

# DNSSEC a CSIRT

aneb co může udělat webhoster pro bezpečnější internet



Ing. Tomáš Hála  
ACTIVE 24, s.r.o.  
[www.active24.cz](http://www.active24.cz)



# Bezpečnost ze dvou pohledů

- technologické zabezpečení
- neustálé sledování nových technologií či postupů a jejich následné nasazování do praxe

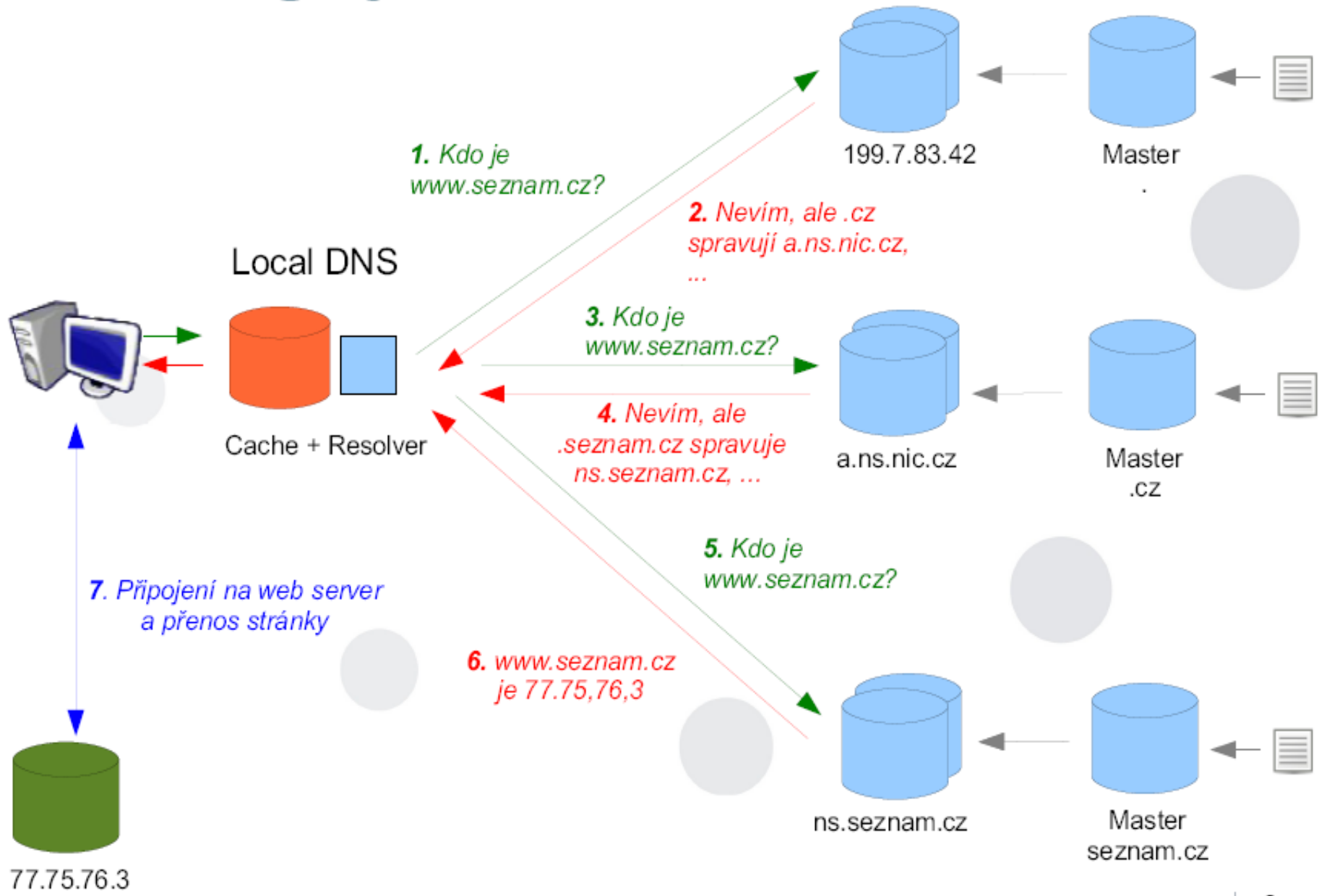


- rychlé a efektivní řešení bezpečnostních incidentů
- spolupráce s jinými subjekty

