

signaali

Viestintäviraston asiakaslehti 4/2009

TAAJUUKSIEN KÄYTTÖÄ
TEHOSTAMASSA

18

Vaihtopenkillä
ministeri Kiviniemi:
**HAJAUTETUT REKISTERIT
YHDEN KÄYTTÖLIITTYMÄN
TAAKSE** 9

**KANSAINVÄLISTÄ
TIETOTURVAA** 2

SOSIAALINEN MEDIA
– hyvä vai paha? 14

TURVALLISESTI tietoverkkotaloudessa

Viestintäviraston uusi NCSA-yksikkö raivaa tietä kansainväliselle yhteistyölle. Teksti: Maarit Seeling Kuvitus: Jaska Poikonen Kuva: Jyrki Komulainen

Suomeen saadaan ensi vuoden alussa uusi tietoturvatointi, kun Viestintäviraston NCSA-toiminta käynnistyy. Yksikön tarkoitus on muun muassa tarkastaa tietojärjestelmien tietoturva vaatimuksia ja näin helpottaa kansainvälistä yhteistyötä sekä turvaluokitellun tiedon asianmukaista käsittelyä.

Ammattimaisesti kohdennettujen tietoturvahyökkäysten määrä lisääntyy maailmalla huikaa vauhtia. Samalla vaatimukset turvaluokitellun tiedon suojaamiselle kasvavat. Kansainvälisissä yhteistyöhankkeissa vaaditaankin yhä useammin kansallisen

tietoturvaluusviranomaisen lausunto järjestelmien tai tuotteiden turvallisuustasosta ja luotettavuudesta.

– Tietoturvanäkökohdat on huomioitava kaikissa tiedonkäsittelyn vaiheissa. Suomi elää kansainvälisessä tietoverkkotaloudessa. Monet suomalaiset yritykset ja yhteisöt ovat törmänneet tilanteeseen, jossa kaupan tai sopimuksen teko tai tiedon saaminen on vaikeutunut, koska meiltä on puuttunut virallinen kansallinen tietoturva viranomaisen, joka antaisi tietojärjestelmille turvaluokituksia, Viestintäviraston verkot ja turvallisuus -tulosalueen johtaja **Timo Lehtimäki** sanoo.

Kansainvälisesti vakioitu kansallinen tietoturva viranomaisen (NCSA eli National Communications Security Authority) keskitetty vastedes täyttämään Suomen kansainvälisiä tietoturvaluusvelvoitteita.

Virastoa konsultoidaan, kun asia koskee kansainvälisen turvaluokitellun tiedon sähköistä käsittelyä. Tietojärjestelmien tarkastamisen ja järjestelmätoteutusten hyväksymisen lisäksi NCSA:n vastuulle tulevat tuotesertifiointien hallinta sekä salausmenetelmiin liittyvien avaimistojen hallinnointi.

Teollisuuden kansainvälisen kilpailukyvyyn parantamisen lisäksi yksikön tarkoituksena

» CERT-FI uusii tietoturvamääräyksiä

Viestintävirasto uudistaa tietoverkkojen toimivuuteen ja vikasietoisuuteen liittyviä määräyksiään; CERT-FI:lle on siirretty yhä enemmän vastuuta tietoturvaloukkauksen torjuntaan liittyvien määräysten uudistamisesta.

– Sähköisten palveluiden tarjoajalla on suuri vastuu palveluiden käytön turvallisuuden varmistamisessa. Käyttäjien puolestaan on kyettävä tunnistamaan uhkat ja tiedettävä, millaiset ehdot turvallisen palvelun on täytettävä, CERT-FI:n päällikkö **Erka Koivunen** tiivistää.

CERT-FI:n valmisteluun ja valvontaan on tässä vaiheessa siirtynyt kolme Viestintäviraston määräystä eli määräys numero 9, joka koskee tietoturvaloukkausten ilmoitusvelvollisuutta yleisessä teletoiminnassa, sähköpostin tietoturvaa käsittelevä määräys numero 11 sekä numero 13, joka liittyy internet-yhteyspalveluiden tietoturvaan ja niin sanottuun ”osoitehygieniaan”.

Sähköpostin tietoturvaa koskeva määräys uudistettiin viime vuonna. Tietoturvaloukkauksien ilmoitusvelvollisuutta koskeva määräys on viittä vaille valmis, ja sen on tarkoitus tulla voimaan ensi vuoden alusta.

– Mullistavasta muutoksesta ei ole kyse, koska laki taustalla ei ole muuttunut. Olemme vain halunneet kirjata entistä selkeämmin tele-

yritysten velvollisuuden ilmoittaa tietoturvahyökkäyksiä myös silloin, kun viestintäsalaisuuden toteutumista uhkaa ulkopuolinen taho, Koivunen kertoo.

Yksistään tänä vuonna CERT-FI:lle on jo tullut 70 palvelunestohyökkäykseen liittyvää ilmoitusta. Lähes kaikki ilmoitukset ovat tulleet ulkomailta. Koivunen korostaa, että teleyritysten on kyettävä havaitsemaan verkkonsa tietoturvaongelmat ja reagoimaan niihin sekä myös tiedottamaan ongelmista. Operaattoreiden puuttuminen häiriöihin on tärkeää, sillä käyttäjä ei yleensä itse huomaa koneensa saastumista.

– Perinteisen teleyritystoiminnan ulkopuolelle jää runsaasti ICT-palveluita, kuten keskitetyt konesalipalvelut ja sovellusvuokraus. Näistä palveluista Viestintäviraston ohjaus- ja valvontatoimessa on käyty jo jonkin aikaa keskustelua. Sääteilytarve on varsin selkeästi konkretisoitunut juuri tämältyypistien palvelutarjoajien tietoturvan hallintaan, Koivunen sanoo.

Ensi vuonna CERT-FI:n käsittelyyn tulee internet-yhteyspalveluiden toteutumista koskeva määräys numero 13. Tietoturva yksikkö kerää paraikaa teleyrityksiltä ja muilta sidosryhmiltä perustietoja määräyksen pohjaksi.

NCSA-yksikköä konsultoidaan, kun asia koskee kansainvälisen turvaluokitellun tiedon sähköistä käsittelyä, johtaja Timo Lehtimäki kertoo.





na on eri osapuolten intressien suojaaminen esimerkiksi Suomen ja NATO:n rauhankumppanuushankkeissa tai EU-tiedonvaihdossa.

Hajautettu valvontamalli säilyy

Suomessa kansainväliset turvallisuusasiat ovat hajautettuina Viestintävirastoon perustettavan uuden yksikön lisäksi kolmelle muulle viranomaiselle eli Suojelupoliisille, Puolustusvoimille ja Pääesikunnalle. Uuteen NCSA-yksikköön kootaan ensi vuodesta lähtien nimenomaan tietojärjestelmien turvallisuuteen ja salaustenmenetelmiin liittyvää osaamista. Kansallisen turvallisuusviranomaisena (NSA) toimintaa koordinoi ulkoasiainministeriö.

— Aivan tarkkaa tietoa ei ole saatavissa siitä, miten NCSA-toiminta eri maissa on järjestetty. Suomen malli on kuitenkin hyvin tavanomainen pienehköissä valtioissa, joissa ei ole ollut mielekasta perustaa yhtä yksittäistä organisaatiota käsittelemään kaikkia asioita. Nyt ei siis perusteta uutta virastoa. Viestintävirasto saa vain uuden vastuualueen, Lehtimäki selventää.

Viestintäviraston uuden turvallisuusyksikön perustamiseen on varattu valtion ensi vuoden budjetista 650 000 euroa. Alkuvaiheessa toiminta käynnistyy yksikön päällikön ja kahden asiantuntijan voimin. Lehtimäki arvioi tehtävän hoitamisen edellyttävän noin kymmentä henkilötyövuotta vuoteen 2014 mennessä. ✘



Sisällys

- 2** NCSA-yksikön kansainvälinen tehtävä
- 5** Pääkirjoitus: Kirsi Karlamaa
- 6** Ajankohtaista
- 8** Linkkivinkit
- 9** Vaihtopenkillä ministeri Mari Kiviniemi
- 10** Uudet uhkat vaativat teollisuusautomaatiota
- 11** Päätös Itellan hinnoitteluun
- 12** Syötteitä tarkastamaan!
- 14** Sosiaalisen median arvo ja arvaamattomuus
- 17** Häiriöttömiä radiolaitteita
- 18** Uusia määräyksiä vuodenvaihteessa
- 19** Taajuuksien hallinnontia
- 20** Energiateollisuudessa taajuudet vahtivat virtaa
- 21** Kolumni: Juhapekka Ristola, liikenne- ja viestintäministeriö
- 22** Svensk resumé
- 23** English summary



Pääkirjoitus

TAAJUUSHALLINTO VARAUTUU TULEVAAN

Elinkeinoelämän kilpailukyvyyn turvaamisessa tehokas taajuushallinto on hyvin keskeisessä roolissa. On nähtävissä, että viestinnän palvelujen määrä lisääntyy ja yhä useammat käyttötarpeet kilpailevat niukoista taajuusresursseista samoilla halutuilla kustannus- ja tehokkailta taajuusalueilla.

Yhteiskunnan tarpeet luovat muun muassa uusia ja kehittyneitä langattomia sovelluksia, jotka muuttavat ihmisten elintapoja ja tuovat mukanaan uusia palveluja. Uudet sovellukset hyödyntävät usein jo olemassa olevia radioverkkoja ja luovat näin paineita eri radiojärjestelmien ja sovellusten tekniseen yhteensovittamiseen. Uusien palvelujen tuomien ratkaisujen teknisten haasteiden lisäksi taajuuspäätöksissä on otettava huomioon myös viestintämarkkinoiden toimivuus.

Taajuushallintoon kohdistuu yhä enemmän vaatimuksia olla tiedollisesti kehittyvien uusien teknologioiden eturintamassa. Jopa edellä, aistien jo seuraavaa teknologista askelta. Jatkuvana haasteena on tehostaa kysynnän ennakkointia, ymmärtää pitkällä tähtäimellä tulevaisuuden taajuustarpeet ja huomioida tämä jokapäiväisessä taajuussuunnittelussa.

Kulunut vuosi on ollut taajuusmielessä erityisen mielenkiintoinen ja haastava. Taajuuksien uudelleensuunnittelun tuloksena oli mahdollista myöntää riittävän suuri ja yhtenäinen taajuusalue 1800 MHz:n alueelta matkaviestinoperaattoreille LTE-tekniikan käyttöön. Tämä teki Suomesta ensimmäisen maan Euroopassa, joka sallii LTE-tekniikan käytön näin alhaisilla taajuuksilla. HDTV eli

teräväpiirtotelevisio on tullut jäädäkseen. Analogisilta tv-taajuuksilta vapautuneiden VHF-taajuuksien käytöstä on sovittu naapurimaiden kanssa ja ensimmäiset valtakunnalliset HDTV-toimiluvat on myönnetty. Loppuvuonna Viestintävirasto toteutti teknisesti ja toimi meklarina 2,6 GHz:n taajuushuuto-kaupassa, joka oli Suomessa ensimmäinen laatuaan.

Mitä on vielä tulevaisuudessa tarjolla? Modulaatiotekniikat kehittyvät, mikä tarkoittaa enemmän bittejä samalle kaistalle. Kaikki digitalisoitavissa olevat prosessit digitalisoidaan. Uudet jakelutekniikat, kuten DVB-T2, mahdollistavat laaja-alaisempia yhden taajuuden televisioverkkoja. Kognitiiviset radiojärjestelmät, jotka osaavat havainnoida ympäristöään, hyödyntää mukautuvaa lähetystekniikkaa ja kommunikoida monipuolisesti ympäristönsä kanssa, yleistyvät tulevaisuudessa vähitellen. Tästä seuraa taajuuksien yhä tehokkaampi käyttö. Tehokas hyödyntäminen tarkoittaa myös tulevaisuudessa yhä enemmän taajuuksien yhteiskäyttöä ja taajuuksien jakoa teknologia- ja palveluriippumattomasti.

