

Data gram

červen 2008

zpravodaj sdružení CESNET

číslo 17

Rok 2007 obhájěn

Pro výzkumný záměr *Optická síť národního výzkumu a její nové aplikace*, jehož je CESNET řešitelem, představoval rok 2007 polovinu předpokládané doby řešení. Součástí pravidelné roční oponentury proto bylo určité bilancování, zda se jeho řešení ubírá správným směrem.

Jako jeden z podkladů jsme připravili obvyklou rozsáhlou roční zprávu shrnující naše aktivity a výsledky dosažené v roce 2007. Kromě vlastního výzkumného záměru přináší základní informace také o souvisejících aktivitách, zejména o zahraničních projektech, jejichž řešení se účastníme. Letošní zpráva má 238 stran a můžete si ji přečíst na adrese



<http://www.cesnet.cz/doc/2007/zprava/>

Vlastní oponentní řízení se konalo se ve středu 6. února v sídle sdružení. Naše výsledky posuzovala šestičlenná komise ve složení:

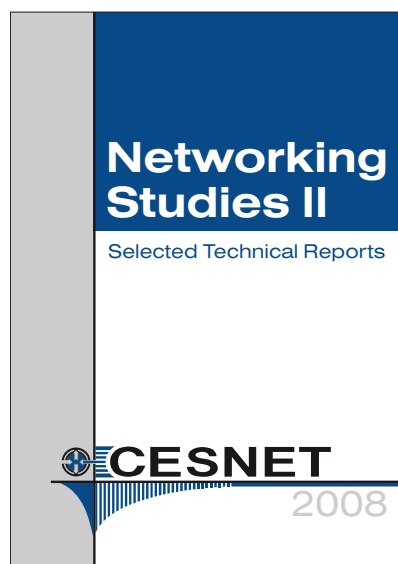
- Ing. Vít Kavan, CSc., MŠMT, předseda
- RNDr. Jaroslav Bobovský, BESET, s. r. o.
- Ing. Michal Dočekal, GTS Novera
- Prof. Ing. Pavol Horváth, CSc., STU Bratislava
- Ing. Pavel Zima, Seznam.cz, a. s.
- RNDr. František Zedník, UP Olomouc

Vycházela ze dvou oponentských posudků, jejichž autory byli pánové

- Mgr. Ondřej Filip, CZ.NIC, z. s. p. o.
- Ing. Tibor Weis, CIT TU Zvolen

Stejně jako v předchozích letech byla oponentura úspěšná. Komise ocenila kvalitu dosažených výsledků, a to i v mezinárodním kontextu. Důkazem je jak přebírání našich výsledků zahraničními institucemi, tak zájem zahraničních partnerů o spolupráci s CESNETem na dalších projektech.

Sborník zpráv 2008



V loňském roce jsme poprvé vydali sborník vybraných technických zpráv nazvaný *Networking Studies* (od roku 2007 vydáváme technické zprávy standardně v angličtině). U našich zahraničních partnerů se setkal s velmi kladným ohlasem, proto jsme se rozhodli v této aktivitě pokračovat a v letošním roce připravit další vydání.

Výsledkem je publikace nazvaná *Networking Studies II - Selected*

Technical Reports. Najdete v ní třináct vybraných technických zpráv z celkového počtu 38, které jsme publikovali během roku 2007. Proti původnímu vydání byly zprávy pro sborník znovu editovány a nově typograficky upraveny.

Přestože zprávy nepokrývají celou šíři našich aktivit, je tematický záběr sborníku značný. Abychom čtenáři usnadnili orientaci, rozdělili jsme jej do čtyř částí nazvaných:

- *CESNET2 network*, kde najdete čtveřici textů skupiny zabývající se rozvojem NREN. Týkají se především rozvoje DWDM infrastruktury a implementace skupinového adresování pro protokol IPv6.
- *Network monitoring* obsahuje informace o třech různých námi vyvinutých nástrojích pro sledování sítě.
- *Quality of service* popisuje analytický model přenosového zpoždění a prostředek pro kvantifikaci nárazového datového provozu.
- *Services and applications* přináší čtyři aplikačně orientované zprávy. Věnují se virtualizaci METACentra, prostředí pro spolupráci distribuovaných týmů a vzdálené konfiguraci zařízení po síti.