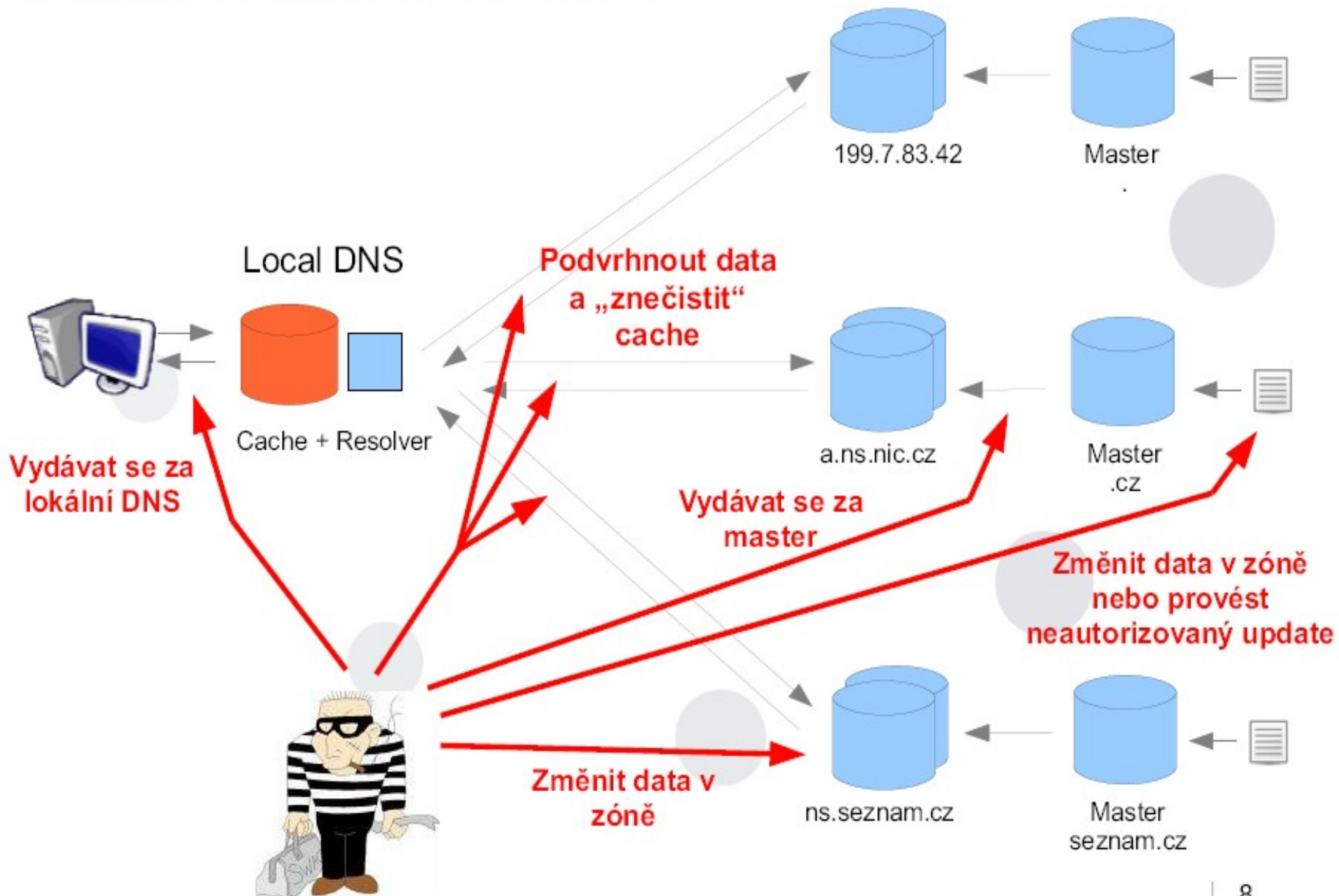
# DNSSEC

- co je DNSSEC?
- už podle jména si většina lidí udělá základní představu (viz naše nedávné výběrové řízení na Linux administrátora)
- jedná se o standardizované doplnění klasického DNS protokolu o prvky elektronického podepisování za účelem eliminace řady bezpečnostních nedostatků současného systému DNS

