Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Zabezpečení počítače proti přístupu na nevhodné stránky

Marek Jína

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jína Marek

Informatika

Název práce

Zabezpečení počítače proti přístupu na nevhodné stránky

Anglický název

Computer security against access to inappropriate websites

Cíle práce

Cílem této práce je zpracování informací o možnostech zabezpečení počítače proti přístupu dětí na stránky s nevhodným obsahem, to znamená na stránky s pornografickým obsahem a jiné stránky, které by dle mínění rodičů mohly nějakým způsobem poškodit zdravý sociální vývoj jejich dítěte.

Metodika

Metodika řešené problematiky zadané bakalářské práce je založena na průzkumu trhu a hledání nejefektivnější varianty pro zabezpečení počítače a internetového prohlížeče, porovnání různých produktů od různých společností a následné vyhodnocení jednotlivých softwareových řešení. Na základě získaných informací o jednotlivých produktech z jejich porovnání vytvořím přehled a hodnocení produktů z hlediska některých kritérií. Na základě tohoto vyhodnocení bude formulován závěr bakalářské práce.

Harmonogram zpracování

1) Příprava a studium odborných informačích zdrojů , upřesnění dílčích cílů práce a volba postupu řešení: 6/2011
2) Zpracování přehledu řešené problematiky dle informačních zdrojů: 7/2011-8/2011
3) Zpracování vlastního řešení, diskuze a zhodnocení výsledků: 9/2011-10/2011
4) Tvorba finálního dokumentu bakalářské práce: 11/2011-2/2012
5) Odevzdání bakalářské práce a teze: 3/2012

Rozsah textové části
30 - 40 stran

Klíčová slova
Zabezpečení PC, ochrana dětí na internetu, blokování internetových strránek, omezení práv na PC

Doporučené zdroje informací

Matt Bishop, Introduction to Computer Security, 2005,0-321-24744-2, Addison Wesley
David LeBlanc, Michael Howard, Bezpečný Kód, 5.11.2008, 978-80-251-2050-7, COMPUTER PRESS
Ondřej Bitto, Jak zabezpečit domácí a malou síť Windows XP, 9.8.2006, 978-80-251-1098-0, COMPUTER PRESS
http://www.parentalcontrol.net
http://www.softforyou.com
http://www.saferinternet.cz

Vedoucí práce
Brechlerová Dagmar, RNDr., Ph.D.

Termín odevzdání
březen 2012

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

prof. Ing. Jan Hron, DrSc., dr.h.c.
Děkan fakulty

V Praze dne 21.11.2011

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Zabezpečení počítače proti přístupu na nevhodné stránky" jsem vypracoval samostatně pod vedením vedoucího bakalářské 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 bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 27. listopadu 2012 _____

Poděkování

Touto cestou bych rád poděkoval všem, kteří mi pomáhali s přípravou práce, nebo mě jakkoli podporovali během jejího vytváření. Zejména pak chci poděkovat vedoucí mé bakalářské práce RNDr. Dagmar Brechlerové, Ph.D. za podnětné rady, čas strávený konzultacemi a její trpělivost. V neposlední řadě bych rád poděkoval všem svým přátelům, kamarádům a rodině za jejich připomínky a náměty.

Zabezpečení počítače proti přístupu na nevhodné stránky

Computer security against acces to inappropriate websites

Souhrn

Bakalářská práce se zabývá zabezpečením počítače proti přístupu na internetové stránky, které rodiče vyhodnotí jako nevhodné vzhledem k jejich dětem. Jedná se o stránky, které by mohly poškodit zdravý sociální vývoj dítěte, tedy o stránky s nevhodnými tématy, například pornografie, nebo stránky, kde se dítě může setkat se šikanou, nebo hrozí odcizení důležitých osobních údajů. Teoretická část rozebírá jednotlivé hrozby, kterým mohou být děti vystaveny na internetu, základní charakteristiku některých nevhodných stránek a popis jednotlivých hrozeb na dané stránce. Praktická část se následně zabývá minimalizováním hrozeb popsaných v teoretické části. Popisuje instalaci a následné nastavení některých volně šiřitelných programů a následně jsou programy srovnány na základě některých parametrů a jsou vyhodnoceny v přehledové tabulce.

Klíčová slova

Zabezpečení PC, ochrana dětí na internetu, blokování internetových stránek, omezení práv na PC, šikana, kyberšikana, nevhodné stránky, pornografie

Summary

This thesis deals with computer security to prevent access to websites that parents evaluate as unsuitable due to their children. These are sites that could harm the healthy social child development, sites with inappropriate themes, such as pornography, or sites where child may encounter bullying or risk alienation important personal data. The

theoretical part discusses the various threats that children can be exposed to on the internet, some basic characteristics of inappropriate sites and description of each threat on a given page. The practical part then deals with minimizing the treats described in the theoretical part. It describes installing and setting up some freeware programs and these programs are compared on the basis of certain parameters and are evaluated in a summary table.

Keywords

PC security, child protection on the internet, blocking websites, restriction of the rights on the PC, bullying, cyberbullying, inappropriate websites, pornography

Obsah

Obsah 3
1 Úvod 5
2 Cíl práce a metodika 6
3 Teoretická část 7
3.1 Kyberšikana 7
3.1.1 Flaming 10
3.1.2 Ponižování a pomlouvání (denigration) 10
3.1.3 Zneužití cizí identity ke kyberšikaně 10
3.1.4 Zveřejňování cizích tajemství s cílem poškodit oběť (outing) 11
3.1.5 Obtěžování (harassment) 11
3.1.6 Stalking / kyberstalking 12
3.1.7 Happy slapping 12
3.1.8 Sexting 13
3.1.9 Kybergrooming 14
3.2 Stránky s nevhodným obsahem 16
3.2.1 Pornografické stránky 16
3.2.2 Stránky podporující rasismus nebo jiné formy násilí 17
3.3 Sociální sítě 17
3.3.1 Facebook 18
3.3.2 Lidé.cz 20
3.3.3 Google+ 22
3.4 Instant messaging 23
3.4.1 ICQ 24
3.4.2 SKYPE 25
4 Praktická část 27

4.1 Windows Live Essentials 2012 27
4.1.1 Instalace 27
4.1.2 První spuštění služby Zabezpečení rodiny 28
4.1.3 Nastavení a používání služby Zabezpečení rodiny 29
4.1.4 Zhodnocení služby Zabezpečení rodiny 34
4.2 Qustodio 35
4.2.1 Instalace aplikace Qustodio 35
4.2.2 Nastavení a používání služby Qustodio 37
4.2.3 Zhodnocení aplikace Qustodio 41
5 Závěr práce 43
6 Citovaná literatura 46
7 Seznam obrázků 48
8 Seznam tabulek 49

1 Úvod

Tématem bakalářské práce je popis jednoho z nejzávažnějších problémů, se kterým se může setkat téměř každý rodič a jeho dítě. V dnešní přetechnizované době je internet vydatným pomocníkem při řešení různých problémů. Je zdrojem širokého spektra informací a zábavy, jako jsou například: videa, hudební videoklipy, filmy, hudba, obrázky ale i sociální sítě, které mohou být i zdrojem různých rizik spojených s používáním malými dětmi.

V současné době je možné na internetu najít téměř cokoliv, od různých pomocníků pro školní mládež v podobě referátů až po odborné články sepsané skutečnými vědci. Internet je ale také plný nejrůznějších hrozeb, kterými se tato bakalářská práce zabývá. Ještě před dvaceti lety číhalo nebezpečí na děti pouze venku a ve výjimečných případech ve vlastní rodině (zneužívané děti, děti umlácené vlastními rodiči), ale dnes číhá i na druhé straně síťového kabelu.

Internet je velkým pomocníkem téměř každého člověka v moderním světě. Využíváme jej každý den, a svůj život si bez něj již mnohdy nedokážeme ani představit. Velká část převážně mladších lidí vyměnila denní tisk za internetové noviny, klasickou poštu za e-maily a mnohdy i televizi za streamované pořady.

Mnoho uživatelů si ani rizika prohlížení internetu spojené s dětmi nedokáže představit, ať už se jedná o prohlížení internetových stránek určených pro dospělé, nebo cílený útok ze strany jiných uživatelů ve formě kyberšikany.

Případy kyberšikany se objevují denně po celém světě, píší o nich noviny a slýcháme o nich z televize. Dítě samotné většinou ani neví, jak se těmto útokům bránit. Způsoby obrany jsou dětem vysvětlovány ve škole a od rodičů, ale ne vždy je dítě dokáže správně použít. Z tohoto důvodu by měl rodič zasáhnout a zajistit svému dítěti dostatečnou prevenci.

2 Cíl práce a metodika

Cíl práce

Cílem této práce je zpracování informací o možnostech zabezpečení počítače proti přístupu dětí na stránky s nevhodným obsahem, to znamená na stránky s pornografickým obsahem a jiné stránky, které by dle mínění rodičů mohly nějakým způsobem poškodit zdravý sociální vývoj jejich dítěte.

Metodika

Metodika řešené problematiky zadané bakalářské práce je založena na průzkumu trhu a hledání nejefektivnějších variant pro zabezpečení počítače a internetového prohlížeče, porovnání různých produktů od různých společností a následné vyhodnocení jednotlivých softwarových řešení. Na základě získaných informací o jednotlivých produktech a z jejich porovnání vytvořím přehled a hodnocení produktů z hlediska některých kritérií. Na základě tohoto vyhodnocení bude formulován závěr bakalářské práce.

3 Teoretická část

3.1 Kyberšikana

Jedním z velkých rizik, se kterým se děti také mohou na internetu setkat, je takzvaná kyberšikana. „*Kyberšikanu (cyberbullying) definujeme jako zneužití ICT (informačních komunikačních technologií), zejména pak mobilních telefonů a internetu, k takovým činnostem, které mají někoho záměrně vyvést z rovnováhy.*“ [1]

„*Za šikanování se považuje, když jeden nebo více žáků úmyslně a opakovaně ubližuje druhým. Znamená to, že vám někdo, komu se nemůžete ubránit, dělá, co je vám nepříjemné, co vás ponižuje, nebo to prostě bolí – strká do vás, nadává vám, schovává vám věci, bije vás. Ale může vám znepříjemňovat život i jinak, pomlouvá vás, intrikuje proti vám, navádí spolužáky, aby s vámi nemluvili a nevšímali si vás.*“ [2]

Rozeznáváme 8 základních druhů šikany:

- **Fyzická přímá aktivní** – Útočníci oběť fyzicky napadají, škrtí ji, kopou, fackují, atd.
- **Fyzická nepřímá aktivní** – Útočník pošle na oběť své kamarády, nenapadá ji přímo on, ale také dochází k fyzickému násilí
- **Fyzická pasivní přímá** – Útočník fyzicky brání oběti k dosažení jejího cíle, například mu zabraňuje nastoupit do tramvaje
- **Fyzická pasivní nepřímá** – Útočník odmítá splnění požadavků oběti, například učitel odmítne žáka pustit ze třídy na toaletu
- **Verbální aktivní přímá** – Útočník oběti nadává, uráží ji, nebo zesměšňuje
- **Verbální aktivní nepřímá** – Útočník šíří o oběti pomluvy, skládá o ní nelichotivé básně, nebo ji zesměšňuje pomocí kreseb
- **Verbální pasivní přímá** – Agresor neodpovídá oběti na pozdrav, na otázky, atd.
- **Verbální pasivní nepřímá** – Blízké okolí se nezastane oběti, pokud je neprávem obviněna z něčeho, co udělali její trýznitelé

Kyberšikana je šikana využívající kybernetických prostředků. Tento druh šikany je velice nebezpečný, protože ne každý hned vnímá projevy kyberšikany jako šikanu. Na rozdíl od klasické šikany zde nedochází k fyzickým útokům, ale pouze k psychickým. Díky anonymitě může být tento druh šikany horší, protože si útočník dovolí víc, než při přímém kontaktu.