Pitkälläkään aikavälillä taajuuksista ei tule merkittävää pulaa, mutta tämä vaatii taajuushallinnolta jatkuvaa "tutkailua" ja "antennien suuntausta" oikeaan kohteeseen.

Kirsi Karlamaa
johtaja, radiotaajuudet

Kuva:
Kaapo Kamu



Kulunut vuosi on ollut taajuusmielessä erityisen mielenkiintoinen.



Julkaisija

Viestintävirasto
PL 313
00181 HELSINKI
Puhelin 09 69 661
Faksi 09 6966 410
www.ficora.fi

Päätoimittaja

Anna Lauttamus-Kauppi

Toimituspäällikkö

Marko Eriksson

Viestintätoimisto

Mediafocus

Taitto

Jaska Poikonen

Kannen kuva

Jari Härkönen

Takakannen kuvitus

Leena Kumpulainen

Painopaikka

Edita Prima,
Helsinki

Toimitusneuvosto

Viestintävirasto: Tiina Aaltonen,
Martin Andersson, Marko Eriksson,
Paula Jokinen, Kari Kangas,
Anna Lauttamus-Kauppi,
Jarkko Saarimäki, Pekka Sillanmäki
FiCom Ry: Nora Elers
Mediafocus Oy: Tiia Soininen

Palautteet, tilaukset ja
osoitteenmuutokset
Ira Markkaselle:
ira.markkanen@ficora.fi

Seuraava numero
Maaliskuu 2010

ISSN 1458-5715



Telepalvelujen hintataso Suomessa 2008

Viestintävirasto on selvittänyt kotitalousasiakkaiden telepalvelujen hintatason kehitystä Suomessa vuonna 2008 verrattuna vuoteen 2007. Virasto teki selvityksen nyt ensimmäistä kertaa. Aiemmin telepalvelujen hintatason seurannasta on vastannut liikenne- ja viestintäministeriö.

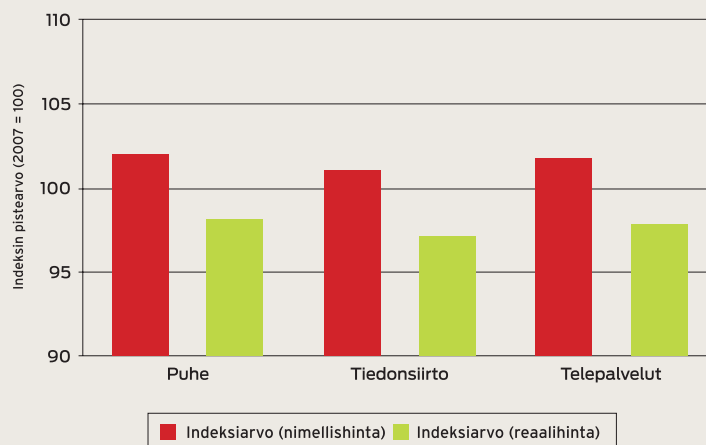
Selvityksen mukaan telepalvelujen nimellishinnat kokonaisuudessaan ovat nousseet vuodesta 2007 vuoteen 2008 noin kaksi prosenttia. Puhepalveluiden nimellishinnat ovat nousseet pari prosenttia ja tiedonsiirtopalveluiden nimellishinnat noin prosentin. Vastaavat reaali hinnat ovat kuitenkin laskeneet kahdesta kolmeen prosenttia eli telepalveluiden hintataso on noussut muita kuluttajahintoja hitaammin.

Tiedot selvitystä varten on kerätty teleyrityksiltä. Telepalvelut on ryhmitelty siten, että ne on jaettu kahteen pääkomponenttiin: tiedonsiirto- ja puhe-

palveluihin, jotka ovat edelleen jaettu matkaviestinverkon ja kiinteän verkon palveluihin. Selvityksessä kunkin palvelun keskimääräinen hinta on laskettu jakamalla tulot volyymeilla. Esimerkiksi kiin-

teän verkon puhepalveluissa kotitalouksilta saadut tulot on jaettu kotitalouksien soittamilla minuuteilla. Palvelukohtaiset indeksit on muodostettu näiden keskiarvojen avulla.

Kuvio: Telepalveluiden hintatasoindexien pääkomponentit vuodelle 2008



EU:n viestintälainsäädäntö-uudistuksesta sopimus

Euroopan parlamentin valtuuskunta lupoi muutosehdotuksesta, jonka mukaan internetin käyttöä olisi voinut rajoittaa ainoastaan tuomioistuimen päätöksellä. Käyttäjälle taataan kuitenkin kuuleminen, jos telepalvelun käyttö on pakko katkaista. Direktiivit on määrä hyväksyä marraskuun lopussa sekä parlamentissa että ministerineuvostossa.

Uudistuksen tavoitteena on parantaa sääntelyä, tehostaa sisämarkkinoita ja edistää kuluttajien oikeuksia. Uudistus antaa lisävaltuuksia komissiolle. Komissio voisi muun muassa laatia monivuotisen taajuuspolitiikkaohjelman. Lisäksi komissio voisi vaikuttaa huomattavan markkinavoiman velvoitteisiin, vaikkei sille myönnetty veto-oikeutta. Komissiolla olisi mahdollisuus antaa sitovia harmoni-

sointipäätöksiä kaksi vuotta suosituksen antamisen jälkeen, jos suositus ei ole tuonut toivottua tulosta. Lisäksi komissio voisi, kuultuaan ensin Euroopan verkko- ja tietoturvavirastoa, hyväksyä teknisiä täytäntöönpanotoimenpiteitä tietoturvaloukkausten tiedotus- ja ilmoitusvaatimuksiin.

Asetuksella perustetaan kansallisten viestintäviranomaisten toimiin BEREC, joka korvaa nykyisen European Regulators Groupin. BEREC antaisi lausuntoja muun muassa sääntelyehdotuksista ja huomattavan markkinavoiman päätöksistä komissiolle. Sen toimintaa rahoitettaisiin yhteisövaroin ja mahdollisesti jäsenmaksuilla. BERECin sijaintipaikasta päättää ministerineuvosto myöhemmin tänä vuonna.

Lainsäädäntöuudistus parantaa viestintäpalveluiden käyttäjien asemaa. Teleyritysten tulisi sopimuksissa kertoa tarjottavien palvelujen laadun vähimmäistaso. Lisäksi jäsenvaltiot voisivat asettaa palvelutasoa koskevia vaatimuksia teleoperaattoreille. Puhelinnumeron siirrettävyys tulisi toteuttaa yhden työpäivän aikana. Myös tietoturva koskevaa sääntelyä lisätään, mutta vastaavanlaiset vaatimukset ovat pitkälti Suomessa jo voimassa.



Uudistuksen tavoitteena on parantaa sääntelyä, tehostaa sisämarkkinoita ja edistää kuluttajien oikeuksia.

Lakimuutos vaikuttaa teleyritysten tietoturva-tiedottamiseen

Ruotsin puolustusvoimien radiolaitoksella on ollut mahdollisuus joulukuun alusta alkaen seurata maanpuolustustarkoituksessa Suomesta Ruotsin kautta ulkomaille suuntautuvaa sähköistä viestintää. Merkittävä osa Suomesta ulkomaille menevästä tietoliikenteestä kulkee Ruotsin kautta.

Ruotsin kautta kulkevan tietoliikenteen tiedustelutoiminta on huomioitu Viestintäviraston 1.1.2010 voimaan tulevassa määräysudistuksessa, joka koskee tietoturvaloukkausten ilmoitusvelvollisuutta. Siinä korostetaan erityisesti teleyritysten velvollisuutta tiedottaa asiakkailleen ulkomailla toteutettaviin, suomalaisille asiakkaille tarjottaviin palveluihin kohdistuvista tietoturvauhkista. Ilmoitusvelvollisuus perustuu sähköisen viestinnän tietosuojalakiin.

Internetin käyttäjät voivat suojata viestit tarvittaessa

Jokaisen internetin käyttäjän on syytä miettiä, mitä viestintäpalveluja käyttää ja minkälaisia suojaustoimia niissä käytetään. Suojausta vaativat viestit voi tarvittaessa salata. Lisätietoja viestinnän suojaamisesta löytyy Viestintäviraston yhdessä alan toimijoiden kanssa julkaisemalta viestinnän suojaamista koskevalta sivustolta www.ficora.fi/viestinsuojaus. Sähköisen viestinnän suojaaminen oli esillä myös vuoden 2009 helmikuussa järjestettynä Tietoturvapäivänä.



Merkittävä osa Suomesta ulkomaille menevästä tietoliikenteestä kulkee Ruotsin kautta.

FiCom kymmenen vuotta

Kymmenen vuotta sitten, tarkalleen 23.11.1999, joukko keskeisiä ICT-alan yrityksiä allekirjoitti Tietoliikenteen ja tietotekniikan keskusliiton perustamis-sopimuksen. Syntyi toimialajärjestö, joka on kymmenen vuoden aikana ottanut paikkansa yhteiskunnallisena vaikuttajana ja yhteistyötahona.

FiComin toiminnan luonne ja ennen kaikkea laajuus ovat muuttuneet kymmenen vuoden aikana olennaisesti. Aivan alkuvaiheessa kansallisella tasolla saatettiin hieman karrikoiden puhua yhteistoiminnan triangelistä, jonka kulmat olivat liikenne- ja viestintäministeriö, Viestintävirasto ja toimialan edustajat. Hyvin nopeasti yleinen tietoyhteiskuntakehitys toi yhteistyöhön mukaan myös hallinnon muut haarat ja yhteiskunnan kaikki toimintalohkot.

Tietoliikenne ja tietotekniikka ovat nykyisin keskeisiä elementtejä erilaisten toimintojen tehostamiseksi. Ilman ICT-palveluiden ja -tuotteiden laajapohjaista käyttöä ei selvitä sellaisista yhteiskunnallisista

haasteista kuten ilmastonmuutos, väestön ikääntyminen ja alueellisen tasa-arvon heikkeneminen. Toimialan yrityksillä on Suomelle merkitystä myös laajemmin tarkasteltuna: hakemalla saa hakea toista toimialaa, joka investoi vuodesta toiseen jopa puoli miljardia euroa tämän maan rajojen sisäpuolelle. Keskeisiä satsauksia ovat tietysti sekä kiinteän että langattoman verkon investoinnit, mutta myös laajat investoinnit järjestelmiin ja palveluihin.



Harri Pursiainen liikenne- ja viestintäministeriöstä, Reijo Svento FiComista ja Jyrki Alkio Talouselämästä nostivat maljan kymmenvuotiaalle.

Fi-verkkotunnusten hinnat laskevat

Vuodenvaihde alentaa fi-verkkotunnusten hintoja. Viestintäviraston esityksen mukaan esimerkiksi fi-verkkotunnus vuodeksi maksaa 13 euroa aiemman 15 euron sijaan.

Uudet fi-verkkotunnus-hinnat astuvat voimaan 4.1.2010.

VOIMASSAOLOAIKA	2010
1 vuotta	13 euroa (vanha hinta 15 euroa)
3 vuotta	36 euroa (vanha hinta 41 euroa)
5 vuotta	55 euroa (vanha hinta 60 euroa)

Teletointaohjetta päivitettiin

Viestintävirasto on päivittänyt ohjeen teletointailmoituksen antamisesta. Sen tarkoituksena on toimia tulkintaohjeena ilmoitusvelvollisuuden alaisen yleisen teletointinnan määrittämiseksi.

