Opravdu bezpečná Windows Vista?

Bezpečí především

Již v minulém čísle jsme se zmiňovali, že klíčovým přínosem operačního systému Windows Vista nebudou „průhledná okna“ nebo animované náhledy, ale nové bezpečnostní prvky. Bylo už totiž na čase...

Text: Petr Kratochvíl, *petr.kratochvil@vogelburda.cz*

NOVÝ SERIÁL – DÍL 3: Náročná budoucnost

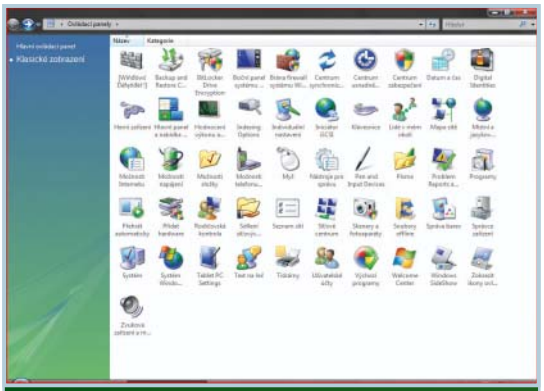
Ano, operační systém Windows XP byl z hlediska bezpečnosti opravdu spíše pro smích, ale zdá se, že Windows Vista mají šanci tuto reputaci změnit. Při testování beta verze jsem si více než kdy jindy uvědomil, že nejslabším prvkem zde bude člověk. Notoričtí odklikávači se totiž novými technologiemi zastavit nenechají. Ale nepředbíhejme.

User Account Control

Jedním ze základních problémů práce ve Windows byla nutnost používání „administrátorského přístupu“. Většina uživatelů si pro práci vytvářela účty s administrátorskými právy, což na jednu stranu minimalizovalo problémy s některými aplikacemi, na straně druhé vytvářelo ideální prostředí pro šíření virů a maximalizaci jejich destrukčního účinku. Ve Windows Vista je to jiné. Můžete být standardně přihlášeni jako „běžní uživatelé“ se všemi „bezpečnostními výhodami“ z toho plynoucími. Ve chvíli, kdy potřebujete vy (nebo libovolný program) provést akci vyžadující administrátorská práva, objeví se na obrazovce příslušné okno a vy se můžete rozhodnout, co dál...

Network Access Protection

Pokud počítač s Windows Vista zapojíte do sítě, které vládne server s Windows „Longhorn“, lze v takové síti provádět bezpečnostní „kouzla“. Windows Vista totiž obsahují „agenta“, který zabrání „potenciálně nebezpečným“ počítačům připojit se do zabezpečené sítě. Takový počítač může být například vpuštěn jen do sekce, kde si může stáhnout aktuální virové signatury, záplaty nebo service packy. Tato novinka by měla ulehčit především administrátorům, kterým doposud mohly jen „vstávat vlasy hrůzou na hlavě“ při sledování připojování nezabezpečených, nebo dokonce zavirovaných počítačů do sítě.



Možnosti: Nabídka ovládacího panelu se poněkud rozrostla...

Firewall

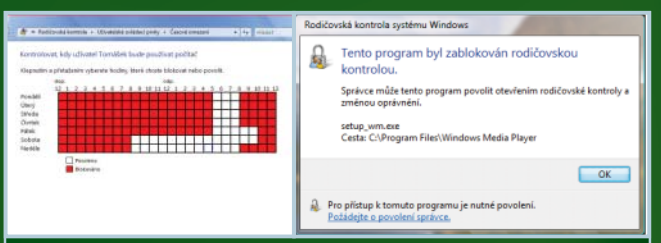
Tento důležitý bezpečnostní prvek znáte už z Windows XP a dalo by se říci, že na první pohled se od něj ani neliší. Ovšem opak je pravda. Prvním důležitým rozdílem je „obousměrná kontrola“. Firewall ve Windows XP hlídá totiž pouze cestu do počíta- →

PARENTAL CONTROL

Novinkou, která potěší především rodiče, je Parental Control (v české verzi „Rodičovská kontrola“). Ano, už ve Windows XP jste měli možnost alespoň částečně řídit a kontrolovat, co vaše děti na počítači provádějí, ale tato kontrola šla buď snadno obejít, nebo vás stála příliš mnoho peněz. Ve Windows Vista najde aktivní rodič vše, po čem kdy toužil.

