Marketingové problémy predmetu Etický hacking

Marketingové problémy predmetu Etický hacking

Marketingové problémy predmetu s názvom Etický hacking, ktorý je vyučovaný na Fakulte managementu Univerzity Komenského v Bratislave sú obsahom predkladaného príspevku. Východiskom je pochopenie aktuálnosti a potenciál inovatívnosti témy etického hackingu v súvislosti s prácou manažéra a následne priblíženie priebehu výučby tohto predmetu. Vzdelávanie študentov prebieha bezpečne pomocou systému virtualizačného prostredia openStack, v ktorom majú študenti možnosť skúšať a testovať informačné a operačné systémy vrátanie sietí v tzv. „sandboxe“ bez rizika interferencie a poškodenia školskej siete. Marketingová podpora predmetu má za cieľ zvýšiť záujem relevantnej cieľovej skupiny študentov, ktorí po ukončení vysokoškolského vzdelania zhodnotia získané poznatky v praxi a budú komunikovať prospešnosť predmetu u študentov rozhodujúcich sa o výbere predmetu Etický hacking.

Úvod

Etický hacking je v súčasnom globalizovanom svete IS/IT prvkom, ktorý rozhoduje o architektúre IS/ICT v podnikoch. Všetky podniky v súčasnosti spracovávajú citlivé dáta ako napr. osobné údaje, preto podľa legislatívy musia vytvoriť bezpečnostný projekt a musia sa zaoberať manažmentom bezpečnosti. Praktickou stránkou testovania bezpečnosti IS/ICT vo firmách je práve etický hacking. Ide o využívanie bežne dostupných, ako aj menej dostupných techník ako sa dostať do systémov, prípadne ich poškodiť. Manažér nemôže tvrdiť, že jeho informačný systém je bezpečný, pokiaľ nespracoval komplexnú sadu bezpečnostných testov a nevyhodnotil ich z hľadiska závažnosti. V súčasnosti existuje medzinárodný štandard OWASP – Open Web Application Security Project, ktorý definuje postupné kroky, ako vykonávať dané testy (OWASP 2016). Na vykonanie týchto krokov v mene spoločnosti je však potrebný špecialista, tzv. „etický hacker“, ktorý musí disponovať dostatočnými znalosťami v tejto oblasti. Príprava týchto špecialistov vyžaduje nielen teoretické poznatky, ale najmä praktické skúsenosti.

Obsah predmetu

Obsahom predmetu Etický hacking je objasniť zložitosť a rozsah problému zabezpečenia systémov pre spracovanie údajov a poskytovanie informácií s dôrazom na úlohu manažéra v procese budovania a prevádzkovania takýchto systémov (Karovič et al. 2016a, Karovič et al. 2016b). Úvod tvoria všeobecné základy bezpečnosti a vymedzenie pojmu „bezpečný informačný systém“. Ďalej sú rozobrané základné technické a programové prostriedky ochrany IS a špecifiká bezpečnosti v sieťach. Kľúčové sú rozdiely pre zásady bezpečnosti pri procese vzniku IS a zásady bezpečnosti pri prevádzke IS. Ľudský faktor a bezpečnostná kultúra organizácie majú napomôcť pri chápaní úlohy manažéra bezpečnosti v organizácii. Teoretické poznatky sú nakoniec zhrnuté v základných bezpečnostných princípoch (Drahošová a Karovič 2015b). Študent sa taktiež má oboznámiť s úlohou

auditu IS. Z týchto tematických okruhov boli v predmete naplánované jednotlivé semináre, ktoré je možné vnímať ako ucelený tematický plán.

Tematický plán predmetu Etický hacking zahŕňa nasledovné oblasti:
1. Úvod do etického hackingu
2. Praktická ukážka nástrojov určených pre penetračné testovanie
3. Praktická ukážka penetračného testu IT bezpečnosti servera
4. Základné princípy počítačových vírusov
5. Demonštrácia monitorovania sietí
6. Možnosti priamych útokov na sieťové zariadenia
7. Demonštrácia možnosti ochrany proti technikám hackerov
8. Personálna bezpečnosť a bezpečnosť biometrických osobných údajov
9. ISO 27001 – systém manažmentu bezpečnosti
10. Zákon č. 122/2013 Z.z. – Zákon o ochrane osobných údajov
11. OWASP – Open Web Application Security Project
13. Sociálne inžinierstvo
14. Trendy v manažmente bezpečnosti
15. Študentský battle v sandboxe

Po úspešnom absolvovaní by mali študenti ovládať základy IT bezpečnosti a mali by byť schopní testovať bezpečnosť IS/ICT vo firme, uplatňovať princípy informačnej bezpečnosti IS/IT vo svojej manažérskej praxi a aktívne pôsobiť v rámci systému riadenia informačnej bezpečnosti vo firme v rôznych fázach vývoja životného cyklu IS/IT.

Inovácia výučby

Inovácia výučby spočíva v použití virtualizačného nástroja simulujúceho reálne sieťové riešenie IS/IKT. Cieľ a prínos výučby je v získaní empirických skúseností vďaka možnosti prakticky vyskúšať techniky útočníka-hackera aj ochrancu-administrátora alebo manažéra bezpečnosti IS/IKT. Na záver semestra bola pre študentov pripravená a odskúšaná malá súťaž, tzv. „študentský battle v sandboxe“. Prvá skupina študentov má za úlohu upraviť a nastaviť zámerne zle zabezpečené technologické riešenia, ktoré boli vytvorené lektorom. Študenti majú k dispozícii komplexnú sieť s aktívnymi sieťovými prvkami a pripravenými aplikáciami, ktoré však nepripravovali oni sami. Druhá, súperiaca skupina študentov má za úlohu hľadať chyby v zabezpečení po opravách prvej skupiny. Obe skupiny študentov predmetu Etický hacking musia realizovať tzv. „black test“ podľa OWASP s nasadením systému Kali Linux (Karovič 2013; Drahošová a Karovič 2015a). Študenti tak majú možnosť reálne otestovať svoje vedomosti a zručnosti a získať tak empirické skúsenosti s ochranou IS/ICT. Práve vďaka praktickým cvičeniam získajú predstavu o penetračných testoch a osvoja si zásady pri riadení bezpečnosti v organizácii.

Marketingové problémy

Etický hacking je nový výberový predmet v učebných osnovách a v súčasnej dobe nie je vyučovaný na žiadnej inej vysokej škole resp. univerzite v Slovenskej republike. Z pohľadu marketingovej teórie je možné považovať tento predmet za produkt, ktorý je zaradený do ponuky ďalších výberových predmetov na Fakulte managementu Univerzity Komenského v Bratislave. Z tejto ponuky si študenti môžu vybrať tie predmety, ktoré sú z ich pohľadu dostatočne atraktívne. Atraktivita predmetu môže byť zložená z rôznych aspektov, ako napríklad: záujem o samotný obsah predmetu a uplatnenie v praxi po ukončení štúdia, záujem o získanie kontaktov na prednášajúcich podieľajúcich sa na výučbe,

