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: 2012

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 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, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích 20. dubna 2012

.....

Jakub Sadil

Anotace

Tato práce pojednává o aktuální situaci mezi studenty učitelství v oboru IT bezpečnosti. Slouží k ucelení pohledu na učitele jako osobu interagující s informačními technologiemi a možnými nebezpečími, která na tuto osobu číhají.

Pomocí dotazníkového průzkumu byla v této práci zjištěna současná míra znalostí a zvyklosti studentů, co se IT bezpečnosti týče. Tato práce, slouží také jako zpráva pro vzdělávací instituce, k lepšímu zhodnocení aktuální kvality výuky IT bezpečnosti či případným úpravám osnov.

Abstract

This work is about a actual situation among rhe pedagogical students in field of IT security. This work is also good for helping us to see the teacher like a person, who is interacting with information technologies, and dealing with dangers, that are awaiting him.

I used a questionary survey to assess a how the pedagogical students are acting in the IT enviroment, and what they know, about IT security. This work can also serce as a report for the educational institutions, for better assesment of quality of IT studies there.

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. Dále děkuji Ing. Pavlu Sadilovi a Mgr. Lence Sadilové.

Obsah

1 Úvod

Tato úvodní kapitola slouží k ucelení náhledu na roli učitele ve výchovném procesu, a upozornit na důležitost jeho znalostí v IT bezpečnosti, pro zdravý vývoj jeho studentů.

Dnes v 21. století se nacházíme v době digitálních technologií. Tyto technologie se nacházejí všude kolem nás a my s nimi přicházíme do kontaktu každý den. Ať už jde o náš mobilní telefon, počítač v práci nebo automobil, který má dnes již nejspíše také v sobě zabudovaný počítač. Nejenže nám tyto technologie náš život v mnohém usnadňují, ale kvůli jejich běžnému výskytu a používání na téměř každodenní bázi, se vystavujeme i mnohým rizikům, která tyto technologie přináší.

Proto je velmi důležité abychom se sami, byť laici, alespoň trochu orientovali v digitálním světě. Základní IT znalosti proto dnes již samozřejmě patří k běžné výbavě mladého člověka. Avšak jak jsem již zmiňoval výše, je potřeba se bránit mnohým nebezpečím, která na nás v digitálním světě číhají, a to zvláště na děti a mládež. A kdo jiný než právě rodiče a učitelé by měli naučit mladého člověka základům v IT bezpečnosti?

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 svůj pohled na roli dospělých v dětském IT světě T.Byron. Zastává názor, že úlohou a zodpovědností dospělého člověka je pomoc dětem zorientovat se v komplikovaném a ne vždy jednoznačném světě digitálních technologií tak, aby se IT svět pro ně stal maximálně bezpečným a neohrožujícím. Učitelé sehrávají významnou roli v duševním, intelektuálním i společenském rozvoji osobnosti mladistvých. Předávají jim nejen své znalosti a zkušenosti, ale zčásti také své postoje k okolnímu světu.

Znalosti dětí školního věku, jejich postoje k informačním technologiím a schopnosti ubránit v digitálním světě své soukromí a to nejen svá data, hesla atd., ale také různé další citlivé 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 také učitelé byli gramotní a znalí alespoň základních postupů, zásad a pravidel, která je potřeba dodržovat, pokud chceme být v digitálním světě v bezpečí.

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

Studium úrovně digitální bezpečnosti, tak je praktikovaná jinde ve světě a její srovnání s Českou republikou nám umožňuje vyhodnotit kvalitu osvěty a výuky v této oblasti v ČR. Přináší porovnání, jaké skutečnosti vedou k únikům dat a s čím se pak následně musíme vypořádávat. Neméně významným přínosem srovnávání se s ostatními zeměmi je také získání nových poznatků a inspirace v tom, co jiné země dělají pro to, aby zvedli úroveň uvědomění o informační bezpečnosti.

2 Cíle práce

Cílem práce je zpráva o stavu informovanosti budoucích učitelů v oblasti IT bezpečnosti, obsahující dotazníkový průzkum provedený mezi studenty učitelství na JČU, zaměřený na jejich konkrétní znalosti a praktické 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 a sloužící k lepší orientaci ve výsledcích a závěrech, které budou z této zprávy vyplývat. Také bude sloužit jako vodítko a zdroj informací pro správnou interpretaci uvedených fakt a závěrů.

Tato zpráva bude k dispozici středním a vysokým školám a jiným vzdělávacím institucím, které by ji mohly případně využít pro optimalizaci výukových a zkouškových procesů u svých studentů. Pokud se tak rozhodnou, mohou díky výsledkům mé práce získat lepší přehled o tom, jakou úroveň mladí učitelé (potenciální budoucí zaměstnanci a nynější studenti) v oboru IT bezpečnosti mají. Školy, jako zaměstnavatelé, tak mají možnost rozšířit si svůj pohled na to, s jakými znalosti a zkušenostmi v oblasti IT bezpečnosti přicházejí nový učitelé. Pedagogicky zaměřené vysoké školy, mohou doplnit své informace o tom, jak kvalitně své žáky vzdělávají právě v oboru digitální bezpečnosti. Což lze mimo jiné použít pro případnou úpravu osnov výuky, či změnu testů zjišťujících informační gramotnost studentů, 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. Rozsáhlou a podrobně zpracovanou zprávu na téma bezpečnosti dětí v digitálním světě a tedy i kompetence, které by měli mít pedagogičtí pracovníci, kteří se o tyto děti starají. Zjistil jsem tak, jak vypadá postoj k digitální bezpečnosti v pedagogickém prostředí jinde ve světě. 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 použiti především při analýze hrozeb jako je spam, hoax či virových hrozeb. Společnost Kaspersky pravidelně vydává velmi podrobné studie, zabývající se především šířením spamu. Tato data byla použita především při sestavování teoretického pozadí.

Velmi praktickým a informacemi nabytým zdrojem se ukázaly 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 práce na této zprávě jsem také nezřídka využíval různé články vydané společností Microsoft, které se týkaly mimo jiné různých aspektů zabezpečení operačního systému.

