EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE
it akadémia

Modul 12: Bezpečnosť pri využívaní IKT

Bezpečná práca s webom

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
www.itakademia.sk
ITMS2014+: 312011F057

5 Bezpečná práca s webom

5.1 Nastavenie webového prehliadača

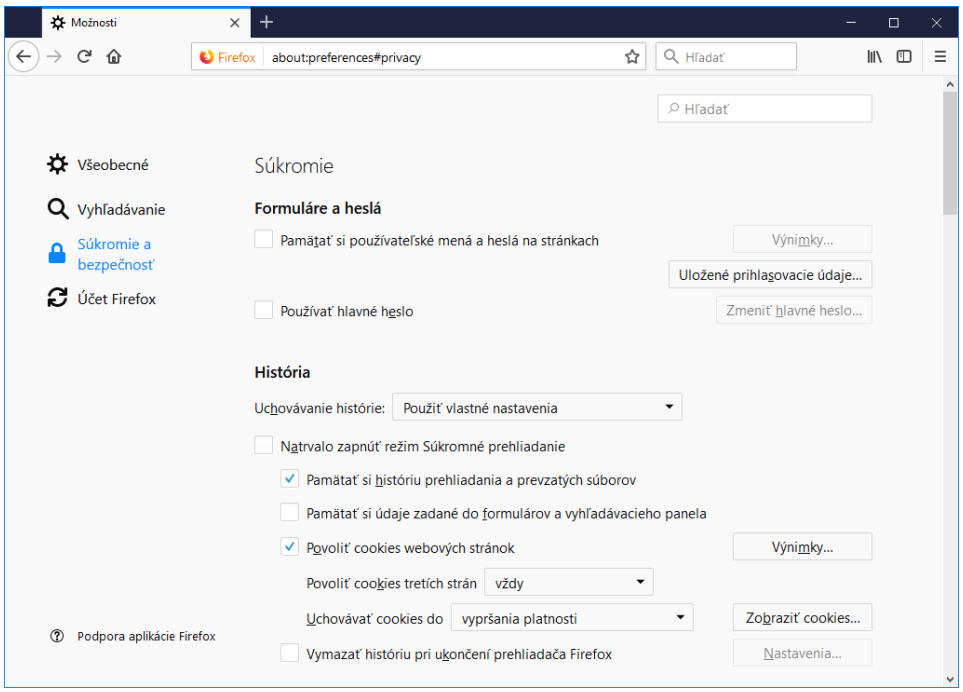
5.1.1 Ako zvoliť vhodné nastavenia pre umožnenie / zakázanie automatického dokončovania a automatického ukladania pri vypĺňaní formulárov a hesiel

Automatické dopĺňanie formulárov na webových stránkach uľahčuje prácu pri častom vypĺňaní rovnakých údajov, ale je vhodné len na vlastnom počítači. Na cudzích alebo zdieľaných počítačoch predstavuje hrozbu - niekto cudzí sa môže dostať k Vašim údajom.

Veľký pozor si musíme dávať na zapamätávanie hesiel. Ak túto funkciu chceme využiť tak jedine v zašifrovanej databáze nejakého spoľahlivého programu na správu hesiel.

Nastavenia automatického dokončovania formulárov sa napr. v prehliadači Mozilla Firefox nachádzajú v nastaveniach pod záložkou "Súkromie a bezpečnosť". V časti "Uchovávanie histórie" nastavíme možnosť "Použiť vlastné nastavenia" a odškrtneme možnosť "Pamätať si údaje zadané do formulárov a vyhľadávacieho panela" (Obrázok 1). Takýmto spôsobom vypneme pamätanie údajov vložených do formulárov.

Ukladanie prihlasovacích údajov môžeme vypnúť v nastaveniach pod záložkou "Súkromie a bezpečnosť" (Obrázok 1). Odškrtneme možnosť "Pamätať si prihlasovacie údaje k stránkam". V prípade, že túto možnosť chceme používať, je dôležité chrániť uložené heslá šifrovaním - to je možné zapnúť zaškrtnutím možnosti "Používať hlavné heslo" a nastavením príslušného hesla.

