UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
PRÍRODOVEDECKÁ FAKULTA

SYSTÉM NA ZVYŠOVANIE POVEDOMIA V OBLASTI INFORMAČNEJ BEZPEČNOSTI

2018 **Peter CHOMIČ**

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

PRÍRODOVEDECKÁ FAKULTA

SYSTÉM NA ZVYŠOVANIE POVEDOMIA V OBLASTI INFORMAČNEJ BEZPEČNOSTI

BAKALÁRSKA PRÁCA

Študijný program:	Informatika
Pracovisko (katedra/ústav):	Ústav informatiky
Vedúci diplomovej práce:	JUDr. RNDr. Pavol Sokol, PhD.
Konzultant diplomovej práce: (nepovinný)	doc. RNDr. Ľubomír Šnajder, PhD.

Košice 2018

Peter CHOMIČ

Zadanie záverečnej práce (ďalej len „zadanie“) je dokument, ktorým vysoká škola stanoví študentovi študijné povinnosti v súvislosti s vypracovaním záverečnej práce.

Ďakujem vedúcemu svojej diplomovej práce JUDr. RNDr. Pavlovi Sokolovi, PhD. za cenné pripomienky a za obetavosť počas jej písania. Veľká vďaka patrí aj mojej rodine, ktorá mi bola veľkou oporou pri písaní práce a poskytla mi rady a pripomienky. Ďakujem aj Michalovi Pavúkovi za jeho pomoc.

Abstrakt v štátnom jazyku

Práca sa zaoberá zvyšovaním povedomia v oblasti informačnej bezpečnosti. Počet bezpečnostných hrozieb a následne útokov, ktoré možno zamedziť zvyšovaním povedomia stále rastie, zvlášť takých, ktoré využívajú sociálne inžinierstvo. Tieto útoky sú omnoho staršie ako Internet. S jeho rozšírením sa však ich počet enormne zvýšil. Napriek už existujúcim mnohým formám, stále sa objavujú ich ďalšie obmeny. Z tohto dôvodu je potrebné pravidelne udržiavať o týchto hrozbách a útokoch bezpečnostné povedomie v rámci širokej verejnosti. Prvým krokom pri zvyšovaní bezpečnostného povedomia je zistiť, ktoré oblasti je potrebné do kampane na zvyšovanie povedomia zahrnúť. Pre úspech kampane na zvyšovanie povedomia je dôležité, akým spôsobom je realizovaná. V práci sú analyzované rôzne prístupy k zvyšovaniu povedomia a metódy, ktoré možno pri ňom použiť. Cieľom praktickej časti je implementácia systému na zvyšovanie povedomia s využitím modifikovaného systému na manažovanie vzdelávania.

Kľúčové slová: zvyšovanie bezpečnostného povedomia, e-learning, sociálne inžinierstvo, phishing, informačná bezpečnosť

Abstrakt v cudzom jazyku

This thesis deals with problem of raising awareness of information security. Number of attacks that can be avoided by raising awareness are on the rise, especially those involving social engineering. These attacks are much older than the Internet, but with its expansion, their numbers have risen enormously and have taken many new forms and new variations are still emerging. It is therefore necessary to regularly maintain awareness of them in the general public. The first step to do so, is to find out which areas should be included in the awareness campaign. For the success of the awareness campaign, it is important how it is implemented. In thesis, we analyze different approaches to awareness raising and the methods that can be used for it. The aim of the practical part is to implement a system for awareness raising using modified learning management system.

Key words: raising of security awareness, e-learning, social engineering, phishing, information security

Obsah

Úvod

Ľudský faktor je považovaný za najslabšiu súčasť zabezpečenia organizácií [1]. Podľa štúdie z roku 2015 [2] je slabé povedomie o informačnej bezpečnosti medzi zamestnancami považované za najväčší problém, brániaci organizáciám obrániť sa proti bezpečnostným hrozbám. Zo štúdie z roku 2017 vyplýva, že slabé povedomie bolo považované za najväčší problém aj v nasledujúcich rokoch. Jeho dopad na obranu organizácií sa každým rokom zväčšoval [52]. Útočníci často využívajú skutočnosť, že zamestnanci sú najľahšou cestou prelomenia bezpečnosti. Najčastejšie využívajú najmä psychologickú manipuláciu, zameranú na získanie informácií. Túto manipuláciu môžeme nazvať sociálnym inžinierstvom.

V roku 2015 boli za najnebezpečnejšie hrozby podľa prieskumu [1] považované:

- **phishing** [1] - pokus o získanie informácií maskovaním sa za dôveryhodnú entitu pri elektronickej komunikácii.
- **Malware** [1] – škodlivý program, pričom treba brať do úvahy, že väčšina prípadov phishingu má za cieľ stiahnutie a inštalovanie malwaru na zariadenie obete [3].

Útočníci často nemuseli vyvinúť veľké úsilie, keďže 63% potvrdených prípadov ukradnutia údajov zahŕňalo predvolené, slabé alebo ukradnuté heslá [3]. Heslá sú nielen slabé, ale málokedy si ich používatelia menia. Prieskum s tisíc účastníkmi z roku 2012 ukázal, že 42% opýtaných si nikdy nemenilo heslo k účtu na sociálnej sieti a 28% si nikdy nemenilo heslo k bankovému účtu [4].

Zvyšovanie povedomia má byť súčasťou bezpečnostnej politiky organizácií. Normy z ISO/IEC 27000 série požadujú, aby všetci zamestnanci organizácie dostávali vzdelanie a školenie pre zvyšovanie povedomia bezpečnosti informácií s ohľadom na ich pracovnú náplň [51]. Takéto školenia v oblasti bezpečností informácií by sa mali konať pravidelne [53]. Tieto normy sú vytvorené medzinárodnou organizáciou pre štandardizáciu (ISO) a medzinárodnou elektrotechnickou komisiou (IEC) a slúžia ako odporúčania v oblasti manažmentu informačnej bezpečnosti.

Témou účinného zvyšovania povedomia sa zaoberá aj naša práca. Práca je rozdelená na tri kapitoly v ktorých prechádza od porovnania a výberu spôsobov zvyšovania povedomia, tém ktoré je potrebné zahrnúť a nástrojov ktoré je možné využiť po návrh a implementáciu riešenia.

Prvá kapitola obsahuje definície základných pojmov a skúma spôsoby, ktorými je možné zvyšovanie povedomia uskutočňovať a spôsoby ako efektívne zdieľať vedomosti. Ďalej v nej zisťujeme, aké témy a v akom rozsahu je potrebné zahrnúť do všeobecného programu na zvyšovanie povedomia. Opierame sa o závery profesionálov v tejto oblasti a o nariadenia smerníc ktoré sa zaoberajú touto témou.

V druhej kapitole sme sa zamerali na analýzu porovnanie existujúcich nástrojov ktoré slúžia na zvyšovanie povedomia v oblasti bezpečnosti. Medzi tieto patrí rôzny software slúžiaci na penetračné testovanie v oblasti sociálneho inžinierstva ako sú napríklad programy na tvorbu a posielanie phishing mailov Porovnávali sme tiež nástroje ktoré je možné využiť pri tvorbe systému na zvyšovanie povedomia, aj keď priamo nie sú tvorené pre tento účel.

V tretej kapitole popisujeme návrh a implementáciu systému na zvyšovanie povedomia ktorý pozostáva z modifikovanej verzie Moodlu a jeho modulov a využíva knižnicu na odhad sily hesiel. Do systému sú zahrnuté moduly umožňujúce interaktívne učenie viacerými spôsobmi a moduly podporujúce gamifikáciu. Okrem návrhu systému popisujeme aj obsah kurzov na zvyšovanie povedomia ktoré sú v ňom vytvorené.

1 Zvyšovanie povedomia v oblasti informačnej bezpečnosti

1.1 Bezpečnostné povedomie

Definície zvyšovania povedomia sa líšia. Niektorí autori rozlišujú medzi zvyšovaním povedomia, tréningom a učením [23]. Iní zahrňujú tréning a učenie do zvyšovania povedomia [24]. Podľa špecifikácie NIST 800-16 **povedomie** nie je tréning a účelom prezentácie povedomia je jednoducho zamerať pozornosť na bezpečnosť [23]. **Bezpečnostné povedomie** môže byť definované ako stav, kde si je zamestnanec vedomý svojich bezpečnostných povinností [26]. To vyžaduje predpoklad, že zamestnanec si uvedomuje existenciu bezpečnostných hrozieb a spôsobov obrany proti nim.

Ak sa za zvyšovanie povedomia pokladá tréning aj učenie, tak existuje mnoho spôsobov, ako ho zvyšovať. Najľahšie využiteľným v školskom alebo pracovnom prostredí je prednáška. Medzi jej výhody patrí to, že účastníci sa môžu pýtať otázky priamo počas prednášky. Súčasne je možné obsah prednášky ihneď prispôsobiť požiadavkám skupiny. Jej hlavnou nevýhodou je to, že účastníci prijímajú informácie pasívne.

Opakom pasívnej prednášky je **interaktívne učenie**. Tento pojem zahŕňa všetky typy aktivít ako je písanie, čítanie, diskusia a riešenie problémov. Aby mohli byť účastníci považovaní za aktívne zapojených, je potrebné zahrnúť aktivity vyžadujúce vyššie myslenie ako je analýza, syntéza a vyhodnocovanie [20]. Medzi techniky interaktívneho učenia patrí učenie, založené na riešení problémov, kooperatívne a kolaboratívne učenie, debaty, hranie na roly, kvízové posedenia a iné [20, 21]. Viaceré výskumné štúdie vyhodnocujúce výsledky študentov ukázali, že mnohé techniky aktívneho učenia sú porovnateľné s prednáškami, ak ide o naučenie sa učiva, ale majú lepšie výsledky pri zvyšovaní schopností rozmýšľať a písať [20]. Pri kolaboratívnom aj kooperačnom učení si študenti zapamätali z lekcií viac [22]. Pri lekcii prerušovanej krátkymi aktivitami si tiež zapamätali viac, pri lekcii zameranej len na riešenie problémov boli výsledky rôzne, čo môže byť ovplyvnené tým, že existuje veľká variácia praktík, ako takú lekciu viesť a množstvo rôznych typov problémov [22].

Technika používaná aj pri zvyšovaní bezpečnostného povedomia je **gamifikácia**. Pri gamifikácii sa do kurzu pridajú herné prvky ako sú levely, trofeje, či odznaky, tutoriál, výzvy, skúsenostné body namiesto známok [29]. Využitie levelov dobre slúži na kontrolu toho, či

účastníci zvládli čiastkové učivo - tí ktorí nezvládli predošlý obsah, nemôžu pokračovať, kým v ňom nedosiahnu určitý level. Rozkorenené úlohy v hrách možno symbolizovať pomocou viacerých verzií zadania s rovnakou správou, ale rôznym obsahom. Táto možnosť voľby môže byť motivujúca kvôli ilúzii voľby [29]. V hre nemôžu chýbať ani odmeny, pričom je dobré, aby rástli geometricky, a tak povzbudzovali súvislú snahu. Ten, kto splní viac úloh za sebou, dostane bonus na zvýšenie motivácie [29]. Ďalšou črtou je **multiplayer** – hra viacerých hráčov, čo je vlastne **kooperatívne učenie**. Pri použití gamifikačného kurzu sa študenti pýtali viac otázok, a chodili viac pripravení. Zvýšila sa aj dochádzka a úspešnosť v testoch [29]. Gamifikáciu odporúča aj Herold R., keď odporúča použiť hry a výzvy v kampani na zvyšovanie povedomia ako prostriedok, ktorý ju urobí zaujímavejšou [27]. Pri gamifikácii mali však študenti zo začiatku kurzu horšie výsledky. V porovnaní s klasickým kurzom sa ich výsledky časom zlepšovali a najlepšie hodnoty dosahovali, keď sa hralo o záverečnú výhru [30]. V čase neskoršej skúšky z kurzu už ale mali nízku úspešnosť. Možno usúdiť, že ich motivácia bola založená hlavne na výhre.

Okrem lekcií sú aj iné možnosti, napríklad tréning pomocou kurzov, distribuovaných cez Internet, kde sú nevýhodami náročnosť udržania pozornosti a nemožnosť komunikácie v prípade otázok. Naopak, výhodou je, že každý môže ísť rýchlosťou, ktorá mu vyhovuje [24]. Komplexná kampaň na zvyšovanie povedomia môže zahŕňať aj plagáty, rozdávanie predmetov s bezpečnostnými sloganmi a ďalšie aktivity, upevňujúce povedomie aj mimo samotných lekcií [24, 27].

1.1.1 Učebné kognitívne štýly a personalizácia

Pri tvorbe obsahu na kampaň pre zvyšovanie povedomia je možné brať do úvahy, že rôzni ľudia si lepšie pamätajú rôzne typy obsahu, teda majú rôzne učebné štýly. Existuje viac definícií pre učebný štýl, jedna ho definuje ako popis postojov a správaní určujúcich preferovaný spôsob učenia jednotlivca [50]. Podľa jedného zdroja rozlišujeme sedem učebných štýlov [24]:

- **Vizuálny človek** - preferuje obrazové informácie a priestorové porozumenie.
- **Aurálny** dáva dôraz na zvuk a hudbu. Verbálny potrebuje reč, či už slovnú alebo písanú.
- **Kinestetický** si lepšie pamätá vysvetlenie s použitím tela a mimiky, v prípade opisov využíva hmatové vnemy. Logický viac využíva logiku, lepšie sa mu pracuje s odôvodňovaním a začleňovaním do systémov. Pre sociálny štýl má najväčší prínos práca v skupine a pre solitárny práca osamote a samoštúdium.

Iné verzie tohto delenia môžu rozlišovať aj podskupiny. Napríklad vizuálny typ človeka sa ďalej delí na objektovo vizuálny – preferencia obrázkov, umenia a priestorovo vizuálny, pri ktorom sa preferujú schematické reprezentácie [37]. Existujú aj úplne iné delenia. Napríklad delenie na dvojice protipólov myslenia: induktívny a deduktívny, aktívny a reflektívny, či sekvenčný a globálny [38], dokonca aj intuitívny a racionálny [37]. Líšia sa aj počty učebných štýlov ktoré rôzne štúdie definujú, napríklad 32 [38] či 16 [50]. Štýly, založené na preferencii zmyslu, môžu byť považované len za jednu z piatich rodín učebných štýlov [50].

Vplyv preferovaných štýlov na výkon študentov bol viackrát skúmaný, ale nedosiahli sa uspokojivé výsledky, podporujúce zvýšený vplyv [36], výsledky neboli konzistentné, či nebolo možné vyvodiť závery [37]. Výsledky štúdie, pozostávajúcej z troch experimentov, ktorú Pashler H. pokladá za obzvlášť informatívnu a dobre dizajnovanú, nepodporili myšlienku potreby rôznych inštrukčných metód pre vizuálne a verbálne zameraných študentov [36]. Hypotéza, že verbálne zameraní študenti potrebujú verbálne metódy inštrukcie a vizuálne zameraní potrebujú vizuálne metódy, nebola potvrdená v žiadnom z experimentov [39].

Možnosťou zabezpečenia osobnejšieho obsahu kurzov aj testov pre každého je **personalizácia**, kde sa obsah generuje na základe zisteného preferovaného učebného štýlu, obťažnosti primeranej študentovi, jeho predošlým znalostiam, schopnostiam, motivácii, záľubám a iným osobným okolnostiam [50]. Takýto adaptívny učebný systém zabezpečí podanie informácií na úrovni, ktorej jedinec rozumie, využíva to, čo už vie, a sú podávané spôsobom, ktorý jedinca zaujme a motivuje.

1.1.2 Zvyšovanie motivácie

Dôležitou súčasťou kampane na zvyšovanie povedomia je okrem poukázania na spôsoby bezpečného správania aj motivovanie k takému správaniu a snaha o zlepšenie postoja zúčastnených k bezpečnosti. Rozdiel medzi motiváciou a postojom je ten, že motivácia je dynamickejšia, rýchlejšie sa mení a je krátkodobá, kým postoj je statickejší [26]. **Motivácia** sa delí na vnútornú a vonkajšiu. Pri vnútorne motivovanom správaní ide človeku o radosť z vykonávania aktivity. Človek podopiera svoje správanie vlastnými vnútornými dôvodmi a túžbami. Primárny faktor je slobodná vôľa a pocit slobody. Medzi ďalšie elementy patrí napríklad pocit výzvy. Človek je vnútorne motivovaný, aj keď robí niečo, čo nechce, ale zhoduje sa to s jeho vnútornými normami a robí to preto, lebo verí, že by sa to malo robiť alebo preto, lebo tým chce dosiahnuť svoje vysnívané ja. Vonkajšia motivácia je spojená s túžbou vyhnúť sa niečomu negatívnemu, napríklad sankcii za nedodržanie bezpečnostných noriem

alebo s túžbou dosiahnuť niečo pozitívne. Pri tvorbe kampane na zvyšovanie povedomia je potrebné adresovať vnútornú aj vonkajšiu motiváciu v ich rôznych formách.