Celkový rozsah letošního sborníku činí 208 stran. Jeho tištěná verze by měla být k dispozici v knihovnách všech našich členů. Elektronickou podobu najdete na stránce

<http://www.cesnet.cz/doc/2008/networking-studies/>

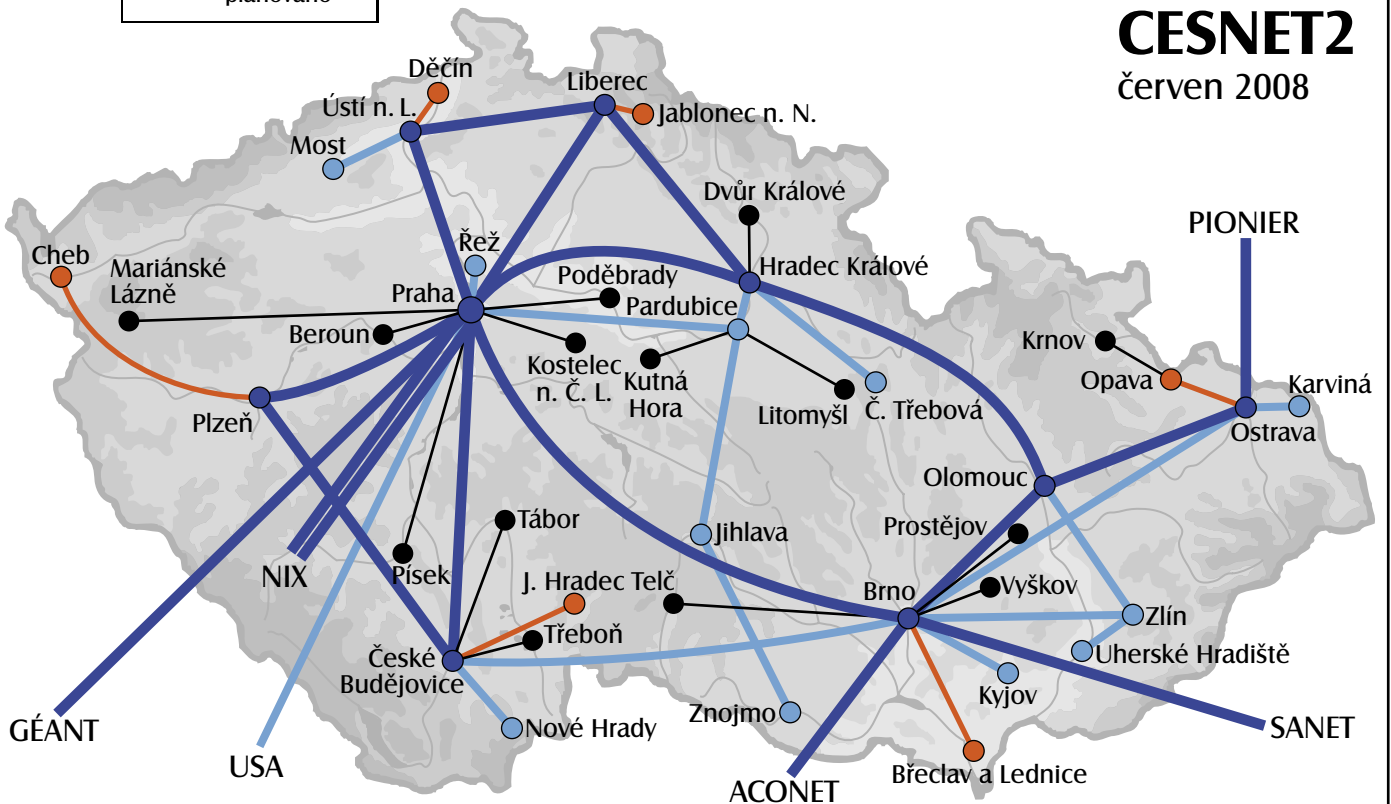
Topologie sítě GÉANT2 a CESNET2

GÉANT2 červen 2008



- 10 Gb/s
- 1-2,5 Gb/s
- 622 Mb/s
- 100-155 Mb/s
- nižší
- - - plánováno

CESNET2 červen 2008



Řešení bezpečnostních incidentů

Jistě není třeba zdůrazňovat, že Internet má kromě řady přínosů i svá nebezpečí. Nevyžádaná reklama v elektronické poště pouze obtěžuje, ale škodlivý software či cílené útoky po síti mohou narušit činnost uživatelských počítačů nebo vést ke ztrátě či zcizení důležitých dat.

Jako reakce na toto nebezpečí vznikají na straně provozovatelů sítí či internetových služeb týmy, které se zabývají odhalováním, řešením a prevencí bezpečnostních incidentů. Bývají označovány zkratkou CSIRT (Computer Security Incident Response Team) nebo CERT (Computer Emergency Response Team). Přestože se zdá, že význam druhé zkratky je poněkud širší, oba pojmy se používají prakticky jako synonyma a v názvech týmů je najdete zastoupeny víceméně náhodně.

