Pedagogická fakulta
Faculty of Education
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích

Pedagogická fakulta

Katedra informatiky

Bakalářská práce

Kompetence studentů učitelství v digitální bezpečnosti

Vypracoval: Jakub Sadil

Vedoucí práce: Mgr. Václav Šimandl

Rok obhajoby: 2013

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta pedagogická
Akademický rok: **2011/2012**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jakub SADIL**
Osobní číslo:	**P10363**
Studijní program:	**B7507 Specializace v pedagogice**
Studijní obor:	**Informační technologie ve vzdělávání**
Název tématu:	**Kompetence studentů učitelství v oblasti digitální bezpečnosti**
Zadávající katedra:	**Katedra informatiky**

Zásady pro vypracování:

Student připraví dotazník, který se bude zaměřovat na znalosti, dovednosti a postoje budoucích učitelů v oblasti digitální bezpečnosti. Dotazník se tedy bude zabývat tématem ochrany dat (před útoky druhých osob, nechtěnými či náhodnými úniky dat, technickými poruchami i uživatelem samotným), ochranou osobnosti uživatele v prostředí internetu, i intranetu nebo autorským právem. Dále se student pokusí odhalit a prozkoumat důvody vedoucí k dodržování či nedodržování základních bezpečnostních pravidel v prostředí internetu a intranetu.

Dotazník bude obsahovat vědomostní, postojové a situační otázky, týkající se základních i pokročilých preventivních bezpečnostních opatření. Na základě sestaveného dotazníku student zorganizuje dotazníkové šetření, jehož respondenty se stanou nejen budoucí učitelé ICT, ale také budoucí učitelé ostatních předmětů (přírodovědných i humanitních). Výsledky získané v dotazníkovém šetření budou statisticky zpracovány.

V teoretické části práce se student zaměří na vymezení jednotlivých oblastí problematiky digitální bezpečnosti a to včetně doporučených modelů bezpečného chování. Dále analyzuje chování běžných uživatelů ICT podle českých i zahraničních výzkumů.

Rozsah grafických prací:	CD ROM
Rozsah pracovní zprávy:	40
Forma zpracování bakalářské práce:	tištěná

Seznam odborné literatury:

1. Byron, T. Safer Children in a Digital World: The Report of the Byron Review. UK Department for Children, Schools and Families, 2008. ISBN: 978-1-84775-134-8.
2. Chráska, M. Metody pedagogického výzkumu. Praha: Grada, 2007. ISBN 80-247-1369-4.
3. i-SAFE. SAFE Internet Safety Activities: Reproducible Projects for Teachers and Parents. Jossey-Bass, 2010. ISBN 978-0470539507.
4. Král, M. Bezpečnost domácího počítače-prakticky a názorně. Praha: Grada, 2006. ISBN 80-247-1408-6.
5. Lang, M. a kol. Social Networking and Personal Data Security: A Study of Attitudes and Public Awareness in Ireland. In Wan, C. et al. (eds) Proceedings of International Conference on Management of e-Commerce and e-Government (ICMeCG), Nanchang, China, September 16-19. IEEE Computer Society, pp. 486-489, 2009.
6. Sechler, J. A Young Adult's Guide to Safety in the Digital Age. CreateSpace, 2010. ISBN 978-1453618414.

Vedoucí bakalářské práce:	Mgr. Václav Šimandl Katedra informatiky
Datum zadání bakalářské práce:	19. dubna 2012
Termín odevzdání bakalářské práce:	26. dubna 2013

Mgr. Michal Vančura, Ph.D.
děkan

L.S.

doc. PhedDr. Jiří Vaníček, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 12. dubna 2012

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval/a samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury. Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění, souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích 20. dubna 2013

.....

Jakub Sadil

Anotace

K výzkumu a mapování pravidel a standardů v digitální bezpečnosti a shrnutí teoretické části práce jsou zkoumány publikace zabývající se IT bezpečností a dále prováděny konzultace s odborníky v oboru. Ke zmapování současného stavu mezi studenty učitelství je použit dotazníkový průzkum, který nebyl prováděn elektronickou formou, aby bylo dosaženo maximálně přesných dat. Těžištěm mého výzkumu se stává postoj studentů k těmto pravidlům a jejich dodržování a schopnost vštípení těchto pravidel i dalším studentům. Teoretická část práce bude sloužit jako podklad pro další nasbíraná data, a také slouží ke konfrontaci s výsledky dotazníkového průzkumu, a lepšímu pochopení možných následků vyplývajících z různých aspektů chování studentů učitelství. Práce je zaměřena na oblast bezpečnosti v IT, se kterou se nejspíše absolventi učitelských oborů budou setkávat. Dále se zaměřuji na praktické dopady znalosti či neznalosti a dodržování či nedodržování bezpečnostních pravidel a zásad, které jsou popsány v teoretické části, či jsou zmíněny v dotazníku, na schopnost efektivně vykonávat učitelské povolání. Jistá část práce je vyčleněna i sociálním sítím a dopadu jejich používání právě na učitele, jeho žáky a kvalitu vzdělávacího procesu. Ze zjištěných a vypsaných informací je zjištěn a zanalyzován stav uvědomělosti studentů učitelství v digitální bezpečnosti. Vznikla tak práce vhodná pro případné využití na vysokých a středních školách (především pedagogicky zaměřených) či gymnáziích k úpravě metodologie a obsahu výuky určitých částí informatiky.

Abstract

For research and mapping of rules and standarts in IT security and summary od theoretical part of this work, I will use publications which are covering different part sof IT security and i will also consult a experts in this field. For mapping current status among the students, will be used a wide questionary survey, which will not be conducted electronicly, but will be

distributed personally, to ensure that collected datas are relavant and gathered from trustworthy sources. Centerpoint of my research will be attitude of students towards those rules, and their abidance of those rules and also the ability,

to pass those knowledge on the other peoples and especially to other students. The theoretical part of my work, will serve as background for more collected datas and to confront results of questionary survey and better understanding of possible consequences resulting from ignoring or obeying those rules by students of pedagogical sciences. My work will be focused on area of IT security, which are graduates most possible to encounter, during thein work. Furthermore, i will focus on practical impacts of familiarity or ignorance of those rules and baselines which are described above, in the theoretical part, or mentioned in the questionary, on the ability to carry out pedagogical related occupations. Certain part of my work will be dedicated to social networks, its usage, possible and impacts the they can have on teacher, hist ability to pass knowlidge, his autority among the students and quality of education process. From collected and summarized datas will be uncovered current status of IT security awareness and will be created work, that could be used to improve the metodology, and content of information technology studies on universities and high schools, mostly on gymnaziums.

Poděkování

Moc děkuji Mgr. Václavu Šimandlovi za trpělivost, vedení a cenné rady které mi v průběhu této práce poskytl a díky nimž jsem byl schopen tuto práci zhotovit. A také děkuji mamince Mgr. Lence Sadilové za cennou psychologickou a materiální podporu. Také děkuji tátovi Ing. Pavlu Sadilovi za podporu psychickou i materiální a pomoc s korekcí práce po stránce pravopisné. Jo a ještě bráchovi :)

Obsah

1. Úvod

Dnes v 21. století se nacházíme v době digitálních technologií. Nachází se všude kolem nás a my s nimi interagujeme každý den. Ať už se svým mobilním telefonem, počítačem v práci či se svým automobilem, který má dnes již nejspíše také v sobě zabudovaný počítač. Nejenže nám tyto technologie náš život v mnohém usnadňují, ale s jejich výskytem a používáním na téměř každodenní bázi, se vystavujeme i mnohým rizikům, která tyto technologie přináší.

Proto je velmi důležité, abychom se sami alespoň trochu orientovali v digitálním světě. Dnes to již patří mezi samozřejmosti, které dnešní mládež umí a zná. Avšak jak jsem již zmiňoval výše, je potřeba se bránit mnohým nebezpečím, které na nás v digitálním světě číhají, a to zvláště na mladistvé. A kdo jiný než právě rodiče či učitelé by měli naučit naši mládež základům v IT bezpečnosti?

1.1 Role učitele v ovlivňování IT gramotnosti mládeže

I když si jsou dnešní děti sebejisté při zacházení s informačními technologiemi, stále se u nich rozvíjí kritické vyhodnocovací znalosti, a proto potřebují naši pomoc, abychom jim dopomohli udělat správná a moudrá rozhodnutí. [1]

Takto shrnula postoj dospělých k dětem i IT světě T. Byron. Její názor dává jasně najevo, že bychom měli dětem pomáhat se orientovat a bránit ve světě digitálních technologií. Učitelé sehrávají významnou roli v duševním, intelektuálním i společenském rozvoji osobnosti mladistvých. Předávají jim nejen své znalosti a zkušenosti, ale zčásti také své přístupy a postoje ke svému okolí. Jak jsem již výše zmiňoval, významnou součástí koloritu 21. století se staly i právě informační technologie a postoje, znalosti a schopnosti žáků (další generace) se ubránit v digitálním světě útokům nejen na svá data,

ale například i na jejich osobní údaje, budou významně formovány právě učiteli, kteří budou tuto (a jistě i následující) generace vyučovat a vzdělávat.

Právě z tohoto důvodu je naprosto nezbytné, aby i učitelé byli gramotní a znalí alespoň základních postupů, zásad a pravidel, které je potřeba dodržovat, pokud chceme být v digitálním světě v bezpečí.

Nezanedbatelný je i dopad, který může mít případný problém související s digitální bezpečností na osobu učitele jako na jedince. Je možné, že díky úniku osobních dat bude ohroženo jeho postavení ve společnosti, osobní vztahy, či dokonce zaměstnání. (viz. Kapitola 5.1)

1.2 Situace ve světě

Při studiu situace v digitální bezpečnosti ve světě si můžeme udělat obrázek, jak jsme na tom v porovnání s ostatními zeměmi, můžeme se dozvědět, jaké události s jaké následky mohou následovat po tom, co uniknou naše data, anebo se můžeme dozvědět, co jiné země dělají pro to, aby zvedly úroveň uvědomění o informační bezpečnosti.

2. Cíle práce

Cílem práce je zpráva obsahující dotazníkový průzkum a metodologii provedení mezi studenty učitelství na vysokých školách, zaměřený na jejich znalosti a zkušenosti v IT bezpečnosti. Dále tato zpráva bude obsahovat vyhodnocení zmíněného dotazníku a konfrontaci tohoto stavu s doporučeným, či ideálním stavem, který bude popsán v teoretické části. Součástí zprávy bude teoretické pozadí vztahující se k tématu, k lepší orientaci v závěrech, které budou z této zprávy vyplývat, ke konfrontaci s výsledky a také bude sloužit jako vodítko a zdroj informací, pro maximální možnost správně interpretovat uvedená fakta a závěry. Tato zpráva bude k dispozici středním a vysokým školám a jiným vzdělávacím institucím, které by ji mohly případně použít pro optimalizaci výukových a zkouškových procesů u svých studentů. Pokud se tak rozhodnou, s pomocí výsledků mé práce budou moci lépe odhadnout úroveň, jakou mladí učitelé (potenciální budoucí zaměstnanci a nynější studenti) v oboru IT bezpečnosti mají a školy tak budou mít lepší přehled nejen o tom, jaké potenciální zaměstnance přijímají, ale v případě pedagogicky zaměřených škol vysokých také o tom, jak kvalitně své žáky vzdělávají právě v oboru digitální bezpečnosti, což lze v případě právě pedagogicky zaměřených vysokoškolských oborů použít pro případnou úpravu osnov výuky, či změně testů, jako je například ITT test zde, u nás na fakultě.

