# Systém na zvyšovanie povedomia v oblasti informačnej bezpečnosti

Peter Chomič

3Ib, 2017 - 2018

**Abstrakt.** Práca sa zaoberá problémom nízkeho povedomia v oblasti informačnej bezpečnosti, dôvodmi prečo je nízke a spôsobmi a metódami ako ho zvýšiť. Cieľom práce je vytvoriť systém na zvyšovanie tohto povedomia modifikáciou systému na manažovanie vzdelávania a tvorbou obsahu v tomto systéme.

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

## 1 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, a jeho dopad na obranu organizácií sa každým rokom zväčšoval [52]. Útočníci skutočnosť, že zamestnanci sú najľahšou cestou prelomenia bezpečnosti často využívajú, hlavne psychologickou manipuláciou zameranou na získanie informácií – 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 software, pričom treba brať do úvahy že väčšina prípadov phishingu ho využíva ako prostriedok k stiahnutiu a inštalovaniu malwaru [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 [5]. Takéto školenia v oblasti bezpečností informácií by sa mali konať pravidelne [6]. Tieto normy sú vytvorené medzinárodnou organizáciou pre

štandardizáciu (ISO) a medzinárodnou elektrotechnickou komisiou (IEC) a slúžia ako odporúčania v oblasti manažmentu informačnej bezpečnosti.

### 1.2 Bezpečnostné povedomie

Definície zvyšovania povedomia sa líšia, niektorí rozlišujú medzi zvyšovaním povedomia, tréningom a učením [7], iní zahrňujú tréning a učenie do zvyšovania povedomia [8]. Podľa špecifikácie NIST 800-16 povedomie nie je tréning a účelom prezentácie povedomia je jednoducho zamerať pozornosť na bezpečnosť [7]. Bezpečnostné povedomie môže byť definované ako stav, kde si je zamestnanec vedomý svojich bezpečnostných povinností [9], na čo si musí byť vedomý existencie bezpečnostných hrozieb a spôsobov obrany proti nim. Táto definícia nevylučuje žiadne formy jeho zvyšovania.

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, následkom čoho podľa okolností možno 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 riešenia problémov. Aby mohli byť účastníci považovaní za aktívne zapojených je potrebné zahrnúť aktivity vyžadujúce vyššie myslenie ako je analýza, syntéza a vyhodnocovanie [10]. Medzi techniky interaktívneho učenia patrí učenie založené na riešení problémov, kooperatívne a kolaboratívne učenie, debaty, hranie na roly, kvízové posedenia a iné [10, 11]. 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 [10]. Pri kolaboratívnom aj kooperačnom učení si študenti zapamätali z lekcií viac [12]. 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 [12].

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 [13]. 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 [13]. 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 [13]. 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 [13]. Gamifikáciu odporúča aj Herold R., konkrétne odporúča použiť hry a výzvy v kampani na zvyšovanie povedomia ako prostriedok ktorý ju urobí zaujímavejšou [14]. Pri

gamifikácii mali však študenti zo začiatku kurzu horšie výsledky, avšak na rozdiel od klasického kurzu sa ich výsledky časom zlepšovali a najlepšie hodnoty dosahovali keď sa hralo o záverečnú výhru [15]. V čase skúšky z kurzu ktorá sa odohrala potom už ale mali nízku úspešnosť, čiže ich motivácia bola založená hlavne na výhre.

Okrem lekcií sú aj možnosti ako 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 [8]. Komplexná kampaň na zvyšovanie povedomia môže zahŕňať aj plagáty, rozdávanie predmetov s bezpečnostnými sloganmi a ďalšie aktivity upevňujúce povedomie aj mimo samotných lekcií [8, 14].

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. Vplyv preferovaných štýlov na výkon študentov bol viac krát skúmaný ale nedosiahli sa uspokojivé výsledky podporujúce zvýšený vplyv [16], výsledky neboli konzistentné, či nebolo možné vyvodiť závery [17]. 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 [16].

