Izpostavljenost tveganjem pri uporabi medmrežja

Matej Breznik, SI-CERT, Ljubljana

Namen:
Namen prispevka je prikazati trenutno pereče grožnje in tveganja, ki ogrožajo slehernega posameznika, uporabnika medmrežja. Posamezniki so tako izpostavljeni predvsem izgubi njihove spletne identitete, njim pomembnih podatkov, nadzora nad elektronskim bančništvom, ali oškodovanjem prek pretiranega zaupanja neznancu.

Metodologija:
Opisana tveganja so delno plod lastnega raziskovalnega dela, delno pa drugih piscev, ki se ukvarjajo z enako problematiko. Izpostavljena so predvsem tveganja, za katera menim, da so še posebej pereča.

Ugotovitve:
Poznavanje obravnavanega področja, kjer se grožnje in tveganja spreminjajo dnevno, je pomembno za slehernega posameznika, saj so z vstopom informacijskih tehnologij v življenje, ti izpostavljeni nevarnostim izgube osebnega dostojanstva, kot tudi materialnega oškodovanja.

Izvirnost:
Prispevek je osnovan na podlagi dnevno beleženih groženj in tveganj, s katerimi se srečujejo posamezniki. V prispevku so obravnavana najaktualnejša tveganja. Z ugotovitijo izvora problema pa ponuja tudi smernice in rešitve.

Ključne besede: spletna tveganja, infomacijska osveščenost, socialni inženiring

1 UVOD

Problematika omrežne varnosti je prisotna od nekdaj. Z množičnim pohodom in bližanjem medmrežja slehernemu posamezniku pa je pridobila na veljavi. Priča smo približevanju medmrežja na vsakem našem koraku in s tem tudi prenosom za nas pomembnih informacij v medmrežje. Tudi oblike običajnega druženja se spreminjajo, tako dandanes posamezniki množično komunicirajo prek medmrežja. Z vsem opisanim je naša spletna identiteta, kot tudi omrežna varnost še posebej pomembna. V primeru slabe zaščite posameznika lahko zloraba privede do kraje identitete, podatkov, denarja ali celo česa hujšega.
V slovenskem prostoru se s problematiko medmrežne varnosti ukvarja nacionalni center za posredovanje pri omrežnih incidentih SI-CERT (Slovenian Computer Emergency Response Team), ki deluje pod okriljem zavoda Arnes. SI-CERT koordinira obveščanje in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji. V njegovo delovno področje spada obravnava varnostnih incidentov, tj. obvestila o zlorabah, okužbah in vdorih v računalniške sisteme. Predstavlja kontaktno točko, ki opravlja posredniško in svetovalno vlogo. V letu 2011 je pod njegovim okriljem nastal tudi projekt Varni na internetu, katerega namen je približati omrežno varnost slehernemu posamezniku. Projekt Varni na internetu, ki ga v celoti financira Ministrstvo za visoko šolstvo, znanost in tehnologijo, tako poskuša na enem mestu zbrati vsa najbolj pereča tveganja, ki v danem trenutku ogrožajo posameznika. Na spletni strani projekta je na voljo tudi enotna prijavna točka za prijavo omrežnega incidenta oziroma spletne prevare. Preko prijavne točke ima posameznik možnost brezplačno pridobiti dodatne ukrepe, ki bodo omogočili lažje reševanje njegove težave.

2 STANJE

Na posameznika glede varnosti informacij s spletnim trgovanjem in uporabo storitev elektronskega bančništva dandanes pretijo različne grožnje: od dobro znanih okužb sistema z namenom kraje podatkov ali izgube informacij ter seveda poskusi goljufij s pomočjo metod socialnega inženiringa.

