

Rekonstrukce Windows XP je tady!



Balík oprav a změn SP2 přichází do distribuce

PATRIK MALINA

Uživatelé Windows pamatují hodně změn a převratných okamžiků, ovšem uvedení balíku úhrnných oprav a změn po názvem SP2 pro Windows XP rozhodně patří mezi ty nejrazantnější. Máte-li pocit, že se vás to netýká, tak alespoň zbystřete: svůj omyl brzy rozpoznáte!

Pokud jste sledovali vývoj a přípravu balíku SP2 pro operační systém Windows XP, možná máte pocit, že jde o prokletí. Významný update pro všeobecně rozšířený klientský operační systém byl vyvíjen poměrně dlouho, jeho termín uvedení byl několikrát posunut či zrušen a testování se protahovalo v podobě dalších a dalších téměř hotových verzí. V průběhu srpna však vše konečně dospělo ke konci. Nebo spíše na začátek?

Nový SP2 znamená zásadní posun především v oblasti zabezpečení Windows XP. S mírnou nadsázkou lze říci, že se v této oblasti jedná o větší posun, než od Windows 2000 k verzi XP. Nežůstalo však zdaleka jen u bezpečnostní problematiky, neboť zajímavého vývoje se dočkaly i další komponenty, mezi nimiž určitě zmíníme třeba klientské rozhraní pro práci s bezdrátovými sítěmi nebo zařízeními standardu Bluetooth.

Ve světle nových skutečností, o nichž si budeme dále povídat, se vysvětlují i důvody věc-

ných odkladů: nové bezpečnostní technologie vyžadovaly důkladné testování a Microsoft se zřejmě obával v oblasti plošného firemního nasazení potíží při jakémkoliv drobné chybičce. Ale SP2 je definitivně skutečností, a proto se pojďme podívat na jeho funkce.

Distribuce

Bezprostřední skutečnost, jež bezesporu zaujme většinu uživatelů, bude jistě samotná velikost distribučního balení SP2. Pokud jste připojeni k internetu tradičním vytáčeným připojením či jinou obdobnou variantou komunikačního kanálu, v podstatě můžete na on-line updatování zapomenout. Při bližším ohledání totiž zjistíte, že kompletní instalace totiž obsahuje zhruba 200 MB zdrojových dat, což jistě není jen tak ke stažení. Napadá-li vás v této souvislosti něco v tom smyslu, že se Microsoft zbláznil a vyměňuje snad polovinu operačního systému, pak nejste až tak daleko od jádra věci. Řada poměrně hlubokých kon-

cepčních zásahů si skutečně vyžádala záměnu velkého počtu systémových komponent a různých nástrojů, takže objem přenášených dat je značný. V době finální přípravy článku byla distribuce SP2 dostupná v podstatě pouze pro firemní nasazení formou síťových instalací, koncoví uživatelé očekávali každou chvíli uvolnění aktualizovaných souborů ve formě tradiční služby Windows Update. Pro úplnost dodejme, že je pochopitelně možné upravit původní instalační zdroj Windows XP (typicky v síťovém distribučním adresáři) pro použití při nových instalacích pomocí technologie tzv. slipstreamu, čímž získáte obcerstvenou instalační variantu. Z uživatelského hlediska se zavádění SP2 v podstatě rovná upgradu na nový operační systém a probíhající procedury to také opticky výrazně připomínají.

Křížácké tažení za bezpečností

Jedním z hlavních motivů, jenž přivedl společnost Microsoft k výsledné podobě balíku SP2, byla přes veškeré úsilí stále se zhoršující „všeobecná bezpečnostní situace“ uživatelů Windows XP. Problém nespočíval ani tak v tom, že by bylo potřeba přidat spoustu nových komponent a funkcí, i když se tak nakonec stalo. Potíž byla spíše toho druhu, že uživatelé existující mechanismy ignorovali či nedokázali účinně používat a výsledkem byly nekontrolovatelné záplavy „červových“ epidemií a podobných katastrof. Na první pohled vypadá, že tvůrcům Windows leží ochrana domácích uživatelů velmi na srdci, ovšem realita bude zřejmě prošíst: zmíněnou laxností při definování bezpečnostních pravidel totiž v důsledku trpěli především velcí firemní zákazníci, jejichž jinak slušně ošetřené počítače se

zkontrolovat, zda služba stále běží a případně ji restartujte.

