Euroopa kriminaalpreventsiooni võrgustik

EUCPN töövahendite seeria

Nr 13

Individuaalsete pettuste ennetamine

Lühikokkuvõte

EUCPN-i sekretariaadi avaldatud seeria 13. töövahendite komplekt keskendub *individuaalsete pettuste ennetamisele.* Eesistujariik Bulgaaria (2018. aasta esimene pool) otsustas keskenduda järgmisele:

"[…] *pettusega seotud küsimused, eelkõige telefonipettused. Seda liiki kuritegevus on viimastel aastatel muutunud tulutoovaks tegevuseks, mis areneb nii riiklikul kui ka piiriülesel tasandil. Sellele tegevusele spetsialiseerunud kuritegelikud rühmitused arenevad dünaamiliselt ja ründavad laiemat valikut ohvreid. Arvestades ohvrite aktiivset osalemist kriminaalsetes stsenaariumides ja nende heauskset pühendumust neile stsenaariumidele ning traumeerivat mõju ohvrite hingeseisundile, tuleb teha tõsiseid ennetavaid jõupingutusi, võttes arvesse kohaliku, riikliku ja piiriülese tasandi eripärasid."*

Individuaalne pettus on pettuse liik, kus kurjategijad petavad tavalisi üksikisikuid. Ohvrid veendakse koostöösse ja pärast seda neid petetakse. Meie praegune arusaam seda tüüpi pettusest on peamiselt seotud selle kaasaegsete vormidega, kusjuures kõige tõenäolisem näide on andmepüük (phishing). Samas on oluline mõista, et individuaalsed pettused on olemas olnud juba pikka aega. Viimaste aastakümnete tehnoloogilised arengud on vaid võimaldanud neid pettusi suuremas ulatuses korraldada, kui kunagi võimalikuks peetud. Kes poleks kunagi elus saanud andmepüügi e-kirja?

Nagu selgub Bulgaaria eesistumise *põhjendusest*, osalevad ohvrid aktiivselt nende ohvristamises. Kurjategija on seadnud sihiks ohvri raha, kuid ta saab sellele ligi vaid siis, kui veenab ohvrit seda tegema. Põhilist taktikat ohvri suunamiseks sellisesse nõustuvasse suhtesse

nimetatakse **manipuleerimisründeks**. See võimaldab kurjategijal tekitada ohvris kindlustunde, mis on pettuse edukuse seisukohalt üliioluline. Sotsiaalpsühholoogia võimaldab meil seda nähtust paremini mõista. Viidates igapäevastele sotsiaalsetele põhimõtetele ja kasutades seda „inimlikku nõrkust", on rikkujad võimelised aktiviseerima midagi, mida nimetatakse „teiseseks veenmisteeks". Esimene tee nõuab palju mõtlemist ja kognitiivset pingutust. Teine aga ei vaja tegelikku täpsustamist ja reageerib peaaegu alateadlikult. Näiteks teeseldes, et ta on mõni autoriteetne isik nagu politseinik, võib kurjategija kergesti saavutada oma ohvrite kuulekuse. Neil sotsiaalsetel ja kognitiivsetel rusikareeglitel on oma igapäevased rakendused, kuid õigusrikkujad saavad neid oma hüvanguks ära kasutada.

Neid petturlikke taktikaid kasutatakse laias **valikus pettustes**. *419 pettused, vanaema pettused, romantikapettused, tegevjuhi pettused…* võimalused on sama lõputud kui petturite kujutlusvõime. See petuskeemide arvukus võimaldab petturitel rünnata korraga väga suurt osa avalikkusest või võtta kasutusele kitsamalt kohandatud lähenemisviis. Üha enam tundub, et rakendatakse seda viimast. Petturid on jõudnud arusaamisele, et ohvrite kavalalt ründamisega on nende „investeeringu tasuvus" suurem. Andmepüügimeilid muutuvad üha keerukamaks ja on suunatud väljavalitud sihtmärgile (rühmale). Üllatav viimane samm selles evolutsioonis kätkeb endas uue ja vanema tehnoloogia kombinatsiooni: telefoni. Häälkõnega andmepüük (vishing) annab võimaluse kombineerida nii interneti kui ka telefoni eeliseid. Internetipõhise telefonikõne tegemisel ei ole peaaegu mingeid kulusid, seda on raskem jälitada ja seda saab teha automatiseeritult. Telefoni kasutamisel on veelgi eeliseid: inimesed usaldavad seda rohkem ja intiimsema õhkkonna tõttu saab ohvreid tõhusamalt veenda. Illustreeriv näide kasvavast rafineeritusest: kurjategijad palkavad isegi emakeelseid kõnelejaid, et telefonikõned tunduksid võimalikult ehtsana.

