

Loll saab Internetis kah peksa

Kaido Kikkas
EIK 2011/2012

Kaido Kikkas 2012. Käesoleva dokumendi paljundamine, edasiandmine ja/või muutmine on sätestatud ühega järgnevatest litsentsidest kasutaja valikul:

* GNU Vaba Dokumentatsiooni Litsentsi versioon 1.2 või uuem

* Creative Commons Autorile viitamine + Jagamine samadel tingimustel 3.0 Eesti litsents (CC BY-SA)

Paar mõtet alustuseks

- „Suurim turvarisk asub alati klaviatuuri ja tooli vahel“ - IT aksioom
- „Lollikindlat masinat ei ole võimalik luua, sest lollid on ülimalt leidlikud.“ - üks amishi talumees Howard Rheingoldile
- „Ei ole küsimus, KAS süsteemi sisse murtakse, vaid MILLAL.“ - Kevin Mitnick
- „We are Samurai... the Keyboard Cowboys... and all those other people who have no idea what's going on are the cattle... Moooo.“ - The Plague

Luud vastu ust

- Siiani kohatav praktika kaugetes paikades (võrrelge mõne tänapäevase kindlustuslepinguga!)
- Turvalisus teeb vahel kummalisi pöördeid – näiteks Eesti saarte looduse säilimine tänu N. Liidu okupatsioonile
- Esineb tihti ka tehnika ajalooos (<== Theobaldi „mindquake“?), sh andmeturbe osas

Paroolinõksud MIT-s

- Tsiteerime veel kord Steven Levy't
- MIT häkkerikogukond tajus juhtkonna poolt sisseviidud paroolinõuet mitte kaitseabinõu, vaid privaatsusele suunatud ründena
- Reaktsioon: soovitati kõigil kasutajatel jätta parool tühjaks (1/5 kasutajaist tegi seda)
- Paarkümmend aastat hiljem on aga olukord väga tublisti muutunud

Vanasti vs tänapäeval

- Vanasti olid arvutid elitaarsed => vähe inimesi, kõrge haridustase, äri ei olnud eriti reaalne
- Tänapäeval võib läänemaailmas olla arvuti isegi kodutul (vt <http://thehomelessguy.blogspot.com/>)
- Tulemus – ühelt poolt minek massidesse ja tubli tõuge ühiskonna arenguks, teisalt aga
 - omapärane arusaam ärist
 - palju otseseid kaabakaid ja kurjameid
 - veelgi rohkem hästivarustatud lolle

Paroolijama jätkub

- MS-DOS ja varased Windowsid olid ühekasutajasüsteemid, võrku ega paroole polnud (Unix oli kaua aega üksnes spetsidele)
- Win 95 tõi primitiivse, näilise parooliküsimise, mis ei kaitsnud midagi ja millest sai Esc-vajutusega mööda
- Kui NT ja 2000 reaalse paroolikaitse said, oli kasutajate põhimassi mõttemall juba omadega ämbris
- Tulemusi on näha tänase päevani (XP, Vista, 7)

Miks pahad ikka Windowsi sihivad?

- Microsoft viitab suurimale turuosale
- Mingil määral tõde, kuid palju tähtsam põhjus on kaugelt suurim süüdimatute kasutajate osakaal. Süsteemi vead on ka abiks, aga tihti ei lähegi neid vaja
- Seega muutub kasutajate harimine lähiajal isegi tähtsamaks süsteemide lappimisest
- Jarno Niemelä, F-Secure: “There is no patch for stupidity”

Karl Marx ja Freddie Mercury

- WTF...? Mida need sellid SIIN teevad?
- Marx: “vastandite ühtsus ja võitlus”
- Mercury: “I can't live with you, I can't live without you....”
- Point: seisu muudab veelgi segasemaks asjaolu, et andmeturve on suur äri, kus võib rääkida ka huvide konfliktist. **Kas McAfee või Symantec oleks õnnelik, kui ühel päeval oleks kogu pahavara ilmast kadunud?**

Pahavaratööstus

- XXI sajandi IT suurim nuhtlus: perverssed ärimudelid ehk olukord, kus sigadustega on võimalik kõvasti teenida
- väga lai valdkond alates nahaalturundusest (ma tean, et sa käid veebist pidevalt kalapüügivärki uurimas, nii et pakun sulle õngeritvu ja kummikuid) ja lõpetades otsese kuritegevusega (identiteedivargused, pealtkuulamine)
- Põhiprobleem: kuidas kaotada ära pahavara loojate stiimulid?

