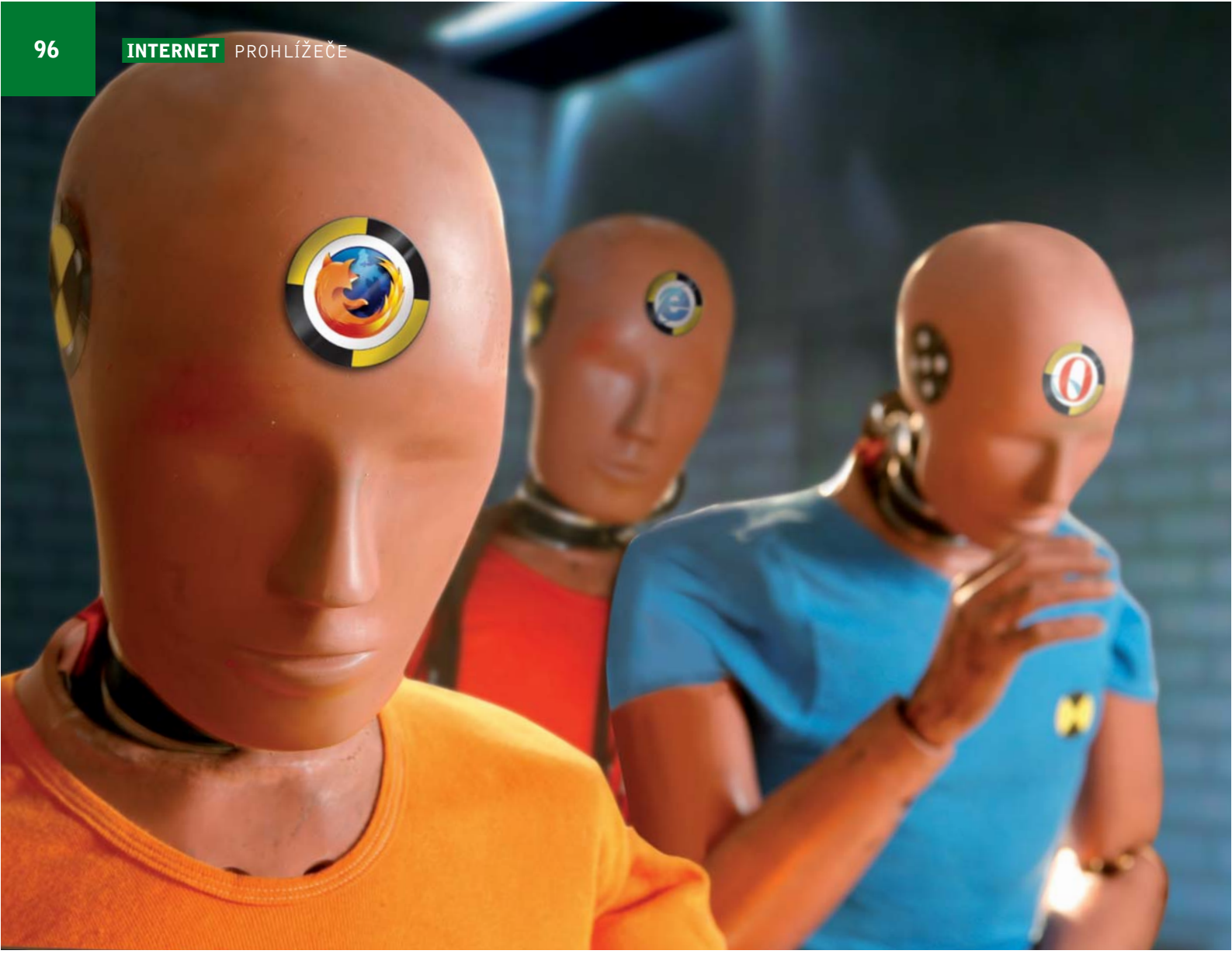


Jak (ne)bezpečné jsou nové internetové prohlížeče?

Nové prohlížeče jsou tu – a s nimi i nové hrozby. Otestovali jsme Internet Explorer, Firefox a Operu, abychom zjistili, který z prohlížečů opravdu chrání uživatele před hijackery, spywarem a hackery. *Valentin Pletzer, Petr Kratochvíl, petr.kratochvil@chip.cz*

V tomto článku najdete

Kde jsou peníze, tam jsou i podvodníci. Čím dál tím více lidí nakupuje na internetu nebo přes internet spravuje svůj bankovní účet – a v přímé úměře s tím stoupá i internetová kriminalita. Žádný program přitom nemusí čelit takovému náporu jako právě internetové prohlížeče.