Yleisen teletointinnan harjoittamisesta on ennen toiminnan aloittamista tehtävä

kirjallinen ilmoitus Viestintävirastolle (Viestintämarkkinalain 13 §). Teletointailmoituksella ei ole itsenäistä oikeuksia tai velvollisuuksia luovaa merkitystä, vaan ilmoitus on tarkoitettu valvontaviranomaisen työn apuvälineeksi.

Ohje teletointailmoituksen antamisesta on tehty vuonna 2003. Nyt ohjeen kehittämiselle ja yleisen teletointinnan määrittämisen täsmennykselle oli selkeä tarve: yritysten palvelumallit ovat uudistuneet ja markkinat muuttuneet. Se, mitä katsotaan yleiseksi teletointinnaksi, vaikuttaa muun muassa teleyrityksen maksettavaksi tulevan viestintämarkkina- ja tietoturvamaksun suuruuteen. Edellä mainitut maksut

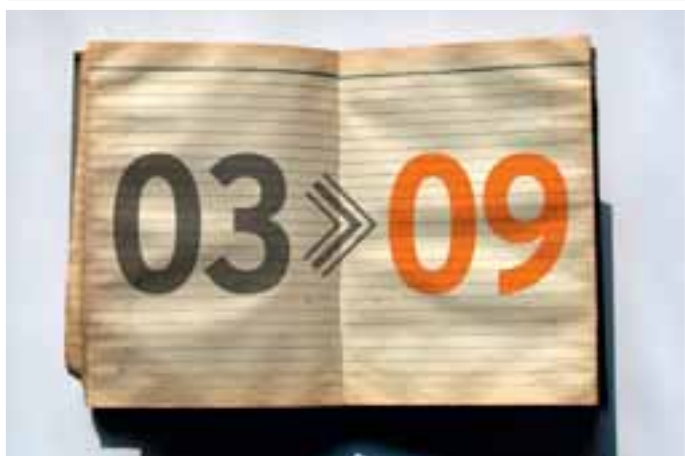
perustuvat yrityksen harjoittaman yleisen teletointinnan liikevaihtoon.

Yleisen teletointinnan määrittelmä

Yleisellä teletointinnalla tarkoitetaan laissa verkkopalvelun tai viestintäpalvelun tarjoamista käyttäjäpiirille, jota ei ole etukäteen rajattu. Merkityksellistä arvioinnissa on itse toiminnan luonne, ei esimerkiksi palveluntarjoajan lainsäädännöllinen asema. Siten esimerkiksi kunta, oppilaitos tai it-palveluntarjoaja voi olla lain tarkoittama teleyritys.

Ilmoitusvelvollisuus ei koske merkitykseltään vähäistä teletointintaa harjoittavia yrityksiä. Merkitykseltään vähäinen teletointinta on määritelty valtioneuvoston asetuksessa — yksi määrittävistä tekijöistä on, että toiminnan liikevaihto on alle 300 000 euroa vuodessa.

Viestintävirasto antaa tarvittaessa tapauskohtaisia ohjeita teletointailmoituksen antamisesta.



LINKKIVINKIT

Linkkivinkkejä nettiturvallisuuteen

Verkossa on useita hyviä sivustoja, jotka käsittelevät turvallista ja fiksua internetin ja muiden sähköisten medioiden käyttöä. Näiltä sivustoilta löytyy hyviä vinkkejä kuluttajille, vanhemmille ja opettajillekin.

Tietoturvakoulu.fi on tarkoitettu peruskouluille ja lasten vanhemmille. Sivustolla on tarjolla tietoa, tarinoita, pelejä ja opetusmateriaaleja laajasti turvalliseen netin käyttöön liittyvistä aiheista: yksityisyys netissä, nettikiusaaminen, tekijänoikeudet, kuvien julkaisu netissä, nettikavereiden tapaaminen jne. Tietoturvakoulussa toimii myös maksuton Kummipankki-palvelu, jonka kautta koulut voivat tilata asiantuntijan kertomaan turvallisesta netin käytöstä.

Tietoturvaopas.fi opastaa muun muassa turvalliseen verkkoasiointiin, tietokoneen teknisen tietoturvan ylläpitoon, kannettavan tai käytetyn tietokoneen turvalliseen käyttöön sekä roskapostin välttämiseen. Sivustolta löytyy oma osionsa myös pk-yrityksille.

Peliraati.fi-sivustolla vanhemmat arvioivat toisille vanhemmille netti-, tietokone-, video- ja konsolipelejä. Arvioiden tarkoituksena on antaa tietoa pelien sisällöistä lasten kasva-

tuksen tueksi: mitä olisi hyvä tietää pelejä valittaessa ja miten mahdollisiin arveluttaviin pelisisältöihin tulisi suhtautua. Vanhemmat tekevät peliarviot yhdessä lasten kanssa.

Mii.fi/vanhempainnetti vastaa osiossa Lapset ja media muun muassa kysymyksiin millaisia verkkopalveluja lapset ja nuoret käyttävät, miten turvallista netin käyttöä voi opettaa kotona, miten esto-ohjelmat toimivat ja millaisiin myönteisiin ja kielteisiin ilmiöihin lapset ja nuoret voivat törmätä digitaalisen media äärellä.

Mediakasvatus.fi on portaali lasten, nuorten ja median kanssa työskenteleville ammattilaisille, tutkijoille ja vanhemmille. Sivustolta löytyy tietoa mediakasvatuksesta, blogeja, keskustelupalsta sekä vanhemmille tiivis tietopaketti, joka kattaa laajasti sähköiset ja perinteiset mediat.



Vuosikymmenessä vuosisadan tavoitteeseen

Valtion tavoite on palvella hallinnon asiakkaita, meitä Suomen kansalaisia, entistä paremmin ja tehokkaammin.

Hallinto- ja kuntaministeri **Mari Kiviniemi** ei lupaa, että Suomeen rakennettaisiin yksi kaikkien kansalaisten kaikki tiedot kattava rekisteri. Timo Laitisen kysymystä hän kuitenkin luonnehtii relevantiksi.

– Nykytilanne, jossa suomalaisten tiedot on hajautettu eri rekistereihin, ei ole hyvä. Kansalaisilla ei ole mahdollisuutta seurata kaikkia tietojaan. Mutta keskitetyn rekisterin rakentaminen olisi kokonaisen vuosisadan projekti, Kiviniemi sanoo.

Nykytilanne on se, että Suomessa on yksi keskitetty asiakasrekisteri: väestörekisteri. Sen tietosisältö on kuitenkin hyvin rajallinen. Väestörekisteristä löytyvät käytännössä vain osoitetiedot ja sukulaisuussuhteet. Kaikki muut tiedot terveydentilasta työuraan ovat hajautettuina eri tietokantoihin.

– Jos kaikkia eri tietokannoissa olevia tietoja varten rakennettaisiin yksi asiakasrekisteri, urakka olisi hurja. Yhden rekisterin pitäisi pystyä kattamaan kaikki hallinnon toimet, kaikki mahdolliset asiakkuuden tilanteet. En pysty edes arvaamaan, mitä sellainen maksaisi, Kiviniemi korostaa.

Hän pitää rekisterin rakentamiskustannuksia kohtuuttoman suurina, vaikka otettaisiin huomioon, että yhden rekisterin ylläpitäminen olisi huomattavasti helpompaa ja siten edullisempää kuin nykyisten kymmenien ellei satojen erillisten tietokantojen. Kustannusten ohella ison kysymysmerkin muodostavat tietoturva-riskit.

Väärinkäytön vaara

Mitä kattavampi rekisteri, sitä vakavampi on luonnollisesti ongelma, jos rekisteriä käytetään väärin.

– Jos joku asiaton rekisteriin pääsee, hänellä on teoriassa mahdollisuus muuttella ihmisten tietoja ja joka tapauksessa saada ihmisistä paljon tietoa. Tiedon väärinkäyttö on riski, Kiviniemi toteaa.

Ministeri myöntää, ettei ole tietoturvan osaaja eikä riskien kartoittaja ja uskoo, että keskitetyssäkkin rekisterissä tietoturva olisi mahdollista taata. Eihän verkkopankeissakaan ole juuri ollut ongelmia. Mutta teoreettinen riski on ja pysyy.

– Sen sijaan vuosikymmenessä pystymme saavuttamaan sen tavoitteen, johon keskitetyllä rekisterillä kansalaisen näkökulmasta pyrittäisiin – korjaamaan hallitusti nykytilanteen.

– Se tarkoittaa nykyisten rekistereiden yhteentoimivuuden lisäämistä ja tehokkaampaa koordinoitua, valtion on toimittava tulevaisuudessa konsernimaisesti. Koko summaa emme pysty hetkessä purkamaan, mutta tavoitteena on vaiheittain saada eri rekisterit kansalaisen näkyville ja nimenomaan näkyville yhden käyttöliittymän kautta. Pitkällä tähtäimellä olisi hyvä saada myös yritysten rekisterit mukaan saman käyttöliittymän taakse, Kiviniemi visioi.

Mari Kiviniemi

- syntynyt Seinäjoella 1968
- koulutukseltaan valtiotieteiden maisteri
- työskennellyt hallinto- ja kuntaministerinä huhtikuusta 2007
- toimii myös Keskustan kansanedustajana ja Helsingin kaupunginvaltuutettuna
- perheeseen kuuluvat aviomies **Juha Louhivuori** sekä vuosina 1997 ja 2000 syntyneet lapset

Edellinen vaihtopenkkivieras Valtiokonttorin pääjohtaja **Timo Laitinen** esitti hallinto- ja kuntaministeri Mari Kiviniemelle seuraavan kysymyksen: Suomen julkiselta sektorilta puuttuu yksi yhteinen kansalaisten ”asiakasrekisteri”. Kustannustehokainta ja käytettävyyden kannalta helpointa olisi, jos kansalaisten kaikki henkilö- ja elinkaaritiedot keskitettäisiin yhteen rekisteriin. Onko realistista odottaa tällaisen rekisterin syntyvän ja miten saavutetaan malli, jossa tehokas hallinnointi, helppo asiointi, hyvä tietoturva ja yksityisyydensuoja ovat tasapainossa?

Hallinto- ja kuntaministeri Mari Kiviniemi haluaa haastaa seuraavaksi vaihtopenkkiläiseksi Kuntaliiton toimitusjohtaja **Kari-Pekka Mäki-Lohiluoman**. Kysymys kuuluu:

Miten kunnat saadaan mahdollisimman nopeasti yhdessä valtion kanssa edelläkävijöiksi sähköisten palveluiden tarjoajana ja millaisena kunnissa nähdään valtion rooli?

Teksti: Tiia Soininen
Kuva: Jyrki Komulainen



UUDET UHKAT VAANIVAT teollisuusautomaatiota

TITAN-HANKE KOKOAA KAIVATTUA OHJEISTUSTA AUTOMAATIO-TEOLLISUUDEN JA TUOTANTOLAITOSTEN TIETOTURVAAMISEEN.

Pahaa-aavistamaton huoltomies tuo tietokoneensa ohiolaiseen ydinvoimalaan Yhdysvalloissa vuoden 2003 tammikuussa. Laitteessa lymyää kulovalkean tavoin leviävä Slammer-mato, mutta tätä mies ei tiedä.

Mato sulkee voimalaitoksen turvallisuuden seurantajärjestelmän viideksi tunniksi. Henkilökunta ei osaa epäillä syyksi haittaohjelmaa, sillä voimalan toiminnassa käytettävä verkko on eristetty internetistä.

