Novinky v .CZ registru a mojeID

Zdeněk Brůna • zdenek.bruna@nic.cz • 20. 06. 2017

CZ.NIC | SPRÁVCE DOMÉNY CZ

Osnova

- FRED
- Registr .CZ
- Infrastruktura
- DNS
- Weby & mojeID

FRED

- Změny v EPP
  - refaktoring EPP
    - kompletní přepis implementace EPP backendu (10 let starý kód)
    - metody pro správu základních objektů (kontakt, doména, nsset, keyset)
    - vyšší bezpečnostní standard
    - odstranění známých chyb v implementaci
    - vylepšení technické dokumentace
    - zpřesnění hlášených návratových chyb
    - další vylepšení
      - authinfo – nepoužívá vizuálně podobné znaky: například „I/l/1“,“O/0“

FRED

- Změny v EPP
  - asynchronní notifikace o EPP operacích (například update kontaktu)
    - oddělení zasílání notifikacích e-mailů od samotných operací
    - operace nebylo možné vypnout / spouštět dle potřeby
    - chyby v notifikacích ovlivňovaly výsledek operace

FRED

- Nová dokumentace FRED
  - obsahuje:
    - feature dokument – pro potenciálního nového uživatele
    - popis architektury – pro vývojáře, správce, helpdesk
    - administrační manuál – pro správce, helpdesk
  - dostupná na:
    - https://fred.nic.cz/page/675/documentation/
    - https://github.com/CZ-NIC/fred-docs
  - letos pokračujeme
    - referenční příručka EPP/XML protokolu

FRED

Statistiky nasazení FREDa k 31.5.2017

Země	TLD	počet domén	populace	rozloha (km^2)
Česká republika	.cz	1 297 352	10 578 820	78 866
Argentina	.ar	413 354	43 886 748	2 780 400
Albánie	.al	18 748	2 821 997	28 748
Kostarika	.cr	17 214	4 509 392	51 100
Makedonie	.mk	16 782	2 062 294	25 713
Tanzanie	.tz	12 253	52 482 726	945 090
Malawi	.mw	9 923	12 158 924	118 480
Angola	.ao	4 012	25 789 024	1 246 700
Faerské ostrovy	.fo	3 228	49 469	1 396
Macao	.mo	2 667	583 737	29
Togo	.tg	1 335	6 020 000	56 785
celkem		**1 796 868**	**160 943 131**	**5 333 307**

zdroje:
www.nic.cz, www.centr.org, http://research.domaintools

FRED


Faroe Island
.fo
Czech Republic
.cz
.mk
Macedonia
.al
Albania
Macau
.mo
Costa Rica
.cr
Togo
.tg
Tanzania
Angola
.tz
.ao
.mw
Malawi
Argentina
.ar

Registr .CZ

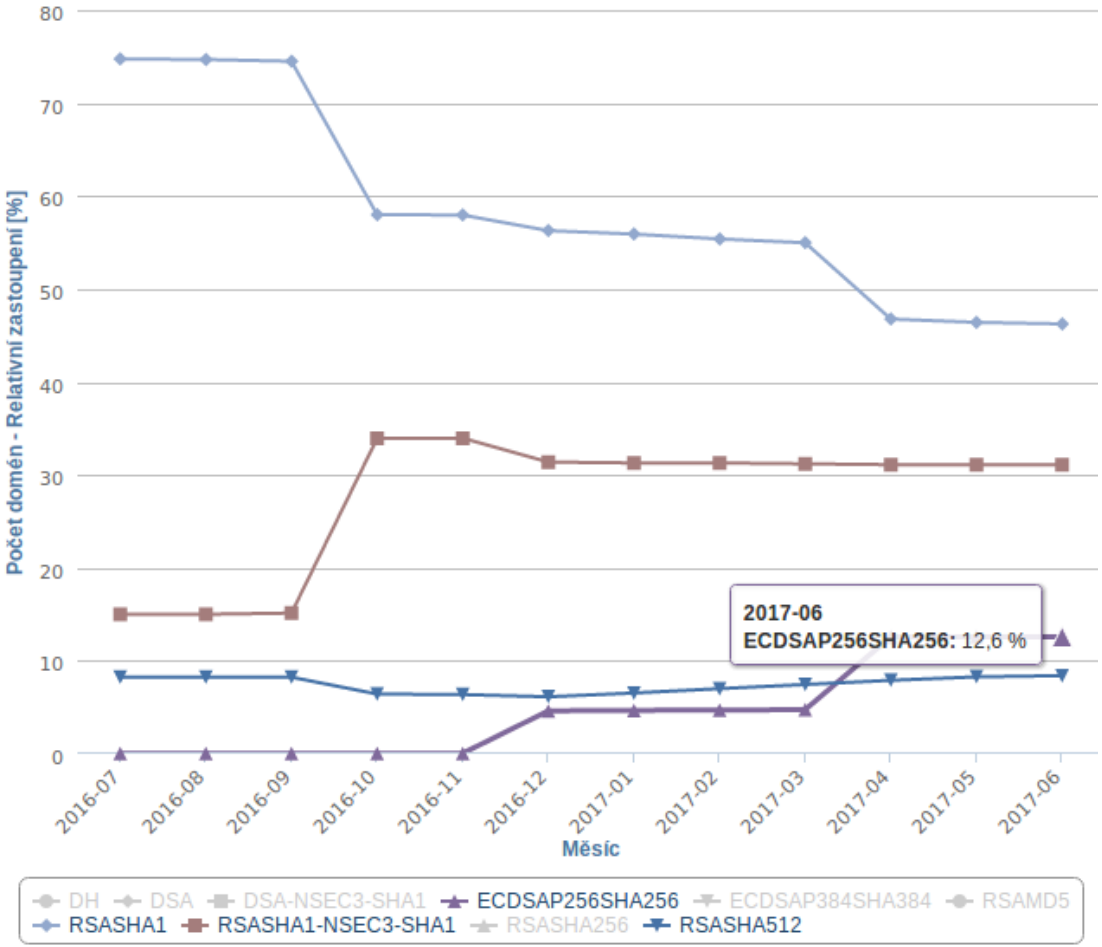
- Automatizovaná správa KEYSETů
  - pro zprovoznění DNSSECu je třeba vložit DNSSEC klíč do registru (registrátorem nebo přes registrátora)
  - v registru .cz se provádí pomocí tzv. KEYSETu (obsahuje klíč, váže se na domény)
    - ne všichni registrátoři podporují - „pouze“ 51,5% .cz domén ma DNSSEC
  - nový standard – nový typ klíčů, automatické vkládání klíče do nadřazené zóny
    - dnes pouštíme
    - DNSSEC bude dostupný dalším držitelům domén
    - detaily Jaromír Talíř v 10:20