OBLASTI ÚTOKU

Bezpečnost především

Podle firmy Symantec je přes 80 procent všech internetových útoků zaměřeno na internetovou stránku nebo prohlížeč. O tom se ostatně v minulosti nejednou

CHIP Shrnutí:

V přímém srovnání zvítězil v testu zabezpečení Firefox, v těsném závěsu za ním následuje Opera. Na posledním místě skončil Internet Explorer, což ovšem neznamená, že nestojí za nic. Vzhledem k tržnímu podílu 87 % je totiž na mušce hackerů nejvíc ze všech prohlížečů. Přesto Microsoftu proklouzlo pár mezer v zabezpečení i do nové verze 7.

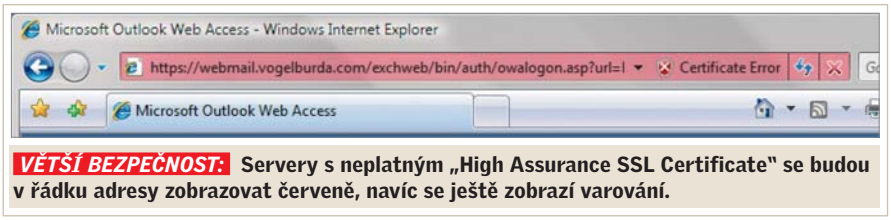
přesvědčili především uživatelé Internet Exploreru. S novou verzí IE7 by se tato situace měla zlepšit a pozadu nezůstali ani ostatní výrobci. Zajímalo nás proto, prostřednictvím kterého prohlížeče můžete surfovat opravdu bezpečně. Nechali jsme proti sobě nastoupit Operu 9.10, Firefox 2.0 a Internet Explorer 7. Stejné kandidáty jsme prověřili i v posledním loňském Chipu. Tehdy jsme se zaměřili především na „uživatelský pohled" a hledali jsme nejlepší browser pro obyčejného surfaře. Tentokrát se na nejpopulárnější prohlížeče důkladně podíváme z hlediska bezpečnosti.

HIJACKING

Obrana proti útokům na prohlížeč

Největším problémem prohlížečů jsou škodlivé kódy, které se hackeři pokoušejí propašovat do počítače přes internetové stránky – především přes spyware a adware. Většinou pak není cílem útoku samotný prohlížeč, ale některý ze zásuvných modulů (doplňků nebo plug-inů). Adware se většinou snaží přimět uživatele k nainstalování takového doplňku, zatímco spyware obvykle proniká přes mezery v zabezpečení v už nainstalovaných doplňcích. Oběť útoku pak ztrácí kontrolu nad prohlížečem a často i nad celým operačním systémem.

Abychom otestovali, jak prohlížeče dokáží takové útoky odvrátit, vypustili jsme na ně trojského koně CoolWebSearch. V IE se bez problémů uhnízdil a vpustil další škůdce. Ti se pak aktualizovali tak rychle a tak často, že náš antivirový program neměl šanci odhalit je podle signatury. Nezbylo nám nic jiného než přeinstalovat celá Windows. Firefox a Opera se podle očekávání ubránily, protože bez ovládacích prvků ActiveX jsou tyto prohlížeče proti útokům tohoto typu imunní.

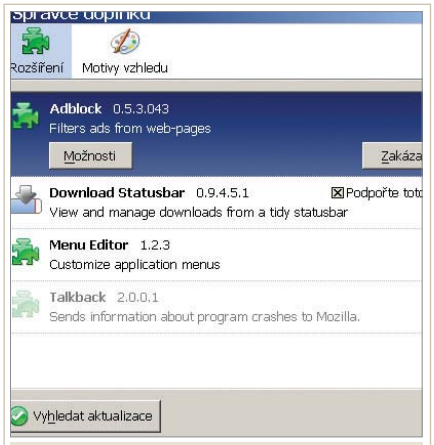


VĚTŠÍ BEZPEČNOST: Servery s neplatným „High Assurance SSL Certificate" se budou v řádku adresy zobrazovat červeně, navíc se ještě zobrazí varování.