1) Protokolování aktivit. Dozvíte se vše o spouštěných programech, navštívených webech nebo stažených souborech.
2) Časové limity. Vadilo vám, že vaše dítě hraje hry až do ranních hodin? Ve Windows Vista lze nastavit, kdy může kdo počítač použít a co na něm může dělat...
3) Kontrola her. Děsí vás krev stříkající po obrazovce, před kterou sedí desetileté dítě? Povolte mu pouze takové hry, které odpovídají jeho věku...
4) Blokování programů. Nejdokonalejším nástrojem je možnost blokovat (nebo povolit) konkrétní programy. Povolte dopoledne Word a Excel a nemusíte se bát, že vás ráno bude budit zvuk střelby...

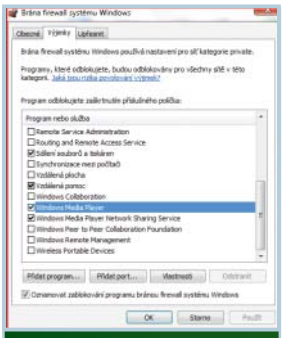
Uživatelská kontrola ve Windows Vista zkrátka nastavuje úplně jiné limity.



Denní rozvrh: Nastavte, kdy a jaký program může váš potomek používat.

če, což v době trojských koní a nebezpečného spywaru zdaleka nestačí. Firewall ve Windows Vista také umí blokovat aplikace (lze zakázat například P2P síť nebo instant messenger). Uživatelé, kteří čekali nástroj typu Kerio Firewall, budou zklamáni, ovšem většině běžných uživatelů už tento vylepšený firewall postačí.

User Account Control: Přístup k některým nastavením závisí na úrovni oprávnění.



Novinky: Firewall ve Windows Vista nabízí leccos nového...

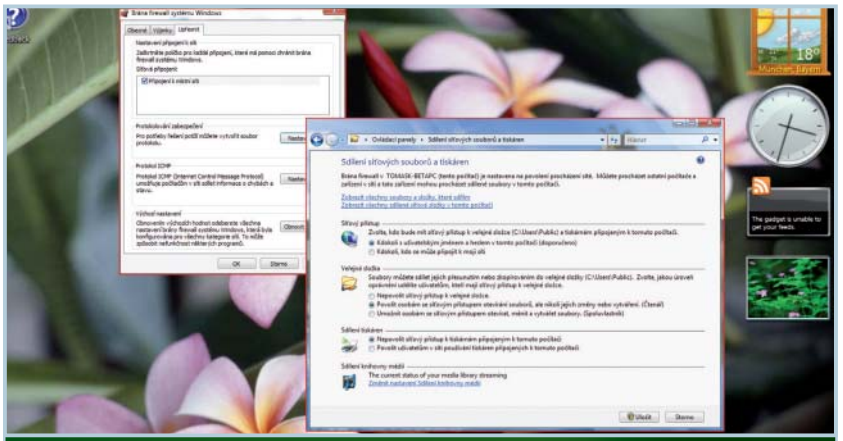
Fix My Settings: Jedním kliknutím nastavíte původní úroveň zabezpečení.

Protected mode

Určitě to zažila většina z nás. Při surfování v Internet Exploreru omylem či nevědomky stáhnete nenápadný programek nebo ActiveX komponentu a začnou se dít věci. Takto aktivovaný škodlivý software si už totiž může ve vašem systému dělat, co se mu zlíbí. A právě tento problém řeší ve Windows Vista tzv. protected mode.

