ÚVT MU
zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě • duben 2007 • roč. XVII • č. 4

Spam – co s ním?

Miroslav Bartošek, ÚVT MU

Elektronická pošta, e-mail, je jedním z obrovských fenoménů posledního desetiletí. Podstatně zefektivnila komunikaci a přispěla tak k výraznému zvýšení produktivity práce ve všech oblastech. Každý, kdo ještě zažil ve své práci předinternetovou éru, mi dá jistě za pravdu, že rozdíl mezi rychlou e-mailovou komunikací s kýmkoliv-kdykoliv-kdekoliv na světě a klasickou papírovou/dopisní korespondencí je nebetyčný. A to nejen při tak komunikačně intenzivních akcích, jako je například pořádání konferencí či odborná spolupráce rozsáhlých týmů, ale i v běžném každodenním životě. Bez e-mailu si lze dnes již stěží představit práci akademika – ale i úředníka, fungování univerzity, ale třeba i osobní komunikaci většiny z nás. E-mail přitom používáme nejen k vlastní komunikaci a výměně dokumentů; e-mailová schránka nám čím dál více slouží také jako pohotový osobní diář, adresář, poznámkový blok, úkolník a efektivní archiv. Prostě bez e-mailu se většina z nás již neobejde.

1 E-mail v ohrožení

Přesto je ale tento efektivní nástroj a každodenní nepostradatelný pomocník stovek miliónů lidí na celém světě v permanentním ohrožení. Tím, kdo na něj se stále zvyšující se intenzitou útočí, a hrozí až jeho totálním ochromením, je SPAM – nevyžádaná pošta. Podle některých odhadů tvoří spam dnes až 90 % veškeré e-mailové komunikace! Devět z deseti e-mailových zpráv nepřináší svým příjemcům žádnou užitečnou či očekávanou informaci. Zaplavuje je naopak spoustou obtěžujících nabídek, připravuje je o čas, peníze a energii. Většina z nás dostává stovky, ti komunikačně čilejší až tisíce, spamů denně! Naštěstí je většina z nich vyřazena antispamovými filtry, takže mezi skutečně doručenou poštu pronikne jen malá část, ale i ta dokáže pěkně komplikovat život. Někdy nám naopak důležitá zpráva nepřijde vůbec, protože ji antispamové filtry chybně vyhodnotily jako spam, a zpráva tak skončila v záplavě tisíců nevyžádaných zpráv na spamových skládkách.

Spam nekomplikuje život jen koncovým uživatelům. Stal se noční můrou počítačových správců a lidí zodpovědných za fungování komunikační infrastruktury organizace. Na centrální poštovní server Masarykovy univerzity přicházelo počátkem roku 2007 téměř milión e-mailových zpráv denně – a tento počet se stále rychle zvyšuje[1]. V průměru deset e-mailů za sekundu, nepřetržitě ve dne i v noci, v pracovní dny i o víkendu, musí být tímto serverem přijato, vyhodnoceno, zkontrolováno ohledně přítomnosti virů, otestováno v rámci ochrany proti spamům, a poté

[1] Po zavedení greylistingu v březnu 2007 stoupl denní počet zpráv již na 1,7 miliónu.

přeposláno na příslušná místa, buď dovnitř univerzity (na fakultní poštovní servery) nebo ven z MU. Pokud by server zkolaboval nebo přestal neustávající příval pošty zvládat, pocítí to okamžitě každý z nás. Proto je nezbytné infrastrukturu univerzitních poštovních serverů průběžně výkonnostně posilovat a vybavovat stále sofistikovanějšími ochrannými nástroji. To stojí peníze a zvyšuje nároky na kapacity specializovaných odborníků.

Mezi spammery a strážci užitečného fungování elektronické pošty zuří permanentní tichá válka. Na každý tah jedné strany reaguje okamžitě protitah druhé strany. Každé opatření proti spamům vede dříve či později k protiopatřením spammerů, která se snaží účinnost zavedených antispamových opatření eliminovat – buď novými technikami maskování spamů nebo razantním zvýšením jejich počtu. Přestože nová antispamová opatření zvýší procento zachycených spamů, vyšší počet útočících spamů znamená i vyšší počet spamů, které tato opatření překonají.

2 Nárůst počtu spamů

Řada uživatelů zřejmě zaznamenala v roce 2006 dramatický nárůst počtu spamů. Čím je tento nárůst způsoben? Zatímco v dřívějších letech byly hlavním zdrojem spamů buď poštovní servery spammerských organizací nebo zneužité nezabezpečené poštovní servery běžných organizací, v současnosti používají spammeři i nové, účinnější postupy. Využívají nedostatečně zabezpečené počítače koncových uživatelů, které infikují a vytváří z nich stroje k rozesílání vlastní pošty. Existují dokonce specializované skupiny hackerů, které nedostatečně zabezpečené osobní počítače cíleně vyhledávají, přeměňují na *zombie* (stroje pod svou vlastní kontrolou) a zapojují je do velmi rozsáhlých sítí *botnets* – některé z nich mají až stovky tisíc strojů. Ty pak prodávají spammerům. Aniž by to daný uživatel tušil, počítač, na kterém doma pracuje, rozesílá současně spamy do celého světa. Spolu se zvyšujícím se počtem domácností vybavených počítači a stále se zlepšujícími parametry jejich připojení na síť (vysokorychlostní Internet) tak roste i potenciál pro zvyšování počtu rozeslaných spamů.

Podle [3] je až 7 % počítačů na Internetu infikováno a hackeři jsou schopni celosvětově získat a přetvořit na zombie více jak 100 000 osobních počítačů týdně. Obrovské a výkonné sítě botnets pak pracují pro spammery téměř bezplatně (na náklady nevědomých majitelů PC) a chrlí do Internetu miliardy spamů denně. I kdyby byla jejich výtěžnost mizivá – řekněme jedna ku miliónu (jen na každý miliontý spam by některý z oslovených „zákazníků“ zareagoval a nabízené zboží/službu si koupil), znamená to pro spammery dostatečný příjem na to, aby se jim jejich „podnikání“ vyplácelo.

3 Vícestupňová ochrana

Jak jsme uvedli již v úvodu, bez soustavných spamových protiopatření by e-mail již dávno přestal být použitelnou službou. Problém je v tom, že žádné protiopatření nevydrží dlouho, není definitivní. Neustále je třeba přicházet s novými technologiemi. Protože žádná z nich nemůže být sama o sobě stoprocentně úspěšná, je třeba tyto technologie kombinovat a vytvářet vícestupňové ochrany.

Problém je i v samotném vymezení spamu; v řadě případů je objektivní identifikace spamu nemožná či nejednoznačná. Ten samý e-mail, který jeden uživatel považuje za obtěžující, může pro jiného uživatele představovat důležitou informaci. Proto musí být antispamové filtry na vyšších stupních ochrany (celouniverzitní, fakultní) nastaveny rozumně konzervativně, aby nenadělaly víc škody než užitku. A proto je také žádoucí doplnit tyto vyšší stupně ochrany osobními filtry přizpůsobenými konkrétním koncovým uživatelům – jejich osobním preferencím a charakteru jejich elektronické pošty. Teprve pak může být antispamová ochrana skutečně účinná.

4 Prevence

Nejefektivnější způsob, jak se vyhnout spamům, je neumožnit spammerům získat vaši e-mailovou adresu. To znamená zacházet s ní jako s citlivým údajem, který není radno sdělovat kdekomu na potkání. Tím je myšleno vyhnout se jak aktivnímu tak pasivnímu zveřejňování e-mailové adresy v prostředí Internetu. Pod aktivním zveřejňováním rozumíme uvádění e-mailové adresy

v různých on-line formulářích, u nichž si nemůžete být jisti seriózností přijímající strany, v otevřených diskusních fórech a v inzerátech, nebo odpovídání na spamy. Stejně tak nebezpečné je ale i pasivní zveřejnění nechráněné e-mailové adresy na webových stránkách. Vyhledávání a sklízení e-mailových adres pomocí automatizovaných sběračů (spambots) z volně přístupných webových stránek a z diskusních fór je jeden z nejčastějších způsobů, jak spammeři přijdou na vaši adresu[2]. Podle výzkumů [4] potřebují dnes spammerské vyhledávače v průměru 19 dnů k tomu, aby odhalily e-mailovou adresu nově zveřejněnou na webu (nejkratší reakce byla do 1 sekundy po vystavení adresy).

5 Způsoby boje proti spamu

V současnosti existuje a průběžně se rozvíjí řada přístupů k boji proti spamu. Z principiálních důvodů (hranice mezi spamem a chtěnou poštou jsou individuální a nelze je jasně definovat, technologie pro rozesílání a maskování spamů se průběžně zdokonalují) nemůže být žádný z nich sám o sobě zcela účinný. Dokáží však poměrně spolehlivě zachytit převážnou část spamu. Při kombinaci různých přístupů a jemném vyladění zohledňujícím jednotlivé uživatele se může dobrá antispamová ochrana blížit až ke stoprocentní účinnosti. Důležité je však nejen co nejvyšší procento zachycených spamů; ještě možná důležitějším kritériem z pohledu koncového uživatele je co nejnižší (nejlépe nulový) počet případů, kdy je jako spam vyhodnocena a nedoručena regulérní zpráva.

Hlavní směry v boji proti spamu jsou následující:

- filtrování podle obsahu zprávy;
- filtrování podle odesílatele;
- ekonomické přístupy;
- legislativní přístupy.

Uvedené směry se v praxi vzájemně kombinují a doplňují.

[2] Z těchto důvodů jsou všechny e-mailové adresy na veřejném webu `http://www.muni.cz` maskovány, tj. zabezpečeny proti rozpoznání a sklízení automatizovanými roboty.

5.1 Filtrování podle obsahu

Podstatou tohoto přístupu je analýza obsahu těla zprávy, její hlavičky či obou těchto částí. Při analýze jsou vyhledávány určité známé charakteristiky spamů – v těch nejjednodušších přístupech jsou to výskyty podezřelých slov či znaků, v propracovanějších přístupech jsou hledány obecnější charakteristiky v širším kontextu, založené na statistikách a umělé inteligenci. Pokročilejší nástroje, jako je například spamassasin, nespoléhají pouze na jeden algoritmus či sadu pravidel. Aby se zpráva vyhodnotila jako spam, musí se současně sejít více podnětů, z nichž každý může mít nastavenu jinou váhu. Takovouto ochranu spammeři hůře překonávají a současně se snižuje riziko chybné identifikace dobré zprávy za spam.