Podľa Bada M. a Sasse A., (2014) primárny cieľ bezpečnostného povedomia je ovplyvniť adopciu bezpečného správania [28]. Aby sa to podarilo, ľudia musia uznať, že informácie sú pre nich relevantné. Inými slovami, informácie sa týkajú rizík, ktoré ich môžu hroziť. Ľudia musia porozumieť a vedieť reagovať na rizikové situácie. Hlavne musia byť motivovaní a zmeniť správanie aj pri všetkých ostatných požiadavkách, ktoré sú na nich kladené [28].

Zameranie sa na motiváciu a zmenu postoja je dôležité. Faktom je, že aj napriek tomu, že ľudia majú potrebné znalosti z oblasti bezpečnosti, v reálnom živote sa takto nesprávajú [28]. Motiváciu sa zaoberá aj ISO/IEC norma, ktorá poukazuje na dôležitosť toho, aby zamestnanci pochopili možný dopad ich správania sa v oblasti bezpečnosti na nich, aj ich organizáciu [53]. Existuje veľa teórií, ktoré sa zaoberajú zvýšením motivácie. Viacero štúdií skúmalo ich využitie v kampaniach na zvyšovanie povedomia. Príkladmi takýchto teórií sú: teória ochrany motivácie, hypotéza očakávanej užitočnosti, teória regulatívneho zamerania [28] a iné teórie, ktoré si teraz rozoberieme.

Teória odôvodneného správania navrhuje vnútorný rozhodovací mechanizmus, založený na predpoklade, že zámer je bezprostredný determinant korešpondujúceho správania sa [26]. Psychologické požiadavky zamýšľaného správania sú postoj, ktorý zahŕňa očakávané dôsledky správania a subjektívne normy, ktoré sa skladajú z vnímaných noriem a motivácie podriadiť sa normám [28]. Preto je dôležité vždy spomínať možné záporné následky, ktoré môžu nastať pri zanedbaní bezpečného správania v danej situácii. Súčasne je potrebné zdôrazniť aj to, že zmena správania redukuje alebo odstráni riziko, keďže motiváciou mnohých je ich blaho. Blaho je používané ako jeden z prístupov na získanie motivácie [26].

Pri poukázaní na následky možno použiť aj príklady reálnych bezpečnostných incidentov z organizácie, ale so zreteľom na starostlivé dodržanie aspektov dôvernosti. Tieto príklady môžu byť použité aj pri učení toho, ako na tieto situácie reagovať a ako sa im vyhnúť [53]. Použitím príkladov z organizácie zabezpečíme aj relevantnosť. Iný spôsob, ako zabezpečiť relevantnosť, je urobiť risk osobným tým, že do motivačného obsahu zahrnieme aj zoznam osobných dát, ktoré o svojich zamestnancoch uchováva organizácia. Súčasne zdôraznime, že v prípade krádeže, či poškodenia údajov sú ohrozené aj ich údaje [24]. Týmto motivujeme aj tú skupinu ľudí, ktorej záleží viac na ochrane vlastných údajov, ako na dátach spracovávaných v zamestnaní.

Na ovplyvnenie zámeru je dobré zdôrazniť, že riziko hrozí každému účastníkovi. Motiváciu podriadiť sa normám a zákonom, či už zo strachu alebo z presvedčenia, možno využiť tým, že v kampani na zvyšovanie povedomia sú zahrnuté aj bezpečnostné normy organizácie a pri každej téme sú rozoberané aj zákony, ktoré sú porušované obchádzaním bezpečnostných procedúr. Pri možných následkoch je dôležité spomínať aj ich závažnosť, či už z hmotného alebo právneho hľadiska. Takto sa vyhneme tomu, aby ľudia vymenili riziko, ktoré podľa nich nemá veľký dopad, za pohodlnosť, získanú obchádzaním bezpečnosti.

Téme adopcie preventívneho správania sa venuje aj **teória sebaúčinnosti**, podľa ktorej táto adopcia závisí od troch faktorov, ktoré je potrebné v kampani docieliť. Prvým je uvedomenie si, že osobe hrozí riziko. Druhým faktorom je očakávanie, že daná zmena správania redukuje riziko. Tretím faktorom je presvedčenie človeka, že je dosť schopný na to, aby sa začal správať preventívne alebo nesprával sa rizikovo [28]. Aby si osoba uvedomila, že jej hrozí riziko, je potrebné, aby poznala motívy tých, ktorí na ňu môžu útočiť a poznala hodnotu informácií, s ktorými prichádza do styku. Podľa Gardnera B. by mala byť prvou témou pri tréningu práve motivácia útočníkov [24]. Medzi motivácie útočníkov patria: prestíž, aktivizmus, peniaze, tajomstvá získané pri industriálnej špionáži ako napríklad neuverejnené patenty a víťazstvo v kybernetickej vojne [24]. Presvedčenie človeka, že je dosť schopný, je dôležité, keďže ľudia zakladajú svoje vedomé rozhodnutia na tom, či sú schopní urobiť to, čo sa od nich požaduje a či im námaha bude stáť za to [28].

Teória plánovaného správania vznikla z teórie odôvodneného správania a je založená na rovnakom predpoklade, ale jej nový základný komponent je behaviorálny zámer [26]. Behaviorálne zámery sú ovplyvňované postojom k pravdepodobnosti, že správanie bude mať chcený výsledok a subjektívnym vyhodnotením rizík a benefitov výsledku [28]. Teória hovorí, že behaviorálne výkony záležia od motivácie (zámeru) a schopnosti (kontrole správania – aká náročná/reálna je možnosť meniť svoje správanie). Skladá sa zo šiestich konštruktov: postoje, zámery, úmysly, subjektívne normy, sociálne normy, vnímaná moc, vnímaná kontrola správania. Posledné dve sú veľmi dôležité pri tvorbe kampane.

Vnímaná moc je prítomnosť faktorov, ktoré môžu uľahčiť alebo brániť vykonaniu činnosti, patriacej ku správaniu tak, ako ich vníma daný človek. Ak sa ľuďom zdá nejaká činnosť dosť ľahká na to, aby ju boli schopní vykonať, budú ochotnejší ju urobiť. Ak si myslia, že by ju nedokázali spraviť, často sa o to ani nepokúsia. Pri tvorbe obsahu je preto potrebné dať dôraz na to, že všetci môžu svojim konaním zabrániť úspešnému vykonaniu útokov a nie sú bezmocní. Vnímaná kontrola správania je to, do akej miery si človek myslí, že má kontrolu nad

tým, čo robí. Ak človek pracuje s ťažko použiteľným systémom, ktorému nerozumie, tak má pocit, že nevie, čo robí a je rýchlo frustrovaný. Pri využití elektronického systému je potrebné myslieť na to, aké zložité je jeho ovládanie. Súčasne je dobré zisťovať spätnou väzbou, či práve jeho zložitosť neprekáža zvyšovaniu povedomia [26, 28]. Takisto je dobré zisťovať spätnú väzbu o zložitosti a pochopiteľnosti obsahu prednášok a otázok testov.

V psychológii **teória regulačného zamerania** tvrdí, že existujú dve spôsoby samoregulácie. V promočne zameranom spôsobe sa správanie ľudí riadi potrebou dosiahnuť blaho, túžbou dosiahnuť svoje ideálne ja a dosiahnuť zisky [54]. V prevenčne zameranom spôsobe samoregulácie sa správanie ľudí riadi potrebou cítiť sa bezpečne a potrebou zosúladiť svoje ja s tým ja, ktorým by podľa vlastného presvedčenia mali byť. To dosahujú plnením povinností a nariadení, prípadne morálneho kódu. Prevencia sa prejavuje tak, že namiesto toho, aby sa primárne snažili o zisk, je ich snaha smerovaná k tomu, aby sa vyhli stratám. Účinnosť kampane môže byť zvýšená použitím promočného aj prevenčného typu správy, prípadne zameraním sa na jeden typ [28], pokiaľ je to za daných okolností lepšie.

1.2 Informačná bezpečnosť

Informačná bezpečnosť sa zaoberá informáciami bez ohľadu na ich formát – zahŕňa papierové dokumenty, digitálne a intelektuálne vlastníctvo a verbálnu alebo vizuálnu komunikáciu. Kybernetická bezpečnosť sa zaujíma o ochranu digitálnych aktív – všetkého od sietí k hardwaru a informáciám, ktoré sú spracované, uložené alebo prenášané informačnými systémami [25]. Existuje veľa definícií informačnej bezpečnosti. Napríklad podľa právnej úpravy v USA informačnou bezpečnosťou je ochrana informácií a informačných systémov proti neautorizovanému prístupu, použitiu, prezradeniu, narušeniu, modifikácii, alebo zničeniu [31]. Nás v tomto smere zaujíma hlavne ľudský element.

Pri zvyšovaní bezpečnostného povedomia existuje niekoľko štandardných oblastí, ktoré by mali byť pokryté: ochrana údajov, heslá, sociálne inžinierstvo, používanie sietí, malware, používanie osobných zariadení, pravidlá čistého stola, bezpečnostné regulácie a politiky organizácie [32]. ISO/IEC 27001 požaduje, aby každý pracovník organizácie poznal jej bezpečnostné politiky aj sankcie za ich porušenie [51]. Medzi témy môžu patriť okrem iného aj spam, softvérové licencie, ukladanie a zálohovanie údajov, odpoveď na bezpečnostné incidenty (koho kontaktovať, čo robiť a čo nie) [35]. Gardner B. a Thomas V. spomínajú aj tému úniku údajov, ktorá pokrýva metadáta a ich odstraňovanie, ničenie dokumentov

a prístrojov pred ich vyhodením, či sociálne siete a nastavenia, ktoré zabraňujú zverejneniu osobných údajov [24]. Zo sociálneho inžinierstva upozorňujú na phishing – identifikáciu a hlásenie phishingových správ. Pri identifikácii je potrebné zamerať sa na maskované odkazy a spoofované - maskované emailové adresy.

ISO/IEC 27003 [53] obsahuje zoznam toho, čo by minimálne mali obsahovať materiály pre školenie v oblasti informačnej bezpečnosti:

- riziká a hrozby, týkajúce sa informačnej bezpečnosti,
- základné termíny informačnej bezpečnosti,
- jasnú definíciu bezpečnostného incidentu, odporučenie, ako možno takýto incident identifikovať, ako sa s ním vysporiadať a podať o ňom správu,
- politiky, smernice a postupy informačnej bezpečnosti organizácie,
- zodpovednosť a kanály pre hlásenie, vzťahujúce sa k informačnej bezpečnosti organizácie,
- odporúčania, ako pomáhať v zlepšovaní informačnej bezpečnosti organizácie,
- odporúčania pre incidenty v oblasti informačnej bezpečnosti a ich hlásenie,
- zdroje ďalších informácií.

ISO/IEC 27002 zase zhŕňa aspekty, ktorými by sa malo zaoberať školenie a vzdelávanie v oblasti informačnej bezpečnosti, Príkladom je osobná zodpovednosť za vlastné konanie a nečinnosť a všeobecná zodpovednosť voči zabezpečeniu a ochrane informácií patriacich organizácii. Ďalším aspektom sú základné postupy v oblasti informačnej bezpečnosti. Napríklad medzi tie postupy môžeme zaradiť podávanie správ o incidentoch a základné opatrenia, medzi ktoré patrí bezpečnosť hesiel, či kontrola malware a pracovnej plochy [53].

Teória ochrany údajov sa zaoberá právnymi predpismi, ktoré zaručujú túto ochranu hlavne pri osobných údajoch a triedením údajov podľa ich dôležitosti a stupňa utajenia. Následne sa venujú manipulácii s údajmi podľa toho, do ktorej triedy patria. Cieľom je, aby používatelia vedeli, s akými údajmi pracujú, aké právne predpisy sa k ním viažu a ako majú s nimi manipulovať a likvidovať ich, komu a za akých okolností ich možno poskytnúť.

1.2.1 Heslá

Pri heslách je potrebné poukázať na dôležitosť ich pravidelnej zmeny a bezpečnostných hrozieb vyplývajúcich z toho, že jedno heslo je používané v rámci niekoľkých

systémov. Heslá by tiež nemali obsahovať osobné údaje, ako je meno zvieraťa, či dátum narodenia [32]. Dôležité je aj to, ako sú chránené uchovávané heslá v elektronickej, či papierovej podobe. ISO/IEC 27004 za **silné heslo** považuje to, ktoré je dlhšie ako osem znakov, neobsahuje informácie, vzťahujúce sa k osobe jeho tvorcu a neskladá sa zo slov, ktoré obsahuje slovník – teda spisovných. Posledná požiadavka k silnému heslu je, aby neobsahovalo iba číselné alebo iba písmenové skupiny znakov [56]. Existujú tri hlavné skupiny metód na odhadnutie sily hesla [33]. Heslo by malo byť považované za silné, ak je ťažko prelomiteľné pre každú z týchto skupín:

- **Založené na útoku** - skóre je odvodené od času, ktorý bol potrebný na prelomenie hesla dopredu určeným útokom/ich postupnosťou.
- **Heuristické** - majú heuristicky (nie presne, podľa skúseností) odvodené pravidlá, podľa ktorých určujú silu hesla, ktorá by sa mala merať v bitoch entropie.
- **Pravdepodobnostné** - založené na štatistike. Útočníci sa snažia zachytiť spôsob, akým ľudia tvoria heslá a odhadnúť, ako veľmi je heslo podobné tomu, ktoré by vytvoril človek.

Útoky využívané v prvej skupine sú napríklad **útok hrubou silou** (brute force) – skúšanie všetkých kombinácií znakov, porovnávanie s uniknutými databázami hesiel a **slovníkový útok**, ktorý môže obsahovať rôzne pravidlá (prvé písmeno je veľké, za slovníkovým slovom nasleduje daný počet číslic a iné). Pravidlom môže byť aj **Levenshteinova vzdialenosť** – počet vkladaní, odoberaní alebo zámen písmen, potrebných na to, aby zo slova vzniklo iné. Inými slovami, keď si zvolíme Levenshteinovu vzdialenosť ako pravidlo slovníka, tak pokryjeme aj podobné slová.

Najpopulárnejší z **heuristických prístupov** je **LUDS** [33] (lower case, upper case, digits, symbols), ktorý silu hesla počíta na základe toho, koľko heslo obsahuje malých písmen, veľkých písmen, číslic a iných znakov. Je dobrý na odhadnutie sily proti útokom hrubou silou. Jeho problémom je, že neberie do úvahy pravdepodobnosť výskytu hesiel a tak heslá, ktoré sú pravdepodobnostnými metódami ľahké odhaliť, označí za silné. Napríklad heslo David-1982 označí za silnejšie ako heslo RpixTsGa napriek tomu, že prvé je typu meno-rok narodenia, čo je typ hesla, ktorý ľudia používajú, kým druhé je nezmyselný sled písmen, ktorý možno prelomiť len útokom hrubou silou.

Pravdepodobnostné prístupy hodnotia silu hesla podľa toho, aká veľká je pravdepodobnosť, že človek by dané heslo použil. Najjednoduchší spôsob, ako to určiť, je porovnanie s verejnými databázami hesiel. Problém je, že databázy nemusia obsahovať všetky

pravdepodobné heslá. Z tohto dôvodu vznikli mnohé štatistické modely (Markov chain model, pravdepodobnostné bezkontextové gramatiky), ktoré sa snažia aj z týchto obmedzených tréningových dát produkovať pravdepodobnosť použitia všetkých hesiel. Markov chain model sa delí na [33]:

- **adaptive memory Markov Chain**, ktorý sa špecifikuje na nájdenie lokálnych vzorcov v hesle, ktoré pozná z tréningovej množiny [33],
- **hierarchical Markov Chain model,** ktorý je zameraný na detegovanie globálnej štruktúry ľudských hesiel. Je založený na hypotéze, že znaky v týchto heslách nie sú zoskupené náhodne, ale spájajú sa podľa určitých pravidiel do väčších štruktúr [33].

1.2.2 Sociálne inžinierstvo

Sociálne inžinierstvo ja založené na technikách, použitých na manipulovanie ľudí na vykonanie želanej akcie alebo vyzradenie informácie [34]. Medzi tieto techniky patrí tzv. **tailgating**, ktorý využíva skutočnosť, že ak človek prechádza cez bod s kontrolou vstupu tesne za niekým, kto kontrolou prešiel, často ho nikto nezastaví. **Vishing a smishing** využívajú telefón so podhodeným (spoofovaným) ID volajúceho, ktoré sa javia ako prichádzajúce zo známeho čísla, na volanie a posielanie SMS správ [24].

