

Technologie pro zajištění bezpečnosti a vysoké dostupnosti webhostingových služeb v praxi



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



O čem přednáška bude

- příklady z praxe při zabezpečování webhostingových služeb
- seznámení s některými novými a zajímavými technologiemi
- nahlédnutí do „kuchyně“ ACTIVE 24, s.r.o.



Obecně k zabezpečení

Obecně k zabezpečení

- dobře nastavený firewall
- pravidelné bezpečnostní aktualizace
- omezení přístupu lokálním uživatelům
- fyzické zabezpečení techniky
- pravidelné zálohování
- nepřetržité napájení
- záložní konektivita
- redundance
- monitoring
-

Obecně k zabezpečení

- dobře nastavený firewall
- pravidelné bezpečnostní aktualizace
- omezení přístupu lokálním uživatelům
- fyzické zabezpečení techniky
- pravidelné zálohování
- nepřetržité napájení
- záložní konektivita
- redundance
- monitoring
-

TOTO VŠE MUSÍ BÝT V DNEŠNÍ DOBĚ SAMOZŘEJMOST
PRO ÚČINNÉ ZABEZPEČENÍ SLUŽEB JE TO ALE MÁLO

Jakým způsobem jsou dnes podnikány útoky?

Jakým způsobem jsou dnes podnikány útoky?

- v drtivé většině případů roboticky
- nejčastěji s využitím rozsáhlých botnetů
- pokud je u bezpečnostního incidentu zaznamenána činnost člověka, bývá to téměř vždy až poté, co dojde ke kompromitaci systému robotem
- ochrany musíme mít ale také proti vlastním zákazníkům
- „útok“ může být způsoben i omylem (cizím i Vaším)

Botnety

- zneužívají primárně nezabezpečené domácí počítače a až následně je tato armáda robotů využita pro skutečné útoky
- síla botnetů je obrovská (příkladem budiž celosvětový pokles objemu spamu na internetu až o 75% po vypnutí klíčové části botnetu Srizbi)
- červ Conficker a jím vytvořený patrně největší botnet současnosti

Co se tedy dá udělat pro větší bezpečnost serverů?

- proaktivní sledování systémů
- neustálé analyzování provozu, logů, anomálií atd.
- zavádění vlastních protiopatření tak, aby měly maximální účinek na ošetřovanou issue a minimální dopad na zákazníka
- sledování trendů, nasazování nových technologií



Vybrané námi používané technologie

- samozřejmě Linux :-) (převážně Ubuntu LTS)
- vlastní řešení FTP autorizace
- inteligentní greylisting
- DNSSEC
- nginx jako reverzní proxy
- LVS, VRRP, Heartbeat



Příklad z praxe I. – FTP autorizace

Příklad z praxe I. – FTP autorizace

- problém s umístováním škodlivého či nelegálního obsahu do www prostoru přes FTP
- změny jsou ale uskutečňovány s použitím regulérních přihlašovacích údajů k danému účtu
- zjištěno, že přihlašovací údaje jsou odcizovány z nezabezpečených domácích počítačů některých našich zákazníků
- co s tím?

Příklad z praxe I. – FTP autorizace

- musíme omezit přístup na FTP, i když klient použije správné přihlašovací údaje!!
- jediné, co při přihlašování víme o klientovi kromě uživatelského jména a hesla, je jeho IP adresa
- drtivá většina takovýchto incidentů je vedena z IP adres patřících zemím jako je Rusko, Brazílie, Kazachstán apod. občas i ze „západních“ zemí jako USA či Německo
- potřebuje se náš zákazník z těchto zemí hlásit na FTP?

Příklad z praxe I. – FTP autorizace

- v drtivé většině případů nepotřebuje, někdy přece jen ano
- jak ale přimět FTP démona, aby odmítal login z těchto IP?
- proftpd provádí autorizaci pomocí modulů PAM
- bohužel neexistuje modul jako pam_geoip
- v nových verzích PAM ale existuje modul pam_exec

Příklad z praxe I. – FTP autorizace

- tedy kompilace nových PAM knihoven
- implementace scriptu, který bude spouštěn pomocí `pam_exec` a následně analyzuje IP adresu klienta a rozhodne o povolení či zamítnutí autorizace
- implementace v jazyce Python využívá knihoven `geoip` a je napojena na naše interní systémy, aby umožňovala zákazníkům ovlivnit „důvěryhodné“ IP adresy oproti default nastavení
- relativně jednoduché a přitom perfektně účinné řešení