„*Zatímco u tradiční šikany lze předpokládat, kdy a kde k útoku dojde (např. ve škole, na hřišti), s kyberšikanou se můžeme setkat* ***kdykoliv*** *a* ***kdekoliv****. Obětí útoku se můžeme stát vždy, když budeme připojeni k internetu, nebo mobilní síti (GSM). V takovémto případě se před kyberútokem nemáme kam schovat. Útočník si nás může najít třeba i o půlnoci v „bezpečí domova“.*“ [3]

S kyberšikanou je nutné bojovat. Server Bezpečně online uveřejnil 10 tipů pro rodiče a učitele, jak kyberšikaně předcházet:

- Naučte děti chránit si soukromí a respektovat soukromí druhých
- Naučte děti nereagovat na urážlivé zprávy
- Mluvte s dětmi o tom, co přesně může být někomu druhému nepříjemné
- Naučte děti blokovat konkrétní uživatele v komunikačních aplikacích
- Vysvětlete dětem, ať urážlivé zprávy ukládají jako důkaz
- Poznejte kamarády svých dětí
- Mluvte se svými dětmi o všem, co na internetu dělají
- Budujte důvěru svých dětí. Svěří se vám v případě, že se dostanou do problémů
- Ujistěte děti, že není jejich vina, když je někdo obtěžuje
- Vysvětlete dětem, jak důležité je chránit si heslo. Hesla si musí chránit – nikomu nesvěřovat

[4]

Každý člověk, který se na kyberšikaně podílí jako útočník, nebo jako spolupachatel, by si měl uvědomit, že v případě, že se na jeho činy přijde a dostane se před soud, může být souzen podle zákona č. 40/2009 sb. Níže jsou vypsány některé

paragrafy, které mohou být v souvislosti s kyberšikanou porušeny, a trestní sazby odnětí svobody, které za porušení těchto paragrafů hrozí.

Tabulka 1 – Trestní sazby některých paragrafů, podle kterých by se dala posuzovat kyberšikana

§ zák. č. 40 /2009 Sb.	Název paragrafu	Trest odnětí svobody
§144	Účast na sebevraždě	až 12 let
§175	Vydírání	až 16 let
§180	Neoprávněné nakládání s osobními údaji	až 8 let
§181	Poškození cizích práv	až 5 let
§182	Porušení tajemství dopravovaných zpráv	až 10 let
§183	Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí	až 8 let
§184	Pomluva	až 2 roky
§191	Šíření pornografie	až 5 let
§192	Výroba a jiné nakládání s dětskou pornografií	až 8 let
§209	Podvod	až 10 let
§230	Neoprávněný přístup k počítačovému systému a nosiči informací	až 8 let
§231	Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	až 5 let
§232	Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti	až 2 roky
§352	Násilí proti skupině obyvatelů a proti jednotlivci	až 3 roky
§353	Nebezpečné vyhrožování	až 3 roky
§354	nebezpečné pronásledování	až 3 roky
§356	Podněcování k nenávisti vůči skupině osob nebo omezování jejich práv a svobod	až 3 roky
§357	Šíření poplašné zprávy	až 8 let

Zdroje: [3] ; [5]

Rozeznáváme několik druhů kyberšikany.

3.1.1 Flaming

Flaming je: „*virtuální agresivita, disinhice na internetu, „rozohňování se," vědomě hostilní (nepřátelské) a urážlivé vzkazy na internetu s cílem někoho dehonestovat a rozčílit*". [6]

Jedná se v podstatě o cílený útok na konkrétní osobu nebo skupinu osob za účelem ponižování. S flamingem je možné se setkat převážně na sociálních sítích, Instant Messagingu, nebo v chatech. Nejúčinnější formou obrany proti flamingu je ignorace. Pokud bude útočník ignorován, po nějaké době ho to přestane bavit a útoků zanechá.

3.1.2 Ponižování a pomlouvání (denigration)

„*Útočník se snaží poškodit pověst obětí a narušit její vztahy tím, že o ní zveřejňuje nepravdivé informace (pomluvy) nebo ji uráží a ponižuje (veřejně kritizuje např. její vzhled, oblékání, chování). Tímto projevem kyberšikany trpí nejen děti. Oběťmi se čím dál častěji stávají také učitelé. Žáci se jim tímto způsobem mstí např. za špatný prospěch.*" [3]

Tento typ šikany je hojně využíván na sociálních sítích, kde útočník pomlouvá oběť přímo na jejím vlastním profilu. Nejúčinnější formou obrany je zablokování útočníka tak, aby nemohl podobné příspěvky na zeď uživatele již psát.

3.1.3 Zneužití cizí identity ke kyberšikaně

Zneužití cizí identity je obzvláště nebezpečné. Dojde k němu tak, že útočník odhalí nebo odcizí oběti uživatelské jméno a heslo třeba k sociální síti, e-mailu, Instant Messengeru, nebo k chatu. Útoky se rozdělují na dva směry:

- **Přímý útok**, kdy útočník šikanuje oběť přímo, to znamená, že mu maže zprávy nebo kontakty, nebo publikuje o oběti jejím jménem nepravdivé informace.
- **Nepřímý útok**, kdy se útočník snaží dostat oběť do problémů tím, že jejím jménem posílá nevhodné zprávy ostatním uživatelům, nebo jejím jménem páchá trestnou činnost.

Z důvodu možnosti lehkého odcizení identity, například ve škole, kdy spolužák zaregistruje heslo, kterým se jiný spolužák přihlašuje například na sociální síť, je velmi doporučeno používat pro každou službu jiné heslo. Není nic horšího, než když útočník získá přístup k více komunikačním kanálům, kde může jednat jménem oběti.

3.1.4 Zveřejňování cizích tajemství s cílem poškodit oběť (outing)

„*Útočník má k dispozici intimní či ztrapňující materiály o oběti (intimní fotografie, důvěrné informace apod.), které může zveřejnit prostřednictvím internetu nebo mobilního telefonu.*“ [3]

Útočník může tyto informace od oběti získat buď dobrovolně tak, že mu je oběť sama poskytne, nebo je může z oběti vylákat například nějakou lstí. Nejúčinnější obranou proti této formě kyberšikany je prevence. Je zapotřebí dát si pozor, komu jsou sdělovány jaké informace, a nejlépe choulostivé informace nebo fotografie neposkytovat vůbec nikomu. I z člověka, který se tváří jako největší kamarád, se může časem stát nebezpečný útočník.

3.1.5 Obtěžování (harassment)

„*Útočník se snaží oběť vyvést z rovnováhy tím, že jí opakovaně telefonuje, prozvání ji, nebo jí píše zprávy (SMS zprávy, e-maily, vzkazy do chatu, diskuze, IM atd.). Jeho cílem je především „otravovat“ oběť, a tím jí znepříjemňovat život.*“ [3]

Obtěžování je velmi nebezpečnou formou šikany a časem může přejít až ke stalkingu. Nejúčinnější formou obrany proti obtěžování je blokace obtěžujícího uživatele. Blokaci je možné provést přímo na sociální síti přidáním uživatele do tzv. blacklistu. Pokud se jedná o mobilní síť, je zapotřebí kontaktovat přímo svého operátora a požádat o zablokování telefonního čísla útočníka.

3.1.6 Stalking / kyberstalking

Kyberstalking je velmi podobný harassmentu. Oba mají za úkol vyvést oběť z rovnováhy prostřednictvím zpráv, pomluv, nebo prozváněním. Kyberstalker ale ještě navíc oběť neustále pronásleduje. V životě stalker stále sleduje oběť fyzicky, ale stalking v kyber prostoru je do jisté míry jednodušší. Útočník neustále sleduje aktivitu své oběti třeba na sociální síti a dá se říct, že ví o každém jejím kroku, aniž by oběť cokoliv zaregistrovala. Proto je velmi důležité si dobře rozmyslet, co na sociálních sítích sdílet za příspěvky.

3.1.7 Happy slapping

„*Happy slapping se objevil poprvé v roce 2005 v jižním Londýně u tzv. hiphopových „gangsta teenagerů“, jež jsou snadno identifikovatelní podle vytahaného oblečení a imitací zlatých přívěsků na krk. S připravenými kamerami, či mobily vyčkali členové gangu na nic netušící oběť, dospělého i dospívajícího, které podrobí dopředu naplánovanému útoku. Ataky se vyznačují nebývalou zákeřností, která je hnána touhou získat co nejvíce šokující agresivní a „obdivuhodné“ video. Obětí bývá nahodilý i známý člověk, avšak útok je iniciován zcela záměrně a nečekaně, nejčastěji zezadu a ve skupině. Získanou nahrávku umístí na web jako další dobrý úlovek. V Británii, kde je „happy slapping“ nejvíce rozšířen, už díky této zvrácené zábavě zemřelo několik lidí. Nečekanost a rafinovanost se stále stupňuje, nikdo si nemůže být na ulici jistý, že zrovna on nebude terčem. Jsou známé případy, kdy zcela neznámému cyklistovi je pro zábavu o očekávání vtipného pádu vražena větev do špic.*“ [7]

*„Účelem happy slappingu je nečekaně fyzicky napadnout buď mladistvého, nebo dospělého člověka, přičemž komplic agresora celý čin nahrává na mobilní telefon nebo kameru. Získané video poté umístí na Internet (např. YouTube). Video je určeno k tomu, aby pobavilo. Obětí se může stát prakticky kdokoliv – někdo, kdo se jen tak projíždí v parku na kolečkových bruslích nebo běhá, někdo kdo pospíchá na autobus, atd. Ve Velké Británii, kde se termín happy slapping používá nejčastěji, je slovo spojováno s pojmy jako je „**chav**" (urážlivé pojmenování určité skupiny dospívajících v Anglii) nebo „**ned**" (obdoba hooligans).*" [8]

Happy slapping je překládán jako veselé fackování. Z počátku byl považován za nevinnou zábavu a žert. S postupem času ale agresivita útočníků roste a v některých zemích je happy slapping považován za trestný čin.

3.1.8 Sexting

Jedná se o složeninu dvou slov a to „Sex" a „Texting", což znamená v angličtině posílání textových zpráv. Jde tedy o posílání zpráv se sexuálním podtextem, nebo o zprávy doplněné erotickou fotografií, nebo videem.

„Stále více dospívajících pořizuje erotické fotky, ať už sebe nebo i někoho dalšího, natáčejí různá odvážná videa a ty pak mobilním telefonem posílají kamarádům a známým. Takové obrázky často skončí i na Internetu např. na stránkách sociálních sítí nebo na různých portálech pro zveřejňování fotek a odtamtud se dostávají k širokému publiku. Často se lechtivé obrázky posílají nejdřív „jen" v páru nebo nejlepším kamarádům a kamarádkám např. jako důkaz lásky nebo přátelství, někdy jsou takové fotky i formou flirtování. Když se ale vztah nebo kamarádství rozpadne, intimní fotky mohou skončit jako pomsta v mobilech dalších známých nebo se veřejně pověsí na Internet. Někdy se původně důvěrné osobní fotky stanou i prostředkem vydírání." [9]

„Sexting představuje velmi rizikové chování, a to hned z několika důvodů:

1. *Potenciálním útočníkům dáváme k dispozici citlivý materiál, který mohou zneužít proti nám.*

2. *Tento materiál může na internetu kolovat několik let, nebo může být použit za několik let od svého vzniku.*
3. *Oběť sextingu může být vystavena tzv. harašení či sexuálním útokům.*
4. *Šiřitelé sextingu se mohou stát pachateli přestupku či trestného činu (šíření dětské pornografie, ohrožování výchovy dítěte apod.)*“

[10]

Problém může nastat v okamžiku, kdy se takovéto obrázky dostanou na internet. Přestože nemusejí být veřejné, ale může je vidět třeba jen pár přátel, i to stačí. Nikdo si nemůže být stoprocentně jistý, že tyto fotografie proti němu někdo nezneužije třeba i v daleké budoucnosti. Takové snímky pak mohou napáchat závažné škody například v kariéře, nebo i v soukromých vztazích.

