prezentace na konferenci Internet a technologie 19 (IT19) v listopadu 2019.





5.2 Technické řešení správy domén

Infrastruktura registru pečlivě dodržuje pravidla diverzity hardwarového vybavení, aby případná chyba konkrétního výrobce hardwaru ovlivnila pouze část infrastruktury a minimalizovala tak možnost výpadku centrálního registru jako celku. V každé lokalitě jsou proto umístěny technologie různých výrobců. Stejný přístup je využit i pro software autoritativních DNS (Domain Name System – systém doménových jmen), který provozujeme na třech odlišných systémech (KNOT, Bind a NSD).

Samotný software centrálního registru je navržen tak, aby bylo možné kdykoliv vyměnit libovolnou součást architektury za její kopii běžící na serveru v dalších lokalitách. Kritickou součástí je pak databáze PostgreSQL, která je v běžném provozu replikována do obou dalších lokalit, a v případě výpadku primární lokality lze provoz převést na replikovanou databázi bez jakéhokoliv omezení či dopadu na funkčnost. Záložní systémy jsou navrženy a provozovány tak, aby byly schopny v případě výpadku jakékoliv komponenty ve velmi krátké době převzít provoz registru.

Systém centrálního registru je připraven pro provoz na IPv4 i IPv6 a jeho současná implementace pro doménu .CZ (stejně jako všechny DNS servery) je provozována na obou těchto protokolech.

V roce 2019 byla nasazena do provozu nová webová aplikace (FERDA) pro administraci dat v registru, která do budoucna zvýší efektivitu práce helpdesku a bude atraktivní součástí systému FRED i pro uživatele v zahraničí. Tato nová webová aplikace s sebou přinesla celou sadu

technologických inovací, které budou postupně rozšiřovány v dalších modulech systému FRED. Využíván je např. framework gRPC pro vzdálené volání procedur, který nahrazuje použití rozhraní CORBA, JavaScriptový framework Vue.js a další moderní JavaScriptové nástroje, jako Webpack nebo Babel. Vyhledávání částečných shod bylo optimalizováno použitím databázových trigramových indexů.

Chování systému registru bylo i v roce 2019 upravováno také podle požadavků registrátorů. Byla implementována možnost měsíční fakturace poměrné části poplatku za připojení do registru (roční perioda je i nadále možná), byl vyvinut a v provozu otestován nástroj pro slučování registrátorů a dále bylo zavedeno informování o změně údajů kontaktu pro všechny určené registrátory domén, na které je takový kontakt navázaný.

Změna legislativy si v průběhu roku 2019 vyžádala změnu způsobu výpočtu DPH. Sdružení také optimalizovalo proces rušení domén v případě kontaktů s nesprávnými údaji mimo EU a upravilo proces administrativních blokad jmen domén a kontaktů v případě soudních sporů, trestních a exekučních řízení a podobně. V testovacím prostředí došlo k automatizaci přípravy anonymizovaných dat, zavedení monitoringu testovacích prostředí včetně periodické kontroly verzí softwarových balíčků a k vylepšení smoketestů (tedy základních testovacích scénářů).

Silnou stránkou systému FRED je jeho [technická dokumentace](#). V roce 2019 došlo k jejímu dalšímu rozšíření. Byl popsán postup pro úpravy šablon webového whoisu a šablon PDF dokumentů. Pro administrátory byly zhotoveny manuálové (man) stránky pro nástroje příkazové řádky (fred-admin) a připraven základ technické a implementační dokumentace k novému webovému rozhraní FERDA.

5.2.1 FRED (Free Registry for ENUM and Domains)

Software pro centrální registr vyvinutý a provozovaný sdružením CZ.NIC byl v rámci podpory menších registrů uvolněn jako otevřený a svobodný. V roce 2019 byly licence systému FRED převedeny na GNU GPLv3+. Menší a začínající registry tak mají šanci provozovat svoji doménu na systému, který byl vyvinut pro provoz české domény, a který je díky svým parametrům a kapacitě připraven na mnohem větší počet jmen domén, než kolik jich je aktuálně v ccTLD .CZ registrováno.

Kromě České republiky řídil tento systém v roce 2019 správu domény také v dalších deseti zemích světa. Využíván je pro správu domény Argentiny (.AR), Kostariky (.CR), Albánie (.AL), Severní Makedonie (.MK), Tanzanie (.TZ), Angoly (.IT.AO a .CO.AO), Malawi (.MW), Lesotha (.LS) a Macaa (.MO). Nasazení v Argentině, s více než 500 000 domén, je druhou největší instancí systému FRED.

Pro implementaci i provoz systému FRED pro jiné TLD nabízí sdružení CZ.NIC podporu.



Země, kde je využíván FRED pro správu domén

5.2.2 Systém autoritativních DNS serverů pro .CZ

Servery spravující záznamy o doménách .CZ jsou provozovány sdružením CZ.NIC v několika lokalitách po celém světě. Kromě tří lokalit v České republice (zmíněných v kapitole 5.1 Datová centra) jsou dalšími Švédsko (Stockholm), Rakousko (Vídeň), Velká Británie (Londýn), Německo (Frankfurt nad Mohanem), Chile (Santiago de Chile), Spojené státy (Redwood City a Culpeper), Japonsko (Tokio) a od roku 2019 pak nově i Brazílie (Sao Paolo) a Itálie (Miláno).

5.2.3 Systém autoritativních DNS serverů pro .CZ

V roce 2019 sdružení CZ.NIC pokračovalo ve zvyšování odolnosti .CZ DNS infrastruktury proti DoS útokům a vykrývání potřeb trvalého růstu běžného provozu. Konkrétně byl dokončen upgrade stávajícího DNS nodu v Německu a pak došlo k instalaci nových nodů ve zcela nových lokalitách, konkrétně v Brazílii a Itálii. Celkově tak DNS infrastruktura pro .CZ doménu na konci roku 2019 disponovala výkonem 100+ fyzických serverů a kapacitou připojení 400+ Gbps distribuovaných v 17 geograficky odlehlých lokalitách deseti zemí na čtyřech kontinentech.

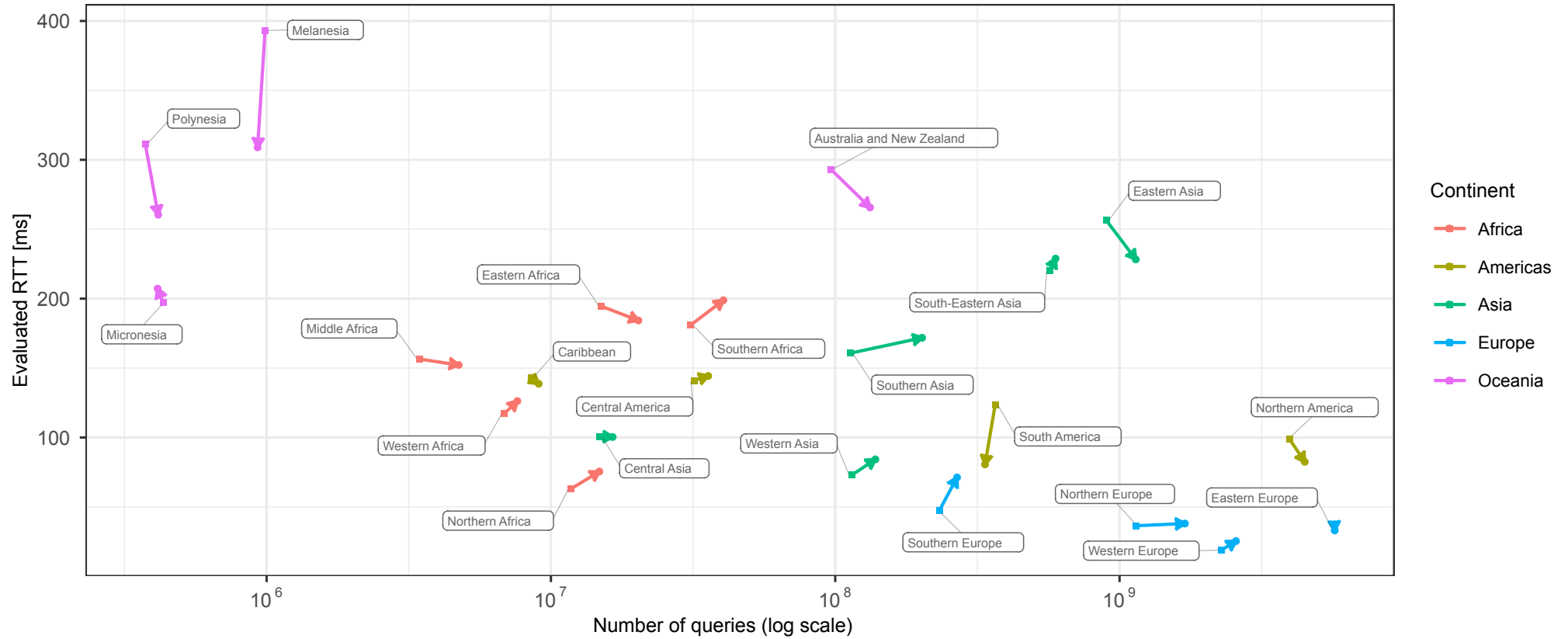
V roce 2019 sdružení také výrazně vylepšilo zpracování a vyhodnocování provozních parametrů z DNS anycastu díky projektu ADAM. Díky tomu bude sdružení schopno v budoucnu lépe řídit jeho rozvoj. Již v roce

2020 budou upgrady a instalace dalších zahraničních lokalit .CZ DNS infrastruktury prováděny v souladu s výstupy z tohoto projektu.

Pro významné poskytovatele internetového připojení provozuje CZ.NIC zrcadla uzlů .CZ DNS anycastu, tzv. ISP DNS Stacky, a to v sítích těchto poskytovatelů. Hlavní výhodou této služby je plná dostupnost služeb v doméně .CZ v případě útoku proti DNS serverům sdružení CZ.NIC. Zákazníků společností s ISP DNS Stackem se tak případný útok nijak nedotkne a internetové služby v doméně .CZ pro ně zůstanou plně dostupné. Další výhodou je zrychlení jejich odezev v síti poskytovatele s ISP DNS Stackem. První společnosti, které se k této aktivitě sdružení CZ.NIC přidaly, jsou Seznam.cz a Vodafone Czech Republic. Na konci roku 2019 byla uzavřena smlouva o provozu dalšího takového DNS zrcadla v síti CESNET.

Change in number of queries vs evaluated RTT by region

For DNS traffic captured on 1-14 May 2019 and 1-14 October 2019

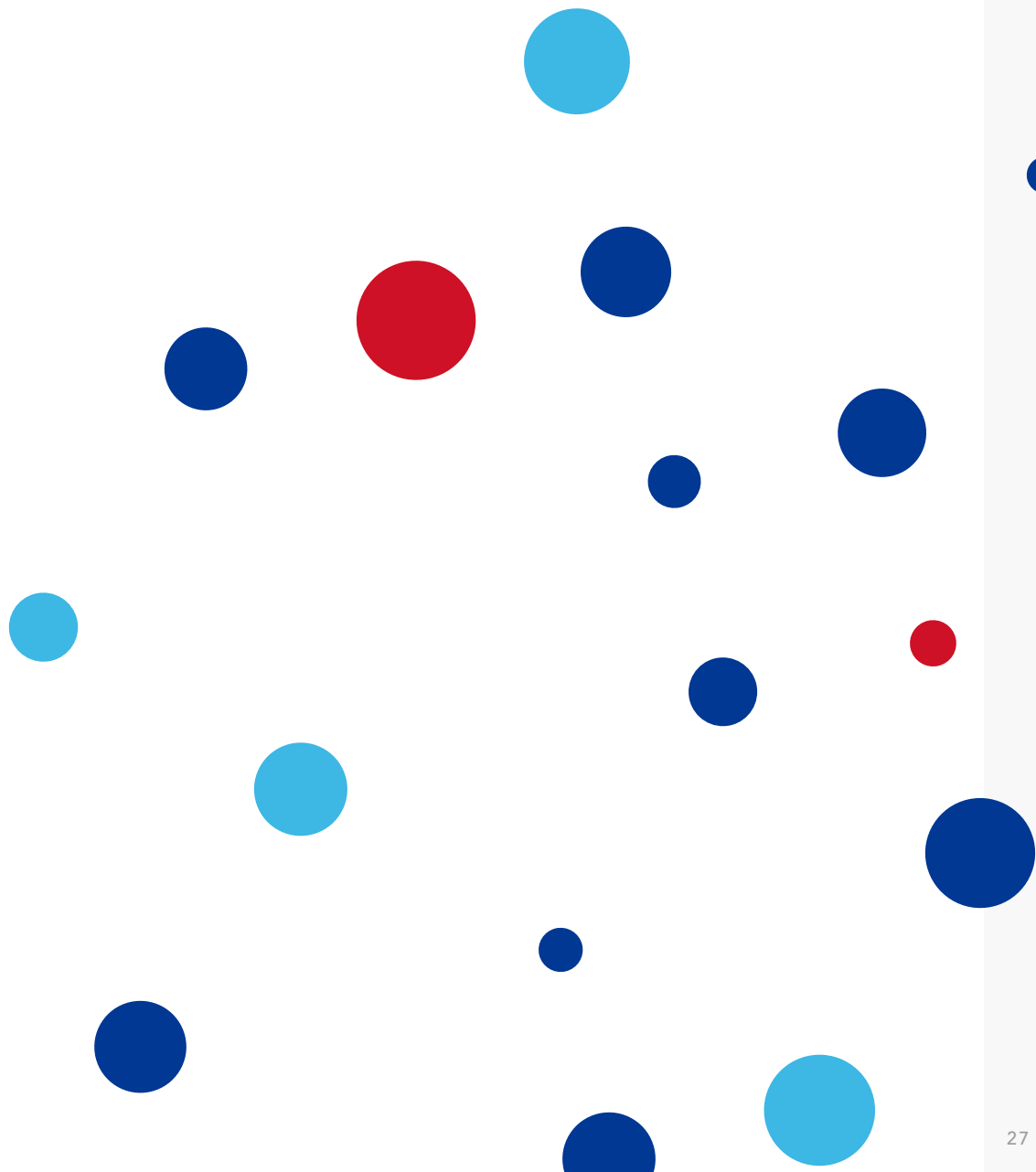


Příklad zhodnocení DNS provozu .CZ domény ve světě podle RTT

*RTT (round-trip-time) je doba, která je třeba pro komunikaci mezi zdrojem DNS provozu a autoritativním DNS serverem.

5.2.4 Utilizace .CZ DNS infrastruktury

Sdružení CZ.NIC se v roce 2018 dohodlo na komerční spolupráci s kanadskou organizací CIRA (Canadian Internet Registration Authority), spočívající v provozování části sekundárních DNS serverů .CA domény. Tato spolupráce v roce 2019 úspěšně pokračovala. Kanadský registr čítá více než 2,8 milionu domén a je tedy přibližně dvakrát větší než ten český. Z technického pohledu se jedná o sdílení kapacity DNS serverů primárně určených pro doménu .CZ s dalším subjektem. Tato kapacita je, díky výrazným upgradům v posledních letech, dimenzována mnohonásobně výše, než je reálné využití, a proto je užitečné a prospěšné ji využít i pro jiné projekty.



5.3 Podpora internetové infrastruktury

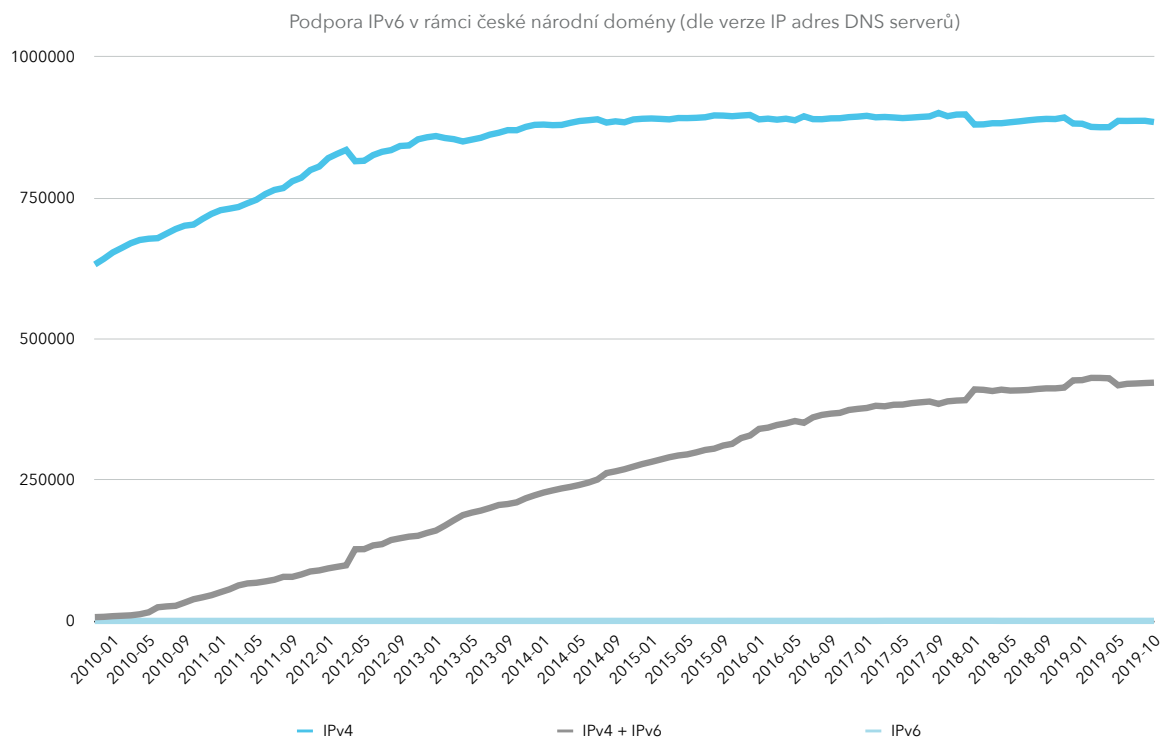
5.3.1 Podpora IPv6

IP adresy představují základní stavební prvek Internetu. Bez IP adres se není možné připojit k celosvětové síti, čímž je znemožněno i vzájemné rozpoznání a propojení počítačů. Stávající prostor IP adres internetového protokolu verze 4 (IPv4) je v podstatě vyčerpán. Odpovědí na nedostatek

IPv4 adres je nová verze internetového protokolu IPv6 nabízející mnohem větší zásobu adres a také nové možnosti.