Ohlasy a výsledky nasazení nové FTP autorizace

- v první řadě jsme od té doby nezaznamenali ani jediný incident s neoprávněným přístupem na FTP!!
- proběhlo několik jednotlivých telefonátů od zákazníků, kteří potřebovali umožnit přístup na FTP z rizikových zemí a ti si jednoduše pro jejich konkrétní web přístup povolili přes naše zákaznické centrum
- omezení rozesílání spamu, umístování nelegálního obsahu, podvodného obsahu typu phishing apod., tedy všech činností, ke kterým byly FTP účty z ukradenými údaji zneužívány

Příklad z praxe II. – greylisting

Příklad z praxe II. – greylisting

- relativně stará technologie, ale má drtivý účinek na spam
- ještě lépe funguje při spojení s často aktualizovanými blacklisty
- odmítá spam hned na začátku procesu přijímání pošty
- greylistování veškerého mailového provozu je nicméně v praxi nereálné kvůli negativním efektům této technologie
- dá se ale použít nějak inteligentně, abychom využili maximum z výhod této technologie a omezili na minimum její nevýhody?

Příklad z praxe II. – greylisting

- možné to je s využitím statistických dat o mailovém provozu
- při velkém objemu pošty se neobejdeme bez technologií, které dokážou spam s velkou procentní úspěšností odrážet hned na začátku procesu přijímání pošty a k tomu je greylisting ideální, protože maily neodmítá definitivně
- při přijímání emailu přes SMTP známe čtyři základní údaje
- dokážeme podle nich s určitou pravděpodobností rozpoznat, jestli je mail regulérní nebo spam?

Příklad z praxe II. – greylisting

- HELO hlavičku je možné kontrolovat pouze omezeně
- Envelope TO a FROM hlavičky samozřejmě kontrolujeme na minimální validnost, ale také je nemůžeme omezovat příliš, pokud chceme zachovat obecnou funkčnost SMTP
- nejvíce se dá statisticky poznat podle IP adresy klienta, který se na SMTP připojuje