Další potíže mohou nastat, pokud si takové zprávy posílají dva nezletilí partneři. Většinou tyto případy nejsou vůbec řešeny, přeci jenom, jedná se o partnery a podle zákonů České republiky je sex nezletilých povolen od patnácti let. Pokud se ale partneři rozejdou a jeden z nich použije tyto fotografie proti druhému, byť je jen třeba ukáže kamarádovi, stávají se oba bývalí partneři pachateli trestného činu. Partner, který ukázal fotografii partnerky někomu jinému, může být obviněn z přechovávání a šíření dětské pornografie a partnerka může být obviněna z trestného činu tvorby a šíření dětské pornografie.

3.1.9 Kybergrooming

Termín kybergroming označuje chování, kdy si útočník vyhlídne na internetu oběť a snaží se o to, aby mu oběť začala důvěřovat tak, aby ji vylákal k osobní schůzce, která má za cíl oběť zneužít.

„*Kybergrooming je druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií. Často je vázán na synchronní i asynchronní komunikační platformy, nejčastěji veřejný chat, internetové seznamky, instant messengery a VoIP (např. ICQ, Skype) a v posledních letech také na sociální sítě (Facebook, Twitter, MySpace, Bebo a další). Internetoví predátoři*

využívají také inzertní portály, na kterých nabízející dětem různé možnosti výdělku či kariéry (např. v oblasti modelingu), často navštěvují portály zaměřené přímo na nezletilé uživatele internetu (dětské portály, portály zaměřené na volnočasové aktivity, herní portály a další internetové stránky).“ [11]

Kybergrooming je největší hrozbou pro děti na internetu, protože útočníci mají za cíl se s obětí vidět a většinou ji i sexuálně zneužít, ať už fyzicky, nebo ke tvorbě fotografií a videí s dětskou pornografií.

„*Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu – od cca 3 měsíců po dobu několika let. Tato doba je přímo závislá na způsobu manipulace a na důvěřivosti oběti. Proces manipulace dítěte prochází čtyřmi základními etapami (příprava kontaktu – kontakt s obětí – příprava na osobní schůzku – osobní schůzka), během kterých může útočník využít velké množství technik a postupů.*“ [11]

Útočník má manipulaci s dítětem rozdělenou do etap:

- **Příprava kontaktu**
- **Falešná identita** – útočník si připravuje identitu pro manipulaci
- **Kontakt s obětí, navázání a prohlubování vztahů**
- **Efekt zrcadlení** – Útočník z oběti získává informace například o zájmech, a pak předstírá, že má stejné zájmy
- **Snaha získat co nejvíce osobních informací o oběti**
- **Profilování oběti**
- **Vábení a uplácení oběti**
- **Snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace**
- **Snahy o izolaci oběti od okolí**
- **Příprava na osobní schůzku**
- **Technika překonávání věkového rozdílu mezi útočníkem a obětí**
- **Vyhrožování a vydírání oběti**
- **Osobní schůzka**

- **Pokračující manipulace**
- **Útok na oběť**

3.2 Stránky s nevhodným obsahem

Asi každý uživatel internetu se někdy setkal se stránkou, která má nevhodný obsah. Na takové stránky se může uživatel internetu dostat velmi rychle a omylem, aniž by je vyhledával. Každý uživatel může mít různé představy o tom, co je nevhodný obsah na internetu, ale vzhledem k dětem by měl být tento obsah velmi jednoznačně definován. Jedná se o stránky s pornografickým obsahem, stránky s násilnými praktikami, stránky propagující rasismus, nebo jiné protisociální cítění, atd.

Před těmito stránkami je zapotřebí děti chránit. Některé děti tyto stránky vyhledávají sami, ať už ze zvědavosti, nebo se o nich doslechly od svých vrstevníků. Server qustodio.com, který nabízí bezplatný program pro zabezpečení internetu, říká, že: „12% všech internetových stránek nabízí pornografii“. [12]

3.2.1 Pornografické stránky

„*Internetová pornografie nabízí návštěvníkům elektronických stránek sexuálně explicitní vyobrazení, videa, texty a tzv. chaty. Mnoho lidí dnes svou sexualitu a vztahy prožívá formou zprostředkované komunikace, jež může zahrnovat i výměnu sexuálně explicitních slov a vyobrazení. Od nástupu celosvětové elektronické sítě a grafických prohlížečů v roce 1995 se produkce a distribuce komerční pornografie formou digitálního obrazu stala populární zábavou dospělých, poskytovanou podnikateli v oblasti e-obchodu. Internetová pornografie je v současnosti nejviditelnějším a nejkontroverznějším projevem pornografie. Od starších forem pornografického zobrazování se liší tím, že uživatelé k tomuto digitalizovanému produktu přistupují prostřednictvím globálních distribučních kanálů internetové sítě. Internetové stránky rovněž zákazníky vybízejí k přímé interakci či poskytování zpětné vazby pornoherečkám/pornohercům formou tzv. chatovacích místností či webových kamer.*“ [13]

Na stránky s touto tématikou je na internetu možné narazit velmi snadno. Stránky je možné vyhledat pomocí nejrůznějších internetových vyhledávačů, ale je možné se na tyto stránky dostat i omylem, prostřednictvím reklamy na různých bannerech umístěných na jiných webových stránkách. „*Pornografie je problémem dnešní společnosti. Snadná dostupnost, nový rozměr, anonymita. Ročně vznikne okolo 6000 filmů, toto odvětví vydělává více než Google, Yahoo a MSN dohromady.*“ [14]

Vzhledem ke snadné dostupnosti těchto stránek je potřeba děti chránit před přístupem na ně. Dříve byl člověk před vstupem na takové stránky varován, že je potřeba být starší osmnácti let, a že se na stránkách nachází pornografický obsah. Uživatel musel potvrdit, že si tuto zprávu přečetl, a že je starší osmnácti let, nebo musel vyplnit datum narození. Poslední dobou už ale tato ochrana na stránkách nebývá, a tudíž se na ně může uživatel dostat jedním kliknutím myši.

3.2.2 Stránky podporující rasismus nebo jiné formy násilí

Stránky, které by jakýmkoliv způsobem podporovaly, nebo oslavovaly rasismus, nebo jiné formy násilí proti určité skupině obyvatelstva, je na internetu zakázáno šířit. Pokud uživatel na internetu tyto stránky najde, je možné je přímo nahlásit Policii ČR prostřednictvím formuláře dostupného na stránkách http://aplikace.policie.cz/hotline/ .

Takový obsah může být nebezpečný obzvláště pro mladší dítě, které ještě nemusí vědět, co je správné a co ne. Může se tedy prostřednictvím těchto stránek dostat k informacím, které nebude umět správně interpretovat, a mohlo by se začít chovat rasově nesnášenlivě, když z toho ještě nemusím mít úplně rozum.

3.3 Sociální sítě

Sociální síť je v současné době asi nejpoužívanějším komunikačním prvkem na internetu hned po e-mailu. „*Pojem „sociální síť“ byl zaveden dlouho před tím, než*

vznikl internet a všechny současné internetové sítě a to již v roce 1954 sociologem z „Manchesterovy školy“ Jamesomem Barnsomem.“ [15]

Sociální sítě jsou fenoménem posledního desetiletí. Slouží ke komunikaci s nejrůznějšími skupinami lidí. Prvotní myšlenka sociálních sítí byla možnost sdílet fotografie a nejrůznější zajímavosti s lidmi ve vašem okolí. Bohužel se ale poslední dobou staly nástroji, které mohou lidem velmi ublížit, pokud s nimi neumí vhodně zacházet.

Na dnešních sociálních sítích si člověk musí dávat pozor na to, kam zabrousí. Provozovatelé sociálních sítí se snaží obsah filtrovat a cenzurovat, ale ne vždy jsou stoprocentně úspěšní. Navíc kromě nevhodného obsahu může člověk narazit i na spoustu virů, spywaru a mallware.

3.3.1 Facebook

Facebook je v současné době nejpoužívanější sociální sítí. Facebook byl poprvé spuštěn v únoru 2004 svým zakladatelem Markem Zuckerbergem a původně sloužil jako sociální síť pro studenty Harvardské univerzity. Postupem času se k síti připojovaly další univerzity nejprve ve Spojených státech amerických a později i z celého světa. První univerzita z České republiky, která byla akreditována k připojení k síti facebook, byla Masarykova univerzita.

11. srpna 2006 došlo ke změně licenčních podmínek facebooku a od tohoto dne se mohl k této síti připojit kdokoliv starší třinácti let. Facebook se postupem času rozrůstal a počet uživatelů stoupal. V říjnu 2012 bylo na facebooku zaregistrováno více než jedna miliarda aktivních uživatelů a jejich počet neustále roste.

Facebook nabízí velkou škálu možností. Dnes už nejde jen o sdílení stavů, fotografií a videí, ale je možné na něm hrát hry, organizovat události, sdružovat si přátele do skupin a mnoho dalších funkcí. Některé základní funkce jsou popsány níže.

Obrázek 1 - Logo sociální sítě facebook

Zdroj: www.facebook.com

Zeď

Zeď je základním stavebním prvkem facebooku. Na zeď si může uživatel sdílet stav, fotografii, nebo video. Na zeď může přidávat příspěvky jak majitel zdi sám, tak také lidé, které má v přátelích. Zeď se může velice snadno stát prostředkem kyberšikany, kdy útočník publikuje na zeď dítěte nevhodné zprávy, nebo obrázky. Takového uživatele je zapotřebí co nejdříve zablokovat.

Zprávy

Tato aplikace funguje v podstatě stejně jako jakýkoliv Instant Messenger. Je možné posílat zprávy lidem, které má uživatel v přátelích, různým skupinám uživatelů, nebo i lidem, které v přátelích nemá, pokud je tato možnost v nastavení povolena. Pokud má uživatel povoleno přijímat zprávy od neznámých uživatelů, vystavuje se riziku zasílání nevhodných zpráv a kyberšikany. Je tudíž velmi žádoucí si dobře rozmyslet, od koho bude uživatel zprávy přijímat a od koho ne.

Události

Pomocí této aplikace lze zvát přátele na akce, které uživatel pořádá, nebo je možné být na nějakou akci pozván. Událost obsahuje základní informace o tom, kdy a kde se koná, je možné zobrazit seznam pozvaných uživatelů, případně je možné zanechat vzkaz na zdi události. V této sekci hrozí, že se dítě může přidat k nevhodné skupině lidí a páchat organizované zločiny či výtržnosti, nebo může být pozváno na nevhodnou schůzku.

Fotografie

Tato aplikace umožňuje uživateli sdílet fotografie a videa. Fotografie je možné třídit do alb tak, aby byly tematicky seskupeny. Na fotografiích je možné označit uživatele, který je na ní vyfotografovaný. Je možné fotografii okomentovat, případně, pokud uživatele někdo označí na fotografii, na které si nepřeje být označen, je možné se z takové fotografie odznačit. Na fotografii se už nebude zobrazovat jméno uživatele a nikdo kromě něj ho nemůže znovu označit.

Skupiny

Facebook umožňuje vytvářet si skupiny třeba mezi spolužáky, spolupracovníky, atd. Skupina má svoji vlastní zeď a příspěvky, které jsou na tuto zeď vloženy, mohou vidět pouze členové skupiny. Skupiny jsou dobré, pokud chce uživatel něco přehledně sdílet s určitým okruhem lidí tak, aby jeho příspěvek nezanikl mezi mořem ostatních příspěvků. Tato aplikace ale bohužel nese rizika, že se dítě stane členem naprosto nevhodné skupiny.

3.3.2 Lidé.cz

Server lide.cz vznikl jako ryze česká sociální síť. Zakladatelem této sociální sítě je společnost Seznam.cz. Tento server má propojenou registraci s dalšími servery této společnosti, jako je Email.cz, Spolužáci.cz, a další.