Mezi dlouhodobé cíle sdružení patří podpora zavádění této technologie na všech úrovních - tj. jak na úrovni obsahu, tak sítí a koncových zařízení. Ve spolupráci s registrátory, kteří jsou často rovněž provozovateli webhostingu, se pak sdružení CZ.NIC snaží o podporu IPv6 na straně webových, e-mailových a DNS serverů. Sdružení se podílí rovněž na prosazování IPv6 ve státní správě.

Díky výše uvedeným aktivitám má podpora IPv6 v České republice rostoucí tendenci a naše země se dle nezávislých průzkumů řadí mezi světové velmoci v zavádění IPv6.

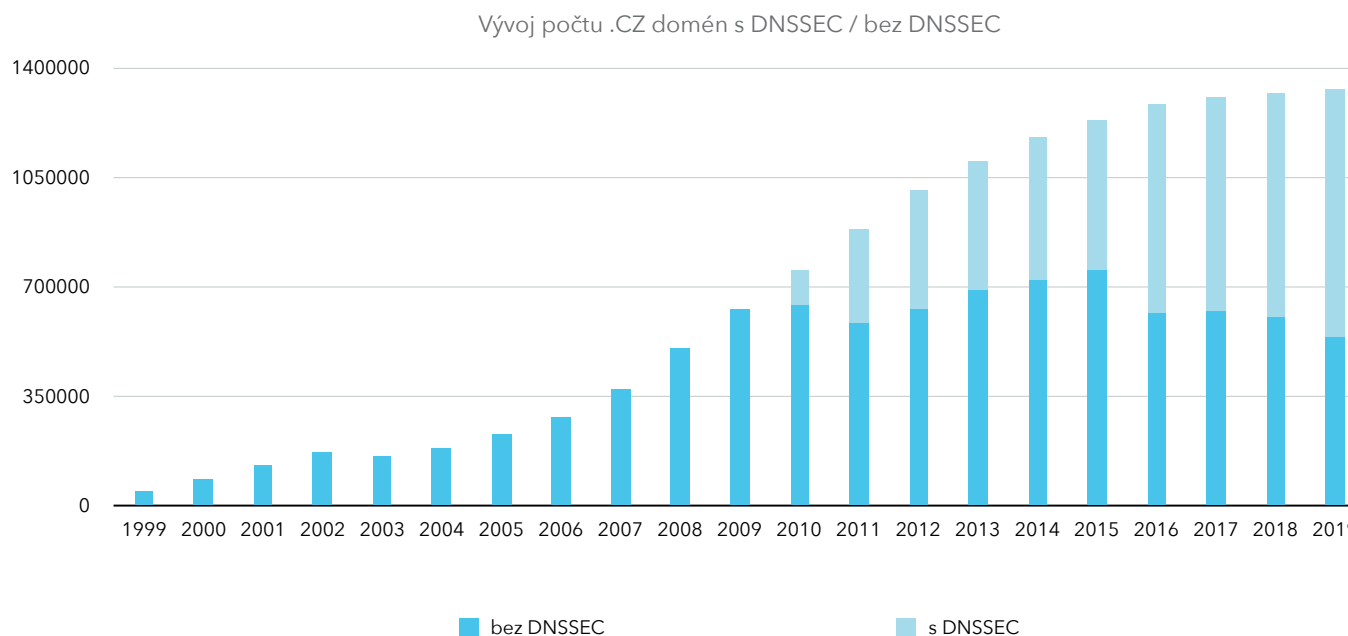


5.3.2 Podpora DNSSEC

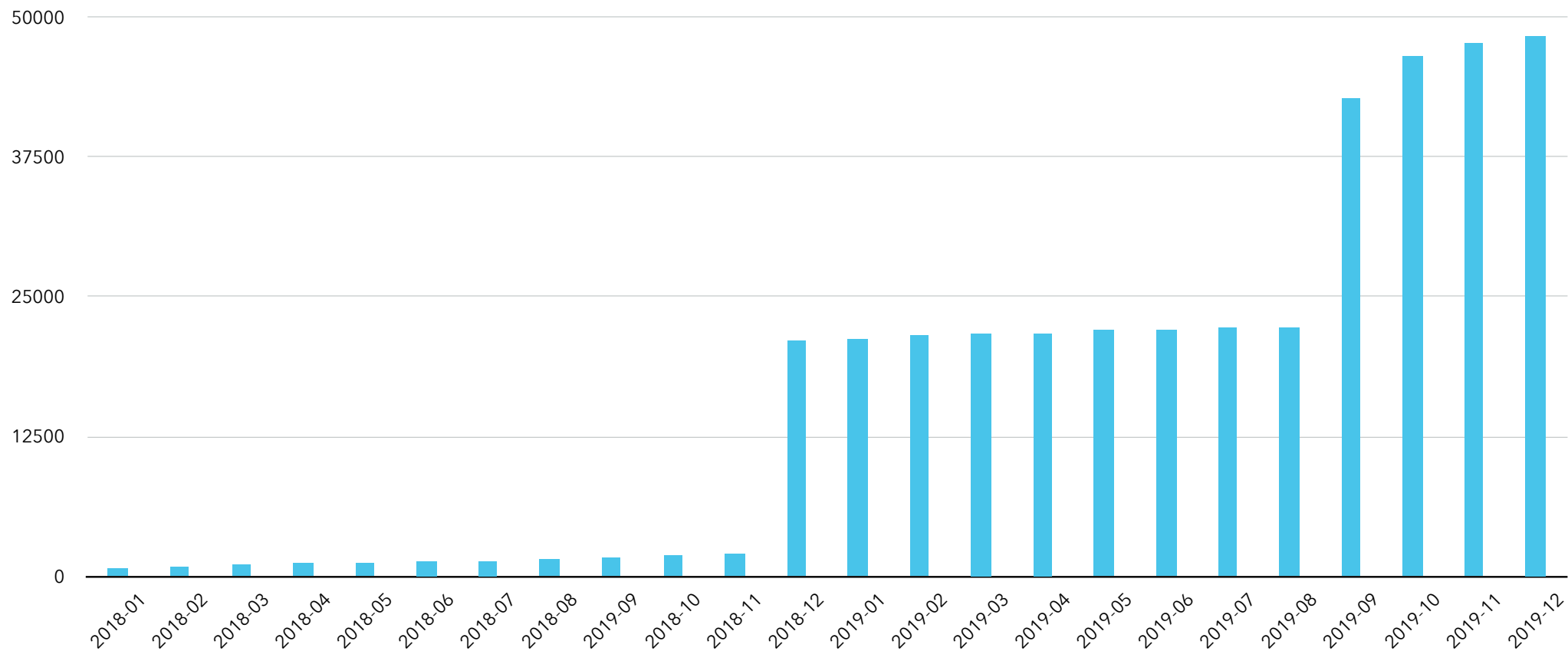
DNSSEC představuje rozšíření DNS, které zvyšuje jeho bezpečnost. Technologie DNSSEC poskytuje uživatelům jistotu, že informace, které z DNS získali, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. V rámci české národní domény .CZ je možné technologii DNSSEC využívat od roku 2008. Počet takto zabezpečených domén od té doby neustále roste, k čemuž přispívá rovněž spolupráce s registrátory. Na konci roku 2019 míra podpory DNSSEC pro .CZ přesáhla 59 %. Podílem podepsaných domén se tak Česká republika řadí jednoznačně mezi světové lídry. Ostatně mezinárodní organizace IANA v listopadu loňského roku jmenovala výkonného ředitele sdružení Ondřeje Filipa do prestižní skupiny zástupců komunity Trusted Community Representatives (TCR). Tato skupina vznikla na základě snah o vyšší zabezpečení systému DNS, a to právě technologií DNSSEC. Vedle podpory ze strany registrátorů je technologie DNSSEC

postupně zaváděna i hlavními poskytovateli internetového připojení v České republice, čímž se tento systém stává plně funkční pro většinu běžných uživatelů Internetu.

Vysoké podpoře DNSSEC pro .CZ doménu napomáhá mimo jiné i podpora automatizované správy DNSSEC klíčů, kterou CZ.NIC zavedl v roce 2017 jako první na světě. To bylo umožněno díky zavedení podpory nových standardů RFC 7344 a RFC 8078 do systému pro správu domén FRED. Tyto standardy jsou tak dostupné všem správcům TLD, kteří systém FRED využívají. Správcům autoritativních DNS serverů pak v zavedení tohoto zjednodušení pomůže KNOT DNS, který je s těmito standardy rovněž kompatibilní. DNSSEC je nyní možné jednoduše zavést i k těm doménám, kde to dříve nebylo možné, například u domén, jejichž registrátor DNSSEC nepodporuje, nebo u domén, jejichž správcem je někdo jiný než registrátor. Tato technologie je nicméně zajímavá i pro registrátory.



Vývoj počtu domén pod systémem automatizované správy DNSSEC klíčů



5.4 Podpora základní infrastruktury Internetu

Sdružení CZ.NIC nadále pokračovalo v provozu zrcadel kořenových serverů F, K a L. Sdružení CZ.NIC tedy provozuje zrcadla tří z celkových třinácti kořenových jmenných serverů, které jsou základem internetového systému jmen domén (DNS). Jejich provozem se zvyšuje nejen bezpečnost a stabilita kořenových serverů v globálním měřítku, ale především jejich dostupnost v evropském regionu. V roce 2019 sdružení aktivně vypomáhalo při upgradu infrastruktury kořenových serverů L.

Kromě těchto kořenových serverů je infrastruktura sdružení využívána také pro podporu rozvíjejících se registrů formou provozu sekundárních jmenných serverů pro jejich ccTLD. Této možnosti pro správu svých národních domén využívají Angola, Tanzanie a Severní Makedonie a od roku 2019 nově i Malawi. V roce 2019 dále sdružení začalo ve svých datacentrech provozovat infrastrukturu pro provoz DNS registru domén Brazílie a asociaci latinskoamerických ccTLD LacTLD.

Další formou podpory směřující k lokální internetové komunitě je hostování serverů některých neziskových organizací – např. serveru projektu Jeden svět na školách organizace Člověk v tísni, nebo provozování serveru s mirrorem populárních linuxových distribucí – Ubuntu, Debian, Fedora, apod.

Sdružení také od roku 2010 provozuje Otevřené DNSSEC Validující Resolvery (ODVR), které jsou volně k využití místo standardních DNS

resolverů, nabízených poskytovateli připojení. V roce 2019 došlo k instalaci nové infrastruktury této služby, která nově běží na sdružením vyvíjeném KNOT Resolveru. Díky tomu je ODVR podporována i šifrovaná DNS komunikace pomocí DNS-over-HTTPS (DoH) a DNS-over-TLS (DoT).

Instalací dedikované anycast infrastruktury pro ODVR došlo k jejímu oddělení od infrastruktury anycastu pro .CZ doménu (z pohledu sdílení hardware ale i IP adres) a tím i ke zvýšení bezpečnosti obou služeb. V průběhu roku 2019 sdružení intenzivně komunikovalo nutnost přechodu uživatelů na tuto novou infrastrukturu, na konci roku 2019 byla již většina provozu odbavována právě z ní a sdružení tak mohlo naplánovat odstavení původní infrastruktury na rok 2020.

Sdružení CZ.NIC je také aktivně zapojeno do projektu celosvětové monitorovací sítě RIPE Atlas. Jako jedna z prvních organizací sdružení podpořilo tento projekt hostováním pevných monitorovacích bodů označovaných jako RIPE Atlas Anchor.

Jednou z klíčových podmínek funkčnosti mnoha počítačových systémů je správná časová synchronizace. Systémy zapojené do Internetu k tomuto účelu využívají internetový protokol NTP. Sdružení CZ.NIC hostuje veřejný NTP server nejvyšší úrovně (stratum 1) řízený GPS a doplněný kvalitním oscilátorem typu OCXO DHQ.

6 Bezpečnostní tým CSIRT

Stále rostoucí význam Internetu a zvyšující se počet jeho uživatelů jsou spojeny s nárůstem počtu bezpečnostních incidentů (zneužití počítače, síťového prvku nebo sítě k nelegálním účelům - např. k rozesílání nevyžádané pošty, porušování autorských práv, phishingu, odposlechu dat) a nárůstem jejich závažnosti. Vzniká tak poměrně akutní potřeba vytvořit, zformalizovat a zefektivnit obranu proti těmto útokům. Pro tento účel jsou vytvářeny tzv. CSIRT týmy (Computer Security Incident Response Teams). Sdružení CZ.NIC se jakožto subjekt s dlouhodobou zkušeností s projekty v oblasti internetové infrastruktury zapojuje do podpory činnosti bezpečnostních týmů na národní i akademické úrovni. Sdružení provozuje rovněž vlastní tým CZ.NIC-CSIRT, který je zodpovědný za řešení incidentů v rámci AS25192 a incidentů dotýkajících se jmenných serverů pro doménu .CZ a 0.2.4.e164.arpa.

Ocenění aktivit sdružení CZ.NIC v oblasti kybernetické bezpečnosti a vyznamenání pro projekty, na kterých sdružení CZ.NIC řadu let pracuje, představuje i skutečnost, že u příležitosti 20. ročníku konference IS2 - Information Security Summit převzal výkonný ředitel sdružení Ondřej Filip ocenění za přínos v oblasti kyberbezpečnosti na území České republiky a vstoupil do Síně slávy Cybersecurity.

6.1 CSIRT.CZ - Národní CERT tým České republiky

Bezpečnostní tým CSIRT.CZ představuje oficiální národní bezpečnostní tým České republiky, který je provozován na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a veřejnoprávní smlouvy uzavřené dne 18. prosince 2015 s Národním bezpečnostním úřadem (NBÚ). Na místo NBÚ

od 1. srpna 2017 nastoupil nově vzniklý Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který se tak stal gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Cílem týmu CSIRT.CZ je především řešení incidentů, které se týkají kybernetické bezpečnosti v sítích provozovaných v České republice.

Tento tým shromažďuje a vyhodnocuje data o oznámených incidentech a ta dále předává osobám zodpovědným za chod sítě nebo služby, která je zdrojem daného incidentu, nebo poskytuje koordinační pomoc. Při své činnosti tým spolupracuje se subjekty jak na národní úrovni (především NÚKIB a dále Policie České republiky (PČR), akademické CSIRT, poskytovatelé internetového připojení (ISP), banky a další), tak na mezinárodní úrovni (národní CSIRT dalších států, Evropská agentura pro bezpečnost sítí a informací (ENISA), EUROPOL a další), se kterými si na základě vzájemné důvěry vyměňuje informace o jednotlivých incidentech a jejich řešeních.

CSIRT.CZ se také podílí na řadě grantových projektů, mezi něž se řadí PROKI (Predikce a ochrana před kybernetickými incidenty), který je podporován v rámci Programu bezpečnostního výzkumu České republiky 2015-2020.

V roce 2019 došlo v projektu PROKI k dalšímu vývoji. Byl proveden kompletní upgrade používaných open source produktů, což přineslo například větší možnosti zabezpečení dat, se kterými se v projektu pracuje.

Novým přírůstkem v projektu je také přístup k výstupům každodenních rozsáhlých skenů prováděných službou Shodan, zprostředkované rakouským CERT týmem pro celou Českou republiku. Byť je povaha těchto dat jiná, než která jsou zpracovávána systémem PROKI, mohou data z Shodanu poskytnout zajímavý kontext pro interpretaci dat z PROKI. Neobsahují totiž pouze zranitelné a závadné služby, nicméně celkový stav sítě - např. jaká služba běží na konkrétním zařízení.

Zapojení dat ze služby Shodan umožnilo otestovat nový způsob analýzy dat, kdy bylo porovnáním informací služby Shodan a informací v PROKI možno identifikovat IP kamery, které byly kompromitovány, a jsou útočníky zneužívány k dalším útokům.

Stejný princip byl v roce 2019 využit i ve spolupráci s komunitou, kdy CSIRT.CZ na základě obdrženého seznamu Industrial Control Systems (ICS) zařízení, alokovaných na IP adresách v České republice, provedl porovnání s informacemi v systému PROKI, což umožnilo identifikovat mezi ICS zařízeními takové stroje, které již byly s velkou pravděpodobností kompromitovány a mohou tak představovat značné bezpečnostní riziko. Provozovatelé těchto zařízení byly na možná rizika upozorněni.

Tým také pokračoval ve spolupráci na projektu SIC CZ (Safer Internet Centre, který je realizován sdružením CZ.NIC pod značkou „Bezpečně na netu“), přesněji s provozem horké linky STOPonline.cz, která je určena pro oznamování nelegálního on-line obsahu, a v osvětě a vzdělávání dětí i rodičů. Dalším projektem, do kterého se v roce 2019 CSIRT.CZ úspěšně zapojil, je projekt Cyber Exchange. Jeho podstatou je technická a administrativní výměna expertů napříč národními a vládními bezpečnostními týmy členských zemí EU zahrnutých do projektu. V rámci projektu tak například vznikla open-source knihovna envelope, která programátorům umožňuje využít komplexní podporu PGP a S/MIME standardů při práci v jazyku Python nebo Bash. V průběhu roku 2019 byl dokončen projekt Podpora rozvoje kapacit v oblasti kybernetické bezpečnosti v České republice, který podporoval další prohlubování národní a mezinárodní spolupráce, ale i další vzdělávání a zvyšování odbornosti členů týmu CSIRT.CZ. V rámci tohoto projektu probíhalo například publikování pravidelného osvětového seriálu Postřehy z bezpečnosti na serveru Root.cz.