... ja turvatööstus

- Lugu kahest arstist, isast ja pojast: “Isa, sina ravisid hr. Smithi 7 aastat, mina tegin ta kahe kuuga terveks!” - “Poeg, ma kasutasin tema raha sinu koolitamiseks.”
- Turvalisuse eest on makstud hallidest aegadest peale: Ja juba varakult taibati:
 - turvalisus on turvatunde müümine
 - tark on hoida ohud eemal, kuid mitte neid likvideerida – nii on töö kindlustatud ka tulevikus
 - vahel saab ka otseselt kokku mängida

Suur Vend...

- Riigipoolne sekkumine kasvab enim just nn. demokraatlikes riikides. N:
 - Carnivore'i paketsniffer
 - FBI Magic Lantern -klahvisalvesti
- Vahepeel käsib Vend tööstusel mitte end segada – näiteks antiviirustel mitte avastada mõnd vajalikku “viirusesarnast eset” (vrkl samalaadsed probleemid tsensuuritarkvaraga)
- Üsna tõsine ja kasvav probleem

...ja tema pahad päkapikud (mõned idas, mõned läänes)

- Poliitiliselt motiveeritud privaatsuserikkumised (vt ida poole)
- majanduslikult motiveeritud rikkumised “avalikõiguslike” libaorganisatsioonide (mis on tegelikult puhtalt ärid – näiteks EAÜ, BSA, MPAA, RIAA) poolt

Varajased vembud

- 1969 – Joe Engressia kasutab tasuta telefonikõnesid vilistamise abil
- 1971 – John “Cap'n Crunch” Draper, 2600Hz. Hiljem teeb esimese “blue boxi”
- Noor Kevin Mitnick (vt tema raamatut „The Art of Deception“ - väga soovitatav lugemine!):
 - bussihäkk
 - taksofoni alttõmbamine mündiheliga
- Põhimotiiviks oli veidi liialdatud uudishimu ja vabadusetaotlus

1994 kui teetähis

- Esimene rämpspostitus (adresseerimata äriiline kiri) Usenetis
- Vladimir Levin vs Citibank – 10M USD
- Kevin Mitnick saadakse kätte, leitakse ca 20 000 krediitkaardinumbrit (mõeldud jooksvate kulude katteks)
- Interneti ärile avamise must pool hakkab nägu näitama (rämpsude ja pettuste kiire kasv, *the September that never ended* sügisel 1993 jne)

Mõned levinumad skeemid

- Töötavad erinevates variatsioonides edukalt juba pikka aega
- Kasutavad oskuslikult ära inimlike nõrkusi
- Suudavad kohaneda palju kiiremini kui seadustik suudab muutuda

1. Lihtsad manipulatsioonitüübid

- Esialgu lihtsalt “cheap offer, no delivery” ehk “liiga hea, et olla tõsi”.
- hiljem pidid hakkama rändama, kuna enamik keskkondi pidas petistele jahti
- tüüpiline kaubitsemisobjekt: väikesed käepärased ja kallid esemed (kellad, fotoaparaadid, ehted)
- tihti kombineeritakse rämpspostiga kas siis sama saatja või “partnerite” poolt

2. Identiteedipettused

- tõusev trend
- numbreid ja isikuandmeid hangitakse kas pahavara, sissekräkkimise või “traditsioonilise” kuritegevuse abil (kontorisse sissemurdmine, arvutivargus)
- Probleem: turvaline pangakanal ei aita, kui klient on turvaalal täiesti võhik

3. Pangapettused

- Enam levinud USA-s, kus kasutatakse endiselt laialt tšekke ja rahaülekandeid
- Tüüpskeem: peta firmalt välja rahaülekande info, seejärel kasuta seda võltstšekkide tegemiseks ja maksa nendega kaupade eest
- Veel üks trend: USA rahakaartide võltsimine

4. Autopettused

- Tüüpiliselt kas
 - kalli auto pakkumine odavalt, küsitakse “vaid veidi raha ülekandekuludeks”
 - saadetakse võltstšekk suuremale summale ja palutakse vahe tagasi maksta

5. Kohtingutüügid (ehk tibitillikad)

- Üks kõige sotsiaalsemat sorti pettus
- veendakse “oma tulevast kaasat” saatma “veidi raha reisikuludeks”
- Mõnel juhul lüpstakse „tulevaselt“ ka muid hüvesid välja

6. Krediitkaardipettused

- Spämmitud päringud firmadesse küsimusega, kas saab maksta kaardiga. Vastanutelt tellitakse varastatud kaartidega
- Edasisaatjaga skeem – kasutatakse kedagi Läänes kontaktisikuna (tihti mõnd kohtingutünga ohvrit), see saadab “kauba” edasi N. riiki. Reeglina jääb vahele vaid kontaktisik

