

Z á p i s
ze schůze Komise pro informační technologie
konané dne 21. září 2011

Přítomni: J. Anděl, V. Babický, L. M. Bárta, Beneš, V. Brunnhofer, I. Černý, O. Číp, Č. Číšecký, P. Divina, M. Duda, M. Indra, M. Jarník, A. Kugler, M. Nečesal, M. Papík, H. Pospíšil, M. Salaj, M. Šimonová, M. Švamberková, M. Tůma, J. Vackář, P. Vaníček, P. Vondrášek

Omluveni: M. Fridrich, V. Havlík, M. Heřman, J. Chudoba, O. Jakl, I. Janda, J. Jursa, L. Pellar, P. Sunega, J. Štrunc, J. Vojířová

Program:

1. Informace o nasazení bezpečnostních zařízení FortiGate v ÚGN
2. Posouzení nových žádostí o dotace
3. Informace o činnosti bezpečnostní skupiny CAS-CSIRT
 - a. Bezpečnostní incidenty
 - b. Problémy s rekurzivními DNS
4. Různé

Schůzi zahájil a řídil předseda Komise M. Tůma.

Ad 1)

V úvodu jednání vystoupili zástupci firmy FORTINET s technickou informací o instalaci firewallu FortiGate -110C v Ústavu Geoniky AV ČR, v. v. i. v Ostravě. Zařízení FortiGate představuje bezpečnostní bránu s pokročilým firewallem, VPN koncentrátorem, prevencí proti průniku do systému (IPS), webové filtrování, antivirus / antispyware / antimalware a antispam. Lze ho považovat za možnou alternativu k zařízením Cisco nebo Juniper. Prezentace tvoří přílohu tohoto zápisu.

Ad 2)

M Indra přednesl dvě žádosti o dotace z prostředků KIT doručených do 20. 9. 2011. Obě žádosti splňovaly dotační kritéria Komise a byly řádně doložené cenovými nabídkami.

- Ústav Informatiky AV ČR, v. v. i. předložil žádost o dotaci ve výši 60tis. Kč na výstavbu infrastruktury Eduroam v budově ÚI. Požadovaná částka představuje 50% z celkových nákladů, doložených cenovou nabídkou fy. Intercom Systems. a.s.
- Fyzikální ústav AV ČR, v. v. i. předložil žádost o dotaci ve výši 113tis. Kč na vybudování přímé optické trasy mezi lokalitami Cukrovarnická a Slovanka FZÚ. Požadovaná částka představuje 50% celkových nákladů, doložených cenovou kalkulací a cenovou nabídkou fy. Fibre Professionals.

Po krátké diskusi a na základě hlasování Komise doporučila poskytnout ze svých prostředků v roce 2011 požadované dotace oběma žadatelům.

Ad 3)

- P. Vaníček stručně informoval o činnosti bezpečnostního týmu CAS-CSIRT. Bezpečnostní tým od svého založení pracuje již zcela rutinně a prakticky denně řeší společně se správci sítí pracovišť AV ČR nahlášené bezpečnostní incidenty. Přesto, že počet bezpečnostních incidentů proti minulému období mírně poklesl, je třeba stále věnovat velkou pozornost zabezpečení lokálních sítí a jednotlivých počítačů nejen proti vnějším ale i proti vnitřním útočníkům. Dále P. Vaníček zmínil stále rostoucí podíl sítí infikovaných počítačů – botnetů sloužících zejména k šíření škodlivých kódů vedoucích k některým zaznamenávaným bezpečnostním incidentům.
- P. Vaníček upozornil na velký počet tzv. otevřených rekurzivních doménových serverů. Jedná se o servery, které poskytují doménové služby externím žadatelům. Povolení této služby může teoreticky umožnit napadení útoky DoS. Správce cz domén CZ.NIC proto důrazně doporučuje nepoužívat doménové servery s otevřenými

rekurzemi. Návod k odstranění rekurzí jsou k dispozici na stránkách CZ.NIC:
<http://podpora.nic.cz/page/530/jak-odhalit-otevreny-rekurzivni-name-server/>

- M. Indra v této souvislosti zdůraznil, že je nutné, aby správci lokálních doménových serverů pro domény třetího řádu vždy konzultovali eventuální úpravy konfigurací serverů (zejména změnu IP adresy, změnu doménového jména nebo změnu sekundárního doménového serveru) se správcem primárního doménového serveru sítě AV ČR Ing. P. Vaníčkem.

Ad 4)

- M. Indra stručně informoval o postupu prací na projektu „Federace identit“, který je řešen v SSČ. Projektem se zabývají pracovníci Divize informačních technologií SSČ za účinné pomoci OIT KNAV AV ČR, kde systém „Identity Provider“ je již funkční. Pilotní verze projektu by mohla být zprovozněna do konce roku 2011.
- M. Šimonová informovala o připravovaném semináři fy. Autocont CZ a. s., který se uskuteční ve vile Lanna dne 9. 11. 2011.

Předpokládaný program semináře:

- Virtualizace - servery a zejména desktopy. Představit stručné porovnání Vmware/citrix/MS
- přístup pro mobilní uživatele - s důrazem na bezpečnost (trápí je zejména možnost zavirování, ale i ochrana citlivých dat na vybraných ústavech)
- bezpečnost - ochrana a zneužití dat, prevence, optimalizace bezpečnosti, patch management!,
- optimalizace tiskového prostředí
- poštovní systémy a systémy pro skupinovou spolupráci, koncepce poštovního serveru - OPTIMALIZOVANÝ DOSTUPNÝ POŠTOVNÍ SERVER
- monitoring - koncových stanic + serverů a aplikací
- M. Šimonová také informovala o nabídce společnosti Alef Nula uspořádat seminář pro pracovníky, dne 29. 10. 2011 proběhne informační schůzka zástupcu SSČ se zástupci společnosti.
- Komise pro informační technologie vzala na vědomí návrh na kooptaci Ing. Martina Papíka, PhD. - vedoucího nově ustaveného odboru Informačních a komunikačních technologií (OKIT) SSČ AV ČR, v. v. i., který bude předložen ke schválení Akademické radě.
- Zápis i prezentace fy. FortiGate budou vystaveny na <https://kit.avcr.cz>

V Praze, dne 27. 9. 2011

Zapsala: M. Šimonová

Schválil: M. Tůma