

PAHANDUSED KÜBERRUUMIS

Enn Tõugu
tyugu@ieee.org

Eesti ühiskond on tugevasti sõltuv Internetist ja seal toimuvatest protsessidest – niinimetatud küberruumist. See sõltuvus on suurem, kui mistahes teisel riigil. Ei kodanikud ega ettevõtted ei saa Eestis tegutseda enam ilma Interneti toeta. Näiteks, üle 98% kõigist pangaoperatsioonidest tehakse meil elektroonselt. Interneti kaudu täidetakse enamus maksudeklaratsioone, kasutatakse avalikke teenuseid, saadakse infot, peetakse sidet, allkirjastatakse dokumente, osaletakse valimistel.

Küberruumi sotsiaalne õhkkond meenutab metsikut läänt, mida vesternites näeme. Seda iseloomustavad anonüümsus, heade tavade vähesus, seaduste puudumine, kiire rikastumise võimalused, karistamatuse tunne. Õnneks valdav enamus küberruumi kodanikke käituvad ikkagi korralikult.

Murelikuks teeb siiski küberkuritegevuse, s.t. Internetis tehtavate väärtoimingute ja kuritegude kiire kasv, ning prognoos, et see kasv jätkub kiirenevas tempos veel mõnda aega. Internetis valitsevate ohtude näiteks võib olla asjaolu, et Internetti ühendatud täiesti kaitseta jäänud arvuti nakatatakse täna praktiliselt mõne minutiga. Kurivara, s.t. tarkvara, mis on spetsiaalselt loodud kuritegevuseks, on muutunud keeruliseks ja hõlpsalt kasutatavaks. Seda saab osta Interneti kaudu mõnesaja dollari eest.

Mõned ülemaailmsed andmed on järgmised:

- On teada ca 13 miljonit kurivara tüüpi
- Küberründed on saanud proffide tegevuseks
- Päevas toimub küberruumis ca 500000 rünnet
- Küberkuriteod on muutumas sündikaatide tegevuseks
- Mõned ründed on väga suured: läinud aastal varastati firmalt TJX rohkem kui 45 miljoni kliendi pangakaardi andmed, selle kuriteo sooritas umbes kümneliikmeline rühm, kuhu kuulus ka vähemalt üks Eesti kodanik.

Enamus küberkuritegusid sooritatakse rahalise kasu saamise eesmärgil. Kuigi Eesti pangad on olnud küberrünnete all juba aastaid, pole need ründed seni meie pankade tegevust oluliselt kahjustanud. Läinud aasta kevadel toimus maailmas esimene küberrünne, mida saab nimetada riiklikuks küberkallaletungiks. See oli rünne Eesti vastu, ja oli seotud prokssõduri rahutustega. Rüninati võrgu-servereid, poliitikute ja asutuste veebilehti, panku jne. Tähelepanu väärivad teenusetökestusründed, milles osales keskele juhtimisele alluv paljudest tuhandetest arvutitest koosnev „sõjavägi”, nn. botnet. Eesti pidas kallaletungile suhteliselt hästi vastu, kuid see sündmus äratas maailmas suurt tähelepanu ja sundis riike pöörama enam tähelepanu küberkaitsele. Suvise Gruusia-Vene sõja ajal toimus küberkallaletung Gruusiale. Rünnete iseloom oli üsna sarnane Eesti vastu suunatud rünnetele. Natukese väiksema ulatusega küberkallaletungi alla sattus sel aastal ka Leedu, kui ta poliitikut esinesid Venemaale ebasobivate avaldustega.

Peale küberkallaletungi töötas Eesti välja oma küberkaitse strateegia, alustas kiirkorras küberkaitse õpetamist kõrgtasemel (magistriõppe raames). Tallinnasse on loodud NATO Kollektiivse Küberkaitse Kompetentsikeskus, mis näitab usaldust Eesti selle ala asjatundjate vastu.