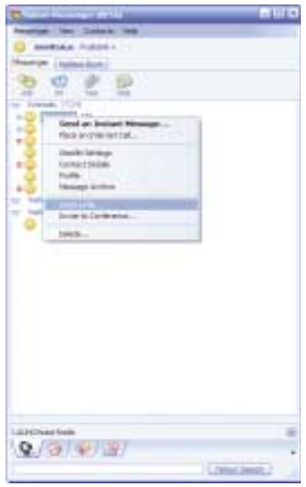
Nový patent Microsoftu

LENKA KARLÍKOVÁ

Společnost Microsoft se opět může pochlubit novým patentem, který tentokrát získala na hardwarová tlačítka. Tuto technologii používají převážně přístroje s PocketPC, tzv. press and hold. Jedná se o vícenásobné stisknutí hardwarového tlačítka u kapesních počítačů, čímž jsou vyvolány funkce, které jsou tomuto stisknutí přiřazeny. Namísto běžného stisknutí se tlačítko podrží déle nebo se stiskne vícekrát. Můžeme tak jednoduše například jedním stisknutím otevřít aplikaci, dvojitým klepnutím otevřít nový dokument nebo spouštět různé programy. Tato funkce se týká například aplikace Pocket Outlook. Patent se netýká stolních počítačů a serverů.
Odkaz: *www.microsoft.com*

Yahoo Messenger 6.0

LENKA KARLÍKOVÁ



Nejnovější verze komunikačního programu Yahoo Messenger nese označení 6.0. Nabízí veškeré funkce, které jsou pro programy tohoto typu nezbytné. Můžeme jeho pomocí chatovat, vyhledávat nové přátele podle přesně zadaných kritérií, účastnit se hlasových a video konferencí, vše také s pomocí webcamu, poslouchat internetová rádia, posílat soubory a URL nebo hrát hry. V nastavení aplikace lze měnit vzhled programu pomocí skinů nebo nastavit informování o nově příchozí poště do Yahoo schránky. Součástí programu Yahoo Messenger (2,7 MB), jenž lze používat i za firewallem, je kalendář, přístup k předpovědi počasí, ke zprávám, sportovním výsledkům a oblíbeným položkám nebo podpora telefonování přes internet. Nevýhodou může být registrace, která je nutná pro získání přihlašovacího jména a po instalaci také stahování dalších souborů potřebných pro běh aplikace.
Odkaz: *messenger.yahoo.com*

Windows MP 10

LENKA KARLÍKOVÁ

Společnost Microsoft zpřístupnila první beta verzi multimediálního přehrávače Windows Media Player 10 s kódovým označením Crescent. Na rozdíl od předchozích verzí je zaměřená především na oblast přenosných zařízení, avšak v tomto oboru má úspěšného konkurenta, společnost Apple. Windows Media Player 10 usnadňuje přenos souborů mezi PC a přenosným zařízením, dokáže také automaticky synchronizovat obsah u zařízení, které Windows rozpoznají jako další disk. Velká část funkcí ovšem bude použitelná až na nových audio- a videopřehrávačích, které by se na trhu měly objevit v druhé polovině tohoto roku. Windows Media Player 10 dále rozšířil širokou řadu souborů, které dokáže přehrávat. Nepřehrává však DVD video. K dalším novinkám patří pozměněné rozhraní, přepracovaný způsob organizace multimediálních souborů a nové možnosti získávání digitálního obsahu z internetu.
Odkaz: *www.microsoft.com*

Systém detekce neoprávněného průniku

Počítač připojený k internetu je na jedné straně úžasná věc. Na straně druhé si ale málokdy uvědomujeme, že toto připojení je obousměrné. Jinými slovy: data mohou do počítače nejen přicházet, ale také z něj odcházet. I bez našeho vědomí. Zabezpečení jednoho domácího počítače je přitom relativně snadným úkolem. S rostoucím počtem strojů zapojených v síti se jedná o otázku těžší a těžší. Zkrátka: čím dál tím více se rozšiřuje počet uživatelů internetu, který je jako komunikační prostředek nejenom účinným prostředkem a pomocníkem, ale také zdrojem a místem nebezpečného chování různých jedinců a okolností, které nás nutí před stále větší bezpečnostní ostražitostí.

A právě proto musíme dbát stejně jako v běžném životě o stále větší a „rafinovanější" zabezpečení, které nás ochrání nejenom před vnějším ohrožením, ale před v poslední době stále více diskutovaném tématu bezpečnosti uvnitř sítě – není tedy zapotřebí jenom ochrana na hlavních vstupech sítí. Dříve jako bezpečnostní prvek stačil firewall na vstupním bodě sítě do internetu, dnes se však musíme bavit i o personálních firewallech, které chrání jednotlivé počítače uvnitř sítě, a to jak před možným ohrožením dat na daných počítačích, tak i před útoky síťových červů uvnitř sítě.

Pro úplnou bezpečnostní komplexnost snad není nutné připomínat důležitost stále kontrolovat aktuálnost všech bezpečnostních záplat, které vydávají výrobci systémů a aplikací a které reagují na nově objevené nedostatky v jejich produktech. Avšak ani to již dnes nestačí a je nutné posílit bezpečnost o další úroveň a o to se snaží právě systém detekce neoprávněného průniku, neboli Intrusion Detection System (IDS).

Obecně se jedná se o systém, který integrujeme do sítě, popř. k operačním systémům tak, aby nás účinně a rychle informoval o situaci, která právě nastala v daném segmentu sítě. (Pozor, nejedná se o další zabezpečení typu firewall apod.) Systém IDS se začal využívat v minimálním množství již někdy v polovině devadesátých let 20. století, avšak teprve nyní přichází na trh řada produktů a systémů IDS nové generace, která detekuje neoprávněný průnik do sítě nejenom na základě databáze známých útoků, ale i na úrovni detekce anomálií v chodu sítí.

A jakým způsobem vlastně IDS funguje?

1. Detekce známých útoků (tzv. detekování na základě datových vzorků) – řešení IDS postavené na tomto systému pracuje s datovými vzorky, které definuji již známé útoky a hrozby. Toto řešení je téměř bezchybné z hlediska správnosti vyhodnocení útoku, proto jej jako základ řešení využívá většina IDS systémů, které se vyskytují na trhu informačních technologií.

2. Detekce anomálií – systém, který umožňuje detekovat odchylky od pravidel chodu sítě. Tento systém je schopen na rozdíl od systému detekce známých útoků detekovat nové, doposud v datových vzorcích nespecifikované útoky. Problém však nastává ve smysluplném nastavení pravidel normálního chodu sítě – tj. efektivně určit, že dané chování sítě je standardní a chtěné. Takto mohou vznikat falešné poplachy, které samozřejmě v případě, že jich vzniká mnoho, mohou degradovat celý systém IDS a snížit tak užitnou hodnotu celého systému.

3. Heuristická analýza – je další metoda, která funguje na bázi statistického vyhodnocování provozu. Metoda však má podobně jako u heuristické analýzy antivirových produktů náchylnost k falešným poplachům.

4. Vyhledávání výjimek z pravidel RFC – systém IDS kontroluje komunikaci a konfrontuje ji s pravidly komunikace definované v RFC. Toto řešení umožňuje vyhledávání anomálií na poli záměrné deformace komunikace mezi útočníkem a jeho potencionálním cílem.

Systémy detekce neoprávněných průniků se rychle stávají stejně nezbytnou součástí vybavení každého počítače připojeného k internetu, stejně jako antivirový program nebo firewall. *TOMÁŠ PŘIBYL, AEC www.aec.cz*