Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Teze diplomové práce

Analýza bezpečnosti a možnosti zabezpečení Google Chrome

Miroslav Štolovský

Analýza bezpečnosti a možnosti zabezpečení Google Chrome

Souhrn

Diplomová práce se zabývá popisem, analýzou a možnostmi zabezpečení v prohlížeči Google Chrome, ale také všeobecně bezpečným používáním Internetu. V teoretické části je popsána historie a vývoj Internetu a internetových prohlížečů. Následuje popis prohlížeče Google Chrome a vysvětlení všech teoretických pojmů, se kterými autor později pracuje. Prvním bodem praktické části je popis všech nastavení, které Google Chrome nabízí. K tomuto bodu jsou uvedena autorova doporučení pro nastavení nejvyšší bezpečnosti. Dalším bodem je vyhodnocení elektronického dotazníku na téma Zásady bezpečného chování na Internetu. V dotazníku jsou řešena témata hesla, phishing a zfalšované stránky, Malware, Adware, Spyware a posledním tématem jsou firewally a antivirové programy. Ke všem analyzovaným tématům jsou uvedena autorova doporučení, jak se chovat při tomto druhu útoku a jak jim také předcházet.

Klíčová slova: Internet, internetový prohlížeč, Google Chrome, zabezpečení, heslo, soubor cookie, cache paměť, phishing, firewall, antivirový program

1 Cíl práce a metodika

1.1 Cíl práce

Cílem této práce je analyzovat možnosti zabezpečení internetového prohlížeče Google Chrome a navrhnout zlepšení z hlediska ochrany soukromí uživatele, zabezpečení připojení a správy hesel.

V praktické části jsou uvedeny konkrétní příklady tohoto nastavení a také uvedeny zásady bezpečného chování na Internetu. Jedná se o řešení a předcházení problémů při používání hesel, při návštěvě podvodných stránek a různých dalších nebezpečích, které mohou nastat při práci na Internetu.

1.2 Metodika práce

V teoretické části práce jsou použity zdroje odborné literatury a důvěryhodné internetové zdroje. Všechny použité zdroje jsou uvedeny v seznamu použité literatury a jsou použity k uvedení pojmů a vysvětlení problematiky.

V praktické části je to analýza a popis funkcionality prohlížeče Google Chrome spolu s uvedenými doporučeními. Dále je použito dotazníkové šetření pomocí elektronického dotazníku ke zjištění chování uživatelů na Internetu. Uživatelé jsou vybírání z řad autorových spolužáků a spolupracovníků. Následně je dotazník vyhodnocen a jsou navržena řešení všech problémů, která jsou předvedena na konkrétních příkladech.

2 Teze

Prohlížeč Google Chrome a jeho vývojáři nabízejí maximum možné ochrany a nastavení. V první řadě se jedné o funkci Upozornění na phishing a Malware. O tuto funkci se stará rozsáhlý tým vývojářů ve společnosti Google. Tým má na starosti odhalování nebezpečných stránek a aktualizaci jejich seznamu pro prohlížeč. Uživatel je při vstupu na takovouto stránku upozorněn, že se jedná o nebezpečí. Nejčastějším nebezpečím, které hrozí na těchto stránkách, je ztráta citlivých údajů a s tím spojené další ztráty například peněžních prostředků, nebo instalace nebezpečného software do uživatelova počítače, což může vést ke stejnému závěru, ztrátě citlivých údajů. Autor proto doporučuje tuto možnost v nastavení Google Chrome nikdy nevypínat a pokud je uživatel upozorněn na takovouto nebezpečnou stránku, je dobré ji ihned zavřít.

Další funkcí, která sice pomáhá uživateli zvýšit komfort při prohlížení stránek, ale také u ní hrozí velké bezpečnostní riziko, je správce hesel. Prohlížeč Google Chrome umožňuje ukládat všechna hesla do správce a ty odsud automaticky načítat. Pokud stejný prohlížeč používá více lidí, jedná se o riziko zneužití hesel. V případě používání prohlížeče více lidmi, autor toto ukládání nedoporučuje. V opačném případě je dobré si rozmyslet, které uložené přístupy jsou zneužitelné. Autor uvádí jako méně nebezpečné například diskuzní fóra, na rozdíl od hesla uloženého například do internetového obchodu. Pro vyšší úroveň bezpečnosti doporučuje autor tuto funkcionalitu vypnout.

Dalším podobným nástrojem je automatické vyplňování formulářů. Prohlížeč Google Chrome si pamatuje fráze, která uživatel zadává do formulářů a při dalším vyplnění je uživateli nabízí k použití. Opět se jedná o zvýšení komfortu při prohlížení, ale plyne z toho stejné riziko, jako bylo zmíněno u ukládaných hesel. Autor proto opět doporučuje tuto funkcionalitu vypnout v pokročilém nastavení prohlížeče.

