Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Analýza bezpečnosti a možnosti zabezpečení Google Chrome

Miroslav Štolovský

© 2015 ČZU v Praze

! ! !

Místo této strany vložíte zadání diplomové práce.
(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou diplomovou práci Analýza bezpečnosti a možnosti zabezpečení Google Chrome jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 20.3.2015 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce panu Ing. Martinu Havránkovi Ph.D. za připomínky, rady a odborné vedení při zpracování této práce.

Analýza bezpečnosti a možnosti zabezpečení Google Chrome

Analysis of safety and security options for 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.

Summary

This thesis deals with the description, analysis and security capabilities in the browser Google Chrome, but also safe use of the Internet in general. The theoretical part describes the history and development of Internet and Internet browsers. A description of Google Chrome and explanations of all the theoretical concepts with which the author later works follows in the that part. The first point of the practical part is a description of all the settings that Google Chrome has. At this point the author's recommendations are given for the highest security settings. Another part consists of an evaluation of the electronic questionnaire concerning the topic Principles of the safe behavior on the Internet. The questionnaire addressed the following topics: Passwords, Phishing and fake sites, Malware, Adware, Spyware and as the last topic firewalls and antivirus programs. The author's recommendations on how to behave in these kinds of attack and also how to prevent them are given to all analyzed subjects.

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

Keywords: Internet, web browser, Google Chrome, security, password, cookie, cache memory, phishing, firewall, antivirus program

Obsah

1 Úvod

Internet vyvolal revoluci ve světě výpočetní a komunikační techniky za účelem rozvoje a podpory klientů a služeb serverů. Dostupnost Internetu spolu s výkonnými, ale cenově dostupnými počítači umožnili paradigma komerčního světa. Vše se velmi zrychlilo přijetím Word Wide Web technologie a webových prohlížečů, což umožňuje uživatelům snadným přístup k informacím. V dnešní době se Internet ukazuje jako zásadní prostředek výměny informací. Jedná se o rozšířenou informační infrastrukturu, mechanismus pro šíření informací a médium pro spolupráci mezi jednotlivci, vládními agenturami, finančními institucemi, akademickými kruhy a podniky všech velikostí, bez ohledu na zeměpisnou polohu.

Lidé jsou stále více závislí na Internetu, ať už se jedná o osobní nebo profesionální využití, e-mailovou komunikaci, přenos souborů, vzdálenou správu zařízení, přístup na webové stránky nebo provádění obchodních transakcí. Se zvyšující se povědomím a popularitou Internetu se začínají objevovat bezpečností problémy. Bezpečnost na Internetu je nejen velmi důležitá, ale i technicky složitější, než tomu bylo v minulosti.

Internet je navržen jako heterogenní platforma tak, že lidé, kteří používají různé počítače a operační systémy spolu mohou komunikovat. Je to rozšířená informační infrastruktura ale ze své podstaty nejistý kanál pro odesílání zpráv. Když je odeslána zpráva nebo paket z jedné webové stránky na druhou, údaje obsažené ve zprávě jsou směrovány přes řadu mezistránek předtím, než dosáhne svého cíle.

Historie Internetu je složitější a zahrnuje mnoho aspektů - technologické, organizační a společenské. Samotný koncept Internetu je velkým krokem na cestě k elektronickému obchodu, celosvětové komunikaci a získávání informací.

Práce se zabývá popisem vzniku celosvětové sítě Internet, jeho rozvojem v České republice. Následuje popis historie internetového prohlížeče, kde jsou uvedeny historické příklady. V další části je to popis funkcionality internetového prohlížeče a následně konkrétní popis prohlížeče Google Chrome, jeho historie a vlastností. Práce je rozdělena do dvou částí. První teoretická část obsahuje kromě výše zmíněného ještě vysvětlení teoretických pojmů, potřebných k práci s praktickou částí.

Vlastní práce obsahuje rozsáhlý popis možností nastavení prohlížeče Google Chrome pro nejvyšší možnou bezpečnost uživatele, konkrétně se jedná o nastavení ochrany soukromí, ukládání hesel, správu údajů o prohlížení, nastavení souborů cookie a Java Scriptu. Pro další část vlastní práce byl použit elektronický dotazník, který je rozeslán vybraným autorovým spolužákům a spolupracovníkům v zaměstnání. Téma dotazníku jsou Zásady bezpečného chování na Internetu. Odpovědi na jednotlivé okruhy jsou autorem analyzovány a jsou navrhována okamžitá řešení problémů. Okruhy dotazníku jsou čtyři a jedná se o nejčastější hrozby Internetu. Jde o práci s hesly, dále pak hrozbu phishingu a zfalšovaných internetových stránek, následují možnosti ohrožení pomocí nechtěných programů, jako jsou Malware, Spyware, Adware. Posledním tématem je obrana proti škodlivému softwaru a nechtěnému úniku informací pomocí Firewallů a Antivirových programů. Celý tento dotazník je postaven přesně na míru dnešním uživatelům Internetu. Má za úkol zdokumentovat jejich chování, a zda mají povědomí o zásadách bezpečného chování na Internetu.

2 Cíl práce a metodika

2.1 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.

2.2 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 vybíráni z řad autorových spolužáků a spolupracovníků. Následně je dotazník vyhodnocen a jsou navržena řešení všech problémů, která jsou předvedena na konkrétních příkladech.

3 Přehled řešené problematiky

3.1 Historie Internetu

Myšlenka komunikace zabalené do paketů putujících po síti nezávislých uzlů vzniká v roce 1964, kdy americká společnost RAND přemýšlí nad zajištěním komunikace po nukleární válce, kdy veškeré známé komunikační technologie budou vyřazeny z provozu. Všechny uzly v síti jsou si rovny, každý z nich může vysílat, předávat a přijímat zprávy. Samotná komunikace je rozdělena na pakety, které jsou sítí posílány samostatně.

Sami o sobě nejsou důležité, důležitý je výsledek po jejich následném složení. Pokud jsou některé uzly vyřazeny z činnosti, dochází k odeslání paketů jiným směrem. Z principu se jedná o robustní řešení problému komunikace po nukleárním úderu, který v té době hrozí doslova každou hodinu.

V roce 1968 tuto myšlenku uvádí v život Národní fyzikální laboratoř ve Velké Británii, společně s Massachusetts Institute of Technology a University of California, Los Angeles. O další vývoj se zajímá vláda USA, konkrétně agentura ARPA (Advanced Research Project Agency), která se rozhodne financovat mnohem rozsáhlejší projekt přímo v USA. Přejímá koncepci paketů putujících po nezávislých uzlech, ale za uzly volí výkonné superpočítače umístěné v národních společnostech a na významných místech, například univerzity, výzkumná centra atp. [15]

3.1.1 ARPANET

V roce 1969 je v University of California, Los Angeles nainstalován první uzel, tvořící zárodek sítě ARPANET, která je pojmenovaná podle svého sponzora, již zmíněné agentury ARPA. Na konci téhož roku jsou po světě instalovány již čtyři uzly, kde tyto čtyři počítače mohou mezi sebou přenášet data, ale zároveň jsou i programovatelné ze vzdálených uzlů. Je možné také sdílení výpočetní techniky, což je velká vzácnost díky nedostatku strojového času v té době. Na patnáct uzlů se rozšiřuje ARPANET v roce 1971, o rok později dosahuje velikosti třicet sedm uzlů.

Již po roce provozu se ARPANET přeměnil na médium výměny informací a osobních zpráv. Jedná se tedy o odklonění od konceptu sídlení výpočetních zdrojů. Uživatelé používají síť k výměně informací při práci na projektech, výměně pracovních či soukromých e-mailových zpráv. Tuto přeměnu jim umožňuje přítomnost osobního účtu a účtu elektronické pošty. Během 70.tých let dochází k expanzi sítě, jedinou podmínkou pro

připojení jakéhokoliv počítače je porozumění stroje paketově orientovanému protokolu. [17]

3.1.2 Protokol TCP/IP

Původně je pro síť ARPANET používán protokol NCP (Network Control Protocol), který je postupně nahrazován propracovanějším protokolem TCP/IP. Tento protokol se dělí na 2 skupiny: Transmission Control Protocol se stará o převod zprávy do souboru paketů na odesílajícím uzlu a sestavení paketů do původní zprávy v cílovém uzlu. Internet Protocol zajišťuje trasování paketů přes jednotlivé uzly sítě. K síti ARPANET se připojují také jiné sítě, ať už dopinkové či univerzitní a je to právě protokol TCP/IP, který se používá pro propojení všech sítí dohromady. [1][12][14]

3.1.3 Vznik Internetu

V průběhu 70. a 80. let je velice snadné připojit počítače do rostoucí sítě sítí, a to hlavně díky protokolu TCP/IP, který je volně dostupný. Samotné připojení k Internetu je pro uživatele velmi levné, nebo dokonce zdarma, protože každý uzel si musí zajistit financování a technickou úroveň vybavení. Co se týče velikosti, je zřejmé, že čím více počítačů (ať již osobních nebo firemních) bude k síti připojeno, síť bude užitečnější.

V roce 1984 přichází na scénu National Science Foundation USA, která iniciuje vývoj sítě NSFNET. Děje se tak prostřednictvím jejího úřadu pro pokročilé vědecké výpočty. Jejím záměrem je zrychlit vývoj této sítě pomocí připojování rychlejších superpočítačů a novějších komunikačních linek. Tato stále se zdokonalující síť je dnes páteří Internetu v USA. Příkladu tohoto rozvoje sítě si všímají i ostatní vládní agentury, Internet se začíná také komercializovat. Objevují se první firmy, které nabízejí připojení komukoliv, kdo má zájem a dostatek peněz.

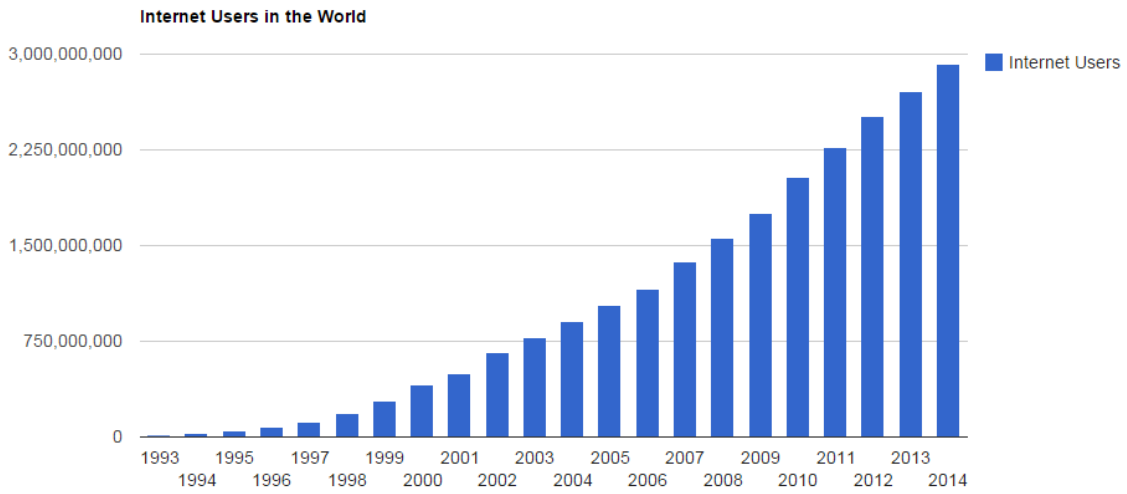
V té době se Internet dělí na skupiny, které jsou charakterizovatelné pomocí tehdy používaných domén:

GOV	Vládní organizace (govermental)
MIL	Vojenské organizace (military)
EDU	Vzdělávací instituce (educational)
COM	Komerční instituce (commercial)
ORG	Nevýdělečné organizace (organization)
NET	Brány pro připojení dalších sítí tzv. Gateways

Tabulka 1 Rozdělení domén tehdejšího Internetu

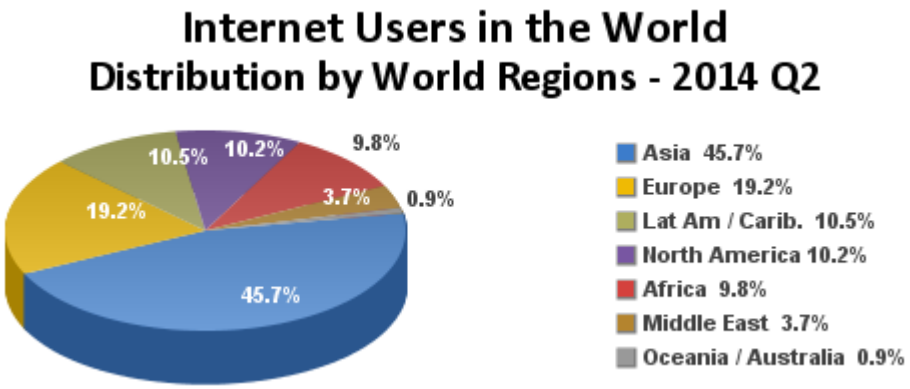
Zdroj: vlastní zpracování

Formální zánik sítě ARPANET je datován na rok 1983. Tento zánik však není uživateli zaznamenán, služby sítě fungují dál a jsou dokonce zdokonalovány. Jedná se o obrovský skok během několika let. V roce 1971 má ARPANET pouhé 4 uzly, dnešní Internet jich obsahuje cca 4 miliony a každá den přibývají další a další. [15] [17]



Obrázek 1 Počet Internetových uživatelů

Zdroj: http://www.internetlivestats.com/internet-users/



Obrázek 2 Podíl uživatelů Internetu podle geografie

Zdroj: http://www.internetworldstats.com/stats.htm

3.1.4 Historie Internetu v ČR

Ještě před příchodem Internetu je v ČR vybudována tzv. statická topologie, kdy adresování paketů není součástí zprávy, ale každý počítač (uzel) ví, kam má zprávu poslat. Konkrétně se jedná o pražský uzel CSP12 a brněnský uzel CSPUM12. Rychlost mezi

Prahou a Brnem je na tehdejší dobu stále velmi malá, konkrétně 9600 bit/s, což síť omezuje pouze na posílání textových zpráv.

Internet se do České republiky dostává po roce 1992, kdy je vybudována síť CESNET, určená pro akademické účely a financovaná sdružením organizací, které jsou do ní zapojeny. Stejně jako statická topologie má CESNET dva základní uzly, v Praze a v Brně. Tyto uzly jsou napojeny na zahraniční síť. [23]

	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
Domácnosti s vlastním osobním počítačem	**21,1**	**24,2**	**28,4**	**29,2**	**30,0**	**35,7**	**39,6**	**47,7**	**54,2**	**59,3**	**64,8**	**67,3**	**68,1**	**72,4**
Domácnosti s připojením k internetu	**5,8**	**7,9**	**11,0**	***12,4***	**19,1**	**26,7**	**32,0**	**41,7**	**49,2**	**56,0**	**61,7**	**65,4**	**67,0**	**72,2**

Tabulka 2 Počítač a internet v českých domácnostech (% podíl počtu domácností)

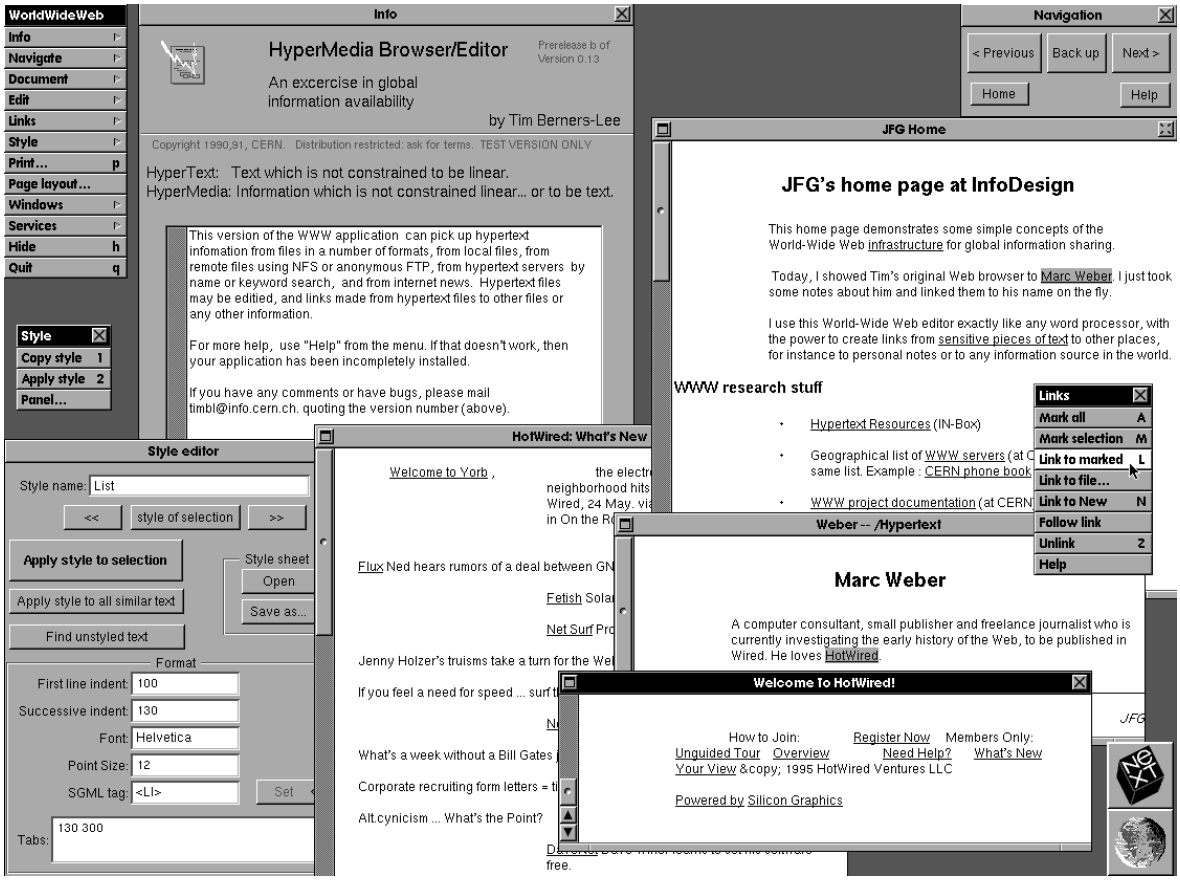
Zdroj: Statistika rodinných účtů – Český statistický úřad

3.2 Internetový prohlížeč

Webový prohlížeč je software, který umožňuje vyhledávání a prezentaci informací na Internetu. Zdrojem informací jsou pro uživatele webové stránky, obrázky, videa nebo jiný obsah umístěný na webu. Ačkoliv jsou prohlížeče určeny pro použití na webu, lze přes ně přistupovat k informacím také na soukromých sítích nebo k souborům v souborových systémech. Například nastavení domácích routerů se dnes provádí výhradně přes webový prohlížeč.

3.2.1 Historie

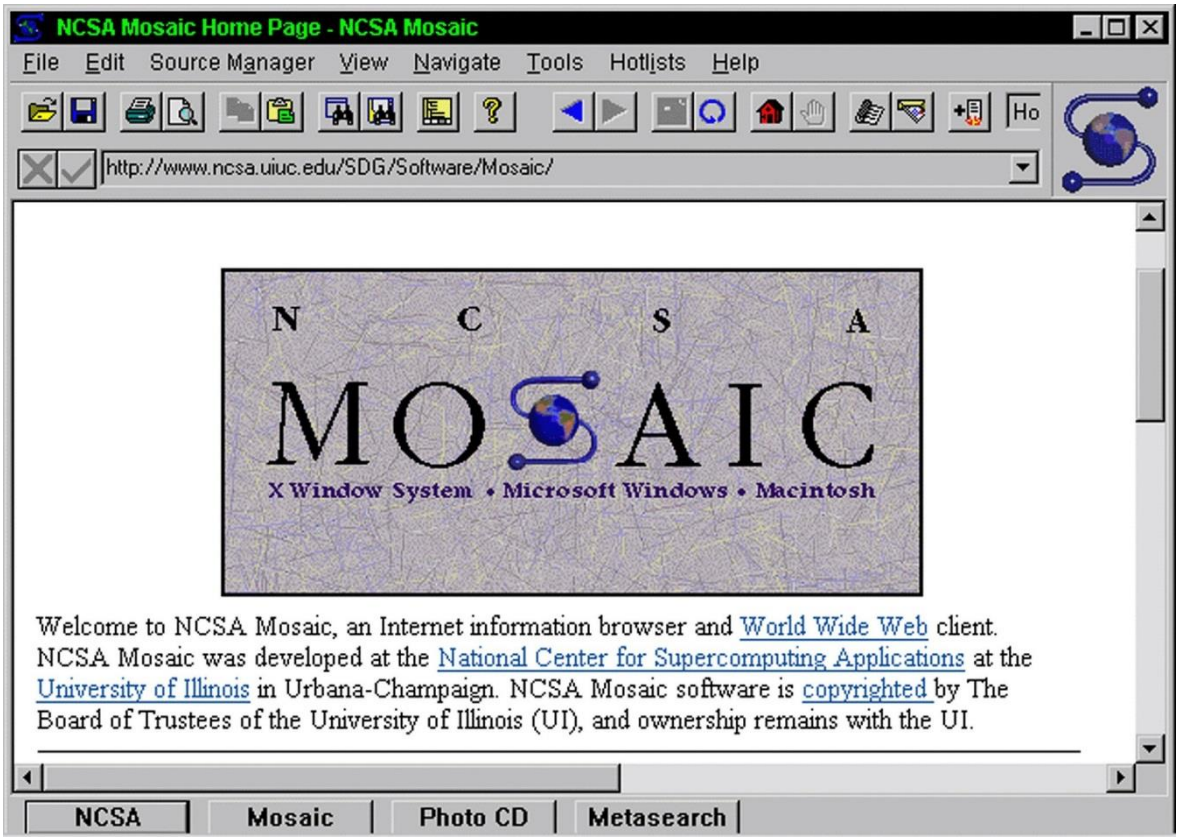
První webový prohlížeč je představen v roce 1990 Sirem Timem Berners-Leem. Berners-Lee je v té době ředitelem Word Wide Web Consortium (W3C), které dohlíží na další vývoj technologie WWW. Prohlížeč je později přejmenován na Nexus. Neobsahuje žádnou grafiku, jedná se pouze o jednoduchý textový prohlížeč.



Obrázek 3 Nexus od Tima Berners-Lee

Zdroj: http://www.w3.org/People/Berners-Lee/WorldWideWeb.html

Prvním dostupným webovým prohlížečem s grafickým uživatelským rozhraním je Erwise, který vytváří Robert Cailiau. V roce 1993 je prohlížeč inovován Marcem Andreesenem a objevuje se prohlížeč Mosaic, který je označen za první světově populární prohlížeč. Představení tohoto prohlížeče vede k masovému používání webu, protože tento prohlížeč dělá z webu snadno použitelné a přístupné místo pro běžného uživatele.