Bezpečnostní týmů existuje celá řada, najdete je u poskytovatelů připojení, síťových služeb i ve větších sítích koncových zákazníků. Účinná opatření proti různým formám internetových útoků zpravidla vyžadují spolupráci několika subjektů. Proto bývá zvykem vytvářet hierarchie a skupiny bezpečnostních týmů. Některé z nich si vypracovaly i systém certifikací osvědčujících, že certifikovaný tým dodržuje dané postupy.

CESNET-CERTS

Základním kamenem infrastruktury pro řešení a prevenci bezpečnostních incidentů v síti CESNET2 je tým CESNET-CERTS založený v roce 2004. Tvoří jej zaměstnanci sdružení a jeho hlavním úkolem je koordinovat bezpečnostní aktivity v rámci sdružení a jeho členů, definovat bezpečnostní politiky, pomáhat připojeným organizacím při zakládání vlastních týmů a při řešení konkrétních incidentů. V neposlední řadě také poskytuje okolnímu světu centrální kontakt pro bezpečnostní otázky, jež se dotýkají sítě CESNET2.

CESNET-CERTS úzce spolupracuje s bezpečnostními týmy organizací připojených k síti CESNET2. Komunikuje s nimi jak individuálně, tak na společných akcích, jako jsou výjezdní semináře CESNETu či odborné semináře věnované bezpečnostní problematice, které pořádá přibližně v ročních intervalech. Informace, jež účastníci seminářů získají, slouží především pro předcházení bezpečnostním incidentům a zvyšují připravenost na jejich řešení.

Vlastní výkonná činnost CESNET-CERTS zahrnuje kromě reakcí na různé problémy také provoz a vývoj systému IDS (Intrusion Detection System), který slouží k odhalování síťových útoků. Je založen na volně šiřitelném programu *LaBrea*, do nějž bylo provedeno několik úprav podle specifických potřeb sítě CESNET2. Velmi pozitivním trendem provozu IDS je výrazný pokles útoků ze strojů v síti CESNET, počet útoků se za uplynulý rok snížil na méně než třetinu v porovnání s rokem 2006.

Program *LaBrea* je velmi účinný, jeho výkon však nestačí na datové toky v řádu gigabitů. Skupina programovatelného hardwaru proto vyvíjí jeho akcelerátor založený na technologii FPGA. Několik akceleračních karet nazvaných *Traffic Scanner* již v síti CESNET2 pracuje, vesměs s kladnými výsledky. Zatímco softwarový *Snort* si poradí s datovými toky v řádu stovek megabitů za sekundu, s kartou *Traffic Scanner* zvládá až 4 Gb/s.

Důležitou složku aktivit CESNET-CERTS tvoří mezinárodní spolupráce. Tým spolupracuje s významnými bezpečnostními platformami, kterými jsou aktivita TF-CSIRT při organizaci TERENA a nadnárodní organizace FIRST (Forum of Incident Response and Security Teams). CESNET-CERTS zatím stále zůstává



jediným oficiálně uznaným CSIRT týmem v České republice. Počátkem letošního roku prošel tzv. *akreditačním* procesem, a tím se dostal do elitního klubu akreditovaných evropských bezpečnostních týmů.

CSIRT.CZ

Získané zkušenosti a mezinárodní vazby uplatňujeme mimo jiné i při spolupráci na budování pracoviště CSIRT.CZ. Jedná se o jeden z dílčích úkolů projektu *Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky*, který je financován Ministerstvem vnitra ČR. CSIRT.CZ je modelovým pracovištěm, které koordinuje a pomáhá při řešení bezpečnostních incidentů vzniklých v sítích provozovaných v České republice v případě, kdy správce sítě na oznámení nereaguje nebo se vyskytne jiný problém. Z tohoto pohledu CSIRT.CZ funguje jako „místo poslední záchrany“, na něž se uživatelé mohou obrátit se žádostí o pomoc.

Pilotní provoz CSIRT.CZ byl zahájen 3. dubna 2008. Jeho chod zatím zajišťují členové týmu CESNET-CERTS. Jejich zkušenosti však mají posloužit především pro rozeběhnutí příslušných mechanismů a výchovu nových členů, kteří pak převzou jeho rutinní chod. Více se dočtete na stránkách

<http://www.csirt.cz/>

<http://www.cesnet.cz/csirt/>

Úvod

Dne 3. 4. 2008 byl spuštěn pilotní provoz CSIRT.CZ. CSIRT.CZ (Computer Security Incident Response Team) je nezávislý modelový bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích ČR.

