Západočeská univerzita v Plzni

FAKULTA PEDAGOGICKÁ

BAKALÁŘSKÁ PRÁCE

VÝUKOVÝ ELEKTRONICKÝ MATERIÁL - POČÍTAČOVÁ INFILTRACE A ZPŮSOBY OCHRANY

Lukáš Franc

Plzeň 2012

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 29. června 2012

……

vlastnoruční podpis

OBSAH

1 ÚVOD

Náplní této bakalářské práce je vytvoření elektronického kurzu na téma Počítačová infiltrace a způsoby ochrany v autorském sytému ProAuthor. Tento elektronický kurz bude nadále sloužit studentům Západočeské univerzity v Plzni, jako výukový materiál.

Toto téma bakalářské práce jsem si vybral proto, že jsem se s ním setkal přímo při studiu předmětu Úvod do informatiky na katedře výpočetní a didaktické techniky v rámci psaní seminární práce. Již při vypracovávání semestrální úlohy mě téma velice zaujalo a chtěl jsem se o něj dále zajímat. Dalším důvodem, proč jsem si vybral toto téma bakalářské práce, byla možnost vytvoření elektronického kurzu.

V dnešní době, kdy je stále více rozvíjeno distanční studium na všech univerzitách, je neustále kladen velký důraz na podporu studentů této formy studia studijními materiály. Velmi rozšířenou formou distanční výuky bývají právě elektronické kurzy. Elektronické kurzy ovšem nemusí sloužit pouze jako podpora pro distanční studium, ale lze je uplatnit i při výuce v prezenčním studiu. Elektronické kurzy jsou elektronickými knihami podobající se klasickým tištěným učebnicím a mají oproti nim spoustu výhod. Jednou z výhod je, že jsou většinou pro studenty daného předmětu zdarma. To je první a velice důležitý faktor, který studentům napomůže přístup k určitým informacím. Další z výhod je, že student nemusí být v neustálém kontaktu s vyučujícím. Své nově získané znalosti si student může následně ověřit v různých úkolech a cvičeních, nebo v testech a autotestech.

Tato textová část je popisem vytváření tohoto kurzu. Zejména se jedná o popis programů, které byly při vytváření kurzu použity. Dále jak bylo postupováno u vytváření studijních článků a nakonec, popis jednotlivých studijních článků a cvičení vytvořených v rámci kurzu.

2 POUŽITÝ SOFTWARE PRO TVORBU KURZU

Při tvorbě e-kurzu Počítačová infiltrace a způsoby ochrany bylo použito několik programů. Mezi tyto programy patří:

- autorský systém ProAuthor,
- Cmap Tools,
- Gimp,
- Macromedia Captivate,
- Microsoft Word 2007,
- operační systém Windows XP Profesional.

Bez těchto programů by e-kurz nemohl vzniknout, a proto je příhodné jejich popsání a vysvětlení jakým způsobem přispěly k vytvoření celého kurzu.

2.1 PROAUTHOR

V dnešní době, kdy se klade velký důraz na kvalitní výuku a podporu studentů, kteří studují jak distanční tak prezenční formou studia, studijními materiály, byl na Západočeské univerzitě v Plzni, panem doc. Ing. Janem Hánem, Ph.D., vyvinut autorský systém ProAuthor. Tento software slouží pro podporu e-learningového vzdělávání a hlavně k vytváření elektronických studijních materiálů, které se mohou publikovat například na serverech pro distanční vzdělávání ve specifickém výstupním formátu do prostředí LMS (Learning Management System). Důležité je uvést, že e-learningové kurzy nejsou jediným výstupem tohoto autorského systému. Dalším z možných výstupů mohou být například vytvoření výukového CD, diskuzí nebo anket. (1)

S tímto softwarem se mohou studenti setkat při studiu předmětu Programování v aplikacích na katedře výpočetní a didaktické techniky, ale také při výuce mnoha dalších předmětů na celé univerzitě. Předmět Programování v aplikacích je uveden záměrně, protože jednou z podmínek úspěšného absolvování tohoto předmětu, je vytvoření dvou studijních článků právě v autorském systému ProAuthor.

2.1.1 POPIS PROGRAMU

Tento program byl hlavním stavebním kamenem při tvorbě e-kurzu. Pro vytvoření e-kurzu byla použita verze programu 6.5.7., která byla použita z důvodu ještě nestabilní nové verze a již jednou nainstalovaného programu při studiu výše zmíněného předmětu Programování v aplikacích, kdy byla tato verze nainstalována na počítačích ve školních učebnách. Dalším důvodem, proč byla použita tato verze, byla i dohoda s vedoucím práce. V následujících řádcích bude podrobněji tento program popsán, hlavně ty části, které byly při vytváření kurzu nejvíce používány.

Výstupem celého programu je elektronická učebnice. Tato učebnice se skládá ze vstupní stránky, která obsahuje název kurzu, jména autorů, či obtížnost kurzu, kterou si může student zvolit. Ze vstupního menu má student na výběr obtížnosti Základní, Středně pokročilý a Pokročilý. Není podmínkou, aby kurz obsahoval všechny tři obtížnosti. Záleží na typu kurzu a hlavně na autorovi, který kurz vytváří. Důležité je, aby student byl, ještě než otevře kurz, obeznámen s tím, jak je kurz náročný

Obrázek 1 Vstupní menu e-kurzu

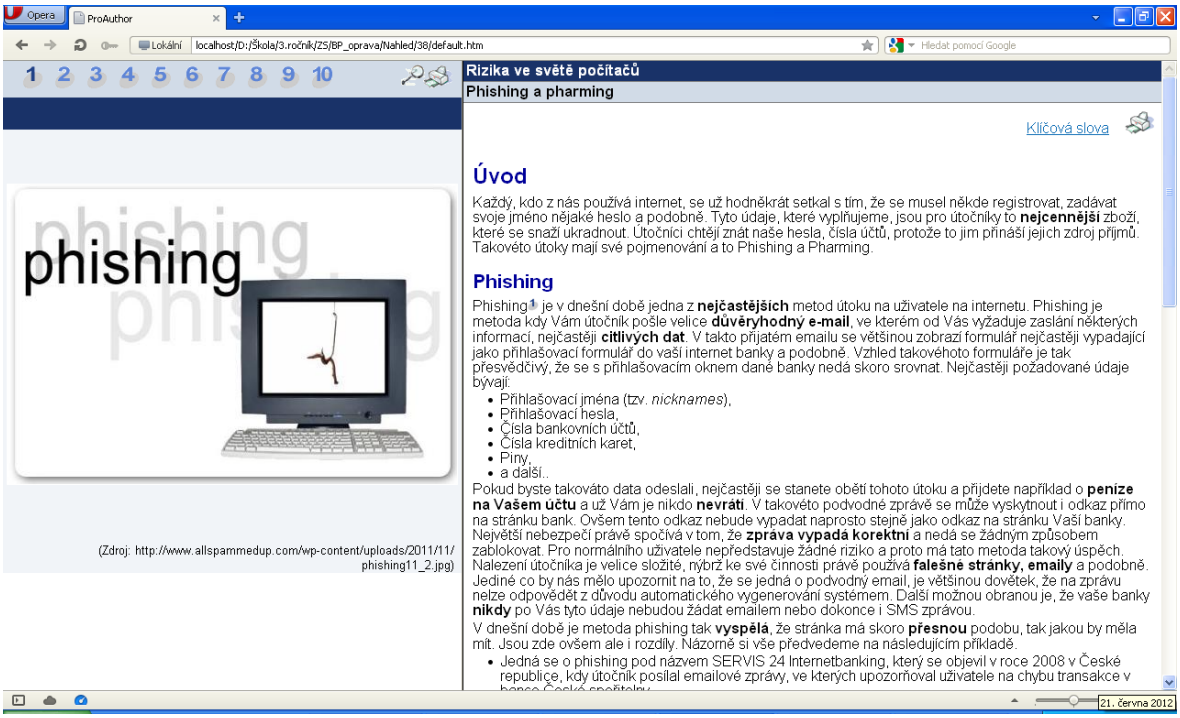
Každá úroveň obtížnosti představuje rozsáhlost a obtížnost kurzu. Obtížnost základní představuje pro studenta, podle rozsahu získaných znalostí po skončení kurzu, základní seznámení s problematikou daného tématu. Středně pokročilý rozšiřuje obtížnost začátečník a student by na konci kurzu už měl být schopen o daném tématu vést delší rozpravu. Obtížnost pokročilý předpokládá, že student již má předešlé znalosti daného tématu, což nemusí být pravidlem, a po prostudování obsahu se ve svých znalostech utvrdí a popřípadě je obohatí.

Po zvolení obtížnosti se studentovi zobrazí obsah kurzu, který je rozdělen na kapitoly obsahující studijní články, úkoly, cvičení, testy, autotesty a popřípadě i diskuze. Po vybrání kapitoly a například studijního článku je vždy student seznámen, co je obsahem studijního článku, jak přibližně dlouho by mělo studium daného studijního článku trvat a jakých dovedností nebo znalostí by měl po prostudování obsahu dosáhnout.

Obrázek 2 Úvodní text a cíle studijního článku

Učiteli, který bude danou problematiku studijního článku přednášet, je zobrazeno, na co si má dát při výuce pozor, či jak výuku obohatit, nebo nad čím by se měl se studenty zastavit a vést s nimi diskuzi.

