PROHLÍŽEČE

Bezpečné surfování

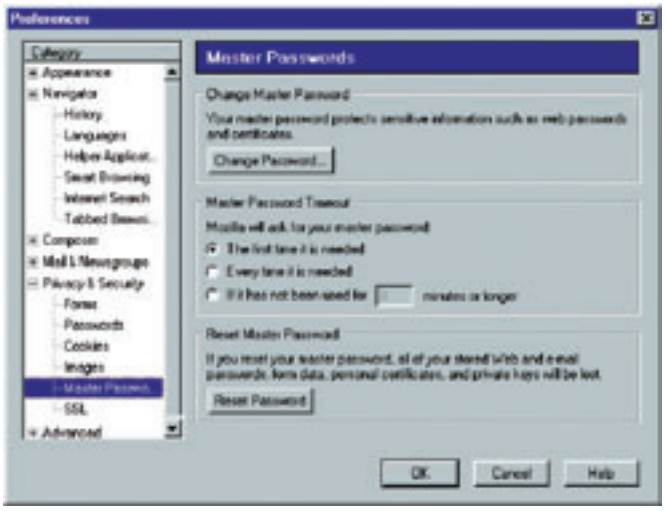
Každý uživatel, který má přístup k internetu, si občas klade otázku týkající se vlastní bezpečnosti při cestách po síti. Periodicky se objevují zprávy o nových virech nebo o útocích hackerů, které jenom zvyšují pocit zneklidnění. A protože převážná většina z nás se dostává do styku se světovou sítí prostřednictvím prohlížeče, nabízí se v první řadě otázka právě jeho bezpečnosti.

Podívejme se tedy blíže na prostředky zabezpečení, které jsou obsaženy v nejpopulárnějších prohlížečích používaných uživateli osobních počítačů.

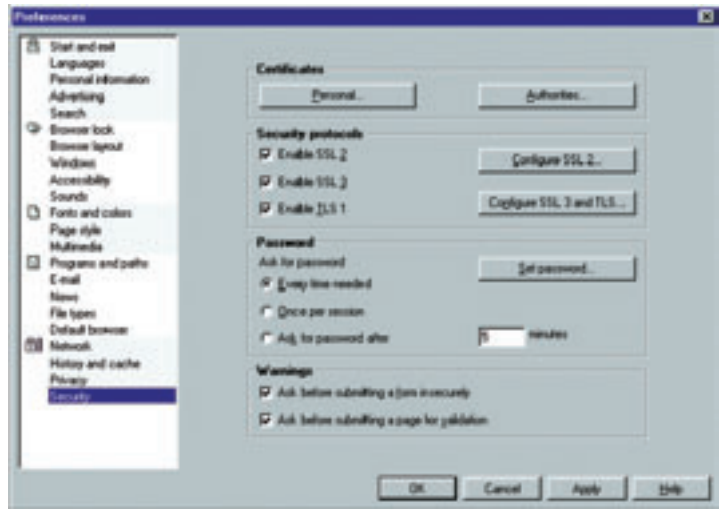
SSL a certifikáty

SSL (Secure Sockets Layer) je protokol určený pro bezpečný přenos dat. Vzpomeňte si, jak začíná adresa, kterou vypisujete v řádce svého prohlížeče. V 99 % případů to bude „http“, což znamená, že pracujete s WWW a používáte hypertextový přenosový protokol (Hypertext Transfer Protocol). Je to smutné, ale obyčejný protokol HTTP negarantuje odpovídající úroveň zabezpečení, protože veškeré informace se předávají v nezašifrované formě otevřenými kanály při nedostatečné úrovni autentifikace (autorizovaný vstup do určitého systému). Uživatel zadá jméno a heslo, které se potom předávají webovému serveru v nezašifrované formě. Kromě toho protokol HTTP neumožňuje identifikovat subjekty, které se zúčastňují výměny informací. Jednoduše řečeno, nemůžeme si být jisti, že subjekty se vydávají za toho, kým doopravdy jsou, a že při přenosu nepovolané osoby nezachytí informaci, jako je PIN kreditní karty nebo heslo poštovní schránky. Protokol HTTPS (analogický HTTP), který používá technologii SSL, ale umožňuje tyto problémy řešit.

Základem HTTPS jsou certifikáty a kryptoochrana (šifrování). Při iniciaci výměny informace si prohlížeč a server vyměňují certifikáty, čímž se navzájem jednoznačně identifikují. Další součinnost a komunikace pak už probíhají šifrovanými kanály. Výsledkem je, že SSL může teoreticky zabezpečit úplnou ochranu jakéhokoliv spojení v rámci internetu. Ale jenom teoreticky. V praxi všechno záleží na bezchybné realizaci této technologie v konkrétním prohlížeči. Zjištěné slabiny se autoři programů snaží odstranit dalšími „záplatami“ nebo servis packy. Vydávání servisních balíků pro programy využívající SSL je v současné době poměrně časté, což svědčí o nedokonalosti realizace SSL protokolu v mnoha v současnosti populárních programech.



Nastavení zabezpečení v prohlížeči Mozilla 1.0 (Master passwords)



Nutné minimum zabezpečení v prohlížeči Opera 6.04

Teď tedy o tom hlavním – o realizaci systému ochrany v různých prohlížečích.

Mozilla 1.0

Prohlížeč, který se mimořádně dlouho nemohl zbavit nuly v pořadovém čísle, se nakonec dočkal a teď existuje jak ve verzích pro Linux, tak i pro Windows. Body menu jsou stejné pro obě varianty a dostat se k nim je možné následujícím způsobem: *Edit-Preferences--Privacy-Security*. Nás zajímají následující z nich:

- Passwords – manažer hesel si je automaticky ukládá a v případě nutnosti sám uvádí jména a hesla k webovým stránkám uvedeným v seznamu.
- Master Passwords – chrání osobní informace (hesla, přístup k certifikátům, práci se smart kartami atd.). Pokud cizí osoba používá váš prohlížeč bez znalosti master hesla, nebude moci použít vaše certifikáty a uložená hesla. To znamená, že uživatel s nepoctivými úmysly, který pracuje s finančními nebo firemními webovými stránkami, se za vás nemůže vydávat a provádět operace vaším jménem. Při uvedení master hesla je možné také zkontrolovat odolnost vůči náhodnému výběru kombinací. Tato funkce je zajímavá a sama o sobě již může garantovat dostatečně vysoký stupeň zabezpečení.
- SSL – nastavení práce dle protokolu SSL (výběr verzí, metod šifrování).
- Certificates – řízení certifikátů a mechanismů ochrany. V tomto bodě je možné přidávat nebo odstraňovat certifikáty webových stránek i svoje vlastní a také certifikáty známých společností již existující v databázi prohlížeče a kontrolovat informaci o nich (například dobu platnosti). Nastavení tohoto bodu jsou prostá a intuitivně srozumitelná, ostatně jako i v jiných zkoumaných prohlížečích.
- Validation – kontrola platnosti certifikátů a řízení certifikátů anulovaných (odvolaných). V prohlížeči je přednastavena automatizace tohoto procesu – volba *Online Certificate Status Protocol* (OCSP) –, což je velice pohodlné.

Autoři tohoto prohlížeče věnují bezpečnosti velkou pozornost a je možné, že v budoucnu Mozilla i díky tomu získá značně vetší množství příznivců než doposud.

Netscape Communicator 4.75

Tento prohlížeč se v poslední době všemožně snaží znovu dobýt ztracené pozice. Již vyšla verze s číslem 7, ale u většiny uživatelů zůstává stále nejpopulárnější stará dobrá 4.75, prověřená roky používání.

- Z hlediska bezpečnosti mezi nimi základní rozdíly neexistují, proto se bez problémů můžeme blíže podívat na Netscape Communicator 4.75.
- Při otevření nastavení bezpečnosti (*Communicator-Tools-Security Info*) uvidíme následující body:
- Security Info – informuje o stavu běžné úrovně bezpečnosti při práci s prohlížečem (například probíhá-li šifrování provozu).
- Passwords – volba možností analogická bodu *Master Passwords* v prohlížeči Mozilla.
- Navigator – nastavení parametrů práce podle protokolu SSL.

Nastavení zabezpečení v prohlížeči Netscape 4.75, bod „Passwords“

Mozilla 1.0
Autor Mozilla.org
http://mozilla.org
Podmínky šíření freeware
Operační systém Windows, Linux

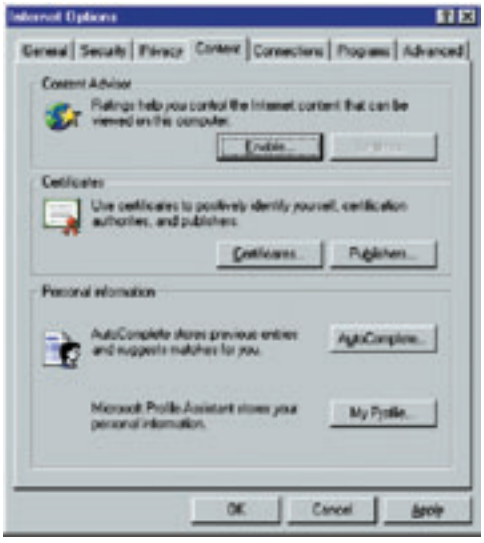
Netscape Communicator 4.75
Autor Netscape Communications Corporation
http://home.netscape.com
Podmínky šíření freeware
Operační systém Windows, Linux

Opera 6.04
Autor Opera Software
www.opera.com
Podmínky šíření adware
Operační systém Windows, Linux

Internet Explorer 6.0
Autor Microsoft
www.microsoft.com
Podmínky šíření freeware
Operační systém Windows

Nastavení bezpečnosti v Internet Exploreru 6.0 je dostatečně široké a uživatel si může sám vybrat tu úroveň, kterou považuje za přijatelnou.

Rozšířené možnosti nastavení bezpečnosti v IE 6.0 (SSL)



Řízení certifikátů a osobních informací uložených v IE 6.0

- Messenger – bezprostředně k prohlížeči se tento bod nevztahuje, jsou to nastavení bezpečnosti pro instant messenger.
- Java/Java Scripts – řízení certifikátů a aktivace Java appletů a skriptů.
- Certificates – řízení certifikátů, prakticky úplně analogické části *Manage Certificate* v možnostech prohlížeče Mozilla.
- Cryptographic Modules – řízení kryptografických modulů, které používá prohlížeč (smart karty a jiné).
- Nastavení Netscape Communicatoru jsou velice podobná těm, která nacházíme v Mozille, což není překvapující, protože oba tyto prohlížeče jsou postavené na stejném jádru.

Opera 6.04

Všechny volby bezpečnosti (*File-Preferences-Security*) jsou v tomto případě omezeny na nezbytné minimum, jsou vměstnány do jediného okna a jejich charakteristiky se málo liší od těch, které existují u „kolegů“. Například část *Password* je fakticky plně analogická s částí *Master Password*s v Mozille.

Jak už bylo řečeno, prostředky bezpečnosti Opery neposkytují uživateli příliš mnoho možností k nastavení, protože jejími silnými stránkami jsou rychlost otevírání stránek a kompaktnost. Právě těmto vlastnostem prohlížeče také věnují autoři programu hlavní pozornost. Ostatně v blízké budoucnosti se předpokládá uvedení verze Opera 7, jejíž programové jádro by mělo být, podle ujištění tvůrců programu, úplně přepsané. Je možné, že se v nové verzi setkáme s jinými prostředky bezpečnosti.

Internet Explorer 6.0

V tomto prohlížeči, kde je nastavování bezpečnosti soustředěno v menu *Tools-Internet Options...-Security*, se věci jeví mnohem zajímavěji: Microsoft (na rozdíl od jiných autorů softwaru) zavedl pojmy „Security Level“ a „Security Zones“. Znamená to, že pro každou oblast je možné stanovit svoji vlastní úroveň bezpečnosti. Celkem existují čtyři zóny:

- Internet – zde jsou zahrnuty všechny webové stránky neuvedené v ostatních zónách. Na rozdíl od jiných zón sem nelze výběrově přidávat samostatně vybrané stránky.
- Local Intranet – zde jsou instalována nastavení bezpečnosti pro zdroje lokální sítě. Když stiskneme tlačítko *Sites...*, je možné vybrat, jaké zdroje budeme do této zóny zahrnovat:
  a) Include all local (intranet) sites not listed in other zones – všechny lokální stránky, které nejsou uvedené v jiných zónách. Jsou to ty stránky, v jejichž názvech nejsou tečky (například *http://honza*, ale ne *http://www.honza.cz*).
  b) Include all sites that bypass the proxy server – všechny stránky připojené přímo k proxy serveru.
  c) Include all network paths (UNCs) – všechny síťové názvy, jako \\honza\public\music a jiné.
- Podobně když klepneme na *Advanced*, dává nám to možnost přidat do této zóny nutné lokální webové zdroje samostatně. Abychom přidali pouze ty, které podporují HTTPS, zvolíme *Require server verification (https:) for all sites in this zone*.
- Trusted sites – spolehlivé webové zdroje, kterým je možné důvěřovat. Všechny operace přidání stránek jsou analogické se zónou Local intranet. Microsoft naléhavě doporučuje přidávat sem pouze stránky s podporou HTTPS.
- Restricted sites – nespolehlivé webové zdroje. Sem se ukládají stránky, jejichž obsah může být pro váš počítač nebezpečný.
- Předpokládají se také čtyři úrovně bezpečnosti, ale pokud vybereme bod menu *Custom level...*, je možné měnit nastavení podle vlastního vkusu:
- High – nejvyšší. Zabezpečuje nejbezpečnější surfování. Některé stránky však mohou být zobrazeny nekorektně: jsou vypnuty ActiveX, Java a jiné nebezpečné

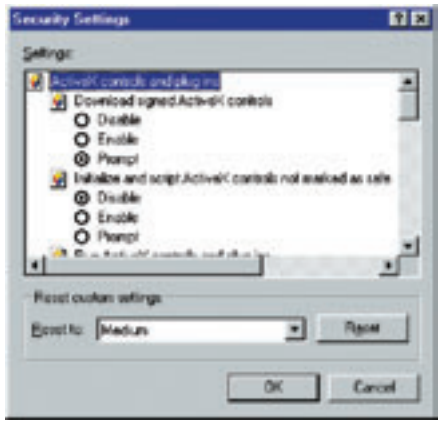
Internet Explorer 6.0 – záplaty pro lídra

Kolem prohlížeče od Microsoftu stále vznikaly různé fámy a skandály. V první řadě byly spojeny s otázkami bezpečnosti a také s tím, že prohlížeč byl hned od počátku součástí operačního systému a zbavit se ho legálními metodami bylo prakticky nemožné. S každou verzí Internet Exploreru se objevovaly dodatky a opravy určené ke zvýšení úrovně jeho bezpečnosti. Výjimkou se nestal ani Internet Explorer 6. 9. září 2002 pro něj firma Microsoft oficiálně vydala soubor oprav Service Pack 1 (Q326489), který procházel beta testováním od začátku července minulého roku. Mezi jinými Microsoft opravil chyby otevírání souborů při SSL nekešovaném spojení (Q323308) a chybu NTLM autentifikace přes SSL (Q325662).
SSL představuje protokol pro výměnu informací v chráněném režimu a v současné době existují verze SSL 2 a SSL 3, mezi kterými není z uživatelského pohledu velký rozdíl. Dosud není jasné, zda se i pro nejpopulárnější prohlížeč objeví nové záplaty, ale pokud můžeme usuzovat podle toho, jak roste popularita jeho konkurentů, autoři z Microsoftu se budou muset o osud svého dítka náležitě starat..

- elementy. Tato úroveň je určena pro práci s Restricted sites.
- Medium – střední. Obyčejná úroveň bezpečnosti je vhodná pro většinu webových stránek, proto se doporučuje pro zónu Internet.
- Medium-low – snížená. Od střední úrovně se liší tím, že jsou vypnuty požadavky na otevření mnoha komponent. Doporučuje se pro zónu Local intranet.
- Low – nízká. Z důvodu zvláště nízké ochrany se doporučuje používat pouze pro Trusted sites.

Je třeba říct, že bez ohledu na četné možnosti nastavení si Internet Explorer vysloužil pověst uživatelsky přátelského, ale špatně zabezpečeného prohlížeče. Mnohokrát se v něm objevily chyby, které autoři museli dodatečně opravovat.

Výše uvedenými body možnosti nastavení bezpečnosti nekončí. Na záložce *Advanced*, skoro na samém konci seznamu nastavení (část *Security*), se nachází řízení SSL protokolu: kontrola anulovaných certifikátů, výběr použitých verzí SSL a některé jiné body. Na záložce *Content* se pak provádí řízení certifikátů (*Certificates*), automatického ukládání hesel (*Personal information-AutoComplete*...)

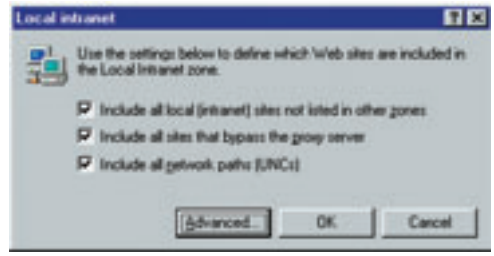


Řízení parametrů úrovní bezpečnosti v IE 6.0 (Custom level)

a personálních údajů (*Personal Information-My Profile*).

Nezapomeňte, že všechny certifikáty mají určitou dobu platnosti, po jejímž vypršení se stávají neplatnými. Na to je třeba dávat pozor a neplatné certifikáty uložené v bázi vašeho prohlížeče je třeba včas anulovat.

Je možné, že některé body v IE se vám budou zdát zbytečné. Ale pokud jim porozumíte a dáte si čas na jejich nastavení, zajistíte si pohodlnou práci s internetem. Alespoň tak



Konfigurace zóny „Local intranet" v IE 6.0

nás o tom ubezpečuje Microsoft...

Nesmíme však zapomínat, že při vší shodě nastavení bezpečnosti v prohlížečích se mohou objevit chyby v realizaci některých metod ochrany. S kterým prohlížečem pracovat, to je věc vkusu, ale v otázkách bezpečnosti mu nemůžeme důvěřovat. Dávat jakákoliv doporučení je poměrně složité. I když Internet Explorer správněji zobrazuje převážnou většinu stránek, s bezpečností to u něho není právě nejlepší. Za sebe mohu říct, že Internet Exploreru dávám přednost vzhledem k jeho „správnému" chápání HTML kódu a Mozille vzhledem k tomu, že autoři programu věnují otázkám bezpečnosti více pozornosti než autoři ostatních programů. ■

■ ■ Konstantin Nikolajenko