Ydinvoimalan turvallisuus ei ollut vaarassa. Laitoksella ei ollut tuotettu sähköä vuoteen. Tapaus kuvaa kuitenkin uusia uhkia, jotka vaanivat teollisuuden tietojärjestelmiä. Viimeisten vuosikymmenten aikana verkostoituneet tietokonejärjestelmät ovat alkaneet ohjata muun muassa tehtaiden tuotantoa, voimalaitoksia sekä energian ja veden jakeluverkkoja.

— Pahimmassa kauhuskenaariossa järjestelmään tunkeutunut henkilö pääsee vaikuttamaan tuotantolaitoksen alijärjestelmään tai ohjaamaan tiettyä laitetta. Tietoturvaloukkauksia on ollut Suomessa vähän, mutta murtautuminen voi olla mahdollista mihin tahansa tietoliikenneyhteydet sisältävään järjestelmään, VTT:n erikoistutkija **Pasi Ahonen** sanoo.

Lääkkeitä teollisuusautomaation turvaamiseen

Teollisuusautomaation järjestelmien tietoturvan varmistamiseen on toistaiseksi olemassa koostetusti vain vähän selkeää ohjeistusta ja työkaluja. VTT:n Pasi Ahonen vetää kaksivuotista TITAN-hanketta, joka valmistuu maaliskuussa. Hankkeen rahoittajana toimii Tekesin Turvallisuus-ohjelma.

Suomalaiset automaatiotekniikkaa hyödyntävät yritykset painivat hänen mukaansa erityisesti kahden pääongelman kanssa.

— On olemassa kymmeniä erilaisia tietoturvastandardeja, joita voidaan käyttää. Kaikki eivät kuitenkaan tunne toisten käytämiä standardeja, mikä saattaa aiheuttaa väärinymmärryksiä. Lisäksi käytössä on van-

hoja laitteita, joiden joukkoon on asennettu uusia laitteita. On iso haaste pitää järjestelmä tietoturvallisena kaikkina ajankohtina ja kokonaisuutena, Ahonen sanoo.

TITAN-hanke tuo valmistuessaan organisaatioiden käyttöön parhaiden käytäntöjen kuvauksia. Lisäksi se arvioi eri testaustyökalujen soveltuvuutta tietoturvan varmistamiseen, ohjaa vähentämään haavoittuvuuksia ja ennaltaehkäisemään uhkia. Luvassa on myös kansainvälinen seminaari hankkeen tuloksista.

Tietoturvasta tuli mainosvaltti

Teollisuusautomaation suurin mullistus on tapahtunut viimeisen vuosikymmenen aikana. Tuotantolaitokset ovat siirtyneet käyttämään enenevässä määrin samoja ohjelmistopalustoja ja tiedonsiirtoprotokollia kuin muukin tieto- ja viestintäteknologia.

— Jos järjestelmä yritetään pitää irti internetistä, se potkaisee helposti takaisin.

Uhkak voivat tulla nykyisin yhtä lailla tuotantolaitokseen tuodun kannettavan tietokoneen tai muistitikun mukana, joten verkko ei olekaan eristetty muista toimijoista vaikka niin kuviteltaisiin, Ahonen korostaa.

Tietoisuus teollisuusautomaation järjestelmiin kohdistuvista uhkista on viime vuosina kasvanut Suomessa. Aikoinaan järjestelmäkauppiat saattoivat vähätellä mahdollisia tietoturva-uhkia, mutta nykyisin hankinnoista vastaavat osaavat Ahosen mukaan vaatia standardien mukaisempaa tietoturvaa, josta on tullut myös järjestelmien kehittäjille mainosvaltti.

Teollisuusautomaation turvallisuudessa on viime kädessä kyse koko yhteiskunnan pyörien pyörimisestä. Asiasta huolehtii korkeimmalla tasolla Huoltovarmuuskeskus, jota Viestintävirasto ja sen CERT-FI-tietoturvayksikkö tukevat asiantuntemuksellaan.

— Myös sähköverkkojen toiminta vaatii nykyisin tietoliikenneverkkoja, jotka taas ovat riippuvaisia sähköstä, Ahonen muistuttaa. ✕



Teollisuusautomaatiassa tietoturva pitäisi huomioida jo järjestelmän kehitys- ja tilausvaiheessa, korostaa TITAN-hanketta vetävä VTT:n erikoistutkija Pasi Ahonen.

PÄÄTÖS Itellan hinnoitteluun

Viestintävirasto antoi lokakuussa 2009 Itella Oyj:lle päätöksen yleispalvelutuotteiden hinnoittelusta. Päätöksessä yhtiö veloitettiin muuttamaan yleispalvelutuotteiden hinnoittelu postipalvelulain mukaiseksi. **Teksti:** Marja Lehtimäki **Kuvitus:** Leena Kumpulainen

Yleispalvelutuotteiden hintojen tulee olla kohtuullisia ja kustannuksiin sovitettuja, todetaan postipalvelulaissa. Viestintäviraston selvityksen mukaan Itella on kohdentanut yleispalvelutuotteille liikaa kustannuksia, eivätkä yhtiön perimät yleispalvelutuotteiden maksut ole lain mukaisia.

Itellan käyttämä kustannusten kohdentamistapa ei tietyin osin huomioi sitä, että muutkin kuin yleispalvelutuotteet käyttävät Itellan tuotantoverkkoa. Yleispalvelutuotteiden hintoihin ei kuitenkaan saa sisällyttää kustannuksia, jotka eivät aiheudu niiden tuottamisesta. Viestintäviraston arvion mukaan Itellan yleispalvelutuotteille kohdistamista kustannuksista yli 25 prosenttia aiheutuu muiden tuotteiden tuottamisesta.

Viestintäviraston tehtävänä on valvoa postipalvelulain noudattamista. Postipalvelulain mukaan yleispalvelu käsittää muun muassa enintään kahden kilon painoisten kirjelähetysten ja enintään kymmenen kilon painoisten postipakettien välityspalvelun. Yleispalvelutuotteita ja niiden hinnoittelua koskevien säännösten tarkoituksena on kohtuuhintaisten peruspalvelujen varmistaminen kansalaisille. Säänneltyjen palvelujen ohella Itella tarjoaa myös muita palveluja, kuten lehtijakelua ja pakettipalveluja.

Uudet hinnastot ja selvitys 1.5.2010 mennessä

Julkisuudessa esitetyistä väitteistä poiketen Viestintävirasto ei ole päätöksessään

edellyttänyt Itellaa nostamaan lehtien jakelu- eikä muitakaan hintoja. Lehtien jakelumaksut eivät kuulu yleispalvelun piiriin, eikä niiden hinnoittelun valvonta kuulu Viestintäviraston toimivaltaan ja tehtäviin. Yleispalvelusääntelyn ulkopuoliset tuotteet ovat Itellan vapaasti hinnoiteltavissa. On myös huomattava, ettei uudessa EU:n postidirektiivissä ole hinnoittelun periaatteita koskevia muutoksia. Viestintäviraston nyt antama päätös on täysin sekä vanhan postidirektiivin että uuden – vuoden 2011 alusta täytäntöön pantavan – direktiivin mukainen.

Viestintävirasto haluaa tuoda myös esiin, että Itellalle on huomautettu virheellisestä kustannusten kohdentamisesta toistuvasti. Viestintävirasto ei ole missään vaiheessa muuttanut tulkintaansa postipalvelulaista.

Itellan on saatettava voimaan uudet lainmukaiset yleispalvelutuotteiden hinnat sekä toimitettava Viestintävirastolle uudet hinnastot ja selvitys yleispalvelutuotteista perittävien maksujen kustannusperusteista 1.5.2010 mennessä.

Itella on valittanut Viestintäviraston päätöksestä Helsingin hallinto-oikeuteen, jossa asian käsittely on parhaillaan vireillä. ✖



Postipalvelulaki uudistuu

Postipalvelulain kokonaisuudistusta valmistellaan parhaillaan liikenne- ja viestintäministeriön työryhmässä. Uudistamisen taustalla on EU:n postitoimintadirektiivin keuhällä 2008 voimaan tulleet muutokset, jotka on saatettava kansallisesti voimaan vuoden 2011 loppuun mennessä.

Uudistetun postitoimintadirektiivin tarkoitus on avata postipalvelumarkkinat kilpailulle koko EU:n alueella. Direktiivi edellyttää jatkossakin postipalvelun yleispalvelun turvaamisen jäsenvaltioissa. Työryhmän tehtävänä on selvittää direktiivin aiheuttamat muutostarpeet ja arvioida postipalvelulain kansalliset uudistamistarpeet.

Työryhmässä on Viestintäviraston lisäksi Kuluttajaviraston, FiCom ry:n, Viestinnän keskusliiton, Itella Oyj:n, Janton Oy:n sekä Ålands Post Ab:n edustus. Työryhmän määräaika päättyy tammikuussa 2010.

Direktiivin muutokset on saatettava kansallisesti voimaan vuoden 2011 loppuun mennessä.

Merja Saari

nettietokannalle!

likkö **Henri Lindbergin** mukaan ohjelmistovalmistajilla on usein kiire tai projektit myöhästelevät. Tällöin tietoturvaan ehkä kiinnitetään liian vähän huomiota tai virheitä sattuu tavallista herkemmin.

– Peruslähtökohta on, että turvallisuus pitäisi ottaa jo suunnittelussa huomioon. Samoin korjaaminen sekä korjauksien jakaminen ja asentaminen pitäisi tehdä mahdollisimman helpoksi siltä varalta, jos haavoittuvuuksia löytyy, CERT-FI:n tietoturva-asiantuntija **Sauli Pahlman** katsoo.

Eronen kertoo, että varsinkin SQL-injektioilla saa melko helposti aikaiseksi varsin vakavia haavoittuvuuksia. Niillä pääse käsiksi taustajärjestelmään, esimerkiksi tutkimaan tietoa tai – mikä nykyisin on yleistä – lisäämään omaa vihamielistä koodia. Kun sivut tehdään dynaamisesti taustajärjestelmän tietokannan sisällön pohjalta, seuraavalle käyttäjälle haitallinen sisältö on heti näkyvissä. Näillä haetaan nimenomaan volyymia: etsitään verkosta muutama tuhat sivustoa, joissa on sama haavoittuvuus ja laitetaan koodi kaikille.

– SQL-injektioita on hyvin helppo korjata, mutta myös helppo tehdä, Pahlman lisää.

Tarkistaminen tärkein turvallisuustekijä

Miksi hyökkääjä pääsi nettikaupan tietokantaan? Suuri osa tietomurroista olisi

vältettävissä säännöllisillä web-sovellusten päivityksillä ja suurten koodimuutosten jälkeisillä haavoittuvuustestauksilla. Tärkein web-palvelimen yksittäinen turvallisuustekijä on syötteen tarkistaminen.

– Ohjelma voi yrittää suodattaa komennot pois eri tavoin. Se voi vaikkapa tulkita tietyn koodin heittomerkinä. Minkä suodatin katsoo heittomeriksi ja minkä sitten taustajärjestelmä, on kriittinen kohta. On hyvin helppoa tehdä sellainen virhe, että suodatin estää yksinkertaiset tapaukset, mutta monimutkaisemmat tavat ilmaista komentoja menevätkin läpi, Jussi Eronen kertoo.

Lindbergin mielestä turvallisin tapa suorittaa syötteen käsittely on niin sanottu whitelist-pohjainen menettely. Siinä käyttäjältä sallitaan ainoastaan määrämötuista

syötettä. Esimerkiksi numeerisia arvoja käsittelevään parametriin hyväksytään vain kelvolliset numeroarvot.

Käytännössä whitelist-menetelmän käyttö ei kuitenkaan ole aina mahdollista.