záujem o získanie hodnotenia resp. kreditov za absolvované štúdium a ďalšie benefity. Výberový predmet sa musí stať dostatočne atraktívnym, pokiaľ má študentov zaujať a tí ho majú uprednostniť pred ďalšími.
Z pohľadu atraktivity témy je možné považovať za zaujímavé zistenie prieskumu Eurobarometra (European Commission 2015) realizovaného v roku 2015 v krajinách Európskej únie, že na Slovensku pokladá počítačovú kriminalitu za problém spoločnosti iba 13% opýtaných Slovákov, pričom za najdôležitejší problém bola označená chudoba (37%), terorizmus (36%) a korupcia (34%). Z tohto pohľadu sa môže javiť problematika hackingu ako špecifická a menej podstatná vo vnímaní celej spoločnosti. O to zaujímavejšie vyznievajú zistenia prieskumu z toho istého roku medzi študentmi Obchodnej fakulty Ekonomickej univerzity v Bratislave (Vokounová 2016), ktorí označili počítačovú kriminalitu za najmenej závažný faktor bezpečnosti spoločnosti (8,5%). Tieto zistenia naznačujú, že téma etického hackingu bude považovaná za menej významná u študentov spoločensko-vedných odborov vo všeobecnosti.
Ďalším faktorom vplývajúcim na atraktivitu predmetu je samotný názov. So slovami „hacking“ „hacker“ sa spája už vo svojej podstate negatívna činnosť, ktorá má byť eliminovaná a od ktorej sa treba dištancovať. Avšak pôvodne sa pod pojmom „hacks“ označovali činnosti na vylepšovanie programov, ktoré mali zvýšiť výkon počítačov. Teda hacking mal pôvodne pozitívny význam. Až neskôr sa začal spájať s aktivitami organizovanými za účelom osobného prospechu (Engebretson 2013). Prívlastok „etický“ dodáva hackingovým aktivitám jasnejší význam. Ide o činnosti a nástroje, ktoré hacker používa za účelom vylepšenia bezpečnosti systémov. Ide o odborníka, ktorý pozná slabé a zraniteľné miesta v systémoch a pri ich ochrane využíva poznatky o správaní útočníkov. Napriek tomu je možné predpokladať, že obsah predmetu Etický hacking bude pre študentov vyvolávať kontroverzné predstavy. Čo však môže byť aj pozitívom, že sa v ponuke ďalších predmetov odlíši.
Pre zvýšenie atraktivity predmetu je potrebné bližšie špecifikovať cieľovú skupinu študentov, ktorým je určený. Primárnu skupinu tvoria študenti so zameraním na manažment informačných systémov. Tejto skupine študentov sa nemusí javiť problematika hackingu ako okrajová a dokonca ani neznáma. Nakoľko ponuka výberových predmetov je pestrá a študenti si ich môžu vyberať aj z ponuky ďalších katedier bolo by zaujímavé uvažovať aj nad oslovením študentov so zameraním na ďalšie funkčné oblasti manažmentu ako napr. marketing, finančný manažment či personálny manažment. Dôvodom je praktické zameranie informačných systémov, ktoré sú súčasťou práce každého manažéra, bez ohľadu na jeho špecializáciu. Podstatným je obsah predmetu a jeho posolstvo pre všetkých študentov/budúcich riadiacich pracovníkov organizácie: Bezpečnosť informačného systému nie je iba otázkou oddelenia informačných systémov. Napríklad marketing firmy sa snaží priblížiť zákazníkovi čo najbližšie, ponúknuť mu hodnotný produkt a to čo pri najmenších nákladoch. Marketéri preto vo svojej práci využívajú databázy, on-line databázy, elektronické obchodovanie, umožňujú zákazníkovi sledovať pohyb objednaného tovaru a platiť za tento tovar bezhotovostne. No v projektoch na priblíženie sa k zákazníkovi zostáva opomenutá bezpečnosť komunikácie a uchovávanie informácií. Únik informácií sa netýka iba malých organizácií. Aj profesionálna internetová spoločnosť Yahoo musela v septembri 2016 priznať, že v roku 2014 došlo k veľkému úniku informácií o najmenej 500 miliónoch užívateľov (Pcrevue.sk 2016). Ponúknutie služieb on-line prístupu do informačných systémov organizácie predstavuje riziko, preto je potrebné počítať s jeho minimalizáciou už na začiatku, pri koncipovaní návrhu rozpočtu projektu vrátane položky bezpečnosť informačného systému. V opačnom prípade môže byť strata súkromia zákazníka spojená s negatívnym postojom a stratou dôvery. Treťou potenciálnou skupinou študentov so záujmom o predmet môžu byť všetci študenti Univerzity Komenského v Bratislave, ktorým umožňuje čl. 21 ods. 5 Študijného poriadku univerzity (2015) zapísať si výberový predmet aj z inej ako domácej fakulty.
Konkrétnym opatrením na zvýšenie záujmu študentov o predmet by mala byť cielená marketingová komunikácia s vyššie uvedenými skupinami študentov. Samotný predmet sa nachádza v ponuke výberových predmetov vo fakultnej ročenke, ktorú študenti dostávajú pri zápise. Na začiatku akademického roka, keď si študenti zostavujú študijný plán by mali dostať informáciu o obsahovej náplni predmetu. Možno pri tom využiť informačné nástenky, elektronickú poštu, letáky. Tiež by bolo

možné zorganizovať informačnú prezentáciu predmetu pred zápismi. Veľmi efektívnou formou komunikácie by mohla byť sila hovoreného slova, kedy by študenti po absolvovaní predmetu poskytli referencie spolužiakom. K predmetu by bolo možné vytvoriť komunitnú webovskú stránku alebo stránku na sociálnej sieti a napĺňať jej obsah diskusiami k téme etického hackingu. Na samotnom predmete by mohli participovať odborníci z praxe, čo by mohlo zvýšiť záujem študentov pri získavaní priameho kontaktu s potenciálnymi zamestnávateľmi a uplatnením sa po ukončení štúdia. Zabezpečenie spätnej väzby k obsahu a forme výučby zo strany študenta by mohlo zvýšiť užitočnosť predmetu a zefektívniť prácu vyučujúcich. Ideálnym stavom by malo byť vytvorenie podmienok na šírenie dobrého povedomia o predmete a jeho prínose, ktoré by sa šírilo spolu s komunikačnými aktivitami vyučujúcich – učiteľov aj zástupcov z praxe.

Záver

V súčasnej dobe je ochrana a zabezpečenie informačného systému respektíve ochrana informácií veľmi zásadnou úlohou manažérov a to nielen v podnikovej sfére. Príprava manažérov na úlohu spojenú s ochranou informácií môže začať už na školách pomocou výučby a to nielen v teoretickej rovine. Predmet Etický hacking pomocou praktického cvičenia, ukážkami techník a premýšľania nad slabými miestami informačných systémov môže napomôcť budúcim manažérom pri riadení bezpečnosti toku informácií v organizáciách (Múčková, Karovič a Krajčík 2015). Výučba predmetu bez použitia virtuálneho prostredia openStack bola veľmi náročnou úlohou a väčšinu ukážok techník a nástrojov nebolo možné realizovať, vzhľadom na zabezpečenie školskej siete. Použitím softvéru openStack bolo dosiahnuté oddelenie systému zabezpečujúceho chod školy a výukového – testovacieho prostredia, v ktorom bolo možné rýchle nasadenie rôznych modelov a testovanie ich bezpečnosti (Openstack, 2016). Najdôležitejším parametrom bolo zabezpečenie oddelenia kritických častí školskej siete od modelov sieti a technológií tvorených vo virtuálnom prostredí openStacku, avšak so zabezpečením prístupu do internetu, čím sme dosiahli, že sa systém javil ako reálny. Prostredie bolo testované jeden semester a výučba prebehla s ohľadom možnosti servera a prispôsobené na jeho funkcionality. Plán budúcej výučby predmetu je orientovaný na zavedenie hybridnej architektúry a testovanie aj iných systémov a architektúr siete.
Marketingové problémy predmetu etický hacking vychádzajú z praktických skúseností s jeho vyučovaním. Súvisia s niekoľkými aspektmi: vnímanie opodstatnenosti témy hackingu u študentov informačných systémov, ale aj študentov ďalších zameraní a formami komunikácie prínosov štúdia predmetu Etický hacking vyplývajúcich z jeho obsahového zamerania. Za kritický faktor v podpore predmetu je možné považovať silu hovoreného slova, marketingovú komunikáciu a spätnú väzbu od študentov.

Literatúra/List of References

[1] Drahošová, M. a Karovič, V., 2015a. Cloud and virtualization in Linux environment. In: CER Comparative European research 2015: International Scientific Conference for PhD students of EU countries [4th]. Londýn, s. 130-33. ISBN 978-0-9928772-8-6. [online]. [cit. 2016-10-13]. Dostupné na: <http://www.sciemcee.org/library/proceedings/cer/cer2015_proceedings02.pdf>
[2] Drahošová, M. a Karovič, V., 2015b. Information security. In: CER Comparative European research 2015 : International Scientific Conference for PhD students of EU countries [4th] – Londýn, s. 134-37. ISBN 978-0-9928772-8-6. [online]. [cit. 2016-10-13]. Dostupné na: <http://www.sciemcee.org/library/proceedings/cer/cer2015_proceedings02.pdf>
[3] Engebretson, P., 2013. The basics of hacking and penetration testing. Ethical hacking and penetration testing made easy. Elsevier, 2013. ISBN 978-0-12-411644-3.
[4] European Commission, 2015. Special Eurobarometer 432, 2015. Europeans´Attitudes Towards Security. [online]. [cit. 2015-08-15]. Dostupné na:

<http://ec.europa.eu/public_opinion/archives/ebs/ebs_432_en.pdf>
[5] Karovič, V., 2013. Linux. In: Digital Science Magazine. 2013. ISSN 1339-3782. [online]. [cit. 2016-04-29]. Dostupné na: <http://digitalmag.sk/linux/>
[6] Karovič, V., Karovič, V., Veselý, P., Olšavský, F. a Greguš, M., 2016a. Nasadenie virtualizačného prostredia openstack na výučbové účely. In: Marketing Science and Inspirations. 2016, 11(1), s. 43-52. ISSN 1338-7944.
[7] Karovič, V., Karovič, V., Veselý, P., Olšavský, F. a Greguš, M., 2016b. Nasadenie virtualizačného prostredia openstack na výučbové účely. In: Marketing Science and Inspirations. 2016, 11(2), s. 2-5. ISSN 1338-7944.
[8] Múčková, O., Karovič, V. a Krajčík, M., 2015. Bezpečnosť ako jeden z prvkov integrovaného systému manažérstva. In: Digital Science Magazine. 2015. ISSN 1339-3782. [online]. [cit. 2016-04-29]. Dostupné na: <http://digitalmag.sk/bezpecnost_ako_jeden_z_prvkov/>
[9] Openstack, 2016. OpenStack Docs: Overview and components, 2016. [online]. [cit. 2016-10-13]. Dostupné na:
<http://docs.openstack.org/liberty/networking-guide/intro-os-networking-overview.html>
[10] OWASP, 2016. [online]. [cit. 2016-10-13]. Dostupné na:
<https://www.owasp.org/index.php/Main_Page>
[11] Pcrevue.sk, 2016. Yahoo potvrdilo veľký únik informácií z roku 2014, 2016. [online]. [cit. 2016-10-13]. Dostupné na:
<http://www.pcrevue.sk/a/Yahoo-potvrdilo-velky-unik-informacii-z-roku-2014>
[12] Vnútorný predpis č. 8/2015 Univerzity Komenského v Bratislave, Študijný poriadok
[13] Vokounová, D., 2016. Rebríček hodnôt mladých ľudí a ich postoj k prisťahovalectvu. In: Marketing Science and Inspirations. 2016, 11(4). ISSN 1338-7944.

