# Vali, kas punane või sinine?

Kaido Kikkas

(Algselt avaldatud ajakirjas "30 pluss" novembris 2015, siin ilmub kokkuleppel toimetusega)

Pealkirjas toodud küsimus pärineb kuulsast ulmefilmist "Matrix", kus nähtav maailm oli vaid masinate loodud illusioon ning tegelikkus oli märksa hirmsam. Peategelasele antakse ühes keskses stseenis valida, kas ta võtab sinise tableti ja elab edasi illusioonis, õndsas teadmatuses - või võtab punase ning saab teada, kuidas asjad päriselt on. Peategelane Neo valib punase. Ent filmis on ka tegelane, kes hakkab hiljem enda valikut kahetsema ning temast saab oma kaaslaste reetur.

Viimastel aastatel on Interneti kiire ja laialdase leviku tagajärjel tohutult kasvanud kasutajate hulk. Paraku on väga suur osa neist täielikus teadmatuses elementaarsetest turvameetmetest.

Võtame lihtsa paralleeli - paljudel lugejatel on ilmselt autojuhiload. Seega peaks veel meeles olema arteriaalse ja venoosse verejooksu erisuste pähetuupimine, ehmatav "äravajumine" õppesõiduplatsi estakaadil ning higistamine nii autokooli kui ARKi eksamitel. Milleks kogu see jama? Põhjus on selles, et auto (või tsikkel) on väga tore asi, ent asjatundmatu inimese käes võib see palju pahandust teha - ja mitte üksnes talle endale, vaid ka paljudele teistele. Seepärast on asjad korraldatud nõnda, et poest auto osta võib iga inimene, ent sellega sealt ärasõitmiseks on vaja juhilube.

Arvuti ja võrguühendus on tegelikult täpselt samasugused väga toredad asjad, mis aga võivad võhiku kätes kurja teha. Paraku ei küsi arvutisoetaja käest aga tänini ükski asutus, kui pikk peaks olema kasutatav salasõna, millised ohud varitsevad Facebookis või miks ei peaks tollele toredale Aafrika sellile, kes lausa raha pakub, vastu kirjutama.  Mis aga peamine – iga kasutaja, kes ei hooli oma arvuti turvalisusest, seab sellega ohtu mitte ainult enese, vaid ka paljude teiste inimeste tegevuse. Toome mõned näited.

Teie arvuti nakatub viirusega. Enamik tänast pahavara suudab end püsivalt Internetti ühendatud nakatunud arvutist edasi levitada ilma kõrvalise abita (ka potentsiaalseid ohvreid suudavad viirused ise otsida). Teie masin muutub lisaks teie enda töö takistamisele otseseks ohuks paljudele teistele.

Teie arvutisse murtakse sisse. Tavaline mõtteviis „Mida mul siit ikka võtta on?“ on aga sügavalt ekslik. Mõned konkreetsed võimalikud tagajärjed:
• Teie arvutist hakatakse levitama rämpsposti. Reaktsiooniks võib olla nii äravihastatud "patsiga poiste" spontaanne küberrünnak kui ka mõne suurema firma poolt algatatud kohtuasi.
• Teie arvutit kasutatakse ebaseadusliku tarkvara („piraattarkvara“) laona. Võimalikud kontrollijad aga võtavad vahele arvuti omaniku. Tõsi, Eesti seadused esialgu otsest koju kontrollima tulekut ette ei näe, töökohtadesse võib aga suurte tarkvarafirmade "erapolitsei" BSA küll külla tulla.
• Teie arvutisse pannakse püsti pornoarhiiv. Tavakujul on tegu lihtsalt küsitava väärtusega asjaga (pluss liikluse aeglustumine klientide arvu suurenedes), mõned erijuhud võivad aga viia väga karmide tagajärgedeni (lasteporno).
• Teie arvutit kasutatakse hüppelauana mõne tähtsa objekti ründamiseks (näiteks FBI peakorter). Reeglina alustab ohver vastutegevust ning jällegi jääb vahele hüppelaua omanik. Tõsi, kuna sarnaseid juhtumeid esineb palju, siis enamasti õnnestub uurijaid veenda, et ka teie masin „maha tõmmati“ ja teie ise ei olnud rünnaku taga. Palju jama on aga igal juhul garanteeritud.
• Teie arvutisse paigaldatakse sniffer ehk pealtkuulamistarkvara, mis registreerib kõik klaviatuurilt tehtud vajutused ja saadab need paigaldajale edasi. Sel juhul võite näiteks pideva internetipanga kasutamise korral millalgi avastada, et kontol pole enam sentigi – pealtkuulaja sai teada nii