# Jak funguje DNS



# Zranitelnost DNS



# DNS – útok podle Kaminského

- nezáplatované DNS servery používají vždy stejný zdrojový port
- drtivá většina DNS dotazů a odpovědí používá UDP, tedy je relativně jednoduché podvrhnout zdrojovou IP adresu
- DNS dotazy a odpovědi v sobě mají uloženo 2-bytové Transaction ID, tedy počet kombinací je přibližně 65 tisíc.
- útok využívá časového okna mezi dotazem a odpovědí
- postup dle Kaminského nevyžaduje čekání na vypršení TTL, tedy tímto způsobem je možné útočit kdykoliv
- v praxi je dnes možné podvrhnout cache DNS serveru s nainstalovanými všemi aktualizacemi řádově během pouhých desítek hodin

# Zpět k DNSSEC - teorie

- zajišťuje elektronické podepsání údajů v DNS zóně, čímž umožňuje klientovi, aby si ověřil, že odpověď od DNS serveru, kterou obdržel, je platná a cestou nedošlo k její modifikaci
- vytváří podobný řetězec důvěry, jaký známe z každodenně používaného protokolu SSL (např. HTTPS)
- je zpětně kompatibilní s původním DNS protokolem, tedy i klienti, kteří DNSSEC nepodporují, mohou běžným způsobem zpracovávat odpovědi DNS na doméně s DNSSEC, jen neověří původ a integritu
- používání DNSSEC omezuje možnosti útoků na mailové služby či obsah www (např. phishing)

# 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 březnu 2009 (loňský InstallFest) chránil DNSSEC cca 600 českých domén, přičemž 550 z nich bylo registrováno přes ACTIVE 24
- k dnešnímu dni chrání DNSSEC přes 94.000 českých domén, přičemž necelých 80.000 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

