.news 05 2008 CZ.NIC

Vážení čtenáři,

dovolte, abych Vás přivítal u dalšího čísla pravidelného čtvrtletníku .news. To minulé bylo svým způsobem slavnostní. V době jeho vydání tomu byl právě rok, kdy CZ.NIC uvedl do komerčního provozu technologii ENUM. I přesto, že toto číslo tak vyjímečné není, zajímavé informace v něm určitě nechybí.

Pravděpodobně ta nejdůležitější a zároveň jedna z nejaktuálnějších se týká bezpečnostní technologie DNSSEC. Když jsme v říjnu loňského roku přecházeli na nový registrační systém, za jednu z priorit roku 2008 jsme tehdy označili jeho rozšíření, a to o technologii DNSSEC. Na konci letošního února jsme uspořádali seminář pro členy a registrátory a představili jim předpokládaný harmonogram implementace této technologie. První viditelný krok budete moci vidět v průběhu dubna, kdy plánujeme spustit podepisování zóny pro ENUM. Testovací provoz nové verze registračního systému bychom chtěli nasadit v srpnu. Ostrý provoz DNSSEC je v plánu na září tohoto roku. Jsem velice rád, že jsme mohli na semináři přivítat i zahraničního hosta, Patrika Wallströma, který prezentoval zkušenosti s technologií DNSSEC ve Švédsku. Spolupráce se švédským správcem národní domény bude pokračovat i nadále. Slibujeme si od ní hlavně cenné informace, které nám umožní co nejhladší průběh implementace DNSSEC v našem systému pro správu domén. Těší mě i váš zájem o .blog, který funguje od konce ledna.

O jeho oblibě svědčí i poměrně vysoká návštěvnost a řada často velmi inspirativních komentářů u jednotlivých textů.

A neodpustím si malou perličku nakonec. Ve čtvrtek 13. března byla zaregistrována 400 000. doména .CZ. Za posledních pět a půl měsíce tak bylo zaregistrováno více než 74 000 nových domén.

Příjemné čtení vám přeje

Ondřej Filip
Výkonný ředitel sdružení CZ.NIC

CZ.NIC zabezpečuje český internet

Zástupci sdružení oznámili na únorovém setkání se svými členy a registrátory, že připravují zavedení technologie DNSSEC (DNS Security Extensions) do systému správy domén. Tuto technologii budou moci na plno využít především firmy, které na svých stránkách poskytují důležité informace či služby a mají zájem na tom, aby jejich uživatelé byli chráněni před útočníky, jež by je mohli přesměrovat na falešné weby. Automaticky se tak nabízejí banky, burzy a třeba také média a vyhledávače.

Spuštění testovací verze pro doménu ENUM je plánováno na duben, pro doménu .CZ na srpen tohoto roku.

S ostrým provozem počítá sdružení od září 2008.

Provoz DNS, doménových jmenných serverů, s sebou v dnešní době přináší různá rizika. Na správném a bezchybném provozu domény záleží mnoha firmám a jednotlivcům včetně těch, kteří žádnou doménu nevlastní. Přes internet probíhá řada finančních, obchodních a jinak důležitých operací. Nezřídka se objevují případy útoků na internetové bankovnictví. V minulosti již byly zaznamenány případy, které byly přímo namířené proti uživatelům internetu v České republice.

DNSSEC zavádí do DNS dotazů digitální podpisy. V případě, že je doména takto chráněna, je odpověď, kterou systém pošle, ověřená a informace správná. V běžném provozu to ale uživatel nepozná. Každá doména, aby mohla být digitálně

podepsaná, musí mít registrovanou veřejnou část digitálního klíče. S tím souvisí to, že zájemci o tuto technologii na ni musí být technologicky připraveni. Firmy musí umět podepisovat záznamy v doméně a zároveň sdružení CZ.NIC prostřednictvím registrátora poskytovat použitý klíč. Ten potom zařadí administrátoři sdružení do serverů, které se starají o doménu .CZ. Technologii DNSSEC používají v Evropě zatím jen dva registry domén nejvyšší úrovně, švédský a bulharský. Česká republika by tak podle všeho mohla být od září tohoto roku třetí zemí, která zavede DNSSEC ve svém systému správy domén.

