rola pro vývoj mobilních telefonů a uvedení nového operačního systému Windows Mobile určeného speciálně pro malá mobilní zařízení, PDA, inteligentní multifunkční mobilní telefony (tzv. smartphony) apod., které díky multimediálnímu vybavení budou moci nabízet nové možnosti. Praha se například v létě 2003 stala jedním z prvních evropských měst zapojených do programu CityTotal. V jeho rámci mohou zájemci využít turistické informační databáze na přenosných počítačích PDA s operačním systémem PalmOS nebo Microsoft Windows CE, které si mohou za poplatek i zapůjčit ve vybraných hotelech. Pro Prahu je k dispozici celkem 10 000 hesel. Také mobilní operátoři nasadili v létě 2003 masivní kampaně na podporu multimediálních zpráv MMS, aby přilákali uživatele na nové typy služeb.

Velkou pozornost věnují výrobci počítačů a mobilů multimédiím a zábavě. Všeobecně se předpokládá, že to bude jedna z klíčových oblastí, odkud si slibují zisky v příštích letech, zvláště v oblasti bezdrátových technologií. Objevily se první herní konzole umožňující simultánní propojení více hráčů pomocí technologie Bluetooth, v případě mobilů je to hlavně GPRS a Java. Rozbíhají se online hry pro javové technologie na mobilech, v této oblasti se rýsují šance i pro české vývojáře.

Kromě her se však začíná rozvíjet také tzv. edutainment, využití multimediálních technologií k výukovým účelům netradiční formou. Během roku 2003 vznikly v ČR zajímavé multimediální projekty, které se dočkaly uznání i v zahraničí. K nejvýznamnějším počinům v této kategorii patří vzdělávací programy a internetové portály pro školství, jako například Brána vědění či Škola online vyvinuté společností LangMASTER a projekt Indoš (Internet do škol), realizovaný ve spolupráci firem AutoCont a Český Telecom, který přes kontroverzní přijetí umožnil připojit všechny české školy k internetu.

Čas smutných rekordů

Rok 2003 však zdaleka nebyl pro oblast ITC procházkou růžovým sadem, kromě všeobecných problémů v důsledku nasycování trhu moderními technologiemi měl i své stinné stránky například v podobě několika rozsáhlých epidemií počítačových virů. Výrobci antivirových programů jej hodnotí jako vůbec nejhorší v dosavadní historii. Naprostá většina počítačů propojených do internetu byla postižena některým z virů jako Lovsan (Win32 Blaster), Sven.A, BugBear.B, Klez nebo SoBig a vývojáři antivirů se shodují, že to nejhorší počítačový svět zjevně teprve čeká. Viry se stávají čím dál dokonalejší a nebezpečnější, zejména kvůli enormní rychlosti svého šíření – zásahy virů SoBig a Blaster32, které využívaly bezpečnostních děr v systémech založených na technologii Microsoftu, dokázaly infikovat globální počítačové sítě světa během pouhých několika hodin.

O upozornění na jednu z nejzávažnějších zjištěných slabin v systému Microsoftu se zasloužili i čeští kryptologové a zároveň navrhli i způsob obrany. V případě úspěšného útoku hackerů na servery, vykazující tuto chybu (SSL/TLS serverů s možností postižení touto chybou jsou podle jejich údajů na internetu v celosvětovém měřítku zhruba dvě třetiny), by byla ohrožena bezpečnost dat například u online nákupů, elektronického bankovnictví a v určitých případech i u zabezpečeného přenosu poštovních zpráv.

Společnost Ernst & Young provedla celosvětový průzkum bezpečnosti informačních systémů (Global Information Security Survey 2003), kterého se zúčastnilo 1400 firem působících ve 26 průmyslových odvětvích. Výsledky studie ukázaly, že více než jedna třetina dotázaných firem je nedostatečně připravena na útok proti svému informačnímu systému a nedokáže jeho napadení odhalit. Pouze 34 % společností uvedlo, že splňuje předpisy v oblasti bezpečnosti informačních systémů. V České republice společnost Ernst & Young ve spolupráci s časopisem DSM a pod záštitou Národního bezpečnostního úřadu provedla na jaře minulého roku »Průzkum stavu informační bezpečnosti v ČR 2003« (dále jen »PSIB 2003«), kterého se zúčastnilo 380 organizací ze všech odvětví průmyslu i státní správy v ČR. Z výsledků vyplývá mj., že »v České republice pětina společností neprovádí analýzu zaznamenaných bezpečnostních údajů (logů) nikdy nebo jen občas. 56 procent společností provádí tuto analýzu pouze v případě potřeby, což je z hlediska efektivního monitorování naprosto nedostatečné«. Mezi nejčastější důvody výpadku bezpeč-