3. Metodologie prováděné práce

3.1 Výzkum již provedených studií podobného tématu a konzultace s odborníky

Nejdříve jsem prozkoumal zprávu The Byron Rewiew, jednu z nejrozsáhlejších a nejpodrobněji zpracovaných zpráv na téma bezpečnosti dětí v digitálním světě a tedy i kompetenci, kterou by měli pedagogičtí pracovníci, kteří se o tyto děti starají, mít. Zjistil jsem, jak vypadá postoj k digitální bezpečnosti v pedagogickém prostředí jinde ve světě a dále mi tato zpráva sloužila jako zdroj mnoha faktů a byla použita jako podklad při vypracovávání nejedné kapitoly této práce.

Zaměřil jsem se také na prostudování zpráv ze společností, jako například Kaspersky Lab. Zprávy z laboratoří Kaspersky byly použity především při analýze hrozeb jako je spam, hoax či virových hrozeb. Společnost Kaspersky uvádí pravidelně velmi podrobné studie, zabývající se především šířením spamu. Tato data byla použita především při sestavování teoretického pozadí.

Velmi praktickým a informacemi nabitým zdrojem se prokázaly být i články a zprávy publikované společností Eset. Tato společnost, zabývající se především vývojem antivirového systému NOD 32, zevrubně analyzuje současný stav hrozeb, jako jsou právě viry. I zde jsem našel data, která jsem využil při sestavování nejen teoretického pozadí pro mou práci.

Během sepisování mé práce jsem i často využíval různé články od společnosti Microsoft, které se týkaly například různých aspektů zabezpečení operačního systému.

Dále jsem prozkoumal práci Mgr. Václava Šimandla a Jana Lhotáka, kteří zpracovali zprávu o konkrétním stavu této problematiky v České republice. Tato zpráva mi dala představu, jak bych mohl svou práci koncipovat a jakým směrem by bylo vhodné se zaměřit. V jejich práci je přítomen i velmi zajímavý dotazníkový průzkum a analýza kompetence žáků v oblasti digitální bezpečnosti, což je téma velmi blízké tématu mému a tak jsem byl snadno

schopen zjistit například to, co se od žáků očekává, že budou v oboru digitální bezpečnosti ovládat a tak jsem byl schopen se díky těmto zjištěným faktům zaměřit na témata, která by mohla být relevantní právě i pro učitele.

I v průběhu vytváření této práce jsem leckdy potřeboval odbornou radu. Mými poradci se stali Mgr. Šimadl, a Ing. František Hodys. Mgr. Šimandl mi poskytl cenné rady o vytváření takto složité práce a poskytl konzultace k všem problémům, které jsem s vypracováváním měl. Ing. Hodys je odborník s dlouholetou zkušeností práce v kantorském kolektivu jako učitel informatiky, statistiky a matematiky. Jeho zkušenosti a rady mi poskytly nápady, jakým směrem by se mohl výzkum ubírat, a poskytoval mi konzultace, pokud jsem si nebyl jistý tím, jaký je současný stav dané problematiky v českém školství.

3.2 Tvorba teoretického pozadí

V teoretickém pozadí jsem se snažil osvětlit problematiku témat, se kterými by se mohli velmi často dostat do styku studenti učitelství. Jedním z těchto témat jsou například i hesla a protože se s nimi dnešní populace setkává (pokud používají informační technologie) každý den, je velmi důležité, aby se nejen studenti ale i všichni, kteří budou tuto zprávu zkoumat, seznámili s jejím obsahem. Problematice hesel jsem se rozhodl věnovat i v kapitole, která se zabývá emailovou komunikací.

Nemalou váhu bylo potřeba věnovat i zálohování, neboť data jsou velmi důležitá a pokud o ně přijdeme, je veliká pravděpodobnost, že nebudeme schopni vykonávat svou práci stejně efektivně jako s nimi, nebo že budeme muset věnovat čas tomu, abychom ona ztracená data znova vytvořili či jiným způsobem vyřešili situaci, která by jinak vyžadovala, abychom ona data měli přístupná.

Dále bylo také po konzultacích s výše zmíněnými odborníky rozhodnuto, že jistá část práce by měla být věnována i systému Microsoft Windows. S tímto systémem totiž budou přicházet do styku nejen studenti učitelství,

ale i jejich studenti či zaměstnavatelé, což znamená, že bude velmi důležité, aby učitelé tyto systémy znali, a věděli, co se v nich nachází a jaká jsou případná potenciální rizika.

Jistou část teoretického pozadí jsem věnoval i problematice firewallu a antivirového systému, protože je velmi důležité, aby osoby které budou dále číst a studovat moji práci, byly obeznámeny se základními fakty a zvyklostmi, které se vážou k těmto dvěma programům zajišťujícím různé bezpečnostní aspekty, které jsou velmi důležité pro bezpečné užívání počítače.

3.3 Tvorba dotazníku

Dotazník byl vytvářen s ohledem na cílovou skupinu, jíž se stali studenti vysokých škol z pedagogické fakulty Jihočeské univerzity v Českých Budějovicích. Otázky jsou krátké, pokud možno jednoznačné a výstižné. Soustředil jsem své otázky na témata, která jsem již dopředu věděl, že budu ve své práci dále rozebírat, a snažil jsem se tak načerpat data, na základě kterých budu vyvozovat závěry plynoucí z nedodržování, či naopak dodržování bezpečnostních zásad a pravidel, která budou v práci prezentována. Tyto zásady a pravidla zde uvádím, pouze pokud jsem si jejich správnost a relevantnost k danému tématu ověřil ve svém průzkumu.

Dotazník obsahoval i otázky týkající se problematiky sociálních sítí. Této problematiky se chci dotknout také, neboť sociální sítě se stávají čím dál více rozšířeným fenoménem[18] a jak jsem zjistil při zkoumání článku Davida R. Brakeho, dopad na studenty je veliký. Což znamená, že se učitel s tímto fenoménem určitě setká a bude se jistě muset vypořádat s případnými riziky, které vyplývají z interakcí na sociálních sítích.

Dotazník byl vyplněn 79 studenty z jihočeské univerzity, kteří studují učitelské obory. Odpovídalo 21 můžů a 58 žen ve věku 21 až 25 let. Data, která byla získána tímto dotazníkovým průzkumem, byla převedena do elektronické podoby, dále byla zanalyzována a následně byla použita jako podklad pro další analýzu problematiky.

3.4 Tvorba a sepisování zprávy o stavu problematiky u nás, a ve světě

V této části práce jsem se snažil popsat některé situace, které se staly v různých částech světa a pokoušel jsem se také zjistit zajímavé a relevantní informace o zacházení s problematikou digitální bezpečnosti v ostatních zemích.

Mým cílem bylo popsání současné situace v naší v republice a vyvození případných následků z toho, co vyšlo, pokud byly konfrontovány výsledky dotazníku s ostatními fakty a daty, které se mi do této práce podařilo nasbírat. Snažil jsem se soustředit na ty nejdůležitější a potenciálně nejrizikovější části digitální bezpečnosti, se kterými se nejspíše bude náš budoucí učitel setkávat. Důležitým aspektem také pro mě bylo to, jak dobře (a jestli vůbec) je schopen učitel vykonávat svoje povolání, pokud je narušen nějaký aspekt digitální bezpečnosti. Potenciálně nebezpečné situace byly popsány v kapitole 5.1, na kterou se poté odvolávám i v několika dalších částech práce. Z této kapitoly lze totiž vyčíst, co se případně může stát, pokud naše osobní data uniknou do nepatřičných rukou. Doufal jsem také, že tato kapitola by mohla pomoci si představit různým čtenářům mé práce, jak velmi nebezpečné může být nedodržování pravidel digitální bezpečnosti v osobním i profesním životě.

4. Teoretické pozadí

4.1 Počítačová bezpečnost a rizika

Našemu počítači a datům v něm uloženým hrozí různá rizika, ať už vnější či vnitřní. Hrozí například, že nám bude PC odcizen, či že bude napaden po stránce softwarové. [2]

Vnitřní nebezpečí je velmi častým nebezpečím, se kterým se počítače často setkávají. Vnitřní nebezpečí pochází od okolností, které nelze ovlivnit, čí od oprávněných uživatelů, kteří svými akcemi neměli původně v úmyslu systém nijak ohrozit. Hrozí například, že hardware bude poškozen, či odcizen, může dojít k výpadku proudu,

4.2 Hesla

Hesla jsou nedílnou součástí zabezpečení elektronických dat již velmi dlouhou dobu. Data, ke kterým chceme umožnit přístup na základě znalosti hesla, jsou zašifrována algoritmem, který data převede (zašifruje) do nečitelné podoby a pokud není k dispozici klíč, kterým byla data zašifrována, v tomto případě heslo, data se jeví jako nesmyslná. [2]

Doba, za kterou je možno prolomit ochranu heslem, záleží hlavně na **síle hesla.**

Síla hesla je určena dvěma faktory. Prvním z nich, je průměrný počet pokusů, kolikrát by musel útočník zkusit náhodnou kombinaci znaků, nežli by doopravdy uspěl a heslo uhádl a zároveň také lehkost, se kterou je útočník schopen ověřit, zda je právě zkoušené heslo správné. Druhým faktorem, který ovšem není ovlivnitelný uživatelem je, jak a kde je heslo skladováno, a také, jak často a kým je používáno. Tento druhý faktor je však ovlivňován původním designem systému, a musí na něj být brán ohled již během implementace.

4.2.1 Zásady pro výběr silného hesla

Pokud chceme, aby naše heslo bylo silné a snáze odolávalo pokusům o prolomení, musíme dodržovat několik zásad a pravidel pro výběr silného hesla. [2]

- Heslo nesmí být snadno uhodnutelné, nesmí se jednat o běžné slovo, jméno či název, ale ani například název uživatelského účtu. Je potřeba se vyvarovat heslům, jako jsou jména dětí, domácích mazlíčků, příbuzných, známých či jejich data narození atd...

- Pokud je heslo tvořeno slovy, mělo by jich obsahovat více než jedno.

- Heslo by mělo obsahovat velká i malá písmena, stejně jako číslice. Pokud je to možné a systém nám to dovolí, silné heslo by mělo obsahovat i speciální znaky, či diakritiku.

- Minimální počet znaků v hesle by měl být 8 (ale raději alespoň 12)

- Heslo by si měl uživatel pouze pamatovat. Neměl by ho přechovávat nikde jinde nežli ve své hlavě. Zvláště nebezpečné je, si heslo napsat například na papírek a ten si někam založit. Pokud je heslo skladováno ve formě snadno přístupné ostatním osobám, je možné ho získat a zneužít.

- Heslo je potřeba jednou za čas změnit, a toto nové heslo by se nemělo podobat heslu předchozímu

4.3 Čtečky otisků prstů

Čtečky otisků prstů se pomalu ale jistě stávají stále více používaným zabezpečovacím systémem v noteboocích. Čtečka otisku prstů, stejně jako jakýkoliv jiný biometrický snímač, nabízí velmi vysokou míru zabezpečení pro naše data, protože záznam o jakémkoliv biometrickém údaji, například otisku prstu, či struktury rohovky, obsahuje velké množství dat a proto je prolomení metodou Brute Force téměř nemožné, protože množství možných kombinací je téměř astronomické. [3]

I přes zjevné klady, čtečky otisků prstů nejsou příliš využívány, kvůli několika neduhům, kterými trpí všechny biometrické systémy. Například se může stát, že se parametry změní. Bříško prstu si může uživatel spálit, zjizvit nebo jinak poškodit a hrozí, že nebude schopen se ke svým datům dostat. Proto někteří uživatelé volí cestu takovou, že používají nejen biometrický snímač, ale jako zálohu mají i heslo, což tedy pro nás výhody biometrického zabezpečení smazává, protože heslo lze prolomit snadněji a tak se případný útočník může zaměřovat na lehčeji prolomitelné heslo, nežli na biometrické ověření identity.

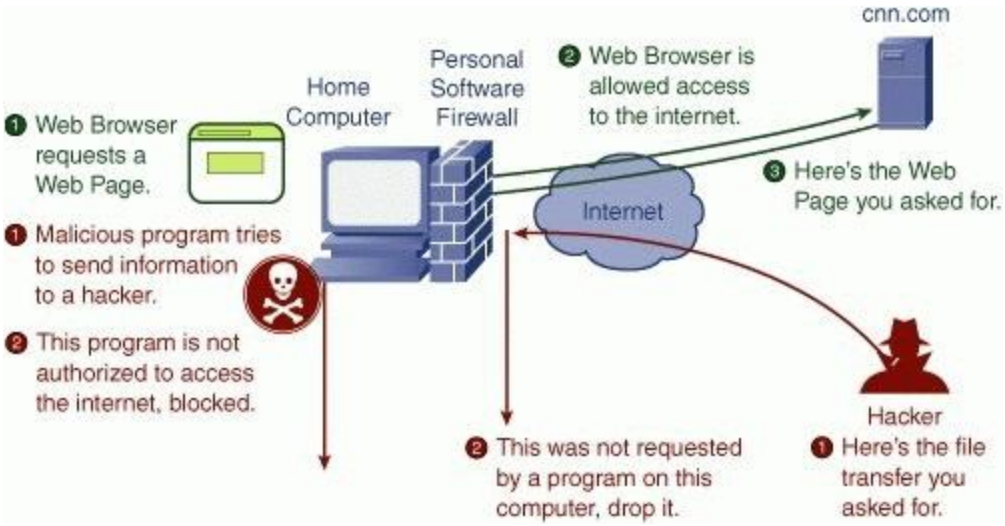
4.4 Zabezpečení v systému Windows

Na systém Windows jsem se rozhodl zaměřit, protože dle statistik je nejpoužívanějším operačním systémem v naší republice (i na světě) [4].

Mezi základními bezpečnostními prvky, které má v sobě systém také integrovány, patří například možnost chránit svůj účet heslem či použít (někdy pouze s použitím dodatečných ovladačů) různé jiné metody ověření identity uživatele. Po více jak 10 pokusech o přihlášení s chybným heslem je systém uveden do nefunkčního stavu a musí být restartován. Toto opatření je velmi účinné, neboť omezuje možnosti vedení Brute force útoku, který se právě pokouší v co nejmenším čase vyzkoušet co nejvíce potenciálních hesel. Mezi jinými metodami ověřování identity uživatele, se často můžeme setkat například s čtečkou otisků prstů.

Po více jak 10 pokusech o přihlášení s chybným heslem je systém uveden do nefunkčního stavu a musí být restartován. Toto opatření je velmi účinné, neboť omezuje možnosti vedení Brute force útoku, který se právě pokouší v co nejmenším čase vyzkoušet co nejvíce potenciálních hesel.

Účet, který je chráněn heslem, nabízí také možnost uložit svá data do složky dokumenty, do které mají povolen přístup pouze účty, které mají plná oprávnění. Systémy Windows nenabízí defaultně žádné další možnosti jak svoje data zabezpečit heslem, či jak je jiným bezpečným způsobem skladovat mimo dosah neoprávněných uživatelů.



[17]

Pokud se pokoušíte připojit k počítači s tímto operačním systémem přes síť, bude vám zpřístupněna složka sdílené dokumenty a budou vám nabídnuty sdílené tiskárny. (To vše za předpokladu že nebylo manipulováno s defaultním nastavením sítí a sdílení.) Pokud však má uživatel na administrátorském účtu nastaveno heslo, vzdálený uživatel bude vyzván, aby ho zadal.

Windows XP sp2 a výše také v sobě obsahuje již od původní instalace zabudovaný firewall. O kvalitě tohoto firewallu budu hovořit níže. Systém již bohužel není vybaven defaultním antivirovým systémem, a proto je velmi důležité počítač jím co nejdříve vybavit. Výjimku tvoří dnes nejnovější operační systém od firmy Microsoft, Windows 8, který nabízí již předem nainstalovaný bezpečnostní balík, který byl dříve znám jako Microsoft security Essential. Součástí tohoto bezpečnostního balíčku je právě mimo jiné i onen zmíněný firewall a antivirový program.

4.4.1 Windows firewall

Operační systémy Windows (pouze v systémech novějších nežli je Windows XP - sp2) přichází s již předem nainstalovaným firewallem. Firewall je softwarový nástroj, který odděluje chráněnou síť (či chráněnou část) od nechráněné a nabízí základní zabezpečení systému při připojení k internetu. [2]

Firewall pracuje velmi jednoduchým způsobem. buď povoluje či zakazuje programům, protokolům, či portům atd... přístup z/do počítače. Pokud se např. neznámý program z internetu pokusí kontaktovat náš počítač, firewall se nás nejdříve zeptá, jestli má tomuto programu povolit připojení. Jsou nám nabídnuty 2 možnosti jak s žádostí o připojení naložit + možnost si volbu zapamatovat. Připojení od určitého počítače můžeme přijmou - tzn. vystavit se riziku infekce zvnějšku (ale zároveň to znamená povolit programu, co se nás tázal, fungovat) anebo odmítnout, což programu sice znemožní fungovat, ale zároveň nás to ochrání před vnějšími vlivy.

4.5 Spam

Spam, neboli nevyžádaná pošta představuje v dnešní době 71% celkového objemu příchozích emailových zpráv. [5] Spam zahlcuje naše schránky a tak nás připravuje o náš čas a zároveň snižuje efektivitu práce, kterou jsme schopni za jednotku času vykonat. Mezi spam můžeme zařadit například pyramidové hry, podvodné loterie, inzerce na neexistující výrobky, různé rafinované žádosti, které se z nás snaží vylákat podvodem osobní údaje či rovnou peníze.

4.5.1 Jak se spamu bránit

Dnešní antispamové programy používají tři základní metody detekce spamu

Byesovský filtr -porovnává obsah e-mailu s tím, co uživatel již dříve označil jako spam. Tato metoda je tím více účinná, čím častěji je využívána.

Blacklist - Je seznam adres, ze kterých spam byl/je rozesílán. E-maily přicházející z adresy která se nachází na blacklistu, jsou rovnou uloženy do schránky pro spam, či jsou namístě vymazány.

Summary search - Tato metoda vyhledává ve zprávách typická slovní spojení či často se vyskytující slova, která jsou pro spam typická.

4.6 Phishing

Oxfordský slovník [18] popisuje pojem phishing jako posílání emailů, které se zdají pocházet od věrohodných společností, za účelem vylákání osobních informací, čísel kreditních karet, hesel a jiných citlivých dat.

Email, který se z uživatele pokusí vymámit jeho osobní či jiná citlivá data, se většinou tváří relativně věrohodně. Jedním ze znaků těchto podvodných mailů bývá špatná emailová adresa. Pokud například uživateli přijde mail z adresy vasebanka@seznam.cz, místo běžné adresy ze které bankovní emaily chodí, je vhodné zkontrolovat, jaká by měla být originální adresa, ze které by tyto maily měly přicházet. To se dá velmi snadno zjistit na oficiálních stránkách dané instituce.

Velmi často se dnes vykytuje i phishing mezi hráči her počítačových. Masivně multiplayerové hry, které se v dnešní době často hrají, bývají placené, a proto pokud hráč vyzradí svoje jméno a heslo, může být připraven o herní účet, do kterého investoval peníze.

4.7 Hoax

Překlad anglického slova Hoax znamená Falešnou zprávu, Mystifikaci, Novinářskou kachnu, Podvod, Poplašnou zprávu, Výmysl, Žert, kanadský žertík.

Typický text poplašné zprávy obsahuje většinou tyto body: [7]

- **Popis nebezpečí (viru)**

Smyšlené nebezpečí (vir) bývá stručně popsané, v případě viru bývá uváděný i způsob šíření.

- **Ničivé účinky viru**

Zde záleží převážně na autorově fantazii. Ničivé účinky mohou být celkem obyčejné, třeba zformátování disku nebo už míň důvěryhodné - zběsilý útěk myši do ledničky, roztočení HDD opačným směrem, výbuch počítače… Autoři hororů zde mohou hledat inspiraci.

- **Důvěryhodné zdroje varují**

Ve většině případů se pisatel poplašné zprávy snaží přesvědčit, že varování přišlo od důvěryhodných zdrojů ("IBM a FBI varují" nebo "Microsoft upozorňuje" atd.)

- **Výzva k dalšímu rozeslání**

Tento bod HOAX vždy obsahuje! Mnoho nezkušených uživatelů se nechá zprávou napálit a bez přemýšlení výzvu uposlechnou. Právě proto se tyto nesmysly lavinovitě šíří.

Jako hoax můžeme také označit šířenou zprávu, která obsahuje nepřesné, zkreslující informace, účelově upravené polopravdy nebo směsku polopravd a lží. [7]

4.8 Zálohování

Zálohování je způsob, kterým chráníme svá data před ztrátou. Podstata zálohování spočívá v nejen v duplikaci dat, ale i jejich skladování na jiném (fyzickém) místě nežli data původní, čímž zvyšujeme pravděpodobnost, že budeme po ztrátě originálních dat schopni alespoň (tu zálohovanou) část obnovit.

Existuje několik druhů záloh, avšak mezi ty nejpoužívanější patří tyto:

Nestrukturovaná: Náročnost na kapacitu: malá až střední

Tato záloha je nejčastěji prováděna laiky. Její podstata spočívá v manuálním výběru důležitých dat, a jejich následná duplikace na záložní médium.

Úplná: Náročnost na kapacitu: velmi vysoká

Během této zálohy jsou zálohována všechna data z originálního média na médium zálohovací. Většinou se vytváří jeden soubor, zvaný image, který představuje kompletní obraz původního média.

Přírůstková: Náročnost na kapacitu: malá až střední, později vysoká

Přírůstková záloha se provádí, pokud je dostupná předchozí, úplná, záloha. Přírůstková záloha vytvoří zálohu dat, která se od poslední úplné, či přírůstkové zálohy změnily. Nevýhoda spočívá v tom, že pokud chceme obnovit data, musíme obnovovat postupně ze zálohy úplné, přes přírůstkové, které následovaly, až do bodu kdy se budeme obnovovat data z naší poslední zálohy. Tento typ zálohování je tím více náročný na kapacitu zálohovacího média (médií), čím více záloh provádím. Také proces případné obnovy dat ze záloh, se stává čím dál tím více zdlouhavým procesem.

4.9 Email

Spolu s tím, jak se postupně internetové připojení stávalo čím dál tím běžnější záležitostí, rozrůstala se i využitelnost digitální pošty, čili emailu (Electronic mail - elektronická pošta). Email nabízí oproti běžné, na papíru probíhající korespondenci spolehlivost a rychlost, se kterou je schopen informace doručit k adresátovi.

Email ale může představovat veliké potenciální riziko. S emailovou zprávou může být doručena příloha, která může obsahovat potencionálně škodlivý kód jako jsou např. viry, či trojské koně.

4.10 Antivirová ochrana

Antivirová ochrana bývá zajištěna v osobních počítačích a chytrých mobilních telefonech především antivirovým programem. Ten má za úkol identifikovat a izolovat potenciální virové hrozby.

Antivirový program používá několik metod detekce hrozeb. Zde zmiňuji pouze ty nejpoužívanější[6]

Algoritmické skenování -Vyhledávají se již známé části kódu či velmi podobné části. Je zde malá pravděpodobnost chybné detekce. Tato metoda není příliš náročná na výpočetní čas a jiné systémové zdroje.

Heuristická analýza - Analyzuje chování zkoumaného souboru uvnitř chráněného prostředí a tím vidí, co by se stalo, pokud by byl kód spuštěn.

Pokud jsou výsledné akce vyhodnoceny jako nežádoucí, je soubor označen jako potenciálně nebezpečný. Tato metoda je středně náročná na výpočetní čas a jiné systémové zdroje.

5. Stav problematiky ve světě

5.1 Možné následky úniku osobních dat ve vztahu k osobě učitele.

Za našimi hranicemi se odehrálo již bezpočet případů, kdy učitelé doplatili na neznalost, či nedodržování základních bezpečnostních pravidel která by měl dodržovat každý, kdo využívá s informační technologie, či s nimi nějakým jiným způsobem interaguje. Dále uvedu několik příkladů, které zveřejnila mezinárodní vzdělávací asociace.[8]

- v roce 1974 v Kalifornii, byl vyhozen ze zaměstnání učitel Lou Zivkovich, protože pózoval nahý v magazínu Playgirl. Dnes, díky pokroku ve sdílení fotografií, nemusíme vůbec být uveřejněni v časopise nazí, stačí, když sami necháme takovou svojí fotku volně (či špatným osobám) přístupnou, například na sociální síti.

-ve Virginii byl propuštěn středoškolský učitel Stephen Murmer po tom, co na internet umístil ukázky svojeho "prdelního umění" (butt art), jak ho sám nazval, kde bylo následně toto "umění" shlédnuto mnoha žáky. Podstata umění spočívala v nanášení barvy na vlastní pozadí a genitálie, a následné obtisknutí na kreslící plochu.

Vedoucí školní kapely Scott Davis z Boward County, ve státě Florida, byl propuštěn poté, co školní zástupci shlédli jeho MySpace profil, (MySpace je sociální síť, jako Facebook, nebo Google+) na kterém sdílel příspěvky, ve kterých dumal a přemýšlel nad sexem, drogami a vlastní depresí.

Díky těmto případům lze snadno dojít k závěru, že sdílení svých osobních zážitků, dat či vyzrazování jiných bezpečnostních informací, se může (zvláště učiteli) dosti vymstít. Je proto důležité tuto problematiku sdílení osobních dat na sociálních sítích dále prozkoumat.

5.2Jak vypadá situace ve školství a digitální bezpečnosti ve světě

[1]Jak uvádí profesorka Tanya Byron ve svém výzkumu, 51% evropských teenagerů v roce 2010 mohlo užívat počítač připojený k internetu bez dohledu

svých rodičů. Dále bylo zjištěno, že 18% mladých lidí používajících internet, zažilo na internetu situaci, která by se dala popsat jako škodlivá či nevhodná.

Toto zjištění vedlo v řadě zemí jako je například Velká Británie k tomu, aby byly podstoupeny kroky, vedoucí k osvětě a pozvednutí znalostí, z oboru informační bezpečnosti.

Ve Velké Británii dokonce byla v roce 2009 spuštěna kampaň mající za účel veřejnost informovat o nebezpečích číhajících v digitálním světě a nutnosti se umět těmto hrozbám bránit.

5.2.1 Absolventi pedagogicky zaměřených škol

Podle průzkumu provedeného ve Velké Británii v roce 2009 [1] si 77% procent absolventů pedagogických oborů myslelo, že disponují dostatečnými znalostmi a zkušenostmi s digitální bezpečností aby byli schopni efektivně připravit a učit svoje studenty jak se chovat v digitálním prostoru.

Velmi důležitý je také postoj učitele k problematice bezpečnosti celkově, protože tím udává příklad i svým studentům. Jak dokládá článek publikovaný mezinárodní vzdělávací asociací[8], studenti mohou a dokonce již i v několika zdokumentovaných případech využili slabin v zabezpečení účtů svých kantorů a zveřejnili citlivá data o těchto osobách, jejich činech a chování. O těchto událostech jsem se zmiňoval v kapitole 5.1.

5.3 Archivace hesel

Pokud člověk používá k přístupu do svého digitálně zabezpečeného prostoru heslo, jistě se dříve či později dostaví potřeba si svoje hesla někam napsat, zálohovat, uschovat či jiným způsobem zabezpečit proti zapomenutí. Fakt, že člověk používá několik různých hesel dokládá i rozsáhlá studie prováděná v letech 2006-2007 firmou Microsoft. [9] V této zprávě je uvedeno, že člověk mezi 10-30 lety využívá průměrně kolem pěti až šesti hesel.

6. Čeští studenti učitelství a digitální bezpečnost

Protože se jistě školy snaží takovýmto věcem předcházet, zaměříme se na různé relevantní a důležité aspekty právě z oboru digitální bezpečnosti, která by mohla ovlivnit pracovní i osobní poměry studenta učitelství, který pokračuje ve svojí studiem započaté kariéře.

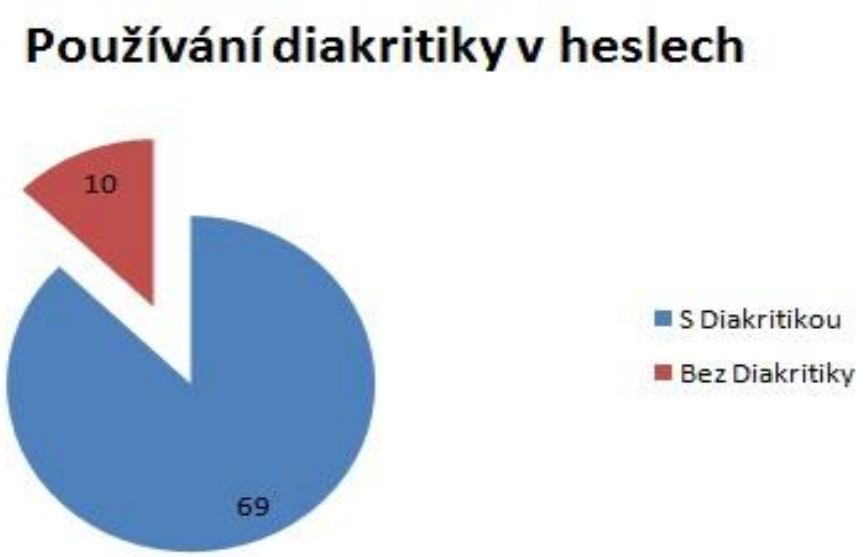
6. 1 Hesla

Jsou nejběžnějším způsobem zabezpečení dat či účtů. Žáci by tedy měli mít vštípeny alespoň základní pravidla a bezpečnostní zásady, které se hesel týkají.

6.1.1 Studenti a hesla

Studenti učitelství používají z větší části ve svých heslech diakritiku či velká písmena jak dokazují data, která jsem nasbíral ve svém průzkumu. 87,4% dotázaných tedy udělalo alespoň první krok vstříc bezpečnějšímu heslu.

Tento fakt je velmi důležitý, neboť se tímto snižuje pravděpodobnost, že data chráněná tímto heslem budou úspěšně napadena, ale také nastává pro učitelovy studenty motivující situace, kdy bude náš potencionální budoucí učitel doopravdy používat to, co bude svoje žáky učit a také od nich vyžadovat. Nelze tedy vynechat ani nezanedbatelný psychologický aspekt, který tato skutečnost přináší.



Pravděpodobnost že autorita učitele bude zpochybněna tím, že jeho data budou úspěšně napadena právě skrze prolomení hesla, klesá spolu s pravděpodobností právě onoho odhalení přístupového kódu. (hesla) Jak bylo výše popsáno, pokud heslo obsahuje diakritiku či velká písmena, nebo jiné speciální znaky, klesá pravděpodobnost, že bude heslo v kratším čase objeveno metodou brute force.

Také klesá pravděpodobnost, že bude heslo uhádnuto. I v případě že by bylo heslo verbálně vyzrazeno, stále například ještě existuje velké množství možností použití velkých či malých písmen, což opět snižuje šanci úspěšného prolomení hesla.

