# Lihtsalt küsi, ehk turvaründed ilma arvutita

Kaido Kikkas

(Algselt avaldatud ajakirjas "30 pluss" aprillis 2016, siin ilmub kokkuleppel toimetusega)

*"Aktiveeri oma rikkusekolle ükskõik millises rahvarohkes ruumis, vehkides seal tohutu kööginoa ja sildiga, kuhu on kirjutatud "Andke kõik oma raha mulle"." - Rohan Candappa, "Väike Tüng Shui käsiraamat"*

Kui senikirjutatud lugudes on läbivaks jooneks arvutis toimuva turvamine selle eri aspektides, siis seekord räägime teemast, mida inglise keeles iseloomustab termin *no tech hacking.* Tegemist on turvarünnetega, mille lõppsihtmärgiks on sageli samuti IT-lahendused, kuid ründevektoriks on taas kord "tihend klaviatuuri ja tooli vahel" ehk inimene (lisaks aga kasutatakse oskuslikult ära ka ümbritsevat keskkonda).

## Kevin: arvutiga ja ilma

Üheksakümnendatel aastatel tekitas USA-s palju kõneainet mees nimega Kevin Mitnick, keda massimeedia nimetas "kõige ohtlikumaks häkkeriks maailmas" ja kellele USA võimud mitu aastat tulutult klaperjahti pidasid. Mitnick tundis arvutiasjandust kahtlemata hästi, ent teadaolevalt tegi ta suure osa enda tuntumatest "vägitegudest" just selsamal mittetehnilisel viisil - kas otsesuhtluse või telefoni kaudu (ja seda ka ajal, mil ta oli üle riigi tagaotsitav). Näiteks kasutas ta "omainimesena" esinemiseks (nagu eelnevast mäletame, on usalduse tekitamine igasuguse pettuse vundamendiks) telefonikõne ajal vestluskaaslase ootele panekut - sel ajal mängis telefonis (muidugi eelnevalt samamoodi telefonist lindistatud) taustamuusika, mis aitas veenda teisel pool olijat, et helistatakse tõepoolest samast ettevõttest.

Kevini meisterlikkusest annab tunnistust ka asjaolu, et ta suutis 1994. aastal üleriigiliselt tagaotsitavana pääseda Eric Weissi nime all aastaks assistendina tööle Denveri advokaadifirmasse Holme, Roberts & Owen. Muuseas, Eric Weiss (täpsemalt küll Erik Weisz) oli laiemalt Houdinina tuntud kuulsa mustkunstniku kodanikunimi...

## Sotsiaalne mõjutamine

Kevin Mitnick on oma raamatus "The Art of Deception" kirjeldanud sotsiaalset mõjutamist vabas tõlkes umbes järgmiselt: see on inimeste veenmine, mõjutamine ja eksitamine uskuma, et mõjutaja on keegi teine kui ta tegelikult on, samuti nendega manipuleerimine. Selle tulemusena suudab pettur kasutada neid soovitava info kättesaamiseks, kusjuures tehnoloogia kasutamine selleks ei ole oluline.

Siin on paar tähelepanuväärset punkti:
* identiteet - mõjutaja peab esimese sammuna tekitama usalduse ning selleks peab ta esinema isikuna, keda ohver kas isiklikult või enda rollist (töö, kool...) tulenevalt usaldab.
* manipuleerimine - selleks kasutatakse tervet psühholoogiliste nõksude arsenali. Christopher Hadnagy mainib enda raamatus näidetena ära vastasmõju ("mina sulle, sina mulle" - manipuleerija "annab midagi ära", tekitab võlatunde ning kasseerib lõpuks midagi olulist vastuteenena sisse), kohusetundele rõhumine ("mis politseinik sa oled, kui sa..."), piiratud võimalused ("otsusta kiiresti, pakkumine aegub tunni aja pärast!") ja mitmed teised.