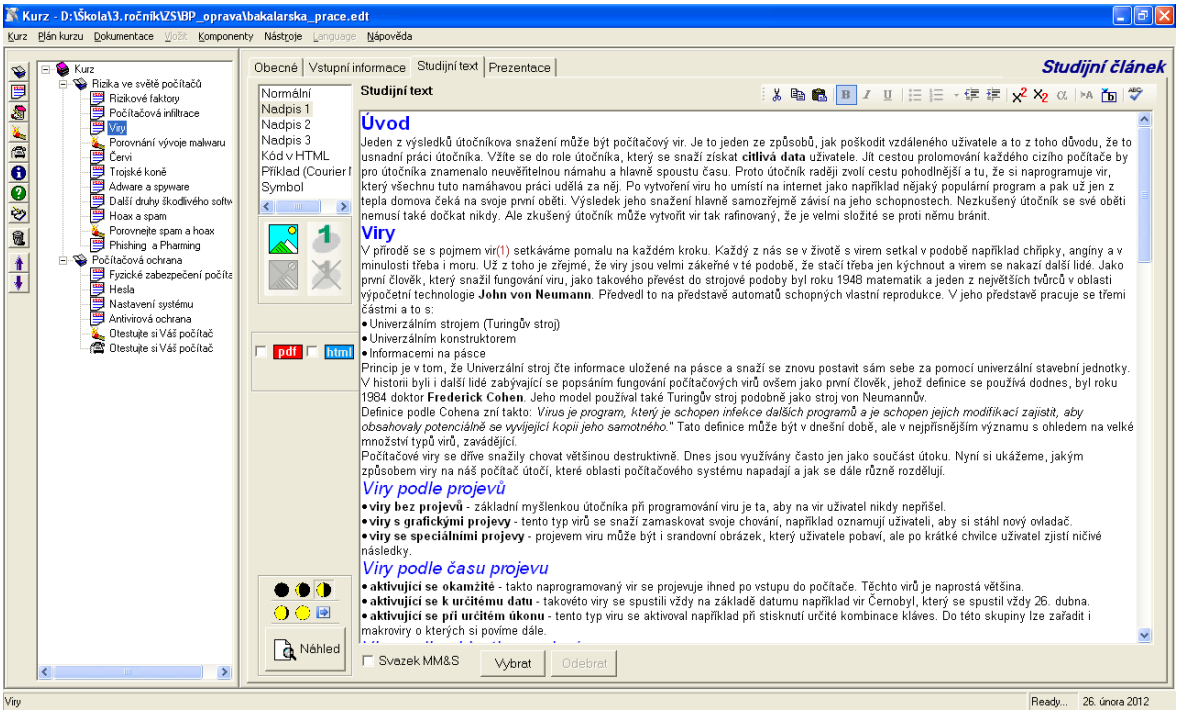
Po zvolení studijního článku se studentovi zobrazí okno, které většinou bývá rozděleno na dvě části. V jeho pravé části bývá text ke studiu a v části levé, podpůrný,



Obrázek 3 Ukázka studijního článku

materiál. Dále má student možnost si studijní články vytisknout a učit se z nich, pokud zrovna nebude mít možnost mít u sebe počítač.

To, co je výstupem celého kurzu, musí být také někde vytvořeno a k tomu slouží vývojové prostředí ProAuthor. Prostředí programu je rozděleno také na dvě části. V levé časti, máme zobrazenou strukturu kurzu s panelem, na kterém jsou umístěna tlačítka pro vkládání nových kapitol, studijních článků, úkolů, cvičení, diskuzí, autotestů, testů, anket. Dále pak tlačítko pro smazání aktivity a dvě tlačítka pro přesun aktivit. Pravá část obsahuje vždy ke každé komponentě záložky, do kterých se vkládají vstupní data. Každá komponenta vždy obsahuje záložku *Obecné* a *Vstupní informace*.



Obrázek 4 Vývojové prostředí programu ProAuthor

Kapitoly jsou studijní aktivitou, která svojí funkcí slouží jako obal pro všechny studijní články a k nim přiřazené aktivity. Ke specifikování kapitoly slouží záložky, v pravé části vývojového prostředí. Ke kapitolám se váží záložky obecné a vstupní informace.

Nejvíce využívanou aktivitou jsou ovšem studijní články. Tato aktivita je základním prvkem pro tvorbu výukových materiálů. Studijní články hlavně obsahují v pravé části, mimo jiné, také záložku *Studijní text*, která autory kurzu zajímá asi nejvíce.

Obrázek 5 Panel nástrojů s aktivitami

Po otevření záložky *Studijní text* se autorovi zobrazí editor, do kterého zadává informace, které chce předat studentovi. Právě v tomto editoru tkví jednoduchost a síla celého vývojového prostředí ProAuthor. Jak bylo výše popsáno, výstupem programu mohou být také HTML stránky. Vývojáři programu ProAuthor mysleli hlavně i na ty autory, kteří umějí v jazyce HTML programovat pouze na omezené úrovni, nebo se s tímto jazykem nesetkali prakticky vůbec, ale chtějí vytvořit kvalitní podpůrný elektronický materiál. Umožnili tedy psát studijní texty formou WYSIWYG. WYSIWYG je zkratkou anglické věty *„What you see is what you get“* což v překladu znamená *„Co vidíš, to dostaneš“*. Výsledkem je, že text, který autor píše je automaticky převáděn do html kódu. Tím dojde k obrovské úspoře času a autor se může více zabývat kvalitou studijního textu, než řešit problémy vzniklé se špatně napsaným zdrojovým kódem.

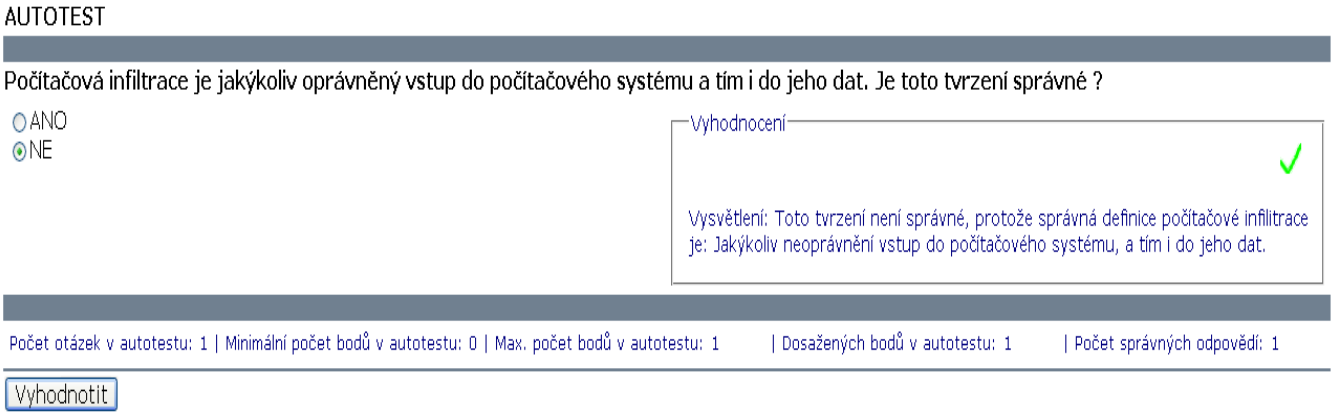
Editor obsahuje základní paletu nástrojů pro formátování textu, a tlačítka pro přidávání a odebírání multimediálních souborů. Dále zde nalezneme tlačítka pro nastavení rozložení levé a pravé strany výstupní obrazovky a tlačítko *Náhled*, za pomocí kterého se autor může kdykoliv podívat, jak vypadá v dané chvíli výstupní obrazovka se zadaným textem.

Obrázek 7 Panel nástrojů

Obrázek 6 Panel nástrojů pro formátování textu a přidávání aktivizujících prvků

Úkoly a cvičení jsou zaměřeny na provedení určitých činností studentem. Student dostane zadání a toto zadání se snaží za pomocí předešlých nabytých znalostí vypracovat. Rozdíl mezi úkolem a cvičením je, že úkol bývá povinný. Úkol je vždy bodově ohodnocen a student je předem obeznámen vždy s minimální hranicí pro úspěšné vypracování úkolu. Cvičení bývá dobrovolné a po zadání úkolu je vždy studentovi k dispozici tip řešení, ve kterém je uvedeno například jaký program má student použít nebo kde může nalézt důležité informace a návrh řešení. Takže pokud si student nebude vědět se cvičením rady, může se podívat na možnost postupu.

Testy a autotesty jsou v použitelnosti podobné jako úkoly a cvičení. Test bývá většinou povinný a autotest nepovinný. U autotestů je student po vyhodnocení nejen seznámen se správnými odpověďmi, ale pokud někde udělal chybu, je mu podáno i vysvětlení a správná odpověď.



Obrázek 8 Ukázka správné odpovědi v autotestu

2.1.2 KLADY

V této části popisu programu budou uvedeny některé klady, které dělají autorský systém ProAuthor, tak silným nástrojem pro tvorbu elektronických materiálů.

Mezi tyto klady patří:

- Vytváření jednotlivých aktivit bez znalosti programování.
- Široká podpora vkládání multimediálních souborů do studijních článků.
- Snadné vytváření úkolů a cvičení.

- Možnost vyexportování studijních textů ve formě Html stránek nebo pdf souboru.

2.1.3 NEDOSTATKY

Tak jako každá mince má dvě strany, tak i autorský systém ProAuthor má svojí druhou odvrácenou stranu a to, že obsahuje i pár nedostatků, které byly odhaleny během vytváření kurzu.

Mezi tyto nedostatky patří:

- V textových polích záložky *Obecné* nelze použít klávesovou zkratku Ctrl + A, která slouží pro vybrání celého textu.
- Při vkládání textu uloženého ve schránce do aktivizujících prvků, dochází ke ztrátě tohoto formátování. Pokud tedy takovýto prvek obsahuje delší text, musí se naformátování provést znovu.
- U editoru studijních článků chybí funkce krok zpět a krok vpřed. Tyto funkce jsou považovány u dnešních programů za velice důležité, protože vytváří daleko snazší práci s programem a autoři jsou tak jištění při udělání nějaké chyby viz například výše ztraceného formátování, návratem do předcházejícího stavu.
- U aktivizujících prvků byla zjištěna ztráta formátování při spuštění programu ProAuthor v operačním systému Microsoft Windows 7. Text se zdál zprvu naformátován, ale po zobrazení náhledu byl text nenaformátovaný. V editoru studijních článků bylo patrné menší odsazení textu, než by mělo v běžných případech při použití aktivizujících prvků být.
- Při kopírování nadpisů dochází ke ztrátě naformátování kopie a text se zobrazí jen jako tučný.
- Při ukládání kurzu se může vyskytnout chyba ukládání a tím následné ztráty dat. Toto se stalo během vývoje kurzu několikrát. Nelze přesně říci, čím je chyba způsobena, ale je nejlepší si kurz zálohovat na více míst najednou a vždy jej často aktualizovat.

- Nemožnost otevření kurzů vytvořených v novějších verzích programu v nižších verzích programu ProAuthor tj. ve verzi programu 6. 5. 7 nelze spustit kurz vytvořený ve verzi 7. 04.00

Je dobré zmínit, že toto jsou chyby, které byly zjištěny při práci s programem ve verzi 6. 5. 7. Nelze tedy stoprocentně říci, že jsou to chyby jediné, a proto jak už bylo výše zmíněno, je dobré provádět časté ukládání a aktualizace dat.

Odstranění všech těchto chyb, nebo zamyšlením se nad nimi, může vést ke zdokonalení programu ProAuthor. Největší slabinou celého programu je jeho textový editor studijních článků, který opravdu postrádá širší možnosti úpravy a formátování textu.

