Zahteve za varovanje e-bančnih storitev - izzivi varovanja

Lucija Zupan, študentka doktorskega študija, Fakulteta za varnostne vede, Univerza v Maribor
Igor Bernik, Fakulteta za varnostne vede, Univerza v Maribor

Namen prispevka:
Prispevek obravnavana primerjavo varnosti spletnih in mobilnih e-bančnih storitev. Opredeljeni so najpogosteje uporabljeni varnostni mehanizmi v e-bančništvu in uvrščeni v posamezne skupine. Opredeljene so najpogostejše grožnje spletnemu in mobilnemu bančništvu, omejeno na fizične osebe. Osvestiti in opozoriti želimo odgovorne za varnostno zaščito in strokovno javnost na tveganja na področju uporabe spletnih in mobilnih bančnih storitev, opozoriti na točke pozornosti v prihodnjem obdobju, kako se banke lahko pripravijo na prihajajoče zahteve in trende. Nakazana je tudi problematika sedanjih in bodočih varnostnih zahtev za bančne storitve iz naslova spreminjajočih se potreb in navad uporabnikov, tehnoloških trendov in zakonodajnih omejitev.

Metode:
Podan je opis priporočljivih varovalnih ukrepov e-banke, ki jih narekuje dobra praksa na podlagi deskripcije. Primerjalno so opisana tveganja in načini vdorov oz. potencialnih groženj e-banki.

Ugotovitve:
Študija prikazuje varnostne mehanizme, ki se uporabljajo v e-bančništvu, slabosti posameznih mehanizmov, kako ti varnostni mehanizmi pripomorejo k premagovanju poznanih scenarijev ogrožanja, kateri varnostni mehanizmi se uporabljajo v slovenskih e-bankah in kateri so naslednji priporočljivi koraki za dvig stopnje varnosti.

Omejitve/uporabnost raziskave:
Obravnavane bodo zahteve za varovanje obstoječih e-bančnih storitev, prispevek pa ne bo obravnaval storitev v povezavi z elektronskim denarjem, niti plačevanja blaga in storitev iz kartičnih računov.

Praktična uporabnost:
Prikazane bodo zahteve za varovanje e-bančnih storitev, ki lahko služijo kot osnova za nadaljnje ukrepe poslovnih bank in posameznikov za varnejše delo pri uporabi spletnega in mobilnega bančništva. Tako bodo podani predlogi za zagotavljanje višje stopnje varnosti in manjše možnosti uresničevanja groženj. Ugotovitve prispevka so pomembne za nadaljnji razvoj in razmišljanje snovalcev in naročnikov rešitev, ter tudi regulatorjev e-bančništva.

Izvirnost/pomembnost prispevka:
Prispevek v celoti prikazuje grožnje varnosti e-bančništva. Pomemben je prikaz groženj varnosti e-bančništva in obravnava le-teh za potrebe zagotavljanja višje stopnje varnosti pri del končnih uporabnikov.

Ključne besede: Informacijska varnost, e-bančništvo, grožnje, zaščita

1 UVOD

E-bančništvo razumemo kot tržne poti, ki strankam z različnimi informacijsko komunikacijskimi tehnologijami (IKT) omogočajo opravljanje bančnih in drugih finančnih storitev brez neposrednega stika z bančnim delavcem (Zakon o plačilnih storitvah in sistemih (ZPlaSS, 2009, 2011). Izzivi, ki ga e-

bančništvu prinašajo neprestane tehnološke spremembe, odprtost bančnega sistema (mednarodna plačila SEPA, skupna evropska valuta) in povečevanje tveganj zaradi sofisticiranih napadov, banke izzivajo k povečanju nadzora na področju zaščite e-bančnih storitev. Na drugi strani se banke srečujejo s spreminjajočimi navadami uporabnikov, ki jim uporaba spletnih storitev ne predstavlja več zadostnega udobja, svobode in učinkovitosti, temveč zaradi fleksibilnosti stremijo k uporabi bančnih rešitev od kjerkoli, kadarkoli. Generacija odraščujoča z IKT, vajena udobja komunikacijske svobode, ki jo zagotavlja stalna on-line povezava, postaja delovno aktivno prebivalstvo. Sklepamo lahko, da bo storitev preko pametnih telefonov v nekaj letih postala vsakdanjost, o čemer pričajo tudi raziskave. E-bančništvo prihaja na prvi tir.

