29.4.2014

Tiedonhankintalainsäädäntö ja kyberuhat: Iki ry:n kommentti

Viite: Kirje 11.4.2014 tiedonhankintalainsäädännön kehittämisestä ja asiaan liittyvästä kuulemistilaisuudesta 6.5.2014.

1. Internet-käyttäjät ikuisesti – iki ry

Internet-käyttäjät ikuisesti iki ry on yleishyödyllinen yhdistys joka pyrkii edistämään viestinnän yleisiä edellytyksiä internetissä. Iki:llä on yli 23.500 jäsentä.

Iki pyrkii edistämään tarkoitustaan mm. tarjoamalla yksityishenkilöille pysyvän internet-identiteetin (ikiosoite@iki.fi) ja siihen liittyvää viestien edelleenohjausta sekä pyrkimällä edistämään mm. tietoturvan parantamista.

Iki on ollut usein ensimmäisten joukossa käytännössä edistämässä internetin tietoturvaa parantavia teknologisia ratkaisuja, ohjeita ja käytäntöjä.

Lisätietoja iki:stä ja sen toiminnasta löytyy www-osoitteesta http://www.iki.fi
ja yhdistyksen sähköpostiosoite on iki-hallitus@iki.fi

2. Tietoturva kuntoon!

Tietoturvan parantaminen ja korkean tietoturvatason säilyttäminen on paras tapa ennalta estää kyberuhkia.

Yhteiskunnassa on tärkeää että kansalaiset ja organisaatiot pystyvät käsittelemään, säilyttämään, hallitsemaan ja siirtämään tietoturvallisesti esim.

- yksityisyyden suojaan kuuluvia tietoja,
- terveystietoja,
- poliittiseen toimintaan, yhdistymisvapauteen ja muihin keskeisiin vapauksiin liittyviä tietoja,
- yritystoiminnan tärkeitä taloudellisia tietoja, sekä
- yhteiskunnan toiminnan kannalta tärkeitä tietoja.

Suomessa kannattaisi pyrkiä saamaan sekä viranomaisten[1] että kansalaisten käyttämien järjestelmien tietoturva mahdollisimman korkealle tasolle ja pyrkiä aktiivisesti edistämään ratkaisuja jotka nostavat tietoturvan tasoa.

Tämä vaatii sekä teknisiä toimenpiteitä että käytäntöihin vaikuttamista. Näin saavutetaan kuitenkin suuria pitkän tähtäimen hyötyjä tietoturvassa ja samalla rakennetaan tehokasta suojaa erilaisia tulevaisuuden kyberuhkia vastaan sekä myös suojaa rikollisuutta vastaan.

2.1. "Salaus aina päälle"

Merkittävä edistysaskel tietoturvatason kohottamisessa on saavutettu ja pystytään saavuttamaan sillä, että pyritään suojaamaan salaamalla tiedot ja tietoliikenne kaikissa tilanteissa, esim.

- Käyttäjän laitteissa (esim. kannettavan tietokoneen tietojen salauksen tekemisellä helppokäyttöiseksi),
- Verkkoyhteyksissä käyttäjän tietokoneesta verkkoon (esim. https:n käyttäminen myös tavallisten verkkosivujen kanssa), ja
- Verkon palvelimien välinen salaus(esim. sähköpostiliikenteen SMTP TLS-salaaminen), sekä
- Organisaatioiden sisäisten verkkojen liikenteen salaaminen (esim. palvelimien välisen liikenteen salaaminen).

Tällöin massavakoilun kustannukset kasvavat tarpeeksi jotta riskit rikoksista ja esim. taloudellisesta vakoilusta vähenevät merkittävästi, ilman että asia muodostuu tavallisille käyttäjille liian vaikea.

Muun muassa Iki on pyrkinyt parantamaan internet-viestinnän tietoturvaa mm.

- Pyrkimällä salaamaan kaikki yhteydet mahdollisuuksien mukaan,
- Käyttämällä tietoturvallisia protokollia (kuten nimipalveluiden DNSSEC),

[1] "Tietoturvaloukkaus Suomen ulkoasiainhallinnossa"
http://formin.finland.fi/public/default.aspx?contentid=291701&nodeid=15148&contentlan=1&culture=fi-FI

- Edistämällä kansalaisten ymmärrystä tietoturvasta ja viestinnän suojaamisesta (mm. IKI PGP CA toiminta),
- Tiedottamalla näihin liittyvistä asioista sekä teknisesti että käyttäjien näkökulmasta, sekä
- Toimimalla esimerkkinä siitä miten asiat voidaan ratkaista tietoturvallisesti.

3. Tiedustelu ja vakoilu

Tiedonhankinta ja valvonta ei välttämättä suoraan liity kyberuhkien havaitsemiseen ja torjumiseen.