püsiparooli kui kogus kokku piisaval hulgal kaardiparoole, et konto tühjaks teha (kahjuks on just veidi vanemate inimeste seas tänini levinud internetipanga kasutamine "vana kooli" paroolikaardi abil).

Need näited olid ehk veidi lihtsustatud, kuid põhimõtteliselt reaalsed. Eespool räägiti üksikust arvutist, ent tänapäeval on kõige levinum stsenaarium nakatatud arvuti lülitamine nn robotvõrku ehk botnetti, mille liikmed sisuliselt moodustavad hajusa superarvuti - näiteks umbkaudu 2008-2012 tegutsenud Confickeri pahavara poolt ehitatud botnet koosnes enam kui 10 miljonist nakatatud arvutist (millest enamiku omanikel polnud tõenäoliselt aimugi, millega nende masin "kohakaasluse alusel" tegeleb!) ning suutis muude sigaduste hulgas saata päevas umbkaudu 10 miljardit rämpssõnumit. Huvilised võivad edasi lugeda ülevaatlikust Wikipedia artiklist https://en.wikipedia.org/wiki/Conficker, kus on ka palju viiteid info algallikatele.

Tuleme korraks tagasi käesoleva loo pealkirja juurde. Sinise tableti nimeks on Mugavus. On ju mugav, kui me ei pea arvutit käivitades parooli või nutitelefoni avamiskujundit sisestama, Facebook avaneb automaatselt ja kunagi ei teki ühtki probleemi ühegi veebilehe kuvamise ega ühegi faili avamisega. Sedasorti mugavuse eest aga makstakse tänapäeva arvutimaailmas kahe veelgi olulisema väärtuse - privaatsuse ja turvalisusega.

Küünilisemad internetispetsid ütlevad, et Internetis on vaid kaks võimalust - kas oled klient (see, kellele kaupa müüakse) või kaup (see, keda - või täpsemalt, kelle infot - müüakse). See võib olla ehmatav tõdemus, kuid paraku on see suures osas tõde. Hea näide on Androidi operatsioonisüsteem, mida kasutab suur osa meie nutiseadmetest - süsteem ja suur hulk kasulikke rakendusi (äppe) tuleb kohe seadme ostmisel kaasa ning paari klõpsu kaugusel on veel lugematu hulk teisi kasulikke vidinaid. Ent Androidi taga seisev Google ei ole tarkvara-, vaid sisuliselt informatsioonieттevõte (nagu ka Facebook) ning kasutajatelt kogutav info on kulla hinnaga (ja seda päris sõna-sõnalt). Ja seda kogub nii Google ise kui ka lugematute tasuta pakutavate äppide autorid.

Väike lihtne näide: kas keegi on proovinud paigaldada näiteks mõnd lihtsat taskulambiäppi (väga mugav asi - telefoni välklamp suudab päris edukalt taskulampi asendada) ja seejuures imestanud, milleks on taskulambil vaja ligipääsu meie kontaktidele, lühisõnumitele ja kalendrile...? Samal teemal soovitaks huvilistel kuulata soomlasest pahavaraspetsi Mikko Hyppöse poolt IT kolledžis peetud avalikku loengut: https://www.youtube.com/watch?v=UXSAaVx2EOo .

Aga mida siis teha? Meenutame veel korra "Matrixit" - kohta, kus Neo külastab Oraaklit. Tolle ukse kohal on ladinakeelne lause "Temet nosce", maakeeles "tunne iseennast". Meie puhul aga tähendab see "tunne enda oskusi ja oma arvutit" ning see on esimene suur samm turvalisuse suunas.