### 1.3 Zvyšovanie motivácie

Dôležitou súčasťou kampane na zvyšovanie povedomia je okrem poukázania na spôsoby bezpečného správania aj dávanie motivácie k takému správaniu a snaha o zmenu postoja zúčastnených k bezpečnosti. Rozdiel medzi motiváciou postojom je ten, že motivácia je dynamickejšia, rýchlejšie sa mení a je krátkodobá v porovnaní s postojom ktorý je statickejší [9]. Motivácia sa delí na vnútornú a vonkajšiu. Pri vnútorne motivovanom správaní človeku o radosť z vykonávania aktivity. Človek podpiera 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. To, čo chce jedinec s vonkajšou motiváciou dosiahnuť nesúvisí s tým, čo pre to robí. 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 [18]. Aby sa to podarilo, ľudia musia uznať, že informácie sú pre nich relevantné, teda že sa týkajú rizík ktoré hrozia aj im, porozumieť a vedieť reagovať na rizikové situácie, a hlavne musia byť motivovaní a chcieť zmeniť správanie aj pri všetkých ostatných požiadavkách ktoré sú na nich kladené [18].

Zameranie sa na motiváciu a zmenu postoja je dôležité, pretože faktom je, že aj napriek tomu, že ľudia majú potrebné znalosti z oblasti bezpečnosti tak sa v reálnom živote takto nesprávajú [18]. 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 [6]. Existuje veľa teórií ktoré sa zaoberajú zvýšením motivácie a viacero štúdií skúmalo ich využitie v kampaniach na zvyšovanie povedomia. Príkladmi takýchto teórií sú: teória ochrany motivácie, hypotéza očakávanej užitočnosti, teória regulatívneho zamerania [18] a iné teórie ktoré si teraz rozoberieme.

Teória odôvodneného správania navrhuje vnútorný rozhodovací mechanizmus založený na predpoklade že zámer je bezprostredný determinant korešpondujúceho správania [9]. 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 [18]. Preto je dôležité vždy spomínať možné záporné následky ktoré môžu nastať pri zanedbaní bezpečného správania v danej situácii a to, že zmena správania redukuje alebo odstráni riziko keďže motiváciou mnohých je ich blaho. Blaho je používané ako jeden z prístupov na získanie motivácie [9].

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.

Priamo téme adopcie preventívne sa venuje aj teória seba účinnosti podľa ktorej táto adopcia závisí od troch faktorov ktoré je potrebné v kampani docieliť. Prvým je realizácia že osobe hrozí riziko, druhým je očakávanie že daná zmena správania redukuje riziko, a tretím je presvedčenie človeka že je dosť schopný na to, aby sa začal správať preventívne alebo nesprával sa rizikovo [18]. 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 [8] by mala byť prvou témou pri tréningu práve motivácia útočníkov. Medzi motivácie útočníkov patria: prestíž, aktivizmus, peniaze, tajomstvá získané pri industriálnej špionáži ako napríklad neuverejnené patenty a víťazstvo v kyber vojne [8]. 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 [18].

V psychológii teória regulačného zamerania navrhuje, že v promočne zameranom spôsobe samoregulácie sa správanie ľudí riadi potrebou dosiahnuť blaho, túžbou dosiahnuť svoje ideálne ja a dosiahnuť zisky [19]. 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 [18], pokiaľ je to za daných okolností lepšie.

### 1.4 Informačná bezpečnosť

Informačná bezpečnosť sa zaoberá informáciami bez ohľadu na ich formát – zahŕňa papierové dokumenty, digitálne a intelektuálne vlastníctvo a verbálnu alebo vizuálnu komunikáciu. Kyber bezpečnosť sa zaujíma o ochranu digitálnych aktív – všetkého od sietí k hardwaru a informáciám ktoré sú spracované, uložené alebo prenášané informačnými systémami [20]. Existuje veľa definícií informačnej bezpečnosti, napríklad podľa zákona spojených štátov ňou je ochrana informácií a informačných systémov proti neautorizovanému prístupu, použitiu, prezradeniu, narušeniu, modifikácii, alebo zničeniu [21]. Nás zaujíma hlavne ľudský element.

