

# signaali

Viestintäviraston asiakaslehti 4/2010

JANNE  
GALLEN-KALLELA-SIRÉN:  
VIESTINTÄÄ  
TAIDEKENTÄLLÄ

9

TERVETTÄ  
JÄRKEÄ  
NETTISURFFAILUUN

2

TEOLLISUUSAUTOMAATIOT  
HOUKUTTAVAT RIKOLLISIÄKIN

14

Suosittu ja säännelty

# TUOTESIJOITTELU

10



**Suurin osa  
lapsista ei  
pidä ongelmana  
sellaista, minkä  
aikuiset kokevat  
uhkana.**

# Tervettä järkeä NETTISURFFAILUUN

Monien internet-palveluiden käyttäminen edellyttää henkilötietojen ilmoittamista; tietojen antamista on mietittävä tapaus kerrallaan.

Teksti: Maarit Seeling

Kuva: iStockphoto

**S**uomalaisen verkonkäyttäjän oikeusturva on suhteellisen hyvällä tolalla, sillä henkilötietolaki säätelee tietojen keräämistä. Lain määräyksiä siitä, mitä ja miten tietoja saa kerätä, on lisäksi täydennetty sähköisiä tietokantoja ja tiedonkeruuta koskevilla määräyksillä. Päätökset noudattavat EU:n tietosuojalainsuuntojen linjauksia.

Silti esimerkiksi verkkokaupat keräävät henkilötietoja asiakasrekistereihinsä. Erilaiset keskustelupalstat edellyttävät lähes poikkeuksetta rekisteröitymistä. Kilpailuun osallistujan tai palautteen antajan tiedot kysytään, jotta hänelle voidaan vastata. Tapahtumajärjestäjät vaativat lippuja varatessa luottokorttitietoja. Lisäksi internetissä surffailusta tallentuu tietoja palvelimille usein ilman, että käyttäjä voi siihen itse vaikuttaa.

– Harkinta on aina paikallaan, kun luovuttaa henkilötietojaan internetissä. Hyvä tapa suojata yksityisyyttään on tiedostaa, mitä tietoja itsestään luovuttaa, kenelle ja mihin tarkoitukseen. Salasanoja tulisi vaihtaa riittävän usein, eikä niitä saisi antaa ulkopuolisille. Identiteettivarkauden mahdollisuus on todellinen, tutkija **Reijo Kupiainen** Tampereen yliopiston tiedotusopin laitokselta summaa.

Hän muistuttaa, että nettiin laitetuista tiedoista jää aina jälki. Siksi jokaisen, niin nuoren kuin aikuisen, pitää olla varovainen sen suhteen, mitä tietoja muiden kanssa jakaa. Yleiseen jakeluun laitettu valokuva saattaa vuosien päästä nolottaa. Silloin kuitenkin liian myöhäistä.

Kupiainen johti Suomen tutkimusryhmää lokakuussa julkistetussa EU Kids Online -tutkimuksessa, jossa selvitettiin internetin riskejä ja tietoturva nimenomaan lasten näkökulmasta. Tutkimusta varten haastatettiin 23 000 eurooppalaista lasta.

## Mediakasvatusta ala-asteille

EU Kids Online -tutkimus suosittaa satsaamista nuorten nettiturvallisuuteen. Esimerkiksi 11–12-vuotialta puuttuvat useimmiten aivan perustaidot siitä, miten yksityisyys suojataan ja epäasialliset yhteydenotot torjutaan.

Omasta mielestään suomalaislapset kuitenkin hallitsevat erilaisia internetin käyttöön liittyviä turvataitoja muita eurooppalaislapsia paremmin. Toisaalta he käyttävät nettiä enemmän, mutta myös yksipuolisemmin kuin eurooppalaiset ikätoverinsa.

Mediakasvatus tulisi Kupiaisen mielestä saada Suomessa koulujen opetussuunnitelmiin. Uudessa tuntijakoesityksessä tilanne näyttää hänen mukaansa sen sijaan entisestään huononevan. Hän sanoo, että nyt mediakasvatus on liiaksi yksittäisten opettajien intressien varassa.

– Käytännössä asiasta ovat huolehtineet meillä vapaaehtoisohjalta erilaiset yhdistykset, kerhot ja muut yhteiskunnalli-

## TURVALLISESTI VERKOSSA

- Vaihda salasanaa riittävän usein äläkä luovuta sitä ulkopuolisille.
- Palveluntarjoaja todennäköisesti kerää tietoja mieltymyksistäsi ja välittää yhteystietojasi eteenpäin, jos palveluun rekisteröityminen tai ohjelman asennus tarjoaa mahdollisuutta erilaisen postin saamiseen. Kieltäydy palvelusta, jos et halua näin tapahtuvan.
- Monet palvelut vaativat vähintään sähköpostiosoitteen. Perusta rinnakkaisosoite, jonka voit tarvittaessa antaa, jos tietojen luovuttaminen muuten epäilyttää.
- Hanki kunnollinen haittaohjelmien poistaja. Poista evästeet säännöllisesti.
- Lue sivuston tietosuojaseloste ennen kun luovutat henkilötietojasi.

Lähteet: Reijo Kupiainen haastattelu ja Nortonin artikkelikirjasto

Lue lisää vinkkejä:  
[www.tietoturvaopas.fi](http://www.tietoturvaopas.fi)  
[www.tietosuoja.fi](http://www.tietosuoja.fi)  
[www.mll.fi](http://www.mll.fi)

set toimijat. Aika erikoista, ettei mediakasvatus kuulu pysyvästi opetussuunnitelmiin, vaikka se on olennainen osa nuorten maailmaa. Nettiturvallisuuksiin olisi opetettava järjestelmällisesti jo ala-asteella, Kupiainen toteaa.

Hän perustelee mediakasvatuksen lisäämisen tarvetta myös sillä, että näin voitaisiin ohjata nuoria monipuoliseen, osallistuvaan ja positiiviseen internetin käyttöön.

– Puolet tutkimukseen osallistuneista lapsista koki, että on helpompi ilmaista itseä netissä kuin oikeassa elämässä. Mahdollisuus nimettömyyteen lisää myös valmiutta osallistua. Käänteinen puoli on tietysti se, että käyttäytymisnormit voivat romahtaa, kun voi esiintyä anonyymisti.

### Puhumalla paras

EU Kids Online -tutkimuksen mukaan vain yksi kahdeksasta eurooppalaislapsista on kokenut jotain epämiellyttävää internetissä. Tutkimuksessa kartoitettiin lasten kokemuksia internetissä olevasta pornografiasta, seksuaalisista viesteistä, kiusaamisesta sekä muiden käyttäjien luomasta haitallisesta materiaalista. Suurin osa lapsista ei kuitenkaan pidä ongelmana sellaista, minkä aikuiset kokevat uhkana.

– Lasten vanhemmat eivät ole useinkaan tietoisia lasten kokemista riskeistä. Suomessa tilanne on keskimääräistä parempi. Meillä 70 prosenttia vanhemmista oli tietoisia esimerkiksi nettikiusaamisesta, kun taas muualla Euroopassa tästä oli tietoisia vain puolet.

Kupiainen muistuttaa, että netinkäytön pelisäännöistä tulisi sopia perheenjäsenten kesken. Oleellista on, että lapsilla ja vanhemmilla on keskenään toimivat puhevälit niin, että vaikeistakin asioista voidaan keskustella.

– Vanhempien on hyvä tietää, millainen online-elämä heidän lapsellaan on, mistä hän on kiinnostunut ja missä liikkuu. On syytä ehkä olla hieman huolissaan, jos jälkikasvu kovasti peittelee tekemisiään, sulkee oven perässään eikä päästä vanhempiaan huoneeseen. Lapsen on uskallettava kertoa ongelmista ilman, että hänen tarvitsee pelätä vanhempien sen takia rajoittavan tietokoneen käyttöä, Kupiainen kiteyttää. ✘

## Sisällys

- 2** Nettisurffailu edellyttää tapauskohtaista harkintaa
- 5** Pääkirjoitus: Anna Lauttamus-Kauppi
- 6** Ajankohtaista
- 8** Linkkivinkit
- 9** Vaihtopenkillä Janne Gallen-Kallela-Sirén
- 10** Tuotesijoittelun uudet pelisäännöt
- 14** Teollisuusautomaatio hyökkäysten kohteena
- 16** Esittelyssä Hollannin OPTA
- 18** ISO 27001 todistaa turvallisuudesta
- 20** Mikä ihmeen pseudoliitti?
- 21** Kolumni: Pauli Aalto-Setälä
- 22** Svensk resumé
- 23** English summary

## Tietoturvapäivä-hanke tukee lasten nettiturvallisuuksikasvatusta

Tietoturvapäivä-hanke on tukenut lasten ja nuorten nettiturvallisuuksikasvatusta vuodesta 2005. Hanke ylläpitää ja päivittää aktiivisesti www.tietoturvakoulu.fi-sivustoa, joka on tarkoitettu pääasiassa koulujen ja vanhempien käyttöön. Sivusto pitää sisällään runsaasti tietoa kasvattajille ja erilaisia tehtäviä, pelejä ja kilpailuja nettiturvallisuudesta peruskoulukäisille lapsille ja nuorille.

Lisäksi hanke jakaa tietoa aiheesta säännöllisin koulupostituksin, esittein ja tapahtumien kautta. Koulujen tukena on myös maksuton Kummipankki-palvelu, jonka kautta voi tilata asiantuntijan puhumaan oppilaille, opettajille tai vaikkapa vanhempainiltaan.

Tietoturvapäivä-hanke on saavuttanut vakaan suosion peruskouluissa, mutta tehtävää riittää edelleen, kuten Reijo Kupiainenkin toteaa.

Nettiturvallisuuksimateriaaleja tekevät myös monet järjestöt, esimerkiksi Mannerheimin Lastensuojeluliitto, Pelastakaa Lapset ja Mediakasvatusseura.

Teksti: Heli Alanko, projektikoordinaattori, Viestintävirasto



# Pääkirjoitus

## Somen vuosi

**O**letteko jo siellä ja jos, niin missä siellä? Kuinka usein päivitätte statustanne? Montako tykkääjää sivullanne on ja miten te heitä sinne saatte? Käykö keskustelu vilkkaana?

Näitä asioita me viestinnän ammattilaiset kysellemme toisiltamme lukuisten sosiaalisen median hyödyntämistä tarkastelevien seminaarien tauoilla. Ja innostusta riittää: sosiaalinen media eli tutummin some on kuluvan vuoden aikana todella lyönyt itsensä läpi myös julkishallinnossa.

Mutta miksi? Miksi lähteä mukaan? Sosiaalinen media tarjoaa hallinnon organisaatioille oivan lisämahdollisuuden parantaa tunnettua ja lisätä vuorovaikutusta sekä asiantuntijasidosryhmien että kansalaisten kanssa. Kun somen käyttöä pohditaan organisaatioissa, avainsanat ovat mielestäni harkinta, resursointi ja organisointi. Kannattaa muun muassa nähdä vaivaa, jotta tunnustetaan ne sosiaalisen median palvelut ja foorumit, joilla oman organisaation läsnäolo on perusteltua ja eri osapuolille hyödyllistä. Julkisella sektorilla pitää olla erityisen tarkkana: ei ole järkeä liikkua trendien perässä uusiin kanaviin, jos ei ensin ole mietitty miksi ja millä tavoin siellä olla ja mitä hyötyjä siitä on asiakkaille ja sitä kautta organisaatiolle itselleen. Olemmehan yhteis-

kuntavastuussa myös viestinnän keinoja ja kanavia valittaessa.

Viestintävirasto jalkautui verkkoyhteisöihin reilu vuosi sitten. Emme tosin ole virastona esillä vaan palveluidemme kautta. CERT-FI ja Tietoturvapäivä-hanke ovat olleet edelläkävijöitä, ja tv-maksut liittyvät seuraan niin kutsutulla Kiitos-kampanjalla tammikuun lopussa.

Viestintäviraston some-kokemukset ovat olleet hyvin myönteisiä. Seuraajajoukkoja tietoturvasivuiltamme on pikku hiljaa saatu kasvatetuiksi ja keskusteluakin käydään. Olemme siis pystyneet jakamaan tietoturvakkeja ja -neuvoja aikaisempaa laajemmalle yleisölle ja entistä vuorovaikutteisemmalla tavalla. Jatkossa muidenkin kuluttajatehtävien, kuten laajakaistan, verkkonäkyvyyttä ja löydettävyyttä on tarkoitus lisätä – asiakkaidemme hyväksi.