2 UPORABA ELEKTRONSKEGA BANČNIŠTVA V EVROPI IN SLOVENIJI

V Evropi uporabnike e-bančništva lahko razdelimo v 4 skupine (Deutche bank, 2011). Prva skupina: Severna Evropa ima 62-77% uporabnikov e-bančništva. Druga skupina: Osrednja Evropa (Nemčija, Avstrija, Francija, Anglija) ima 35-54% uporabnikov e-bančništva. Amerika se z 41% uporabnikov e-bančništva prav tako uvršča v drugo skupino. Tretja skupina: Južna in vzhodna Evropa ima 32% uporabnikov e-bančništva, mednje spada tudi Slovenija. V četrto skupino uvrščamo države, kjer vzpon v uporabi e-bančništva šele pričenja (Deutche bank, 2011). Slovenija se lahko dobrih praks uči od držav osrednje Evrope (zanimivi sta predvsem Avstrija in Nemčija). V Sloveniji e-bančništvo po zadnjih podatkih MOSS vsaj mesečno uporablja 43% rednih uporabnikov spleta v starosti od 10 do 75 let (Moss, 2011) in sicer predvsem demografske skupine, ki spadajo med delovno aktivno prebivalstvo. Razlog v širokem razmahu uporabnikov je v t.i. klik generaciji, ki je praktično nedosegljiva po drugih tržnih kanalih. Slovenija primerjalno z državami Evropske Unije pri uporabi e-bančništva glede na posamezno državo celo zaostaja za 20-40%, zato se v Sloveniji v prihodnje pričakuje še nadaljnji prirast uporabnikov. Mobilno bančništvo v Sloveniji ni zelo razširjeno, glede na tuje raziskave pa je pričakovati, da bo z leti naraščalo (Deutche bank, 2011, eMarketer 2010, Nielsenwire, 2010). Pogoj za razširitev mobilnega bančništva sta razvoj in uvedba aplikacij, ki bodo podprle nabor storitev preko e-banke (eMarketer, 2010). Večina mobilnih bank na slovenskem trgu je obstoječa aplikacija e-banke prilagojena za uporabo na pametnih telefonih, tabličnih računalnikih in dlančnikih z operacijskim sistemom: Android, Apple iOS, Windows Mobile. Mobilne platforme so zaradi razmeroma nizkega števila uporabnikov in heterogenosti mobilnih platform v Sloveniji za e-bančne napadalce nezanimive, z višanjem števila uporabnikov, bo tudi motiv napadalcev narasel. V državah kjer dostopa do interneta zaradi geografskih, tehničnih in ekonomskih omejitev ni možno zagotoviti (npr. Turčija) je razmah mobilnega bančništva večji.

2.1 Relevantni scenariji zlorab e-bančništva

Seznam relevantnih scenarijev je širok, omejili se bomo le na nekatere izmed njih (Zupan, Vodopivec, 2010): manipulacija DNS pri uporabniku, kraja zasebnega ključa PKI, prestrezanje gesel, kraja seje, mož v brskalniku - Man in the browser (MItB) napad, trojanski konji in botneti, zvabljanje (angl. Pharming), ribarjenje (angl. Phishing), DNS cache poissoning v omrežju, zlonamerno pre-usmerjanje IP prometa, ponarejena ali zavajajoča strežniška digitalna potrdila, MItM napad. V nadaljevanju so zaradi razumevanja članka na kratko opisani napadi ribarjenja, zvabljanja in Mož v sredini (krat. MItB). Ribarjenje (Phishing) je eden od najpogostejših napadov v e-bančništvu (OWASP, 2011 in Symantec, 2010). V običajnem scenariju napadalec pošlje elektronsko sporočilo, ki uporabnika skuša zvabiti na lažno stran banke, pod pretvezo, da se mora zaradi preverjanja podatkov ali ponovnega aktiviranja računa prijaviti in opraviti preveritev. Mož v brskalniku (angl. man in the browser, krat. MitB) je vrsta napada, pri katerem trojanski konj okuži spletni brskalnik na način, da ta lahko spreminja spletno stran, vsebino transakcije, ali izvede plačilno transakcijo brez vednosti uporabnika. Farming ali zvabljanje

(angl.:pharming) je vrsta napada, pri katerem se v sistemu domenskih imen preusmeri uporabnika na lažno spletno mesto z namenom kraje in zlorabe uporabnikovih avtentikacijskih elementov oz. kraje identitete.

Mobilno bančništvo je zaradi relativno majhne razširjenosti uporabe manj ranljivo kot spletno bančništvo. Mobilne naprave predstavljajo posebno kategorijo na področju zlorab, ki ji poleg zgoraj opisanih grozijo še nekatere specifične vrste napadov (Zupan in Vodopivec, 2010 in MMA, 2009): napad na A5/1 šifriranje, MITM napad med bazno postajo in uporabnikom, SMishing in potvarjanje SMS sporočil, mož v mobilniku, kloniranje, ugrabitev (hijacking), zlonamerno programje, preusmerjanje glasovno ribarjenje, kraja naprave. Varnost mobilne banke je vedno potrebno obravnavati v kontekstu uporabniških navad (npr. uporaba nezaščitenih WiFi omrežij, uporabljena zaščita na nivoju operacijskega sistema itn). Mobilno bančništvo je v splošnem ranljivo na krajo naprave, zato pri izgubi ali kraji telefona velja še posebno dobro proučiti navodila banke.