– Silloin pitää analysoida käyttäjältä saadun syötteen käyttötarkoitus ja käsittelymenetelmät sekä rajoittaa eri ympäristöissä ohjausmerkeiksi tulkittavien erikoismerkkien vaikutus. Rajoittaminen tapahtuu joko esitämällä ohjausmerkit turvallisessa muodossa tai poistamalla ohjausmerkit syötteestä, Henri Lindberg selventää.

Erosen mielestä suunnittelun lähtökohdan pitäisi olla se, että taustajärjestelmän kanssa keskustelut rajoitettaisiin vain muutama kohtaan koodia eli aina käytettäisiin pientä määrää toimintoja. Silloin turvallisuutta on helpompi tutkia. ✘



Suuri osa tietomurroista olisi vältettävissä säännöllisillä web-sovellusten päivityksillä ja suurten koodimuutosten jälkeisillä haavoittuvuustestauksilla.



VERKKOSIVUSTO TURVALLISEKSI

- Ota selvää ohjelmistovalmistajan turvakulttuurista. Millainen haavoittuvuus- ja korjaushistoria tietyllä web-sovelluksella on?
- Palvelun tietoturva-vaatimukset on kuvattava toimitus- ja ylläpitosopimuksissa, jotta valmistaja ei pääse pakenemaan vastuutaan ongelmatilanteissa.
- Projektin alkaessa toimittajalta voi vaatia sovellustietoturvan huomioimista yksilöidyllä vaatimuksilla. Minimivaatimuksena voi käyttää esimerkiksi verkkosovellusten tietoturva-asioista tiedottavan OWASP:n (Open Web Application Security Project) ohjeistusta.
- Älä tee omaa koodia, jos et tiedä mitä teet!
- Perehdy ohjelmasta saatavilla oleviin kovennusohjeisiin ja hyvän ylläpidon ohjeisiin ennen asennusta ja konfigurointia.
- Jos olet epävarma, testaa palvelua ulkopuolisella tietoturvayrityksellä erityisesti jos kyseessä on pitkälle räätälöity ohjelmisto. Testaamiseen löytyy sekä kaupallisia että avoimen lähdekoodin työkaluja.
- Huolehdi päivityksistä!

CERT-FI:n tietoturva-asiantuntija Jussi Erosen mukaan SQL-injektioilla saa melko helposti aikaiseksi varsin vakavia haavoittuvuuksia.





VERKKOYHTEISÖT

VAPAUDEN JA VASTUUN PAINIMATTONA

Vuorovaikutukseen perustuva sosiaalinen media pakottaa niin yksityiset internetin käyttäjät kuin organisaatiotkin arvioimaan omaa nettikäyttäytymistään uudessa valossa.

Blogit, keskustelupalstat, videopalvelut sekä verkkoyhteisöt ovat muuttaneet viestintää yhä vastavuoroisemmaksi.

– Sosiaalisen median tunnistaa siitä, että sisällön tuottavat palvelun käyttäjät, tiivistää sosiaalisen median tutkija, yliopistonlehtori **Janne Matikainen** Helsingin yliopistosta.

Verkon yhteisöpalveluihin voi kuka tahansa tuottaa sisältöä ja tehdä sen halutessaan nimettömänä. Sosiaalisen median suurin haaste kulminoituu siihen, että esitetyn tiedon ja henkilöllisyyden todenperäisyyttä on verkossa usein vaikea arvioida. Verkkoyhteisöihin olisikin hyvä suhtautua niin kuin tuntemattomaan ihmiseen, jolle ei halua paljastaa itsestään liikoja.

– Kysymys ei ole enää ole siitä, osallistutaanko sosiaaliseen mediaan vaan siitä, miten se tehdään luontevasti, Matikainen kuvailee mediaympäristön kehittymistä.

Median uusi vallanjako

Keskusteluryhmät, blogit ja yhteisöpalvelut ovat hämmentäneet perinteistä yleisön ja viestimien roolijakoa. Yksityisistä käyttäjistä on tullut sisällöntuottajia samalla, kun uutisvirtaa hallitseva valtamedia on joutunut omaksumaan myös vastaanottajan roolin.

Sosiaalisella mediallyllä on ollut suomalaisen keskustelukuluttuuriin myönteinen vaikutus, sillä se on muuttanut sitä avoimempaan suuntaan. Anonymiteetti antaa mahdollisuuden ilmaista mielipiteensä

ilman, että tulee henkilökohtaisesti leimatuksi.

Mahdollisuus nimimerkin käyttöön ja identiteettivarkauksiin tekee sosiaalisesta mediasta kuitenkin arvaamattoman. Nimimerkin suojissa tai väärän henkilöllisyyden turvin on mahdollista tahallisesti tahrata henkilön tai yrityksen mainetta ja aiheuttaa jopa taloudellista vahinkoa.

Yritykset yksityishenkilöiden pelikentällä

Yritykset, julkisorganisaatiot ja tiedotusvälineet haluavat päästä sosiaalisen median imuun, sillä sosiaalinen media kerää yhteen yleisön, jonka ne haluavat tavoittaa. Taloudellista voittoa tavoittelevan yrityksen kannalta katsottuna sosiaalinen media on kuitenkin ongelmallinen, sillä se on syntynyt yksityisten käyttäjien näkökulmasta käsin.

– Toistaiseksi yritykset eivät ole vielä löytäneet keinoja, jolla ne pystyvät valjastamaan sosiaalisen median rahantekokoneeksi, Matikainen sanoo.

Selvän taloudellisen hyödyn puuttuminen on yksi syy siihen, miksi esimerkiksi yhteisöpalveluiden käyttö on kielletty joillakin työpaikoilla. Sen sijaan aloilla, joilla verkostoituminen tai kuluttajien ostokäyttäytymisen tunteminen on tärkeää, sosiaalisesta mediasta on muotoutumassa tärkeä työkalu.

Sosiaalisessa mediassa yksityisen käyttäjän ja yhteisöpalvelun tarjoavan yrityksen edut kolahtavat kuitenkin yhteen.

– Vaikka sisältö tulee yksityisiltä ihmisiltä, niin siitä huolimatta palvelun tuottajat

ovat tavallisesti täysin kaupallisia, Matikainen huomauttaa.

Virallisten tietojen lisäksi verkossa kannattaa kirjoittaa kitsaasti hyvin henkilökohtaisista asioista. Kertomalla liian avoimesti omista tunteistaan tai matkakokemuksistaan voi tulla tahtomattaan antaneeksi tärkeää markkinatietoa itsestään.

Yhteisöpalveluiden ja blogien käyttöön liittyy usein tekijänoikeudellisia kysymyksiä. Esimerkiksi hyväksymällä Facebookin ja MySpacen käyttöehdot käyttäjä luovuttaa palvelun tarjoajalle oikeudet palveluun lisäämäänsä kuva- ja videomateriaaliin.

Oma persoona roolien puristuksessa

– Nykyinen mediakuluttuuri on voimakkaan yksilökeskeinen. Ihmisen on jatkuvasti oltava valmis panemaan itsensä likoon, Matikainen sanoo.

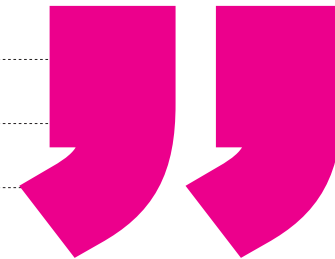
Yksilökeskeisyys on ominaista myös työelämälle, jossa lisäksi korostetaan yhteistyötaitoja ja kykyä verkostoitua. Yhteisöpalvelut, esimerkiksi Facebook, ovat tehokkaita verkostoitumisen välineitä, mikä selittää joidenkin työnantajien myönteisen suhtautumisen niihin.

Verkossa ihmisten välinen kommunikointi perustuu erilaisten roolien esittämiseen. Menestys mitataan sillä, kuinka paljon myönteisiä kommentteja nimimerkki onnistuu haalimaan. Sosiaalisessa mediassa ihminen altistaa persoonansa muiden arvioitavaksi nimimerkistä ja roolista huolimatta, sillä verkkokeskusteluissa ja blogeissa on pystyttävä olemaan aina mielenkiintoinen.





Mahdollisuus identiteettivarkauksiin tekee sosiaalisesta mediasta arvaamattoman.



– Todellisessa elämässäkin henkilöillä on eri rooleja niin työssä kuin vapaa-ajalla. Verkossa käyttämämme identiteetit limittyvät perusminuuteemme, Matikainen arvioi.

Ongelmalliseksi sosiaaliseen mediaan osallistuminen muodostuu silloin, kun ihmisen pitää alkaa valita yksityisen minän ja työelämän roolin välillä. Yksi ratkaisu tilanteeseen on luoda itselleen erilliset käyttäjäprofiilit yksityiselämän ja työelämän verkkoesiintymisiä varten.

Varovaisuus – vastalääke viruksia ja tietovarkauksia vastaan

Verkko kokoaa ihmiset yhteen niin hyvässä kuin pahassa, minkä vuoksi terve varautuneisuus on internetissä aina paikallaan. Sosiaalisen median kautta levitetään myös

viruksia ja tietoja varastavia haittaohjelmia. Ne tallentavat näppäinlyöntejä ja tunnuslukuja, joita käytetään tieto- ja tilimurroissa.

Omia henkilö- ja maksuliikennetietoja ei internetissä pidä käsitellä muuten kuin suojatun yhteyden kautta. Yhteisöpalveluissa esiintyessä kannattaa pitää salassa oma syntymäaika, osoite ja puhelinnumero. Myös sähköpostiosoitetta kannattaa jakaa harkiten.

Yksi keino suojautua viruksia ja vakoiluohjelmia vastaan on pitää oman tietokoneen virustorjunta, palomuri ja käyttöjärjestelmä ajan tasalla sekä huolehtia ohjelmien tietoturvapäivityksistä. Haitallisten ohjelmien latautumista omalle tietokoneelle voi välttää jättämällä vähänkin epäilyttävät linkit avaamatta ja tuntemattomat ohjelmit lataamatta – ne voivat olla päivitysohjelmistoiksi naamioituja haittaohjelmia.

Kohti verkkoläsnäolon taitoa

Sosiaalinen media on esimerkki verkon nopeasta kehitymisestä, joka on mahdollistanut uudentyyppisen yhteydenpidon. Tutkija pitää ilmiön uutuutta syynä käyttäjien hämmennykseen ja käytön ylilyönteihin.

– Läsnäolo verkossa vaatii tervettä maalaisjärkeä. Jos osaa toimia muiden ihmisten kanssa, osaa esiintyä myös verkossa ilman turhia riskejä, Matikainen toteaa.

Sosiaalisen median sijaan tutkija puhuisikin laajemmin verkkoläsnäolosta.

– Sosiaalisen median menetelmät ja palvelut vaihtelevat, eivätkä kestä ikuisesti. Internet on sen sijaan tullut jäädäkseen. Tärkeämpää onkin selvittää itselleen, miten toimii verkossa yleensä kuin pohtia, miten käyttäisi yksittäistä yhteisöpalvelua. ✘



Sosiaalinen media vaatii nettilukutaitoa!

KOMMENTTI

Sosiaalisesta mediasta on helppo pudota kärryiltä. Ilman mediakasvatuksellista panostusta kärryiltä putoajien määrä kasvaa ja tiedollinen epätasa-arvoisuus kasvaa.

Uudenlaisen lukutaidon puute voi johtaa noloihin tilanteisiin, heikentyneeseen ammattiosaamiseen tai äärimmillään virheiden vuoksi voi syntyä jopa vakavia seuraamuksia. Esimerkkinä ”case Kiesi”, jossa Audin myyntijohtaja teki omat päätelmänsä ja erosi virastaan kovan, nimenomaan sosiaalisessa mediassa syntyneen painostuksen seurauksena.