P.S. Virta vie myös somesta pois päin. Viimeisimmän tiedon mukaan muun muassa **Lady Gaga** ja **Justin Timberlake** pidättäytyvät sosiaalisen median käytöstä kerätäkseen poissaolollaan miljoona dollaria **Alicia Keysin** hyväntekeväisyyskampanjaan ”Keep a Child Alive”. Saa nähdä, tuleeko läsnäolon sijaan poissaolosta pian se kaikkein hypetyn trendi?



**Olemme yhteiskunta- vastuussa myös viestinnän keinoja ja trendejä valittaessa.**



**Anna Lauttamus-Kauppi**  
Viestintäjohtaja, päätoimittaja

Kuva:  
Kaapo Kamu

### Julkaisija

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

### Päätoimittaja

Anna Lauttamus-Kauppi

### Toimituspäällikkö

Heli Tarkiainen

### Viestintätoimisto

Mediafocus

### Taitto

Jaska Poikonen

### Kannen kuva

Susa Junnola

### Painopaikka

Edita Prima,  
Helsinki

### Toimitusneuvosto

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

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

Seuraava numero  
Maaliskuu 2011

ISSN 1458-5715



## Lapsille haitallisten kuvaohjelmien valvonta keskitetään yhdelle viranomaiselle

**Kuvaohjelmalainsäädännön** uudistamista koskeva lakiesitys on annettu eduskunnalle lokakuussa. Tarkoituksena on uudistaa lainsäädäntö vastaamaan paremmin muuttunutta mediaympäristöä sekä panostaa valvonnan ohella muihin lasten turvallisuutta edistäviin toimenpiteisiin kuten mediakasvatukseen ja kasvattajille suunnattuun tiedottamiseen. Kuvaohjelmien ennakkotarkastuksesta on tarkoitus luopua, mutta ikärajajärjestelmä säilytettäisiin.

Ennakkotarkastuksen sijaan ohjelmien luokittelu siirtyy pääosin toimialan itsensä tehtäväksi. Ohjelmien luokittelijoiden tulisi kuitenkin olla viranomaisen hyväksymiä ja riippumattomia kuvaohjelmaluokittelijoita. Lakimuutoksen tarkoituksena on myös yhdenmukaistaa nykyistä kuvaohjelmien luokittelua niin, että luokittelu koskisi sekä elokuvia, televisio-ohjelmia että pelejä riippumatta siitä, levitetäänkö niitä tallenteina tai esitetäänkö niitä teatterissa, televisiölähteyksinä tai internetissä.

Käytettävät ikärajat olisivat 7, 12, 16 tai 18 vuotta. Lisäksi ohjelmiin tulee lisätä sisältöä – kuten väkivaltaa, seksiä, kauhua tai päihteitä – kuvaava symboli. Kuvaohjelmien valvonta muuttuisi kauttaaltaan jälkikäteen tapahtuvaksi. Tätä tehtävää hoitamaan perustetaan Mediakasvatus- ja kuvaohjelmakeskus nykyisen valtion elokuvatarkastamon pohjalle. Televisiotoimintaa koskevat lasten suojeluun liittyvät valvontatehtävät siirtyisivät tähän uuteen keskukseseen. Lain on tarkoitus astua voimaan vuoden 2012 alussa.



Kuvaohjelmien luokittelussa käytettäväksi ikärajoiksi on ehdotettu 7, 12, 16 ja 18 vuotta.

## Lain muutos virallisti Viestintäviraston NCSA-FI-yksikön aseman

**Viestintäviraston** NCSA-FI-yksikön (National Communications Security Authority) toiminta vahvistui, kun kansainvälisistä tietoturvallisuusvelvoitteista annetun lain muutokset tulivat voimaan 1.11.2010. NCSA-FI on Viestintävirastossa toimiva kansallinen tietoturvallisuusviranomainen, joka toimii asiantuntijana turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvis-

sä turvallisuusasioissa ja hoitaa näihin liittyviä kansainvälisistä tietoturvallisuusvelvoitteista johtuvia tehtäviä.

Suomi on valinnut kansainvälisten tietoturvallisuusvelvoitteiden järjestämisestä hajautetun organisointimallin. Ulkoasiainministeriö toimii kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaisesti Suomen kansallisena turvallisuusviranomaisena (NSA, National

Security Authority). Laissa määritetään myös muita määrättyjä turvallisuusviranomaisia (DSA, Designated Security Authority). Viestintävirasto suorittaa NSA:n valtuuttamana kansalliselle tietoturvallisuusviranomaiselle (NCSA, National Communications Security Authority) kuuluvia tehtäviä.



## Määräys 28 H/2010 M: Kohti parempaa yhteentoimivuutta ja tietoturva

**Viestintävirasto** on uudistanut ja koonnut yhteen aiemmin määräyksiin 28 ja 49 hajautetut velvoitteet viestintäverkkojen ja -palveluiden yhteentoimivuudesta. Velvoitteita on arvioitu uudestaan ja käytännössä kaikkia velvoitteita tai ainakin niiden perusteluja ja soveltamisohjeita on muutettu tai täydennetty.

Monia PSTN/ISDN-perusteisia vaatimuksia on poistettu, koska ne eivät enää ole välttämättömiä. Toisaalta määräykseen on myös lisätty kokonaan uusia kaikkia viestintäverkkoja ja -palveluita koskevia vaatimuksia. Määräyksen soveltamisalaa on laajennettu koskemaan kattavasti IP-pohjaisia viestintäverkkoja ja -palveluita. Tämä tarkoittaa muun muassa etenkin VoIP-palveluiden parempaa huomioimista. Määräykseen on lisäksi siirretty kaikkiin IP-pohjaisiin viestintäverkkoihin ja -palveluihin soveltuvia kohtia Viestintäviraston määräyksestä 13 internet-yhteyspalvelujen tietoturvasta ja toimivuudesta.

Määräyksen tarkoituksena on edistää eri teleyritysten viestintäverkkojen ja palveluiden yhteenliitettävyyttä sekä viestintäpalveluiden päästä–päähän-yhteentoimivuutta. Tavoitteena on ennaltaehkäistä viestintäverkkojen ja -palveluiden yhteenliittämiseen liittyviä ongelmia ja edistää näin uusien palveluiden käyttöönottoa. Määräyksellä on tarkoitus varmistaa, että teleyritykset pitävät huolta yhteenliittämisen ja asiakasrajapintojensa tietoturvasta ja parantaa siten viestintäverkkojen ja -palveluiden toimintavarmuutta.

Määräys 28 H/2010 M Viestintäverkkojen ja -palveluiden yhteentoimivuudesta tulee voimaan 1.4.2011. Tämä ja muut viraston määräykset löytyvät osoitteesta [www.ficora.fi](http://www.ficora.fi) -> Määräykset ja päätökset -> Määräykset.

## Kuluttajat arvostavat eniten puhelin- ja laajakaistaliittymän teknistä toimivuutta ja laskutuksen selkeyttä

**Puhelin- ja laajakaistaliittymän** tekninen toimivuus sekä laskutuksen selkeys ja virheettömyys ovat kuluttajien mukaan keskeisimmät viestintäpalveluiden laatua kuvaavat tekijät. Myös asiakaspalvelun asiantuntemus ongelmatilanteissa koetaan liittymätyypistä riippumatta yhdeksi neljästä tärkeimmästä laatutekijästä.

Toimituksen sujuvuus sovittuun mukaisesti on matkapuhelinliittymissä ja kiinteissä laajakaistaliittymissä merkittävä laatutekijä. Mobiililaajakaistaliittymää hankittaessa myös myyjän asiantunteva palvelu koettiin tärkeäksi. Lankapuhelinliittymää käytettäessä operaattoria kohtaan tunnettu luottamus nousee kolmanneksi merkittävimmäksi laadun osatekijäksi.

Kuluttajien mielestä operaattorit ovat onnistuneet monissa asiakkaiden tärkeiksi kokemissa laatutekijöissä. Reagointinopeus asiakkaiden tarpeisiin ja yhteydenottoihin on ainoa kriittinen kehityskohde. Sen merkittävyys

on keskitasoa, mutta toteutuminen on heikohkoa. Matkapuhelinpalveluissa myös asiakaspalvelun asiantuntemus ongelmatilanteissa ja mobiililaajakaistapalveluissa luvattu tiedonsiirtonopeus ovat melko kriittisiä tekijöitä. Vaikka ne ovat asiakkaille tärkeitä, operaattorit eivät ole kyenneet toteuttamaan kumpaakaan osatekijää kuluttajia täysin tyydyttävällä tavalla.

Jatkuvat tekniset murheet ja laajakaistan luvattua heikompi suorituskyky ovat tekijöitä, jotka voisivat helpoiten johtaa operaattorin vaihtamiseen. Myös kilpailijan edullisempi hintataso saattaa vaikuttaa vaihtohalukkuuteen, mutta hintaa ei kuitenkaan nosteta aivan tärkeimmäksi syyksi vaihtaa liittymää.

Tiedot käyvät ilmi Viestintäviraston syyskuussa 2010 teettämästä telepalveluiden laatu tutkimuksesta, joka on luettavissa viraston verkkosivuilla osoitteessa [www.ficora.fi](http://www.ficora.fi).

## Oma identiteetti kullan kallis

**Tietoturvapäivää** ja -viikkoa vietetään 8.2.2011 kahdeksatta kertaa. Tällä kertaa kampanjan kantavana teemana on yksityisyys netissä. Lisäksi käsitellään sosiaalisen median tietoturvakysymyksiä laajemminkin.

Sosiaalinen media on tuonut netin ongelmatilanteet entistä lähemmäs tavallisen netinkäyttäjän arkea. Turvallinen verkkoyhteisöjen käyttäminen vaatii kuitenkin tarkkaavaisuutta ja oman yksityisyyden varjelu on entistäkin tärkeämpää. Omien tietojen kertomista kannattaa miettiä niin sosiaalisissa medioissa kuin muissakin verkkopalveluissa. Yhteisöpalveluissa on hyvä harkita myös klikkauksiaan, sillä huijaukset saattavat näyttää varsin viattomilta viesteiltä kavereilta.

Tietoturvaviikko alkaa 7.2.2011 ja pitää sisällään taas monia tapahtumia: muun muassa seminaareja, koulutapahtumia ja yleisöluennon. Tietoturvapäivä näkyy aiempaa enemmän myös verkossa, joten pidä silmät auki surffatessa. Jo nyt kannattaa

käydä klikkaamassa Tietoturvapäivän Facebook-sivun tykkää-nappia osoitteessa [www.facebook.com/tietoturvapäivä](http://www.facebook.com/tietoturvapäivä).



## Viestintävirasto keventää vähittäismarkkinoiden sääntelyä

**Viestintävirasto** poisti 10.11.2010 teleyrityksille antamallaan huomattavan markkinavoiman päätöksillä kiinteän verkon puhelinpalvelujen ennakkosääntelyn.

Annetut päätökset koskevat kiinteässä puhelinverkossa kotitalous- ja yritysasiakkaille tarjottavia lankapuhelinliittymiä sekä kiinteistä puhelinliittymistä soitettuja paikallispuhelupalveluja. Nyt annetuilla päätöksillä Viestintävirasto kumoaa aikaisemmin vuonna 2004 teleyrityksille antamansa sääntelypäätökset, joilla pyrittiin kilpailun lisäämiseen vähittäismarkkinoilla.

Viestintävirasto katsoi markkina-analysissään, että kolmen matkaviestinverkko yrityksen sekä useiden matkaviestinverkossa toimivien palveluyritysten aikaansaama kilpailupaine on siinä määrin merkittävä,

että kotitalous- ja yritysasiakkailta on riittävät mahdollisuudet kilpailuttaa nykyinen lankapuhelinpalvelujen tarjoaja tai vaihtaa palveluntarjoajaa. Toinen merkittävä ennakkosääntelyn poistamista tukeva asia oli se, että matkaviestinverkossa tarjottavat matkapuhelinliittymät ovat korvanneet suurelta osin lankapuhelinliittymien käytön. Esimerkiksi enää yksi prosentti suomalaisista kotitalouksista käyttää ainoastaan lankapuhelinliittymää, kun vastaavasti 75 prosentilla on käytössä ainoastaan matkapuhelinliittymää.