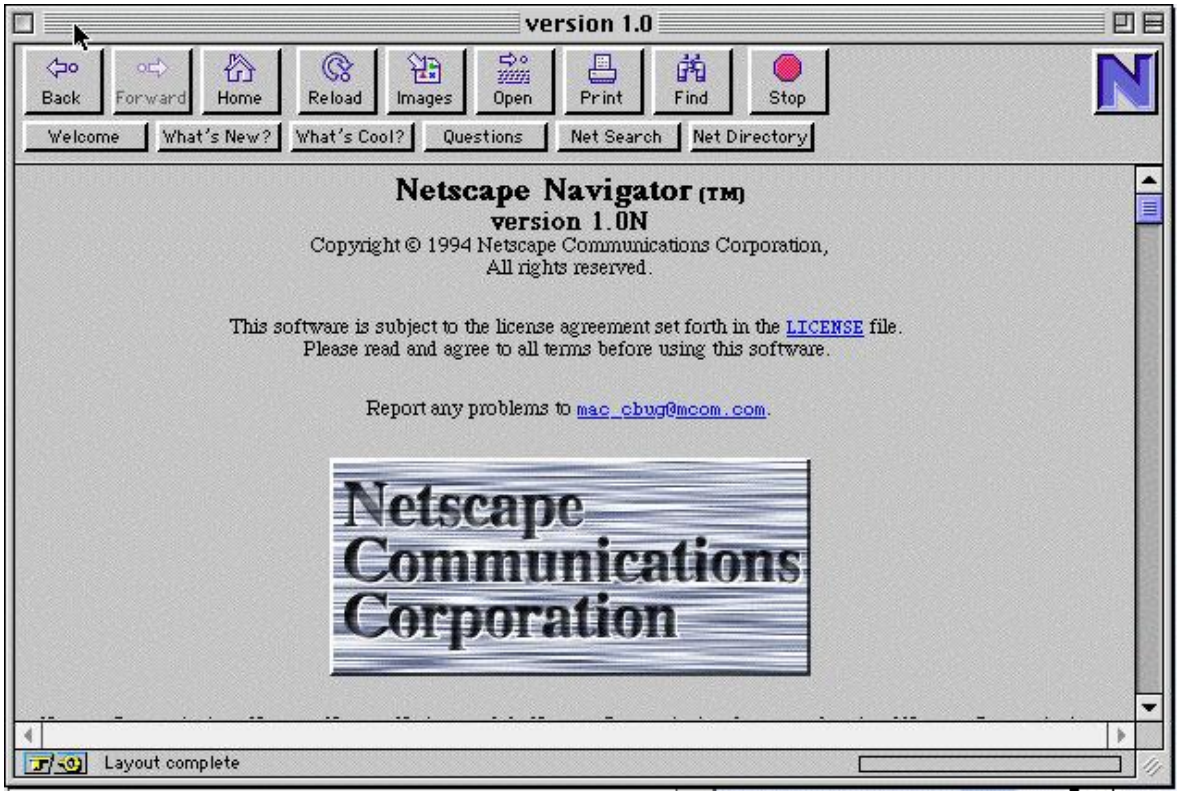


Obrázek 4 Internetový prohlížeč Mosaic

Zdroj: http://www.mystatesman.com/

V této době vede Andreseen centrum pro superpočítače (National Center for Supercomputing Applications – NCSA), ale brzy zakládá vlastní firmu pojmenovanou Netscape.

V roce 1994 vydává nástupce prohlížeče Mosaic, prohlížeč Netscape Navigator, který si velmi rychle získává na popularitě a na svém vrcholu je používán u 90% návštěvníků webu.



Obrázek 5 Netspace Navigator

Zdroj: http://www.pcworld.com/

V roce 1995 vstupuje do hry také Microsoft se svým prohlížečem Internet Explorer a začíná tvrdý konkurenční boj o získání uživatelů. V roce 2002 dosahuje IE vrcholu s 95% uživatelů.

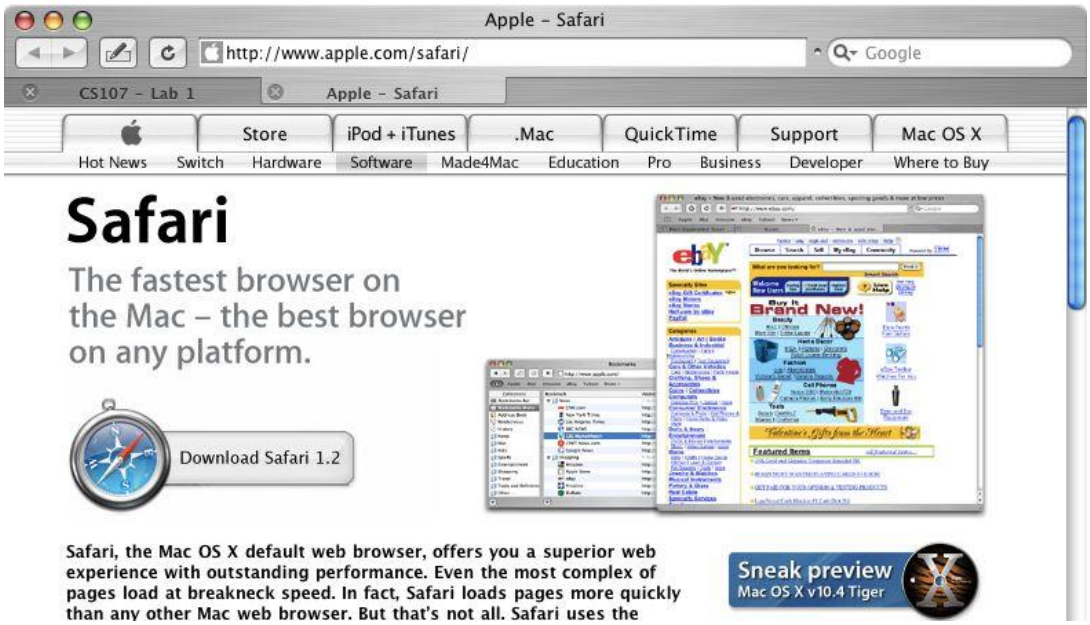
V roce 1996 se poprvé objevuje prohlížeč Opera, která ovšem nikdy nedosahuje masového rozšíření jako její konkurence. Jedinou úspěšnou verzí z hlediska rozšíření je Opera-mini, která je předinstalovaná na více než 40 milionech mobilních zařízení. Dnes Opera dosahuje na 3,2% uživatelů.

V roce 1998 se Mozilla Foundation snaží dosáhnout stejného cíle jako Netspace, ale pomocí prohlížeče používajícího volně stažitelný kód programu. Firefox 1.0 je vydán v roce 2004 a v dnešní době je na poli prohlížečů číslo tři s 15,6% uživatelů.

Obrázek 6 Mozilla Firefox

Zdroj: http://www.qweas.com/

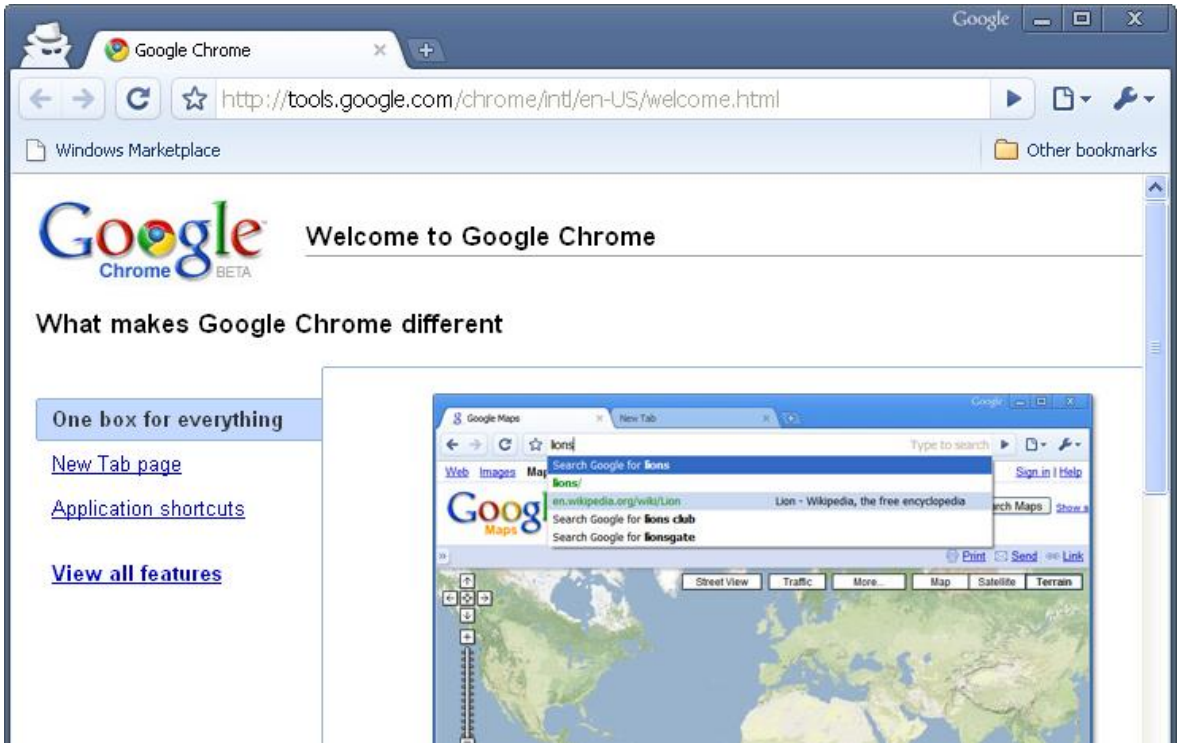
Firma Apple přichází se svým prohlížečem Safari v roce 2003. Na počítačích Apple se systémem OS X je sice dominantní, ale na celém trhu jí patří pouze 14,6% podíl.



Obrázek 7 Safari od Apple

Zdroj: http://www.bowdoin.edu/

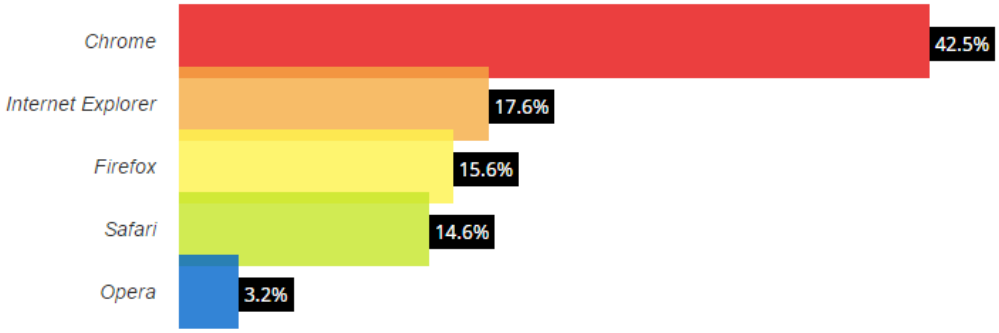
Největším hráčem na poli prohlížečů je Google Chrome, který má premiéru v září roku 2008. Jeho nástup je opravdu raketový, po velmi krátké době předhání všechny konkurenty a v dnešní době mu patří 42,5% trhu.



Obrázek 8 Google Chrome

Zdroj: http://www.google-chrome-brothersoft.com/

Obrázek níže ukazuje dnešní podíl uživatelů Internetu podle toho, jaký používají prohlížeč.



Obrázek 9 Podíl prohlížečů na Internetu

Zdroj: http://www.w3counter.com/globalstats.php

3.2.2 Funkce

Hlavním účelem prohlížeče je přinášet informace uživateli, umožnit jejich zobrazení a dát mu k nim přístup pro práci s nimi. Proces začíná zadáním adresy požadované stránky, takzvané URL – Uniform resource locator. URL je spojená také s URI, což je Uniform resource indetifier. Jedná se o předponu před adresou, tedy např.: HTTP, HTTPS, FTP aj. HTTP slouží k zobrazování internetových stránek, stejně jako HTTPS, kde „s“ na konci značí secured, tedy zabezpečené internetové stránky. Protokol HTTP neznačí nezabezpečené stránky, ale technologie použitá pro HTTPS je trochu jiná. FTP znamená File Transfer Protocol, tedy protokol pro přenos souborů, který slouží k připojení vzdáleného datového úložiště.

Po načtení zdroje je zobrazena webová stránka. K zobrazení slouží jazyk HTML a přidružený obsah, například CSS, který informuje, jaký má mít stránka vzhled, pozadí, písmo, členění textu atp. Kromě HTML mohou webové prohlížeče zobrazovat také jiný obsah – obrázky, audio, video, flash animace atd. [16] [18] [19] [25] [28]

3.3 Google Chrome

Jedná se o volně stažitelný internetový prohlížeč vyvinutý firmou Google. V dnešní době je to nejvíce používaný prohlížeč s podílem 42,5% z celkového počtu uživatelů. Aplikace funguje na všech rozšířených operačních systémech. Jedná se o: Microsoft Windows XP SP2, Windows Vista, Windows 7, Windows 8, dále také serverové systémy Windows server 2003, 2008, 2008 R2, 2012, operační systém OS X od Apple ve verzi 10.6 a pozdější, Linux ve všech verzích a distribucích. A v neposlední řadě je aplikace vyvinuta pro mobilní operační systémy Android 4.0 a pozdější a iOS 6.0 a pozdější. Jak je vidět z výčtu, konverze je opravdu široká a pokud k tomu přidáme vysokou stabilitu systému, je podíl uživatelů Google Chrome snadno pochopitelný.

Obrázek 10 Logo Google Chrome

Zdroj: http://www.diit.cz/

3.3.1 Historie

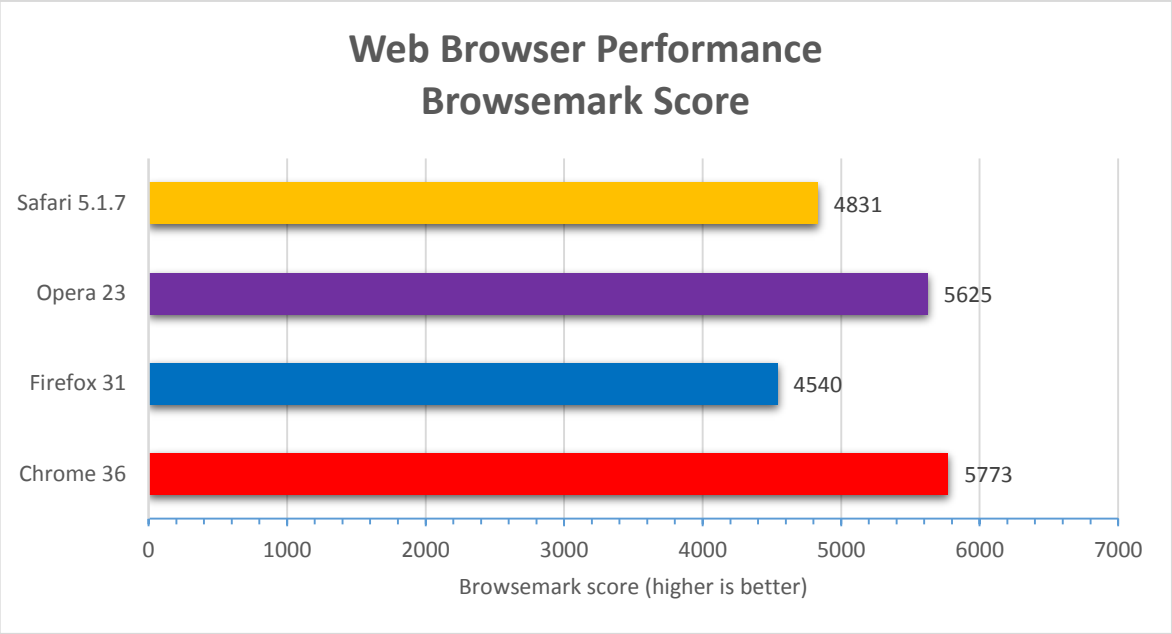
Prvními vývojáři Google Chrome jsou Sergey Brin a Larry Page, kteří najímají několik programátorů v té době již úspěšného prohlížeče Mozilla Firefox. Svou práci přestavují generálnímu řediteli firmy Google Ericu Schmidtovi, který do té doby odmítá vývoj vlastního prohlížeče, protože se nechce pouštět do velmi lítého konkurenčního boje o přízeň uživatelů Internetu. Ukázka software ale zcela mění jeho názor.

Prohlížeč je oficiálně představen 2. září 2008, vydání je určeno pro operační systém Windows XP a podporuje 43 světových jazyků. Velice rychle si získává 1% podíl u uživatelů, a to ještě v roce 2008. Na začátku roku je ohlášeno vydání verzí i pro ostatní operační systémy, tedy pro OS X od Apple a Linux. Stává se tomu tak až na konci roku, v prosinci. Pozdní vydání těchto verzí je odůvodněno delším testováním, aby vyšlé verze byly opravdu dokonalé. V roce 2010 vychází verze 5.0, kterou již podporují všechny operační systémy najednou. V roce 2010 dochází také k jinému milníku, Google Chrome je jedním z 12 prohlížečů, které si lze zvolit jako výchozí při instalaci Microsoft Windows.

V roce 2012 je spuštěna beta verze Google Chrome pro Android 4.0. S nástupem Android 4.1 je na mnoha zařízeních Chrome předinstalovaný jako výchozí prohlížeč. [21]

3.3.2 Vlastnosti

Hlavní snahou Google Chrome je být rychlý, bezpečný, jednoduchý a stabilní. Rozdíly od konkurence jsou značné. Prohlížeč působní minimalisticky, což je do té doby velmi nezvyklé. Silnou stránkou je výkon aplikace, autor se nikdy nesetkává s chybovou hláškou označující nějaký nedostatek výkonu aplikace. Všechny tyto názory podporuje i nezávislý test zveřejněný časopisem PC World v září 2009. K testu jsou použity aplikace BrowserMark a PeaceKeeper, samotné testování spočívá v rychlosti načtení kompletního obsahu HTML 5. Níže na obrázku je výsledek, který lze snadno interpretovat. Google Chrome je vítěz, ovšem Opera je v těsném závěsu. Tyto dva produkty jsou opravdu jedinou konkurencí, ačkoliv celkový podíl uživatelů zcela jasně vychází vstříc prohlížeči Chrome. [24]



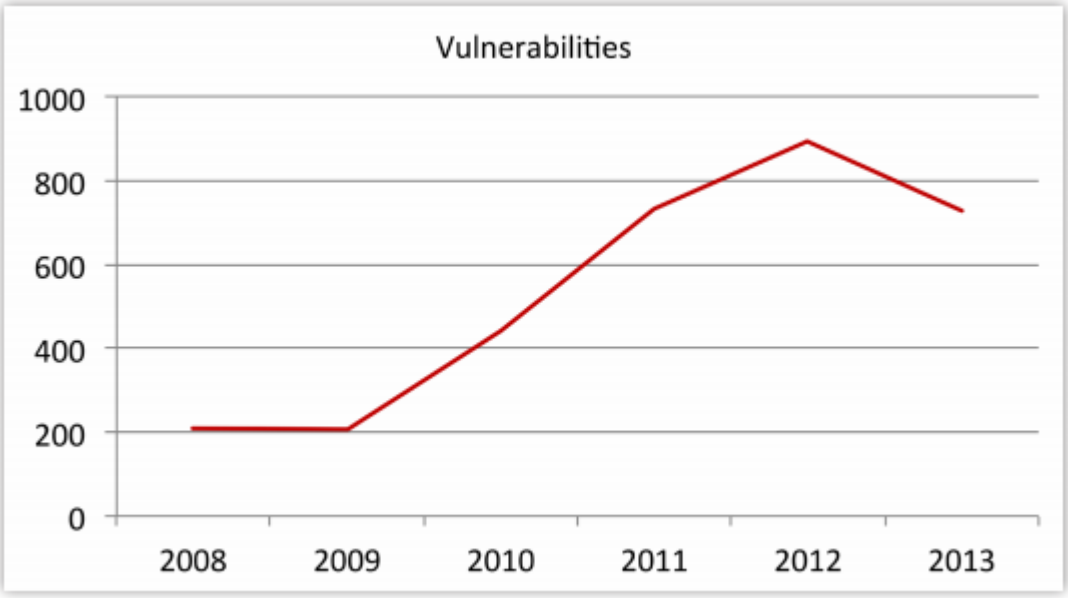
Obrázek 11 Výsledek porovnání prohlížečů z hlediska výkonu

Zdroj: http://www.pcworld.com/article/2605933/browser-comparison-how-the-five-leaders-stack-up-in-speed-ease-of-use-and-more.html

Prohlížeč Google Chrome pravidelně aktualizuje dvě černé listiny, konkrétně černé listiny pro phishing a pro Malware. Hrozba phishingu je dnes velmi rozšířená a dle autorova názoru se s ní setkal již každý. Jedná se o podvodný e-mail, který ovšem předstírá, že pochází z internetových stránek banky, úřadů státní správy, sociálních sítí, aukčních portálů, energetických společností, společností poskytujících úvěry atp. V této e-mailové komunikaci je adresát vyzván k zadání citlivých osobních údajů přes falešnou stránku, na kterou je v komunikaci uveden odkaz. Tyto stránky bývají na oko identické od pravých, ale zadáním citlivých údajů, například jména a hesla k internetovému bankovnictví, jsou schopni útočníci toto konto vykrást. Naproti tomu Malware je malý počítačový program, který slouží k vniknutí do operačního systému, nebo také k jeho poničení. Někdy bývají splněny obě vlastnosti tohoto útoku, program vnikne do systému, ukradne citlivá data, jako jsou právě přihlašovací údaje například do bankovnictví a posléze se sám smaže a k tomu zničí další důležitá data. Příkladem šíření tohoto nechtěného software je také e-mailová komunikace, která obsahuje například upozornění o smyšlené neuhrazené faktuře, kde je uživatel upozorněn, aby zaplatil dle souboru, který nalezne v příloze. Otevřením této přílohy dochází k automatickému běhu programu uvnitř a instalaci škodlivého software. Takto napadené systémy mohou být například použity k páchání další podvodné činnosti, jako je rozesílání těchto podvodných e-mailů, šíření

nezákonného obsahu nebo zapojení do distribuovaných útoků (tzv. DDoS) způsobujících nefunkčnosti jiných systémů. Google představuje skenování stahovaných souborů už ve verzi 17 v roce 2012. [2]

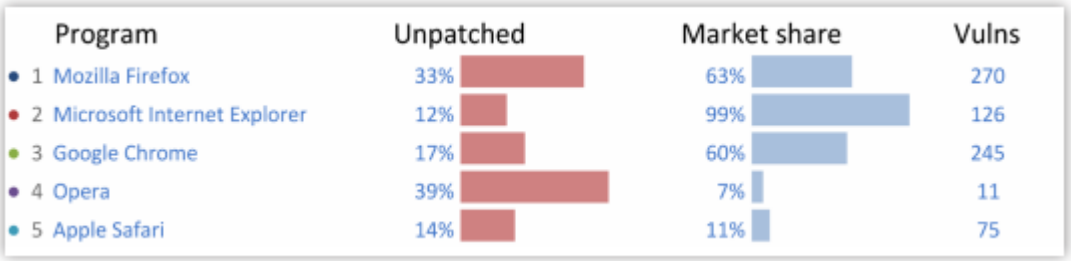
Všechny prohlížeče jsou testovány z hlediska zranitelnosti, není tomu jinak ani u Google Chrome. V některých případech jsou nabízeny i odměny pro útočníky, kteří pouze upozorní na chybu. V roce 2012 se francouzskému teamu hackerů podaří převzít plnou kontrolu nad operačním systémem právě přes Google Chrome. Šéf bezpečnosti Jason Kersey dokonce pogratuluje útočníkům a označí jejich kousek za umělecké dílo, které si zaslouží uznání a obdiv. Opravy bezpečnostní chyby byly implementovány do systému Chrome během deseti hodin. Firma Secunia, která se specializuje na odhalování těchto bezpečnostních rizik, vydává každoročně tabulku srovnání chyb prohlížečů seřazených podle důležitosti. Na grafu níže je vidět, že počet chyb klesá, ale přesto se jedná o velmi vysoké číslo.