Samas on meie praegune arusaam individuaalsest pettusest siiski piiratud. Selle kuriteoga seondub tohutu **tundmatu arv**, sest väga palju neist pettustest jäävad teatamata. Ohvrid ei tea, et nad on ohvriks langenud, nad ei taju seda piisavalt rängana, nad ei usu, et teatamine viib kuhugi, või nad lihtsalt ei tea, kuhu üldse teatada. Ja veel: kuna ohvril on aktiivne roll tema enda ohvristamises, siis tekivad tal enesesüüdistamine ja piinlikkus, mis takistavad ohvril oma lugu rääkida. Mõnedel pettustel on isegi „sisseehitatud" teatamisvastased mehhanismid, kus ohvrid peavad tegema skeemis midagi ebaseaduslikku, inkrimineerides end selle käigus. Pettusest teatamine tundub iseenda ülesandmisena.

See tundmatu arv on andnud tõuke ka **müüdile**, et eakad on selle kuriteo peamised ohvrid, kuna nad on kerge saak. Mõned uuringud on tõestanud vastupidist, kuigi tuleks olla ettevaatlik, kuna tehtud on vaid piiratud uurimistööd. Sellest hoolimata on teatatud, et noorem elanikkond ja keskealine rühm on petturitele vastuvõtlikumad. Veel üks müüt, mis eksisteerib, on see, et ohvreid kujutatakse tavaliselt hariduseta või finantsiliselt kirjaoskamatutena, kuid tõde tundub olevat vastupidine. Üht võimalikku selgitust nimetatakse „teadmise ja tegemise lüngaks": inimesed tunnevad edukalt ära petuskeemi märgid, kuid ei suuda seda teadmist enda olukorrale rakendada.

Kahjuks ei ole nn **„lollide nimekirjad"** müüt. Telefonipetturid leiavad oma ohvrid juhusliku valikuna või avalikke registreid vaadates, kuid nad jagavad ka omavahel nimekirju juba petetud ohvritest. Selliste nimekirjade kasutamine näitab korduva ohvriks langemise kõrget taset. Näiteks proovivad mõned petturid „aidata" teil kaotatud vara tagasi saada…

Kuna selle kuriteo toimepanemist on äärmiselt raske tuvastada, on vajadus ennetamise järele suur. Siiski on individuaalsete pettuste kohta läbi viidud vähe akadeemilisi ja hindavaid uurimusi. Sellest hoolimata võime ära tuua mõned üldised leiud. Levinuim ennetustaktika on avalikkuse harimine. Seda võib teha üldises teadlikkuse tõstmise kampaanias, kuid eriti on sellel märgata mõningaid positiivseid mõjusid, kui see antakse edasi mingis koolitusvormis. Sisuliselt püüavad need koolitused täita eelnimetatud „teadmise ja tegemise lünka". Teine võtmetaktika on töötada ohvritega. Nende aktiivse rolli ja mitmekordse ohvristumise ohu tõttu tuleks ohvreid toetada ja teavitada neid nende spetsiifilisest positsioonist.