Základním prvkem tohoto serveru je profil uživatele. Na profil si uživatel může přidat fotografie a videa, napsat základní informace o sobě a přidávat přátele. Profil jako takový je pouze základní funkcí. Kromě profilu jsou na serveru ještě další části a to chat, diskuze, videa a seznamka.

Obrázek 2 - Logo lide.cz

Zdroj: www.lide.cz

Chat

Chat funguje jako klasický online chat. Místnosti jsou rozděleny do osmi tematických okruhů:

- Města a místa
- Seznámení a flirt
- Sex a vše kolem něj
- Hudba
- Pokec a zábava
- Koníčky a zájmy
- Sport
- Ostatní

Po vybrání si z jednoho tematického okruhu se objeví seznam místností, kam je možné vstoupit a zahájit chat. Některé místnosti mohou mít omezený vstup jen pro některé uživatele, nebo je zapotřebí mít na serveru prochatován určitý počet hodin. Po vstupu do místnosti je možné zahájit chat buď se všemi uživateli místnosti, nebo je možné si „šeptat“ jen s určitými uživateli. Sekce Sex a vše kolem něj je striktně omezena pouze pro uživatele starší osmnácti let. Bohužel je pro vstup do této sekce pouze potřeba kliknutím myši potvrdit uživatelovu zletilost. Dítě se tedy do této sekce může dostat velice jednoduše.

Diskuze

Jedná se o klasickou diskuzi, která je rozdělena do základních dvanácti kategorií. Po vybrání si kategorie se objeví další podsložky, ve které je možné si vybrat téma, o kterém chcete diskutovat. Tato diskuze je hlídána administrátory, takže by se nemělo stát, že by na ní dítě přišlo do styku s nevhodnými informacemi, nebo tématy.

Videa

Jedná se o klasický videolog, fungující například na principu serveru youtube.com, nebo stream.cz. Videa přidaná do této sekce jsou kontrolována administrátory, tudíž by se nemělo stát, že se sem dostanou nevhodná videa, která by neměly vidět děti.

Seznamka

Seznamka je aplikace, která umožňuje uživateli podat inzerát na seznámení, nebo inzeráty procházet. Seznamka je rozdělena na pět základních kategorií, a to: Vážná seznámení; Dopisování & přátelé; Tanec; Pojďme, cestujme; Sport. Každá kategorie má pak další podkategorie, ze které si uživatel vybere, které inzeráty chce procházet. Další možností je zvolit si své pohlaví, pohlaví, které hledám, věkový rozsah vyhledávaných partnerů a region, odkud se budou potenciální partneři vyhledávat.

Pro dítě může být nebezpečná sekce vážná seznámení, kde se může třeba za třináctiletou holčičku vydávat pedofil, který se snaží děti vylákat ven, aby je mohl zneužít. Je to velmi rizikové místo, a proto by měli být rodiče obezřetní, jestli se jejich děti nepohybují v této sekci.

3.3.3 Google+

Google+ je sociální síť, kterou provozuje společnost Google. Služba Google+ byla poprvé spuštěna 28. června 2011 pouze na pro několik uživatelů vlastnících účet gmail na základě pozvánek. Počet uživatelů, kterým byla pozvánka zaslána, byl několikrát navýšen až 20. září 2011 byla služba zpřístupněna všem uživatelům.

Obrázek 3 - Logo sociální sítě Google+

Zdroj: http://plus.google.com

Google+ měl na začátku velký potenciál na to, stát se nejvyužívanější sociální sítí na světě, o čemž svědčí i velký nárůst počtu uživatelů v prvních týdnech provozu. Po pár měsících ale zájem o službu upadá, a revoluce v používání sociálních sítí se nekoná.

Google+ je téměř totožný jako facebook, má velmi podobné funkce a strukturu, tudíž na něm hrozí stejná rizika.

3.4 Instant messaging

Instant messaging (IM) je služba využívající internet, která umožňuje uživatelům vidět, kteří přátelé jsou momentálně online, a umožňuje jim napsat zprávu, poslat nějaký soubor, komunikovat prostřednictvím hlasu, nebo videa. IM má oproti e-mailu tu výhodu, že komunikace probíhá v reálném čase, to znamená, že druhá strana dostane odeslanou zprávu téměř okamžitě.

„*Instant messaging zrychluje komunikaci a umožňuje snadnou spolupráci mezi více lidmi. Narozdíl od emailu nebo telefonu druhá strana ví, zda je účastník k dispozici či nikoliv. Většina IM systémů umožňuje nastavit away message, tedy zprávu podle které lze zjistit, zda je uživatel přítomen přímo u svého počítače. Na druhou stranu uživatele nikdo nenutí, aby na zprávy odpovídali ihned. Tímto způsobem se IM komunikace stává méně vyrušující než třeba telefon a to je částečný důvod, proč je tento způsob komunikace stále více oblíben v obchodním prostředí. Instant messaging je ideální pro rychlou výměnu internetových adres, kusů zdrojového kódu a dalších věcí, které se např. v telefonní komunikaci špatně přenášejí.*“ [16]

IM je velice hojně využíván ke kyberšikaně z důvodu anonymity. Pro založení účtu není potřeba vyplňovat téměř žádné údaje, někdy stačí jen e-mailová adresa, která ale není většinou veřejná a ani nemusí být existující. Provozovatelé IM nevyžadují aktivaci prostřednictvím e-mailu.

„*Prostřednictvím IM lze posílat hrubé vzkazy či přílohy. Trýznitelé občas používají IM účet jiné osoby, aby jeho prostřednictvím posílali hrubé nebo oplzlé zprávy lidem ze seznamu přátel oběti.*“ [17].

V současné době díky nástupu a masivnímu rozšíření sociálních sítí dochází k úpadku v používání Instant Messagingu. Přesto se ale stále na internetu najde spousta aktivních uživatelů, kteří IM využívají denně, a proto je potřeba se tímto tématem, jako potenciální hrozbou, zabývat.

3.4.1 ICQ

Název ICQ vznikl z fonetického přepisu anglické věty „I seek you“(hledám tě). Jedná se o software pro IM využívající protokolu OSCAR. Služba byla poprvé spuštěna v listopadu 1996. Od tohoto roku několikrát změnila svého majitele. Protokol ICQ se stal první rozsáhle využívanou službou pro IM na internetu, později si ji nechala firma Mirabilis, která tuto službu vyvinula, patentovat.

Obrázek 4 - Logo ICQ

Zdroj: www.icq.com

Nevýhodou ICQ je velká anonymita a téměř nulová ochrana uživatelů. Každému uživateli je přiděleno unikátní přihlašovací číslo, tzv. UIN (Universal Internet Number / Unified Identification Number). Ostatní údaje, které uživatel zadá při registraci, jako jsou jméno, příjmení, datum narození, přezdívka a e-mail, je možné kdykoliv změnit.

ICQ umožňuje svým uživatelům rozesílat zprávy jejich přátelům, skupinový chat, hlasovou konverzaci a v poslední verzi i videokonverzaci. Dále je možné přátelům odesílat různé soubory z počítače, jako jsou obrázky, videa, atd., nebo je možné hrát pomocí ICQ i hry. Pokud má uživatel na ICQ dobitý kredit, je také možné zasílat sms zprávy na mobilní telefony.

Služba ICQ je také hojně užívána ke spamu, kdy uživateli přijde zpráva od jiného uživatele, nejčastěji z Ruska. V takovéto zprávě bývá většinou odkaz na nějakou internetovou stránku, kde je možnost zakoupit si určitý produkt, nebo je člověk přesměrován na nějakou stránku s virem, anebo pornografickým materiálem. Důrazně je tedy doporučeno ignorovat zprávy od uživatelů, kteří nejsou v seznamu přátel, a obsahují odkaz na nějakou internetovou stránku.

3.4.2 SKYPE

Skype je program pro IM, který pochází z Estonska a jeho tvůrci jsou Niklas Zennström a Janus Friis, kteří jsou také tvůrci programu Kazaa. Základní funkce Skypu jsou shodné s ICQ, to znamená, že je možné chatovat s jedním nebo více přáteli, hrát hry, odesílat si soubory s jinými uživateli, atd. Původní název, o kterém tvůrci uvažovali, byl „Sky peer-to-peer“, který byl následně zkrácen na „Skyper“. Vzhledem k tomu, že v některých státech již byly domény pod názvem skyper zaregistrovány, rozhodli se tvůrci odebrat poslední písmeno z názvu a tak vzniknul název Skype.

Obrázek 5 - Logo Skype

Zdroj: www.skype.com

Výhodou oproti jiným IM je velice propracované a dobře funkční hlasové a video hovory. Toto je pravděpodobně jeden z hlavních důvodů, díky kterým služba Skype nezanikla a je doposud hojně využívána. Skype na rozdíl od ICQ netrpí na

spamy, ale hrozby pro mladé uživatele jsou na něm stejné. Hlavní nevýhodou je anonymita.

4 Praktická část

Tato část bakalářské práce se zabývá způsobem, jak dětem co nejúčinněji zamezit v přístupu na stránky s nevhodným obsahem, nebo na jakékoliv jiné stránky, na které nechtějí jejich rodiče, aby děti přistupovali.

Do porovnání byly vybrány dva freewareové programy, jeden od společnosti Microsoft a druhý od Qustodio. Program od firmy Microsoft byl vybrán z důvodu snadného získání a velké důvěře od většiny lidí k této společnosti. Program od firmy Qustodio byl vybrán na základě toho, že na svých internetových stránkách píšou, že je jejich program nejlepší z volně stažitelných programů.

Aby bylo možné tyto programy využívat, je zapotřebí mít na počítači alespoň dva uživatelské účty. Jeden účet administrátorský, který využívá rodič a je chráněný heslem, a alespoň jeden účet uživatelský, který využívá dítě a heslem chráněný být může, ale nemusí.

4.1 Windows Live Essentials 2012

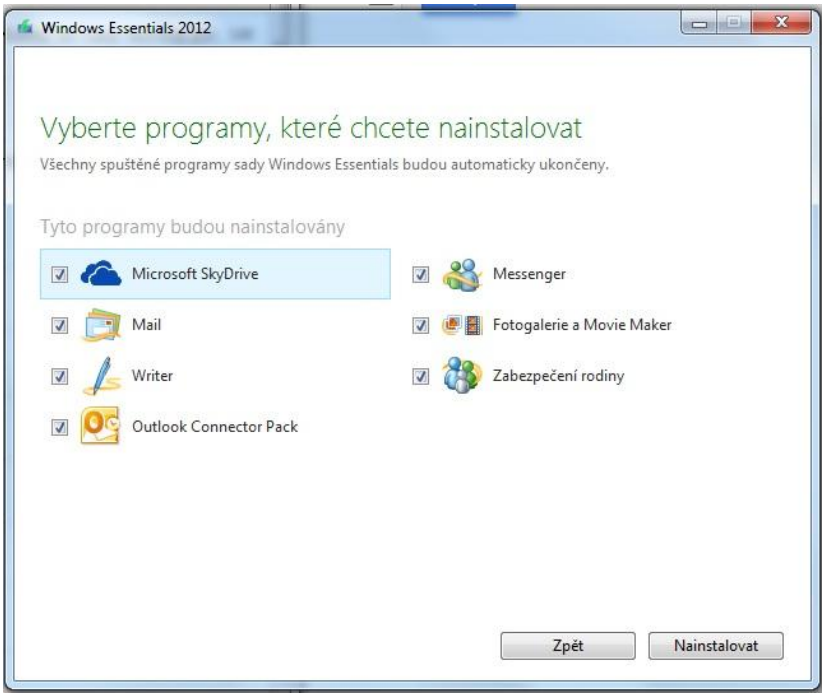
Jedná se o balíček služeb, který byl vydán firmou Microsoft a je zdarma ke stažení pro systém Windows 7 na internetové adrese http://windows.microsoft.com/cs-CZ/windows7/Protecting-your-kids-with-Family-Safety. Tento balíček se skládá ze sedmi programů: Microsoft SkyDrive, Mail, Writer, Outlook Connector Pack, Messenger, Fotogalerie a Movie Maker, Zabezpečení Rodiny. Program Zabezpečení Rodiny je jediný program, který bude pro naše účely používán.

