Phishing na vlastní kůži

Jan Soukal, Jan Vykopal, ÚVT MU

Na množství nevyžádané pošty plné reklamních sdělení jsme si bohužel už zvykli. V posledních měsících se však do e-mailových schránek uživatelů po celém světě dostává stále více podvodných dopisů [1], které se snaží uživatele dostat do úzkých a přinutit je vyzradit citlivé údaje – tzv. *phishing*. Tyto podvodné e-maily mají nejrůznější podobu: od zpráv napsaných velmi špatnou češtinou, kde útočník použil strojový překladač (např. službu Google Translator) až po sofistikované útoky, které cílí na uživatele určitých služeb.

Nevyžádanou poštu se daří automaticky detekovat a filtrovat s obtížemi, u (cíleného) phishingu je situace ještě horší v případě, kdy je zneužit existující účet uživatele a z něj jsou jeho obvyklým kontaktům rozeslány podvodné e-maily. Software, který má rozhodnout, zda jde o podvodný e-mail či nikoliv, nemá žádné rozpoznávací vodítko.[1] S tímto typem útoku se bohužel setkáváme stále častěji.

Rozhodnutí, zda jde o podvrh, tedy zůstává na člověku, příjemci zprávy. I když útočníci používají pokročilé metody, jak příjemce obelstít, je přesto možné se takovému útoku ubránit. Pokud ovšem příjemce ví jak. Tradiční školení uživatelů nejsou podle našeho názoru příliš účinná, proto jsme zvolili výuku zážitkem.

1 Škola hrou

Nápad vzdělávat uživatele „hrou“ není ojedinělý. Celosvětově pozorujeme nastupující trend tohoto typu edukace. Situaci lze ilustrovat na americké společnosti Wombat Security Technologies [2], spin-offu Carnegie Mellon University z Pittsburghu, jež při bezpečnostních školeních využívá právě interaktivního zapojení uživatelů – například odesíláním testovacích phishingových zpráv uživatelům nebo nabídkou počítačových her přibližujících bezpečnostní témata i laikům.

[1] Zpráva směřuje od důvěryhodného či známého poštovního serveru do schránky na jiném známém serveru (třeba i v rámci jedné organizace) atp.

studenti	185
neakademičtí pracovníci	68
akademičtí pracovníci	15
absolventi	14

Tabulka 1: Struktura účastníků[3]

Bezpečnostní akci *Phishing na vlastní kůži*[2] jsme připravili pro všechny zájemce z řad studentů, zaměstnanců i absolventů MU, kteří si chtějí vyzkoušet, zda rozpoznají podvodné dopisy. Účastníci akce dostanou v průběhu 30 dnů od přihlášení námi připravené podvodné e-maily, které se je snaží vyprovokovat k nějaké akci, tak jak to dělá typický útočník. Účastníci dopředu nevědí, kdy jim e-mail přijde a co bude obsahovat. Po skončení akce obdrží vyhodnocení, ve kterém se dozví, jak si vedli, jak vypadaly rozeslané e-maily, které nástrahy odhalili a v čem spočívalo nebezpečí.

2 Průběh akce

Akce byla spuštěna 11. března 2011. Přestože akce stále běží (zájemci se mohou dál hlásit), předpokládáme, že většina zájemců se již přihlásila a akci dokončila. Níže uvedené statistiky jsou vztaženy k datu 10. května 2011. Do akce se přihlásilo celkem 264 zájemců, 9 se v průběhu odhlásilo, akci tedy dokončilo 255 účastníků.

Strukturu účastníků ilustrují tabulky 1, 2, 3. Dvě třetiny z přihlášených tvořili studenti Masarykovy univerzity, zbytek pak především neakademičtí pracovníci. Zajímavým faktem je jistě i účast absolventů, byť v rámci akce představovali pouze 5% menšinu.