2.2 Primeri napadov

V letu 2009 beležimo prelomno leto v porastu on-line kriminalnih dejanj. Škoda realiziranih on-line napadov je prvič v zgodovini presegla škodo v realnem svetu (Ždrnja, 2009). V e-bančništvu največji strah in trepet predstavljajo trojanski konji, ki jih uporabniki največkrat pridobijo z zlonamerno elektronsko pošto ali na okuženih spletnih straneh. Trojanski konji se namestijo na komitentov brskalnik, kjer (npr. s keyloggerjem) pridobivajo podatke o uporabniških imenih in geslih ter jih pošiljajo na oddaljeno lokacijo. Najbolj znan trojanski konj je ZEUS. Izvedenka Zeusa t.i. Spyeye je sposoben izvajati tudi MItB napad, kjer prevzame kontrolo nad brskalnikom, omogoča nadzor in usmerjanje prometa v omrežju, vriva HTML v sejo brskalnika in prestreza informacije, ki jih uporabnik vpiše v spletno stran (Gallagher, 2011). l.2010 se je pojavila tudi izvedenka ZEUS-a za mobilne naprave, ki je posebej načrtovana za napade na uporabnike e-bank, katerim odtuji podatke o bančnem računu in druge uporabniške podatke (Heisse Security, 2010). Ključna tarča so uporabniki pametnih telefonov. Tudi v Sloveniji v zadnjih dveh letih beležimo porast zlorab e-bančništva. V lanskem letu so predvsem odmevali phishing napadi. V l.2010 beležimo še en odmeven dogodek in sicer s trojanskim botnetom Mariposa (poimenovan po španski kriminalni organizaciji), so preko 13.000 uporabnikom odtujili uporabniška imena, gesla in druge podatke za izvedbo napada. (Slovenska policija, 2010). V letošnjem letu je bil medijsko izpostavljen predvsem primer kraje denarnih sredstev podjetju iz okolice Kranja, in sicer so napadalci s kombinacijo socialnega inženiringa in namestitvijo trojanskega konja podjetju odtujili 105.000 EUR (Slovenska policija, 2011). Dogodek je bil hitro raziskan, zlikovci pa identificirani.

3 ZAKONODAJA ZA UREDITEV VARNEGA E-BANČNIŠTVA

Evropska unija je že pred leti izdala direktivo, ki ureja medsebojno razmerje med banko in komitentom in določa način, kako se porazdeli škoda pri v primeru kraje sredstev na komitentovem računu. V Sloveniji področje varstva sredstev komitenta ureja ZPlas (Zakon o plačilnih storitvah in sistemih, 2009, 2011) , ki predpisuje odgovornost uporabnika do 150 EUR, vse kar je nad to mejo krije banka, razen, če komitentu ni dokazana huda malomarnost oz. namerna prevara. Meja med hudo malomarnostjo uporabnika in nivojem povprečnega obvladovanja informacijske tehnologije s strani uporabnika je v praksi zabrisana, presoja o tem je na strani sodišča. Banke so postavljene pred nov izziv: rešitve e-bančništva urediti na način, da te ne bodo zahtevale naprednih znanj s področja informacijske tehnologije, bodo varne in hkrati čimbolj enostavne za uporabo in vzdrževanje (npr. obnova certifikatov, postopki v primeru izgube TAN generatorja, mobilnega telefona itn). Pozor! Država predpisuje povrnitve za kraje državljanom, ne pa tudi podjetjem. Ti so prepuščeni sami sebi in so dolžni sami preverjati ali je morebiti v njihovem računu prišlo do zlorabe. Zakonodaja evropske Unije ne ponuja regulativnih podlag. »Razen v Kaliforniji ni nikjer uzakonjeno, da bi morala katera koli institucija, vključno z bankami, javno obveščati oškodovane ali objavljati zlorabe in tako vsaj osveščati svoje (poslovne) uporabnike«. (Šalamun, 2011). Poseben problem

pri učinkovitem izsledovanju kriminalnih združb predstavljajo tudi trenutne omejitve pravne ureditve v Sloveniji (Bernik in Prislan, 2010). Določeno oviro predstavljajo pravne zahteve za varstvo osebnih podatkov in zasebnosti komunikacij, ki jih morajo banke in organi pregona upoštevati.
Evropska komisija je l.2006 podprla uvedbo EMV standardov, katerih uvedba je obvezna v vseh državah EU. Več kot polovica vseh bančnih kartic v Evropi trenutno uporablja tehnologijo EMV. Prav tako je Evropska centralna banka predpisala obvezno uvedbo centraliziranega sistema za preprečevanje vseh vrst zlorab (predvsem iz naslova uvajanja SEPA v tistem obdobju). Nadaljnji možen korak EU regulative, je predpis obvezne rabe EMV CAP[1] tehnologije (oz. tehnologije, ki zagotavlja avtorizacijo transakcij), glede na trenutno razširjenost tovrstne tehnologije v evro območju.