Pro vlastní analýzu obsahu jsou používány různé technologie: jednoduchá filtrační pravidla, klasifikace využívající strojového učení, systémy založené na kompresních technikách, vyhledávání podobností v textu či obrazu.

Jako protizbraň proti filtrování obsahu používají dnes spammeři často obrazová sdělení, jejichž analýza je obtížnější a méně propracovaná než v případě textů. Vlastní tělo zprávy pak obsahuje žádný nebo jen neutrální text pro zmatení filtrů. Samotná informace je převedena do obrazové podoby a uložena v příloze e-mailu.

5.2 Filtrování podle odesílatele

U těchto způsobů filtrace nejde o to, co zpráva obsahuje, ale kdo ji poslal. Tradiční přístupy využívají seznamy špatných adres – blacklists – z nichž je příjem pošty zablokován, a oproti tomu seznamy důvěryhodných adres – whitelists – z nichž je naopak zpráva přijata vždy, bez ohledu na její obsah. Blacklisty mají tři zásadní slabiny: (a) adresu odesílajícího stroje lze zfalšovat; (b) s tím, jak se rozesílání spamů přesunulo z pevných serverů na zneužité koncové stanice zombie, není pro spammery problém rozesílající stroje rychle měnit; (c) jestliže se hackerům podaří zneužít některý počítač či adresu uvnitř důvěryhodné organizace, může se celá tato organizace dostat na blacklist a následně do velkých potíží, protože nevinné e-maily od jejích uživatelů mohou někteří příjemci odmítat (do

této situace se čas od času dostává i MU). Proto je dobré používat blacklisty s rozumem – pouze jako pomocné doplňkové kritérium, nikoliv jako kritérium jediné a rozhodující. Řada poštovních správců využívání blacklistů odmítá zcela.

Mezi novější technologie filtrování podle odesílatele patří *greylisting* (viz článek Mirka Rudy v tomto čísle Zpravodaje). Vychází z toho, že zombie pro rozesílání spamů se nechovají jako standardní poštovní servery – rychle rozešlou kvantum zpráv a tím to pro ně končí, mizí aby nebyly odhaleny. Naproti tomu standardní poštovní servery jsou konstruovány tak, aby zajistily spolehlivé fungování pošty i při běžných provozních potížích, kdy se často nemusí podařit doručit příjemci zprávu hned napoprvé (například proto, že příjemcův poštovní server je dočasně mimo provoz). Při greylistingu jsou příchozí zprávy přijímajícím poštovním serverem nejprve vždy odmítnuty, a teprve ty zprávy, které po stanovené době přijdou znovu, jsou skutečně doručeny adresátům. Na rozdíl od blacklistů nemá greylisting žádný fixní seznam „špatných hochů“ – všechny považuje za rovnocenné a rozhoduje se až podle jejich konkrétního chování, nikoliv podle jejich adresy.

Jiný přístup využívají systémy založené na *spolehlivém prokázání identity odesílatele*. Využívají často kryptografické techniky, jejichž cílem je prokázat příjemci, že odesílatel zprávy je skutečně ten, za kterého se vydává. Přijímány jsou například pouze zprávy s ověřeným digitálním podpisem nebo jiným důvěryhodným znakem od odesílatele, počítače nebo domény. Problémem je zatím nižší míra standardizace a penetrace potřebných technologií i globální bezpečnostní infrastruktury. Uvedený přístup však má vysokou potenciální účinnost; na rozdíl od jiných přístupů necílí na odstraňování následků, ale přímo na léčení základní příčiny spamu, kterou je nedostatečně zabezpečená infrastruktura elektronické pošty a Internetu obecně.

Další z přístupů spadají do kategorie tzv. *systémy úkol/odpověď* (challenge/response). Základní idea spočívá v tom, že pokud důvěryhodnost odesílatele není příjemci známa, zašle poštovní server příjemce odesílateli určitý úkol (challenge) a teprve po jeho úspěšném vyřešení je e-mail příjemci skutečně doručen. Úkol je navržen tak, aby byl snadno splnitelný člověkem, nikoliv však počítačem (čtenář se již asi setkal s takovými úkoly v podobě obrázků obsahujících slovo zapsané různě zpotvořenými písmeny). Tímto způsobem se příjemce může bránit proti zprávám rozesílaným softwarovými roboty.

5.3 Ekonomické přístupy

Tyto přístupy se snaží změnit ekonomickou základnu samotné existence spamu. Tou je fakt, že spammera dnes rozesílání i obrovského množství e-mailů téměř nic nestojí (na rozdíl třeba od klasických papírových letáků, jejichž netriviální cenu musí zaplatit inzerent – a navíc je tato cena vždy přímo úměrná množství letáků). Čili cílem je zavést taková opatření a technologie, aby se masové rozesílání spamů ekonomicky nevyplácelo. Jednou z možností je zavedení malých poplatků za odeslanou poštu (s případnou refundací prokazatelně seriózním zákazníkům). Tento model může být atraktivní zejména pro velké poskytovatele služeb elektronické pošty, naráží ale na různé politické a společenské bariery, a neřeší také problém spamů ze zneužitých počítačů.

Určitou ekonomickou zpětnou vazbu je možné zavést i jiným způsobem než přímými finančními platbami. Jednou z možností je modifikace systémů typu úkol/odpověď (viz výše), kdy přijímající poštovní server zvyšuje odesílajícímu serveru cenu za rozesílání pošty tím, že příjem zprávy podmiňuje vyřešením výpočetně náročného úkolu u odesílajícího serveru. Při malém počtu posílaných e-mailů tato dodatečná zátěž nevadí, při hromadném rozesílání pošty však již ano.

5.4 Legislativní přístupy

Řada vyspělých zemí světa přijala v posledních letech zákony, které hromadné rozesílání nevyžádaných zpráv omezují a ty nejhorší spammerské praktiky přímo zakazují. Antispamová legislativa existuje i u nás, ale například také v USA (CAN-SPAM Act 2003), odkud dnes pochází celosvětově nejvíce spamu. Již to samo o sobě demonstruje, nakolik jsou legislativní opatření

v praxi skutečně účinná. Anti-spamové zákonodárství je určitě velmi potřebné a důležité, protože vymezuje právní rámec, umožňuje slušným firmám používat Internet pro reklamní účely v rámci daných pravidel a naopak trestně stíhat spammery. Je však zřejmé, že problém spamu nevyřeší, a že hlavní tíha boje proti spamu leží v oblasti technologií.

Literatura

[1] J.Goodman, G.V.Cormack, D.Heckerman. *Spam and the Ongoing Battle for the Inbox*. Communication of the ACM, Vol. 50, No. 2, February 2007. Pro uživatele MU dostupné elektronicky na `http://doi.acm.org/10.1145/1216016.1216017`

[2] B.Leiba, N.Borenstein. *A Multifaceted Approach to Spam Reduction*. Proceedings of the Conference on Email and Anti-Spam, 2004. Dostupné elektronicky na `http://www.ceas.cc/papers-2004/127.pdf`

[3] M.Furst. *Botnets. No. 1 emerging Internet threat.* CNN, January 31, 2006. `http://www.cnn.com/2006/TECH/internet/01/31/furst/`

[4] Project Honey Pot. `http://www.projecthoneypot.org` □

E-mail a centrální poštovní server Masarykovy univerzity

Miroslav Ruda, ÚVT MU

Prudký nárůst objemu elektronické pošty, zapříčiněný bohužel zejména vzrůstem podílu spamu, si vyžádal v poslední době změny konfigurace centrálního poštovního serveru MU (serveru `relay.muni.cz`). Cílem tohoto článku je popsat současnou konfiguraci poštovního serveru a poskytované služby, se zaměřením na novou službu – greylisting [1].

Poštovní server relay.muni.cz je centrální bod e-mailové komunikace Masarykovy univerzity se světem. Přes tento server prochází každý e-mail ze světa na adresy MU, každý e-mail posílaný ze strojů MU do světa, ale i každý e-mail putující mezi jednotlivými fakultami MU.

Pro doručování pošty je použit program sendmail[1]. Vedle bohaté možnosti konfigurace samotného serveru umožňuje tento program i implementaci dalších kontrol pomocí samostatně stojících služeb, které s centrálním poštovním programem komunikují přes standardizované rozhraní API milter[2]. I většina našich kontrol e-mailových zpráv je implementována jako milter služby. Některé z nich jsou převzaty ze světa, jiné jsou vyvinuty přímo na ÚVT MU. Je potřeba si uvědomit, že již před nasazením greylistingu zpracovával tento server přibližně milión (!) e-mailů denně, a že kontroly musí být proto pečlivě navrženy tak, aby je bylo možné provádět v reálném čase a na hardware, který je k dispozici[3].

Kontroly na našem poštovním serveru můžeme rozdělit do kategorií antivirová kontrola, antispamová kontrola a další kontroly validity e-mailu, a budou postupně popsány v dalších kapitolách. Na konci článku pak popíšeme, jak lze použít server relay.muni.cz pro odesílání pošty i na cestách, z míst mimo MU.

1 Antivirová kontrola

Centrální server provádí antivirovou kontrolu pro veškerou poštu přicházející do domény `muni.cz`, a pro všechnu poštu odcházející z jednotlivých fakult do světa nebo na jiné fakulty MU. Pro kontrolu je použit antivirus firmy Kaspersky Lab[4], komunikace se samostatně stojícím antivirovým programem je zajištěna vlastním milter klientem.

Vedle samotné antivirové kontroly jsou všechny e-maily kontrolovány dalším filtrem, který odmítá veškeré e-maily s přílohami, které jsou potenciálně nebezpečné pro klienty na operačním systému MS Windows (spustitelné `.exe` soubory, přílohy typu `.vbs` apod.). Pro testy je použit program vbsfilter[5]. Seznam odmítaných příloh je dostupný na webu ÚVT MU[6].