7. Phishing

- Üldise terminina tähistab kellegi petmist avaldama enda isiklikku infot
- “ph” - võib tähistada nii tüüpilist kräkkerislängi kui “password harvesting”-i
- Varasem kuldne jahimaa oli AOL, tänapäeval on selleks erinevad sotsiaalportaalid (eriti MySpace)

8. Tehnotüügid

- otsene hõivamine ja rootkit'id
- pahavara, trooja hobused
- XSS (*Cross-Site Scripting*)
- DNS-rünnakud (*pharming*)
- võltsnimed ja homoglüüfründed

Netimanipulaatori põhitõed

- Kogu näiliselt süütute päringute abil maksimaalselt palju infot objekti kohta
- Kasutades kogutud infot, mängi omainimest ning saa ligipääs olulisele infole
- Kasuta saadud tähtsat infot oma äranägemise järgi

Näide 1: Martini audit

- 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 täienduskooolitusi?
 - Mis on osakonna personalikulude kontonumber raamatupidamises?
 - Mitu töötajat on lahkunud viimase aasta jooksul?
 - Milline on osakonna üldine tööõhkkond?
- Mis siin valesti on...?

Näide 2: abivalmis helpdesk

- Vajalik varustus: mobla + kõnekaart
- 1. kõne: firma raamatupidamisse hr. Sepale; mängida helpdeski 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 „helpdeskile“ 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 mälu tühjaks ja võtta aku välja)

Näide 3: laud teistpidi!

- Uus spordiala: *mugu-baiting*
- 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 asju tegema panna
- Parimad pojad on saanud ise raha või lennutanud nigeerlase tema enda kulul New Yorki kohtuma
- Vt näiteks <http://www.whatsthebloodypoint.com>

Nigeria(tm)

- Miks ikkagi?
 - pikaaegne ebakindlus ja korrupsioon (rikas maa ebakindla võimu all, pikk sõjaväevõimu periood)
 - tohutu vaesus ja ebavõrdsus – 60% elanikest on allpool vaesuspiiri, 80% naftatuludest läheb 1%-le elanikkonnast
 - suur maa, palju rivaalitsevaid hõime
 - inglise keel kui ühiskeel (muid keeli ca 250)
 - kirjaoskuse protsent 68%, üsna hea haridustase
 - üsna hea tehno-infrastruktuur
 - pikk pettustetraditsioon (ammu enne Vörku)

Web 2.0 või Nuhk 2.0?

- Enamik sotsiaalseid võrgustikke moodustavad nn usaldusvõrgustikud (sõbralisti liikmed on „omad“)
- Kohati kaugelt liiga palju isiklikku infot!
- Enamik manipulatsioone algab usalduse tekitamisest – sellise võrgustiku puhul on väga suur hulk tööd tihti juba ette ära tehtud
- Suur probleem – teenuste põimumine!
- Gazzag.com'i juhtum 2006. aastal

Vastuabinõud?

- Seadusandlikud sammud, eriti aga selle muutmine paindlikumaks
- Hästi defineeritud eeskirjad
- Piisav tehniline teadlikkus, eriti aga tavakasutajate harimine
- Kodanikualgatuse korras vastutegevus (NB! Eetiliselt hall tsoon, kohati ka illegaalne)
- ...

Paar soovitus Web 2.0 jaoks

- kasuta võrgustiku/rakenduse enda turvamehhanisme maksimaalselt
- kui võimalik, ära kasuta konsolideeritud sisselogimist (N: Google'i parool)
- ära taaskasuta paroole
- õpi tundma tarkvara võimalikke vigu ja tuntumaid ründevariante
- loo isiklik turvapoliitika erainfo avaldamise jaoks (mida võib üles panna, mida mitte)

Ekskaak soovitab

- "Turvalisus tuleb tehnoloogia, väljaõppe ja protseduurireeglite kaudu" – Kevin Mitnick, turvakonsultant (!)
vt ka *The Art of Deception*
- Tehnoloogia: võrgud, tule müürid, viirusetõrje...
- Väljaõpe: teadlikkus manipulatsioonidest
- Protseduurid: kindel turvapoliitika ja -nõuded
- https://www.sans.org/reading_room/whitepapers/engineering/a_multilevel_defense_against_social_engineering_920

Kokkuvõtteks

- Tänapäevase IT-maailma pahupooleks on vastik kokteil võrgu laia levikust, lahjadest seadustest, ebaeetilistest ärihuvidest ja inimlikust lollusest
- Esmane vastuabinõu: „Õppida, õppida, õppida“ (ja õpetada ka!)

Side lõpp.
