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 je vytvoriť systém na jeho zvyšovanie modifikáciou systému na manažovanie vzdelávania s využitím softwaru na penetračné testovanie a phishingové kampane.

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 [2] je slabé povedomie o informačnej bezpečnosti medzi zamestnancami považované za najväčší problém organizáciám obrániť sa proti bezpečnostným hrozbám. 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].

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 1000 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].

1.2 Prehľad súčasného stavu

Na vyššie uvedené bezpečnostné hrozby v súčasnej dobe existuje niekoľko riešení, ktorých cieľom je zvyšovanie povedomia osôb, najmä však zamestnancov. Takéto riešenia je možné rozdeliť podľa cieľovej skupiny na:

- 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 môže pokryť len veľmi malú časť bezpečnostných problémov. Je otázne, či nejako ovplyvní bezpečnostné povedomie 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].

Pre spoločnosti už existujú komplexné riešenia, či už platené alebo open source. Príkladom spoločnosti tvoriacej platené riešenia je PhishingBox [10], 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 [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.

Pri open source riešeniach je viacero phishing simulátorov, napríklad Spear Phisher [13], Phishing Frenzy [14], King Phisher [15] ktoré sa kvalitou a ponukou vyrovnajú plateným. Spear Phisher umožňuje sledovanie výsledkov phishing kampane kde ukladá kliknutia na stránku aj na prílohu. Má v sebe e-mailový server. King Phisher umožňuje aj klonovať stránky, čo dodá väčšiu dôveryhodnosť stránkam na odkazoch v maili. Tiež umožní pridať do správy obrázky, kalendárové pozvánky a prílohy. Z kampane si ukladá to, či bolo kliknuté na stránku a zadané heslá. Je možné posielať si SMS notifikácie, keď prídu výsledky z kampane a cez modul umožňuje aj SMS phishing.Phishing Frenzy umožňuje klonovať stránky, pridávať prílohy do mailov, pri kampani sledovať otvorenie mailu, návštevy stránky a zadanie hesiel. 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]. Na testovanie sily hesiel existujú knižnice vo viacerých jazykoch ako zxcvbn [18] pre JavaScript či nbvcxz [19] pre Javu.

2 Systém na zvyšovanie povedomia v oblasti informačnej bezpečnosti

Pre plné využitie open source riešení je potrebné ich integrovať do jednej aplikácie, prípadne zabezpečiť komunikáciu medzi nimi. Súčasne je potrebné zabezpečiť automatizáciu, teda plánovanie a uskutočnenie bezpečnostných kurzov, ktoré sú pri platených riešeniach zabezpečené ako služba od daného poskytovateľa. Tiež je potrebné postarať sa o zber a analýzu výsledkov simulácií a prípadných zmien programu.

Cieľom práce je na základe analýzy štandardov, noriem v oblasti informačnej bezpečnosti a na základe porovnania existujúcich prístupov a nástrojov pre zvyšovanie bezpečnostného povedomia využiť open source riešenia na vytvorenie systému na zvyšovanie povedomia v oblasti informačnej bezpečnosti.

2.1 Návrh riešenia

Navrhovaný systém má byť postavený na systéme Moodle [20], hlavne kvôli tomu že má veľké množstvo pluginov v porovnaní s ostatnými LMS. Súčasne má širokú ponuku typov testov a ako jeden z mála má H5P plugin [24] na tvorbu interaktívneho html5 obsahu. Má mať šesť modulov, ktoré pokrývajú základné aspekty informačnej bezpečnosti z pohľadu používateľov:

- správania sa na Internete vrátane prezerania webového obsahu,
- používanie a správa hesiel,
- e-mailová komunikácia,
- komunikácia a profily v rámci sociálnych sietí,
- Wi-Fi a
- malware.

Systém bude mať možnosť nastavenia obťažnosti úloh. Obťažnosť úloh a obsahu sa na začiatku nastaví pre každú oblasť podľa začiatočných kontrolných otázok určených na zistenie vedomostnej úrovne používateľa a neskôr sa bude meniť podľa výsledkov jeho úloh. Na konci bude záverečný dotazník určený na zistenie aktuálneho bezpečnostného povedomia používateľov, ktorého výsledky budú použiteľné pre ďalšie zlepšovanie systému. Nasledujúce kapitoly sa budú podrobnejšie zaoberať jednotlivými modulmi.

2.2 Modul pre e-mailovú komunikáciu

Tento modul bude pokrývať 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.

Používatelia si nastavia v Moodli svoj e-mail, na ktorý im budú chodiť správy, niektoré obsahujúce aj prílohy, či odkazy na stránky. Na začiatku budú mať 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.

Obťažnosť e-mailov pri phishingu bude určovať URL adresa pri odkazoch, kde pri náročnejších úlohach je možné použiť unicode znaky z iných jazykov nerozlíšiteľné od latinských (napríklad z jazyka hindi), štylistika, gramatika, typ oslovenia.