[1] www.sendmail.org

[2] www.milter.org

[3] V současnosti je to 2xdual core Xeon, s 8GB RAM a operačním systémem Linux

[4] `http://www.kaspersky.com`

[5] `http://aeschi.ch.eu.org/milter/vbsfilter.c`

[6] `http://www.ics.muni.cz/techinfo/abuse.html`

2 Antispamová kontrola

Na centrálním serveru není vhodné kontrolovat každý e-mail antispamovými filtry typu Spamassasin. Důvodem jsou jednak vysoké nároky na hardwarové vybavení, které je vhodné rozprostřít mezi více podřízených serverů, a hlavně nemožnost konfigurace specifické pro každého uživatele – vlastnost u heuristického rozpoznáváni spamů velice žádaná. Je nutné si uvědomit, že na univerzitě je skladba uživatelů velice pestrá, a že u mnoha jednoduchých antispamových testů často používaných v komerčních firmách lze najít v našem prostředí protipříklad (lékaři opravdu mohou diskutovat o VIAGŘE, na katedry jazyků mohou chodit e-maily v ruštině nebo čínštině, IT oddělení může uvítat nevyžádaný e-mail o slevách serverů firmy XXX, nelze přijímat e-maily jen z domény `.cz` apod.).

Antispamová kontrola je proto rozdělena na několik fází. Na centrálním serveru je odfiltrována pošta, která je spamem prokazatelně, a heuristické analýzy typu program Spamassasin jsou ponechány až na poštovní servery jednotlivých fakult, kde si už uživatelé mohou nastavení ovlivňovat. Na centrálním serveru proto provozujeme dva filtry: dopřednou kontrolu existence adresy příjemce a nově, od 1.března 2007, i greylisting.

2.1 Dopředná kontrola

Dopředná kontrola, poskytovaná programem milter-ahead[7] funguje tak, že adresa příjemce je překontrolována na podřízených poštovních serverech již v průběhu přijímání pošty ze světa, ještě před přijmutím těla e-mailu. Pokud je adresa neplatná, je e-mail okamžitě odmítnut. Tím je zaručeno i to, že centrální server nepřijme e-mail s podvrženou adresou odesílatele a po zjištění, že adresa příjemce je neplatná, neposílá e-mail neplatnému odesílateli, a tím se sám nepodílí na rozesílání spamu.

2.2 Greylisting

Druhá antispamová kontrola, greylisting, vychází z předpokladu, že spammer rozesílá poštu v takovém množství, že je pro něho obtížné přeposlat znovu e-mail, který je poprvé dočasně odmítnut.

Centrální poštovní server MU proto při prvním pokusu o doručení pošty odpoví druhé straně dočasnou chybou, s odpovědí „pošta nemůže být přijata, zkuste to znovu za 25 minut". Dočasné odmítnutí pošty je při e-mailové komunikaci na Internetu standardní věc, používá se např. při přeplněném disku, přetíženém serveru apod.

Při dočasném odmítnutí pošty si poštovní server MU uloží do své greylistové databáze trojici údajů: „adresa odesílatele, adresa příjemce, IP vzdáleného stroje". Pokud do pěti dnů dorazí e-mail se stejnou trojicí (zpravidla ten samý e-mail při druhém pokusu o doručení), je už přijat a trojice je na 180 hodin (o trošku víc než týden) uložena do *whitelistové* databáze. Pokud se vzdálený server pokusí o druhé doručení dříve než po 25 minutách, je opět odmítnut, opět dočasně, jen je mu prozrazeno, kolik minut ještě musí čekat.

Pokud již je trojice údajů ve whitelistové databázi a přijde další e-mail se stejnou trojicí, poštovní server MU takový e-mail propustí okamžitě a opět prodlouží platnost položky ve whitelistové databázi.

Zpoždění při e-mailové komunikaci tak nastane jen při prvním výskytu trojice „příjemce, odesílatel, server", tj. při prvním e-mailu z neznámé adresy. Pokud pak z této adresy chodí alespoň jeden e-mail týdně, zpoždění už by nemělo nastat. Výsledné počáteční zpoždění je zpravidla kratší než hodina (záleží na poštovním serveru druhé strany, jak brzy po uplynutí 25minutového nepřijímacího intervalu MU přepošle dočasně odmítnutý e-mail znovu).

Greylisting se nevztahuje na stroje z domény muni.cz, neaplikuje se na spojení, při kterém se uživatel nejdříve prokázal heslem nebo certifikátem (viz. 4) a neaplikuje se na domény vyjmenované v permanentní whitelistové databázi (viz níže).

Problémy mohou nastat u nestandardních poštovních serverů, které reagují špatně na dočasnou chybu. Použití metody greylistingu je však

[7] `http://www.milter.info/sendmail/milter-ahead/`

ve světě poměrně rozšířené, a proto by podobně problémy měly být vzácné. Další kategorie problémů může nastat u domén, které odesílají e-maily přes farmu několika strojů (např. `gmail.com`): pokud se odmítnutý e-mail pokusí podruhé doručit jiný stroj, s jinou IP než ten původní, je opět zařazen do greylistové databáze. Podobné problémy je nutné nahlásit správcům na ÚVT a můžeme je buď řešit nebo je možné přidat stroj/celou doménu na trvalý whitelistový seznam. Velké domény, které jsou tímto problémem známé, jsou již vyjmenovány v greylistovém programu, který používáme.

Aby se zpomalení komunikace s většími servery ještě více předešlo, testujeme i variantu, kde je automatický whitelisting platný pro všechny e-maily pocházející ze stejného stroje. Idea je taková, že pokud server zopakoval jeden e-mail po 25 minutách, dá se předpokládat, že se stejně zachová i k další poště. Při takové konfiguraci pak stačí jediný e-mail z domény `seznam.cz`, a všechny další e-maily z poštovního serveru domény `seznam.cz` jsou již přijímány bez zpoždění.

Pro implementaci byl použit program `milter-greylist`[8]. V současné době je greylisting aplikován na veškerou poštu do domén `muni.cz` a `linux.cz`.

S nasazením greylistingu bylo také nutné vyřešit problém záložního poštovního serveru. Tuto službu nám dosud poskytoval server `rs.cesnet.cz` na CESNETu. S nasazením greylistingu by ale bylo nutné implementovat stejný greylisting i na tomto serveru a v ideálním případě i synchronizovat greylistovou databázi mezi těmito stroji. To se ukázalo jako neschůdné, a proto byl záložní server zrušen. V současné době provádíme finální testy synchronizace greylistové databáze mezi dvěma servery na ÚVT MU (což při milionech záznamů v databázi a řádově deseti změnami za vteřinu je samo o sobě zajímavý problém) a v nejbližší době začneme provozovat oba servery v plně zástupném režimu.

2.3 Černé listiny

Jednou z metod používaných ve světě je metoda „černých listin" (blacklists) – veřejně dostupných služeb, kde jsou vyjmenovány IP adresy serverů, přes které byl spam rozesílán. Vzhledem k nespolehlivosti těchto služeb (i vzhledem k tomu, jak často se na podobných serverech objevují adresy našich serverů nebo serverů největších českých e-mailových poskytovatelů) centrální server nekontroluje IP adresu odesílatele proti černým listinám typu `spamcop.net`. IP adresa stroje komunikujícího s naším poštovním serverem je uložena do hlavičky `X-Muni-Spam-TestIP` a podřízené fakultní servery si mohou takový test provést později. Navíc programy typu Spamassasin už takový test nabízí pro všechny servery, přes které daný e-mail prošel.

3 Další testy validity e-mailu

Centrální server detekuje i několik dalších „podezřelých" typů e-mailu a odmítá jejich přijetí. Vedle standardních testů (typu test na platnost domény z adresy odesílatele) používáme vlastní filtr, který detekuje zacyklení při přeposílání pošty (ať už mezi doménami MU, na veřejné poštovní servery nebo na SMS servery), příliš vnořené MIME maily používané občas i na zmatení antivirových či antispamových programů a k dispozici je i filtr milter-regex[9], který umožňuje specifikovat libovolný regulární výraz, jehož výskyt je pak testován ve hlavičkách i celém těle každého e-mailu.

4 Autentizace při odesílání pošty

Poštovní server `relay.muni.cz` přijímá poštu pro příjemce v doméně `muni.cz` a `linux.cz` od libovolného stroje. Pro odesílání pošty poskytuje tuto službu všem strojům jen z IP rozsahu 147.251.0.0/16 (doméně `muni.cz`). Aby mohl být server použit také pro rozesílání pošty i uživateli na cestách nebo z domácího připojení, umožňuje server autentizaci odesílatele. V takovém případě přijímá server libovolnou poštu i od strojů mimo doménu muni.cz a např. také obchází greylisting.

[8] http://hcpnet.free.fr/milter-greylist/

[9] `http://www.benzedrine.cx/milter-regex.html`

Poštovnímu serveru je možné se prokázat heslem do kerberovských realmů IS.MUNI.CZ (sekundární heslo ISu, tedy heslo poštovní schránky na mail.muni.cz), ICS.MUNI.CZ a META. V takovém případě je nutné nakonfigurovat poštovního klienta tak, aby si vynutil TLS (šifrované spojení) a jako login pak použít např. `učo@is.muni.cz`.

Druhou možností je autentizace uživatelským nebo serverovým certifikátem – v současné době podporujeme pouze certifikační autoritu CESNETu[10], ale nebráníme se podpoře i dalších certifikačních autorit.

5 Závěrem pár čísel

Závěrem pár čísel o provozu a účinnosti jednotlivých filtrů (podrobnější informace viz článek Radima Peši v tomto čísle Zpravodaje).

Před nasazením greylistingu se centrální server MU zabýval denně přibližně miliónem e-mailů (směrem do MU i ven z MU, včetně hostovaných domén typu linux.cz, včetně opakovaných pokusů o doručení apod.). Z tohoto počtu bylo asi 250.000 e-mailů odmítnuto dopřednou kontrolou, přes 270.000 e-mailů překontrolováno antivirem (v té době největším konzumentem výpočetního výkonu) a přibližně 265.000 e-mailů bylo zasláno podřízeným fakultním serverům.

Několik dní po nasazení greylistingu bylo z více než miliónu e-mailů propuštěno přibližně 40.000 e-mailů a dalších 40.000 nebylo greylistingem kontrolováno (pocházelo z domény muni.cz, přišlo ze serveru rs.cesnet.cz – v té době ještě záložního apod.). Přibližně 60.000 e-mailů bylo překontrolováno antivirem a přibližně 45.000 e-mailů bylo zasláno podřízeným fakultním serverům. V greylistové databázi bylo přibližně sedm a půl miliónu záznamů, z nich jen 5 procent prošlo do whitelistové databáze.