Ďalšou, veľmi často využívanou a úspešnou metódou sociálneho inžinierstva je **phishing**. Pri phishingu ide o posielanie správ, ktorých zdroj sa javí ako dôveryhodný. Phishingové maily často vytvárajú pocit naliehavosti napríklad tvrdením, že konto vlastníka bude deaktivované, ak sa ihneď nevykoná žiadaná akcia [24]. Ďalší často využívaný obsah týchto emailových správ typ obsahuje tvrdenie, že vlastníkovi konta bola poslaná e-karta a musí kliknúť na odkaz, aby si ju vyzdvihol.

Pri pokuse dostať obeť na svoju stránku využívajú útočníci viaceré techniky. Tieto techniky sa využívali na presvedčenie ľudí o tom, že doména odkazu je tá pravá, či ako spôsoby na obídenie spamových filtrov. Jednou z nich je využitie toho, že hierarchia domén v odkaze ide smerom nadol sprava, kým ľudia v mnohých kultúrach čítajú odkazy zľava. Teda v odkaze google.scam.com je google nižšia doména ako scam, teda odkaz je na stránku scam.com, podstránku google. Ďalší spôsob je pridanie znaku @ do adresy. Tento znak sa má používať na autentifikáciu, stránka http://login:password@domain.com znamená, že používateľ sa chce prihlásiť na stránku domain.com s nejakým menom a heslom. Ak stránka nevyžaduje

autentifikáciu, tak je všetko v odkaze pred týmto znakom prehliadačom ignorované [57], teda odkaz trusty@not.com odkazuje na stránku not.com. Ďalší trik je používanie domén, ktoré začínajú na „com-“. Doména http://google.com-scam.eu/find odkazuje na stránku com-scam.eu. Znak používaný na maskovanie odkazov je „&zwj“ známy ako **zero-width joiner**. Používa sa na spájanie viacerých znakov v jazykoch Hindi a emotikonoch do jedného symbolu. Ak nie sú použité tieto znaky, tak nemá žiaden význam a prehliadač ho ignoruje. Podobne sa používa aj znak, známy ako soft-hyphen (), ktorý slúži na pridanie pomlčky v slove, pokiaľ je riadok kratší ako slovo. Ináč sa ignoruje. Ďalšie používané znaky sú: indikátor sekvencie (& ordm;), ktorý môže byť interpretovaný niektorými prehliadačmi ako písmeno o, a superskripty 1 a 2 (& sup1 ;, & sup2;), ktoré môžu byť interpretované prehliadačmi ako číslice 1 a 2 [57].

Pri doménach sa využíva aj IDN (internationalized domain name – medzinárodné doménové meno). Tieto domény používajú znaky mimo ASCII rozsahu ako je cyrilika, azbuka či kanji. Niektoré z týchto znakov sú takmer identické s latinskými písmenami. Toto viedlo k **homografickým útokom**, pri ktorých sa registrovali phishingové domény so znakmi, ktoré sa v prehliadači nedali rozpoznať od latinských. Aby sa nemusela meniť infraštruktúra, tak bol vytvorený kód, ktorý vyjadruje Unicode znaky v UTF-8 kódovaní do znakov, ktoré podporuje ASCII kódovanie – Punycode [74].

Prehliadače implementovali rôzne spôsoby obrany proti homografickým útokom, často využívajúc zobrazenie v Punycode. Internet Explorer zobrazí Punycode vtedy, keď doména obsahuje znaky rôznych skriptov, napríklad latinské a azbuku [74]. Podľa novšieho článku [75] majú tento spôsob implementované všetky webové prehliadače. Webové prehliadače Mozilla a Safari zobrazujú znaky domény, ktoré nie sú ASCII v Punycode, pokiaľ nie sú TLD (top level domain – domény najvyššieho stupňa). Tieto domény podliehajú zákonom, ktoré zamedzujú spoofing. Jedna z požiadaviek vlastnenia TLD s homografmi je, aby daný subjekt vlastnil stránku aj s druhým homografom [74]. Webový prehliadač Mozilla má tiež definované povolené kombinácie skriptov, ktorých porušenie má za následok zobrazenie v Punycode, aj keď je to TLD. Okrem toho má manuálne nastavenie, ktoré zobrazí všetky znaky okrem ASCII v Puncyode bez ohľadu na iné okolnosti. Chrome zobrazí Punycode napríklad aj vtedy, keď sú všetky znaky cyrilické (teda rovnaký skript) a podobné ASCII znakom a TLD nie je medzinárodná, teda nepoužíva IDN, čo sa týka krajín, ktoré používajú latinské písmená, teda v Rusku sa zobrazí cyrilikou [75]. Webový prehliadač Google Chrome politika zobrazovania IDN domén má až desať rôznych pravidiel. Problém zobrazovania IDN je veľmi delikátny kvôli

tomu, lebo je potrebné vybalansovať pravidlá tak, aby sa zamedzilo zneužitiu a zároveň umožniť čo najväčšiu použiteľnosť pre tých, ktorých jazyk má znaky mimo ASCII kódovania.

Spear-phishing je cielený a správa je tvorená špeciálne pre prijímateľa. Spear-phishing zasahuje oveľa menší počet obetí ako phishing, väčšinou menej ako päť na organizáciu [24], ale jeho úspešnosť je o dosť väčšia. Tieto emailové správy väčšinou obsahujú osobné oslovenie, ich obsah je tvorený špeciálne pre situáciu, v ktorej sa obeť nachádza a obsahuje adresáta, ktorému obeť dôveruje a pozná ho, prípadne od neho očakáva správu. Tiež obsahuje podpisový blok s logom a kontaktnými informáciami, pokiaľ je to vhodné [24]. Dôvodom, prečo je ich tak málo, je potreba vykonať prieskum obete, zahrňujúci získavanie informácií zo stránky jej organizácie, z jej účtoch na sociálnych sieťach a iných zdrojov informácií, ktoré je možné získať [24].

1.2.3 Verejné počítačové siete a počítačové siete organizácie

Používanie sietí sa zaoberá témami ako sú možnosti izolácie vnútornej siete a dôvody potreby tejto izolácie, pripojenie sa do vnútornej siete cez VPN. Ďalšia téma sú verejné siete a ich riziká. Pri verejných sieťach je zameranie na to, aké sú možnosti bezpečného pripojenia sa cez nich, a aké typy informácií môžu získať rôznymi spôsobmi útočníci v prípade, keď na danej sieti odpočúvajú či ju vlastnia, prípadne ak vlastnia hotspot – prístupový bod na danú sieť. Existuje veľa spôsobov, ako sa brániť rôznym útokom, ktorých cieľom je získať dáta z komunikácie po sieti. Teraz si prejdeme niektoré z nich.

VPN - virtuálna súkromná sieť má za cieľ rozšíriť súkromnú sieť tak, aby sa cez verejnú sieť dalo z koncových súkromných sietí komunikovať tak, ako keby boli komunikujúci priamo spojení v súkromnej sieti. Aby mohlo byť emulované priame spojenie komunikujúcich pakety musia byť zabalené v hlavičke, ktorá obsahuje smerovacie informácie. Aby bolo emulované súkromné spojenie, dáta sú šifrované. Časť siete, v ktorej sú dáta zabalené je známa ako tunel. Celé spojenie, v ktorom sú posielané šifrované dáta je VPN [80].

TLS a jeho predchodca SSL sú kryptografické šifrovacie protokoly. Využívajú asymetrickú kryptografiu – využíva sa dvojica kľúčov, pričom to, čo je jedným zašifrované je možné odšifrovať len pomocou druhého. Po tom, čo server a klient naviažu spojenie a navzájom si pošlú náhodné hodnoty, pošle server svoj certifikát obsahujúci svoj verejný kľúč. Klient použije tento kľúč, aby sa autentifikoval a na zašifrovanie prvotného tajomstva. Klient tiež skontroluje, či je server tým, komu bol certifikát vystavený. Server môže tiež žiadať klientov certifikát, v tomto prípade mu klient pošle svoj certifikát obsahujúci jeho verejný kľúč.

Klient pošle Client Key Exchange správu po tom, čo vytvorí prvotné tajomstvo využijúc obe náhodné hodnoty. Toto tajomstvo je zašifrované verejným kľúčom servera predtým ako sa mu pošle. Obe strany si vypočítajú druhotné tajomstvo a z neho vytvoria session key – kľúč platný pre dané spojenie. Na to, aby server mohol vytvoriť tajomstvo, musí vedieť rozšifrovať správu svojim súkromným kľúčom, čo dokáže jeho identitu. Klient informuje server, že ďalšie správy už budú šifrované. Po tom, čo už má každý kľúče klient pošle hash celej doterajšej komunikácie, aby sa verifikoval. Server hash overí a pošle klientovi identickú správu a hash konverzácie doteraz. Ak klient dešifruje správu a skontroluje hash, tak proces úspešne skončil a nasledujúce správy už budú obsahovať šifrované dáta prenosu. Hashe zabezpečujú, že sa zistia všetky modifikácie komunikácie počas ich prenosu [81].

HTTPs je rozšírenie HTTP protokolu slúžiaceho na komunikáciu cez počítačové siete. Na rozdiel on HTTP pridáva prvok šifrovania do komunikácie. Protokol v staršej verzii využíval SSL, neskôr, keď bolo SSL považované za nedostatočné začal používať jeho nasledovníka TLS. Komunikácia pomocou HTTP protokolu prebieha pomocou požiadaviek a odpovedí na nich [82].

2 Súčasne riešenia na zvyšovanie bezpečnostného povedomia

Keďže v súčasnosti sa útoky využívajúce sociálne inžinierstvo a nízke bezpečnostné povedomie obetí zaradzujú k tým ktoré spôsobujú najväčšie škody v priemyselnej sfére aj verejnosti [83], vzniklo množstvo prostriedkov na obranu proti nim. Takéto riešenia sa buď zameriavajú na zvyšovanie povedomia, zlepšenie schopnosti rozoznávať útoky, alebo slúžia ako nástroje na simuláciu útokov umožňujúc tak testovať správanie pri útokoch, prípadne zahŕňajú obe zložky.

Na obranu proti bezpečnostným hrozbám, využívajúcim sociálne inžinierstvo v súčasnej dobe, existuje niekoľko riešení, ktorých cieľom je zvyšovanie povedomia osôb. Takéto riešenia je možné rozdeliť podľa cieľovej skupiny na riešenia pre:

- deti,
- jednotlivcov,
- spoločnosti.

Pre deti existuje viacero hier s danou tematikou, ktoré sú zvyčajne vyvíjané neziskovými organizáciami a univerzitami [5, 6, 7]. Učenie prebieha hravou formou, ale hra zvyčajne pokrýva len veľmi malú časť bezpečnostných problémov. Je otázne, či nejako ovplyvní bezpečnostné povedomie a vytvorí správne návyky len kvôli faktu, že hry sú zamerané na bezpečnostnú tematiku.

Pre jednotlivcov je tiež obsah tvorený prevažne neziskovými organizáciami, čo vplýva aj na kvalitu daných riešení. Zvyčajne ide o súbor článkov s doplnkovými videami a rôznymi plagátmi, či infografikami. Napríklad od National Cyber Security Alliance [8] alebo iniciácie STOP. THINK. CONNECT., ktorá zastrešuje viacero organizácií [9]. Riešenia sa zameriavajú na hrozby a praktiky, ktoré sa týkajú hlavne jedinca, ako je phishing, ochrana a zverejňovanie osobných údajov, či online nakupovanie.

Pre spoločnosti už existujú komplexné riešenia, či už platené alebo open source, zamerané na tréning a testovanie zamestnancov. Príkladom spoločnosti, tvoriacej platené riešenia, je PhishingBox [10], predávajúci nástroj na tvorbu phishingových kampaní, ktorý je možné integrovať do systémov na manažovanie vzdelávania, slúžiacich na šírenie a testovanie vedomostí (LMS). Iným príkladom je spoločnosť KnowBe4 [11], ktorá ponúka programy zahŕňajúce phishingové testy, testy na silu hesiel a materiály, vrátane interaktívnych modulov pre LMS, aj prístup k ich LMS cez cloud. Ďalším príkladom je Wombat Security Technologies [12], ktorý ponúka okrem phishingového aj smishingový simulátor. Smishingový útok zahŕňa

maskovanie identity ako pri phishingu, ale doménou útoku sú SMS správy. Existuje tiež veľa možností na zabezpečenie nielen materiálov, ale aj prednášok so špecialistami v tejto oblasti.

V nasledujúcich kapitolách porovnávame existujúce riešenia pre testovanie phishingu, nástroje na porovnávanie bezpečnosti webových prehliadačov a hesiel. Nakoniec sa zameriame na systémy na riadenie vzdelávania. Ak pri porovnávaní riešení berieme do úvahy vek najnovšej verzie, tak čas, od ktorého ho počítame, je druhá polovica novembra 2017.

2.1 Systémy na testovanie útokov sociálneho inžinierstva

Pri open source riešeniach existuje niekoľko simulátorov phishingových útokov. Príkladmi sú napríklad Spear Phisher [13], Phishing Frenzy [14], King Phisher [15], ktoré sa kvalitou a ponukou vyrovnajú plateným. V nasledujúcich podkapitolách sa bližšie budeme venovať analýze jednotlivých simulátorom. Výsledky následne zhrnutie do tabuľky.

2.1.1 Spear Phisher

Spear Phisher [13] je vytvorený v programovacom jazyku Python využívajúc webové prostredia (frameworky) Django a Bottle. Slúži na tvorbu a posielanie phishingových emailov. Súčasne slúži na sledovanie výsledkov phishingovej kampane, kde ukladá kliknutia na podvrhnuté webové stránky. Kampaní môže bežať viacero naraz. Má v sebe SMTP server a pristupuje sa naňho cez webový prehliadač. Najnovšia verzia má viac ako 3 roky. Napriek tomu má malú, ale postačujúcu dokumentáciu. Pri pokuse o jeho použitie sme sa stretli s chybami, ktoré znemožňovali využiť ho na posielanie emailových správ.

2.1.2 King Phisher

King Phisher [15] je funkcionalitou podobný Spear Phisherovi. Jeho osobitnosťou je, že klientska časť môže bežať aj na systéme Windows. Klientska časť predstavuje aplikáciu, ktorá beží osobitne, nie cez webový prehliadač. To, že nemá webové rozhranie, je podľa autorov výhoda, keďže sa vyhne webovým zraniteľnostiam ako je XSS (cross site scripting) – posielanie spustiteľných skriptov stránke namiesto textových údajov. Umožňuje klonovať webové stránky, čo dodá väčšiu dôveryhodnosť odkazom v emailovej správe. Tiež umožňuje pridávať do emailovej správy obrázky, kalendárové pozvánky a prílohy cez grafické rozhranie. Z kampane si ukladá to, či bolo kliknuté na webovú stránku, resp. či bolo zadané prihlasovacie heslá. Je možné pomocou neho zasielať SMS notifikácie, keď prídu výsledky z kampane. Je modulárny s možnosťou tvorby nových modulov. K tomuto napomáha aj dobre spracovaná

dokumentácia (posledná verzia je z júna 2017). Vývojári v tomto nástroji pripravili aj viacero vzorových emailových správ a webových stránok pre použitie v rámci phishingových kampaní.

2.1.3 Phishing Frenzy

Phishing Frenzy [14] je vytvorený v Ruby. Konkrétne využíva Ruby on Rails Framework vytvorený pre tvorbu webových aplikácií. Toto prostredie využíva aj pri posielaní emailových správ. Na administráciu sa používa webový prehliadač. Umožňuje klonovať webové stránky, pridávať prílohy do emailových správ a pri phishingovej kampani umožňuje sledovať otvorenie emailovej správy, návštevu webovej stránky a zadanie hesiel. Sledované údaje vrátane hesiel si môže ukladať. Je možné vytvoriť aj šablóny pre neskoršie použitie napriek priemernej dokumentácii. Najnovšia verzia je z apríla 2018, čo znamená, že ide o aktuálny a živý projekt.

2.1.4 Gophish

Gophish [40] je ako jediný zo spomínaných nástrojov napísaný v GO. Veľa funkcií je podobných King Phisherovi. Tiež umožňuje klonovať webové stránky, pridávať prílohy, ukladať heslá a kliknutia na odkaz. Spúšťa sa cez webový prehliadač. Výstup editora zobrazuje pri písaní webovú stránku, ako ju budú vidieť používatelia. Z tohto dôvodu je ľahké písať webové stránky pre odkazy. Ako jeden z uvedených beží aj na operačnom systéme Windows. Najnovšia verzia programu 0.4.0 je zo septembra 2017, ktorá obsahuje aj dobre spracovanú dokumentáciu. Pre používateľov sú pripravené aj vzorové webové stránky s emailovými správami, ktoré sa dajú použiť v programe.

