

SLÁVA, JE TU JARO!

Informační technologie září na CeBITu

Bohužel mi čas nedovolil zastavit se na CeBITu na víc než jedno dopoledne, a proto berte moji zprávu pouze jako průlet zoufalce obrovským mraveništem, plným lidí a výrobků.

Prvním a nejdůležitějším poznatkem letošního CeBITu bylo, že zde nebyl žádný software, který by stál za řeč. Doby, kdy jsme tancovali kolem ohňů s nápisem CorelDRAW nebo jiných programů, jsou dávno pryč. Všechno je jen evoluce. Kancelářské balíky jakbysmet. Takže software – mrtvo. Nic převratného. Díky tomu po několika letech v rámci CeBIT Highlights nebyla udělena ani jedna cena. A prodejci hardwaru hlásí nedobré časy. V lednu a v únoru se prodávalo méně než loni a před několika lety. Mnozí z nás nakoupili na Vánoce 2000 na dluh, ale – není to třeba právě i o tom, že své nevzhledné krabice s pevnými disky zakončené klávesnicemi a monitory nemáme čím krmit? Kde jsou revoluční počiny typu Kai Power Tools, které zářily na CeBITu před několika lety?

Za druhé: Olympus přichází na trh s novými digitálními přístroji dvoumegapixelové třídy Camedia C-1 a C-700 Ultra Zoom. V prvním případě jde o kompaktní přístroj do kapsy, který atakuje desetitisícovou hranici (zatím přesná cena ještě není známa, ale mohlo by to tak být, že?), v druhém případě jde o přístroj v provedení pravá zrcadlovka, dost podobná řadě přístrojů řady C-30x0. Pro informaci – v loňském roce došlo k poklesu prodeje klasických fotopřístrojů v České republice ze 186 na 170 tisíc, přičemž pokles prodeje byl zcela dorovnán, ba i předstížen prodejem přístrojů digitálních.

Za třetí: Už brzy zahodíme 3,5" mechaniky s kapacitou 1,44 MB. Toshiba totiž předvedla v zákulisí alternativu pro svou řadu notebooků – je jí mechanika DVD/CD-R. Tedy mechanika, která dovede číst DVD a zároveň dokáže vypalovat média CD-R. Skvělý nápad! Sem s ním!

Za čtvrté: Ve všem je WiFi, neboli technologie bezdrátových sítí s rychlostí 11 Mb/s a rychle se šíří technologie Bluetooth. Acer, Toshiba a další – ti všichni jsou při tom. Při tom jsou ale i výrobci mobilních telefonů, kteří své nové mobily vybavují právě technologií Bluetooth. Super, kontakt přes infraport byl tedy slepou uličkou...

Za páté: Naštvala mne Nokia. Zbaběle utekla od projektu telefonu řady 7110. Tento stroj, mně sympatický možností obsluhy za vydatné pomoci roleru, kolečka, které urychluje spoustu činností, nebude mít asi nástupce. Pracovníci Nokie na moje dotazy reagovali zapšklým mlčením. Škoda.

Za šesté: CeBIT je jednoznačně největším evropským veletrhem. Nikoli však světovým. Světové novinky jsou vždy prezentovány na Comdexu, to je bez debat. Tedy pokud jde o vize a jejich uvedení do života. Pokud však jde o technologie týkající se mobilních telefonů a jejich podpory, díky (prozatím) odlišným standardům evropským a americkým je CeBIT jediným a největším veletrhem, kde můžete vedle sebe vidět giganty typu Bosch, Ericsson, Motorola, Nokia, Panasonic, Sony i jejich (ne)přátele z Dálného východu – a srovnat, co pro vás je nebo bude lákadlo, které budete chtít nosit v kapse či kabelce. Super.

Za sedmé: Především kvůli šestému bodu se vyplatí do Hannoveru zajet a srovnat, co se v kategorii komunikací na trhu vyskytuje – zvláště, když se cesta díky dokončení nové dálnice z Drážďan přes Lipsko zkrátí o zhruba sto kilometrů. Skvělé.

Za osmé: Vyplatilo se zajít do americké expozice, kde firma Boeing, výrobce letadel ze Seattlu, ukazovala on-line připojení k internetu, které "chodí" ve výšce dvanácti kilometrů i při rychlostech kolem osmi set kilometrů v hodině. Spojení je možné díky vysokorychlostnímu komunikačnímu systému Connection. Systém nabízí rychlost 25x vyšší, než nabídne dnešní průměrný modem připojený k telefonní síti. A tak si budete moci připojit do zásuvky v sedadle notebook nebo "pédéáčko" a sledovat video, poslouchat internetová rádia – a cestování bude veselejší. Princip je v obousměrné satelitní komunikaci, která bude komerčně dostupná v USA na přelomu let 2001/2002, v Evropě v roce 2003 a v Asii a v Pacifiku o rok později. Klasickou otázkou zatím zůstává, kolik bude stát minuta připojení...

Potřebujeme vůbec vzdělání?

Na konferenci Internet ve státní správě a samosprávě (ISSS 2001, Hradec Králové 26. a 27. 3. 2001) jsem si uvědomil, jak je nám lhostejné vzdělání lidí. Primátor pořadatelského města Hradce Králové upozornil na to, že své úředníky vychovává pro vstup do EU tím, že zaměstnanci chodí na školení ECDL (European Computer Driving Licence, evropský "řidičák" na počítač), a mají tak možnost získat vzdělání, které umožní mj. bezproblémovou práci s kancelářskými aplikacemi. To je výhoda – a například v Maďarsku je každý žadatel o práci ve státní správě povinen předložit toto osvědčení. V Hradci jsou ale asi jediní, kteří dávají do vzdělání lidí nemalé částky. Jinak je to, jak jsem vyrozuměl, bída a utrpení.