V současné době již nepoužíváme záložní server rs.cesnet.cz, testujeme uvolněnější whitelisting a byl dále optimalizován provoz některých filtrů. Počet e-mailů, kterými se server denně zabývá, narostl na 1,7 miliónu, na podřízené servery na fakultách prošlo přibližně 70.000 e-mailů a antivirus překontroloval přibližně 80.000 e-mailů. Počet odhalených virů nadále kolísá mezi 2.000 a 4.000 denně, počet odmítnutých příloh se pohybuje mezi 1000 a 2000 denně, počet e-mailů odmítnutých dopřednou kontrolou zůstává nad 200.000. Greylistová databáze obsahuje více než 8 miliónů záznamů, poměr e-mailů, které přes greylisting projdou, zůstává okolo 5 procent.

V době psaní článku zůstává otevřenou otázkou výhodnost uvolnění whitelistingu. Dalšími experimenty bude potřeba ověřit, jak velké množství spamu projde díky této metodě, a zda by nebylo výhodnější použít klasickou metodu a staticky vyjmenovat domény, kterým důvěřujeme.

[10] `http://www.cesnet.cz/pki/cs/ch-intro.html`

Literatura

[1] Satrapa P.: *Greylisting: nová metoda boje proti spamu*. Server Lupa, 23. 4. 2004. ISSN 1213-0702, `http://www.lupa.cz/clanky/greylisting-nova-metoda-boje-proti-spamu/` □

E-mail, spam a greylisting MU

Radim Peša, ÚVT MU

Objem elektronické pošty přepravované poštovními servery MU neustále narůstá. Výraznou část poštovního provozu přitom představuje spam – nevyžádané obtěžující e-maily. Rozsah spamu již dosáhl stupně, který pro řadu uživatelů znamená výraznou degradaci elektronické pošty jako nástroje efektivní komunikace. Na druhé straně představuje spam stále větší zátěž i pro poštovní infrastrukturu MU (centrální poštovní server MU a na něj navazující poštovní servery fakult a dalších součástí univerzity). V tomto článku uvedeme číselné údaje ilustrující objem elektronické pošty na MU a dopad nových opatření na omezení množství spamu – zavedení greylistingu na centrálním poštovním serveru MU.

1 Objem elektronické pošty na MU

Před zavedením celouniverzitního antispamového opatření ve formě greylistingu počátkem března 2007 [1] zpracovával centrální poštovní server MU téměř milión elektronických zpráv denně. Po zavedení greylistingu tento počet ještě

Denní počet zpráv	5.–11.2.	5.–11.3.
Doručené zprávy	387 833	74 105
Nedoručené (AV ochrana)	11 995	2 853
Nedoručené (neexistující uživatel)	216 966	188 440
Nedoručené (ostatní chyby)	272 971	102 642
Nedoručené (greylisting)	—	1 340 654

Tabulka 1: Objem pošty MU před a po greylistingu

stoupl, protože část dočasně odmítnutých zpráv přichází na MU opakovaně.

Celkový objem elektronické pošty na MU lze charakterizovat tabulkou 1. Ukazuje průměrné denní počty zpracovávaných (tj. doručených i nedoručených) zpráv na centrálním poštovním serveru MU, a to ve dvou různých týdnech. Týden 5.-11.2.2007 charakterizuje období před zavedením greylistingu MU a týden 5.- 11.3.2007 období těsně po zavedení greylistingu.

Řádek „doručené zprávy“ udává celkových počet e-mailů, které centrální poštovní server MU uspěšně odeslal kterýmkoli směrem – dovnitř MU nebo ven z MU. Nedoručené (AV ochrana) jsou zprávy přicházející do univerzity, které nejsou doručeny, protože obsahují počítačový vir nebo spustitelnou přílohu, které se do MU nedoručují [2]. Nedoručené (neexistují uživatel) jsou zprávy, které byly adresovány na neexistující uživatele – například spamy generované slovníkovou metodou. Nedoručené (ostatní chyby) jsou všechny ostatní zprávy, které nebylo možné z jiných důvodů doručit. Nedoručené (greylisting) se vyskytují až po zavedení greylistingu a zahrnují pokusy o předání zprávy, které byly odmítnuté metodou greylistingu (viz popis greylistingu ve [1]).

2 Situace kolem spamu na fakultách

V průběhu měsíce února byl proveden mezi laboratořemi výpočetní techniky (LVT) jednotlivých fakult dotazníkový průzkum zaměřený na problematiku spamu a její závažnost v rámci fakult MU.

Ze šetření vyplynulo, že všude je prováděna filtrace spamu na úrovni fakultních poštovních serverů – nejčastěji s využitím antispamového nástroje Spamassasin (na dvou fakultách i v kombinaci s dalšími filtry jako je dSpam). Individuálně v některých případech je navíc využívána antispamová kontrola v klientských poštovních programech uživatelů. Podpora koncovým uživatelům při nastavování a ladění jejich osobních filtrů je poskytována obvykle jen na vyžádání.

Nastavení antispamových nástrojů se na jednotlivých fakultách výrazně liší v závislosti na zvyklostech správců a uživatelů. Rovněž se liší hodnocení závažnosti problematiky spamu a obecné úspěšnosti jejího řešení na jednotlivých fakultách či pracovištích. LVT hodnotily situaci na svých fakultách v rozmezí od relativně dobrá až po velmi vážná; přičemž situaci jako vážnou až velmi vážnou hodnotili zástupci 5 fakult.

Přestože účinnost samotných fakultních antispamových filtrů je ze strany správců hodnocena vesměs jako velmi dobrá, vnímá většina LVT spam jako závažný problem a boj se spamem pro ně představuje značnou zátěž. Navíc ani vysoká účinnost fakultních filtrů nemusí nutně znamenat dostatečnou antispamovou ochranu na individuální úrovni u všech uživatelů. V závislosti na charakteru pošty, způsobu jejího využívání a dalších okolnostech může být situace u jednotlivých uživatelů značně rozdílná.

3 Greylisting MU a jeho přínosy

Od 1. března 2007 bylo na centrálním poštovním serveru MU nasazeno celouniverzitní antispamové opatření v podobě tzv. greylistingu [1]. Cílem tohoto opatření bylo snížit celkovou zátěž přinášenou spamy na univerzitní poštovní infrastrukturu (nároky na výpočetní a paměťové kapacity fakultních a dalších poštovních serverů) a současně i snížit počet spamů u koncových uživatelů.

Centrální poštovní server MU relay.muni.cz tak v současnosti provádí již dva typy filtrování elektronické pošty:

- *antivirová ochrana* – filtrují se zprávy obsahující počítačové viry a přílohy vybraných typů, jejichž přijímání na MU je z důvodů antivirové ochrany zakázáno [2];
- *antispamová ochrana* – filtrují se zprávy které nejsou doručovány podle standardních pravidel pro rozesílání elektronické pošty.

Podívejme se, jak se aplikace greylistingu na centrálním poštovním serveru MU projevila na množství e-mailových zpráv doručovaných na jednotlivé fakultní servery. V tabulce 2 jsou uvedeny denní průměry počtu doručovaných zpráv na jednotlivé fakulty v týdnu 5.2.-11.2.2007 (před zavedením greylistingu) a v týdnu 5.3.-11.3.2007 (po zavedení greylistingu).

Uvedená tabulka vypovídá o poklesu celkového množství doručované pošty o 80 % až 90 %. Můžeme předpokládat, že tento rozdíl je – až na výjimky – tvořen nedoručováním elektronických zpráv obsahujících spam.

Další zajímavý údaj – kolik spamu je i po zavedení greylistingu na fakultní stroje doručováno – není už tak snadné zjistit. Jisté vodítko může ale poskytnout záznam z antispamového nástroje Spamassasin na serveru dior.ics.muni.cz pro poštu ÚVT MU. Na základě především analýzy obsahu označuje Spamassassin přijímanou poštu jako spam nebo normální poštu. V následující tabulce jsou vidět denní statistiky ze Spamassissinu ÚVT MU ze stejných týdnů jako v předchozí tabulce (před zavedením greylistingu a po něm).

a) ÚVT MU – stav před zavedením greylistingu:

Den	Spam	Normální	Podíl spamu
PO 5.2	8834	3474	72 %
ÚT 6.2	8188	3588	70 %
ST 7.2	8584	4024	68 %
ČT 8.2	8966	3650	71 %
PÁ 9.2	8376	3174	73 %
SO 10.2	7895	2124	79 %
NE 11.2	7769	2014	79 %

b) ÚVT MU – stav po zavedení greylistingu:

Den	Spam	Normální	Podíl spamu
PO 5.3	539	2102	20 %
ÚT 6.3	606	1807	25 %
ST 7.3	630	1921	25 %
ČT 8.3	579	2055	22 %
PÁ 9.3	671	1635	29 %
SO 10.3	519	713	42 %
NE 11.3	521	741	41 %

Před nasazením greylistingu byly přibližně tři čtvrtiny kontrolované pošty rozpoznány Spamassassinem jako spam. Po zavedení greylistingu se tento podíl snížil na jednu čtvrtinu v pracovní dny (o víkendu se poměr vzhledem k nižšímu počtu normální pošty mění). Zavedením greylistingu rovněž poklesl počet zpráv označených jako normální pošta. Pravděpodobně se jedná o spam, který nástroj Spamassasin nerozpoznával, což je potřeba při interpretaci uvedených čísel brát v úvahu.

Uvedené údaje vypovídají o dvou vybraných týdnech a mapují skokový rozdíl způsobený zavedením greylistingu. Na jejich základě se greylisting jeví jako velmi účinná součást protispamových opatření. Pro přesnější vyhodnocení účinnosti bude třeba sledovat vývoj v rámci delšího časového období.

Dva týdny po nasazení greylistingu na centrálním poštovním serveru MU byl u fakultních LVT dotazníkovou formou ověřen výsledek opatření. Podle přijatých odpovědí byl na jednotlivých fakultách zaznamenán úbytek přijímaného spamu o 80 % až 90 %. Současně na nebyly na většině fakult zaznamenány zásadní stížnosti ze strany uživatelů na změny v chování poštovního systému (zpoždění v doručování zpráv z neznámých adres nebo nedoručení očekávané zprávy). V jednom odůvodněném případě byly vybrané e-mailové adresy vyňaty z režimu greylistování; šlo o adresy používané pro potřeby trvalých rychlých odpovědí v rámci speciálního výzkumu.