6.1.1 Statistika provozu

V roce 2019 řešil CSIRT.CZ 954 bezpečnostních incidentů. Zároveň znovu narostl počet odpovědí v souvislosti s řešením těchto incidentů. Celkem bylo odesláno 13 883 e-mailů, tj. o 3 821 více než v roce předešlém. S jedním incidentem mohou být spojeny až desítky odeslaných e-mailů z důvodu komplexnosti útoků (botnety, zranitelná zařízení, kompromitované účty, apod.).

Již v roce 2016 byl sdružením CZ.NIC, resp. jeho bezpečnostními experty, vyvinut open-source nástroj Convey, který umožňuje automatizovat komunikaci ohledně bezpečnostních incidentů, do nichž je zapojeno více stran. V roce 2019 byla utilita Convey obohacena o další vlastnosti, které umožňují členům týmu pracovat daleko efektivněji. Jedná se například o naučení práce s kvótami LACNICu nebo schopnost převádění napříč 50 datovými typy konkrétních hodnot. Zároveň byla zjednodušena instalace tohoto nástroje. Díky zveřejnění na GitLabu ho nyní mohou využívat všechny bezpečnostní týmy v komunitě i mimo ni.

V roce 2018 byl také vytvořen doplněk „csirt.cz-boost“ do prohlížeče, který zrychluje práci s interně používanými aplikacemi – zvláště s OTRS. V roce 2019 došlo k vylepšení tohoto doplňku o automatické určení jazykové šablony odpovědi na základě domény příjemce, zobrazení malého náhledu problémové stránky nebo automatické dopočítávání metadat potřebných pro řešení konkrétních incidentů.

Počet řešených incidentů

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

* Sensor Network není započten do celkového počtu

Součástí procesu řešení incidentů je také rozesílání informací v případě zranitelných systémů.

Statistikám jednotlivých typů incidentů stále vévodí phishing, na druhém místě je pak incident označovaný jako Probe. Pod tento typ incidentu řadíme mimo jiné brute force útoky na uživatelské účty, respektive pokusy o prolomení hesla na cílených strojích. Jedná se o typ útoku, kde útočník po zjištění přihlašovacích údajů může zneužít napadený stroj ve svůj prospěch a pro páchání dalších útoků v kyberprostoru. Tyto praktiky jsou momentálně mezi útočníky velmi oblíbené. Na třetím místě se pak nachází nevyžádaná pošta.

6.1.2 Osvětová a vzdělávací činnost

Během roku 2019 vystupovali členové týmu CSIRT.CZ na nejrůznějších konferencích a odborných skupinách (Internet a technologie, Pracovní skupina CSIRT.CZ, Internetem bezpečně, TF-CSIRT, Policejní akademie České republiky, Festival bezpečného Internetu (FBI19), Řešení elektronického násilí a kyberkriminality, Ministerstvo průmyslu a obchodu ČR). Členové týmu také v případě potřeby komentovali aktuální dění v plošných médiích.

Mimo to bylo v roce 2019 připraveno nové školení Úvod do forenzní analýzy paměti, které mělo úspěšnou premiéru v prosinci. Celkově pak CSIRT.CZ realizoval čtyři běhy školení Bezpečnost a soukromí na Internetu, a dvě specializovaná školení pro Policii České republiky. Dále pak jedno školení pro zaměstnance Nestlé Česko s. r. o., jedno specializované školení pro Státní úřad pro jadernou bezpečnost a jedno pro Českou národní banku.

Další publikační činnost pak zahrnovala uveřejňování osvětových i vzdělávacích článků. Konkrétně se jedná o čtyřadvacet dílů seriálu Postřehy z bezpečnosti na serveru Root.cz a řadu tematických příspěvků na blog.nic.cz. Dle aktuálních témat a situace na poli kybernetické bezpečnosti byly publikovány i články v tištěných médiích: za zmínku stojí uvést příspěvky v časopise IT Systems o bezpečnosti protokolu MQTT nebo o modelování rizik v CVSS. CSIRT.CZ také pokračoval v publikování návodů pro správce a uživatele na vlastních webových stránkách.

CSIRT.CZ ve spolupráci s Akademií CZ.NIC v roce 2019 také organizoval školení bezpečnostních týmů v ČR zahraničními lektory z agentury ENISA (Mobile forensics, Memory forensics).

6.1.3 Národní a mezinárodní spolupráce

Strategickým partnerem v oblasti národní spolupráce je NÚKIB a Vládní tým České republiky, tedy GovCERT (Vládní CERT). S těmito subjekty spolupracuje CSIRT.CZ například v oblasti legislativy, kybernetických cvičení, formulování společných stanovisek v rámci CSIRT Network i na dalších projektech. Národní a Vládní CERT se několikrát ročně setkávají při různých příležitostech, což poskytuje dostatečný prostor pro pravidelné informování o práci jednotlivých týmů a jejich případnou koordinaci. Kromě toho se obě organizace pravidelně spoluúčastní setkání v rámci TF-CSIRT či CSIRT Network.

Pro úspěšné řešení incidentů je důležité udržovat kontakty s českými poskytovateli Internetu. Právě pro zlepšení komunikace a spolupráce na národní úrovni jsou důležitá setkání Pracovní skupiny CSIRT.CZ. Nepsaným pravidlem se stalo, že v první polovině roku byla sdružením pořádána tzv. „velká“ Pracovní skupina CSIRT.CZ, kam jsou pozváni všichni, kdo se o problematiku kybernetické bezpečnosti zajímají. O toto setkání je vždy velký zájem. V roce 2019 se Pracovní skupina věnovala tématům jako jsou citlivá data a zranitelnosti na českém webu, systémy NERD či PROKI, protokol DANE pro bezpečný transport pošty, DNS firewall a další. Velmi cenná byla také účast zástupců Vojenského zpravodajství, kteří přišli s členy pracovní skupiny diskutovat návrh novely zákona o Vojenském zpravodajství.

Národní a mezinárodní spolupráce zahrnuje také podporu pro týmy, které chtějí vstoupit do organizací TF-CSIRT a FIRST. To u některých typů členství zahrnuje provedení tzv. on-site visit, což obnáší kontrolu

funkčnosti a plnění požadavků u zájemců, kteří chtějí do těchto organizací vstoupit.

V roce 2019 se CSIRT.CZ zapojil do mezinárodních cvičení, jako je Locked Shields (technické cvičení organizované NATO), Cybersecurity Summer BootCamp, CyberSOPex 2019 a vybraných školení SANS Institute.

6.1.4 Preventivní činnost

Rok 2019 byl opět věnován i oblasti prevence, a to především pokračováním ve vytěžování informací z provozovaných honeypotů a v rozvoji projektu PROKI, kde se podařilo dosáhnout již výše uvedeného významného kvalitativního posunu analýz díky zařazení dat ze služby Shodan.

V roce 2019 došlo také k realizaci distribuce informací vztahujících se ke zranitelnosti CVE-2019-11510 v Pulse Secure VPN, která umožňovala potenciálnímu útočníkovi přístup k privátním klíčům a heslům uživatelů. Z tohoto důvodu sdružení požádalo společnost Bad Packets LLC, která zranitelnost našla, aby poskytla seznam zranitelných serverů, které diagnostikovala v České republice. Těmto subjektům bylo rozesláno upozornění.

6.1.5 Skener webu

Skener webu je jedna z preventivních bezpečnostních služeb, která byla spuštěna v roce 2013. Tato služba je určena provozovatelům a správcům webů, kterým pomáhá odhalit potenciální zranitelnosti jejich internetových prezentací. Služba je určena především neziskovým organizacím a veřejné správě. Analýza zranitelnosti probíhá ve dvou fázích.

Nejdříve pomocí automatických nástrojů a následně je proveden manuální test webu zkušeným testerem, který mimo jiné vyhodnotí nalezené zranitelnosti v kontextu celého webu a navrhne vhodná řešení. Na konci je žadateli poslána závěrečná zpráva, která obsahuje nalezené zranitelnosti, jejich ohodnocení dle závažnosti a také návrhy na jejich možná řešení. Při analýze potenciálních zranitelností služba staví jak na vlastních měřeních a zkušenostech bezpečnostního týmu, tak na seznamu Top 10 obecně nejzávažnějších bezpečnostních rizik podle projektu Open Web Application Security (OWASP).

Celkově bylo v roce 2019 otestováno 38 domén na základě 19 objednávek - z toho 6 domén u významných subjektů a 2 v rámci projektu Safer Internet Centre.

6.1.6 Penetrační testování

CSIRT.CZ v roce 2019 spustil pilotní provoz nové komerční služby penetračního testování. Prvním zájemcem, který tuto službu využil, byl kraj Vysočina. Otestováno bylo více než 20 domén. I na základě kladné zpětné vazby klienta bylo rozhodnuto o zahájení poskytování služby v plném rozsahu v průběhu roku 2020.

6.2 CZ.NIC-CSIRT

Tým CZ.NIC-CSIRT je zodpovědný za řešení incidentů dotýkajících se nameserverů pro doménu .CZ, 0.2.4.e164.arpa a AS 25192. Na základě Pravidel registrace je sdružení CZ.NIC oprávněno zrušit delegaci jména domény, jestliže je užíváno takovým způsobem, při němž dochází k ohrožení národní či mezinárodní počítačové bezpečnosti. K tomu může dojít například tak, že prostřednictvím jména domény či služeb, které jsou jeho prostřednictvím dostupné, dochází k distribuci škodlivého obsahu (viry, malware) nebo je předstírán obsah jiné služby (phishing). Ke zrušení jména domény může tým CZ.NIC-CSIRT přistoupit rovněž v případě, že server dostupný prostřednictvím jména domény je řídicím centrem sítě propojeného hardwaru distribuujícího škodlivý obsah (botnet).

Činnost CZ.NIC-CSIRT v roce 2019

V rámci činnosti CZ.NIC-CSIRT je provozován vlastní systém sloužící k vyhledávání napadených stránek u domén .CZ (MDM). V rámci sdružení CZ.NIC zajišťuje CZ.NIC-CSIRT implementaci a plnění mezinárodně uznávané certifikace systému řízení bezpečnosti informací (ISMS) podle normy ISO 27001. V roce 2019 proběhl externí audit, který potvrdil, že CZ.NIC i nadále plní všechny požadavky této normy. V souvislosti s určením registru domény .CZ jako základní služby se v roce 2019 CZ.NIC-CSIRT soustředil na zmapování zákonných požadavků na provozovatele základních služeb, na úpravu vnitřních směrnic a na přípravu podkladů pro technické oddělení, které část požadavků realizuje.

7 MojelD

MojeID je unikátní služba umožňující uživatelům Internetu v České republice používat pro přihlašování k různým internetovým službám jednotné identifikační údaje. Tato služba, provozovaná sdružením CZ.NIC, byla uvedena do provozu v roce 2010 a slouží tak svým uživatelům již desátým rokem.

Pokud uživatel Internetu používá mojeID, nemusí si pro každou novou službu zakládat samostatný účet a procházet tak zdoluhavým registračním procesem. Místo toho své registrační údaje zadá jen jednou, do mojeID, kde jsou tyto údaje ověřeny a následně využívány pro přihlašování k internetovým službám. Provozovatelé implementující mojeID tak nejenže zvýší uživatelský komfort své služby, ale také získají ověřené informace o svých návštěvnicích, kterým následně mohou poskytnout další výhody.

Služba mojeID vychází z otevřeného standardu OpenID rozšířeného o unikátní vlastnosti, které jiné OpenID služby nemají – například předávání údajů uživatelských identit při každém přihlašování uživatele a ověřování uživatelů v různých úrovních různými metodami.

Při vývoji této služby byl kladen důraz především na bezpečnost a důvěryhodnost celého systému, stejně jako na ochranu osobních údajů. Registr uživatelských údajů je chráněn na stejně vysoké úrovni jako registr .CZ domén a uživatel může při každém přihlášení sám určit, které z údajů ze svého profilu danému poskytovateli, k jehož službám se chce pomocí mojeID přihlásit, předá. Uživatel tak získává kontrolu nad svými údaji a ví, jaké údaje, kterému subjektu a kdy propůjčil.

Služba se neustále vyvíjí a reaguje na aktuální potřeby svých uživatelů. V minulých letech představila například veřejný profil, díky kterému mojeID může sloužit jako internetová vizitka, možnost přímého založení účtu mojeID a předvyplnění údajů přímo z uživatelských účtů služeb Facebook, LinkedIn a Google, nebo kompletní redesign webových stránek.

Rok 2019 byl zaměřen na zvýšení uživatelského komfortu a bezpečnost. Uživatelé se nyní při změně hesla musí autorizovat prostřednictvím SMS a k autentizaci mohou nově využít i bezpečnostní klíč se standardem FIDO 2. Pro zvýšení komfortu při validaci účtu byla zavedena nová bezplatná možnost validace účtu mojeID prostřednictvím poskytnutí souhlasu o předání údajů třetí osobně na pracovištích Czech POINT.

7.1 Podpora mojeID

Klíčovým faktorem systematického rozšiřování služby mojeID je její podpora ze strany poskytovatelů internetových služeb. Rostoucí nabídka míst, kde lze uplatnit mojeID, má vliv na získávání nových uživatelů, pro které je důležité, aby se pomocí jednoho jména a hesla mohli přihlašovat k co nejvíce službám – ať již k těm, které používají každodenně, nebo k těm (např. internetovým obchodům), na které zavítali poprvé – a mojeID jim ušetřilo čas při registraci a zajistilo kontrolu nad poskytovanými údaji.

Ve vztahu k poskytovatelům služeb je, kromě snahy o pronikání do nových segmentů, důležitý také fokus na udržení či upevnění pozic v oblastech stávajících, jako jsou elektronické obchody, které se např. zajímají o možnost ověření zletilosti svých zákazníků v případě specifického zboží či služeb, komunitní servery, webové prezentace měst a obcí, portály občana nebo knihovní systémy.

V roce 2019 byl zaznamenán výrazně větší zájem o službu mojeID ze strany vývojářů pro města a obce. Jedná se především o tzv. portály občana. Dlouhodobě probíhá spolupráce s vývojáři společností Datron a Vera. Objevuje se i řada individuálních implementací od menších

vývojařů. MojeID je v současné době zcela jednoznačně vnímáno jako prostředek pro ověření a identifikaci uživatelů Internetu.

7.2 Externí validační místa

Rozšiřování sítě validačních míst, které jsou prostředkem, jak uživateli usnadnit proces validace, tj. nejvyššího stupně ověření ve službě mojeID, pokračovalo také v roce 2019. Nová validační místa byla otevírána především ve městech a obcích ve spojitosti s Portály občana – Bílovice nad Svitavou, Lysá nad Labem, Turnov a Kraslice.

V roce 2019 byla rozšířena agenda validačních míst o ověření kontaktu při jeho převodu z centrálního registru (tedy rejstříku pro registraci jmen domén v ccTLD .CZ) do registru identit (tedy do služby mojeID) se změnou údajů. Zatím bylo možné toto ověření provádět pouze formou ověřeného podpisu.

Nezanedbatelným aspektem provozu sítě externích validátorů je rovněž systematická práce se stávajícími validačními místy a jejich zaměstnanci. V roce 2019 byla spuštěna recertifikace validátorů formou aktualizovaného vzdělávacího kurzu. Během prvních měsíců po spuštění se recertifikovalo téměř 60 % validačních míst.

7.3 Uživatelé mojeID

Uživatelská báze je nejcennějším aktivem služby mojeID. Bez rostoucího počtu uživatelů by bylo obtížné získávat stále významnější poskytovatele služeb a dostávat službu do povědomí široké veřejnosti. V průběhu roku 2019 vzrostla uživatelská báze mojeID o 53 584 nových uživatelů na celkových 663 286 uživatelů.

Pokračoval také trend rostoucího podílu validovaných uživatelů, jejichž celkový počet se na konci roku vyšplhal na 26 219. Tento výsledek lze přičíst dvěma hlavními faktorům – pokračování zájmu o validaci v souvislosti se státní loterií Účtenkovka a nově také možnosti validovat účet mojeID prostřednictvím informačního systému datových schránek nebo na Czech POINTech.

Úroveň zabezpečení účtu mojeID

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

7.4 MojED jako nástroj pro přeshraniční autentizaci v Evropě

I v roce 2019 se sdružení CZ.NIC aktivně podílelo na zapojení České republiky do budování infrastruktury pro přeshraniční elektronickou identifikaci, tak jak ji definuje nařízení eIDAS. Toto nařízení navazuje na práci v rámci pilotního projektu STORK (Secure idenTity acrOss boRders linKed), kterého se naše sdružení účastnilo spolu s Ministerstvem vnitra České republiky (MV ČR). Po celý rok 2019 provozovalo sdružení CZ.NIC bránu, která vznikla právě v rámci projektu STORK a která umožňovala přihlášení do služeb Evropské komise pomocí mojED. Tato brána bude v budoucnu kompletně nahrazena oficiálním eIDAS uzlem pro Českou republiku.