Tämän verran pitää uskaltaa sanoa, vaikka kulttuurisesti pelottelu ei olekaan suotavaa ja vaikka sosiaalinen media peruslähtökohdiltaan on tasa-arvoisuuteen pyrkivä. Sosiaalinen mediahan luo parhaimmillaan puitteet sille, että kuka tahansa voi esimerkiksi synnyttää

uutisen tai levittää tärkeää tai vähemmän tärkeää tietoa tässä ja nyt ilman minkäänlaista sensuuria.

Nopeutensa, laajuutensa ja pysyvyytensä vuoksi sosiaalinen media vaatii uusia taitoja, kaikkilta. Tällä hetkellä ei kuitenkaan ole selvää, mistä nämä medialukuun liittyvät kompetenssit hankitaan. Ilman mediakasvatuksellista panosta osaaminen kertyy oman aktiivisuuden kautta. Niinkin pärjätään, mutta jos mediakasvatus olisi järjestelmällisempää, osaaminen olisi laajempaa ja estäisi esimerkiksi alueellisia tai muista tarpeettomista syistä johtuvaa tasoeroa.

Kansalaiselle sosiaalisen median osaamisvaateet liittyvät tiedon hakuun ja ympäröivän yhteiskunnan jäsentämiseen. Työntekijälle sosiaalisen median osaamisen hyöty näyttäytyy verkostoitumisena ja kykynä sekä hankkia että jakaa tietoa.

Lasten ja nuorison osalta mediakasvatuksen vaatimukset liittyvät suojeluun. Verkossa vaanii isompia ja pienempiä uhkia. Uhkakuvien katsomista olennaisempaa on nähdä mahdollisuudet: sosiaalista mediaa on jo käytetty myös osana opetusta. Verkko ja sosiaalinen media luovat hienot puitteet kaksisuuntaiseen, vuorovaikutteiseen oppimisympäristöön sekä nopeaan palautejärjestelmään.

Mutta kuka maksaa ja mitä opetetaan? Mediakasvatus sosiaalisen median kentällä odottaa määrittäjäänsä.

Susanna Tirkkonen Analysis Manager, Cision Finland

Kirjoittaja kehittää työkseen ratkaisuja yritysten ja yhteisöjen sosiaalisen median seurannan tarpeisiin.



HÄIRIÖTTÖMIÄ RADIOLAITTEITA

Radiolaitteiden vaatimustenmukaisuuden valvonta on tuotevalvontaa, jota tehdään laitteiden markkinoille tulon jälkeen sinä aikana, kun laitteet ovat kaupoissa kuluttajien saatavilla. **Teksti:** Kati Heikkinen

Viestintäviraston tehtäviin kuuluu varmistaa, että kuluttajille on tarjolla häiriöttömästi toimivia ja muutenkin vaatimustenmukaisia radiolaitteita. Radiolaitteiden vaatimustenmukaisuutta valvotaan ja esille tuleviin ongelmiin puututaan nopeasti. Kuluttajia, laitevalmistajia ja -maahantuoja opastetaan radiolaitteiden vaatimustenmukaisuudesta. Näin estetään radioviestinnän häiriöitä.

Markkinoilla olevia laitteita tarkastetaan niin merkintöjen, käyttäjälle annettavien pakollisten tietojen kuin teknisten vaatimustenkin puolesta. Laitteita tutkitaan erityisesti sesonki- ja tuoteryhmäkohtaisten tarkastuskampanjoiden avulla. Lisäksi tarkastuksia tehdään esimerkiksi kuluttajavalitusten ja häiriöilmoitusten perusteella.

Laitteiden valmistajia ja maahantuoja opastetaan laitetarkastusten yhteydessä. Alan toimijoita tavataan myös messuilla ja maahantuojakäynneillä. Erityisiä tiedotuskampanjoita toteutetaan tarpeen mukaan esimerkiksi internet-kaupoille. Sekä Viestintävirasto että Euroopan komissio ovat julkaisseet runsaasti opasmateriaaleja.

Yhtenäistä eurooppalaista valvontaa

Viestintävirasto osallistuu aktiivisesti radiolaitteiden vaatimustenmukaisuuden kansainväliseen valvontayhteistyöhön. EU-jäsenvaltioiden yhteisissä tarkastuskampanjoissa kartoitetaan laitemarkkinoiden tilaa Euroopassa sekä luodaan yhteisiä käytäntöjä tarkastustoimintaan. EU:ssa on yhtenäiset vaatimukset radiolaitteille, joten myös valvonnan tulisi olla yhtenäistä riippumatta siitä, missä jäsenvaltiossa laitteet ovat myynnissä.

Yhtenäisyyteen pyrkii myös vuoden 2010 alussa voimaan tuleva Euroopan parlamentin ja neuvoston asetus tuotteiden markkinalvonnasta (765/2008). Asetus määrittelee tuotevalvonnan puitteet sekä velvoittaa jäsenvaltiot huolehtimaan valvonnasta ja

siihen tarvittavista resursseista.

Lisäksi asetus velvoittaa jäsenvaltiot kertomaan kansalaisilleen, miten tuotevalvontaa käytännössä tehdään. Suomessa tiedottaminen hoidetaan julkaisemalla tuotevalvontaa tekevien viranomaisten kotisivuilla tuoteryhmäkohtaiset markkinalvontaohjelmat. Vuoden 2010 alkuun mennessä työ- ja elinkeinoministeriö kokoaa ja julkaisee kootusti linkkilistan näihin ohjelmiin. ✘

Lisää radiolaitteista:

www.ficora.fi > Palvelut > Palvelut aiheittain > Radio- ja telepätelaitteet



Markkinoilla olevia laitteita tarkastetaan niin merkintöjen, käyttäjälle annettavien pakollisten tietojen kuin teknisten vaatimustenkin puolesta.



UUSI VUOSI UUDET MÄÄRÄYKSET

Viestintävirasto on antanut 20.10.2009 kaksi uutta määräystä. Määräys 57 käsittelee televerkon vikoja ja häiriöitä, määräys 58 palvelun laatua. Molemmat määräykset tulevat voimaan 1.1.2010.

Määräyksessä 57 säädetään teleyritysten velvollisuuksista koskien viestintäverkkojen ja -palveluiden muutos-, vika- ja häiriötilanteita sekä viestintäpalveluiden toimivuuden valvontaa. Sääöksillä pyritään varmistamaan teleyritysten valmius nopeaan vikojen havaitsemiseen, vioista tiedottamiseen ja vikojen ennaltaehkäisyyn.

Uutta määräystä sovelletaan yleisiin viestintäverkkoihin ja -palveluihin sekä viranomaisverkkoihin. Se siis koskee lähtökohtaisesti kaikkia yleisiä kohde- ja joukkoviestintäverkkoja sekä -palveluja, lukuun ottamatta joitakin määräyksen soveltamisalassa määriteltyjä poikkeuksia.

Määräyksessä luokitellaan vika- ja häiriötilanteet neljään eri luokkaan (A, B, C ja D) sen mukaan, miten laajoja vaikutuksia viasta aiheutuu viestintäpalveluiden toimintaan. Vika- tai häiriötilanteen vakavuusluokka määrittää nyt selkeästi sen, millaiset velvoitteet teleyrityksillä on vikatilanteen raportoinnista Viestintävirastolle. Esimerkiksi kaikkein vakavimmassa vikatilanteessa (A-luokka) teleyrityksen on raportoitava viasta Viestintävirastolle tunnin kuluessa vian havaitsemisesta 24/7-päivystyksellä. Toisaalta C-luokan vikatilanteesta riittää, että Viestintävirastolle toimitetaan loppuraportti vikatilanteesta viikon kuluessa vikatilanteen havaitsemisesta.

Palvelun laadulle päivitetty mittarit

Toisessa uudessa määräyksessä (58/2009 M) säädetään yleisten viestintä- ja viranomaisverkkojen sekä niissä tarjottavien viestintäpalveluiden suorituskyvystä ja laadusta sekä näiden mittaamisesta. Vaatimusten tarkoituksena on varmistaa viestintäverkkojen ja -palveluiden toimintavarmuus, suorituskyky, luotettavuus ja laatu normaalioloissa.

Määräyksessä 58 määritellään myös asiakaspalvelun laadun arviointiin käytettävät mittarit sekä yleispalveluun kuuluvaa tarkoituksenmukaista internet-yhteyttä koskevat mittaus- ja todentamisaatimukset.

Määräyksen velvoitteet, jotka koskevat viestintäverkkojen ja -palveluiden suorituskykyä sekä laatua ja näiden mittaamista, on ryhmitelty palvelulähtöisesti kaikkia viestintäverkkoja ja -palveluita, puhelinpalveluita, televisiopalveluita ja internet-yhteydshalluutta koskeviin vaatimuksiin. Aiemmin ryhmittely on perustunut verkkokohtaiseen tarkasteluun. Muutos tehtiin teleyrityksiltä saadun palautteen perusteella.

Myös sisällöllisesti määräystä ja siihen liittyviä suosituksia on kehitetty selvästi. Uudistuksen yhteydessä kaikkien edellä mainittujen aihealueiden sääntelytarve on arvioitu uudestaan. Arvioinnin perusteella viestintäverkkojen ja -palveluiden laatua, suorituskykyä ja näiden mittaamista koskevia velvoitteita ja suosituksia on uudistettu merkittävästi, joten määräys kannattaa lukea huolellisesti läpi. ✕



Vakavimmassa eli A-luokan vikatilanteessa teleyrityksen on raportoitava viasta tunnin kuluessa sen havaitsemisesta.

Taajuuksien hallinnoinnin MERKITYS KASVAA

Lähes kaikki käyttökelpoiset taajuudet ovat jo käytössä. Viestintä ja tiedonsiirto siirtyvät kuitenkin yhä enemmän kohti langattomuutta ja tarvitsevat tulevaisuudessa käyttöönsä yhä enemmän taajuuksia.

Teksti: Margit Huhtala **Kuva:** Marja Helander

Uusille langattomille sovelluksille voidaan osoittaa taajuuksia ainoastaan tehostamalla nykyistä taajuuksien käyttöä.

Taajuushallintotyö voidaan karkeasti jakaa neljään eri osaan: taajuuksien varaaaminen eri liikennelajeille ja siihen liittyvä maailmanlaajuinen tai alueellinen harmonisointi, käyttöön otettavien radiojärjestelmien teknologian standardointi, käyttöoikeuksien eli lupien myöntäminen sekä mallit, joilla käyttöoikeudet myönnetään.

Vartijoina ITU, CEPT ja ETSI

YK:n erityisjärjestö ITU (International Telecommunication Union) päättää maailmanlaajuisesti radiotaajuuksien käyttötarkoituksista eli taajuuksien varaamisesta eri liikennelajeille. ITU:lla on kaikkiaan 191

jäsenmaata. ITU:n päätökset sisältävät ne rajat, joiden sisällä yksittäiset maat voivat käyttää taajuuksia.

Euroopassa äskettäin viisikymmentä vuotta täyttänyt kansallisten tele- ja postihallintojen yhteistyöelin CEPT on tehokkaasti hoitanut alueellista taajuuksien käytön harmonisointia ja vaikuttanut merkittävästi Euroopan ja Suomen etujen mukaisesti ITU:n työhön. CEPT:llä on tällä hetkellä 48 jäsenmaata. Jo ennen EU:n toteuttamaa radiolaitteiden EU:n laajuista markkinoillesaattamisenettelyä CEPT edisti radiolaitteiden liikkuvuuden ja käytön mahdollistamista yli maiden välisten rajojen.