V grafickém rozhraní Security Center nalezne uživatel přístup ke konfiguraci nejdůležitějších částí z pohledu ochrany počítače. Z tohoto místa je přístupné ovládání osobního firewallu, definování chování služby Automatic Update pro stahování aktuálních záplat, dále lze detekovat instalovaný antivirový software a přistupovat ke konfiguraci internetového zabezpečení. Samozřejmě jsou odkazy na stránky s nápovědou a on-line propojení na zpravodajství o aktuálních hrozbách na internetu.

Reinkarnace osobního firewallu

Poměrně zajímavým vývojem prošla součást, na níž jsme narazili již v „běžném“ provedení Windows XP. Ochraný prvek pro kontrolu síťového provozu pod názvem Internet Connection Firewall je standardní součástí základní instalace systému již od počátku a dokáže odvést dobrou práci. Přesto si tvůrci systému velmi dobře uvědomovali jeho omezení, související především s minimálními možnostmi konfigurace, což stále a neomylně vedlo uživatele k používání jiných programů tohoto druhu.

V SP2 se osobní firewall převtěljuje do nástroje s řádově lepšími možnostmi pro správu a je vybaven opravdu žádoucími nastaveními při ochranné komunikačních toků. Zásadní je již změna režimů jeho běhu, ačkoliv vypadá na první pohled nenápadně. Uživatel může ochranu buď úplně vypnout, druhou možností je pak zapnutí s akceptováním ručně nastavitelných výjimek (dále je ještě zmíníme). Třetí variantu představuje opět spuštěný firewall, ovšem s vyloučením všech definovaných výjimek. Režim poslední, nejpřísnější, je především určen pro situace, kdy se třeba s mobilním počítačem ocitnete v cizí síti.

Právě správa výjimek pro připojení je další znatelnou novinkou. Zde se tvůrci přiblížili konkurenci a nabízejí možnost přiřadit povolení pro komunikaci na bázi aplikace, což uživatelům značně usnadňuje orientaci v problému. Ale nežůstalo jen u lepší ovladatelnosti – definice pravidel na aplikační bázi totiž přináší zcela zásadní principiální změnu hluboko v nitru firewallu. Dřívější způsob nastavení výjimek pomocí čísel portů byl totiž těžko použitelný v situaci, kdy si aplikace otevírala více kanálů s neočekávanými parametry. V nové podobě firewall otevírá porty dynamicky, podle požadavků aplikace, již jste toto právo přiřadili. Na první pohled nenápadná, ale v praxi vynikající proměna. Kromě přednastavených služeb pro sdílení souborů a tiskáren či terminálovou vzdálenou plochu je možné pochopitelně přidávat další uživatelské definice, založené jak na konkrétní aplikaci, tak na tradičních číslech portů protokolové sady TCP/IP.

Řídíme zabezpečení

Z pohledu správy operačního systému je zásadní novinkou komponenta Security Center, jež poskytuje centrální rozhraní pro konfiguraci zabezpečení a sledování běhu jednotlivých komponent. Nejedná se jen o pouhé vylepšení grafického uživatelského rozhraní – na pozadí tohoto Bezpečnostního centra stojí samostatná služba operačního systému, jež průběžně hlídá ostatní součásti a v případě nesrovnalostí reaguje grafickým upozorněním podle aktuálního nastavení. Právě tato služba je zodpovědná za zobrazení ikony v prostoru systémové lišty vpravo dole „vedle hodin“, a pokud by tedy na počítači došlo k náhlému „zmizení“ ovládacího bezpečnostního centra, zkuste

Právě s výběrem určitých sítí souvisí i další zásadní vylepšení, jímž je přiřazení bezpečnostních pravidel určitému definovanému síťovému rozhraní. Pokud váš počítač disponuje více síťovými adaptéry, několika možnostmi připojení internetu pomocí vytáčené linky či připojením do firemní sítě prostřednictvím VPN, lze působnost firewallu jednoznačně vymezit na potřebná rozhraní.

Z dřívějších možností pochopitelně zůstalo k dispozici podrobné protokolování událostí a detailní nastavení průchodu služebního protokolu ICMP pro kontrolu konektivity, příjemnou novinkou je pak pro běžného uživatele volba „Restore Defaults“, dovolující při narušení konfigurace navrátit firewall do „továrního“, výchozího nastavení.

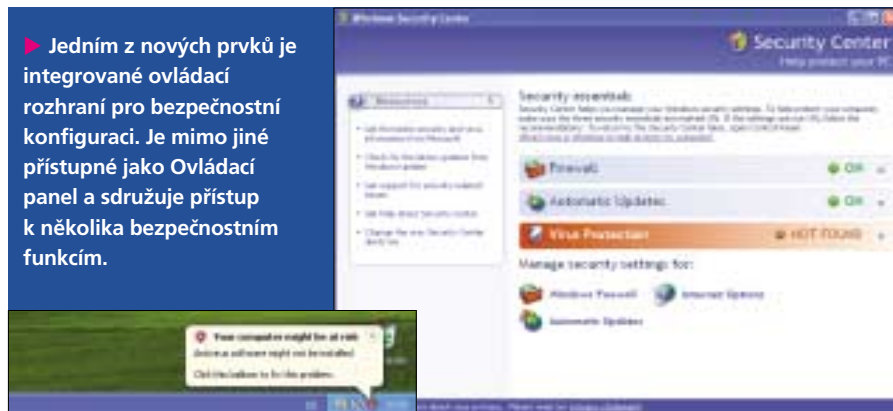
Na závěr doplníme informaci o vlastnosti, která je o to důležitější, o čem méně je vidět. Nové provedení firewallu totiž při startu operačního systému nabíhá velmi časně a nedává síťovým rozhraním čas pokusit se o nechráněnou komunikaci, což dřívější verze takto důsledně neuměla. Neznatelně, ale zásadní vylepšení!

Bojujeme s víry

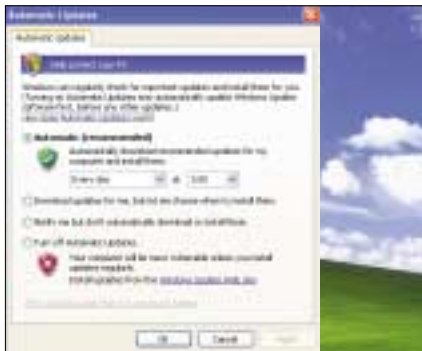
Protože tento titulek možná vzbudil velké naděje či naopak obavy, je potřeba jej uvést na pravou míru. V první řadě, Microsoft neimplementoval do systému žádný vlastní antivirus, ani nevybral pro tento úkol některého z dodavatelů. V rozhraní Bezpečnostního centra je však k dispozici položka, jež dovoluje kontrolovat běh této životně důležité součásti a indikovat nefunkčnost či nepřítomnost na počítači. Co tedy tvůrci SP2 připravili, je rozhraní pro antivirové aplikace, jež se mohou takto napojit na „centrální zpravodajství“ a podávat informaci o své práci. Pomocí tohoto rozhraní je podporováno připojení nejběžnějších antivirových programů a jejich výrobci jistě budou nadále na této vymoženosti pracovat.



Velkým strašidlem byly vždy pro MS Internet Explorer funkční komponenty typu ActiveX. Nové rozhraní dovoluje všechny prvky explicitně ošetřit, resp. jim zabránit v činnosti, a v případě pokusu o automatické stahování dojde k jeho podchycení.



Jedním z nových prvků je integrované ovládací rozhraní pro bezpečnostní konfiguraci. Je mimo jiné přístupné jako Ovládací panel a sdružuje přístup k několika bezpečnostním funkcím.