V nasledujúcej tabuľke porovnávame funkcionalitu phishingových riešení. Zamerali sme sa na ich funkcionalitu, najmä na možnosť ukladania štatistík a ich rozsah, možnosť pridať prílohy a schopnosť klonovať webové stránky.

názov	jazyk	ukladanie štatistík	prílohy	klonovanie stránok	OS	databáza
Social Engineer Toolkit	Python	nie	áno	áno	Linux, OS X	?
Spear Phisher	Python	návšteva stránky a otvorenie prílohy	áno	nie	testované na Ubuntu	MySQL
King Phisher	Python	návštevy stránky, zadané heslá	áno	áno	server Linux, client	SQLite, PostgreSQL
Go Phish	Go	otvorenie mailu, návšteva stránky, vložené údaje	áno	áno	Windows, OS X,	Mysql
SPToolkit rebirth	PHP	návšteva stránky, vložené údaje	nie	nie	?	MySQL
Phishing Frenzy	PHP/Ruby	otvorenie mailu, návšteva stránky, zadané heslá	áno	áno	Debian, Ubuntu	MySQL

Tab. 1 porovnanie phishingových riešení

Mnoho ďalších útokov, spojených aj so sociálnym inžinierstvom, sa dá simulovať pomocou nástrojov na penetračné testovanie, ako je Social Engineer Toolit (SET) [16], či Browser Exploitation Framework (BEeF) [17].

2.1.5 Zhrnutie

Porovnanie sme urobili za cieľom vybrať riešenie, ktoré nám umožní posielať účastníkom kurzu v systéme na riadenie vzdelávania emailové správy s predstieraným (spoofovaným) odosielateľom na simulovanie phishingu. Pri našom pokuse sme ako SMTP server využili Postfix a skúsili sme poslať spoofovanú emailovú správu na služby ako Gmail a Outlook. Obe služby nás blokovali a správu sme nemohli odoslať. Blokovanie bolo pravdepodobne spôsobené riešením na ochranu proti emailovému phishingu, ako je Sender Policy Framework (SPF). Toto prostredie funguje tak, že spoločnosti dopredu oznámia, ktoré emailové servery môžu posielať správy, ktorých odosielateľmi sú oni, teda adresou je ich doména. Ak príde emailová správa z iného emailového servera, v ktorej ako adresu odosielateľa používa doménu danej spoločnosti, ale nie je poslaná z jej serverov, tak je zahodená [79]. Potom sme skúsili prenos cez Gmail účet. Vo výslednej emailovej správe sme nemali správne predstieraného (spoofovaného) odosielateľa. Nakoniec sme sa rozhodli, že nebudeme posielať emailové správy účastníkom, ale urobíme šablóny emailoých sprav, ako to má vo svojom phishingovom teste uvedený vládny tím na riešenie bezpečnostných incidentov – CSIRT.SK [76]. Pri tomto riešení vieme ľahko získať aj údaje používateľov na simuláciu spear-phishingu. Z týchto dôvodov sme nepoužili ani jedno z porovnávaných riešení.

2.2 Systéme na testovanie bezpečnosti webových prehliadačov a hesiel

2.2.1 Social Engineer Toolit (SET)

Social engineer toolkit (SET) [16] je nástroj slúžiaci na penetračné testovanie, ktorý využíva **Metasploit** prostredie. Toto prostredie sa využíva na spúšťanie kódu zneužívajúci známe zraniteľnosti. Metasploit umožňuje previesť veľké množstvo útokov zameraných hlavne na sociálne inžinierstvo. Celé jeho rozhranie je menu v príkazovom riadku a všetky podrobnosti sa nastavujú v konfiguračnom súbore.

Čo sa týka útokov, využívajúcich sociálne inžinierstvo, možno si vybrať napríklad phishingový útok s predstieranou (spoofovanou) adresou. Ďalším príkladom je Java applet útok so spoofovaným Java certifikátom, ktorý používateľovi ponúkne možnosť nainštalovať si škodlivý Java applet – malú aplikáciu. Ponúka aj útok s plnou obrazovkou (full screen útok) využívajúci HTML5 full screen API v prehliadačoch, kde sa prepíše odkaz zobrazený pri držaní kurzora nad textom odkazu. Medzi jeho základné služby patrí zberanie mien a hesiel s klonovanou stránkou. Má aj tabnabbing, kde po kliknutí na odkaz je používateľovi prezentovaná správa informujúca ho o tom, že webová stránka sa načíta. Keď používateľ zmení kartu, v prehliadači sa stránka zmení na naklonovanú verziu. SET môže vykonať aj SMS spoofing útoky na webový prehliadač.

Tento nástroj má v sebe zahrnuté aj útoky z Fast Tracku, softwaru na penetračné testovanie, využívajúceho Metasploit. Má možnosť prepojenia s ettercapom – programom pre útoky na sieti pre DNS spoofing. Možno si ho rozširovať modulmi. Ide o živý projekt s veľmi dobre spracovanou dokumentáciou.

2.2.2 Browser Exploitation Framework (BEeF)

BEeF [17] sa používa na penetračné testovanie so zameraním na slabosti prehliadača. Každý, kto navštívi stránku na beef serveri, má tzv. „zahákovaný“ prehliadač, čo znamená, že útočník môže na ňom vykonávať útoky. To samozrejme poskytuje veľa

možností. Nezameriava sa na sociálne inžinierstvo ako celok, ale okrem iného obsahuje aj veľa útokov, ktoré sociálne inžinierstvo využívajú.

Z nich môžeme spomenúť modul na tzv. session timeout útok oznamujúci, že sme boli odhlásení zo stránky pre nečinnosť, pričom sa presmerovala webová stránka na jej klon. Ďalej poskytuje tabnabbing útok, falošný flash update pre inštaláciu rozšírenia do prehliadača, clickjacking – nalákanie na kliknutie na niečo, čo používateľ nechcel. Pri tomto využíva neviditeľné iframy – HTML tagy, ktoré umožňujú vkladať do stránky iné webové stránky, ktoré v tomto prípade nie sú viditeľné. Možno si ho rozširovať modulmi. Dokumentácia nie je úplná. Najnovšia verzia je približne 2 roky stará.

2.2.3 Testovanie sily hesiel

Na testovanie sily hesiel existujú knižnice vo viacerých jazykoch ako **zxcvbn** [18] pre JavaScript či **nbvcxz** [19] pre Javu.

Zxcvbn [18] (a jeho deriváty pre rôzne jazyky) sú knižnice, ktoré odhadujú silu hesla. Zxcvbn vytvorili pracovníci Dropboxu, ale ide o program s otvoreným zdrojovým kódom. Používa anglický slovník, databázu mien a priezvisk a desaťtisíc bežných hesiel, ktoré označuje ako slabé. Ďalej používa hľadanie vzorov – skúša nájsť l33t slová (nahrádzanie písmen podobne vyzerajúcimi číslami, čo nie je bezpečné). Súčasne so slovami v slovníku porovná aj ich palindromy – reverzované slová. Rozozná sekvencie (123, abc), opakovanie podreťazcov cez regulárne gramatiky, sekvencie, ktoré sú robené na klávesnici – klávesové vzory pre viacero typov klávesníc a dátumy. Pre každý typ vypočíta skóre v entropii s predpokladom, že útočník pozná typ hesla. Ako výsledok berie najmenšiu entropiu všetkých typov, do ktorých patrí vstup. Výstupom je čas, ktorý je potrebný na zlomenie hesla, ak útočník použije typ, ktorý má najmenšiu entropiu. Predpokladá sa, že útočník nie je pripojený k internetu, čiže má rýchly prístup k heslám a používa viacero jadier paralelne. Knižnica pri zadaní slabého hesla varuje používateľa aj s odôvodnením, prečo ide o slabé heslo.

Nbvcxz [19] je port zxcvbn pre Javu, ale má pridaných niekoľko zmien. Prvou zmenou je porovnávanie hesiel pri rôznych typoch vzorov. Ako výsledok vráti najmenšiu nájdenú entropiu. Pri porovnávaní so slovníkom možno použiť Levenshteinovu vzdialenosť - počet vkladaní, odoberaní alebo zámen písmen, potrebných na to, aby zo slova vzniklo iné. Ľahko je možné pridať nové slovníky, alebo pozmeniť staré. Možno ho použiť ako osobitný konzolový program, alebo ako knižnicu pre vlastný program.

V nasledujúcej tabuľke (Tab. 2) porovnávame knižnice na určovanie sily hesiel. Atribúty porovnania boli existencia blacklistu a slovníka, odhalenie vzorcov na klávesnici, počítanie entropie, odhaľovanie sekvencií písmen a čísel a ich opakovanie.

názov	jazyk	blacklist	vzorce na klávesnici	slovník	entropia	sekvencie, opakované znaky
zxcvbn	JS	áno	áno	aj s pravidlami (napr. dátumy)	áno	áno
python-zxcvbn	Python	áno	áno	áno	áno	áno
nbvcxz	Java	áno	áno	aj Levenshtein distance	áno	áno
ng password meter	JS	nie	nie	nie	nie	áno
ng password strength	JS	nie	nie	nie	nie	áno
passwordmeter	JS	nie	nie	nie	nie	áno
passwordmeter	Python	áno	nie	v budúcnosti	nie	áno
password strength meter	JS	nie	nie	nie	nie	áno
jquery entropizer	JS	nie	nie	nie	áno	nie

Tab. 2 Porovnanie knižníc na určovanie sily hesiel

2.2.4 Zhrnutie

Medzi knižnicami na testovanie sily hesiel sme hľadali také, ktoré by sme mohli využiť pre tvorbu aplikácie, v ktorej by si mohli používatelia vyskúšať silu rôznych hesiel. Naša požiadavka pri výbere knižnice spočívala v tom, aby knižnica nepočítala silu hesla podľa daných pravidiel, ako je napríklad požadovanie znaku či čísla, keďže takéto heslá sú účinné len proti útokom hrubou silou. Pokiaľ nie sú heslá výnimočne dlhé, tak ich účinnosť aj tak nie je veľká. Väčšina riešení ale používala presne tento typ určovania sily hesla. Knižnica zxcvbn (a jeho deriváty) počíta silu hesla úplne iným spôsobom - pomocou najmenšieho súčtu entropie častí hesla, tvorených vzorcami, ako sú opakovania, postupnosti, nahradzovanie písmen číslami, palindromy a ďalšie. Inými slovami sa predpokladá, že útočník pozná vzorce, ktoré tvoria heslo a vyberie si tie, cez ktoré ho najskôr prelomí.

Jediné nami porovnávané riešenie okrem Zxcvbn ktoré počítalo entropiu, bol **jQuery Entropizer**. Tento však na rozdiel od Zxcvbn nemal blacklist bežných hesiel, ani slovník. Súčasne nerozoznával vzorce na klávesnici, čiže heslá týchto typov by označil za silnejšie, ako by boli pre útočníka, ktorý by tieto vzorce skúšal pri prelomení. Na základe tohto porovnania sme sa rozhodli pre knižnicu Zxcvbn..

2.3 Systémy na riadenie vzdelávania (LMS)

Možnosťou pri tvorbe systému na zvyšovanie povedomia je aj využitie existujúcich systémov používaných pri vzdelávaní. Takýmito sú **systémy na riadenie vzdelávania** (LMS) slúžiace na šírenie a testovanie vedomostí. Pri teoretickej časti zvyšovania povedomia to uľahčí sledovanie výsledkov a tvorbu spoločných kurzov, lekcií a testov, ktoré majú LMS implementované vo veľkej variabilite. Existuje veľké množstvo LMS. My budeme porovnávať len riešenia s otvoreným zdrojovým kódom. V nasledujúcich kapitolách popíšeme rôzne LMS a sústredíme sa na možnosti tvorby kurzov a testovania.

Následne tieto systémy porovnáme. Najprv na základe databázových systémov, operačných systémov a štandardov, špecifikácií, či protokolov, ktoré využívajú. Ďalšie porovnanie je založené na kritériách, ktoré potrebujeme pri tvorbe kvalitnej kampane na zvyšovanie povedomia v oblasti informačnej bezpečnosti. Medzi tieto kritéria patrí široká podpora pre gamifikáciu a ponuka rôznych možností pre interaktívne učenie.

Keďže kombinácia metód doručenia obsahu (text, video, obrázky) ho delí na segmenty rôznych typov, čím ho robí ľahšie pochopiteľným [24], tak požadujeme aj podporu rôznych typov obsahu. Okrem uľahčenia pochopenia obsahu ide aj o jeho zaujímavosť kvôli motivácii a z toho dôvodu Herold R. odporúča okrem iného zahrnúť fotky, videá, grafický materiál, animáciu a zamerať sa na interaktivitu [27]. Pre oblasť bezpečnosti sú veľmi dôležité videá a simulácie, keďže môžu byť použité na ukážku rôznych útokov. To má oveľa väčší dopad na účastníka ako jednoduchý popis útoku [24].

Prostredie H5P vytvorený v JavaScripte ponúka interaktívny HTML5 obsah, čo zahŕňa rôzne typy interaktívnych obrázkov, videí, prezentácií, kvízov a iného. Toto prostredie je dostupné ako doplnok v rôznych LMS. Naším ďalším kritérium je existencia H5P doplnku alebo ekvivalentného riešenia v LMS. Inými slovami takého riešenia, ktoré zabezpečuje interaktívne video, obrázky a kvízy s takýmto interaktívnym obsahom, respektíve v prípade videa kvíz, ktorý je vo videu – teda video obsahujúce otázky.

Ďalšie kritériá sa zameriavajú na kvízy. Pri tvorbe kvízov je veľmi dôležité pri nesprávnej odpovedi vysvetliť, prečo bola nesprávna, tak, aby účastník vedel, kde urobil chybu [24]. Z tohto dôvodu je ďalším kritériom možnosť dávať spätnú väzbu založenú na odpovedi po tom, čo ju účastník označí v kvíze. Posledným kritériom je možnosť označovať odpovede v kvíze na škále istoty (CBM – Confidence/Certainty-Based Marking) a podľa toho ich hodnotiť. CBM hodnotí lepšie správne odpovede, pri ktorých sú si študenti istí. Naopak sťahuje viac bodov za nesprávne odpovede, pri ktorých sú si študenti istejší. Takéto kvízy nútia účastníkov hlbšie premýšľať a pomáhajú im odhaliť ich slabosti v danej oblasti [44]. Je ale dôležité nastaviť bodovanie jednotlivých stupňov tak, aby neprofitovali príliš sebaistí alebo naopak nesmelí účastníci [44]. Mnohé LMS podporujú Likert Scale otázky, teda také, ktorých odpoveď sa označuje na stupnici súhlasu. Tieto otázky sú ale rozdielne od CBM tým, že samotná odpoveď sa označuje na stupnici, kým CBM je spôsob hodnotenia istoty odpovede a aplikuje sa až po odpovedi na otázku.

2.3.1 Chamilo

Tento LMS vznikol ako nový projekt, ktorý sa odklonil od pôvodného LMS Dokeos. Odvtedy sa dosť zmenil. Umožňuje vytvárať kurzy, ale tiež si ich importovať z HotPotatoes, Qti2 a Excelu. Možno tvoriť skúšky, testy, kvízy, zadania, prieskumy, sledovať progres žiakov a ich dochádzku, a mnoho iného (chat, fórum..). Možno posielať mailové notifikácie účastníkom kurzu, podporované sú aj automatické notifikácie, napríklad učiteľ môže dostať notifikáciu vždy, keď študent ukončí kvíz. Účastníci si môžu v aplikácii posielať maily aj medzi sebou. V najnovšej verzii, ktorá ešte nemá dokumentáciu, ponúka aj gamifikačný mód, ktorý umožňuje rozdávať body a hviezdy za rôzne úlohy.

V kurzoch možno uchovávať HTML, PowerPoint, Excel, Flash, Word dokumenty. Pri testoch je ponúknutých veľa možností, napríklad počet možností pri odpovedi, časové obmedzenia a tiež možnosť, kde podľa odpovede bude rozhodnutá nasledujúca otázka, čo umožňuje budovať scenáre. Otázky môžu mať jednu alebo viac ponúknutých odpovedí s jednou/viac správnymi odpoveďami alebo vlastnú odpoveď, dokonca aj výber správnej časti obrázku, spájanie textových dvojíc, hlasové odpovede. Po každej odpovedi môže študent dostať feedback. Otázky možno združovať do kategórií a levelov obťažnosti. Najnovšia verzia má 4 mesiace [41].

2.3.2 OPEN edX

EdX bol vytvorený na Harvarde a MIT ako MOOC (massive open online course) poskytovateľ – teda poskytovateľ online kurzov pre veľký počet používateľov. EdX beží na Open edX platforme, čo je CMS (control management system), skladajúci sa zo Studia a Open edX LMS. Platforma umožňuje posielať mailové notifikácie, aj hromadné maily. Na tvorbu kurzov slúži Studio. Do kurzov možno vkladať HTML, videá, diskusie a zadania. Pre HTML ponúka až dva editory. V zadaniach možno požadovať textové, číselné odpovede, viac odpovedí na otázku, ale aj menej štandardné veci ako matematické vzorce, drag and drop otázky pre obrázok, možno obmedziť počet odpovedí, dávať pomocné texty, ktoré môžu byť adaptívne - závisia od odpovede, aj keď tieto nie sú oficiálne podporované.