Obrázek 12 Počet chyb zabezpečení 5 nejpoužívanějších prohlížečů

Zdroj: http://secunia.com/?action=fetch&filename=secunia_vulnerability_review_2014.pdf

Testovány jsou prohlížeče Google Chrome, Mozilla Firefox, Internet Explorer, Opera a Safari. Dohromady je zjištěno 727 chyb, jedná se o chyby označené jako vysoce kritické. Na dalších obrázcích je rozdělení těchto chyb na konkrétní prohlížeče s dvěma dalšími ukazateli. Prvním ukazatelem je podíl trhu, kde je na počítačích nainstalován software Secunia PSI, který umožňuje tyto chyby sledovat. Druhým ukazatelem je procento neopravených chyb ve smyslu nevydané opravy od vývojářů nebo liknavosti uživatelů si tuto opravu stáhnout. [26]

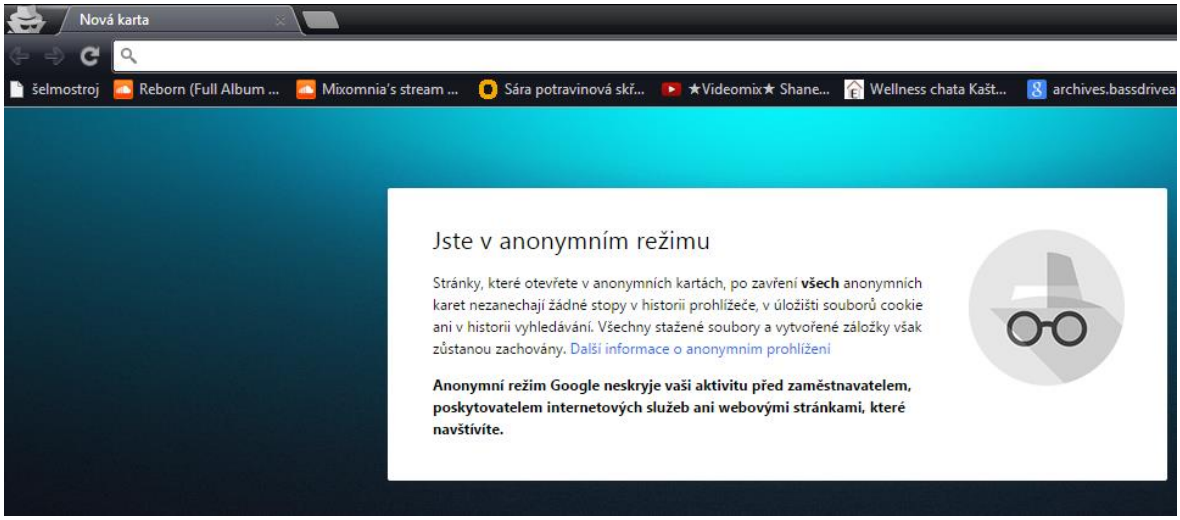


Obrázek 13 Rozpad porovnání chyb zabezpečení prohlížečů

Zdroj: http://secunia.com/?action=fetch&filename=secunia_vulnerability_review_2014.pdf

Z hlediska sledování práce s prohlížečem jsou v Google Chrome použity sledovací nástroje, které jsou buď vypnutelné, nebo ne. Při instalaci je to náhodně vygenerovaný token, který slouží k měření úspěšnosti instalace. Dále se jedná o predikce zápisu do adresního řádku prohlížeče, kdy si prohlížeč pamatuje uživatelem napsané vyhledávací hesla. Server Google Update sbírá veškeré informace o instalaci prohlížeče a poté o jeho užívání. Zapisuje si datum instalace, odkud byl instalační soubor stažen atp. Samotnou kapitolou je služba Google Analytics, která se zaměřuje na vyhledávání přes Google. Tato služba sleduje vyhledávání na stránce google.com, nemá nic společného s prohlížečem. Uživatelé něco hledají, například domácí spotřebiče a později při prohlížení Internetu jsou jim v reklamách nabízeny právě tyto spotřebiče. Jedná se o data, která byla sesbírána právě pro vyhledávání a propojena s uživatelem (pomocí IP adresy, MAC adresy), aby mu v pozdějších fázích návštěvy Internetu mohla být nabízena cílena reklama. Tento marketingový nástroj může být leckdy obtěžující, ale z pohledu prodejů velmi efektivní. [8]

V prohlížeči Google Chrome existuje tzv. Anonymní mód, který zabraňuje ukládání stop v historii prohlížeče. Co zůstává zachováno, jsou uložené soubory a vytvořené záložky.



Obrázek 14 Anonymní režim Google Chrome

Zdroj: vlastní zpracování

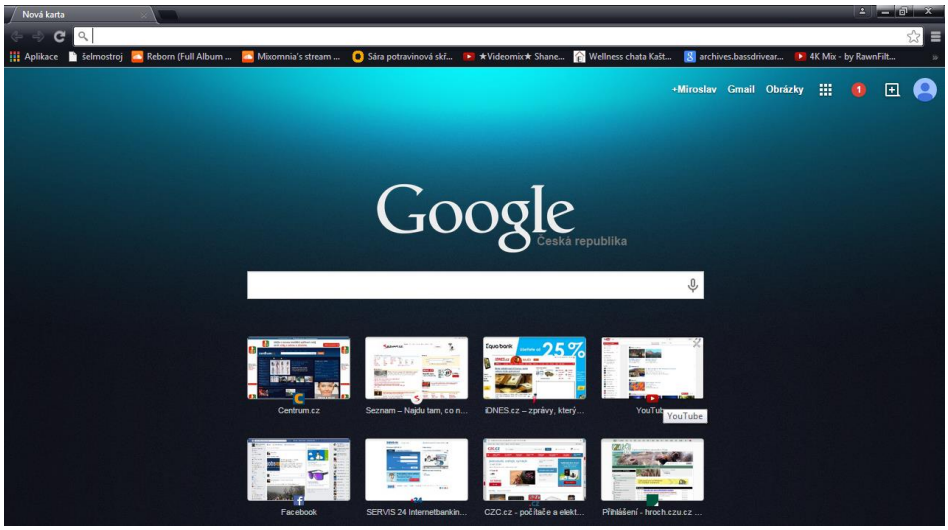
Velkou předností Google Chrome je použití utility Správce úloh, stejné jako tomu je v operačních systémech Windows. Správce úloh umožňuje zobrazit, které stránky a zásuvné moduly používají nejvíce paměti a procesoru a umožňuje je ukončit. V samotném jádru Chrome je implementována architektura více procesů, kdy každému zásuvnému modulu nebo otevřené stránce je přidělen právě jeden proces. Toto zabraňuje vzájemnému rušení zpracování úkolů a zároveň to zvyšuje stabilitu a bezpečnost celé aplikace. Potenciální útočník, který získá kontrolu nad jedním procesem, se nemůže dostat k dalšímu. Například od Internet Explorer je to změna, kdy po pádu Chrome dochází k pádu pouze části, kdežto Internet Explorer padá celý.

Obrázek 15 Chyba v Google Chrome

Zdroj: http://www.googlechromefans.com/

Uživatelské rozhraní Google Chrome je opravdu minimalistické. Zcela nahoře již není lišta s názvem programu, ale karty otevřených webových stránek, které se dají přesouvat mezi sebou, nebo vytažením ven z prohlížeče otevřít nové okno. Při otevření nové karty či okna je v Google Chrome k dispozici tzv. úvodní obrazovka, která obsahuje odkaz na osm nejčastěji používaných stránek a samozřejmě také vyhledávací pole Google. Pokud uživatel vlastní jakýkoliv účet od Google, vpravo nahoře je ovládací panel pro jeho účet. Je zde přístup k sociální síti Google+, přístup k e-mailové schránce Gmail, k disku a všem ostatním službám Google. Pod kartami vlevo jsou tři tlačítka pro pohyb zpět, vpřed a znovunačtení. Tomuto řádku dominuje Omnibox, který slouží k zadávání adresy nebo k přímému vyhledávání přes google.com. Omnibox při psaní textu nabízí buď nejčastěji uživatelem zadávané fráze, nebo přímo návrhy internetových adres, seřazených opět podle frekvence návštěvnosti a relevance. V pravé části Omniboxu je znak hvězdičky, který slouží pro rychlé ukládání stránek do Oblíbených položek uživatele, vpravo vedle hvězdičky je vlastně menu celé aplikace s možnosti otevření nové stránky, karty, anonymního režimu, nastavení prohlížeče, historie atd.

Google Chrome obsahuje i další nástroje, které jsou pro běžného uživatele nadbytečné. Je to možnost zobrazení zdrojového kódu stránky. Tato možnost se velmi osvědčila autorovi práce při předmětu ICT pro manažery, kdy bylo nutné napsat webové stránky. Analýza některých prvků moderních internetových stránek právě přes zdrojový kód byla neocenitelným pomocníkem. Dále jsou to nástroje po vývojáře, které poskytují zcela vyčerpávající informace o stránce, běžících procesech na ní, objektech atp. [20]



Obrázek 16 Úvodní stránka Google Chrome

Zdroj: vlastní zpracování

3.4 Vysvětlení pojmů používaných ve vlastní práci

Soubory cookie jsou textové soubory, které obsahují informaci o stavu prohlížeče při návštěvě internetové stránky. Pro každou je založen samostatný soubor, který slouží k poskytnutí informace serveru o návratu uživatele. Pokud uživatel provede na internetové stránce nějaké nastavení, vyplní formulář, zaregistruje se, soubor cookie tyto informace uloží a použije při pozdější návštěvě. Nejčastěji se soubory cookie používají pro ukládání adres.

JavaScript – jedná se o na světě nejpoužívanější programovací jazyk napsaný jazykem HTML, vyvinutý v roce 1995 Brendanem Eichem. Jde o klientský skript. Program se odesílá do prohlížeče uživatele a tam je vykonáván. Účelem jazyka je učinit internetové stránky více dynamické. Pomocí jazyka jsou ovládány interaktivní prvky, jako jsou tlačítka, textové pole. Také se s jeho pomocí tvoří animace a efekty obrázků.

URL znamená uniform resource locator, tedy v překladu jednoznačné určení zdroje. Používá se pro přesnou identifikaci dokumentů na Internetu. Dokumentem může být internetová stránka, soubor. Uživatel chápe URL jako internetovou adresu, která se dělí na více částí. První část je protokol, nejčastěji se jedná o HTTP. Dalšími části jsou doména nejvyššího řádu (com), doména druhé úrovně (google) a doména třetí úrovně (www). Dále může url obsahovat koncovku, číslo portu, jméno a heslo pro přístup, parametry stránky atd.

Hypertext Transfer Protocol (HTTP) je počítačový protokol určený k přenosu dokumentů ve formátu HTML. Funguje na principu dotaz-odpověď, internetový prohlížeč se v tomto případě chová jako klient, která zasílá dotaz na server, tedy požadovanou internetovou stránku. Server odpovídá na tento dotaz prohlížeči a zobrazí požadovanou stránku nebo nabídne požadovaný soubor.

Cache paměť prohlížeče zabírá část na disku uživatele a slouží k ukládání součástí internetových stránek pro jejich rychlejší načítání. Jedná se například o obrázky, javascript, kaskádové styly css. Pro správné fungování stránek je někdy nutné cache paměť aktualizovat pomocí příkazu CTRL+F5.

Digitální certifikát vydává certifikační autorita a jedná se o digitálně podepsaný veřejný šifrovací klíč. Certifikát slouží k ověření identity uživatele, pokud chce uživatel navázat zabezpečenou komunikaci a zajistit šifrování přenášených dat. V zabezpečené komunikaci hraje důležitou roli soukromý klíč, který je unikátní pro každého uživatele a je

nutné ho chránit. Z hlediska bezpečnosti se jedná o nejslabší článek kvůli možnému odcizení a zneužití nepovolanými osobami.

Plugin je slovo převzaté z angličtiny a dá se volně přeložit jako zásuvný modul. Prohlížeče se dnes dají pomocí těchto rozšíření proměnit na velmi všestranný nástroj. Dokáží zobrazit dokumenty všech typů, přehrát videa a zvuky všech formátů a činí prohlížení stránek více komfortním. Existují například zásuvné moduly, které brání zobrazování reklam na stránkách, umožňují ztmavit pozadí stránky při přehrávání videa atp.

Antivirus je program na ochranu proti škodlivému software. Na trhu je několik stovek těchto produktů, ale do absolutní špičky patří jen pár. Vývojáři těchto programů neustále aktualizují tzv. virové definice, kdy antivirus dostává informace o chování virů a jiného škodlivého software. Antivirus provádí průběžné skenování operačního systému a navštěvovaných stránek a na každé podezřelé chování uživatele upozorní, nebo přímo provede definované kroky. Nejčastěji se jedná o zamezení přístupu na stránky, umístění souboru do karantény, kde nemůže provádět své procedury, nebo přímo smazání infikovaného souboru.

Firewall je anglické označení brány, která odděluje provoz mezi Internetem jako takovým a domácí sítí. Monitoruje odchozí a příchozí provoz uživatelova počítače a dle nastavených pravidel zabraňuje průniku nezvaných návštěvníků zvenčí nebo naopak odesílání informací z počítače do sítě bez vědomí uživatele.

Jako Adware jsou označovány programy, které uživateli zobrazují reklamy při práci. Do počítače se mohou dostat s instalací nějaké programu, který je bezplatný. Vývojáři těchto bezplatných aplikací využívají právě Adware a s ním spojenou reklamu k financování vývoje. Nezkušený uživatel, si takovýto škodlivý software nainstaluje do počítače velmi snadno, protože pouze potvrdí všechny položky v instalaci. Je proto nutné se instalaci věnovat a instalovat opravu pouze chtěné programy. Existuje více druhů agresivity těchto programů. Jedná se o zobrazování reklamy v prohlížeči až po změnu nastavení domovské stránky, které je velmi těžké změnit zpátky. Hlavním rozdílem oproti Spyware je instalace se souhlasem uživatele.

Spyware se instaluje bez vědomí uživatele a většinou slouží k odesílání dat z počítače, aniž je o tom uživatel informován. Nejčastěji jsou to statistiky návštěv. Ale tyto programy dokáží odesílat i citlivá uživatelská data jako jsou přihlašovací údaje, hesla, čísla

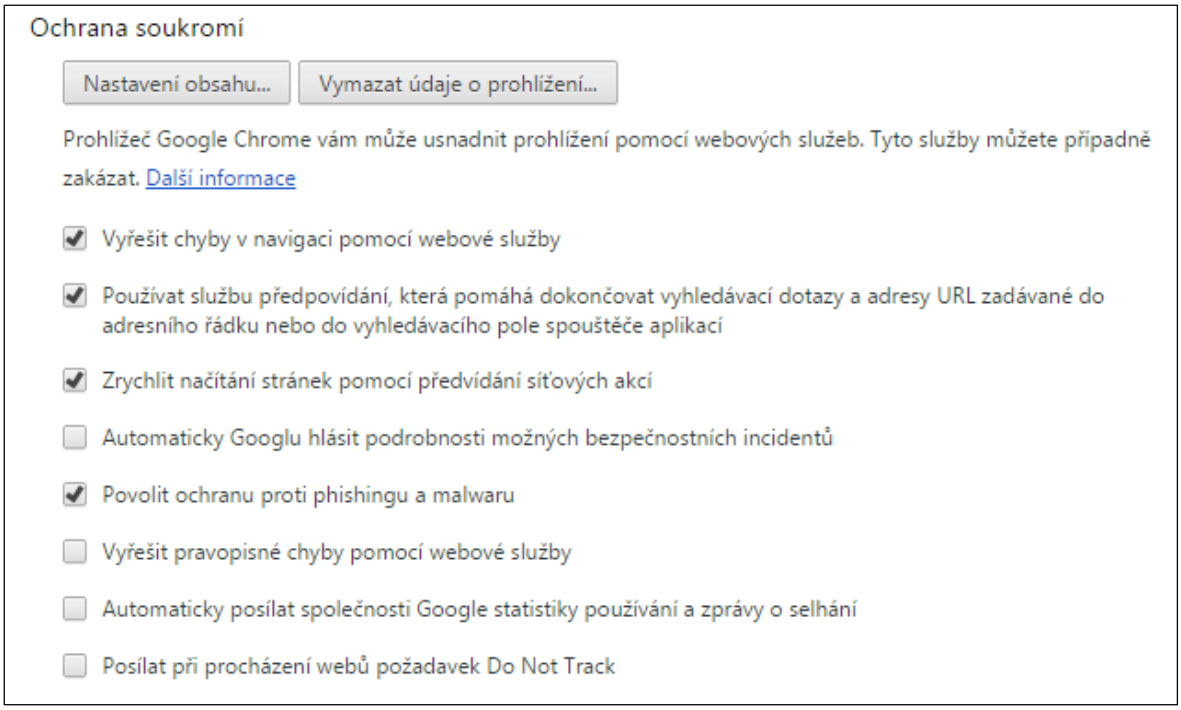
účtů, karet atp. Existuje také Spyware, který dokáže otevřít tzv. zadní vrátka operačního systému a umožnit útočníkovi získat plnou kontrolu nad počítačem. Toto z nich dělá potenciální hrozbu, kterou je nutné řešit.

Zkratka PIN pochází z anglického Personal Identification Number, tedy v překladu osobní identifikační číslo. Jedná se o autorizační nástroj, který se váže na uživatelova práva nakládat například s platební kartou, s mobilním telefonem atp. Rozsah PINu není nikde stanoven, ale například u platební karty se jedná o kombinaci čtyř číslic. Zadání kombinace je možné několikrát opakovat, ovšem po vyčerpání pokusů dojde k zablokování tohoto kódu a je nutné kontaktovat instituci, která PIN kód vydává. Toto je také jedna z ochran, kterou PIN kód nabízí.

4 Vlastní práce

4.1 Možnosti zabezpečení Google Chrome

4.1.1 Ochrana soukromí



Obrázek 17 Ochrana soukromí Google Chrome

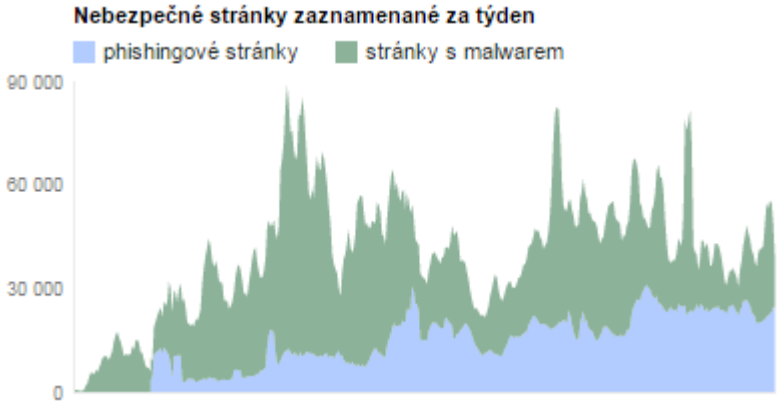
Zdroj: vlastní zpracování

Prohlížeč Google Chrome umožňuje velmi pokročilé nastavení způsobu prohlížení stránek. Tato služba se nazývá Ochrana soukromí a poskytuje uživateli více možností, například integrovanou ochranu proti phishingu, Malware. Tuto asistenci lze v prohlížeči úplně vypnout a zamezit tím jakémukoliv odesílání zpráv s informacemi o prohlížení do společnosti Google. Pro odesílání a ukládání informací o prohlížení vydává společnost Google tzv. Sdělení k ochraně soukromí pro Google Chrome, které podléhá zásadám ochrany soukromí společnosti Google. Zkrácená verze sdělení k ochraně soukromí je uvedena v Přílohách této práce.

Služba Ochrana soukromí je po instalaci prohlížeče spuštěna. Prohlížeč povoluje soubory cookie, obrázky a JavaScript.

4.1.2 Upozornění na phishing a Malware

Tyto výrazy jsou vysvětleny v teoretické části práce. Ve společnosti Google pracuje nemalý tým bezpečnosti, který vyvíjí a aktualizuje službu bezpečného prohlížení, které rozpoznává stránky s nebezpečným obsahem. Na tyto stránky poté upozorňuje uživatele a správce webu. Tato služba se netýká jen prohlížeče Google Chrome, ale je poskytována skrz celý Internet všem prohlížečům. Služba Bezpečné prohlížení běží neustále a každý den zkontroluje přibližně miliardu adres webových stránek. Nálezů je mnoho a u všech nebezpečných stránek je zobrazeno upozornění. Nejčastěji se právě jedná stránky s Malware a phishingové stránky. Stránky s Malware jsou schopny do cizích počítačů nainstalovat software, který dokáže ukrást soukromé údaje, případně dokáže ovládnout počítač a páchat z něj další trestnou činnost jako jsou další šíření Malware a virů, nebo distribuované síťové útoky (DDoS) sloužící k vyřazení určitých stránek z provozu. Phishingové stránky jsou vlastně podvržené stránky, které mají vypadat jako originál, ale zadané citlivé údaje jsou poté zneužity v uživatelův neprospěch.