Annettujen päätösten jälkeen kotitalous- ja yritysasiakkaiden riittävien puhelinpalvelujen saanti turvataan puhelinpalvelujen tarjontaa koskevalla yleispalvelusääntelyllä niillä alueilla, joilla kilpailun on katsottu olevan riittämätöntä turvaamaan peruspuhelinpalvelujen saatavuus.



1 % kotitalouksista käyttää ainoastaan lankapuhelinliittymää. 75 % käyttää ainoastaan matkapuhelinliittymää.

## LINKKIVINKIT

### Päivitettyä tietoturvatietoa

Tietoturvaopas.fi-sivustolle päivitetään ennen helmikuun Tietoturvapäivää runsaasti uutta tietoa sosiaalisten medioiden turvallisesta käytöstä, linkkihuijauksista ja yksityisyyden suojasta.

[www.tietoturvaopas.fi](http://www.tietoturvaopas.fi)



### Tervetuloa tietoturvakouluun

Kouluikäiset lapset ja nuoret ovat monesti aikuisia kokeneempia verkkoyhteisöjen käyttäjiä, mutta tarvitsevat silti vähintään yhtä paljon opastusta yksityisyytensä suojelemiseen ja turvalliseen surffailuun. Oppilaille onkin suunnitteilla erilaisia tehtäviä ja kilpailu [tietoturvakoulu.fi](http://tietoturvakoulu.fi)-sivustolle.



## INTIIMI SUHDE

Kuvan maailma ja viestintä-  
teknologia kuuluvat yhteen,  
Janne Gallen-Kallela-Sirén sanoo.

Teksti: Tiia Soininen Kuva: Jyrki Komulainen

**Kesäkuussa 2010** New Yorkin Guggenheim-museo ryhtyi yhteistyöhön YouTube'n kanssa: yleisö sai lähettää nettiin omia videoteoksiaan, joista parhaat pääsisivät videotaiteen näyttelyyn. videoita lähetettiin yli 23 000 kappaletta!

– Meillä Helsingissä puolestaan oli kesällä 2010 näyttely *Toden näköistä – nettisukupolven maalareita*, jossa perehdyttiin siihen, miten internetin olemassaolo on vaikuttanut kuvataiteilijoiden visuaaliseen näkemykseen maailmasta. Internetistä lainataan teemoja, mutta yhtä lailla myös tyylejä. Perinteistä öljyväritekniikkaa käyttävä taiteilija saattaa esimerkiksi pikselöidä kuvapintansa tavalla, joka muistuttaa digitaalista kuvapintaa, Helsingin taidemuseon johtaja **Janne Gallen-Kallela-Sirén** kertoo.

Hänen mukaansa virta viestintäteknologian ja taiteen välillä on kahdensuuntaista. Teknologia vaikuttaa yhtä lailla taiteen ja taiteilijoiden kuin yleisön ja taiteen suhteeseen.

### Välitöntä vuoropuhelua

Yleisön ja taiteen välistä vuoropuhelua viestintäteknologian kehitys on Gallen-Kallela-Sirénin mukaan monipuolistanut. Onhan kanavia käytössä aiempaa enemmän.

– Yleisöllä on mahdollisuus kommentoida yksittäisiä näyttelyitä, teoksia, taiteilijoita – ja yksittäisiä museonjohtajia – ilman ins-

titutionaalisen median filteriä, hän toteaa.

Sosiaalisen median, sähköpostin ja tekstiviestien ansiosta tiedonsiirto myös taidekentällä on nopeutunut.

– Kansalliset umpiot ovat auenneet, taide ja sen vastaanotto on maapalloistunut. Sata vuotta sitten värivalokuva oli vielä tulevaisuutta, taideteoksien toisinnot olivat mustavalkotekniikalla tai esimerkiksi litografioina toteutettuja. Nyt jokainen voi ottaa kännykkä- tai digikameralla kuvan teoksesta, lähettää sen ystäväpiirilleen ja sanoa, että tätä minä ihailen suuresti tai tästä en sitten pidä ollenkaan.

### Kun puhutaan kuvasta, puhutaan viestintäteknologiasta

Taidemaailmassa pätee sama kuin maailmassa muutenkin: nuorempi sukupolvi on alttiimpi hyödyntämään uusia teknologioita, iäkkäämmät kokevat ne vieraammiksi.

Helsingin taidemuseolla on Facebookissa oma sivustonsa. Taidemuseolaiset ovat myös itse aktiivisia netin käyttäjiä. Internetin yhdistämä alan ammattilaisten verkosto auttaa esimerkiksi amanuensseja niin tutkimuksellisten kuin näyttelytekniistenkin ongelmien ratkaisemisessa.

Janne Gallen-Kallela-Sirén uskoo, että viestintäteknologian kehittymisen myötä me maailmankansalaiset seisomme nyt kuvan vuosituhannen kynnyksellä.

– Kun puhutaan kuvasta, puhutaan myös



viestintäteknologiasta. Ne ovat intiimissä suhteessa keskenään. Kyse on siitä, miten kuvaa voidaan käsitellä, tuottaa, manipuloida ja siirtää. Olemme seitsemänvuotiaasta lähtien pöntänneet koulunpenkeillä luku- ja kirjoitustaitoa. Tämän päivän maailmassa, jossa kuva on dominoivassa asemassa, meidän on aika alkaa opetella visuaalista lukutaitoa.

*Filosofian tohtori Janne Gallen-Kallela-Sirén (s. 1970) on toiminut Helsingin taidemuseon johtajana vuodesta 2007.*



### KIERTÄVÄ KYSYMYS

Edellinen vaihtopenkkivieras Sampo Oyj:n hallituksen puheenjohtaja **Björn Wahlroos** esitti Helsingin taidemuseon johtaja **Janne Gallen-Kallela-Sirénille** kysymyksen: Miten viestintäteknologian kehittyminen on vaikuttanut taiteen ja yleisön väliseen kommunikaatioon?

Janne Gallen-Kallela-Sirén haluaa haastaa seuraavaksi vaihtopenkkiläiseksi Helsingin kaupungin sivistys- ja henkilöstötointa johtavan apulaiskaupunginjohtaja **Tuula Haataisen**. Helsingin kaupunki on Suomen suurin työnantaja, sen palveluksessa työskentelee noin 40 000 ihmistä. Kysymys kuuluu:

**Miten viestintäteknologia edesauttaa työssä jaksamista ja henkilöstön hyvinvointia?**

# TUOTESIJOITTELULLE PELISÄÄNNÖT

Luonteva näkyvyys toimii parhaiten.

Teksti: Minna Kalajoki Kuvat: Susa Junnola

**R**uokaohjelman keittiökalueteet eivät ole sattumalta tietynmerkkiset. Ne on tuotesijoitetu ohjelmaan. Yhä suosituimpi mediainnonnan muoto, tuotesijoittelu, sai toukokuussa 2010 uudet, selkeät pelisäännöt.

Tuotesijoittelulla tarkoitetaan tuotteen tai palvelun sijoittamista osaksi mediasisältöä niin, että se istuu ohjelman sisältöön. Sijoitettu tuote ei kuitenkaan saa olla pääroolissa.

EU:n audiovisuaalisten mediapalvelujen direktiivi mahdollisti vastikkeellisen tuotesijoittelun sallimisen nyt säädetyllä tavalla. Lakia päätettiin tältä osin muuttaa, sillä rajanveto sallitun tuotesijoittelun ja kielletyn piilomainonnan välille koettiin tärkeäksi.

Uudistettu laki televisio- ja radiotoiminnasta sisältää selkeät säännöt tuotesijoittelun ilmoittamisesta ja toteutustavasta. Vastikkeellinen tuotesijoittelu on sallittu elokuvissa ja tv-sarjoissa, urheiluohjelmissa sekä kevyissä viihdeohjelmissa. Tuotesijoittelua ei saa käyttää lastenohjelmissa. Tuotesijoittelulla ei saa vaikuttaa ohjelmien sisältöön, eikä tuotteita saa aiheettomasti korostaa esimerkiksi kuvausteknisin keinoin.

Kuluttajalle näkyvin muutos on, että tuotesijoittelusta pitää ilmoittaa ohjelman alussa, lopussa ja jokaisen mainoskatkon jälkeen. Ilmoitusvelvollisuutta sovelletaan vain itse tuotettuihin tai tilattuihin ohjelmiin.

## Piilomainontaan puututaan

Uusi laki koskee myös internetin kautta jaettavia televisio-ohjelmia ja elokuvia sekä tilausohjelmalveluita. Lain valvonta säilyy Viestintäviraston ja kuluttaja-asiamiehen vastuulla.

– Tuotesijoittelu ei ollut ennenkään kiellettyä, ja valvonnassa keskitytään siihen

mihin aikaisemminkin eli puuttumaan kiellettyyn piilomainontaan, Viestintäviraston viestintäpalvelujen valvonnasta vastaava apulaisjohtaja **Merja Saari** selventää.

Saaren mukaan alkuvaiheessa ratkaisuja varmasti tarvitaan, jotta rajanveto selkenee. Lain astuttua voimaan tuotesijoittelua on ryhdytty käyttämään enemmän, ja toimintakenttä muuttuu jatkuvasti.

– Tuotesijoittelua kehitetään kovaa vauhtia, ja uusia ilmiöitä syntyy. Niitä pitää arvioida tapauskohtaisesti. Yhteistyö kaupallisten kanavien kanssa toimii kuitenkin hyvin. Tietojen vaihdosta ja jatkuvasta yhteydenpidosta on jo sovittu, Saari kertoo.

Kaupallinen kanava uskoo tuotesijoittelun valvonnassa enemmän mediakasvatukseen kuin tiukkaan sääntelyyn. Sääntely ei kuitenkaan voi ulottua läheskään kaikkiin kuluttaviin mediasisältöihin.

– Tuotesijoittelu on yksi tapa mainostaa, vanhempien tulisi selittää sitä lapsilleen aivan kuten perinteistä mainontaa. Suomalaiset tv-katsojat ovat niin valveutuneita, että älähtävät kyllä, jos tuotesijoittelu menee yli. Fiksua katsojia ei tarvitse suojella, vaan tärkeintä on tarkastella asioita katsojalähettöisesti, MTV Median viestintäpolitiikan apulaisjohtaja **Petra Wikström-Van Eemeren** huomauttaa.

Kaupallisilla kanavilla tuotesijoittelu lisääntyy nopeaa tahtia. Yleisradio on linjannut, ettei mainosluonteista tuotesijoittelua sallita sen omissa ohjelmissa. Maailmanlaajuisesti tuotesijoittelun käytön arvioidaan kaksinkertaistuvan nykyisestä vuoteen 2014 mennessä.

MTV Media näkee tuotesijoittelun kaikkia osapuolia hyödyttävänä mediainnonnan muotona.

– Katsojatutkimukset osoittavat katsojien hyväksyneen tuotesijoittelun, mainostajien mielestä se toimii hyvin ja tuotantoyhtiöt

suhtautuvat siihen myönteisesti. Lisäksi tuotesijoittelu avaa uusia mahdollisuuksia kotimaiseen ohjelmatuotantoon, Wikström-Van Eemeren sanoo.

## Tärkein kriteeri: luonteva näkyvyys

Mainostajat ovat hyvin kiinnostuneita tuotesijoittelusta, vaikka sen tehon mittaaminen on tavanomaista mainontaa vaikeampaa. Tehokkuus riippuu muun muassa ohjelman katsojamäärästä sekä siitä, kuinka usein ja kuinka pitkään tuote tai palvelu on esillä.

– Tuotesijoittelu hinnoitellaan aina tapauskohtaisesti. Mainostajilla on toiveensa tuotteen näkyvyyden suhteen, mutta kanava päättää ohjelman sisällöstä ja kulusta. Ehdottomasti tärkein kriteeri on luonteva näkyvyys, eikä tuotesijoittelu missään nimessä vaikuta ohjelmasisältöihin. Ohjelmissa ei jatkossakaan vilise logoja eikä tuotteisiin zoomailla, Wikström-Van Eemeren vakuuttaa.



**Ohjelmissa ei jatkossakaan vilise logoja eikä tuotteisiin zoomailla.**

Tuotesijoittelu ärsyttää katsojia  
vain, jos se tehdään huonosti,  
MTV Median viestintäpolitiikan  
apulaisjohtaja Petra Wikström-  
Van Eemeren sanoo.