V roce 2019 také provozovalo sdružení CZ.NIC na základě smlouvy se Správou základních registrů v produkčním provozu eIDAS uzlu umožňující používat pro české online služby přihlašovací prostředky oznámené ostatními členskými státy EU a zároveň middleware komponentu nutnou pro přihlašování německým eOP. Jediným členským státem, který oznámil svůj prostředek elektronické identifikace a splnil příslušné technické specifikace, zůstalo po celý rok pouze Německo. V průběhu roku se také začalo pracovat na spuštění druhé komponenty eIDAS uzlu, která umožní držitelům českých eOP jejich využití pro zahraniční online služby. Jako součást plnění smlouvy pokračovalo po celý rok aktivní zapojení

zaměstnanců sdružení do fungování Evropskou komisí zřízených platforem eIDAS Cooperation Group a eIDAS Technical SubGroup.

Zmíněné iniciativy vycházejí z koncepce činnosti sdružení zahrnující zejména spolupráci se státem v oblasti rozšiřování eGovernmentu a sdružení se jim bude věnovat i v roce 2020.

8 Laboratoře CZ.NIC

Laboratoře CZ.NIC jsou organizačně odděleným výzkumným a vývojovým pracovištěm, které se zaměřuje především na inovativní projekty ve prospěch české i světové internetové komunity. Projekty jsou zaměřené zejména na infrastrukturní protokoly a služby, monitorování provozu DNS a síťovou bezpečnost. Některé z projektů záměrně podporují významné trendy současné digitální společnosti, jakými jsou například otevřená data, eGovernment, open source software nebo podpora znevýhodněných uživatelů. Laboratoře CZ.NIC jsou personálně zastoupeny ve všech regionálních pobočkách sdružení, tedy nejen v Praze, ale též v Brně, Českých Budějovicích a v Plzni, a proto intenzivně využívají nástroje pro distribuovaný softwarový vývoj a další prostředky pro vzdálenou spolupráci (videokonference, diskusní fóra apod.). Laboratoře CZ.NIC a zaměstnanci, kteří na jejich projektech pracují, mají v zahraničí velmi dobré jméno. To potvrzuje i získání ceny R&D Working Group Champion programátorem pro výzkum a vývoj Maciejem Andzińskim. Cenu uděluje každé dva roky organizace CENTR sdružující nejen evropské doménové registry.

Stručné shrnutí činnosti za rok 2019

Laboratoře CZ.NIC se v roce 2019 soustředily především na další rozvoj již existujících projektů. Stěžejními projekty jsou:

- systém ADAM pro monitorování a analýzu služeb poskytovaných sdružením,
- multiprotokolový směrovací démon BIRD,
- dvojice DNS serverů – autoritativní Knot DNS a rekurzivní Knot Resolver,
- výuková aplikace Tablexia určená pro děti s dyslexií a jinými poruchami učení,
- router Turris zaměřený na bezpečnost koncových domácích a SOHO sítí.

8.1 ADAM - monitoring a analýza DNS provozu

Důležitým předpokladem spolehlivého fungování DNS serverů domény .CZ, doménového registru a dalších služeb poskytovaných sdružením je mimo jiné systematický a detailní monitoring reálného DNS provozu a jeho okamžitá i dodatečná analýza. Těmito postupy je možné včas odhalit případné technické problémy anebo síťové útoky, jimž je infrastruktura DNS permanentně vystavena, ale také efektivně plánovat další rozvoj infrastruktury a služeb.

Účelem projektu ADAM (Advanced DNS Analytics and Monitoring) je vývoj nástrojů pro efektivní a robustní sběr a zpracování dat o DNS transakcích, zdokonalení a rozšíření metod jejich analýzy, a také vývoj vhodných uživatelských rozhraní a reportovacích metod.

V roce 2019 byla ve spolupráci s FIT VUT Brno dokončena první verze DNS sondy. Jde o softwarový nástroj pro vysokorychlostní zpracování DNS provozu v reálném čase, generování zvolených výstupních dat ve formátu C-DNS nebo Parquet a jejich následné ukládání na disk anebo odesílání na vzdálené sběrné místo. DNS sonda bude postupně nasazena na všechny DNS servery, které jsou spravovány sdružením, a nahradí současné nepříliš efektivní postupy.

Dalším softwarovým nástrojem vyvinutým v roce 2019 je DNS crawler. Jeho úkolem je pro zadaný seznam jmen domén získat a verifikovat vybraná data z DNS, ale také získat informace z webového a mailového serveru

každé domény. Architektura DNS crawleru umožňuje komunikovat s více doménami současně (i z více spolupracujících počítačů), a umožňuje tak zpracování dat z velkého počtu domén v relativně krátkém čase. Pro rok 2020 je plánováno použití DNS crawleru k pravidelnému skenování celé zóny .CZ s cílem včasného odhalení konfiguračních i bezpečnostních problémů.

V oblasti uveřejňování výstupů projektu ADAM různým okruhům příjemců (interně pro účely sdružení, registrátorům a členům anebo široké veřejnosti) bylo navrženo a implementováno aplikační programové rozhraní typu REST API, které umožní různá data a statistiky získávat ve strojově čitelné podobě vhodné k dalšímu zpracování. Do tohoto rozhraní jsou průběžně přidávány další datové položky.

8.2 BIRD

Směrovací démon pro dynamické směrování IP protokolu je určený pro Linux a BSD. Projekt vznikl na půdě Matematicko-fyzikální fakulty Univerzity Karlovy a Laboratoře CZ.NIC se podílejí na jeho dalším vývoji. V současné době je nejpoužívanějším softwarem pro route servery v peeringových centrech na světě. Podle průzkumu organizace EURO-IX jej používají více než dvě třetiny z nich.

V roce 2019 bylo vydáno pět nových verzí 2.0.x a čtyři ve starší 1.6.x. Hlavním úkolem prací na tomto software v roce 2019 byla stabilizace nové větve 2.0.x tak, aby bylo možné ji nasazovat v produkčním prostředí. To se zcela podařilo a uživatelé tak již běžně na tuto řadu migrují. Ve verzích 1.6.x již nejsou přidávány žádné nové funkce. Další důležitou inovací bude změna architektury tak, aby podporovala multithreading, což bude úkolem v roce 2020.

8.3 Datovka

Projekt Datovka vyvíjí multiplatformní aplikaci pro efektivní obsluhu datových schránek v systému ISDS. Aplikace je dostupná jako open source software pro desktopové operační systémy Windows, macOS a Linux, a také pro obě hlavní mobilní platformy Android a iOS.

V roce 2019 byla v desktopové i mobilní aplikaci uživatelům nabídnuta podpora přihlašování mobilním klíčem. V obou aplikacích byly zjednodušeny konfigurační soubory – konfigurace, která se bezprostředně netýká uživatelských účtů, se ukládá do oddělených databází.

V desktopové aplikaci proběhly úpravy mající za cíl dovolit aplikaci pracovat v izolovaném prostředí (sandboxu). Nově je možné na desktopu u existujících účtů změnit přihlašovací jméno v případě, kdy uživateli byly k datové schránce vygenerovány nové přihlašovací údaje.

V mobilní aplikaci přibyla možnost pracovat se soubory v iCloudu na zařízeních s iOS. Podobně jako na webovém portálu ISDS je v mobilní Datovce možné vytvářet textové přílohy datových zpráv ve formátu PDF. Přidána byla také podpora pro zálohování uložených dat stejně jako jejich obnovování ze zálohy.

8.4 Knot DNS a Knot Resolver

Knot DNS je softwarová implementace autoritativního DNS serveru. Mezi jeho hlavní cíle patří dosahování vysokého výkonu při zpracovávání DNS dotazů a efektivní správa obsáhlých TLD zón, včetně pokročilé automatizace podepisování DNSSEC. Po deseti letech vývoje bylo dosaženo nejen hlavních cílů projektu, ale projekt si rovněž získal uznání v komunitě DNS i mezi uživateli.

V roce 2019 byla velká pozornost věnována výkonovým optimalizacím při podepisování DNSSEC. Díky tomu byl Knot DNS úspěšně nasazen organizací DENIC (správce německé domény .de) k podepisování německé zóny, což umožnilo výrazně zkrátit prodlevu mezi úpravou zóny a její propagací na veřejné DNS servery. Knot DNS byl rovněž úspěšně nasazen organizací DK Hostmaster k podepisování dánské zóny. Na základě průběžné komunikace s dalšími evropskými správci národních domén lze očekávat, že další významná nasazení v budoucnu ještě přibudou.

Projekt Knot Resolver vyvíjí nezávislou implementaci rekurzivního DNS resolveru. V roce 2016 byl nasazen jako výchozí resolver pro routery Turris Omnia. Dalšího velkého nasazení se dočkal v roce 2018 na veřejný resolver Cloudflare na IP adrese 1.1.1.1. Ve stejném roce byla přidána ochrana před Random Subdomain útoky pomocí tzv. agresivní DNSSEC cache.

V roce 2019 byla přidána experimentální podpora pro DoH protokol a byla provedena optimalizace pro zlepšení propustnosti. Dalšího nasazení se Knot Resolver dočkal nepřímo, když na něm postavila své

vlastní DNS řešení firma Whalebone. Díky tomu na začátku roku 2020 Knot Resolver používá více než stovka ISP a telekomunikačních operátorů.

8.5 Tablexia

Tablexia je moderní vzdělávací aplikace pro děti s dyslexií na druhém stupni základních škol. Je určena k využití jak ve školách jako doplnění standardní výuky, tak v pedagogicko-psychologických poradnách a dalších poradenských zařízeních určených pro žáky s výukovými obtížemi. Je k dispozici zdarma na Google Play, App Store, a desktopová verze pak na webu projektu.

V roce 2019 se sdružení připojilo k projektu Safer Internet. V rámci této spolupráce byla věnována pozornost vývoji dvou nových her, které jsou zaměřeny na trénink prostorové orientace a paměti. Tyto oblasti byly zvoleny z důvodů, že nadměrné používání aplikací a mobilních zařízení má vliv na kognitivní schopnosti a zejména na pozornost, paměť, soustředění a prostorovou orientaci.

Vznikly tak hry Archiv, kde je hlavním cílem detektiva zapamatovat si a správně poté přiřadit předměty k číslům, kterými byly dané předměty



označeny a Na stopě, kde se detektiv musí zorientovat ve městě a vypátrat zloděje, dříve než vychladnou jeho stopy. Hry byly ke konci roku 2019 připravené k vydání a vyzkoušení s dětmi. Trénink pozornosti je v plánu na rok 2020.

V průběhu roku byly odladěny drobné chyby v desktopové verzi aplikace a byly také realizovány některé grafické úpravy, především v souvislosti se situací, kdy se hráči podaří dosáhnout zisku všech trofejí i všech detektivních hodností. Pro tyto příležitosti byla vytvořena animace a také navrženo zcela nové prostředí.

8.6 Turrís

Začátek roku 2019 byl v projektu Turrís ve znamení dokončování nového modulárního bezpečného síťového zařízení Turrís MOX. Během první poloviny roku 2019 byla rozeslána všechna zařízení Turrís MOX určená prvním zákazníkům – podporovatelům z crowdfundingové kampaně. V druhé polovině roku došlo k uvedení zařízení do maloobchodního prodeje v České republice i v zahraničí.

V návaznosti na kampaň došlo také k vývoji některých nových funkcí pro Turrís OS. Jmenovitě například snadná možnost instalace Nextcloud a s tím související podpora více disků nebo třeba možnost bootovat po síti a z jednoho místa spravovat více routerů.

Zároveň začaly v důsledku úspěšného prodeje docházet skladové zásoby routerů Turrís Omnia. Výroba další série byla započata na podzim roku 2019. Nové routery získaly certifikaci FCC a je tedy možné je prodávat i v USA, což by mělo v roce 2020 vést k růstu povědomí o projektu Turrís, ale i k rozšíření sítě pro sběr dat do nových lokalit.

Výrazně postupoval i vývoj Turrís OS – systému pohánějícího zařízení Turrís. Po úvodním testování byla verze systému Turrís OS 4.0 postavená na nové verzi OpenWRT nasazena na Turrís MOX i na nově vyráběné routery Turrís Omnia. CZ.NIC díky změně vývojového modelu nových verzí Turrís OS během roku 2019 významným dílem přispěl do open-source projektu OpenWrt a přiblížil sdružením vyvíjený Turrís OS více upstreamovému projektu. Zároveň započaly práce na plánu, jak automaticky zmigrovat starší zařízení na nový systém bez ohrožení konfigurace uživatelů.

Mezi další zajímavé funkce, které jistě stojí za zmínku, je spolupráce s RIPE, kdy se povedlo integrovat software z projektu RIPE Atlas. Libovolný router Turrís tak lze snadno proměnit v sondu a přispět tak ke globálním statistikám o stavu Internetu.

Webové rozhraní pro ovládání routeru se také dočkalo velkých změn, a to hlavně pod povrchem. Změny by měly do budoucna usnadnit další rozšiřování a zároveň více sjednotit vzhled napříč funkcemi. Uživatelům byla dána nová verze k dispozici k testování. Obsahuje jak nové funkce, tak přepracovaný vzhled a ovládání pro větší uživatelské pohodlí.

Nový systém sběru dat doznal také velkého pokroku. Je nyní nabízen v rámci Turrís OS 4.0 a vyšší a během roku byl doplněn o řadu nových minipotů – pastí na útočníky. Zároveň byl dále propagován a dočkal se zájmu z řad uživatelů. V rámci projektu byl zprovozněn web view.sentinel.turris.cz obsahující globální statistiky o útocích a poskytující unikátní vzhled do bezpečnosti na Internetu. Zároveň byla obranná část – dynamický firewall – zpřístupněna odborné veřejnosti pro soukromé použití a ochranu jejich vlastních serverů. V následujícím roce je v plánu implementovat další pastí na útočníky, umožnit uživatelům přístup ke statistikám jen z jejich zařízení a zajistit lepší kontrolu nad provozovanými službami přímo na routeru.

9 Vzdělání a osvěta

9.1 Komunikace s veřejností

V roce 2019 pokračovala již zavedená a osvědčená spolupráce s veřejnoprávními, ale i soukromými médii. O sdružení CZ.NIC tak informovaly deníky, rozhlasové a televizní stanice a významnější mediální servery zabývající se Internetem a technologiemi.

Sdružení vydalo 14 tiskových zpráv a 20 tiskových sdělení, jejichž příjemci byli odborní novináři, tak novináři z médií zaměřených na širší veřejnost či specifické skupiny příjemců. Tato sdělení publikuje sdružení CZ.NIC v sekci [Novinky](#) na svých stránkách www.nic.cz. Sekce Novinky je též součástí informačních stránek vzdělávacího centra sdružení (Akademie CZ.NIC), bezpečnostního týmu CSIRT.CZ nebo vybraných projektů Laboratoří CZ.NIC.

Komunikace se týkala především témat spojovaných se základní činností sdružení, s jeho klíčovými projekty a aktivitami, ale také s tématy, která s činností sdružení souvisí, jako jsou kyberbezpečnost, ochrana osobních údajů nebo vzdělávání a osvěta v oblasti Internetu a internetových technologií.

Stejně jako v předešlých letech se tiskové výstupy objevovaly především v technicky zaměřených médiích. Nejčastěji se jednalo o portály Root.cz a Lupa.cz. V tištěné podobě se potom jednalo hlavně o časopisy Securityworld a IT Systems. Témata spojená s on-line bezpečností dětí na Internetu byla pak prezentována v časopise Řízení školy.

Zaměstnanci sdružení CZ.NIC publikovali v roce 2019 více než 60 autorských článků. Ondřej Filip, výkonný ředitel sdružení CZ.NIC, ale i další zaměstnanci byli hosty televizních nebo rozhlasových pořadů

především v České televizi, v Českém rozhlasu nebo na Frekvenci 1. Zájem byl o témata spojená s bezpečností v kyberprostoru, mobilním Internetem nebo českou národní doménou.

Nedílnou součástí komunikace s veřejností jsou pro správce české národní domény účty na sociálních sítích – Facebook, Twitter, Google+ (pouze do dubna 2019) a nově i LinkedIn. Příznivci jsou v pravidelných příspěvcích informováni o aktivitách sdružení, akcích a aktuálním dění v jednotlivých projektech. Nejsledovanějším účtem byl ten twitterový, který měl na konci roku 4 297 followerů, což je o 9 % více než v roce 2018. Hned za ním byl účet na Facebooku, kde mělo sdružení 2 984 fanoušků. Novinkou bylo oživení účtu na LinkedInu – k jeho sledování se přihlásilo 1 040 zájemců.

Důležitou součástí komunikace představují rovněž newsletter NIC-NEWS, jehož prostřednictvím jsou zasílány zprávy těm, kteří se přihlásili do stejnojmenné e-mailové konference, a online zápisník Blog zaměstnanců CZ.NIC. Díky aktivitě pracovníků sdružení bylo na blogu v roce 2019 publikováno 47 příspěvků. [Blog](#) plní roli oficiálního komunikačního kanálu sdružení, takže z něho čerpají i novináři z různě zaměřených médií.

	Výstupy v médiích		Sociální sítě (fanoušci)	
	Autorské články	Blog	Facebook	Twitter
2012	21	97	900	630
2013	29	95	1 100	1 000
2014	38	84	1 500	1 750
2015	57	82	1 800	2 370
2016	57	59	2 600	3 088
2017	73	49	2 826	3 573
2018	56	55	2 905	3 942
2019	63	47	2 984	4 297

Interní komunikaci pak zajišťuje především zpravodaj IN, který dostávají zaměstnanci CZ.NIC zpravidla jednou až dvakrát za 14 dní.