2.1 Okužbe

V zadnjem času pa so posebej na pohodu okužbe posameznikovega sistema znane tudi kot t.i. drive-by-download okužbe (Naraine, 2009). O temu tipu okužb govorimo, kadar se na posameznikov sistem, ne da bi to sam želel ali vedel, sproži prenos škodljive programske opreme (t.i. malware). Potrebno se je zavedati, da ne gre le za ogroženost pri brskanju po straneh slabega slovesa. Napadalci namreč izkoriščajo zlorabljene uredniške dostope popolnoma legitimnih spletnih strani, ki jih najdemo ob običajnem brskanju oziroma jih morda celo redno obiskujemo. Z zlorabo dostopa ali prek ranljivosti nameščene spletne aplikacije napadalci na stran podtaknejo škodljivo kodo, ki se nato izvrši na sistemu nič hudega slutečega obiskovalca.
Žal pa se je navkljub skrbi uporabnika oziroma skrbnika sistema določenemu tipu ranljivosti v programski opremi le stežka izogniti; gre za t.i. zero-day ranljivosti (Paul Ducklin, 2010). V tem primeru gre za ranljivosti, ki so bile odkrite in izpostavljene javnosti oziroma zaprti skupini še preden jih je lahko proizvajalec programske opreme odpravil oziroma za njih izdal ustrezen popravek. Tako so te ranljivosti med napadalci najbolj priljubljene, saj zoper njih še ni na voljo popravek in imajo kot take tudi določeno vrednost na trgu izkoriščevalcev. Posledice okužbe uporabnikovega sistema imajo lahko različne razsežnosti. Od nedolžnega poskusa prodaje lažne protivirusne programske opreme do, v zadnjih letih vse pogostejše, kraje podatkov z okuženega sistema uporabnika. Izpostavljena so predvsem shranjena gesla na uporabnikovem sistemu (denimo gesla za dostop do elektronske pošte, različnih spletnih storitev...), kot tudi shranjeni podatki na uporabnikovem okuženem sistemu, ki omogočajo dostop do elektronskega bančništva.

2.2 Socialni inženiring

Nevarnost, ki preži na uporabnike, pa je lahko tudi bolj sociološke narave. Po mojem mnenju gre v večini primerov predvsem za stvar zaupanja. Ko govorimo o spletnih goljufijah, mislimo predvsem na goljufije, ki izkoriščajo bodisi slabo obveščenost uporabnika oziroma žrtve bodisi pretiranega zaupanja prodajalcu oziroma slepega zaupanja določeni spletni prodajalni.
Denimo, da prek elektronske pošte prejmemo ponudbo za prenos neverjetno velike količine denarja, ki ga je neznan pošiljatelj našel v Iraku, sedaj pa nas prosi za pomoč pri prenosu. V takih primerih gre za poskus t.i. nigerijske prevare oziroma prevare 419 (Slovenian Computer Emergency Response Team [SI-CERT]). V kolikor se strinjamo s prenosom, nas pošiljatelj oziroma prevarant postavlja pred nešteto majhnih ovir, za katere moramo najprej plačati sorazmerno majhne vsote denarja, kot na primer odprtje računa za prenos denarja, izdajanje različnih potrdil o izvoru denarja itd. Na ta način lahko prevarant od nas izvabi kar nekaj denarja, za nameček pa nas pri svojih dejanjih poskuša prepričati v resničnost trditev z lažnimi sporočili bank, državnih uradov, ali pa nam pošlje celo prirejeno izdajo kakšnega uglednega časopisa, ki potrjuje njegove trditve. Načini, prek katerih nas prevarant poskuša prepričati, so različni: lahko nam sporoča, da smo zadeli na loteriji (za katero mimogrede, nismo kupili niti srečke), da smo plemič, ki ga čaka zapuščina, da je kot rečeno našel veliko vsoto denarja, nas pa prosi za pomoč pri prenosu, itd. Stik z nami poskušajo prevaranti vzpostaviti na različne načine: od klasičnega načina elektronskih sporočil, do bolj naprednega načina prek spletnih oglasnikov. Prevaranti namreč zlorabijo naš kontakt v spletnih oglasnikih za navezavo stika z nami (Varni na internetu). Pri tem pa ima njihovo sporočilo tudi večjo možnost, da se prebije skozi filtre neželene pošte, saj za posredovanje svojega sporočila zlorabijo kar kontaktni obrazec spletnega oglasnika. Prevarante, ki se skozi povpraševanje najprej zanimajo za naš prodajani artikel oziroma nepremičnino, potem pa nam še mimogrede sporočajo, da imajo v posesti večjo vsoto denarja, ki bi jo, kot že prej omenjeno, želeli prenesti na varno, je zlahka prepoznati. Težje pa je recimo prepoznati primere prevar, v katerih denimo prevaranti kupujejo naš oglaševani fotoaparat za nečaka iz Nigerije. Tako nam prevarant sporoči, da se zanima za naš fotoaparat, ter da bi ga želel kupiti za svojega nečaka, ki se nahaja v Nigeriji. Običajno nam ponudi celo večji znesek od zahtevanega ter nas tako dodatno spodbudi v prodajo. Tekom prodaje nas z lažnimi sporočili spletnih bank in posrednikov, kot je na primer PayPal, poskuša pripraviti do tega, da artikel pošljemo, v zameno za sprostitev sredstev na naš račun. Na koncu smo poslali oglaševani prodajani artikel prevarantu in ostali brez plačila zanj. Enako velja za lažne spletne prodajalne, kjer nam trgovec ponuja

