9 771854 022001

letnik 7

6-7

APRIL-MAJ-JUNIJ 2011

KAZiN

PRIMORSKI ŠTUDENTSKI UNIVERZITETNI ČASOPIS

INTERVJU: MILENA ZUPANČIČ

AKCIJA: INSTITUCIJE EU ZAPOSLUJEJO MLADE DIPLOMANTE

ZMENEK NA SPLETU ALI ŽIVLJENJSKA PREIZKUŠNJA

Prostovoljno delo v državah v razvoju // Utemeljen strah pred lastno tehnologijo // Ko petje postane način življenja – Perpetuum Jazzile

KAZALO

MITJA TRETJAK,
vodja skupine
za medije ŠOUP

Za nami je sedma sezona *Kažina.* Bogato posejana študentska njiva je bila v tem študijskem letu tarča pogostih in včasih zahrbtnih napadov, doživela je tudi toče in nevihte. Po njej so se sprehodili različni paraziti in roparji, tako da se je v zadnjih, predvsem predreferendumskih mesecih, spremenila v bojno polje. Vseeno pa je študentska zemlja, pognojena s trdim delom, kljubovalnostjo in kančkom upora, obrodila nekaj sadov. Njihov okus pa je v teh tednih večinoma mešanica sladkosti doseženih ciljev in grenkobe še nerešenih težav. Pa vendar so sadovi med nami in polnijo velike košare. Kot vsi pridelovalci takšne in drugačne zemlje pa se študentje dobro zavedajo, da bo kmalu potrebno znova sejati, če si želijo novih žetev.

Tudi s *Kažinom* je (bilo) podobno. Vsak mesec smo sejali in nato želi, kot vedno smo posvečali največ pozornosti težavam mladih, poročali pa smo tudi o dosežkih in izpostavljali svetle žarke, ki občasno pronicajo skozi oblake današnjih sivih dni. Ustvarjali smo za naše široko bralstvo, ki nam po sedmih letih še vedno stoji ob strani in nas podpira.

Pogosto se sprašujem, kako obsežen je krog ljudi, mladih in manj mladih, ki spremlja naše objave. Pred enim letom je raziskava o branosti našega časopisa med študenti pokazala, da nas na Primorskem (in tudi dlje) poznajo, cenijo in tudi berejo. To, da nas berejo, sem nalašč postavil na zadnje mesto, kajti najbolj nas je presenetil pridobljeni podatek, da študentje na splošno precej malo berejo. Ne samo *Kažin,* temveč tudi drugo čtivo, dnevno časopisje ali periodiko. Podatek bi moral presenetiti, če ne celo alarmirati, kajti od študirajoče populacije se (še vedno?) pričakuje, da je najbolj ažurna, najbolj osveščena in zato tudi najbolj kritična. Sprašujem pa se: ali to (upanje) še vedno obstaja?

Občutek imam, da je to držalo le nekoč, ko smo študente dojemali kot bodoče potencialne intelektualce, voditelje, kulturne delavce, ekonomiste itd. Bili so upi družbe. Študij je pomenil začetek življenjske poti, ki jih je praviloma peljala čedalje više, do vrhov kritičnega mišljenja in pogosto tudi same družbe. Kaj pa danes? Ali se študent sploh počuti takšnega? Ali še vedno verjame, da bo s pridobljeno izobrazbo prišel visoko, daleč in še dlje? Da bo zaradi pridobljenega znanja in naziva dejansko postal *nekdo?*

Verjetno je univerzitetna izobrazba izgubila na pomenu, oziroma spremenila se je v nekaj drugega. Zato se sprašujem, ali ne bi bilo smiselno, če bi si nanovo osmislili sam koncept študenta in vlogo študirajoče populacije? Na tak način bi se izognili marsikateremu razočaranju in neizpolnjenim pričakovanjem, hkrati pa bi dejanskemu stanju ali pa celo resnici, iskreno pogledali v oči.