VÝVOJ REGISTRACÍ DOMÉN OD PŘECHODU NA NOVÝ REGISTRAČNÍ STYSTÉM

Půl roku od spuštění nového registračního systému pro správu domén ENUM a .CZ vzrostl jejich počet oproti půlroku předchozímu o 60 procent. V současném systému jsou registrace nejen jednodušší, ale i rychlejší.

VÍCE

ON-LINE ROZHOVOR S ONDŘEJEM FILIPEM NA ŽIVĚ.CZ

Článek na aktuální téma městských domén jehož autorem je Ondřej Filip, výkonný ředitel sdružení, stejně jako zajímavou diskusi, kterou tento text vyvolal, si mohou zájemci přečíst na internetových stránkách Živě.cz.

ZÁJEM O ENUM MEZI FIRMAMI ROSTE

Výsledky pravidelného výzkumu společnosti Digimark s názvem „Telekomunikace a VoIP v českých firmách 1/2008“ ukázaly, že se o ENUM stále více mluví a to především ve firmách. Současně s tím roste i počet těch, kteří by ENUM v nejbližší době rádi zavedli.

VÍCE

VÍTE, ŽE

... byla ve čtvrtek 13. března, ve 22 hodin a 20 minut, zaregistrována doména s pořadovým číslem 400 000?

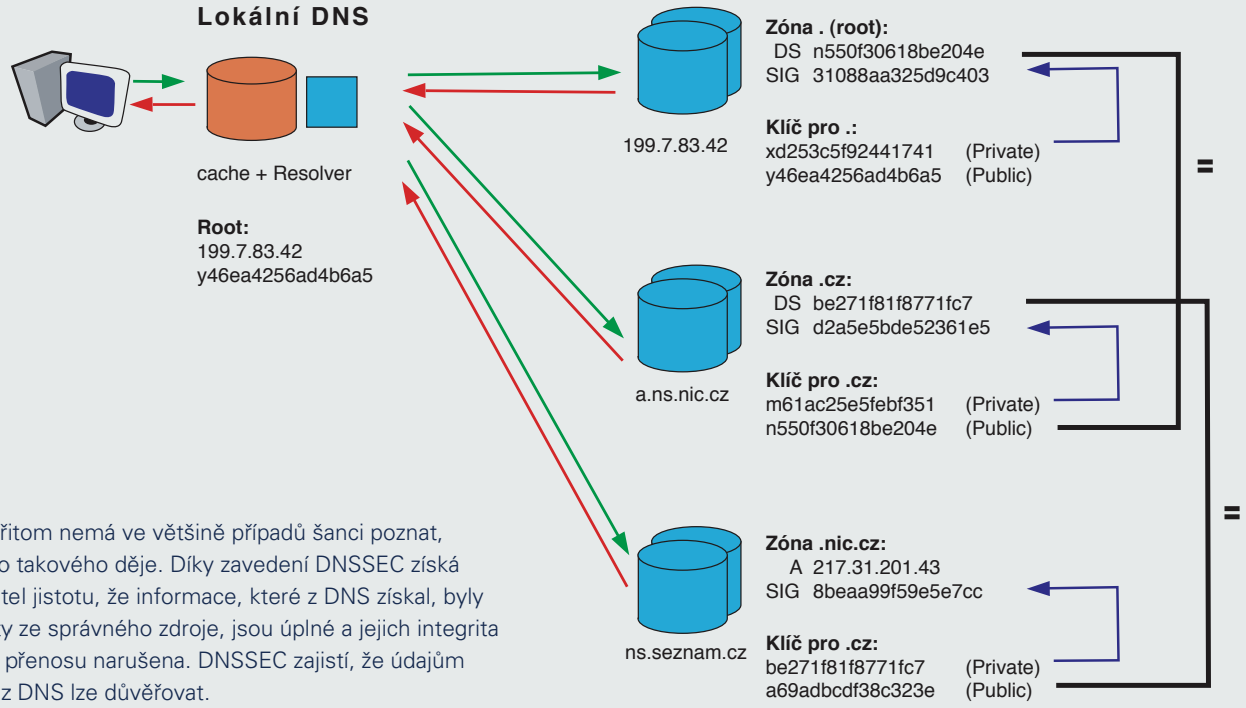
Od spuštění nového systému pro správu domén v loňském roce se do této doby zaregistrovalo přibližně stejné množství domén jako od ledna do října 2007, tedy za 9 měsíců. Počet domén, které byly do 13. března zaregistrovány v novém systému, je rovnoměrně rozložený mezi soukromé osoby a firmy. Na obě dvě skupiny připadá přibližně polovina z více než 74 000 nových domén.