Tuotesijoittelu sopii parhaiten ohjelmiin, joissa tuotteita näkyisi muutenkin. Eniten tuotesijoittelua käytetään ruoka- ja sisustusohjelmissa sekä erilaisissa kilpailuissa.

– Kilpailuohjelmassa tehtävänä voi olla auton myyminen eli auto tarvitaan joka tapauksessa. Jos mainostaja saa automerkkinsä näkyviin, kanava saa mainostuloja, eikä automerkin näkyminen millään lailla heikennä katselukokemusta, niin kaikki osapuolet voittavat. Parhaiten tuotesijoittelu onnistuu silloin, kun sen olemassaoloa ei edes ajattele. Se ärsyttää vain, jos se tehdään huonosti, Wikström-Van Eemereren huomauttaa.

### Mainostajat eivät sanele

Tuotesijoittelu täydentää mediamainonnan kenttää, sillä perinteinen mainoskatkomainonta pitää pintansa. Tallentavien digiboksin uskottiin vähentävän mainoskatkomainonnan määrää, mutta esimerkiksi MTV Median katsojatutkimukset osoittavat, että

95 prosenttia ohjelmista katsotaan edelleen suorana.

Mainoskatkomainosten ja tuotesijoittelun lisäksi ohjelmia voidaan myös sponsoroida. Näkyvyys moninkertaistuu, kun mainostaja voi samaan aikaan olla ohjelman sponsori sekä mainostaa mainoskatkoilla. Lisäksi tuotteita voi olla sijoitettuna ohjelmaan.

Aluksi tuotesijoitteluun suhtauduttiin kriittisesti, sillä mainostajien pelättiin saavan sananvaltaa ohjelmien sisältöön.

– Mainostajat eivät sanele, mistä ja miten ohjelmia tehdään. Tuotesijoittelu on vain yksi mediamainonnan muoto, jonka yhteydessä noudatetaan lakia ja sisällöllisiä linjauksia. Esimerkiksi uutisiin ei ikinä tule tuotesijoittelua, Wikström-Van Eemereren alleviivaa.

### Mahdollisuus kotimaiselle tuotannolle

– Yksi tuotesijoittelun hyvistä puolista on, että sen avulla voidaan tuottaa en-

tistä enemmän ja entistä laadukkaampia kotimaisia televisio-ohjelmia, Wikström-Van Eemereren mainitsee.

Tulevaisuudessa tuotesijoittelua nähdään myös televisiodraamassa.

– Kotimaisen televisiosarjan tuottaminen maksaa helposti kymmenen kertaa enemmän kuin amerikkalaisen ostaminen. Suomalaiset katsojat kuitenkin rakastavat kotimaista tv-draamaa, ja sen tuotannon jatkuvuuden varmistamiseksi tuotesijoittelu on hyvä keino. Lisäksi tuotesijoittelu mahdollistaa uudentyypisiä ohjelmia ja tuo mainostajiksi yrityksiä, jotka eivät muuten ehkä mainostaisi, Wikström-Van Eemereren sanoo.

MTV Media seuraa tarkalla silmällä tuotesijoittelun yleistymistä ja alan kehitystä.

– Ohjelmatyyppejen ja -formaattien kehittyessä tuotesijoittelulle avautuu koko ajan uusia mahdollisuuksia. Tulevaisuudessa kehitetään varmasti uusia, innovatiivisia tapoja tuoda erilaisia tuotteita ja palveluita luontevasti esille ohjelmissa, Wikström-Van Eemereren arvioi. ✘

## » ENEMMÄN NETTIÄ, VÄHEMMÄN TELEVISIOTA

Viestintäviraston mediapalvelujen käyttöä luotaavasta kuluttajatutkimuksesta ilmenee, että tv-ohjelmia tai niiden kaltaisia sisältöjä seurataan entistä vähemmän televisiosta ja yhä enemmän netistä. Mobiilisti mediaa ei kuitenkaan juuri kuluteta.

Suunnanmuutoksesta huolimatta mediasisältöjä seurataan edelleen selvästi eniten televisiosta kaikkina vuorokauden aikoina. Suoria televisiolähetyskatseluita noin 9,7 tuntia viikossa.

Televisiosta tallennettuja ohjelmia katsotaan noin 4,8 tuntia viikossa ja ulkopuolisia tallenteita noin 3,2 tuntia viikossa.

Nettiä käytetään usein, mutta lyhyemmän aikaa kerrallaan: televisio-ohjelmien kaltaisia videoita katsotaan noin 2,4 tuntia ja lyhyitä videoleikkeitä noin 1,7 tuntia viikossa.

Audiovisuaalisten sisältöpalvelujen kuluttotottumukset ovat muuttuneet eniten nuorilla, alle 24-vuotiailla vastaajilla. Netin päivittäinen käyttö on lisääntynyt, samoin tilausohjelmien käyttö, kehityspäällikkö **Tiina Aaltonen** Viestintäviraston markkinaselvitysyksiköstä kertoo.

Vastaajien arvioissa itse muutosta he uskovat television katselun vähenemisen olevan voimakkaampaa kuin netin käytön lisääntymisen. Television viikoittainen suora katselu

vähentyy etenkin nuorilla, mutta koko väestön keskuudessa televisio on vanhana mediana edelleen vahvoilla.

Nuoret ottavat odotetusti uutta teknologiaa haltuun nopeammin, ja käyttävät mediaa monipuolisesti.

Kokonaismuutos on kuitenkin verrattain hidasta, koska nuoret ovat pieni väestöryhmä.

Aaltosen mielestä on mielenkiintoista nähdä, muuttuuko nuorten median käyttö siinä vaiheessa, kun he perustavat perheen.

Jatkuuko ahkera netin käyttö silloinkin, vai palataanko siinä vaiheessa perinteisen television pariin?

Aaltosen mukaan sisältöjen katselu mobiilisti ei ole minkään vastaajaryhmän suosiossa. Erityisesti nuorilta puuttuu sitä kohtaan kiinnostusta, maksuhalukkuutta ja katseluun sopivia laitteita.

Mediasisältöjen kuluttaminen on kehityksessä entistä monipuolisemmaksi, kun sisältöjä katsotaan yhä enemmän eri lähteistä ja katselualustoilta. Viestintävirasto tutkii mediapalvelujen käyttöä vuosittain tutkimuksessaan, jonka kohderyhmänä ovat 15–64-vuotiaat internetiä käyttävät kuluttajat.

Viestintäviraston valvontarooli ulottuu kaikkiin televisio-ohjelmiin rinnastettaviin mediapalveluihin.

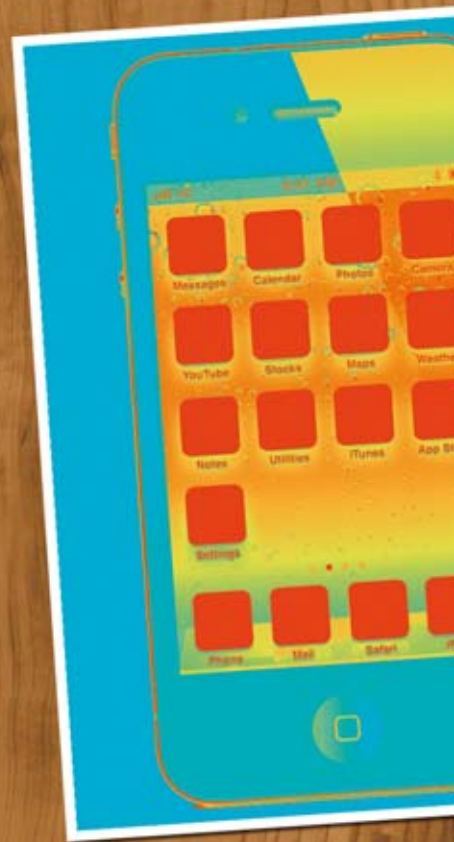
Valvonta ulottuu myös tilausohjelmien palveluihin, mutta on rajattu niihin kaupallisiin toimijoihin, jotka ovat sijoittautuneet Suomeen.

Ei siis kaikkialle, missä jotakin liikkuu, Viestintäviraston apulaisjohtaja **Merja Saari** havainnollistaa.

Saaren mukaan mediakentän pirstaloituminen on lisännyt työmäärää jo pelkästään siksi, että perinteinen televisio muuttuu kanavien lukumäärän kasvaessa.

Työmäärä lisääntyy selvästi, sillä valvonnan laajetessa pitää myös pysyä kartalla valvonnan piiriin kuuluvista palveluista ja niiden tarjoajista. Kaikkea ei edes voida valvoa samalla tarkkuudella, vaan jatkossa valvonnassa painottuvat entistä selkeämmin eniten käytetyt palvelut, Saari linjaa.





# TEOLLISUUSAUTOMAATIO HYÖKKÄYSTEN KOHTEENA

Hyökkääminen teollisuusautomaatioon on verrattain helppoa, sillä sen tietoturvassa on usein puutteita. Onnistuneilla iskuilla saattaa olla vakavia seurauksia kansalaisten arkeen.

**T**ietoturvahyökkäykset teollisuusautomaatiojärjestelmiä kohtaan ovat yleistyneet viime vuosina. Ajankohdainen esimerkki teollisuusautomaatiojärjestelmästä on älykäs sähköverkko, jonka yleistymisen laajentaa mahdollista hyökkäyspinta-alaa huomattavasti. Kotitalouksia varustetaan etäluettavin älymittarein, ja kaksisuuntaisessa jakeluverkossa kulkee sähköä lisäksi tietoa.

Älymittareita voi esimerkiksi manipuloida niin, että kulutetun sähkön määrä muuttuu. Seuraava aste on mittareiden haltuunotto ja käsittely niin, että niistä saa sähköä ilmaiseksi. Pihistettyä sähköä voisi älyverkossa jopa myydä eteenpäin.

– Vaarana on myös sähköverkon joutuminen epästabiiliin tilaan, millä voi olla laajakantoisia seurauksia. Jos verkossa liikuvan sähkön määrä yhtäkkiä merkittävästi muuttuu, verkko voi jopa kaatua. Viestintäviraston CERT-FI:n tietoturva-asiantuntija **Tommi Hasu** kertoo.

## Sähköjakelu seis?

Älykkään sähköverkon kriittinen lenkki on jakeluverkko, jossa kotitalouksien älymitarit kommunikoivat sähkölaitoksen kanssa. Jos jakeluverkko saadaan hallintaan, voidaan esimerkiksi päästä käsiksi laskutukseen tai irrottaa etälaitteet verkosta.

Kotitalouksien älymittareista ei toistaiseksi ole päästy murtautumaan ”alhaalta ylös”, eli mittareista jakeluverkkoon tai sähkölaitoksen hallintaverkkoon ja saatu niitä hallintaan. Menetelmien kehittyessä pääsy voi kuitenkin olla vain ajan kysymys.

Jakelu- ja hallintaverkkoihin voidaan kuitenkin päästä muita reittejä pitkin, esimerkiksi suunnittelu- ja toimistoverkon kautta. Haittaohjelmia on onnistuttu asentaa

maan hallintaverkkoihin jopa muistitikujen avulla. Hallintaverkkojen prosessiohjaimista pyritään keräämään konfiguraatiodietoja ja teknisiä asiakirjoja. Jakeluverkon prosessiohjaimiin tunkeutumalla voidaan keskeyttää koko sähköjakelu.

Toistaiseksi hyökkääjillä ei ole ollut teknistä osaamista pitääkseen verkkoja hallussaan pidempiä aikoja. Tämä onnistuu ennen pitkää, sillä teollisuusautomaatioprosessin ymmärtäminen ei yleensä ole vaikeaa. Hyökkääjä voi jopa arvaamalla paikallistaa prosessin heikot kohdat.

– Myös jakeluverkkojen langattomuus lisää riskejä. Esimerkiksi tuulivoimaturbiineita hallitaan nykyään langattomilla laitteilla. Ennen piti saada piuha irti, jos halusi sabotoida turbiinin toimintaa. Nykyään hallintaverkon voi saada haltuunsa yksinkertaisesti tunkeutumalla lähiverkkoon, Hasu huomauttaa.

Langattomuus merkitsee myös sitä, että madot ja muut haittaohjelmat leviävät verkossa salamannopeasti.

## Paljon potentiaalista tuhoa

Älykkään sähköverkon lisäksi kaasunjakelu ja suuret teollisuuslaitokset saattavat olla uhattuina. Jos esimerkiksi elintarviketehaan linjastoa ohjaavaan automaatiojärjestelmään saa syötettyä haittaohjelman, seurauksena voi olla ruokamyrkytysaalto. Täsmäiskut yhtä toimialaa tai yksittäistä yritystä kohtaan saattavat lisääntyä.