4 VAROVALNI MEHANIZMI E-BANČNIŠTVA

Najpomembnejši člen pri varnem poslovanju z e-banko je uporabnik. Uporabnik mora poskrbeti za primerno zaščito informacijskih sredstev uporabljenih v procesu poslovanja z e-banko. Pri tem veljajo splošna navodila za boljše varovanje osebnih elektronskih identifikacijskih elementov ter računalniškega okolja: redno nameščanje varnostnih popravkov/ nadgradenj ter posodabljanje operacijskega sistema, brskalnika, antivirusne in ostale programske opreme idr. Primerna zaščita uporabnikov prestavlja v 80% primerih zmanjša verjetnost zlorab.
»Glede na določila ZPlas je pomembno, da potrošnik pri uporabi e-banke upošteva navodila banke in pozorno spremlja tudi njena obvestila o varnem poslovanju. Potrošnik mora poskrbeti za varno uporabo računalnika s primernimi zaščitnimi programi in skrbno varovati svoje identifikacijske elemente za dostop do banke. Prav tako mora takoj, ko zazna zlorabo ali sumi, da je prišlo do nje, obvestiti banko in policijo. Če tega ne stori, lahko banka zavrne povrnitev škode« (ZPS, 2010).
V splošnem varnost e-banke na strani komitenta zagotavljamo na treh segmentih:

- vzpostavitev varne povezave s pomočjo šifriranega kanala med e-banko in komitentom.
- dostop do e-banke in njenih storitev (identifikacija in avtentikacija)
- izvajanje plačnih transakcij v e-banki (avtorizacija)

Avtentikacija strežnika
Da se potrošnik lahko prepriča ali je obiskal avtentično spletno stran banke se mora banka najprej avtenticirati s strežniškim digitalnim potrdilom, na podlagi katerega brskalnik prepozna ali je spletno mesto zaupanja vredno. Tehnologija uporabnike učinkovito ščiti pred zvabljanjem in ribarjenjem.
Identifikacija in avtentikacija uporabnika
V uporabi so različne metode identifikacije (postopek prepoznavanja uporabnika pri dostopu v informacijski sistem) in avtentikacije (preverjanje istovetnosti identitete) uporabnika. npr. uporabniško ime je element identifikacije, geslo pa element avtentikacije. Povečevanje naporov v zaščito »vhodnih vrat« v e-banko učinkovito zmanjša možnost zlorab.
Avtorizacija transakcije
Varovalne mehanizme za avtorizacijo transkacij v e-bančništvu lahko delimo glede na število uporabljenih avtorizacijskih faktorjev:

- uporaba enostopenjskega avtorizacijskega faktorja (uveljavitev statičnega ali dinamičnega gesla za izvedbo avtorizacije transakcije).
- uporaba dvostopenjskega avtorizacijskega faktorja (avtorizacijski podatki za izvedbo avtorizacije transakcije so sestavljeni iz dela transakcijskih podatkov in dela avtorizacijskih podatkov). Opisani postopek (sestavljeni parameter) lahko izvedemo na več načinov:
    - za vsako transakcijo se preko neodvisnega kanala končnemu uporabniku s strani banke pošlje SMS z avtorizacijsko kodo.

[1]EMV je interoperabilna tehnologija za avtentikacijo plačil s kreditnimi katicami, ki pokriva POS terminale in bankomate za Europay, Viso in Mastercard (krat. EMV). Chip Authentication program (krat. CAP) je standard, ki je bil razvit kot podpora transakcijam preko telefona ali interneta, pri katerih ni prisotna EMV kartica.

- končni uporabnik na ločeni za napadalca nedostopni napravi (npr. čitalec pametnih kartic v katerega vstavi bančno kartico) vnese PIN in potrdi znesek transakcije. Naprava iz zneska transakcije in PIN-a generira enolično identifikacijsko številko, ki jo uporabnik vnese v spletno banko.