Registr .CZ

- přechod na ECDSA
  - DNSSEC využívá asymetrické šifrování
  - různé šifrovací algoritmy (RSA -> ECDSA)
  - vyšší bezpečnost
  - .cz registr již ECDSA podporuje pro SLD
  - IANA ohlásila podporu pro kořenovou zónu „na léto“

Registr .CZ

- přechod na ECDSA
  - podíl DNSSEC algoritmů v .cz zóně
  - ZONER, IGNUM



Infrastruktura

- upgrade HW (obměna switchů v ČRa, obměna serverů registru)
- náhrada routeru Brocade BIRDem v jedné lokalitě
- nová pásková mechanika
- upgrade SW
  - Upgrade OS - Ubuntu Precise -> Ubuntu Xenial
  - upgrade PSQL – na verzi 9.6

DNS

- snížení TTL v zóně .cz
  - TTL udává, jak často se ptá DNS resolver autoritativního DNS
  - nižší TTL:
    - změny v DNS záznamech se projeví rychleji
    - zvýší se zátěž DNS systému
  - v únoru a březnu 2017 jsme **snížili z 5 hodin na 1 hodinu**
    - postupné snižování (monitoring dopadů)
    - prevence příliš velkého zvýšení počtu dotazů DNS resolverů

DNS

- snížení TTL v zóně .cz
  - skokový nárůst všech DNS dotazů, které expirovaly z cache DNS resolverů

22.2. 2017 - nárůst o 59,45%

zvýšený počet NXDOMAIN odpovědí

DNS

- upgrade DNS infrastruktury
  - současný DNS anycast
    - 3 x v ČR (3 x 5 serverů / 10 + 10 Gbps)
    - 8 x zahraničí (8 x 2 servery / 1 Gbps)
    - provoz: 25 000 qps / desítky Mbps
    - odolnost: 20 000 000 qps / 60 Gbps
    - četnost a intenzita DDoS útoků roste
    - důležitost fungování DNS roste

DNS

- upgrade DNS infrastruktury
  - popis záměru
    - zvýšení odolnosti na: 100 mil. qps / 200 Gbps
    - vylepšit monitoring
    - zachovat diverzitu

DNS

- upgrade DNS infrastruktury
  - plánované změny infrastruktury
    - upgrade konektivity do NIX.CZ (2 x 100 Gbps)
    - upgrade routerů a DNS serverů ve 2 lokalitách
    - posílení významných zahraničních lokalit (UK)
    - zprovoznění DNS uzlů v sítích významných ISP

Weby & mojeID

- zvýšení bezpečnosti
  - HTTPS jako default (Let‘s Encrypt)
  - podpora HSTS
  - bezpečnostní opatření v Django 1.10
    - monitoring porušení CSP, SRI
    - secure flagy u CSRF a session cookies
    - bezpečnostní hlavičky X-Content-Type-Options a X-XSS-Protection
    - chybí odstranit inline JS a CSS (pro mojeID v plánu na Q3)
  - https://observatory.mozilla.org/

MojeID

- příklady větších novinek
  - ověřování dalších e-mailových adres v mojeID
  - nová dokumentace mojeID (https://www.mojeid.cz/dokumentace/html/)
  - certifikace OpenID Connect
  - zapojení do EduID
  - rozšíření předávaných informací o stavu ověření uživatele
  - systém na podporu validačních míst
  - weblate

MojeID

- na čem pracujeme
  - validace pomocí Datové schránky (červenec)
  - validace pomocí zaslání výpisu z ROB / ISZR (Q3/Q4)

Výměna kořenového klíče

- výměna KSK kořenové zóny
  - provádí ICANN
  - plán: https://www.icann.org/resources/pages/ksk-rollover/#timeline
    - nový KSK bude publikován v DNS 11.07.2017
    - nový KSK začne podepisovat kořenovou zónu **11.10.2017**
    - revokace starého KSK 11.1.2018
  - prověřte DNSSEC validující resolvery
    - automatická změna trust anchor (RFC 5011)
    - právo zápisu do souboru, kde je uložen klíč

Děkuji za pozornost

Zdeněk Brůna • zdenek.bruna@nic.cz