Pri zvyšovaní bezpečnostného povedomia existuje niekoľko štandardných oblastí ktoré by mali byť pokryté: ochrana dát, heslá, sociálne inžinierstvo, používanie sietí, malware, používanie osobných zariadení, zákon čistého stola, a bezpečnostné regulácie a politiky organizácie [22]. ISO/IEC 27001 požaduje aby každý pracovník organizácie poznal jej bezpečnostné politiky aj sankcie za ich porušenie [5]. Medzi témy môžu patriť okrem iného aj spam, softvérové licencie, ukladanie a zálohovanie dát, odpoveď na bezpečnostné incidenty – koho kontaktovať, čo robiť a čo nie [23]. Gardner B. a Thomas V. spomína 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 [8]. Zo sociálneho inžinierstva upozorňuje na phishing – identifikáciu a hlásenie phishingových správ. Pri identifikácii je potrebné zamerať sa na maskované odkazy a spoofované mailové adresy.

## 2 Súčasné riešenia

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 [24, 25, 26]. 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 [27] alebo iniciácie STOP. THINK. CONNECT., ktorá zastrešuje viacero organizácií [28]. 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 [29], ktorý predáva nástroj na tvorbu phishingových kampaní ktorý je možné integrovať do systémov na manažovanie vzdelávania ktoré slúžia na šírenie a testovanie vedomostí (LMS). Iným príkladom je spoločnosť KnowBe4 [30], 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 [31], 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 odsekoch porovnávame existujúce riešenia. Najprv porovnávame simulátory phishingu, potom nástroje na porovnávanie sily hesiel a nakoniec systémy na manažovanie vzdelávania.

Pri open source riešeniach existuje viacero phishing simulátorov slúžiacich na znázornenie útokov, napríklad Spear Phisher [32], Phishing Frenzy [33], King Phisher [34] ktoré sa kvalitou a ponukou vyrovnajú plateným. Výsledky porovnania sú zhrnuté v nasledujúcej tabuľke.

| 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

Porovnanie sme urobili za cieľom vybrať riešenie ktoré nám umožní posielať účastníkom kurzu v LMS mailové správy so spoofovaným odosielateľom na simulovanie phishingu. Pri našom pokuse sme ako SMTP server využili Postfix a skúsili sme poslať spoofovany mail na Gmail aj Outlook, ale obe nás blokovali a správu sme nemohli odoslať. Potom sme skúsili prenos cez moje Gmail konto ale vo výslednom maili sme nemali správne spoofovaného odosielateľa. Nakoniec sme sa rozhodli že nebudeme posielať maily účastníkom ale urobíme šablóny mailov ako to má vo svojom teste CSIRT [35]. Pri tomto riešení vieme ľahko získať aj osobné údaje používateľov na simuláciu spear-phishingu. Z týchto dôvodov sme nepoužili ani jedno z porovnávaných riešení.

Ďalšie porovnávanie je o knižniciach na testovanie sily hesiel ktoré by sme mohli využiť pre tvorbu aplikácie v ktorej by si používatelia mohli skúšať silu hesiel.. Naša požiadavka pri tvorbe aplikácie bola, aby nepočítala silu hesla podľa

daných pravidiel ako je napríklad požadovanie znaku či čísla, keďže takéto heslá sú účinné len proti brute-force útokom, a pokiaľ nie sú výnimočne dlhé tak ich účinnosť aj tak nie je veľká. Väčšina riešení ale používala presne tento typ určovanie sily hesla. 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 tvorí 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 rozidel od Zxcvbn nemal blacklist bežných hesiel ani slovník a 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 porovnanie sme sa preto rozhodli pre Zxcvbn.

Posledné porovnávanie sa týkalo LMS. 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. Naším ďalším kritérium je riešenie ktoré zabezpečuje interaktívne video, obrázky a kvízy s takýmto interaktívnym obsahom. Ďalšie kritériá sa zameriavajú na kvízy. Pri tvorbe kvízov je veľmi dôležité pri nesprávnej odpovedi vysvetliť prečo bola nesprávna aby účastník vedel kde urobil chybu [8]. Preto je ďalším kritériom možnosť dávať feedback založený 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.