* soovitav info - selle kättesaamine võib toimuda nii ühekorraga kui astmeliselt. Päriselu juhtumites on levinum just viimane - esmalt küsitakse mõnd vähemtähtsat detaili, mille teadmine aga annab petturile võimaluse esineda mõne tähtsama infotüki valdaja ees kas autoriteetse isiku või siis (taas kord) omainimesena.
* tehnoloogia - selle kasutamine ja tase (kõrgtehnoloogia nagu IT ja elektroonika *contra* madal nagu tabalukud, turvauksed jms) võib sedalaadi skeemides kõvasti varieeruda.

## Kasulikud oskused

Lisaks heale suuvärgile ja kiirele reaktsioonile on olemas veel mõned võtted, mida selles vallas palju kasutatakse:
* Prügistuhnimine (*dumpster diving*) - sihikule võetakse prügi: nii töölaudade alused paberikorvid kui suuremad prügikonteinerid. Paberikorvidest võib leida kollaseid lipikuid PIN-koodide ja paroolidega, konteineritest aga märksa pirakamat saaki (laisk ametnik eelistas mitte seista paberihundi järjekorras ja viskas kogu eelmise aasta arvetekogumi lihtsalt prügikasti). Kui prügikonteineri juurde võib pääseda vahel lihtsalt tänavalt, siis kabinettide paberikorvide kättesaamine vajab sageli mõne teise tehnika appivõtmist. See-eest võib hea õnne korral olla saagiks ka paber märkega "Ametkondlikuks kasutamiseks" või koguni "Riigisaladus" (see ei ole fantaasia - sarnaseid juhtumeid on teada piisavalt).
* Üleõlapiilumine (*shoulder surfing*) - see tähendab sageli lihtsalt õiges kohas seismist (enamasti ohvri selja taga) ning soovitava info kättesaamist vaatluse teel. Infoks võib olla ukse numberluku kood, tahvelarvuti või nutiseadme PIN või sisenemismuster, arvuti parool või vahel ka otse kuvarilt mahaloetav tundliku sisuga teave. Lisaks konkreetsetes sihtmärkidest asukohtadele (kuhu ründaja soovib sisse pääseda) on juhusliku üleõlapiilumise jaoks väga viljakad jahimaad näiteks lennujaamad, aga ka kõikvõimalikud ooteruumid, kohvikud jne. Klassikalise sihtmärgi näitena võime ette kujutada lennujaamas lendu ootavat ülikonnastatud härrasmeest, kelle lahtise sülearvuti kaanel ilutseb kaugele nähtav kleeps "Kaitsepolitsei"...
* Sappavõtmine (*tailgating*) - sarnaneb eelmisega, kuid on eeskätt mõeldud kinnistest ustest sissepääsemiseks. Väga paljude tähtsate paikade uksed sulguvad küll vedru jõul ise, kuid tihtipeale on sulgumine aeglane: keegi ei taha saada jama kaela ukse vahele jäänud kaastöötaja või ka lihtsalt häälekalt kinniprantsatava ukse tõttu. See meetod kasutab ära inimloomuse üht nõrka kohta - enamik inimesi on kasvatatud viisakateks ning teise nina ees ukse kinnilöömine ei tundu just ilus (isegi siis, kui on tegu Eriti Tähtsa Uksega, kust võõrad ei tohi läbi pääseda). Nii antaksegi uks kenasti tagaliikujale üle - eriti veel siis, kui too kannab kaelas või rinnas midagi kohalikku töötõendit meenutavat ja seisis suitsu tehes juba enne selle ukse taga.

Ülalmainitud kolme tehnika edu võtmeks on suutlikkus jätta endast "ma kuulun siia"-mulje. Ühe hea näitena räägitakse lugu algajast lennuturbespetsist, kellele juhendaja andis õppeülesandeks paigaldada reisilennuki Wi-Fi ruuterisse "pealtkuulamisseade" - ja seda reisi ajal, kogu meeskonna ja reisijate kohal viibides! Õnnetu praktikant jõudis juba võimatu missiooni peale ahastusse minna, viimaks aga tõmbas juhendaja kotist välja "nähtamatuks tegeva riietuse". Selleks oli tavaline töömehe helkurvest... Ja nagu arvata oli, ei äratanud lennuki elektroonika kallal toimetav kollase vesti kandja kohapeal kelleski kahtlust (sest kõik jäi ju kenasti tööle!).