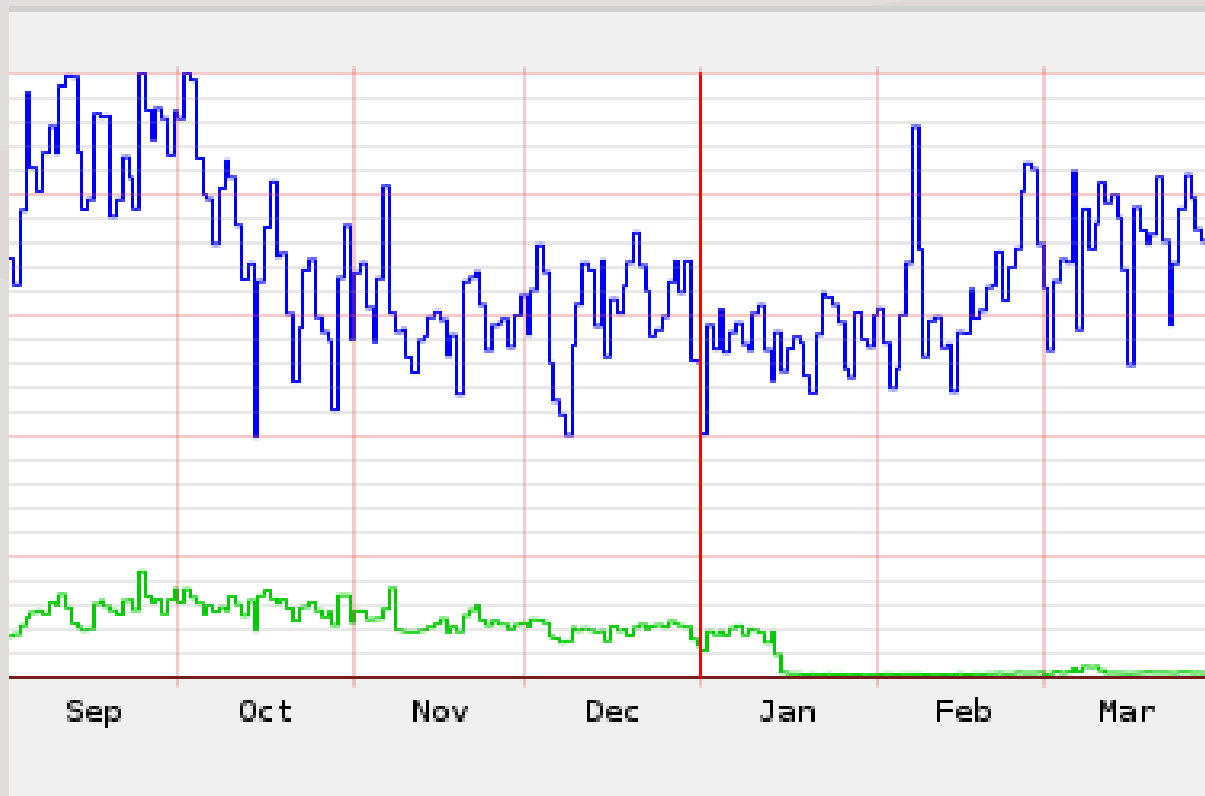
Příklad z praxe II. – greylisting

- drtivá většina spamu pochází z botnetů a zahraničních sítí s nulovou kontrolou provozu
- greylist tedy aplikujeme pouze na emaily z těchto předem „podezřelých“ zdrojů
- tím se zajistí, že valná většina spamu musí projít greylistem a valná většina regulérní pošty je přijata ihned
- a opačně: minimum spamu je přijato bez greylistování a zároveň minimum regulérní pošty musí greylistem projít

Příklad z praxe II. – greylisting

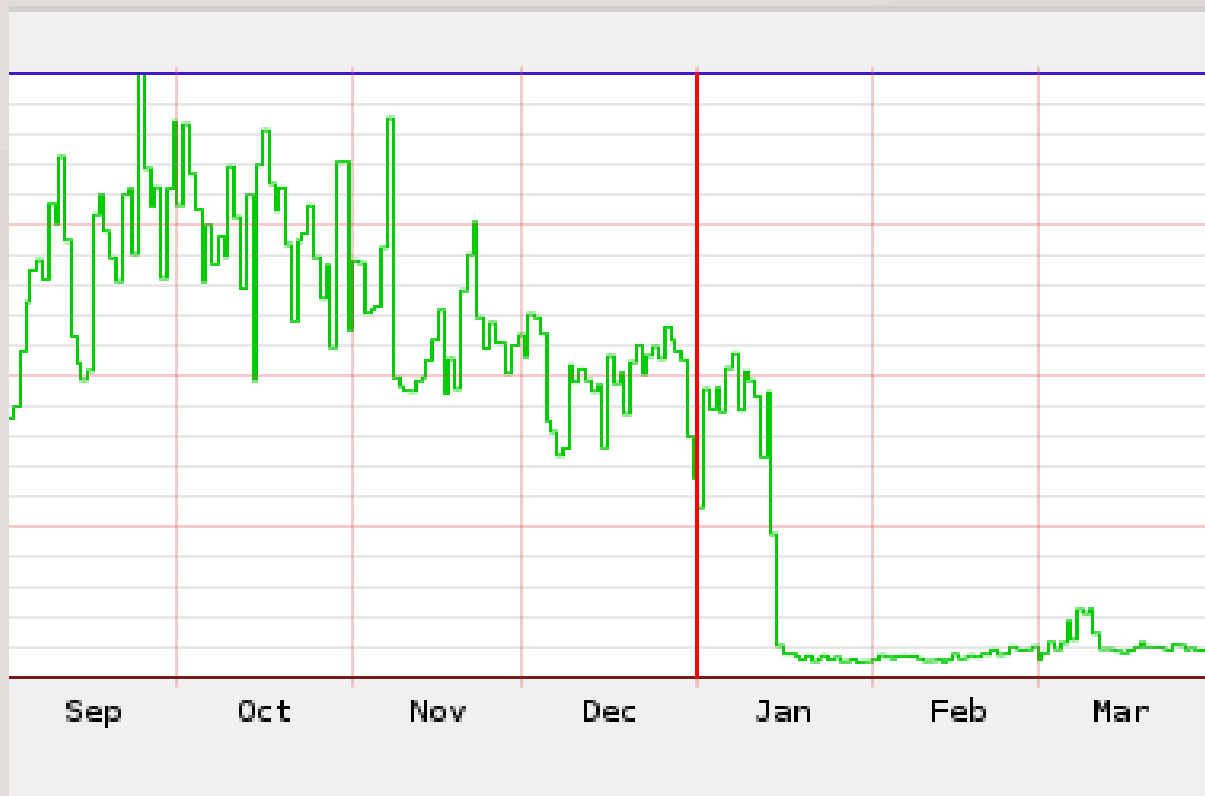
- implementací greylistingu existuje celá řada
u nás používáme na většině emailových systémů postfix
a greylistování je realizováno pomocí démona polycyd
- polycyd může být už při základním nakonfigurování velmi efektivní
- zároveň má velmi přehledný kód a dá se tedy snadno přizpůsobovat
Vašim potřebám tak, aby podrobil IP adresu klienta různým testům,
které určí, jestli mail greylistem bude procházet nebo ne
- umožňuje kontrolu i dalších SMTP hlaviček a tedy můžete např.
greylisting vypnout pro konkrétní schránku či doménu