artikle oziroma storitve po smešno nizkih cenah. Tako bi tu izpostavil primere lažnih prodajaln letalskih kart, spletnega hotelskega rezervacijskega servisa ter prodajaln trenutno aktualnih artiklov. Lahko se zgodi, da na neki hotelski rezervacijski strani rezerviramo hotelsko nočitev, ob prihodu na kraj pa o tem nič ne vedo. V nekaterih primerih prodajalec kupcu celo izda kupljeno blago z namenom ustvarjanja zmede med uporabniki. V teh primerih je moč v spletnih klepetalnicah najti objave, tako zadovoljnih kot razočaranih kupcev, ki niso prejeli blaga. Med kupci pa se vzpostavi dialog, saj kupci, ki so prejeli blago, kar ne morejo verjeti, da ga drugi niso. V primeru nakupa blaga pa nas lahko tudi v elektronskem poštnem nabiralniku pričaka obvestilo, da je bilo blago zadržano na carini in da moramo še nekaj malega doplačati, da bo lahko odposlano naprej. Prevaranti se v večini primerov poslužujejo plačilnih servisov, kot sta na primer Western Union ali MoneyGram, saj lahko na ta način zakrijejo sledove poti denarja.

2.3 Posledice

V primeru kraje gesel lahko govorimo kot o posledici več dejavnikov:

- pretiranega zaupanja med uporabniki: ko uporabnik sam zaupa svoje geslo znancu,
- uporaba enostavnega gesla, ki ga je napadalec zlahka uganil (zelo pogosta je uporaba gesel v obliki imena in letnice rojstva),
- geslo je bilo pridobljeno kot posledica okužbe,
- geslo je bilo prestreženo pri dostopu z javnega mesta, kot posledica okužbe sistema, prek katerega smo do storitve dostopali; na okuženem sistemu se v teh primerih običajno nahaja programski prestrezovalnik oziroma beležnik tipk, t.i. keylogger (Grebennikov, 2007), ki zabeleži sleherni pritisk na okuženem sistemu,
- geslo je bilo prestreženo kot posledica uporabe javnega omrežja. Največkrat govorimo o javno dostopnih odprtih brezžičnih Wi-Fi omrežjih, kjer se naši nešifrirani podatki prenašajo v vidni obliki in jih lahko drugi uporabniki omrežja prestrežejo in zlorabijo. V nekaterih primerih pa lahko napadalec celo zlorabi odprtost omrežja z namenom preusmeritve in prestrezanja naših podatkov. V teh primerih lahko s pomočjo t.i. man-in-the-middle napada (Open Web Application Security Project [OWASP]) prisluškuje in prireja naš promet. Prirejanje prometa mu v tem primeru omogoči tudi druge napade, kot je na primer, t.i. SSL strip (Marlinspike, 2009), kjer nam prisluškovalec poskuša v primeru ogleda spletne strani prek šifrirane povezave, podtakniti spletno stran v nešifrirani obliki. V tem primeru spletno stran odšifrira napadalec sam, kar pa mu v nadaljevanju omogoča spremljanje naših aktivnosti in poslanih podatkov s tega spletnega mesta.

V primeru, da posameznik nasede zavajajoči ponudbi goljufa, ga ta lahko prepriča k nakazilom zelo velikih zneskov. Za prepričevanje žrtve goljuf uporablja različne metode: od potvorjenih sporočil uradnih ustanov, na primer bank, do potvarjanja oziroma prirejanja časopisnih izdaj, z namenom, da prepriča žrtev v pravilnost svojih lažnih trditev.

