DNSSEC - aktuální stav a zkušenosti z praxe

Ing. Tomáš Hála
ACTIVE 24, s.r.o.
www.active24.cz

DNSSEC - historie a současnost

- na konci září 2008 byla na CZ doméně spuštěna podpora DNSSEC

- jako jediný registrátor CZ domén jsme spustili podporu DNSSEC pro naše zákazníky ve stejný den jako CZ.NIC

- v červnu 2009 (IT '09) chránil DNSSEC 889 českých domén, přičemž 800 z nich bylo registrováno přes ACTIVE 24

- k dnešnímu dni chrání DNSSEC téměř 99.000 českých domén, přičemž více než 84.000 z nich je registrováno přes ACTIVE 24

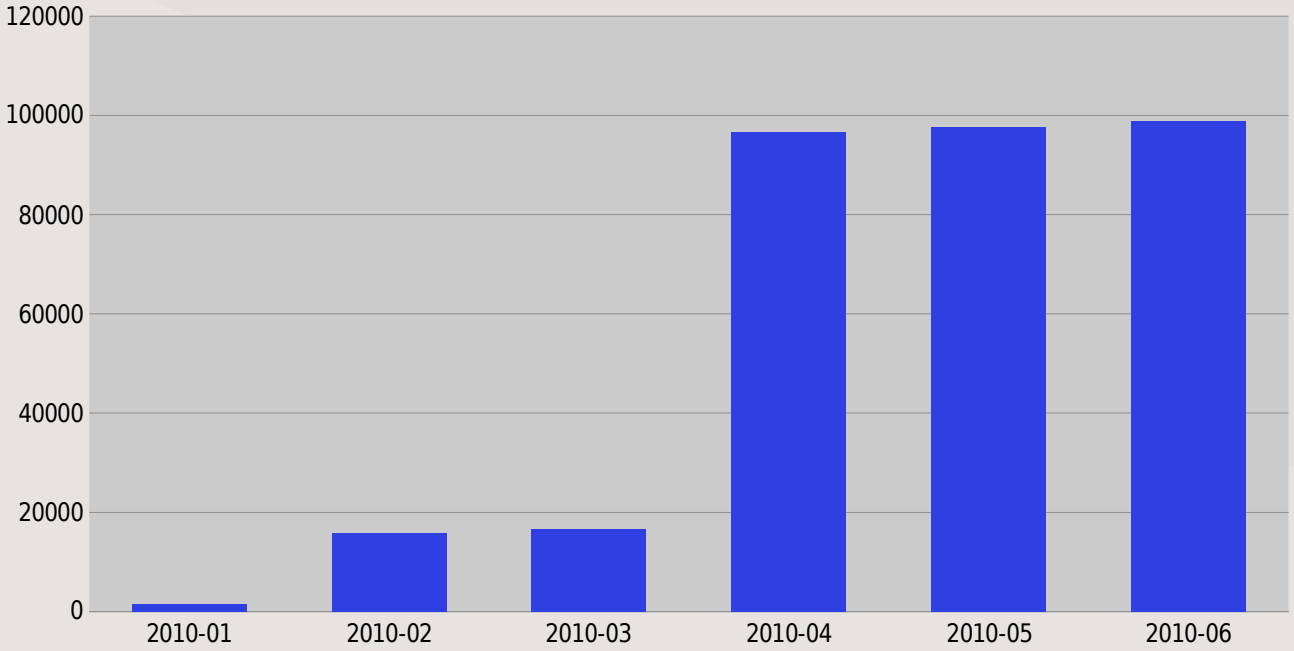
- DNSSEC je automaticky a zdarma aktivní na každé u nás registrované CZ doméně provozované na našich DNS serverech