Z technického hľadiska bude posielanie správ, ktoré používatelia dopredu poskytnú zabezpečené e-mailovým serverom, cez ktorý bude phishing program posielať správy. Phishingovým programom je jeden z open source programov ako, je King Phisher [15] alebo Spear Phisher [13]. Pri týchto programoch je posielanie e-mailov interaktívne, vyžaduje sa činnosť používateľa. Preto bude musieť byť použitý program modifikovaný, aby automaticky vyberal maily z databázy na základe odporúčanej obťažnosti pre jednotlivých používateľov a posielal na ich e-mailovú adresu.

2.3 Modul pre správu a používanie hesiel

Obsahom tohto modulu budú rôzne spôsoby prelomenia hesiel, ako je útok hrubou silou (brute-force), zoznamy uniknutých hesiel, pravdepodobnostné metódy. Vysvetlíme pojem entropie, používanie slovníkov, l33t slová (nahrádzanie písmen podobne vyzerajúcimi číslami ktoré nie je bezpečné) 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.

Po vysvetlení pojmov by museli používatelia v Moodli zadať heslo podľa požiadaviek a zároveň ho po istej dobe (najlepšie pri najbližšom kurze) zadať znovu, aby ukázali že si ho pamätajú. Ďalšou aktivitou by bol kvíz, kde by mali ponúknuté rôzne heslá a mali by určiť, proti akému typu útoku sú zraniteľné.

Modul bude zabezpečený cez JavaScript aplikáciu založenú na knižnici zxcvbn ktorá bude v Moodle kurze spustená cez iframe embedder [21], ktorý ponúka H5P plugin. Ten umožňuje tvorbu interaktívneho HTML5 obsahu. Zxcvbn porovnáva heslá so s anglickým slovníkom, databázou mien, priezvisk, 10000 najčastejšími heslami a klávesnicovými vzorcami na rôznych typoch klávesníc. Súčasne hľadá sekvencie (aj obrátené) písmen a číslic, roky a dátumy s rozoznaním l33t a počíta entropiu hesla.

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. Samotná knižnica zxcvbn pri zadaní slabého hesla varuje používateľa aj s dôvodom, prečo je slabé.

2.4 Modul pre komunikáciu a profily v rámci sociálnych sietí

Cieľom 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 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 budú vyhodnocovať pripravené príspevky na Facebooku z hľadiska bezpečnosti.

Interaktívne obrázky budú image hotspots [22] (umožňujúce na obrázku vytvoriť viacero bodov a po kliknutí na ne urobiť rôzne akcie) z H5P pluginu. Test s príspevkami bude klasický test ponúkaný Moodlom s preddefinovanými odpoveďami, z ktorých treba vybrať správnu. Obťažnosť bude určovať, ktoré príspevky budú vybrané, pričom pri náročnejších príspevkoch bude menej očividné ako môžu ohroziť pisateľa.

2.5 Modul pre wi-fi

Tento modul sa bude zaoberať hlavne verejnými Wi-Fi sieťami. Vysvetlíme ich riziká a kryptografické protokoly na zabezpečenie bezdrôtových sietí. Súčasne spomenieme, že ak pri pripojení na Wi-Fi sieť nie je požadované heslo tak je nešifrovaná, a čo to pre používateľa znamená. Ďalej sa budeme zaoberať Wi-Fi sieťami a prístupovými bodmi nastraženými útočníkom a spôsobmi ako ich rozpoznať. Prejdeme rôzne spôsoby obrany ako je VPN, SSL enkrypcia, vysvetlíme si dôležitosť HTTPs protokolu. Ukážeme, ako vypnúť zdieľanie súborov.

Po kurze bude nasledovať 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 zistíme, 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 sú Wi-Fi siete sú dôveryhodné.

Všetky testy budú pokryté priamo Moodlom. Pri všetkých testoch ide o výber z viacerých možností. 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 testu je zistenie toho, či si po skončení kurzu účastníci pamätajú ako odlíšiť dôveryhodné siete.

2.6 Modul pre malware

V tomto module chceme ukázať, akými spôsobmi je malware distribuovaný a ako sa môže prejavovať na počítači. Budeme používateľov upozorňovať 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.

Ukážeme im, ako skontrolovať kontrolný súčet súboru (checksum). 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. Modul bude implementovaný ako kurz a vedomostný test v Moodli.