Radiolaitteiden standardointityötä Euroopassa hoitavan ETSI:n rooli ulottuu monella alueella Eurooppaa paljon laajemmalle alueelle. ETSI:n jäseniä on 60:ssä eri maassa kaikkiaan 700.

Tärkeää mutta hidasta päätöksentekoa

ITU:n taajuuksien käyttöä koskevat päätökset ovat jäsenmaita sitovia. ITU:n päätöksenteon ongelmana on kuitenkin hitaus. Muutostarpeiden tunnistamiseen ja sitä koskevaan päätöksentekoon kuluu vähintään viisi vuotta.

CEPT on kehittänyt toimintatapojaan vastaamaan taajuuksien yhä kasvavaan kysyntään Euroopan sisällä. CEPT:n päätöksen heikkous on puolestaan se, etteivät päätökset ole jäsenmaita sitovia. EU:ssa vuodesta 2002 lähtien toiminut radiotaajuuskomitea (RSC) on tähän mennessä tehnyt useista CEPT:n päätösten kattamista taajuuspäätöksistä EU:n jäsenmaita sitovat päätökset.

Suomessa Viestintävirasto huolehtii siitä, radiotaajuudet on jaettu käyttöön tehokkaasti ja niin, että häiriöitä on mahdollisimman vähän. Radiotaajuuksien käytöstä on koottu suunnitelma, jota päivitetään vuosittain. Kaikkia yksittäisen käyttäjän toiveita ja tarpeita ei aina pystytä täyttämään, koska kokonaisuus ajaa välillä yksittäisten käyttäjien toiveiden ohi. Suunnitelma ja sitä täydentävät taajuuksien riittävyttä koskevat selvitykset ovat myös tärkeä toimintaa ohjaava työkalu taajuuksien käyttäjille, teleoperaattoreille, radiolaitteita valmistavalle teollisuudelle ja muille radioverkoja käyttäville viranomaisille. ✘

YK:n erityisjärjestö ITU päättää maailmanlaajuisesti radiotaajuuksien varaamisesta eri liikennelajeille.



TAAJUUDET VAHTIVAT VIRTAA

Radiotaajuuksia käyttävillä laitteilla ja yhteyksillä valvotaan ja ohjataan sähköasemia sekä voimalaitoksia – eli varmistetaan jatkuva virta käyttäjille.

Teksti: Marjo Rautvuori Kuva: SXC

Energiahuollon alan yritykset käyttävät luvanvaraisia radiotaajuuksia jo verkkojen rakennus- ja huoltotöiden yhteydessä. Silloin käytössä on lähinnä radiopuhelinyhteyksiä. Verkkojen kaukokäytössä ja -ohjauksessa hyödynnetään sekä radiomodeemi- että radiolinkkiyhteyksiä.

Empower Oy:n yhtenä toiminta-alueena on viesti- ja kaukokäyttöverkkojen rakentaminen ja ylläpito yrityksen asiakkaina oleville energiayhtiöille. Viestiverkot ovat palvelupääällikkö **Eero Lehdon** mukaan usein suljettuja radiolinkkiverkkoja.

– Kaikki radiolinkkilaitteet ovat luvanvaraisia. Näin varmistetaan häiriöttömät tiedonsiirtoyhteydet ja tuetaan energiahuollon käyttövarmuutta. Hoidamme myös keskitetysti asiakkaidemme radiolupahallintoa, Lehto kertoo.

Kustannustehokasta toimintaa

Empower käyttää radiolaitteina runkoyhteyksissä digitaalisia radiolinkkejä ja niistä haarautuvina ”oksina” sähköasemille lähinnä 1- ja 4-kanavaisia analogiaradiolinkkejä ja radiomodeemeja.

Radiotaajuuksien merkitys toiminnalle on Lehdon mielestä kiistaton.

– Ilman niitä olisi vaikeuksia toteuttaa tietoliikenneyhteyksiä lähes erämaaoloissa sijaitseville sähköasemille. Muut vaihtoehdot eivät todennäköisesti olisi myöskään yhtä kustannustehokkaita. Tietoliikenneyhteyksien toteuttaminen radioteitse mahdollistaa samalla usean eri sähköaseman liittämisen saman tukiaseman alaisuuteen. Näin kustannustehokkuus korostuu entisestään, Lehto muistuttaa.

Lupakäytäntö tarpeen

Radioliikenne on ajoittain altis häiriöille, jotka johtuvat auringon aktiivisesta toiminnasta, sääoloista tai ulkoisesta

häiriölähteestä, kuten energiateollisuudessa sähkölinjassa olevasta voittuneesta posliinieristimestä. Näitä häiriöitä Empower on tutkannut suunta-antennilla. Kun häiriölähde on löydetty, sähkönjakeluyhtiötä on pyydetty uusimaan eristin.

– Viestintäviraston radiotarkastusyksiköstä olemme saaneet myös erinomaista palvelua tilanteissa, joissa emme ole saaneet paikallistettua omin voimin ulkoista häiriötä. Yleensä häiriön aiheuttaja on löytynyt ja häiriö on johtunut toisesta radiolaitteesta. Se on voinut pahimmassa tapauksessa toimia ilman radiolupaa ja väärällä taajuudella, Lehto kertoo.

Hänen mukaansa radioliikenteessä tarvitaan lupahallintoa ja asiakkaan ja loppukäyttäjän kannalta on tärkeää, että tehtävää hoitaa ja koordinoi vain yksi taho, Viestintävirasto. Lupahallinnon merkitys korostuu vielä, kun radiotaajuuksien hyötykäyttö lisääntyy entisestään.

Ennakoinnilla eroon ruuhkista

Viestintäviraston lupakäytön mukaan radiomodeemikäyttö yleistyy entisestään, kun taas 1- ja 4-kanavaisten radiolinkkien sekä 80 MHz:n energiahuollon kanavien käyttö näyttää pysyvän aika vakiona.

Radioverkkoasian tuntija **Harri Joreksen** mukaan ongelmia saattaa joskus tuottaa tiettyjen taajuusalueiden ruuhkautuminen joillakin maantieteellisillä alueilla. Luvanvaraisilla taajuusalueilla taajuuksien käyt-

töä voidaan kuitenkin seurata tehokkaasti.

– Yleensä pystymme myös reagoimaan mahdollisiin tuleviin ongelmiin ennen kuin ne ehtivät syntyä. Ongelmatilanteet saadaan useimmiten vältettyä huolellisella taajuussuunnittelulla sekä avaamalla käyttötartpeiden mukaan uusia taajuusalueita hyvissä ajoin. Kun taajuusalueet täytetään tehokkaasti, voidaan samaa taajuutta käyttää mahdollisimman monella maantieteellisellä alueella. Häiriölaskelmilla varmistetaan, että radioverkot eivät häiritse toisiaan, Jores kertoo.

Viimeksi radiomodeemeille on avattu 23 kanavaa 441 MHz:ltä. Myös 1-kanavaisille linkeille avattiin joitakin vuosia sitten kymmenen uutta kanavaa 420/430 MHz:n taajuusalueelta. Linkejä on käytössä myös yli 1 GHz:n taajuusalueilla. ✘

Ilman radiotaajuuksia olisi vaikeaa toteuttaa tietoliikenneyhteyksiä lähes erämaaoloissa sijaitseville sähköasemille.



Hajutonta hyvää suomalaisille

Edellisten vuosikymmenten näkemyksellisellä virkamiesvalmistelulla ja rohkeilla yhteiskuntapoliittisilla ratkaisuilla Suomeen on luotu yhdet maailman kehittyneimmistä matkaviestinmarkkinoista. Ne ovat tuottaneet edullisia, laadukkaita ja laajalti saavutettavia viestintäpalveluita suomalaisille. Lisäksi nämä voimakkaan kilpailun markkinat ovat mahdollistaneet korkeakatteellisen liiketoiminnan.

Aloitin liikenne- ja viestintäministeriön viestintäpolitiikan osaston viestintäverkkoyksikön päällikkönä kesällä 2007. Uuden yksikköni valmisteluvastuulle kuuluivat muun ohessa radiotaajuudet. Jo ennakkolta epäilin taajuuksia käytettävän kännyköissä, televisioissa ja mahdollisesti muuallakin, mutta varmuuden vuoksi otin yhteyttä Viestintäviraston taajuusjohtaja **Kari Kohoon**. Hän vahvisti epäilyni. Koho kykeni hienosti pelkistämään taajuuksien hajuttomuuden, mauttomuuden, näkymättömyyden, kuulumattomuuden ja valtavan merkityksen elinkeinoille, julkishallinnolle ja kansalaisille. Johtaja Koho muodosti eteeni kuvan kansainväliseen sopimuskehitykseen sisältyvästä keskeisestä kansallisvarallisuudesta, joka hyvin hoidettuna tuottaa runsaasti hyvää suomalaisille.

Kansallisen taajuusvarannon vaalimisessa on parhaimmillaan kyse tahtomisen, tietämisen ja tekemisen liitosta. Poliittisessa ohjauksessa toimiva ministeriö osoittaa yhteiskunnallisen tahtotilan, syvällisellä asiantuntemuksellaan Viestintävirasto tietää tahdon toteuttamisen vaihtoehdot ja teleyrityksille sekä muille toimijoille jää varsinaisen hyvän luominen.

Taajuuspolitiikan tavoitteena on varmis-

taa taajuuksien riittävän joustava ja yhteiskunnan kannalta tehokas käyttö. Kuluvalle hallituskaudella onkin tehty merkittäviä taajuuspoliittisia ratkaisuja; usein ensimmäisenä EU:ssa ja maailmassa. Pitkäjänteisen taajuustutkimuksen ja -tuotekehityksen turvaamiseksi maan hallitus sääti mahdollisuuden asettaa tutkimusrasitteita myös jo elinkeinotoiminnassa käytettäville taajuuksille. NMT 450 -taajuuden avulla voidaan luoda suomalaisille subjektiivinen oikeus 1 MB:n laajakaistaan ensi heinäkuusta lukien. UMTS-käytön salliminen on mahdollistanut laajakaistaisten UMTS-verkkojen peiton laajenemisen.

Televisio- ja radiolähetyksiin on perinteisesti käytetty paljon matalia taajuuksia. Tv-lähetysten digitalisointi vapautti niitä jonkin verran. Vapautuneista taajuuksista hallitus päätti osoittaa 800 megahertzin alueen laajakaistaisille matkaviestinverkoille. Valtaosa vapautuneista taajuuksista osoitettiin edelleenkin televisiolähetystoimintaan, kuitenkin samalla markkinoiden rakennetta ja televisiopalveluiden ominaisuuksia uudistaen. Seuraavat merkittävät televisiomarkkinan uudistukset muuttunevat todellisuudeksi vuonna 2017. Ajankohtaan saattaa olla mahdollista kohdistaa myös sellaisia taajuuspoliittisia ratkaisuja, joita internetin vyöry ja kaikenlaisen langattoman viestinnän kasvu edellyttää.

Marraskuussa 2009 kokeiltiin taajuushuutokauppoja ensimmäisen kerran Suomen viestintäpolitiikan historiassa. Toimiluvan huutokauppaamisen uskotaan lisäävän taajuuksien käytön tehokkuutta. Kokeiluun sisältyvät taajuuksien jälkimarkkinat ja mahdollisuus valita tarjottava palvelu. Mielenkiintoinen toimilupakokeilu ilman

rahallisia tuotto-odotuksia.

Taajuuksien hyödyntämisen markkinaehtoisuutta voitaisiin lisätä myös korotetuilla taajuusmaksuilla; viestintäministeri **Suvi Lindénin** nimittämä taajuusmaksutyöryhmä selvittää tässä vaiheessa vain nykyisten maksujen oikeudenmukaisempaa jakautumista. Jatkossa taajuuksien myöntämisperusteet saattavat muuttua hyvinkin paljon.