Dále jsem prostudoval také práci Mgr. Václava Šimandla a Jana Lhotáka, kteří zpracovali zprávu o konkrétním stavu této problematiky v České republice. To mi pomohlo vytvořit si představu, jak bych mohl svou práci koncipovat a jakým směrem by bylo vhodné se zaměřit. Součástí jejich práce

je i velmi zajímavý dotazníkový průzkum a analýza kompetence žáků v oblasti digitální bezpečnosti, což je téma velmi blízké tématu mému. Díky tomu jsem si ujasnil, co se v současnosti od studentů očekává, že budou v oboru digitální bezpečnosti ovládat. Takto zjištěná fakta mě přivedla k tématům, která pokládám za důležitá právě pro vzdělání budoucích učitelů a jejich následné působení na studenty v oblasti bezpečnosti IT.

V průběhu vytváření této práce jsem leckdy potřeboval odbornou radu. Mými poradci se stali Mgr. Šimadl a Ing. František Hodys. Ing. Hodys je odborník s dlouholetou zkušeností učitele informatiky, statistiky a matematiky. Jeho zkušenosti a rady mi byly cenným zdrojem informací a zároveň inspirací při hledání, jakým směrem by se mohl můj výzkum ubírat. Poskytl mi neocenitelný vhled do dané problematiky v současném českém školství.

3.2 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 díky studiu literatury (viz. seznam použité literatury) a osobní zkušenosti pokládám za důležitá, či jiným způsobem ovlivňující problematiku kompetence studentů učitelství v oblasti IT bezpečnosti. Snažil jsem se tak načerpat data, na jejichž základě budu vyvozovat závěry plynoucí z nedodržování či naopak dodržování bezpečnostních zásad a pravidel, která budou dále v mé 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 12 otázek. První 3 otázky byly otázky na pohlaví, obor a věk, abych si byl jist, že data, která z dotazníku získám, jsou opravdu relevantní k tématu (tzn., že další otázky jsou zodpovězeny pouze studenty pedagogických oborů). Z dalších otázek bylo 6 typu ano/ne/nevím. Jedna otázka týkající se zálohování dávala studentům možnost se rozepsat o způsobu, kvalitě, kvantitě či časových intervalech v jakých zálohují.

Dotazník obsahoval i otázku týkající se problematiky sociálních sítí. Tato otázka obsahovala situační podotázky, kde žáci vybírali z modelových situací ty, které sami praktikují na sociálních sítích jako je například Facebook, či Google+. Tuto otázku jsem zvolil záměrně s vědomím, že sociální sítě se stávají velmi rozšířeným fenoménem[18] a jak jsem zjistil při zkoumání článku Davida R. Brakeho, dopad používání sociálních sítí na studenty se stává stále větší a má velký potenciál dalšího růstu. Což znamená, že se učitel bude jistě muset s tímto fenoménem setkat a vypořádat se s případnými riziky, které vyplývají z interakcí na sociálních sítích. Poslední otázka se týká znalosti pojmů jako je Hoax, Spam, či phishing a schopnosti se jevům, které tyto pojmy zastupují, bránit.

Dotazník byl vyplněn 79 studenty z JČU, 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 opisem, neboť dotazníkový průzkum byl prováděn v tištěné podobě. Po zapsání výsledků to tabulkového procesoru Excel, jsem využil různé funkce a filtry, abych byl schopen rychle a efektivně získat potřebná data a hodnoty.

3.3 Tvorba teoretického pozadí

V teoretickém pozadí jsem se snažil osvětlit témata IT bezpečnosti a problémy, se kterými by se mohli velmi často dostat do styku právě studenti učitelství. Jedním z těchto témat jsou například hesla. Právě z důvodu, že se dnešní populace setkává s nějakým typem hesla každý den a to často i ve značné míře. Problematice hesel jsem se rozhodl věnovat například i v kapitole, která se zabývá emailovou komunikací.

Stejnou důležitost přikládám také problematice zálohování, neboť data jsou dnes často ukládána, zpracovávána a uchovávána v elektronické podobě. Jejich ztráta je dnes pokládána za jednu z nejvýznamnějších hrozeb. Pokud o ně z nějakého důvodu přijdeme, je veliká pravděpodobnost, že nebudeme schopni vykonávat svou práci stejně efektivně jako s nimi, nebo že budeme muset věnovat značný čas tomu, abychom ona ztracená data znova vytvořili.

Po konzultacích s výše zmíněnými odborníky jsem se rozhodnul, že jistá mé část práce by měla být věnována také systému Microsoft Windows. S tímto systémem totiž budou často přicházet do styku nejen studenti učitelství, ale i jejich žáci či zaměstnavatelé. Což znamená, že je velmi důležité, aby budoucí pedagogové tyto systémy znali, orientovali se v nich a měli přehled o tom, jaká sebou nesou případná potenciální rizika.

Jistou část teoretického pozadí jsem věnoval i problematice firewallu a antivirového systému. Jsem totiž přesvědčen o tom, že pokud budou dále číst a využívat moji práci, osoby, které nejsou odborníky v IT problematice, je nezbytné, aby byly obeznámeny se základními fakty a zvyklostmi, které se vážou k těmto dvěma systémům ochrany, zajišťujícím různé bezpečnostní aspekty, které jsou velmi důležité pro bezpečné užívání počítače

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

V této části práce jsem se snažil popsat reálné situace, které se týkají zkoumané problematiky jak v ČR. 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 ČR a vyvození případných následků plynoucích z vyhodnocení sebraných dat a konfrontovat výsledky dotazníku s ostatními zjištěnými fakty a daty. Snažil jsem se soustředit především na nejdůležitější a potenciálně nejnebezpečnější části oblasti digitální bezpečnosti, se kterými se s velkou pravděpodobností bude 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, tj. podcení-li ochranu osobních dat. Potenciálně nebezpečné situace byly popsány v kapitole 5.1. Tato kapitola nastiňuje možné důsledky úniku a následného zneužití osobních dat. Věřím, že tím mohu přispět

k pochopení závažnosti hrozícího nebezpečí při nedodržování pravidel digitální bezpečnosti v osobním i profesním životě.