VÍCE

O DNSSEC

Podobně jako jiné služby na internetu byl i systém doménových jmen (DNS – Domain Name System) vytvořen v době, kdy bylo k "síti" připojeno pouze malé množství uzlů a jejich provozovatelé se vzájemně znali.
S tím, jak používání internetu narostlo, bylo nutné začít řešit bezpečnost jednotlivých služeb.
Všichni uživatelé internetu se už neznají a je smutným faktem, že ne všichni se k němu připojují s bezelstnými úmysly.
DNSSEC je rozšíření systému DNS, které zvyšuje bezpečnost služby doménových jmen.
Principem DNS je překlad jmenných internetových adres jako například www.nic.cz nebo www.dobradomena.cz na adresy číselné, kterým počítače rozumějí a dokáží pomocí nich zajistit zobrazování webových stránek, odeslání e-mailů, telefonování po internetu a další běžné internetové služby. DNSSEC zvyšuje bezpečnost při používání DNS tím, že brání podvržení falešných, pozměněných nebo neúplných údajů o doménových jménech.
Služba DNS, bez zabezpečení technologií DNSSEC, "nabízí" eventuálnímu útočníkovi několik způsobů, jak narušit komunikaci a podvrhnout správné údaje.
Tím, že útočník změní údaje o doménových jménech, ovlivní fungování dalších internetových služeb, které může tímto zásahem zneužít.
Útočník potom můženapříklad:

- odposlouchávat cizí e-maily
- pomocí falešných webových stránek získávat hesla, přístupové kódy či údaje o platebních kartách apod.
- obcházet antispamovou ochranu v DNS a posílat spam
- podvrhnout zprávy a informace na webových stránkách
- přesměrovávat či odposlouchávat telefonní hovory vedené přes internet



Uživatel přitom nemá ve většině případů šanci poznat, že se něco takového děje. Díky zavedení DNSSEC získá jeho uživatel jistotu, že informace, které z DNS získal, byly poskytnuty ze správného zdroje, jsou úplné a jejich integrita nebyla při přenosu narušena. DNSSEC zajistí, že údajům získaným z DNS lze důvěřovat.

Jak DNSSEC funguje?

DNSSEC zavádí do DNS asymetrickou kryptografii – používání jednoho klíče na zašifrování a jiného klíče na dešifrování obsahu. Obdobný princip je základem známějšího šifrování zpráv pomocí PGP nebo podepisování e-mailů elektronickým podpisem. V případě DNSSEC si držitel domény vygeneruje dvojici soukromého a veřejného klíče. Svým soukromým klíčem pak elektronicky podepíše technické údaje, které o své doméně do DNS vkládá. Pomocí veřejného klíče je pak možné ověřit pravost tohoto podpisu. Aby měli všichni tento klíč dostupný, publikuje jej ke své doméně u nadřazené autority. To je pro všechny domény .CZ v registru domén .CZ. I na úrovni registru domén .CZ jsou technická data v DNS podepsána a veřejný klíč k tomuto podpisu je opět správcem registru předán nadřazené autoritě. Vytváří se tak řetěz důvěry, který zajistí, že údajům můžeme důvěřovat, pokud je řetěz ve všech svých krocích nepřerušen a všechny elektronické podpisy souhlasí, viz schéma.