Obrázek 18 Nebezpečné stránky zjištěné službou Bezpečné prohlížení

Zdroj: http://www.google.com/transparencyreport/safebrowsing/

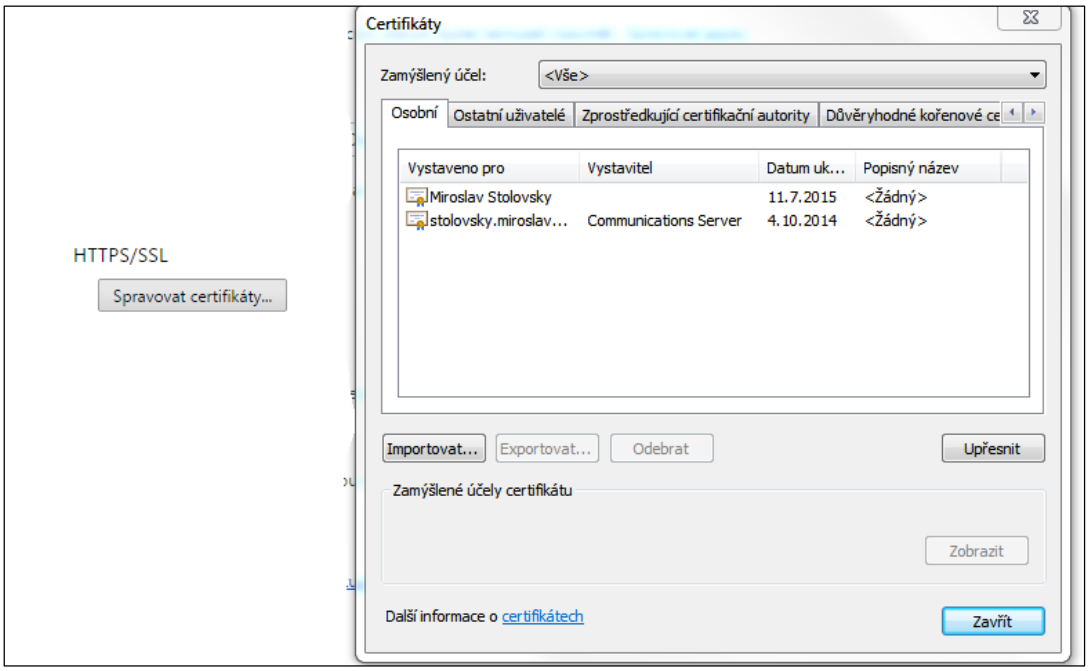
Po zjištění takové hrozby je kontaktován správce napadeného webu, kde mu je společností Google nabídnuta pomoc při odstranění nebezpečí. Ta probíhá buď formou označení škodlivého kódu, nebo přímou konzultací bezpečnostních pracovníků.

4.1.3 Protokol SSL

Zkratka znamená Secure Sockets Layer a zajišťuje zabezpečení komunikace pomocí autentizace a šifrování. Jedná se o vrstvu, která je vložena mezi transportní vrstvu (TCP/IP) a vrstvu aplikační (HTTP). Pokud dojde k vytvoření SSL session je komunikace zašifrována a bezpečná proti odposlechu. Autentizace vytvoření session se provádí pomocí certifikátů. Tyto certifikáty vystavují důvěryhodné certifikační autority a používají se například při komunikaci se státními institucemi, pojišťovnami, bankami atp.

Šifrování SSL je asymetrické, každá z komunikujících stran má dva klíče, veřejný a soukromý. Veřejný klíč je předáván všem, kteří chtějí komunikovat. Pomocí tohoto klíče je zpráva zašifrována, ale rozšifrovat ji dokáže jen ten uživatel s odpovídajícím soukromým klíčem. Samotné SSL spojení je trochu složitější. Klient vysílá požadavek na ustavení SSL spojení serveru, který mu vzápětí odpovídá. Odpověď obsahuje požadovaný certifikát serveru, kterým si naopak klient ověří autorizaci serveru. Poté klient zašifruje zprávu veřejným klíčem a odesílá zprávu serveru, který ji rozšifruje soukromým klíčem. Dojde k vytvoření a potvrzení hlavního šifrovacího klíče a od této doby spolu klient a server komunikují zašifrovaně potvrzeným klíčem. Nyní již je tato komunikace neodposlechnutelná.

V prohlížeči Google Chrome je toto nastavení velmi jednoduché, vlastně jen přepne uživatele do správce certifikátů. V rámci bezpečnosti se důrazně nedoporučuje osobní certifikáty exportovat na přenosná zařízení a ty předávat jiným osobám. V dnešní době se certifikáty používají pro mnohou komunikaci a ověření identity osob, firem a úřadů. Odcizení soukromého certifikátu může mít fatální následky, ve smyslu likvidace peněžních prostředků soukromé osoby či firmy, nebo například obrovské riziko zadlužení. [27]



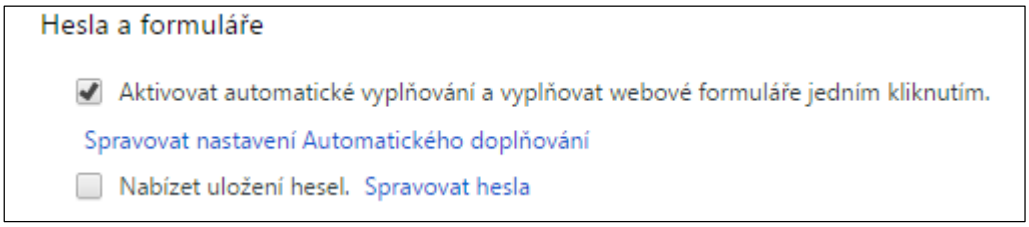
Obrázek 19 Správce certifikátů

Zdroj: vlastní zpracování

4.1.4 Správce hesel

Stejně jako ostatní prohlížeče umožňuje i Google Chrome ukládat hesla do tzv. správce hesel. Z pohledu bezpečnosti se ovšem jedná o velké riziko. Pokud se na PC střídá více uživatelů a mají jeden uživatelský účet, je ukládání hesel na jednotlivé stránky velmi riskantní. Samozřejmě, že některé stránky jako například internetové bankovnictví, různé internetové servisy pojišťoven, stavebních spořitelen, energetických společností možnost nenabízejí, ostatní stránky ale ano. Velké nebezpečí se týká například dnes velmi populárních sociálních sítí, kdy nezvaný návštěvník PC může napáchat velké škody. Na sociálních sítích se může o škody psychické, ale pokud je v prohlížeči uloženo heslo například do internetového obchodu, může se jednat i o škody materiální.

Pro zachování bezpečnosti je doporučeno ukládat hesla stránek pouze v takových případech, kdy nehrozí jakékoliv nebezpečí zneužití. Pro absolutní bezpečnost doporučuje autor práce tuto funkci úplně vypnout. Vypnutí služby se provádí v Nastavení prohlížeče odškrtnutím políčka Nabízet uložení hesel.



Obrázek 20 Správce hesel

Zdroj: vlastní zpracování

Pokud jsou již nějaké hesla uložena, nebo si uživatel potřebuje ověřit, že nejsou, je v nastavení prohlížeče umístěna položka Spravovat hesla. Zde jsou vidět všechna uložená hesla, která jsou plně editovatelná, tedy je možné je upravovat nebo smazat. Celá tabulka je rozdělena na dvě části, uložená hesla a tabulka stránek, pro které je uživatel zvolena možnost „Nikdy neukládat heslo“.

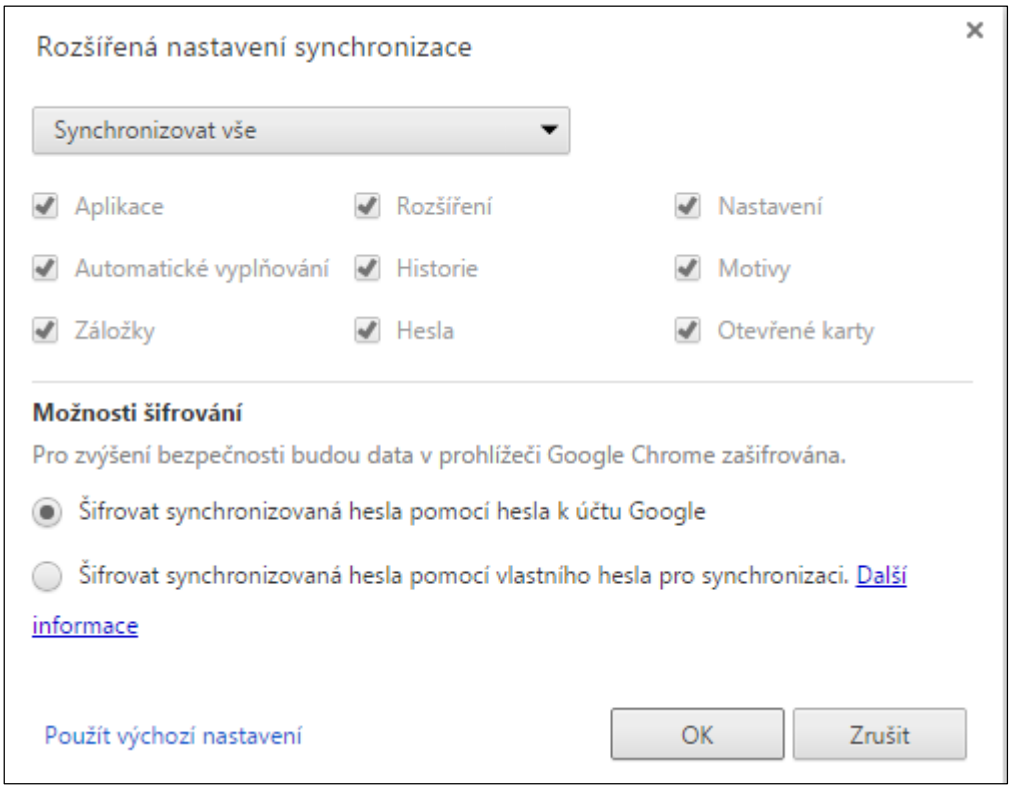
4.1.5 Přihlášení do Google Chrome

V nové verzi prohlížeče představuje společnost Google možnost přihlásit se do prohlížeče. Uživatelé tím dostávají jedinečný nástroj používat stejné nastavení prohlížeče na všech zařízeních. Synchronizují se aplikace, záložky, rozšíření, historie, ale i hesla.

Obrázek 21 Tlačítko pro přihlášení do Google Chrome

Zdroj: vlastní zpracování

Nastavení rozsahu synchronizace může uživatel upravovat a provádí se v rozšířeném nastavení synchronizace. Na výběr jsou dvě možnosti, synchronizovat všem, nebo si zaškrtnutím políček udělat výběr. Jedná se opět o bezpečnostní riziko. Sdílení informací na více zařízení přináší uživatelský komfort, ale pokud uživatel zůstane na nějakém zařízení přihlášen a k tomuto zařízení se dostane nepovolaná osoba, může útočník způsobit velké škody. Je proto nutné používat tuto možnost pouze v případech, kdy si je uživatel naprosto jist, že tato situace nemůže nastat. Autorovo doporučení je jednoduché, pro komfort uživatele stačí mít na ostatních zařízeních dostupné pouze záložky a grafické motivy. Vše ostatní může být zneužito v neprospěch uživatele.



Obrázek 22 Nastavení synchronizace

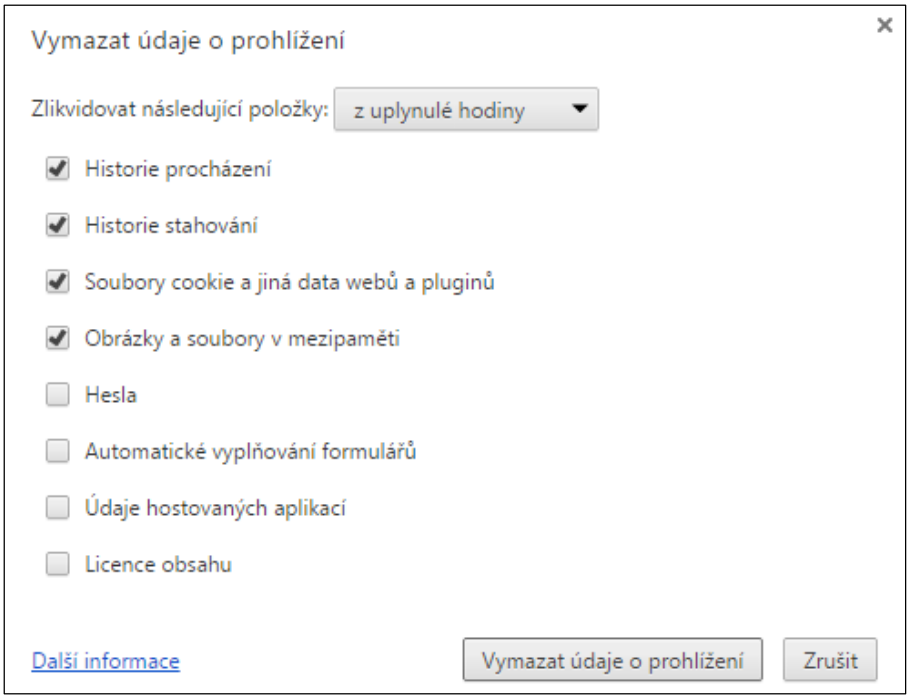
Zdroj: vlastní zpracování

Důležitou součástí správce je možnost šifrování. Kdy může uživatel použít k synchronizaci heslo do účtu Google, nebo zadat unikátní heslovou frázi. Unikátní heslová fráze je potřeba zadat na všech ostatních zařízeních a to jednotlivě. Pokud se uživatel rozhodne synchronizovat, doporučuje autor použít možnost zadání unikátní heslové fráze. Při zvolení této možnosti jsou data uložena pouze v počítači uživatele a nejsou odesílána na servery Google. Při zvolení první možnosti je tomu naopak, šifrování probíhá pomocí přihlašovacích údajů Google. Při zapomenutí šifrovacího hesla má Google připraven nástroj, který smaže všechna synchronizovaná data na serverech a odpojí všechna zařízení. Všechna data zůstanou uložená na lokálních discích jednotlivých zařízení, uživatel neztratí nastavení stránek, hesel atp. Pro obnovení synchronizace je nutné nastavit novou heslovou frázi a provést novou synchronizaci. Službu hodnotí autor jako velmi přínosnou, ale jak je již zmíněno výše, je nutné postupovat s opatrností.

4.1.6 Cache paměť a údaje o prohlížení

Do tzv. cache paměti, tedy vyrovnávací paměti prohlížeče, jsou ukládány buď celé webové stránky, nebo jejich části, které slouží k pozdějšímu rychlejšímu načítání a tedy i k menšímu zatížení sítě. Jedná se například o obrázky, nebo textové a JavaScript dokumenty, které jsou uloženy na lokálním disku uživatele. Nejen, že je občas nutné tyto soubory obnovit ke správnému načtení stránky, ale všechny tyto údaje poskytují případnému útočníkovi cenné údaje o aktivitě uživatele a autor proto doporučuje tyto údaje průběžně mazat. Navíc může promazáním některých položek dojít ke zrychlení běhu prohlížeče, který nemusí pracovat s tak rozsáhlými soubory uloženými na lokálním disku.

Pro smazání veškerých údajů o prohlížení, tedy všech, které jsou na obrázku č. 23, slouží v nástrojích příkaz „Vymazat údaje o prohlížení“. V první možnosti je na výběr časové období, volbou „od počátku věků“ dojde k vymazání všech zaškrtnutých možností.



Obrázek 23 Smazání údajů o prohlížení

Zdroj: vlastní zpracování

Tyto příkazy jsou neselektivní, smažou tedy celou oblast za určené časové období. Pokud uživatel potřebuje smazat je určité položky z údajů o prohlížení, práce je složitější.

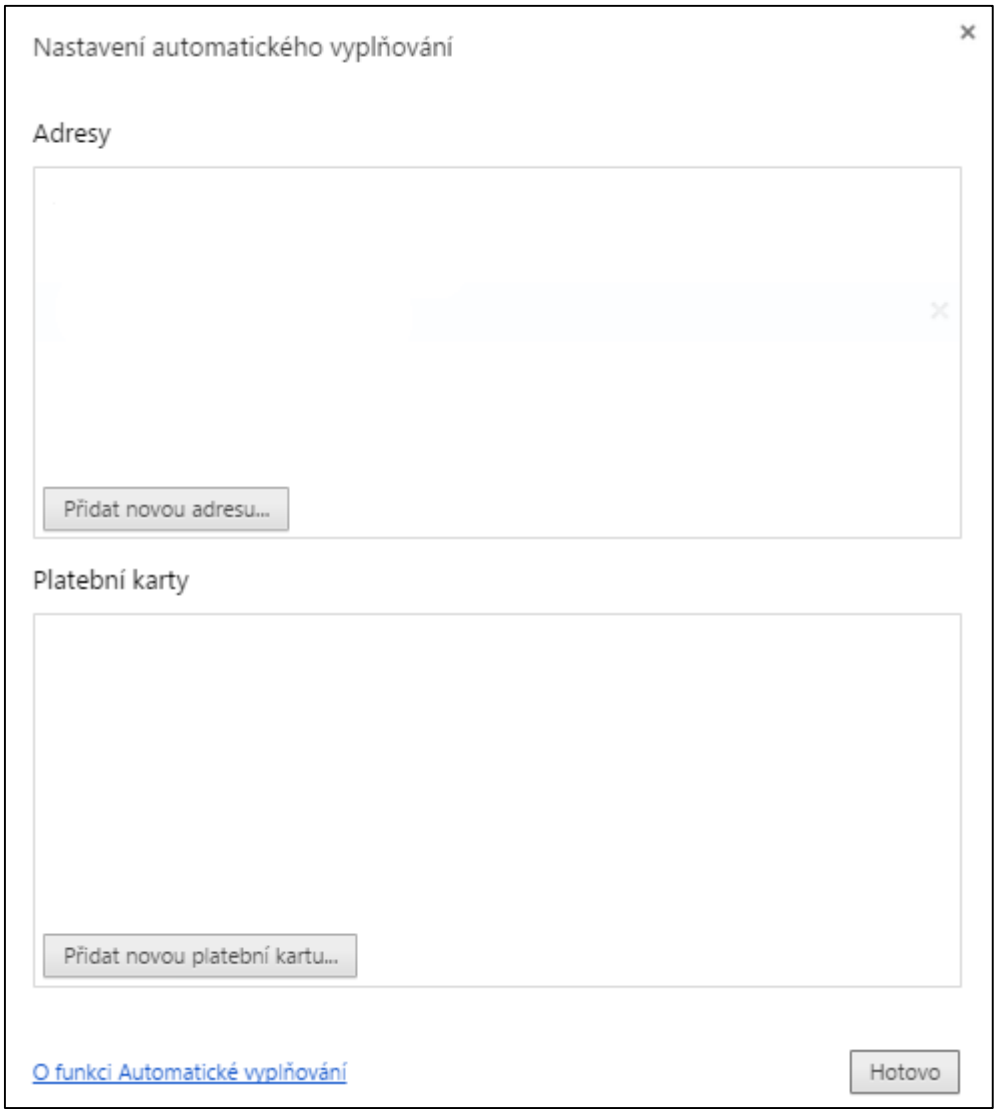
Pro výmaz konkrétních stránek z historie prohlížení je nutné přejít v menu prohlížeče do položky Historie. Zde lze zaškrtnutím tlačítka vedle stránky a kliknutím na tlačítko odstranit odebrat vybrané položky. Historie se v Google Chrome ukládá za posledních 90 dní, nejsou zde přítomny stránky, které již jsou ze seznamu smazány, nebo je uživatel navštíví v režimu anonymního prohlížení. Pokud si uživatel přeje, aby nebyla jakkoliv zaznamenána historie jeho prohlížení, je dobré použít anonymní režim prohlížeče.

Pro odstranění konkrétních položek z historie stahování, je nutné v menu prohlížeče přejít na kartu Stažené soubory a zde kliknout na soubor určený ke smazání.

4.1.7 Automatické vyplňování formulářů

Prohlížeč Google Chrome umožňuje ukládání informací, které uživatel vyplňuje do formulářů na internetových stránkách. Opět se zde jedná o uživatelský komfort, který je velmi snadno použitelný proti uživateli. Tato funkce je po instalaci prohlížeče zapnuta, autor doporučuje ji zcela vypnout nebo používat na prověřených stránkách. Nebezpečí pro uživatele hrozí ze strany zcizení zařízení, nebo povolení automatického vyplnění u stránek, které uchovávají data pomocí skrytých polí.

Vypnutí automatického vyplňování se provádí v pokročilých nastaveních prohlížeče, stejně tak i úprava nebo vymazání položek. V úpravě položek lze editovat adresy, záznamy o platebních kartách. K smazání jednotlivých položek slouží X vedle každého řádku. K celkovému výmazu všech položek automatického vyplňování slouží nástroj Vymazat údaje o prohlížení.



Obrázek 24 Nastavení automatického vyplňování

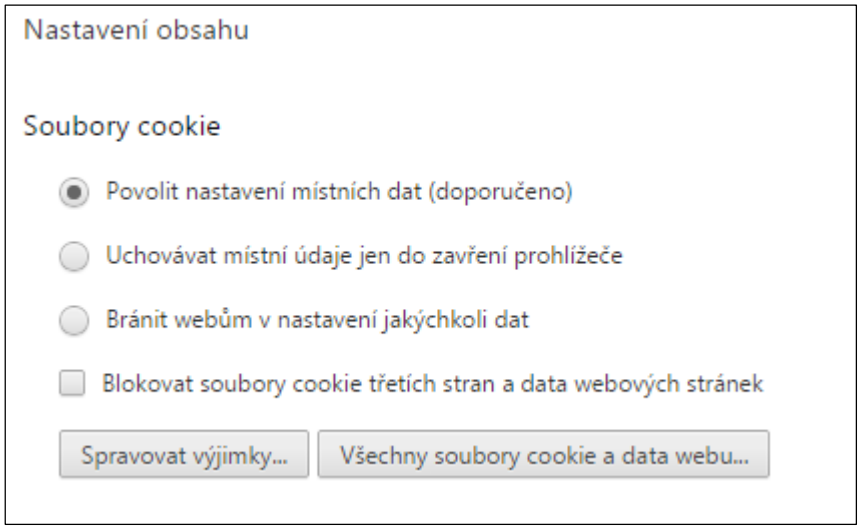
Zdroj: vlastní zpracování

4.1.8 Nastavení práce se soubory cookie, JavaScriptu, pluginů

Soubory cookie jsou uloženy na lokální disky počítače uživatele, jsou tam uloženy webovými stránkami a obsahují informace o uživateli, jeho nastavení nebo profilech. Zásadou je, že všechny dnešní stránky vysílají upozornění, že tyto soubory používají. Prohlížeč Google Chrome tuto možnost povoluje ihned po instalaci. Nastavení je editovatelné, a to v nastavení obsahu. Soubory jsou smazatelné buď jednotlivě, nebo hromadně pomocí dialogu Smazat údaje o prohlížení. Jelikož se cookie dělí na 2 části (cookie první strany a cookie třetích stran), lze blokovat v prohlížeči buď všechny, nebo jen cookie třetích stran. Pokud se uživatel rozhodne pro blokování všech souborů cookie,

nebude fungovat většina webových stránek, které vyžadují přihlášení. Tato chyba je po načtení stránky označena symbolem koláčku s křížkem v adresním řádku prohlížeče.
Pro větší komfort lze zaškrtnout jen možnost blokovat soubory třetích stran a data webových stránek. Pokud uživatel nechce mít počítač zahlcen větším počtem souborů, lze v dialogovém okně nastavení obsahu zaškrtnou políčko Uchovávat místní údaje jen do uzavření prohlížeče. Toto nastavení způsobí, že po ukončení prohlížeče jsou všechny soubor cookie smazány.