9.2 Popularizační seriály

Prozatím nejrozsáhlejší osvětovou aktivitou sdružení zaměřenou na širokou veřejnost je seriál Jak na Internet. Se svými 125 epizodami vysílanými na kanálech České televize v letech 2012–2019 dosáhl celkem na 225 milionů zhlédnutí. Vedle médií veřejné služby nachází seriál uplatnění rovněž v lokálních kabelových televizích. O popularitě seriálu svědčí také opakovaně příznivé výsledky v průzkumech povědomí u internetové veřejnosti. Pořad Jak na Internet zná více než čtvrtina (25–35 %) uživatelů Internetu.

Jak na Internet dnes již není pouze televizní seriál. Kanál YouTube prezentující on-line verzi jednotlivých epizod dosahuje přibližně půl milionu celkových zhlédnutí. S videoobsahem se lze setkat také v zábavních portálech autobusů a vlaků RegioJet nebo na Metodickém portálu RVP.cz

pro učitele. Rovněž rozšiřující texty publikované na stránkách jahnainternet.cz získávají na oblibě, o čemž svědčí mj. fakt, že jsou hojně citovány v absolventských pracích (viz. Theses.cz). Seriál vychází rovněž v komiksovém knižním zpracování.

Sdružení CZ.NIC v minulosti také umožnilo vzniknout několika koprodukčním pořadům České televize určeným pro děti a mládež. Šlo například o dvě sezóny seriálu Nauč tetu na netu nebo vybrané epizody z cyklu Lovci záhad. Na cílovou skupinu seniorů je zase zaměřen původní seriál Nebojte se Internetu (nebojteseinternetu.cz). Všechny uvedené videomateriály byly rovněž v roce 2019 dostupné on-line a systematicky využívány organizacemi zaměřujícími se na vzdělávání vybraných rizikových skupin – dětí a seniorů.

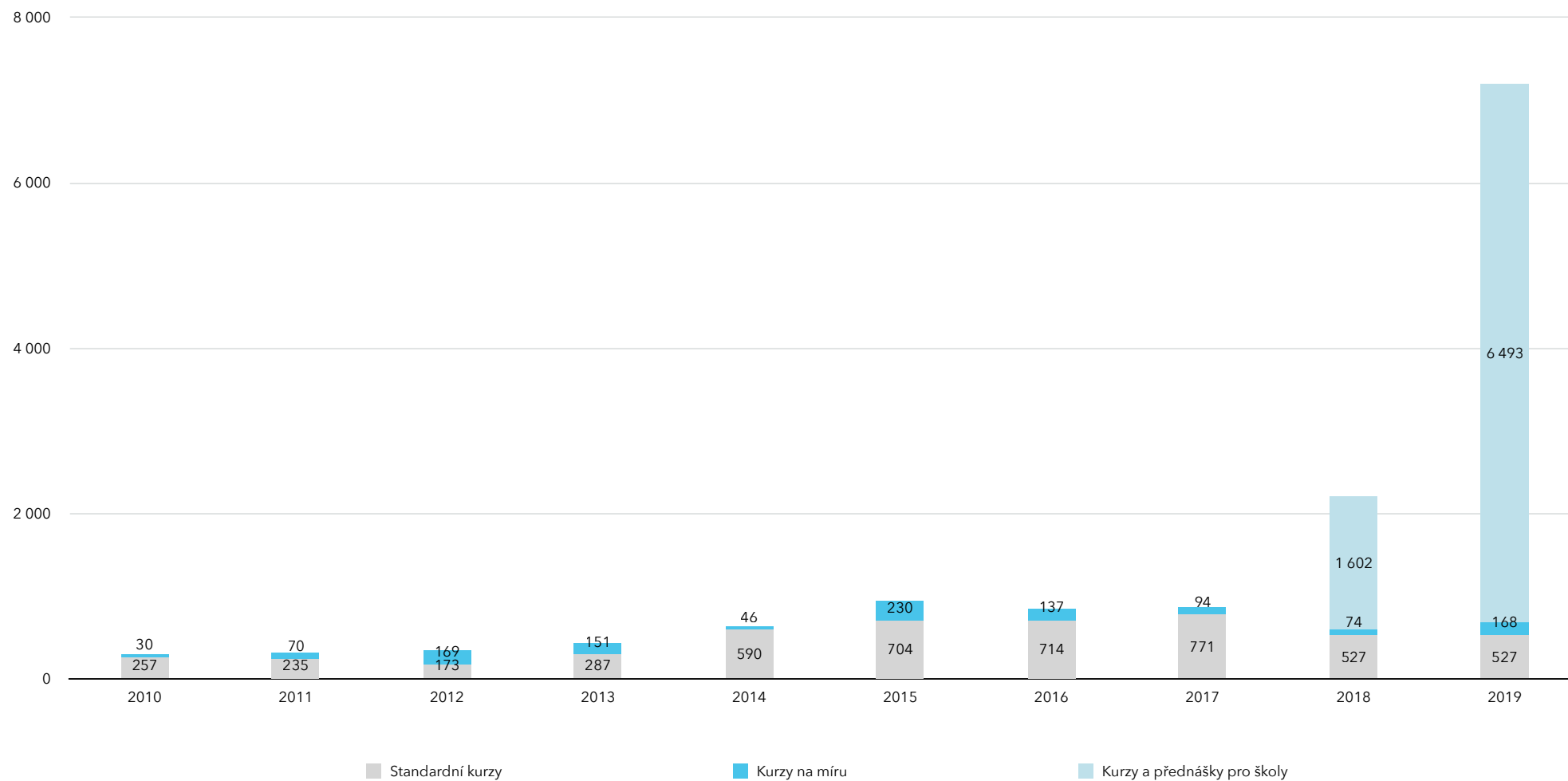
9.3 Výukové středisko Akademie CZ.NIC

V roce 2019 rozšířila Akademie CZ.NIC portfolio nabízených kurzů o tři novinky: Sphinx pro dokumentaristy, Kyberšikana a další rizikové jevy na Internetu, Forenzní analýza. Vedle těchto prezenčních kurzů vznikl v Akademii ve spolupráci s NÚKIB také nový elektronický kurz Digitální stopa pro žáky základních škol, jehož cílem je ochránit děti před riziky, která jim v kyberprostoru hrozí.

Akademie CZ.NIC v roce 2019 poskytovala svůj prostor nejenom pro interní školení a setkání zaměstnanců sdružení, ale také dalším organizacím a uskupením, jako jsou například ENISA, Vzdělávací institut střeďočeského kraje nebo PyLadies. V létě proběhl ve spolupráci

s Prahou 3 v prostorách akademie týdenní dětský Kybertábor. Akademie CZ.NIC nenabízí jen prostor, ale poskytuje také podporu dalším vzdělávacím aktivitám. V roce 2019 to byla zejména soutěž SOČ (Středoškolská odborná činnost).

Vývoj počtu studentů v Akademii CZ.NIC



Seznam odborných kurzů realizovaných v Akademii CZ.NIC v roce 2019

Název	Počet běhů	Počet studentů
3D tisk	1	7
Ansible - úvod do hromadné automatizace	6	88
Bezpečnost a soukromí na Internetu	3	28
Bezpečnost mobilních aplikací	1	8
Bezpečnost webových aplikací	1	5
Digitální design bez bariér pro začátečníky	2	18
DNSSEC - zabezpečení DNS	4	46
Dokumentování softwaru nástrojem Sphinx	1	3
Git - univerzální verzovací systém	2	25
IPv6 pro pokročilé	1	14
Kyberšikana a další rizikové jevy na Internetu	2	19
Nařízení eIDAS přehledně	2	16
Pokročilé síťování v Linuxu	6	90
Principy a správa DNS	3	35
Směrovací protokol BGP	2	28
Technical Writers' Exchange of Experience Workshop	1	20
Turris prakticky	2	23
Úvod do forenzní analýzy paměti	1	10
Úvod do Linuxu	3	29
Vim pro pokročilé	1	15

Seznam kurzů na míru realizovaných v Akademii CZ.NIC v roce 2019

Název	Počet běhů	Počet studentů
Bezpečné chování na internetu	1	30
Kyberšikana a další rizikové jevy na Internetu	8	60
Nelegální on-line obsah	3	78

Seznam kurzů a přednášek pro školy realizovaných v roce 2019

Název	Počet běhů	Počet studentů
(Ne)bezpečný mobil	62	1 310
Beseda s knihou "ON-LINE ZOO"	82	1 813
Digitální stopa	29	594
Fungování Internetu	58	1 235
Kyberšikana	34	1 034
Nelegální on-line obsah	18	507

Celkový počet všech kurzů realizovaných v Akademii CZ.NIC v roce 2019

Typ kurzu	Celkový počet běhů	Celkový počet studentů
Odborné kurzy	45	527
Kurzy na míru	12	168
Školy	283	6 493
Celkem	340	7 188

9.4 Konference

Sdružení CZ.NIC uspořádalo 14. a 15. listopadu 2019 tradiční konferenci Internet a Technologie (19). Poslední ročník konference nabídl příspěvky, které informovaly o novinkách ve světě domén a o aktualitách v klíčových projektech sdružení. Zařazeny byly také prezentace týkající se témat spojených s DNS nebo internetovou bezpečností.

V roce 2019 se sdružení CZ.NIC představilo na řadě akcí a odborných konferencích v České republice i v zahraničí. Z těch tuzemských jmenujme například InstallFest, Linux Days, Openalt, MakerFaire, Kam kráčejí komunikační sítě, Festival bezpečného Internetu (FBI), Internet 2020 nebo seminář o IPv6. V rámci zahraničních akcí se sdružení objevilo například na OpenCamp, FOSDEM nebo Peering Days.

Sdružení CZ.NIC, NIX.CZ a CESNET uspořádala v roce 2019 komunitní setkání CSNOG 2019 (Czech and Slovak Network Operators Group). Hlavním cílem této akce byla vzájemná výměna zkušeností mezi poskytovateli přístupu k internetu, provozovateli telekomunikačních sítí, registrátory domén provozovateli počítačových sítí a technickými nadšenci, a také diskuze nad aktuálními tématy a sdílení řešení vedoucích k rozvoji internetových sítí v České a Slovenské republice. Setkání proběhlo 28. a 29. května 2019 v Brně a zúčastnilo se ho 130 účastníků.

V souladu se svou strategií hostilo sdružení CZ.NIC společně s partnerem CISCO mezinárodní setkání internetových odborníků, vědců a inženýrů IETF 104. Do Prahy se jich mezi 23. až 29. březnem sjelo celkem 1 233.

9.5 Edice CZ.NIC

Vydávání odborných a popularizačních publikací s tématy souvisejícími s Internetem a jeho technologiemi je již tradiční osvětovou aktivitou sdružení. V Edici CZ.NIC vycházejí knihy v tištěné i elektronické verzi. Elektronické verze knih jsou zdarma ke stažení na webové stránce knihy.nic.cz a také v síti distributorů obsahu (Palmknihy, Wooky, eReading, Městská knihovna v Praze a nově v síti Flexibooks), a to ve formátu PDF nebo formátech určených pro elektronické čtečky (EPUB a MOBI). Tištěné knihy jsou nově k mání také v knižních distribučních sítích Kosmas, Euromedia Group, Pemic Books a na Slovensku v síti IKAR, čímž se

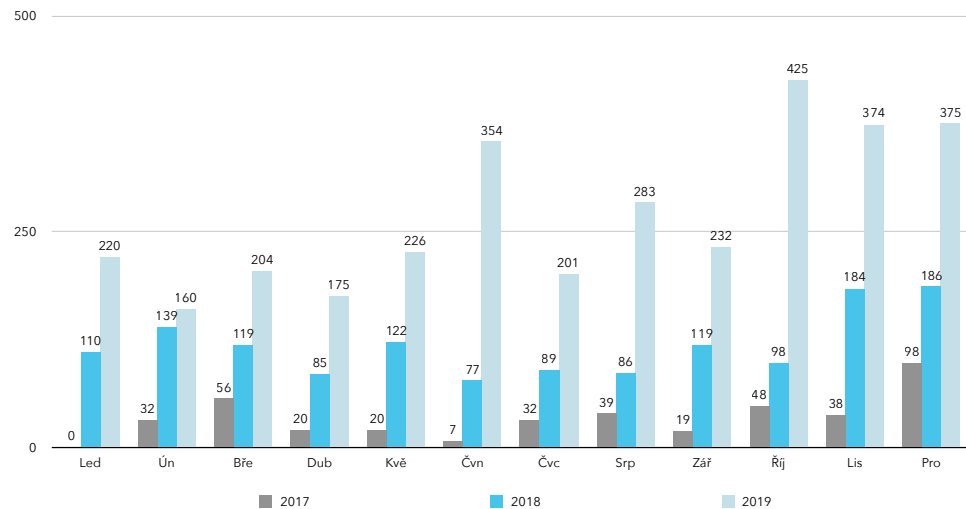
titulům Edice otevírá cesta na pulty stovek kamenných i internetových knihkupectví nejen v České republice, ale i na Slovensku.

Nově se otevřela i spolupráce v distribuci elektronických knih prostřednictvím portálu BookPort, který provozuje Grada. V distribuci tištěných knih se sdružení zaměřilo na další oborově specializované prodejní kanály. První vlaštovky jsou např. HW Kitchen jako distributor EduShieldu a knihy Hradla, volty, jednočipy. Druhá je pražská ZOO, která podpořila distribuci On-line ZOO knihy a omalovánky. V oslovování těchto menších, ale oborově specializovaných prodejních kanálů se bude pokračovat i v roce 2020.

V roce 2019 se Edice rozšířila o další tři tištěné tituly a audio knihu, čímž se nabídka rozrostla na 23 odborných či populárně naučných titulů. První titul Porty, bajty, osmibity osvědčeného autora Martina Malého je volným pokračováním jeho loni vydané publikace Hradla, volty, jednočipy. Autor popisuje konstrukci již složitějších obvodů. Na příkladu tří podrobně popsaných konstrukcí se čtenář naučí základní principy fungování osmibitových počítačů. Druhým titulem je již čtvrté aktualizované vydání velice žádané publikace IPv6 – Internetový protokol verze 6 zkušeného vysokoškolského pedagoga Pavla Satrapy. Třetí kniha Kryptografie okolo nás autora Karla Burdy popisuje využití kryptografie v běžném životě. V knize jsou vysvětleny vlastnosti vybraných kryptografických funkcí, jako je šifrování, hešování a podobně.

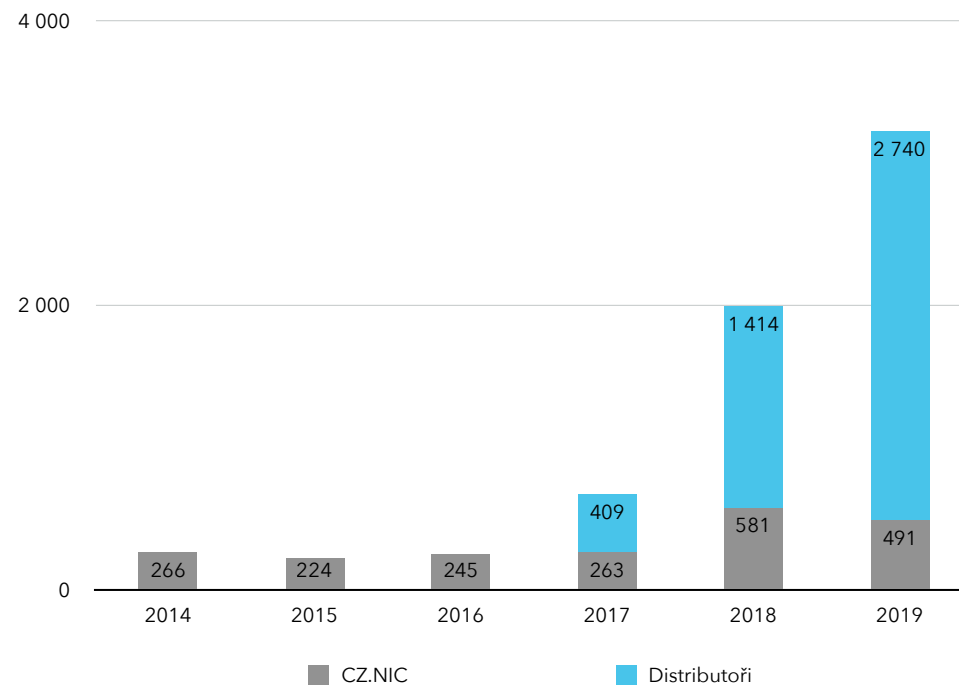
Zcela novým počinem je v Edici první vydaná audio kniha On-line ZOO, která navazuje na již dříve vydanou stejnojmennou publikaci. Mluvené slovo tak může jednoduše zpřístupnit základy bezpečného chování na Internetu i těm nejmenším.

Vývoj prodeje titulů v Edici CZ.NIC



V roce 2019 bylo v Edici CZ.NIC prodáno celkem 3 229 kusů tištěných knih, což představuje ve srovnání s rokem 2018 nárůst o 230 %.

Přehled prodeje knih podle distributorů



10 Spolupráce a partnerství

Internet dnes bez nadsázky představuje nejvýznamnější komunikační nástroj, který propojuje desítky milionů uživatelů na všech kontinentech. Často můžeme slyšet, že Internet nemá hranice a nespadá do pravomocí žádné vlády. To však neznamená, že Internet by nebyl řízen a neměl svá pravidla. Ta však, na rozdíl od mnoha jiných odvětví, často vytváří internetová komunita (včetně zaměstnanců sdružení CZ.NIC) představující velkou rodinu příznivců a podporovatelů této celosvětové sítě.

K tomu, aby úsilí žádného člena či organizace nepřišlo nazmar, je pak nezbytná vzájemná spolupráce, a to jak na národní, tak mezinárodní úrovni.

Spolupráce s tuzemskými partnery pomáhá najít ten nejpříjemnější systém správy národní domény pro českého uživatele a zároveň přispět, především díky projektům našich Laboratoří, k rozšíření nových technologií a k rozvoji informační společnosti.