Co se změní se zavedením DNSSEC?

DNSSEC je se stávajícím DNS zpětně kompatibilní, obě varianty fungují současně. Pro běžného uživatele se tedy okamžikem zavedení DNSSEC pro domény .CZ nezmění pravděpodobně nic. A to až do momentu, kdy na příslušném DNS serveru nezačne DNSSEC používat. To může být v případě expertů přímo na uživatelově počítači, v případě firem na firemním serveru, v případě domácích uživatelů na serveru jejich poskytovatele internetového připojení. Poskytovatelům služeb a obsahu pak DNSSEC nabízí možnost zvýšit bezpečnost a důvěryhodnost svých služeb. Pro zavedení DNSSEC budou potřebovat zajištění a správu digitálních podpisů svých údajů v DNS a publikování příslušných šifrovacích klíčů do registru domén .CZ. ■

Setkání s registrátory

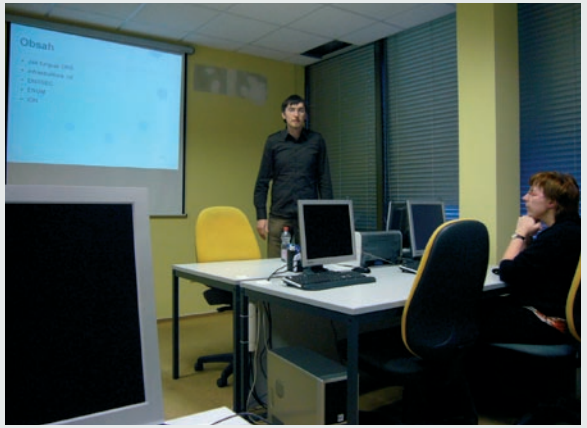
Na konci února se ve strašnickém konferenčním a kulturním centru InGarden konalo tradiční setkání s registrátory. Tentokrát se ho zúčastnili i někteří členové CZ.NIC. Zástupci sdružení zde totiž představili bližší informace k zavedení technologie DNSSEC do systému pro správu domén .CZ a ENUM.
Této technologické inovaci, jejímž úkolem je zvýšit bezpečnost DNS, zástupci managementu CZ.NIC věnovali celé dopoledne. Prezentace šly za sebou tak, aby posluchači postupně získali informace o historii a současné situaci ve světě, o technických parametrech a o harmonogramu a jednotlivých krocích při zavádění DNSSEC.
Na setkání vystoupil se svou přednáškou také Patrik Wallström (na fotografii) ze Švédska a představil zkušenosti s DNSSEC v tamním národním doménovém registru. V druhé části určené už pouze zástupcům registrátorů odpovídali na dotazy hosté z Úřadu na ochranu osobních údajů. Po nich představil ředitel provozu Martin Peterka registrátorský intranet a blokování transferu a změn. Na úplný závěr projektový manažer Pavel Tůma seznámil všechny přítomné s projektem, který má zatím pracovní název Certifikace registrátorů. ■