Kľúčové slová/Key Words

etický hacking, marketing predmetu, sila hovoreného slova, marketingová komunikácia
ethical hacking, marketing of subject, word of mouth, marketing communication

JEL klasifikácia

I23, M31

Résumé

Marketing problems of subject called Ethical hacking

Marketing problems of subject called ethical hacking, which is taught at the Faculty of Management at Comenius University in Bratislava are listed below. The starting point is to understand the timeline and potential of innovation of topics of ethical hacking in connection with the work of managers elucidated during this teaching subjects. Education of students progresses through the security system OpenStack virtualization environments in which students have the opportunity to test information operating systems including the so-called “Sandbox” without risk of interference damage to the school network. Marketing support of subject aims to increase the interest of relevant target groups of learners who, after completing university education will evaluate the lessons learned in practice, we communicate the usefulness of the object in the student’s Crucial is the choice of subjects Ethical Hacking. A critical factor in promoting the subject can be considered the strength of the spoken word marketing communication tools.

Kontakt na autorov/Address

Ing. Vincent Karovič, PhD., Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: vincent.karovic@fm.uniba.sk

Mgr. Vincent Karovič, Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: vincent.karovic2@fm.uniba.sk

PhDr. Peter Veselý, PhD., MBA, Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: peter.vesely@fm.uniba.sk

Mgr. František Olšavský, PhD., Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: frantisek.olsavsky@fm.uniba.sk

Recenzované/Reviewed

10. november 2016 / 13. november 2016

Nasadenie virtualizačného prostredia OpenStack na výučbové účely. Časť II.

Nasadenie virtualizačného prostredia OpenStack na výučbové účely. Časť II.

Hlavným cieľom nasadenia virtualizačného prostredia OpenStack na výučbu je poskytnúť lektorom a študentom plnohodnotné konfigurovateľné prostredie pre rôzne predmety výučby modelovania reálnych procesov. Pre potreby príspevku sú predstavené možnosti využitia OpenStacku ako voľne dostupného open source softvéru vo vyučovaní predmetov Účtovníctvo na počítači, Etický hacking, Manažment bezpečnosti a Marketingový výskum. Implementácia virtualizácie vychádza pri každom predmete z jeho obsahového zamerania s dôrazom na čo najvernejšie zobrazenie reálnych podmienok hospodárskej praxe. Nakoľko existujú relevantné obmedzenia pri práci s údajmi, či už na úrovni technického zabezpečenia pri ich získavaní, spracovaní, distribúcie, ich ochrany, ale aj zabezpečenia celého informačného systému, v návrhovej časti sa za jednotlivé predmety uvádzajú konkrétne riešenia, ako tieto úzke miesta prekonať. Na záver sú identifikované prínosy navrhovaných riešení pre inováciu samotnej výučby s dôrazom na realizovateľnosť a simuláciu čo najvernejších podmienok, s ktorými sa študenti môžu stretnúť v praxi.

2.4. Marketingový výskum

Cieľom predmetu je poskytnúť študentom poznatky o poslaní, procese a aplikácii metód marketingového výskumu s dôrazom na jeho praktické využitie v marketingovom manažmente. Marketingový výskum je prezentovaný ako nástroj, prostredníctvom ktorého sú prepojení marketingoví manažéri so spotrebiteľmi, zákazníkmi a verejnosťou (Richterová 2006, s. 9). Predmet poskytuje pohľad na informačné potreby podniku a konfrontuje ich s potenciálom jednotlivých nástrojov marketingového výskumu tieto informácie získať, spracovať a interpretovať.

Riešený problém:
Študenti počas prednášok majú možnosť sa oboznámiť s procesmi získavania, spracovania a interpretácie marketingového výskumu. Veľmi vhodnou a v praxi marketingového výskumu dnes už nevyhnutnou požiadavkou je zapojenie informačných technológií. Tieto nachádzajú uplatnenie v celom procese realizácie marketingového výskumu počnúc identifikovaním potreby nedostatku konkrétnych informácií pre manažérske rozhodovanie až po realizáciu samotného prieskumu v praxi formou elektronického dopytovania, využitia technických prostriedkov v procese pozorovania a následne spracovania získaných údajov. Keďže zásadným problémom v marketingovom výskume je dodržať základné princípy – objektivita, etika a systematika marketingového výskumu (Richterová 2006, s. 12-14) a súčasne je možné zaznamenávať tlak na zvyšovanie efektivity realizácie aktivít marketingového výskumu obzvlášť v podmienkach medzinárodného marketingu, stáva sa využitie výpočtovej techniky nevyhnutnosťou. Problém vo vyučovaní nastáva s obmedzenými užívateľskými právami, ako aj s možnosťou využitia rôznych platforiem komerčných aj voľne prístupných pri realizácii elektronického dopytovania ako napríklad qualtrics.com (2016), surveymonkey.com (2016) alebo google docs (2016). V súčasnosti neexistuje univerzitná platforma pre realizáciu elektronického dotazníka pre študentov na Univerzite Komenského v Bratislave. Keďže využitie komerčných aplikácií je pre študentov obmedzené, nemajú tak priestor plne využiť všetky možnosti, ktoré by za bežných okolností v business sfére mali k dispozícii. Ide hlavne o problém spustenia WEB aplikácií tak, aby tam mohli na nich realizovať najmä zber údajov, ich kontrolu, cielené zameranie na požadovaný segment respondentov, či ako uvádza Vilčeková (2010) zabezpečenie veľkosti vzorky.

Navrhované riešenie:
Virtualizácia vytvorí niekoľko databázových serverov a prezentačných serverov založených na odlišných technológiách, ako je napr. PHP, MySQL alebo MS SQL, .NET 4.X. Správca siete vytvorí viacero image virtualizovaných systémov, pretože si vyžadujú prvotne množstvo nastavení a bezpečnostných politík. Vyučujúci tieto image potom môže ľubovoľne nasadzovať, pričom študentom poskytne plnohodnotné prístupy tak, ako by ich mali realizované v business sfére. Tak sa dá aplikovať množstvo prípadov nasadenia výpočtovej techniky pri marketingovom výskume. Marketingový výskum by takto presnejšie reflektoval požiadavky na marketingový manažment v rozsahu nových prístupov ako uvádzajú Pajtinková a Gubíniová (2014), ale aj v ochrane značiek ako uvádza Smolková (2014), či pri komunikácii vernostných programov v maloobchode (Šeliga a Štarchoň 2013).

Inovácia výučby:
Tak ako v predchádzajúcom prípade je možnosť aj tu realizovať tzv. študentský battle v sandboxe. Tento spôsob realizácie je vhodný pre študentov na uvedomenie si, že aj zdanlivo jednoduchá operácia zberu dát napríklad cez elektronický dotazník alebo zapojenie technických prostriedkov pri pozorovaní môže predstavovať veľmi veľké bezpečnostné riziko. Realizácia takéhoto spôsobu výučby študentom prinesie priame skúsenosti s nasadením výpočtovej techniky pri realizácii aktivít marketingového výskumu, čo doteraz bolo možné iba vo veľmi obmedzenej miere.