DNSSEC - historie a současnost

DNSSEC - historie a současnost

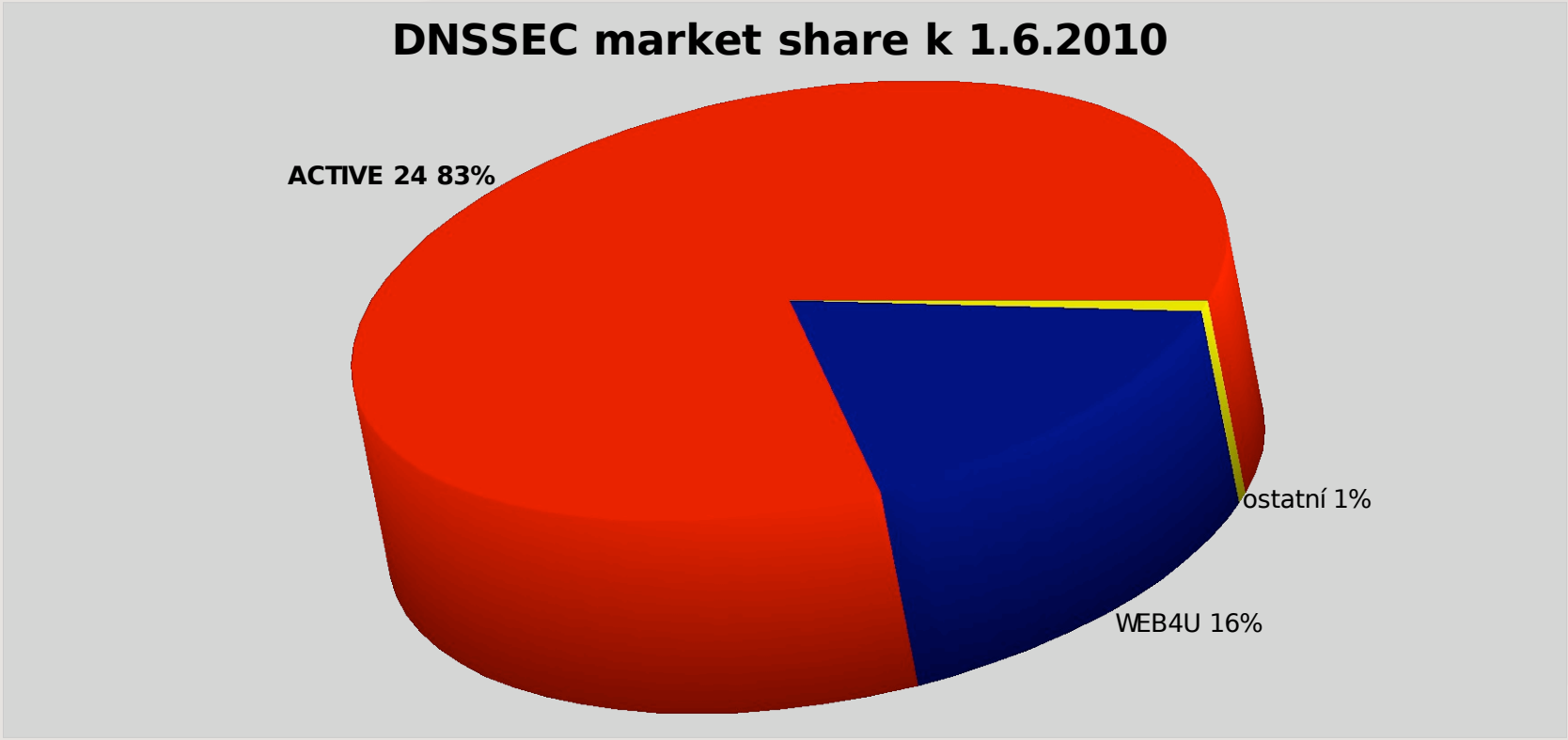
Počet zabezpečených domén od 1.1.2010

leden 2010 – podpis všech domén WEB4U
březen 2010 – podpis všech domén ACTIVE 24



DNSSEC - historie a současnost

k 1.6.2010 bylo podepsáno **98 661** domén ~ **15%** z celkového počtu



DNSSEC - historie a současnost

- uvedené údaje mj. znamenají, že ACTIVE 24 je největším registrátorem domén chráněných pomocí DNSSEC na světě!