4.1.1 Instalace

Po otevření staženého souboru z webu se instalační program ptá, jestli chce uživatel nainstalovat celý balíček, nebo pouze vybrané programy. Pokud uživatel zvolí

pouze vybrané programy, objeví se nabídka se seznamem programů, které je možné nainstalovat. Tento výběr zobrazuje obrázek 6.

Obrázek 6 - Instalace Windows Essentials 2012



Zdroj: Vlastní práce

Po zvolení příslušných programů, které uživatel potřebuje, probíhá již instalace plně automaticky a není dále vyžadována žádná interakce ze strany uživatele.

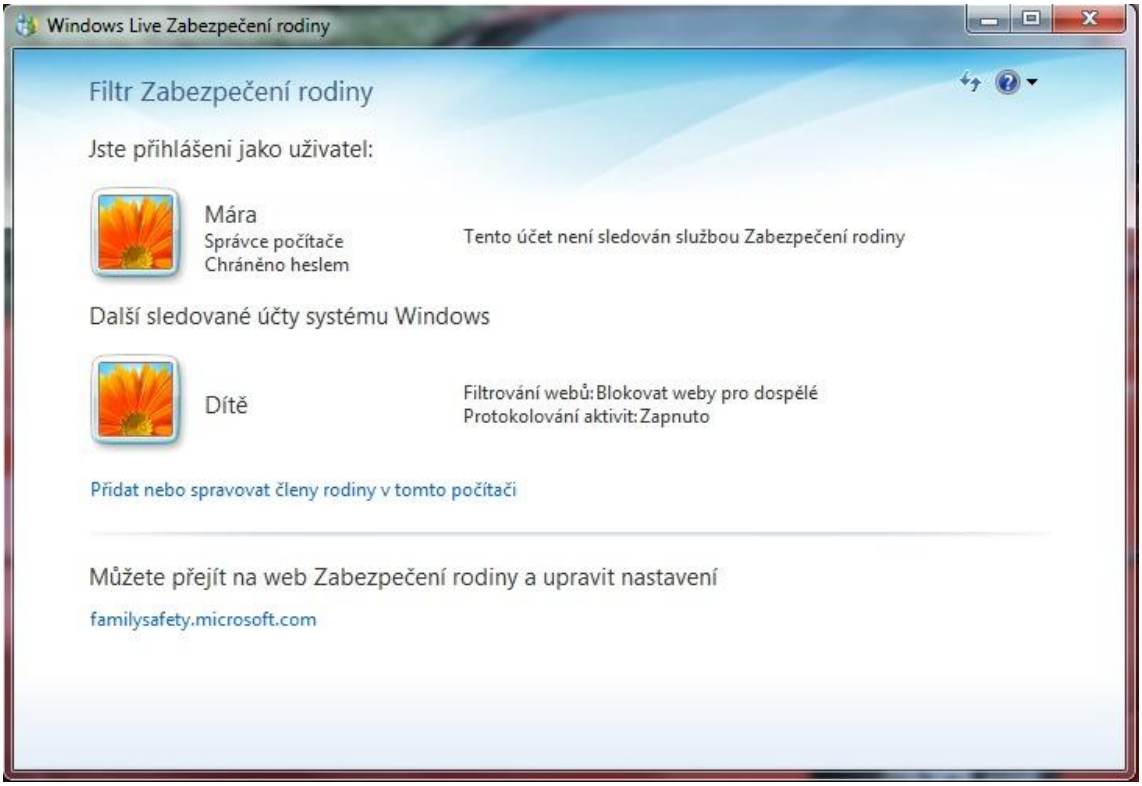
4.1.2 První spuštění služby Zabezpečení rodiny

Při prvotním spuštění služby Zabezpečení rodiny je uživatel vyzván k zadání svého přihlašovacího jména a hesla do služby Windows Live. Pokud uživatel dosud není registrován ve službě Live, je možné registrovat se na internetových stránkách http://home.live.com.

Po zadání uživatelského jména a hesla se objeví uživateli tabulka s účty, které jsou na počítači nainstalovány, pro výběr účtu, který je třeba monitorovat. Je možné zvolit více uživatelských účtů a pro každý nastavit jiná práva, například pro různě staré děti. Po zvolení příslušného účtu je základní nastavení hotovo a uživatel může přejít na

internetovou adresu http://familysafety.microsoft.com, kde je k dispozici nastavení blokace.

Obrázek 7 - Dokončení prvního spuštění služby Zabezpečení rodiny

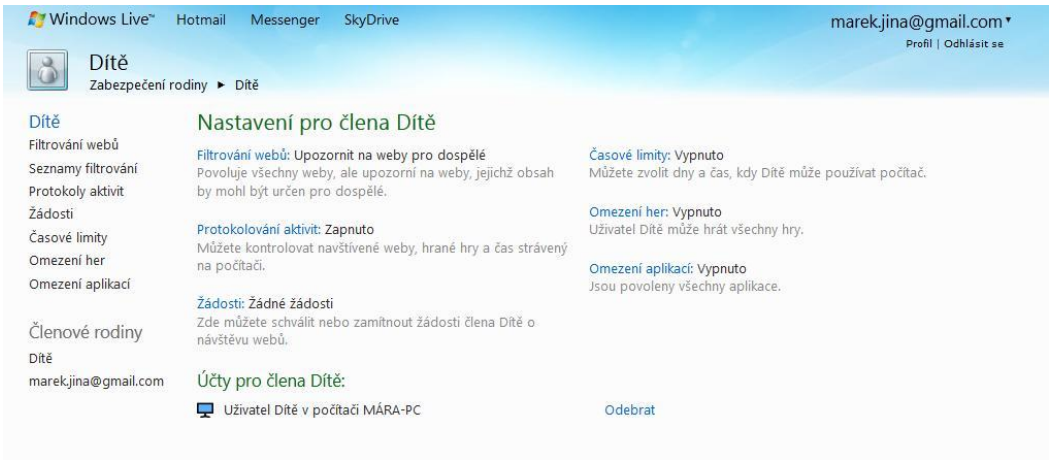


Zdroj: Vlastní práce

4.1.3 Nastavení a používání služby Zabezpečení rodiny

Po přihlášení se na stránku http://familysafety.microsoft.com se uživateli zobrazí možnosti nastavení blokace počítače pro daného uživatele. Toto nastavení je rozděleno do sedmi základních kategorií, podle toho, jaké jsou možnosti uživatele v dané sekci. Úvodní stránka po přihlášení je zobrazena na obrázku 8.

Obrázek 8 - Úvodní stránka nastavení služby Zabezpečení rodiny

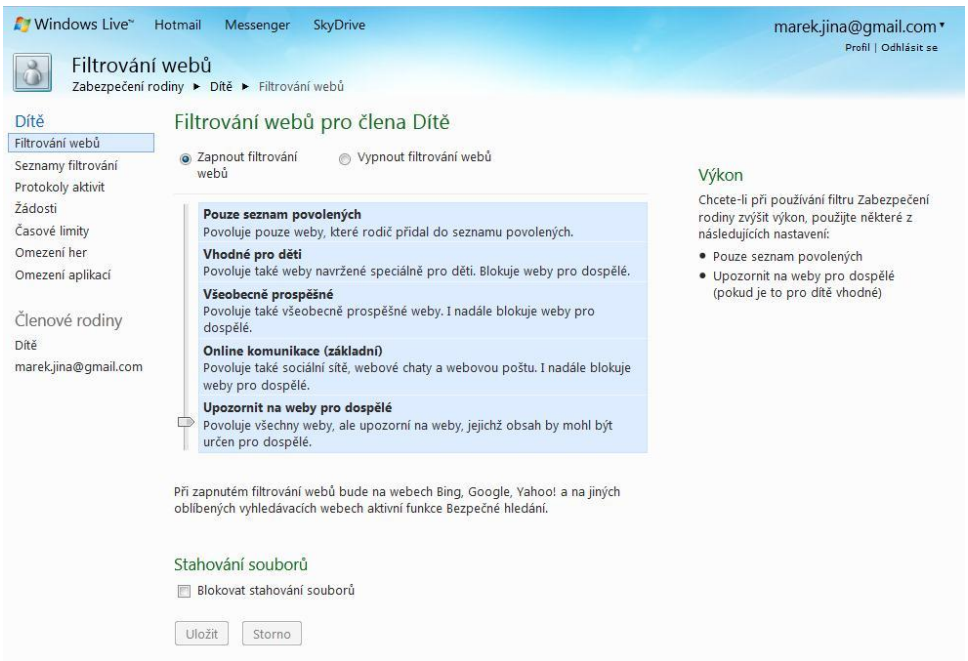


Zdroj: Vlastní práce

Filtrování webů

V této sekci si může uživatel nastavit, zda chce blokovat webové stránky pro své dítě, a pokud ano, je možné specifikovat kritéria blokace. Další možnost, kterou lze nastavit v této sekci, je zákaz stahování souborů z internetu. V nastavení blokování webů si může uživatel vybrat z pěti možností. Možnosti blokace jsou vyobrazeny na obrázku 9.

Obrázek 9 - Blokování webů



Zdroj: Vlastní práce

- **Upozornit na weby pro dospělé:**

Toto nastavení nechává dítěti víceméně volnou ruku v přístupu na internetové stránky. Pokud je stránka, na kterou se chce dítě podívat, vyhodnocena jako stránka pro dospělé, objeví se upozorňovací stránka s textem „Váš rodič pravděpodobně nechce, abyste navštívili tento web“ a dvěma možnostmi. Dítě může buď na stránku vstoupit, nebo se vrátit zpět. Pokud se dítě rozhodne na stránku vstoupit, stránka je automaticky přidána do seznamu povolených webů.

- **Online komunikace (základní)**

Toto nastavení umožňuje prohlížení jakýchkoliv webů, kromě těch, které byly společností Microsoft vyhodnoceny, jako weby pro dospělé. Pokud se dítě na takovýto web pokusí vstoupit, objeví se upozorňovací stránka s textem „Tato stránka je blokována“. Pokud si dítě myslí, že tato stránka by neměla být blokována, je možnost přes tlačítko požádat rodiče o odblokování stránky. Další výhodou tohoto nastavení je, že vyhledávací stránka google.com je přepnuta do režimu bezpečného vyhledávání, který znemožňuje vyhledávat stránky a obrázky s tématy pro dospělé.

- **Všeobecně prospěšné**

Oproti předchozímu nastavení jsou navíc blokovány sociální sítě (facebook, Google+) a stránky pro chat a IM (icq.com, meebo.com). Bohužel databáze umí u českých stránek rozlišit pouze to, zdali se jedná o stránky pro dospělé, či nikoliv. Nejsou tudíž zablokovány české chatovací portály a sociální síť lide.cz. Pokud chce rodič tyto stránky zablokovat, musí je ručně přidat do seznamu blokovaných stránek. Pokud dítě narazí na stránku, která by podle něj neměla být blokována, může opět pomocí tlačítka požádat rodiče o odblokování takové stránky.

- **Vhodné pro děti**

Toto nastavení umožňuje zobrazit pouze webové stránky, které byly společností Microsoft schváleny, jako stránky pro děti. Pro ČR nemá Microsoft databázi těchto stránek vytvořenou, tudíž pokud není stránka na seznamu povolených webových stránek, nezobrazí se. Seznam povolených webových stránek firmou Microsoft je možné zobrazit po kliknutí na příslušný odkaz na stránce s blokovací hláškou.