Záver

Mimoriadne dôležitý aspekt virtualizácie vo výučbovom procese je, že výučba sa dostala do miesta, kde zdroje spoločnosti nie sú dostačujúce na poskytovanie zodpovedajúcej hardvérovej výbavy pri zodpovedajúcej softvérovej skladbe a nutnej pružnosti pri často sa meniacich požiadavkách na systémy výpočtovej techniky. Paradoxne tento stav priviedol k postupu vpred, čo má za následok aj zvýšenie úrovne vzdelania v tejto oblasti. Moderné hardvérové výpočtové kapacity sú obvykle nákladné a pri zvyšovaní ich množstva narastá počet ľudí, ktorí sa ako administrátori rôznych úrovní musia o tieto prostriedky starať. Vyspelým východiskom z tejto situácie sa ukazuje aj zavádzanie virtualizačných prostriedkov, ktoré by mohlo viesť k zefektívneniu celého výučbového procesu.
Pre zaručenie ochrany privátnosti vyučujúcich a študentov, bezpečnosti a interoperability výmeny údajov je vhodná:
1. ochrana informácií šifrovaním,
2. identifikácia vyučujúcich a študentov (stanovenie identifikátorov),
3. ochrana, ktorá zaistí, že sa k údajom nedostane nepovolaná osoba (autentifikácia a autorizácie na rôznych úrovniach systému),
4. audit prístupu k zdieľaným údajom,
5. umožnenie neadresných výstupov pre potreby administrácie systému,
6. dokonalý personálny manažment pre správu systému od lokálnych uzlov až po centrum,
7. zváženie stupňa decentralizácie a centralizácie systému s ohľadom na celú šírku problematiky (ochrana dát, prístupnosť dát, finančné náklady, rýchlosť prístupu, parciálna nedostupnosť dát a iné).

Treba si však uvedomiť, že dokonalý audit môže byť aj brzdou pre funkčnosť systému. Bolo by vhodné skonštruovať karuselový mechanizmus pre parciálne audity vykonávané v rôznej škále sledovaných aktivít, ktorý by nepravidelne náhodne vyberal vždy iba určitú časť ukazovateľov tak, aby tým netrpela funkčnosť systému. Tiež je potrebné zabezpečiť pravidelnú kontrolu log súborov a ich pravidelnú archiváciu.
Služba by mala zabezpečovať vyučujúcim a študentom adresný prístup k vybraným virtualizovaným prostriedkom a narábať s nimi pri výučbovom procese, riešení zadaných výučbových projektov a iných aktivitách súvisiacich s predmetom výučby. Vedľajším efektom správy vedenia virtualizovaných prostriedkov je časová nenáročnosť a fakt, že údaje zaznamenané do systému nie je nutné vkladať viacnásobne.

Poznámky/Notes

V texte boli použité tieto základné pojmy a skratky:
HW – hardvér (hardware)
SW – softvér (software)
TCPIP – transfer control protocol internet protocol

Literatúra/List of References

[1] Fei, L. a Chunhua, G. a Xiaoke, L., 2015. Constructing a virtual computer laboratory based on OpenStack. In: Computer Science & Education (ICCSE). 10th International Conference. Cambridge: IEEE, 2015, s. 794-799. ISBN 978-1-4799-6598-4.
[2] Frisch, G. a Greguš, M., 2009. It’s time to act! How an open source portfolio analysis can support small and medium sized enterprises to get into e-business. In: Striving for Competitive Advantage & Sustainability: New Challenges of Globalization. Montclair: Montclair State University, 2009, s. 1147-1157. ISBN 978-0-9797659-5-7.
[3] google.com, 2016. [online]. [cit. 2016-01-13]. Dostupné na: <https://www.google.com/intl/sk/docs/about/>
[4] Greguš, M. a Lenhard, H. T., 2012. Case study – virtualization of servers in the area of healthcare-IT. In: International journal for applied management science and global developments.

2012, 1 (2012), s. 1-10. ISSN 2195-4135.
[5] Jackson, K., 2012. OpenStack Cloud Computing Cookbook. London: Packt Publishing Ltd., 2012. ISBN 978-1-84951-732-4.
[6] Le, X. a Dijiang, H. a Wei-Tek, T., 2012. V-lab: a cloud-based virtual laboratory platform for hands-on networking courses. In: ITiCSE ’12 Proceedings of the 17th ACM annual conference on Innovation and technology in computer science education. Haifa, Israel: ITiCSE, 2012, s. 256-261. ISBN 978-1-4503-1246-2.
[7] Olšavský, F., 2007. Nové prístupy vo vzdelávaní. In: Marketing Science and Inspirations. 2007, 2(3), s. 22-23. ISSN 1338-7944.
[8] Pajtinková, Bartáková, G. a Gubíniová, K., 2014. Moderné prístupy k marketingovému riadeniu v súčasnosti. In: Marketing Science and Inspirations. 2014, 9(2), s. 2-11. ISSN 1338-7944.
[9] qualtrics.com, 2016. [online]. [cit. 2016-01-10]. Dostupné na: <http://www.qualtrics.com/>
[10] Richterová, K. et al., 2006. Marketingový výskum. Bratislava: Vydavateľstvo Ekonóm, 2006. ISBN 80-225-2064-0.
[11] Smolková, E., 2014. K problému ochrany značky a duševného vlastníctva. In: Marketing Science and Inspirations. 2014, 9(3), s. 33-46. ISSN 1338-7944.
[12] surveymonkey.com, 2016. [online]. [cit. 2016-01-10]. Dostupné na: <https://www.surveymonkey.com/>
[13] Šeliga, M. a Štarchoň, P., 2013. Marketingová komunikácia a vernostné programy vybraných medzinárodných maloobchodných reťazcov na slovenskom trhu. Časť II. In: Marketing Science and Inspirations. 2013, 8(2), s. 37-41. ISSN 1338-7944.
[14] Vilčeková, L., 2010. Návrh veľkosti vzorky v marketingovom výskume. In: Marketing Science and Inspirations. 2010, 5(2), s. 23-25. ISSN 1338-7944.
[15] Wannous, M. a Nakano, H., 2010. NVLab, a networking virtualWeb-based laboratory that implements virtualization and virtual network computingtechnologies. In: IEEE Trans. Learning Technol. 2010, 3(2), s. 129-138. ISSN 1939-1382.
[16] Wannous, M. a Amry, M. S. a Nakano, H. a Nagai, T., 2014. Work-in-progress: Utilization of cloud technologies in an E-learning system during campus-wide failure situation. In: Interactive Collaborative Learning (ICL). International Conference. Dubai, UAE: Institute of Electrical and Electronics Engineers Inc., 2014, s. 13-16. ISBN 9781479944378.

Kľúčové slová/Key Words

výskumné inštitúcie vyššieho vzdelávania, vzdelávanie, manažment, bezpečnosť, OpenStack, marketingový výskum, virtualizácia
higher education research institutions, education, management, OpenStack, marketing research, virtualization

JEL klasifikácia

I23, M15

Résumé

The deployment of the virtualization environment OpenStack in education. Part II.

The main goal of the deployment of virtualization environments OpenStack in education is to provide lecturers and students the full configurable environment for teaching of the different subjects focusing on modeling of the real processes. In the contribution OpenStack is presented as a free open source software and platforms for cloud computing licensed under the Apache license. The

separation of the sensitive systems from open networks and the learning environment is essential for the safety of the school information system. The four cases represent teaching subjects – Accounting on PC, Ethical hacking, Security management and Marketing research in which can be implemented OpenStack and authors are expressing how significant this innovation can be in the education process when it comes to the security of data, their collecting, processing and distribution in it. The proposal of the innovations in education of the selected subjects may affect managerial and marketing skills and knowledge of students with great success.

Kontakt na autorov/Address

Mgr. Vincent Karovič, Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: vincent.karovic2@fm.uniba.sk

Ing. Vincent Karovič, PhD., Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: vincent.karovic@fm.uniba.sk

PhDr. Peter Veselý, PhD., MBA, Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: peter.vesely@fm.uniba.sk

Mgr. František Olšavský, PhD., Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: frantisek.olsavsky@fm.uniba.sk

RNDr. Michal Greguš, PhD., Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: michal.gregusml@fm.uniba.sk

Recenzované

10. február 2016 / 17. február 2016

Nasadenie virtualizačného prostredia OpenStack na výučbové účely. Časť I.

Nasadenie virtualizačného prostredia OpenStack na výučbové účely. Časť I.

Hlavným cieľom nasadenia virtualizačného prostredia OpenStack na výučbu je poskytnúť lektorom a študentom plnohodnotné konfigurovateľné prostredie pre rôzne predmety výučby modelovania reálnych procesov. Pre potreby príspevku sú predstavené možnosti využitia OpenStacku ako voľne dostupného open source softvéru vo vyučovaní predmetov Účtovníctvo na počítači, Etický hacking, Manažment bezpečnosti a Marketingový výskum. Implementácia virtualizácie vychádza pri každom predmete z jeho obsahového zamerania s

dôrazom na čo najvernejšie zobrazenie reálnych podmienok hospodárskej praxe. Nakoľko existujú relevantné obmedzenia pri práci s údajmi, či už na úrovni technického zabezpečenia pri ich získavaní, spracovaní, distribúcie, ich ochrany, ale aj zabezpečenia celého informačného systému, v návrhovej časti sa za jednotlivé predmety uvádzajú konkrétne riešenia, ako tieto úzke miesta prekonať. Na záver sú identifikované prínosy navrhovaných riešení pre inováciu samotnej výučby s dôrazom na realizovateľnosť a simuláciu čo najvernejších podmienok, s ktorými sa študenti môžu stretnúť v praxi.