3 UKREPI

Za zaščito pred nevarnostmi z naslova okužb lahko poskrbi vsak uporabnik sam z rednim posodabljanjem protivirusne zaščite, sistema, brskalnika ter njegovih vtičnikov (t.i. plugins). Ravno brskalnikovi vtičniki so zaradi svoje dostopnosti največkrat žrtev napada Prek njih napadalec pridobi začetni vstop v naš sistem. Tako je potrebno poskrbeti, da imamo na svojem računalniku vedno nameščene zadnje različiče denimo vtičnika Adobe Flash Player kot tudi druge vtičnike. Za zaščito lahko poskrbi tudi ponudnik z rednim posodabljanjem ter ustrezno uredniško politiko. Prav tako bo v primeru vdora ponudnik načeloma lažje reševal nastalo zagato, če bo njegova spletna stran gostovala znotraj Slovenije oziroma znotraj EU. Kot kupec pa se je potrebno zavedati, da večina spletnih posrednikov ne nosi odgovornosti za morebitne zlorabe svojih oglaševalcev. Tako nam denimo pri zlorabi v večini primerov ne pomeni popolnoma nič, če smo oglas zasledili na kakšnem znanem posredniškem portalu. V izogib nevarnostim na spletu pa je nedvomno pomembno tudi, da je uporabnik na tekočem z nevarnostmi, ki prežijo nanj.

4 ZAKLJUČEK

Razširjenost medmrežja po celotnem svetu je vsekakor prinesla informacijski napredek, od katerega imamo največjo korist prav posamezniki. Možnosti komunikacije z vsakomer ter medsebojnega povezovanja so tako rekoč neomejene. Razširjenost pa prinese tudi tveganja in grožnje. Tako so v praksi prevaranti oziroma pisci zlonamerne programske opreme vedno korak pred zaščito. Z vedno novimi tehnikami prevar oziroma metod okužb, ki igrajo na osebno noto posameznika ter izkoriščajo pomanjkljivosti v posameznikovem sistemu, imajo storilci vedno znova priložnost, da namestijo škodljivo programsko opremo oziroma ob posameznikovi nevednosti iz njega iztisnejo kakšen evro.
Ob uporabi medmrežja velika večina uporabnikov meni, da uživajo enako pravno varnost kot v vsakdanjem življenju. Vendar temu velikokrat ni tako, saj ima v veliko primerih zakonodaja med posameznimi državami le nekaj stičnih točk. Tako denimo kupec, ki kupuje obutev prek spleta v tujini morebiti ne uživa enake pravne varnosti, kot bi jo v primeru, če bi čevlje kupoval prek spleta pri nas. Prav tako je problematična zakonodaja, ki obravnava storilce. V nekaterih bolj revnih državah sveta celo velja, da krasti denar oziroma ogoljufati prek spleta sploh ni sporno, saj storilec vendar jemlje denar bogatim in ga prinaša revnim, spet v drugih, kjer se spopadajo z visoko stopnjo pouličnih pobojev, pa jim tako medmrežni kriminal ne predstavlja prioritetnega problema.

VIRI

Naraine, R. (15.4.2009). Drive-by Downloads. The Web Under Siege. Pridobljeno 3.1.2012, na http://www.securelist.com/en/analysis/204792056/Drive_by_Downloads_The_Web_Under_Siege

Ducklin, P. (23.12.2010). Internet Explorer zero-day exploit - explanation and mitigation. Pridobljeno 3.1.2012, na http://nakedsecurity.sophos.com/2010/12/23/internet-explorer-zero-day-exploit-explanation-and-mitigation/

Slovenian Computer Emergency Response Team. Primeri spletnih goljufij. Pridobljeno 15.12.2011, na http://www.cert.si/varnostne-groznje/spletne-goljufije/primeri.html

Varni na internetu (3.8.2011). Goljufi vas iščejo tudi na nepremicnine.net. Pridobljeno 15.12.2011, na http://www.varninainternetu.si/2011/goljufi-vas-iscejo-tudi-na-nepremicnine-net/

Grebennikov, N. (29.3.2007). Keyloggers: How they work and how to detect them. Pridobljeno 3.1.2012, na http://www.securelist.com/en/analysis/204791931/Keyloggers_How_they_work_and_how_to_detect_them_Part_1

Open Web Application Security Project. Man-in-the-middle attack. Pridobljeno 3.1.2012, na https://www.owasp.org/index.php/Man-in-the-middle_attack

Marlinspike, M. (2009). New Tricks For Defeating SSL In Practice. Pridobljeno 15.12.2011, na http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf