HODNOCENÍ BAKALÁŘSKÉ PRÁCE

Oponent práce

Autor práce: Veronika Staňková

Název tématu: Softwarové zabezpečení osobního počítače v systémech Windows

Splnění bodů zadání	○ úplně	◉ částečně	○ nesplněno
Případný komentář:			

	Předmět hodnocení	Nadprůměrné	Průměrné	Podprůměrné
1	Formulace cílů a metodika zpracování práce	○	○	◉
2	Logická struktura a členění práce	○	○	◉
3	Rozsah a úroveň použitých zdrojů, bibliografické citace (dle platné ČSN ISO), poznámkový aparát	○	○	◉
4	Jazyková, stylistická úroveň a formální úprava práce	○	○	◉
5	Kvalita zpracování tématu práce	○	○	◉
6	Formulace vlastních závěrů, vlastní přínos autora práce	○	○	◉
7		○	○	○

Doplnění hodnocení, připomínky, dotazy:
Není formulován cíl práce. O metodice se v práci dozvídáme pouze zprostředkovaně v konkrétní podobě na několika málo místech. Pokud se tak děje, jedná se často o nepřehledně zmatečný způsob. Na s. 22 dole lze nalézt nesrozumitelné vysvětlení toho, že v prvních dvou tabulkách jsou zařazeny pouze antivirové systémy, které se účastní více než jednoho ze čtyř jmenovaných testů, což je však vzápětí v první tabulce popřeno, protože v ní nacházíme např. Comodo IS, který se účastnil pouze jednoho z nich. Metodicky dobře nepůsobí ani velmi vágní a krátká kapitola o kritériích hodnocení antivirových systémů na s. 25, která měla patřit v práci mezi klíčové. Není tedy překvapivé, že u doporučených antivirových systémů ve čtvrté kapitole tato kritéria nejsou dostatečně aplikována. Výběr zvolených testů je zdůvodněn velmi vágně v jedné větě. Významnou metodickou chybou je také podcenění časového vlivu (výběr malého počtu časových období u některých testů, které navíc nejdou až do měsíce, v němž byla práce odevzdána). U všech popsaných testů chybí interpretace výsledků pod jejich tabulkami. Vážnou metodickou chybou je i nedostatečné zdůvodnění způsobu přepočtů výsledků (počínaje např. volbou váhy jednotlivých testů). Nedostatečně odůvodněné je i připisování mediánu netestovaným produktům (např. i kvůli tomu, že se v něm mísí komerční a nekomerční produkty).
Text práce není jako celek dobře strukturován podle zadání. Kapitola o historii působí nadbytečným dojmem. U jednotlivých druhů počítačových rizik se naopak v zadání práce požadovaná stručná historie s dostatečným množstvím konkrétních příkladů nenachází. Naopak lze u některých nalézt rovnou odkazy na způsoby ochrany, které by se měly v práci nacházet až později (např. u stealth virů). Členění první kapitoly se od s. 6 zdá být určeno náhodným pořadím (spyware a adware mezi makroviry a skriptovými viry apod.). Členění informací ve třetí kapitole je špatné, protože již na s. 22 je operováno s testy, které budou představeny až posléze. Mezi kapitolami 3 a 4 se některé informace zbytečně dublují a dochází se na jejich základě k pozoruhodně rozdílným závěrům (např. na s. 37 je Comodo IS doporučován, v další kapitole je již psáno, že je jeho hodnocení zjevně zkresleno). Překvapivě až v kapitole představující vybrané produkty se dozvídáme zásadní věci k připisování výsledků testů jednotlivým produktům (např. Avast! a AV-test).
Úroveň použitých zdrojů je místy velmi pochybná. Týká se to např. seznamu použitých odborných výrazů a zkratek, kde autorka uvádí v nevhodné obecné podobě Wikipedii, kterou nelze pro práci tohoto druhu chápat jako relevantní zdroj. Poznámky pod čarou použité k doplnění zdrojů ke kapitolám jako celku