- **Pouze seznam povolených**

Při tomto nastavení je možné dítětem otevřít pouze ty stránky, které rodič předem přidal do seznamu povolených stránek. Při pokusu o přístup na jiné stránky se objeví blokovací hláška, s možností požádání rodiče o přístup na příslušnou stránku.

Seznamy filtrování

Tato sekce umožňuje rodiči zadání webových stránek, na které má mít dítě přístup i proti pravidlu nastavení v sekci Filtorvání webů, a také umožňuje zablokovat stránky, na které by Filtr webů dítě pustil.

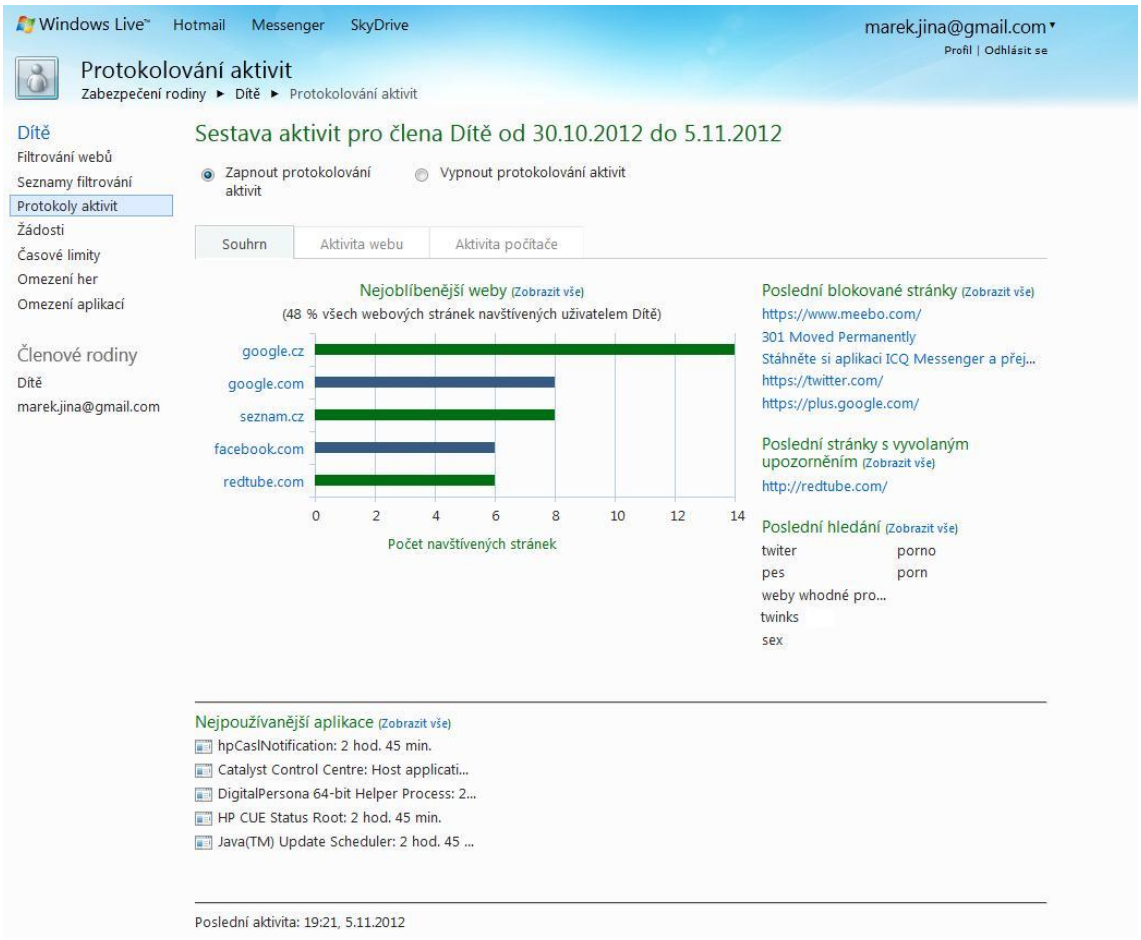
Protokoly aktivit

V této části vidí rodič, co přesně jeho dítě kdy na počítači dělalo, které stránky navštěvovalo, atd., pokud má tuto funkci aktivovanou. V záložce souhrn je vidět, na které weby chodí dítě nejčastěji, poslední blokované stránky, poslední stránky s vyvolaným upozorněním, poslední věci, které dítě na webu hledalo pomocí nějakého search enginu, a nejpoužívanější aplikace. Úvodní stránka protokolu aktivit je zobrazena na obrázku 10.

Další záložkou je aktivita webu, kde rodič vidí, které stránky dítě navštívilo a kolikrát, a také jestli bylo dítě na základě filtru na danou stránku puštěno, nebo mu byl přístup odepřen.

Poslední záložkou je aktivita počítače, kde rodič vidí informace o tom, jak dlouho bylo dítě přihlášené na počítači za určité období, jaké aplikace dítě na počítači používá, jaké soubory stahuje a jaké hry hraje.

Obrázek 10 - Protokol aktivit



Zdroj: Vlastní práce

Žádosti

V této sekci vidí rodič žádosti o povolení webových stránek, které dítěti nebyly zobrazeny v závislosti na filtru, a dítě požádalo o jejich povolení. Rodič může žádost o povolení buď přijmout, nebo odmítnout. Pokud se rodič nepřihlásí do aplikace a nepotvrdí žádosti, je mu jednou za týden odeslán e-mail, se žádostí o povolení stránek.

Časové limity

Rodič si zde může nastavit přesnou dobu, kdy jeho dítě může využívat počítač. Nastavení je zde rozděleno po jednotlivých dnech v týdnu a každý den je rozdělen po půl hodinách. Pokud se dítě pokusí přihlásit v okamžiku, kdy to nemá od rodiče povolené, objeví se mu pouze hláška, že účet je časově blokován a přihlášení se nezdaří.

Tuto ochranu je ale možné obejít přenastavením systémového času přímo v BIOSu. Pokud by chtěl rodič tuto funkci používat, je doporučeno nastavit si v BIOSu heslo.

Omezení her

Uživatel má v této části možnost nastavit dítěti blokaci her. Jsou zde dvě kritéria, podle kterých je možné hry blokovat. Hry je možné blokovat buď podle věkového určení, podle systému hodnocení PEGI, nebo je možné blokovat hry, podle seznamu her, které jsou v počítači nainstalovány.

Omezení aplikací

Poslední oddíl umožňuje rodičům zablokovat jakoukoliv aplikaci, která je v počítači nainstalována. Toto je vhodné, například pokud rodič nechce, aby jeho dítě používalo IM klienty. Pokud jsou v seznamu nainstalovaných programů, může je jednoduše zablokovat.

4.1.4 Zhodnocení služby Zabezpečení rodiny

Instalace programu Microsoft Live Essentials 2012 a její součásti Zabezpečení rodiny je velmi jednoduché. Následné nastavení je velmi intuitivní, ale pro uživatele, který nemá velké zkušenosti s ovládáním PC, může být z počátku obtížné. Po několika minutách a detailním seznámením se s ovládáním programu již každý uživatel musí být schopen základního nastavení programu.

Nastavení a omezení programu je velmi účinné a během testování nedošlo k žádnému pochybení ze strany programu. Filtrování webových stránek probíhalo naprosto v souladu s nastavením a nepodařilo se přijít na žádný jednoduchý způsob, jak tuto ochranu obejít. Pokud bude ale dítě trošku zběhlejší v IT, způsob, jak obejít tento program najde. Během testování byly nalezeny 3 způsoby, jak program obejít tak, aby stránky nebyly filtrovány a nebyla logována moje aktivita. První způsob je nabootování počítače z vyměnitelného média (v tomto případě bylo použito live CD s Linuxem, verzi knoppix). Druhým způsobem je spuštění počítače v nouzovém režimu. Program je

v nouzovém režimu neaktivní. Třetí způsob je rozlomení administrátorského hesla do Windows (na internetu je k dispozici spousta programů, které to umí). Jediná potíž, která nastala, byla, že sociální síť lide.cz nebyla zavedena v seznamu sociálních sítí, avšak tento problém lze vyřešit blokováním této stránky ručně.

Výhody:

+ Snadná dostupnost
+ Možnost ovládání nastavení z jakéhokoliv počítače
+ Vysoká účinnost

Nevýhody:

– Složitější nastavení
– Neexistence databáze stránek vhodných pro děti v češtině
– Nutnost registrace ve službě Microsoft Live

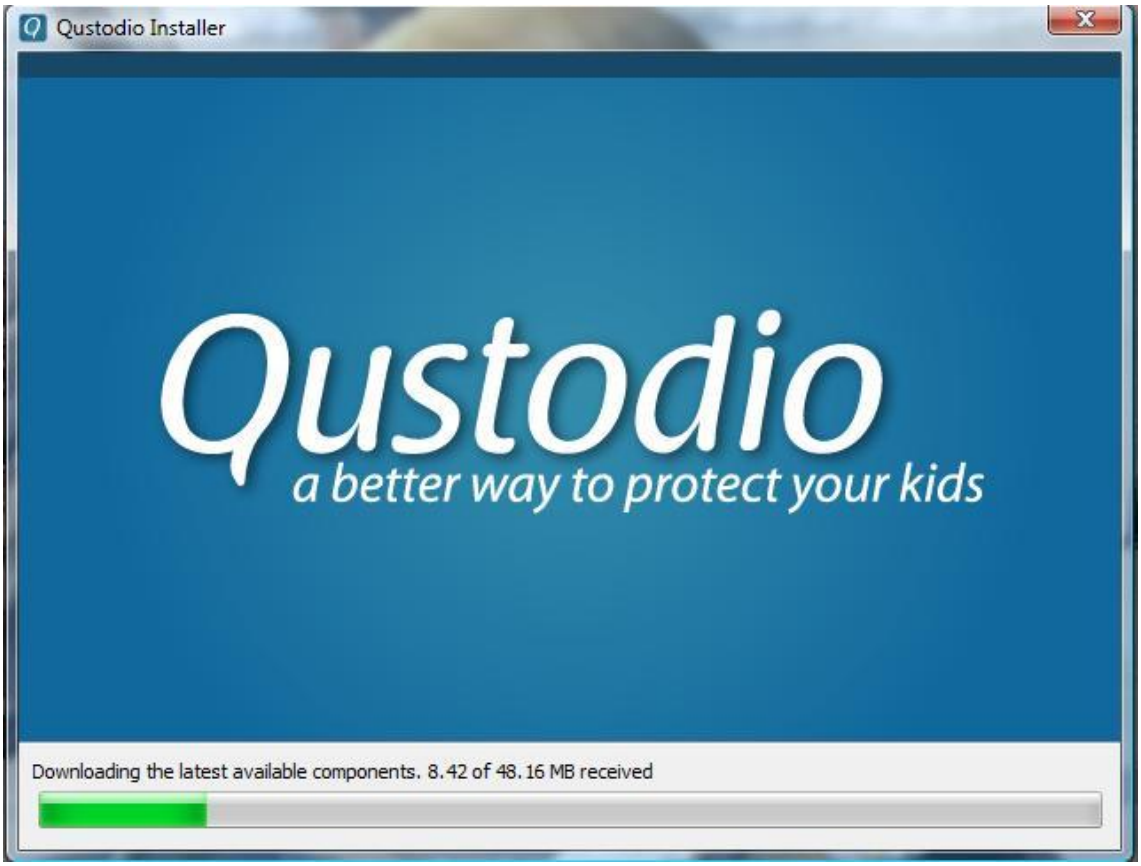
4.2 Qustodio

Firma Qustodio píše na svých internetových stránkách, že jejich software, který je volně dostupný, je nejlepší pro zabezpečení internetu. Tento program je volně ke stažení na internetových stránkách http://www.qustodio.com.