Bistvena lastnost dvostopenjskih avtorizacijskih faktorjev je, da je vsaka posamezna transakcija predhodno overjena in avtorizirana (npr. z vnosom sestavljenega PIN-a ali digitalnega podpisa transakcije). Druga pomembna lastnost dvostopenjske avtorizacije je, da napadalec zgolj s krajo avtentikacijskih podatkov ne more izvajati plačil, saj je geslo časovno omejeno, poleg tega za izvedbo napada potrebuje še aktivno sejo, in elemente avtorizacije (pri dvojni avtorizaciji gre običajno tudi za več uporabljenih mehanizmov, nekaj kar uporabnik ve in nekaj kar uporabnik ima) (Oesterreichische nationalbank, 2008).

V bankah zahodno evropskih držav so se v zadnjih letih razširile rešitve, ki uporabljajo t.i. EMV CAP (Chip authentication Program) tehnologijo. CAP imetnikom kartic s tehnologijo EMV in osebnim čitalnikom kartic omogoča preverjanje pristnosti storitev. Čitalnik ustvari geslo za enkratno uporabo, ki se uporabi za avtorizacijo transakcij elektronskega bančništva. V Nemčiji so rešitve dobile komercialno ime Chip TAN generatorji (Oesterreichische nationalbank, 2008). To so posebne od računalnika neodvisne naprave, v katero uporabnik po predhodnem vnosu PIN vstavi bančno (smart) kartico, napravo nato približa dinamični grafiki na zaslonu, ki napravi pošlje informacijo o znesku transakcije. V naslednjem koraku naprava zgenerira posebno TAN kodo, ki je enolično sestavljena iz osebnega PIN-a in zneska transakcije. TAN kodo uporabnik nato vnese v spletno mesto e-banke, ki predstavlja avorizacijsko kodo (Sparkasse, 2009). Tehnologija učinkovito ščiti pred MItB napadi. Znani so primeri smrtnih žrtev zaradi nepremišljene uvedbe CAP tehnologije oz. čitalcev EMV CAP, zato je potrebna preudarna raba tovrstne tehnologije (Drimer, Murdoch in Anderson, 2009). MasterCard je l. 2009 predstavil inovativno rešitev, t.i. program za preverjanje pristnosti z integriranim vezjem (angl. Chip Authentication Program oz. CAP) na mobilnih telefonih. Rešitev omogoča, da uporabnik na mobilnemu telefonu ustvari dinamično geslo (unikatni podpis za vsako transakcijo), ki je sestavljeno iz dela transakcije in PIN-a. Na mobilnih telefonih sta možna dva načina izvedbe. Pri prvi različici se dinamično geslo, s pomočjo CAP programa generira na strežniku in s sporočilom SMS pošlje imetniku kartice. Imetnik kartice pridobljeno geslo v nadaljevanju uporabi za avtorizacijo bančne transakcije. Rešitev SMS-CAP deluje na vseh mobilnih aparatih. Druga različica uporablja program, ki deluje na mobilnem telefonu in od imetnika kartice zahteva vnos osebne identifikacijske številke (PIN). Na zaslonu telefona se nato prikaže CAP geslo, ki ga uporabnik vpiše v aplikacijo mobilne banke. Ta različica deluje le na pametnih telefonih ali telefonih, združljivih s programskim jezikom Java. (Moj Mikro, 2009). Z uvedeno rešitvijo v igro varnega mobilnega bančništva konkurenčno stopajo tudi mobilni aparati. Intel je oktobra letos objavil novico, da bo IIPT (Intel Identity protection technology) čipe vgrajeval tudi na matične plošče prenosnih računalnikov (Intel, 2011).

Realizacija dvostopenjske avtorizacije transkacije je poleg uvedbe TAN generatorjev (bodisi na EMV CAP čitalcu ali mobilnem telefonu), vpeljavi potrditvenega SMS sporočila možen tudi potrditveni telefonski klic. Preverjanje transakcije po glasovnem kanalu s klicem na znano telefonsko številko uporabnika (angl. Out of band - voice channel transaction verification) zanesljivo ščiti pred MItB napadi.

4.1 Stanje v slovenskih bankah

V splošnem lahko rečemo, da slovenske banke uporabljajo različno stopnjo varnosti pri izbranih varovalnih mehanizmih e-bančništva, od uporabe statičnih gesel do naprednejših rešitev z dvostopenjsko avtorizacijo. Pri evaluaciji uporabljenih varovalnih mehanizmov v slovenskih spletnih bankah smo se omejili na rešitve fizičnih oseb in oprli na raziskavo, ki jo je opravila zveza potrošnikov Slovenije l. 2009 (ZPS, 2009) in objavljene podatke slovenskih bank na spletnih straneh. Tako smo preverili aktualnost podatkov iz ZPS raziskave in trenutno ponudbo slovenskih bank. Stanje se od leta 2009 ni bistveno spremenilo, nekatere banke so v svoje rešitve dodale dodatne varnostne elemente (npr. varnostno geslo za potrjevanje novih transakcij s pomočjo navidezne tipkovnice, možnost SMS obveščanja o transakcijah, možnost nastavitve osebnega sporočila na prvi strani, obvezna menjava vstopnega gesla vsake tri mesece,