▲ **Stále agresivnější internetové prostředí přináší agresivnější odezvu: nastavení automatických updatů doznalo jak kosmetických, tak funkčních změn, jež směřují k nekompromisnímu bezobslužnému záplatování.**

Štít pro webovou komunikaci

Zajímavého vylepšení se v SP2 dočkala i další kmenová součást Windows XP, prohlížeč Internet Explorer. Ačkoliv je již dnes nabitý všemožnými pravidly pro omezení potenciálních rizik, dosud chyběla jinak všeobecně používaná a uživateli ceněná komponenta pro blokování pop-up („vyskakovacích“) oken. Konfiguraci této funkce naleznete v ovládacím panelu Internet Options v dolní části na kartě Privacy. Kromě toho, že filtr lze úplně vypnout, je pochopitelně možné definovat úroveň ochrany, což učiníte po stisknutí tlačítka Settings. Nejprísrnější režim blokuje vše, co se pokusí o otevření i po uživatelské výslovné pokusu, prostřední volba hlídá především automatická okna a nejbenevolentnější varianta dovoluje úplné otevření automatických oken, ovšem jen ze stránek označených jako bezpečné. Samozřejmě i v případě této funkce lze definovat seznam výjimek a označit tak stránky, které budou automaticky důvěryhodné. Protože práce s pop-up okny je často žádoucí, Internet Explorer je samozřejmě vybaven novým prvkem grafického rozhraní, pomocí něhož lze zablokovaná okna výslovně povolit a otevřít. To vše v režii uživatele.

Další změny v Internet Exploreru jsou o něco méně nápadné, avšak také poměrně důležité. Přeprogramovány byly dialogy pro stahování souborů a především pro spuštění vzdálených skriptů či programových komponent ActiveX. Tvůrci zapracovali do prohlížeče nové rozhraní pro správu „odsouhlasených“ či „zamítnutých“ programových kódů, důsledně lze sledovat digitální podpisy těchto komponent a samozřejmě kdykoliv dodatečně konfiguraci upravit.

Bez updatu ani ránu

Nezbytným základem bezpečnosti systémů Microsoftu zůstává průběžná aktualizace operačního systému pomocí bezpečnostních záplat. Výrobce si je této skutečnosti plně vědom a aby uživatel ještě těsněji přiblížil k provádění pravidelných aktualizací, bez nichž může dojít skutečně k fatálním situacím, přeprogramoval i tuto součást, zná-

mou jako Windows Update, v případě firemního nasazení pak součást pokročilejší služby SUS (System Update Services). V novém Bezpečnostním řídicím centru najdete související volby pod označením Automatic Updates.

Služba je schopna zajistit několik úrovní ošetření operačního systému. Nejdůležitější variantou je automatická detekce nových záplat pro váš systém, jejich bezodkladné stažení z internetu a následná instalace. Tuto operaci lze načasovat buď v každodenním cyklu, nebo v režimu „jednu týdně“, samozřejmě s určením hodiny během dne. Druhým, mírnějším režimem je automatická detekce a stažení záplat, ovšem s vyčkáváním, až uživatel potvrdí instalaci. Třetí funkční konfigurací je detekce dostupnosti updatů na internetové stránce, bez downloadu či instalace. Větší benevolence neexistuje – poté lze již službu pouze zcela odstavit mimo provoz. V případě potřeby lze z téhož grafického rozhraní samozřejmě aktualizaci zavolat interaktivně, v daný okamžik, tak jak jsou důslední uživatelé zvyklí z dřívější verze.

Právě v oblasti automatických bezpečnostních updatů se výrazně uplatnila výše zmíněná taktika pasivní ochrany systému i při laxním přístupu uživatele. Komponenta je ve výchozí podobě nastavena tak, aby systém žádal a prováděl prostřednictvím funkčního internetového připojení pravidelné sledování výskytu nových záplat a následnou instalaci po úspěšném stažení. Záměru odpovídá i grafická interpretace těchto nastavení: pokud funkci budete vypínat, samozřejmě bude následovat opakované neodbytné varování a „šikanování“ nedůsledného uživatele, s cílem



▲ **Spolu s řadou nových funkcí přichází i upravená administrátorská šablona pro mechanismus doménové správy Group Policy. Nových položek je celá řada a rozhodně stojí za vyzkoušení.**

přimět jej alespoň občas k průběžné kontrole a případnému zavedení opravných záplat. Ne že by celou službu nebylo možné zcela pozastavit, ovšem pokud zůstane v běhu, svou „hlídaci“ a povzbuzovací funkci zastane velmi dobře. Nutno dodat, že z hlediska uživatelské čitelnosti probíhá updatování transparentně a celkem bezbolestně.