6.1.2 Archivace hesel

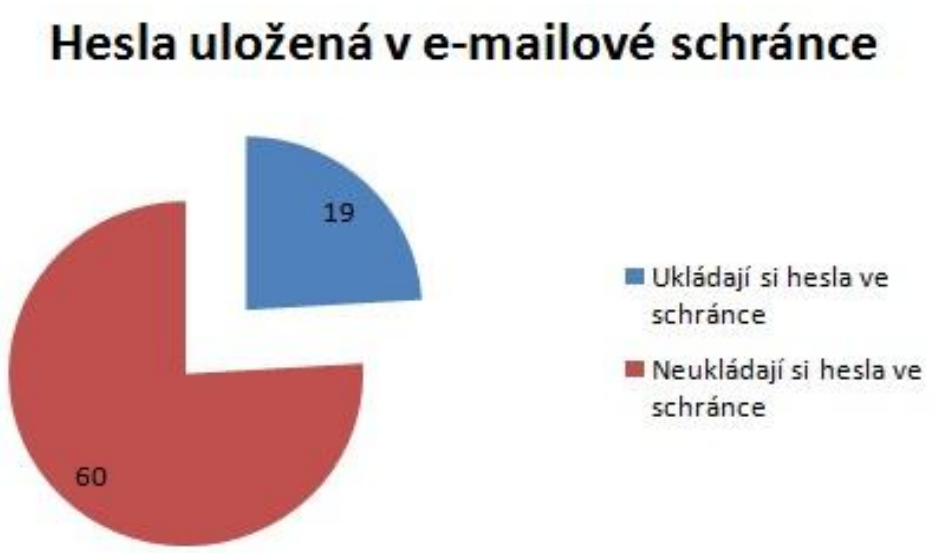
Díky výše uvedenému faktu že průměrný člověk používá pět až šest hesel, se již dostavuje potřeba svoje hesla někde skladovat, aby byla snížena pravděpodobnost, že heslo bude zapomenuto, a data či služby, které toto heslo chránilo, se stanou nepřístupnými. Jedním z míst kde lze hesla skladovat s dojmem, že jsou bezpečná se může zdát naše emailová schránka. Tento trend, uchovávat svá hesla v emailové schránce se začal pomalu rozšiřovat s masivnějším nástupem internetu do domácností. Pokud se uživatel totiž zaregistruje ať už na diskusní fórum, k používání nějaké online služby či třeba i jenom k hraní online hry, s emailem potvrzujícím registraci, povětšinou přichází i původně zadané registrační údaje, aby si je mohl uživatel zkontrolovat. Když se tedy uživatel emailové schránky rozhodne si svoje heslo nechat někde snadno dostupné, jediné co musí udělat, je nesmazat email se kterým přišlo potvrzení o registraci spolu s registračními údaji.

Pokud člověk aktivně využívá všechny svoje hesla i v hlubinách internetu právě k registracím na služby odesílající zpět email s registračními údaji, vystavuje se tak riziku, že v případě že někdo zjistí jak se dostat dovnitř jeho emailové schránky, můžou být hesla, co v ní byla uložena, zkompromitována a spolu s nimi i relevantně velká část účtů tyto hesla využívajících.

Jak dokládá můj výzkum a jak se můžete dozvědět z přiloženého grafu, přibližně čtvrtina studentů učitelství používá svou emailovou schránku přesně k tomuto účelu (skladování hesel). Tímto se tedy dostávají do situace, kdy jsou jimi používaná hesla, a tím pádem i data a údaje která tyto hesla chrání, oddělena od internetu pouze chatrným zabezpečením poskytovatele emailové schránky a pouze jediným heslem které by potenciálnímu útočníkovi, který by se snažil hesla získat, stálo v cestě.

V případě, že by chtěly osoby zajistit svoje hesla pečlivěji, lze doporučit pouze neskladovat je na jednom místě, čili decentralizaci. Pokud možno neskladovat vůbec svoje hesla v digitální podobě, protože jak uvádí světová vzdělávací asociace, nikdy bychom neměli do digitální podoby vkládat nic, co nechceme, aby viděli naše děti, známí, rodiče, kolegové či podřízení. Mezi takovéto věci, které nechceme vidět na veřejnosti, jistě patří i naše hesla.

Jednou z možností jak lépe chránit svoje hesla, pokud už se rozhodneme je mít uložena v emailové schránce, je používat poštovní klienty jako je například Mozilla Thunderbird nebo známý Outlook. Pokud si nastavíme, že naše emaily mají být stahovány, na místní disk a poté vymazány, jsou tím pádem data obsažená v těchto emailech (včetně hesel) uložena na našem místním disku a nejsou již přístupna tak velkému množství potenciálních útočníků, jako kdyby byly dané emaily skladovány na internetovém úložišti.



Jak uvádí přiložený graf, téměř čtvrtina dotázaných studentů učitelství používá svoji emailovou schránku mimo jiné právě i ke skladování svých hesel. Toto je vzhledem k výše vyvozeným závěrům pro onu čtvrtinu potenciálně nebezpečná situace, které by mohlo být využito k získání nejen osobních údajů, ale právě i oněch používaných hesel.

V případě že tedy chceme svoje hesla udržet v bezpečí, měli bychom si je v nejlepším případě pamatovat, a nezvěčňovat je do žádné fyzické podoby, ani podoby elektronické. Je důležité udržet svoje hesla a jména účtů v anonymitě, protože skrze ně, je možno osobu velmi lehce zdiskreditovat, či jiným způsobem narušit její soukromý či profesní život.

6.2 Otisk prstu místo hesla

S rozvojem informačních technologií se začaly rozšiřovat i mezi běžnou populaci přenosné počítače neboli notebooky. V dnešní době jsou nejen ve střední, ale nižší cenové kategorii už běžně dostupné i takové přenosné počítače, které jsou vybaveny snímačem otisku prstu.

Díky tomuto faktu, se nabízí školám, které vybavují učitele notebooky, příležitost zakoupit takové přenosné počítače, které jsou touto čtečkou vybaveny. Instalace i běžné používání čtečky není náročné a je lehce zvládnutelné i pro méně technicky zdatné jedince.

V případě, že by školy distribuovaly mezi učitele notebooky vybavené touto čtečkou, odpadla by potřeba chránit svá data heslem, které může být uhádnuto, či jiným způsobem prolomeno. Čtečka v tomto případě nabízí lepší poměr cena/úroveň zabezpečení nežli standardní zabezpečení pomocí hesla.

6.3 Zabezpečení v místní síti (s operačním systémem Windows)

Když se student či učitel přihlašuje do školní sítě, je vyzván, aby zadal svoje uživatelské jméno a heslo. Po tom co je provedena autentizace a následně i autorizace, je právě tomu jednomu přihlášenému uživateli umožněn přístup a udělena práva k určitým síťovým službám, úložištím a jiným síťovým prvkům. Uživatel je nyní v síti přihlášen s určitými právy, avšak na lokální stanici (počítači u kterého sedí), je přihlášen pouze jako uživatel s omezeným oprávněním (v operačních systémech Windows) [11].

Toto jednoduchá bezpečnostní opatření je velmi důležité pro zachování bezpečnosti lokální pracovní stanice. Z účtu s omezeným přístupem nelze, nebo velmi složitě, instalovat aplikace. Lze do počítače nahrávat pouze specielně upravené tzv. portable aplikace. Díky tomuto faktu se stává pro případného útočníka opět o něco obtížnější infiltrovat, či jiným způsobem napadnout daný systém.

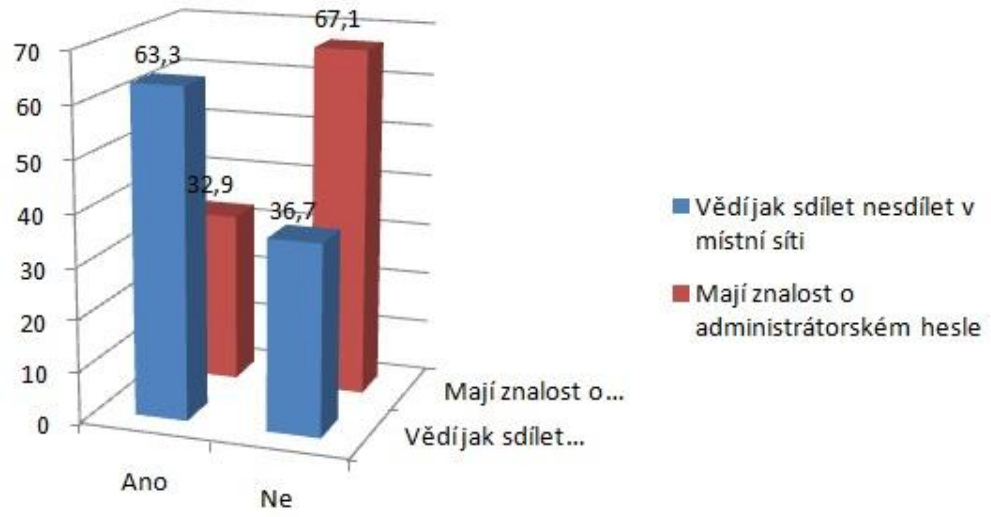
Tento fakt ale nebrání oprávněným uživatelům s počítačem normálně pracovat. Plně přístupné jsou jim složky, jako jsou například dokumenty. Jak jsem zjistil během svých konzultací s odborníky s dlouholetou praxí v oboru, většinou učitelé hesla a přihlašovací jména, která by jím administrátorský přístup do počítače povolila, neznají a znát ani nepotřebují. V případě že je potřeba upravit, doinstalovat, či odinstalovat nějakou aplikaci na lokální pracovní stanici, bývá touto prací pověřen správce sítě, a nevzniká tak potřeba šířit mezi nepověřený personál administrátorská hesla k pracovním stanicím.

Z výše uvedených faktů tedy vyplývá, že v současné době je na českých školách adekvátně dobře zabezpečen uživatelský aspekt místních sítí ve vztahu k bezpečnosti sítě jako celku, jejích uživatelů i dat na ní uložených.

6.3.1 Potenciální nebezpečí práce v síti

Místní síť se stává pro data velmi nebezpečným místem, protože jsou zde téměř všechna zařízení navzájem vidět a není problém, aby mezi sebou komunikovala. Přístup z jedné pracovní stanice k druhé, je rychlý a jednoduchý. Stačí se pouze (v systému Windows) podívat do Míst v síti (speciální složka v systému Windows, ve které se zobrazují ostatní zařízení připojené do stejné sítě) a odtud jsou ostatní počítače vidět jako složky jen čekající na otevření.

Tyto počítače bývají chráněny dvěma nejpoužívanějšími způsoby, kterými jsou ochrana heslem a ochrana odepřením přístupu neautentizovanému a neautorizovanému uživateli (nesdílením). V základním nastavení systému Windows, je povoleno sdílení, které není chráněno heslem (Windows XP) a je také defaultně sdílena složka sdílené dokumenty.