Zahraniční spolupráce pomáhá nejen sledovat světové trendy, ale díky aktivní účasti zaměstnanců sdružení se rovněž podílí na jejich vytváření a ovlivňuje tak naše každodenní životy.

Díky své vysoké odbornosti jsou zástupci sdružení, a to jak členové managementu, tak ostatní zaměstnanci, vítanými hosty tuzemských i mezinárodních odborných fór.

10.1 Česká republika

Díky významu realizovaných aktivit je CZ.NIC přirozeným partnerem jak veřejné správy, tak zájmových sdružení působících v oblasti Internetu.

10.1.1 Spolupráce s veřejnou správou

Význam systému správy jmen domén a související internetové infrastruktury je srovnatelný s významem jiných kritických infrastruktur, například v oblasti energetiky a dopravy. Sdružení CZ.NIC, jako správce národní domény .CZ, považuje ochranu této infrastruktury za svoji povinnost i morální závazek vůči České republice. Navazuje spolupráci s řadou státních orgánů, jako jsou Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), Český telekomunikační úřad (ČTÚ), Ministerstvo vnitra České republiky (MV ČR) a Ministerstvo průmyslu a obchodu České republiky (MPO ČR).

Spolupráce s českým státem v oblasti kritické infrastruktury byla v roce 2017 prohloubena zahájením projektu „Zabezpečení DNS serverů v ČR“, který je realizován v rámci Programu bezpečnostního výzkumu pro potřeby státu v letech 2016–2019.

Zástupci sdružení CZ.NIC z oddělení „Rozvojových projektů“ se významně podíleli na implementaci nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (tzv. nařízení eIDAS). Kolega Jaromír Talíř se v souvislosti s provozem národního eIDAS uzlu zmiňovaného v kapitole 7.4 pravidelně účastnil jakožto zástupce České republiky zasedání eIDAS Technical SubGroup, která definuje technické standardy přeshraniční autentizace. Další z kolegů zase působil v expertních skupinách Evropské komise i při Ministerstvu vnitra.

Postavení důvěryhodného a spolehlivého partnera veřejné správy pak sdružení CZ.NIC potvrdilo rovněž v rámci projektu Safer Internet Center

(viz kapitola Grantové projekty), kdy převzalo provoz policejní linky pro hlášení kybernetické kriminality, a dále prohloubilo spolupráci s kraji, zejména pak projektem Kraje pro bezpečnější Internet.

Dále sdružení spolupracuje s Policií České republiky, s exekutorskými úřady, se soudy a úřady dle zákonného zmocnění, tedy s Úřadem pro ochranu osobních údajů, živnostenskými a finančními úřady, Českou obchodní inspekcí, Celní správou apod.

10.1.2 Spolupráce s neziskovým sektorem a společenská odpovědnost

Člověk v tísni

Mezi další společenské aktivity sdružení CZ.NIC patří podpora organizace Člověk v tísni, a to zejména jeho vzdělávacího projektu Jeden svět na školách, který nabízí školám dokumentární filmy a doprovodné metodické pomůcky k výuce aktuálních témat současného světa a novodobé historie.

Náš stát, naše data (Nadace OSF)

Náš stát, naše data je projektem Nadace OSF. Sdružení CZ.NIC je dlouhodobým partnerem projektu, jehož hlavními cíli jsou prosazování principů a standardů otevřených dat, stejně jako propagace, osvěta a koordinace aktivit i odborníků věnujících se tomuto tématu. Součástí tohoto partnerství byla v roce 2019 také účast na 4. ročníku veletrhu Open

Data Expo, kde se sdružení účastnilo s prezentacemi zaměřenými na Otevřená data a Turrís. Zástupci sdružení zasedli v odborných porotách soutěže Společně otevíráme data, která již posedmé v řadě ocenila nejlepší veřejné aplikace v kategoriích Transparentnost, Participace, Data v každodenním životě, Open Source a Solution App využívající otevřená data pro společensky prospěšné služby. Podpořeny byly také meet-upy, setkávání a budování platformy Česko.Digital – komunity špičkových vývojářů, designérů a produktových specialistů, kteří chtějí ve svém volném čase pomáhat státu i nestátním organizacím a dělat tak Česko lepším místem k životu.

Pomoc zvířatům

Sdružení CZ.NIC dlouhodobě přispívá pražské a zlínské zoologické zahradě na chov kasuára přílbového, jehož původním domovem je Nová Guinea a Austrálie.

10.1.3 Členství v oborových a zájmových organizacích

Česká televize - Děčko

Sdružení mělo i v roce 2019 svého zástupce v Děčkolegiu, neformálním sboru poradců, který poskytuje odborné rady, zpětnou vazbu a názory na program a obsah populárního dětského kanálu České televize Děčko a také napomáhá seznamovat rodiče s mediální problematikou.

NIX.CZ

Největší český Internet Exchange Point (IXP) zastřešuje tuzemské i zahraniční poskytovatele internetových služeb za účelem vzájemného propojení svých sítí. Sdružení NIX.CZ je největším IXP v ČR a jedním z nejvýznamnějších na světě. Sdružení CZ.NIC je členem NIX.CZ a aktivně přispívá k jeho činnosti především prostřednictvím projektu FENIX. Významné je i využití produktů Laboratoří CZ.NIC, zejména BIRD, v rámci NIX.CZ.

Zapojení v projektu FENIX

V roce 2013 pomohlo sdružení CZ.NIC založit na platformě největšího českého peeringového uzlu NIX.CZ projekt FENIX. Jeho hlavním smyslem je zajistit v případě masivních DoS útoků dostupnost internetových služeb mezi subjekty zapojenými do této aktivity. Projekt FENIX je určen společností, které poskytují připojení významným poskytovatelům připojení i obsahu, kteří potřebují zajistit provoz i v těch nejkritičtějších situacích.

Zapojení v projektu FENIX je umožněno všem subjektům, které splní vstupní podmínky. Tyto podmínky rezonují s tím, co sdružení CZ.NIC dlouhodobě svou činností prosazuje, tedy zejména s rozvojem důvěryhodné, bezpečné a stabilní internetové infrastruktury a obecně prospěšných služeb. Pro vstup do projektu FENIX je tedy například nutné provozovat svůj CERT/CSIRT tým, podporovat IPv6 a DNSSEC, mít implementován response rate limiting a používat filtrování zdrojových adres ve své síti ve smyslu BCP-38.

10.2 Zahraničí

Díky aktivitám sdružení na mezinárodní internetové scéně si zainteresované zahraniční organizace čím dál častěji vybírají CZ.NIC jako partnera pro spolupráci a Českou republiku jako místo konání svých setkání. Sdružení CZ.NIC tuto skutečnost vítá, neboť tak zástupci lokální

internetové komunity získávají snadnější přístup jak k zajímavým tématům, tak k předním světovým odborníkům ze světa Internetu.

10.2.1 Členství v oborových a zájmových organizacích

APWG (Anti-Phishing Working Group)

Globální koalice soukromých společností, státních institucí a bezpečnostních složek zaměřená na celosvětový boj s kybernetickým zločinem, především spamem.

CENTR (Council of European National Top Level Domain Registries)

Nezisková organizace sdružující správce národních i generických doménových jmen nejvyšší úrovně. Orientována je především na evropské registry, ale mezi členy jsou i zástupci vzdálenějších regionů – například Kanady či Japonska. Sdružení CZ.NIC je členem od roku 2001 a pravidelně se účastní jednotlivých jednání pracovních skupin. V čele CENTR Technical Working Group byl v roce 2019 Jaromír Talíř.

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

Důvěryhodná platforma, na které se setkávají klíčové subjekty a sdílejí své zkušenosti z DNS provozu, analýz a výzkumu tak, aby mohly co nejlépe a nejučinněji koordinovat svoji činnost, především v oblasti bezpečnosti. I v roce 2019 byl členem představenstva DNS-OARC Jaromír Talíř, již třetí

zástupce České republiky a sdružení CZ.NIC, a bude jím na základě volby valné hromady i v roce 2020.

EURid (The European Registry of Internet Domain Names)

Sdružení, které na základě pověření Evropské komise spravuje doménu nejvyšší úrovně .EU. CZ.NIC je jeho přidruženým členem a má svého zástupce v představenstvu.

EuroISPA (European Internet Services Providers Associations)

Evropská asociace poskytovatelů internetových služeb (ISP), která je největší organizací, sdružující více než 2 300 organizací z celého světa. Hlavním cílem EuroISPA, jejímž členem je sdružení CZ.NIC od roku 2008, je zastupovat ISP v rámci legislativních procesů Evropské unie a napomáhat výměně zkušeností mezi jednotlivými poskytovateli internetových služeb.

CSIRT Network

Zájmová skupina CSIRT týmů, která plní roli kontaktního místa pro povinné osoby identifikované ve směrnici NIS (směrnice Evropského Parlamentu a Rady EU o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii). Skupina řeší primárně technické otázky související s vykonáváním této agendy. V roce 2019 se tým CSIRT.CZ aktivně účastnil většiny setkání, kde se řešily například výstupy projektu Melicertes, který byl v CSIRT.CZ nasazen v rámci projektu CEF.

FIRST (Forum of Incident Response and Security Teams)

První mezinárodní organizace sdružující bezpečnostní týmy. Má kolem 400 členů a významně jsou v ní zastoupeny týmy americké a evropské. Jde o jedinou organizaci, která poskytuje členství týmům z celého světa a zastřešuje také produktové týmy. Členem organizace FIRST se tým CSIRT.CZ stal v roce 2015.

ICANN (Internet Corporation for Assigned Names and Numbers)

Mezinárodní nezisková organizace založená v roce 1998, jejímž hlavním úkolem je nejen správa a přidělování generických doménových jmen nejvyšší úrovně (gTLD) a národních doménových jmen nejvyšší úrovně (ccTLD), ale také IP adres. Sdružení CZ.NIC jako správce národní domény vysílá své zástupce na pravidelná jednání a jeho odborníci se aktivně zapojují do činnosti pracovních skupin. Ondřej Filip, výkonný ředitel sdružení CZ.NIC, v rámci ICANN působí jako člen prestižního výboru SSAC (Security & Stability Advisory Committee).

IETF (Internet Engineering Task Force)

Organizace založená již v roce 1986, která je bezprostředně spjata se zrodem Internetu. Tvoří ji mezinárodní komunita předních odborníků, síťových architektů i zástupců komerční sféry. IETF schvaluje a prosazuje internetové standardy, tzv. RFC dokumenty, kterými se řídí většina internetového provozu, a na některých z nich se aktivně podílí naši zaměstnanci. Setkání členů této organizace se také již několikrát uskutečnilo díky spolupráci sdružení CZ.NIC v Praze.

Pracovníci Laboratoří CZ.NIC se v IETF podílejí zejména na činnosti pracovních skupin DNSOP (provoz DNS), NETCONF (konfigurace síťových zařízení) a NETMOD (modelování konfiguračních a stavových

dat). Ladislav Lhotka, vedoucí Laboratoří CZ.NIC, je autorem nebo spoluautorem šesti standardů RFC. V březnu 2019 byl vydán nový internetový standard RFC 8528, který definuje volitelné rozšíření jazyka YANG pro modelování konfiguračních a stavových dat. I pod tímto standardem je podepsán Ladislav Lhotka.

INHOPE (International Association of Internet Hotlines)

INHOPE představuje mezinárodní asociaci více než 50 tzv. horkých linek zaměřených na boj s nezákonným on-line obsahem, převážně dětskou pornografií, a jeho eliminaci. Mezi hlavní přínosy členství v INHOPE patří přístup do databáze ICCAM (odvozeno z „I see Child Abuse Material“) a možnost efektivní spolupráce s dalšími zeměmi i institucemi, zejména Interpolem, při odstraňování nelegálního obsahu. Sdružení CZ.NIC s jím provozovanou linkou STOPonline.cz se stalo přidruženým členem asociace v červnu 2017. V roce 2018 sdružení v rámci realizace projektu Safer Internet Center získalo v této prestižní asociaci plné členství a o rok později získalo od této asociace speciální finanční odměnu jako ocenění za vysoký počet zpracovaných hlášení.

RIPE NCC (Réseaux IP Européens Network Coordination Centre)

Nezávislá nezisková organizace podporující internetovou infrastrukturu. Mezi její klíčové aktivity patří provoz RIR (Regional Internet Registry), který alokuje internetové zdroje a související služby (např. IP adresy) svým členům. Sdružení CZ.NIC se jako jeden z členů účastní nejen pravidelných setkání, ale participuje také na dalších tematických jednáních a školeních, která tato organizace pořádá. V roce 2019 se stal členem představenstva této organizace výkonný ředitel sdružení CZ.NIC Ondřej Filip.

TF-CSIRT

TF-CSIRT je organizace, která sdružuje bezpečnostní týmy převážně z Evropy. Tým CSIRT.CZ má v této organizaci nejvyšší možnou úroveň členství – certified. CZ.NIC-CSIRT je jejím akreditovaným členem.

11 Grantové projekty

V souladu se svým dlouhodobým cílem, zaměřeným na rozvoj internetových technologií a informační společnosti, a střednědobou koncepcí sdružení na roky 2016–2019 se sdružení CZ.NIC aktivně zapojilo do řady grantových projektů.

Grantové projekty představují velmi významný zdroj financování sdružení. Projekty rovněž podporují rozvoj a vzdělávání zaměstnanců CZ.NIC a umožňují jim podílet se na unikátních projektech, které často pomáhají určit budoucí směrování informační společnosti, projekty významně přispívají především k rozvoji bezpečnostního týmu CSIRT.CZ.

Díky evropským projektům se sdružení významně podílí také na budování infrastruktury určené především pro přeshraniční elektronické služby veřejné správy. Projekty realizované na národní úrovni významně přispívají k rozvoji projektu Turrís a realizace těchto projektů zároveň pomáhá posilovat postavení sdružení jako důvěryhodného partnera státu.

11.1 Zapojení do projektů evropské spolupráce

V únoru 2019 se sdružení CZ.NIC připojilo k realizaci nového projektu SPARTA. V průběhu roku 2019 také schválila Evropská komise nový projekt RegID, jehož realizace proběhne v letech 2020–2021.

V roce 2019 byly za podpory Evropské komise realizovány následující projekty.

CyberExchange

Sdružení CZ.NIC je koordinátorem mezinárodního projektu CyberExchange, který reaguje na zvyšující se hrozby v oblasti kybernetické bezpečnosti a z toho vyplývající nutnosti přeshraniční spolupráce v boji proti nim. Do projektu je zapojeno celkem jedenáct národních a vládních bezpečnostních týmů z České republiky, Chorvatska, Lotyšska, Lucemburska, Malty, Polska, Rakouska, Rumunska, Řecka a Slovenska.

Zástupci těchto týmů se v průběhu projektu účastní stáží, během nichž mají možnost vyměnit si vzájemně zkušenosti a posílit své odborné kapacity. Projekt dále podporuje technické stáže, kde se zaměřuje na podporu při nasazování softwarových nástrojů, které byly jednotlivými týmy vyvinuty tak, aby sloužily širší bezpečnostní komunitě a boji proti kybernetickým hrozbám i v jiných zemích. Tím projekt vhodně doplní platformu MeliCERTes, která představuje jeden z takzvaných stavebních bloků přeshraničních služeb digitální infrastruktury.

V roce 2019 se uskutečnilo celkem čtrnáct výměnných stáží, přičemž dvou z nich se zúčastnil i CSIRT.CZ. Díky těmto dvěma výměnám proběhl například návrh a zkušební deployment aplikace Zone Monitor, která čerpá ze seznamu nově přidávaných certifikátů a hlídá, zda se mezi nimi vyskytuje doména podezřelá na phishing, nebo vydání knihovny Envelope, která abstrahuje vnitřní strukturu e-mailového objektu a tím významně zjednodušuje práci s posíláním e-mailů a šifrováním technologiemi GPG a S/MIME.

CZ.PEPS (Czech Pan European Proxy Services)

Cílem projektu CZ.PEPS, který probíhal v letech 2016–2019, byla především implementace a provoz národní infrastruktury (tzv. eIDAS node) pro přeshraniční uznávání elektronické identifikace v Evropě,

a to v souladu s nařízením Evropského parlamentu a Rady č. 910/2014 (tzv. eIDAS). Problematika fungování eIDAS uzlu je podrobněji popsána v kapitole 7.4.

SIC CZ (Safer Internet Center - Bezpečnější Internet)

Sdružení CZ.NIC přebralo od roku 2019 koordinaci národních aktivit zaměřených na zlepšení on-line bezpečnosti dětí a prevenci v České republice a novým projektem „Bezpečně na netu“ navazuje na projekt Saferinternet.cz, ukončený v prosinci 2018. Do nového projektu je od začátku zapojena také Linka bezpečí, která zvýšila díky tomuto partnerství své kapacity zaměřené na případy spojené především s kyberšikanou, sextingem nebo lákáním na nebezpečné schůzky. Jako národní centrum chceme přispět hlavně k tomu, aby jednotlivé projekty v rámci České republiky nevznikaly jako konkurenční, ale chceme tyto jednotlivé aktivity propojovat, vedeme proto dialog s mnoha partnery nebo zástupci státu.

Kromě vzdělávacích kurzů pro školáky, kteří jsou nejdůležitější cílovou skupinou, jsou realizovány semináře pro odbornou veřejnost, pedagogy, rodiče nebo státní správu. Do konce roku 2019 bylo uskutečněno 318 vzdělávacích akcí na 180 místech České republiky. Mezi tato místa patří i návštěva patnácti dětských domovů. Vlastní konference byly uspořádány dvě. První na květnovém Zlínském filmovém festivalu pro děti a mládež, kde současně proběhl Youth panel a Advisory board. Uskutečnil se také seminář v Senátu Parlamentu České republiky.