Bulgaaria eesistumise ajal kogus sekretariaat selle teema kohta mitmeid **häid praktikaid**. Neid saab liigitada vastavalt sihtgrupile. Esimene kategooria keskendub kogu elanikkonnale. Need on teadlikkuse tõstmise kampaaniad, nagu näited Bulgaariast, Rootsist, Belgiast või Europolist. Need hõlmavad raadioesinemisi, plakateid, flaiereid, vidinaid jne, mis annavad avalikkusele kasulikku teavet ja näitavad, kuidas kaitsta end kahjustamise eest. Teine tegevuste kogum on suunatud eakatele. Siin kasutatakse rohkem interaktiivseid meetodeid, nagu Tšehhi Vabariigi juhtumil. Eakad osalevad interaktiivses harivas näidendis, kus nad õpivad tundma kõige tavalisemaid petuskeeme ja seda, kuidas neile reageerida. See „läbielatud kogemus" peaks võimaldama neil reaalelu stsenaariumides adekvaatselt reageerida. Selle projekti hindamine tõestas, et see oletus on tõsi, sest antud grupp keeldus võltstehingutest kaks ja pool korda rohkem kui kontrollgrupp, kes ei vaadanud näidendit. Ja viimane ennetustegevuste kategooria keskendub ohvritele. Näited Austraaliast,

Ühendkuningriigist ja Kanadast näitasid vajadust seda tüüpi ennetuse järele. Siiski on – isegi ülemaailmselt – vähe individuaalsete pettuste ohvritele mõeldud tugiteenuseid.

Lõpuks korraldas EUCPN-i sekretariaat erinevate ekspertidega töötoa, et koostada mõned **soovitused**, kuidas telefonipettusi vältida. Need on struktureeritud vastavalt kuritegevuse ennetamise viiele strateegiale. Esimene võimalik strateegia on suurendada pingutusi, mida kurjategija peab tegema, et pettus õnnestuks. Telefoninumbrite avaldamise ja neile juurdepääsu piiramine suudab seda juba saavutada. Teine meetod võib olla piirata telefoninumbrite hulka, mida ühel isikul on lubatud omada, või vähemalt siduda see pangakonto või ID-koodiga.

Teine strateegia on suurendada riske. Siin on olulise tähtsusega teabe jagamine. Selline jagamine ei tohiks peatuda avaliku või erasektori piiridel ega riigipiiridel. Kõigil partneritel on oluline infomõistatuse pusletükk. Teadmine, millega on tegemist, suurendab võimalust selle toimumine üldse ära hoida. Pole vast vaja öeldagi, et aruandlus tuleks muuta lihtsamaks ja kättesaadavamaks. Teavet tuleb koguda, enne kui seda saab jagada. Tehti ka muid soovitusi, nt helistaja anonüümsuse vähendamiseks, muutes helistaja asukoha varjamise peaaegu võimatuks. Ka hääletuvastustarkvara võiks siin huvi pakkuda.

Selle kuriteo toimepanemisega saadavate tulude vähendamine on kolmas strateegia telefonipettuste ennetamiseks. Siin on peamine soovitus ebaseaduslikult saadud varade konfiskeerimine. Selleks on määrava tähtsusega raha liikumise jälgimine, et tuvastada kahtlased tehingud. Meie eksperdid soovitasid selle hõlbustamiseks kogu EL-i hõlmavat algatust koostöös pangandussektoriga.

Veel üks strateegia on kiusatuste vähendamine. Sellega seoses on tähtis mitte jagada liiga palju teavet selle kohta, kuidas pettus tegelikult teostati, takistamaks jäljendajaid. Lisaks võib see aidata ära hoida mõningaid korduva ohvristamise vorme. Ja viimane strateegia oli kõrvaldada vabandused. See keskendub peamiselt teadlikkuse tõstmisele telefonipettuste kohta ja selle kohta, kuidas ennast kaitsta. Siin on peamisteks näideteks eelpool toodud head praktikad. Teadlikkuse tõstmise kampaaniad peaksid levitama sama sõnumit. Seetõttu tuleb avaliku ja erasektori partnerlused ja rahvusvaheline koostöö luua selliselt, et see oleks võimalikult järjepidev: *lihtsalt ütle „ei“.*