Pro konkrétní stránky lze nastavit konkrétní chování prohlížeče ohledně souborů cookies. Toto nastavení se provádí v menu Spravovat výjimky.



Obrázek 25 Nastavení obsahu - soubory cookie

Zdroj: vlastní zpracování

V pokročilých nastaveních, konkrétně v Nastavení obsahu jsou obsaženy nejdůležitější položky nastavení prohlížeče Google Chrome. V práci jsou již popsány Soubory cookie, následuje popis dalších položek.

Obrázky, zobrazování obrázků je po instalaci prohlížeče povoleno, jsou stahovány automaticky při načítání internetové stránky. Tuto funkci je možné vypnout, ale nejedná se o žádné bezpečnostní riziko, takže úprava tohoto nastavení není nutná.

JavaScript, pomocí tohoto jazyka jsou stránky upraveny tak, že jsou více interaktivní pro uživatele. Společnost Google monitoruje vývoj tohoto jazyka a stránky, na kterých je jazyk používán. Z hlediska bezpečnosti se jedná o málo rizikový prvek a je tudíž

možné nechat funkci v prohlížeči povolenou. Naopak její vypnutí má za následek nesprávné fungování některých stránek.

Pluginy jsou nástroje, které prohlížeči umožňují zobrazit zvláštní typy obsahu, jako jsou například soubory Adobe Flash Player, ve kterém jsou spuštěny animace, Adobe readeru, který umožňuje čtení PDF dokumentů přímo v prohlížeči a dalších. Pro instalaci, spuštění, vypnutí a odinstalaci pluginů slouží samostatná položka menu prohlížeče, která se nazývá rozšíření. Tato položka umožňuje získání pluginů z knihoven společnosti Google. Tyto knihovny jsou velmi rozsáhlé a tvorbě pluginů se věnuje množství společností i jednotlivců. Tito malí pomocníci činí prohlížení internetu snazším a více komfortnějším. Společnost Google provádí neustálou kontrolu knihoven pluginů, tudíž lze považovat instalaci jakéhokoliv rozšíření z tohoto umístění za bezpečné.

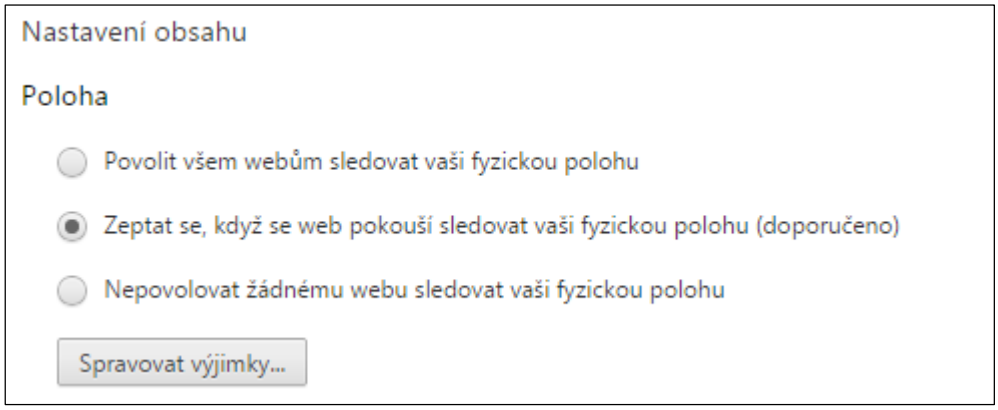
Vyskakovací okna, prohlížeč brání automatickému zobrazování vyskakovacích oken, tím zabraňuje uživateli navštívit nechtěně otevřené stránky a zabránit například zcizení uživatelských údajů po jejich zadání na podvodné stránce. Tuto funkci lze samozřejmě vypnout, což ovšem autor důrazně nedoporučuje. Tento nástroj považuje za velmi silný v boji proti internetové kriminalitě a komfortu prohlížení internetových stránek. Toto nastavení je opět možné modifikovat pro každou stránku zvlášť a to pomocí sekce Spravovat výjimky, kdy je možné některým stránkám povolit vyskakovací okna a některým nikoliv. Zprávu o zamýšleném otevření vyskakovacího okna obdrží uživatel pod adresním řádkem. Je tedy na něm, zda tuto možnost povolí či ne. Autor zde nemůže uvést jednoznačné doporučení. Uživatel se musí rozmyslet podle potřeby a podle bezpečnosti stránek.

4.1.9 Práce se zeměpisnou polohou uživatele

Polohu počítače určuje služba Google Location Services, která odhaduje umístění pomocí IP adresy. Určená poloha slouží k zobrazení užitečnějších informací, například pří vyhledávání. Tato služba není spuštěna bez povolení uživatele. Po navštívení stránek, které umožňují práci s polohou uživatele, je uživateli zobrazena výzva, zda si přeje povolit sdělení zeměpisné polohy. Pokud zvolí uživatel povolení polohy, je v adresním řádku zobrazena příslušná ikona terčíku.

Provedená nastavení i absolutní vypnutí sdělení polohy se provádí v Nastavení obsahu, kdy jsou na výběr možnosti povolení sdělení polohy všem webům, možnost otázky a nepovolení webům sledování polohy. Pro přesné nastavení pro jednotlivé stránky slouží

možnost Spravovat výjimky. Autor doporučuje nastavení otázky na sdílení polohy, například pro vyhledávání obchodů, restaurací nebo kin, je tato funkce velmi užitečná. [4] [9] [20]



Obrázek 26 Nastavení určení polohy

Zdroj: vlastní zpracování

4.2 Zásady bezpečného chování na Internetu

V rámci dalšího pokračování práce je vytvořen dotazník ohledně bezpečnosti na Internetu. Dotazník je vytvořen pomocí nástroje Google Forms je rozeslán na 30 autorových spolužáků a spolupracovníků v zaměstnání. Dotazník je směřován hlavně na využívání počítače v domácím prostředí, neboť sítě jsou zabezpečeny zcela jinak. Celá dedikovaná oddělení se starají o jejich bezpečnost, ovšem u domácích sítí je to zcela naopak, a pokud uživatel není odborník, zabezpečit svůj počítač bývá složité.

4.2.1 Hesla

Z pohledu IT odborníka je nutné představit další pojmy z informatiky. V tomto tématu se jedná o autentizaci, která představuje prokázání určité identity. Hodně uživatelů Internetu si toto plete s identifikací, což není nic jiného než pouhé potvrzení identity. Autentizace je tedy pro ověření identity nejdůležitější a také nejkomplikovanější. K autentizaci uživatele se nejčastěji používají právě hesla, která mají svou výhodu v tom, že není třeba žádné zvláštní vybavení, ale také nevýhodu v možnosti být sdělena jiným uživatelům a v možnosti být uhádnuta a zachycena.

Prvním tématem v dotazníku jsou hesla. Otázek je položeno celkem pět:

- Používáte na Internetu hesla?
- Používáte je na více internetových stránkách?
- Pokud ano, používáte na všech stejné heslo?
- Jaká je průměrná délka vašich hesel?
- Používáte hesla složená z malých a velkých písmen, číslic a speciálních znaků?

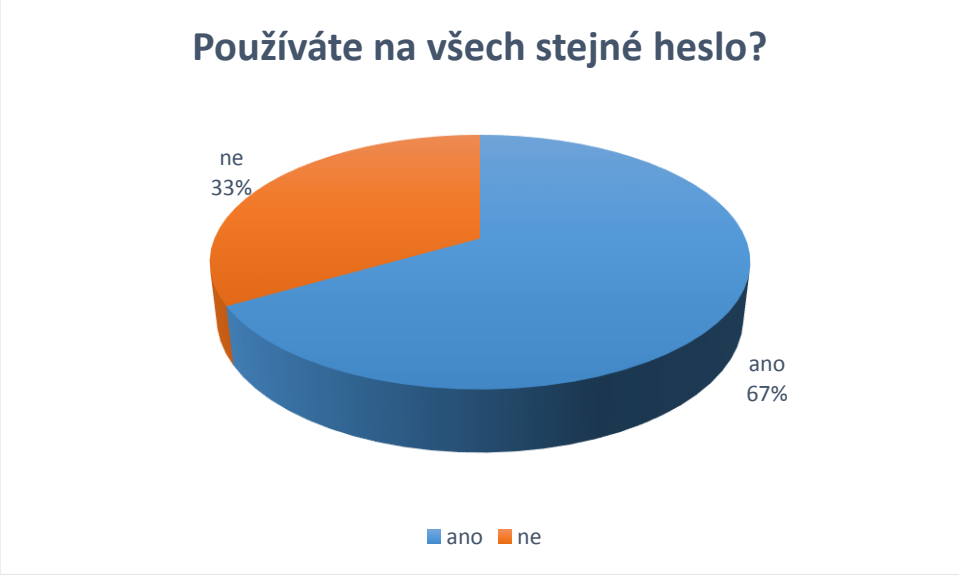
Grafy níže ukazují vyhodnocení prvního tématu dotazníkového šetření:

Graf 1 Vyhodnocení otázky č. 1

Zdroj: vlastní zpracování

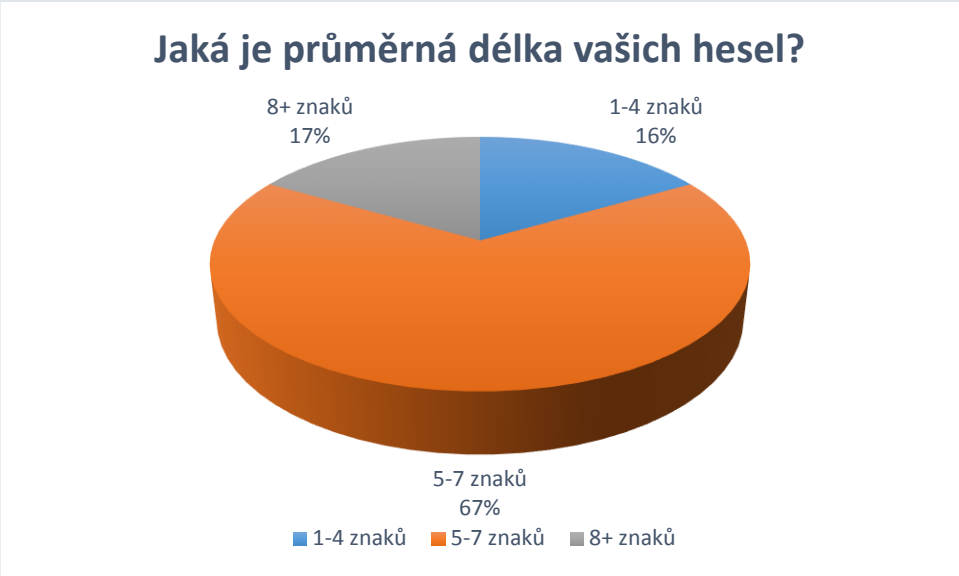
Graf 2 Vyhodnocení otázky č. 2

Zdroj: vlastní zpracování



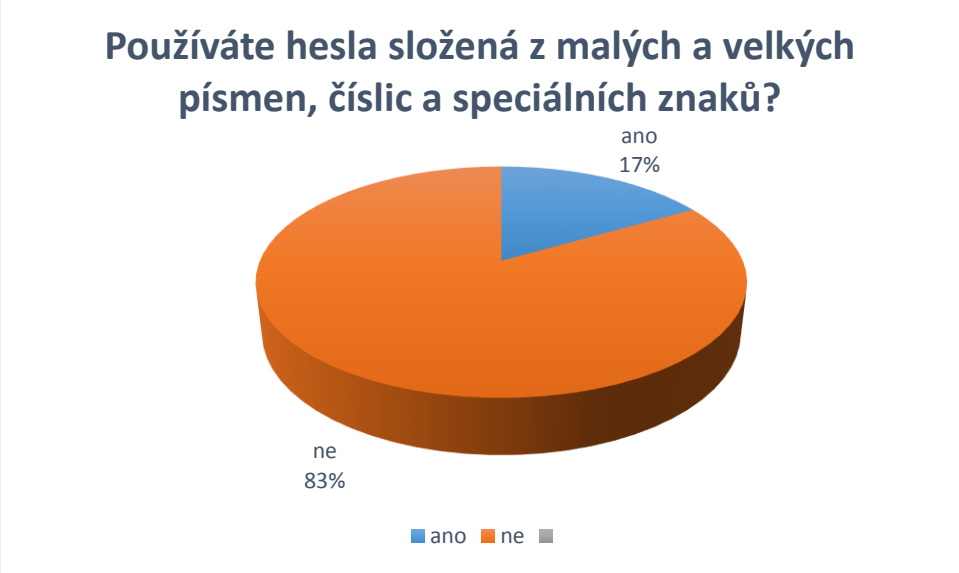
Graf 3 Vyhodnocení otázky č. 3

Zdroj: vlastní zpracování



Graf 4 Vyhodnocení otázky č. 4

Zdroj: vlastní zpracování



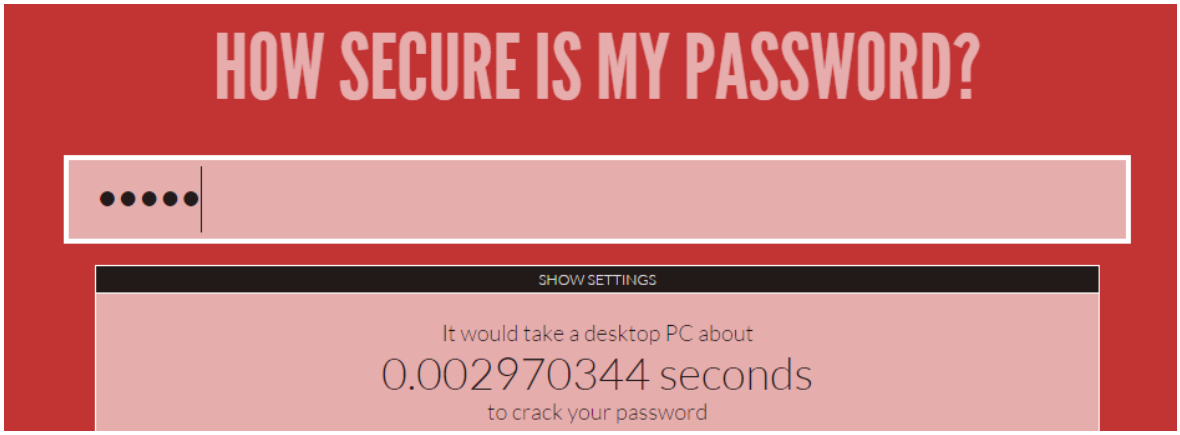
Graf 5 Vyhodnocení otázky č. 5

Zdroj: vlastní zpracování

První otázka v dotazníku je zcela jasná a odpovědi jsou predikovatelné. Každý uživatel používá na Internetu hesla, například pro přístup k emailu, sociální síti, do internetového bankovnictví, na různá fóra atp. Tomu se v dnešní době nedá zabránit, protože se jedná o velmi levnou techniku. S výše popsaným souvisí i druhá otázka, kdy případů autentizace je opravdu mnoho.

Co se týče třetí otázky, jedná se o velkou chybu používat stále stejné heslo pro všechny systémy. Případnému útočníkovi stačí získat toto heslo a dostane se všude. Je tedy důrazným doporučením používat jiná hesla. Je dobré rozlišit například důležitost stránek. Jinou hodnotu má prolomení internetového bankovnictví, kde uživatel může přijít o finance a samozřejmě jinou hodnotu má například diskuzní fórum, kde je riziko škody minimální. Dalším doporučením je tato hesla měnit co nejčastěji. Některé internetové stránky, aplikace či operační systémy mají nastavené automatické upozornění po uplynutí určité doby. Jedná se o upozornění ke změně hesla, ale ta nemusí být provedena. V sofistikovanějších aplikacích může být uživatel donucen toto heslo změnit, nebo mu aplikace přestane fungovat. Což může být uživateli hodnoceno jako „hrubost“, ale je nutné si uvědomit, že tato změna má své opodstatnění a je nutná pro bezpečnost. Další velkou chybou uživatelů je zaznamenávání hesel, ať už kdekoliv. Nejčastějšími případy jsou hesla do operačních systémů počítačů nalepené na monitoru, nebo ještě hrozivější případy nalepení PINu na zadní stranu platební karty atp. Tato rizika jsou spojená s dnešní hektickou dobou, kdy jsou na uživatele kladeny velké nároky na jeho paměť. Existuje tolik uživatelských účtů a oprávnění, že má uživatel tendenci si věci zjednodušovat a používat buď stejné heslo, nebo si ho někam zapsat. Ovšem jedná se o největší chybu, kterou může udělat. Je proto nutné si hesla nepsat na žádné veřejné místo, a pokud už je nutné si ho nějak zaznamenat, tak odděleně od nástroje, ke kterému patří. A v neposlední řadě autor doporučuje nesdělovat hesla svým přátelům nebo známým. Pro některé uživatele se jedná o nemyslitelnou věc, ale tyto případy zneužití jsou stále velmi časté.

Pro demonstraci výsledků třetí a čtvrté otázky je použit internetový odkaz, který zjišťuje sílu uživatelského hesla, ať už se jedná o délku, nebo použití velkých a malých písmen, číslic a speciálních znaků.



Obrázek 27 Síla hesla 1

Zdroj: https://howsecureismypassword.net/

Obrázek 28 Síla hesla 2

Zdroj: https://howsecureismypassword.net/

V prvním případě bylo zvolené heslo „karel“. Na příkladu lze vidět, že prolomení hesla by běžnému počítači trvalo ani ne sekundu. Na prolomení hesla se používají dvě odlišné techniky, brute force attack a dictionary attack. Brute force attack (útok hrubou silou) je způsob zjištění hesla, kdy speciální program zkouší všechny existující kombinace číslic a písmen, dokud nepřijde na to správné. Jedná se o časově náročnou činnost, která ale končí úspěchem. Dictionary attack naopak využívá jakéhosi slovníku hesel, které postupně zkouší aplikovat. Jedná se o rychlejší metodu, ale nemusí vždy skončit úspěchem, protože záleží na velikosti slovníku a také na složitosti použitého hesla. U tohoto případu by šlo použít obě metody, slovníků nejčastějších hesel jsou na Internetu stovky. Existují dokonce samostatné statistiky nejčastěji používaných hesel a dělení uživatelů. Zde jsou příklady nejčastěji zvolených hesel:

- Vlastní jméno
- Jméno partnera
- Jméno domácího mazlíčka
- Datum narození
- Rodné příjmení matky
- Datum narození rodinného příslušníka
- Adresa uživatele
- Kombinace čtyř číslic – nejčastěji 1111, 1234, 000, 4321 atp.
- Oblíbená barva

V druhém případě bylo zvoleno heslo „KArEL1968*/“. Je patrné, že metoda dictionary attack je zde nepoužitelná a musí nastoupit brute force attack. Heslo je prolomitelné, ale údaj o času potřebnému k prolomení v tisících letech jasně značí sílu hesla. Už samotná změna velikosti písmen přidává na síle. Ale nejdůležitější je délka a přítomnost speciálních znaků a číslic. Uvedené heslo ovšem jeví známky jakési posloupnosti, pro absolutní bezpečí doporučuje autor udělat znaky více náhodnými, například včlenit číslice do textu atp.

Vyšší zabezpečení vykazují tzv. jednorázová hesla, která jsou používána aplikacemi pro dodatečnou autentizaci uživatele. Jedná se o heslo, které se dá použít pouze jednou a poté již ztrácí svou platnost. Příkladem tohoto hesla je autorizace platby zadané v internetovém bankovnictví, kdy na ověřený mobilní telefon přijde unikátní kód k potvrzení platby. Zde opět vyvstává problém, kdy útočník kontaktuje uživatele, že zadal špatné telefonní číslo a požaduje přeposlání zprávy na svůj mobilní telefon. Lze se setkat s případy, kdy to uživatel opravdu učiní a přijde tak například o své finanční prostředky. Doporučení je zcela jasné, je nutné tyto unikátní kódy nikomu nesdělovat ani nepřeposílat. Jsou vygenerovány pouze pro potřebu jednoho uživatele a na jeho vlastní žádost.

Zcela odlišný způsob autentizace se používá v čipových kartách a pomocí biometrický údajů. Čipová karta je uživatelem vlastněné zařízení, které pracuje metodou výzva/odpověď a obsahuje jeho tajný klíč. Při interakci se čtečkou dochází k ověření tohoto klíče, ověření uživatelem zadaného PINu vázaného ke kartě a uskutečnění transakce. Jedná se sice o velmi vyspělou technologii, ovšem bezpečnostní rizika jsou i

zde. Pokud je pominuta možnost odcizení karty a prolomení PINu, je zde možnost získání kopie tajného klíče uživatele, protože musí existovat jejich databáze pro porovnání a uskutečnění transakce. Jedná se o velmi citlivou informační databázi, která by v žádném případě neměla být instalována na veřejné počítače. Této hrozbě lze zabránit pomocí kryptografických nástrojů. Druhý jmenovaný způsob autentizace je použití biometrických údajů, jako je například otisk prstu, podpis, lidský hlas. Tento způsob autentizace vyžaduje speciální hardware. Při dnešní pokročilé technologii se jedná o stále se rozšiřující způsob autentizace. Čtečky otisků prstů jsou instalovány v noteboocích, mobilních telefonech, na vstupech do různých institucí atp. Relativně největší výhodou tohoto způsobu autentizace je nemožnost předání a ukradení identifikátoru. Slovo relativní je na místě, protože existují případy, kdy byl identifikátor odcizen.

4.2.2 Phishing a zfalšované internetové stránky

Dalším tématem dotazníku je zkušenost respondentů s phishingem. Před samotnými otázkami obsahuje dotazník vysvětlení phishingu.