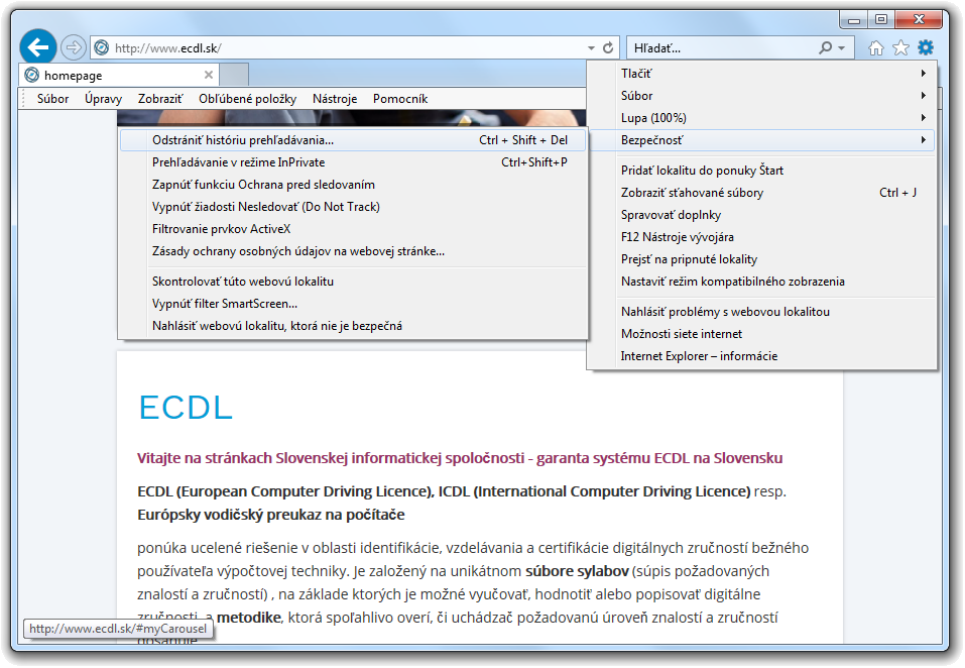


Obrázok 1: Konfiguračný dialóg webového prehliadača Mozilla Firefox

5.1.2 Ako odstrániť z webového prehliadača súkromné údaje, ako sú história prehliadania, pamäť dočasných súborov (cache), heslá, cookies, údaje automatického dokončovania

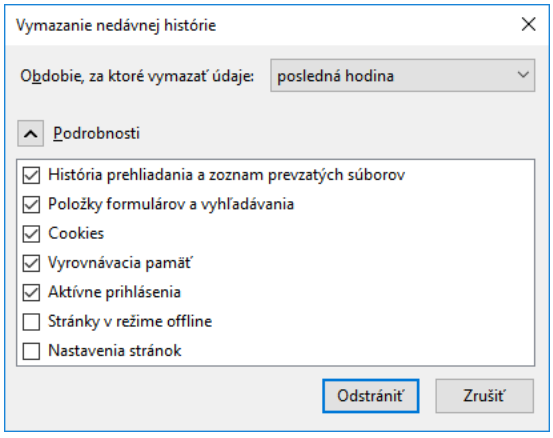
Vymazanie súkromných údajov z prehliadača (cookies, história navštívených stánok, história prevzatých súborov, dočasné kópie navštívených stránok, hodnoty z formulárov) môže byť vhodné najmä na cudzom alebo zdieľanom počítači.

V prehliadači Internet Explorer je možné odstrániť históriu prehliadania cez Nastavenia a časť Bezpečnosť, kde sa nachádzajú aj ďalšie možnosti (Obrázok 2).



Obrázok 2: Nastavenia v prehliadači Internet Explorer

V prehliadači Mozilla Firefox klikneme v menu na tlačidlo "Knižnica", ďalej "História" a "Vymazať nedávnu históriu". V dialógovom okne máme na výber obdobie, za aké je možné súkromné údaje vymazať a v časti "Podrobnosti" je možné vybrať konkrétne údaje, ktoré chceme zmazať (Obrázok 3).



Obrázok 3: Vymazanie histórie vo webovom prehliadači Mozilla Firefox

5.2 Bezpečné prehliadanie webu

5.2.1 Ktoré činnosti na webe by sa mali uskutočňovať iba na zabezpečených webových stránkach

Zabezpečenie komunikácie cez protokol HTTP rieši jeho rozšírenie protokol HTTPS (HTTP over SSL/TLS).

Protokol SSL/TLS využíva asymetrickú kryptografiu a zabezpečuje:

- autentifikáciu servera (aby sme vedeli, že komunikujeme s tým správnym);
- šifrovanie prenášaných údajov (nie je možné získať informácie odpočúvaním);
- kontrolu integrity prenášaných údajov (nie je možné nepozorovane zmeniť prenášané informácie)

Certifikát servera umožňuje webovému prehliadaču vytvoriť zabezpečené pripojenie k serveru.

Všetky aktivity, pri ktorých sa vyžaduje autentifikácia používateľa, by sa mali vykonávať iba na zabezpečených webových stránkach. Patria tu najmä prístup k elektronickej pošte, on-line nákupy, finančné transakcie, práca v informačných systémoch, komunikácia na sociálnej sieti a pod.

5.2.2 Poznať spôsoby ako si potvrdiť autenticitu web stránky (kvalitný obsah, všeobecné uznávaný zdroj, platné URL, prítomné informácie o spoločnosti alebo vlastníkovi stránky, kontaktné informácie, bezpečnostný certifikát stránky, overený vlastník domény)

Existujú viaceré spôsoby ako si potvrdiť, že stránka, ktorú navštevujete je skutočne autentická a nejedná sa o podvrhnutú stránku.

Jedným s kritérií, ktoré môžu potvrdiť autentickosť je kvalitný obsah. Podvrhnuté stránky majú často v obsahu gramatické chyby, nezrozumiteľný text a podobne.

V prípade podozrenia je vhodné zadať názov stránky do vyhľadávača a pozrieť sa na hodnotenie tejto stránky.

