Kas krüpto on nüüd surnud?

13 aastat tagasi - 06.09.2013 Autor: Aare Kirna

(Arvutikaitse.ee, 6. september 2013)

Snowdeni viimased paljastused väidavad, et Ameerika Ühendriikide ja Suurbritannia valitsusasutused suudavad kuulata pealt krüpteeritud võrguliiklust, mis toimub näiteks teie arvuti ja Hotmaili, Yahoo, Google'i või Facebooki vahel. Et see võimalik oleks, kuulatakse pealt rahvusvahelisi sidekaableid ja võrgusõlmi, sunnitakse tarkvaratootjaid kirjutama oma krüptotoodetesse tagauksi ning püütakse kirjutada krüptostandardeid ümber selliselt, et need oleksid vähem muukimiskindlad.

Kas see tähendab, et kogu krüptograafiline usaldusahel, mis laseb meil suhteliselt muretult internetis raha kulutada, petta saamist kartmata valitsuse, ettevõtete ja üksteisega suhelda ning olla kindlad, et meie info ei jõua valedesse kätesse, on nüüd mõttetuks muutunud ning me peaksime paberi ja pastaka juurde tagasi pöörduma?

Jah ja ei.

On tõsi, et kui näiteks HTTPS, SSL ja VOIP sisaldavad tagauksi ja turvaauke NSA jaoks, võivad neidsamu auke kasutada ka kõik teised peale NSA. Ja isegi kui tagaustes on (ehkki tõenäoliselt pigem pole) korralikud kontrollmehhanismid, mis välistavad nende kuritarvitamist, on NSA motiivid igal juhul kaheldavad. Tasub meeles pidada, et Eesti ei ole veel Ameerika Ühendriikide osariik ning meie riigi ja selle kodanike huvid ei pruugi nende omadega kaugeltki kattuda. Pealegi, nagu Bruce Schneier väga õigesti märgib, on Hiinal, Venemaal ja teistel sarnastel režiimidel nüüd hea ettekääne internetti samal viisil kuritarvitada.

Samas, kui väidetavasse pealtkuulamismehhanismi veidi süveneda, siis selgub, etkrüptoalgoritme, see tähendab matemaatilisi põhimõtteid, mille alusel krüpteeritud sõnumeid kokku pannakse, NSA-l siiski murda pole õnnestunud. Aga ega neil seda vaja ei olegi, sest palju aega ja ressurssi nõudvast koodimurdmisest lihtsam on murda inimesi, kes koodi töötlevat tarkvara kirjutavad või krüpteeritud sõnumeid edastavat infrastruktuuri käigus hoiavad. Sellest, kuidas Ameerika valitsusasutused terrorismi tõkestamise või mõnel muul ettekäändel Facebooki, Google'i või mõne teise suure sotsiaalvõrgustiku haldaja käest täiesti otse ja

seaduslikult nende kasutajate andmeid küsivad, on viimasel ajal juba väga palju räägitud, samuti ka seda, et ookeanitaguste sotsiaalvõrgustike või tasuta meili- ja sõnumiteenuste kasutajaist on väga naiivne oma andmete privaatsust eeldada.

Turvaekspertide hinnangul on juhul, kui Snowdeni väited tõele vastavad, pealtkuulatavad enamik suurte Ameerika tarkvaratootjate krüptotoodetest. Rahulikumad võivad olla selliste toodete kasutajad, mille lähtekood on avalik või mis ühilduvad rohkem kui ühe tarkvarafirma toodetega. Seda põhjusel, et tagaustel on väga raske jääda märkamatuks, kui sama koodi uurib mitu sõltumatut tarkvaraarendajat. Samuti ei ole mõtet murda sisse suvalise kasutaja arvutisse – asjatu vahelejäämise risk on liialt suur.

Kas see kõik puudutab ka meid siin Eestis?