Microsoft se s ovládacími prvky ActiveX, náchylnými k útokům, bohužel nerozloučil. To je ovšem fatální chyba, protože na rozdíl od javovských appletů mají programy ActiveX stejná práva jako prohlížeč. Ještě i ve Windows XP tak mají přístup ke kompletnímu operačnímu systému. Změna se chystá teprve se systémem Vista. Jediným plusem tak je, že IE instaluje ovládací prvky už pouze se souhlasem uživatele. Navíc se pak dají zakázat a vymazat prostřednictvím jednoho centrálního rozhraní.

Doplňky můžete samozřejmě zakazovat a mazat i ve Firefoxu a v Opeře, kde jsou navíc většinou programovány v JavaScriptu. I ten může být za určitých okolností škodlivý, ale zásahy do operačního systému jako takového jsou prakticky vyloučeny. Uživatelé Opery se znalostmi programování mohou často zneužívané funkce JavaScriptu dokonce zakázat.

O tom, co se stane, když prohlížeč spustí příkazy JavaScriptu bez jakéhokoli filtru, jsme se přesvědčili v našem testu. Vytvořili jsme HTML stránku s typickými prvky podvodných stránek. Pomocí kódu s několika málo řádky jsme pak nechali zmizet adresu stránky v prohlížeči a nahradili jsme ji adresou



PLNÁ KONTROLA: Ve všech prohlížečích se dají nežádoucí doplňky a moduly kdykoli zakázat nebo vymazat.

www.citibank.com na stavovém řádku. Firefox a Internet Explorer se nám tak podařilo bez problémů přelstít!

PODVODNÉ STRÁNKY

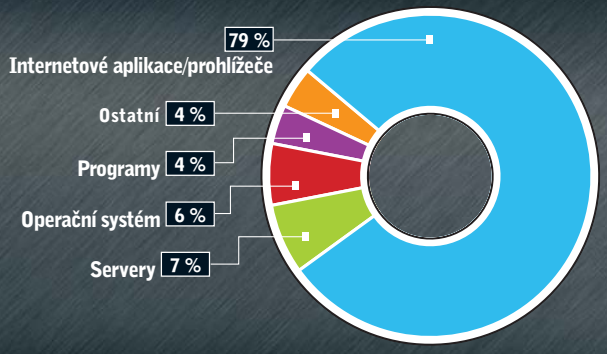
Nová ochrana proti on-line podvodům

Finta, kterou používají on-line podvodníci, je stále stejná. Navedou uživatele na falešnou internetovou stránku a vylákají z něj hesla, údaje o kreditní kartě, PIN nebo jiné přístupové údaje k bankovnímu účtu. Nejlepším místem ochrany proti takovým útokům by měl být přímo internetový prohlížeč, proto by před návštěvou potenciálně podvodných stránek měl varovat zabudovaný filtr podvodných stránek, jak ho známe z různých balíků bezpečnostních aplikací.

Ochranu proti podvodným stránkám už nabízejí všechny z testovaných prohlížečů. Opera svým uživatelům tuto funkci nabídla až od verze 9.10. V našem testu fungovala tato ochrana u všech prohlížečů spolehlivě. Prohlížeče poznaly všechny náhodně vybrané podvodné stránky a zobrazily jasné a nepřehlédnutelné varování. Pokud je ochrana aktivní, prohlížeč pomocí heuristické analýzy ověřuje každou načítanou stránku, zda neobsahuje rysy typické

Na co hackeři útočí

Přímé útoky na počítač jako takový jsou na internetu stále vzácnější. Mnohem zajímavější jsou pro hackery internetové stránky a prohlížeče, přes které se mohou dostat k heslům a přístupovým údajům a ukrást bankovní údaje.



Zdroj: www.symantec.com

→ pro podvodné stránky. K tomu se používá ještě „bílý seznam“ důvěryhodných internetových stránek a „černý seznam“ se známými podvodnými stránkami. Tyto seznamy se automaticky aktualizují a ukládají na pevný disk.

Protože se však neustále objevují nové a nové podvodné stránky, spojí se prohlížeč s aktualizačním internetovým serverem, jakmile narazí na adresu, kterou ještě nezná. Jako minus jsme v testu hodnotili skutečnost, že v případě IE není možné samostatně zakázat připojení k aktualizačnímu serveru, což znamená, že by Microsoft mohl sestavovat profily uživatelů podle toho, jak surfují po internetu.

