16. 8. 2004

Novinky v zabezpečení Windows XP Service Pack 2, 1. část

Všeobecně známým faktem je snaha Microsoftu zaměřit připravovaný opravný balíček Service Pack 2 pro operační systém Windows XP hlavně na zvratové změny v politice zabezpečení celého systému. Právě SP2 by měl přinést změnu od principu „zakaž si, co chceš“ na pracnější, ale bezpečnější formu „povol si, co je nutné“.

Po instalaci SP2 totiž budou ve výchozím stavu zapnuty všechny možnosti zabezpečení tak, aby se systém stal co nejméně zranitelným. Současně existující bezpečnostní rizika se Microsoft snaží eliminovat změnami ve čtyřech základních kategoriích:

- rozšířená ochrana sítě
- ochrana operační paměti
- vyšší zabezpečení emailové komunikace
- vyšší ochrana prohlížení webového obsahu

Součástí SP2 jsou také další rozšiřující aplikace (Direct X 9c, Windows Media Player 9), které jsou částečně upraveny také ve stejném duchu – zvýšení bezpečnosti a výkonu. Největší počet zdokonalení se v rámci SP2 však týká ochrany síťového provozu. V tomto článku se podíváme podrobněji na všechny inovované prvky a na to, jaké potenciální výhody mohou přinést do zlepšení současného kritického stavu počítačové bezpečnosti.

Vše se točí okolo Centra zabezpečení

Jedním z hlavních rizik pro celkovou počítačovou bezpečnost jsou domácí uživatelé. Právě pro ně musí být vše přehledné a částečně i „obrázkové“, což pravda někdy profesionální správci a zkušení uživatelé jen těžko vydýchávají.

Centrum zabezpečení připravuje jakousi centrální správu klíčových prvků zabezpečení – sleduje stav tří bezpečnostních funkcí: brána firewall, automatické aktualizace a antivirovou ochranu.

Centrum zabezpečení neustále kontroluje stav jednotlivých komponent a v případě zjištění nefunkčnosti některého ze subsystémů varuje uživatele pomocí ikony ve tvaru obláčku v pravé oznamovací části panelu se Start nabídkou. Pravda - tento prvek ve formě neustálého připomínání může „nesvědomité“ uživatele někdy dohánět k šílenství. Pro ostřílené profesionály, kteří vědí, co dělají, ale nabízí možnost deaktivace „na vlastní nebezpečí“.

U firewallu je kontrolována jeho aktivace na všechna aktivní síťová rozhraní, u automatických aktualizací je uživatel nucen nastavit pravidelnou kontrolu dostupnosti aktualizací a v sekci antivirů se kontroluje přítomnost antivirového řešení s čerstvou virovou databází.

Samozřejmě Centrum zabezpečení není vázáno pouze na produkty Microsoftu, ale nabízí otevřené rozhraní pro produkty třetích stran, pomocí kterého se tyto produkty informačně propojí s Centrem zabezpečení.

Ochrana proti virům - Antivirové řešení

V rámci SP2 pro Windows XP není dodáváno antivirové řešení, jak se v minulosti často proslýchalo. Nicméně Centrum zabezpečení přítomnost antiviru vyžaduje a jen tak se nenechá od svého záměru odradit.

Do okna Centra zabezpečení si Windows umí vytáhnout informaci o činnosti antiviru a o aktuálnosti virové databáze. Částečně tak možná tato funkce bude překrývat informace automatické aktualizace vlastního antivirového řešení – pokud vám antivir zestárne a nebudete ho mít zaktualizovaný, začne vás k tomu nutit všudypřítomná informační bublina v oznamovací oblasti Windows.

Nová verze Windows Update verze 5

Vlastnostem a novým prvkům v aktualizačním rozhraní Windows Update verze 5 jsme se již věnovali v **samostatném článku**.

Po instalaci Windows XP SP2 je tato verze aktualizačního portálu již vzata za standard a je tudíž používána ze všech přístupových míst (menu, Start nabídka, Ovládací panel atd.).

Aktualizace systému z Centra zabezpečení

Centrum zabezpečení zajišťuje propojení s automatickými aktualizacemi ručně dostupnými z Windows Update 5.

Ve výchozím stavu jsou automatické aktualizace povoleny, což by většině neznalých běžných uživatelů mělo při dostupnosti internetového připojení udržet počítač aktuální.

Pro znalejší je možno v konfiguraci nastavit frekvenci pravidelných kontrol nových aktualizací a hlavně režim fungování automatických aktualizací – od automatického stáhnutí na pozadí, přes pouhou notifikaci, až po úplné vypnutí, což samozřejmě Microsoft logicky tvrdě nedoporučuje.

Nepotřebné služby – vypnout!

S postupem času se v rámci zpětné kompatibility s Windows nese několik systémových služeb, které se používají v malé míře a současně mohou působit jako potenciální „bezpečnostní díra“. V rámci SP2 došlo proto k vypnutí několika systémových služeb. Vypnutím je myšlena jejich deaktivace v panelu Služeb – tj. v systému stále existují, jen jsou ve výchozím stavu vypnuty. V případě nutnosti jdou tedy individuálně zapnout.

Mezi vypnuté služby například patří Služba výstrahy nebo Kurýrní služba, která mohla být (bez zapnutého firewallu) zneužívána i k zasílání nevyžádaných reklamních zpráv.

Příští zastávka – ochrana sítí

Související v Databázi znalostí:
Firewall ve Windows XP
Firewall hlásí blokaci

Podle dlouhodobějších ohlasů testerů SP2 pro Windows XP je jeho nasazení znát převážně na starších nebo „nečistě“ napsaných aplikacích, které při provozu s novými systémovými restrikcemi mohou mít problémy. Na jednu stranu jde o další starosti, na druhou stranu se autoři aplikací budou muset zamyslet nad svými aplikacemi a přepsat je tak, aby neporušovaly bezpečnostní principy, které mohly v předchozích verzích působit chyby, nestabilitu a napadnutelnost celého systému.

V příštím díle tohoto článku se budeme věnovat změnám, které nový SP2 přináší do oblasti zabezpečení síťového provozu a celou sérii uzavřeme povídáním o nových vlastnostech Internet Exploreru a ochraně proti přetečení zásobníku a haldy.

Autor: Vít Jurásek

Zdroj: Živě