Tento fakt může být velmi nebezpečný. Pokud by totiž náš student učitelství, či snad už učitel, uložil svá data (například test, který chce rozdat někdy žákům) do složky sdílené dokumenty, které se neliší od obyčejné složky dokumenty ničím jiným než slovem "sdílené" v názvu, vzniká nám zde

možnost (pokud jsme připojeni v té samé síti samozřejmě) si bez jakýchkoliv bezpečnostních mechanismů které by nám v tom bránily, data z této složky stáhnout. V případě, že by se této situace rozhodli žáci, kteří mají onen test podstoupit, využít, byla by znehodnocena učitelova práce, kterou odvedl (příprava na výuku, výuka, zkoušení a následné testování výsledků). V případě úniku a využití výše zmíněného testu je zde přítomno nebezpečí, že budou znehodnoceny nejen výsledky testu, ale pokud by test unikl o týden nebo víc dříve nežli by byl test zadán, žáci by mohli věnovat výuce daného tématu mnohem méně pozornosti, právě z důvodu, že již mají k dispozici testové otázky a není tedy pro ně důležité naučit se na test, ale pouze ho vypracovat a otázky si zapamatovat.

Jak naznačuje výše popsaná teoretická situace, nebezpečí vycházející ze sdílení dat, které není chráněno heslem, se prokázala být potenciálně velmi nebezpečnou, zvláště v prostředí jako je školní počítačová síť. A to právě z důvodu, že počítače, na kterých pracují jak učitelé, tak žáci se nachází ve stejné síti a doméně a je tedy možné přistupovat z jednoho počítače nacházejícího se v této síti do počítače jiného, pokud jsou ovšem nějaká data sdílena, a nechráněna heslem. Jak sdílet či nesdílet data na síť [12] by měli znát všichni absolventi středních škol, kteří složili maturitní zkoušku z informatiky. Lze tedy předpokládat, že někteří studenti by byli schopni této potenciální slabiny v zabezpečení využít, nejspíše i ve svůj osobní, či studijní prospěch.

6.3.2 Potenciální výhody práce v síti

Další možností jak se bránit úniku dat na síť, je sdílet pouze to, o čem vím, že by mohlo být veřejně přístupné. Toto se může stát i velmi zajímavým a pro učitele výhodným. Lze totiž studentům poskytnout studijní materiály v digitální podobě skrze sdílení dat v počítačové školní síti. Lze i nastavit různým uživatelům různá oprávnění pro dané složky, a lze tak tedy snadno vytvořit bezpečnou lokaci v síti, odkud si studenti mohou stáhnou materiály ke studiu, či jiná relevantní data, která učitel shledá pro žáky důležitými. Také

lze zřídit odkladiště, kam mohou studenti svoje data nahrávat, čehož lze využít například pro odevzdávání úkolů.

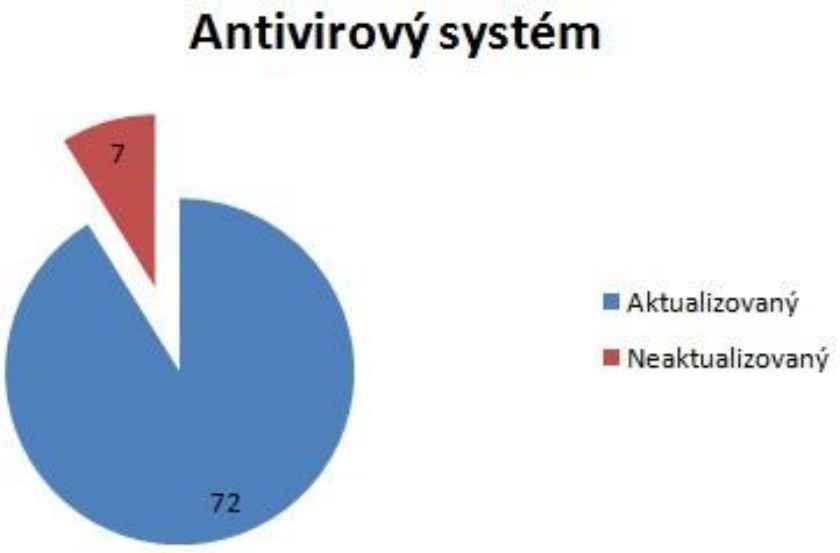
6.5 Aktualizace jako důležitá součást zabezpečení

Ve světě vzájemně propojených zařízení například místní sítí či internetem je velmi důležité bránit se i vnějším hrozbám jako jsou viry, spyware, adware či jiné formy nebezpečných kódů. K šíření potenciálně nebezpečného kódu může sloužit i například přenosné datové úložiště jako je třeba flashdisk, či externí pevný disk, CD, DVD a další datová média. Aby takovéto kódy měly menší šanci se do našeho počítače dostat, je potřeba ho chránit.

6.5.1 Antivirový program

Antivirový program by měl být nedílnou součástí softwarového vybavení každého počítače. Antivirový program však k tomu aby plně využil svého potenciálu detekovat a neutralizovat či jinak zneškodnit škodlivý kód, vyžaduje aktuální databázi obsahující informace jak ten či onen virus najít a zneškodnit. Pokud tato databáze není udržovaná, dochází ke snížení schopnosti detekce nových škodlivých kódů (protože se metody jejich přímé detekce nevyskytují v databázi antiviru a jedinou možností jak je tedy detekovat zůstává heuristická analýza, která není vždy vhodná, viz teoretické pozadí).

Jak dokazuje níže přiložený graf, přibližně 9% dotázaných neví či neaktualizuje svůj antivirový program. Díky tomuto faktu se stává oněch cca. 9% počítačů snadněji napadnutelnými z vnějšku, což může ohrozit



schopnost učitele vykonávat svoje povinnosti. V případě, že byl napaden počítač v místní (například školní síti, neboť tam se budou naši budoucí učitelé vyskytovat) síti, ostatní počítače jsou tím pádem neustále vystaveny kompromitovanému zařízení, které může sloužit jako zadní vrátka pro další infiltraci oné sítě. V tom méně katastrofickém scénáři je pouze práce na infikovaném stroji o něco ztížená, například celkovým zpomalením, vyskakujícími reklamami či jiným druhem projevu nežádoucího kódu.

6.5.2 Operační systém

Operační systém stejně jako jakýkoliv jiný program může obsahovat různé chyby, kterých lze využít k infiltraci zařízení, na kterém je onen systém spuštěn. Tyto díry v kódu se snaží výrobce odstranit tím, že když je chyba odhalena, vydá aktualizaci, která ji opraví. Stejně jako u antivirového systému, i zde je tedy potřeba pravidelně provádět aktualizace.

Jak nám ukazuje přiložený graf, přes 40% studentů učitelství neaktualizuje či neví o tom, jestli jsou u nich na počítači prováděny aktualizace operačního

systému. Toto je velmi alarmující zjištění, neboť potenciální hrozby, které by mohly daný počítač ohrozit, jsou velmi nežádoucí jak pro uživatele počítače, tak pro ostatní zařízení, která se nachází ve stejné síti jako ono zařízení s neaktualizovaným operačním systémem.

Mezi hrozby, které se stávají na počítači, který není aktualizován, patří například větší náchylnost ke kritickým systémovým chybám zapříčiněnými

výjimečným sledem příčin, které se vyskytly v nesprávný čas na nesprávném místě a tak mohly zapříčinit pád systému, protože obsahoval chyby v programování, které toto dovolily. Mezi takovéto chyby můžeme řadit například pád aplikace, či v horším případě celého systému, kvůli špatné komunikaci s ovladačem, špatnému přerozdělení systémových prostředků atd. Je faktem, že těchto chyb s dalšími záplatami operačního systému ubývá. Díky tomu se snižuje i riziko ztráty dat, napadení systému, či například infikování systému virem, který k infiltraci použil chybu v kódu, která mu umožnila se dostat přes bezpečnostní prvky. Je tedy velmi důležité, aby byl systém udržován aktuální.

Z těchto výše uvedených faktů tedy vyplývá, že pokud náš budoucí učitel nebude udržovat svůj systém aktuální, zvyšuje se pravděpodobnost, že se bude muset vypořádávat se vzniklými komplikacemi v systému, což ho samozřejmě stojí určité úsilí, a čas a dokud problém nebude vyřešen (nezíská zpět data, neodstraní viry z počítače a podobně), stává se méně produktivním zaměstnancem.

6.6 Sociální sítě a jejich vliv na učitele

Jak uvádí článek zabývající se problematikou sociálních sítí ve škole, [14] stále více stoupá obliba sociálních sítí a služeb jako je Youtube, Twitter atd. Také stále více žáků již dnes používá chytré mobilní telefony s přístupem na internet a mají tak tedy možnost se často na sociálních sítích vyskytovat. Stále více se však vyskytují názory [15], že používání těchto sítí není z pedagogického hlediska správné z toho důvodu, že žákům klesá prospěch. Z mého dotazníkového průzkumu bylo zjištěno, že přes 90% studentů učitelství má dnes na sociální síti svůj účet a aktivně ho využívá. Proto je potřeba, aby učitel věděl jak se v tomto prostředí pohybovat tak, aby nedošlo k úniku osobních dat, či aby nebyla zneužita nějaká informace, která je na sociální síti sdílena.

Jak již bylo zjištěno při průzkumu, který prováděl Worchestrův polytechnický institut [16], pokud jsme přihlášeni na sociální síti, náš účet lze identifikovat pomocí sady unikátních znaků specifických právě pro náš jeden účet. Tento

identifikační prvek je přenášen spolu s instrukcemi k provedení určité akce, a proto je tedy pro osobu, která zná tento náš identifikační kód, teoreticky možné dohledat jednotlivé aktivity, které byly prováděny právě z onoho jednoho profilu.

V teoretickém případě že by byly tyto údaje využity v neprospěch například učitele, mohly by být použity k cílené reklamě, nebo v horším případě lze tyto informace využít k cílené manipulaci s danou osobou. Pokud by tedy teoreticky například žáci studující předmět u učitele, který by sdílel úplně všechny informace, které nám sociální sítě sdílet dovolují, bylo by pro dané žáky jednodušší ovlivňovat rozhodovací procesy učitele, nebo by například mohli využívat znalostí osobního života učitele k tomu, aby s nimi bylo zacházeno jinak nežli s jeho spolužáky. Dále se zvyšující se znalostí dané osoby se i zvedá pravděpodobnost, že bude uhodnuto heslo. Možnými následky vyzrazení hesla se zabývám výše. Bylo zjištěno po konzultacích s učiteli na středních školách, že převládá mezi učiteli názor, že pokud se učitelé socializují se svými žáky ve větší než malé míře, trpí tím autorita učitele. Protože je autorita velmi důležitou vlastností každého pedagoga, je možné, či dokonce pravděpodobné, že pokud klesne autorita učitele před jeho žáky, tak se učitelova schopnost předat informace dále snižuje. Toto je nežádoucí fakt jak pro žáky, kteří tímto vstřebávají méně informací, tak pro zaměstnavatele, protože klesá efektivita práce zaměstnance.

S odkazem na kapitolu práce číslo 5.1, kde je uvedeno několik případů, které již nastaly v důsledku sdílení nevhodných dat na webu, či sociálních sítích, se již nebudu ve větší míře zabývat možnými důsledky úniku osobních dat či jiných privátních údajů.