Ve spolupráci s internetovou televizí MALL.TV byl natočen úspěšný seriál #Martyisdead (mall.tv/martyisdead), který je inspirován skutečnými případy kyberšikan. Seriál získal cenu pro nejlepší webseriál střední a východní Evropy na festivalu Serial Killer a v současné době má statisíce zhlédnutí. Natočen byl také krátký snímek režiséra Braňy Holička Maturant, který se věnuje tématům závislosti, pravdě a lži na internetu. Současně s ním

vznikla i metodika, jak s tímto filmem pracovat ve školách. Za zmínku stojí i letní kampaň věnovaná nebezpečným výzvám v online prostředí (online challenge). Pro nejmenší děti pak sdružení rozvíjí rakouský projekt ON-LINE ZOO, pro který byly vytvořeny omalovánky a audiokniha.

K úspěšným službám patří i linka STOPonline.cz, která je určena k hlášení nezákonného obsahu, zejména zneužívání dětí, nepatřičné dětské nahoty a kybergroomingu. Linka je provozována na základě memoranda s Národní centrálou proti organizovanému zločinu a Policií České republiky. V roce 2019 přijala celkem 3 224 hlášení, což je o 800 případů více než o rok dříve. Ještě výraznější růst pak byl zaznamenán u počtu případů nahraných do mezinárodní databáze ICCAM, kdy počet nahlášených stránek vzrostl z 371 v roce 2018 na 640 incidentů nahraných v roce 2019. Tento nárůst byl způsoben jak zvyšujícím se povědomím o práci STOPonline, tak také vlastní analytickou činností operátorů STOPonline.

Vedle kyberšikan se projekt zaměřuje i na bezpečné užívání mobilních zařízení a aplikací. Z tohoto důvodu byly k aplikaci Tablexia vytvořeny tři nové hry, které jsou zaměřeny na trénink pozornosti, prostorové orientace a paměti. Právě tyto kognitivní funkce jsou nejčastěji postihovány nadměrným užíváním mobilních zařízení a aplikací.

Podpora rozvoje kapacit v oblasti kybernetické bezpečnosti v České republice (Strengthening cyber-security capacities in the Czech Republic)

Projekt realizovaný v letech 2017-2019 byl zaměřen především na posílení znalostních a technických kapacit národního bezpečnostního týmu CSIRT.CZ a jeho roli vycházející z evropské směrnice o informační a síťové bezpečnosti (tzv. NIS Directive). V průběhu realizace projektu se podařilo vytvořit a implementovat nástroj „Routing hijack monitoring“, který usnadňuje boj proti kybernetickým útokům. Rovněž se podařilo

národnímu bezpečnostnímu týmu CSIRT.CZ získat nejvyšší status (certified) u TF-CSIRT. Součástí projektu byla též podpora zakládání bezpečnostních týmů v České republice a jejich internacionalizace v rámci TF-CSIRT.

Součástí projektového konsorcia byl i český neutrální propojovací uzel NIX.CZ, který ve spolupráci se sdružením CZ.NIC v rámci projektu rozvíjel především projekt FENIX.

THREAT-ARREST

Cílem vědeckého projektu THREAT-ARREST, realizovaného v rámci prestižního evropského programu Horizon 2020, je vyvinout pokročilou platformu pro školení zahrnující emulaci, simulaci herní a vizualizační kapacity sloužící různým typům subjektů (tzv. stakeholders) k přípravě a rozvoji odborných znalostí v oblasti ochrany vysoce rizikových kybernetických systémů a organizací včetně schopnosti čelit pokročilým, známým i novým počítačovým útokům.

Za účelem dosažení tohoto cíle je v rámci projektu plánováno především vyvinutí tzv. CTPP (Cyber Threat and Training Preparation) platformy určené k nácviku obrany před kybernetickými útoky a zlepšování ochrany vybraných systémů.

SPARTA (Horizon 2020)

V roce 2019 se sdružení CZ.NIC, společně s Vysokým učením technickým v Brně a sdružením CESNET zapojilo do dalšího projektu realizovaného v rámci programu Horizon 2020 – SPARTA, v němž došlo ke spojení 44 organizací zaměřených na vědu a výzkum, technologické inovace a společenské vědy. Tato komunita si klade za cíl přehodnotit dosavadní způsob provádění výzkumu kybernetické bezpečnosti v Evropě. V rámci spolupráce dojde k vývoji a sdílení řešení, která pomohou

bezpečnostním expertům předcházet počítačové kriminalitě a zvyšovat kybernetickou bezpečnost.

11.2 Zapojení do národních a dalších projektů

Vedle evropských projektů se sdružení CZ.NIC zapojuje rovněž do národních projektů, především do bezpečnostního výzkumu ČR.

Ludus

V říjnu 2019 skončil tříletý projekt podpořený Technologickou agenturou ČR v rámci programu Epsilon. Sdružení CZ.NIC na něm spolupracovalo s ČVUT. Projekt využíval vědeckých poznatků konkrétně z oblasti strojového učení a aplikace teorie her, a to ke zvýšení kolaborativní obrany proti internetovým útokům. V rámci projektu byl vytvořen herně-teoretický model, který na základě síťové interakce umožňuje vytvořit filtrovací pravidla pro ochranu routerů.

Dále byla představena celková bezpečnostní metrika za účelem detekce útoků a měření míry bezpečnosti jednotlivých zařízení. Jako infrastruktura pro testování a demonstraci tohoto systému byla využívána síť routerů Turris.

Predikce a ochrana před kybernetickými incidenty (PROKI)

Cílem projektu podpořeného v rámci bezpečnostního výzkumu ČR na léta 2015–2020 je zejména vybudování systému zaměřeného na

analýzu informací o kybernetických incidentech z celé řady zdrojů a vyhodnocení těchto informací Národním bezpečnostním týmem CSIRT.CZ, provozovaným sdružením CZ.NIC dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Vybudovaný systém následně umožní sdílení informací o kybernetických nebezpečích mezi klíčovými hráči, především národním a vládním CERT/CSIRT a významnými ISP.

Vybudování a ověřovací provoz systému Cyber Threat Intelligence (CTI)

Projekt je podpořený Ministerstvem vnitra ČR v rámci Programu bezpečnostního výzkumu pro potřeby státu 2016–2021. Zaměřuje se na posílení ochrany kritické informační infrastruktury a dalších důležitých informačních systémů a sítí. Prostřednictvím vybudování účinného systému detekce, identifikace a predikce kybernetických hrozeb a vyhodnocování kybernetických bezpečnostních incidentů (tzv. Cyber Threat Intelligence) se snaží omezit škody způsobené kybernetickou kriminalitou.

Součástí projektu je též distribuce a umístění více než 800 hardwarových sond založených na routerech Turris, které budou v prostředí vybraných subjektů veřejné správy fungovat jako zařízení pro sběr dat a zároveň ochranu před kybernetickými útoky.

12 **Struktura sdružení**

12.1 Členská základna

Členská základna sdružení je tvořena celou řadou subjektů, které se významným způsobem podílejí na fungování českého Internetu. Mezi členy lze nalézt nejen zástupce poskytovatelů internetových a telekomunikačních služeb, registrátory jmen domén, vydavatele internetových i tištěných médií či podnikatele v elektronickém obchodu, ale i subjekty, pro které je Internet a jméno domény důležitým komunikačním nástrojem.

Sdružení CZ.NIC je tak jedním z míst, kde se mohou tyto reprezentanti setkávat a zároveň ovlivňovat budoucí směřování českého Internetu. Široké spektrum podnikatelských aktivit členů a jejich zapojení do činnosti sdružení, ať již formou účasti na valných hromadách, pracovních skupinách a seminářích, v e-mailových konferencích, či přímo prací v orgánech sdružení, obohacuje a dále rozšiřuje znalostní portfolio sdružení a umožňuje mu nadále zefektivňovat jeho řízení a reagovat na neustálý vývoj, který je pro Internet typický.

Podmínky členství

Členem sdružení se může stát právnická osoba, která splní obecné podmínky členství, mezi něž patří umístění sídla nebo organizační složky na území některého z členských států Evropské unie, držení alespoň jednoho jména domény v ccTLD .CZ a zaplacení vstupního členského příspěvku.

Členové sdružení jsou rozděleni do tří komor – komory držitelů jmen domén, komory ISP a komory registrátorů. Speciální podmínky členství v jednotlivých komorách určují stanovy. Komorové uspořádání přináší prospěch členům sdružení, kteří tak mohou společně s dalšími podobně

orientovanými subjekty snáze formulovat a hájit své názory a zájmy. Komorové uspořádání rovněž zefektivňuje průběh a jednání orgánů sdružení, zejména kolegia a valné hromady.

12.1.1 Počet členů dle komor

K 31. 12. 2019 mělo sdružení CZ.NIC celkem 116 členů. V komoře držitelů jmen domén přibyli tři noví členové, v komoře ISP jeden člen a dva členové opustili komoru registrátorů.

Rozdělení členů dle komor

Komora držitelů jmen	62 %
Komora ISP	23 %
Komora registrátorů	15 %

Vývoj počtu členů dle komor

Rok	Komora držitelů jmen domén	Komora ISP	Komora registrátorů	Celkem
2005	19	10	9	38
2006	27	8	11	46
2007	27	14	11	52
2008	30	15	12	57
2009	32	17	14	63
2010	37	21	19	77
2011	50	24	20	94
2012	61	27	18	106
2013	65	27	19	111
2014	69	24	20	113
2015	72	23	20	115
2016	67	25	20	112
2017	71	26	18	115
2018	69	26	19	114
2019	72	27	17	116

12.1.2 Přehled členů dle komor

Přehled členů v jednotlivých komorách k 31. 12. 2019.

Komora držitelů jmen domén (společnost, IČO)

ABRATICA s. r. o.	26108534
ACOMWARE s. r. o.	25047965
ADAPTIVITY s. r. o.	24156027
AdminIT s. r. o.	27864901
Advio Network, s. r. o.	28565673
Adytia Innovation OÜ	14498430
AKREDIT, spol. s r. o.	25797387
ALEF NULA, a. s.	61858579
ALENSA, s. r. o.	27179681
AliaWeb, spol. s r. o.	26117363
Asociace pro elektronickou komercij, z. s.	68684797
AUDITEL, s. r. o.	26775034
CD PROFESIONAL security agency, s. r. o.	25712713
CISCO SYSTEMS (Czech Republic) s. r. o.	63979462
ComSource s. r. o.	29059291
Com-Sys TRADE spol. s r. o.	16188781
CQK HOLDING a. s.	28405579
CYBERSALES a. s.	26199653
Datahost s. r. o.	26390973
DELL Computer, spol. s r. o.	45272808
ECOMOLE LTD.	9526615
ekolo.cz s. r. o.	27141659
EXPLORER, a. s.	26726653

Fortion Networks, s. r. o.	26397994
Greenlux s. r. o.	28608747
Holubová advokáti s. r. o.	24686727
H17 Networks, s. r. o.	27374041
ICZ a. s.	25145444
igloonet, s. r. o.	27713482
I. H. P. společnost s ručením omezeným	48117846
INBES, spol. s r. o.	14502593
Intell. Net s. r. o.	27971546
Internet Info, s. r. o.	25648071
Internet Mall, a. s.	26204967
i - registry s. r. o.	28451082
Klíč, spol. s r. o.	28129377
Laurián s. r. o.	29018919
MAFRA, a. s.	45313351
Mailkit s. r. o.	26449901
MARIAS s. r. o.	26136139
MASANTA s. r. o.	25730533
MEDIA FACTORY Czech Republic a. s.	26288311
Michal Krsek & partneři s. r. o.	27418570
MITE Infonet s. r. o.	25660292
Moonlake Web Services, s. r. o.	29249911
Neutral czFree eXchange, z. s. p. o.	75093201
NEW MEDIA GROUP s. r. o.	26124611
Nux s. r. o.	27234631
Občanské sdružení Ubuntu pro Českou republiku	22674608
Orego finance s. r. o.	24718955
Panificium, s. r. o.	4526767
PharoCom s. r. o.	25172131
Prague Business Office s. r. o.	27143481
Pražský Účetní Servis s. r. o.	26740575
Q3, s. r. o.	26226073
Qrator Labs CZ s. r. o.	3620174

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

Komora ISP (společnost, IČO)

ABAK, spol. s r. o., čes. ABAK, GmbH něm. ABAK, Co.Ltd. angl.	40763153
CASABLANCA INT s. r. o.	25079832
CentroNet, a. s.	26165473
CESNET, z. s. p. o.	63839172
COOLHOUSING s. r. o.	14893983
ČD - Telematika a. s.	61459445
České Radiokomunikace a. s.	24738875
Dragon Internet a. s.	27237800
Družstvo EUROSIGNAL	26461129
Faster CZ spol. s r. o.	60722266
FreeTel, s. r. o.	24737887

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

Komora registrátorů (společnost, IČO)

ACTIVE 24, s. r. o.	25115804
Dial Telecom, a. s.	28175492
e-BAAN Net s.r.o.	26867257
IGNUM, s. r. o.	26159708
INTERNET CZ, a. s.	26043319
KRAXNET s. r. o.	26460335
Media4web, s. r. o.	26735903
ONE.CZ s. r. o.	25503651
ONEsolution s. r. o.	27710335
O2 Czech Republic a. s.	60193336
Seonet Multimedia s. r. o.	27522041
Seznam.cz, a. s.	26168685
Stable.cz s. r. o.	28741048

TELE3 s. r. o.	26096960
TERMS a. s.	14499037
Web4U s. r. o.	26058774
ZONER software, a. s.	49437381
Web4U s. r. o.	26058774
ZONER software, a. s.	49437381

12.2 Orgány sdružení

12.2.1 Valná hromada

Nejvyšší orgán sdružení představuje valná hromada, ve které jsou všichni členové sdružení. Ti jsou rozděleni do tří komor – komory registrátorů, komory ISP a komory držitelů jmen domén. Právo zúčastnit se jednání valné hromady a prosazovat své nápady, názory a připomínky má každý člen sdružení.

12.2.2 Kolegium

Kolegium je orgánem sdružení složeným ze členů volených jednotlivými komorami valné hromady a případně dalšími osobami. Mezi pravomoci kolegia patří například schvalovat koncepci a rozpočet sdružení, schvalovat smlouvy uzavírané mezi sdružením a státem nebo volit a odvolávat členy představenstva a členy dozorčí rady. Kolegium má celkem 21 členů, z toho

18 členů volí jednotlivé komory valné hromady. Tři členové jsou nominováni orgány veřejné správy. Funkční období členů kolegia je tříleté.

Členové kolegia volení valnou hromadou v období od 1. 1. 2019 - 18. 12. 2019

Komora držitelů jmen domén

- Marek Antoš
- Dan Ohnesorg
- Jan Redl
- Karel Taft
- Pavel Tvrdík
- David Vorlíček

Komora ISP

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

Komora registrátorů

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

Členové kolegia volení valnou hromadou v období od 19. 12. 2019 - 31. 12. 2019

Komora držitelů jmen domén

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

Komora ISP

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

Komora registrátorů

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

Členové kolegia nominovaní orgány státní správy:

- Zina Bumbálková, Ministerstvo průmyslu a obchodu České republiky
- Marie Moravcová, Hospodářská komora České republiky
- Jiří Peterka, Český telekomunikační úřad

12.2.3 Představenstvo

Představenstvo je statutárním orgánem, řídí činnost sdružení a zastupuje jej.

Členové představenstva v období 1. 1. - 31. 12. 2019

- Karel Taft (* 1971), předseda představenstva
- Marek Antoš (* 1979), místopředseda představenstva
- Tomáš Košňar (* 1965), člen
- Martin Kukačka (* 1980), člen
- Jiří Kysela (* 1955), člen

12.2.4 Dozorčí rada

Kontrolní orgán sdružení, který dohlíží na výkon působnosti představenstva a uskutečňování činnosti sdružení.

Členové dozorčí rady 1. 1. - 31. 12. 2019

- Jan Redl, předseda dozorčí rady
- Ilona Filípková, člen
- Vlastimil Pečínka, člen

12.2.5 Management

- Ondřej Filip, výkonný ředitel
- Martin Peterka, provozní ředitel, zástupce výkonného ředitele
- Tomáš Fuňka, finanční ředitel
- Zdeněk Brůna, technický ředitel
- Ladislav Lhotka, vedoucí výzkumného týmu (Laboratoře CZ.NIC)
- Michal Hrušecký, vedoucí oddělení vývoje hardware
- Jaromír Talíř, technický partner
- Ondřej Písek, marketingový ředitel
- Vilém Sládek, PR manažer

13 Lidské zdroje

Síla sdružení spočívá v profesně způsobilých a kvalifikovaných zaměstnancích, kteří jsou nezbytní pro naplňování jeho cílů a další rozvoj. U mnohých zaměstnanců lze bez nadsázky tvrdit, že se jedná o přední odborníky v oboru, kteří mají nejen tuzemské, ale rovněž mezinárodní renomé. Za účelem posílení jednotlivých kompetencí se všichni zaměstnanci průběžně dále vzdělávají, a to jak v oblasti cizích jazyků, tzv. měkkých dovedností, nebo v odborných znalostech, tak aby dosáhli maximálních odborných a osobních kvalit a svými znalostmi a dovednostmi přispívali k dalšímu rozvoji sdružení a tím i českého Internetu.