V podpore štandardov vedie Moodle, druhý je Sakai ktorý nepodporuje len jeden štandard. Interaktívny obsah tak, ako sme požadovali poskytovali až štyri LMS, všetky využívajúc riešenia tretích strán, pričom Moodle umožňoval využiť obe hlavné riešenia – Kalturu a H5P. Gamifikáciu podporovalo mnoho LMS, často ale len odznakmi a certifikátmi. Ďaleko najširšiu podporu gamifikácie mal Moodle. Feedback pri otázkach kvízu podporoval takmer každý, niektorí podporovali aj feedback po kvíze ktorý záležal od skóre. CBM podporoval len Moodle. Keďže Moodle najlepšie vyhovoval našim kritériám, rozhodli sme sa pre neho. Moodle má tiež najviac pluginov z porovnávaných LMS a podporuje najviac DBMS – databázových systémov.

# 2 Systém na zvyšovanie povedomia v oblasti informačnej bezpečnosti

Obsah delíme na niekoľko tematických modulov predstavujúcich kurz pozostávajúci z lekcií zakončených kvízmi. V moduloch ktoré delia používateľov podľa levelu ich predošlých znalostí bude viacero verzií kvízov rozdelených 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. Zahrnuli sme tieto témy: tvorba a správa hesiel, e-mailová komunikácia, komunikácia a profily v rámci sociálnych sietí, wi-fi, malware. 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.

## 2.1 E-mailová komunikácia

Tento modul pokrýva oblasti sociálneho inžinierstva - phishing, spear-phishing – cielený phishing, a ďalej 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 [8].

V lekcii budú mať účastníci zopár 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 mail za pravý, 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. Maily sú ponúknuté vo fiktívnych situáciách so scenárom. Spear phishing simulujeme tým, že v mailoch používame osobné údaje účastníkov získané z Moodlu. Šablóny mailov máme z viacerých zdrojov, väčšinou boli ponúkané so simulátormi phishingu ktoré sme analyzovali [36, 37, 38].

Obťažnosť mailov určuje štylistika, gramatika, typ oslovenia, grafická stránka kde bude rozhodovať prítomnosť loga a podpisového bloku/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 ktoré 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 [39].

## 2.2 Správa a používanie hesiel

Obsahom tohto modulu sú rôzne spôsoby prelomenia hesiel. 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. Spomenieme riziká ukladania hesiel v počítači, či riziko používania malého počtu hesiel. Zdôrazníme 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 keď heslo bude mať výrazné nedostatky. Žiadne heslá nebudeme ukladať v nijakej 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 tak sme sa rozhodli že v tomto module nebude delenie podľa obťažnosti.

## 2.3 WI-FI

Tento modul sa zaoberá hlavne 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 čo to pre používateľa znamená – jeho dáta 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 ako je VPN, SSL enkrypcia, vysvetľuje sa 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 zabezpečujú, a aký je rozsah ich ochrany. 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.

## 2.4 Malware

V tomto module chceme ukázať, akými spôsobmi je malware distribuovaný a ako sa môže prejavovať na počítači. Používateľov upozorňujeme nielen pred spustiteľnými súbormi, ale aj pred PDF, Microsoft Office dokumentami, či viacerými typmi obrazových súborov, ktoré sú využívané na prenos malwaru hlavne cez email. Ďalším cieľom modulu je, aby používatelia vedeli rozpoznať znaky infikovaného počítača. Tými sú napríklad vyskakujúce reklamy, vysoké využitie procesora či internetového pripojenia, e-maily, či príspevky na sociálnej sieti posielané z účtu používateľa.

## 2.5 Implementácia

Okrem samotného Moodlu využívame aj viacero pluginov na zabezpečenie gamifikácie, interaktívneho učenia a delenia podľa obťažnosti. Pre zabezpečenie rozdelenia účastníkov podľa levelu znalostí sme použili Adaptive Quiz modul vytvorený Middlesgburgskou univerzitou [40]. Tento plugin využíva algoritmus postavený na psychometrickom Raschovom modeli. Jeho algoritmus vypočíta úroveň znalostí účastníka pomocou otázok so zadanou obťažnosťou pričom počas kvízu vypočítava akú ďalšiu otázku položí tak, aby úroveň určil čo najpresnejšie. Počíta aj odchýlku [41]. Obťažnosť otázke určia špeciálne pomenované tagy z Moodlu. Pôvodne sme chceli výsledky Adaptive Quizu použiť ako user profile field – dátové pole v profile, a podľa neho obmedzovať prístup ku kvízom, ale potom sme sa rozhodli obmedzovať ho podľa známky z Adaptive Quizu ktorá je rovná jeho výsledku, prípadne ju je možné váhami upraviť ak to situácia vyžaduje.