6.6.1Současný stav používání sociálních sítí mezi studenty učitelství

V provedeném výzkumu, na který odpovídalo 79 respondentů z Jihočeské Univerzity, se můžeme dozvědět, že přibližně 9% dotázaných studentů nevlastní profil na sociální síti, a nemohou tedy být ohroženi tím, že svoje data boudou sdílet na sociální síti. Jsou však stejně ohroženi pokud svoje data budou sdílet jinde na internetu. Dnes nemusíte svoje fotografie umístit na sociální síť. Stačí je vyvěsit na nějaké službě zabývající se sdílením tohoto typu dat, a napáchaná škoda může být stejná, či možná být velmi podobná.

Nyní se tedy zaměříme na jednotlivé údaje, které byly zjištěny dotazníkovým průzkumem. Jak nám sděluje graf, který máme možnost zde vidět, 75 - 80% dotázaných sdílí svoje místo či datum narození, využívá sociálních sítí ke studiu a organizuje akce. Právě například organizování akcí je sice velmi často využívanou funkcí sociálních sítí, ale lze se takto dozvědět o onom jedinci kdy, kde a dokonce i s kým se bude v určitý čas nalézat, někdy i co tam bude dělat. Díky tomuto faktu se otevírá možnost, že veliké procento učitelů, by mohlo být snadněji nežli normálně (bez sociálních sítí) přistiženo svými žáky na různých akcích. Pokud je například učitel viděn svými žáky na diskotéce, je zde možnost, že bude jeho autorita druhý den zpochybněna před ostatními žáky.

Naopak velkým přínosem by se mohl stát pro budoucího učitele i fakt že sociální sít sám kdysi využíval ke studiu. Nyní by mu tato zkušenost mohla být přínosná, neboť bude mít znalosti nutné k tomu, aby svoje žáky poučil o tom, jak bezpečně na sociální síti sdílet svoje (například i studijní) data pouze s určitým kolektivem, jak zabezpečit skupinu, či jak efektivně a bezpečně pracovat s citlivými daty, jako je například studijní materiál.

Naopak pravidelné sdílení fotek sebe či svých přátel by se mohlo prokázat jako potenciálně velmi nebezpečné. Z výsledků dotazníkového průzkumu vyplývá, že přibližně 20% dotázaných studentů právě svoje fotografie tímto způsobem pravidelně sdílí. Jako potenciální riziko se jeví negativní dopad na autoritu učitele jako člověka vedoucího své žáky. Pokud by tedy byl učitel znám svým studentům i právě ze sociálních sítí jako například mladý člověk, který tráví svůj čas různými volnočasovými aktivitami, mohlo by to mít negativní dopad na vnímání učitele jako autority a tím by byla snížena učitelova schopnost předávat dále informace. Což je například pro zaměstnavatele velmi nežádoucí jev, protože poté není zaměstnanec schopen vykonávat svou práci v rámci svých jinak běžných možností.

Ne příliš potěšujícím z hlediska kompetence studentů učitelství v bezpečnosti na sociálních sítích může být i fakt, že sedm dotázaných (ze 79) sdílí svoje příspěvky na sociální síti veřejně pro všechny, kteří by měli zájem je vidět. Za zmínku však stojí, že například na nejrozšířenější sociální síti Facebook jsou příspěvky daného uživatele od základu označeny jako přístupné pouze pro ty, které má daný uživatel přiřazené ve svém účtu jako přátele a nikomu jinému. Znamená to, že oněch sedm dotázaných muselo samo ručně otevřít nastavení zabezpečení účtu a tam ručně změnit nastavení sdílení svých příspěvků na veřejné. Toto alarmující zjištění, že studenti učitelství sami chtějí, aby jejich osobní data byla viděna všemi, nejen jejich přáteli, může vést k velmi nepříjemným situacím, jako například těm, které jsou popsány v kapitole 5.1.

Zajímavostí je, že v poslední době na sociální síti Facebook někdy mění zásady zabezpečení účtu, což v případě, že nejsou nové změny v zabezpečení

postřehnuty uživatelem, může uživatel ztratit pojem o jejich existenci a tím celkově může klesnout jeho informovanost o aktuálním stavu zabezpečení osobních údajů či jiných citlivých dat na sociální síti.

7. Závěr

7.1 Závěrečné vyhodnocení problematiky, případná doporučení, upozornění na důležité informace

Na závěr této práce bych rád shrnul fakta, závěry, a části práce, které mi připadají nejdůležitější a potenciálně nejvíce ovlivňující osobu učitele.

Velmi důležitým zdrojem informací se v této práci stává teoretická část, můžeme se v ní dočíst o alespoň základních bezpečnostních mechanismech a v ideálním případě by měli alespoň část z toho, co se tam lze dočíst, ovládat právě i studenti učitelství. A to právě proto, aby tyto znalosti mohli předávat dále.

Jako jedním z hlavních částí své práce mohu označit dotazníkový průzkum. Obsahuje velmi zajímavý pohled do českého vysokého pedagogického školství, z pohledu digitální bezpečnosti.

Jak dokazuje analýza dotazníkového průzkumu, situace v naší republice není mezi studenty učitelství, co se znalostí či dodržování bezpečnostních pravidel zrovna ideální. V každé jednotlivé otázce kterou jsem v dotazníku položil, se ukázalo, že jistá (větší nežli zanedbatelná) část studentů ignoruje či neví nějakou část digitální bezpečnosti, kterou by jako budoucí učitel, který bude vzdělávat žáky, měl ovládat.

Velmi zarážející je například údaj, že 70% studentů učitelství vůbec nedisponuje informacemi o administrátorském hesle ve svém počítači. Toto lze považovat za totální ignorování jakýchkoliv bezpečnostních zásad, protože stejně jako osoba vlastnící dům, má k němu i klíč, tak osoba vlastnící počítač má administrátorské heslo. Jeho neznalost je zarážející, nežádoucí, a potenciálně velmi nebezpečná pro uživatele.

Další nepříliš potěšující informací je, že 37% dotázaných studentů neví, jak sdílet či nesdílet data v síti. Vzhledem k faktu, že intranet (místní síť) byl designován především a hlavně pro to, aby se sdílela data, je tento výsledek dotazníkového šetření velmi znepokojivý. Sdílení je mocným nástrojem a v rukou zkušených se může stát velmi užitečným nástrojem, ale také skrývá potenciál být nebezpečným mechanismem, kterým se naše osobní data můžou, například vinou neopatrného zacházení či třeba i jen pouhé neznalosti, dostat do špatných rukou.

Takovýchto zjištění (jak jste se mohli při četbě této práce přesvědčit) bylo učiněno hned několik. Avšak jako jednu z nejtragičtějších, a nejvíce zarážejících odpovědí jsem obdržel na otázku, zda sdílí uživatelé sociálních sítí své příspěvky s veřejností nejen přáteli. Aby někdo sdílel své příspěvky, musí sám toto nastavit ve vlastnostech zabezpečení oné sociální sítě. Je tedy velmi smutné, že vysokoškolští studenti nejenže nevědí, jestli a jaké mají administrátorské heslo (toto je nevědomost), ale oni sami z vlastní iniciativy sdílí potenciálně zneužitelné informace veřejnosti (toto je vlastní vůle, schválně sdílet informace s neznámými osobami).

Jak si sami můžete představit, na základě zjištěných informací, nelze doporučit českým vysokým pedagogickým školám nic jiného, nežli se ve větší míře (nežli je ta stávající) věnovat problematice digitální bezpečnosti. Je třeba se zaměřit na práci nejen s místním počítačem (OS, antivirový systém, hesla, aktualizace atd..), ale i zdůraznit svým žákům (studentům učitelství) jak se chovat v místní síti, jak ji využít ke sdílení či nesdílení dat, a jakým způsobem ji lze využít ve výuce. Také je potřeba se zaměřit na výuku ohledně bezpečnosti v sociálních sítích. Sociální sítě se v dnešní době staly globálně rozšířeným fenoménem a jejich popularita stále roste, je proto nanejvýše žádoucí, aby naše budoucí generace učitelů měla znalosti týkající se bezpečného pohybu a sociálních interakcí právě v prostředí těchto sítí.

Závěrem lze tedy říci, že stav této problematiky u nás, je nepříliš lichotivý, a ve vlastním zájmu případných budoucích zaměstnavatelů (škol, či jiných

pedagogických institucí) by měla být úroveň informovanosti o digitální bezpečnosti zvednuta. Tohoto lze dosáhnout například úpravou osnov vysokých pedagogických škol a fakult, ale například i tak jednoduchým činem, jako je například i osobní vzor. Pokud student učitelství vidí, že jeho vysokoškolský profesor sám tyto zásady dodržuje, dostavuje se u něj, alespoň částečně motivace, dodržovat ty samá bezpečnostní pravidla, jako osoba, co mě vyučuje.

Musíme se tedy všichni snažit udělat z našich studentů učitelství kompetentnější osoby v oboru digitální bezpečnosti proto, aby i naše budoucí generace mohly těžit z informací, které by jim tito vzdělaní učitelé mohli potenciálně někdy v budoucnu předat.

8. Reference

[1]BYRON, Tanya. *Byron review*: *do we have safer children in a digital world*. [online]. 2010 [cit. 2013-02-11]. Dostupné z: http://media.education.gov.uk/assets/files/pdf/d/do%20we%20have%20safer%20children%20in%20a%20digital%20world%202010%20byron%20review.pdf

[2] KRÁL, Mojmír. *Bezpečnost domácího počítače: prakticky a názorně*. 1. vydání. Praha: Grada, 2006, ISBN 80-247-1408-6.