Používajú sa aj čiastočné ohodnotenia za správne zodpovedanú časť otázky, nastavenia zahŕňajú aj váhu hodnotenia otázky. Tvorba vlastných zadaní je podporovaná pomocou nástroja, v ktorom možno tvoriť JavaScriptové stránky, predstavujúce zadania. Tiež možno robiť zadania, hodnotené cez vlastný Python skript. Možno aj nastaviť ďalšie otázky podľa predošlých odpovedí.

Oživenie kurzu prináša modul Opia na tzv. explorations, čo sú tutoriály formou dialógov s otázkami s interaktívnym obsahom. Zatiaľ jej chýba interaktívne video, ale ponúka viacero typov interaktívnych obrázkov. Gamifikáciu podporuje možnosťou dávať odznaky a vlastné certifikáty za splnenie cieľov. Je aj veľa oficiálne nepodporovaných nástrojov, ktoré vytvárajú vlastné vylepšenia ako chemické rovnice, umožňujú prezerať si 3D molekuly, mutácie DNA a mnoho iného [42]. Na programe sa intenzívne pracuje – nové commity sú na github zverejňované takmer každý deň.

2.3.3 Opigno

Je to LMS postavený na Drupale, čo je CMS – control management system. Ako Drupal LMS má H5P plugin. Najnovšia verzia je z mája 2016. Je možné v ňom vytvárať lekcie, ktoré môžu byť teoretické alebo robené ako testy. Lekcie sú v kurzoch, pričom je možné stanoviť potrebnú známku na úspešné zvládnutie lekcie, ako aj celého kurzu. Ponúka fórum, chat a videokonferencie. Podporené je aj vkladanie videí a priečinkov so súbormi pre študentov. Je možné integrovať Mozilla Open Badges – odznaky, ktoré možno v kurze dávať ako odmeny za splnenie určených kritérií. Okrem odznakov možno tvoriť a rozdávať aj vlastné certifikáty.

Otázky možno ponúkať v náhodnom poradí. Pri kvízoch ponúka rôzne možnosti, napríklad možnosť označiť odpoveď ako pochybnú, ak si študent nie je istý, feedback, alebo

možnosť odpovedať na otázku opakovane, kým nebude odpoveď správna. Počet pokusov o odpoveď môže byť aj obmedzený. Typy otázok sú: vypĺňanie prázdnych častí textu, viac odpovedí, drag and drop, spájanie dvojíc, esej, pravda/nepravda, Likert scale otázka, ktorá je tu nazvaná slide. Je možné dávať aj záporné skóre za nesprávne odpovede [43].

2.3.4 Sakai

Je to jediný z porovnávaných LMS vytvorený v Jave. Najnovšia verzia je z júna. Ponúka chat, fóra, nástroj na posielanie mailov a možnosť výmeny súkromných správ, ktoré sa posielajú do schránky, viazanej ku kurzu.. Možno posielať aj skupinové maily. Na tvorbu obsahu ponúka WYSIWIG editor, ináč nazývaný aj rich-text editor. Vďaka integrácii Dropboxu je možné vytvárať v Sakai priečinky, prepojené na Dropbox, vďaka čomu sú pri každej zmene zálohované.

Pri testoch je na výber viacero typov otázok, ako je otázka s niekoľkými možnosťami odpovede, pravda/nepravda, textová odpoveď, vypĺňanie medzier v texte, kalkulované otázky, kde sa požaduje výsledok vzorca s náhodnými premennými, ďalej hotspot otázky, kde sa vyznačuje časť obrázku, a hlasové odpovede. Kaltura plugin umožňuje pridať kvíz formou interaktívneho videa. Kaltura je mediálna platforma pre tvorbu a prehrávanie videa a nahrávok. V Kalture je možné vytvoriť aj videokvíz.

Okrem samotných testov a kvízov je možné vytvárať aj lekcie, rôzne zadania a prieskumy s tvorbou štatistík. Pri prieskume je možné použiť Likert scale otázky. Pri známkovaní testov sa ponúka hodnotenie priemerom aj vážené hodnotenie, kde je možné vytvoriť váhové kategórie otázok a v nich pridávať vážené otázky, čím sa ich váha znásobí váhou kategórie. Možno pridávať aj negatívne hodnotenie. V niektorých typoch otázok je možnosť čiastočného hodnotenia [45].

2.3.5 ATutor

Ponúka tvorbu kurzov, známkovaných testov a prieskumov. Pri tvorbe testov sa určuje počet pokusov, minimálne skóre na úspešné ukončenie, feedback pri úspešnom skončení aj zlyhaní kvízu, ale nie feedback po otázkach. Pri tvorbe otázok sú na výber možnosti: odpoveď formou názoru na stupnici, spájanie dvojíc, otázka s viacerými možnosťami na odpoveď, kde môže byť správna jedna alebo viacero, zoradenie odpovedí podľa atribútu, textová odpoveď a pravda/nepravda. Otázky môžu byť pridávané aj v náhodnom poradí. Po

skončení testu sú ponúkané štatistiky, obsahujúce súhrn výsledkov, známky a počty označených odpovedí pri otázkach s viacerými možnosťami.

Gamifikáciu podporuje s GameMe modulom, ktorý umožňuje dávať odznaky a body za rôzne udalosti. Pomocou bodov študenti zvyšujú level na svojom účte. ATutor tiež ponúka chat, možnosť posielania mailov, aj hromadných, priamo v LMS. Okrem mailov možno posielať aj textové správy a notifikácie v schránke, viazanej ku kurzu. Medzi možnosti LMS patrí tvorba a manažovanie súborov v kurze. Študenti môžu tvoriť skupiny. Vstup do kurzu možno obmedziť na základe príslušnosti k skupine. V skupine môže byť zvolený asistent s obmedzenými právami popri rolách učiteľa, študenta a administrátora. Dokumentácia je slabšia, roztrieštená na veľa stránok. Najnovšia verzia je z júna 2016 [46].

2.3.6 ILIAS

Tento LMS je z Nemecka. Ponúka tvorbu kurzov, fóra, blogy, testy a prieskumy. ILIAS má integrovaný aj chat server. Pri kurzoch možno požadovať splnenie podmienok v predošlých kurzoch, ináč bude kurz pre účastníka zamknutý. Podobné obmedzenie prístupu možno nastaviť aj pri kvízoch/testoch. Pri testoch možno pridávať pomocný text pri zlej odpovedi s voliteľnou redukciou skóre a feedback. Študent môže o tento pomocný text požiadať aj bez zadania odpovede, čo tiež vedie k penále. Ako jeden z mála LMS podporuje interaktívne video pluginom, ktorý vo videu umožňuje pridávať komentáre, dokonca aj sériu otázok, čím vznikne kvíz.

Pri tvorbe kvízov môžu byť použité otázky s viacerými správnymi odpoveďami, s nastavením mínusových bodov za nesprávne alebo neoznačené správne odpovede. Pri otázkach s požadovanou textovou odpoveďou je možné nastaviť dopĺňanie, kde sa postupným písaním zobrazujú možnosti, ktoré vyhovujú textu. Existujú aj iné typy otázok, napríklad výber správneho slova v texte, spájanie dvojíc, zoraďovanie, hot spot image, Java applet, Flash applet otázky, ktoré už nemajú byť podporované od najnovšej verzie z bezpečnostných dôvodov, vzorec s dynamickými hodnotami premenných. Otázka môže vyžadovať ako odpoveď aj súbor.

Možno definovať minimálny počet bodov pre úspešné ukončenie, aj pre jednotlivé známky. Pri odpovediach môžu študenti použiť rich text editor, ktorý im umožní pridávať aj tabuľky. Aplikácia môže zasielať mailové notifikácie v prípade určených udalostí, zabudované je aj posielanie mailov, ktoré možno poslať aj skupinám, vytvoreným v ILIASe. Dokumentácia je na dobrej úrovni. Najnovšia verzia je z októbra [47].

2.3.7 Canvas

Tento LMS je jediný zo zoznamu, vytvorený v Ruby. Ponúka tvorbu kurzov, chat, zadania, kvízy, prieskumy. Je tu aj možnosť virtuálnych lekcií, ktoré sú zabezpečené integrovanou aplikáciou BigBlueButton, ktorá ponúka zdieľanie videa, zvuku, chatu a obrazovky. Využíva aj platenú aplikáciu Arc na výučbu pomocou videa, ktorý umožňuje manažovanie videa, jeho zdieľanie a hlavne diskusiu a komentáre priamo vo videu. Na kontrolovanie dochádzky majú integrovanú aplikáciu tretej strany. Namiesto integrovanej podpory mailov majú vlastnú verziu posielania správ, ktorá je veľmi podobná mailom z pohľadu používateľa. Má schránku a je možné posielať aj hromadné správy. Je možné integrovať interaktívne videokvízy vďaka Kaltura/Canvas integrácii.

LMS ponúka prepracované štatistiky o používateľoch a kurzoch, pri ktorých je cieľom autorov predvídanie rizikových študentov a meranie efektivity rôznych štýlov učenia. Štatistiky sú hierarchicky usporiadané, na vrchole sú pre celú organizáciu. V kurzoch je možné robiť oznámenia, o ktorých študenti dostanú notifikácie. Pri tvorbe obsahu je možné využívať vnútorný rich text editor. Pri otázkach sú možnosti: viac odpovedí, pravda/nepravda, vypĺňanie, text, súbor, spájanie dvojíc a výsledky pre vzorec s dynamickými hodnotami premenných, nehodnotená Likert scale otázka.

Ako odpoveď na zadanie možno odoslať aj súbor, na jednom dokumente môže priamo v LMS spolupracovať viac študentov. Študenti môžu mať aj svoje súbory určenej veľkosti. Ako hodnotené zadanie môže byť použitá aj diskusia. V kvíze je možné dostať feedback po otázke. Pri spolupráci využíva Google Docs Collaboration. Študenti môžu za aktivity dostávať odznaky. Dokumentácia je bohatá, niekoľko tisíc strán. Najnovšia verzia je len 9 dní stará [48].

2.3.8 Moodle

Najviac používaný LMS zo spomenutých. Má veľké množstvo používateľov – až 130 miliónov. Ponuka zahŕňa tvorbu kurzov, lekcií, zadania, chat, fórum, prieskumy a kvízy. Pri tvorbe lekcií je aj možnosť tvorby scenárov, kde je podľa odpovede rozhodnuté, ktorá stránka sa zobrazí ako nasledujúca. Je tu aj možnosť virtuálnych lekcií, ktoré sú zabezpečené integrovanou aplikáciou BigBlueButton, ktorá ponúka zdieľanie videa, zvuku, chatu a obrazovky. V kurzoch možno sledovať aj dochádzku.

Každý kurz má fórum oznámení, kde sú prihlásení všetci študenti a slúži pre učiteľa na ohlásenie dôležitých tém ku kurzu. Okrem toho možno priamo z Moodlu posielať aj maily. Testy sú hodnotené, možno si nastaviť vlastnú škálu známkovania a vlastné metódy výpočtu

známky. Testom možno nastaviť aj váhu, čo sa odrazí v známke celého kurzu. V ponuke je aj obmedzenie prístupu do testov na základe viacerých atribútov, ako je doterajšia známka v kurze, či počet povolených opakovaní. Je možné aj ohraničiť čas, ktorý môže študent stráviť pri teste. Možno zamknúť otázky testu, kým nebudú zodpovedané iné otázky, ktoré sú vyžadované. Feedback ku otázke možno dať hneď po označení odpovede aj na konci kvízu.

Pri testoch sú na výber nasledujúce typy otázok: výsledky vzorca s dynamickými premennými, drag and drop do textu alebo do obrázku, ktorý môže byť rozdelený na časti, výber z viacerých možností, kde môže byť viacero správnych, párovanie, chýbajúce slovo, pravda/nepravda, zoraďovanie, esej. Pre prieskum je možné pridať aj nehodnotenú Likert scale otázku. Pri type otázok, ktoré obsahujú viacero možností, je možné dať negatívne skóre za nesprávne možnosti. Umožňuje aj tvorbu otázok so škálou istoty. Moodle má H5P plugin, čiže podporuje aj H5P kvízy. Má aj Kaltura Video Package plugin podporujúci kvízy s interaktívnym videom. Moodle široko podporuje gamifikáciu vďaka pluginom. Je možné pridávať odznaky za splnenie úloh, certifikáty, levely, ktoré možno zvyšovať prechádzaním kurzov, skryté predmety v obsahu kurzov, kvízy tvorené spôsobom hier, zbieranie známok za úlohy, kompetetívne rebríčky, skóre, a iné.

Ďalšie typy otázok sú poskytované pluginmi, napríklad matematické výrazy, odpovede, zodpovedajúce regulárnym výrazom, otázky tvorené Java molecular editorom, ktorý umožňuje tvorbu dizajnu molekúl. Vďaka pluginu možno testovať aj Java zdrojové kódy. Ponúka aj PhET interaktívne simulácie, [77] ktorých obsah môže byť tvorený v Jave, Flashi alebo HTML5. V Moodli je možné funkcionalitu rozšíriť pluginmi, čo je využité aj pri jeho tvorbe – verzia 3.4 má v sebe takmer štyristo pluginov. Má aj veľkú podporu vývojárov pri ich tvorbe. Z LMS, ktoré sme porovnávali, mal najviac ponúkaných pluginov. Najnovšia verzia je 6 dní stará. Dokumentácia je výborná [49].

Tabuľka č.3 porovnáva LMS z pohľadu použitia databázových systémov, podporovaných operačných systémov a jazykov, v ktorých boli vytvorené.

názov LMS	jazyk	databáza	podporovaný OS	iné
Chamilo	JS/PHP	MySQL, MariaDB	Windows, Linux, OS X	fork of Dokeos
Open Edx	Python/JS	MySQL, SQLite, MongoDB	Ubuntu	OLI cez LTI
Opigno	PHP/JS	MySQL, MariaDB, PostgreSQL	Windows, Linux, OS X	postavený na Drupale
Sakai	Java	HSQL, MySQL, Oracle	Linux/Windows/ OS X, Solaris	Wordpress cez LTI
Atutor	PHP	MySQL	Windows, Linux, OS X	IMS content packaging, QTI
ILIAS	PHP/JS	MySQL, MariaDB	Debian, Red Hat, Ubuntu	IMS QTI
Moodle	PHP/JS	MySQL, PostgreSQL, MariaDB, MS SQL, Oracle, SQLite	Linux,Windows, Solaris, OS X, NetWare	
Canvas LMS	Ruby/JS	PostgreSQL	Linux, OS X	

Tab. 3 Porovnanie LMS

Tabuľka č.4 porovnáva LMS z hľadiska štandardov, či protokolov, ktoré sú dôležité pri výbere LMS. Tieto štandardy, resp. protokoly uľahčujú získavanie obsahu, zálohovanie, či prechod na iný LMS, ktorý uznáva rovnaké štandardy. Porovnávané štandardy sú: SCORM (Sharable Content Object Reference Model), ktorý je najrozšírenejší, iné štandardy a špecifikácie, ktoré boli zväčša vytvorené ako jeho nástupcovia. Tieto štandardy a špecifikácie slúžia pre import a export obsahu do a z LMS a tak zaručujú, že je možné použiť ten istý obsah (napríklad kvíz) vo všetkých LMS, ktoré ho podporujú, alebo dokonca ho vytvoriť v programe, ktorý sa zaoberá len tvorbou obsahu a potom ho nasadiť v LMS. Niektoré protokoly rozširujú svoju pôsobnosť aj mimo prenosu obsahu.

názov LMS	SCORM	IMS LTI	AICC - HACP	xAPI	IMS Common Cartridge
Chamilo	1.2	v budúcnosti	áno	nie	nie
Open Edx	1.3	áno	nie	nie	nie
Opigno	1.3	v budúcnosti	nie	áno	nie
Sakai	1.3	áno	nie	áno	áno
Atutor	1.2	áno	v budúcnosti	nie	áno
ILIAS	1.3	áno	mali po verziu 5.2	v budúcnosti	nie
Moodle	1.2 (1.3 cez plugin)	áno	áno	áno	áno
Canvas LMS	1.3	áno	nie	čiastočne	len import

Tab. 4 Porovnanie LMS štandardov

Ďalší štandard je LTI (Learning Tools Interoperability), ktorý okrem iného definuje spôsob, ako by sa mali spúšťať aplikácie tretej strany z LMS s jediným prihlásením. Myšlienkou je, aby mohol administrátor LMS ovládať nástroje na učenie na diaľku priamo zo svojho systému. AICC (Aviation Industry CBT Computer-Based Training Committe) je skupina, ktorá tvorí štandardy pre letectvo, ale sú tak všeobecné, že sa často využívajú aj v iných oblastiach. Ich HCP (HTTP-based AICC/CMI Protocol) sa využíva vo viacerých LMS a bol základom pre SCORM. xAPI bolo navrhnuté ako nasledovník SCORMu a na rozdiel od jeho využitia XML využíva JSON ako data formát a ponúka nový pohľad na zdieľanie obsahu, zahŕňajúci ukladanie celého učiaceho progresu do tzv. LRS (Learning Record Store), ktorý môže fungovať mimo LMS a možno sa naň pripojiť z mnohých typov zariadení, ktoré môžu byť aj off-line v čase používania, synchronizácia sa vykoná neskôr. Posledným je IMS Common Cartidge, špecifikácia definujúca formát pre tvorbu a zdieľanie digitálneho edukačného obsahu [49].