2.2 CMAPTOOLS

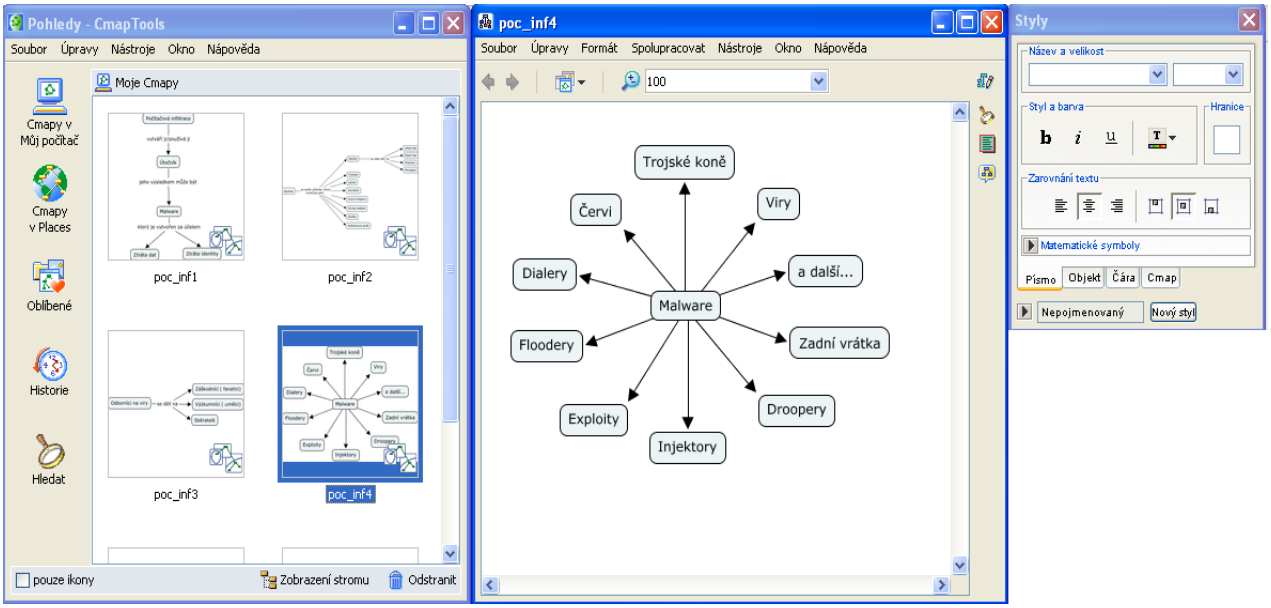
Do elektronického kurzu byly vkládány pro podporu studijních článků také takzvané pojmové mapy. Tyto pojmové mapy byly vytvářeny ve specializovaném freewarovém programu CmapTools od společnosti IHMC. Pojmové mapy jsou skvělou pomůckou k vyjádření určitého textu v grafické podobě, která napomáhá studentům k lepšímu pochopení a zapamatování si určité látky.

V tomto programu lze vytvářet různé typy pojmových map. Mezi tyto typy patří například pojmová mapa:

- Pavouková
- Hierarchická
- Systémová
- Vývojový diagram

V e-kurzu byly použity hlavně pojmové mapy pavoukové a hierarchické. Mezi jednotlivé pojmy lze vkládat popisky, které dále více zpřesňují návaznost jednotlivých pojmů. Program CmapTools nabízí také možnosti tvoření pojmových map za pomocí obrázků. Tato forma vytváření pojmových map velice rozšiřuje jejich použití pro výuku a z programu samotného dělá velice kvalitní nástroj na podporu výuky. Obrázkové pojmové

mapy jsou výbornou pomůckou při výuce u dětí, které si mou tak snáze zapamatovat určitou látku. Například koloběh vody.



Obrázek 9 Ukázka pracovního prostředí programu CmapTools

Při práci s tímto programem bylo skvělé, jak rychle se dala vytvořit i větší pojmová mapa. Vytváření jednotlivých pojmů, provazování mezi nimi je otázka několika kliknutí myši. Výborným nástrojem pro formátování jednotlivých pojmů, jsou styly. V tomto nástroji si autor může vytvořit svůj vlastní styl nebo použít již nějaký předem definovaný. V těchto stylech lze nastavit velikost textu, styl a barvu, zarovnání textu. Kromě písma lze ve stylech formátovat i samotný objekt, čáry a i celou pojmovou mapu.

Všechny vytvořené pojmové mapy lze spravovat v samostatném okně, kde je můžeme kopírovat, mazat, přidávat mezi oblíbené, či je dokonce sdílet na internetu. Mezi našimi pojmovými mapami můžeme i vyhledávat, nebo se podívat do historie, ve které je zobrazeno, kdy jsme s jakou mapou pracovali.

Výhody tohoto programu jsou:

- rychlost a jednoduchost vytváření pojmů,
- snadné propojení jednotlivých pojmů,
- vytváření obrázkových pojmových map,
- grafická úprava pojmů,

- jednoduchá správa vytvořených pojmových map,
- sdílení pojmových map na internetu.

Nedostatky jsou:

- omezenost tvarů pojmů na čtverec, elipsu a kruh,
- spojování pojmů omezeno k přichycení spojnicových čar k spojovým bodům.

Všechny tyto výhody i nevýhody byly zjištěny při používání tohoto programu a to přesně verze 5. 04. 02. Je tedy možné, že nedostatků tak i výhod je daleko více.

2.3 MICROSOFT WORD 2007

Tento textový editor z balíku kancelářských programů Microsoft Office 2007, byl použit při psaní této práce a také při sepisování jednotlivých studijních článků. Byl také hlavně použit proto, že oproti textovému editoru v programu ProAuthor, automaticky opravuje naspaný text, nebo špatně napsaná souvětí. Dále umožňuje funkce vracení vzad a vpřed, které byly hojně využívány.

2.4 GIMP

Program GIMP se řadí mezi freewarové bitmapové editory. Při úpravě fotografií byla použita verze programu 2.6. Tento program obsahuje širokou paletu nástrojů. Nejvíce využívaná funkce tohoto programu byla funkce Křivky. Za pomoci této funkce se upravoval jas v celém obrázku. Z nástrojů samotných byly nejvíce využívány nástroje Perspektiva a Škálování, pro změnu perspektivy a velikosti fotografie.

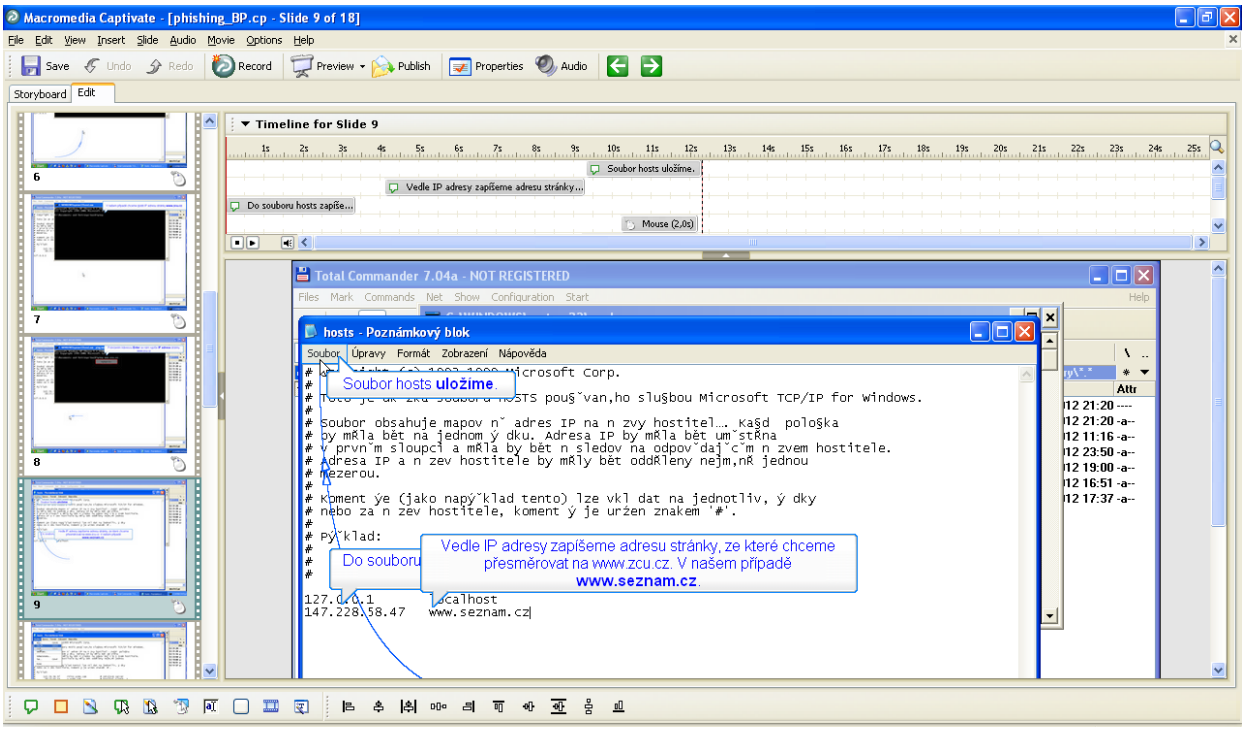
Všechny použité obrázky a fotografie v kurzu byly v tomto programu upravovány. Nejvíce tedy fotografie v kapitole *Způsoby ochrany* ve studijním článku *Fyzické zabezpečení počítače*.

2.5 MACROMEDIA CAPTIVATE

Program Captivate od společnosti Macromedia je program pro podporu výuky v podobě vytváření animací. Program je zaměřen na snímání obrazovky a veškerého pohybu na ní. Zejména snímání pohybu myši, psaní textu, otevírání oken atd. Vše je zaznamenáno a rozděleno do jednotlivých snímků, ze kterých je následně vytvořen

konečný klip. Ten je možno uložit ve formě flashové animace ve formátu *.swf. To ovšem není jediný formát, do kterého lze ukládat. Možnosti exportů jsou široké. (2)

Program vyniká hlavně tím, že lze jednotlivé snímky editovat. Při editaci můžeme vkládat různá textová pole, ve kterých můžeme upřesňovat, co se právě odehrává na obrazovce. Další výhodou editace může být úprava pohybu myši nebo přidávání zvukového komentáře.



Obrázek 10 Ukázka editace snímku a přidaných textových polí.

Tento program byl při vytváření kurzu využit hlavně ve studijním článku *Phishing a pharming*, ve kterém bylo na názorných příkladech ukázáno, jak tyto typy útoků vypadají.

2.6 WINDOWS XP PROFESIONAL

Jako poslední program, který pomohl vzniknout e-kurzu, tak i této bakalářské práci, byl operační systém Microsoft Windows XP Profesional. V dnešní době samozřejmě existují již novější verze operačního systému Windows (Windows Vista, Windows 7), ovšem i tato verze byla plně dostačující a vyhovující.