vyvolávají dojem, že uvedené kapitoly nemají žádný vlastní přínos autorky práce. Práce se zdroji zde proběhla špatně. Podobně je chybou, že k argumentaci o rozšíření spamu jsou použity dva roky staré statistiky.
Jazyková úroveň je standardní. Text bakalářské práce je ovšem překvapivě napsán v první osobě jednotného čísla. Formálně se v práci nachází mnohé nedostatky (např. spojovníky na místech, kde by měly být pomlčky, nesrozumitelné spojení „panická historie" na s. 2, apod.). Text je psán nečekaně literárním stylem (např. spojení „pěknou ostudu" na s. 3). V textu práce se mísí náhodně minulý a přítomný čas (nejen např. na s. 3 dole). V textu lze nalézt překvapivě krátké odstavce, které obsahují i pouhou jedinou větu. V práci se nachází velké množství nekvalitních obrázků (nejen např. obrázek 10 na s. 44). U výčtu na přelomu s. 4 a 5 chybí odrážky. V textu se vyskytují chyby v zápisu procent (rozdíl mezi 90 % a 90%). Podstatně lépe měly být využity pevné mezery. V práci se nachází kapitoly, které obsahují pouze tabulku. Pod tabulkami se běžně nachází poznámky s hvězdičkami, které v tabulce nejsou použity. V práci lze nalézt nesmyslně volné části (např. na s. 25 dole). V práci se na mnoha místech objevuje chybně matouseck.com. Barevné zvýraznění v některých případech zhoršilo čitelnost tabulek. V tabulce č. 4 na s. 28 jsou modré všechny řádky, což značí, že poznámka u dvou hvězdiček ztrácí smysl.
Kvalitu zpracování tématu práce snižují mnohé nedodělky. V již kritizované kapitole o historii chybí mnohé významné skutečnosti (např. proč se příslušný vir jmenoval Michelangelo a jeho šíření bylo ohlášeno na 6. března). V téže kapitole nacházíme i velmi nečekaná sdělení (např. na s. 3 se dozvídáme, že posledním známým virový hit se vyskytl v roce 2000). Vše vyplývá ze špatné práce s již zmíněnými nepříliš kvalitními zdroji (v kapitole o historii jde o sekundární zdroj, který je pouze neuměle přepsán). Je překvapivé, že se v kapitole o základních druzích softwarových bezpečnostních rizik v některých částech nevyskytují jasné definice (vše začíná již částí o virech, kde je více slov věnováno tomu, co virus není). Nedošlo ani k dobrému vysvětlení mnoha podstatných skutečností (např. rozdělení virů na rezidentní a nerezidentní a jejich vztah k boot virům). Mnohá vysvětlení jsou neúplná (např. pouze jeden z způsobů využití zranitelnosti pomocí exploitu apod.). Ve druhé kapitole nejsou dostatečně popsány jednotlivé prvky ochrany a jejich funkce (např. jasné pojmenování různých činností antivirového systému, fungování antispamu apod.). Není v ní ani patrné, že jednotlivé druhy ochrany jsou dnes již často integrovány společně v jednom balíku. Překvapivě velký prostor je věnován Centru zabezpečení v MS Windows, v němž jsou opakovaně popsány věci, které by měly být dříve podrobněji zmíněny samostatně (např. o aktualizacích, firewallu atd.). Ve třetí kapitole je na konci prvního odstavce napsáno, že první dvě tabulky mohou uživatelům pomoci v první fázi výběru antivirového nástroje, aniž by bylo zmíněno, jakým způsobem se tak má dít. O jednotlivých testech se dozvídáme v práci málo informací (počínaje tím, že většinou není např. ani zřejmé, kdo za nimi stojí). V tabulce č. 5 se mnoho informací ztrácí (např. není jasné, zda jde u některých produktů o placenou verzi). U tabulky č. 7 je nedostatečné vysvětlení, které navíc nesouhlasí s jejím obsahem (např. v záhlaví je pouze AV-comp. 2/2011). Popisy vybraných antivirových systémů jsou velmi obecné a působí spíše jako reklamní sdělení.
Vlastní přínos autorky v práci uvádí často čtenáře práce do nejistoty (např. na s. 23 Avast! Free Antivirus 64bitovou verzi nemá, na s. 41 ji ovšem již obsahuje). Autorka vybrala obecně dobré testy, ale práce s nimi dopadla podstatně hůře (např. výsledky v příloze 1 u Avast! Free Antivirus nesouhlasí s údaji, které jsou uvedeny v tabulce č. 4). Kvůli uživatelům navíc mohly být pro porovnání zařazeny i další z jiných zdrojů (např. periodik). Ve vlastním zhodnocení výsledků testu se nachází další nedostatky (např. porovnávání procent u nejlepšího nekomerčního a komerčního produktu a vyvozování závěrů z nich, i když se nekomerční produkt zúčastnil jediného testu). Výsledky hodnocení jsou interpretovány pokaždé jinak (např. na s. 36 se vyplatí si připlatit za komerční produkt, na s. 39 je však již nepochybné, že kombinace více nekomerčních řešení je plně dostačující). V závěru práce autorka konstatuje, že bezpečnostní balíky jsou si velmi podobné, což je pro úspěšné vyústění bakalářské práce velmi málo.
Navržená známka odpovídá plně výše zmíněným zásadním nedostatkům.

Otázky k obhajobě:
1. Na jaké období a proč bylo načasováno šíření ILOVEYOU?
2. Jaké znáte konkrétní stealth viry pod Windows?
3. Jaký je vztah mezi trojským koněm, downloaderem a backdoorem?
4. Jakým způsobem probíhá detekce rootkitu?
5. Existují statistiky podporující tvrzení na s. 15 o službě Gmail a jejím antispamovém filtru?
6. Jaké konkrétní možnosti zabezpečení představuje Centrum zabezpečení v OS MS Windows?
7. Jaká kritéria hodnocení splňují v práci doporučené antivirové systémy?
8. Jaké jsou výsledky testů antivirových systémů, které jsou uveřejňovány pravidelně v odborných periodicích?
9. Jaký je rozdíl mezi prázdnými a různě formátovanými buňkami s obsahem N/A v tabulce č. 5 na s. 30?

Celkové hodnocení práce	○ **výborně**	○ **velmi dobře**	○ **dobře**	◉ **nevyhovující**

Hodnocení vypracoval: Mgr. Zbyněk Filipi

2.7.2012
Datum

Podpis