Tabuľka č.5 porovnáva LMS podľa nami stanovených kritérií: H5P doplnok alebo jeho ekvivalent, možnosti gamifikácie, feedback v kvízoch a otázky so stupňom istoty (CBM).

názov LMS	H5P plugin/ ekvivalent	gamifikácia	feedback po otázke	CBM
Chamilo	H5P v budúcnosti	áno	áno	nie
Open Edx	Opia	áno	áno	nie
Opigno	H5P	áno	áno	nie
Sakai	Kaltura plugin a hotspot obrázky v kvíze	nie	áno	nie
Atutor	nie	áno	nie	áno
ILIAS	Interactive Video plugin, hotspot obrázky v kvíze	v budúcnosti	áno	nie
Moodle	H5P a Kaltura	áno	áno	áno
Canvas LMS	Kaltura, hotspot otázky v budúcnosti	áno	áno	nie

Tab. 5 Porovnanie LMS II

2.3.9 Zhrnutie

Cieľom porovnania systémov na riadenie vzdelávania bol výber toho systému, ktorý by nám najviac vyhovoval pri tvorbe kampane na zvyšovanie povedomia v oblasti informačnej

bezpečnosti. V podpore štandardov vedie Moodle. Druhý je Sakai, ktorý nepodporuje len jeden štandard. Interaktívny obsah v takom rozsahu, ako sme požadovali, poskytovali štyri LMS. Všetky využívali riešenia tretích strán, pričom Moodle umožňoval využiť obe hlavné riešenia – Kalturu a H5P. Gamifikáciu podporovalo mnoho LMS, často ale len odznakmi a certifikátmi. Najširšiu podporu gamifikácie mal Moodle. Feedback pri otázkach kvízu podporoval takmer každý. Niektoré systémy podporovali aj spätnú väzbu po kvíze, ktorá záležala od skóre. CBM podporoval len Moodle. Keďže Moodle najlepšie vyhovoval našim kritériám, rozhodli sme sa pre neho. Moodle má tiež najviac doplnkov z porovnávaných LMS a podporuje najviac DBMS – databázových systémov.

3 Systém na zvyšovanie povedomia v informačnej bezpečnosti

Systém na zvyšovanie povedomia v oblasti bezpečnosti je program s cieľom trénovať používateľov proti potenciálnym hrozbám pre informácie organizácie. Tento systém ukazuje, ako sa vyhnúť situáciám, ktoré môžu ohroziť dáta organizácie [24]. Náš program je postavený na systéme na riadenie vzdelávania Moodle.

3.1 Návrh systému

Obsah kurzu delíme na niekoľko tematických modulov pozostávajúci z lekcií, zakončených kvízmi. V moduloch, ktoré delia používateľov podľa levelu ich predošlých znalostí, bude viacero verzií kvízov. Tieto budú rozdelené podľa obťažnosti, do ktorej budú účastníci zaradení na začiatku modulu pomocou testu. Táto obťažnosť je dynamická a každým testom sa upravuje podľa celkových výsledkov. Opustili sme myšlienku podobného delenia na základe učebných štýlov, keďže štúdie nepotvrdili ich pozitívny vplyv pri výučbe, ako sme už poukázali. Témy sme vyberali z tých, ktoré sme spomenuli v kapitole Informačná bezpečnosť. Do systému sme zahrnuli nasledujúce témy:

- tvorba a správa hesiel,
- e-mailová komunikácia,
- komunikácia a profily v rámci sociálnych sietí,
- Wi-fi.

Pri tvorbe obsahu využívame spôsoby zvyšovania motivácie, ktoré sme preberali v kapitole Zvyšovanie motivácie. Pri návrhu tematických modulov dávame dôraz na gamifikáciu a interaktívne učenie, o ktorých sme písali v kapitole Bezpečnostné povedomie.

3.1.1 E-mailová komunikácia

Tento modul pokrýva oblasti sociálneho inžinierstva - **phishing, spear-phishing** – cielený phishing, **spam** – nechcené správy a **hoaxy** – klamlivé správy. Cieľom je ukázať používateľom príklady týchto správ, poukázať na možnosti ich odhalenia a dať im možnosť pokúsiť sa odhaliť ich v teste. Pri tvorbe spear phishingových mailov sme vychádzali z návodu

Gardnera B. (2014), podľa ktorého predmet správy musí zaujať pozornosť a správa musí vyvolať pocit urgentnosti. Kvôli dôveryhodnosti má správa obsahovať logá, pri správe od osoby aj podpisový blok. Pre správy, ktoré sa javia ako automaticky generované, aj blok o súkromí [24].

V lekcii budú mať účastníci niekoľko emailových správ, obsahujúcich bežné znaky phishing/spam/hoax správ aj s ich popisom. V teste potom budú musieť rozhodnúť, ktoré z nich neboli pravé aj s uvedením dôvodu. Ak budú považovať emailovú správu za pravú, budú musieť vyhodnotiť, či je v poriadku aj prípadná príloha alebo odkaz. Na konci dostanú hodnotenie súčtom kladných a záporných bodov za správne a nesprávne hodnotenie, kde sa budú započítavať záporne aj falošne pozitívne odhady. Emailové správy sú ponúknuté vo fiktívnych situáciách so scenárom. Spear phishing simulujeme tým, že v emailových správach používame osobné údaje účastníkov získané z Moodlu. Šablóny mailov máme z viacerých zdrojov, väčšinou boli ponúkané so simulátormi phishingu, ktoré sme analyzovali [62, 63, 64].

Obťažnosť emailových správ určuje štylistika, gramatika, typ oslovenia, grafická stránka, pri ktorej bude rozhodovať prítomnosť loga a podpisového bloku alebo bloku o súkromí. Ďalším určujúcim faktorom budú techniky, ktoré využívajú útočníci pri pokuse dostať obeť na svoju stránku, či obídenie spamových filtrov, ktoré sme spomínali v kapitole Informačná bezpečnosť v časti o phishingu. Medzi nich patrí pridávanie neviditeľných znakov a znakov podobných latinským písmenám a číslam. Tieto je možné odhaliť nástrojmi, ktoré prekladajú znaky na ich poradie v rozsahu kódovania Unicode alebo na kód, ktorý sa používa pre reprezentáciu Unicode znakov do obmedzenejšieho kódovania ASCII [74].

3.1.2 Správa a používanie hesiel

Obsahom tohto modulu sú rôzne spôsoby prelomenia hesiel, ktoré sme spomínali v kapitole Informačná bezpečnosť v časti o heslách. Vysvetlíme pojem entropie, používanie slovníkov, l33t slová a klávesnicové vzory. Na základe týchto metód ukážeme používateľom, ako sa vyhnúť rôznym typom slabých hesiel a ako si vytvoriť heslo, ktoré odoláva viacerým prístupom prelomenia. Ďalším cieľom je, aby si používatelia osvojili zásady používania hesiel. V rámci modulu spomíname riziká ukladania hesiel v počítači, či riziko používania malého počtu hesiel. Súčasne zdôrazňujeme potrebu meniť si heslo po určitej dobe, vyplývajúcu z možnosti krádeže databázy hesiel, ktoré je potom možné offline prelomiť.

Používateľom ponúkame aj možnosť vyskúšať si silu rôznych hesiel aj s varovaniami pri hesle s nedostatkami. Žiadne heslá nebudeme ukladať v žiadnej forme. Ďalšou aktivitou je kvíz, kde sú ponúknuté rôzne heslá a používatelia by mali určiť, proti akému typu útoku sú zraniteľné. Je diskutabilné, či tento modul potrebuje modifikáciu obsahu, založenú na obťažnosti. Keďže po získaní informácií o heslách, ktoré sme spomínali, by nemalo byť náročné vytvoriť heslo spĺňajúce požiadavky. Z tohto dôvodu sme sa rozhodli, že v tomto module nebudeme deliť úlohy podľa obťažnosti.

3.1.3 Komunikácia a profily v rámci sociálnych sietí

Cieľom tohto modulu je poukázanie na nebezpečenstvo zverejňovania svojich osobných údajov na sociálnych sieťach, z ktorého vyplýva možnosť krádeže identity. Súčasne je cieľom poukázať na nebezpečenstvo komunikácie s neznámymi jedincami a na spôsoby, ktorými môžu využiť získané informácie. Po vysvetlení spomenutých rizík a ich možných následkov budú mať používatelia test, kde budú na interaktívnych obrázkoch určovať, ktoré nastavenia v zobrazenom profile na Facebooku odkrývajú osobné údaje. Nasledovať bude test, v ktorom sa budú z hľadiska bezpečnosti vyhodnocovať pripravené príspevky na nástenke Facebooku.

3.1.4 Wi-Fi

Tento modul sa zaoberá najmä verejnými Wi-Fi sieťami a ich rizikami. Preberajú sa tiež kryptografické protokoly na zabezpečenie šifrovania bezdrôtových sietí. Súčasne spomíname, že ak pri pripojení na Wi-Fi sieť nie je požadované heslo, tak je nešifrovaná a dáta používateľa idú po sieti v textovej podobe. Ďalej sa modul zaoberá Wi-Fi sieťami a prístupovými bodmi, nastraženými útočníkom a spôsobmi, ako ich rozpoznať. Ukazujú sa rôzne spôsoby obrany, napríklad VPN, SSL šifrovanie. Súčasne sa vysvetľuje dôležitosť HTTPs protokolu. Ukazujeme, ako vypnúť zdieľanie súborov v sieti a nastavenia pre verejné siete v operačnom systéme.

Po kurze nasleduje test, ktorý bude slúžiť na zistenie toho, či používatelia porozumeli, akými spôsobmi môžu byť ohrození, a aký to môže mať dopad. V ďalšej časti testu zisťujeme, či rozumejú, ako ich rôzne riešenia chránia, a aký je rozsah ich zabezpečenia. Na konci budú mať k dispozícii test, kde budú mať popísanú situáciu a ponúknutý zoznam dostupných sietí. Následne budú musieť určiť, ktoré Wi-Fi siete sú dôveryhodné.

Tu je tiež diskutabilné, či je potrebná modifikácia obsahu na základe obťažnosti. Keďže v poslednom teste ide pri rozhodovaní len o názov siete v rámci kontextu a to, či je zaheslovaná, tak po pozornom sledovaní kurzu by mal byť test pre účastníkov triviálny. Cieľom ostatných testov je zistenie toho, či si po skončení kurzu účastníci pamätajú preberanú látku, nevyžadujú však žiadne schopnosti. Z toho dôvodu nie je v module delenie podľa obťažnosti.

3.2 Implementácia systému

Okrem samotného Moodlu využívame aj viacero doplnkov na zabezpečenie gamifikácie, interaktívneho učenia a delenia podľa obťažnosti. Pre zabezpečenie rozdelenia účastníkov podľa levelu znalostí sme použili **Adaptive Quiz modul** vytvorený Middlesgburgskou univerzitou [59]. Tento doplnok využíva algoritmus, postavený na **psychometrickom Raschovom modeli** [59]. Jeho algoritmus vypočíta úroveň znalostí účastníka pomocou otázok so zadanou obťažnosťou, pričom počas kvízu vypočítava, ktorú ďalšiu otázku položí tak, aby úroveň určil čo najpresnejšie. Počíta aj odchýlku [58]. Obťažnosť otázky určia špeciálne pomenované tagy z Moodlu. Pôvodne sme chceli výsledky Adaptive Quizu použiť ako dátové pole v profile (user profile field) a podľa neho obmedzovať prístup ku kvízom. Potom sme sa rozhodli obmedzovať ho podľa známky z Adaptive Quizu, ktorá je rovná jeho výsledku, prípadne ju môžeme váhami upraviť, ak to situácia vyžaduje. Tento kvíz má vcelku podrobné štatistiky výsledkov (Obr. 1).

Obr. 1 Adaptive Quiz štatistika

Doplnok sme trochu upravili tým, že už pri inštalácii sa uložia tagy pre tri levely a pridali sme možnosť nastavení, kde je možné zadať, koľko levelov chceme mať a tým sa pridá požadované množstvo tagov. Pri ukladaní do databázy sme využili **Moodle Data Manipulation API,** vďaka ktorému je možné použiť jednu syntax pre všetky databázové systémy. Na nasledujúcom príklade vidíme, ako vyzerá syntaxt tejto API:

```
$tag = new stdClass();
$id = $DB->insert_record('tag', $tag);
```

Pri nastavení sme potrebovali zisťovať, koľko už tagov v databáze je. Táto požiadavka sa nám vykonávala neustále, preto sme ju presunuli zo stránky nastavení kvízu. Kvôli tomu, že nastavenia v Moodle doplnkoch sú tvorené pomocou jednej generickej stránky, ktorej obsah sa dynamicky tvorí podľa modulu a aktuálny modul nepoznáme, museli sme zmeniť aj kód jadra Moodlu.. Konkrétne sme v súbore adminlib doplnili metódu config_write ktorá sa spustí, len keď niekto mení nastavenia doplnkov:

```
if ($this->plugin == 'adaptivequiz') {
    $newlevel = get_config('adaptivequiz', 'levels');
    $queryresult = $DB->get_field_sql('SELECT name FROM {tag} WHERE name LIKE
    \'adpq%\' ORDER BY id DESC LIMIT 1');
    $result= filter_var($queryresult, FILTER_SANITIZE_NUMBER_INT);
```

Po získaní počtu existujúcich tagov sme už len vytvorili nové. Mazanie sme neriešili, keďže tagy sa mažú po tom, čo sa zmaže posledný prvok ktorý ich obsahuje. Navyše mazať tagy, ktoré niekto využíva nemá zmysel.

Keďže používame delenie na tri úrovne (easy, normal, hard), tak sme upravili kód jadra Moodlu. Ten podľa názvu kvízu filtruje otázky z banku podľa úrovne ich tagu takým spôsobom, že pred ich pridaním kontroluje, či nepatria k niektorej náročnosti. Ak áno, tak ich filtruje pomocou nasledujúceho kódu:

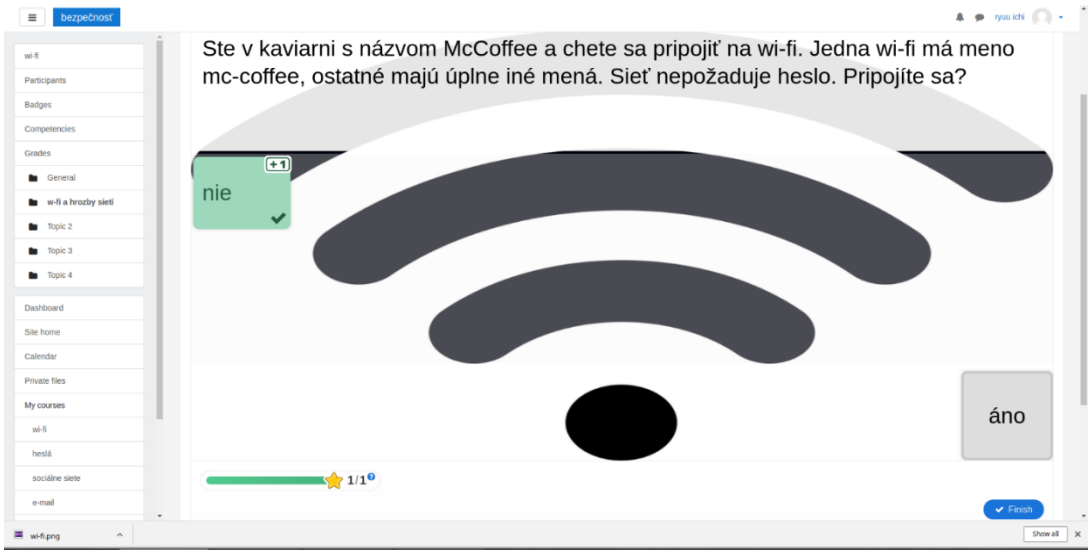
```
$quizzz = $DB->get_record('quiz', array('id' => $quiz->id), 'name');
$tagy = core_tag_tag::get_item_tags_array('core_question', 'question',
$questionid);
$difficulties = array ("easy", "medium","hard");
```

```
        if (((strpos($quizzz->name, 'easy') !== false) && (in_array("adpq_1",
$tagy)))
        ||      ((strpos($quizzz->name,      'medium')      !==      false)      &&
(in_array("adpq_2", $tagy)))
```

...