Hasu muistaa esimerkin kylmän sodan ajoilta, jolloin Yhdysvaltain tiedustelupalvelu tiesi Neuvostoliiton kopioivan kaasuputkilaitteistoja. Laitteistoon syötettiin tarkoituksella väärä ohjelmisto, jonka kopiointi johti tuhoisaan kaasuräjähdykseen Siperiasa 1980-luvulla.

– Todennäköinen vaarallisen räjähdysen aiheuttaja on tavallinen sähkö- tai kaasuverkko. Ydinvoimat pelottavat monia, mutta niissä on paljon muita turvamekanismeja.

Vaikka teollisuusautomaation uhkat ovat selvästi kasvaneet, niihin on reagoitu maltillisesti. Joissakin maissa sähkölaitokset ovat maksaneet mukisematta lunnaita, kun hyökkääjät ovat ilmoittaneet ottaneensa sähköverkon haltuun. Julkisuuteen on tullut lähinnä häiriköintityyppisiä tietomurtoja.

– Ulkomailla kiristysvaatimuksiin on suostuttu, ja tapauksista on tyypillisesti vaiettu. Tilanne on aivan toinen kuin tietoliikennealalla, jolla tietoa on perinteisesti jaettu avoimesti, Hasu sanoo.

## Teollisuusautomaation tietoturva laahaa jäljessä

Hasu vertaa teollisuusautomaatiohyökkäyksiä tietoliikenneverkoissa ilmenneisiin ilkeävaltatapauksiin 1990-luvulla. Nykyään tietoverkkorikollisuus on ammattimaista, ja teollisuusautomaatiohyökkäykset seuraavat perässä.

– Ammattirikollisuus lisääntyy iskuissa teollisuusautomaatiojärjestelmiin. Aika on otollinen, sillä rikollisten keinot ovat kehittyneet, mutta teollisuusautomaation tietoturva on suurin piirtein samalla tasolla kuin tietoverkkojen 90-luvulla.

Pääsy teollisuusautomaatioverkostoihin saattaa olla suorastaan helppoa, mutta pelkkä sisäänpääsy ei välttämättä vielä aiheuta tuhoa. Tämä on merkittävä ero verrattuna tietokoneurtoihin, jolloin pelkkä koneelle pääsy voi avata polun arvokkaisiin tietoihin.

Tuhoa aiheuttaakseen pitää päästä askel eteenpäin sille tietokoneelle, jolta löytyvät teollisuuslaitoksen kokonaiskonfiguraatio ja laitteiden ohjauksoodit. Vasta silloin saadaan selville järjestelmän komponentit ja laitteet. Tämän tiedon avulla murtoyritykset ja häirintätyökalut voidaan kohdistaa haluttuun kohteeseen.

## Eriyttäminen ja valvonta suojaavat

Teollisuusautomaatiohyökkäyksiltä voi suojautua tavallisin verkkosuojautumisen menetelmin. Ainakin hallintaverkko pitää

eriyttää avoimesta verkkoympäristöstä ja tietoliikennettä valvoa. Useimmiten verkkoarkkitehtuuri onkin kunnossa, mutta haasteena on teollisuusautomaatiolaitteiden ja -ohjelmistojen tietoturvan taso.

Toisinaan jopa liikenteen salaus on puutteellista. Jos hyökkääjä pääsee kiertämään tietoturvamekanismin ja lähestyy järjestelmää hallintaverkon puolelta, ei siinä vaiheessa usein enää kyseenalaisteta annettuja käskyjä. Yksinkertainen sisäänkirjautumisvaatimus olisi hyvä suojauskeino.

- Helpoin tapa aiheuttaa tuhoa on tunkeutua suoraan suunnittelutyöasemiin esimerkiksi kohdistetulla sähköpostihyökkäyksellä. Eristettyyn hallintaverkkoon ei tarvitse edes yrittää päästä sisään, Hasu selvittää.

Teollisuusautomaatiolaitteiden pitkä elinkaari aiheuttaa myös ongelmia. Uusien laitteiden ja menetelmien tietoturva on parempi, mutta monet laitteistot ovat yksinkertaisesti vanhoja. Vielä tällä hetkellä hyökkääjät ovat askeleen edellä.

- Voi mennä muutamia vuosia ennen kuin puolustusmekanismit saadaan nostettua hyökkääjien käyttämien menetelmien tasolle. Teollisuusautomaation laitevalmistajat ovat tässä työssä keskeisessä roolissa. Järjestelmiä pitää voida päivittää ja korjata ongelmien ilmetessä, Hasu painottaa.

#### **Yhteistyössä on voimaa**

CERT-FI ja muut toimijat ovat korostaneet, että teollisuusautomaatioon tarvitaan lisää tietoturvaosaamista ja alan tutkimusta. Yksi ongelma on, että teollisuusautomaatiota on paljon kriittisessä infrastruktuurissa, eli tiedot ovat ainakin jossain määrin salassa pidettäviä.

- Tilanne on kuitenkin nopeasti muuttumassa. Tietojen pimittäminen ei enää onnistu, vaikka järjestelmät liittyisivät kansalliseen turvallisuuteen. Viimeistään Stuxnet havahdutti huomaamaan, että vain tietoa avoimesti vaihtamalla pysytään hyökkääjien kintereillä, Hasu alleviivaa.

Suomessa tehdään jo merkittävää työtä automaatiojärjestelmiin kohdistuviin tietoturvauhkiin varautumisessa. Esimerkkinä mainittakoon energia-yhtiöiden ja CERT-FI:n vuoden 2009 alussa perustama tiedonvaihtoryhmä e-CIP, jonka tavoitteena on vaihtaa tietoa ajankohtaisista tietoturvauhkista sekä parhaista käytännöistä niiden torjumisessa.

Myös järjestelmätoimittajien ja järjestelmien tilaajien kanssa ollaan perustamassa vastaavaa ryhmää, jonka tarkoitus on käsitellä automaatiojärjestelmiin kohdistuvia tietoturvauhkia. ✘

**Yksinkertainen sisäänkirjautumisvaatimus olisi hyvä suojauskeino.**

## STUXNET MUUTTI MAAILMAN

Viime kesänä löydetty Stuxnet oli ensimmäinen selvästi teollisuusautomaatioon kohdistettu haittaohjelma. Monimutkaisen ja teknisesti äärimmäisen kehittyneen ohjelman kohteena olivat teollisuusautomaation prosessiohjaimet.

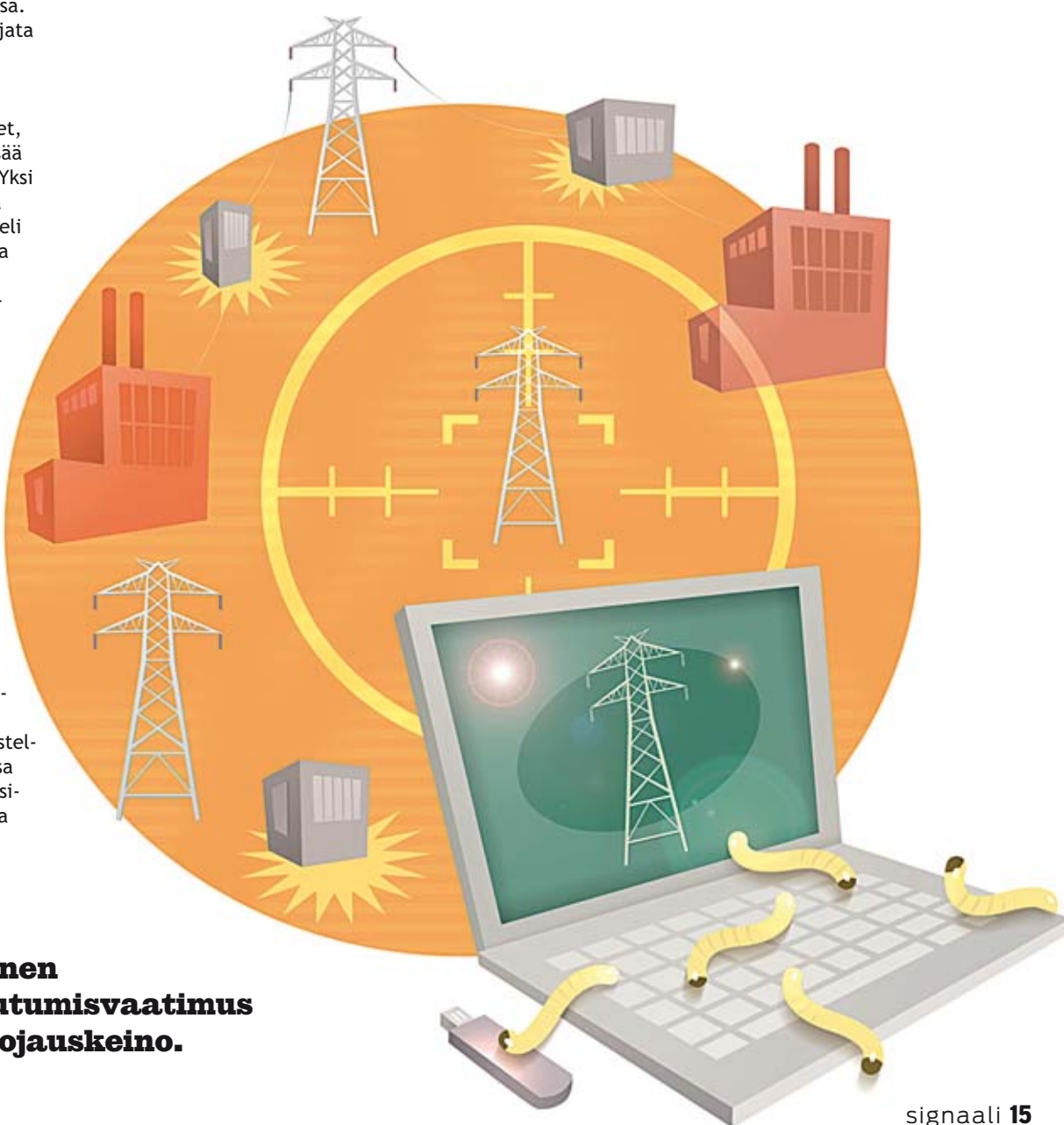
Tapausta tutkittaessa ilmeni, ettei ohjelman kohteena ollut tietty teollisuusautomaatiojärjestelmä, vaan yksittäinen laitos. Kohteen epäillään yleisesti olleen iranilainen ydinvoimala.

- Vielä ei tiedetä, kuka ohjelman takana on ja mikä oli sen kohde. Koodista tietoja tuskin saadaankaan irti, sen verran kehittyneet järjestelmät oli. Huolestuttavinta on, että Stuxnetin päämäärä oli selvästi jokin muu kuin rahanteko, Tomi Hasu sanoo.

Haittaohjelman rakenne viittaa siihen, että kyseessä on useista komponenteista koottu yleiskäyttöinen haittaohjelmatyökalu, jolloin ohjelmaa voidaan helposti muokata muihin tarkoituksiin ja kohteisiin. Ensimmäistä kertaa teollisuusautomaatioon kohdistuvassa haittaohjelmassa oli myös rootkit-ominaisuus, jolla ohjelma piilottaa itsensä.

Stuxnet-haittaohjelman käyttämät haavoittuvuudet on nyt korjattu, mutta sen nerokkaasta toimintaperiaatteesta ja teknisistä ominaisuuksista on jo otettu ja otetaan jatkossakin varmasti mallia.

Hasun mukaan viimeistään nyt on selvää, että teollisuusautomaatiojärjestelmiin pystytään tunkeutumaan ja saamaan aikaan vakavaa vahinkoa. Tapaus onkin nostanut teollisuusautomaation tietoturvayhteistyön aivan uudelle tasolle.





HOLLANNIN  
OPTA

# Telemarkkinat saatava pelaamaan KAIKKIEN PARHAAKSI

Hollannin OPTA edistää kilpailua ja kuluttajansuojaa. Teksti ja kuvat: Jussi Tuormaa, München

**L**uottamus ja reilu kilpailu ovat avain- sanoja hollantilaisen televiestinnän sääntelijän OPTA:n (Onafhankelijke Post en Telecommunicatie Autoriteit) toiminnan ymmärtämiseksi. Se haluaa palvella markkinoiden kaikkia osapuolia, niin yrityksiä kuin kuluttajia, ja toimia kaikkien parhaaksi.