4.2.1 Instalace aplikace Qustodio

Instalace produktu Qustodio je velmi jednoduchá a není nutná téměř žádná interakce uživatele. Instalační program po stažení a spuštění kontroluje na internetu dostupnost nejnovější verze programu a stahuje si aktualizace. Po stažení nejnovější dostupné verze již začne plně automatická instalace. Aktualizaci před instalací zobrazuje obrázek 11.

Obrázek 11 - Stahování nejnovější aktualizace programu Qustodio



Zdroj: Vlastní práce

Po proběhnutí instalace je uživatel dotázán, jestli již má Qustodio účet. Pokud ano, je požádán o registrační e-mailovou adresu a heslo, pokud účet nemá, je nutná registrace. K registraci stačí vyplnit jméno a příjmení, registrační e-mailovou adresu a heslo. Po úspěšné registraci je odeslán na zadanou adresu e-mail, který je nutné potvrdit pro plnou funkčnost programu.

Dalším krokem potřebným k dokončení instalace je zadání počtu dětí, které počítač využívají. Po vyplnění počtu dětí se uživatel dostane na obrazovku, ve které nastavuje rok narození dítěte, jeho pohlaví a ikonku kontaktu. Základní nastavení dítěte je zobrazeno na obrázku 12. Podle roku narození se nastaví základní pravidla pro přístup na internetové stránky, podle kategorií. Po výběru dítěte je zapotřebí dítě spárovat s profilem, pomocí kterého se do počítače přihlašuje. Tímto je instalace kompletní.

Obrázek 12 - Nastavení dítěte

Zdroj: Vlastní práce

4.2.2 Nastavení a používání služby Qustodio

Nastavení programu Qustodio probíhá online přímo pomocí webových stránek http://family.qustodio.com. Po přihlášení se pomocí e-mailu a hesla se rodiči objeví výpis posledních aktivit jeho dítěte na počítači v časovém přehledu.

Ovládací panel aplikace je rozdělen do tří hlavních kategorií, a to: Activity Summary; Activity Timeline; Rules & Settings.

Activity Summary

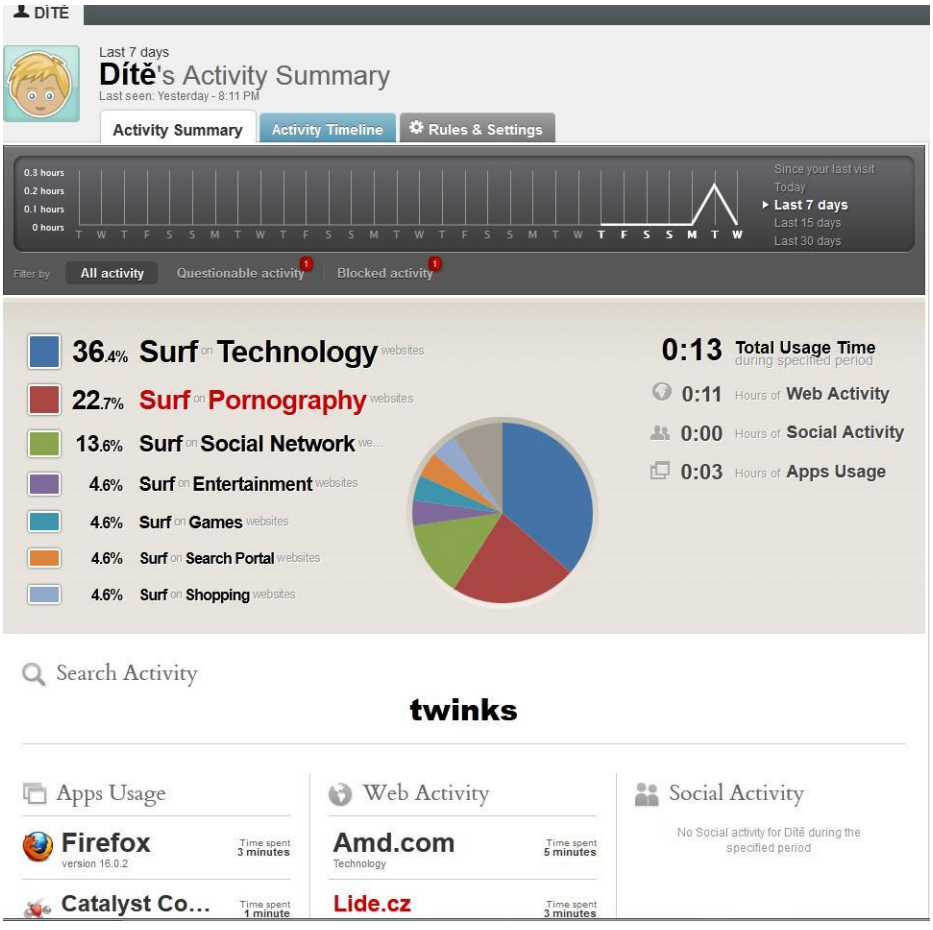
V této záložce může rodič vidět veškerou aktivitu jeho potomka na monitorovaném účtu. V horní liště je vidět graf používání počítače a rodič si může

zvolit, jestli chce zobrazit aktivitu od jeho poslední návštěvy, za dnešek, za posledních 7 dní, za posledních patnáct dní, nebo za posledních 30 dní. Výpis aktivit je vyobrazen na obrázku 13.

Po rozkliknutí příslušného časového období se objeví koláčový graf rozdělený procentuálně podle kategorie, do kterých spadají navštívené internetové stránky. Vedle grafu se objeví časový výpis, jakou dobu strávilo dítě na PC, kolik času z této doby strávilo na internetu, sociálních aktivitách a v různých aplikacích. Výpis je možné filtrovat pro všechny aktivity, diskutovatelné aktivity a blokované aktivity.

Pod grafem je dále výpis vyhledávaných položek v search enginu například na stránkách google.com, výpis použitých aplikací, výpis navštívených internetových stránek, a výpis sociálních aktivit.

Obrázek 13 - Výpis aktivit



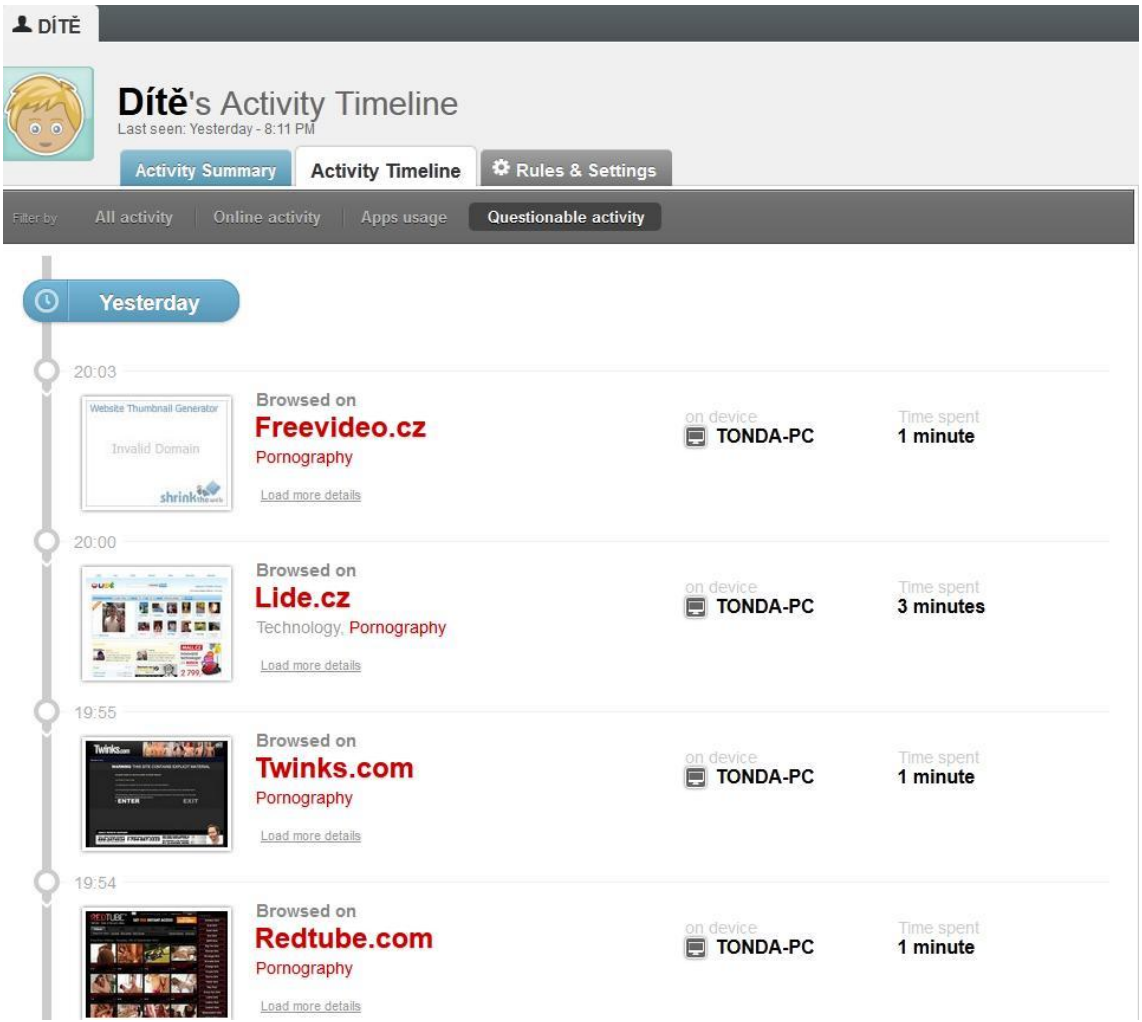
Zdroj: Vlastní práce

Activity timeline

Tato položka umožňuje výpis aktivit sledovaného potomka v časovém sledu od nejnovější po nejstarší. Jsou zaznamenány veškeré návštěvy internetových stránek a spuštění veškerých programů. U každé aktivity je doba, jak dlouho na dané stránce dítě surfovalo a na jakém sledovaném zařízení to bylo. Ukázka výpisu v časovém sledu je na obrázku 14.

Aktivity je možné filtrovat podle druhu, a to na všechny aktivity, aktivity prováděné online, použité aplikace a diskutovatelné aktivity. U každé aktivity webových stránek je možné načíst informace o tom, které podstránky dítě navštívilo.

Obrázek 14 - Výpis aktivit seřazený podle času



Zdroj: Vlastní práce

Rules & Settings

V této sekci se nachází veškeré možnosti nastavení programu Qustodio. Nastavení je rozděleno do dvou hlavních kategorií a to Web Browsing Rules, kde uživatel nastavuje pravidla přístupu na internetové stránky, a Time Usage Limits, kde je možné nastavit, kdy může dítě počítač používat, a kdy ne.

Web Browsing Rules

V této sekci se nastavují pravidla přístupu na internetové stránky. Aplikace Qustodio umožňuje filtraci internetových stránek buď zapnout, nebo vypnout. Pokud uživatel zapne filtraci, objeví se rozdělení internetových stránek do základních dvaceti devíti kategorií. Rodič si může u každé z těchto kategorií zvolit, zdali chce kategorii svému dítěti povolit, zablokovat, nebo ji může povolit s tím, že pokud se jeho potomek dostane na stránky s touto kategorií, je mu odesláno o tom upozornění. Výpis kategorií je zobrazen na obrázku 15.

Další nastavovací možností jsou nekategorizované stránky, kdy uživatel může zvolit, jestli svému potomkovi povolí zobrazování internetových stránek, které nejsou zařazeny do žádné z výše uvedených kategorií.

Dále je možné nastavit stránky s výjimkou, které se zobrazují, nebo jsou zakázány i přes kategorizační pravidla. Poslední možností je zapnutí bezpečného vyhledávání, které znemožňuje v hlavních search enginech, jako je google.com, nebo yahoo.com, vyhledávat stránky s obsahem pro dospělé.