3 VÝVOJ KURZU

Tak jako každá práce má nějaký svůj systém a postup, podle kterého se postupuje, tak i při vývoji elektronického kurzu se autor musí držet nějakého předem předepsaného nebo vymyšleného postupu. Za pracovní postup považujeme seznam činností, podle kterých se postupuje při práci. Pracovní postup dodává práci určitou organizaci a řád. Díky tomuto řádu se může dosáhnout nejen kvalitní práce, ale také hlavně obrovská úspora času.

Čas je při práci jedním z důležitých faktorů. Většinou mají autoři předem zadaný počet hodin, který mají na celkové vytvoření kurzu. Ve většině případů tento čas nesmějí překročit, protože kurz, který autor vytváří, může být součástí velkého projektu, ve kterém každé zdržení může vést k nedodržení termínu dokončení celého projektu, který byl dohodnut ve smlouvě. To může mít za následek sankce, které mohou být v podobě snížení celkové odměny za vytvoření projektu a vrhání špatného světla na autora za nedodržení svých závazků čímž může být ohrožena i budoucí spolupráce.

Kvalita je další faktor, který má za následek použitelnost kurzu a pokud by kvalita nebyla odpovídající, může se ohrozit i výuka studentů v podobě chybných údajů uvedených ve studijních článcích. Kvalita může být ovlivněna špatným výběrem zdrojů, ze kterých bude autor čerpat. Při tvorbě odborných kurzů je důležité opřít se již o předem napsanou literaturu a čerpat z ní. Je důležité pročíst si o jednom tématu více publikací a následně, ze získaných informací, vytvořit vlastní formulaci. Pokud ovšem nastane situace, že některé informace nelze přeformulovat jinak, než bylo již dříve napsáno, je povinností autora tyto informace citovat. Následně v závěru článků nebo kapitol se musí ovšem uvést, ze kterých titulů autor čerpal. Pokud tedy autor má vybrané zdroje, ze kterých bude čerpat, může se začít zabývat tím, který software využije pro jejich zpracování.

Ke zpracování textových informací může autor využít rovnou textový editor, který má v sobě zabudovaný program ProAuthor. Tento textový editor, jak bylo popsáno v kapitole 2.1.3, obsahuje určité nedostatky a není tedy úplně nejvhodnější, ovšem obsahuje řadu funkcí, které v klasickém textovém editoru nejsou. Například vkládání aktivizujících prvků. Nabízí se tedy možnost, za cenu ztráty času, použít jiný textový editor. Dnes je zřejmě nejlepší program Microsoft Word z kancelářských balíků Microsoft Office,

jejíž nejnovější verze je 2010. Nemusí být ovšem používán pouze tento program, ale klidně celá škála dalších textových editorů, které jsou autorovi k dispozici. Většinou má autor předem stanoveno, který software musí použít, či měl by použít.

Dalším z kroků autora je aby si uvědomil, jak dlouhé články budou, aby nenarušil časový rozsah kurzu. Má-li autor zpracované články v některém z textových editorů, může postoupit dál a začít jimi plnit daný kurz v některém z programů k tomu určených. Tím programem může být již výše zmíněný autorský systém ProAuthor. V takovýchto programech již autor může studijní články upravovat do výsledné podoby.

3.1 POUŽITÉ POSTUPY PŘI TVORBĚ STUDIJNÍCH ČLÁNKŮ

Při tvorbě studijních článků pro e-kurz *Počítačová infiltrace a způsoby ochrany* byla snaha použití výše popsaného hrubého postupu. Ovšem ne vždy šlo tento postup splnit do posledních detailů.

Po obdržení zadání byla, jako první věc, promyslet z jakých zdrojů se bude čerpat. Na internetu bylo zjištěno několik titulů, které by mohly být vhodným základem pro získání informací o daném tématu. Jako první publikací byla kniha Počítačové viry – analýza útok a obrana od Petera Szora. (3) Peter Szor je jedním ze světových odborníků na počítačové viry a tato publikace mne zaujala rozdělením a zpracováním jednotlivých kapitol. Dalším důvodem, proč byla využita tato publikace, byl rok vydání. Rok vydání byl jakousi zárukou aktuálnosti tématu. Druhou publikací byla Bezpečnost domácího počítače: prakticky a názorně od Mojmíra Krále (4). Tato kniha byla vybrána kvůli názorným ukázkám zabezpečení počítače a popisem jednotlivých skupin malwaru, protože obsahovala některé zajímavé informace oproti předešlé publikaci. Jako velký zdroj informací posloužil internet a to zejména internetové portály Živě (5), Hoax (6) a Lupa (7). Po vybrání literatury následovalo samotné prostudování částí literatury, která bude použita a následná konzultace s vedoucím práce o tom, zda se dané části knih mohou v kurzu použít.

Následujícím krokem bylo vymyšlení obsahu kurzu. Prvotní podmínkou bylo, aby každý studijní článek obsahem navazoval na předchozí a tím se vytvořilo pro studenta příjemné navazování látky, jako v jiných tištěných učebnicích. Základem pro vytvoření obsahu bylo rozdělení celkové problematiky počítačové infiltrace a způsobů ochrany do

dvou kapitol. Dvě kapitoly byly zvoleny z toho důvodu, aby byla oddělena kapitola zabývající se útoky od kapitoly o obraně. V kapitole o útocích bylo potřeba vymyslet, jak rozdělit toto široké téma do několika studijních článků, aby kapitola studentovi předala co nejvíce důležitých, užitečných a zajímavých informací. V druhé kapitole byla situace o něco snazší, ale o to bylo složitější vymyšlení názvu studijního článku, který obsahoval více témat najednou. Další podmínkou bylo stanovení průměrné doby studia u každého studijního článku. Tato doba studia byla nejdříve nastavena s přibližným odhadem. Konečný čas byl upraven až po sepsání obsahu studijního článku.

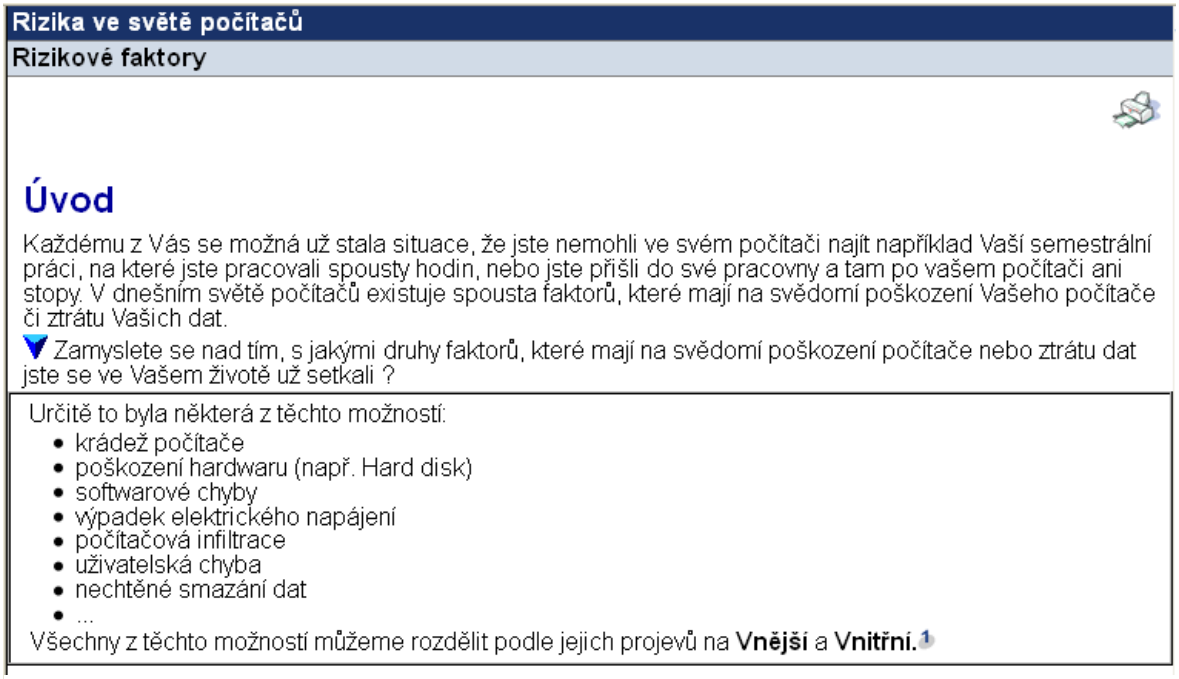
Když bylo známo, kolik průměrně bude zabírat studentům studium daných článků, přišel čas na promyšlení obsahu každého článku tak, aby opravdu jeho obsah byl co nejvíce výmluvný a hlavně splňoval předem daný časový harmonogram. Obsah byl nejdříve vždy sepsán v textovém editoru Microsoft Word 2007 hlavně kvůli korekci chyb a kvůli jeho pružnosti, protože jak bylo zmíněno v kapitole o problémech programu ProAuthor, editor studijních článků není tak efektivní jako u Microsoft Word 2007. Obsah byl vždy čerpán ze dvou již výše zmíněných tištěných zdrojů. Ovšem velmi často bylo čerpáno i z internetu. Pokud se čerpalo z internetu, bylo velice důležité ověřit si pravdivost každého zdroje. Mohla by totiž potom vzniknout chybná formulace v kurzu, což by přímo devalvovalo motivaci studentů k dalšímu učení. Pokud bylo provedeno ověření správnosti daných zdrojů a došlo k prostudování daných témat, byla vždy vytvořena formulace vlastními slovy jejich obsahů. Tímto mohly vzniknout všechny studijní články. Jako efektivní součást tvorby e-kurzu se ukázala skutečnost použít pomocný bodový seznam ke každé studijní aktivitě. Autor poté může s tímto „tahákem“ operovat velice rychle a prohazovat aktivity mezi sebou, či tu a tam vyměnit odstavce či doplnit informace, které se mu zdají důležité v tu danou chvíli. Tento pomocný seznam byl nápomocný především při posledních korekcích podpůrného výukového materiálu a výrazně uspořil čas.