Plugin 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.

Kvôli tomu, že nastavenia sa v Moodle pluginoch sú tvorené pomocou jednej generickej stránky ktorej obsah sa dynamicky tvorí podľa modulu sme museli zmeniť aj kód jadra Moodlu. Zmena bola potrebná aby sme mohli pri zmene nastavení zistiť počet tagov v databáze. Keďže používame delenie na tri levely tak sme upravili kód jadra Moodlu aby podľa názvu kvízu (easy, normal, hard) filtroval otázky z banku podľa levelu ich tagu. Neimplementovali sme plné filtrovanie keďže príde do Moodlu v polovici mája, a nie je žiaden dôvod mať dve metódy filtrovania otázok v kvíze.
H5P plugin [42] nám dodáva interaktívny obsah. Framework H5P poskytuje okrem iného interaktívne video ktoré môže obsahovať otázky typu výber z možností, doplnenie slova, drag and drop, ďalej 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. Pre kvízy s interaktívnym videom využívame aj plugin Kaltury pre Moodle [43].

Na gamifikáciu používame odznaky ktorých podpora je zabudovaná v Moodle. 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 [44]. Ďalej používame Stash plugin [45] ktorý umožní pridávať zberateľské predmety priamo do textu kurzu čím je podporené čítanie lekcií. Plugin Stash availibility [46] umožní 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 [47] 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 čítanie lekcie a všetky body sa sčítajú do jedného výsledku čo motivuje študenta venovať sa všetkým aktivitám.

Druhým je Level Up! block [48] ktorý tiež umožňuje pridávanie bodov za plnenie aktivít a má rebríček, rozdiel je v tom, že sú v ňom aj levely, a teda po určitom počte bodov získa študent ďalší level. Dodatočné pluginy umožňujú použiť level ako požiadavku na otvorenie obsahu ako sú kvízy [49] alebo dokonca celé kurzy [50]. Tento plugin vychádza v dvoch verziách – oklieštenej ktorá je zadarmo a platenej ktorá ponúka väčšiu funkcionalitu. Väčšina pluginov pre Moodle je neplatená a open source ako samotný Moodle a toto je veľmi zriedkavý jav.

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 plugin CBM Grade Summary [51]. Pri CBM v Moodli majú rôzne stupne určitosti danú pravdepodobnosť určitosti ktorú vyjadrujú v rozsahu 0-100%. Presnejšie, stupne majú takéto pravdepodobnosti: Pri stupni 1 si je študent istý na menej ako 67 percent, pri stupni 2 si je istý na až 80 percent a pri treťom si je istý na viac ako 80 percent. Skóre sa pri stupňoch dáva takto: jeden, dva a 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 z časti hádaním [52].

My používame zmenený kód jadra Moodlu ktorého autorom je profesor Tony Gardner-Medwin [53] ktorý vytvoril aj CBM plugin. Vďaka týmto zmenám Moodle vypočíta známku z priemeru týchto pravdepodobnosti, keďže pri počítaní známky z CBM skóre sa dalo dosiahnuť až 300% známky, teda už pri tretinovom hodnotení by bola dosiahnutá maximálna známka, čo 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.
Posledným komponentom systému ja naša JavaScript aplikácia postavená na knižnici zxcvbn ktorá ponúka možnosť využitia dotykovej obrazovky na písanie keďže v aplikácii je zahrnutá aj klávesnica.

# 3 Záver

Po preštudovaní noriem, štandardov, literatúry zaoberajúcej sa tvorbou programov na zvyšovanie povedomia sme si vybrali ktoré oblasti informačnej bezpečnosti bude náš program pokrývať. V ďalšom kroku sme sa zamerali na problematiku zvyšovania povedomia z psychologického hľadiska, kde sme si preštudovali rôzne prisviedčacie prístupy a techniky a možnosti ich využitia pri zvyšovaní povedomia v oblasti bezpečnosti. Potom sme si vybrali potrebné nástroje vo forme open source programov a navrhli a implementovali sme samotný systém a teda sme splnili všetky ciele práce.