- zároveň s námi se tak český registr CZ.NIC spravující národní doménu .CZ a tedy i celá Česká republika stávají největšími uživateli technologie DNSSEC v celosvětovém měřítku

- v počtu domén jsme tak překonali i Švédsko, které DNSSEC nasazovalo jako první a stále jej aktivně propaguje a rozšiřuje

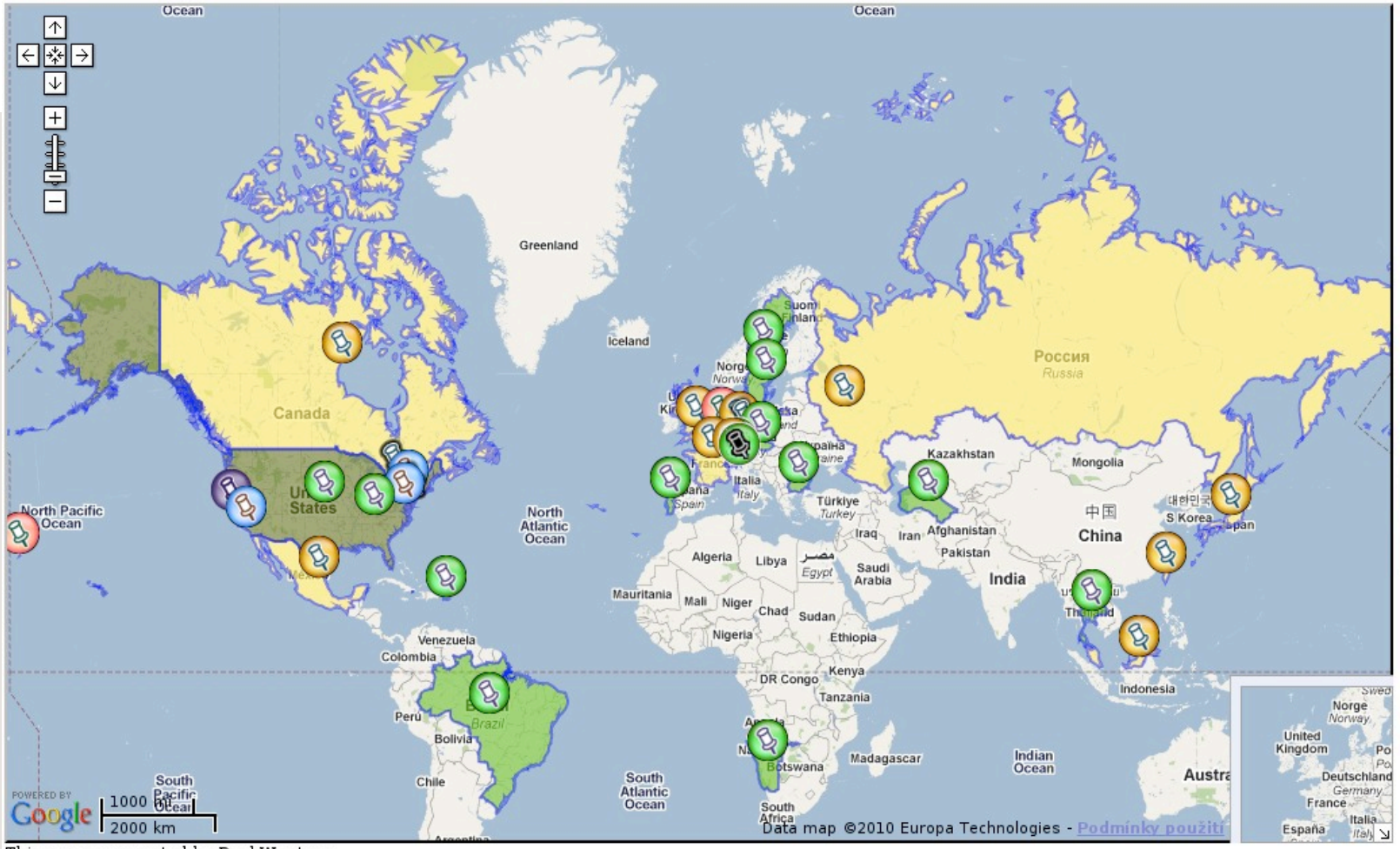
- chráněno je nyní cca 15% českých domén (je to hodně nebo málo?)