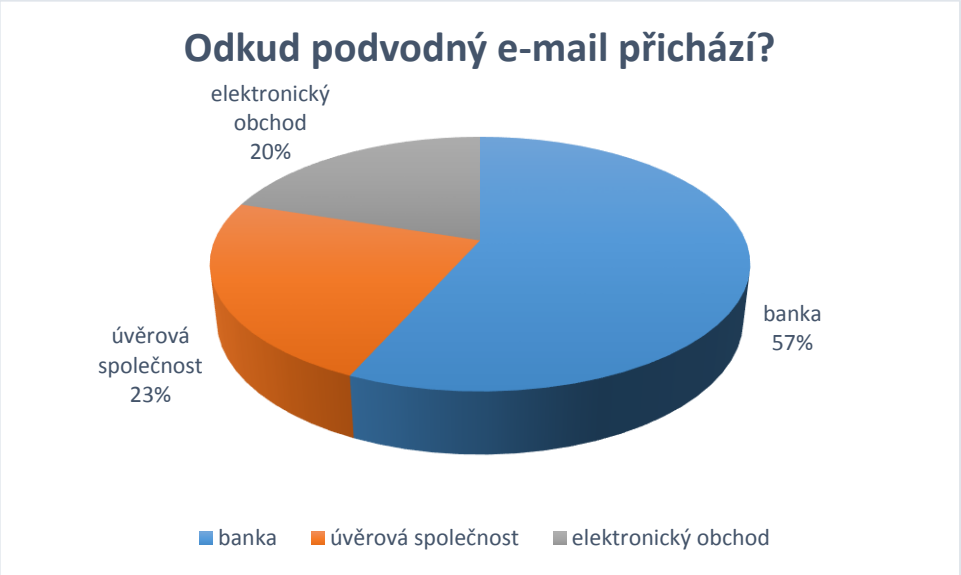
Anglické slovo a termín phishing je složenina ze dvou výrazů a to fishing a phreaking. Slovo fishing znamená rybaření, tedy chytání ryb na návnadu, význam je tedy zcela jasný. U slova phreaking je to složitější, jedná se opět o složeninu slov phone a freaking. Phone freaking je způsob nabourávání telefonní sítě pomocí píšťalky umístěné v sáčku od brambůrek, která vydává tón o stejné frekvenci jako ústředna propojující hovory. Jedná se tedy o podvodnou techniku, kdy si hacker vlastně „může zavolat zadarmo“. Tato technika se dnes nepoužívá, její použití se datuje do padesátých až sedmdesátých let minulého století v USA. Termín phishing se tedy dá vysvětlit jako podvodné chytání na návnadu. Jeho hlavním účelem je získat citlivé uživatelské údaje, nejčastěji právě hesla, PINy, čísla kreditních karet, přihlašovací údaje atp. Tyto údaje buď chtějí zaslat e-mailem, nebo je v těle e-mailu odkaz na zfalšovanou stránku, která se ovšem tváří věrohodně.

- Setkáváte se s těmito druhy e-mailů?
- Odkud podvodný e-mail přichází?
- Znáte případy z médií?
- Jak na ně reagujete?

Graf 6 Vyhodnocení otázky č. 6

Zdroj: vlastní zpracování

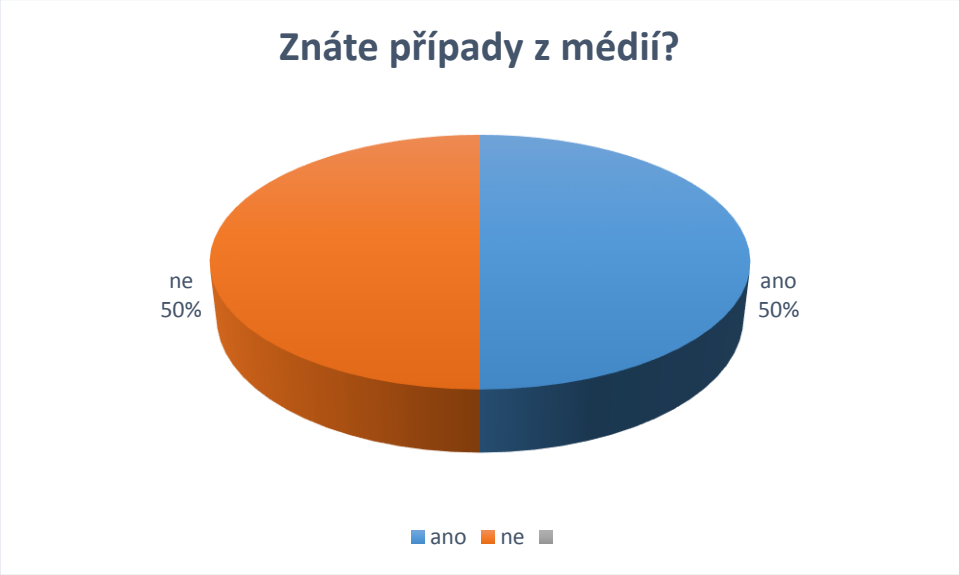
Je vidět, že tento problém je v dnešní době velmi rozšířený a setkávají se s ním všichni. Existuje stále hodně důvěřivých uživatelů, které tyto zprávy nejsou schopni identifikovat a citlivé údaje útočníkům poskytnou. V poslední době se také rozšiřuje další druh phishingu. Jsou to podvodné vymáhací e-maily, které obsahují přílohu. Jedná se další pokus útočníka, tentokrát o ovládnutí počítače a opět získání uživatelských údajů včetně hesel.



Graf 7 Vyhodnocení otázky č. 7

Zdroj: vlastní zpracování

E-maily nejčastěji přicházejí z bankovních institucí. Z pohledu útočníka se jedná o nejsnazší získání údajů k obohacení, protože maskuje tyto podvodné e-maily jako přístupy do internetového bankovnictví nebo portálů na poskytování půjček. Z pohledu uživatele se jedná o největší riziko spojené s finančními prostředky, ať už s krádeží naspořených prostředků na účtech nebo uzavření úvěrových smluv na jejich osobní údaje.



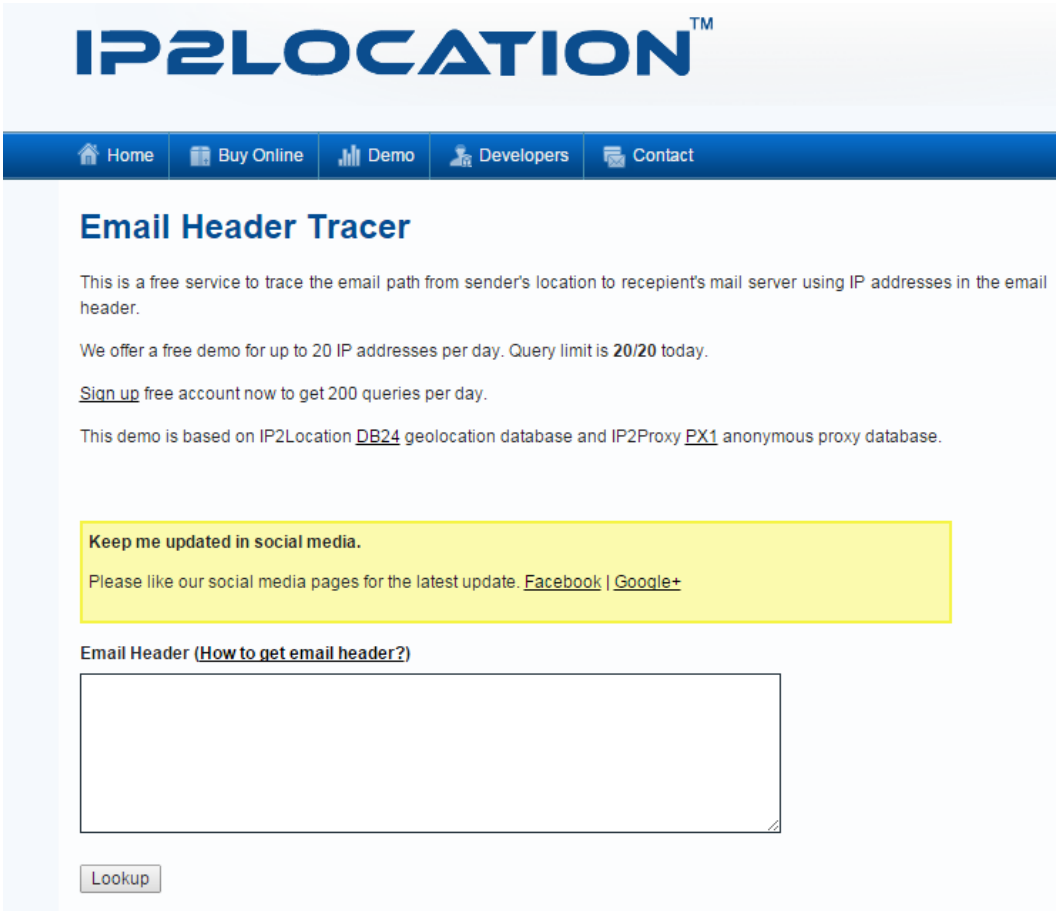
Graf 8 Vyhodnocení otázky č. 8

Zdroj: vlastní zpracování

Graf 9 Vyhodnocení otázky č. 9

Zdroj: vlastní zpracování

Obrana proti phishingu není jednoduchá, záleží hodně na informovanosti uživatelů. Je nutné říci, že všechny seriózní instituce nikdy nenutí uživatele k zaslání uživatelských údajů jakoukoliv formou, ať už elektronickou, telefonickou nebo písemnou. Všechny tyto citlivé transakce typu předání jména a hesla k účtu, PINu ke kartě probíhá osobně na pobočce nebo pomocí zabezpečených obálek. Všechny tyto podvodné e-maily vždy obsahují nějakou chybu, pokrok falzifikátorů je velký, ale dobrým znakem podvrhu je například špatná čeština. Dalším nástrojem na odhalení podvodu je prověření odesílatele e-mailu, kde stačí dle návodu vložit hlavičku emailu a aplikace zjistí odesílatele. Zde je ukázka:



Obrázek 29 Zjištění odesílatele e-mailu

Zdroj: http://www.ip2location.com/free/email-tracer

Co se týče příloh v neprověřených e-mailech, vždy platí NEOTVÍRAT. Můžou totiž obsahovat škodlivé programy, které mohou poničit počítač a například odeslat uživatelská data na předem definovanou adresu. Tomu problému se věnuje další kapitola.

Dalším problémem spojeným s phishingem jsou podvržené internetové stránky, které sice vypadají jako originál, ale opět se jedná o útok na citlivé údaje. Tyto odkazy bývají součástí podvodných e-mailů a jejich účel je stejný. V dotazníku se tomuto tématu věnovaly tři otázky:

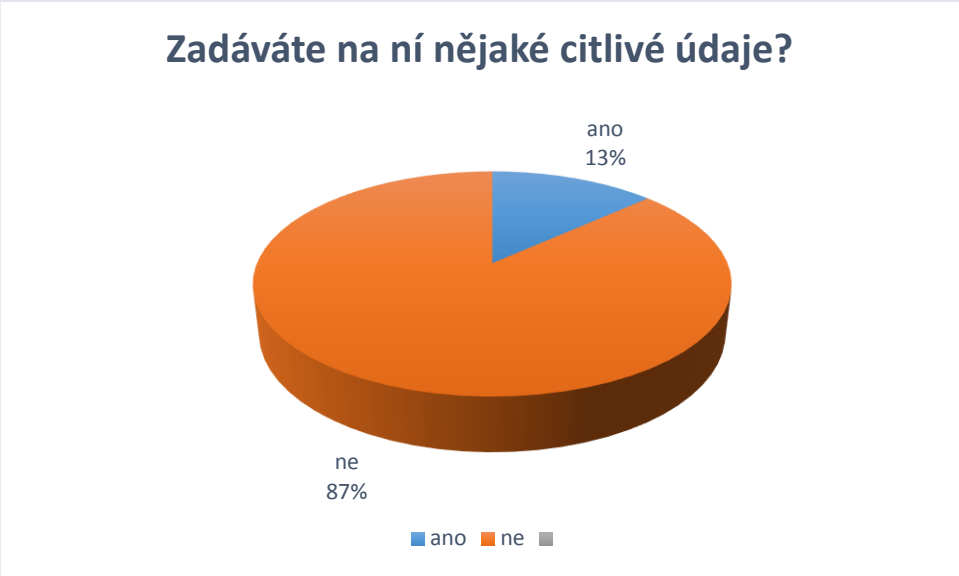
- Kliknete na odkaz v e-mailu od neznámého odesílatele?
- Ověříte si stránku, na kterou Vás odkaz přenesl?
- Zadáváte na ní nějaké citlivé údaje?

Graf 10 Vyhodnocení otázky č. 10

Zdroj: vlastní zpracování

Graf 11 Vyhodnocení otázky č. 11

Zdroj: vlastní zpracování



Graf 12 Vyhodnocení otázky č. 12

Zdroj: vlastní zpracování

V textu e-mailu se většinou nachází nějaké upozornění. Nejčastěji se jedná o výzvu k aktualizaci údajů, nebo jakási výzva o vypršení registrace. Stále platí varování, že seriózní instituce tyto výzvy neposílají elektronicky a nepožadují jejich vyplnění na internetových stránkách. Vše se děje buď přímým kontaktem, nebo v zabezpečených internetových aplikacích. Již je popsáno, jak prověřit odesílatele e-mailové zprávy. Je nutné se věnovat i zjištění původu internetových stránek. Níže je jasný příklad podvržené stránky České spořitelny, kdy je nutné si všimnout internetové adresy:

Obrázek 30 Podvržená internetová stránka

Zdroj: www.csas.cz

V tomto případě je podvod evidentní, ovšem opět platí, že je nutné informovat uživatele, kam se v takovémto případě dívat. Dalším dobrým identifikátorem podvržených stránek je špatná úroveň češtiny. Pokud uživatel narazí na takovéto stránky, měl by ihned stránky opustit. Některé instituce dokonce nabízejí program odměn za poskytnutí informací o takovýchto stránkách a s podvodníky usilovně bojují.

Samozřejmě platí, že nejlepší obranou a prevencí tohoto útoku je neklikat na žádné odkazy obsažené v neautorizovaném e-mailu, ale pokud se tak děje, existují nástroje na prověření domény internetové stránky. Nejznámějším nástrojem na zjištění původu a majitele domény je portál WHO.IS

Obrázek 31 Zjištění majitele stránky

Zdroj: https://who.is/

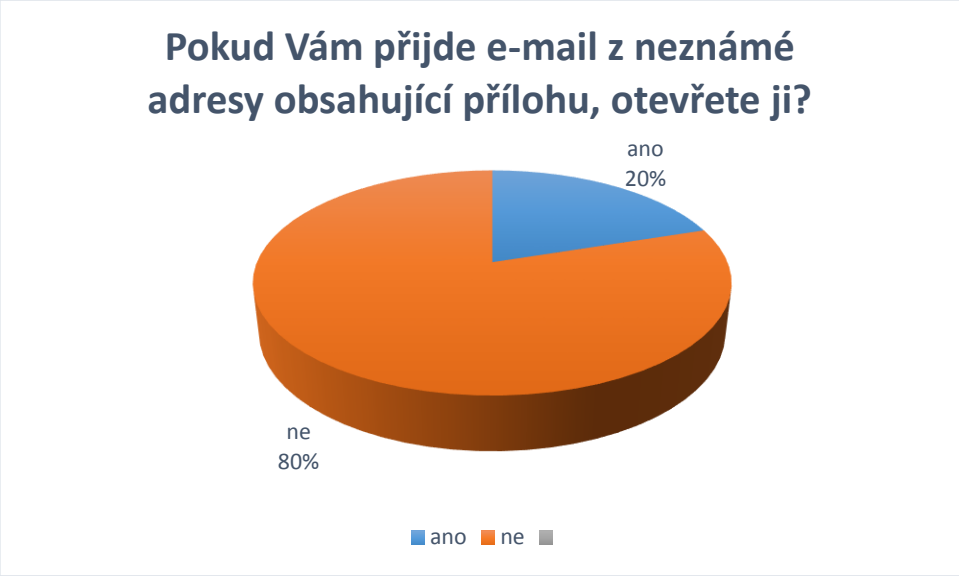
Pokud uživateli nesedí jakékoliv údaje o majiteli stránky, má tyto stránky okamžitě opustit a v žádném případě na nich nezadávat jakékoliv údaje.

Dalším problémem podvodných stránek může být také registrace. Jsou známy případy, kdy se uživatel zaregistruje pod dojmem přístupu zdarma a po určité době jsou po něm požadovány poplatky za návštěvy stránek atp. Proti této podvodné taktice opět existuje účinná obrana. V prvním případě se jedná o prevenci, tedy nutnosti prověření všech informací o registraci na dané stránce, nezadání citlivých osobních údajů, zjištění informací o stránce samotné. Pokud se uživatel přeci jen zaregistruje a jsou po něm později požadovány jakékoliv finanční prostředky za používání, je nutné se obrátit na sdružení ochrany spotřebitelů a podobné instituce.

4.2.3 Malware, Spyware, Adware

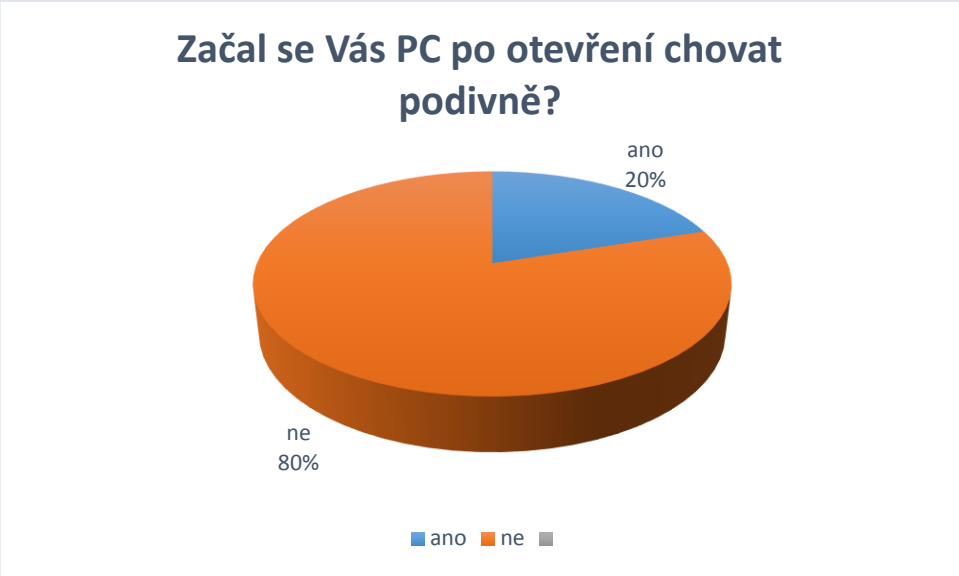
V dalším tématu jsou respondentům položeny otázky na tzv. škodlivý software, který úzce souvisí s dotazováním v předchozím tématu. Po nechtěné instalaci takovéhoto software již dochází k nějakým konkrétním problémům. Otázky jsou položeny tyto:

- Pokud Vám přijde e-mail z neznámé adresy obsahující přílohu, otevřete ji?
- Začal se Váš PC po otevření chovat podivně?
- Načítá se dlouho internetový prohlížeč, změnila se Vám domovská stránka?



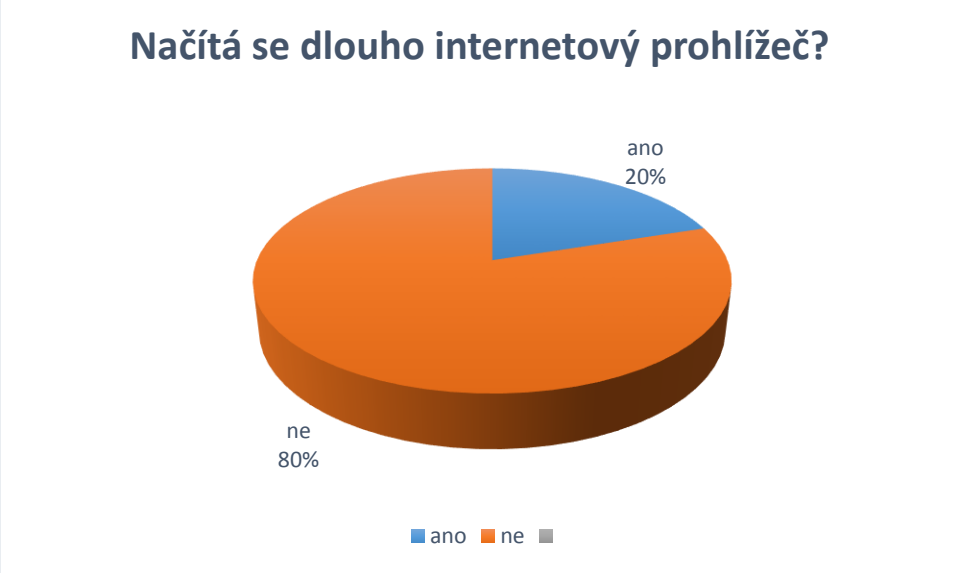
Graf 13 Vyhodnocení otázky č. 13

Zdroj: vlastní zpracování



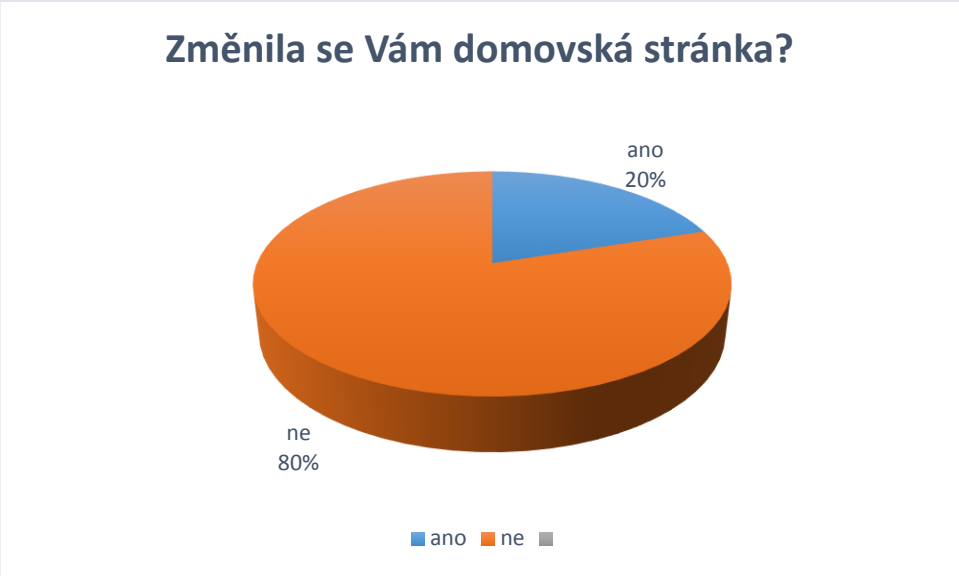
Graf 14 Vyhodnocení otázky č. 14

Zdroj: vlastní zpracování



Graf 15 Vyhodnocení otázky č. 15

Zdroj: vlastní zpracování



Graf 16 Vyhodnocení otázky č. 16

Zdroj: vlastní zpracování

Pro účinnou obranu je nutné nejdříve vysvětlit všechny pojmy a uvést krátkou historii. Akronym Malware vzniká spojením dvou anglických slov malicious software, tedy v překladu škodlivý software. Tyto programy představují největší hrozbu pro uživatele. Samotné programy se dělí do několika kategorií:

- Viry – jedná se o škodlivé kódy, které se dokáží sami duplikovat a rozesílat se na další počítače. Jejich účelem je buď pouze duplikace, mazání dat v počítači nebo vyřazení počítače z provozu. Poslední dvě jmenované jsou největší hrozby, ale je nutné se virů zbavit celkově.
- Červy – jsou velkou obdobou virů, rozdíl je v jejich replikaci. Červy zůstávají v paměti počítače a zůstávají zde bez povšimnutí, dokud rychlost jejich replikace nepřesáhne kapacitu paměti a v tu chvíli mohou být odhaleni.
- Trojské koně – jméno pochází ze starých řeckých bájí a pověstí a přesně odpovídá účelu. Program se tváří jako běžná aplikace, ale na pozadí své činnosti provádí škodlivou činnost.
- Rootkit – tento druh software nemá český překlad, slovní spojení se dá přeložit jako kořenová sada. Jedná se o sadu nástrojů, které může útočník použít pro přístup k systému a jeho celkové ovládnutí. Tyto nástroje také

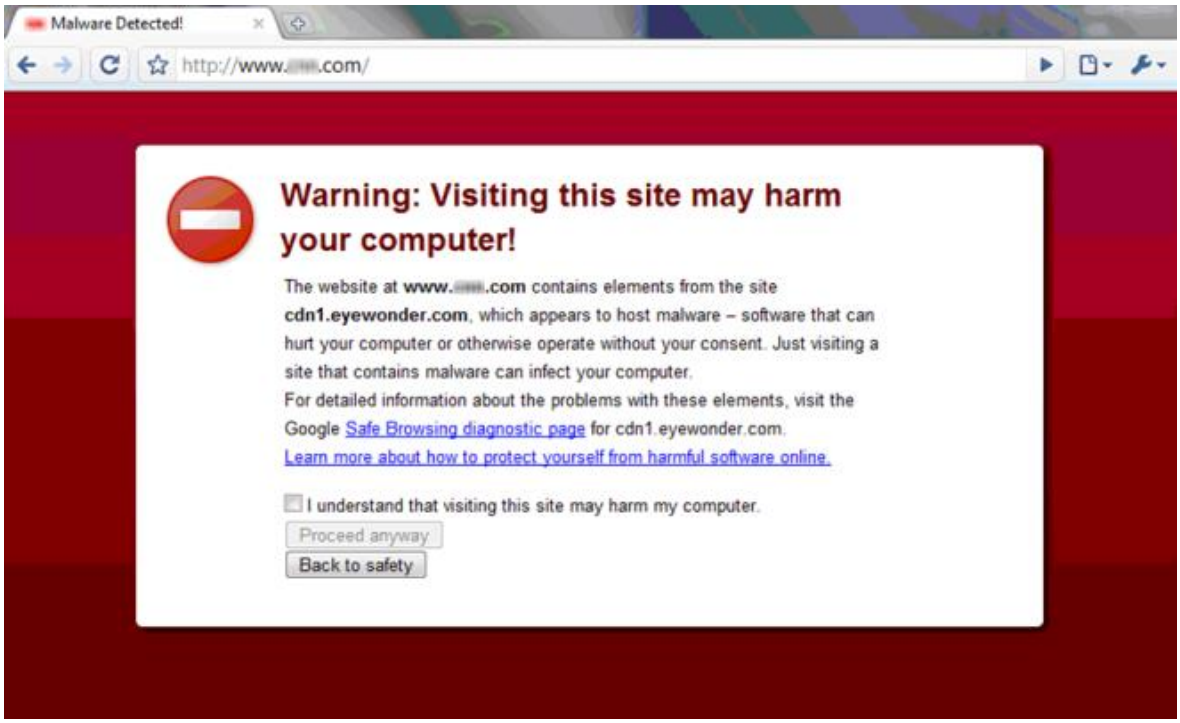
umožnují sledovat uživatelská jména a hesla, iniciovat útoky proti obraně systému a skrývat svou přítomnost mazáním důležitých záznamů.

- Bot – jedná se o obdobu rootkitu, která slouží k jedinému účelu. Získání kontroly nad počítačem. Takovýto počítač se označuje jako zombie.

Historie škodlivého softwaru sahá do osmdesátých let minulého století. V roce 1983 student Fred Cohen poprvé popisuje program označovaný jako virus, který se dokáže šířit z počítače na počítač. Prvním virem se stává v roce 1986 *The Brain*. Jelikož je Internet ještě omezenou sítí jen pro vyvolené, virus se šíří pouze půjčováním disket, proto nemá takový dopad, jak by mohl mít. Tehdejší správci sítě těmto problémům nevěnují žádnou pozornost. Vše se mění až v roce 1999, kdy virus známý jako *Melissa* zaplavuje a ohrožuje Internet. Od té doby se pojem virus, nebo Malware začíná považovat za hrozbu a řešit. Ve věku Internetu se používá srovnání s virem *Slammer*, který se dokáže rozšířit na stovky tisíc počítačů a ochromit Internet za méně než 30 minut.

S tímto souvisí varování, že všichni uživatelé Internetu mají být bdělí a co nejvíce chránit sami sebe před těmito hrozbami. Jelikož jsou součástí celosvětové sítě, ochrana jen jejich počítače znamená ochranu části sítě a může zabránit dalšímu šíření těchto hrozeb. Ochranou proti virům se zabývá další kapitola, ale některá doporučení je možné uvést již nyní. Při obdržení e-mailu, u kterého uživatel nedokáže určit odesílatele, nebo tento e-mail obsahuje podezřelou přílohu, by měl uživatel e-mail rovnou smazat. Existuje totiž důvodné podezření, že příloha obsahuje Malware a může ohrozit uživatelovu bezpečnost. Pokud počítač obsahuje účet User, nebo se přes něj dokonce uživatel hlásí do počítače, tento účet by neměl mít administrátorská práva. Toto omezení se nejčastěji používá v zaměstnání, kdy je k instalaci jakéhokoliv software nutné kontaktovat správce sítě, který má za úkol zabezpečit a zamezit jakémukoliv poškození počítačů. Dalším doporučením je nenavštěvovat podezřelé internetové stránky. Všechny stránky je dobré prověřit, jak je již zmíněno v přecházejícím tématu. Dalším velkým zdrojem Malware je sdílení souborů. Nejeden uživatel dnes na síti stahuje soubory pomocí technologie P2P, tedy přímé sdílení souborů mezi uživateli. Z pohledu útočníka se jedná o ideální prostředí pro šíření trojských koní a červů. Škodlivý software se tváří jako součást sdílených souborů a právě spustitelné soubory tuto hrozbu oživí.

Je také důležité zmínit, jak uživatel pozná, že je jeho počítač napaden tímto softwarem. Počítač se ve většině případů chová zvláštně. V různých úložištích se objevují nebo naopak mizí soubory. Operační systém běží pomaleji, internetové stránky se načítají pomaleji. Ikonka činnosti pevného disku bliká a vše vypadá, jakože počítač pracuje, ačkoliv uživatel přímo neprovádí žádnou činnost. Operační systém zamrzá, nebo kolabuje úplně a nedá se s ním pracovat. Všechna tato vodítka mohou znamenat, že je počítač napaden a proto nutné okamžitě zahájit nápravu. Nejlepším nástrojem je používání antivirového programu, který sám o sobě obsahuje další podprogramy, které slouží k vyhledání a odstranění veškerého Malware. Více o tomto programu je popsáno v další kapitole.



Obrázek 32 Upozornění na Malware v Google Chrome

Zdroj: www.Malware-info.com

Ačkoliv jsou Adware a Spyware spojovány v jedno, je mezi nimi obrovský rozdíl. Adware slouží k přidávání reklamy, Spyware dokáže sledovat aktivitu uživatele, zaznamenávat údery na klávesnici, uživatelská jména a hesla. Obě popsané skupiny programů souvisí s anonymitou prohlížení internetových stránek. Konkrétně tím, že tuto anonymitu porušují, ať již pomocí přidávání reklam tzv. „na míru“ nebo v horším případě krádeží identity a přihlašovacích údajů.

Program Adware se do počítače dostane vědomě, a to při schvalování instalace jiného programu. Uživatel, který pouze nepozorně odsouhlasí jakoukoliv položku v instalaci, se vystavuje právě této hrozbě instalace Adware. Takovýto program poté běží na pozadí a sbírá data o navštívených stránkách, která pak odesílá k vývojáři. Na základě těchto informací, které jsou poté použity firmami nabízejícími zboží. Pak dokáže být uživateli nabídnuta přesně cílená reklama pomocí reklamních bannerů na stránkách, v programech atp.

Obrana proti této hrozbě je proto jednoduchá, stačí se věnovat každé nové instalaci programu do počítače a nevyužívat za každou cenu neplacené produkty, protože právě u nich je vysoké riziko instalace Adware.

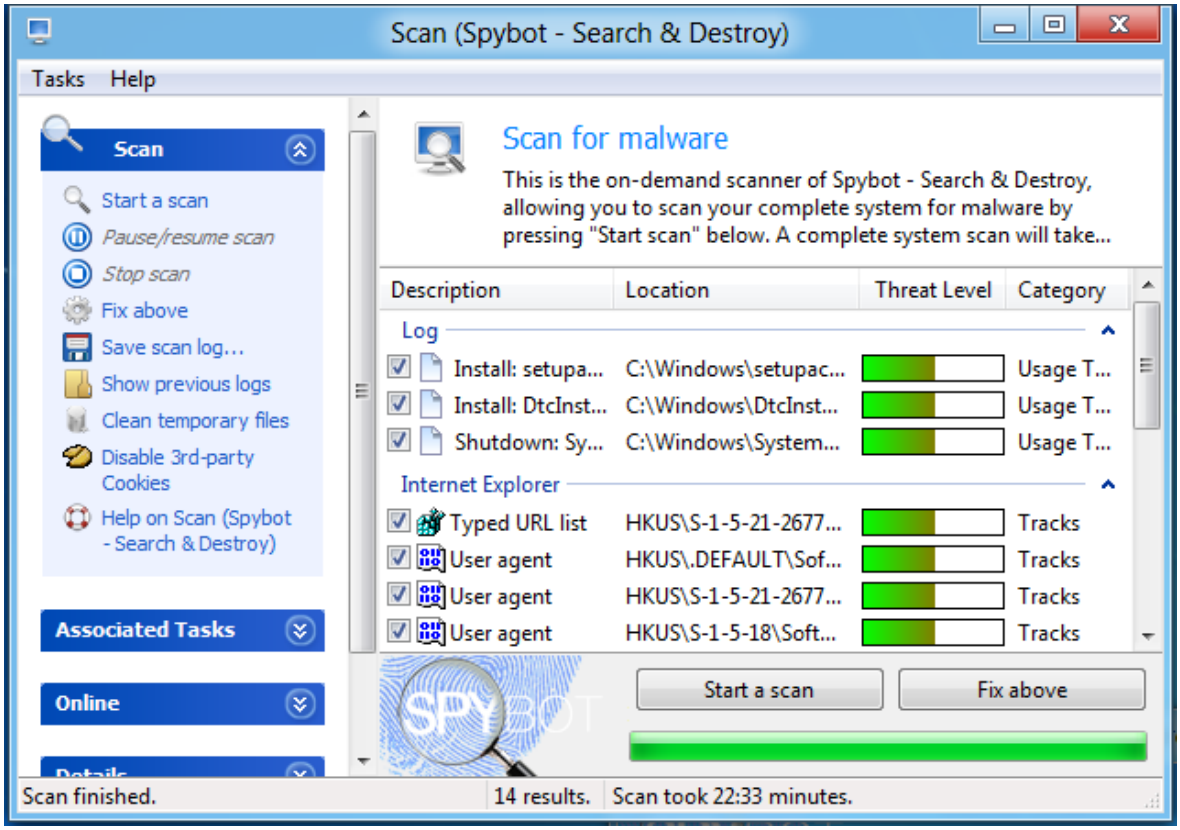
Obrázek 33 Ukázka nechtěné reklamy způsobené přítomností Adware

Zdroj:www.pctools.com

Adware je považován za legální, protože je instalován s vědomím uživatele. Oproti tomu Spyware je zcela nelegální a mnohem větší bezpečnostní hrozbou. Svou podstatou se Spyware blíží spíše k Trojskému koni, pracuje bez jakéhokoliv vědomí uživatele. Nejčastěji probíhá instalace skrz zranitelné místo v internetovém prohlížeči, odstranit je není zcela jednoduché. Jsou známy i případy, kdy je nutné odinstalovat internetový

prohlížeč, z důvodu velké provázanosti Spyware a možného zbytkovému kódu, který by v počítači zůstal. Spyware můžeme i rozdělit do dvou kategorií. První z nich je software na sledování zaměstnanců, který je sice instalován bez vědomí uživatele, ale za to se souhlasem vlastníka. Tento software dokáže sledovat aktivitu zaměstnanců, využívání Internetu, soukromých e-mailů atp. Z pohledu vlastníka se jedná o bezpečnostní opatření, ale i nástroj na sledování využití pracovní doby zaměstnance. Druhou kategorií je software, který se používá k odcizení citlivých osobních údajů. V tomto případě se již jedná o trestnou činnost.

Z pohledu uživatelé pracovních stanic se první kategorii Spyware zabránit nedá, ale z pohledu uživatele domácího počítače je obrana nutností. Bohužel se tato obrana neobejde bez instalace specializovaného programu, který dokáže hrozbu vyhledat a zničit. Firmy, které se specializují na vývoj tohoto software, denně vyhledávají, analyzují a vytváří postupy pro jejich zničení. Pokud je nainstalován software od takovéto firmy, je nutné pro jeho absolutní funkčnost ho neustále aktualizovat a provádět kontrolu systému v pravidelných intervalech. Po kontrole je uživatel vyzván k vyřešení nalezených hrozeb, většinou se jedná o smazání veškerého kódu z počítače. Tento kód může být umístěn na všech možných úložištích v počítači, v registrech atp. Pouze dobrý program dokáže tento kód odhalit všude a tam ho také zničit. Autor doporučuje program Spybot dostupný na adrese http://www.safer-networking.org/. Program má velmi jednoduchou instalaci, po které je uživatel vyzván k aktualizaci Spyware definicí a následně je provedeno skenování systému a upozornění na nalezené hrozby, po kterém následuje vyčištění systému.



Obrázek 34 Ukázka programu Spybot

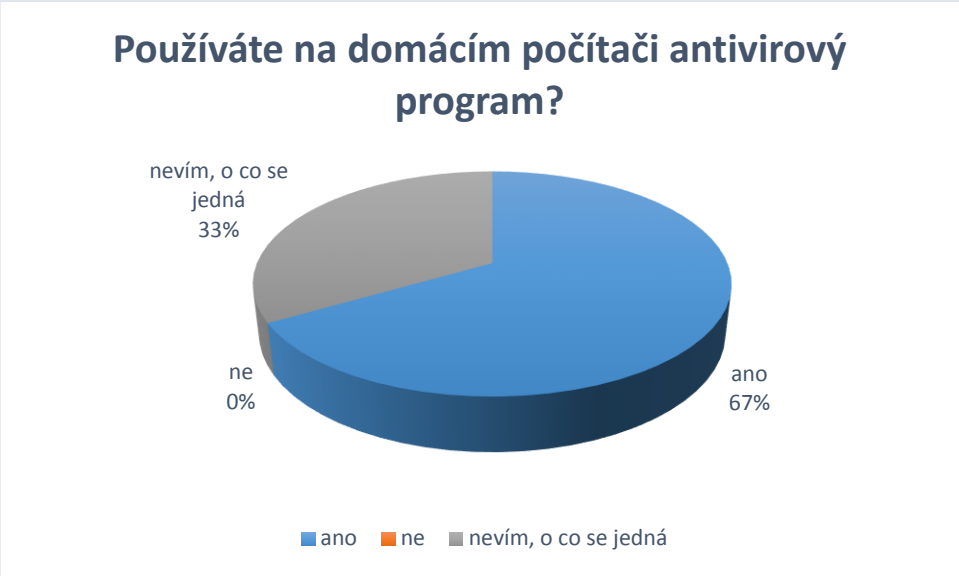
Zdroj: www.safer-networking.org

4.2.4 Firewally a antivirové programy

Poslední tématem v dotazníku Zásady bezpečného chování na Internetu je téma, které opět úzce souvisí s předešlým. Jedná se o ochranu pomocí antivirových programů a firewallů. Základní firewall je součástí operačního systému, ale existují i jiné produkty, které lépe chrání počítač. Nicméně odpověď na otázku o využití antiviru přinesla pro autora překvapivé zjištění. Otázky jsou použity jen dvě, ale jsou zcela dostačující.

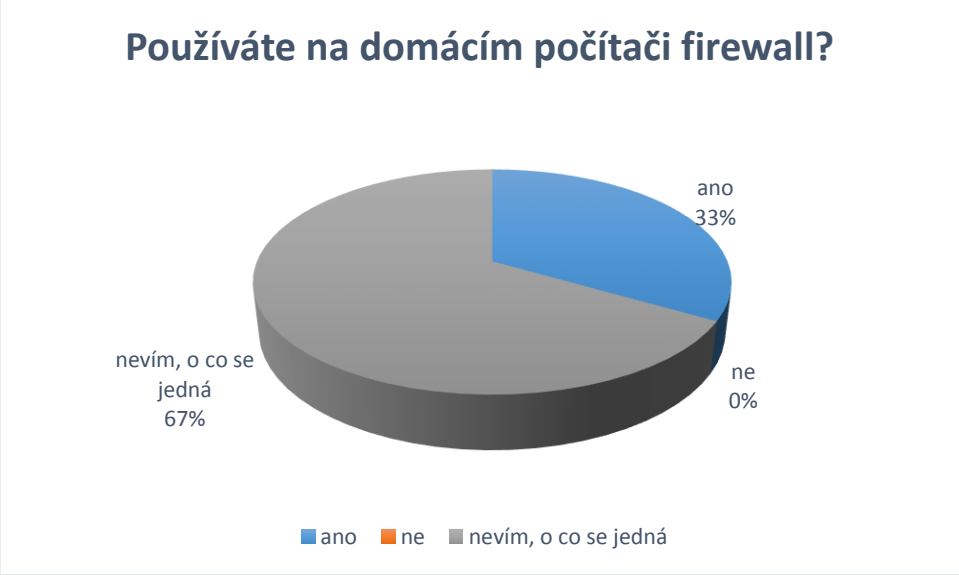
- Používáte na domácím počítači antivirový program?
- Používáte na domácím počítači firewall?

Z klasické dichotomické otázky s možnostmi ano/ne přidává ještě autor třetí možnost, a to „nevím, o co se jedná“.



Graf 17 Vyhodnocení otázky č. 17

Zdroj: vlastní zpracování



Graf 18 Vyhodnocení otázky č. 18

Zdroj: vlastní zpracování

Autor toto zjištění považuje za velmi znepokojivé a jako obrovskou bezpečnostní hrozbu pro uživatele a pro širší okruh lidí, právě z důvodu šíření škodlivého softwaru přes tyto nechráněné počítače. Další hrozbou je možné získání kontroly na počítači respondentů a jejich zapojení do trestné činnosti na poli počítačového zločinu.

První vývoj antivirového programu nelze přesně určit, ale lze zmínit první neutralizaci počítačového viru, provedenou Berntem Fixem v roce 1987. Za první antivirový program lze považovat Solomon´s Anti-Virus Toolkit vyvinutý v roce 1988, který je později uveden na trh, a to v roce 1991.

Je velmi důležité mít na počítači nainstalovaný antivirový program, který dokáže odhalit a chránit systém před viry, červy, trojskými koni a dalšími hrozbami popsanými výše. Sofistikovanější antivirové programy dokáží odhalit a zablokovat také Spyware a programy k otevření „zadních vrátek“ systémů sloužících k ovládnutí počítače. Všechny známé antiviry používají tři druhy zkoumání:

- Skenování v reálném čase
- Manuální skenování
- Heuristickou analýzu

Skenování v reálném čase má za úkol ochránit počítač právě v době, kdy uživatel přistupuje na Internet, nebo pracuje s různými programy. Při této proceduře dochází ke kontrole síťového provozu, kde je hledán škodlivý kód, dále je kontrolována příchozí e-mailová komunikace a její přílohy. Tyto úkoly jsou spuštěny při užívání počítače a pro uživatele probíhají v pozadí a automaticky, nemusí je tedy spouštět.

Manuální skenování spouští uživatel sám a předchází tomu určitý signál, že něco není v pořádku, nebo pokud chce získat jistotu u určitého souboru. Další velmi doporučovanou možností je spouštění manuálního skenování periodicky. Tato možnost a aktuální antivirové definice zajistí uživateli maximální možnou bezpečnost. Manuální skenování jde více do hloubky než kontrola v reálném čase, odhalení hrozby je tedy pravděpodobnější. Periodické skenování sice zabírá hodně výpočetní kapacity, ale právě z důvodu bezpečnosti je nezbytné.

Třetí formou ochrany je heuristická analýza, která se nezabývá konkrétními hrozbami, tedy nemá nadefinované určité kusy škodlivého kódu, které má hledat, ale používá obecné charakteristiky podezřelého chování škodlivého software, které se zaměřuje na síťový provoz nebo e-mailovou komunikaci. Porovnáváním tohoto chování se správným chováním aplikací dokáže odhalit odchylky a upozornit uživatele na podezřelé chování programů.

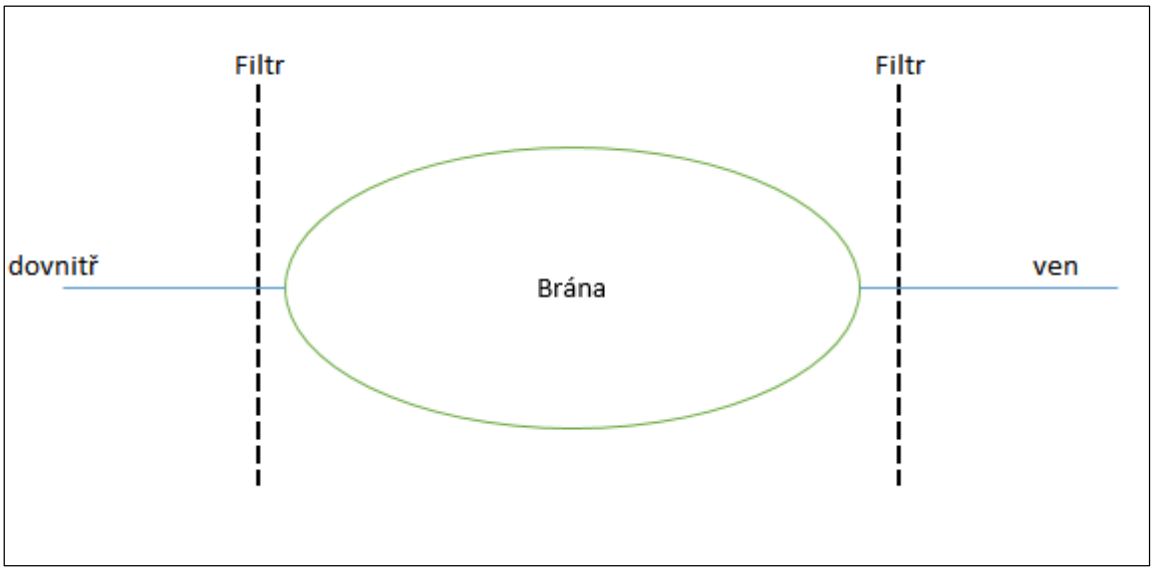
Nejdůležitější tématem u antivirových programů jsou aktualizace. Pouze aktualizovaný antivirový program dokáže poskytnout ochranu systému a uživateli. Techniky útoků a škodlivé programy se neustále vyvíjí, stejně tak se proti nim vyvíjí obrana, ovšem pokud tato obrana není naistalována, uživatel může být ohrožen. Proto platí doporučení, aktualizovat antivirový program denně.