Firefox spolupracuje při aktualizaci s Googlem – adresy načítaných stránek jsou předávány ověřovacímu serveru tohoto vyhledávacího obra. Pokud se vám to nelíbí, můžete funkci jednoduše zakázat a používat pouze lokální databázi.

Nový bezpečnostní certifikát „High Assurance SSL Certificate“ podporují všechny testované prohlížeče. Tímto certifikátem nebude v budoucnu šifrována pouze komunikace mezi prohlížečem a serverem, jak je tomu dnes v případě SSL, ale navíc bude nezávislým autentizačním místem ověřována i protistrana. Jedině takové stránky se pak v řádku adresy v prohlížeči zobrazí zeleně. Zatím však tento certifikát nepoužívají žádné banky ani provozovatelé jiných internetových portálů.

SPRÁVA COOKIES: **V Opeře si můžete nastavit, aby se cookies vymazaly se zavřením prohlížeče.**

Mírně nás rozladil filtr v Internet Exploreru, který počítač zatěžoval víc než je zdrávo. Situaci vyřešil až patch (kb928089), který se objevil těsně před koncem testu. Filtr v Opeře podobnými problémy netrpěl, ovšem jeho stabilita nebyla v některých případech ideální...

LOKÁLNÍ ZABEZPEČENÍ

Cookies, vyrovnávací paměť a bezpečnost hesel

Podvodné stránky a přímé útoky přes internet nejsou jediná nebezpečí, která na uživatele číhají v prohlížeči. Často neprávem opomíjenou oblastí je totiž lokální zabezpečení dat. Nestává se sice často, že by se hacker dostal přímo do počítače a tím i k jednotlivým souborům, ale pokud už do systému pronikne nějaký trojský kůň, nemusí být útočník vůbec na místě, aby získal pří- →

Útoky: Jak hledají hackeři mezery v zabezpečení internetových prohlížečů

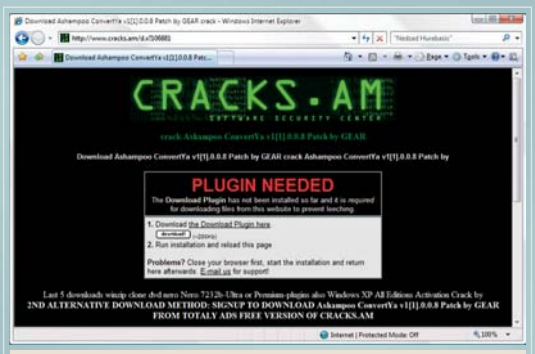
Neuplyne jediný měsíc, aby Microsoft nemusel vydávat nějakou aktualizaci pro Internet Explorer. Přímo děsivým příkladem je „Měsíc bezpečnostních mezer v prohlížeči“. Hacker H. D. Moore tehdy po celý měsíc zveřejňoval ve svém blogu *http://browserfun.blogspot.com* každý den jeden nedostatek v zabezpečení, v některých případech i s velmi podrobným návodem, jak ho zneužít. Jak ale hackeři vlastně odhalí tolik slabých míst?

Slabé místo ActiveX

Pohled do seznamu všech bezpečnostních mezer jasně ukazuje, že prakticky všechny útoky jsou zaměřeny na doplňky a zásuvné moduly, tedy nikoli na program internetového prohlížeče jako takový. To ale neznamená, že by Microsoft za slabá místa nemohl. Odborníci na bezpečnost kritizovali systém ovládacích prvků ActiveX už od začátku. Nejvíc jim vadilo, že ovládací prvky ActiveX mají příliš rozsáhlá oprávnění. Pokud pak hacker najde nějakou mezeru v zabezpečení, je dost pravděpodobné, že se mu podaří proniknout až do operačního systému. Na takové mezery narazí hackeři náhodou, pokud mají dobrý „čich“. Jenom málokdy totiž rozloží nějaký doplněk prohlížeče až na strojový kód. Mnohem užitečnější informace získávají z pádu prohlížeče. K němu dochází buď zase náhodou, nebo je vyvolávají útoky hrubou silou s využitím nástrojů jako „Axman“.

Slabé místo Windows

Dalším problémem, se kterým se potýká především Internet Explorer, jsou tzv. sdílené knihovny (DLL). Aby například nebylo nutné zapisovat pro každý program zvlášť, jak mají být zobrazovány obrázky ve formátu GIF, uloží se taková funkce do souboru DLL. Tutéž část kódu pak využívá hned několik programů v počítači. Pokud hacker odhalí slabé místo v knihovně DLL, týká se to i Internet Exploreru, využívá-li příslušnou „sdílenou knihovnu“. Výhodou pro hackera je to, že upravený soubor GIF s vloženým trojským koněm se hodí pro nejrůznější programy. Nejjednodušší je ale uložit trojského koně na webovém serveru. Jakmile se totiž stránka načte v okně prohlížeče, je počítač infikován.