Před sepsáním každého studijního článku bylo zapotřebí sepsat úvodní slovo pro studenta, tzn. co je obsahem studijního článku a na co by se měl student připravit. Dalším krokem bylo sepsání cíle studijního článku, tzn. co by se mělo projevit na studentovo schopnostech a znalostech po prostudování daného tématu. U těchto částí kurzu bylo důležité vymyslet motivační text pro studenta, který mu je zobrazen ještě před

zobrazením studijního článku. Tento text by měl studenta naladit a motivovat ke studiu daného tématu. Ukázkou takovéhoto motivačního textu může být následující úvodní slovo pro studenta ze studijního článku *Viry* v kapitole *Rizika ve světě počítačů*:

„Dostáváte se k hlavnímu článku kapitoly. V tomto článku se dozvíte co to přesně vir je a jak se dělí i jak se některé projevují. Tato kapitola je náročnější, ale nebojte se, pokud budete postupovat postupně a systematicky, na konci si řeknete, že strach byl zcela zbytečný.“

Při vytváření studijních článků byla snaha v každém z nich vytvořit za pomocí aktivizujícího prvku problémovou otázku. Za pomocí tohoto prvku, lze studenta zaujmout a vytrhnout ze čtení zamyšlením se nad danou otázkou. Pokud student zná odpověď na tuto otázku, mohl ji klidně přeskočit a věnovat se dále textu. Pokud ovšem odpověď neznal, mohl si po kliknutí na tuto otázku rozbalit odpověď. Tento prvek studijní článek oživí něčím novým a studentovi studijní článek nebude připadat tak strohý a monotónní.



Obrázek 11 Použití aktivizujícího prvku ve studijním článku Rizikové faktory

Další částí, kterou bylo nutno brát na vědomí, byly pokyny pro tutora, které slouží hlavně pro člověka, který bude dané téma přednášet. V této části bylo vždy nutno tutorovi sdělit informace, které nejsou na první pohled z článku patrné, a které mohou hrát zásadní roli pro správné předání informací studentům. Mohou to být například jen uvedené správné programy pro demonstraci určitého problému nebo upozornění

studentů na určitou část textu, která je důležitá. Toto vše vede k tomu nejlepšímu podání dané látky.

Důležité, pro konečnou efektivnost, bylo proložit kurz bylo proložit kurz doplňujícími cvičeními, která pomohou znalosti nabyté teoreticky aplikovat do praxe. Cvičení muselo obsahovat zadání, které by se dalo splnit s předešlými získanými informacemi a také doplněné o vymyšlený postup, který by sloužil studentovi jako návod, pokud by nevěděl jak cvičení zvládnout.

Jako poslední částí vývoje elektronického kurzu byla konečná výstupní kontrola. Tato kontrola byla provedena nejen autorem samotným tak, že znovu zkontroloval veškerý obsah a funkčnost jednotlivých částí kurzu a opravil případné nalezené chyby, ale kurz byl také předán další pověřené osobě, která měla na starost kontrolu kurzu. Tato pověřená osoba sepsala na kurz posudek a také seznam chyb, které autor přehlédnul a vrátil zpátky kurz autorovi k přepracování. Po konečné korekci chyb mohl být kurz konečně připraven k publikaci.

3.2 PROBLÉMY

Problémy byly, jsou a budou nedílnou součástí při tvorbě jakéhokoliv studijního materiálu. S problémy musí vždy autor počítat a být na ně ve svém pracovním plánu připraven minimálně tak, že si nechá pro případné potíže časovou rezervu. Problémů může být spousta. Níže budou popsány pouze ty problémy, které se vyskytly při tvorbě e-kurzu *Počítačová infiltrace a způsoby ochrany*.

Hned po obdržení zadání pro tvorbu elektronického kurzu se vyskytl problém s vyhledáním odpovídajících zdrojů, které by byly aktuální a důvěryhodné s praktickými příklady. Největší problém byl se sehnáním tištěných zdrojů. Nejpříhodnějším způsobem bylo vypůjčení literatury z Univerzitní knihovny Západočeské univerzity v Plzni a Studijní vědecké knihovny Plzeňského kraje. Velkou výhodou byla nulová pořizovací cena, ale bohužel omezená doba vypůjčení. Tudíž musel být dán pozor na dobu prodloužení výpůjčky nebo vrácení těchto knih zpátky do knihoven.

Další problém bylo vymyšlení obsahu, co se předem daného časového rozsahu studia na daný studijní článek týče. To znamenalo leckdy vybrat opravdu jen to nejdůležitější, co se daného tématu týkalo a muselo se vynechat i více poněkud

zajímavějších informací. Studijní článek musí být proto tedy stručný, ale musí mít i přesto vysokou vypovídající hodnotu. Tento problém je častým jevem kurzů, které mají předem stanovenou časovou délku studia. Pokud ovšem kurz takto omezen není, lze vytvořit opravdu rozsáhlý a kvalitní studijní materiál plný praktických ukázek, cvičení, úkolů atd.

Upravení konečné doby studia u každého studijního článku byl problém i po jeho dokončení, protože autor nedokáže přesně určit, jak dlouho bude ten který student daný studijní článek studovat. Každá student má pokaždé s daným tématem jiné zkušenosti.

Mezi problémy, které mohou vzniknout při tvorbě, řadíme také problémy s programovým a fyzickým vybavením počítače. Nikdy nevíme, kdy se může v činnosti programu vyskytnout chyba nebo kdy může selhat kterákoliv část počítače. Chyby autorského systému ProAuthor byly popsány v kapitole 2.1.2. Chyby tohoto programu dělaly při práci největší problémy, protože tento program byl základem pro tvorbu e-kurzu.

Takovéto chyby nelze na sto procent přepokládat, a proto by měl každý autor vždy pravidelně zálohovat svoje data. Takovýto kolaps se může stát klidně ke konci práce, a pokud data nemáme zálohovaná na více místech najednou, selhání harddisku může být pro autorovu práci definitivní konec.

4 STRUKTURA KURZU

V této kapitole bude popsáno, proč byly dané studijní články zařazeny do kurzu a co bylo důležité kde vytvořit a podobně. Nebude zde doslova uvedeno, co který studijní článek obsahuje, jelikož to je uvedeno v samotném kurzu, ale spíše bude popsáno, proč je některá definice nebo ukázka uvedena na takovém místě na kterém je a podobně.

4.1 KAPITOLA RIZIKA VE SVĚTĚ POČÍTAČŮ

První kapitola je rozdělena na deset studijních článků a tři cvičení. Studijní články jsou uspořádány tak, aby na sebe navzájem navazovaly.

U některých studijních článků může vzniknout dojem, že daná problematika je daleko složitější a rozsáhlejší, než je vůbec ve skutečnosti prezentována. Proto je u každého studijního článku uvedena literatura nebo odkazy na články z internetu, ze kterých lze se o daném tématu dozvědět daleko více.

4.1.1 STUDIJNÍ ČLÁNEK: RIZIKOVÉ FAKTORY

Rizikové faktory jsou prvním studijním článkem kapitoly Rizika ve světě počítačů. Tento studijní článek má jednoduchou úlohu a to uvést studenta do problematiky všech možných faktorů, které mají za příčinu poškození počítače jak hardwarově, tak softwarově. Tyto faktory byly vypsány jak textově, tak i graficky za pomocí pojmových map.

4.1.2 STUDIJNÍ ČLÁNEK: POČÍTAČOVÁ INFILTRACE

Aby studenti mohli vůbec začít studovat nějaký typ škodlivých programů nebo technik, bylo zapotřebí definovat základní pojmy jako co je počítačová infiltrace, kdo je útočník, či co je malware. Malware je v tomto studijním článku pouze definován jako pojem z toho důvodu, že jednotlivé typy malwaru představují samostatné studijní články. Proto je tento studijní článek zařazen ještě před první studijní článek zabývající se malwarem.

4.1.3 STUDIJNÍ ČLÁNEK: VIRY

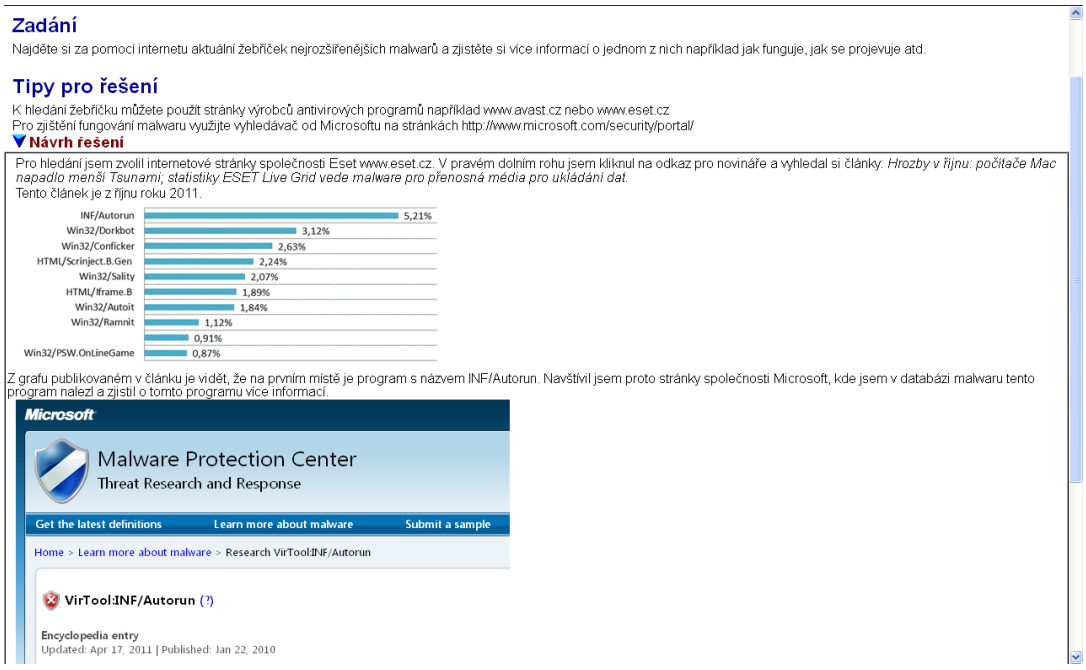
Studijní článek s názvem viry, je nejdelším článkem z celého kurzu. Je to zároveň první článek zabývající se přímo už jedním z druhů malwaru. Byla mu přiřazena také největší časová náročnost na studium.

Po uvedení základních definic a modelů popisující viry, bylo vhodné rozdělit viry do několika kategorií. Jelikož existuje spousta možností, jak viry rozdělit a navíc některé viry se dají zařadit do více kategorií najednou, bylo vybráno a popsáno pět nejdůležitějších rozdělení. Konkrétně to jsou rozdělení podle projevů, podle času projevu, podle oblasti napadení, podle chování a podle umístění v paměti. Byl totiž problém v tom, jak lze viry rozdělit, protože v dnešní době to lze provést více způsoby. Z tohoto důvodu bylo rozdělení převzato z knihy Bezpečnost domácího počítače: prakticky a názorně od Mojmíra Krále (4).