uporaba navidezne tipkovnice za vnos vstopnega gesla). Večina bank ni izvedla bistvenih razlik pri prijavi v spletno banko ali avtorizaciji transakcij. Načine identifikacije/avtentikacije uporabnikov slovenskih bank lahko v grobem uvrstimo v tri skupine. Prva skupina uporablja uporabniška imena in generatorje naključnih števil oz. časovno omejenih gesel. Druga skupina za avtentikacijo uporablja digitalna potrdila. Ta so lahko nameščena na pametni kartici ali pa na trdem disku. Dostop do potrdila na trdem disku nadzira operacijski sistem, ki je ranljiv na vrsto napadov, zato je taka hramba zelo tvegana. Poleg tega se pri hrambi potrdila na disku generirani zasebni ključ začasno shrani v RAM, od koder ga je kasneje možno odtujiti. Tehnologija pametnih kartic in pametnih USB ključev ne dopušča izvoza zasebnega ključa, zato jo uvrščamo med bolj primerne metode. Tretja skupina uporablja dvostopenjske avtorizacijske faktorje, ki poleg avtentikacije uporabnika preverjajo tudi avtentičnost transkacije.
Glede na trenutno uporabljene kombinacije zaščite v slovenskih bankah lahko pridemo do naslednjih zaključkov :
1. V rešitvah, kjer je za avtentikacijo uporabljeno zgolj uporabniško ime in statično geslo obstaja nevarnost napadov z zvabljanjem in ribarjenjem ter nevarnost odtujitve gesel s pomočjo namenskih programov (keylogger). Zveza potrošnikov Slovenije banke, ki vstopne strani nimajo zaščitene pred ribarjenjem, poziva, da razmislijo o uvedbi zaščite z namenskimi orodji kot je VeriSign Secured Seal. Ta tehnologija potrošnikom omogoča enostavnejše preverjanje identitete e-bančnega spletnega mesta in lahko bistveno pripomore k omejitvi napadov.
2. V rešitvah, kjer se za identifikacijo uporabnika e-banke uporablja digitalno potrdilo, shranjeno na disku, obstaja nevarnost kraje potrdila z diska ali pomnilnika računalnika. Običajno se v kombinaciji z digitalnim potrdilom za avtentikacijo uporablja statično geslo, ki ga napadalec z uporabo programov za odtujitev gesel relativno enostavno pridobi. »Uporaba digitalnega potrdila sicer omogoča obrambo pred ribarjenjem in napadi tipa man in the middle, ne omogoča pa zadostne obrambe pred MItB napadi. Elektronski podpisi transakcije z digitalnimi potrdili za napadalce predstavljajo oviro, vendar ne pomagajo pri kraji certifikata in zasebnega ključa. Pri napadu MItB mora napadalec ponarediti še prikaz podatkov ob podpisu, kar je manj verjetno a ni nemogoče«. (Zupan in Vodopivec, 2010).
3. Rešitve, ki za avtentikacijo uporabnika e-banke in avtorizacijo transakcije uporabljajo dinamično geslo (TAN), ki ni povezano s transakcijo, ne zagotavljajo zadostne varnosti. »Podatki o zlorabah v tujini kažejo, da so rešitve z gesli za enkratno uporabo, ki jih lahko uporabljamo za vstop v storitev in potrditev posameznega plačila ranljivi na napad MItB. Geslo, ki je neodvisno od vsebine transakcije, napadalec lahko pridobi s tem,da nadzira uporabnikov brskalnik in zamenja le ciljni račun ter znesek transakcije« (RIS, 2010).
4. Rešitve, ki za avtentikacijo uporabnika in avtorizacijo transakcije uporabljajo dinamično geslo, generirano na od računalnika neodvisni napravi, danes predstavljajo največji nivo varnosti za uporabnika e-banke. »Proti napadom MItM in MItB se lahko zaščitimo z uvedbo mehanizma za preverjanje izvršene transakcije (plačila) na način, da je zagotovljeno načelo »sign what you see«. Še posebej je to zagotovilo pomembno pri izvajanju novih transakcij (plačevanje na nov račun)« (Moj mikro, 2010). Teh rešitev v slovenskih bankah nismo zasledili v večjem obsegu. Pomembno je tudi poudariti, da je potrebno določen varovalni mehanizem oceniti z vidika odpornosti na kombinirane grožnje in ne le posamezno. Če npr. ne zagotovimo ustrezne zaščite elementov za izvedbo avtorizacije transakcije, se pomen avtorizacije izniči.
V letu 2011 medijsko ni bilo izpostavljenih veliko zlorab spletnega ali mobilnega bančništva. Banke so se usmerile v širitev ponudbe on-line storitev z mobilnimi bankami, manj pa so se posvetile celostni prenovi obstoječih spletnih bank. Eden glavnih razlogov je zagotovo finančni vidik prenove, sprememba vseh povezanih poslovnih aplikacij, zalednih sistemov in nenazadnje tudi podpora vpeljanim novim rešitvam (Service desk). Projekt je bistveno bolj zahteven, kot izgleda na prvi pogled, zato so banke pri tovrstnih podvigih zadržane.