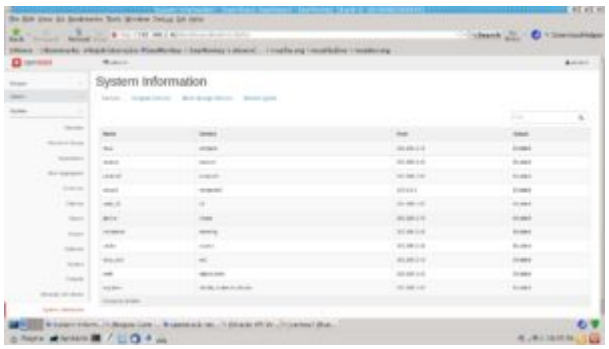
Úvod

Zapojenie virtualizačného prostredia OpenStack do výučby má pomôcť lektorom a študentom pracovať vo flexibilnom prostredí pre predmety, ktorých výučba si vyžaduje modelovanie procesov blízkych realite, v akých sa organizácie reálne nachádzajú. Povolenie prístupu s plnými užívateľskými právami v bežnom modeli výučby nie je možné, no vo virtuálnom prostredí je ľahké realizovať aj modely s plnými prístupovými a administrátorskými právami. Zároveň zo strany administrácie systému je možné vytvoriť podmienky pre ľahkú zálohovateľnosť a obnoviteľnosť užívateľských prostredí, pri plnom oddelení užívateľa od reálnych systémových prostriedkov.
Základným technologickým východiskom pre ukladanie dát a iných prostriedkov a nástrojov v takomto systéme bude správne navrhnutý a riešený cloud. Cloud je v tomto prípade dôležitá technológia. Tento článok sa bude zaoberať rôznymi pohľadmi na procesy elektronizácie výučbového procesu a spôsobmi manipulácie s dátami a inými prostriedkami a nástrojmi s tým súvisiacimi vo virtuálnom prostredí. Použitý termín dôležitá technológia znamená, že daná technológia má v súčasnosti, alebo možno bude mať v budúcnosti, vplyv aj na obchodný model sledovaných procesov. Cloudové technológie vzhľadom k svojej inovatívnosti prinášajú veľké zmeny do niektorých firemných a tým aj do výučbových procesov.
Detailnejšia analýza využívania cloudových technológií povedie k záveru, že nie je možné, aby proces elektronizácie výučbových procesov preskočil túto etapu vývoja informačných a komunikačných technológií. Prinajmenšom je nutné, aby existovala stratégia ako reagovať na záplavu inovácií, ktoré so sebou prináša vývoj a výskum v oblasti cloudových technológií. Je potrebné upozorniť na fakt, že cloudové technológie priamo, či nepriamo súvisia aj s mobilnými technológiami.
Zavedenie cloudových a mobilných technológií do elektronizácie školstva priamo ovplyvní veľa procesov vo výučbe. S ohľadom na hodnotový reťazec sledovaného objektu sú tieto procesy rozdelené na procesy, ktoré sú súčasťou základných činností a procesy, ktoré sú súčasťou podporných činností. Priamo s týmito otázkami súvisí bezpečnosť cloudových riešení. Aj keď má cloud computing veľa výhod a predstavuje zníženie nákladov, či už na elektrickú energiu, nákup hardvéru alebo pracovnú silu, predstavuje aj možné riziká. Treba však zvážiť, či sú tieto riziká prijateľnejšie oproti pôvodnému riešeniu. Riziko spojené s bezpečnosťou cloudových riešení predstavujú hlavne public cloudy. Pri týchto cloudoch sú dáta ukladané v cudzej infraštruktúre. K dátam má okrem zainteresovaných prístup aj správca vzdialeného serveru. Dalo by sa predpokladať, že okrem správcu servera k dátam nemá prístup nikto iný a pokiaľ je všetko dôkladne zašifrované a zabezpečené, že dáta sú zabezpečené lepšie ako vo vlastných serveroch. Tento predpoklad však nie je veľmi odôvodnený a preto je skôr na mieste zamýšľať sa nad ďalšími spôsobmi riešení. Ochrana údajov školského výpočtového systému je ďalšia kategória, ktorá musí byť v týchto súvislostiach riešená. Nevyhnutné je riešiť otázky ako izolovať chránené školské údaje, s ktorými sa v cloude nebude pracovať od dát uložených v cloude, zamedziť priesahu komunikácie v cloude od komunikácie v školskom systéme, pri zabezpečení prístupu aplikácií cloudu na internet a otázku, kto bude zodpovedať za prípadný únik dát, či postih vinníka.
Celkom iná situácia nastáva pri využívaní vlastného privátneho izolovaného cloudu. V takomto prípade je potrebné sa zamerať predovšetkým na otázky okolo informačnej bezpečnosti. Privátny výučbový cloud odlúčenie štruktúr na internú a externú nevytvára, a teda ani riziká takéhoto typu

nevznikajú.
Inou otázkou je zabezpečenie konektivity k dátovým zdrojom cloudu pre pracovníkov, ak potrebujú prístup k dátam z externého prostredia. Základným predpokladom pre riešenie tohto problému je spoľahlivé a vysokorýchlostné pripojenie k sieti internet. V dnešnej dobe sa dá predpokladať, že väčšina zainteresovaných bude mať dostatočne stabilné a rýchle pripojenie k internetu. Stabilita by v prípade nasadenia riešení výučbových cloudov nemala byť limitujúcim faktorom. Výpadky pripojenia prípadne zníženie prenosových kapacít, nepredstavujú pre tento typ cloudu veľké riziko. Jedným zo spôsobov ako vylúčiť riziko výpadkov spojenia, prípadne ho minimalizovať, je vytvorenie jedného alebo viacerých nezávislých paralelných pripojení k internetu. Pre prípad nasadenia výučbového cloudu sa však s touto alternatívou nepočíta.
Projekt virtualizácie pri výučbovom procese sa vo svete ešte v plnom rozsahu nerealizoval. Vytvorenie virtualizovaných systémov pre výučbové účely prinesie možnosti ľahšej obnovy systému pri plnej škálovateľnosti a konfigurovateľnosti a tiež modelovanie situácií a činností, ktoré je nepredstaviteľné na reálnom hardvéri.

1 Predstavenie systému OpenStack

OpenStack je voľne dostupný open source softvér a platforma pre cloud computing licencovaný pod Apache licenciou. Pozostáva z viac modulov, kde každý plní špecifickú funkcionalitu. Pre potreby virtualizácie je používaný modul Nova, pre správu obrazov inštancií je využívaný modul Glance, objektový úložný priestor má na starosti Swift, webové rozhranie zabezpečuje modul Horizon, správu užívateľov spravuje Keystone, sieť zabezpečuje Neutron, telemetriu servera Ceilometer a blokový úložný priestor Cincer. Možností modulov, ktoré sú aplikovateľné v OpenStacku je viac. Nasadenie modulov závisí od požiadaviek na systém a použitého hardvéru určeného pre nasadenie systému OpenStack. OpenStack umožňuje využívanie viacerých virtualizačných nástrojov KVM/QEMU, Xen server, Hyper-V, Vmware, LXC. V našom riešení je využívaný štandardný virtualizačný nastroj KVM, ktorý postačuje našim požiadavkám.



Obrázok 1: OpenStack Dashboard
Zdroj: vlastné spracovanie

Obrázok 2: Grafický prehľad administrátora pre jednotlivé virtuálne stroje o využívaní zdrojov OpenStacku
Zdroj: vlastné spracovanie

1.1 Zaškolenie vyučujúcich a študentov

Permanentné zmeny v informačných systémoch a aplikáciách vyžadujú vysoký stupeň iniciatívy od používateľov, aby s týmito systémami pracovali zodpovedne. Ťažko ale možno považovať za vhodný spôsob naučiť sa zvládať neustále zložitejšie systémy učením sa naostro v praxi bez predchádzajúceho školenia v cvičnom prostredí. Používateľské príručky buď nie sú k dispozícii vôbec, alebo ak sú, mnohokrát nie je dostatok času na ich prečítanie. Školenie zvyčajne nepokrýva potreby používateľov informačných systémov a znalosť jednej izolovanej oblasti nepostačuje, pretože nezohľadňuje interakcie medzi rôznymi systémami. Okrem toho sú školenia drahé a účastníci počas účasti na nich chýbajú na výkon pracovných povinností u svojich zamestnávateľov.

1.2. Oddelenie citlivých systémov od otvorených sietí a výučbového prostredia

Kým sú citlivé informácie a údaje prístupné len v internej počítačovej sieti, riziko narušenia bezpečnosti sa obmedzuje výhradne na zamestnancov podniku. Ak sa však systém pripojí na sieť internet, je treba zobrať do úvahy hrozbu rizika, že tretie strany môžu zneužiť jeho zraniteľné miesta. Bezpečné pripojenie informačných systémov na sieť internet si vyžaduje od príslušných správcov príslušné znalosti, bez nich sa nedá vyhnúť chybám v konfigurácii. Informačné systémy a v nich obsiahnuté citlivé údaje sú vo viacero prípadoch nedostatočne izolované od otvorených počítačových sietí, alebo dokonca nie sú izolované vôbec. Mnohí správcovia informačných systémov sa nazdávajú, že firewall postačuje na ochranu počítačovej siete, externý audit vykonaný bezpečnostnými špecialistami však dokáže odhaliť zraniteľné miesta. Virtualizované výučbové prostredie tieto riziká podstatne znižuje.