PIRÁTSKÁ KOPIE JAKO LÁKADLO **Uživatelé, které přiláká „cracknutý“ software, si mají dobrovolně nainstalovat potřebný doplněk – a s ním samozřejmě i trojského koně.**

Slabé místo – uživatel

Nejsilnější „zbraní“ hackerů však zůstávají samotní uživatelé. Dokud bude moci neznalý uživatel sám spouštět škodlivé programy, budou existovat také hackeři, kteří najdou cestu, jak ho k tomu přimět. Nejlepším příkladem jsou doplňky, které se v Internet Exploreru od Service Packu 2 pro Windows XP už neinstalují automaticky. Od té doby umisťují hackeři škodlivé doplňky na často navštěvované internetové stránky a přidávají k nim vhodné upozornění pro instalaci. Uživateli tak prodávají malware jako užitečný program.

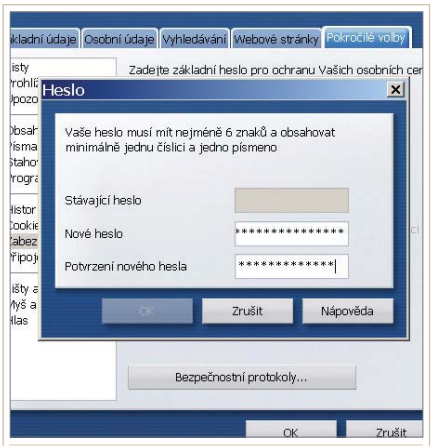
→ stup k datům v počítači, například k těm, která jsou uložena ve vyrovnávací paměti (cache) prohlížeče. Z obsahu vyrovnávací paměti se totiž dá zjistit, které internetové stránky uživatel navštěvuje. Často také obsahuje důvěrné informace, například poštu, kterou si uživatel čte prostřednictvím webového rozhraní.

V našem testu jsme zkusili zjistit, co zajímavého se nachází ve vyrovnávací paměti prohlížeče našeho kolegy – samozřejmě s jeho svolením. Obsah vyrovnávací paměti se nám podařilo načíst ve všech třech prohlížečích a kolegovi jsme pak poslali e-mail s jeho přístupovým heslem do jednoho diskusního fóra. Pokud je však komunikace šifrována pomocí protokolu SSL, neukládají se internetové stránky do vyrovnávací paměti a o důvěrná data se bát nemusíte.

Bezpečný prohlížeč by proto měl nabízet možnost jednotlivé soubory uložené ve vyrovnávací paměti jednoduchým způsobem vymazat. V tom Internet Explorer pokulhává za Firefoxem i Operou. Jeho uživatelé totiž mohou maximálně nastavit velikost vyrovnávací paměti a vymazat ji celou najednou. Pokud by chtěli mazat jednotlivé soubory, museli by se nejdřív prokousat nic neříkajícími názvy, pod kterými je prohlížeč ukládá. Naproti tomu konkurence umožňuje nejen mazání a kontrolu adresáře vyrovnávací paměti, ale také podrobné mazání jednotlivých stránek.

Velmi podobné je to v případě cookies. Jediný pohled do adresáře Cookies stačí k tomu, abychom často i po týdnech (podle platnosti cookies) zjistili, kdy a kde se prohlížeč na internetu pohyboval. Uživatelé IE mohou sice podrobně nastavit, jaké cookies jsou povolené a jaké ne, ale automatické mazání všech cookies při zavření prohlížeče, nebo dokonce při odchodu ze stránky Microsoft nenabízí. Nejpropracovanější řešení nabízí Opera, ve které můžete nejen ukládat nastavení pro každou stránku zvlášť, ale dokonce i načítat a upravovat cookies.

