# Sotsiaalvõrgustikud ja sotsiaalsed manipulatsioonid

TPK2012
Kaido Kikkas

# Üks lollakas tsitaat

- “LIHTSALT KÜSI: aktiveeri oma rikkuse-kolle ükskõik millises rahvarohkes kohas, vehkides seal tohutu kööginoa ja sildiga, kuhu on kirjutatud “ANDKE KÕIK OMA RAHA MULLE!” - Rohan Candappa, “Tüng Shui käsiraamat”

# Näide

- Osakonna raamatupidaja tädi Maalile helistab „Martin Meri siseauditi osakonnast“. Küsib järjekorras selliseid küsimusi:
  - Mitu töötajat on teie osakonnas?
  - Kui palju on kõrgharidusega töötajaid?
  - Kui tihti korraldatakse osakonnas täienduskoolitusi?
  - Mis on osakonna personalikulude kontonumber raamatupidamises?
  - Mitu töötajat on lahkunud viimase aasta jooksul?
  - Milline on osakonna üldine tööõhkkond?
- Mis siin valesti on...?

# Veel üks

- Vajalik varustus: vana mobla + kõnekaart
- 1. kõne: firma raamatupidamisse hr. Sepale; tutvustada end IT-tugiisikuna ja küsida, kas kõik on ikka korras ja jätta „igaks juhuks“ oma telefon. Muu hulgas küsida ka võrgukaabli pesa numbrit
- 2. kõne: firma IT-osakonda. Jätta mulje, et räägitakse „hr. Sepa kontorist“ ja paluda konkreetse numbriga kaablipesa välja lülitada
- Oodata, kuni hr. Sepp paanikasse läheb ja „tugiisikule“ oma probleemiga helistab

# ...

- Tunnikese pärast on asi korras – muidugi tuleb helistada vahepeal uuesti IT-osakonda ja paluda ühendus sisse lülitada
- „Et seda enam ei juhtuks“, paluda hr. Sepal alla laadida üks programm ja käima panna. See ei tee midagi nähtavat – vabandada, et „oih, ei tööta“ ja paluda allalaetu kustutada
- Korras: sniffer/rootkit/trooja hobune on paigas
- (Telefon pärast prügikasti - muidugi enne teha ilusti igas mõttes puhtaks)

# *Social engineering*

- Erinevates teadusharudes erinev tähendus:
  - Sotsioloogias mõeldakse siin sekkumist sotsiaalsetesse protsessidesse (neutraalne või isegi positiivne termin)
  - Politoloogias mõistetakse selle all suurte inimrühmade mõjutamise kunsti (eeskätt meedia, aga ka seadusandluse, maksunduse jm kaudu)
  - Andmeturbes peetakse eeskätt silmas identiteediga manipuleerimist – manipulaator veenab ohvrit selles, et ta on keegi teine

# Mitnick útleb:

- *Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology* (The Art of Deception)

- “I realized one day while riding the bus that the security of the bus transfer I had purchased relied on the unusual pattern of the paper-punch, that the drivers used to mark day; time, and route on the transfer slips. A friendly driver, answering my carefully planted question, told me where to buy that special type of punch. The transfers are meant to let you change buses and continue a journey to your destination, but I worked out how to use them to travel anywhere I wanted to go for free.

  Obtaining blank transfers was a walk in the park. The trash bins at the bus terminals were always filled with only-partly used books of transfers that the drivers tossed away at the end of the shifts. With a pad of blanks and the punch, I could mark my own transfers and travel anywhere that L.A. buses went. Before long, I had all but memorized the bus schedules of the entire system.

  (This was an early example of my surprising memory for certain types of information; I can still, today, remember phone numbers, passwords, and other seemingly trivial details as far back as my childhood.)” - The Art of Deception

# Stanley Mark Rifkin

- Miskipärast on seda nimetatud suurimaks arvutikuriteoks – arvutit aga eriti ei kasutatudki:
  - Sai teada päeva ülekandekoodi (Stan tegi Martinit!)
  - Tegi 10,2 MUSD ülekande Šveitsi
  - Lendas sinna ja ostis 8,3M eest Rosalmazist teemante
  - Lendas tagasi ja smugeldas läbi tolli USAsse
  - (jäi vahele müüa üritades, kuna diiler andis üles)

(http://www.edwardjayepstein.com/diamond/chap20.htm)