Z hlediska názornosti a aktuálnosti, byl u některých typů virů uveden i příklad konkrétního viru a jeho krátký popis. Například po celkovém rozdělní virů byl zmíněn v dnešní době nejvíce diskutovaný virus Flame, u kterého byla uvedena video ukázka rozhovoru reportéra pořadu Události a komentáře s odborníkem, zabývající se ochranou před viry, ze společnosti Kaspersky Lab. Tato ukázka by měla studentovi přinést jinou formou popsání konkrétního druhu viru.

4.1.4 CVIČENÍ: POROVNÁNÍ VÝVOJE MALWARU

Jako prvním cvičením v kapitole rizika ve světě počítačů, je studentovi zadán úkol, ve kterém musí na internetu naleznout aktuální žebříček rozšířenosti malwaru a zjistit bližší informace o malwaru, který je na prvních místech.



Obrázek 12 Ukázka cvičení Porovnání vývoje malwaru

Cílem tohoto cvičení by mělo být, že se student seznámí s vyhledáváním informací o aktuálních hrozbách, které číhají ve světě počítačů a zjistí z výsledných informací i to, jak se například proti těmto hrozbám bránit, či jak je popřípadě ze svého počítače odstranit.

4.1.5 STUDIJNÍ ČLÁNEK: ČERVI

Po virech jsou dalším studijním článkem červi. Tento studijní článek je zařazen po virech z toho důvodu, že červi jsou si s viry velice blízcí. To bylo také důležité studentům naznačit hned na začátku studijního článku. Nedílnou součástí bylo ovšem hned podat rozdíly mezi červi a viry, aby nedocházelo k záměně virů za červi a obráceně. Na toto byl kladen zřetel, protože většina lidí většinou označuje jakýkoliv malware za viry, nebo červi.

4.1.6 STUDIJNÍ ČLÁNEK: TROJSKÉ KONĚ

Jak už název tohoto typu malwaru napovídá, je úzce spojen se starou řeckou bájí o dobývání Tróji. To bylo příhodné pro styl napsání úvodu a první části tohoto studijního článku. Bylo snahou, aby si studenti uvědomili skoro stejnou taktiku počítačových útočníků, jako vojáků v oné řecké báji. Jak bylo použito spojení báje a popisu trojských koní znázorňuje následující ukázka.

Úvod

Samotný název Trojské koně nás přesouvá do minulosti a to zejména do báje o obléhání města Trója, řeckými vojsky. Řekové Tróju dobyli a to brilantním strategickým tahem. Postavili velkého dřevěného koně, do kterého se nechali zavřít a věnovali ho Trojanům jako dar. Ti si koně šťastně odtáhli do svého města s pocitem výhry a po oslavách během noci, když všichni šli spát, z koně vylezli řečtí vojáci, otevřeli brány řecké armádě a ta během noci Tróju dobila. Vraťme se ale zpět do 21. století a podívejme se na to, jak takové dobývání uživatelských počítačů alias Trójí vypadá.

Trojské koně

Jak již víme hlavními vlastnostmi virů je napadat další programy a potřebují ke svému životu právě cizí program. Rozdíl mezi virem a trojským koněm(1) je ten, že trojský kůň se ***nereplikuje*** *(nevytváří kopie sebe sama) a nemusí se* ***připojovat*** *k hostitelskému souboru. Trojského koně můžeme ve svém počítači nejčastěji nalézt jako* ***samostatný spustitelný soubor*** **.exe, který v sobě obsahuje pouze škodlivý kód.*

*Hlavním cílem trojských koní je **upoutat něčím uživatele**, aby si jej stáhli do svého počítače. Takový to program se může tvářit jako **užitečný legální program**, ovšem to je jen převlek, jako dřevěný kůň ve slavné řecké báji. Uvnitř programu číhá další program, ale ten už má podobu řeckých vojáků, kteří jen čekají na signál. Jakmile si program stáhneme, nainstalujeme a pustíme jej, je to jako bychom otevřeli řeckým vojákům vrátka. Druhá část programu, která není navenek vidět během spuštěného programu, začíná provádět škody. Většinou se jedná o již dříve zmíněné **sociální inženýrství**.*

4.1.7 STUDIJNÍ ČLÁNEK: ADWARE A SPYWARE

Tyto dva malwary jsou si velmi podobné, a proto bylo zvoleno jejich zařazení do společného studijního článku.

4.1.8 STUDIJNÍ ČLÁNEK: HOAX A SPAM

Hoax není otázkou jen současné doby, ale byl tady již i před dobou internetové komunikace. Z tohoto důvodu se zde vybízela i možnost upozornit na tento fakt aktivizujícím prvkem. Opět tyto dva typy jsou si celkem podobné, a proto byly uvedeny v jednom studijním článku. Na tento studijní článek následuje cvičení, pro které je třeba pochopení této problematiky.

4.1.9 CVIČENÍ: POROVNEJTE HOAX A SPAM

V tomto případě jsou uvedeny dvě ukázky a student musí poznat, která ukázka je spam, a která hoax. Toto cvičení je dobré pro otestování jestli si studenti zapamatovali základní vlastnosti hoaxu a spamu.

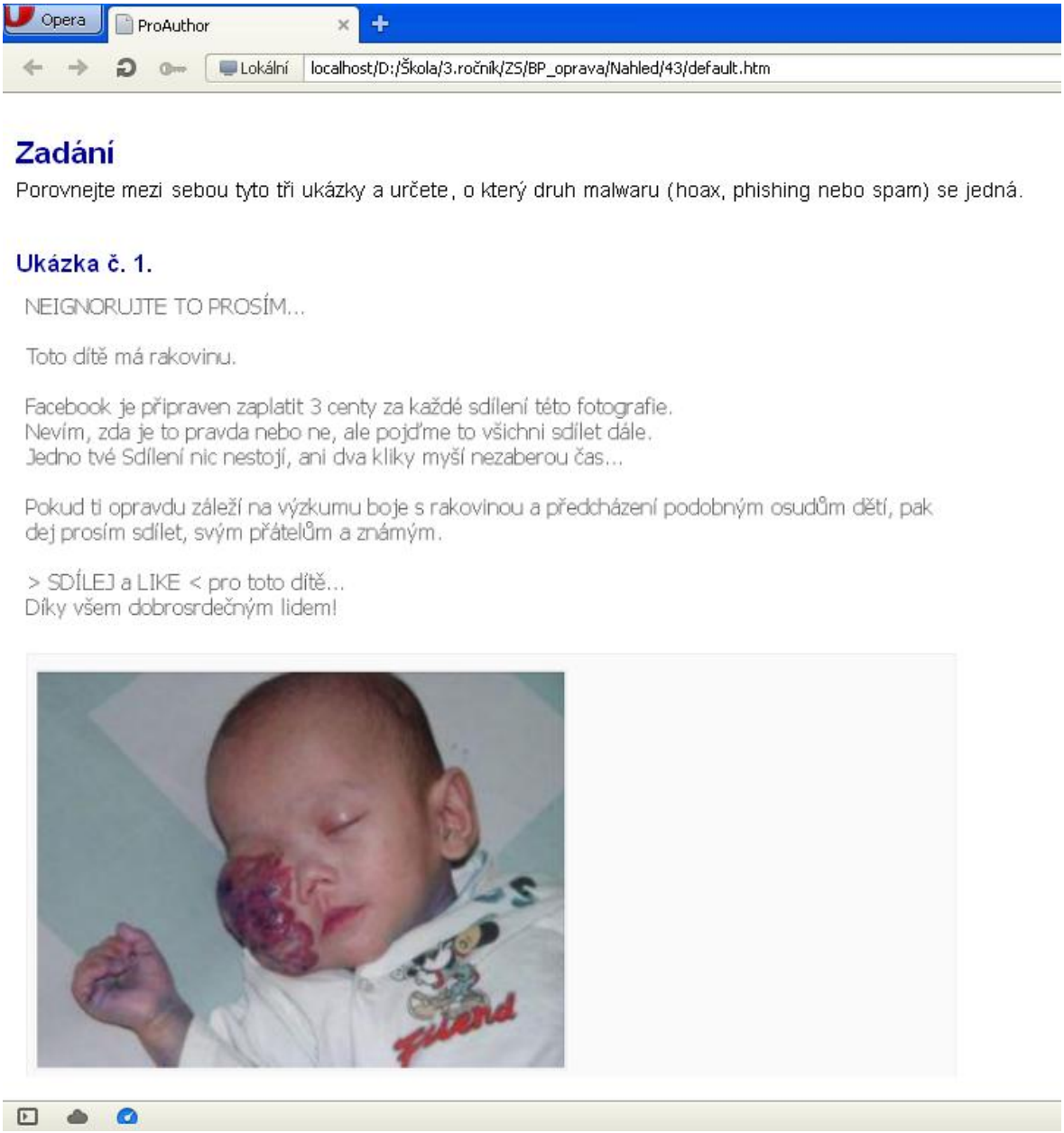
4.1.10 STUDIJNÍ ČLÁNEK: PHISHING A PHARMING

Tento studijní článek se do důležitosti vyrovnává se studijním článkem virů. U tohoto studijního článku bylo příhodné uvést příklady, na kterých si studenti mohou prohlédnout fungování těchto technik. Příklad phishingu byl vybrán z databáze případů phishingu na stránkách http://www.hoax.cz/phishing/.

U pharmingu byly vytvořeny názorné animace, které přímo demonstrují tuto techniku. Studenti si mohou tak všimnout, jak lehce lze přesměrovat na podvodné stránky útočníků, nebo jak bezpečně přistupovat na stránky bankovnictví za pomocí IP adresy.

4.1.11 CVIČENÍ:POROVNEJTE HOAX,SPAM A PHISHING

Do první kapitoly bylo ještě jednou zařazeno cvičení podobné předchozímu na porovnání hoaxu a spamu, ale rozšířeného také o phishing.



Obrázek 13 Ukázka cvičení porovnání hoaxu, spamu a phishing u

4.1.12 PROGRAMY PRO ŠÍŘENÍ MALWARU

Původně tento studijní článek byl součástí následujícího studijního článku *Další druhy škodlivého softwaru.* Ovšem kvůli rozsáhlosti a různorodým typem jednotlivých

programů bylo vhodné tyto články rozdělit. Tento studijní článek popisuje programy, které napomáhají v cestě malwaru do počítače oběti. Jednotlivé programy jsou seřazeny podle toho, jak jsou malwarem využívány.