– Kilpailunäkymät ovat hyvät, toteaa **Remko Bos**, OPTA:n markkinaosaston johtaja. Laajakaistamarkkinoilla entisen valtion-yhtiön, telejätti KPN:n, ovat haastaneet kaapeli-tv-yhtiöt. Useimmilla kotitalouksilla on kaksi laajakaistaista liittymää, niin kuparikaapeliliittymä (dsl) kuin kaapeli-tv-liittymä.

OPTA on tyytyväinen siihen, että se on onnistunut rohkaisemaan yrityksiä seuraavan sukupolven huippunopeiden viestintäverkkojen rakentamiseen. KPN on alkanut vetää optista kuitua (FTTH) koteihin yhdessä Reggiefieberin kanssa. Myös kilpailijoilta on saatu tukea.

– Olemme taanneet KPN:lle kannattavat sijoitukset kuituverkkoon jälleenmyyntitariffien pitkäaikaisella ennustettavuudella, joka ylittää normaalin kolmen vuoden sääntely-jaksomme. Verkon käyttö on samalla taattu myös kilpailijoille niiden siihen tekemiä sijoituksia vastaan, Remko Bos kertoo.

Toisaalta uuden kuituverkon liittymiä on vuodesta 2009 alkaen myyty vasta 440 000 kotitalouteen. OPTA:ssa ei olla kasvulukuihin tyytyväisiä, sillä Bosin mukaan KPN:n ja Reggiefieberin hanke on edistynyt odotettua hitaammin. Syynä on hänen mukaansa kaapeli-tv-yritysten vahva asema nopeiden nettiyhteyksien tarjonnassa. Nytemmin onkin mietitty, pitäisikö sääntelyä tehostaa myös kaapeli-tv-yritysten suuntaan.

## Tilaa kolmannellekin toimijalle

Sääntelyviranomaiset eivät voi puuttua suoraan yritysten toimintaan, elleivät ne ole toimineet pelisääntöjen vastaisesti. Sen sijaan viranomaiset pyrkivät kehittämään

markkinoiden rakenteita, ja luomaan parempia edellytyksiä kilpailulle – laajakaistamarkkinoilla olisi Bosin mukaan tilaa jopa uudelle, kolmannelle merkittävälle markkinatoimijalle KPN:n ja kaapeli-tv-yritysten rinnalla. Kun teleyritys, ja varsinkin yritys, jolla on niin sanottu huomattava markkina-voima (HMV), kärkeä pelisääntöjen rikkomisesta, OPTA voi rangaista sitä hyvinkin ankarasti – kuten KPN:ää sen yritysasiakkailleen myöntämistä alennuksista vuosina 2004–2005. Se sai 17 miljoonan euron sakot ja joutui lisäksi maksamaan 18 miljoonan euron korvaukset kilpailijoilleen.

OPTA analysoi jatkuvasti telemarkkinoita ja niiden ajankohtaisia ongelmia. Se pyrkii poistamaan kilpailun esteitä, sovittamaan yritysten välisiä riitoja, tutkimaan kuluttajien valituksia sekä takaamaan kuluttajille enemmän valinnanvaraa ja kohtuulliset hinnat. OPTA myös pyytää asianosaiset aina mukaan ratkaisemaan ongelmia ja ottamaan kantaa uusiin sääntelytoimenpide-esityksiin.

Remko Bos

Danyel Molenaar

Rutger Fortuin



## **OPTA on onnistunut rohkaisemaan yrityksiä seuraavan sukupolven huippunopeiden viestintäverkkojen rakentamiseen.**

Sääntelyviranomaisen korostaa kunkin osapuolen vastuuta pelisääntöjen tuntemuksessa ja noudattamisessa. Samalla se itse tuntee erityistä vastuuta ajaa aktiivisesti kuluttajansuojaa – ja vaatii myös teleyrityksiltä sen kunnioittamista (duty of care).

– OPTA:n päätehtäviä kuluttajansuojasioissa on toimia roskapostin ja haittaohjelmien leviämistä vastaan, kertoo **Danyel Molenaar**, kuluttaja- ja nettiturvallisuusosaston varajohtaja. Toimintaa tehostamaan on perustettu myös oma nettisivusto, spamklacht.nl, jonka kautta surffaajat voivat auttaa viranomaisia jäljittämään roskapostihäiritsejä. Lisäksi OPTA pystytti vuonna 2007 yhdessä kilpailu- ja kuluttajavirastojen kanssa kuluttajille tarkoitetun neuvonta- ja tiedotussivuston [www.consuwijzer.nl](http://www.consuwijzer.nl). Sivusto on ollut suuri menestys, mutta samalla myös vaativa haaste. Sivuston jo yli kahdesta miljoonasta vierailusta valtaosa koskee energiamarkkinoita, mutta merkittävä osa myös telemarkkinoita.

Suosion myötä OPTA:n kuluttajaneuvonnassa panee nyt yhden henkilön sijaan jo viisi päätoimista työntekijää parastaan.

– Me todella yritämme auttaa netin käyttäjiä, Molenaar sanoo.

### **Rajansa paikallisille poikkeuksille**

OPTA:aa tulevat työllistämään kotimarkkinoiden lisäksi myös kansainväliset markkinat ja EU-lainsäädännön toimeenpano Hollannissa. Remko Bos osoittaa ymmärrystä paikallisille ratkaisuille, ja toivookin EU-maiden telesääntelyviranomaisten miettivän yhteiselimessään BEREK:ssä, milloin ja missä harmonisointi on paikallaan ja missä taas ei.

Paikallisten olosuhteiden tai poikkeusten korostamisessa ei Bosin mielestä saa kuitenkaan mennä liian pitkälle.

– Kun telemarkkinoiden sääntelyn pääperiaatteista on sovittu, niiden on pädetävä niin paikassa A kuin paikassa B. ✘



## **Hollannin suvereenit sääntelijät**

**Hollannissa** televiestinnän markkinat ovat kehittyneet pitkälle ja ne toimivat hyvin.

Markkinoita sääntelee Den Haagissa sijaitseva, vuonna 1997 perustettu OPTA – Onafhankelijk Post en Telecommunicatie Autoriteit ([www.opta.nl](http://www.opta.nl)). Se kustantaa toimintansa 90-prosenttisesti yrityksiltä viestintämarkkinoiden sääntelystä perittävillä maksuilla.

Kun OPTA sääntelee televiestinnän markkinoita, niin toinen riippumaton sääntelyviranomaisen, Hilversumissa sijaitseva ja vuonna 1988 perustettu CvdM – Commissariaat voor de Media ([www.cvdM.nl](http://www.cvdM.nl)) valvoo mediamarkkinoita ja mediassa julkaistavia sisältöjä. Kommissariaatin toiminnan rahoittaa suurimmalta osin opetus- ja kulttuuriministeriö, mediateollisuuden osuus jää 20–25 prosenttiin.

OPTAssa on noin 130 työntekijää, joista valtaosa työskentelee kahdella pääalueella, viestintämarkkinoiden analysoimisessa ja kilpailun edistämässä sekä kuluttajasuojatehtävissä. Toisin kuin meillä, radiotaajuuksien sääntelystä vastaa Hollannissa talousministeriö (Ministerie van Economische Zaken). CvdM:llä taas on 57 työntekijää. Molempien silmäteränä on kilpailun toimivuus.

OPTAn mukaan telemarkkinoiden toimivudelle on jo riski, kun niin sanotulla huomattavan markkinavoiman omaavalla teleyrityksellä on yli 25 prosentin markkinaosuus. Hollannissa entisen valtion teleyrityksen KPN:n tällaista mahtiasemaa ovat mobiilimarkkinoilla tasapainottaneet ulkomaiset kilpailijat (T-Mobile ja Vodafone) ja laajakaistamarkkinoilla kaapeli-tv-yritykset.

Mediamarkkinoilla, lehdistössä ja televisiossa, vallitsee vähintään kolmen suuren yrityksen jako, mutta kaapeli-tv:ssä toimii valtakunnallisesti vain kaksi yritystä. Niitä kuitenkin täydentää joukko alueellisia yrityksiä.

CvdM korostaa kuluttaja-asioissa, kuten lastensuojelussa, media-alan itsesääntelyä. Se antaa alan oman organisaation Nicamin (Nederlands Instituut voor de Classificatie van Audiovisuele Media) itse valvoa tuotteidensa sisällön sopivuutta eri ikäryhmille. Kuluttaja voi hakea tietoa Nicamin tarkistamista tuotteista Kijkwijzer-nettisivustolta.

Teknisen kehityksen vauhdissa on vaikea pysytellä mukana, myöntää **Rutger Fortuin**, joka CvdM:ssa vastaa EU:n AVMS- eli audiovisuaalisia mediapalveluja koskevan direktiivin kansallisesta toimeenpanohankkeesta. Kun netissä syntyy televisionomaista ohjelmatoimintaa, sen toteutuksessa on hänen mukaansa noudatettava tunnettuja journalistisia periaatteita.

– Koko nettiä ei voi kontrolloida, sanoo puolestaan **Marcel Betzel**, CvdM:n strateginen neuvonantaja.

– Mutta verkossa toimiviin uusiin mediayrityksiin – kuten YouTubeen tai tulossa olevaan Google-TV:hen – voidaan soveltaa voimassaolevia sääntelyperiaatteita. Betzelin mukaan toinen vaihtoehto olisi alkaa säännellä koko mediaa uusin kriteerein.

Marcel Betzel



# TODISTETUSTI

Uutisissa kerrotaan lähes päivittäin uudesta tietokoneviruksesta tai tietomurtojen aiheuttamista vahingoista. Viestintävirastolle myönnettiin lokakuussa ISO 27001 -sertifikaatti, joka osoittaa sen tietoturvan hallintajärjestelmän olevan kunnossa.

**Teksti:** Maarit Seeling **Kuvat:** Jyrki Komulainen

**V**iestintäviraston turvallisuuspäällikkö **Jani Arnell** iloitsee myönnetystä sertifikaatista. Takana on parin vuoden tiukka rutistus, jonka aikana Itämerenkadun toimipisteen tietoturvarutiinit rukattiin askel askeleelta täyttämään tiukan sertifikaatin vaatimukset.

Poikkeukselliseksi saavutuksen tekee se, että sertifikaatti kattaa koko viraston organisaation ja kaikki sen toiminnot. Ylipäänsä vain noin 20 toimijalle Suomessa on myönnetty oikeus ISO 27001 -sertifikaattiin.

– Meille oli tärkeää osoittaa sidosryhmillemme, että virastossamme toteutettava tietoturva on laadukasta ja että pyrimme jatkuvasti kehittämään sitä. Kansallisena tietoturvaviranomaisena haluamme todistaa toimivamme edustamiemme arvojen mukaisesti. Sertifioitua, kansainväliset vaatimukset täyttävää järjestelmää voi pitää eräänlaisena käyntikorttina ulospäin, Arnell määrittää.

ISO 27001 -sertifikaatin myönsi Inspecta Sertifiointi Oy, jonka tuotepäällikkö **Jyrki Lahnahti** kertoo, että tietoturvallisuuden hallintajärjestelmäsertifikaatteja myönnettäessä kiinnitetään erityistä huomiota organisaation riskienhallintakykyyn ja dokumentaation hallintaan. Lisäksi organisaation on osoitettava halunsa järjestelmälliseen tietoturvallisuuden parantamiseen.

– Sitoutuminen tietoturvallisuuden jatkuvaan parantamiseen näkyy muun muassa siinä, miten tähän toimintaan annetaan resursseja. Arvioinneissa ei tarkastella vain dokumentteja vaan itse tekemistä, johta-

mista ja sitä, miten ne käytännössä toimivat, Lahnahti toteaa.

## Tietoturvavaateet kiristymässä

Kiinnostus tietoturva-asoiden hallinnan osoittamiseen sertifikaatilla on viime aikoina selvästi lisääntynyt. Jyrki Lahnahti kertoo, että viimeisen puolentoista vuoden aikana Inspecta on tehnyt sertifiointiin liittyviä arviointeja enemmän kuin usean sitä edeltäneen vuoden kuluessa yhteensä.

Yhdeksi syyksi organisaatioiden kiinnostuksen viriämiseen hän mainitsee heinäkuun alussa annetun asetuksen valtionhallinnon tietoturvavaatimuksista.