1.3. Manažérsky prístup k nasadeniu systému

Zmysel existencie každej výrobnej alebo nevýrobnej organizácie je určovaný jej stratégiou, ktorá následne určuje presnú podobu obchodných procesov. Tie v každej organizácii umožňujú dosahovať ciele stanovené stratégiou, školstvo nevynímajúc. Obchodné procesy si pre svoje fungovanie vyžadujú služby informačných a komunikačných technológií. Tieto služby dnes už nie sú ani v školstve ničím výnimočným. Sú prostriedkom pre dosiahnutie poskytnutia kvalitnejších služieb. Len kvalitné prostriedky informačných a komunikačných technológií a služby nimi poskytované však dnes nestačia pre úspech v podnikaní. Okrem kvalitných informačných a komunikačných technológií je nevyhnutné zabezpečiť koordinované a kontinuálne riadenie ich spravovania a bezpečnosti. V uvedenej súvislosti je možné hovoriť o systéme riadenia správy a informačnej bezpečnosti spolu.

2 Možné vzory nasadenia výučbového virtualizačného cloudu

V súčasnej dobe sa na výučbu používajú laboratóriá výpočtovej techniky, kde v rámci učebne na každom počítači je nainštalovaný jeden operačný systém, Windows 7. Pre výučbu štruktúry predmetov uvedenej v ďalšej časti je potrebných viacero plne konfigurovateľných operačných systémov.

2.1 Účtovníctvo na počítači

Obsahom predmetu Účtovníctvo na PC je prakticky poukázať na rôzne podnikové informačné systémy používané v podnikoch s dôrazom na účtovnú časť informačných systémov.

Riešený problém:

V súčasnej dobe sa na výučbu používajú laboratóriá výpočtovej techniky, kde v rámci učebne na každom počítači je inštalovaných niekoľko informačných systémov. Pre príklad uvádzame napríklad MONEY S3, MONEY S4, ABRA, SUNSOFT, MRP WIN, POHODA, OMEGA atď. V praxi to znamená, že správca informačného systému univerzity, prípadne fakulty, musí do každého image inštalovaného v laboratóriách výpočtovej techniky, inštalovať všetky programy vrátane ich aktuálnych knižníc a vo veľa prípadoch musí nastaviť aj Microsoft SQL server. Vzhľadom na bezpečnostnú politiku prideľovania práv jednotlivým užívateľom potom počas vyučovania nie je možné zrealizovať žiadnu zmenu a ani nainštalovať novú verziu. V minulosti sa stávalo, že vo veľkej časti počítačov došlo k zmene parametrov nastavení účtovných informačných systémov, ktoré sa však nedali opraviť bez asistencie správcu informačného systému.
Ďalší z existujúcich problémov je, že vzhľadom na politiku práv užívateľa nebolo možné dostatočne ukázať, ako pracujú databázové jadrá informačných systémov. Taktiež nie je možné zmerať, ako zaťažuje systém pri prevádzke počítačovú sieť. V praxi taktiež dochádzalo k situácii, že študenti v informačných systémoch nahadzovali rôzne vstupné doklady, čo výrazne menilo účtovné výkazy. Tieto dáta bol problém obnoviť, pretože všetko bolo inštalované lokálne a výrobcovia informačných systémov nepredpokladali, že ich produkty budú využívané na študijné účely, a preto postrádali nástroje na rýchlu obnovu kompletného prostredia. Majú nástroje na obnovu účtovných dát, ale často nemajú nástroje na obnovu kompletného prostredia, to znamená, že ak študent zmenil nastavenia spôsobu účtovania, tak to zostalo zmenené, aj keď sa dáta obnovili. Toto prinášalo v procese vyučovania výrazné disproporcie.

Navrhované riešenie:

Navrhovaný systém virtualizácie umožňuje vyučujúcemu komfortný spôsob riadenia výučby. Vyučujúci si môže pripraviť viacero image pre jednotlivé účtovné informačné systémy. Tieto môže priradiť potom študentom na prístup. V prípade zmeny dát študentmi vyučujúci iba obnoví image a problém je vyriešený. Taktiež problém s nastaveniami je vyriešený, nakoľko vyučujúci má oprávnenie lokálneho administrátora na svojom image. Takto spustený image ako taký neovplyvňuje pôvodnú sieť. Študenti budú spúšťať svoj image na lokálnom počítači cez webové rozhranie. Problém s užívateľskými právami na lokálnych počítačoch v laboratóriách VT je teda vyriešený. Navyše, virtualizovaný systém typu SANDBOX je uzavretý sieťový systém a ako taký dokáže poskytnúť metriku. Teda dokáže merať prenesené dáta, robiť online ako aj offline analýzu prietoku dát a všeobecne reporty využívania systému.
Pre vyučujúceho to znamená vytvorenie viacerých image, kde podkladové licencie virtualizovaného PC budú v rámci MSDNAA licencií. Táto činnosť mu však umožňuje, aby mal dané inštalácie image plne pod kontrolou.

Inovácia výučby:

Proces výučby vzhľadom na navrhovanú technológiu výrazne pomôže v prezentácii skutočne nasaditeľných riešení podnikových informačných účtovných systémov. Študenti budú môcť reálne vidieť viac ako jeden informačný systém a môžu sami vyskúšať technologické riešenie a funkcionalitu viacerých informačných systémov.

2.2 Etický hacking

Obsahom predmetu Etický hacking je objasniť zložitosť a rozsah problému zabezpečenia systémov pre spracovanie údajov a poskytovanie informácií s dôrazom na úlohu manažéra v procese budovania a prevádzkovania takýchto systémov. Po úspešnom absolvovaní budú študenti ovládať základy pre IT bezpečnosť a budú schopní testovať bezpečnosť IS/ICT vo firme, uplatňovať princípy IS/IT informačnej bezpečnosti vo svojej manažérskej činnosti a pôsobiť v rámci systému riadenia informačnej bezpečnosti vo firme, v rôznych fázach vývoja životného cyklu IS/IT vo všetkých manažérskych pozíciách.

Obrázok 3: Virtuálny stroj s Linuxovou distribúciou Kali Linux pre výučbu predmetu Etický hacking
Zdroj: vlastné spracovanie

Obrázok 4: Topológia virtuálnych sietí v prostredí OpenStack pre výučbu predmetu Etický hacking
Zdroj: vlastné spracovanie

Riešený problém:

Problematika etického hackingu je podľa súčasne platnej legislatívy výrazným prvkom, ktorý rozhoduje o architektúre IS/ICT v podnikoch. Podniky vždy spracovávajú osobné údaje. Musia vytvoriť bezpečnostné projekty a musia sa zaoberať manažmentom bezpečnosti. Praktickou stránkou testovania bezpečnosti IS/ICT vo firmách je práve etický hacking. Ide teda o využívanie bežne dostupných, ale aj menej dostupných techník, ako sa dostať do systémov, prípadne ich poškodiť. Manažér nemôže tvrdiť, že jeho informačný systém je bezpečný, pokiaľ nespracoval komplexnú sadu bezpečnostných testov a nevyhodnotil ich z hľadiska závažnosti. Na to existuje medzinárodný štandard OWASP – Open Web Application Security Project, ktorý definuje postupné kroky, ako vykonávať dané testy. Priamo však nedefinuje, ako ich vykonať. K tomu je potrebný práve etický hacker, ktorý v mene spoločnosti vykoná tieto kroky, pričom potrebuje dostatočné znalosti v tejto oblasti. V škole až doteraz nebolo možné zaviesť daný predmet do výučby, nebol vytvorený dostatočne izolovaný systém (sandbox), ktorý by mohol slúžiť práve na simuláciu práce etického hackera.