Blokace transférů

Nový systém pro správu domén .CZ funguje již více než šest měsíců, během nichž sdružení vyhodnocovalo připomínky uživatelů. Jejich hlavní část se týkala především toho, že stále neexistuje žádná zvýšená ochrana doménového jména, zejména možnost zablokovat provádění změn nad doménami a kontakty.
Aby CZ.NIC vyhověl především žádostem držitelů domén, rozhodli se jeho zástupci doplnit systém o dvě nové funkcionality. První je možnost zablokovat transfer, druhou potom zablokování jakýchkoliv změn nad doménou, kontaktem nebo sadou jmenných serverů.
Po realizaci těchto změn budou moci držitelé pomocí formuláře na internetových stránkách CZ.NIC požádat o příslušnou blokaci. Jakmile potom doručí CZ.NIC potvrzení (buď úředně ověřeným podpisem nebo e-mailem, podepsaným kvalifikovaným certifikátem), bude jim přímo na úrovni centrálního registru příslušná operace zablokována. Odblokování bude probíhat stejným způsobem.
Výsledkem bude, že změna nepůjde žádným způsobem provést. Kromě toho bude zastavena možnost vyžádat si heslo k transferu. Držitel už tedy nebude obtěžován e-maily s heslem, které od nikoho nechtěl.
Tento návrh byl představen registrátorům na pravidelném setkání. Pokud k němu zástupci sdružení nedostanou žádné závazné připomínky, budou v nejbližších dnech tyto změny realizovány. ■

Prezentace na školách mají úspěch

V předchozím čísle jsme vás informovali o spolupráci s počítačovou školou Gopas. Zde také v polovině ledna proběhlo první setkání s lektory, pro které byla připravena prezentace na téma DNS a novinek z oblasti českého, ale i světového internetu. Přestože bylo setkání plánováno na 45 minut, protáhla se přednáška díky řadě dotazů na více než hodinu a půl. Stejná situace se opakovala také při další přednášce. Tentokrát prezentoval projektový manažer sdružení Pavel Tůma posluchačům z počítačové školy S-COMP CENTRE.



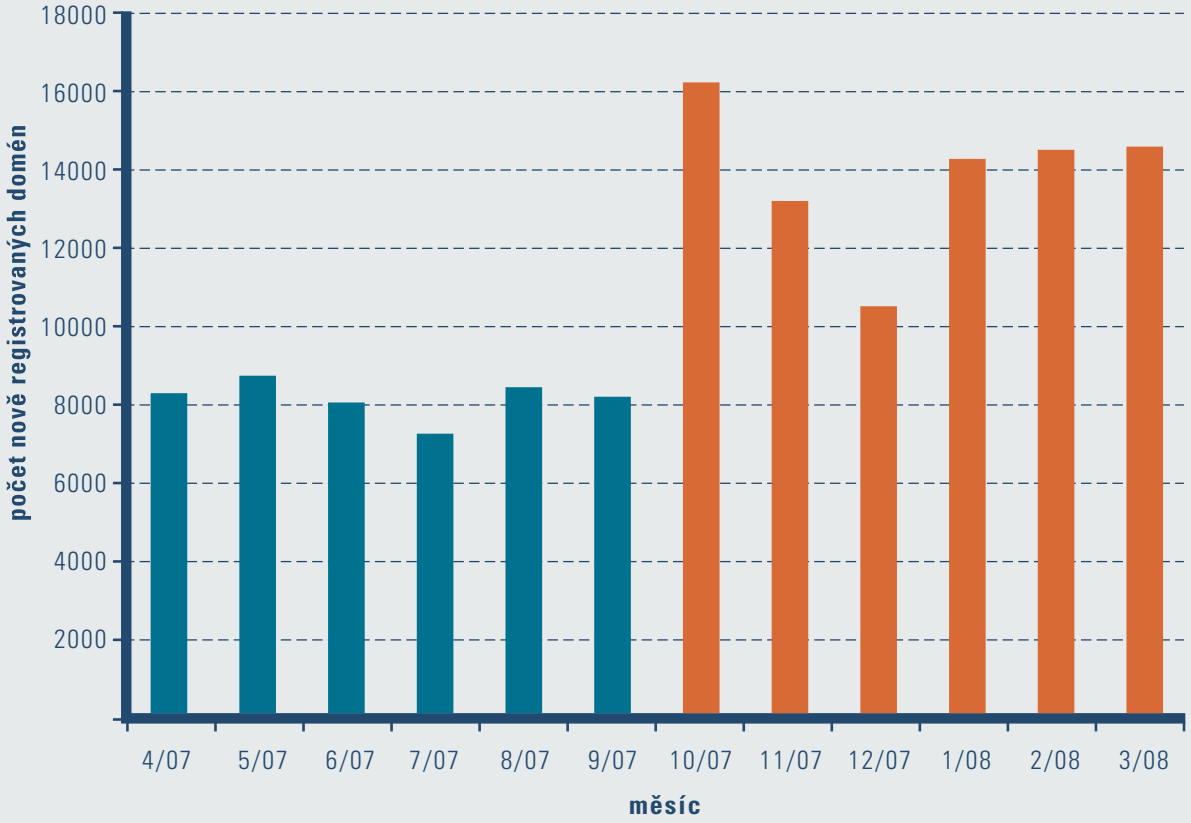
I zde se ukázalo, že řada z těch, kteří přišli, slyšela některé z informací poprvé. Třetí a zatím poslední z přednášek absolvoval Pavel Tůma na Střední průmyslové škole v Praze 10. Tady už nebyli mezi posluchači pouze učitelé, ale i samotní žáci. Do posluchárny si našly cestu odhadem čtyři desítky studentů.
Sdružení osloví i další střední a vysoké školy stejně jako specializovaná výuková střediska, jimž by přednáška na téma DNS a internetu dokázala vhodně doplnit vykládané informace o tom, jak telekomunikační síť funguje a co se na ní v nejbližší době připravuje. Současně ale uvítáme, pokud se nám zájemci o prezentaci ozvou sami a to na e-mailovou adresu vilem.sladek@nic.cz. ■