Nejmenší vliv na lokální zabezpečení má správa hesel. Heslo vám sice pomůže



SPRÁVCE HESEL: Opera umožňuje nastavit si hlavní heslo, což je rozumný kompromis mezi zabezpečením a pohodlím.

ochránit počítač před vaším synem, ale určitě ne před vážně míněnými útoky hackera. Všechny testované prohlížeče umí automaticky doplňovat přístupová hesla na internetové stránky. Opera a Firefox na rozdíl od Internet Exploreru však nabízejí rozumný kompromis mezi zabezpečením →

CHIP PŘEHLED: Internetové prohlížeče

Test zabezpečení

1

Mozilla Firefox 2.0
Na prvním místě se umístil opensourcový prohlížeč, který je nejen bezpečný, ale navíc i rychlý.

2

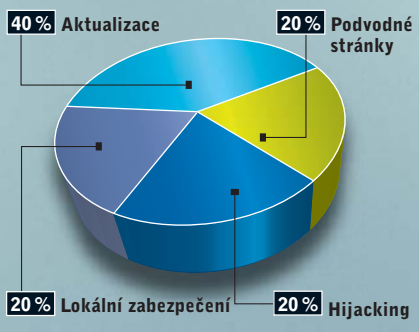
Opera 9.10
Druhé místo patří rychlému prohlížeči, který v nejnovější verzi nabízí i ochranu proti phishingu.

3

Microsoft Internet Explorer 7
Na posledním místě skončil i přes obrovskou snahu dohnat své konkurenty IE. Nedostatky v zabezpečení nás podle všeho čekají i v jeho sedmé verzi, což ho v našem testu stálo body.

JAK JSME TESTOVALI PROHLÍŽEČE

Všechny tři prohlížeče byly podrobeny důkladnému testu zabezpečení. Abychom si udělali představu, jaké nedostatky v zabezpečení nás čekají v budoucnu, využili jsme databázi společnosti Secunia, která se věnuje právě bezpečnosti dat. Do hodnocení jsme zahrnuli i slabá místa v samotném počítači, jako vyrovnávací paměť, cookies nebo hesla. Naopak nehodnotili jsme výkonnost nových verzí prohlížečů ani jejich doplňkové funkce. K testování jsme použili počítač s procesorem AMD 64 3000+ 2 GHz a 1 GB RAM. Prohlížeče jsme testovali ve Windows XP Pro a ve Windows Vista.



Přehled	1 MÍSTO	2 MÍSTO	3 MÍSTO
Program	**Firefox 2.0**	**Opera 9.10**	**Internet Explorer 7**
Výrobce	Mozilla	Opera Software	Microsoft
Internet	*www.mozilla.org*	*www.opera.com*	*www.microsoft.com*
Hodnocení bezpečnosti	95	93	64
	■■■■■	■■■■■	■■■□□
Podvodné stránky (20 %)	97	90	85
Hijacking (20 %)	97	97	67
Místní zabezpečení (20 %)	97	97	67
Aktualizace (40 %)	92	90	49
Bezpečnost			
Filtr podvodných stránek	Místní seznam nebo připojení na server Googlu	Připojení na server Opery (zdroj: GeoTrust a Phishtank)	Připojení na server Microsoftu
Podpora SSL / High Assurance SSL	● / ●	● / ●	● / ●
Správa doplňků (ochrana proti hijackingu)	Možnost zakázat a vymazat	Možnost zakázat a vymazat	Možnost zakázat a vymazat
Správa vyrovnávací paměti	Možnost nastavit velikost a vymazat všechny nebo jednotlivé stránky	Možnost nastavit velikost a vymazat všechny nebo jednotlivé stránky	Možnost nastavit velikost a vymazat všechny stránky najednou
Správa cookies	Možnost vymazat jednotlivé a všechny cookies a blokovat jednotlivé stránky	Možnost vymazat, blokovat a upravovat cookies	Možnost vymazat jednotlivé a všechny cookies, blokování stránek složité
Správa hesel / hlavní heslo	● / ●	● / ●	● / –
Způsob aktualizace	Automaticky	Automaticky/manuálně	Přes Windows Update
Průměrná doba odezvy na nedostatek v zabezpečení [1]	1 den	3 dny	9 dnů
Neodstraněné nedostatky v zabezpečení v předchozích verzích / počet nedostatků celkem [2]	3 / 36	0 / 15	19 / 106
Výkonnost			
Načtení HTML stránky	400 ms	376 ms	741 ms
Provedení příkazů JavaScriptu	7,8 s	7,3 s	17,7 s
Funkce			
Blokování reklamních oken	Dá se nastavit pro každou stránku zvlášť	Dá se nastavit pro každou stránku zvlášť	Dá se nastavit pro každou stránku zvlášť
Hledání internetových stránek	Možnost přidat další vyhledávače pomocí odkazů v JavaScriptu	Možnost manuálně přidávat další vyhledávače	Možnost přidávat další vyhledávače pomocí OpenSearch-XML
Prohledávání internetových stránek	Okamžité vyhledání (slova barevně označená)	Standardní pole pro zadání hledaného výrazu	Standardní pole pro zadání hledaného výrazu
Prohlížení v panelech (několik stránek v jednom okně)	●	●	●
Čtečka RSS	RSS zobrazeny jako záložky nebo internetové stránky	RSS se zobrazují ve čtečce	RSS se zobrazují jako internetové stránky
Správa oblíbených	Propracovaná	Propracovaná	Propracovaná
Možnost změnit vzhled	●	●	–
Přizpůsobení stránky (prohlížení / tisk)	● / ●	● / ● (včetně změny formátování)	● / ●
Kontrola pravopisu	● (formou aktualizace)	●	–
Možnost uložení aktuální relace	●	● (včetně obnovení po pádu prohlížeče)	–
Možnost nastavit víc úvodních stránek	●	●	●
Dodržování standardu W3C	Dobré	Velmi dobré	Uspokojivé
Myší gesta	Pouze formou doplňku	●	Pouze formou doplňku
Poštovní klient	Thunderbird	●	Outlook Express