## Saulusest sai Paulus

Märkus: kui keegi lugejaist peaks mõlgutama mõtet ise "inimhinge inseneriks" hakata, siis igaks juhuks olgu öeldud, et ka Mitnick kukkus lõpuks kinni. Tänaseks on ta juba mõnda aega vangist väljas, on poolt vahetanud ning tegutseb sestsaati edukalt turvanõustajana.

Nõustaja Mitnick on aga pakkunud ühe väga hea valemi andmeturbe tarvis. See on kombinatsioon tehnoloogiast (tulemüürid, lukud, paroolid...), koolitusest (ehk personali oskusest pahalasi ja nende levinumaid skeeme ära tunda) ning reeglistikust (näiteks iivelduseni korratud ja ikka veel vahel eiratav manitsus "sina ei pea enda parooli mitte üles kirjutama ja kuvari külge kleepima" - kui see lisada ettevõtte sisekorraeeskirjadesse ning selle vastu eksimine võib tähendada töökoha kaotust, jõuab see inimestele märksa paremini kohale). Mistahes komponendi unarussejätmine tähendab lahjat lõpptulemust (nagu korrutis matemaatikas: kui üks teguritest on null või väga väike, on seda ka tulemus). Seetõttu tuleks erinevatel turvalisuse eest seisjatel pöörata võrdväärset tähelepanu kõigile kolmele.

## Kokkuvõtteks

Mõned soovitused:
* Ehkki mõned peavad rumalust ainsaks lõputuks asjaks maailmas, tasub sellega ometi võidelda ning vähemalt püüda inimesi harida ja informeerida. See kehtib ka turvalisuse osas - personali pidev teavitamine ja koolitamine võib olla küll kulukas, kuid see on tõenäoliselt odavam, kui mõne uue Kevini tegevuse tagajärjed.
* Asutustes ja ettevõtetes peaks olema väga selgelt kirja pandud keelatud tegevuste loetelu, mis võiks olla kõikidel väljapoole suhtlevate töötajate (müügiesindajad, tellerid...) jaoks silma all. Näiteks "seda-ja-seda telefoni/mobiili/e-kirja/Skype'i teel edastada ei tohi".
* Kehva tehnilise varustusega tark inimene on raudselt üle hästivarustatud lollist, kuid parim lahendus oleks anda inimesele nii varustus kui teadmised.  Seetõttu tasub ka turvatehnika osas ajaga kaasas käia.
* Füüsiline töökeskkond tasuks eespoolkirjeldatud võtteid arvestades üle vaadata. Välisuksed (sh tagauksed ja kaubalaadimissillad), koodisisestuspuldid jne. Ka tuleks olla mõnel juhul olla ettevaatlik inventarile kleebitavate siltidega (vt sülearvutinäidet eespool).
* Võimaluste piires tasub alati tutvustada töötajatele mujal asutuses/ettevõttes töötajaid ja seal toimuvat. Kui näiteks turundusjuht teab, et firma serverid töötavad OpenBSD peal, siis "IT osakonnast" sissetulev kõne teemal "Meie Windowsi server läks katki, peame teie turundusinfo ümber tõstma ja selleks on parooli vaja" peaks tal punase lambikese veidi lihtsamini põlema lööma.
* Kõige kergem saak manipulaatorile on frustreeritud töötaja. Seepärast on oluline ka hea tööõhkkonna säilitamine.

Lisalugemiseks huvilistele soovitaks seekord Johnny Longi raamatut "No Tech Hacking: A Guide to Social Engineering, Dumpster Diving and Shoulder Surfing", Christopher Hadnagy "Social Engineering: The Art of Human Hacking" ning juba eespool tutvustatud Kevin Mitnicki raamatuid (eriti "The Art of Deception: Controlling the Human Element of Security").

... ja tegelikult on ka motos kasutatud Tüng Shui raamat hea lugemine. :)