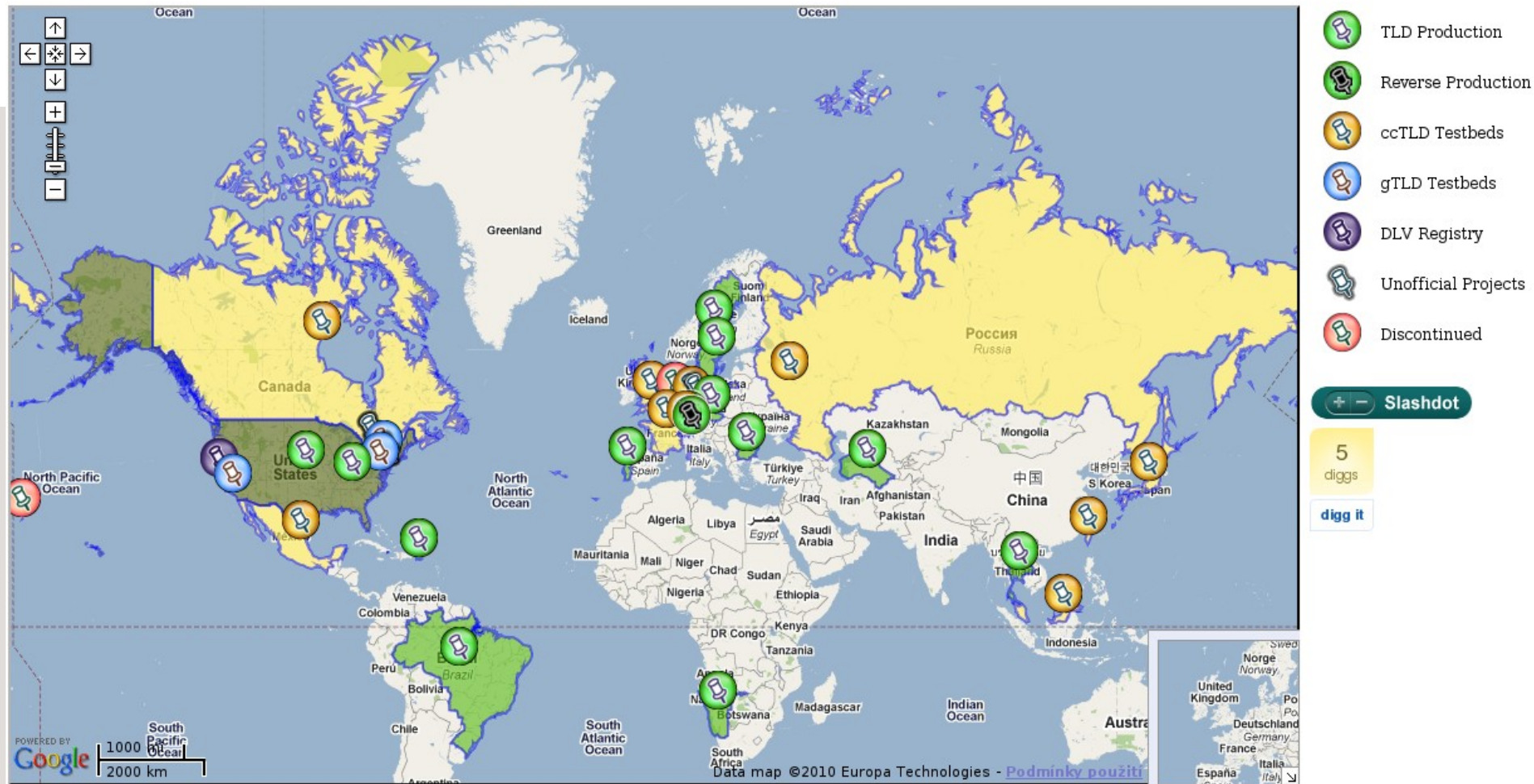
- uvedené údaje mj. znamenají, že ACTIVE 24 je největším registrátorem domén chráněných pomocí DNSSEC na světě!
- zároveň s námi se tak český registr CZ.NIC spravující národní doménu .CZ a tedy i celá Česká republika stávají největšími uživateli technologie DNSSEC v celosvětovém měřítku
- v počtu domén 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 březnu 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/](http://www.xelerance.com/dnssec/)



# DNSSEC - historie a současnost

- 27.1.2010 byla podepsána kořenová zóna na L-Root
- Early May, 2010: All root servers are now serving the DURZ (deliberately unvalidatable root zone). 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 1, 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](http://www.root-dnssec.org)



# DNSSEC v praxi

- nárůst velikosti zón až dvacetinásobně  
(při uvažování velikosti bloku filesystemu jen cca 3 násobně)
- několikanásobně vyšší potřeba výpočetního výkonu při generování podepsané zóny
- ačkoliv to procentuálně zní děsivě, v reálu jde v absolutních číslech o více-méně zanedbatelný nárůst
- důležité bylo správné ošetření manipulace s NSSETy a KEYSETy

# 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

- podrobné info na [www.dnssec.cz](http://www.dnssec.cz) (provozuje CZ.NIC)

- plugin do Firefoxu od CZ.NIC laboratoře



[www.google.cz/search?q=dnssec+plugin+pro+firefox](http://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