Esmalt tasub kriitilise pilguga hinnata enda teadmisi IT-vallas. Kui leiame, et neid on vähevõitu, on kaks võimalust: kas hangime neid ise juurde või leiame kellegi, kelle teadmisi saame kasutada. Kolmandat võimalust eriti ei ole.

Seejärel aga tuleks vaadata üle enda arvuti või nutiseade. Taas kord paralleelina autosõiduga - tänapäeval ei eelda keegi, et me peaksime ise enda auto mootoris kolvirõngaid vahetama, kuid peame käima regulaarselt hoolduses ning saama hakkama ka rehvirõhu kontrollimise või aknapesuvee juurdevalamisega, tankimisest rääkimata. Rääkimata veel sellest, et autoga sõitmine eeldab kogu "kasutajaliidese" (rool, pedaalid, käigukang...) valdamist sel tasemel, et me teistele inimestele ohtu ei kujutaks.

Nõndasamuti peaks "arvutijuht" teadma, millised on tema "sõiduki" põhiomadused - millised seadmed on arvutiga ühendatud, kui palju on põhimälu- ja kõvakettaruumi, milline on kasutatav operatsioonisüsteem ning millise täiendava tarkvara oleme sinna ise paigaldanud. Nii nagu autojuht

kasutab kesklukustust ja immobilaiserit, peaks "arvutijuht" kasutama paroole ja muid ligipääsu reguleerivaid vahendeid (sõrmejäljelugeja, nutiseadmete sissepääsumustrid jne). Tankimise asemel tuleb arvuti operatsioonisüsteemi regulaarselt uuendada. Nagu autojuht peaks üldiselt teadma oma asukohta, nii peaks seda suutma ka Internetis olles. Ja viimaks, nii nagu autovõtmeid ei jäeta laokile, ei jäeta ka enda isikuandmeid ja muud olulist infot.

Niisiis kokkuvõtlikult: esimesed sammud IT-turvalisuse poole (ajatus kümne käsu vormis) on

1. Tunne iseennast ja oma teadmisi-oskusi arvutiasjanduse vallas.
2. Tea, kust vajadusel nõu küsida.
3. Tunne enda arvutit. Kasuks tuleb nii peamiste komponentide üldine tundmine (kaks levinud tavainimese eksitust on protsessori samastamine arvutikastiga ning põhimälu ja kõvaketta segiajamine) kui ka enda arvuti põhiparameetrite teadmine (kõvaketta maht, põhimälu suurus, aga miks mitte ka protsessori ja videokaardi tüüp).
4. Tea, millist operatsioonisüsteemi arvuti või nutiseade kasutab.
5. Tea, milline tarkvara oli arvuti või seadmega ostes kaasas ja mida on sinna hiljem lisatud (eriti oluline nutiseadmete puhul, kus äppide üle arvepidamine võib kergesti sassi minna).
6. Oska enda arvuti tarkvara (nii operatsioonisüsteemi kui muud tarkvara) uuendada ning tee seda regulaarselt (või lülita sisse automaatne uuendamine).
7. Kasuta alati elementaarseid turvamehhanisme (paroolid, PIN-id, tuvastussümbolid, sõrmejälg), kindlasti tasub endale selgeks teha korralike paroolide valimine.
8. Hea oleks teada (kasvõi kõige üldisemal tasemel) IT-maailma riske ja ohtusid. Tundmatu vastane on alati hirmsam kui tuntud.
9. Internetti kasutades tea alati, kus oled, ning ära kaota valvsust. Igasuguse info sisestamise eel küsi endalt kaks küsimust - "Kes seda küsib?" ja "Kas tal on vaja seda teada?".
10. Ära lase end lolliks teha. Nagu ka tavaelus: kui mõni ettepanek tundub liiga hea, et olla tõsi, siis enamasti peab kahtlus paika.

Loodetavasti hakkab siin ilmuma edaspidi juba detailsemaid näpunäiteid enda kaitsmiseks IT-maailmas. Kaitsmine algab aga vajaduse teadvustamisest. Nii et - punane või sinine?