60procentní nárůst v počtu domén .CZ

Ve středu 2. dubna uplynul půlrok od spuštění nového systému pro správu domén .CZ. Za tu dobu vzrostl jejich počet oproti půlroku předchozímu o 60 procent. V systému, který vyvinuli zaměstnanci sdružení během roku a půl, jsou registrace domén jednodušší a rychlejší. Nárůst počtu registrací určitě ovlivnila i cena; domény s koncovkou .CZ jsou v nabídce většiny registrátorů od loňského října levnější.

„Cílem nového systému bylo zpřístupnit doménu .CZ co nejširší veřejnosti a je vidět, že se nám jej daří úspěšně naplňovat. V nejbližší budoucnosti očekáváme, že se počet registrací bude postupně zvyšovat, poslední tři měsíce tomu alespoň nasvědčují. Průměrně jich teď registrujeme okolo 14 000 za měsíc," komentoval tuto zajímavou informaci výkonný ředitel sdružení Ondřej Filip.

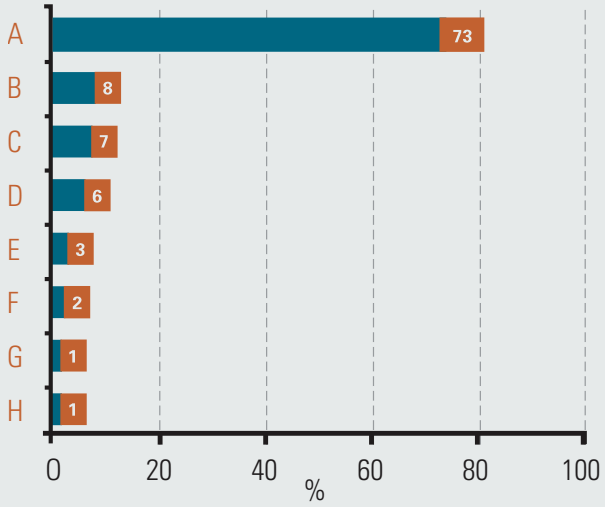
Nově registrované domény (duben 2007 – březen 2008)



Zájem o Enum mezi firmami roste

ENUM se pomalu dostává nejen do povědomí telekomunikačních operátorů a odborné veřejnosti, ale stále více si ho začínají všímat i koncoví uživatelé a to zejména firmy. Tento fakt potvrdily i výsledky pravidelného výzkumu trhu VoIP, který provádí každý rok společnost Digimark. Přestože valná většina firem stále o ENUM neslyšela, je potěšující, že 6 % dotázaných plánuje ENUM ve své firmě zavést. Výzkum také ukázal, že až na úzkou skupinu „odmítačů" IP telefonie, nejsou v zavádění ENUM ve firmách řádné nepřekonatelné problémy. Proto se v tomto roce zaměříme zejména na odstranění té největší překážky, kterou je neznalost ENUM mezi koncovými uživateli.