5 ZAKLJUČEK

V evropskem prostoru je v e-bančništvu zaznati razširjeno uporabo tehnologije za avtorizacijo transkacije. Pričakuje se lahko, da bo Evropska unija zaradi uvedbe SEPA regulativno uredila tudi področje uporabe

tehnologije v e-bančništvu, saj trenutno ni predpisanih konkretnejših smernic glede tega. Slovenske banke se kljub temu, da je tehnologija za povečanje zaščite e-bančništva (npr. avtorizacija transakcij s čitalci bančnih kartic EMV CAP, potrditvenimi SMS sporočili ali potrditvenimi telefonskimi klici) že nekaj časa na voljo, niso odzvale z množično vpeljavo. Razlog temu lahko iščemo v dejstvu, da vpeljava varovalnega mehanizma kot je CAP predstavlja znaten finančen zalogaj, saj pomeni spremembo obstoječe aplikacije e-banke, nabavo opreme za odčitavanje EMV kartic (če je izbrana ta rešitev), uvedbo klicnega centra ipd. V prihodnosti bodo slovenske banke morale poskrbeti za odpornost na najbolj značilne scenarije ogrožanja e-bank, še posebej z razširjenostjo mobilnega bančništva. Zaradi večje izpostavljenosti mobilnih naprav, bodo banke morale posvetiti pozornost zaščiti mobilnih rešitev. Slovenske banke predvsem ne smejo zaspati na lovorikah trenutnega zatišja s strani napadalcev na e-banke, ostati morajo v kondiciji s tem, da dobro zaščitijo tako interne bančne sisteme (po nekaterih napovedih naj bi bil to kronski dragulj bodočih napadov na e-bančne sisteme (Kolšek, 2011), kot tudi front-end aplikacije. Poleg tega je potrebno pri načrtovanju rešitev upoštevati tudi nova tveganja, ki se odpirajo z uvedbo mobilnih rešitev. Priložnosti za nadaljnje raziskovanje se kažejo predvsem v oblikovanju konsistentne uporabniške izkušnje, ki pogojuje dobro razumevanje potreb in navad uporabnikov, upoštevanje ranljivosti in groženj izbrani tehnologiji ter zakonodajnim omejitvam.

VIRI

Bernik, I. in Prislan, K. (2011), Informacijsko bojevanje v Sloveniji - od tradicionalno lokalnega v globalni kibernetski prostor, VARSTVOSLOVJE, 13(3), 261-279, pridobljeno 6.10.2011 na http://www.fvv.uni-mb.si/varstvoslovje/articles/VS-2011-3-03_Bernik_Prislan.pdf

Deutche bank (2011), Update on online and mobile banking, Pridobljeno 1.11.2011 na http://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD0000000000279995/Update+on+online+and+mobile+banking%3A+47%25+of+Germans+will+use+online+banking+in+2012.pdf;jsessionid=E3D65C7ECE9B35412C4FF5BDBAB9E071.srv12-dbr-de

Drimer, S., Murdoch, S.J. in Anderson R. (2009) Optimised to Fail: Card Readers for Online Banking, Pridobljeno 5.12.2011 na: http://www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf

eMarketer (2010), Mobile Banking Set to Soar, Pridobljeno 6.10.2011 na: http://www.emarketer.com/Article.aspx?R=1007686

Gallagher S. (2011), $20 banking hacks turn n00bs into financial fraudsters, pridobljeno 1.11.2011 na: http://arstechnica.com/business/news/2011/11/20-banking-hacks-turn-n00bs-into-financial-fraudsters.ars

Heisse Security (2010), Banking-Trojaner ZeuS nimmt SMS-TAN-Verfahren ins Visier, pridobljeno 5.12.2011 na: http://www.heise.de/security/meldung/Banking-Trojaner-ZeuS-nimmt-SMS-TAN-Verfahren-ins-Visier-1096613.html

Intel (2011), Access Accounts More Securely with Intel® Identity Protection Technology; pridobljeno 5.12.2011 na: http://download.intel.com/technology/security/downloads/324770.pdf