Ohlasy a výsledky zavedení greylistingu



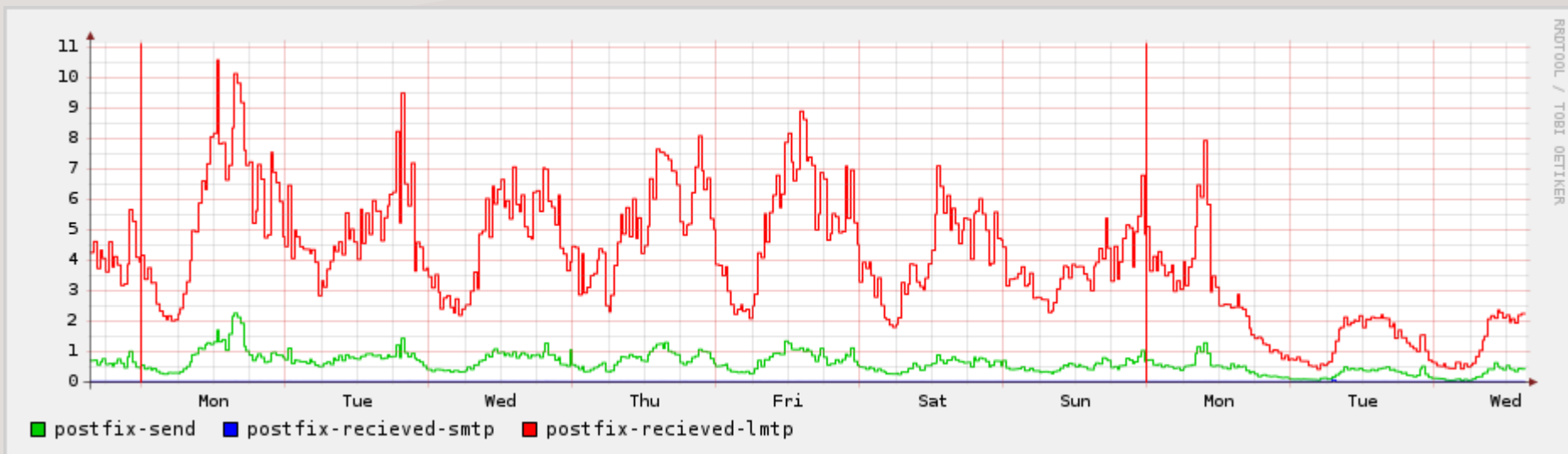
provoz na záložním MX v době, kdy primární servery normálně pracují

Ohlasy a výsledky zavedení greylistingu



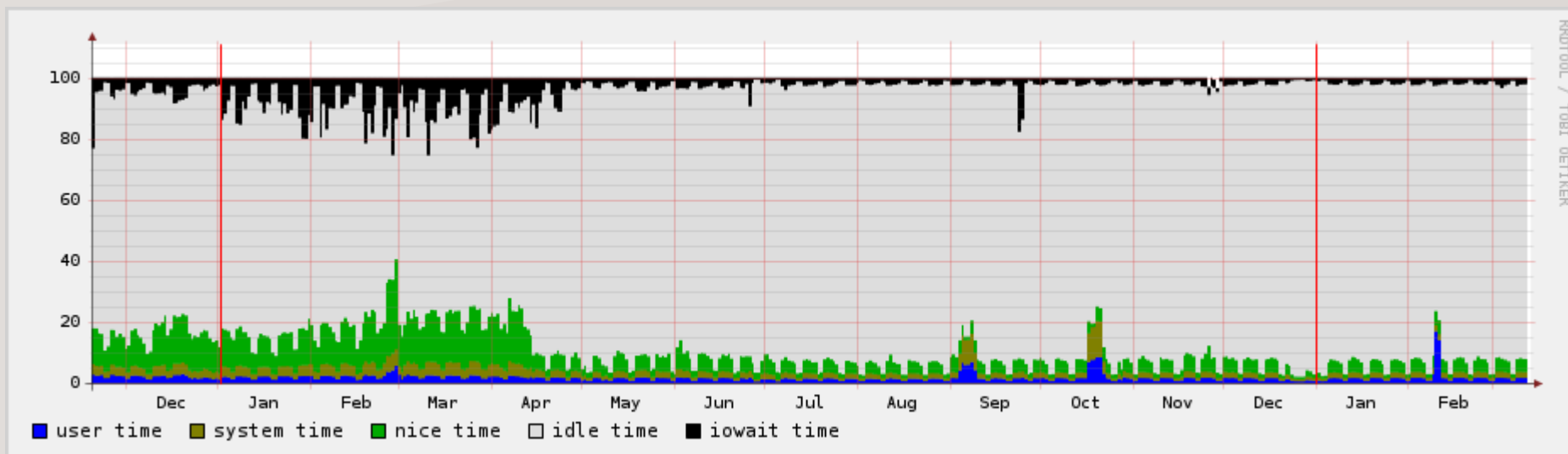
provoz na záložním MX v době, kdy primární servery normálně pracují

Ohlasy a výsledky zavedení greylistingu



provoz na jednom z mailových backendů

Ohlasy a výsledky zavedení greylistingu



využití CPU na jednom z mailových backendů

Ohlasy a výsledky zavedení greylistingu

- přímé reakce od zákazníků, kteří volali jen proto, že jim klesl objem doručeného spamu tak, že se ptali po příčinách a i děkovali
- kladné ohlasy od zákazníků na veřejných diskusních fórech
- velké ulehčení práce všem mailovým serverům, které dále zpracovávají přijaté emaily, neboť počet zpracovávaných mailů klesl celkově o 70%
- jen několik jednotlivých případů, kdy zákazník zaznamenal zdržení mailu, které skutečně způsobil greylisting s tím, že pokud si dále nepřál být touto metodou chráněn, greylisting si pro konkrétní schránku snadno sám vypnul přes naše zákaznické centrum

Příklad nové technologie v praxi - DNSSEC

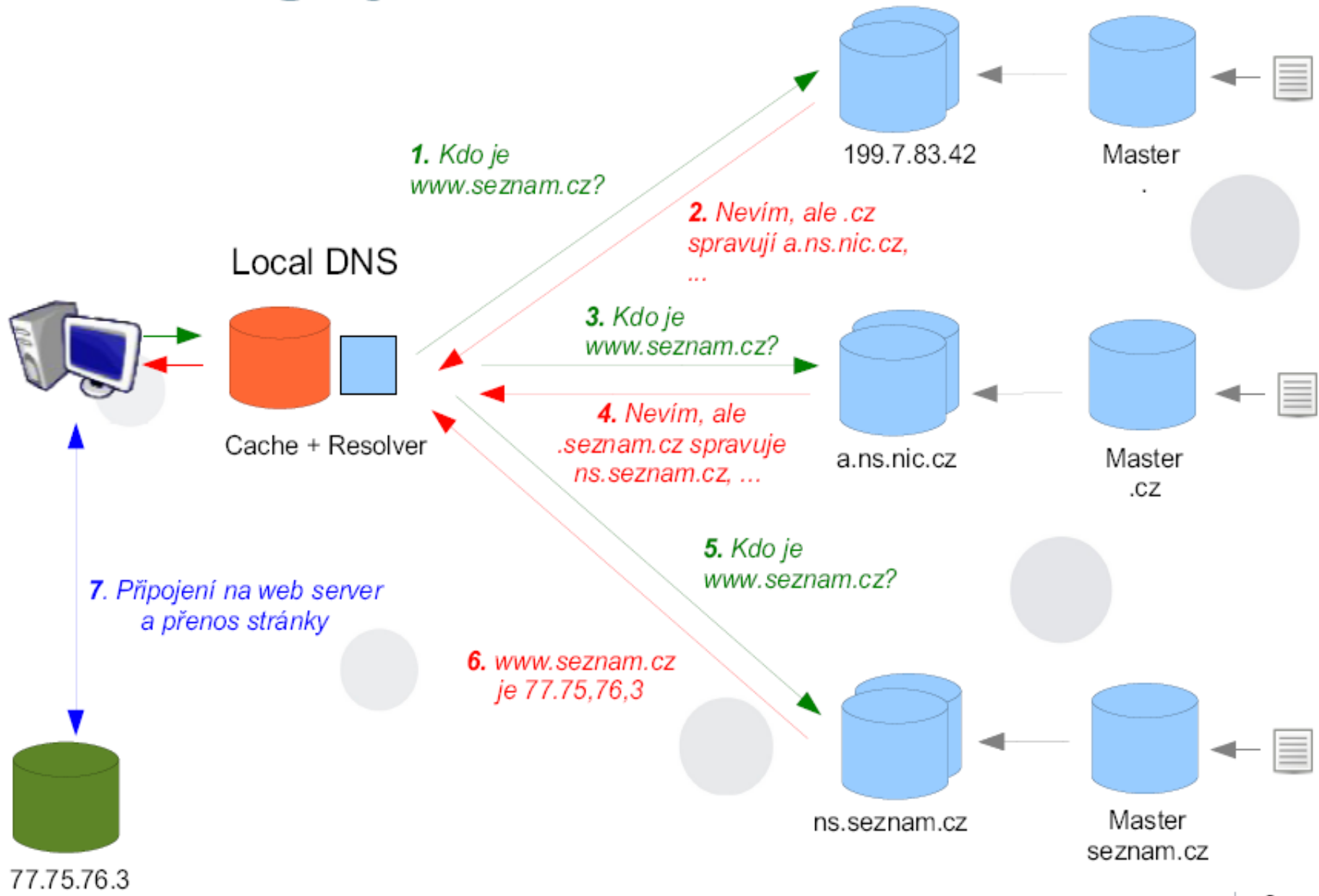


Příklad nové technologie v praxi - DNSSEC

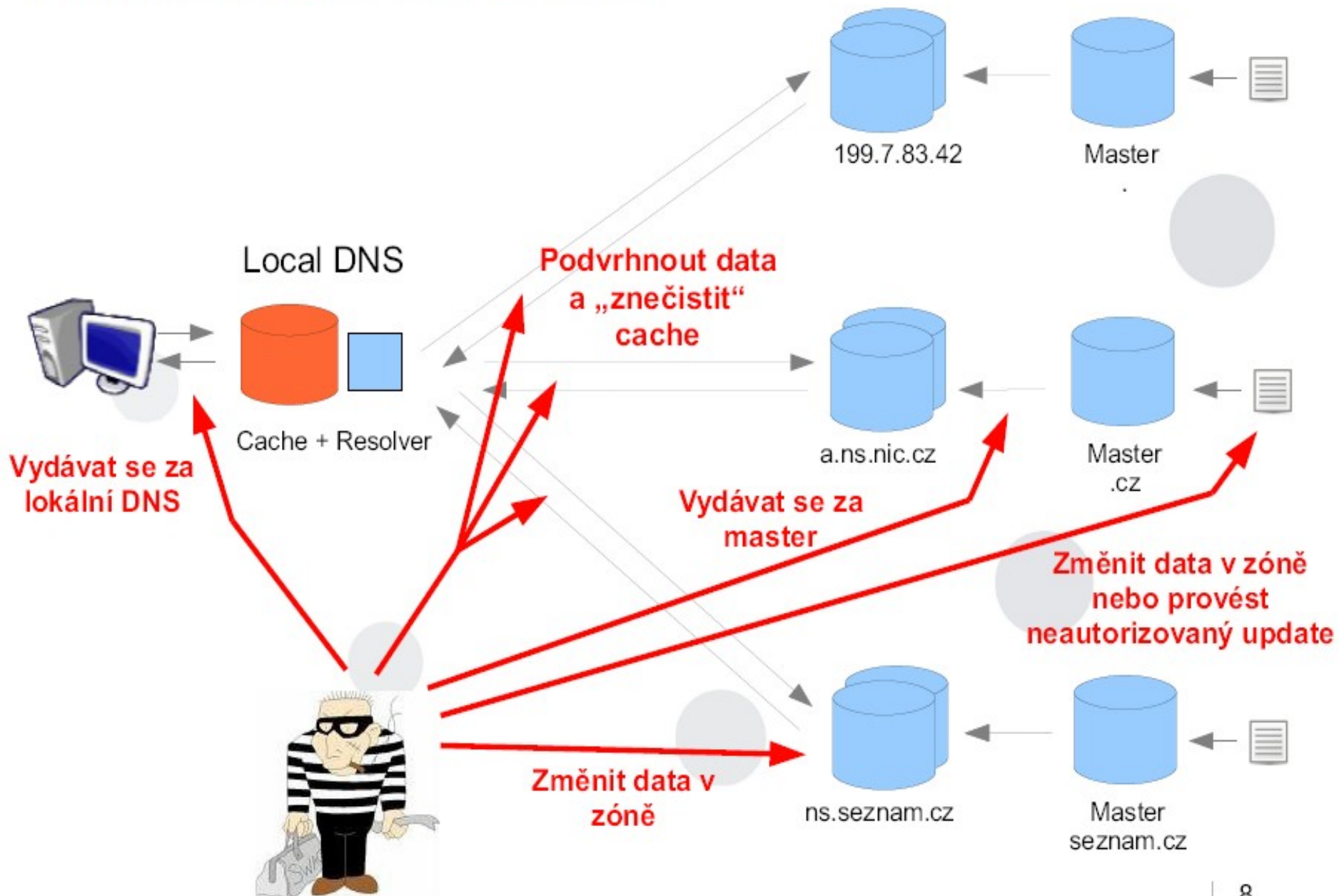
- na konci září 2008 byla na CZ doméně spuštěna podpora DNSSEC
- jedná se o standardizované doplnění klasického DNS protokolu o prvky elektronického podepisování
- jako jediný registrátor CZ domén jsme spustili podporu DNSSEC pro naše zákazníky ve stejný den jako CZ.NIC
- v současné době funguje DNSSEC pouze na pěti národních doménách včetně té naší
- aktuálně je DNSSEC aktivní na 611 českých doménách, přičemž 550 z nich je registrováno přes ACTIVE 24
(údaj k 10.3.2009)



