Datum: 7. 12. 2021

BANKART, procesiranje
plačilnih instrumentov d.o.o.,
Ljubljana

Celovška cesta 150
1000 Ljubljana
T: +386 1 583 41 71
E: dusanka.sercer@bankart.si
www.bankart.si

Zadeva: Zlorabe izvedene s prevaro imetnikov in zlorabljanje mobilnih denarnic

Spoštovani,

s strani bank smo bili obveščeni o prevarah z izvedbo močno avtenticiranih spletnih transakcij (ECI5). Značilnost teh zlorab je prevara naivnih komitentov bank oziroma imetnikov plačilnih kartic, ki so prevarantom posredovali vse svoje »osebne« in varnostne elemente/podatke, da so lahko prevaranti pridobili dostop do njihovih mobilnih denarnic ali digitalnih identitet (Rekono) in posledično izvajali potrjevanje spletnih transakcij, ki zahtevajo močno avtentikacijo.

1. Potek prevare

V okviru prevar z izvedbo močno avtenticiranih spletnih transakcij ECI5 se po do sedaj znanih podatkih pojavljata dva scenarija:

a) Prevaranti po telefonu kontaktirajo imetnika kartice in ga v sklopu pogovora prepričajo, da jim posreduje vse podatke za registracijo Rekono računa (preko Rekono OnePass aplikacije) ali registracijo mobilne denarnice, kar prevarantu v nadaljevanju daje možnost, da se močna avtentikacija spletnih transakcij izvaja preko potisnih sporočil na registrirano napravo brez nadaljnjega vedenja uporabnika.
Od imetnika prevarant pridobi *ime*, *priimek*, *datum rojstva*, *davčno številko*, *zadnjih 6 številk ene od plačilnih kartic* in *pripadajočo PIN številko*. Pri pregledanih primerih je naivni imetnik tudi potrdil (oziroma prevarantu posredoval) enkratno kodo, prejeto v obliki SMS sporočila na mobilno številko, ki jo je posredoval banki in je vezana na kartico. Enkratna koda je obvezna za uspešno registracijo v mobilno denarnico oziroma Rekono.
   - V primeru zlorabe z registracijo Rekono računa si prevarant s tem pridobi/prevzame digitalno identiteto imetnika kartice in neovirano izvaja potrjevanje spletnih transakcij, ki zahtevajo močno avtentikacijo. S popolnim dostopom do Rekono računa na ime imetnika kartice lahko v nadaljevanju tudi spremeni mobilno številko na katero se posredujejo nadaljnja enkratna gesla (OTP) in nastavijo dodatno geslo za spletne nakupe. Tako prevaranti lahko izvajajo potrjevanje spletnih plačil tudi brez mobilne aplikacije – z dodatnim geslom in OTP. V tem primeru ne gre samo za dostop do mobilne aplikacije, ampak lahko tudi za krajo (digitalne) identitete imetnika kartice, saj se lahko v spletu predstavljajo in elektronsko podpisujejo v imenu uporabnika določene dokumente (povečanje limita, sklenitev kredita, …).
   - V primeru zlorabe registracije v mobilno denarnico, prevarant prav tako pridobi možnost potrjevanja spletnih plačil preko potisnih sporočil, digitalizira pa lahko tudi vse (fizične) kartice prevarane osebe in izvaja transakcije tudi na vseh fizičnih prodajnih mestih. Tako si lahko zagotovi tudi dostop do Flik plačil in posredno sredstev na transakcijskem računu uporabnika.

b) Komitent banke prejme SMS, da mu bodo blokirali kartico, če se takoj ne prijavi na dotično spletno stran (»fishing«). Komitenti na dotični spletni strani (katere naslov in izgled je podoben kot od posamezne banke) vnesejo vse »osebne« in varnostne elemente/podatke. Prevaranti nato poskusijo narediti spletno transakcijo, ki je najverjetneje zavrnjena, saj niso mogli izvesti močne avtentikacije. Posledično ponovno pokličejo komitenta in ga prepričajo, da jim poda vse manjkajoče informacije za registracijo mobilne denarnice, s pomočjo katere prevaranti lahko avtenticirajo spletno transakcijo (oziroma digitalizirajo vse preostale kartice uporabnika). Postopek za podajanje potrebnih podatkov naivnemu komitentu predstavijo kot pogoj za deblokacijo oziroma nadaljnjo uporabo kartice.