Navrhované riešenie:

Práve navrhovaný systém virtualizácie spĺňa parametre na vytvorenie sandboxu, teda plne izolovaného priestoru, kde je možné vykonávať simulované akcie s cieľom postupného plnenia krokov podľa OWASP. Na jednej strane sa vytvoria WEB servery na rôznych OS a platformách. Na týchto WEB serveroch budú nasadené štandardizované aplikácie, napr. WORDPRESS, JOOMLA, PRESTASHOP, ZENCARD, OPENCARD atď. Študenti budú mať virtualizované prostredie systému WINDOWS a najmä systému KALI LINUX. Práve systém KALI LINUX je vyvinutý spoločnosťou, ktorá uskutočňuje medzinárodné certifikácie etických hackerov. Systém dokáže monitorovať siete, dokáže analyzovať sieťovú komunikáciu až na úroveň fyzických paketov.
Vyučujúci si musí pripraviť viacero image virtualizovaných systémov, napríklad Microsoft Server, Microsoft SBS 2011, Ubuntu, Mint, SCIENTIFIC LINUX a KALI LINUX. Tieto image budú dôkladne zálohované pre prípad poškodenia útokom. V rámci návrhu architektúry hybridnej siete si vyučujúci pripraví model segmentácie siete, umiestnenia serverov a virtuálnych prvkov ako sú switche a routery. Tieto sa dajú jednoducho virtualizovať. Tu je potrebné uviesť, že miera ochrany nastavení routerov je nižšia, ako ochrana značkových drahých routerov, na študijné účely však bohate postačuje. Okrem toho je potrebné fyzicky dodať aj jeden WIFI router pre demonštráciu ulomenia WEP, WPA alebo WPA2 šifrovania.

Inovácia výučby:

Prvýkrát je možné použiť tzv. študentský battle v sandboxe. Ide o to, že časť študentov má aj predmety zaoberajúce sa tvorbu aplikácií, kde výsledkom býva web aplikácia. Battle v sandboxe znamená, že práve táto skupina študentov musí nasadiť svoje aplikácie na WEB servery a musí ich nastaviť na najvyšší level bezpečnosti. Skupina študentov predmetu Etický hacking musí uskutočniť tzv. black test podľa OWASP s nasadením systému KALI LINUX, ktorý je vo virtualizovanom prostredí. Obe skupiny tak budú mať empirické skúsenosti s bezpečnosťou IS/ICT. Študenti tak budú mať k dispozícii komplexnú hybridnú sieť s aktívnymi sieťovými prvkami a pripravenými aplikáciami, ktoré nepripravovali oni sami, ale ich kolegovia študenti s cieľom čo najlepšie ich zabezpečiť.

2.3 Manažment bezpečnosti

Obsahom predmetu Manažment bezpečnosti je objasniť zložitosť a rozsah problému zabezpečenia systémov pre spracovanie údajov a poskytovanie informácií s dôrazom na úlohu manažéra v procese budovania a prevádzkovania takýchto systémov. Po úspešnom absolvovaní budú študenti ovládať základy pre IT bezpečnosť a budú schopní testovať bezpečnosť IS/ICT vo firme, uplatňovať princípy IS/IT informačnej bezpečnosti vo svojej manažérskej činnosti a pôsobiť v rámci systému riadenia informačnej bezpečnosti vo firme, v rôznych fázach vývoja životného cyklu IS/IT vo všetkých manažérskych pozíciách.

Riešený problém:

Manažment bezpečnosti sa zaoberá najmä legislatívnou časťou bezpečnosti, rozoberá bezpečnostné riziká na viacerých úrovniach. Doplňujúcou zložkou je predmet Etický hacking, ktorý reálne testuje bezpečnosť. Problémom najmä z minulosti je, že pri prednáške nie je možné poukázať na fyzickú formu bezpečnosti, študentom nie je možné zadať praktické cvičenie s ohľadom na to, že bezpečnostný stupeň ochrany fakultnej siete je veľmi vysoký a stupeň obmedzenia práv študentov veľmi vysoký. Študenti teda momentálne nie sú schopní reálne vyskúšať návrh riešenia firewalov, PGP šifrovania, správy podpisových kľúčov alebo zavedenie protokolu https na web server. Tieto obmedzenia sa nedali prekonať, pretože by vyvolali bezpečnostný precedens, ktorý by sa dal zneužiť pri publikovaní študentmi. Študenti teda mali k dispozícii veľmi obmedzené prostriedky IS/ICT a mali najmä prednášky, ktoré si však často nevedeli v reáli dostatočne dobre predstaviť.

Navrhované riešenie:

Systém virtualizácie umožňuje vytvoriť viac použiteľných obrazov operačných systémov, ktoré môžu byť pre praktický výklad nasadené v laboratóriách výpočtovej techniky bez toho, aby sa akýmkoľvek spôsobom narušila súčasná bezpečnostná politika fakulty. Študenti tak budú mať možnosť vidieť nasadenie rôznych operačných systémov v praxi, získajú možnosť oboznámiť sa s technikami používanými na zabezpečenie a monitorovanie nasadeného hybridného IS/ICT.
Vyučujúci si musí pripraviť viacero image virtualizovaných systémov, napríklad Microsoft Server, Microsoft SBS 2011, Ubuntu, Mint, SCIENTIFIC LINUX a KALI LINUX. Na týchto image sa budú počas prednášok implementovať jednotlivé spôsoby zabezpečenia hybridných sietí, vrátane podpisových politík, PGP šifrovania atď.

Inovácia výučby:

Aj pri tomto predmete je možné použiť tzv. študentský battle v sandboxe. Študenti pripravia server s WEB aplikáciami a zabezpečia ho na najvyššiu možnú úroveň podľa stupňa svojich vedomostí. Na tento server potom budú ukladané WEB aplikácie inej skupiny študentov, ktorí sa venujú tvorbe WEB aplikácií. Okrem toho musia nainštalovať na daný server aj štandardizované aplikácie napr. PRESTASHOP, JOOMLA, WORDPRESS, OPENCARD atď.

2.4. Marketingový výskum

Cieľom predmetu je poskytnúť študentom poznatky o poslaní, procese a aplikácii metód marketingového výskumu s dôrazom na jeho praktické využitie v marketingovom manažmente. Marketingový výskum je prezentovaný ako nástroj, prostredníctvom ktorého sú prepojení marketingoví manažéri so spotrebiteľmi, zákazníkmi a verejnosťou (Richterová 2006, s. 9). Predmet poskytuje pohľad na informačné potreby podniku a konfrontuje ich s potenciálom jednotlivých nástrojov marketingového výskumu tieto informácie získať, spracovať a interpretovať.

Riešený problém:

Študenti počas prednášok majú možnosť sa oboznámiť s procesmi získavania, spracovania a interpretácie marketingového výskumu. Veľmi vhodnou a v praxi marketingového výskumu dnes už nevyhnutnou požiadavkou je zapojenie informačných technológií. Tieto nachádzajú uplatnenie v celom procese realizácie marketingového výskumu počnúc identifikovaním potreby nedostatku konkrétnych informácií pre manažérske rozhodovanie až po realizáciu samotného prieskumu v praxi formou elektronického dopytovania, využitia technických prostriedkov v procese pozorovania a následne spracovania získaných údajov. Keďže zásadným problémom v marketingovom výskume je dodržať základné princípy – objektivita, etika a systematika marketingového výskumu (Richterová 2006, s. 12-14) a súčasne je možné zaznamenávať tlak na zvyšovanie efektivity realizácie aktivít marketingového výskumu obzvlášť v podmienkach medzinárodného marketingu, stáva sa využitie výpočtovej techniky nevyhnutnosťou. Problém vo vyučovaní nastáva s obmedzenými užívateľskými právami, ako aj s možnosťou využitia rôznych platforiem komerčných aj voľne prístupných pri realizácii elektronického dopytovania ako napríklad qualtrics.com (2016), surveymonkey.com (2016) alebo google docs (2016). V súčasnosti neexistuje univerzitná platforma pre realizáciu elektronického dotazníka pre študentov na Univerzite Komenského v Bratislave. Keďže využitie komerčných aplikácií je pre študentov obmedzené, nemajú tak priestor plne využiť všetky možnosti, ktoré by za bežných okolností v business sfére mali k dispozícii. Ide hlavne o problém spustenia WEB aplikácií tak, aby tam mohli na nich realizovať najmä zber údajov, ich kontrolu, cielené zameranie na požadovaný segment respondentov, či ako uvádza Vilčeková (2010) zabezpečenie veľkosti vzorky.

Navrhované riešenie:

Virtualizácia vytvorí niekoľko databázových serverov a prezentačných serverov založených na odlišných technológiách, ako je napr. PHP, MySQL alebo MS SQL, .NET 4.X. Správca siete vytvorí viacero image virtualizovaných systémov, pretože si vyžadujú prvotne množstvo nastavení a bezpečnostných politík. Vyučujúci tieto image potom môže ľubovoľne nasadzovať, pričom študentom poskytne plnohodnotné prístupy tak, ako by ich mali realizované v business sfére. Tak sa dá aplikovať množstvo prípadov nasadenia výpočtovej techniky pri marketingovom výskume. Marketingový výskum by takto presnejšie reflektoval požiadavky na marketingový manažment v rozsahu nových prístupov ako uvádzajú Pajtinková a Gubíniová (2014), ale aj v ochrane značiek ako uvádza Smolková (2014), či pri komunikácii vernostných programov v maloobchode (Šeliga a Štarchoň 2013).

