Nové low-endy

ČESTMÍR ŽÁK

■ V průběhu několika posledních měsíců se nám již začínalo zdát, že společnost Sony Ericsson na kategorii low-end u mobilních telefonů dočista zapomněla. Objevily se dokonce jisté spekulace, podle nichž měl Sony Ericsson produkci low-endů zcela zastavit.

O tom, že ani jedna z výše uvedených skutečností není tak docela pravdivá, nás přesvědčily dva zcela nové Sony Ericssony z kategorie těch nejlevnějších. Jedná se o modely, jež byly označeny jako J200 a T290. Oba do jisté míry vycházejí z předchozího low-endového modelu T230 – nabízejí podobné funkce a v designu přístrojů bychom při troše snahy našli příbuzné prvky. Primární úkol těchto Sony Ericssonů spočívá jednoduše v tom, aby uživateli zprostředkovaly základní sadu funkcí (hovory, SMS, možnosti personalizace, hry, budík apod.) v co možná nejpřívětivějším kabátu.

Jako první se podíváme na zoubek telefonu J200: je to přístroj klasické konstrukce s rozměry 101 × 43 × 19 mm a hmotností 74 gramů. Pasivní barevný displej se vyznačuje rozlišením 128 × 128 pixelů při 4 096 barvách, zamrzí však u něj absence podpory multimediálních zpráv MMS. Telefonní seznam pojme až 200 kontaktů, těšit se můžete také na čtyřicetihlasé polyfonní vyzvánění, infraport či stereofonní radiopřijímač (v podobě příslušenství).

Druhý v pořadí, Sony Ericsson T290, na trhu zřejmě vystřídá model T230. Jeho pasivní STN displej dostal od výrobce do vínku rozlišení 101 × 80 pixelů a schopnost odlišit až 4096 barev. Na rozdíl od modelu J200 dokáže T290 pracovat se zprávami MMS. V případě potřeby lze přístroj propojit s počítačem pomocí USB kabelu (existuje však i kabel pro sériový port). Při vyzvánění se T290 pochlubí přehráváním až 32 hlasů na-

jednou, mnoho uživatelů ocení rovněž funkci stereofonního FM rádia (opět v podobě příslušenství).

Oba zmíněné přístroje se dostanou na asijské trhy začátkem roku 2005, v globálním měřítku bychom se s nimi měli setkat v únoru nebo březnu 2005. Cena přístrojů pravděpodobně nepřekročí hranici 4 500 Kč.

Odkaz: *www.sonyericsson.com*

Začíná elektronický džihád

Na konci srpna letošního roku došlo v kybernetickém světě ke kroku, jehož okamžité dopady byly minimální, ale dlouhodobé důsledky mohou být dalekosáhlé. Některé arabské www servery totiž začaly své čtenáře informovat (a některé i vyzývat k aktivní účasti) o tom, že se na čtvrtek 26. srpna 2004 chystá „protiizraelský elektronický džihád" (tedy svatá válka).

Výzva se obracela na spřízněné hackery celého světa, aby v tento den „napadli izraelské webové zdroje". Podotýkáme, že se nejednalo o žádnou oficiální aktivitu, nýbrž o spontánní kampaň arabských hackerů, kteří tak ve světě informačních technologií přecházejí z oblasti pasivního boje (vytváření protiizraelských www stránek) do výrazně agresivnějšího způsobu odporu. Aktivita navíc svědčí o tom, že útočníci přikládají kybernetickému světu skutečně zásadní význam.

Už před dnem konání „akce" se nechal slyšet Eugene Kaspersky z bezpečnostní firmy Kaspersky Lab: „Neočekáváme, že by se tento den mohlo stát něco zásadního. Nebezpečí vidím spíše v použití termínu „elektronický džihád" a v tom, že má jít o agresivní útok. Pandořina skříňka byla otevřena. A dříve nebo později uvidíme důsledky."

Dnes už víme, že elektronický džihád úspěšný nebyl. Resp. počet a struktura zasažených stránek byly tak nízké, že se běžných uživatelů prakticky nedotkl – u nás ani kdekoliv jinde ve světě. Nebezpečí ale spočívá v tom, že byl vytvořen nebezpečný precedens. Některá z dalších podobných výzev už úspěšná být může a pro internet by mohla představovat velké nebezpečí. Internet byl totiž tímto aktem povýšen na plnohodnotné kolbiště srovnatelné s reálným světem.

Možností útoků je přitom několik a je otázkou, pro kterou se případní útočníci rozhodnou. Nejméně pravděpodobná je přitom pasivní forma odporu: založení vlastních www stránek nebo bojkot některých cizích webů. Tato varianta je totiž z hlediska ostatních účastníků internetu svým způsobem dokonce příjemná.

Další možností je útok proti vybraným cílům – stránkám či serverům na internetu. Takový útok lze provést podle několika různých scénářů. Buď přímým útokem proti příslušnému cíli, anebo jeho vyřazením z provozu v poslední době tak oblíbenou metodou DoS (Denial of Service), resp. DDoS (Distributed DoS). Nejnebezpečnější možností je útok proti celé infrastruktuře internetu metodou „padni kam padni" – útoky na root servery apod. V úvahu připadají i další možnosti – třeba infiltrace zevnitř (obtížné, nicméně ne nemožné a navíc velmi nebezpečné).

Mimochodem, význam internetu a ICT technologií obecně si začínají čím dále více uvědomovat nejen extremisté, ale také regulérní bezpečnostní složky. Přestože většina armád světa ohledně možnosti využití škodlivých počítačových kódů zarytě mlčí, několik informací podobného charakteru proniklo na veřejnost. Tchaj-wanská armáda prý má arzenál agresivních virů, které jsou schopné v případě potřeby napadnout čínské cíle. Oficiálně to přiznal Lin Chin-Ching, vysoký úředník na oddělení informatiky tchajwanského ministerstva obrany. Upozornil, že budou použity jako regulérní zbraně v okamžiku, pokud by Čína zaútočila jako první. Lin navíc přímo varoval Čínu před možnými provokacemi: „Tchaj-wanské armádní počítače jsou před nepřátelskou infiltrací chráněné velmi dobře. Ať tak či tak, v každém případě jsme schopni a připraveni zasáhnout."

Jak vidno, informační technologie mohou být prostředkem i cílem. Každopádně v srpnu 2004 vznikl nebezpečný precedens. Nad už tak dost pošmournou bezpečností internetu se stáhla další mračna.

TOMÁŠ PŘIBYL, AEC
www.aec.cz