– Peli on nyt myös selvästi kovenemassa. Tiedon määrä kasvaa ja sitä siirretään yhä useammin juuri digitaalisesti. Tietoturvaohjelmat ja -loukkaukset lisääntyvät samassa tahdissa. On herätty huomaamaan, että asialle on pakko tehdä jotain, Lahnahti pohtii.

ISO 27001 -sertifikaatin vaatimusten täyttämiseksi Viestintävirastossa muun muassa luotiin erilaisia malleja tietoturva-asiakirjojen, tallenteiden ja muiden prosessien hallinnalle. Organisaatiota ja vastuita selkeytettiin ja ne vietiin osaksi työjärjestystä. Lisäksi tietoturva liitettiin osaksi tulosaikajäsenä ja se kytkettiin myös toiminta- ja taloussuunnitelmaan sekä riskienhallintaan.

– Toimenpiteet lisäävät tietoturva-asoiden merkittävyyttä ja tehostavat sen valvontaa. Uudistusten jalkauttaminen edellyttää ehdottomasti myös henkilöstön jatkuvaa kouluttamista, Arnell kertoo.

Sertifikaatin saaminen oli vain välietappi.

*Inspecta Sertifiointin Jyrki Lahnahti muistuttaa, että arvioinnissa tarkastellaan tekemistä ja johtamista – ja sitä, miten ne käytännössä toimivat.*



**Vain noin 20 toimijalle Suomessa on myönnetty oikeus ISO 27001 -sertifikaattiin.**

# TURVALLINEN

– Meidän on osoitettava, että toimimme sertifikatin mukaisesti ja että parannamme ja kehitämme tietoturvaamme edelleen. Mistään kertaluonteisesta rupeamasta ei siis ollut kysymys. Standardin mukaisen tietoturvatason ylläpitäminen vaatii jatkuvaa työtä, Arnell sanoo.

Sertifiikaatin voimassaoloa ja standardin vaatimusten täyttymistä valvotaan vuosittaisilla seuranta-arvioinneilla, jotka perustuvat dokumenttien tarkistamiseen ja henkilöstön haastatteluihin. Viestintäviraston kokoisessa organisaatiossa seurannat vievät kahdelta arvioijalta 2–3 työpäivää.

– Luovuttaessamme ISO 27001 -sertifiikaattia Viestintäviraston pääjohtajan sijainen **Jorma Koivunmaa** totesi arviointiviikon olleen varsinainen piinaviikko. Me totesimme, että näitä piinaviikkoja on luvassa myös jatkossa. Tämä on pysyvä kumppanuussuhde, Lahnelahti naurahtaa. ✘

## Isosti laadukasta

ISO 27001 on kansainvälinen standardi, joka määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset, riskien arvioinnin ja ehkäisevien toimenpiteiden toteutumisen.

Tiukalla seulalla pyritään pitämään tietovarojen säilyminen luottamuksellisenä, virheettömänä ja tarvitsijoiden saatavilla. Suojaa tarvitsevaa omaisuutta ovat esimerkiksi digitaalinen tieto, paperiasiakirjat, tietokoneet sekä tiimien ja yksittäisten työntekijöiden tietotaito.

*Viestintäviraston turvallisuuspäällikkö Jani Arnell iloitsee siitä, että sertifiikaatti kattaa kaikki Viestintäviraston toiminnot.*

ISO 27001

# PSEUDOLIITIT TARKENTAVAT SATELLIITTIPAIKANNUSTA

Satelliittipaikannus tarkentuu, kun avuksi otetaan satelliittien tapaan toimivat maanpäälliset pseudoliitit. Läpimurron uskotaan tapahtuvan muutaman vuoden kuluessa. Teksti: Marjo Rautvuori

**Satelliittipaikannus** tapahtuu yli 20 000 kilometrin korkeudesta satelliittien vastaanottimeen tiettyä koodia lähettävien tietojen perusteella. Tarkkuus on noin kymmenen metriä. On kuitenkin paljon paikkoja, joihin satelliittien tasainen signaali ei näy eikä kuulu. Sellaisia ovat esimerkiksi tunnelit, syvät kuilut, korkeiden talojen reunustamat kadut, kaivokset, isot terminaalit tai muut laajat sisätilat.

Pseudoliitit eli pseudosatelliitit ovat satelliittipaikannuksen apuvälineitä, jotka tuovat tarkkuutta paikannukseen ja toimivat myös hankalissa olosuhteissa ja tiloissa. Tekniikka jäljittelee GPS-satelliitteja maan päällä ja toimii läheltä hyvin pienellä teholla. Saavutettava paikannustarkkuus on senttimetriluokkaa.

– Pseudoliitit eivät ole mikään uusi asia. Niistä puhuttiin jo 1900-luvun viimeisinä vuosikymmeninä. Nyt asian suhteen on kuitenkin aktivoitunut kansainvälisesti, kertoo radioverkkoasiantuntija **Kalle Pikkarainen** Viestintävirastosta.

Parhaillaan päivitetään Euroopan elektronisen kommunikaatiokomitean (ECC) raporttia. Regulointiryhmä valmistelee ehtoja. Niissä määritellään muun muassa laitteiden tehorojoja häiriöiden hallitsemiseksi. Sen jälkeen Euroopan standardointijärjestö (ETSI) määrittelee laitevalmistajille tarvittavat standardit.

Kun näihin asioihin saadaan selkeät määrittelyt, Pikkarainen arvelee pseudoliittien läpimurron tapahtuvan todennäköisesti jo muutaman vuoden kuluessa. Toiminnan hän uskoo säilyvän radioluvanvaraisena.

## Häirintä estettävä

Kiinnostus pseudoliittien hyödyntämiseen on suuri. Suomessa Space Systems Finland Oy on tehnyt useita testejä, yksin ja yhdessä Geodeettisen laitoksen sekä mahdollisten tulevien käyttäjien, kuten Helsingin sataman, kanssa.

Kriittisiä pseudoliitteihin liittyviä kohtia Pikkarainen nimeää viisi: asennus, säteilyteho, pseudoliitin käyttämä koodi, taajuus ja paikkatiedon väärentäminen.

– Asennuksessa pitää huomioida, etteivät laitteet sotke satelliittipaikannusta eivätkä toisaalta ole liian lähellä vastaanotinta, koska tällöin ne voivat tukkia sen.

Pseudoliittien lähetysteho on pieni, sisätiloissa milliwatin miljoonasosa ja ulkoikäytössä milliwatti. Sisäkäyttöön rakennetaan paikannusta varten vähintään neljän pseudoliitin verkosto. Ulkokäytössä voidaan yhdistää satelliittien ja yhden tai useamman pseudoliitin käyttö. Tällöin häirintä voidaan minimoida teknisesti käyttämällä pseudoliitin signaalilähetyksessä pulssilähetystä.

Satelliittikoodistossa on oma osa, PRN 1–32, satelliiteille ja pseudoliiteille, jotka käyttävät koodistoa 32:sta ylöspäin. Taajuuksissa GPS ja pseudoliitit käyttävät samaa nykyisen GPS:n taajuutta. Näin vastaanottimena voidaan käyttää samaa laitetta, jonka ohjelmistoon tarvitaan vain pieni muutos. Muut paikannukset, kuten Bluetooth vaatisivat vastaanottimeen isot muutostyöt.

## Lukuisia käyttökohteita

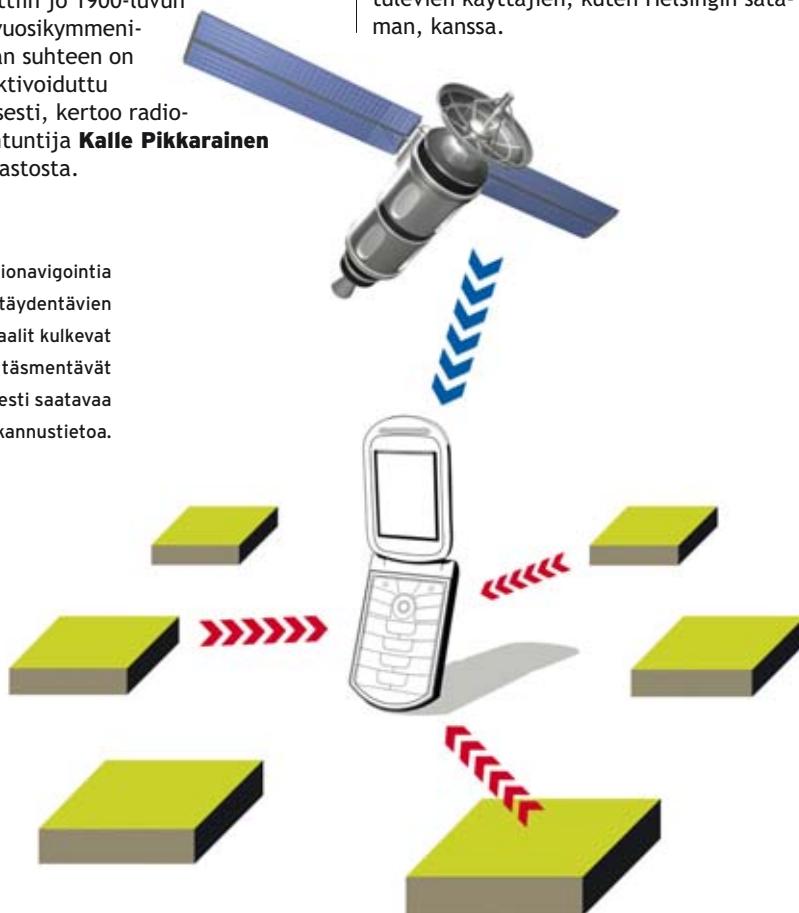
Satelliittipaikannuksen täsmennystarvetta on monilla toiminta-alueilla. Pikkarainen uskoo, että jos hinta ei jarruta pseudoliittien markkinoille tuloa, ne leviävät nopeasti.

– Ammattikäyttöön, kuten tavaroiden siirtoon, lentokentille ja messukeskuksiin pseudoliittien tuomalle paikannustarkennukselle löytyy varmasti kysyntää. Esimerkiksi Pariisin Charles de Gaullen lentokentälle on jo olemassa asennussuunnitelmat. Kattorakenteisiin sijoitettavia pseudoliitteja on siinä tiiviinä nauhana.

Myös viranomaiskäyttöön, kuten poliisille ja palokunnalle, on Pikkaraisen mielestä helppo löytää käyttömahdollisuuksia.

– Esimerkiksi savuisissa palokohteissa, joissa ihminen ei voi työskennellä, voidaan pseudoliittien ansiosta ohjata robotin työtä. Lentokenttien lähestymislentojen ohjaukseen pseudoliitit voivat taas antaa tarpeellista lisätietoa, asiantuntija havainnollistaa. ✘

Satelliitin radionavigointia lähietäisyydeltä täydentävien pseudonaattien signaalit kulkevat samaan vastaanottimeen ja täsmentävät näin oleellisesti saatavaa paikannustietoa.



## Oman elämänsä kustantajat

**” Tunnustan.** Olen ammatti- ja tapajournalisti. Tähänastisen aikuisen työelämäni olen saanut tehdä työtä mediassa. Olen kiinnostunut viestinnästä ja vuorovaikutuksesta tavalla, joka ei ole itsesuojeluvaistoni kannalta ollut aina järkevää. Media kun on jokaisen suomalaisen arvosteltavissa ja haukuttavissa, sillä jokainen suomalainen luulee olevansa viestinnän ammattilainen – kuten saunomisessa ja viinanjuonnissakin Niin kuin onkin.

Ulkomaantoimittajana Sarajevossa, jo kauan ennen Facebookia ja koko internetiä, kansalaisjournalismi oli meistä luotiliiveillä ja pitkillä lounailla pönäköityneistä journalisteista pelkkä vitsi. Tapana oli ehdottaa samassa keskustelussa puhujalle myös kansalaishammaslääkäreitä ja kansalaissähkömiestä.

Mihin sitä ammattilaista.

Tätä kirjoittaessa kaikki on toisin. Digitaalinen ja sosiaalinen vallankumous on tehnyt jokaisesta kansalaisesta toimittajan ja vanha viestinnän mallimme sisällöstä harvoilta monille on kääntynyt pääläelleen. Viestiksi monelta harvoille. Facebookissa on jo 500 miljoonaa käyttäjää, YouTubessa 250 miljoonaa videota. Seitsemän vuotta sitten kumpaakaan ei ollut olemassa.

