Talouselämä lehdelle **04.11.2020**

Uusi suunta kyberturvalliseen Suomeen

Vastaamon tietomurto on ikävä muistutus tietoyhteiskunnan riskeistä ja nykyisen Internetin ongelmista. Reitittävässä IP-verkossa, jollainen Internet on, on mahdollista väärentää paketin lähdeosoite ja tehdä näin palvelunestohyökkäyksen jäljittäminen vaikeaksi. Hyökkääjä voi myös kirjoittaa nimipalvelukyselyyn uhrin osoitteen, mikä saa nimipalvelimen heijastamaan hyökkäyksen uhriin. Joko tarkoituksella tai vahingossa on mahdollista kaapata jonkin reitin koko liikenne kulkemaan väärän verkon kautta. Tämä avaa mahdollisuuden yrittää mies-keskellä hyökkäystä, jossa välitettävää tietoa voi vaikkapa väärentää. Sovellustasolla hyökkäysmahdollisuuksia tuntuu olevan loputon lista.

Internetin tietoturvaa on rakennettu paikka paikan päälle. Usean kymmenen vuoden ponnistuksin ovat syntyneet virustorjunta ohjelmat, palomuurit, tunkeutumisen tunnistaminen ja esto jne. Kaikki nämä ratkaisut on rakennettu alustalle, jossa on IP:n lisäksi vieläkin turvattomampi alla oleva pakettien välitys esim. Ethernetiä käyttäen. Ratkaisujen heikoin lenkki on, että ihmiset tekevät virheitä. Tietoturvan tasoa takaa vaihteleva osaamisen taso täydellisestä tietämättömyydestä ja välinpitämättömyydestä huippuammattilaisuuteen. Toinen heikkous on, että ohjelmistoja pitää jatkuvasti päivittää ja aina löytyy syitä viivästää päivitys tai jättää se tekemättä. Tietoturvan ammattilaisia ei riitä korjaamaan tilannetta. Asia ei ole ratkea lisäkoulutuksella, tarve on liian suuri. Niin kauan kuin tapa rakentaa verkkoja ja tietoturvaa ei muutu, yleistä tietoturvan tasoa ei saada ratkaisevasti parannettua siitä, mitä se nyt on.

5Gn ansiosta syntyy koko ajan uusia kriittisiä digitaalisia palveluita, joista kehittyneet yhteiskunnat ovat yhä enemmän riippuvaisia. 5G rakentaa fyysisen ja digitaalisen maailman rajapintaa, joka hakkeroimalla on mahdollista tehdä fyysisen maailman rikoksia tietoverkkoa hyödyntäen. Jos näin jatketaan, valtiot joutuvat panostamaan kasvavia summia tehottomaan digirikosten torjuntaan samaan aikaan kun turvattomuus kasvaa. Fyysisen ja digimaailman rajapinta on erittäin houkutteleva kohde valtioiden salaisille armeijoille jatkaa poliittista kilvoittelua toisin keinoin. 5G onkin tullut maailman politiikan keskiöön. Voi vain kuvitella, miten keskiöön 6G joutuu.

Tarvitaan selkeästi uusi suunta tietoturvan tason nostamiseen. Sellainen voi olla kaiken tärkeän, yhteiskunnan kannalta oleellisen tietoliikenteen siirtäminen perinteisestä Internetistä erityisverkkoihin. Niitä voi olla useita rinnakkaisia. Jokaisessa verkossa pääsääntöisesti vain sisäinen legitiimi liikenne on mahdollista ja sallittua. Internetin kaapatuista laitteista käsin ei voisi lainkaan hyökätä erityisverkon laitteita tai tietokantoja vastaan. Yksi sopiva kohde olisi terveyssektorin erityisverkko. Toinen esimerkki olisi kaiken rahaan, maksamiseen ja laskuttamiseen liittyvän datan verkko.

Kehitys on tuonut markkinoilla ohjelmoitavat verkkolaitteet. On menossa muutos, jossa jopa IP-verkon reitittimet korvataan ohjelmoitavilla laitteilla. Siksi tuollaisesta erityisverkkojen rakentamisesta on tulossa pelkkä ohjelmistokysymys. Erillisiä laitteita tarvitaan joko hyvin vähän tai ei lainkaan. Erityisverkot voivat hyödyntää monia matkaviestinverkkojen ohjelmistoratkaisuja kuten vahvaa tunnistautumista.

Kuluttajat pääsevät käyttämään erityisverkon palveluja SIM-kortillisella laitteella. Ratkaisu suojaa parhaiten, kun myös kuluttajan laite virtualisoidaan, eli laitteessa voi olla useita ”loogisia” tietokoneita. Silloin erityisverkon ja Internetin hyökkäysrajapinta kaventuu virtualisointialustaan.

Turvallisten erityisverkkojen rakentamisen voi aloittaa olemassa olevalla tekniikalla. Panostamalla tutkimukseen ja tuotekehitykseen ratkaisua voidaan merkittävästi parantaa. Ponnistus on äärellinen. Ohjelmoitavien verkkolaitteiden ansioista jopa IP protokolla itse voidaan korvata verkkotekniikalla, josta IP perusvirheet on korjattu.

Kehitystä voidaan tukea viranomaistoimin, jotka muutenkin ovat välttämättömiä. Kriittisen infran rakentamisen ja operoinnin tason varmistamiseksi, sääntelyä ja valvontaa on syytä kiristää ja verkoista vastaavien ihmisten osaamisvaatimuksia tiukentaa. Kun riittävän tehokas ja joustava tapa rakentaa erityisverkkoja on todennettu, sääntelijän pitää vaatia tekniikan käyttöä esim. terveyssektorilla ja vastaavissa kriittisissä kohteissa.

Raimo Kantola
Professori, Aalto Yliopisto