Komunikujeme bezdrátově

Výrazný důvod k radosti rozhodně mají uživatelé bezdrátové komunikace, a to jak vyznačiči Wi-Fi

přenosů, tak příznivci krátkodosahové technologie Bluetooth. Již v průběhu uvolňování postupných testovacích verzí SP2 bylo patrné, že klientské rozhraní pro práci s Wi-Fi sítěmi dozná zajímavých změn. Výsledek je rozhodně příjemným překvapením. Již samotná konfigurace potřebných parametrů pro zprovoznění bezdrátových přenosů je snazší díky zcela novému průvodci, při jehož použití možná oceníte i jednu nenápadnou drobnost: poprvé zadané parametry je možné okamžitě uložit na externí médium (USB paměťový disk) a jak asi správně tušíte, pouhým přenosem na další počítače a opětovným zavoláním průvodce tak můžete následně snadno konfiguraci opakovat. Do zcela nové podoby se přerodilo ovládací rozhraní dostupných bezdrátových sítí, jež před SP2 v podstatě téměř neexistovalo. V současném provedení máte k dispozici kvalitní přehled možností připojení, konfigurace je po ruce a je tedy zase o důvod méně instalovat ne vždy spolehlivý a stabilní proprietární software výrobců bezdrátových síťových karet.

Příjemného překvapení se dočkali také uživatelé zařízení pro komunikaci pomocí Bluetooth. Funkcionalita, již jste dříve museli opět zajišťovat povětšinou externí aplikací od výrobce příslušného hardwaru, je nyní dostupná přímo v klientském nástroji ve Windows. Tento ovládací panel je k dispozici od chvíle, kdy nějaké zařízení Bluetooth připojíte, a nabídne vám přehled dostupných komunikačních partnerů stejně jako možnost nastavit základní parametry pro spojení, včetně ochrany sdíleným klíčem. Uživatelsky velice snadné je pak přenášeni souborů či přímá správa vzdálených zařízení pomocí přehledného grafického rozhraní.

Pro každého něco

Ačkoliv z předchozích odstavců by se mohlo zdát, že změny v SP2 se týkají jen síťování či bezpečnosti, zdaleka tomu tak není. Přestože bezpečnostní problematika byla již rozebrána důkladně, čekají na uživatele i jiné zajímavosti. Třeba majitelé varianty Windows XP Tablet PC Edition budou možná

docela překvapeni, že po aplikaci balíku Service Pack se bude jejich systém rovnou tvářit jako Windows XP Tablet PC Edition 2005! K nejzásadnějším změnám v tomto případě došlo u nástrojů pro přímý vstup informací pomocí dotykového panelu, takže uživatelé mohou ocenit flexibilnější chování kontextových vstupních dialogů či vylepšené možnosti při optickém rozpoznávání rukou přímo zapisovaných textů. Zkrátka nepřijdou ani fanové multimediálních aplikací. Jako součástí SP2 se totiž objeví také úhrnná sada komponent, jež zčásti přišly již dříve, avšak takto pohromadě dosud distribuovány nebyly. Nedílnou součástí systému se tak stává dříve volitelný Windows Media Player 9, který možná již nějakou dobu používáte, do aktuální verze 2004 se též promění Windows XP Media Center Edition.



▲ **Podpora bezdrátových sítí byla zásadně vylepšena, a to nejen v podobě nového ovládacího panelu pro vyhledávání a konfiguraci dostupných zdrojů. Samozřejmostí je co možná nejsilnější zabezpečení.**



▲ **Zajímavou drobností při použití průvodce pro konfiguraci bezdrátové sítě je možnost definované údaje snadno přenášet na další stroje pomocí USB paměťového zařízení.**

Ve firemní síti

Tak významná proměna klientského operačního systému, jaká se odehrává v SP2, pochopitelně nemohla zůstat bez odezvy na straně nástrojů a řešení pro korporátní implementace. Kromě důsledného testování, jež mělo zajistit co možná nejhladší nasazení balíku na klientské počítače v rozsáhlejších sítích, samozřejmě tvůrci připravili též prostředky pro centrální řízení nově zavedených funkcí.