● ano – ne

špičková třída (100–90)
vyšší třída (89–75)
střední třída (74–45)

Všechna hodnocení jsou v bodech (max. 100)

1) Zdroj: Symantec
2) Zdroj: Secunia

→ a pohodlím, protože všechna uložená hesla jsou chráněna jedním hlavním heslem. To je sice dobrá věc, ale potřebné heslo se dříve či později tak jako tak objeví v nešifrované podobě – nejpozději při zadávání na příslušné internetové stránce. V tom okamžiku ho může hacker s přístupem do počítače zachytit.

AKTUALIZACE

Mezery v zabezpečení a aktuálnost záplat

Zatím nejsou u nových verzí prohlížečů známy prakticky žádné mezery v zabezpečení. Hackeři tak čekají, až se nové verze víc rozšíří. Podle předchozích verzí však můžeme odhadnout, na co bychom se pak měli připravit. Smutným rekordmanem je tady IE, ve kterém hackeři odhalili přes 100 mezer, z nichž téměř 20 dosud nebylo odstraněno. Ve srovnání s tím eviduje firma Secunia *(www.secunia.com)*, která se věnuje zabezpečení dat, u Firefoxu 36 mezer v zabezpečení, u Opery dokonce jenom 15. Mnohem zajímavější je však pro hackery doba, po kterou mohou díry v zabezpečení zneužívat. I tady dopadá nejhůř Internet Explorer. Podle společnosti Symantec trvalo Microsoftu v prvním pololetí roku 2006 v průměru devět dní, než přišel s bezpečnostní záplatou. Opensourcové komunitě kolem Firefoxu na to stačí jeden jediný den, vývojáři Opery potřebují tři.

Velký počet nedostatků v zabezpečení a doba, která uplyne do jejich odstranění, tak podle všeho zůstává největším problémem Microsoftu.

Je opravdu nejbezpečnější IE6?

Zatímco soutěže „Můj browser toho umí víc než tvůj" už se pomalu stávají minulostí, popularita srovnání bezpečnosti nebezpečně roste. To, kam až se v této oblasti lze dostat, ukazuje „analýza" serveru Popular Technology.net, která tvrdí, že IE6 je bezpečnější než Firefox 1.x *(www.populartechnology.net/2006/09/internet-explorer-6x-more-secure-than.html)*. Srovnání na základě počtu nalezených zranitelností na první pohled opravdu jednoznačně pasuje IE6 do role favorita, ale... Autor pomíjí závažnost jednotlivých chyb, nezmiňuje rychlost oprav, a navíc ignoruje množství neopravených problémů – ovšem výsledek je jednoznačný: surfujte s Internet Explorerem 6. Reakcí na tento „test" bylo víc než dost – za zmínku stojí například „domácí" komentář Pavla Cvrčka: *http://jasnapaka.bloguje.cz/393926-proc-je-firefox-1-x-bezpecnejsi-nez-internet-explorer-6-0.php*. V každém případě platí, že uživatelé Firefoxu se tomuto srovnání mohou jen smát...