[3] DAIL, Vincent. Biometric fingerprint reader. [online]. 2013 [cit. 2013-04-21]. Dostupné z: http://www.biometric-security-devices.com/biometric-fingerprint-reader.html

[4] Top 7 OS in Czech Republic. STATCOUNTER. [online]. 2014. vyd. [cit. 2013-04-21]. Dostupné z: http://gs.statcounter.com/#os-CZ-monthly-201203-201303

[5] Kaspersky spam report 2014. KASPERSKY LAB. [online]. 2013 [cit. 2013-04-03]. Dostupné z: http://www.kaspersky.com/about/news/spam?time=1362081600

[6] Heuristic Analysis. ESET. [online]. 2014. vyd. [cit. 2013-04-10]. Dostupné z: http://www.eset.com/us/resources/white-papers/Heuristic_Analysis.pdf

[7]Hoax: Co je hoax. DŽUBÁK, Josef. HOAX.CZ. [online]. 2013. vyd. [cit. 2013-04-22]. Dostupné z: http://www.hoax.cz/hoax/co-je-to-hoax

[8]The Whole World (Wide Web) is Watching. In: *National Education Asociation* [online]. 2008. vyd. [cit. 2013-04-11]. Dostupné z: http://www.nea.org/home/12783.htm

[9]A Large-Scale Study of Web Password Habits. In: *Microsoft Corp.* [online]. 2007. vyd. [cit. 2013-04-11]. Dostupné z: http://research.microsoft.com/pubs/74164/www2007.pdf

[11]What is the difference between a domain, a workgroup, and a homegroup. MICROSOFT CORP. [online]. 204. vyd. [cit. 2013-04-14]. Dostupné z: http://windows.microsoft.com/en-sg/windows7/what-is-the-difference-between-a-domain-a-workgroup-and-a-homegroup

[12]Katalog požadavků k maturitě z informatiky. In: [online]. 2010 [cit. 2013-02-11]. Dostupné z: http://www.novamaturita.cz/index.php?id_document=1404034533&at=1

[13]Windows Update. MICROSOFT CORP. [online]. 204. vyd. [cit. 2013-04-16]. Dostupné z: http://windows.microsoft.com/en-US/windows/help/windows-update

[14]Social media. In: Teaching TImes [online]. 2014. vyd. [cit. 2013-04-20]. Dostupné z: http://www.teachingtimes.com/kb/31/social-media.htm

[15]Teachers blame Facebook and Twitter for pupils poor grades. [online]. s. 2 [cit. 2013-04-20]. Dostupné z: http://www.telegraph.co.uk/education/educationnews/8142721/Social-networking-teachers-blame-Facebook-and-Twitter-for-pupils-poor-grades.html

[16]DORSEY, Michael. Online Social Networks Leak Personal Information to Third-Party Tracking Sites. [online]. s. 1 [cit. 2013-04-20]. Dostupné z: http://www.wpi.edu/news/20090/privacy.html

[17]Basic definition of firewall. [online]. [cit. 2013-04-21]. Dostupné z: http://www.chesave.com/2013/03/basic-definition-of-firewall.html#.UXP_2sqbFKo

[18]LIVINGSTONE, Sonia a David R BRAKE. On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications. *Children* [online]. roč. 24, č. 1, s. 75-83 [cit. 2013-04-22]. ISSN 09510605. DOI: 10.1111/j.1099-0860.2009.00243.x. Dostupné z: http://doi.wiley.com/10.1111/j.1099-0860.2009.00243.x

[19]Oxford Dictionaries: Definition of Phishing. [online]. [cit. 2013-04-22]. Dostupné z: http://oxforddictionaries.com/definition/english/phishing

9. Přílohy

9.1 Dotazník - zadání

Kompetence studentů učitelství v IT bezpečnosti

1) *Pohlaví* ☐ *muž* ☐ *žena*

2) *Věk* ☐ *let*

3) *Obor* ☐

4) *Používáš v hesle čísla, diakritiku či Velká písmena (nebo jiné znaky)?* ☐ *Ano* ☐ *Ne*

5) *Archivuješ si v emailu zprávy obsahující Některá z tvých důležitých hesel?* ☐ *Ano* ☐ *Ne*

6) *Používáš na svém PC aktualizovaný Antivir?* ☐ *Ano* ☐ *Ne* ☐ *Nevím*

7) *Aktualizuješ svůj operační systém?* ☐ *Ano* ☐ *Ne* ☐ *Nevím*

8) *Víš jak sdílet/nesdílet soubory v síti?* ☐ *Ano* ☐ *Ne*

9) *Má tvůj Pc na účtu Administrator heslo?* ☐ *Ano* ☐ *Ne* ☐ *Nevím*

10) *Zálohuješ na externí média nebo cloud? Pokud ano, tak kam a jak často?*

☐

11) *Zaškrtni co je pravda (jak se chováš na sociální síti)*

- ☐ *Sdílím datum narození popř. místo narození*
- ☐ *Sdílím svou adresu*
- ☐ *Pravidelně sdílím fotografie sebe, a svých přátel/rodiny*
- ☐ *Sdílím informace o svém osobním životě* (např. poměry, jak pracovní tak osobní)
- ☐ *Sociální síť využívám také jako pracovní/studijní nástroj*
- ☐ *Sociální síť využívám k organizaci setkání, výletů, akcí...* (Popř. využívám online kalendář na sociální síti)
- ☐ *Své příspěvky na sociální síti sdílím nejen přátelům, ale jsou veřejně přístupné.*
- ☐ *Stane se, že si přidám do přátel i někoho koho neznám*
- ☐ *Nemám účet na sociální síti*

12) *Zaškrtni pojmy které znáš, a víš jak se těmto formám útoku bránit*

☐ *Phishing* ☐ *Hoax* ☐ *Spam*

9.2 Dotazník - vyhodnocení

1	2	3	4	5	6	7	8	9	10	10 - čas	11	12
b	21	zš	a	b	a	a	b	a	flash	0.25	a d e f	c
b	26	čj-vv	a	b	a	b	a	a	disk		a e f	b c
b	23	čj-vv	b	b	a	b	a	b	flash		e	c
b	22	čj-vv	a	a	b	a	a	c	disk	3	a d e f	c
b	22	nj-ov	a	b	a	b	b	c	flash, mail	0.25	e	ne
b	25	nj-ov	a	b	a	a	a	c	flash		a c d f	c
a	22	z-ov	a	b	a	a	a	b	ne		i	c
b	23	vv-ov	a	a	a	b	b	b	disk	1	a e f	c
a	23	m-sv	b	a	a	c	b	c	flash	0.25	a b c d f h	c
b	25	aj-ov	a	b	a	b	a	c	disk	3	i	c
b	22	čj-ov	a	b	a	a	a	b	ne		a d e f g h	ne
a	22	ite	a	b	a	a	a	b	disk, pc		e f	a c
a	21	ite	a	b	a	a	a	a	ne		a e f	a c
a	21	ite	a	b	a	a	a	a	ne		a e f	a c
a	21	ite	a	a	a	a	a	b	ne		a b e f	c
b	21	ite	a	b	a	a	a	a	disk	2	a c e f	c
a	20	ite	a	a	a	a	a	b	disk		a e f h	a b c
a	22	ite	a	a	a	c	a	b	disk, flash		f	b c
a	22	ite	a	b	a	a	a	a	cloud, disk, flash		e f h	a b c
b	22	m-it	a	b	a	a	b	b	disk	1	a e f	c
b	21	m-it	a	b	a	a	b	a	ne		a e f	c
a	21	m-it	a	b	a	a	a	a	cloud		a e f	a b c
a	21	ite	a	a	a	b	a	b	disk, dvd		a f	a b c
b	23	tev	a	b	a	b	b	a	C:\	0,5	e	c
b	24	m-it	a	b	a	a	a	b	ne		a e f	c
b	23	m-aj	a	b	a	b	a	b	ne		e	ne
b	23	m-aj	a	b	a	a	a	c	ne		a c d f	c
b	22	m-aj	a	b	a	b	b	c	ne		a d	c
b	23	čj-ov	a	a	a	a	a	a	disk, flash	1	e f	c
b	23	vuz-př	a	b	a	c	b	a	ne		a c d f	c
b	24	čj-ov	a	a	a	a	b	a	flash		a d e f	c
b	22	aj-ov	a	b	a	a	a	a	disk	1	e f	c
b	22	čj-ov	a	b	a	a	b	b	flash		a e f	c
b	23	čj-ov	a	a	a	a	b	a	flash		a e	c
b	23	z-sv	a	b	a	a	a	a	disk		a d e f	c
a	22	nš	a	b	a	a	b	c	flash, disk		a d e f	c
b	22	nš	a	b	a	a	a	b	ne		a e f	c
a	23	pzv	a	a	a	a	b	c	disk	12	a b d e f h	b c
a	24	pev	a	b	a	a	a	b	disk, cd	3	i	c

1	2	3	4	5	6	7	8	9	10	10 - čas	11	12
b	23	aj-fj	a	b	a	a	b	c	flash		a i	c
b	23	aj-fj	a	b	a	b	a	b	ne		a f	c
b	24	an-nj zš	a	a	a	a	b	a	disk, flash		a b c d e f g h	b c
b	24	an-nj zš	b	b	a	c	b	b	ne		i	c
b	23	an-nj	a	b	a	b	b	c	disk, flash	1	a e f	c
b	22	an-nj	b	b	a	a	a	b	disk, flash, dvd		a e f	c
b	22	an-ov	a	b	a	b	a	c	ne		a d e f	c
b	24	aj-ov	a	b	c	a	a	b	ne		a e f	c
a	23	aj-ov	a	b	a	b	a	b	flash		e f	c
b	24		b	b	a	a	b	b	ne		a e f	c
b	26		a	b	a	a	b	b	disk, flash		a e f	b c
b	21		a	b	a	c	a	c	ne		a e f	c
b	21	zš	a	b	a	c	a	c	ne		a c e f	c
b	21	zš	b	b	a	b	b	c	ne		a b c e f	ne
b	22	zš	a	a	a	c	b	c	ne		a b e f	ne
b	21	zš	a	a	c	b	b	c	ne		a c e	ne
b	22	zš	a	a	a	a	a	b	cd		a c	c
b	21	zš	a	b	a	b	b	c	ne		a f	ne
b	21	zš	a	a	a	a	a	a	disk	1	a e f	c
b	21	zš	a	b	a	a	b	c	ne		e f	c
b	21	zš	b	b	a	c	a	b	ne		a c d e	c
a	21	zš	a	b	b	b	a	a	disk		a e f	b c
a	24	zš	a	a	a	a	a	a	ne		a c e f g h	a b c
b	23	aj-nav	b	b	a	c	b	a	disk, flash	0.03	i	b c
a	23	fv-tv	b	b	a	a	b	b	flash		i	c
b	25	aj-nav	a	b	a	b	a	b	disk	3	a f	b c
b	22	z-aj	a	b	a	b	a	a	disk, cd, pc		a b c d e f g h	c
b	22	z-sv	a	b	a	a	a	a	cd, flash		a d f	c
b	22	z-ov	b	b	a	a	a	b	disk		a e f	c
b	22	čj-aj	a	b	a	a	a	c	flash		a e	c
a	24	čj-aj	a	b	a	a	a	a	disk, flash, cd		a d e	a b c
b	23	vv-ov	a	b	a	a	a	a	dvd		a d e	c
b	22	m-ov	a	b	a	c	a	a	disk	12	a e f	c
a	24	m-geog	a	b	b	b	a	b	disk	12	a c d e f g h	b c
b	22	z-aj	a	b	a	b	b	b	unknown	0.25	a e	a c
b	24	m-ch	a	b	b	b	a	b	ne		a e	c
a	23	čj-aj	a	a	c	b	a	c	dvd	1	a b e f	ne
b	23	čj-aj	a	a	a	a	b	a	cd, dvd	6	a c e f	c
b	24	nj-hv	a	b	a	a	a	c	flash		a c e g	c
b	21	pev	a	b	a	a	a	b	ne		f	c