2. Možnosti preventivnega ukrepanja in preprečevanja tovrstnih prevar

Na osnovi potrjenih zlorab, po zgoraj opisanem scenariju, smo opravili analizo iz katere je razvidno, da so bile sumljive transakcije imetnika opravljene v kratkem času po izvedbi registracije in prijave v mobilno denarnico oziroma registracijo v Rekono. Znesek zlorabljenih transakcij ponavadi bistveno odstopa od povprečnega zneska imetnikovih POS transakcij v preteklem obdobju. Na podlagi ugotovljenega smo v PRM sistemu opredelili *novo UAN pravilo »DeclineHighAmt_AfterFirstLogin«*.

Pravilo je zgrajeno na UAN profilu imetnika in se aktivira v primeru:

- Je bila v manj kot 24-ih urah od registracije v mobilno denarnico ali e-banko
- S strani imetnika izvedena POS card-not-present transakcija, pri kateri:
    - je znesek transakcije 10x večji od povprečnega zneska POS transakcije na nivoju UAN številke
    - je za imetnika na profilu posamezne uporabljene kartice oziroma PAN številke zaznan trgovec, pri katerem pred tem uporabnik ni opravil transakcije

Pravilo se trenutno izvaja le v NRT načinu procesiranja za vse banke, ki uporabljajo orodje za spremljavo zlorab PRM. Vse primere, ki so jih do sedaj identificirale banke, bi zaznalo tudi opisano pravilo. V času od 23.11. do 25.11. se je v PRM po omenjenem pravilu sprožilo preko 100 alarmov. Pravilo se lahko implementira v RT procesiranje s čimer bi bile vse transakcije, ki bi jih pravilo zaznalo, zavrnjene.

Prav tako je sumljive transakcije zaznalo novo pravilo ADAPTIVE_CARD_MODEL, sestavljeno pravilo, ki upošteva več dejavnikov tveganja v transakciji in se v proži v primeru prekoračenega izračuna stopnje tveganja transakcije (Risk Score) in se trenutno še testira na SIM okolju PRM. Pred prenosom navedenega pravila v produkcijo, kar se predvideva januarja 2022, bodo banke o tem podrobno obveščene.

V okviru preventivnega ukrepanja lahko tudi pri pošiljanju SMS OTP gesla za registracijo v mobilne denarnice, na željo banke, besedilo dopolnimo z dodatnim opozorilnim tekstom, ki bi opozarjal na ustrezno ravnanje s prejetim geslom (npr: Gesla ne delite z drugimi osebami niti, če se oseba identificira kot predstavnik banke. V primeru težave ali suma prevare se takoj obrnite na 080 XXXX BANKA) in tako morebiti naivnega uporabnika pozovemo, da ponovno premisli o posredovanju teh podatkov tretji osebi.

3. Zaključek

Če bi banke želele, zaradi preprečevanja opisanih zlorab, implementirati katero od zgoraj opisanih možnosti naj za implementacijo pravila *»DeclineHighAmt_AfterFirstLogin«* v PRM RT način, svojo zahtevo oddajo preko B2B portala. Za dopolnitev SMS OTP sporočila pa naj se banke obrnejo na skrbnike mobilnih aplikacij.

Poleg tega bi želeli izpostaviti, da je pri tovrstnih prevarah, po mnenju Bankarta, zelo pomembno ozaveščanje uporabnikov o varni uporabi in vpisovanju/posredovanju različnih podatkov, ki se jih od njih zahteva. Transakcije, ki so izvedene, so namreč po sami strukturi avtentične in jih je skoraj nemogoče ločiti od pravih, uporabnikovih, transakcij. Posledično je tudi preprečevanje s spremljanjem tovrstnih transakcij delno učinkovito in ima vpliv tudi na dejanske komitente banke.

Lep pozdrav!
Duša Corl Šercer