Veľmi dobrým pomocníkom je overiť si názov domény v adresnom riadku prehliadača - ak napríklad chcem navštíviť stránku univerzity a v adresnom riadku vidíme niečo ako sk.uni-verzita.ru, je celkom zrejmé, že sa nejedná o stránku slovenskej univerzity.

Na stránkach regulárnych spoločností bývajú uvedené kontaktné informácie (vrátane platného telefónneho čísla).

Ak je stránka dostupná cez šifrované spojenie (https://) je možné vo webovom prehliadači overiť organizáciu/majiteľa certifikátu stránky.

Je tiež možné overiť majiteľa danej domény cez nástroj whois (dostupný aj cez webové stránky - https://whois.sk-nic.sk).

5.2.3 Čo znamená a spôsobuje presmerovanie na podvrhnuté webové stránky (pharming)

Pharming je presmerovanie komunikácie s vybraným serverom na iný server ovládaný útočníkom tým, že sa presmeruje názov webovej stránky na inú adresu. Každej mennej adrese, (napr. www.upjs.sk), prislúcha číselná, tzv. IP adresa (v tomto prípade 158.197.16.80). Presmerovanie takejto adresy môže útočník uskutočniť buď napadnutím servera DNS, ktorý prevádza menné adresy na IP adresy, alebo priamo na počítači používateľa zmenou súboru hosts, v ktorom sú lokálne uložené IP adresy pre vybrané menné adresy.

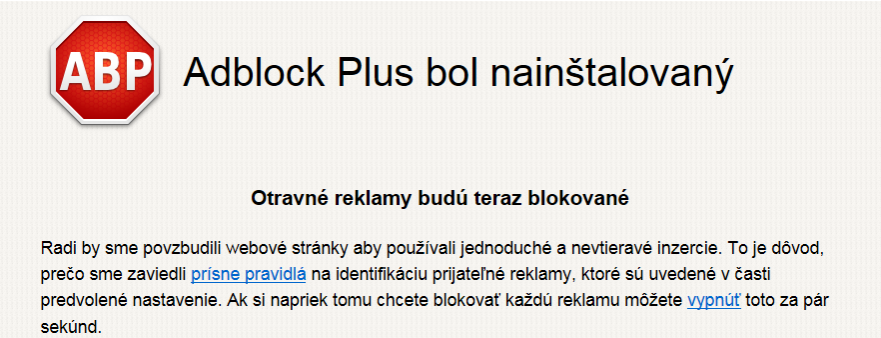
Ak používateľ zadá mennú adresu do internetového prehliadača, namiesto požadovanej stránky (napr. banky) sa zobrazí jej dokonalá napodobenina. Používateľ teda nezistí, že sa nachádza na inej stránke. Po zadaní údajov ich získa neoprávnená osoba, ktorá takúto falošnú stránku vytvorila.

Samotný útok môže prebiehať rôznym spôsobom. Veľmi často sa založí webová stránka, ktorá vyzerá ako presná kópia už existujúcej dôveryhodnej stránky, alebo ponúka nejaké výhody po prihlásení cez ich webovú stránku. Napr. ponúkajú rôzne „skvelé“ služby (napr. vzácne predmety do hier, stiahnutie programov zadarmo po registrácii atď.). Prihlasovacie meno a heslo zadané do falošnej stránky získa útočník, ktorý ich môže priamo zneužiť, prípadne predať ďalším osobám, ktoré o to majú záujem.

5.2.4 Účel, funkcia a druhy softvéru na kontrolu obsahu webových stránok, ako sú softvér na filtrovanie internetového obsahu, softvér na účely rodičovskej kontroly

Antivírusový softvér chráni používateľa pred malwarom ako takým, nechráni však používateľa pred obsahom webových stránok. Softvér na kontrolu obsahu webových stránok slúži na obmedzenie alebo monitoring prístupu k určitému druhu obsahu na webe, prípadne k určitým konkrétnym stránkam.

Podľa účelu a funkcií sa jednotlivé druhy softvéru od seba líšia. Softvér na blokovanie nežiaducej reklamy na internete obmedzí jej zobrazenie vo webovom prehliadači (Obrázok 4). Niektoré webové portály žiaľ žijú prevažne z tejto reklamy.



Obrázok 4: Softvér na blokovanie reklamy

Účelom softvéru na kontrolu obsahu webových stránok je zamedziť používateľovi v prístupe k niektorému typu obsahu (hazard, pornografia a pod.) alebo zamedziť v prístupe ku konkrétnej stránke.

Špecifickú skupinu tvorí softvér, ktorý zabezpečuje tzv. rodičovskú kontrolu. Jednou z najdôležitejších funkcií je filter webových stránok , ktoré môžeme navštíviť. Odporúča sa, aby sme vyplnili zoznam stránok, ktoré nebude možné navštíviť. Ak existuje veľa takýchto adries, môžeme naopak vyplniť "biely zoznam" . Používateľ (dieťa) bude môcť navštíviť iba stránky z tohto zoznamu. V rámci rodičovskej kontroly je možné stanoviť kedy a ako dlho môže používateľ používať zariadenie.

Obrázok 5: Rodičovská kontrola v programe Windows Defender