Inovácia výučby:

Tak ako v predchádzajúcom prípade je možnosť aj tu realizovať tzv. študentský battle v sandboxe. Tento spôsob realizácie je vhodný pre študentov na uvedomenie si, že aj zdanlivo jednoduchá operácia zberu dát napríklad cez elektronický dotazník alebo zapojenie technických prostriedkov pri pozorovaní môže predstavovať veľmi veľké bezpečnostné riziko. Realizácia takéhoto spôsobu výučby študentom prinesie priame skúsenosti s nasadením výpočtovej techniky pri realizácii aktivít marketingového výskumu, čo doteraz bolo možné iba vo veľmi obmedzenej miere.

Záver

Mimoriadne dôležitý aspekt virtualizácie vo výučbovom procese je, že výučba sa dostala do miesta, kde zdroje spoločnosti nie sú dostačujúce na poskytovanie zodpovedajúcej hardvérovej výbavy pri zodpovedajúcej softvérovej skladbe a nutnej pružnosti pri často sa meniacich požiadavkách na systémy výpočtovej techniky. Paradoxne tento stav priviedol k postupu vpred, čo má za následok aj zvýšenie úrovne vzdelania v tejto oblasti. Moderné hardvérové výpočtové kapacity sú obvykle nákladné a pri zvyšovaní ich množstva narastá počet ľudí, ktorí sa ako administrátori rôznych úrovní musia o tieto prostriedky starať. Vyspelým východiskom z tejto situácie sa ukazuje aj zavádzanie virtualizačných prostriedkov, ktoré by mohlo viesť k zefektívneniu celého výučbového procesu.
Pre zaručenie ochrany privátnosti vyučujúcich a študentov, bezpečnosti a interoperability výmeny údajov je vhodná:
1. ochrana informácií šifrovaním,
2. identifikácia vyučujúcich a študentov (stanovenie identifikátorov),
3. ochrana, ktorá zaistí, že sa k údajom nedostane nepovolaná osoba (autentifikácia a autorizácie na rôznych úrovniach systému),
4. audit prístupu k zdieľaným údajom,
5. umožnenie neadresných výstupov pre potreby administrácie systému,
6. dokonalý personálny manažment pre správu systému od lokálnych uzlov až po centrum,
7. zváženie stupňa decentralizácie a centralizácie systému s ohľadom na celú šírku problematiky (ochrana dát, prístupnosť dát, finančné náklady, rýchlosť prístupu, parciálna nedostupnosť dát a iné).

Treba si však uvedomiť, že dokonalý audit môže byť aj brzdou pre funkčnosť systému. Bolo by vhodné skonštruovať karuselový mechanizmus pre parciálne audity vykonávané v rôznej škále sledovaných aktivít, ktorý by nepravidelne náhodne vyberal vždy iba určitú časť ukazovateľov tak, aby tým netrpela funkčnosť systému. Tiež je potrebné zabezpečiť pravidelnú kontrolu log súborov a ich pravidelnú archiváciu.
Služba by mala zabezpečovať vyučujúcim a študentom adresný prístup k vybraným virtualizovaným prostriedkom a narábať s nimi pri výučbovom procese, riešení zadaných výučbových projektov a iných aktivitách súvisiacich s predmetom výučby. Vedľajším efektom správy vedenia virtualizovaných

prostriedkov je časová nenáročnosť a fakt, že údaje zaznamenané do systému nie je nutné vkladať viacnásobne.

Poznámky/Notes

V texte boli použité tieto základné pojmy a skratky:
HW – hardvér (hardware)
SW – softvér (software)
TCPIP – transfer control protocol internet protocol

Literatúra/List of References

[1] Fei, L. a Chunhua, G. a Xiaoke, L., 2015. Constructing a virtual computer laboratory based on OpenStack. In: Computer Science & Education (ICCSE). 10th International Conference. Cambridge: IEEE, 2015, s. 794-799. ISBN 978-1-4799-6598-4.
[2] Frisch, G. a Greguš, M., 2009. It's time to act! How an open source portfolio analysis can support small and medium sized enterprises to get into e-business. In: Striving for Competitive Advantage & Sustainability: New Challenges of Globalization. Montclair: Montclair State University, 2009, s. 1147-1157. ISBN 978-0-9797659-5-7.
[3] google.com, 2016. [online]. [cit. 2016-01-13]. Dostupné na: <https://www.google.com/intl/sk/docs/about/>
[4] Greguš, M. a Lenhard, H. T., 2012. Case study – virtualization of servers in the area of healthcare-IT. In: International journal for applied management science and global developments. 2012, 1 (2012), s. 1-10. ISSN 2195-4135.
[5] Jackson, K., 2012. OpenStack Cloud Computing Cookbook. London: Packt Publishing Ltd., 2012. ISBN 978-1-84951-732-4.
[6] Le, X. a Dijiang, H. a Wei-Tek, T., 2012. V-lab: a cloud-based virtual laboratory platform for hands-on networking courses. In: ITiCSE '12 Proceedings of the 17th ACM annual conference on Innovation and technology in computer science education. Haifa, Israel: ITiCSE, 2012, s. 256-261. ISBN 978-1-4503-1246-2.
[7] Olšavský, F., 2007. Nové prístupy vo vzdelávaní. In: Marketing Science and Inspirations. 2007, 2(3), s. 22-23. ISSN 1338-7944.
[8] Pajtinková, Bartáková, G. a Gubíniová, K., 2014. Moderné prístupy k marketingovému riadeniu v súčasnosti. In: Marketing Science and Inspirations. 2014, 9(2), s. 2-11. ISSN 1338-7944.
[9] qualtrics.com, 2016. [online]. [cit. 2016-01-10]. Dostupné na: <http://www.qualtrics.com/>
[10] Richterová, K. et al., 2006. Marketingový výskum. Bratislava: Vydavateľstvo Ekonóm, 2006. ISBN 80-225-2064-0.
[11] Smolková, E., 2014. K problému ochrany značky a duševného vlastníctva. In: Marketing Science and Inspirations. 2014, 9(3), s. 33-46. ISSN 1338-7944.
[12] surveymonkey.com, 2016. [online]. [cit. 2016-01-10]. Dostupné na: <https://www.surveymonkey.com/>
[13] Šeliga, M. a Štarchoň, P., 2013. Marketingová komunikácia a vernostné programy vybraných medzinárodných maloobchodných reťazcov na slovenskom trhu. Časť II. In: Marketing Science and Inspirations. 2013, 8(2), s. 37-41. ISSN 1338-7944.
[14] Vilčeková, L., 2010. Návrh veľkosti vzorky v marketingovom výskume. In: Marketing Science and Inspirations. 2010, 5(2), s. 23-25. ISSN 1338-7944.
[15] Wannous, M. a Nakano, H., 2010. NVLab, a networking virtualWeb-based laboratory that implements virtualization and virtual network computingtechnologies. In: IEEE Trans. Learning Technol. 2010, 3(2), s. 129-138. ISSN 1939-1382.
[16] Wannous, M. a Amry, M. S. a Nakano, H. a Nagai, T., 2014. Work-in-progress: Utilization of cloud technologies in an E-learning system during campus-wide failure situation. In: Interactive

Collaborative Learning (ICL). International Conference. Dubai, UAE: Institute of Electrical and Electronics Engineers Inc., 2014, s. 13-16. ISBN 9781479944378.

Kľúčové slová/Key Words

výskumné inštitúcie vyššieho vzdelávania, vzdelávanie, manažment, bezpečnosť, OpenStack, marketingový výskum, virtualizácia
higher education research institutions, education, management, OpenStack, marketing research, virtualization

JEL klasifikácia

I23, M15

Résumé

The deployment of the virtualization environment OpenStack in education

The main goal of the deployment of virtualization environments OpenStack in education is to provide lecturers and students the full configurable environment for teaching of the different subjects focusing on modeling of the real processes. In the contribution OpenStack is presented as a free open source software and platforms for cloud computing licensed under the Apache license. The separation of the sensitive systems from open networks and the learning environment is essential for the safety of the school information system. The four cases represent teaching subjects – Accounting on PC, Ethical hacking, Security management and Marketing research in which can be implemented OpenStack and authors are expressing how significant this innovation can be in the education process when it comes to the security of data, their collecting, processing and distribution in it. The proposal of the innovations in education of the selected subjects may affect managerial and marketing skills and knowledge of students with great success.

Kontakt na autorov/Addressses

Mgr. Vincent Karovič, Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: vincent.karovic2@fm.uniba.sk

Ing. Vincent Karovič, PhD., Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: vincent.karovic@fm.uniba.sk

PhDr. Peter Veselý, PhD., MBA, Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: peter.vesely@fm.uniba.sk

Mgr. František Olšavský, PhD., Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: frantisek.olsavsky@fm.uniba.sk

RNDr. Michal Greguš, PhD., Univerzita Komenského v Bratislave, Fakulta managementu, Katedra marketingu, Odbojárov 10, P. O. Box 95, 820 05 Bratislava 25, e-mail: michal.gregusml@fm.uniba.sk

Recenzované

10. február 2016 / 17. február 2016