Koskaan ennen emme ole tuottaneet sisältöä niin sankoin joukoin niin harvalle oikeasti kiinnostuneelle.

Minusta se on merkittävää ja demokratiaa lisäävää dialogia. Kun jokainen meistä voi nyt aloittaa oman elämänsä kustantajana, niin pyynnöstä nostan esille kolme näkökulmaa.

Ensinnäkin vapaan dialogin vastuullisuus voi tulla aloittavalle blogiajalle kalliiksi. Kuten aloittavalle kansalaissähkömiehelle ensimmäinen virhekytkentä. Mediassa tätä on harjoiteltu satoja vuosia. Sananvapaus ja yksityisyydensuoja muodostavat janan, jolla uutiskohteen sijainti on jokaista juttua julkaistaessa aina harkittava erikseen. Päätäjillä ja julkisuuden henkilöillä julkaisukynys on alempi. Naapurisi nauttii suurempaa yksityisyydensuojaa kuin **Matti Vanhanen**. Mediassa vastuun kantaa lopulta päätömittaja, joka viime kädessä valitsee mitkä jutut ja kuvat julkaistaan.

Vaikka journalistin tehtävä onkin viihdyttää, välittää tietoa ja toimia kriitikkona, tulee joka jutun olla totta. Jopa hienompien ihmisten parhaissa, maan suosituimmissa ja luetuimmissa lehdissä, keltaisessa lehdistössä, kaiken tulee olla todistettavasti totta.

Verkkokeskustelussa vastuun kantaa kirjoittaja itse. Kunnianloukkauksesta saa rangaistuksen. Oikeusjärjestelmämme suojelee kansalaista väärältä väitteeltä, panettelulta ja kiusaamiselta.

Kannatan jälkimoderointia ennakkosen suurin sijaan, sillä uskon suomalaisten oppivan ja vastuullisten verkkoyhteisöjen myös neuvovan, mitä toisesta saa sanoa ja mitä ei. Jos ei sitä elämä ole vielä opettanut.

Toiseksi verkossa sana on teko. Digitaalinen jalanjälkemme kaiku seuraaville sukupolville. Ja sitä seuraaville. Viaton Facebook-päivitys pannaan aikakapseliin ja luetaan uudestaan kymmenen vuotta

myöhemmin. Wikileaks on opettanut, että jopa Yhdysvaltain ulkoministeriön salaisimmat viestit voi yksi sotamies varastaa ja julkaista.

Mitä jos Googlella, Facebookissa tai pankissasi joku saisi saman idean?

Kolmanneksi. Julkisuutta ei kannata niin suuresti himoita, mitä tuoreimmatkin trendimittarit nyt näyttävät nuorten tekevän. Entinen BB-tähti ei julkisuudellaan ansaitse latin latia ja vain yksi ihmiskokeeseen alistettu sai siitä kunnan palkkion ylipäätään. Avatessaan pandoran lippaansa sitä on vaikea panna enää kiinni. Kannattaako kaikkein tärkeimmät asiansa jakaa tuntemattomille?

Omaa julkisuuttaan ei todellisuudessa voi hallita, vaikka konsultit niin väittävät. Julkkiksen harha median hallinnasta johtuu siitä, että julkisuuskaarensa huipulla pääsee hetkeksi valitsemaan mille medialle ja missä sävyssä haastattelunsa antaisi. Se menee ohi.



**Jokainen suomalainen luulee olevansa viestinnän ammattilainen.**



## Bevisligen säker

**I oktober beviljades kommunikationsverket certifikatet ISO 27001 som bevisar att Kommunikationsverkets hanteringssystem för informationssäkerheten är i skick.**

**Kommunikationsverkets** säkerhetschef **Jani Arnell** är nöjd över det beviljade certifikatet. Det är resultatet av ett några år långt hårt arbete där informationssäkerhetsrutinerna på kontoret vid Östersjögatan sågs över för att uppfylla certifikatets stränga krav. Endast cirka 20 aktörer i Finland har rätt att använda certifikatet.

ISO 27001-certifikatet beviljades av Inspecta Sertifiointi Oy. **Jyrki Lahnalhti**, som är produktchef på Inspecta Sertifiointi, berättar att man vid beviljandet av certifikatet fäster särskild uppmärksamhet vid organisationens riskhanteringsförmåga och dokumentationshantering. Dessutom ska organisationen påvisa sin vilja att systematiskt förbättra informationssäkerheten.

– Engagemanget för en fortlöpande förbättring av informationssäkerheten syns också i resurserna. Vid revisionerna granskar man inte bara dokument utan själva rutinerna, ledningen och hur de fungerar i praktiken, säger Lahnalhti.

Beviljandet av certifikatet var en mellanlapp. – Vi måste visa att vi agerar enligt certifikatet och att vi förbättrar och vidareutvecklar vår informationssäkerhet, säger Arnell. Certifikatets giltighet och uppfyllandet av kraven i standarden övervakas genom årliga uppföljande revisioner.

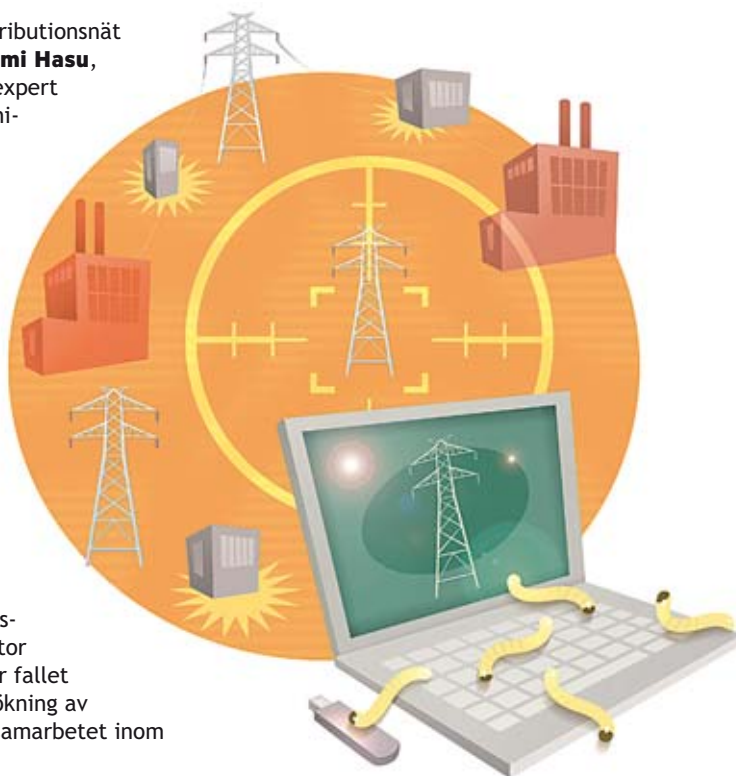
## Industriautomation mål för attacker

**Det är relativt enkelt att attackera industriautomation, eftersom det ofta finns brister i dessa systems informationssäkerhet. Fallet Stuxnet i somras ledde till en ökning av samarbetet för informationssäkerhet inom industriautomation.**

**Angreppen** mot industriella automationssystem har ökat under de senaste åren. Ett exempel är smarta elnät: i hushåll installeras smarta elmätare som kan avläsas på distans, och det dubbelriktade distributionsnätet förmedlar inte bara el utan också information. Den kritiska länken är distributionsnätet via vilket de smarta mätarna i hushållen kommunicerar med elverket. Om man lyckas kapa distributionsnätet kan man till exempel komma åt faktureringen eller koppla loss utrustningen för distansavläsning.

– Även trådlösa distributionsnät ökar riskerna, säger **Tomi Hasu**, informationssäkerhetsexpert på CERT-FI vid Kommunikationsverket. Trådlösheten innebär att maskar och andra virusprogram blixtnsamt kan sprida sig över nätet.

Stuxnet, som upptäcktes i somras, var det första virusprogrammet som helt tydligt var riktat mot industriautomation. Enligt Hasu är det senast nu klart att det går att tränga sig in i industriautomationsystem och förorsaka stor skada i dem. Därför har fallet lett till en betydande ökning av informationssäkerhetssamarbetet inom industriautomation.



## Produktplacering sker inte slumpmässigt

**Köksutrustningens märken har inte valts slumpmässigt i ett matprogram. De har medvetet placerats i programmet.**

**I maj 2010** infördes nya, klara spelregler för produktplacering. Den nya lagen gäller också tv-program och filmer samt beställ-tv som distribueras över internet. Kommunikationsverket och konsumentombudsmannen ansvarar för tillsynen.

– Produktplacering har inte heller tidigare varit förbjudet, och tillsynen fokuserar på samma område som tidigare, det vill säga att ingripa i otillåten smyg reklam, säger **Merja Saari**, biträdande direktör för övervakning av kommunikationstjänster vid Kommunikationsverket.

Produktplacering har blivit vanligare, och verksamhetsfältet förändras hela tiden. – Tittarundersökningarna visar att tittarna har accepterat produktplaceringen, enligt annonsörerna fungerar den bra och produktionsbolagen förhåller sig positivt

till den, säger **Petra Wikström-Van Eemeren**, biträdande chef för MTV Medias kommunikationspolitik. Vad gäller tillsynen av produktplaceringen tror den kommersiella tv-kanalen mer på mediefostran än sträng reglering.



**Den nya lagen gäller också tv-program och filmer samt beställ-tv som distribueras över internet.**

## Product placement is no coincidence

**The kitchen equipment brands we see on TV cookery shows are not accidental. The shows use product placement.**

**In May 2010**, new, clear ground rules were created for product placement. The new law also applies to TV shows, movies and video-on-demand services distributed via the Internet. Supervision of the law continues to be the responsibility of FICORA and the Consumer Ombudsman.

“Product placement as such has never been prohibited. Supervision will continue to focus on subliminal advertising, which is banned”, explains **Merja Saari**, Deputy Director responsible for FICORA’s Communications Services Supervision.

Product placement has increased, and continues to evolve. “Viewer research has indicated that viewers accept product placement, advertisers think it is effective, and production companies see it as positive”, says **Petra Wikström-Van Eemeren**, Vice President of Media Policy at MTV Media. The commercial TV channel would rather see product placement supervision carried out through media education than by strict regulation.



**The new law applies to TV shows, movies and video-on-demand services distributed via the Internet.**

## Industrial automation under attack

**Attacks on industrial automation are relatively easy, as information security is often inadequate. Last summer, the Stuxnet incident led to improvements in information security for industrial automation.**

**In the past** few years, security attacks against automated industrial systems have become increasingly common. Intelligent electricity grids are one good example: households are equipped with remotely readable intelligent meters, so that in addition to electricity, information is passed through the bidirectional distribution network. The distribution network is the critical link where households’ intelligent meters communicate with the power company. If the distribution network is taken over, it is possible to access invoicing information or disconnect remote equipment from the network.

“Wireless distribution networks add to the risks”, says **Tomi Hasu**, Information Security Adviser to FICORA’s CERT-FI unit. Wireless implementation also allows worms and other malware to spread through the network extremely fast.

Stuxnet, discovered last summer, was the first malware program clearly targeted at industrial automation. According to Hasu, it should be clear that industrial automation systems can be accessed with serious and harmful consequences. The Stuxnet incident did, in fact, help to increase co-operation on information security for industrial automation significantly.

## Proven safe

**In October, the Finnish Communications Regulatory Authority (FICORA) was awarded the ISO 27001 certificate, certifying compliance by its information security management system.**

**FICORA’s** Chief Security Officer **Jani Arnell** is delighted with the award of the certificate. The past couple of years have seen intense effort, as the information security procedures of its Itämerenkatu offices were fine-tuned to comply with the extremely strict requirements of the standard. In Finland, only around 20 organisations have been awarded the certificate.

The ISO 27001 certificate was awarded by Inspecta Certification. According to **Jyrki Lahnelahti**, Product Manager at Inspecta, the certification process pays particular attention to an organisation’s risk management capability and documentation management systems. Furthermore, the organisation must demonstrate a strong intention to improve information security systematically.

“Commitment to the continuous improvement of information security was also evident in resourcing. Audits do cover not only documentation, but also the way things are done, managed and dealt with in practice”, says Lahnelahti.

Being awarded the certificate is only one step on the journey. “We must demonstrate that our operations are in line with the certificate’s requirements, and that we continue to improve and develop our information security”, says Arnell. The validity of the certificate, as well as compliance with its requirements, is monitored through annual follow-up assessments.





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