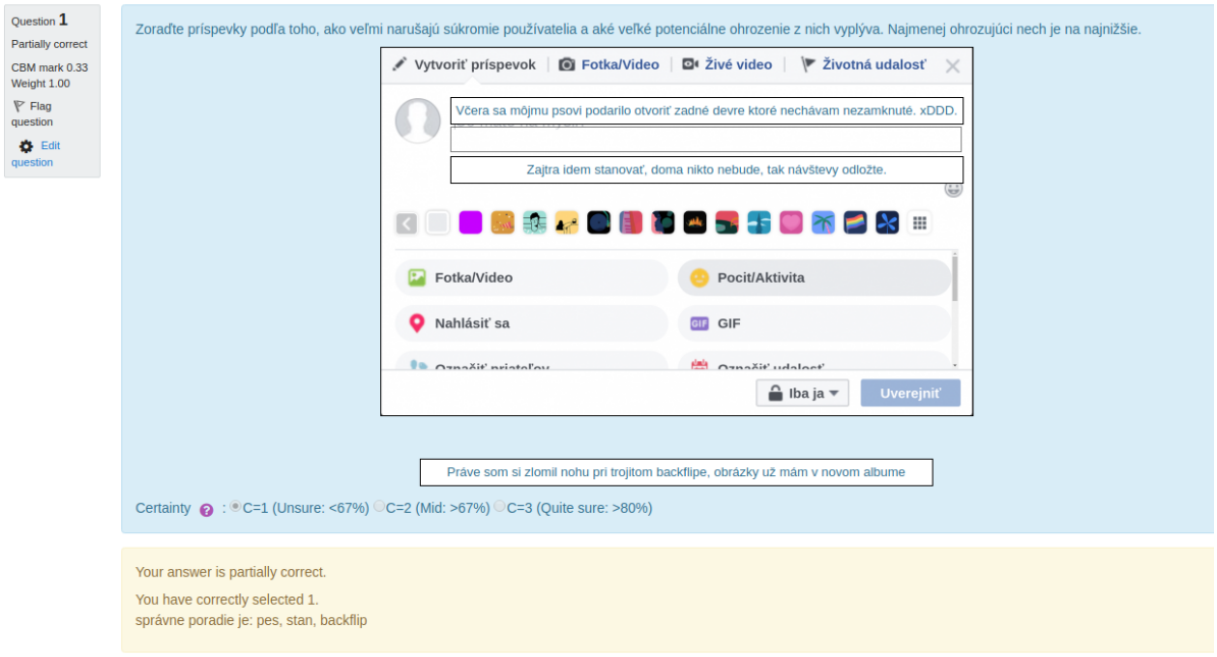
V rámci systému sme neimplementovali plné filtrovanie, keďže bude implementované v Moodli v polovici mája 2018 a nie je žiaden dôvod mať dve metódy filtrovania otázok v kvíze.

H5P plugin [60] nám dodáva interaktívny obsah. Framework H5P poskytuje okrem iného interaktívne video, ktoré môže obsahovať otázky typu: výber z možností, doplnenie slova, drag and drop (Obr. 2), interaktívne obrázky, obsahujúce tie isté typy otázok, pričom obrázky môžu byť združené do prezentácie, tvoriacej kvíz. Otázka môže zahrňovať aj zoradenie obrázkov a označenie bodov – hotspot otázky. Možno vytvoriť aj všeobecný kvíz, ktorý kombinuje viacero typov interaktívnych otázok a ich počet, sa novými verziami rozrastá.



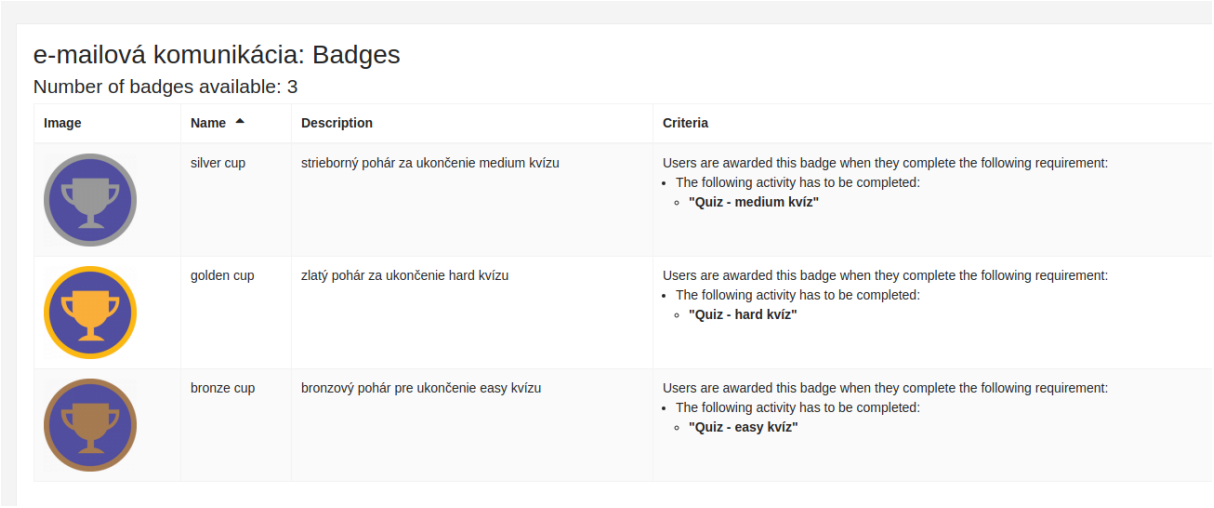
Obr. 2 H5P drag and drop

Pre kvízy s interaktívnym videom nevyužívame plugin Kaltury pre Moodle [61], pre jeho funkčnosť je potrebný Kaltura Application Framework ktorý je spoplatnený. Okrem H5P doplnku na tvorbu interaktívneho obsahu využívame aj samotný Moodle ktorý podporuje viacero typov interaktívnych obrázkov, napríklad na Obr. 3 možno vidieť jeden z dvoch typov drag and drop otázky.



Obr. 3 Moodle drag and drop

Na gamifikáciu používame odznaky, ktorých podpora je zabudovaná v Moodle. Ukážka týchto odznakov je zobrazená na Obr. č. 4.



Obr. 4 Moodle badges

Odznaky máme zo stránky moodlebadges.com, ktorá ponúka sto odznakov rôznych typov. Pre manuálne pridelenie veľkého množstva odznakov používame **Badge Awarder plugin**, ktorý umožní spracovaním štruktúrovaného CSV súboru prideliť odznaky [65]. Moodle má aj **Stamp Collection doplnok** [78] pre rozdávanie známok (niečo ako digitálne poštové známky).

Známky si na rozdiel odznakov môžu vymieňať aj študenti medzi sebou. My sme sa rozhodli pre odznaky, pretože sú v jadre Moodlu. Z tohto dôvodu je ich podpora je zaručená aj v budúcich verziách. Ďalej používame **Stash doplnok** [70], ktorý umožní pridávať zberateľské predmety priamo do textu kurzu, čím je podporené čítanie lekcií. Doplnok **Stash availibility** [71] umožňuje využiť vlastnenie predmetu ako požiadavku pre otvorenie obsahu, čo možno využiť napríklad pri kvíze, ktorý nadväzuje na lekciu.

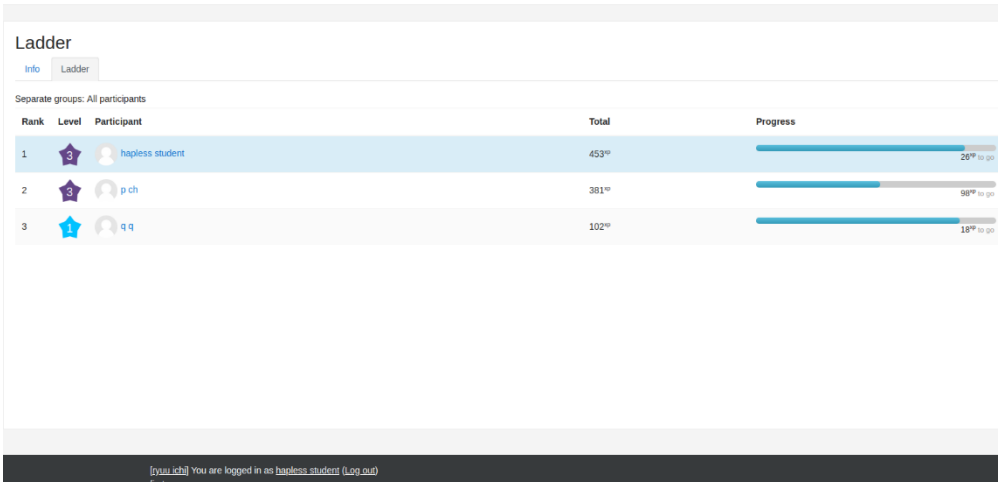
Používame dve systémy bodovania na podporu gamifikácie. Podľa spätnej väzby sa v budúcnosti môžeme obmedziť len na jeden z nich. Prvý je **Ranking block** [66], ktorý umožňuje získavať body za plnenie rôznych aktivít, vrátane známkovaných, kde body pripočíta ku známke a kumulatívne body účastníkov zobrazuje v rebríčku. Jeho výhodou oproti klasickým známkam je to, že body možno získať aj za neznámkované aktivity, ako je napríklad čítanie lekcie. Všetky body sa sčítajú do jedného výsledku, čo motivuje študenta venovať sa všetkým aktivitám. Jeho nevýhodou z hľadiska gamifikácie je absencia levelov. V rebríčku má len kumulované body (Obr. 5).


Ranking details: First 3 students

Pos	Fullname	Points
1	hapless	4.0
2	p	-
2	q	-

Obr. 5 Ranking block

Druhým systémov bodovania je **Level Up! block** [67], ktorý tiež umožňuje pridávanie. Tento systémov má rebríček v ktorom je možné vidieť získaný level, aj body chýbajúce do nasledujúceho levelu (Obr. 6). Rozdiel medzi ním a prvým riešením je v tom, že sú v ňom aj úrovne. Teda po určitom počte bodov získa študent ďalší level. Dodatočné doplnky umožňujú použiť level ako požiadavku na otvorenie obsahu, napríklad kvízy [68] alebo dokonca celé kurzy [69]. Tento doplnok vychádza v dvoch verziách, v základnej, ktorá je zadarmo a platenej, ktorá ponúka väčšiu funkcionalitu.

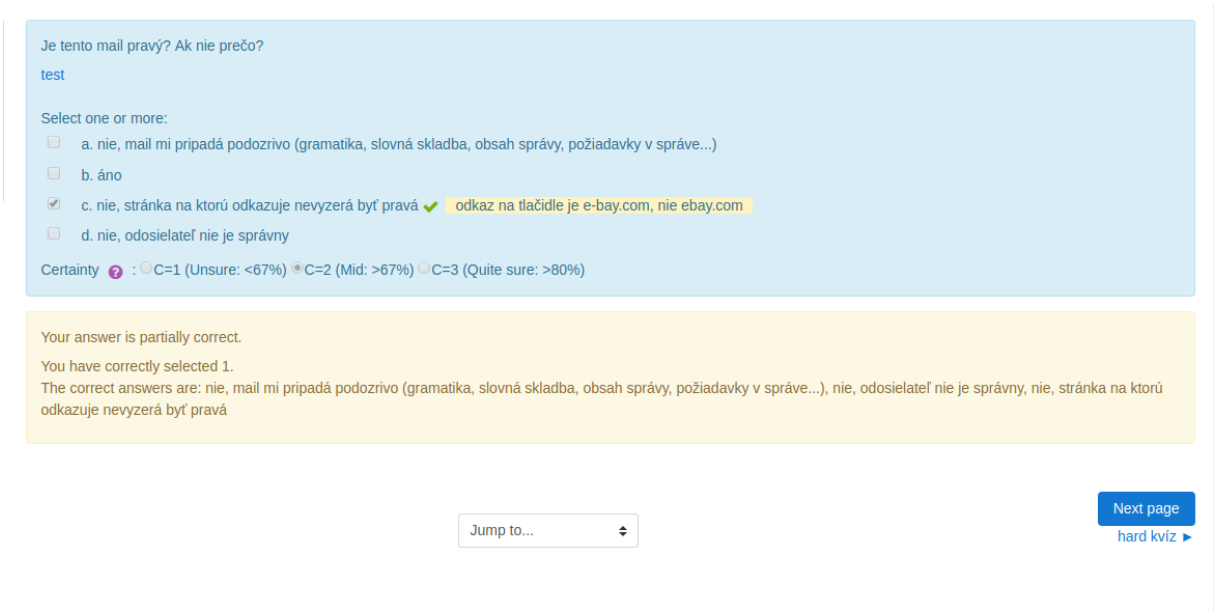


Obr. 6 Level up!

Používame aj CBM, o ktorom sme písali v kapitole LMS. V Moodli je jeho podpora zabudovaná, ale pre podrobné výsledky kvízov, ktoré používajú CBM, je potrebný doplnok **CBM Grade Summary** [72]. Pri CBM v Moodli majú rôzne stupne určitosti danú pravdepodobnosť určitosti, ktorú vyjadrujú v rozsahu 0-100%. Stupne majú takéto pravdepodobnosti:

- pri stupni 1 si je študent istý na menej ako 67 percent,
- pri stupni 2 si je študent istý na 67 až 80 percent a
- pri treťom si je študent istý na viac ako 80 percent.

Skóre sa pri stupňoch dáva takto: jeden, dva, resp. tri body pre náležité stupne a nula, mínus dva a mínus šesť pre nesprávne odpovede pri náležitých stupňoch. Bez označenia odpovede je skóre nula. Nesprávna odpoveď pri maximálnom stupni určitosti má dvojnásobnú penaltu, pretože má slúžiť na vyburcovanie študenta k tomu, aby sa zamyslel nad dôvodom svojej chyby a venoval väčšiu pozornosť vysvetleniu daného problému. Takáto odpoveď si tiež zaslúži väčšiu penaltu ako nesprávna odpoveď, ktorá je sčasti hádaním [44]. Na Obr. 7 možno vidieť vyhodnotenú otázku s použitím CBM.



Obr. 7 CBM

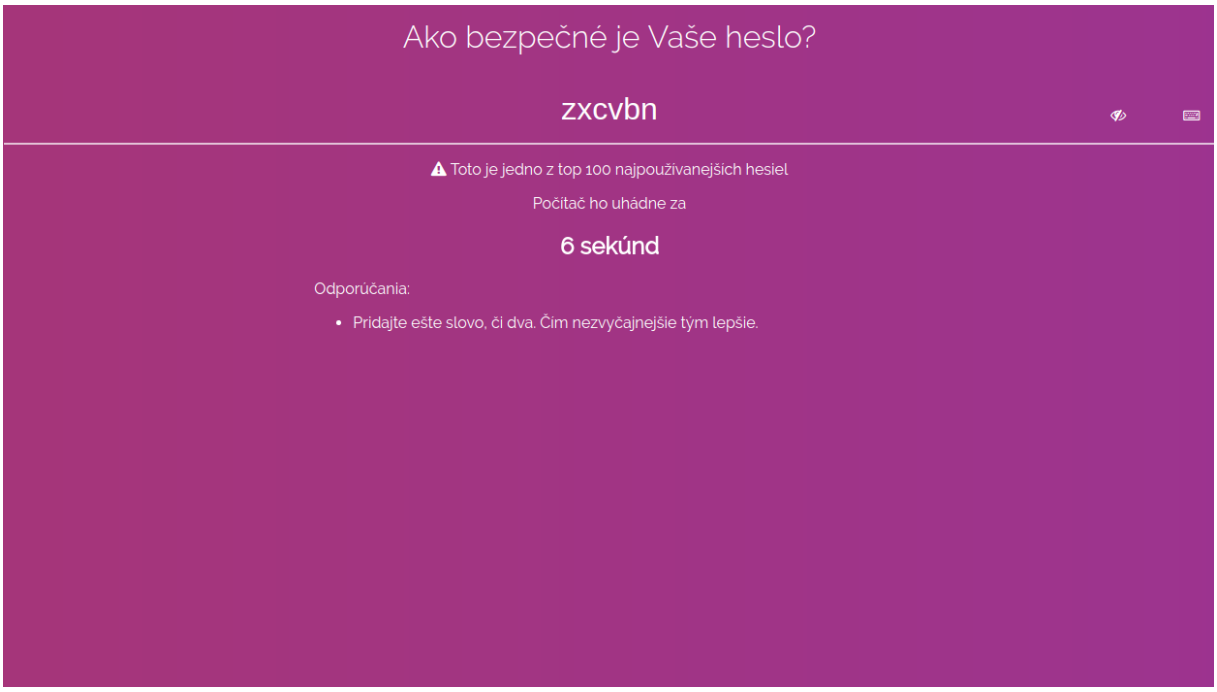
My používame zmeny v kóde jadra Moodlu, ktorých autorom je profesor Tony Gardner-Medwin [73]. Tento autor vytvoril aj CBM doplnok. Vďaka týmto zmenám Moodle vypočíta známku z priemeru týchto pravdepodobností, keďže pri počítaní známky z CBM skóre sa dalo dosiahnuť až 300% známky. Teda už pri tretinovom hodnotení by bola dosiahnutá maximálna známka. To sa dalo obísť nastavením neobmedzenej známky. Lenže potom známka presahovala maximum za daný kvíz, čo by narušilo celkové známky kurzu, keďže za kvíz by sa dalo získať viac bodov, ako učiteľ určil.