Za předpokladu, že řízení větší sítě je postaveno na službě Active Directory, tedy prostřednictvím doménové technologie Windows 2000 či Windows 2003 Server, se nám nabízí optimální mechanismus pro centralizované ovládání klientských nastavení pomocí mechanismu Group Policy. Spolu s SP2 byla připravena nová administrativní šablona, jež zahrnuje bohatou škálu nastavení nových funkcí pro zabezpečení a dovoluje tak ovládat vymoženosti SP2 pomocí osvědčené technologie. Z pohledu správce je asi nejsnazším postupem pro přidání administrativních šablon cesta možná trochu překvapivá: po instalaci SP2 na první, třeba testovací stroj

s Windows XP, stačí na tomto počítači otevřít novou konzoli MMC, přidat snap-in Group Policy s odkazem na potřebnou doménovou politiku a otevřít ji pro editaci. V tuto chvíli dojde, pokud je doménová struktura ve výchozím nastavení, k automatickému updatu administrativních šablon na doménovém řadiči a postupně při replikacích v celé síti. Pokud je takové chování pro vás naopak nežádoucí, nezapomeňte funkci zakázat prostřednictvím parametru v administrativní šabloně v položce Group Policy.

Z hlediska samotné volby parametrů jsou jednotlivé novinky rozestry napříč šablonami, takže nenajdete nic jako „SP2 na jednom místě“. Obohaceny byly především parametry pro automatický update, ve složce Networks najdete zcela novou podsložku Windows Firewall. Ta obsahuje dvě identické kolekce nastavení, určující chování klientských počítačů a jejich firewallů v závislosti na tom, zda je uživatel přihlášen do domény či spouští stroj pouze pod lokálním nedoménovým účtem. I tato koncepce je opravdu velmi zdařilá.

Máme se bát?

Instalace „rekonstrukčního“ balíku pro Windows XP rozhodně představuje výrazný krok vpřed. Jak uživatelé domácích počítačů, tak administrátoři rozsáhlých firemních sítí v něm oprávněně mohou očekávat a spatřovat další posun v možnostech zajištění odolnosti systému proti nežádoucím kalamitám, ovšem jako vždy v případě, že nové funkce budou nakonfigurovány a zapnuty.

Na druhou stranu tak zásadní kúra, jakou vaše počítače projdou, nemůže zůstat zcela bez následků, a na tuto skutečnost je potřeba se připravit. Pomineme-li potenciální chyby a nefunkčnosti, s nimiž koncový uživatel bojuje těžko, stále tady zůstává nezanedbatelný fakt, že některé důvěrně známé aplikace či rozhraní Windows se najednou budou chovat neočekávaně a překvapivě. Nechtě se tedy pohybujete v domácím či firemním prostředí, věnujte alespoň minimální úsilí seznámení s novinkami, jež přicházejí, a počtěte se či další uživatele o některých funkcích, jež např. výrazně ovlivňují chování Internet Exploreru. Nenastanou-li jiné potíže, může být hledání dobrého soužití s novými Windows XP současně seznámením s novými a zajímavými funkcemi.

P. S.: Na sklonku prázdnin je SP2 v mnoha firemních sítích nekompromisní realitou. Uživatelé i správci mohou doceňovat nové vymoženosti, na druhou stranu se třeba objevily první problémy při komunikaci s některými typy přenosných počítačů. Na webových stránkách se též objevují první články o tom, jak obelstít některá zbrusu nová bezpečnostní nastavení Internet Exploreru. Výrobce kontruje prohlášením, že na všechny scénáře zkrátka systém nepamatoval a cíle vývojářů zahrnovaly jen určitou skupinu problémů. Prostě a jednoduše řečeno, Windows XP SP2 jsou opět krokem vpřed, ovšem ani tentokrát to zákonitě nemohl být krok poslední.

4 0497/OK □