2.7 Modul správania sa na Internete

Tu sa zameriame na rôzne hrozby spojené s používaním Internetu, ktoré možno odhaliť bez technickej podpory. Cieľom je, aby používatelia vedeli nájsť a analyzovať indície toho, že ide o útok a včasne sa mu vyhnúť.
Prvý typ útoku využíva Java Applet (applet je malá aplikácia) kde s použitím SETu naklonujeme žiadanú stránku a odkaz na svoju stránku zavesíme do kurzu v Moodli. Po kliknutí na odkaz budú používatelia presmerovaní na našu stránku a budú požiadaní o spustenie Java aplikácie. Po potvrdení budú presmerovaní na stránku, ktorá bola skopírovaná a Java applet bude spustený. Keďže Java seba podpísaných vydavateľov zobrazuje ako neznámych, potom na vyhnutie sa stačí spúšťať aplikácie len od vydavateľov, ktorým dôverujeme, čo spomenieme v kurze. V minulosti to bol najúspešnejší útok z ponuky SETu kvôli tomu, že bolo možné podhodiť vydavateľa aj v seba podpísaných aplikáciách. V súčasnosti je tiež použiteľný najmä kvôli nepozornosti používateľov.

Ďalší útok využíva HTML5 FullScreen API. Používatelia budú mať v kurze odkaz na legitímnu stránku, avšak po kliknutí naň sa namiesto predvoleného presmerovania na stránku zavolá nami pripravená stránka. Na tejto stránke sa spustí skript, ktorý si zistí náš prehliadač a operačný systém. Následne sa zobrazí nám klonovaná stránka, ktorá ihneď vojde do full screen módu, s niekoľkými zmenami. V oblasti prehliadača, kde je názov stránky vidí obeť názov legitímnej stránky aj s HTTPs certifikátom, ak ho pôvodná stránka má. Jediná indikácia je to, že stránka vošla do full screen módu. Tento útok je možné vykonať v SETe, ale je možné ho urobiť aj ako JavaScript aplikáciu, ako to bolo urobené v projekte [23]. V tomto prípade by ho bolo možné integrovať pomocou H5P pluginu do stránky kurzu.
Pri ďalšom útoku využijeme SET na klonovanie stránky. V kurze zavesíme odkaz veľmi podobný názvu stránky. Môžeme použiť znaky iných jazykov, aby sa ešte viac podobal odkazu na stránku ktorá bola klonovaná ako sme spomínali pri e-mailovom module. Po kliknutí na odkaz sa zobrazí klonovaná stránka pýtajúca prihlasovacie údaje. Po ich zadaní a po pokuse sa o prihlásenie je presmerovaný na stránku ktorú sme klonovali, ale v SETe sú už uložené jeho údaje. Keďže nás nezaujímajú prihlasovacie údaje používateľov, môžeme využiť SET len na klonovanie stránok a samotný útok robiť bez neho.

Tabnabbing je názov ďalšieho útoku s využitím SETu kde po kliknutí na odkaz je používateľovi prezentovaná správa informujúca ho o tom, ž stránka sa načíta. Po tom, čo používateľ zmení kartu v prehliadači sa stránka zmení na našu klonovanú. Pri najbližšej návšteve používateľ zadá údaje. Indikátorom útoku je to, že stránka sa „načíta“ len po zmene karty.
Keďže chceme používať SET počas kurzov pasívne v pozadí, budeme ho musieť modifikovať, keďže útoky a ich nastavenia sa zadávajú len interakciou s používateľom.

V tomto module sú testy zbytočné, keďže okrem samotného odkazu, ktorý sa trénuje v e-mail module, je možné všetky útoky veľmi ľahko odhaliť. To je možné, keď používateľ pozná ich indikátory a očakáva ich.

3 Záver

Po preštudovaní noriem, štandardov, literatúry zaoberajúcej sa tvorbou programov na zvyšovanie povedomia sme analyzovali ankety zameriavajúce sa na úroveň vedomostí a zvyky v oblasti bezpečnosti. Ďalej sme študovali správy bezpečnostných spoločností zhrňujúce počty úspešných útokov podľa kategórií. S ohľadom na tieto dáta 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 sme samotný systém. Teraz nás čaká samotná implementácia systému.

Poďakovanie. Týmto sa chcem poďakovať JUDr. RNDr. Pavlovi Sokolovi, PhD. za cenné rady, pomoc a odborné vedenie pri príprave vedeckého článku.

Literatúra

1. EY: Path to cyber resilience: Sense, resist, react. EY's 19th Global Information Security Survey 2016-17. Survey, EY (2017), s. 13
2. CyberEdge: 2015 Cyberthreat Defense Report North America & Europe. Report, CyberEdge Group (2015), s. 22
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), s. 3
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 Phiser, 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.Moodle https://github.com/moodle/moodle
21.H5P Iframe Embedder, https://h5p.org/iframe-embedder
22.H5P Image Hotspots, https://h5p.org/image-hotspots
23.Feross Aboukhadijeh: Fullscreen API attack, https://github.com/feross/fullscreen-api-attack
24.H5P supported frameworks, https://h5p.org/