Drage bralke in dragi bralci, želim vam prijetne poletne mesece.

besedilo
MATJAŽ KLJUN

MED VSEM ZNANO SAGO WIKILEAKS SO PODPORNIKI SLEDNJE (SKUPINA ANONYMOUS) VDRLI V STREŽNIKE PODJETJA HBGARY, KI PONUJA VARNOSTNE REŠITVE TUDI AMERIŠKI VLADI, IN PRIDOBILI DOSTOP DO ELEKTRONSKIH PREDALOV POMEMBNIH LJUDI V PODJETJU. PREJŠNJI MESEC SO NAPADALCI PRIŠLI DO PODATKOV RSA (VARNOSTNEGA ODDELKA EMC, KI JE VODILNO SVETOVNO PODJETJE NA PODROČJU INFORMACIJSKIH INFRASTRUKTUR) IN TAKO POTENCIALNO PRIZADELI NJIHOV VARNOSTNI SISTEM SECUREID (NAČINA DVOSTOPENJSKE AVTENTIKACIJE, PODOBNE AVTENTIKACIJI NEKATERIH SPLETNIH BANK, KJER ZA PRIJAVO POTREBUJEMO PIN IN NAKLJUČNO GENERIRANO ŠTEVILO).

NEVARNOSTI ELEKTRONSKE POŠTE

Kako lahko taka podjetja oz. njihovi zaposleni, ki ponujajo varnostne rešitve, klonejo? Pri obeh napadih so napadalci uporabili socialni inženiring. Ta vključuje prijeme, s katerimi žrtev nagovarjamo k razkritju osebnih podatkov z namenom izvedbe kaznivih dejanj (kraja denarja iz bančnih računov, napad na računalniški sistem ...). Metode socialnega inženiringa so med drugim ribarjenje gesel preko lažnih spletnih strani (phishing), predpriprava na vprašanja o zasebnosti žrtve in posledično ustvarjanje avtoritete (pretexting), quid pro quo (ponujanje nečesa v zameno za nekaj – na primer navidezno pomoč uporabniku v zameno za geslo), nastavljanje prenosnih medijev z zlonamerno kodo kot vabo (baiting) in kraja podatkov preko lažnih interaktivnih telefonskih tajnic (IVR phishing). Med najbolj uporabnimi orodji socialnega inženiringa je elektronska pošta. Poglejmo si njeno uporabo v zgoraj omenjenih napadih.

Kako do podatkov

V prvem primeru se je napad začel z napadom na spletno stran podjetja HBGary. Ker je stran enega najbolj znanih podjetij na področju varnosti IT vsebovala precej ranljivosti, so napadalci prišli do zgoščenih gesel vrhovnega in še enega direktorja (Aarona Barra in Teda Vere). Gesla so nato zlomili z napadom s pomočjo slovarja (glej okvir), saj sta obe gesli vsebovali le šest malih črk in dve številki. Nato so napadalci ugotovili, da obe osebi uporabljata isto geslo tudi za elektronsko pošto, Twitter in LinkedIn. Ko so napadalci imeli dostop do elektronskih predalov, so vso elektronsko pošto prečesali in ugotovili ogromno podatkov, med katerimi je bilo tudi geslo skrbnika strežnika. Za dokončanje napada so potrebovali le še uporabniško ime in geslo navadnega uporabnika, ki bi se lahko prijavil kot skrbnik (skrbnik sistema zaradi varnostnih razlogov nima neposrednega dostopa do strežnika; nanj se mora najprej prijaviti kot navaden uporabnik in nato preko tega kot skrbnik). Preko poštnega predala direktorja so z dobro zastavljenimi vprašanji pripravili drugega zaposlenega, da je izdal podatke za račun navadnega uporabnika. Tako so napadalci prišli do skrbniškega dostopa do strežnika podjetja in posredno do precej kočljivih podatkov.

V drugem primeru podjetja RSA se je celoten napad začel z elektronsko pošto. Napadalci so dvema skupinama zaposlenih poslali elektronsko pošto z naslovom *Plan zaposlovanja 2011*. Elektronska pošta se je sicer znašla med neželeno pošto, a je enega od zaposlenih zanimalo, kaj je v njej. Ko je odprl priponko, v kateri je bila tudi pokvarjena Flash video datoteka (takšna kot jih na primer pregledujemo na YouTubu), je nevede preko le-te namestil tudi trojanskega konja (programček, ki napadalcu omogoči vstop v računalnik žrtve). Tako so napadalci dobili nepooblaščen dostop do računalnika zaposlenega in nato preko tega tudi do delov sistema, od koder so odtujili podatke.