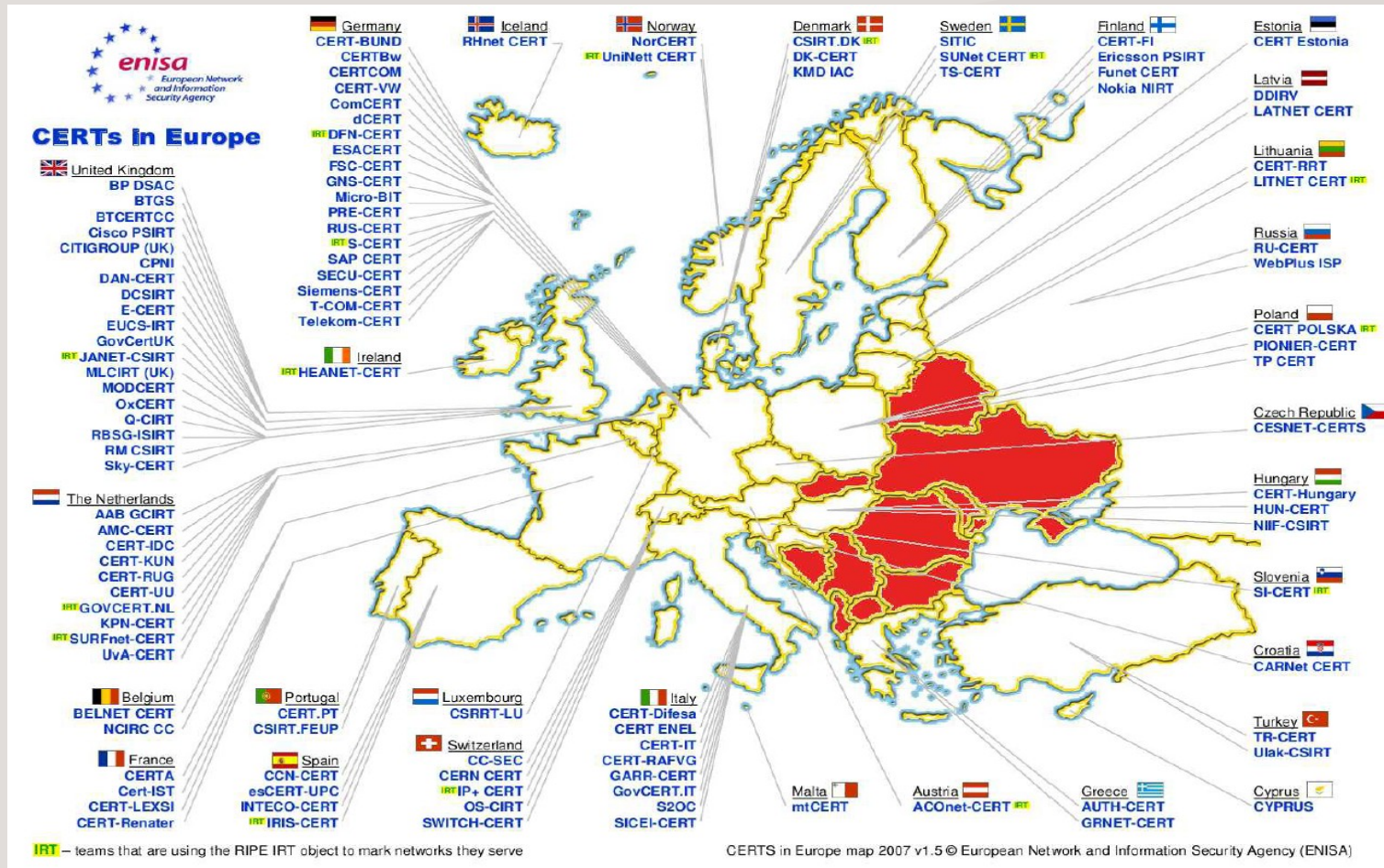
# CSIRT/CERT

# CSIRT/CERT

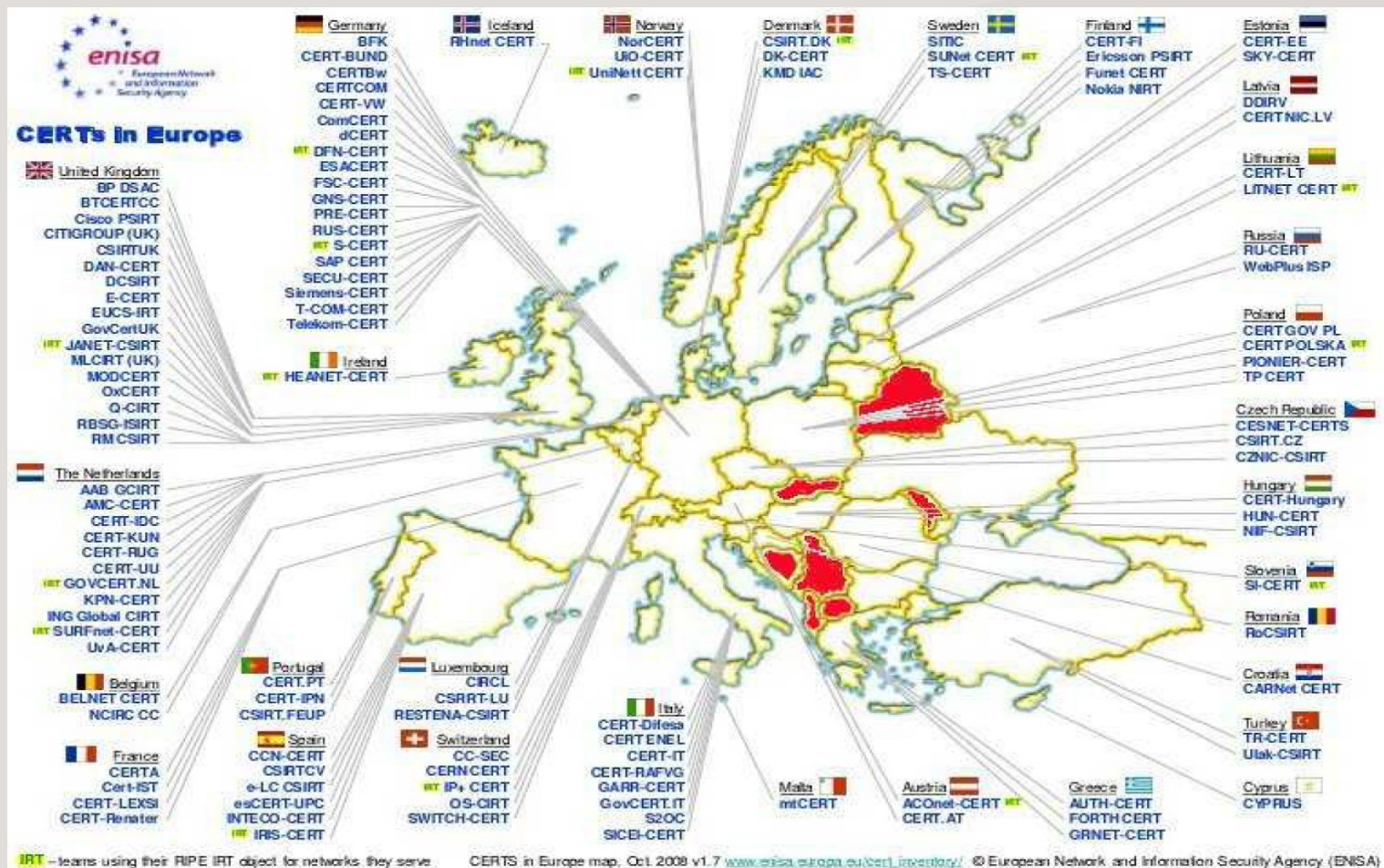
- Computer Security Incident Response Team resp. Computer Emergency Response Team
- hierarchický koncept bezpečnostních týmů, které spolupracují při řešení bezpečnostních incidentů na síti
- obvykle jsou to týmy v rámci společností jako ISP, poskytovatelé obsahu, banky apod. a nad nimi týmy národní
- národní týmy fungují ve většině civilizovaných zemí světa, ale jsou různě organizovány resp. spadají pod různé instituce



# CSIRT/CERT – jako to vypadá v Evropě (r. 2008)?



# CSIRT/CERT – jako to vypadá v Evropě (r. 2009)?



# CSIRT/CERT – co tyto týmy řeší?

- nejlépe si to ilustrujeme na příkladech:
- banka XYZ sídlící např. v Austrálii zjistí, že na serveru provozovaném v České republice jsou umístěny phishing stránky vykrádající přístupové údaje klientům banky
- banka potřebuje kontakt na někoho, s kým řešit urychlené odstranění tohoto obsahu, aby své klienty chránila
- oficiální cesta přes policii je v praxi nepoužitelná kvůli době trvání
- další příklady?