4 Teoretické pozadí

4.1 Počítačová bezpečnost a rizika

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

Vnitřní rizika jsou velmi častým nebezpečím, se kterým se počítače dnes a denně setkávají. Vnitřní hrozby pochází ze situací, které nejsme schopni ovlivnit (hardwarové selhání, výpadek proudu,…) čí od oprávněných uživatelů, kteří svými akcemi neměli původně v úmyslu systém nijak ohrozit a poškodit (neodborná manipulace, nehody,…).

4.2 Hesla

Hesla jsou nedílnou součástí zabezpečení elektronických dat již řadu let. Data, ke kterým chceme umožnit přístup pouze sobě nebo jiným oprávněným osobám jsme navyklí chránit zabezpečovacím heslem. 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 odhadnutelné. Nemělo by se jednat o běžné slovo, jméno či název, ale ani například název uživatelského účtu.

- Je záhodno vyvarovat se používání hesel 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 napsat si heslo například na papírek a ten si viditelně umístit k počítači nebo založit ke svým běžně používaným dokladům. Pokud je heslo skladováno ve formě snadno přístupné ostatním osobám, je možné ho jednoduše získat a zneužít.

- Heslo je potřeba jednou za čas změnit. Toto nové heslo by se však 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, neboť množství možných kombinací je téměř astronomické. [3]

I přes zjevné klady, čtečky otisků prstů nejsou příliš využívány a to především kvůli několika konkrétním 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. Tato kombinace však rázem výhody biometrického zabezpečení smazává, protože heslo lze prolomit snadněji než napodobit biometrický údaj. Z toho důvodu se případný útočník může zaměřit na lehčeji prolomitelné heslo a obejít tak biometrické ověření identity.

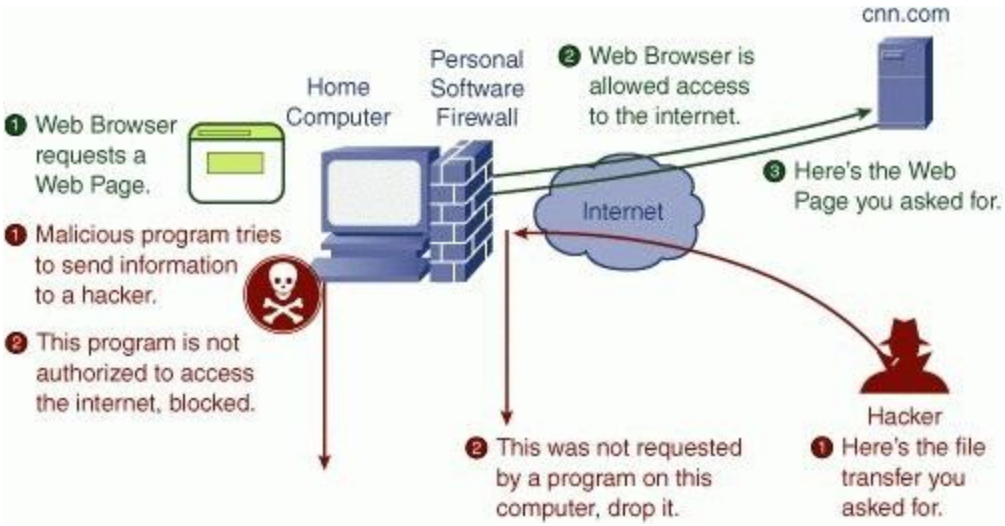
4.4 Zabezpečení v systému Windows

Na systém Windows jsem se rozhodl zaměřit, protože dle statistik je nejpoužívanějším operačním systémem jak v ČR, tak ve 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 používaným systémem Windows se můžeme setkat například s čtečkou otisků prstů.

Účet který je chráněn heslem, nabízí také možnost uložit svá citlivá data do složky Dokumenty, do které mají povolený přístup pouze ty účty, které mají správcem – majitelem nastavená 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.



Obr. 1 - Jak funguje firewall

[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, čímž je nastavena ochrana pro nepovolený přístup.

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 dovybavit. Výjimku tvoří dnes nejnovější operační systém od firmy Microsoft, Windows 8, který nabízí již předem nainstalovaný bezpečnostní balík dříve známý jako Microsoft security Essential. Součástí tohoto bezpečnostního balíčku je právě 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. Povoluje či zakazuje programům, protokolům, či portům atd. přístup z/do počítače. Pokud se neznámý program např. z internetu pokusí kontaktovat náš počítač, firewall se nás nejdříve zeptá, jestli má tomuto programu povolit připojení. Poté jsou nám nabídnuty 2 možnosti jak s žádostí o připojení naložit + možnost si volbu zapamatovat. Připojení od jiného počítače můžeme přijmou - tzn. vystavit se riziku infekce zvnějšku (ale zároveň to znamená povolit programu, co se nás tázal fungovat) anebo odmítnout, což externímu 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 e-mailových zpráv. [5] Spam zahlcuje naše schránky nevyžádanými informacemi a připravuje o náš čas. Zároveň snižuje efektivitu práce, kterou jsme schopni za jednotku času na počítači vykonat. Mezi spam můžeme zařadit například nevyžádané reklamy, pyramidové hry, podvodné loterie, inzerce na neexistující výrobky, různé rafinované žádosti které se z nás snaží vylákat podvodem osobní údaje či rovnou peníze.

Spam se stal velmi obtěžujícím a nebezpečným jevem v dnešním digitálním světě. Je rozesílán většinou ze zotročených (zombie) počítačů. [2] Z obyčejného osobního počítače se může stát počítač rozesílající spam třeba pokud je napaden virem, který je určen k ovládání počítače na dálku či přímo designován k tomu, aby donutil tento infikovaný počítač rozesílat spam. Síť nakažených počítačů jedním druhem viru, který slouží například k rozesílání spamu, či DDOS útokům, se nazývá botnet.