Obrázek 15 - Kategorizace internetových stránek

Zdroj: Vlastní práce

Time Usage Limits

Tato funkce umožňuje rodiči nastavení počítače tak, aby jej nemohl jeho potomek používat v okamžiku, kdy to nemá dovoleno. Nastavení je možné provést pro každý den jiné tak, jak nejlépe rodiči vyhovuje. Nastavení se provádí po celých hodinách.

Další možností omezení používání počítače je časové omezení. Uživatel může použít jiné nastavení pro všední den a jiné pro víkendový den. Nastaví si zde přesný čas, který má jeho potomek dovoleno strávit na počítači, například 3 hodiny za den pro všední den a 5 hodin pro víkend.

Posledním nastavením je způsob znemožnění použití počítače. Rodič má možnost zakázat dítěti používání internetu, nebo celého počítače. Dále se může nechat upozornit, pokud dítě tento povolený čas překročí.

4.2.3 Zhodnocení aplikace Qustodio

Instalace aplikace Qustodio je velmi jednoduché a zvládne ho každý i méně schopný uživatel PC. Nevýhodou této aplikace je, že je pouze v anglickém jazyce,

z tohoto důvodu nemusí vyhovovat všem. Filtrování stránek probíhá naprosto spolehlivě a během testů se mi nepodařilo dostat na žádnou stránku, kterou zakazovala pravidla.

Oproti aplikaci Zabezpečení rodiny od firmy Microsoft existuje ještě jeden způsob, jak aplikaci obejít. Pomocí příkazového řádku je možné vypsat si všechny běžící procesy pomocí příkazu tasklist. Následně už si stačí jen najít PID procesu s názvem QAppTray a následně proces ukončit příkazem taskkill –PID číslo_procesu. Program se tímto deaktivoval a bylo možné procházet web bez omezení a bez monitorování.

Velkou potíží při testování programu ale bylo to, že druhý den přestal program filtrovat a monitorovat aktivitu na zabezpečeném účtu. Myslel jsem si, že došlo k poškození programu v PC, ale ani odinstalace, vyčištění registrů a opětovná instalace nepomohla. Zkoušel jsem aplikaci nainstalovat i na dalším počítači, ale na něm opět nefungovala. Předpokládám, že buď došlo k nějaké blokaci mého účtu na serveru Qustodio, nebo měla online aplikace, která nastavuje pravidla, výpadek. Aplikace nebyla funkční do konce testů. Qustodio má na svých internetových stránkách formulář pro hlášení výpadků aplikace, ale odpověď na důvod nefunkčnosti aplikace se mi nedostala ani po jednom týdnu od nahlášení potíží a dvou urgencích.

Výhody:

+ Vysoká účinnost
+ Možnost ovládání nastavení z jakéhokoliv počítače

Nevýhody:

– Program je dostupný pouze v angličtině
– Výpadek programu během druhého dne testování
– Nutnost registrace u společnosti Qustodio

5 Závěr práce

V praktické části této práce byly testovány dva programy, a to Zabezpečení rodiny, které je součástí balíčku Windows Live Essentials 2012 a Qustodio. Tato část zhodnocuje oba testované programy a porovnává je mezi sebou.

Základní jednotlivá testovaná kritéria jsou sepsána v následující tabulce. Každému programu byla udělena známka jako ve škole 1 – nejlepší, 5 – nejhorší. Výsledná známka je průměrem dílčích známek.

Tabulka 2 – Hodnocení testovaných aplikací

Hodnocené kritérium	Aplikace		Info
	Zabezpečení rodiny	Qustodio	
Instalace	1	1	
Základní nastavení	3	2	
Srozumitelnost	2	4	Qustodio - Pouze AJ
Účinnost filtrů	1	1	
Spolehlivost	1	5	Qus. - Přestal fungovat
Zabezpečení obejití programu	2	3	
Protokolování aktivit	2	1	
Časové limity	1	2	
Kategorizace stránek	2	1	
Omezení aplikací	1	5	Qustodio - Neexistuje
Omezení her	1	5	Qustodio - Neexistuje
Výsledná známka	**1,55**	**2,73**	

Zdroj: vlastní práce

Významy jednotlivých hodnocených kritérií:

- **Instalace** – Známka je udělena za obtížnost instalace
- **Základní nastavení** – Známka je udělena za složitost základního nastavení programu vzhledem k možnosti menší počítačové gramotnosti uživatele
- **Srozumitelnost** – Známka je udělena za srozumitelnost jednotlivých nastavovacích prvků. Program Qustodio má známku sníženou za absenci českého jazyka.

- **Účinnost filtrů** – Známka je udělena za účinnost ochrany dítěte vzhledem k nastaveným filtrům.
- **Spolehlivost –** Známka je udělena za spolehlivost programu jako celku. Program Qustodio dostal nedostatečnou z toho důvodu, že přestal fungovat již druhý den po instalaci a firma nebyla schopna odpovědět na dotaz, proč se tak stalo a problém vyřešit.
- **Zabezpečení obejití programu** – Známka je udělena za ochranu proti prolomení programu
- **Protokolování aktivit –** Známka je udělena za přehlednost a grafické zpracování výpisu činností dítěte na webu a PC
- **Časové limity –** Známka je udělena za možnost časového omezení práce dítěte na PC
- **Kategorizace stránek** – Známka je udělena za správnou kategorizaci internetových stránek vzhledem k nastavení filtru
- **Omezení aplikací –** Známka je udělena za možnost omezení používání některých aplikací na PC. Qustodio tuto funkci nemá
- **Omezení her –** Známka je udělena za možnost omezení používání některých her na PC. Qustodio tuto funkci nemá

Během testování obou programů nebyla zjištěna žádná nesrovnalost proti požadovanému chování. Filtrování stránek a následné protokolování probíhalo u obou aplikací přesně podle aktuálního nastavení a nebyla zjištěna žádná slabina filtrů. Filtry bezchybně reagovaly i na pokusy o jejich obejití pomocí různých proxyserverů a anonymizérů. Ani jeden pokus o prolomení filtrů nebyl úspěšný.

Dalším klíčovým testem byla možnost úplného vyřazení programů z činnosti. Obě aplikace dle očekávání nefungovaly v nouzovém režimu, a dítě by tak mohlo procházet internet bez omezení a protokolování. Další možností vyhnutí se filtrům je spuštění jiného operačního systému z přenosného média, tomu ovšem může rodič zabránit nastavením v BIOSu a následným zaheslováním BIOSu. Tímto nastavením

BIOSu je snížena i možnost prolomení administrátorského hesla. Program Qustodio je ale možné vyřadit z provozu i pomocí příkazového řádku příkazem taskkill.

Co se týká spolehlivosti, nebyla v testovaném období odhalena žádná pochybnost ze strany aplikace Zabezpečení rodiny. Program Qustodio ale druhý den přestal úplně filtrovat síťovou komunikaci i protokolovat aktivitu. Nepomohlo přeinstalování ani instalace na jiné PC. Mohlo dojít k výpadku služby ze strany poskytovatele, nebo jakéhosi zablokování testovaného účtu, když k blokaci nebyl žádný zjevný důvod. Díky této skutečnosti aplikace Qustodio byla v tomto testu ohodnocena známkou nedostatečně.

Dle testovaných kritérií byla výsledná známka lepší u aplikace společnosti Microsoft. Qustodio na svých internetových stránkách uvádí, že jejich software je nejlepší z volně dostupných, což podle tohoto testu není. Pravděpodobně měla firma Qustodio jiná kritéria pro testování.

6 Citovaná literatura

1. Co je kyberšikana? In: *e-bezpečí* [online]. 22. 5. 2009 [cit. 2012-10-20]. Dostupné z: http://cms.e-bezpeci.cz/content/view/14/39/lang,czech/
2. KOLÁŘ, M. *Specifický program proti šikanování a násilí ve školách a školských zařízeních*. Praha: MŠMT ČR, 2003.
3. KREJČÍ, M. V. *Kyberšikana - Kybernetická Šikana*. Olomouc: 2010. ISBN 978-80-254-7791-5.
4. Kyberšikana. In: *Betpečně online* [online]. 2011 [cit. 2012-10-29]. Dostupné z: http://www.bezpecne-online.cz/pro-ucitele-a-rodice/teenageri-a-komunikace-na-internetu/kybersikana
5. Zákon č. 40/2009 Sb. trestní zákoník. In: *Trestní zákoník České Republiky* [online]. 1. 1. 2010 [cit. 2012-10-29]. Dostupné z: http://business.center.cz/business/pravo/zakony/trestni-zakonik/
6. KOHOUTEK, R. Pojem flaming v internetu. In: *slovnik-cizich-slov.abz.cz* [online]. [cit. 2012-10-24]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/slovo/flaming-v-internetu
7. Happy slapping (spokojené fackování). In: *nebudobet.cz* [online]. 2012 [cit. 2012-10-29]. Dostupné z: http://www.nebudobet.cz/?page=happy-slapping
8. Happy slapping. In: *e-bezpečí* [online]. 15. 11. 2008 [cit. 2012-10-29]. Dostupné z: http://cms.e-bezpeci.cz/content/view/71/39/lang,czech/
9. Sexting a Kybergrooming. In: *Safer internet* [online]. 2012 [cit. 2012-10-29]. Dostupné z: http://www.saferinternet.cz/pro-rodice/sexting-kybergrooming
10. Co je sexting. In: *sexting.cz* [online]. 2012 [cit. 2012-29-10]. Dostupné z: www.sexting.cz
11. KOPECKÝ, K. a V. KREJČÍ. *Rizika virtuální komunikace*. NET UNIVERSITY, s.r.o. 15. 12. 2010. 978-80-254-7866-O.
12. In: *qustodio.com* [online]. [cit. 2012-11-01]. Dostupné z: http://www.qustodio.com/
13. JACOBS, K. Pornografie na internetu. In: *ATLAS TRANSFORMACE* [online]. [cit. 2012-11-01]. Dostupné z: http://www.monumenttotransformation.org/atlas-transformace/html/p/pornografie/1-pornografie-na-internetu.html

14. Webové stránky, které se zabývají problematikou pornografie. In: *4youth.cz* [online]. [cit. 2012-11-01]. Dostupné z: http://www.4youth.cz/odkazy/66-problematika-pornografie.html
15. Historie sociálních sítí. In: *socialnisite.cz* [online]. 25. 11. 2008 [cit. 2012-10-20]. Dostupné z: http://socialnisite.cz/info/historie_socialnich_siti
16. Komunikace po internetu (Instant Messaging). In: *NovyMalin.net* [online]. [cit. 2012-11-03]. Dostupné z: http://www.novymalin.net/clanky/komunikace-po-internetu-instant-messaging.html
17. Jakou technologi trýznitel používá. In: *teachtoday* [online]. [cit. 2012-11-03]. Dostupné z: http://cs.teachtoday.eu/cs/Current-Issues/Cyberbullying/How-technology-is-used-to-bully.aspx

7 Seznam obrázků

Obrázek 1 - Logo sociální sítě facebook 19
Obrázek 2 - Logo lide.cz 20
Obrázek 3 - Logo sociální sítě Google+ 22
Obrázek 4 - Logo ICQ 24
Obrázek 5 - Logo Skype 25
Obrázek 6 - Instalace Windows Essentials 2012 28
Obrázek 7 - Dokončení prvního spuštění služby Zabezpečení rodiny 29
Obrázek 8 - Úvodní stránka nastavení služby Zabezpečení rodiny 30
Obrázek 9 - Blokování webů 30
Obrázek 10 - Protokol aktivit 33
Obrázek 11 - Stahování nejnovější aktualizace programu Qustodio 36
Obrázek 12 - Nastavení dítěte 37
Obrázek 13 - Výpis aktivit 38
Obrázek 14 - Výpis aktivit seřazený podle času 39
Obrázek 15 - Kategorizace internetových stránek 41

8 Seznam tabulek

Tabulka 1 – Trestní sazby některých paragrafů, podle kterých by se dala posuzovat kyberšikana 9
Tabulka 2 – Hodnocení testovaných aplikací 43