4 Závěr

Dá se předpokládat, že s tím, jak bude větší část spammerů nacházet účinné protizbraně, bude význam greylistingu v budoucnu slábnout. A

Denní počet zpráv	Před greylistingem	Po greylistingu	Pokles počtu zpráv
PřírF	53 999	8 303	85 %
FI	48 321	8 187	83 %
PedF	31 225	3 030	90 %
FF	29 120	3 637	88 %
LF	23 663	3 352	86 %
ÚVT	20 557	3 968	81 %
FSS	17 092	3 060	82 %
ESF	10 261	1 407	86 %
PrávF	8 798	1 233	86 %
Rektorát	7 041	1 246	82 %
FSPS	5 931	953	84 %
SKM	1 571	237	84 %

Tabulka 2: Denní průměrné počty e-mailů dle fakult

bude třeba hledat nová opatření. Nicméně v současné době umožňuje greylisting – spolu s pokračujícím filtrováním a protispamovými opatřeními na úrovni fakult i jednotlivých uživatelů – udržet systém elektronické pošty v chodu a ve stavu únosném pro uživatele MU.

Literatura

[1] M.Ruda. *E-mail a centrální poštovní server Masarykovy univerzity*. Zpravodaj ÚVT MU. ISSN 1212-0901, 2007, roč. XVII, č. 4l

[2] ÚVT MU. *Pravidla pro přijímání pošty v doméně muni.cz*. Dostupné na `http://www.ics.muni.cz/techinfo/abuse.html`

Jak se chránit proti spamu

Miroslav Bartošek, ÚVT MU

Idylické časy, kdy Internet byl výlučnou doménou vědců a ohleduplných uživatelů respektujících psaná i nepsaná pravidla síťové etikety (netiquette), jsou nenávratně pryč. Dnešní Internet je nástroj, který na jednu stranu fantastickým způsobem rozšiřuje informační a komunikační možnosti běžného člověka, na druhou stranu skýtá mnohá rizika a nebezpečí – zejména pro nepoučeného a neopatrného uživatele.

V oblasti elektronické pošty jsou hlavními riziky šíření virů/červů a spam. Přestože hlavní tíha boje proti těmto rizikům leží na správcích počítačů a síťových služeb, na individuální úrovni rozhoduje o mnohém sám uživatel. Svými znalostmi a svým chováním ovlivňuje z nemalé části míru svého vlastního ohrožení i ohrožení dalších uživatelů. V případě elektronické pošty může podstatným způsobem ovlivnit množství spamu přicházejícího z Internetu na jeho adresu, stejně tak jako množství spamu, který skončí nerozpoznaný přímo v jeho poštovní schránce. K tomu je ale třeba znát a dodržovat jistá pravidla. Ty lze shrnout do sedmi oblastí:

1. Chraňte svou e-mailovou adresu.
2. Svou poštu čtěte bezpečným způsobem.
3. Poštu posílejte bezpečným způsobem.
4. Neodpovídejte na spam.
5. Filtrujte svou poštu.
6. Buďte obezřetní.
7. Udržujte své počítače v zabezpečeném stavu.

1 Chraňte svou e-mailovou adresu

Obecná zásada říká, že nejefektivnější způsob jak se vyhnout spamům je neumožnit spammerům získat vaši e-mailovou adresu. Nejčastěji získávají spammeři adresy automatizovaným sběrem přímo z webu (z webových stránek, diskusních skupin) nebo tím, že jim ji sami předáte (vyplněním e-mailové adresy při on-line nákupech a registracích). Z toho vyplývají i následující doporučení:

- Neuvádějte svou nechráněnou adresu na webu ani ve volně přístupných elektronických diskusích.
- Pokud již svou adresu potřebujete či musíte na webu uvést, zamaskujte ji tak, aby ji byl schopen přečíst a správně interpretovat člověk, nikoliv však program-sběrač (např. jantecka-novak (na) muni-tecka-cz). Případně použijte speciální dočasnou adresu, kterou můžete později snadno změnit či zrušit.
- Ověřujte si, zda se vaše adresa vyskytuje všude na webu pouze v chráněném tvaru. Zatímco adresy uváděné na univerzitním webu jsou chráněné, uživatelé sami (nebo jejich partneři) zřizují různé osobní stránky, stránky řešených projektů, konferencí apod., kde již adresy chráněné být nemusí.
- Pro případné on-line nákupy a rizikovější operace na webu si založte svou druhou e-mailovou adresu u volně dostupných poskytovatelů (seznam, gmail apod.). Nikdy nepoužívejte pro tyto účely svou primární pracovní adresu. Sekundární adresu v případě její kompromitace snadno změníte, kdežto měnit primární pracovní adresu je problematické. Adres můžete mít samozřejmě i více – každou z nich pro jiný účel.

2 Svou poštu čtěte bezpečným způsobem

Některé spammerské e-maily jsou konstruovány tak, aby poskytly spammerům informaci o tom, zda je vaše e-mailová adresa platná či nikoliv. V kladném případě se cena vaší adresy pro spammery zvyšuje a můžete očekávat ještě větší přísun spamu. Často také dochází k propojování spamu s viry a červy. Při čtení spamů můžete být přesměrováni na spammerské stránky, odkud mohou být do vašeho počítače zavlečeny různé typy nákazy. Proto je užitečné zavést a dodržovat určitou disciplínu, pravidla a nastavení pro bezpečné čtení pošty:

- Buďte obezřetní, podezřelé dopisy raději vůbec neotevírejte; případně je čtěte pouze v režimu zobrazení jednoduchého textu (plaintext).
- U svého poštovního klienta si vypněte automatické zobrazování náhledů (preview), automatické stahování grafiky v HTML e-mailech a další potenciálně nebezpečné funkce, které sice zvyšují uživatelské pohodlí, současně ale lze jejich prostřednictvím aktivovat škodlivý software obsažený ve zprávách či odkazovaných www-stránkách.
- Obraťte se na svého počítačového správce, ať vám doporučí vhodného poštovního klienta a pomůže s jeho bezpečným nastavením.
- Nikdy neklikejte na odkazy uvedené ve spammerských dopisech.

3 Poštu posílejte bezpečným způsobem

Některé způsoby rozesílání pošty mohou znamenat větší riziko prozrazení vaší adresy, či adres vašich kolegů. Současně je vhodné vždy uvažovat nad tím, co a jak vy sami rozesíláte, abyste (byť nevědomky) nepřispívali ke zvyšování spamové zátěže:

- Nerozesílejte řetězové dopisy. Vaše adresa se tak dostává na nekontrolovatelné množství počítačů, odkud může prosáknout až do spammerských databází.
- Ochraňujte e-mailové adresy jiných lidí. Při posílání e-mailu na velké množství adres může být vhodnější uvést tyto adresy do pole BCC (blank copy), namísto klasického CC (copy to).
- Zvažujte pečlivě, které vaše e-maily je skutečně nutné posílat na hromadné adresy, za nimiž se skrývá velké množství příjemců (např. posílání e-mailů na aliasy celé organizace či pracoviště).
- Nespamujte.

4 Neodpovídejte na spam

Z hlediska reakce na obdržený spam může být v našich zeměpisných šířkách někdy vhodné rozlišovat „měkký spam" rozesílaný spíše nezkušenými či naivními tuzemskými podnikateli od „tvrdého spamu" valícího se zpravidla ze zahraničí. Zatímco v prvním případě se dá uvažovat o vhodné formě komunikace s odesílatelem za účelem dalšího zamezení spamu (ale pouze pokud jste si jisti jeho identitou a relativní seriózností), ve druhém případě je doporučení jednoznačné – na spam nikdy nereagujte!

– Ignorujte spamy, které proniknou až do vaší poštovní schránky (smažte je bez čtení, neodpovídejte na ně).
– Nereagujte na výzvy REMOVE, tj. na informaci vyzývající vás k tomu, abyste klikli na zadanou webovou adresu, pokud si dané zprávy nepřejete dále dostávat. Nejenže skuteční spammeři nemají žádný zájem vás chránit (proč by to také dělali), takže z databáze adres vás neodstraní; tyto webové adresy jsou navíc často určeny pouze k ověření platnosti vaší adresy, v horším případě i k zavlečení infekce do vašeho počítače.
– Nikdy nekupujte žádné zboží/služby přes spam. Spammerství může fungovat pouze proto, že se spammerům vyplácí. Při obrovském množství rozeslaných spamů jim k tomu stačí, aby na jejich nabídky zareagovalo třeba jen mizivé procento oslovených. Proto nikdy nepodporujte spam tím, že byste využívali jím nabízených služeb.
– Nebombardujte spammery odvetnými e-maily. Adresy odesílatele jsou u spamu dočasné, zfalšované, nebo jsou použity zneužité adresy nevinných obětí, takže na skutečného původce spamu nemáte obvykle šanci dosáhnout.

5 Filtrujte svou poštu

Spam je do jisté míry individuální záležitost – co je spamem pro jednoho uživatele, nemusí být spamem pro jiného. Proto jsou hromadné antispamové filtry (univerzitní, fakultní) nastaveny dost konzervativně a nemohou zajistit absolutní ochranu všem uživatelům. Přestože účinnost fakultního filtru bývá obecně velmi vysoká, i více než 90 %, může se stát, že ve vašem konkrétním případě nemusí být dostatečná (a na druhou stranu se dokonce může stát, že je pro vás příliš restriktivní). V takovém případě se může vyplatit nastavit si svůj osobní antispamový filtr. Záleží samozřejmě na vašich znalostech, dovednostech a ochotě naučit se něco nového k dané problematice a v praxi to aplikovat.