Dnes důležitým a často zmiňovaným tématem je anonymita na Internetu. V této práci se jedná o tři témata, cache paměť a údaje o prohlížení, soubory cookie a zeměpisná poloha uživatele. Co se týče cache paměti a údajů o prohlížení, jsou tato data ukládána zcela automaticky a nelze je nijak vypnout. Jelikož jsou zde ukládány celé internetové stránky, nebo jejich části a další data, která mohou případnému útočníkovi poskytnout informace pro útok. Autor doporučuje tato data promazávat. Ta jsou uložena na disku počítače. Další výhodou průběžného mazání je i zrychlení práce s prohlížečem. Soubory cookie jsou také ukládány na disk uživatele a obsahují informace o uživateli a nastavení jeho prohlížeče.

Jedná se o větší riziko, než jsou předešlá data o prohlížení. Jelikož je ukládání souborů cookie povoleno ihned po instalaci prohlížeče, doporučuje autor jejich správu. Protože by úplné vypnutí znamenalo nefunkčnost většiny stránek, doporučuje autor blokování cookie třetích stran a poté nastavit možnost „Uchovávat místní údaje jen do uzavření prohlížeče“. Po ukončení prohlížeče jsou všechny soubory smazány. Další zmiňovaným tématem je práce se zeměpisnou polohou uživatele. Prohlížeč nabízí službu, která dokáže odhadnout polohu uživatele a například při hledání mu nabídnout odkazy, kterou jsou mu nejblíže. Opět se jedná o uživatelský komfort, ale někteří uživatelé by to mohli brát jako zneužitelný zásah do soukromí. Uživatel je vždy tázán, zda konkrétní stránce má prohlížeč sdělit zeměpisnou polohu. Autor v tomto případě doporučuje sdělovat polohu pouze v nutných případech.

V druhé části vlastní práce autor řeší elektronický dotazník týkající se chování uživatelů na Internetu právě z pohledu možných hrozeb.

Dotazník vypovídá o malé informovanosti uživatelů o hrozbách zneužití. U tématu hesla je jasné, že uživatelé používají hesla na Internetu, ale v případě zadání jednoho hesla na více stránkách vzniká riziko, že pokud útočník získá správné heslo, může ho zneužít na dalších stránkách. Pokud je takovéto heslo používáno na stránkách dnes moderního internetového bankovnictví, portálů pojišťoven a různých úvěrových institucí, mohou být napáchané škody velmi rozsáhlé. Autor proto doporučuje používat vždy rozdílná hesla a navíc tato hesla měnit v pravidelných intervalech. V práci je zmíněno, že některé portály změnu hesla vyžadují, což autor považuje za správnou vlastnost. S touto problematikou úzce souvisí i síla hesla. Autor demonstruje, jak pouhé rozšíření heslové fráze o čtyři číselné znaky a dva speciální znaky, zvýší několikanásobně bezpečnost heslové fráze. Jsou zde také uvedeny příklady nejčastějších hesel, jako například vlastní jméno, jméno partnera, datum narození, ostatní významná data atp. Pro vyšší bezpečnost jsou dnes používána hesla v kombinaci s jednorázovými hesly. Jako příklad lze uvést internetové bankovnictví, kdy při zadávání platby musí uživatel zadat ještě potvrzovací kód, který mu přijde sms zprávou na mobilní telefon.

Dalším tématem dotazníku je téma phishingu a zfalšovaných stránek. Z výsledků je patrné, jak tato hrozba rozšířená. Drtivá většina odpovídajících se setkala s těmito podvodnými e-maily a lze říci, že většinou se odesílatel tváří jako peněžní instituce. Z pohledu útočníka je to také nejjednodušší způsob, jak se dostat k finančním prostředkům

případné oběti. Pouhá polovina dotázaných ví, jak se v daném případě chovat a to autor považuje za velmi málo. Z dalších odpovědí je možné vyčíst, že přes jednu třetinu kliká na uvedený odkaz, který je přesměruje na podvodnou stránku, a dokonce čtyři odpovídající na ní zadávají požadované údaje. Autor v takovýchto případech doporučuje maximální ostražitost. Uvádí příklady, jak si ověřit pravost odesílatele e-mailu a případné internetové stránky. V každém případě doporučuje těmto e-mailům nevěnovat pozornost a okamžitě je mazat, protože všechny instituce nejsou oprávněny vyžadovat údaje touto cestou, ale pouze formou osobního kontaktu na pobočce instituce.