# Mugu-baiting

- Veebis leviv vastuoluline “spordiala”
- Põhiidee: vastatakse mõne “Dr Mobutu” kirjale, mängitakse lolli valget meest (stiilipunkte annab endale võimalikult napaka nime väljamõtlemine nagu Gerald Womo Milton Glockenspiel) ja üritatakse seejärel õnnetu “ettevõtja” igasuguseid huvitavaid asju tegema panna
- Parimad pojad on saanud ise raha või lennutanud nigeerlase tema enda kulul New Yorki kohtuma
- Vt näiteks www.whatsthebloodypoint.com, www.419eater.com või www.scamorama.com

# Web 2.0

- Üldiselt väga hea asi:
  - Suured koostööprojektid (Linux, Wikipedia jpm)
  - Meediaväljund palju rohkematele inimestele (sh erinevad vähemusgrupid)
  - Võimalus tunduvalt suurendada senist suhetevõrgustikku
- Viimasest paraku tuleb ka üksjagu ohte

# Paar lihtsat näidet

- MSN: omg is this you lol? [URL]
- Facebook: You look just awesome in this new movie! [video]

- Märkus: natuke aitab siin mitteinglise emakeel – ehkki üllatavalt tihti ei jaga ka maarahva seast pärit MSNi kasutajad ära, et omamaine sõber hakkas just miskipärast temaga ameerika keeles rääkima...

# Põhiline probleem

- Igasuguse manipulatsiooni esimene etapp on ohvri usalduse tekitamine
- Tänastes sotsiaalvõrgustikes on see samm juba tehtud
- Gazzag.com 2006 - hiljem kasutavad samalaadseid asju ka teised (Netlog, hi5 jne)

# Mida annab teha

- "Turvalisus tuleb tehnoloogia, väljaõppe ja protseduurireeglite kaudu" – Kevin Mitnick
- Isiklik Facebooki eeskiri ei ole halb mõte
- Kuhu pannakse sõbraks kinnitamise piir:
  - Ainult vähesed ja valitud, päris õiged sõbrad
  - Inimesed, keda ma päriselus tunnen
  - Igaüks, kes selleks soovi avaldab
- Vastavalt sellele tuleb ka sõbralistist tulevat filtreerida!

# Võrdluseks: SANSi soovitused ettevõttele

- Baastase: üldine turvapoliitika, mis arvestab ka manipulatsiooniürituste võimalikkust
- Perimeetritase: kogu personali üldine turvakoolitus (sh kahtlase päringu äratundmine)
- Kindlusetase: vastumeetmete õpetamine võtmeisikutele
- Püsivustase: pidev meeldetuletamine
- Häiretase: “maamiinide” kasutamine eri tasandeil
- Tegevusetase: juhtumitele reageerimine

# Mõned “pähetaotavad” asjad

- Andmed ja info on väärtuslikud
- Sõbrad pole alati sõbrad (jälle!)
- Paroole ei anta edasi
- Suled ei tee lindu ehk munder ei tee spetsialisti (iga patsi/habet ja kampsunit kandev ning mälupulgaga vehkiv kodanik pole firma itimees)

# “Maamiinid”

- Erinevad meetodid, mis on võimelised manipulatsiooniprotsessi eri etappidel häiret andma:
  - Koosseisuline nuhk Albert – kodanik, kel on loomulik kalduvus kõike teada, mida on täiendatud koolitusega manipulatsioonide osas
  - Jagatud logimine – päringud registreeritakse nii, et neid näeb koheselt mitu inimest
  - Tagasihelistamispoliitika – ei anta numbreid välja, vaid palutakse numbrit, kuhu helistada
  - Ootele panek – närvidel mängimine
  - Kontrollküsimused (sh ka võltsküsimused)

# Kokkuvõtteks

- Usaldus kui võtmetegur
- Sotsiaalseid manipulatsioone esineb ühiskonna kõigil tasanditel (poliitika, äri, meedia, eraelu...)
- Veel kord Mitnick: tehnoloogia, väljaõpe, eeskirjad

# Natuke lugemist

- http://smallbluegreenblog.files.wordpress.com/2010/04/eicar98.pdf
- http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics
- http://faculty.nps.edu/ncrowe/oldstudents/laribeethesis.htm
- http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/
- http://www.social-engineer.org/
- http://www.darkreading.com/

# Selle jutu lõpp