– Ověřte si u vaší fakultní Laboratoře výpočetní techniky či správce vaší pošty, jak vaše fakulta/katedra provádí filtraci spamů, zda je fakultní ochrana skutečně aktivována i pro vaši e-mailovou adresu a jak s ní uživatel může dále pracovat (změny nastavení, přístup k zachyceným spamům při vyhledávání nedoručené pošty atd.).
– Není-li ve vašem případě fakultní antispamový filtr dostatečně účinný, aktivujte po dohodě se správcem vaší pošty svůj osobní filtr. Může jít buď o filtr nabízený přímo vaším poštovním klientem na vašem počítači nebo o osobní nastavení fakultního filtru na fakultním poštovním serveru.
– Pokud váš osobní filtr podporuje techniku učení se na příkladech, doučujte ho tím, že mu budete předkládat jak nezachycené spamy (spam) tak i zprávy označené chybně za spam (ham). Obvykle je třeba předložit učícímu se filtru až několik stovek spamů a současně také několik stovek hamů, aby se dosáhlo maximální účinnosti rozpoznání vašeho typu spamu při minimální chybovosti. Toto je důležité také proto, že spammeři reagují na tento typ ochrany změnou struktury svých e-mailů a bez trvalého „doučování" se kvalita filtrace může v čase postupně zhoršovat.
– Filtrační program spamassassin používaný na fakultách MU umožňuje vytvářet relativně jednoduchým způsobem i osobní filtrační pravidla, a to přímo koncovými uživateli [1]. Tato pravidla mohou poskytnout nejvyšší stupeň ochrany ušitý na míru přímo danému uživateli.
– Aktualizujte své osobní antispamové filtry.

6 Buďte obezřetní

Internet v současnosti již není (a stěží kdy v dohledné době bude) tak idylické a bezpečné prostředí jako ve svých počátcích. Je třeba s tím počítat, a být poučený a obezřetný. V případě spamů již nejde dnes jen o to, že obtěžují. Čím dál více dochází k jejich propojování s počítačovými viry, červy, trojskými koni a různými podvodnými aktivitami. Čili stávají se i nebezpečnými.

– Buďte obezřetní a podezřívaví při otevírání dopisů od neznámých osob či institucí, při jejich čtení a reakcích na ně.
– Buďte obezřetní při brouzdání po Internetu; nebezpečné mohou být zejména stránky

s pornografií, hrami a dalšími „chytlavými" tématy.

7 Udržujte své počítače v zabezpečeném stavu

Podle některých odhadů je až 7% počítačů připojených do Internetu napadeno různou formou nákazy, včetně programů, které se navenek zdánlivě nijak škodlivě neprojevují, umožňují však hackerům ovládat váš počítač bez vašeho vědomí a zneužívat ho pro různé účely. Například pro rozesílání spamu. Proto:

- Mějte na svých počítačích nastaveny ochranné firewally, pravidelně aktualizované antivirové programy a další ochranné nástroje proti škodlivým programům.
- Provádějte pravidelné instalace bezpečnostních záplat svého operačního systému a programů (lze nastavit, aby se provádělo automaticky – konzultujte se svým počítačovým správcem).
- Čas od času požádejte počítačového správce o provedení bezpečnostního auditu vašeho počítače (kontrolu a vyčištění od případných nákaz a nežádoucích programů, aktualizaci používaného programového vybavení, kontrolu bezpečnostních nastavení apod.)
- Zabezpečte a pravidelně aktualizujte bezpečnostní opatření nejen pro svůj počítač v práci, ale i pro své domácí počítače.

Jako v každém nebezpečném prostředí, ochrana „policií" (v případě Internetu pak správci počítačů a počítačových služeb) je vždy omezená, a její úspěšnost je velmi závislá na ochotě a spolupráci jednotlivců. V případě Internetu to platí dvojnásob – bez aktivního zapojení poučených (a trvale vzdělávajících se) uživatelů zůstane boj proti spamům sysifovským úsilím.

Literatura

[1] M. Bartošek. *Vylaďte si svůj SpamAssassin (2).* Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. XVI., č. 2, str. 5–8. □

Nový personální a mzdový systém Masarykovy univerzity

Jana Kohoutková, ÚVT MU

Před necelým rokem jsme na stránkách Zpravodaje psali o spolupráci mezi ekonomicko-účetním informačním systémem Magion a ekonomicko-správním intranetem Inet MU (viz [1]) a na závěr jsme poznamenali, že od ledna 2007 budou na MU uvedeny do provozu také moduly pro personalistiku a mzdy IS Magion a že o tom ve Zpravodaji rádi poreferujeme. Měsíce se jako obvykle překulily rychleji, než by si účastníci dění přáli, a personálně-mzdové moduly IS Magion již Masarykově univerzitě spočítaly dvojí mzdy. Je tedy čas dodržet slovo a podat slíbený referát.

1 Éra informixová

Celouniverzitní databáze personálně-mzdových dat a systémy pro jejich správu a zpracování se na MU vyvíjejí od roku 1994.[1] V roce 1994 bylo do provozu uvedeno centrální zpracování mezd, v roce 1998 byla do centrální databáze a správy přenesena personální administrativa (tzv. *Jednotný systém personalistiky – JSP*). Databází byl Informix, zvolený po pečlivém zvažování na základě srovnávacích studií, viz [2]. Programy pro správu a zpracování dat byly napsány nad Informixem v jazyce 4GL a uživatelé s nimi pracovali přes alfanumerický terminál (v režimu terminál–server). V roce 1999 systém zakotvil na serveru *bombur* (spolu s databází a programy ekonomického IS Magion, provozovaného na MU od roku 1998) a pod tímto jménem jej také znali uživatelé. Programy zpracování mezd a JSP byly kompletně vytvořeny na MU, ve spolupráci ÚVT a personálních útvarů. Za první desetiletí provozu prošel systém řadou obměn a rozšíření, stále však na stejných technologických principech, tedy Informix a 4GL.

V dubnu 2004 se MU rozhodla převést centrální personálně-mzdovou a ekonomickou databázi z platformy Informix na perspektivnější

[1] Před tímto datem (od roku 1986) bylo elektronické zpracování mezd MU řešeno typovým projektem ČVUT na technologii indexsekvenčních souborů v programovacím jazyce Cobol.

Oracle. Z tohoto rozhodnutí přímo plynula nutnost nahradit dosavadní personálně-mzdový systém novým systémem – novým po stránce databázového i programového řešení. Následovalo rozhodnutí „koupit, nikoli vyvíjet“, tedy nepokračovat již ve vývoji vlastními silami, ale pořídit systém od externího dodavatele. Důvodem pro toto rozhodnutí bylo, že aplikační oblast personalistiky a mezd je do značné míry typizovaná, má pevné místo na softwarovém trhu, dodavatelé dávají záruky odborného zázemí a sledování vývoje v této oblasti (jak uživatelských požadavků tak souvisejících předpisů a legislativy) a MU musí přednostně soustředit své vývojové kapacity do těch aplikačních oblastí, kde je vlastní vývoj nahraditelný těžko nebo vůbec. Na podzim se na MU prezentovala řada potenciálních externích dodavatelů, zástupci MU navštívili několik univerzit na různých místech ČR, proběhl rozsáhlý sběr a analýza požadavků a vše vyústilo v zadávací dokumentaci pro výběrové řízení na *Personální a mzdový systém v rámci IRIS MU* (zkráceně PaMS).

V roce 2005 dále pokračovala migrace Informixu na Oracle (v lednu databáze univerzitní telefonie, v červenci ekonomická databáze IS Magion[2] a následně databáze Clearingu MU) a především kroky k novému PaMS. Výběrové řízení se uskutečnilo v dubnu a květnu. Sice rozřadilo uchazeče na silnější a slabší (technickými požadavky, požadavky na zkušenost s rutinním provozem v prostředí vysoké školy, atestačními požadavky), avšak nikdo z trojice, která nakonec podala nabídky,[3] nesplnil všechny požadavky zadání. Soutěž tedy skončila bez určení vítěze, ale přinesla MU větší míru poznání, že volba dodavatele nového PaMS značně ovlivní vývoj informační podpory v dalších oblastech – především ekonomické, manažerských nadstavbách, nebo chystané spisové službě – a že si MU musí ujasnit (s potřebným výhledem do budoucna), jaké požadavky chce klást na spolupráci PaMS s okolními systémy. Například vazby mezi PaMS a ekonomickým systémem (EIS) mohou být poměrně volné, jak tomu bylo doposud na bomburu, ale také mohou být velmi úzké, mají-li zajišťovat transparenci dat a identické výstupy ze strany PaMS i EIS, zohledňující i zpětné přepočty event. opravy v účtování mezd. Čím užší mají být vazby, tím větší výhodou až nutností je společné jádro těchto systémů.

[2] Programy IS Magion byly z bomburu odsunuty již o rok dříve, a sice na terminálové servery (verze ve 4GL byla nahrazena grafickým klientem, napsaným v PowerBuilderu).

[3] Magion System, a.s. nabídl EIS Magion, Elanor spol. s r.o. nabídl IS Elanor Global, VARIAS CZ, a.s. nabídl mySAP ERP.

2 Rozvojový projekt 2006

Poučení z výběrového řízení 2005 šlo ruku v ruce se skutečností, že stávající personálně-mzdový systém je opět o rok starší a blíže k hranici životnosti a jeho inovaci nelze odkládat. S touto myšlenkou byl na podzim 2005 podán rozvojový projekt MU na rok 2006 nazvaný „Rozvoj datové a aplikační infrastruktury MU“, v němž jednu ze tří částí představoval „Rozvoj informačního systému MU“. Cílem bylo:

- na základě analýzy informačních požadavků a potřeb vybrat externího dodavatele základního SW podporujícího řízení MU v oblastech personálně-mzdové, ekonomické a v manažerských nadstavbách,
- v první etapě implementace vybraného SW zavést základní moduly pro personalistiku a mzdy tak, aby jejich reálný provoz mohl být zahájen k 1.1.2007, včetně jejich provázání s dalšími informačními systémy MU.

Řešení bylo navrženo ve čtyřech na sebe navazujících etapách: [1]

1. analýza požadavků MU na informační podporu v personálně-mzdové a ekonomické oblasti v souvislosti s dalšími informačními subsystémy MU (do 31. 3.);
2. výběr externího dodavatele základního SW pro pokrytí těchto oblastí (do 30. 6.);
3. pořízení informačního subsystému pro personalistiku a mzdy a implementace jeho základních modulů (do 31. 12.);
4. návrh a základní nastavení rozhraní vůči souvisejícím informačním subsystémům MU (do 31. 12.).

Projekt úspěšně prošel hodnotícím řízením, byla mu udělena finanční dotace a půlstovka řešitelů z celé MU si vykasala rukávy.