4.1.13 DALŠÍ DRUHY ŠKODLIVÉHO SOFTWARU

Tento studijní článek je zařazen na konec této kapitoly, protože krátce popisuje další druhy škodlivých programů, které mohou uživatele počítačů potkat. Mezi těmito programy jsou zárodky, floodery, dialery, logické bomby, generátory virů, zábavné programy. Tyto programy jsou sami o sobě velmi zajímavé a je škoda, že není prostor pro jejich bližší zkoumání. Každý z nich by si určitě zasloužil minimálně svůj vlastní studijní článek, ale tím by se přesáhl časový rozpočet hodin, který byl pro tento výukový kurz přidělen. Pokud si ovšem student chce zjistit v rámci samostudia o daných tématech více, může použít doporučenou literaturu uvedenou ve zdrojích.

Následující ukázka znázorňuje, jakým způsobem byly psány studijní články v této kapitole. Pro tuto ukázku bude použit studijní článek *Phishing a pharming*.

Úvod

Každý, kdo z nás používá internet, se už hodněkrát setkal s tím, že se musel někde registrovat, zadávat svoje jméno nějaké heslo a podobně. Tyto údaje, které vyplňujeme, jsou pro útočníky to ***nejcennější*** *zboží, které se snaží ukradnout. Útočníci chtějí znát naše hesla, čísla účtů, protože to jim přináší jejich zdroj příjmů. Takovéto útoky mají své pojmenování a to Phishing a Pharming.*

Phishing

Phishing(1) je v dnešní době jedna z ***nejčastějších*** *metod útoku na uživatele na internetu. Phishing je metoda kdy Vám útočník pošle velice* ***důvěryhodný e-mail****, ve kterém od Vás vyžaduje zaslání některých informací, nejčastěji* ***citlivých dat****. V takto přijatém emailu se většinou zobrazí formulář nejčastěji vypadající jako přihlašovací formulář do vaší internet banky a podobně. Vzhled takovéhoto formuláře je tak přesvědčivý, že se s přihlašovacím oknem dané banky nedá skoro srovnat. Nejčastěji požadované údaje bývají:*

- *Přihlašovací jména (tzv. nicknames),*
- *Přihlašovací hesla,*
- *Čísla bankovních účtů,*
- *Čísla kreditních karet,*
- *Piny,*

•*a další..*

*Pokud byste takováto data odeslali, nejčastěji se stanete obětí tohoto útoku a přijdete například o **peníze na Vašem účtu** a už Vám je nikdo **nevrátí**. V takovéto podvodné zprávě se může vyskytnout i odkaz přímo na stránku bank. Ovšem tento odkaz nebude vypadat naprosto stejně jako odkaz na stránku Vaší banky. Největší nebezpečí právě spočívá v tom, že **zpráva vypadá korektní** a nedá se žádným způsobem zablokovat. Pro normálního uživatele nepředstavuje žádné riziko a proto má tato metoda takový úspěch. Nalezení útočníka je velice složité, nýbrž ke své činnosti právě používá **falešné stránky, emaily** a podobně. Jediné co by nás mělo upozornit na to, že se jedná o podvodný email, je většinou dovětek, že na zprávu nelze odpovědět z důvodu automatického vygenerování systémem. Další možnou obranou je, že vaše banky **nikdy** po Vás tyto údaje nebudou žádat emailem nebo dokonce i SMS zprávou.*

*V dnešní době je metoda phishing tak **vyspělá**, že stránka má skoro **přesnou** podobu, tak jakou by měla mít. Jsou zde ovšem ale i rozdíly. Názorně si vše předvedeme na následujícím příkladě.*

•*Jedná se o phishing pod názvem SERVIS 24 Internetbanking, který se objevil v roce 2008 v České republice, kdy útočník posílal emailové zprávy, ve kterých upozorňoval uživatele na chybu transakce v bance České spořitelny.*

•*Na obrázku(2) vidíme podvodný email, který přišel uživateli. Je vidět, že **logo i grafika odpovídá právě bance Česká spořitelna**. Ovšem pokud budeme pozorní, můžeme si na obrázku všimnout, po najetí na odkaz, **zvláštní adresy**, na kterou nás má odkaz nasměrovat. Další čeho si můžeme všimnout, je že v názvu odkazu se vykytuje ve slově aktivovaných a služby **azbuka**.*

•*Po kliknutí na odkaz, jsme přesměrovaní na přihlašovací obrazovku(3) do služby servis24, která má funkci internetové bankovnictví. S obrázkem(3), na které je podvodná stránka, můžeme porovnat obrázek (4), kde je originální stránka služby servis24. To hlavní, čeho si můžeme všimnout, je že se **zcela liší adresy stránek**.*

•*Pokud se přihlásíme, zjistíme například, že při přidávání nového produktu(5) podvodná stránka **neakceptuje**, ani přes chybové hlášení, diakritiku a mezeru.*

•*Když bychom provedli skenování komunikace, zjistili bychom, že server, se kterým komunikujeme se nachází v **Thajsku(6)**.*

*Phishing nemusí ovšem být zaměřen pouze jen na bankovnictví. Útočníci se můžou skrývat za jakoukoliv společností, která zprostředkovává nějaké služby a je do ní potřeba se přihlásit, nebo zadávat jiné osobní údaje. Jeden z mnoha příkladů může být podvodný email(7), zkoušející získání informací od studentů ZČU, k jejich **univerzitním emailovým účtům**.*

Pharming

*Pharming(8) můžeme považovat za **náročnější variantu phishingu**. Pharming se týká právě podoby podvodných internetových stránek při lákání uživatele. Když běžný uživatel zadává*

název internetové stránky do prohlížeče, nejčastěji ho zadává v podobě www.banka.cz. Služba DNS ***převede*** *tento název* ***na IP adresu****, například ve tvaru 123.456.789.123 a právě* ***útočníci napadají IP adresy*** *daných stránek, které jsou uloženy v počítači, kde existuje paměť těchto navštívených IP adres. Správná adresa banky je pak pharmerem* ***upravena*** *na IP adresu stránky podvodné. Výsledkem je, že se připojujete na nesprávný server, na nesprávnou stránku, která bude vypadat podobně jako stránka originální.*

Postup útočníka, by byl následující:

1.Útočník by si vyhlédnul nejprve stránku, kterou by se snažil napodobit. Tu by také následně vytvořil.

2.Útočník by musel vytvořit, nebo stáhnout například trojský kůň, kterým by se mohl dostat do počítače oběti a tam modifikovat soubor ***hosts*** *uložený ve složce* ***etc****, ke které se dostane za pomocí této cesty: C:\Windows\system32\drivers\etc. Soubor hosts obsahuje tabulku o dvou sloupcích, kde první sloupec obsahuje IP adresy a druhý sloupec názvy k nim přiřazené. Zde dojde k těm nejdůležitějším krokům útočníka.*

3.Útočník ***změní IP adresu*** *originální stránky, na IP adresu svojí podvodné stránky. Nyní už jen útočník čeká na připojení uživatele na jeho stránku.*

4.Když uživatel zadá originální název stránky do prohlížeče, ***bude přesměrován*** *na stránky vytvořené útočníkem a pokud si nevšimne, že je stránka falešná,* ***stává se obětí*** *pharmingu.*

Názorná ukázka toho, jak změnit IP adresy v souboru hosts, můžete vidět na animaci(9).

Proti tomuto typu útoku se dá už ***těžce bránit****. Jedinou možností je připojovat se na www stránky Vašich bank pomocí IP adres. IP adresu banky můžete zjistit za pomocí příkazového řádku a to příkazem:ping www.nazevbanky.cz, který vám vypíše IP adresu vaší banky. Poté místo názvu zadáte do prohlížeče tuto IP adresu. Zjištění a připojení se pomocí IP adresy ke službě servis24, můžete vidět na animaci(10)*

Shrnutí

Je vidět, že způsobů na to, jak vylákat z uživatele počítače jeho osobní údaje je hned několik a doufám, že po prostudování těchto článků už budete opatrnější při nakládání s Vašimi údaji. ***Uvědomte si, že identitu máte jen jednu a to je to jediné, co musíte na internetu ze všeho nejvíc chránit****.*

4.2 KAPITOLA POČÍTAČOVÁ OCHRANA

Druhá a zároveň poslední kapitola je kapitola Počítačová ochrana. Tato kapitola byla rozdělena do čtyř studijních článků, jednoho úkolu a k němu následující diskuze. Tato kapitola je uvedena jako druhá, protože je dobré nejdříve si představit všechna rizika, která mohou vzniknout při práci s počítačem a teprve podle jejich charakteru stanovit patřičnou obranu.

4.2.1 STUDIJNÍ ČLÁNEK: FYZICKÉ ZABEZPEČENÍ POČÍTAČE

Studijní článek Fyzické zabezpečení počítače je v této kapitole první, protože je třeba nejdříve zajistit, aby studenti věděli, jak zabezpečit počítač jinak než softwarově, ale hlavně také protože někdy fyzická ochrana počítače je mnohem důležitější z hlediska ztráty dat, než ta softwarová. Tento studijní článek svým obsahem navazuje na první studijní článek *Rizika ve světě počítačů* v první kapitole tohoto kurzu.

Fotografie, které jsou přiloženy k tomuto studijnímu článku, byly pořízeny v prostorách Západočeské univerzity v Plzni, Fakulty pedagogické, katedry výpočetní a didaktické techniky. Tyto snímky byly uvedeny z toho důvodu, že znázorňují jakými prostými, ale účinnými, prostředky lze počítač uchránit proti krádeži.

Následující ukázka byla vybrána jako znázornění psaní studijních článků v této kapitole.

Úvod

Vzhledem k názvu toho článku, se na úvod zamyslete nad touto větou: ,,Svoji bakalářskou práci začínám psát v internetové kavárně. A proč?"

Jednou z Vašich odpovědí mohlo být:

- *Protože mi můj počítač ukradli.*
- *Protože jsem nepoužil kvalitní přepěťovou ochranu a můj počítač vyhořel.*
- *Protože jsem nad svým PC měl umístěné akvárko s rybičkami.*
- *a tak dál...*

Každá z předchozích odpovědí má za příčinu použití slabého zabezpečení proti působení vnějších vlivů.