Jak funguje DNS



Zranitelnost DNS



Příklad nové technologie v praxi - DNSSEC

- 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)

Ještě jedna zajímavá technologie v praxi - nginx

Ještě jedna zajímavá technologie v praxi - nginx

- jedná se o webový server a reverzní proxy s minimálními nároky na systémové prostředky a minimální režii
- je naprogramován velmi robustně, efektivně a velmi rychle se vyvíjí
- na jeho základě vyvíjí Google „svou“ ncache
- jako webový server používáme na Linuxových systémech apache, který zajistí veškerou funkcionalitu, kterou od nás zákazníci webhostingu očekávají, zároveň má ale své „provozní“ mouchy
- nginx dokáže řadu těchto much eliminovat nebo minimalizovat

Ještě jedna zajímavá technologie v praxi - nginx

- jeden z problémů apache při hostingovém nasazení je jeho velká režie na každé spojení klienta
- s rostoucím počtem klientů značně roste počet běžících procesů apache a tím se obsazuje paměť a zvedá se režie systému
- nginx má naopak režii minimální a využívá thready – na průměrném hostingovém serveru dokáže obsluhovat všechny klienty jedním nebo dvěma procesy

Ještě jedna zajímavá technologie v praxi - nginx

- nasazením nginx jako reverzní proxy před apache server kombinujeme výhody aplikačních možností apache serveru s provozními výhodami nginx
- na jednom z hostingových serverů, na který byl veden DDoS útok a apache server již nezvládal obsluhovat všechny přicházející požadavky, jsme nasazením nginx dosáhli úplného zklidnění situace
- podobně pomáhal nginx zvládat nápor návštěvníků na serverech nedávného mistrovství světa v klasickém lyžování v Liberci

Závěr

- uvedené příklady demonstrují, jak otevřené technologie mohou velmi úspěšně pomáhat při řešení každodenních otázek bezpečnosti, stability a dostupnosti služeb
- důležité je, že žádná sebemodernější technologie není samospasitelná a je potřeba ji nasazovat citlivě s ohledem na zákazníky a služby, které jim poskytujeme
- otevřené technologie nám dávají možnost použít kvalitní základ konkrétního projektu a přizpůsobit si ho pro nasazení do našeho vlastního specifického prostředí – nejsme pak vázáni hotovým produktem třetí strany a jeho omezeními