3 Plány, cíle a realita v roce 2006

Prvním krokem řešení projektu byla revize analýzy informačních potřeb a požadavků MU provedené pro výběrové řízení 2005 ve světle jeho průběhu a výsledků. Revize proběhla v lednu 2006 a potvrdila požadavek budovat co nejužší vazby mezi personálně-mzdovým a ekonomickým IS. Jinými slovy, potvrdila rozhodnutí orientovat se na jednoho společného dodavatele těchto systémů. Na tomto základě oslovila MU společnost Magion System, a. s., jakožto jediného dodavatele ekonomického IS provozovaného na MU, výzvou k rozšíření stávající dodávky ekonomických modulů o moduly PaM. Následně, 15. března 2006, spolu obě strany podepsaly smlouvu o dílo na dodávku modulů PaM, rozdělenou do etap *Analýza a návrh řešení*, *Realizace*, *Pilotní provoz*, *Příprava rutinního provozu* a *Rutinní provoz se zvýšenou podporou* tak, aby plný rutinní provoz systému zajistil zpracování mezd MU od ledna 2007.

Následovala druhá část analytických prací, tentokrát již ve spolupráci MU se smluvním dodavatelem. Za základ bylo vzato tzv. „standardní řešení“ PaM Magion a k tomuto byly navrženy úpravy a rozšíření, v mnoha směrech velmi zásadní, dle požadavků a specifikací MU (na návrzích spolupracovali zástupci – v převážné míře zástupkyně – RMU, součástí MU a ÚVT). Výsledkem byl 450stránkový dokument, podrobně popisující řešení a cílové funkce systému. V květnu byl dokument obhájen interní oponenturou a akceptován řídícím výborem projektu a bez odkladů začaly implementační práce a na ně navazující testování, školení a integrační práce.

V průběhu června–října 2006 byly implementovány a funkčně otestovány jednotlivé moduly PaM systému, pokrývající všechny oblasti správy a řízení lidských zdrojů, tj. správu kmene osob (neboli centrální evidenci osob), evidenci organizační struktury, systemizaci pracovních míst, evidenci pracovních, řídících a akademických funkcí, personální evidenci zaměstnanců, zpracování mezd, podporu vzdělávání a BOZP, správu výběrových řízení, evidenci členství v radách a komisích a samozřejmě správu systému.

V listopadu 2006 byla funkčnost modulů úspěšně prověřena 1měsíčním pilotním provozem, běžícím duplicitně s rutinním provozem stávajícího systému v plném rozsahu pěti součástí MU (RMU, tří fakult – lékařské, informatiky a sportovních studií – a SKM). Pilotní provoz byl uzavřen duplicitním zpracováním mezd za listopad ve stávajícím systému a nově vyvíjeném PaM Magion a jejich vzájemným odsouhlasením, opět v plném rozsahu duplicitního zpracování.

Prosinec 2006 byl (snad jen s výjimkou Štědrého večera) věnován jednak přípravě přechodu od pilotního do rutinního provozu a dále implementaci integračních rozhraní na okolní systémy. V prvé řadě se jednalo o integraci PaM Magion s ekonomickými moduly IS Magion a s elektronickým docházkovým systémem MU, které jsou pro provoz PaM Magion nezbytné. Další integrační rozhraní byla budována na Inet MU, veřejnou internetovou prezentaci, dále studijní informační systém IS MU, stravovací systémem Kredit a další subsystémy informační infrastruktury MU.

4 Události do března 2007

Začátkem ledna 2007 byly naposledy spočítány mzdy MU v informixovém prostředí. Ve čtvrtek 11. ledna byly zakonzervovány veškeré vazby informixové databáze na okolní systémy a odstartoval proces migrace dat z Informixu do databáze PaM Magion. Proces zahrnoval rozšíření a úpravy datových struktur a aplikací dosud provozovaného EIS Magion, konverzi dat z informixovské databáze (byla provedena včetně historie), nastavení a vyladění parametrů PaM Magion a komplexní sadu kontrol. V pátek v pravé poledne byl přerušen provoz EIS Magion.[4] Migrace byla dokončena a prověřena během víkendu a v pondělí 15.1. byly ekonomické moduly IS Magion opět uvolněny do rutinního provozu. Kontroly dat PaM, nastavení číselníků a nastavení přístupových práv uživatelům pokračovaly ještě v následujících dnech a 22. 1. byl systém uveden do plně rutinního provozu na všech součástech MU. Bezprostředně následovalo napojení

[4] Jakkoli informováni se značným předstihem a opakovaně, nechali se někteří uživatelé jmenovitě telefonicky žádat, aby svou práci přerušili. Inu, nejsou vždy všichni za všechny…

docházkového systému (konec měsíce se nezadržitelně blížil), samozřejmostí bylo okamžité připojení stravovacího systému, který pro svůj provoz vyžaduje aktuální data PaM (kdo je či není v daném dni na MU v aktivním pracovním poměru).

Světu byla veřejně publikovatelná data z databáze PaM Magion zpřístupněna v únoru – a sice číselník pracovišť, základní osobní data (jména, příjmení, tituly), údaje o pracovních poměrech (pracovní funkce a zařazení na pracoviště podle kmenových úvazků resp. zdrojů financování) a údaje o výběrových řízeních. Práce na napojení www.muni.cz dostaly přednost před intranetovými aplikacemi, aby veřejná tvář MU byla aktualizována v nejkratším možném čase.

V průběhu února a března byly dále řešeny návaznosti na ekonomický systém, zejména tzv. „rozpouštění“ náhrad za dovolenou, zaúčtování mezd na zakázky a tvorba a účtování sociálního fondu. Ruku v ruce šly návaznosti na IS MU, tj. poskytování dat o organizační struktuře (číselníku pracovišť), osobách a jejich pracovních poměrech, a rovněž vytvoření rozhraní pro integraci kmene osob v PaM Magion s evidencí osob ve studijním systému. Obdobně byly postupně napojeny další systémy (systém Celouniverzitní počítačové studovny, geografické aplikace aj.). Propojení PaM Magion s Inetem si necháme do další kapitoly.

Počátkem února byly v PaM Magion zpracovány mzdy za leden 2007 a tím nový systém definitivně zakotvil v informační infrastruktuře MU. Zpracování mezd zatím probíhá pod dohledem dodavatele. Podmínkou pro úspěšné splnění smlouvy z 15. 3. 2006 je bezproblémový provoz systému po dobu dvou měsíců a dvojí úspěšně zpracování mezd samostatně řízené z MU. Tato šťastná tečka se očekává v květnu letošního roku.

Se zprovozněním nového PaMS MU je svázán konec třináctileté historie Informixu na MU a konec tříleté historie jeho postupného převodu na Oracle. V létě 2006 byla přenesena provozní databáze Celouniverzitní počítačové studovny, v listopadu databáze fotografií osob a identifikačních průkazů MU (viz také [3]), nu a nakonec v lednu 2007 personálně-mzdová databáze. Server bombur je od ledna v režimu archivního provozu, s nímž se počítá ještě do konce letošního roku.[5] Poté budou data překopírována na Oracle a případné ojedinělé přístupy k nim budou nadále zprostředkovávat nikoli již programy napsané v Informix 4GL, ale databázové dotazy a skripty napsané přímo nad Oracle.

5 Plány a cíle 2007 aneb Jak mají spolupracovat PaM Magion a Inet

S dalšími výhledy do letošního roku se můžeme společně vrátit tam, odkud článek vyšel, tedy ke spolupráci modulů PaM Magion a Inetu.

Podobně jako u ekonomických modulů IS Magion platí i pro moduly PaM, že poskytují informační podporu uživatelům na úrovni rektorátu a součástí MU (vedení a odborným pracovníkům univerzity a jednotlivých součástí, s přístupy k datům celé univerzity resp. součásti), zatímco dalším úrovním uživatelů poskytuje přístup k personálně-mzdovým datům jednak Inet (vedoucím a sekretariátům jednotlivých pracovišť a jednotlivým osobám z MU – zaměstnancům, studentům a dalším spolupracovníkům) a dále www.muni.cz (světu). Uživatelů na úrovni RMU a součástí je přibližně pět desítek (výhledově do jednoho sta), na úrovni pracovišť a jednotlivců přibližně 3,5 tisíce osob (téměř 80 % zaměstnanců), uživatelů „ze světa“ více než 14,5 tisíce různých IP adres týdně.

Do nasazení modulů PaM probíhala spolupráce mezi IS Magion a Inetem pouze na úrovni surových dat, uložených v relačních datových strukturách. Aplikace Inetu četly data přímo z databáze Magionu, a také do ní přímo zapisovaly, „povolení“ čtení a zápisu byla dána pouze neformálními dohodami mezi firmou Magion a vývojovým týmem Inetu. Do projektu PaMS MU byla proto začleněna také implementace tzv. *integračního rozhraní*, garantujícího poskytování vybraných dat z databáze PaM Magion ve vzájemně dohodnuté a dokumentované podobě, s cílem odstínit Inet od případných změn vnitřních datových struktur PaM Magion. Rozhraní je zatím implementováno databázovými objekty (tabulkami

[5] Archiv je potřebný zejména kvůli přístupu k historickým personálně-mzdovým datům, která nebylo možné nebo účelné přenést do PaM Magion.

a pohledy), připravuje se však jeho rozšíření do podoby API typu webových služeb, aby bylo možno vyvážet z IS Magion i složitěji předzpracovaná data. Rozhraní slouží především Inetu, ale jsou přes ně předávána data PaM i všem dalším spolupracujícím systémům MU.

Nadstavby nad PaM Magion v Inetu MU jsou umístěny v podmenu Personalistika a jedná se o přehledy a) osobních dat, b) pracovních poměrů, c) mzdových údajů, a dále komponenty používané napříč celým Inetem, především vyhledávání osob a evidence tzv. „aktivních osob“, tedy aktuálních zaměstnanců, studentů a pracovníků na dohody. Přehledy osobních dat a údajů o pracovních poměrech jsou již v Inetu zveřejněny a více se o nich dočtete v dnešních Tipech z Inetu. Mzdové přehledy se v Inetu objeví počátkem dubna.