Kas me võime julgelt oma e-panku kasutada ja e-Eestiga edasi suhelda? Kas Keskerakonnal ongi õigus ning ID-kaart kõlbab nüüd ainult autoklaasilt jää kaapimiseks?

Mis e-valimistesse puutub, siis nii palju kui mina tean ja ajaloost õppinud olen, on pabersedelitegavalimistel oluliselt lihtsam ja odavam susserdada kui e-häälte puhul.

ID-kaardi turvalisus peaks olema oluliselt kõrgem kui lõppkasutaja arvuti oma. Selle krüptot pole minu teada veel murda õnnestunud, samuti pole kuulda olnud, et keegi ID-kaardi tarkvara arendajatele täiendavate tagauste sisseprogrammeerimise eest maksnud oleks (ja niipalju kui mina tarkvaraarendusest tean, tasuta seda tööd vaevalt et keegi ette võtaks). Mõistagi poleks sugugi liigne valitsuse esindajate kinnitus, et meie riik ei tee tagauste teemal NSA-ga koostööd.

Eestis tegutsevad pangad on oma e-kanalite turvalisuse pärast muretsenud juba pikka aega. See on väljendunud näiteks koodikaardi ülekandelimiitide koomaletõmbamises ning ID-kaardi ja Mobiil-ID propageerimises. Teoreetiliselt peakski ID-kaardiga krüpteeritud pangasessioon olema turvalisem kui USA teenusepakkujalt ostetud veebiserveri sertifikaadiga krüpteeritud turvakanal, mida kasutatakse juhul, kui logite panka sisse koodikaardiga.

Mida saame meie, tavakasutajad teha selleks, et meid pealt ei kuulataks?

1. Seda, et meie poliitikud lombitagusele Suurele Vennale iitsatada julgeksid, et Eesti Vabariigi kodanikel on ka mingid inimõigused ning ootused oma privaatsuse austamiseks, on vist natuke palju tahetud. Aga valimised ei olegi nii väga kaugel ja praktika näitab, et sel ajal vähemalt tehakse nägu, et valijaid kuulatakse. Nii et, hea kodanik – suhtle oma saadikuga, päri aru ja küsi tulevikuplaanide kohta!

2. Pidage meeles, et kui kasutate Facebooki, Gmaili ja muid sarnaseid teenuseid, siis kõik, mis liigub läbi Ameerika serverite, jääb sealse jurisdiktsiooni alla ja Ameerika valitsusel pole meie kui välismaalaste suhtes isegi neid kohustusi, mida ta omaenda kodanike suhtes Snowdeni väitel ignoreerib.

3. Eesti on väike, kõik tunnevad üksteist ja iga vähegi suurem sigadus tuleb ükskord välja. Seega tasub kohalikke teenusepakkujaid ning võrke usaldada rohkem kui ookeanitaguseid, olgu need siis meili- või hostinguteenuse pakkujad, digitaalsete sertifikaatide või muude kohalike turvatoodete müüjad.

4. Avatud lähtekoodiga tarkvara on üldiselt nuhkimiskindlam. See ei tähenda, et peaksite loobuma näiteks Microsofti toodetest, eriti kui need on muutunud teie igapäevase töö ja meelelahutuse lahutamatuks osaks. Ehkki Ameerika firmad on muidugi kohustatud tegema seda, mida nende valitsus käsib, on nende peamiseks eesmärgiks siiski kasum, ja nad on täiesti valmis astuma vägagi otsustavaid samme, veenmaks oma miljoneid kliente, et nende privaatsusega on lood hulga paremad kui viimaste uudiste valguses paistab. Aga kui teil on pidevalt tegemist ärisaladustega või tahate lihtsalt elada teadmisega, et teie eraleu pole kellegi teise asi, võiksite eelistada Linuxi-põhiseid lahendusi.

Veel samal teemal.

AARE KIRNA
Arvutikaitse.ee

- Uudised
- Turvalisus