Pri emailových správach simulujeme osobné údaje jednoducho. Stačí nám využiť premennú Moodlu user ktorá pre každého používateľa vráti jeho údaje:

```
require('/var/www/moodle/config.php');
global $USER;
$firstname = $USER->firstname;
```

Posledným komponentom systému ja nami vytvorená JavaScript aplikácia, postavená na knižnici zxcvbn. Táto aplikácia ponúka možnosť využitia dotykovej obrazovky na písanie, keďže v aplikácii je zahrnutá aj klávesnica. Knižnicu zxcvbn potom, čo sa vytvorí, je ľahké používať. Na stránke ju stačí zavolať ako script, potom jej posielať vstupy a spracovať

a vypisovať jej výstupy. Výstupy obsahujú odhadnutý čas na prelomenie, a v špecifických prípadoch aj varovanie, či odporúčanie ako je možné vidieť na Obr. 8.



Obr. 8 zxcvbn aplikácia

Záver

V práci sme riešili to, ako vytvoriť čo najviac efektívny systém na zvyšovanie povedomia v oblasti informačnej bezpečnosti. Cieľom tohto systému je, aby zvyšoval povedomie o bezpečnostných hrozbách a zároveň motivoval k bezpečnému správaniu. Dosiahnutie tohto cieľa je komplexný interdisciplinárny problém, pri ktorom je potrebné zamerať sa nielen na to, v čom je potrebné zvyšovať povedomie, ale aj ako to robiť. Vzhľadom na to, ako rýchlo sa útoky sociálnym inžinierstvom vyvíjajú, a na rozdiely medzi ľuďmi, neexistuje univerzálne, či najlepšie riešenie tohto problému. Napriek tomu sú pokroky v tejto oblasti veľmi potrebné, keďže ľudia sú dlhodobo najslabšou súčasťou informačných systémov

Prvým cieľom našej práce bola analýza štandardov, noriem a štúdií v oblasti informatickej bezpečnosti z pohľadu zvyšovania povedomia v oblasti informačnej bezpečnosti vybraných cieľových skupín. Našou cieľovou skupinou boli ľudia, ktorí majú minimálne predošlé vzdelanie v informačnej bezpečnosti, a teda sú najviac zraniteľní útokom sociálnym inžinierstvom. V práci sme analyzovali normy a štandardy popisujúce požiadavky pre obsah a spôsob zavedenia kampane na zvyšovanie povedomia a odbornú literatúru zaoberajúcu sa tvorbou takýchto kampaní. Na základe ich požiadaviek sme určili témy kampane a ich rozsah.

Naším druhým cieľom bolo porovnať existujúce prístupy a nástroje pre zvyšovanie povedomia v oblasti informačnej bezpečnosti. Keďže kampane často nedosahujú žiadané výsledky, zamerali sme sa na prístupy, ktorými možno zvýšiť ich efektivitu. Preskúmanie problematiky z psychologického hľadiska ukázalo, že medzi účinne spôsoby podávania informácie patrí gamifikácia a interaktívne učenie. Neúčinným sa ukázalo používanie kognitívnych učebných štýlov. Obsah je však dobré prispôsobiť účastníkovým znalostiam, schopnostiam a motivácii.

Keďže cieľom kampane je adopcia bezpečného správania, schopnosť kladne ovplyvniť motiváciu a postoj účastníka k tejto oblasti je jedným z hlavných kritérií určujúcich jej úspech. Z toho dôvodu sme analyzovali viaceré metódy zvyšovania motivácie a ich využitie pri zvyšovaní povedomia v oblasti informačnej bezpečnosti.

Pri kampaniach na zvyšovanie povedomia sa často využívajú phishingové testy a iné spôsoby útokov využívajúce sociálne inžinierstvo. Z toho dôvodu sme pri porovnaní nástrojov analyzovali softvér slúžiaci na vedenie phishingových kampaní a nástroje slúžiace na penetračné testovanie v oblasti sociálneho inžinierstva. Okrem nich sme porovnali aj knižnice odhadujúce silu hesiel, a LMS ktoré, aj keď sa priamo netýkajú informačnej bezpečnosti či

zvyšovaniu povedomia, poskytujú infraštruktúru dôležitú pre kampaň na zvyšovanie povedomia.

Posledným cieľom bolo navrhnúť, implementovať a vyhodnotiť systém pre zvyšovanie povedomia v oblasti informačnej bezpečnosti pre vybranú cieľovú skupinu. Pri návrhu systému sme zahrnuli tri komponenty: aplikáciu na simuláciu phishingu, knižnicu na určovanie sily hesiel a systém na manažovanie učenia. V systéme sme nepoužili aplikáciu na simuláciu phishingu, keďže nedosahovali nami určené požiadavky. Z knižníc na určovanie sily hesiel sme vybrali zxcvbn, ktorú sme použili v JavaScript aplikácii na určenie sily hesla. Zo systémov na manažovanie učenia sme vybrali Moodle, ktorý najlepšie vyhovoval naším požiadavkám, aj keď sme pre ich splnenie museli použiť viacero doplnkov a modifikovať aj jadro Moodlu.

Obsah pozostáva z kurzu a jednotlivých lekcií zakončených kvízmi. Testy v niektorých kurzoch využívajú delenie podľa náročnosti, ktorá sa dynamický mení podľa výsledkov počas priebehu kurzu. Pri návrhu obsahu dávame dôraz na interaktívne učenie a gamifikáciu.

V budúcnosti by bolo dobré urobiť porovnanie výsledkov používateľov tohto systému a študentov bežného pasívneho kurzu z informačnej bezpečnosti. V takomto porovnaní by bolo dobré, ak by rôzne kurzy systému používali len určité prístupy zvyšujúce efektívnosť zvyšovania povedomia aby bolo možné určiť efektívnosť jednotlivých prístupov. Zastúpenie efektívnych postupov by sa potom posilnilo, menej efektívne by boli potlačené.

Pre budúci vývoj by bolo potrebné robiť pravidelné dotazníky o jednotlivých aspektoch systému a tieto spolu s výsledkami kurzov analyzovať za použitia vhodnej metriky. Optimálne by bolo, ak by boli zber a analýza dát do čo najväčšej miery automatizované.

Čo sa týka doplnkov, tak adaptive quiz má ešte veľa nedostatkov oproti bežnému Moodle kvízu, ktoré by bolo dobré odstrániť. Napríklad podporuje len dve druhy feedbacku, z ktorých ani jeden nie je CBM. Nepodporuje všetky spôsoby správania sa otázok. Nie je možné nastaviť hodnotenie, po ktorom bude kvíz považovaný za ukončený. Síce je možné nastaviť hodnotenie za úspešné zvládnutie kvízu, lenže aj tí čo ho zvládli neúspešne, ho prejdú. Pri bežnom kvíze je možné pokladať kvíz pri neúspešnom hodnotení za neukončený, čo môže motivovať neúspešných riešiteľov zopakovať si kvíz, pokiaľ je opakovanie povolené. Aj keď adaptive quiz ponúka prehľadnejšiu štatistiku, nie je možné ju exportovať, čo by bolo v prípadnej automatickej analýze potrebné. Navyše univerzita, ktorá vyvíjala doplnok, ukončila túto činnosť.

Zoznam použitej literatúry

1. EY: Path to cyber resilience: Sense, resist, react. EY's 19th Global Information Security Survey 2016-17. Survey, EY (2017)
2. CyberEdge: 2015 Cyberthreat Defense Report North America & Europe. Report, CyberEdge Group (2015)
3. Verizon: 2016 Data Breach Investigations Report. Report, Verizon (2016), s. 17
4. National Cyber Security Alliance, McAfee, JZ Analytics: 2012 NCSA / McAfee Online Safety Survey. Survey, NCSA (2012)
5. the University of Adelaide: Security Awareness games, https://www.adelaide.edu.au/technology/secureit/games/
6. Digizen: digizen game, http://www.digizen.org/resources/digizen-game.aspx
7. Federal Trade Commision: The Case of the Cyber Criminal, https://www.consumer.ftc.gov/media/game-0013-case-cyber-criminal
8. Stay Safe Online: Resources, https://staysafeonline.org/resources/
9. STOP. THINK. CONNECT: Resources, https://stopthinkconnect.org/resources
10. PhisingBox, https://www.phishingbox.com
11. KnowBe4, https://www.knowbe4.com/
12. Wombat Security, https://www.wombatsecurity.com
13. The Hermit: Spear Phisher, https://github.com/kevthehermit/SpearPhisher
14. Phishing Frenzy, https://www.phishingfrenzy.com/
15. Secure State: King Phisher, https://github.com/securestate/king-phisher
16. TrustedSec: Social Engineer Toolkithttps://github.com/trustedsec/social-engineer-toolkit
17. Browser Exploitation Framework, http://beefproject.com/
18. Dropbox: zxcvbn, https://github.com/dropbox/zxcvbn
19. Go Simple: nbvcxz, https://github.com/GoSimpleLLC/nbvcxz
20. Bonwell, Charles C., and James A. Eison. 1991. Active Learning; Creating Excitement in the Classroom. ASHE-ERIC Higher Education Report No. 1. Washington, D.C.: The George Washington University, School of Education and Human Development
21. Interactive Teaching Styles Used in the Classroom, https://education.cu-portland.edu/blog/classroom-resources/5-interactive-teaching-styles-2/
22. Prince, M., 2004. Does active learning work? A review of the research. *Journal of engineering education*, *93*(3), pp.223-231.

23. NIST, S., 1998. 800-16 (1998). National Institute of Standards and Technology (NIST) information technology training requirements: A role-and performance-based model (NIST Special Publication 800-16). Washington, DC: US Department of Commerce.

24. Gardner, B. , Thomas, V. Building an Information Security Awareness Program. Defending Against Social Engineering and Technical Threats . Waltham (USA): Syngress, 2014. ISBN 978-0-12-419967-5.

25. ISACA. Cybersecurity Fundamentals Study Guide. Rolling Meadows (USA): ISACA, 2015. ISBN 978-1-60420-594-7.

26. Siponen, M.T., 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), pp.31-41.

27. Herold, R. Managing an Information Security and Privacy Awareness and Training Program. Second Edition. New York: CRC Press, 2011. ISBN 978-1-4398-1050-7.

28. Bada, M. and Sasse, A., 2014. Cyber Security Awareness Campaigns Why do they fail to change behaviour?.

29. Thornton, D. and Francia, G.I., 2014. Gamification of information systems and security training: issues and case studies. *Inf. Secur. Educ. J*, *1*(1), pp.16-24.

30. Labuschagne, W.A. and Eloff, M., 2014, July. The effectiveness of online gaming as part of a security awareness program. In *13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece* (p. 125).

31. US Government, Legal Information Institute, Title 44, Chapter 35, Subchapter 111, §3542, Cornell University Law School, www.law.cornell.edu/uscode/44/3542.html.

32. Andress, J. The Basics of Information Security. Understanding the Fundamentals of InfoSec in Theory and Practice. Second Edition. Waltham (USA): Syngress, 2014. ISBN 978-0-12-800744-0.

33. Galbally, J., Coisel, I. and Sanchez, I., 2017. A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms. *IEEE Transactions on Information Forensics and Security*, *12*(12), pp.2829-2844.

34. Mitnick, K.D. and Simon, W.L., 2011. The art of deception: Controlling the human element of security. John Wiley & Sons.

35. Wilson, M. and Hash, J., 2003. Building an information technology security awareness and training program. *NIST Special publication*, *800*(50), pp.1-39.

36. Pashler, H., McDaniel, M., Rohrer, D. and Bjork, R., 2008. Learning styles: Concepts and evidence. Psychological science in the public interest, 9(3), pp.105-119.

37. Mayer, R.E., 2011. Does styles research have useful implications for educational practice?. Learning and Individual Differences, 21(3), pp.319-320.

38. Felder, R.M. and Silverman, L.K., 1988. Learning and teaching styles in engineering education. Engineering education, 78(7), pp.674-681.

39. Massa, L.J. and Mayer, R.E., 2006. Testing the ATI hypothesis: Should multimedia instruction accommodate verbalizer-visualizer cognitive style?. Learning and Individual Differences, 16(4), pp.321-335.

40. Gophish, https://getgophish.com/

41. Chamilo, https://chamilo.org/

42. OPEN edX, https://open.edx.org/

43. Opigno, https://www.opigno.org/en

44. Gardner-Medwin, A.R., 2006. Confidence-Based Marking-towards deeper learning and better exams In: Innovative Assessment in Higher Education. Ed.: Bryan C and Clegg K.

45. Sakai, https://www.sakaiproject.org/

46. ATutor, http://www.atutor.ca/

47.ILIAS, https://www.ilias.de

48. Canvas, https://www.canvaslms.com/

49. Moodle, http://moodle.net/stats/

50. Liyanage, M.P.P., Gunawardena, K.L. and Hirakawa, M., 2014. Using Learning Styles to Enhance Learning Management Systems. ICTer, 7(2).

51. Česká technická norma 2014. ČSN ISO/IEC 27001 (36 9790).

52. CyberEdge: 2017 Cyberthreat Defense Report. Report, CyberEdge Group (2015)

53. Česká technická norma 2014. ČSN ISO/IEC 27002 (36 9790).

54. Crowe, E. and Higgins, E.T., 1997. Regulatory focus and strategic inclinations: Promotion and prevention in decision-making. Organizational behavior and human decision processes, 69(2), pp.117-132.

55. Česká technická norma 2011. ČSN ISO/IEC 27003 (36 9790).

56. Česká technická norma 2011. ČSN ISO/IEC 27004 (36 9790).

57. Vergelis, M., Shcherbakova, T., Demidova, N. and Gudkova, D., 2015. Kaspersky security bulletin. spam and phishing in 2015. Kaspersky.

58. Linacre, J.M., 2000. Computer-adaptive testing: A methodology whose time has come. Chae, S.-Kang, U.–Jeon, E.–Linacre, JM (eds.): Development of Computerised Middle School Achievement Tests, MESA Research Memorandum, 69.

59. Moodle plugin Adaptive Quiz, https://moodle.org/plugins/mod_adaptivequiz

60. Moodle plugin H5P, https://moodle.org/plugins/mod_hvp

61. Modle plugin Kaltura Video Package, https://moodle.org/plugins/view.php?id=447

62. King Phisher mail templates, https://github.com/securestate/king-phisher-templates

63. Gophish mail tmplates, https://github.com/rfdevere/templates

64. Phishing Frenzy mail templates, https://github.com/pentestgeek/phishing-frenzy-templates

65. Moodle plugin Badge Awarder, https://github.com/pentestgeek/phishing-frenzy-templates

66. Moodle plugin Ranking block, https://moodle.org/plugins/block_ranking

67. Moodle plugin Level up!, https://moodle.org/plugins/block_xp

68. Moodle plugin Level up! Availibility, https://moodle.org/plugins/availability_xp

69. Moodle plugin Level up! Enrol, https://github.com/branchup/moodle-enrol_xp

70. Moodle plugin Stash, https://moodle.org/plugins/block_stash

71. Moodle plugin Stash Availibility, https://moodle.org/plugins/availability_stash

72. Moodle plugin CBM Grade Summary, https://moodle.org/plugins/quiz_cbmgrades

73. Modifikácia jadra Moodlu pre CBM, http://tmedwin.net/cbm/moodle/download/

74. McElroy, T., Hannay, P. and Baatard, G., 2017. The 2017 homograph browser attack mitigation survey.

75. Phishing attack using IDN, https://www.csoonline.com/article/3191651/security/phishing-attacks-using-internationalized-domains-are-hard-to-block.html

76. CSIRT phishing test, https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html

77. PhET simulácie, https://phet.colorado.edu/

78. Moodle Stamp Collection plugin, https://docs.moodle.org/34/en/Stamp_collection_module

79. Wong, M. and Schlitt, W., 2006. Sender policy framework (SPF) for authorizing use of domains in e-mail, version 1 (No. RFC 4408).

80. Microsoft Windows Server dokumentácia, Virtual Private Networking: An Overview, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb742566(v=technet.10)

81. Microsoft Windows Server dokumentácia, SSL/TLS in Detail, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785811(v=ws.10)

82. Javvin Technologies, 2005. Network Protocols Handbook. Javvin Technologies Inc. (2005)

83. ENISA Threat Landscape Report 2017. Report, ENISA (2017)

84. MetaSploit Framework, https://www.metasploit.com/

85. jQuery Entropizer, https://github.com/jreesuk/jquery-entropizer

Prílohy

Príloha A: CD médium – diplomová práca v elektronickej podobe, prílohy v elektronickej podobe

Príloha B: CD médium – modifikovaná Moodle inštancia, zxcvbn aplikácia a dáta obsahujúce kurzy