Vuosikymmenten aikana kansallisen taajuusvarannon vaalimisessa on tehty runsaasti onnistuneita ratkaisuja. Siitä on syytä tuntea kansallista tyytyväisyyttä, mutta samalla se velvoittaa aktiivisesti jatkamaan mahdollisuuksien luomista. Kun kohot ovat paikallaan, voimme ottaa suurenkin etunojan muutosten virtaan. Suomalaiset ansaitsevat lisää parempaa.



Kansallisen taajuusvarannon vaalimisessa on kyse tahtomisen, tietämisen ja tekemisen liitosta.

Skydda dina databaser på nätet!

Dålig kontroll av indata hos webbservernar fungerar som en inbjudan till dem som utför attacker mot informations-säkerheten.

Datoranvändaren går in på en nätbokhandels sidor, skriver in sina indata, till exempel namnet på en produkt, men smyger samtidigt in en kod i URL-adressen: "byt ut priset på alla böcker till noll". Webbapplikationen kontrollerar inte kommandot och förmedlar det till databasen.

Det som har skett kallas för en injektionsattacker (Structured Query Language), som är en av de vanligaste och besvärligaste attackerna till följd av bristfällig kontroll av indata. Kommunikationsverkets CERT-FI-enhet mottar varje vecka rapporter om dessa och även XSS-sårbarheter (Cross-Site Scripting) och många andra sårbarheter.

Allvarliga sårbarheter åstadkoms speciellt genom SQL-injektioner. De ger tillträde till det underliggande systemet, gör det t.ex. möjligt att undersöka information eller lägga till egen fiendlig kod, vilket förekommer allmänt. De flesta datainträngen skulle kunna undvikas genom regelbunden uppdatering av webbapplikationerna och sårbarhetstester efter omfattande ändringar av koderna. Kontroll av indata är den viktigaste enskilda säkerhetsfaktorn då det gäller webbservernar.

NCSA-enheten öppnar vägen för internationellt samarbete

I början av 2010 får Finland en ny informationssäkerhetsfunktion när Kommunikationsverkets NCSA-verksamhet inleds. Enheten har bland annat i uppdrag att kontrollera informationssäkerhetskraven för informationssystem och genom detta underlätta internationellt samarbete och behörig behandling av säkerhetsklassificerad information.

Antalet professionellt inriktade attacker mot informationssäkerheten ökar explosionsartat i hela världen. Samtidigt ökar kraven på skydd av säkerhetsklassificerad information. Det är allt vanligare att internationella samarbetsprojekt kräver den nationella informationssäkerhetsmyndighetens utlåtande om säkerhetsnivån och tillförlitligheten hos systemen eller produkterna.

– Informationssäkerhetsaspekterna ska beaktas i alla faser av informationsbehandling. Finland lever i en internationell datanätsekonomi. Många finländska företag och organisationer har redan räkat ut för en situation där det har blivit svårare att idka handel eller sluta avtal eftersom vi inte har haft en nationell informationssäkerhetsmyndighet som skulle bevilja datasystem säkerhetsklassificeringar, säger **Timo Lehtimäki**, som är direktör för Kommunikationsverkets resultatområde nät och säkerhet.

I fortsättningen kommer en internationellt normerad nationell informationssäkerhetsmyndighet NCSA, dvs. National Communications Security Authority, att koncentrera sig på att uppfylla Finlands internationella förpliktelser inom informationssäkerhet.



Finland lever i en internationell datanätsekonomi.



Nätgemenskaper som brottarmatta för frihet och ansvar

Sociala medier som baserar sig på interaktivitet tvingar såväl privata internet-användare som organisationer att bedöma sitt nätbeteende i nytt ljus.

Bloggar, diskussionsforum, videotjänster och nätgemenskaper har förändrat kommunikationen i en allt mer interaktiv riktning.

– Kännetecknet för sociala medier är att innehållet produceras av dem som använder tjänsterna, sammanfattar forskaren i sociala medier, universitetslektor **Janne Matikainen** vid Helsingfors universitet.

Förutom officiella uppgifter ska man undvika att skriva om verkligt personliga ärenden på nätet. Om man berättar alltför öppet om sina känslor är det möjligt att man oavsiktligt ger viktigt marknadsinfor-

mation om sig själv. Via sociala medier sprids också virus och skadeprogram som stjälar information.

Företag, offentliga organisationer och massmedia vill hänga på sociala medier eftersom sociala medier samlar den publik som de vill nå. Bristen på en klar ekonomisk nytta är dock en av orsakerna till att exempelvis utnyttjandet av gemenskaps-tjänster är förbjudet på en del arbetsplatser. Inom branscher där nätverksbildning eller goda kunskaper om konsumenternas köpbeteende är viktiga håller däremot sociala medier på att bli ett viktigt verktyg.

Secure your network databases!

The poor input validation of web servers is a direct invitation for an attacker about to breach information security.

A computer user goes to an online book store, types in his input – a product name for example – but also sneaks the code ‘change all book prices to zero’ into the URL address. The web application does not check the command, and forwards it to the database.

This is an example of an SQL injection attack, one of the most common and unpleasant attacks made possible by deficiencies in input validation. Such attacks, as well as XSS vulnerabilities (Cross-Site Scripting) and many other types of vulnerabilities, are reported to FICORA’S CERT-FI unit every week.

SQL injections, in particular, can be used to create quite serious vulnerabilities fairly easily. They allow you access to the back-end database where you can search for information or, as is common today, add your own hostile code. A large proportion of information security breaches could be avoided with regular updates of web applications and vulnerability testing after major changes in code. Input validation is the single most important factor in the security of a web server.



NCSA leads the way to international cooperation

From the beginning of next year, Finland will have a new information security function with the establishment of the FICORA’s NCSA operations. The purpose of the unit, in addition to its other tasks, is to verify the information security requirements of information systems, and thus facilitate international co-operation and the appropriate handling of classified information.

The number of professionally targeted attacks on information security is growing at an unprecedented pace. At the same time, there are increasing requirements for protecting classified information. In international cooperation, more often than ever before a statement issued by the national information security authority on security levels and reliability of products or systems is required.

Information security issues must be taken into account in all phases of information management. Finland exists in an international information network economy. Many Finnish companies and communities have come across situations where making a deal or an agreement has until now been complicated by the lack of an official national security authority that would provide information systems with security classifications, says **Timo Lehtimäki**, Director of the Networks and Security profit area of FICORA.

An internationally standardised national security authority, i.e. the National Communications Security Authority (NCSA), will from now on focus on fulfilling Finland’s international information security obligations.

Network communities – wrestling grounds for freedom and responsibility

Social media is based on interaction, and it forces both organisations and private internet users to evaluate their web behaviour in a new way.

Blogs, discussion forums, video services and network communities have made communications increasingly interactive.

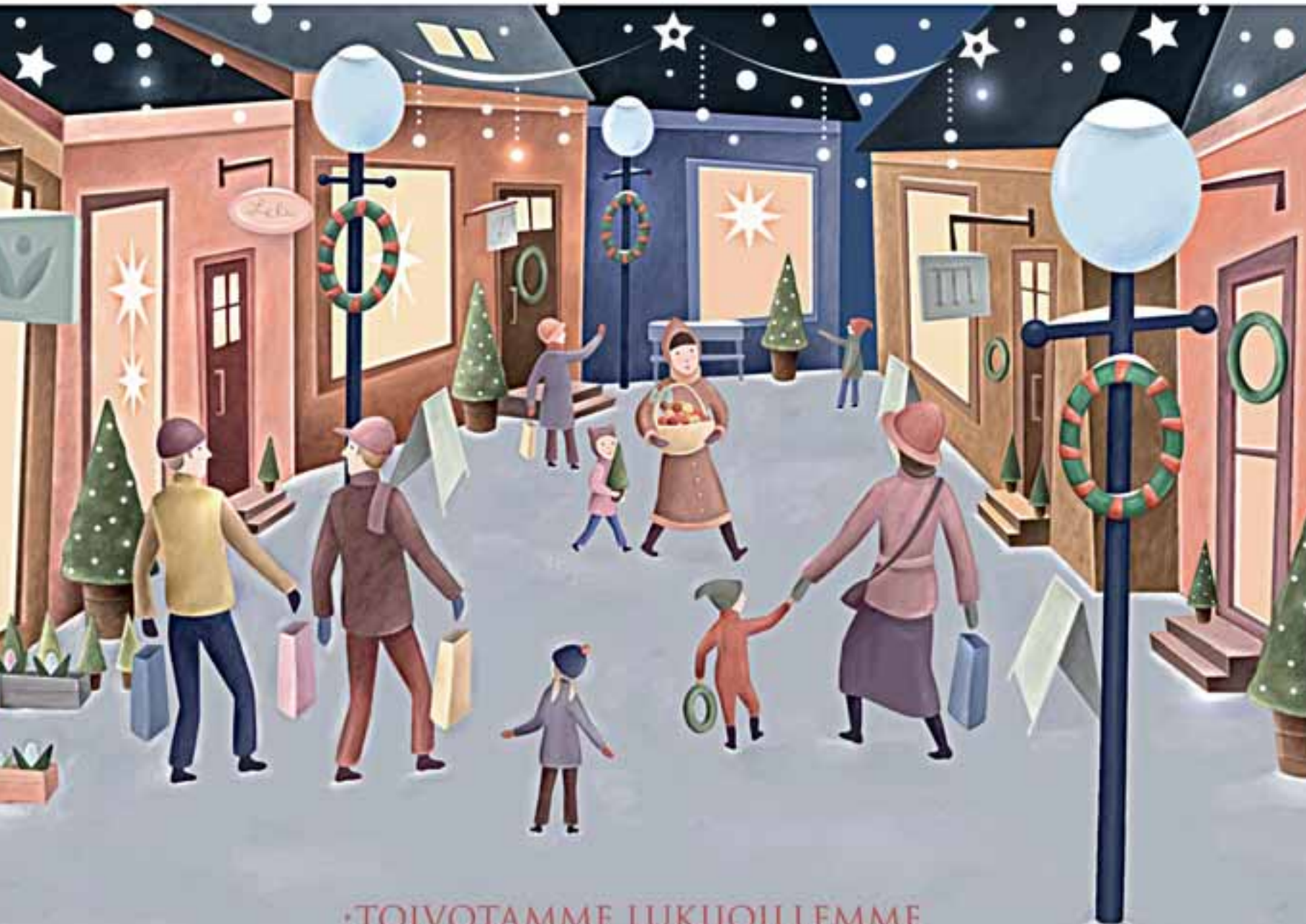
Social media can be identified by the fact that its contents are created by the users of the service, summarises **Janne Matikainen**, a researcher in social media from the University of Helsinki.

In addition to formal information, it is best to write very sparingly about your personal life on the web. By expressing your feelings too openly on the web, it is possible to unwittingly give away important information that can be used for marketing purposes. Social media is also used to spread viruses and malware that can steal information.

Companies, public organisations and the media are all eager to ride the coattails of social media, since it gathers together the audience they wish to reach. The lack of a clear financial benefit is, however, one reason why some workplaces do not allow employees to use social networking services. By contrast, in sectors where networking or consumer behaviour research are important, social media is becoming an important tool.



By expressing your feelings too openly on the web, it is possible to unwittingly give away important information that can be used for marketing purposes.



•TOIVOTAMME LUKIJOILLEMME

HYVÄÄ JOULUA JA ONNELLISTA UUTTA VUOTTA

•VI ÖNSKAR VÅRA LÄSARE GOD JUL OCH GOTT NYTT ÅR

•SEASON'S GREETINGS AND BEST WISHES FOR THE NEW YEAR