**Poďakovanie.** 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.

## Literatúra

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. Česká technická norma 2014. ČSN ISO/IEC 27001 (36 9790).
6. Česká technická norma 2014. ČSN ISO/IEC 27002 (36 9790).
7. 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.
8. 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.
9. Siponen, M.T., 2000. A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), pp.31-41.
10. 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
11. Interactive Teaching Styles Used in the Classroom, https://education.cu-portland.edu/blog/classroom-resources/5-interactive-teaching-styles-2/
12. Prince, M., 2004. Does active learning work? A review of the research. Journal of engineering education, 93(3), pp.223-231.
13. 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.
14. 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.
15. 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).
16. 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.
17. Mayer, R.E., 2011. Does styles research have useful implications for educational practice?. Learning and Individual Differences, 21(3), pp.319-320.
18. Bada, M. and Sasse, A., 2014. Cyber Security Awareness Campaigns Why do they fail to change behaviour?.
19. 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.
20. ISACA. Cybersecurity Fundamentals Study Guide. Rolling Meadows (USA): ISACA, 2015. ISBN 978-1-60420-594-7.

21. US Government, Legal Information Institute, Title 44, Chapter 35, Subchapter 111, §3542, Cornell University Law School, www.law.cornell.edu/uscode/44/3542.html.
22. 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.
23. Wilson, M. and Hash, J., 2003. Building an information technology security awareness and training program. NIST Special publication, 800(50), pp.1-39.
24. the University of Adelaide: Security Awareness games, https://www.adelaide.edu.au/technology/secureit/games/
25. Digizen: digizen game, http://www.digizen.org/resources/digizen-game.aspx
26. Federal Trade Commision: The Case of the Cyber Criminal, https://www.consumer.ftc.gov/media/game-0013-case-cyber-criminal
27. Stay Safe Online: Resources, https://staysafeonline.org/resources/
28. STOP. THINK. CONNECT: Resources, https://stopthinkconnect.org/resources
29. PhisingBox, https://www.phishingbox.com
30. KnowBe4, https://www.knowbe4.com/
31. Wombat Security, https://www.wombatsecurity.com
32. The Hermit: Spear Phiser, https://github.com/kevthehermit/SpearPhisher
33. Phishing Frenzy, https://www.phishingfrenzy.com/
34. Secure State: King Phisher, https://github.com/securestate/king-phisher
35. CSIRT phishing test, https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html
36. King Phisher mail templates, https://github.com/securestate/king-phisher-templates
37. Gophish mail tmplates, https://github.com/rfdevere/templates
38. Phishing Frenzy mail templates, https://github.com/pentestgeek/phishing-frenzy-templates
39. McElroy, T., Hannay, P. and Baatard, G., 2017. The 2017 homograph browser attack mitigation survey.
40. Moodle plugin Adaptive Quiz, https://moodle.org/plugins/mod_adaptivequiz
41. 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.
42. Moodle plugin H5P, https://moodle.org/plugins/mod_hvp
43. Modle plugin Kaltura Video Package, https://moodle.org/plugins/view.php?id=447
44. Moodle plugin Badge Awarder, https://github.com/pentestgeek/phishing-frenzy-templates
45. Moodle plugin Stash, https://moodle.org/plugins/block_stash
46. Moodle plugin Stash Availibility, https://moodle.org/plugins/availability_stash
47. Moodle plugin Ranking block, https://moodle.org/plugins/block_ranking
48. Moodle plugin Level up!, https://moodle.org/plugins/block_xp
49. Moodle plugin Level up! Availibility, https://moodle.org/plugins/availability_xp
50. Moodle plugin Level up! Enrol, https://github.com/branchup/moodle-enrol_xp
51. Moodle plugin CBM Grade Summary, https://moodle.org/plugins/quiz_cbmgrades
52. 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.
53. Modifikácia jadra Moodlu pre CBM, http://tmedwin.net/cbm/moodle/download/