V tomto modu se vám už při surfování v Internet Exploreru nic podobného stát nemůže. IE7 (a jím aktivované programy) totiž nemůže bez uživatelova souhlasu měnit uživatelská nastavení nebo pracovat se systémovými soubory. Protected mode povolí internetovým aplikacím ukládat pouze do složky Temporary Internet Files.

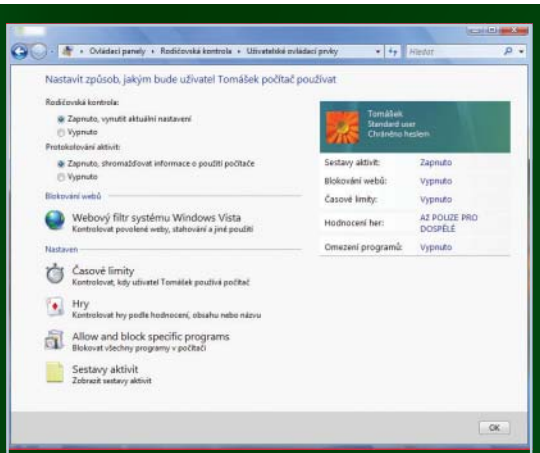
Co se týká zápisu do registrů nebo jinam než do povolené oblasti, pro tyto a podobné „rizikové činnosti“ vyžaduje systém příslušnou akci (schválení činnosti nebo administrátorské heslo). Zjednodušeně lze říci, že při surfování v „protected modu“ běží Internet Explorer odděleně od systému a ostatních aplikací.



Sdílení: Také sdílení souborů a tiskáren nabízí více možností...

Fix My Settings

Velké množství uživatelů instaluje a používá aplikace s implicitním nastavením. Pravda také je, že celá řada těchto aplikací vyžaduje pro svou plnou funkčnost nižší úroveň zabezpečení, než je nastavena v Internet Exploreru. V tomto případě je pak po použití takové aplikace důležité vrátit nastavení na původní bezpečnostní úroveň. A právě k tomuto účelu bude v Internet Exploreru 7 sloužit funkce Fix My Settings. Ta vás upozorní na surfování s rizikovým nastavením, bude vás varovat při změně bezpečnostních nastavení a ve finále umožní jedním kliknutím změnit bezpečnostní nastavení na původní hodnoty. ■ ■ ■



Rodičovská kontrola: Vše, po čem náročný rodič touží.

ZAŠIFROVÁNÍ DISKU

Zašifrování pevného disku, dosud známé pod kódovým jménem Secure Startup, se ve Windows Vista nazývá BitLocker Drive Encryption. Podle přání zašifruje kompletní obsah pevného disku a kontroluje systémový přístup při bootování, a to ještě dříve, než je vlastní operační systém zaveden. Aby to všechno fungovalo, musí PC disponovat TPM (Trusted Platform Module). Bezpečnostní čip je už pevně nainstalován na základních deskách některých nových PC.

Avšak BitLocker může používat i ten, kdo počítač kompatibilní s TPM nevlastní. Program totiž umožňuje uložit klíč na externí paměťové médium, například do USB paměti, nebo si počítač při zavádění systému Vista vyžádá heslo.

Tato funkce však není úplně nová. Už pod Windows XP bylo možno data zašifrovat „palubními“ prostředky. Rozdíl spočívá v rozšíření bezpečnostního záběru – data jsou zde chráněna už před vlastním bootováním. Hackeři tak nemají možnost přístupu ke chráněným datům ani oklikou přes jiný operační systém, například přes Linux zavedený z CD. Jak bezpečný BitLocker je, to naznačuje zpráva BBC. Podle ní britská vláda zvažuje požadavek na Microsoft, aby jí dal k dispozici „backdoor“, tedy jakýsi dodatečný klíč k BitLockeru. Něco takového vyžadují tajné služby a jiné úřady jen v případech, kdy se obávají, že by k chráněným systémům neměly žádnou možnost přístupu.