Pokud by se někdo, třeba i díky naší Chip Akademii, stal držitelem certifikátu ECDL, není nijak zvýhodněn při přijímání na místo ve státní správě, jinde ani nemluvě. A tak může dostat přednost člověk, na jehož počítačové vzdělání bude třeba vyložit během krátké doby nemalé částky. V době, kdy se i na této konferenci hovořilo o využití digitálního podpisu v praxi – a dokonce poslanec Mlynář a ministr Březina přislíbili, že podpoří chod celého aparátu tak, aby daňové přiznání za tento rok již v příštím roce mohlo být přijato elektronicky. Bude ho ale mít kdo přijmout, když na druhé straně bude panovat počítačová negramotnost? I proto mne zneklidňuje, jak málo se věnujeme možnostem vzdělávání pro naši elektronickou budoucnost.

PGP lze prolomit

Vlastimil Klíma a Tomáš Rosa, které znáte ze stránek Chipu, jsou těmi, kteří našli v digitálním podpisu PGP díрку. Ač se to “našeho” digitálního podpisu (odhlasovaného loni poslanci) netýká, hovoří se o tom, že tvůrce PGP, pan Zimmerman, prý nechal ve svém dítku tunýlek záměrně, aby bylo možné sledovat dění na informační dálnici. Že by novodobý Big Brother?

Zábavné bylo sledovat počínání našich médií, která naházela do jednoho pytle šifru, digitální podpis a možnost odtajnit důležitá data (aby ne, když nečtou články obou autorů v Chipu), přičemž nepochopila, jak se věci mají – že jde jen o PGP. Celá věc kolem PGP (Pretty Good Privacy) tkví v tom, že zatím neexistuje algoritmus na rozlousknutí podpisu jako takového, za určitých okolností však lze ze zprávy vystrachat privátní klíč. Toho může někdo využít k tomu, aby vaším jménem třeba někoho urazil nebo za vás něco objednal.

Jak je to možné? Pokud se dostanete k souboru elektronického podpisu a jeho obsah nahradíte libovolnou posloupností binárních znaků a pokud následně zachytíte e-mail podepsaný za pomoci tohoto nového souboru, oba tvůrci vytvořili algoritmus, který dokáže útočnickovi předložit soukromý klíč uživatele. S jeho pomocí pak můžete podepisovat poštu za uživatele, a tím se za něj vydávat. Z toho plyne, že se máte více a pečlivěji starat o to, kam a komu dáváte svá privátní data. Nejlépe je nedávat je nikomu a držet si je ve svém šuplíku. A ten raději zamykat.

Omyl médií spočíval v tom, že prohlásila, že je prolomen klíč digitálního podpisu, což není pravda. Uvedená věc se týká jen systému PGP. A ještě k tomu klíče k podepisování, nikoli k šifrování. K tomu, aby došlo k získání privátního klíče, musíte najednou získat přístup k soukromému klíči uživatele a následně pak zachytit zprávu napsanou už s jeho “upraveným” obsahem. Nic víc – opakují, že se to “našeho” elektronického podpisu netýká vůbec a šifrování není ohroženo.

Vlastova a Tomášova činnost byla překotně odsouzena jako pokus o zviditelnění sebe sama i firmy ICZ, pro kterou pracují. Já se však domnívám, že záměrem bylo upozornit především na to, že “něco podobného” se může přihodit i jinde, ne jen v PGP. Nic víc. O to více mne překvapila unáhlená negativní hodnocení tohoto počínu od politiků, jako například Vladimíra Mlynáře i dalších “internet boys”.

Važme slova a nedělejme humbuk tam, kde bychom se měli spíše zamyslet. Jde přece o peníze na našich kontech, o naše soukromí, o věrohodnost toho, co sami napíšeme – nebo ne? To nám snad nemůže být jedno.

Amerika v nás

Všimli jste si toho, jak se přizpůsobujeme okolnímu světu? Amerika v nás. Všude, kde jsme se donedávna setkávali s hezkými a pěkně oblečenými lidmi, najednou potkáváme produkty pytlodní a bezpohlavní americké módní kultury. Zřejmě na tom začínáme být špatně, že nechceme ani s nikým komunikovat. Chceme být uzavřeni ve své ulitě, a pokud už musíme ven, mezi lidi, snažíme se co nejvíce schovat v davu, nevyčníknout, neupozornit na sebe. Proto si nasazujeme na nohy šedivé pytláky, na uši sluchátka, nosíme černé brýle, v ruce máme mobilní telefony, do kterých civíme a během pochodu po chodníku klepeme krátké textové zprávy.

Extrém jsem nedávno viděl v jedné kavárně. U několika stolů seděli pytlodní jedinci. Přišli se bavit. Všichni proto mlčeli a civěli na mobil a psali a psali. Co chvíli se ozvalo tutu-tutu a jeden (jedna) z nich ožil(a). Povídá: “Koukejte, píše mi Viki.” A začal(a) číst SMS. A za chvíli drtil(a) odpověď. U stolu neprobíhala žádná jiná komunikace. Posmutněl jsem. Jestli tohle je opravdu to, co nám přinášejí moderní komunikační technologie – v podobě absolutního odosobnění vztahů – tak se toho úplně otevřeně děším.

Hezké jaro! Ale netrapte se. Ne všichni přijali anonymní kulturu...

Milan Loucký, milan.loucky@vogel.cz