Naše cíle

Cílem CSIRT.CZ je pomáhat provozovatelům internetových sítí v České republice zřizovat jejich vlastní bezpečnostní týmy a bezpečnostní infrastrukturu, řešit bezpečnostní incidenty a tím zlepšovat bezpečnost jejich sítí i globálně Internetu.

CSIRT.CZ také pomáhá předávat hlášení o bezpečnostních incidentech správcům těchto sítí nebo členům, z nichž incidenty pocházejí, ale které se službami nereagují. V tomto směru tedy slouží jako jakýsi "místní poslední záchraný" pro případ, že jiné metody kontaktování správců sítí selhají.

Tým

Tým CSIRT.CZ vznikl v září 2007. V současnosti se skládá ze členů bezpečnostního týmu CESNET-CERTS, kteří budou při práci

E-infrastruktura a Česká republika

V pondělí 9. června CESNET uspořádal seminář, jehož cílem bylo upozornit na vývoj budování výpočetní infrastruktury v Evropě, na zaostávání České republiky v této oblasti a na všeobecný nezájem tuto oblast v ČR řešit. Seminář byl součástí aktivit týkajících se strategických úvah a diskusí o stanovení další koncepce rozvoje sdružení CESNET. Hlavním řečníkem byl Dr. Eugene Yeh, ředitel NCHC - National Center for Supercomputing na Taiwanu. Pan Yeh zavítal do České republiky se svými kolegy v rámci své evropské cesty, během níž navštívil celosvětové setkání OpenGrigForum OGF23 a významná evropská superpočítačová centra.

NCHC je zároveň provozovatelem národní akademické sítě TWAREN (<http://www.nhc.org.tw/en/>). Svým určením a zaměřením je velice podobné sdružení CESNET. Díky státní podpo-



ře e-infrastruktury poskytované Taiwanem se počítačové vybavení a síťová infrastruktura, které v posledních letech NCHC vybudovalo, dostaly na čelní pozice v Asii a zároveň zaujímají vysoké postavení v celosvětovém měřítku superpočítačů (žebříček TOP500, viz www.top500.org).

Ve světě existují dva základní modely budování národní e-infrastruktury zahrnující bohaté komunikační, výpočetní a úložné služby. NCHC představuje příklad prvního přístupu, kdy je národní e-infrastruktura budována jednou organizací, jež zajišťuje jak komunikační, tak výpočetní a úložné služby.

V mnoha evropských zemích se spíše uplatňuje druhý model - dvě nezávislé organizace, z nichž jedna se zabývá síťovým prostředím a druhá výpočetními a úložnými službami (ať už tuto oblast nazýváme superpočítače nebo počítače pro High Performance Computing, HPC) a podporou aplikací, které se na nich dají řešit. Jako příklad bylo na semináři představeno několik zemí provozujících alespoň jedno superpočítačové centrum zajišťující výpočetní servis pro náročné výpočty. Patří mezi ně Itálie (GARR-CENICA), Finsko (FUNET-CSC), Nizozemsko (URFNET-SARA) či Španělsko (REDIris-BCC). V zemích, jako je Německo či Velká Británie, je podobných center vždy několik a specializují se na konkrétní problematiku.

V poslední době se v Evropě rozeběhly nové projekty z této oblasti, jež podporuje i 7. rámcový program EU. Jedním z významných je projekt PRACE (Partnership for Advanced Computing in Europe, www.prace-project.eu) zabývající se právě tím, jak efektivně řešit výpočetně náročné problémy moderní vědy v kvantové chemii, studiu nanomateriálů, geofyzice, proudění plynů a kapalin, vývoji léčiv a dalších oblastech. Česká republika je bohužel jedinou zemí, jež není v projektu zastoupena.

CESNET Conference 2008

Po dvou letech od CESNET Conference 2006 pořádáme v září letošního roku druhou mezinárodní odbornou konferenci, tentokrát s podtitulem *Security, middleware and virtualization - glue of future networks*. Zaměřuje se především na vyšší vrstvy datových komunikací, řešící otázky identity uživatelů, jejich přístupových práv, zabezpečení a také na metody virtualizace

a budování virtuálních infrastruktur. Pokud vás tato problematika zajímá, rádi vás přivítáme mezi účastníky. Konference, jejímž jazykem je angličtina, se koná 25.-26. září 2008 v Praze. Podrobnosti najdete na stránce

<http://www.ces.net/conference08/>



CESNET 08

conference

Prague, 25-26 September 2008

security
middleware
virtualization