Musíme si uvědomit, že odcizení nebo zničení počítače dnes není nic neobvyklého a pokud si nebudeme svůj počítač dostatečně chránit, můžeme o něj velice lehce přijít. Je velký rozdíl mezi zabezpečením počítače(1) v naší domácí pracovně a zabezpečením firemního počítače v pracovních prostorách firmy. Největší rozdíl bude v použitých ***nákladech na zabezpečení****. Ovšem my toto hledisko nebudeme řešit a podíváme se na tento problém obecněji.*

Fyzické zabezpečení

Náš počítač je hmotný majetek jako každý jiný a pokud o něj nechceme přijít, musíme si ho také umět ochránit. Svůj počítač hlavně musíme chránit před tzv. ***fyzickými útoky****. Mezi tyto útoky patří zcizení nebo jakékoliv poškození počítače a jeho částí. Prvním naším krokem k zabránění těmto útokům, by mělo být* ***správné zabezpečení místnosti****, kde svůj počítač budeme používat.*

Zabezpečení místností

Jedním z těchto zabezpečení může být:

- ***Bezpečností dveře(2) a okna*** *- V dnešní době již existují spousty typů bezpečnostních dveří a oken. Dveře jsou vyrobeny tak, že nejdou vypáčit či odemknout obyčejným klíčem. Okna mohou mít například použitý speciální nerozbitný materiál místo skla.*

- ***Autentizace osoby před vstupem do místnosti*** *- Nejčastěji pro autentizaci osoby se dnes používají různé vstupní hesla, vstupní karty ale i použití biometrických prvků jako například otisky prstů, scan sítnice, rozpoznání hlasu nebo obličeje. Na obrázku (3) je čtečka karet pro přístup do učeben Jednotného Integrovaného Systému na Západočeské univerzitě v Plzni.*

- ***Kamerový systém*** *- Tento typ zabezpečení slouží hlavně jako pomocník pro případné dopadení zloděje nebo k záznamu co se v naší místnosti nebo i před ní dělo v určitý okamžik. Ovšem tento prvek může být pro zloděje i odstrašujícím faktorem.*

- ***Systém sledování pohybu*** *- Tento systém funguje na tichém (například pomocí SMS zprávy)zalarmování určité pověřené osoby, při detekci pohybu v dané místnosti.*

*Dalším naším krokem by mělo být **správné vybavení místnosti**. Tím nejhlavnějším bodem tohoto kroku by mělo být použití kvalitních elektrických zástrček s integrovanou **přepěťovou ochranou**. Pokud takovéto zásuvky nevlastníte lze dokoupit prodlužovací kabel, který tuto ochranu má zabudovanou. Problém s napájením může mít za následek **nevratné poškození hardwaru počítače a hlavně ztráty vašich dat**. Proti výpadku elektrického proudu, který má za následek hlavně ztrátu vašich neuložených dat, se můžeme chránit **záložními zdroji napětí**. Tyto zdroje jsou schopny v sobě uchovat dostatečné množství elektrické energie, která Vám dá potřebný čas k tomu, abyste mohli svoje data uložit. Kapacita těchto zdrojů se liší od pár minut až po hodiny. Od toho se také odvíjí jejich pořizovací cena.*

*Dalším bodem tohoto kroku může být i vybavení místnosti proti výskytu požáru z méně **nehořlavých materiálů**, například kovový pracovní stůl či přímo protipožární ochrana, která zalarmuje pověřené bezpečnostní složky.*

Zabezpečení počítače

*Posledním krokem by mělo být **zabezpečení počítače** jako takového. Tato zabezpečení mohou být:*

- ***Pevné připoutání počítače k pracovnímu stolu** za použití různých zámků. Z obrázku (4),(5) a (6) je vidět, že k tomu může posloužit i obyčejný zámek a řetěz. Pro uzamčení notebooků slouží speciální zámky. Názorný příklad je na obrázku (7).*

- ***Uzamykatelné skříně** - Dnešní trh nabízí již spousty počítačových skříní, které mají **uzamykatelný přední kryt**, který brání k zapnutí počítače.*

- ***Autentizace osoby před přihlášení do systému -** totožné s bodem **Autentizace osoby před vstupem do místnosti**. Na obrázku (8) můžeme vidět snímač otisků prstů na notebooku.*

- ***Pravidelné zálohování dat -** Bod, na který mnoho uživatelů dnes zapomíná. Pravidelná záloha našich dat na jiná zapisovací média (externí disky(9), flash disky(10)...) nám snižují ztrátu dat minimálně o 50%. Proto věnujte tomuto bodu velkou pozornost.*

Shrnutí

Tyto typy zabezpečení jsou velice nákladné. Proto pokud si tento luxus uživatelé nemohou dovolit, platí jednoduché zásady, jako ***nenechávejte svůj počítač bez dozoru či důkladně zamykejte dveře a okna v místnosti s počítačem, nenechávejte pracovat cizí osoby na vašem počítači bez vaší přítomnosti****. Ovšem u zabezpečení počítače musíte hlavně zvážit to, zda je to vůbec z hlediska využití vhodné a do takového zabezpečení investovat svoje finance.*

4.2.2 STUDIJNÍ ČLÁNEK: HESLA

S hesly se setkáváme při používání počítače na každém kroku. Tento studijní článek je pro ochranu dat důležitý, a proto byl zařazen hned po studijním článku *Fyzické zabezpečení počítače* a ještě před různými druhy softwarů zabezpečující počítače.

4.2.3 STUDIJNÍ ČLÁNEK: SOFTWAROVÉ ZABEZPEČENÍ POČÍTAČE

Tento studijní článek by měl vyzdvihnout ty nejdůležitější aspekty softwarové ochrany počítače, a proto také na to bylo dbáno. Mezi tyto aspekty byly zařazeny aktualizace, firewall, nastavení webových prohlížečů. Bylo vhodné tyto tři různé programové zabezpečení spojit do jednoho studijního článku, jelikož svým správným nastavením napomáhají k zabezpečení celého systému.

4.2.4 STUDIJNÍ ČLÁNEK: ANTIVIROVÁ OCHRANA

Studijní článek Antivirová ochrana nebyl uveden ve studijním článku *Softwarové zabezpečení počítače*, protože je to primární software pro ochranu uživatelů proti malwaru. Z těchto důvodů je uveden samostatně a podrobněji popsán.

4.2.5 CVIČENÍ: OTESTUJTE SI VÁŠ POČÍTAČ

Závěrečné cvičení se váže na předešlý studijní článek. To, co se studenti dozvědí v předešlém studijním článku, by si měli také prakticky vyzkoušet a seznámit se blíže s nějakým z antivirových softwarů. Jejich cílem bude provést na svých počítačích antivirovou kontrolu a výsledky těchto kontrol uvést v následující diskuzi.

4.2.6 DISKUZE: OTESTUJTE SI VÁŠ POČÍTAČ

Jak již bylo naznačeno, tato diskuze navazuje na předešlé cvičení. V této diskuzi by studenti měli diskutovat mezi sebou o tom, jak probíhal jejich test a jestli se vyskytly nějaké problémy, či dokonce byl nalezen nějaký malware.

5 ZÁVĚR

Zadáním této bakalářské práce bylo vytvoření elektronického kurzu v autorském systému ProAuthor, který bude sloužit jako podpora pro studenty *distanční formy studia.* Výsledkem je v celku kvalitní studijní materiál, který může být rozšířen a využíván studenty.

Během tvorby e-kurzu bylo nutné řešit nejrůznější problémy, které se vyskytly, a nebylo možné je opomenout. Tyto problémy byly blíže specifikovány v předešlých kapitolách. Přes všechny problémy byla vynaložena snaha se co *nejvíce* přiblížit ke zdárnému konci.

Obtížnost celého kurzu byla zvolena na základní, čemuž odpovídá i obsah jednotlivých studijních článků. Pro docílení atraktivnosti programu byly studijní články doplněny o obrázky a animace.

Po absolvování kurzu by studenti měli být schopni se orientovat v problematice počítačové infiltrace a obrany proti ní a měli by být též schopni vysvětlit jednotlivé pojmy a demonstrovat je na příkladech. Kurz bude užitečný i studentům, kteří před započetím studia již mají zkušenosti v oblasti počítačové infiltrace a obrany, neboť jim dopomůže si danou problematiku zopakovat a rozšířit svoje znalosti o nové poznatky.

Pro nadčasovost e-kurzu je nutné jej pravidelně aktualizovat, neboť studenti by měli být o nových hrozbách informováni z toho důvodu, že malware a podvodné techniky na internetu se neustále vyvíjejí

Tvorba bakalářské práce byla zábavná a velmi obohacující nejen díky prohloubení znalostí popisovaného tématu, ale také z hlediska tvůrčího přemýšlení a zdokonalení se v práci s jednotlivými programy využívaných při tvorbě elektronického kurzu.

6 SEZNAM OBRÁZKŮ

7 SEZNAM LITERATURY

1. RENTEL a.s. *Autorský systém ProAuthor.* [Online] http://rentel.cz/rentel/rentelweb.nsf/0/proauthor.

2. **Brichta, Ondřej.** www.zive.cz. *Recenze Macromedia Captivate - pomocník při výuce počítačových programů.* [Online] 9. 5 2005. http://www.zive.cz/clanky/recenze-macromedia-captivate---pomocnik-pri-vyuce-pocitacovych-programu/sc-3-a-124410/default.aspx.

3. **Szor, Peter.** *Počítačové viry: analýza útoku a obrana.* Brno : Zoner Press, 2006. 80-868-1504-8.

4. **KRÁL, Mojmír.** *Bezpečnost domácího počítače: prakticky a názorně.* Praha : Grada Publishing, a.s., 2006. 80-247-1408-6.

5. Živě. [Online] 1996-2012. www.zive.cz.

6. Hoax. [Online] 2000-2012. www.hoax.cz.

7. Lupa.cz. [Online] 1998-2012. www.lupa.cz.

8 RESUMÉ

The main task of the bachelor thesis was to create an electronic course in the authorial system „ProAuthor“, that will serve as a support for students from distance form of studies. The result is highquality study material, which could be extended and used by students

During the creating of e-course was unnecessary to deal with various problems, that appeared and it was not able to omit them. These problems were specified in more detail in the previous chapters. Despite of all problems there was an effort to move closer to the successful end.

The difficulty of the whole e-course was chosen on the basic level, which corresponds to the content of particular study articles. To reach the attractiveness of the program were study articles enriched by pictures and animations.

After finishing the e-course students should be knowledgeable in issues dealing with computer inflitration and protection against it. They should be also able to explain particular expressions and illustrate them on examples. The course will be also useful to students, that have some previous experiences in the field of infiltration and protection before beginning with course, because this is a good way how to review the issues and to extend them with new piece of knowledge.

Dealing with timelessness, periodical updating will be necessary, because students have to be informed about new threats due to the development of malware and fraudulent techniques.

Creating of the bachelor thesis was funny and really enriching not only becasuse of the widening of knowloedge about described issue, but also from the point of view of creative thinking and improvement in the work with particular programs that are being used when the e-course is being created.

9 PŘÍLOHY

Přílohou této bakalářské práce je CD, na kterém jsou zdrojové kódy elektronického kurzu, vygenerovaný elektronický kurz a tato textová část ve formátu pdf a docx. Na tomto CD byly vytvořeny celkem tři složky. Konkrétně složky BP, E-kurz, Zdrojove_kody