DNSSEC - historie a současnost

- v červnu 2009 fungoval DNSSEC pouze na pěti národních doménách včetně té naší

World Wide DNSSEC Deployment

See also DNSSEC Theory and World Wide Deployment by Paul Wouters, November 21, 2007, SecTor



This map was created by Paul Wouters

zdroj: www.xelerance.com/dnssec/

DNSSEC - historie a současnost

- 27.1.2010 The first root server (L-Root) begins serving the signed root in the form of the DURZ (deliberately unvalidatable root zone).

- Early May, 2010: All root servers are now serving the DURZ. The effects of the larger responses from the signed root, if any, would now be encountered.

- May and June, 2010: The deployment results are studied and a final decision to deploy DNSSEC in the root zone is made.

- July 15, 2010: ICANN publishes the root zone trust anchor and root operators begin to serve the signed root zone with actual keys The signed root zone is available!
  zdroj: www.root-dnssec.org

DNSSEC v praxi

- nárůst velikosti zón až dvacetinásobně
  (při uvažování velikosti bloku filesystému jen cca 3 násobně)

- několikanásobně vyšší potřeba výpočetního výkonu
  při generovaní podepsané zóny

- ačkoliv to procentuálně zní děsivě, v reálu jde v absolutních
  číslech o více-méně zanedbatelný nárůst

DNSSEC v praxi

- důležité bylo správné ošetření manipulace s NSSETy a KEYSETy

- problém tzv. DNSSEC smrti

- nutnost přepodepisování zón kvůli expiraci podpisu a rotace klíčů

- validace Unbound / Bind

- nepochopení technologie zákazníky

- vymlouvání se na DNSSEC při technických problémech

DNSSEC – co dál?

- systém DNS má vždy dvě strany – autoritativní servery na straně jedné a DNS cache servery resp. resolvery na straně druhé

- na straně autoritativních serverů došlo díky ACTIVE 24 ke značnému rozšíření této technologie v ČR

- na straně druhé, tedy zejména u ISP zajišťujících připojení k internetu, se stále čeká, až se ledy pohnou a to i přesto, že validace DNSSECu je výrazně jednodušší na zprovoznění než správné podepisování a propagace zón

- v současnosti je tedy největší výzvou přesvědčení velkých českých ISP, aby na svých DNS cache serverech pro zákazníky zapnuli DNSSEC validaci

DNSSEC – několik tipů na závěr

- podrobné info na www.dnssec.cz (provozuje CZ.NIC)

- plugin do Firefoxu od CZ.NIC laboratoře

www.google.cz/search?q=dnssec+plugin+pro+firefox

- základní debug pomocí „dig +dnssec +cd domeny.cz @dnsserver“

- rhybar.cz – fungující doména se záměrně nevalidním podpisem

- zprovoznění validace je práce na pár minut (bind, unbound)

- pozor při použití více cache DNS serverů na klientské straně

Závěr

- vyzkoušejte DNSSEC – není to nic složitého!

- ptejte se po validaci u svého ISP

- podepsání můžete realizovat svépomocí (na svých DNS serverech) nebo stačí zaregistrovat či převést svou doménu k tomu správnému registrátorovi :-)

Prostor pro Vaše dotazy