Z hlediska účasti studentů vzhledem k domovským fakultám popsané v tabulce 2 je vhodné zmínit 43% zastoupení Filozofické fakulty MU, která tímto předstihla i Fakultu informatiky MU s 30% účastí. Za tento malý „zázrak“ vděčíme pracovníkům Filozofické fakulty a zejména Ústřední knihovny FF, kteří velmi aktivně propagovali naši akci prostřednictvím vlastních webů a

[2] `https://security.ics.muni.cz/15-Phishing-na-vlastni-kuzi`

[3] V případě, kdy je účastník současně student i zaměstnanec univerzity, je započítán do obou kategorií.

Filozofická fakulta	79
Fakulta informatiky	55
Přírodovědecká fakulta	23
Ekonomicko-správní fakulta	7
Lékařská fakulta	7
Fakulta sociálních studií	7
ostatní fakulty	7

Tabulka 2: Účast studentů podle fakult

Filozofická fakulta	22
Fakulta informatiky	11
Institut biostatistiky a analýz	10
Lékařská fakulta	8
Ústav výpočetní techniky	7
ostatní	25

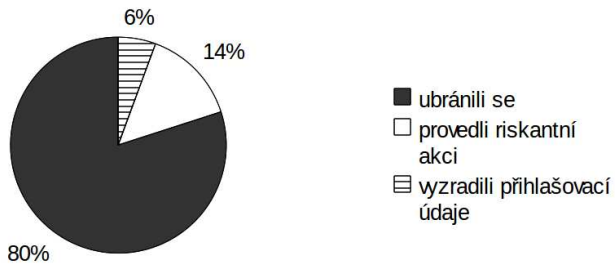
Tabulka 3: Účast zaměstnanců podle fakult a ústavů

vývěsek, a významně tak přispěli k hojné účasti mezi laickou veřejností fakulty.

V případě zaměstnanců přihlášených do akce nejsou patrné tak významné rozdíly, jako jsme zaznamenali v kategorii studentů. Opět dominuje Filozofická fakulta, rozložení mezi jejími následovníky je však, jak ilustruje tabulka 3, již velmi rovnoměrné. Za zmínku stojí, že vyjma nejvíce zastoupené Filozofické fakulty jsou následující 4 fakulty výhradně přírodovědného zaměření.

Samotná akce měla v původním návrhu obsahovat tři nástrahy. První ilustruje typický phishingový útok, s jakým se může uživatel nejčastěji setkat, další dvě pak měly účastníkům přiblížit méně známé, avšak o to zákeřnější možnosti phishingu. Všechny tři nástrahy byly vytvořeny podle reálných útoků, jež v poslední době zvířily vody českého internetu.

Při tvorbě a úvodním rozeslání třetí nástrahy jsme ale podcenili situaci. Útok, jejž jsme zamířili na Informační systém MU, byl totiž natolik propracovaný a důvěryhodný, že místo zamýšlené osvěty šířil mezi uživateli spíše nedůvěru vůči univerzitnímu IS. Údajně se mluvilo dokonce o úspěšném „hacknutí“ IS. Z tohoto důvodu jsme nakonec třetí nástrahu z akce stáhli a její podobu ilustrovali v rámci interaktivního článku na našem bezpečnostním webu `https://security.ics.muni.cz`.

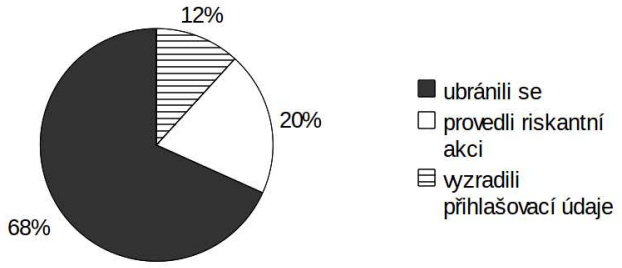


Obrázek 1: první nástraha

Obr. 2 ilustruje úspěšnost uživatelů v odhalování první nástrahy akce. Pětina účastníků se v rámci první nástrahy zachovala riskantně (nějakým způsobem reagovala na zaslaný e-mail), nebo dokonce vyzradila přihlašovací jméno a heslo. Zajímavý trend lze pozorovat mezi studenty přihlášenými do akce. Největší poměr „podvedených“ studentů jsme zaznamenali v případě bakalářských programů. U studentů navazujícího magisterského studia, a ještě výrazněji u doktorského pak poměr klesá.