Samostatný díl nadstavby nad PaM Magion představuje napojení systému SUPO, viz [4]. Jedná se o evidenci souhlasů zaměstnanců s prováděním převodů částí mezd na jejich účet v SUPO, přebírání příkazů k převodům částí mezd ze SUPO do PaM Magion, provádění těchto příkazů při zpracování mezd a vracení potřebných dat a informací do SUPO. Tato část nadstavby je v plánu na letošní letní prázdniny.

6 Poděkování

Na závěr mi dovolte využít příležitosti a poděkovat lidem, o jejichž práci právě dopsané řádky mluví – v prvé řadě generaci tvůrců a provozovatelů PaMS MU v prostředí Informix 4GL a v dalším sledu všem spoluřešitelům rozvojového projektu.

Z úctyhodné řady jmen, která nemohu všechna uvést (a ani bych se nechtěla pokoušet, vědoma si rizika, že některé může vyklouznout), vybírám konkrétně dvě: pány Dr. Jaroslava Šmardu a Dr. Petra Píska. Oba vystupují v obou skupinách a představují kontinuitu znalostí a zkušeností, nasbíraných za dlouhé roky provozu informixového systému, v novém PaM Magion. Jejich podíl na analýze a návrhu rozšíření a úprav PaM Magion byl stěžejní, a přístup k předávání vlastních znalostí dalším pokračovatelům nemohu nazvat jinak než noblesním. Jardo a Petře, upřímně děkuji.

Literatura

[1] J. Kohoutková. *Jak spolupracují Magion a Inet.* Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč. XVI, č. 5, s. 5-10.

[2] M. Benešovský. *Výběr databázového systému pro MU (1).* Zpravodaj ÚVT MU. ISSN 1212-0901, 1992, roč. II, č. 3, s. 9-11.

[3] Z. Machač. *Fotografování osob a výroba identifikačních karet na MU.* Zpravodaj ÚVT MU. ISSN 1212-0901, 2007, roč. XVII, č. 3, s. 12-15.

[4] A. Jurtíková, J. Ocelka, J. Staudek. Clearing MU - zúčtovací systém pro bezhotovostní uhrazování poskytovaných služeb. Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. XVI, č. 1, s. 11-13. □

Tipy z Inetu: Personální údaje a údaje o pracovních poměrech

Petr Láznický, ÚVT MU

1 Přehled aplikací

V Inetu jsou k dispozici následující aplikace zobrazující personální údaje a údaje o pracovních poměrech zaměstnanců:

- aplikace *Osobní list* na adrese `https://inet.muni.cz/app/osoby/persdata` zobrazuje zaměstnanci (a obecně libovolné osobě z databáze osob MU) aktuální stav osobních údajů, které o něm vede Masarykova univerzita;
- aplikace *Osobní data* na adrese `https://inet.muni.cz/app/osoby/oslist_prehled` vypisuje vedoucímu pracoviště přehled základních osobních údajů zaměstnanců na tomto pracovišti, zaměstnanci vypisuje údaje, které o něm vidí jeho vedoucí (jedná se o výběr z osobního listu zaměstnance);
- aplikace *Pracovní poměry* na adrese `https://inet.muni.cz/app/osoby/pracovni_pomery_prehled` vypisuje vedoucímu pracoviště přehled pracovních poměrů zaměstnanců na tomto pracovišti, zaměstnanci vypisuje údaje, které o něm vidí jeho vedoucí;

– aplikace *Průběh zaměstnání na MU* na adrese `https://inet.muni.cz/app/osoby/prubeh_zamestnani` vypisuje zaměstnanci historii jeho pracovních poměrů na MU.

Aplikace jsou přístupné v podmenu *Personalistika*, *Osobní list* a *Průběh zaměstnání na MU* v sekci *Individuální informace*, *Osobní data* a *Pracovní poměry* v sekci *Přehledové sestavy*.

2 Aplikace zblízka

Uvedené přehledy, které zobrazují v Inetu personální údaje a údaje o pracovních poměrech zaměstnanců, jsou vytvořeny jako aplikační nadstavba nad personálně-mzdovým systémem provozovaným na MU. Zpřístupňují jednak podrobné údaje samotným zaměstnancům a dále strukturované výběry vedoucím pracovišť. Vedoucí pracovišť tak mají stále k dispozici aktuální základní osobní a kontaktní údaje o svých podřízených, včetně údajů o pracovních poměrech. Zaměstnanci mají přehled o základních údajích, které o nich vede MU, a v případě aplikace *Osobní list* mají možnost vybrané údaje i aktualizovat.

Aplikace *Osobní list* vypisuje osobní údaje v rozsahu: identifikační údaje osoby, základní osobní údaje, údaje o průkazu totožnosti a identifikační kartě zaměstnance MU, adresa trvalého bydliště, kontaktní adresa, dosažené vzdělání včetně průběhu a rodinní příslušníci. Zaměstnanec má možnost aktualizace některých údajů – konkrétně rodinného stavu, čísla občanského průkazu a kontaktní adresy. Tato funkčnost je v současné době dočasně nepřístupná z důvodu odstraňování nekonzistencí mezi personální databází a databází studijního systému IS MU, které vznikly v důsledku nasazení nového personálně-mzdového systému začátkem letošního roku. Plné obnovení funkcí předpokládáme v průběhu dubna 2007.

Aplikace *Osobní data* vypisuje přihlášené osobě její osobní údaje v rozsahu: jméno, UČO, datum narození, bydliště a telefon. Je-li osoba zároveň vedoucím pracoviště, má možnost zobrazit si přehled těchto údajů za všechny zaměstnance svého pracoviště. Má-li vedoucí více podřízených pracovišť, má možnost vybrat si více pracovišť současně. Kliknutím na jméno zaměstnance ve výpisu je možné zobrazit jeho kontaktní údaje na MU.

Aplikace *Pracovní poměry* slouží především jako přehled pro vedoucí pracovníky, zaměstnanci MU poskytuje informaci o jeho pracovních poměrech. Přihlášené osobě se vypisují údaje o jejích aktuálně platných pracovních poměrech na MU v rozsahu: označení a druh pracovního poměru, datum zahájení, případně ukončení pracovního poměru, kmenové pracoviště, funkční zařazení, dále celkový úvazek a rozdělení pracovního poměru na části podle zdrojů financování (tj. po pracovištích a zakázkách) včetně data, odkdy daný stav platí. Vedoucí pracoviště má možnost zobrazit si přehled údajů ve stejném rozsahu za všechny zaměstnance pracoviště. Nejprve se vypisují kmenoví zaměstnanci pracoviště a potom, odděleni čarou, také další zaměstnanci, kterým je z pracoviště financována část jejich pracovního poměru (úvazku). Nakonec je uveden celkový přepočtený stav zaměstnanců na daném pracovišti.

Aplikace *Průběh zaměstnání na MU* vypisuje zaměstnanci historii jeho pracovních poměrů. Výpis je v rozsahu: údaje o pracovním poměru (datum a číslo smlouvy, označení a druh pracovního poměru, datum zahájení, datum ukončení, kmenové pracoviště, funkční zařazení), historie pracovních zařazení (datum vzniku, datum ukončení, pracoviště, funkční zařazení, velikost úvazku, tarifní třída, stupeň, částka mzdy) a historie zdrojů financování (datum vzniku, datum ukončení, pracoviště, zakázka, velikost úvazku) se zvýrazněním aktuálně platných údajů. Pracovní poměry jsou řazeny podle aktuálnosti, nejdříve aktivní, potom ukončené, a dále sestupně podle data ukončení, resp. zahájení. Ve výpisu nejsou uvedeny pracovní poměry, které jsou již v personálně-mzdové databázi MU zaznamenány, avšak mají datum vzniku pozdější, než je aktuální datum.

3 Novinky z PaMS Magion

V lednu 2007 byl uveden do provozu nový personálně-mzdový systém MU – PaMS Magion. S tím souvisí i zvětšení rozsahu údajů zobrazovaných v Inetu. U zaměstnance se už nesleduje jen kmenová fakulta, ale přímo kmenové

pracoviště, na kterém je svým pracovním poměrem zařazen. Při přechodu na nový systém byl tento údaj hromadně vyplněn podle pracoviště ve zdroji financování, v případě více zdrojů bylo kmenové pracoviště vyplněno podle pracoviště u většího úvazku, v případě stejných úvazků bylo vybráno náhodně jedno z pracovišť. Personalistky fakult v těchto případech provedly kontrolu a ruční doladění údajů.

Osobní data vedená v systému PaMS Magion a ve studijním systému IS MU jsou vzájemně synchronizována, tj. změny provedené v jednom systému se automaticky objeví i ve druhém. S novým PaMS Magion došlo k rozšíření synchronizovaných údajů. Synchronizují se základní osobní údaje, tituly před a za jménem, rodné příjmení, rodinný stav, místo a stát narození, státní příslušnost, příznak trvalého pobytu, adresa trvalého bydliště a kontaktní adresa a průkazy osob (občanský průkaz, cestovní pas). V současné době ještě probíhá dolaďování synchronizovaných údajů mezi oběma systémy.

Databáze PaMS Magion je rovněž zdrojem dat pro veřejnou internetovou prezentaci MU www.muni.cz. I tady došlo ke změnám oproti dřívějšímu stavu. Příznak „zveřejnit na webu" je nyní veden jak u kmenového pracoviště zaměstnance, tak u pracoviště ze zdroje financování. Viditelnost příslušnosti zaměstnance k pracovišti je v obou případech standardně nastavena na „ano", na požádání ji může příslušná personální referentka zakázat. Je-li viditelnost kmenového pracoviště povolena, vypisuje se na něm zaměstnanec vždy, i kdyby z něj aktuálně nebyl vůbec financován.

Naším přáním je, abyste v Inetu našli vždy údaje, které potřebujete a které vám pomohou ve vaší práci. Máte-li nějaká přání nebo nápady na vylepšení výše popsaných aplikací, uvítáme je na e-mailové adrese `pmd-inet@ics.muni.cz`. □

Obsah

Editor: Miroslav Bartošek • Vydavatel: Masarykova univerzita • Žerotínovo náměstí 9, 601 77 Brno, CZ
tel.: 549 492 100 • e-mail: zpravodaj@muni.cz • WWW: http://www.ics.muni.cz/zpravodaj/
Sazba systémem LaTeX 2ε písmem LucidaBright • Tisk: Grafex Blansko • *Neprodejné* • ISSN: 1212–0901