Předposlední téma dotazníku se věnuje nežádoucímu a škodlivému software. Některé případy úzce souvisí s předchozím tématem, kdy e-maily obsahují přílohu se škodlivým programem. Uživateli stačí pouze kliknout na tuto přílohu a díky uvnitř obsaženému škodlivému kódu může dojít k úniku osobních údajů a další materiálním škodám. Z výsledků tohoto tématu vyplývá, že se najdou lidé, kteří tyto přílohy otevírají, což je opět velká chyba. Autorovým doporučením je i tomto případě e-maily mazat, v žádném případě neotevírat přílohy. Co se týče ostatního škodlivého software, který se dokáže do počítače dostat jinou cestou, je nutné být při instalaci jakéhokoliv software pozorný a instalaci pročítat krok po kroku. Právě v případech nepozornosti se do PC dostávají programy, které poté mohou napáchat škody. V případě Spyware tomu tak není, tento škodlivý software se do počítače dostává bez vědomí uživatele. Pro ochranu a prevenci autor doporučuje instalaci programu Spybot, který dokáže tento druh software vyhledat a odstranit. Navíc nabízí funkci imunizace, která má preventivní účinek a brání instalaci Spyware do počítače.

Posledním tématem dotazníku jsou firewally a antivirové programy. Pro autora je výsledek velmi překvapivé. Třetina dotázaných neví, co je to antivirový program. Viry jsou v dnešní době jednou z největších hrozeb a je nutné se proti nim bránit dobrou antivirovou ochranou. Autor v práci zmiňuje v současné době nejznámější antivirové programy a produkty, způsoby jejich skenování systému a hlavní pravidlo používání antivirového programu. Tím jsou aktualizace. Je důležité mít nainstalován antivirový program, ale je mnohem důležitější udržovat virové definice aktuální. S antiviry souvisí také firewally, které jsou také důležitou součástí ochrany uživatele. V dnes nejrozšířenějším operačním systému Microsoft Windows je tato ochrana zapnuta automaticky, ale i ta může být překonatelná, pokud je nastavena špatně. Při povolování přístupu k internetu je nutné dávat pozor a autor radí k těmto případům přizvat zkušenějšího uživatele a tato nastavení optimalizovat.

3 Seznam použité literatury

ATKINS, D. *Internet security professional reference*. Indianopolis: New. Riders Publ., 1996. ISBN 1-56205-557-7.

BEDNÁŘ, V. *Alternativní webové prohlížeče: Firefox, Opera, Mozilla, Maxthon a další.* Brno: Computer Press, 2006. ISBN 80-251-0566-0.

BRADLEY, T., CARVEY H. A. *Essential computer security: everyone's guide to e-mail, internet, and wireless security*. Rockland: Syngress, 2006. ISBN 1-59749-114-4.

CONTI, G. *Googling security: how much does Google know about you?* Upper Saddle River: Addison-Wesley, 2009. ISBN 978-0-321-51866-8.

DEFRANCO, JOANNA F. *What every engineer should know about cyber security and digital forensics.* Boca Raton: CRC Press, 2014. ISBN 978-1-4665-6452-7.

ENDORF, C. F., SCHULTZ, E., MELLANDER, J. *Detekce a prevence počítačového útoku.* Praga: Grada, 2005. ISBN 80-247-1035-8.

CHESWICK, W. R., BELLOVIN, S. M. *Firewally a bezpečnost Internetu aneb Jak zahnat lstivého hackera.* Veletiny: Science, 1998. ISBN 80-86083-01-2.

ISKRA, J. *Google : vyhledávání, Gmail, Google Talk a další služby.* Brno: Computer Press, 2006. ISBN 80-251-1043-5.

LONG, J. *Google Hacking*. Brno: Zoner Press, 2005. ISBN 80-86815-31-5.

PAVLÍČEK, A., GALBA, A. *Moderní informatika*. Praha: Professional Pub., 2012. ISBN 80-7226-682-9.

PETROWSKI, T., KURKA T. *Bezpečí na internetu pro všechny*. Liberec: Dialog, 2014. ISBN 978-80-7424-066-9.

PHORA, V. V. *Internet security dictionary*. New York: Springer, 2002. ISBN: 0-387-95261-6.

PROSISE, CH., MANDIA, K. *Počítačový útok: detekce, obrana a okamžitá náprava*. Praha: Computer Press, 2002. ISBN 80-7226-682-9.

RHEE, M. Y. *Internet security: cryptographic principles, algorithms and protocols.* Chichester: Wiley, 2003. ISBN 0-470-85285-2.

TROST, R. *Practical intrusion analysis: prevention and detection for the twenty-first century*. Upper Saddle River: Addison-Wesley, 2010. ISBN 978-0-321-59180-7.