Kolšek M. (2011), How To Rob An Online Bank And Get Away With It, pridobljeno 4.1.2012 na: http://www.deepsec.net/speaker.html#PSLOT03

Moj mikro (2009), Program za preverjanje pristnosti, pridobljeno 1.11.2011 na: http://www.mojmikro.si/news/program_za_preverjanje_pristnosti

Moj mikro (2010), Kako varne so slovenske e-banke (1.del), pridobljeno 5.12.2011 na: http://www.mojmikro.si/center/povem_naglas/kako_varne_so_slovenske_e-banke

MOSS (2011): Spletno bančništvo vsaj mesečno uporablja 43% rednih uporabnikov spleta v Sloveniji , Pridobljeno 6.10.2011 na: http://www.ris.org/db/27/12174/Raziskave/Spletno_bancnistvo_vsaj_mesecno_uporablja_43_rednih_uporabnikov_spleta_v_Sloveniji/?&cat=705&p1=276&p2=285&p3=1318&p4=1357&id=1357

Mobile marketing association (2009), Mobile banking overwiev, Pridobljeno 1.11.2011 na: http://mmaglobal.com/mbankingoverview.pdf

Nielsenwire (2010): Mobile Banking in U.S. Grows 129% in Last Two Years http://blog.nielsen.com/nielsenwire/consumer/mobile-banking-in-u-s-grows-129-in-last-two-years/
Oesterreichische nationalbank (2008), Risikoanalyse eBankingangebote Östrerreichischer kredit institute, pridobljeno 6.10.2011 na: http://www.a-sit.at/pdfs/20080613_studie_sicherheit_im_e-banking_nach_feedback_durch_die_wko_tcm14-86337.pdf
OWASP (2011): What is phishing, pridobljeno 1.11.2011 na: https://www.owasp.org/index.php/Phishing#What_is_Phishing.3F
Slovenska policija (2010), Zlorabe elektronskega bančništva - opozorilo uporabnikom, pridobljeno 5.12.2011 na: http://www.policija.si/index.php/component/content/article/230-kriminaliteta/7411-zlorabe-elektronskega-bannitva-opozorilo-uporabnikom-elektronskih-bannih-storitev?tmpl=component&print=1&page=&lang=
RIS (2010) Varnost slovenskega e-bančništva je 'solidna'?, pridobljeno 1.11.2011 na: http://www.ris.org/db/26/11518/Novice/Varnost_slovenskega_e-bančništva_je_'solidna'?/?&cat=705&p1=276&p2=285&p3=1318&p4=1357&id=1357
Slovenska policija (2011): Kranjskemu podjetju s socialnim inženiringom izmaknili 105 tisoč evrov, Pridobljeno 5.12.2011 na: http://www.racunalniske-novice.com/novice/dogodki-in-obvestila/kranjskemu-podjetju-s-socialnim-inzeniringom-izmaknili-105-tisoc-evrov.html
Sparkasse (2009), Überweisung mit der chipTAN, Pridobljeno 5.12.2011 na: http://www.youtube.com/watch?v=U7PnC1S-j4I
Symantec (2010), Internet Security Threat Report, Volume 16, Pridobljeno 1.11.2011 na: http://www.symantec.com/business/threatreport/
Šalamun S. (2011), Monitor PRO, Zgodba o pobeglem drobižku, Pridobljeno 5.12.2011 na: http://www.monitorpro.si/41904/praksa/zgodba-o-pobeglem-drobizku
Zakon o plačilnih storitvah in sistemih [ZPlaSS], (2009, 2011) Ur.l. RS, št. 58/2009 , Ur.l. RS, št. 34/2010, 9/2011-ZPlaSS-B
ZPS (2010), Oškodovanje potrošnikov pri uporabi spletne banke, pridobljeno 1.11.2011 na http://www.zps.si/osebne-finance/varnost-placil/oskodovanje-potrosnikov-pri-uporabi-spletne-banke.html?Itemid=666
ZPS (2009), Varnost spletnih bank, pridobljeno 6.10.2011 na: http://www.zps.si/osebne-finance/varnost-placil/varnost-spletnih-bank.html?Itemid=666
Zupan L. in Vodopivec T. (2010) ; Vloga revizorja informacijskih sistemov pri zagotavljanju varnosti in kakovosti e-bančnih storitev, 14. Konferenca revizorjev informacijskih sistemov, Zbornik str.161-201
Ždrnja B. (2009), Napadi na Internet bankarstvo, Konferencija o hakerskim pretnjava, Pridobljeno 1.11.2011 na: http://hacking.algebra.hr/predavaci/Bojan%20%C5%BDdrnja.pptx