Pokud je Váš počítač napaden takovýmto virem, lze pozorovat pokles v rychlosti reakcí na zadané instrukce, pomalé fungování internetového

připojení. Tyto efekty jsou přímým následkem toho, že infikovaný počítač používá svou výpočetní kapacitu a internetové připojení k rozesílání spamu.

Jak tedy z těchto faktů vyplývá, je potřeba se bránit zahlcení spamem, ale to nejen svou obezřetností, ale i udržováním svého PC v co nejbezpečnějším stavu, (aktualizovaný systém či antivirový program) abychom sami nepřispívali k šíření spamu do digitálního prostoru.

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 nebo jsou namístě vymazány.

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

4.6 Phishing

Pojem phishing popisuje oxfordský slovník,[18] jako posílání emailů, které mají vzbudit dojem, že pochází 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 měli přicházet. To se dá velmi snadno zjistit na oficiálních stránkách dané instituce.

Velmi často se dnes vykytuje i phishing mezi hráči počítačových her. Masové multiplayerové hry, které jsou v dnešní době poměrně rozšířené a často hrané, bývají placené. Proto, pokud hráč vyzradí svoje jméno a heslo a umožní tak přístup další osobě/osobám, může být připraven společností provozující tuto hru 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 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 tím stává stále 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, vysokou spolehlivost a rychlost, se kterou je schopen informace doručit k adresátovi.

Email však představuje i potenciální riziko. S emailovou zprávou může být doručena příloha, která obsahující 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.

Mimo Českou republiku se odehrálo již několik případů, kdy učitelé doplatili na neznalost či nedodržování bezpečnostních pravidel, která by měly osoby využívající informační technologie nebo osoby s nimi nějakým jiným způsobem interagující znát a mít na paměti.

Dále uvedu několik modelových příkladů, které nám pomohou získat podvědomí o tom, jaké situace již vznikly a jaké byly jejich konkrétní následky. Tyto situace zveřejnila mezinárodní vzdělávací asociace.[8]

- V roce 1974 v Kalifornii byl propuštěn 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 svoji intimní fotku volně 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 své úvahy o sexu, drogách a vlastních depresích.

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

5.2 Jak vypadá situace ve školství a digitální bezpečnosti ve světě

Jak uvádí profesorka Tanya Byron ve svém výzkumu[1], 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, že byly podstoupeny kroky vedoucí k osvětě a pozvednutí znalostí, z oboru informační bezpečnosti.

Ve Velké Británii byla dokonce v roce 2009 spuštěna informační kampaň mající za účel veřejnost informovat o nebezpečích číhajících v digitálním světě a způsobech jak se 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 důležité jsou nejen teoretické znalosti učitele a jeho deklarovaný postoj k problematice digitální bezpečnosti a ochrany dat, ale také jeho praktický osobní příklad. 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 zaznamenat, nějakým způsobem je uschovat, zálohovat či jinak zabezpečit proti možnosti 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 věku využívá průměrně kolem pěti až šesti různých hesel.

6 Čeští studenti učitelství a digitální bezpečnost

Jsem přesvědčen, že si české školy uvědomují rizika spojená s používáním informačních technologií snaží se prosazovat politiku informační bezpečnosti a předcházet tak problémům plynoucím z neznalosti fungování digitálního prostředí. Zaměřím se proto na ty aspekty bezpečnosti, které pokládám za podstatné a schopné ovlivnit pracovní i osobní poměry studenta učitelství a potažmo budoucího pedagoga. V této kapitole budu prezentovat fakta a závěry, které vyplývají z provedeného výzkumu, pocházejí z konfrontace dotazníku s teoretickým pozadím či konzultací s odborníky.

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 i velká písmena, jak dokazují data, která jsem nasbíral ve svém průzkumu. 87% dotázaných tedy udělalo alespoň první krok vstříc bezpečnějšímu heslu.

Obr. 2 - Grafické znázornění počtu studentů, kteří používají speciální znaky, velká písmena, či diakritiku v heslech

Tento fakt je velmi důležitý, neboť se tím snižuje pravděpodobnost, že data chráněná takto utvořeným heslem budou úspěšně napadena V zásadě zde také vzniká důležitý předpoklad pro to, aby se budoucí učitel mohl stát vzorem pro své studenty tím, že doopravdy používá to, co bude své žáky učit a také od nich vyžadovat. Nelze proto opomenout 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 odhalení správně vytvořeného 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. Stejně tak se významně snižuje možnost uhádnutí hesla. 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

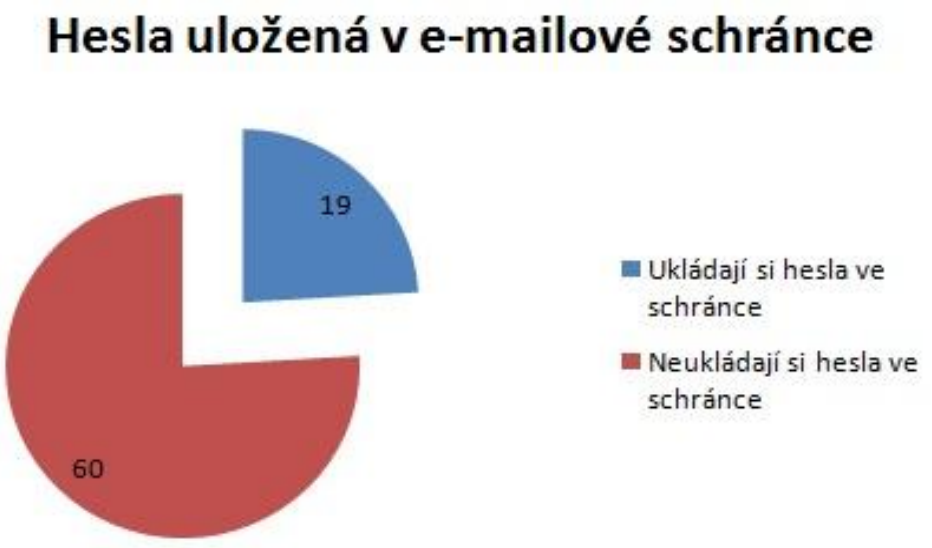
Díky výše uvedenému faktu, že průměrný člověk používá pět až šest hesel, se již dostavuje potřeba svoje hesla někde skladovat, aby tím byla snížena pravděpodobnost, že heslo bude zapomenuto a data či služby, které toto heslo chránilo, se stanou nepřístupnými.

Jedním z míst, kde lze hesla skladovat v domnění, že jsou zde bezpečná, se může jevit naše emailová schránka. Tento trend, uchovávat svá hesla v emailové schránce se začal pomalu rozšiřovat s masivnějším nástupem internetu do domácností. Pokud se tak uživatel zaregistruje třeba na diskusní internetové fórum, přihlásí se k používání nějaké online služby nebo jen hraní online hry, zadává vždy svoji emailovou adresu a s emailem potvrzujícím registraci ke zvolené službě, povětšinou přichází i původně zadané registrační – přístupové údaje a zvolené heslo, 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 svoji emailovou adresu i v hlubinách internetu právě k registracím na služby odesílající zpět email s registračními údaji, vystavuje se tak riziku, že v případě, že se někomu podaří dostat dovnitř jeho emailové schránky, mohou být hesla v ní uložená zkompromitována a zneužita, stejně jako i relevantně velká část účtů tato hesla využívajících.

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

V případě, že hodláme 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. [2]



Obr. 3 - Graf znázorňující kolik studentů učitelství si uchovává svá hesla v emailové schránce

Jednou z možností jak lépe chránit svoje přístupová hesla je používat svoji paměť a neskladovat je v elektronické podobě či na dobře přístupných místech. Za bezpečné heslo lze považovat pouze to heslo, které není nikde zaznamenáno, pouze v naší vlastní paměti. (Pokud se však přesto rozhodnete skladovat svoje hesla v elektronické podobě, lze použít například různé šifrovací algoritmy a svoje hesla zálohovat například na nepoužívaný nebo k tomuto důvodu koupený flashdisk či jiné relativně spolehlivé médium). Také lze uzamknout svoje hesla (spolu s jinými cennými věcmi, kterými můžeme disponovat) na bezpečné místo (trezor).

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 možné neopatrného člověka velmi lehce zdiskreditovat nebo jiným způsobem narušit její soukromý či profesní život.

6.2 Otisk prstu místo hesla

S rozvojem informačních technologií se začalo rozšiřovat používání přenosných počítačů neboli notebooků. 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 jednoduché bezpečnostní opatření je velmi důležité pro zachování bezpečnosti lokální pracovní stanice. Z účtu s omezeným přístupem nelze vůbec, 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, nebo 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.

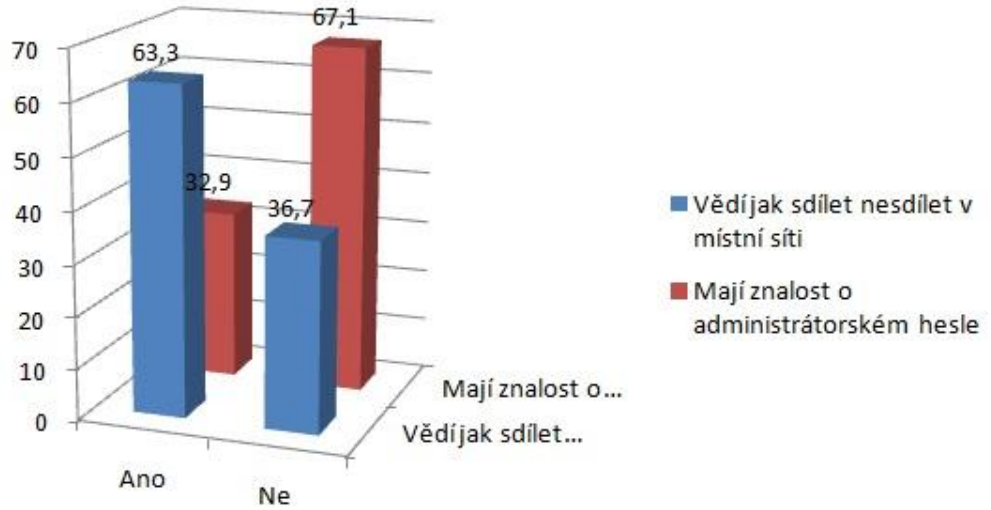
Z výše uvedených faktů tedy vyplývá, že v současné době je na českých školách adekvátně dobře zabezpečen uživatelský aspekt místních sítí ve vztahu k bezpečnosti sítě jako celku, jejích uživatelů i dat na ní uložených.

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 pouze (v systému Windows) kouknout 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 učitel, uložil svá data



Obr. 4 - Graf znázorňující procentuální vyjádření dat získaných z dotazníku, ohledně sdílení dat v síti a administrátorských hesel

(například test který chce rozdat 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 bránili, data z této složky stáhnout. V případě že by se této situace rozhodli žáci 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 probíranou látku, ale pouze zapamatovat si získané otázky a odpovědi.

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

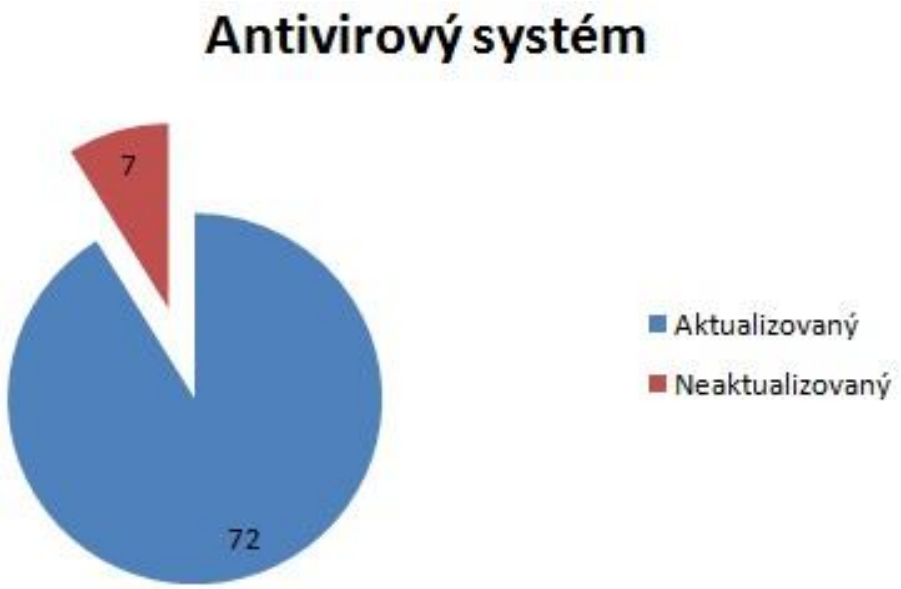
Další možností jak se bránit úniku dat na síť, je sdílet pouze to, o čem vím, že by mohlo být veřejně přístupné. Toto se může stát i velmi zajímavým a pro učitele výhodným. Nabízí to možnost učiteli jednoduše poskytnout studentům studijní materiály v digitální podobě, skrze sdílení dat v počítačové školní síti. Lze také nastavit různým uživatelům různá oprávnění pro dané složky a tímto způsobem snadno vytvořit bezpečnou lokaci v síti, odkud si studenti mohou stáhnout materiály ke studiu či jiná relevantní data, jež učitel shledá pro žáky důležitými. Další variantou je zřídit odkladiště, kam mohou studenti svoje data nahrávat, čehož lze využít například pro odevzdávání úkolů.

6.4 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 například přenosné datové úložiště jako je třeba flashdisk, nebo externí pevný disk, CD, DVD a další datová média. Aby takovéto kódy měly menší šanci se do našeho počítače dostat, je potřeba ho chránit.

6.4.1 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 nebo 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).



Obr. 5 - Graf znázorňující kolik studentů učitelství aktualizuje svůj antivirový systém

Jak dokazuje přiložený graf, přibližně 9% dotázaných 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 síti (především školní síti, neboť tam se budou testovaní budoucí učitelé vyskytovat), ostatní počítače jsou tím pádem neustále vystaveny kompromitovanému zařízení, které může sloužit jako zadní vrátka pro další infiltraci oné sítě. V méně katastrofickém scénáři je pouze práce na infikovaném stroji o něco stižená, například celkovým zpomalením, vyskakujícími reklamami či jiným druhem projevu nežádoucího kódu.

6.4.2 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

Obr. 6 - Grafické znázornění aktuálnosti operačních systémů studentů učitelství

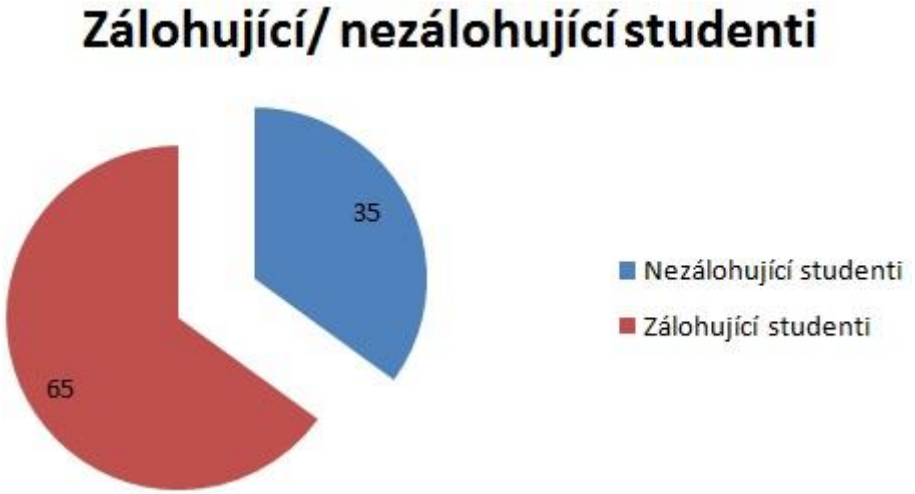
systému. Toto je velmi alarmující zjištění, neboť potenciální hrozby, které by mohly daný počítač ohrozit jsou velmi nežádoucí jak pro uživatele počítače, tak pro ostatní zařízení která se nachází ve stejné síti jako ono zařízení s neaktualizovaným operačním systémem.

Mezi hrozby, které se stávají na počítači, který není aktualizován aktuálními, patří například větší náchylnost ke kritickým systémovým chybám zapříčiněným výjimečným sledem příčin, které se vyskytly v nesprávný čas na nesprávném místě a tak mohly způsobit 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, nebo infikování systému virem, který k infiltraci použil chybu v kódu, jež 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 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 i čas a dokud problém nebude vyřešen (nezíská zpět data, neodstraní viry z počítače a podobně) stává se méně produktivním zaměstnancem.

6.5 Zálohování a studenti učitelství

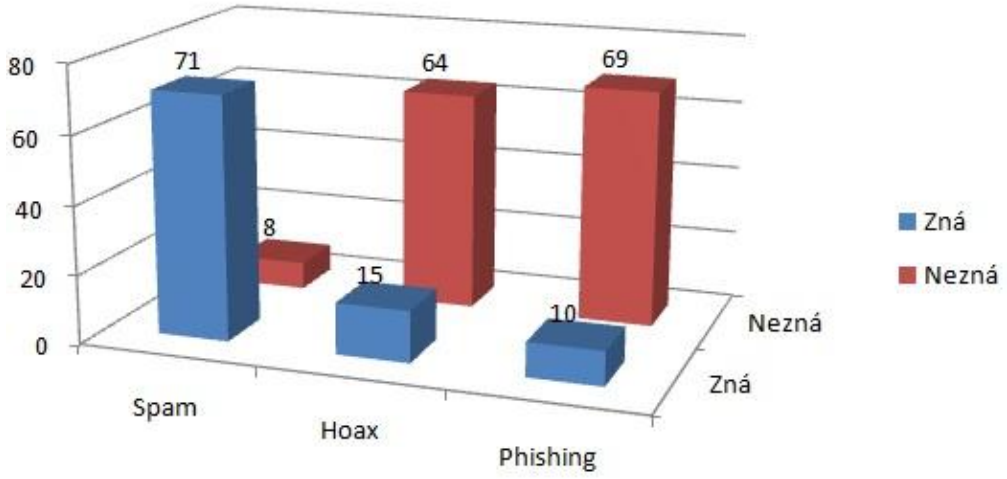
Z výsledků získaných z dotazníkového průzkumu, bylo zjištěno, že 35% dotázaných, svá data nezálohuje žádným způsobem. K totální ztrátě dat, tak může dojít například při selhání pevného disku, krádeže či mechanického poškození disku, či jiného skladovacího zařízení.



Obr. 7 - Procentuelní zobrazení zálohujících studentů učitelství

Dále bylo zjištěno, že 30% dotázaných studentů učitelství svá data zálohuje na externí harddisk, či paměť typu flash. Tyto metody zálohování nabízí osobě (v tomto případě naším studentům učitelství) dlouhodobé, odolné a snadno přenositelné. Díky tomu, hrozí menší nebezpečí, že během jedné události, která nás donutí zálohu použít (ztráta originálních dat) budou zasažena i data zálohovaná. Například při požáru, je možné, že flashdisk bude mít člověk u sebe, nebo například při přepětí v síti, že nebude zrovna zapojen atd... Proto je tento způsob zálohování výhodnější, nežli například zálohování dat, do stejného počítače, i když na jinou diskovou jednotku.

Dále bylo v dotazníkovém průzkumu zjištěno, že 13% studentů učitelství stále používá k zálohování CD či DVD disky. Tyto disky mají vůči moderním metodám úschovy dat hned několik nevýhod. Tou hlavní je, že v případě špatného skladování, či už například i lehčího mechanického poškození, může dojít k téměř celkové ztrátě skladovaných dat. Další nevýhodou je také omezená životnost těchto disků. Nelze proto tento způsob zálohování doporučit. Dokonce v případě skladování většího množství dat, mohou být i náklady na nákup těchto, většinou nepřepisovatelných disků vyšší, nežli v případě využití cloudového úložiště, flash disku či externího HDD.



Obr. 8- Výsledné odpovědi z dotazníku na téma znalostí daných pojmů

6.6 Studenti a Spam, Phishing a Hoax

Z přiloženého grafu lze vyčíst, že 71 ze 79 dotázaných, zná, a ví jak se bránit spamu. To je potěšující zjištění, neboť jak je uvedeno výše, (kapitola 4.5) tak

spam tvoří 71% celkového objemu internetové pošty. Lze proto bez problémů předpokládat, že se s ní náš budoucí potencionální učitel setká.

Nepříliš podobné znalosti, však dnešní studenti učitelství mají, co se týče Hoaxu, či Phishingu. (kapitoly 4.6 a 4.7) pouze 15 ze 79 dotázaných odpovědělo kladně na otázku, zda vědí co je Hoax, a jak se mu bránit. Na stejnou otázku, ale týkající se Phishingu odpovědělo kladně pouze 10 dotázaných.

Zajímavostí je, že přibližně 40% dotázaných studentů, kteří studují informační technologie, (ať už jako obor v učitelském, či neučitelském studiu) zná více nežli jeden pojem najednou, ne pouze spam. Jak můžete vidět na grafu nahoře, většinou byl znám většinou pouze jeden pojem, a tím je právě spam.

Lepší přehled o pojmech Phishing, Hoax a Spam, najdete ve výše zmíněných kapitolách.

6.7 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 čím dál tím víc žáků používá chytré mobilní telefony s přístupem na internet a mají tak 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. Přesto však bylo mým dotazníkovým průzkumem zjištěno že přes 90% studentů učitelství, má dnes na sociální síti účet a aktivně ho využívá. Z tohoto důvodu je potřeba aby učitel věděl jak se v tomto prostředí pohybovat tak, aby nedošlo k úniku osobních dat či aby nebyly zneužity informace, které jsou na sociální síti sdíleny.

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 žáci studující u učitele, který by sdílel úplně všechny informace, které nám sociální sítě sdílet dovolují, měli přístup k těmto informacím, bylo by pro ně snadnější ovlivňovat rozhodovací procesy učitele. Také by třeba mohli využívat znalostí osobního života učitele k tomu, aby s nimi bylo zacházeno jinak nežli s jeho spolužáky.

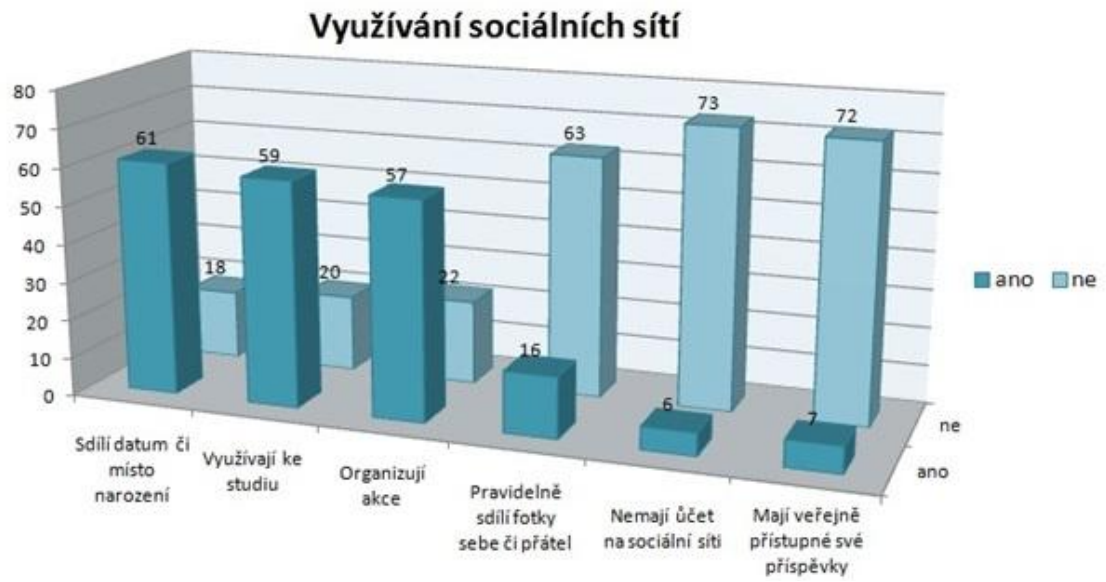
Se zvyšujícím se počtem informací o osobě, která tato data zveřejňuje, se také zvedá pravděpodobnost, že bude uhodnuto její heslo. Možnými následky vyzrazení hesla se zabývám výše.

Bylo zjištěno, po konzultacích s učiteli na středních školách, zde převládá názor, že pokud se učitelé stýkají na sociálních sítích 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 pedagogicky působit 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.

6.7.1Současný 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 jejich sdílením. 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



Obr. 9 - Otázky týkající se aktivit studentů učitelství na sociálních sítích

může být stejná, nebo velmi podobná.

Nyní se tedy zaměříme na jednotlivé údaje, které byly zjištěny dotazníkovým průzkumem. Jak nám sděluje graf, který máme možnost zde vidět, 77% dotázaných sdílí svoje místo či datum narození, využívá sociálních sítí ke studiu a veřejně 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. Popřípadě také co tam bude dělat. Díky tomuto faktu se zde otevírá možnost, že veliké procento učitelů, by mohlo být snadněji nežli normálně (bez sociálních sítí) sledováno svými žáky na různých akcích a jejich soukromý

život by se tak mohl stát veřejným školním tématem a jejich autorita zpochybněna před ostatními žáky.

Naopak velkým přínosem, by mohl pro budoucího učitele být fakt, že se orientuje v prostoru sociálních sítí a je schopen žákům nabídnout alternativu jejich využití například ke studiu. Tyty zkušenosti mohou být motivující a přínosné, neboť jako učitel bude mít dostatek znalostí a zkušeností potřebných k tomu, aby mohl mezi studenty důvěryhodně a efektivně poučit o tom, jak se bezpečně pohybovat na tomto území, jak na sociální síti sdílet svoje data (například i studijní) pouze s určitým kolektivem, jak zabezpečit skupinu či jak efektivně a bezpečně pracovat s citlivými údaji.

Nutno však také zmínit, že 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 pedagogicky působícího na žáky.

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 příteli, 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 provozovatel občas 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.

Jedním z hlavních zdrojů informací týkajících kompetencí studentů učitelství v oblasti digitální bezpečnosti je v této práci její teoretická část. V ní je možné se dočíst o základních bezpečnostních mechanismech a ochranný prvcích, které by v ideálním případě měli alespoň části ovládat, právě studenti učitelství. A to právě pro to, aby tyto znalosti mohli sami efektivně využívat a svým příkladem předávat dále.

Další zásadní částí mé práce je 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 nezná nějakou část oblasti digitální bezpečnosti, kterou by jako budoucí učitel, který bude vzdělávat žáky, měl ovládat.

Zarážející je například údaj, že 70% studentů učitelství vůbec nedisponuje informacemi o administrátorském hesle ve svém počítači. Toto lze považovat za velmi nežádoucí, protože administrátorské heslo nám dává téměř plný přístup k našemu počítači. Jeho neznalost je proto z tohoto důvodu zarážející, nežádoucí a potenciálně velmi nebezpečná pro uživatele.

Další, nepříliš potěšující informací je, že 37% dotázaných studentů, neví jak bezpečně sdílet či vůbec 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, ale také v sobě 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. Lze například zmínit to, že někteří studenti učitelství, jsou ochotni sdílet svoje osobní informace na sociálních sítích i s neznámou a nekonkrétní veřejností. Jakýkoliv únik či zveřejnění osobních informací, je nežádoucím jevem, a je proto potřeba, aby naši budoucí učitelé zacházeli co nejopatrněji se svými osobními údaji. Jednoho dne, totiž budou pověřeni správou osobních údajů nejen svých, ale i svých studentů. Jejich zodpovědností bude tyto údaje nejen chránit, ale také naučit své žáky, jak by si sami měli svá osobní data spravovat a chránit.

Jak si sami můžete představit, na základě zjištěných informací, nelze doporučit českým vysokým pedagogickým školám nic jiného, nežli se ve větší míře věnovat problematice digitální bezpečnosti. Je třeba se zaměřit na práci nejen s místním počítačem (OS, antivirový systém, hesla, aktualizace atd..), ale také klást důraz na zodpovědné chování v místní síti, dostatek informací o možnostech jejího využití ke sdílení či nesdílení dat a jejím dalším možném využití při 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.

Je ve vlastním zájmu případných budoucích zaměstnavatelů (škol, či jiných pedagogických institucí), aby úroveň informovanosti o digitální bezpečnosti byla zvednuta. Tohoto lze dosáhnout například úpravou osnov vysokých pedagogických škol a fakult, ale i tak jednoduchým činem, jako je osobní vzor. Pokud student učitelství vidí, že jeho vysokoškolský profesor sám tyto

zásady dodržuje, dostavuje se u něj, alespoň částečně motivace, dodržovat ta samá bezpečnostní pravidla, jako člověk, který je mu příkladem a autoritou.

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

8 Klíčová slova

Klíčová slova: Vzdělávání, bezpečnost, informační technologie, studium, vysoká škola, kompetence, studenti

Keywords: Education, security, information technologies, studies, university, competency, students

9 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

10 Přílohy

10.1 Dozazník

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*