Kdybychom k výsledkům první nástrahy přistupovali jako k obecné statistice náchylnosti uživatelů MU vůči phishingu, mohli bychom být se závěry z akce velmi spokojeni. Je-li pouhých 6 % uživatelů svolných k vyzrazení přihlašovacích údajů, lze mluvit o vysoké míře odolnosti proti tomuto typu útoku. Je však třeba zmínit, že první nástraha představuje skutečně typický phishingový útok se všemi nedostatky, které běžnému uživateli výrazně ulehčují rozpoznání phishingu. Stejně tak je nutné k hodnocení přistupovat střízlivě i z toho důvodu, že uživatelé se do akce hlásili vědomě a mohli tak být obezřetnější ke každému nestandardnímu e-mailu.

V rámci druhé sofistikovanější nástrahy, jejíž výsledky shrnuje obr. 2, se k nezodpovědnému chování podařilo zlákat o 12 % více uživatelů než v předchozím případě. Procento uživatelů ochotných vyzradit přihlašovací údaje se dokonce zdvojnásobilo!



Obrázek 2: druhá nástraha

Nárůst „podvedených“ uživatelů v tomto případě jednoznačně přikládáme kvalitě zpracování phishingu, který byl oproti první nástraze vypracován vcelku profesionálně a běžnému uživateli nenechával příliš prostoru pro rozpoznání útoku.

Na druhou stranu je nutno přiznat naše očekávání, že účastníků ochotných vyzradit heslo bude ještě více. V rámci nástrahy byla cílem útoku aplikace, jejíž používání je sice na MU vcelku rozšířeno, rozhodně se však nejedná o masově využívanou aplikaci typu IS MU. Je proto možné, že na část uživatelů tato nástraha nefungovala právě proto, že popisovanou aplikaci neznají nebo ji příliš často nepoužívají.

3 Závěr

Interaktivním bezpečnostním školením *Phishing na vlastní kůži* prošlo za tři měsíce od jeho spuštění pestré spektrum univerzitních uživatelů – od bakalářských, magisterských i doktorských studentů, provozních pracovníků až po profesory a vedoucí pracovníky. Ti všichni si mohli sami vyzkoušet, jak budou reagovat na reálné útoky, které se dnes a denně objevují v jejich e-mailových schránkách. Pozitivní ohlas akce mezi účastníky je pro nás signálem pro pokračování v tomto způsobu vzdělávání. Akce stále probíhá a zájemci si stále mohou *na vlastní kůži* zkusit, jak si s phishingem poradí.

4 Poděkování

Autoři článku děkují Tomáši Plesníkovi za pomoc s přípravou samotné akce i zpracováním statistik, Martinu Vizvárymu za vytvoření grafů a všem, kteří zprostředkovali informaci o konání akce potenciálním zájemcům.

CSIRT-MU je tým Masarykovy univerzity zodpovědný za řešení počítačových bezpečnostních incidentů. Pro uživatele připravuje bezpečnostní web na adrese `https://security.ics.muni.cz/`.

Literatura

[1] IID. eCrime Trends Report: First Quarter 2011. Technická zpráva. `http://www.internetidentity.com/images/stories/docs/ecrime_trends_report-q1-2011_by_iid.pdf`

[2] Webové stránky společnosti Wombat Security Technologies. `http://www.wombatsecurity.com/`. □