Napad na tarčo

Pri obeh primerih je sicer šlo za skrbno pripravljene napade s točno določeno tarčo. A če ljudje, ki se ukvarjajo z računalniško varnostjo oz. o računalnikih vedo veliko, podležejo takim napadom oz. pre-

varam, jim navadni smrtniki lahko še prej. Zadnje čase se na primer precej govori o *botnetih* (eden je bil celo povezan s študentom mariborske univerze). Botnet je skupina računalnikov, ki jih nadzoruje in upravlja nepooblaščena oseba. Večina računalnikov v botnetih so osebni računalniki posameznikov, pri čemer slednji tega ne vedo. Računalniki v botnetu se najpogosteje uporabljajo za razpošiljanje neželene elektronske pošte in za napade na druge računalniške sisteme. Uporabniki računalnikov, vključenih v botnet, najpogosteje preko elektronske pošte vede ali nevede namestijo botnet zlonameren program (ponavadi preko priponke kot v primeru podjetja RSA). Poleg omenjenih napadov s pridobitvijo gesel ali z namestitvijo zlonamerne programske opreme na računalnik žrtve obstaja še vrsta prevar, ki se tudi izvajajo preko elektronske pošte. Najbolj znana so nigerijska pisma (ali prevare 419), v katerih prevaranti skušajo žrtev prepričati v posredovanje pri denarnih poslih. Kljub temu da so ti napadi že precej znani, se vedno najdejo ljudje, ki jim podležejo. Tudi v Sloveniji smo lahko zasledili primere, ko so bili zasebni prodajalci avtomobilov preko elektronske pošte zaprošeni, da bi avtomobil prodali nekomu v tujino za višjo ceno, kot so jo sami zahtevali. Za sprožitev celotnega postopka pa naj bi plačali nekaj 100 evrov na račun v tujino. Nekateri so to tudi storili.

Kako se zavarovati

Pred nekaterimi poskusi napadov in prevar se lahko preprosto zavarujemo, pri nekaterih moramo uporabiti nekaj zdrave pameti, pri nekaterih pa moramo biti precej podkovani, da se jim lahko izognemo. Dobra novica je, da je teh slednjih zelo malo. Pri vsemu pa se je dobro držati spodnjih napotkov:

1. Uporabljamo različna in težko zlomljiva gesla za različne storitve. To niti ni tako hudo kot zveni. Lahko na primer uporabljamo isto geslo z različnimi predponami. Če nekdo pridobi geslo za na primer Facebook, še vedno nima dostopa do drugih storitev, ki jih uporabljamo.
2. Nikoli ne izdamo svojih podatkov, kot so uporabniška imena, gesla, TRR, rojstni podatki ipd. preko elektronske pošte. Podjetja, kot so banke, spletne trgovine in tudi državne ustanove (davčna uprava, statistični urad ipd.), tega nikoli ne bodo zahtevala od nas preko elektronske pošte. Če menimo, da je elektronsko sporočilo verodostojno, raje prej pokličemo (a ne preko telefonske številke v elektronskem sporočilu), ali pa se osebno zglasimo na banki ali upravni enoti.
3. Ne klikamo na spletne povezave v elektronski pošti, tudi če le-te pridejo od nam znanih oseb (na primer elektronske čestitke, razglednice). Zlonamerna elektronska pošta je lahko poslana v imenu ljudi, ki jih poznamo, kar je pogost pojav. Pri klikanju na spletne povezave uporabimo nekaj zdrave pameti in pogledamo, kam povezava vodi. Če nas usmeri na znan strežnik, kot je na primer YouTube (prvi del naslova mora biti http://www.youtube.com/...), je na povezavo verjetno varno kliknit. Lahko so pa naslovi zelo podobni pravim, na kar moramo biti posebej pozorni.
4. Ne odpiramo priponk elektronske pošte. Predvsem to velja za namestitvene datoteke. V zadnjem času tudi video posnetki in PDF datoteke vsebujejo ranljivosti. Če dobimo na primer pripet PDF, Word ali podoben dokument, ki ga nismo pričakovali, ga lahko odpremo s spletnim pregledovalnikom (na primer Google Docs), ali pa vprašamo pošiljatelja, zakaj nam je poslal dokument.
5. Nikoli ne privolimo v posredovanje denarja. Tudi če nas prijatelj na potovanju v tuji deželi zaprosi za denar, ga vprašamo po drugih kanalih o njegovih potrebah (telefon). Pogost znak prevare je tudi, če osebo spoznamo preko spletnih strani za *parčkanje* in nas ta čez pol leta zaprosi za denar. Predvsem pa ne verjemimo sorodnikom in bančnim uslužbencem, ki bdijo nad bogastvom preminulih afriških diktatorjev. Znana so tudi sporočila o prispelih pošiljkah DHL, FedEx ipd. in če jih nismo naročili, ne privolimo v vnaprejšnje pošiljanje denarja.
6. Ne odgovarjamo in ne odpiramo spletnih povezav reklam, na katere se nismo sami prijavili. Tudi za reklamna sporočila, na katera smo se prijavili, preverimo, kam spletne povezave vodijo (glej točko 3), saj so le-ta lahko lažna. Reklamna sporočila, ki ponujajo čudežna zdravila in poceni viagro, so v 99,99 odstotkov primerov prevare.
7. Ne verjemimo raznim zadetkom na loteriji, verižnim shemam obdarovanja in zelo zanimivim poslovnim priložnostim. Tudi te so v 99,99 odstotkov primerov le prevare.
8. Ne verjemimo grozilnim sporočilom, ki na primer trdijo, da bodo ukinili naš elektronski račun, ali pa nas izbrisali iz registra državljanov, če nemudoma ne posredujemo svojih podatkov (glej točko 2).
9. Imejmo nameščeno sodobno programsko opremo z vsemi popravki in uporabljamo zaščitno programsko opremo (kot na primer Avast, MS security essentials ...).
10. Če že verjamemo nečemu v elektronski pošti, vprašajmo za nasvet, pokličimo trgovino, pobrskajmo po spletu za podobne primere ali pa za nekaj dni prestavimo odločitev!

NAPAD S SLOVARJEM

Pri napadu s slovarjem ima napadalec zelo dolg seznam besed in nizov, ki so kombinacija teh besed, števil in drugih znakov. Seznam se imenuje slovar. Za primer vzemimo seznam treh gesel: pikapolonica, heker1, 123geslo123. Nobeno od teh gesel ni preveč varno, kljub temu da so dolga in da vsebujejo črke ter števila. Gesla so ponavadi shranjena zgoščeno, kar pomeni, da se naše geslo preko zgoščevalne funkcije spremeni v zaporedje bitov predpisane dolžine (na primer geslo pikapolonica se preko zgoščevalne funkcije MD5 pretvori v c810cdeb3ad101e94ad83dd8c472892d, heker 1 v a03ccfe175bbf3b7abe94af8d99e7a12 ipd.). Pomembno je, da postopek ni dvostranski in da iz zgoščene vrednosti ne moremo dobiti nazaj gesla. Lahko pa napadalec, ki si pridobi zgoščeno geslo, zgosti vsako besedo iz seznama in jo primerja s pridobljeno zgoščeno vrednostjo. Če se zgoščena vrednost niza iz slovarja ujema z zgoščeno vrednostjo pridobljenega gesla, je napadalec odkril geslo. Gesla naj zatorej ne vsebujejo navadnih besed, imen s kombinacijo številk na koncu ali začetku.

NAPAD Z GROBO SILO (BRUTE FORCE):

Pri napadu z grobo silo napadalec poskuša zgostiti različne možne kombinacije znakov in zgoščeno vrednost primerjati s pridobljeno zgoščeno vrednostjo gesla. Tak napad je časovno precej potraten (tudi z zelo zmogljivimi računalniki) in posledično redko zanimiv. Če napadalec vzame na primer samo male črke abecede (25) in ugiba, da je geslo dolgo osem znakov, je vseh možnih kombinacij (na vsakem od osmih mest je lahko 25 različnih znakov) preko milijon. V resnici je kombinacij mnogo več: velike in male črke (50 v naši abecedi), števila (10) in ostali znaki. Gesla so lahko dolga od enega pa do poljubno mnogo znakov in razbijanje lahko traja tudi stoletja, kar ni več uporabno.