Haitallisen vakoilun estäminen luo merkittävän suojan kyberuhkia vastaan. On siis tärkeää pyrkiä siihen että kansalaisten tiedot on suojattu mahdollisimman hyvillä teknologioilla koska se luo pitkällä tähtäimellä vahvan tietoturvatason joka suojaa rikollisuutta ja kyberuhkia vastaan.

Tiedustelu ja vakoilu ovat teknisesti ja tietoturvan kannalta hyvin lähellä toisiaan. Jos tietojärjestelmissä tai tietoliikenneyhteyksissä on tai rakennetaan tiedustelumahdollisuuksia, samoja teknisiä "aukkoja" voidaan käyttää myös vihamieliseen vakoiluun ei haluttujen tahojen toimesta.

Tästä on useita toteutuneita esimerkkejä eri maista (esimerkiksi puhelimien salakuuntelu Kreikassa käyttäen tiedustelua varten rakennettua laillista takaovea[2]).

Usein rikollisuus ja vakoilu, niiden uhka tai riski on paljon suurempi uhka talouden kehitykselle sekä kansalaisten ja yhteiskunnan vakaudelle ja vauraudelle verrattuna mahdollisiin epäsuoriin hyötyihin mitä tiedustelulla pystytään saavuttamaan.

4. Varautuminen kyberuhkiin

Tehokas ja järkevä tapa varautua kyberuhkiin olisi ennakolta suunnitella niihin reagoimiseen järkevät toimintamallit.

Internet ja sen luotettava toiminta on keskeinen osa nykyisen yhteiskunnan toimintaedellytyksiä. Tämän vuoksi myös kyberhyökkäykset tulevat tulevaisuudessa olemaan yhä todennäköisempiä sekä kaupallisten että muiden syiden vuoksi.

Esimerkiksi CERT-FI ja internet-palveluntarjoajat voisivat ennalta rakentaa toimintamallit ja kommunikaatiokanavat jotka voidaan ottaa käyttöön yhteen tai useampaan tahoon kohdistuvan kyberhyökkäyksen tapahtuessa.

Tällöin voitaisiin ennalta varautua ja minimoida hyökkäyksen vaikutuksia tehokkaalla yhteistoiminnalla ilman jatkuvia toimenpiteitä, jatkuvaa valvontaa tai ylimääräisiä tietoturvariskejä.

[2] http://en.wikipedia.org/wiki/Greek_wiretapping_case_2004–05

5. Yhteiskunnalle tärkeiden asioiden avoin valmistelu ja seuranta

Yhteiskunnan tärkeimpien asioihin liittyviä muutoksia pitäisi valmistella mahdollisimman avoimesti ja vahvan kansalaiskeskustelun kautta.

Internet ja sähköinen viestintä on nykyään erittäin merkittävä osa kansalaisten keskinäistä kanssakäymistä ja viestintää, mikä on länsimaisen demokraattisen valtion peruskiviä. Sen vuoksi kirjesalaisuuden ja vastaavien tietosuojalakien tulee kattaa myös kehittyvät viestintävälineet.

Mahdollisen valvonnan seuranta ("trust but verify") pitäisi myös järjestää avoimesti niin että kansalaisten luottamus voidaan pitää korkealla tasolla, sekä vähintään jälkeenpäin saada tietoon tapahtuneen valvonnan laji ja laajuus.

6. Taloudelliset vaikutukset

Suomessa on vahva tietotekninen palvelu- ja teknologiasektori jonka osuus kansallisen vaurauden luojana kasvaa jatkuvasti.

Tämän sektorin toiminnan kannalta on tärkeää että se voi tarjota sähköisiä palveluita ilman riskejä yksityisyyden suojan murtamisesta tai vakoilusta.

Jos luottamus yrityksiin rapistuu, siitä voi seurata merkittäviä strategisia pitkän tähtäimen taloudellisia tappioita, kuten on käynyt esim. amerikkalaisten yritysten tarjoamien palveluiden kanssa luottamuspulan vuoksi[3].

Suomessa on myös erittäin korkealaatuista tietoturvaosaamista ja siihen liittyvää vientiliiketoimintaa, esimerkiksi viime aikojen Heartbleed tietoturva-aukko löydettiin myös suomalaisen teknologiaosaamisen voimin[4].

7. Luottamus Suomeen

Suomen kannalta on tärkeä ylläpitää Suomen mainetta ja käytäntöjä puolueettomana ja tietoturvallisena maana joka voi nauttia korkean sisäisen ja ulkoisen luottamustason tuomasta vauraudesta ja vapaudesta.

---

[3] http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html
[4] "Haavoittuvuus OpenSSL-kirjaston versiossa 1.0.1", CERT-FI, https://www.cert.fi/haavoittuvuudet/2014/haavoittuvuus-2014-049.html