Na trhu je mnoho produktů, antivirové ochrany. Některé jsou bezplatné pro domácí použití, což je pro uživatele výhoda. Je dobré, vybrat si jednu z velkých vývojářských firem, kde je zaručena kontinuita vývoje produktu a zajištěna častá aktualizace. Níže na obrázku jsou názvy a loga největších antivirových firem a jejich produktů.

Obrázek 35 Firmy a antivirové produkty

Zdroj: www.support-igsa-co.uk

Firewall je dalším způsobem ochrany uživatele buď před průnikem útočníka do systému, nebo naopak před odeslání citlivých informací vně systému. Anglický význam slova firewall je zeď bránící rozšíření ohně. Obecně se skládá z několika různých částí:



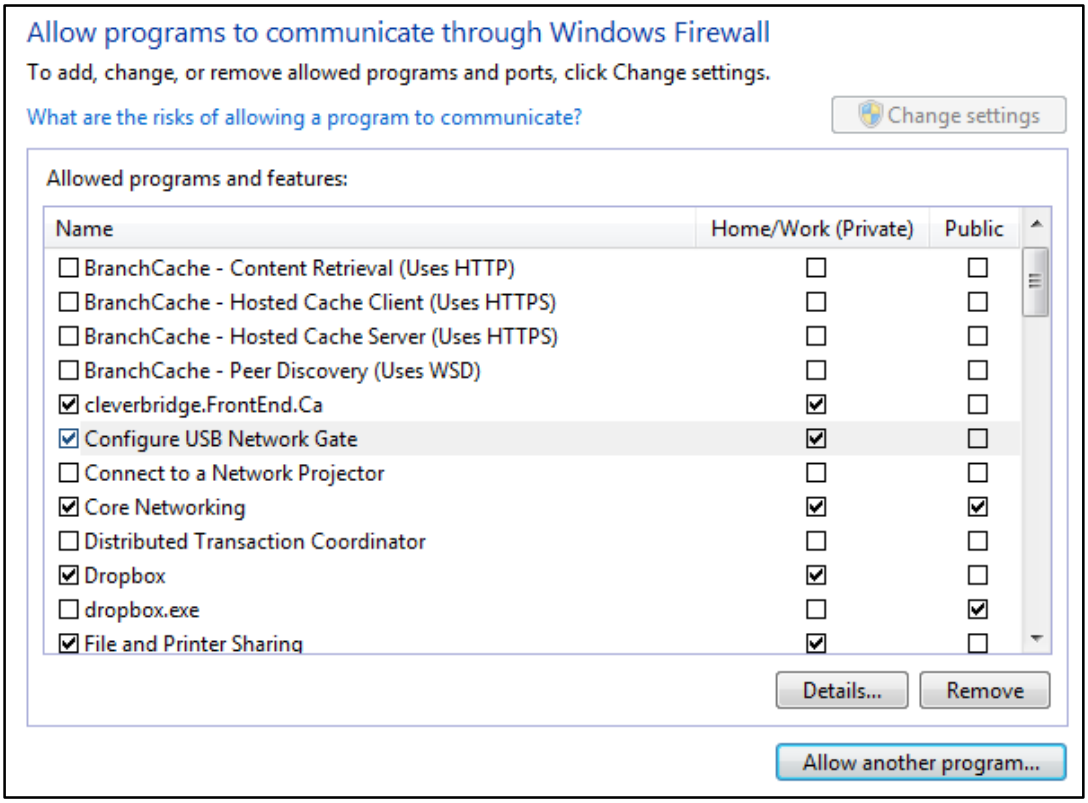
Obrázek 36 Schéma firewallu

Zdroj: Firewally a bezpečnost Internetu

Filtry blokují určité druhy přenosů. Brána je počítač, který tyto filtry kompenzuje. Filtry jako takové prověřují veškerou komunikaci, která prochází přes bránu (místo připojení počítače do sítě). Kontrola je prováděna přes dvě podmínky:

- Jsou data odesílaná do sítě odesílána záměrně?
- Jsou data přicházející do systému žádoucí?

Pro obě tyto podmínky platí, že pokud firewall odhalí jakoukoliv odchylku, přenos přeruší a na proces upozorní uživatele. Nastavení firewallu je proto důležitou součástí správy systému. Při instalaci software, který jakýmkoliv způsobem odesílá nebo přijímá data ze sítě, je uživatel upozorněn, zda chce tento síťový provoz dovolit. Proto je velmi důležité prověřit, zda daný program funguje správně a je bezpečný. Pouze po tomto prověření je možné udělit oprávnění. Všechna tato povolení se dají spravovat samostatně pro každý program a to přímo v nastavení Výjimek firewall. Níže je ukázka správy výjimek pro Windows Firewall, která je pro běžného počítačového uživatele dostačující.



Obrázek 37 Nastavení výjimek u Windows Firewall

Zdroj: www.wiki.eltima.com

Pro tento běžně používaný firewall se rozlišuje nastavení pro různá síťová připojení. Brána používá jiná nastavení pro soukromé a jiná pro veřejné sítě. Předpokladem je, že veřejná síť je méně bezpečná než síť soukromá, proto je nutné po připojení na tyto sítě věnovat pozornost povolení přístupu aplikací do sítě. Brána firewall je přítomna v nejpoužívanějším systém Microsoft Windows automaticky. Je dobré se jejímu nastavení věnovat, uživatel leckdy odhalí programy, u kterých nechce, aby komunikovali s okolním světem. Není tedy nic jednoduššího přizpůsobit nastavení podle svého a komunikaci těmto programům zakázat. [3] [5] [6] [7] [10] [11] [13]

5 Zhodnocení a závěr

Bezpečnost na Internetu je dnes velmi ožehavé téma, ačkoliv dle zjištění autora také téma podceňované. Vývojáři internetových prohlížečů se snaží dělat maximum pro minimalizaci rizik, ovšem záleží pouze na uživateli, zda tuto minimalizaci alespoň trochu podporuje.

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. Hlavními tématy jsou hesla, hrozba phishingu a zfalšovaných internetových stránek, instalace nežádoucího a škodlivého software a používání ochranných programů jako jsou například antivirus a firewall. Do průzkumu zapojil autor své spolužáky a spolupracovníky. Níže v tabulce jsou shrnuty výsledky:

Hesla			
	Ano	**Ne**	
1. Používáte na Internetu hesla?	30	0	
2. Používáte je na více internetových stránkách?	30	0	
3. Pokud ano, používáte na všech stejné heslo?	20	10	
4. Jaká je průměrná délka vašich hesel?	**1-4 znaků**	**5-7 znaků**	**8+ znaků**
	5	20	5
	Ano	**Ne**	
5. Používáte hesla složená z malých a velkých písmen, číslic a speciálních znaků?	5	25	

Phishing a zfalšované internetové stránky			
	Ano	**Ne**	
6. Setkáváte se s těmito druhy e-mailů?	30	0	
7. Odkud podvodný e-mail přichází?	**Banka**	**Úvěr. společnost**	**Elektronický obchod**
	17	7	6
	Ano	**Ne**	
8. Znáte případy z médií?	15	15	
9. Jak na ně reagujete?	**Mažu**	**Nevím, co mám dělat**	**Otvírám přílohu**
	13	4	13
	Ano	**Ne**	
10. Kliknete na odkaz v e-mailu od neznámého odesílatele?	12	18	
11. Ověříte si stránku, na kterou Vás odkaz přenesl?	3	27	
12. Zadáváte na ní nějaké citlivé údaje?	4	26	
Malware, Spyware, Adware			
	Ano	**Ne**	
13. Pokud Vám přijde e-mail z neznámé adresy obsahující přílohu, otevřete ji?	6	24	
14. Začal se Váš PC po otevření chovat podivně?	6	24	
15. Načítá se dlouho internetový prohlížeč?	6	24	
16. Změnila se Vám domovská stránka?	6	24	
Firewally a antivirové programy			
	Ano	**Ne**	**Nevím, o co se jedná**
17. Používáte na domácím počítači antivirový program?	20	0	10
18. Používáte na domácím počítači firewall?	10	0	20

Tabulka 3 Výsledky dotazníkového šetření [jedná se o počty odpovědí]

Zdroj: vlastní zpracování

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.

6 Seznam použité literatury

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

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

[3] 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.

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

[5] 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.

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

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

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

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

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

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

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

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

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

[15] 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.

[16] ABOUT-THE-WEB.COM. Browsers [online] c2007. Dostupné z WWW:
<http://www.about-the-web.com/shtml/browsers.shtml >

[17] BARTOŠEK, M. Krátce z Historie internetu. [online] c2011. Dostupné z WWW:
<http://ics.muni.cz/bulletin/articles/22.html >

[18] BERNERS-LEE, T. The WorldWideWeb browser. [online] c2010. Dostupné z WWW:
<http://www.w3.org/People/Berners-Lee/WorldWideWeb.html >

[19] GARSIEL, T. How browser works [online] c2000. Dostupné z WWW:
<http://taligarsiel.com/Projects/howbrowserswork1.htm >

[20] GOOGLE. Chrome help center. [online] c2015. Dostupné z WWW:
<https://support.google.com/chrome/?hl=en >

[21] GOOGLE. Chrome Releases. [online] c2015. Dostupné z WWW:
<http://googlechromereleases.blogspot.cz/ >

[22] GOOGLE. Sdělení k ochraně soukromí pro Google Chrome. [online] c2015. Dostupné
z WWW: <https://www.google.com/intl/cs/chrome/browser/privacy/ >

[23] CHURÝ, L., METELKA, J. Internet a jeho historie v ČR. [online] c2005. Dostupné
z WWW: <http://programujte.com/clanek/2005122001-internet-a-jeho-historie-v-cr/ >

[24] LACOBI, J. L. Browser Comparison. [online] c2014. Dostupné z WWW:
<http://www.pcworld.com/article/2605933/browser-comparison-how-the-five-leaders-stack-up-in-speed-ease-of-use-and-more.html >

[25] MIT, ERCIM, KEYIO, BEIHANG. About W3C [online] c2015. Dostupné z WWW:
<http://www.w3.org/Consortium/ >

[26] SECUNIA. Secunia vulnerability review 2014 [online] c2015. Dostupné z WWW:
<http://secunia.com/?action=fetch&filename=secunia_vulnerability_review_2014.pdf>

[27] SSL-CERTIFIKATY.CZ SSL protokol. [online] c2015. Dostupné z WWW:
<https://www.ssl-certifikaty.cz/o-certifikatech/ssl-protokol/ >

[28] WAYNER, P. Battle of the Web browsers. [online] c2011. Dostupné z WWW:
<http://www.infoworld.com/article/2623985/applications/
battle-of-the-web-browsers.html >

7 Přílohy

Informace zasílané společnosti Google při používání produktu Chrome

Pokud pomocí jakéhokoli prohlížeče (včetně Chrome) kontaktujete servery Google, obdrží společnost Google ve výchozím nastavení standardní informace protokolu včetně IP adresy vašeho počítače a jednoho nebo několika souborů cookie.

Kromě toho mohou některé funkce Chrome odesílat společnosti Google nebo vašemu výchozímu vyhledávači omezené množství dalších údajů:

- Pokud jako svůj vyhledávač vyberete Google, Chrome při spuštění nebo změně sítě kontaktuje společnost Google a pokusí se určit nejlepší místní webovou adresu pro odeslání zadaných vyhledávacích dotazů. Když do adresního řádku (omniboxu) prohlížeče Chrome nebo do vyhledávacího pole Spouštěče aplikací zadáváte webovou adresu nebo dotaz, napsaná písmena se mohou odesílat do vašeho výchozího vyhledávače, aby vám mohla predikční funkce vyhledávače automaticky doporučit hledané výrazy nebo webové adresy. Jste-li přihlášeni, pak navíc text, který zadáte do vyhledávacího pole Spouštěče aplikací, může být odeslán do Googlu, abychom vám mohli doporučovat hledané kontakty nebo aplikace. Pokud se rozhodnete předpokládaný dotaz nebo adresu použít, Chrome může z prohlížeče do výchozího vyhledávače odeslat i tuto informaci. Další informace ovypnutí předpokládaných dotazů navrhovaných serverem v omniboxu a zásadách protokolování předpokládaných dotazů v omniboxu společnosti Google.
- Pokud zadáte neexistující adresu URL, může ji Chrome odeslat společnosti Google, abychom vám pomohli najít správnou adresu URL. Tyto informace můžeme také v souhrnné formě použít k tomu, abychom pomohli ostatním uživatelům webu – například abychom jim sdělili, že je určitý web mimo provoz. Další informace o vypnutí návrhů při chybách navigace.
- Pokud aplikaci, rozšíření nebo webu udělíte oprávnění k použití zasílání zpráv v cloudu od Googlu nebo pokud použijete Synchronizaci Chrome, Chrome vygeneruje náhodné ID zařízení. Toto ID zařízení je sdíleno se společností Google, avšak nemají k němu přístup třetí strany. Když zařízení přestanete používat nebo odstraníte profil Google, ID zařízení bude zrušeno. Chrome z ID zařízení odvodí ID

registrace, které bude sdíleno s aplikacemi, rozšířeními a weby za účelem bezpečného přenosu zpráv ze serverů Google do prohlížeče.

- Pokud se do prohlížeče Chrome, operačního systému Chrome OS nebo do zařízení Android s předinstalovanou aplikací Chrome přihlásíte pomocí svého účtu Google, aktivuje se funkce synchronizace. Některé informace, jako například historii, adresy URL přidané do záložek spolu s obrázkem a ukázkovým textem ze stránky, hesla a další nastavení, společnost Google uloží na svých serverech a přidruží je k vašemu účtu Google. Informace uložené v účtu Google jsou chráněny zásadami ochrany soukromí společnosti Google. Tyto informace ukládáme také proto, abychom vám je mohli zpřístupnit v jiných instancích Chromu, do kterých se přihlásíte. Přečtěte si také o specifických informacích, které lze synchronizovat, a o zakázání funkce synchronizace Chrome.
- Používáte-li v Chromu funkci Automatické vyplňování, která za vás automaticky vyplňuje webové formuláře na základě podobných formulářů, které jste vyplnili dříve, bude Chrome do společnosti Google odesílat omezené množství informací o stránkách s webovými formuláři. Bude se odesílat například kód vytvořený z adresy URL jednosměrnou hašovací funkcí a struktura formuláře, abychom pro daný webový formulář mohli Automatické vyplňování zlepšit. I když údaje, které Chrome odesílá, mohou obsahovat informace o tom, že jste zadali informace do formuláře, text zadaný do jednotlivých polí společnosti Google odeslán nebude. Tento text bude odeslán pouze v případě, že v Chromu zvolíte možnost ukládání dat do účtu Google prostřednictvím funkce synchronizace.
- Používáte-li funkci sdílení polohy, která umožňuje sdělovat webovým stránkám vaši polohu, odesílá Chrome informace o místních sítích službám určování polohy Google. Ty pak podle nich určí přibližnou polohu. Další informace o službách určování polohy Google a povolení nebo zakázání funkcí sdílení polohy v prohlížeči Google Chrome. Informace o místních sítích mohou – v závislosti na možnostech zařízení – obsahovat údaje o nejbližších směrovačích sítě Wi-Fi, identifikátory nejbližších vysílačů mobilní sítě, informace o síle signálu sítě Wi-Fi nebo mobilní sítě a adresu IP, která je aktuálně přiřazena vašemu zařízení. Tyto údaje slouží k přibližnému určení vaší polohy a k zajištění provozu, podpory a zlepšení celkové kvality prohlížeče Chrome a služeb určování polohy společnosti

Google. Popsané shromážděné informace budou nejdříve anonymizovány a sloučeny a poté je společnost Google využije při vývoji nových služeb nebo za účelem zvyšování celkové kvality dalších služeb Google.

- Pokud se pokusíte připojit k webu pomocí zabezpečeného připojení a prohlížeč toto připojení zablokuje, protože určité informace naznačují, že na vás v síti někdo aktivně útočí (útok typu „man in the middle“), může Chrome informace o připojení odeslat společnosti Google, abychom mohli určit rozsah a mechanismus útoku.

Informace odesílané společnosti Google při používání funkce Bezpečné prohlížení v produktu Chrome nebo v jiných prohlížečích

Google Chrome a některé prohlížeče třetích stran (mimo jiné určité verze prohlížečů Mozilla Firefox a Apple Safari) obsahují funkci Bezpečné prohlížení. Bezpečné prohlížení přenáší mezi prohlížečem a servery společnosti Google informace o podezřelých stránkách – například pokud navštívíte stránky podezřelé z phishingu nebo šíření malwaru.

Prohlížeč pravidelně kontaktuje servery Google a stahuje nejnovější seznam pro Bezpečné prohlížení, který obsahuje známé phishingové a malwarové stránky. Google v rámci tohoto kontaktu neshromažďuje žádné informace o účtu ani jiné informace, které by bylo možné použít ke zjištění totožnosti, obdrží však standardní informace protokolu včetně IP adresy a jednoho nebo několika souborů cookie. Nejnovější kopie seznamu se ukládá místně v systému.

U každé navštívené stránky bude zkontrolováno, zda se na tomto místně uloženém seznamu nenachází. Jestliže se na seznamu nachází, prohlížeč odešle společnosti Google otisk adresy URL vytvořený jednosměrnou hašovací funkcí, aby společnost Google mohla do prohlížeče odeslat další informace. Podle těchto informací nemůže společnost Google zjistit skutečnou adresu URL. Další informace o principu této kontroly.

Následující odstavec se týká pouze chování funkce Bezpečného prohlížení v produktech Chrome:

- Některé verze produktů Chrome obsahují technologii Bezpečného prohlížení, která dokáže identifikovat potenciálně škodlivé weby nebo stažené spustitelné soubory, které Google zatím nezná. Informace týkající se potenciálně škodlivých webů nebo stahovaných spustitelných souborů (včetně úplné adresy URL webu nebo stahovaného spustitelného souboru) mohou být odeslány společnosti Google s

cílem zjistit, zda je daný web nebo stahovaný soubor škodlivý. Společnost Google v rámci tohoto kontaktu neshromažďuje žádné informace o účtu ani jiné informace, které by bylo možné použít ke zjištění totožnosti, obdrží však standardní informace protokolu včetně adresy IP, navštívené adresy URL a jednoho nebo několika souborů cookie.

- Chrome pomocí technologie Bezpečné prohlížení pravidelně kontroluje váš počítač a vyhledává v něm nežádoucí software, který zabraňuje změně nastavení nebo jiným způsobem narušuje zabezpečení a stabilitu prohlížeče. Je-li takový software zjištěn, může vám Chrome nabídnout možnost stažení nástroje na odstranění softwaru, abyste jej mohli odstranit.
- Pokud se zdá, že navštívená stránka obsahuje Malware, můžete povolit odeslání dalších dat, která budou použita ke zlepšování funkce Bezpečné prohlížení. Tato data budou odeslána, když zavřete stránku s upozorněním funkce Bezpečné prohlížení nebo z ní přejdete někam jinam. Zprávy odesílané společnosti Google mohou obsahovat data jako adresu URL nebo obsah daného webu, popřípadě adresu URL stránky, která vás na tento web přesměrovala. Společnost Google pomocí těchto údajů může ověřit, zda se na stránce stále vyskytuje potenciálně škodlivý obsah.

Informace odesílané provozovatelům webových stránek, které navštívíte pomocí Chromu

Stránky navštívené pomocí prohlížeče Google Chrome automaticky obdrží standardní informace protokolu podobné těm, které jsou odesílány společnosti Google. Tyto weby také mohou odesílat vlastní soubory cookie nebo do vašeho systému ukládat svoje soubory. Soubory cookie a další data webů můžete na stránce nastavení v Chromu omezit.

Pokud jsou v Chromu povoleny funkce předpovídání síťových akcí, Chrome může vyhledávat IP adresy všech odkazů na webových stránkách a otevírat síťová připojení za účelem rychlejšího načtení webových stránek. Webové stránky také mohou používat technologii předběžného vykreslování k předběžnému načtení odkazů, na které byste mohli následně kliknout.

Pokud Chrome budete používat v anonymním režimu nebo v režimu hosta, prohlížeč nebude navštíveným webům zasílat žádné již existující soubory cookie. Při práci v těchto režimech mohou weby do systému ukládat nové soubory cookie, tyto soubory cookie nicméně zůstanou uloženy (a budou používány při komunikaci s weby) pouze dočasně – do doby, než anonymní režim nebo režim hosta ukončíte. Jakmile zavřete prohlížeč či všechna otevřená anonymní okna, popřípadě ukončíte režim hosta, budou tyto soubory vymazány.

Pokud v produktu Chrome povolíte používání funkce určování polohy, může tato služba sdělit vaši polohu navštívenému webu. Žádnému webu však nesdělíme vaši polohu bez vašeho souhlasu. Společnost Google nemá žádnou kontrolu nad weby třetích stran nebo jejich postupy v oblasti ochrany soukromí. Než vydáte souhlas se sdílením informací o poloze s určitým webem, důkladně posuďte jeho zásady ochrany soukromí.

- Informace ukládané do systému při používání produktů Chrome

Produkty Chrome ukládají některé informace místně do systému. Mezi ně mohou patřit:

- základní informace o historii prohlížení, například adresy URL navštívených stránek, textové a obrázkové soubory těchto stránek z mezipaměti a seznam některých IP adres, na které navštívené stránky odkazují,
- prohledávatelný index většiny navštívených stránek (kromě zabezpečených stránek s webovou adresou „https“ – např. některé stránky bank),
- miniatury většiny vámi navštívených stránek,
- soubory cookie nebo soubory z webu, které do systému uložily navštívené webové stránky,
- místně uložená data doplňků,
- záznamy o stahování z webových stránek

[22]