Zavádění ENUM ve firmách



A – o ENUM jsme doposud neslyšeli
B – neplánujeme: není kdo by se tím zabýval
C – neplánujeme: nemáme IP telefonii a nebudeme zavádět
D – ENUM plánujeme zavést
E – neplánujeme, nerozumíme přínosům
F – neplánujeme, uvedené služby nejsou přínosné
G – ENUM již používáme
H – neplánujeme: jiný důvod

Vybráno z .blogu

IPv6 v kořenové zóně

(autor: Ondřej Surý, Technický ředitel CZ.NIC, publikováno: 12. února 2008)

O IPv6 se diskutuje už dlouhá léta. Někdy okolo roku 1992 začalo být IETF jasné, že IPv4 adresy dochází a byla nastartována iniciativa IPng (první RFC na toto téma bylo RFC 1550). Přibližně o tři roky později byl vybrán návrh IPv6 (základní specifikace IPv6 se nachází v dokumentu RFC 2460). Proces, který následoval v běžném světě, bych označil jako: „Jak se vyhnout nasazení IPv6." Masivní nasazení technologie překladu adres (NAT/PAT) postupné ubývání IPv4 adres zpomalil, ale nezastavil. Velmi pěkné pojednání o tom, kdy IPv4 adresy dojdou má na svých stránkách Geoff. Podle jeho posledního modelu nám dojdou adresy někdy v roce 2011 – 2012.

Nicméně rozhodně nelze sedět a čekat, až IPv4 adresy dojdou. Přechod na IPv6 nejde udělat přepnutím jednoho přepínače a internetová infrastruktura na tento přechod musí být připravena. Všechny systémy provozované sdružením CZ.NIC jsou v tuto chvíli provozovány na IPv4 i IPv6 adresách, včetně našich DNS serverů.

Z pohledu IPv6 došlo minulý týden k důležitému kroku na straně serverů obsluhující kořenovou (root) zóny. IANA přidala do této zóny IPv6 záznamy pro polovinu, (přesněji šest ze třinácti) DNS serverů – – A,F,H,J,K a M.

Běžného uživatele se tato změna nejspíš nedotkne, i když vím o minimálně jedné komunitní síti, která má (a možná, že už to opravili) IPv6 routing natolik rozbitý, že by to mohlo dělat problémy. Nicméně z pohledu další budoucnosti je to výrazný signál, že je potřeba začít IPv6 brát vážně.

Krátká poznámka na závěr. Pokud provozujete BIND jako resolver a zároveň používáte IPv6, budete asi chtít zaktualizovat named.root soubor. Stáhnout si jej můžete z Internicu.

CZ.NIC adoptoval Kasuára přílbového

Na začátku března adoptovalo sdružení v trojské zoologické zahradě Kasuára přílbového. Více než měsíc se tak podílí na nákladech na krmení a chov tohoto výjimečného zvířete. Kasuár přilbový (Casuarius casuarius) měří až 170 centimetrů a ve volné přírodě byste ho našli v australských lesích a pralesích. Přestože je na první pohled velice zajímavý, řada z nás ho jistě ve střední části trojské zahrady snadno mine. Kasuár se dokáže pohybovat rychlostí až 50 kilometrů za hodinu, a to nikoli letem, ale během. V případě nebezpečí neklove, ale kope, popřípadě se spoléhá na údery zakrnělých křídel opatřených dlouhými ostrými bodci. Více si o něm mohou všichni fandové divoké zvěře přečíst na stránkách Zoologické zahrady hl. m. Prahy.