13.1 Stav a vývoj počtu zaměstnanců

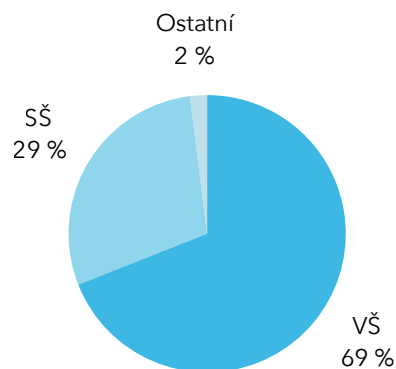
V roce 2019 mírně stoupl počet zaměstnanců sdružení. Zásadní novinkou je, že byl do sdružení přijat finanční ředitel. Posílily týmy zajišťující vývoj a bezpečnost a z laboratoří se vyčlenilo nové samostatné oddělení vývoje HW.

Oddělení	Stav			
	Počet zaměstnanců (k 31. 12. 2018)	Počet úvazků (k 31. 12. 2018)	Počet zaměstnanců (k 31. 12. 2019)	Počet úvazků (k 31. 12. 2019)
Vedoucí pracovníci (management)	7	7,000	8	8,000
Marketing/PR	8	7,500	8	7,750
Akademie	2	2,000	2	2,000
Vývoj	20	18,200	22	19,275
Síťová správa	12	10,875	10	8,875
Laboratoře CZ.NIC	50	42,250	27	24,100
Právní	2	1,625	2	1,750
Sekretariát	2	2,000	2	2,000
HR	1	0,800	1	1,000
Zákaznická podpora	11	10,800	11	10,800
CSIRT	9	8,550	10	9,000
Oddělení vývoje HW	0	0,000	25	20,750
EU projekty	3	3,000	3	3,000
Celkem	127	114,600	131	118,300

13.2 Struktura zaměstnanců

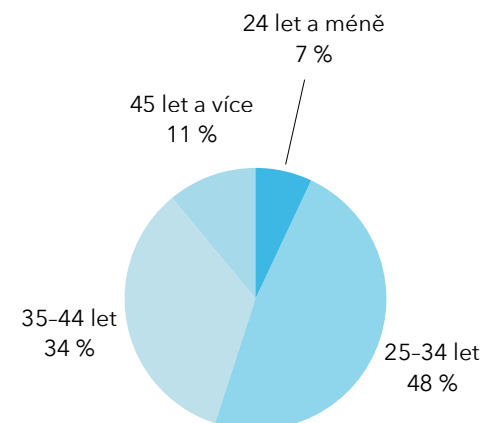
Struktura zaměstnanců dle vzdělání

Většina zaměstnanců sdružení má vysokoškolské vzdělání. Sdružení CZ.NIC dává příležitost k získání profesních zkušeností i čerstvým absolventům vysokých škol, pro které se snaží budovat vhodné podmínky, a to včetně umístění do poboček v Brně, Českých Budějovicích a Plzni. I díky tomu se podařilo udržet, a dokonce mírně navýšit, podíl vysokoškolsky vzdělaných pracovníků.



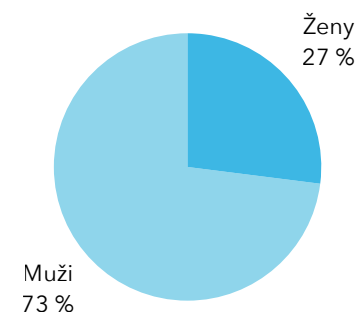
Struktura zaměstnanců dle věku

Věkový průměr zaměstnanců sdružení je 35 let. Z hlediska věkové struktury převládají zaměstnanci ve věku od 25 do 34 let.



Struktura zaměstnanců dle pohlaví

Při přijímání nových zaměstnanců podporuje sdružení CZ.NIC rovné příležitosti a zapojení žen. V roce 2019 se ve sdružení opět podařilo navýšit počet zaměstnaných žen. Má na tom jistě svůj podíl i možnost pracovat na zkrácený úvazek, který umožňuje skloubit pracovní a rodičovské povinnosti. Vzhledem ke struktuře absolventů technických oborů vysokých škol však, podobně jako v jiných technologických firmách, stále převládá podíl mužů.





14 Vybrané finanční ukazatele

14.1 Hospodářský výsledek po zdanění

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

V tisících Kč

14.2 Rozvaha

	2011	2012	2013	2014	2015	2016	2017	2018	2019
Aktiva celkem	361 566	387 674	405 154	431 392	449 278	491 643	503 747	534 656	569 478
Stálá aktiva	8 781	63 840	77 095	101 406	89 398	84 611	85 885	89 103	89 001
Nehmotný majetek	0	300	249	331	281	1 914	659	1 438	1 333
Hmotný majetek	8 781	63 540	76 846	101 075	89 117	82 697	85 226	87 665	87 668
Finanční investice									
Cenné papíry									
Oběžná aktiva	351 125	322 087	326 095	327 745	358 842	406 080	416 699	444 082	479 202
Zásoby	278	189	277	453	798	14 340	20 829	40 435	41 045
Dlouhodobé pohledávky	1 379	1 335	59	59	58	58	304	258	264
Krátkodobé pohledávky	12 180	10 676	18 540	22 100	4 948	6 282	16 870	8 602	10 161
Finanční majetek	337 288	309 887	307 219	305 133	353 038	385 400	378 696	394 787	427 732
Ostatní aktiva	1 660	1 747	1 964	2 241	1 038	952	1 163	1 471	1 275
Pasiva celkem	352 036	387 674	405 154	431 392	449 278	491 643	503 747	534 656	569 478
Vlastní jmění	243 795	261 094	274 591	288 397	302 395	324 045	332 308	338 039	358 705
Základní jmění									
Kapitálové fondy									
Fondy tvořené ze zisku	44 597	44 597	93 784	107 393	121 198	135 197	156 847	167 121	172 853
Hospodářský výsledek minulých let	166 570	199 937	167 198	167 198	167 198	167 198	165 185	165 185	165 185
Hospodářský výsledek účetního období	32 628	16 560	13 609	13 806	13 999	21 650	10 276	5 733	20 667
Cizí zdroje	15 988	17 684	27 479	22 497	32 140	48 059	53 906	67 723	68 862
Rezervy	9 530	884	1 832	1 662	2 662	2 359	3 064	6 454	8 691
Dlouhodobé závazky		241	304	235	1 344	617	8 571	9 990	23
Krátkodobé závazky	15 988	16 559	25 343	20 600	28 134	45 083	42 271	51 279	60 148
Bankovní úvěry									
Ostatní pasiva	92 253	108 896	103 084	120 498	114 743	119 539	117 533	128 894	141 911

V tisících Kč

14.3 Výkaz zisků a ztrát

	2011	2012	2013	2014	2015	2016	2017	2018	2019
Výkony a prodej	127 135	134 030	142 295	155 134	167 480	195 269	196 746	189 797	213 574
Z toho tržby a prodej	127 133	134 144	138 755	150 880	166 318	194 897	196 746	189 797	213 574
Aktivace	0	0	3 379	4 044	797	153	0	0	0
Výkon. spotřeba a náklady	44 440	70 414	67 042	66 335	64 701	73 668	75 970	67 523	70 268
Přidaná hodnota	82 693	63 616	75 253	88 799	102 779	121 754	120 776	122 274	143 306
Osobní náklady	39 227	43 328	57 245	66 541	72 930	85 706	98 706	111 018	117 380
Odpisy majetku	6 145	4 183	4 922	13 296	15 552	16 807	16 524	12 747	17 104
Zúčtování rezerv	533	313	1 020	-137	1 020	-124	393	2 256	3 683
Jiné provozní výnosy	1 208	1 082	2 290	2 029	1 800	1 884	12 184	13 304	13 813
Jiné provozní náklady	351	626	916	1 432	994	1 789	1 865	1 701	1 322
Provozní hospodářský výsledek	37 795	16 245	13 442	9 664	14 259	19 450	15 472	8 807	17 548
Jiné finanční výnosy	8 435	6 724	78 118	42 736	40 943	13 555	96 788	57 582	30 343
Jiné finanční náklady	4 623	685	74 915	38 254	39 428	11 731	100 810	58 233	25 590
Hospodářský výsledek z finančních operací	3 812	6 039	3 203	4 482	1 515	1 824	-4 022	-651	6 039
Hospodářský výsledek za běžnou činnost	41 607	22 284	16 645	14 146	15 774	21 274	11 450	8 156	23 587
Daň z příjmů	8 979	5 724	3 036	340	1 775	-376	1 174	2 423	2 920
Hospodářský výsledek po zdanění	32 628	16 560	13 609	13 806	13 999	21 650	10 276	5 733	20 667

V tisících Kč

14.4 Vývoj tržeb

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

V tisících Kč

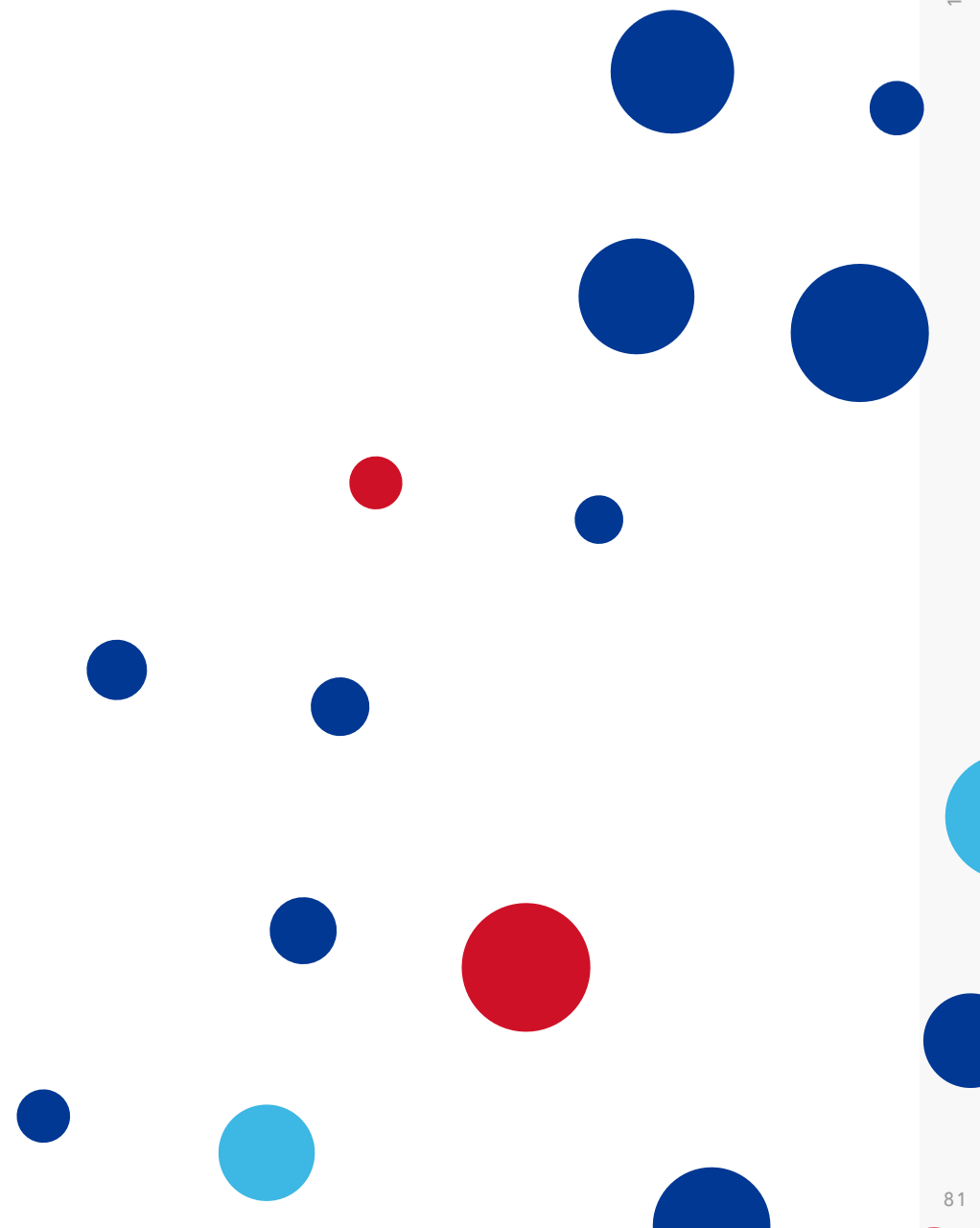
15 Seznam dodavatelů

Seznam dodavatelů dle čl. 45.4. Stanov:

České Radiokomunikace a. s.

IČO 24738875

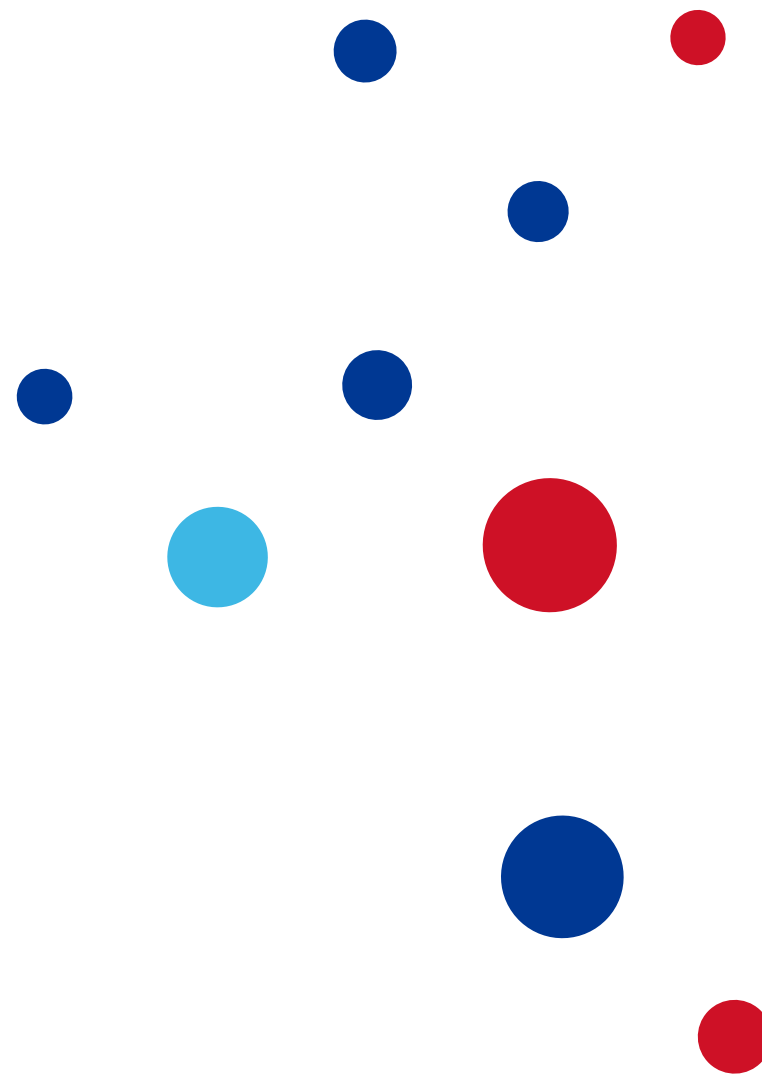
5 656 598,40 Kč





16 Údaje o skutečnostech mezi dnem účetní závěrky a valnou hromadou

V uvedené době nedošlo k žádným událostem, které mají vliv na údaje předkládané v účetní závěrce za rok 2019.



17 Zpráva auditora

ZPRÁVA NEZÁVISLÉHO AUDITORA pro členy zájmového sdružení právnických osob

Výrok auditora

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

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

Základ pro výrok

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



Ostatní informace uvedené ve výroční zprávě

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

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

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

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

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

Odpovědnost představenstva CZ.NIC za účetní závěrku

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





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

Odpovědnost auditora za audit účetní závěrky

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

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

- Identifikovat a vyhodnotit rizika významné (materiální) nesprávnosti účetní závěrky způsobené podvodem nebo chybou, navrhnout a provést auditorské postupy reagující na tato rizika a získat dostatečné a vhodné důkazní informace, abychom na jejich základě mohli vyjádřit výrok. Riziko, že neodhalíme významnou (materiální) nesprávnost, k níž došlo v důsledku podvodu, je větší než riziko neodhalení významné (materiální) nesprávnosti způsobené chybou, protože součástí podvodu mohou být tajné dohody (koluze), falšování, úmyslná opomenutí, nepravdivá prohlášení nebo obcházení vnitřních kontrol.
- Seznámit se s vnitřním kontrolním systémem CZ.NIC relevantním pro audit v takovém rozsahu, abychom mohli navrhnout auditorské postupy vhodné s ohledem na dané okolnosti, nikoli abychom mohli vyjádřit názor na účinnost jejího vnitřního kontrolního systému.
- Posoudit vhodnost použitých účetních pravidel, přiměřenost provedených účetních odhadů a informace, které v této souvislosti představenstvo CZ.NIC uvedlo v příloze účetní závěrky.

3 ADU.CZ s.r.o. - společnost zapsána v Obchodním rejstříku u Krajského soudu v Českých Budějovicích, oddíl C, vložka 4943
Záměstí 68, 387 06 Malenice, IČO: 62522078, DIČ: CZ62522078



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

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

Ve Strakonících, dne 16. června 2020

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



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

4 ADU.CZ s.r.o. - společnost zapsána v Obchodním rejstříku u Krajského soudu v Českých Budějovicích, oddíl C, vložka 4943
Záměstí 68, 387 06 Malenice, IČO: 62522078, DIČ: CZ62522078



18 Sídlo a kontaktní údaje

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

Milešovská 1136/5
130 00 Praha 3

IČ: 67985726
DIČ: CZ67985726
Tel.: +420 222 745 111
Fax: +420 222 745 112
www.nic.cz

Sdružení je zapsáno ve spolkovém rejstříku vedeném u Městského soudu
v Praze, spisová značka L 58624.

CZ.NIC - nepřetržitá zákaznická podpora

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