# CSIRT/CERT – co tyto týmy řeší?

- nespolupracující provideři – jak je přesvědčit ke spolupráci?
- spolupráce při odhalování škodlivého provozu na síti
- národní týmy pomáhají koordinovat rychlý společný postup v případě rozsáhlých distribuovaných útoků

# CSIRT.CZ – jak to vypadá v ČR?

- oficiální CSIRT týmy existují pouze dva – v rámci akademické sítě CESNET a centrálního registru CZ.NIC
- národní CSIRT.CZ funguje od r. 2008 jen jako modelový pilotní provoz na základě grantu MV ČR a jeho chod zajišťují členové CESNET-CERTS
- funguje pracovní skupina CSIRT.CZ, v rámci které řeší zainteresované subjekty v ČR další směřování národního týmu
- ACTIVE 24 se této skupiny účastní jako jediný webhoster a doménový registrátor v ČR (?!)

# CSIRT.CZ – jak to vypadá v ČR?

- kromě oficiálních CSIRT týmů funguje u alespoň trochu zodpovědných institucí kontakt prostřednictvím `abuse@`
- skutečně zodpovědné instituce incidenty nahlášené na tuto adresu reálně řeší a to bez zbytečných odkladů
- většina institucí nahlášené incidenty řeší až v případech, kdy způsobují škodu jim samotným
- existuje řada institucí/providerů, kde bezpečnostní incidenty neřeší nikdo a na zasláná hlášení nikdo nereaguje!



# CSIRT.CZ – jak to vypadá v ČR?

- koncepce CSIRT týmů vyžaduje zejména spolupráci
- v případě subjektů, které nekomunikují resp. nespolupracují, nastupuje národní tým, aby komunikaci zprostředkoval
- podobně pomáhá zprostředkovat komunikaci se subjekty, u kterých není zřejmý kontakt na bezpečnostní tým
- s výhodou zprostředkovává komunikaci také se zahraničními subjekty oslovováním příslušných národních CSIRT týmů

# CSIRT.CZ – jak to vypadá v ČR?

- spolupráce probíhá zejména na dobrovolné bázi, ale může být i vynucena tam, kde mají národní CSIRT týmy širší pravomoci vyplývající ze zákona (např. Estonsko)
- aktuální informace z politické stránky věci:
- materiál „Řešení problematiky kybernetické bezpečnosti České republiky“, který tuto oblast zahrnuje, byl projednán bezpečnostní radou státu a čeká se na jeho schválení vládou (cca za 14 dní)
- na post ředitele odboru kybernetické bezpečnosti MV ČR, který se touto oblastí začal od 1. února 2010 oficiálně zabývat, byl jmenován Ing. Aleš Špidla, který bude přítomen na zasedání pracovní skupiny CSIRT.CZ koncem března

# CSIRT tým u ACTIVE24

- tým nemá oficiální registraci, ale je ve všech ohledech aktivní
- drtivá většina komunikace probíhá přes [abuse@active24.cz](mailto:abuse@active24.cz)
- fungování zajišťuje tým Linuxových administrátorů a to i v rámci pohotovostního provozu mimo pracovní dobu
- řeší se nejčastěji spam, phishing, ale také závažná trestná činnost (např. šíření dětské pornografie)



# CSIRT tým u ACTIVE24

- okamžité řešení každé příchozí stížnosti na spam, který pochází z naší sítě či propaguje stránky hostované na našich serverech
- následné nalezení zdroje a jeho technické zablokování
- předání informací a doporučení zákazníkovi tak, aby se situace již neopakovala
- v případě phishingu okamžité odstranění obsahu, dohledání způsobu, jak byl obsah na server umístěn a dále ve spolupráci se zákazníkem odstranění příčiny



# CSIRT tým u ACTIVE24

- objevuje se i phishing na podvodně registrovaných doménách nasměrovaných na mnoho IP po celém světě – slouží-li doména prokazatelně pouze k tomuto účelu, je zrušena její delegace
- v případě šíření dětské pornografie nebo jiné závažné trestné činnosti je kromě dříve uvedených postupů i aktivně zahájena spolupráce s orgány činnými v trestním řízení
- toto vše se zdá jako samozřejmost, ale v praxi je to bohužel spíše vzácné – provideři velice často alibisticky poukazují na mezery v českých zákonech a incidenty neřeší, dokud neobdrží soudní příkaz



# 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 :-)
- spolupracujte při řešení incidentů, ať se svou nečinností nepodílíte na kriminalitě na internetu

