

Turvalliset ja luotettavat palvelut viihdepalvelu- ja peliyritysten elinehto

LUOTI-artikkeli 1/2006

Kimmo Lehtosalo, Elias Pöyry

Suomalaiset pelitalot ovat nousseet viimeisten vuosien aikana otsikoihin. Pienet pelitalot kehittävät liiketoimintaa markkinoilla hakeakseen tarvittavaa kasvua. Monet ovat tässä jo onnistuneet. Toiset menestyneiden pelien seurauksena, toiset taas yritysostojen myötä. Tosin ostokohteena on pääsääntöisesti ollut suomalainen yritys. Menestys viihdepalvelu- ja peliteollisuudessa on monen tekijän summa. Ylivoimaisten tuotteiden lisäksi tarvitaan monia jatkuvuutta tukevia elementtejä. Yksi näistä tekijöistä on palvelun luotettavuus. Tuotteita ja palveluja kehittävät yritykset eivät näe suuria ongelmia luotettavien ja tietoturvallisten palvelujen kehittämisessä, mutta yritykset myöntävät, että turvallisuudella on liiketoiminnan jatkuvuuden kannalta aivan keskeinen rooli. Vakavampi tietoturvaloukkaus saattaa pahimmillaan karkoittaa käyttäjät ja siten vahingoittaa liiketoiminnan pyörittämistä. Viihdepalvelu- ja peliyrityksen uskottavuus ruokkii palvelujen käytön kasvua ja houkuttelee mukaansa oikeanlaisia kumppaneita.

LUOTI-ohjelma teki loppuvuoden 2005 aikana kohdennetun kierroksen suomalaisten tai Suomessa toimivien viihdepalvelu- ja peliyritysten keskuudessa. Ohjelman tekemän kierroksen tavoitteena oli hakea näkemyksiä alan yrityksiltä toimialan ja palvelujen kehittymisestä sekä ohjelman näkökulmasta erityisesti tietoturvallisuuden roolista palvelujen kehittämisessä ja käyttämisessä. Tämän kierroksen lisäksi perehdyttiin myös alan yleisiin trendeihin meillä ja maailmalla internet-hakujen ja tutkimusraporttien avulla.

Tämä artikkeli sisältää koosteen vuoden 2005 syksyn ja loppuvuoden tulema. Lisäksi tähän artikkeliin on kerätty joitain case-esimerkkejä meille tutuista suomalaisista toimijoista. Lisää tietoa tietoturvan merkityksestä ja haasteista viihdepalvelujen piirissä tuotetaan LUOTI-ohjelman pilottihankkeiden kautta. Ohjelma käynnisti vuoden 2005 lopulla kolme pilottihanketta. Ohjelman piiriin valitut monen toimijan väliset hankkeet saivat ohjelman kautta käyttöönsä tietoturva-asiantuntijan, jonka tehtävänä on tunnistaa palveluihin kohdistuvia riskejä sekä suunnitella keinoja näiden riskien ehkäisemiseksi ja välttämiseksi. LUOTI-pilottihankkeiden tulokset julkistetaan keväällä 2006. Vuoden 2006 pilottihankkeet käynnistetään alkuvuoden aikana.

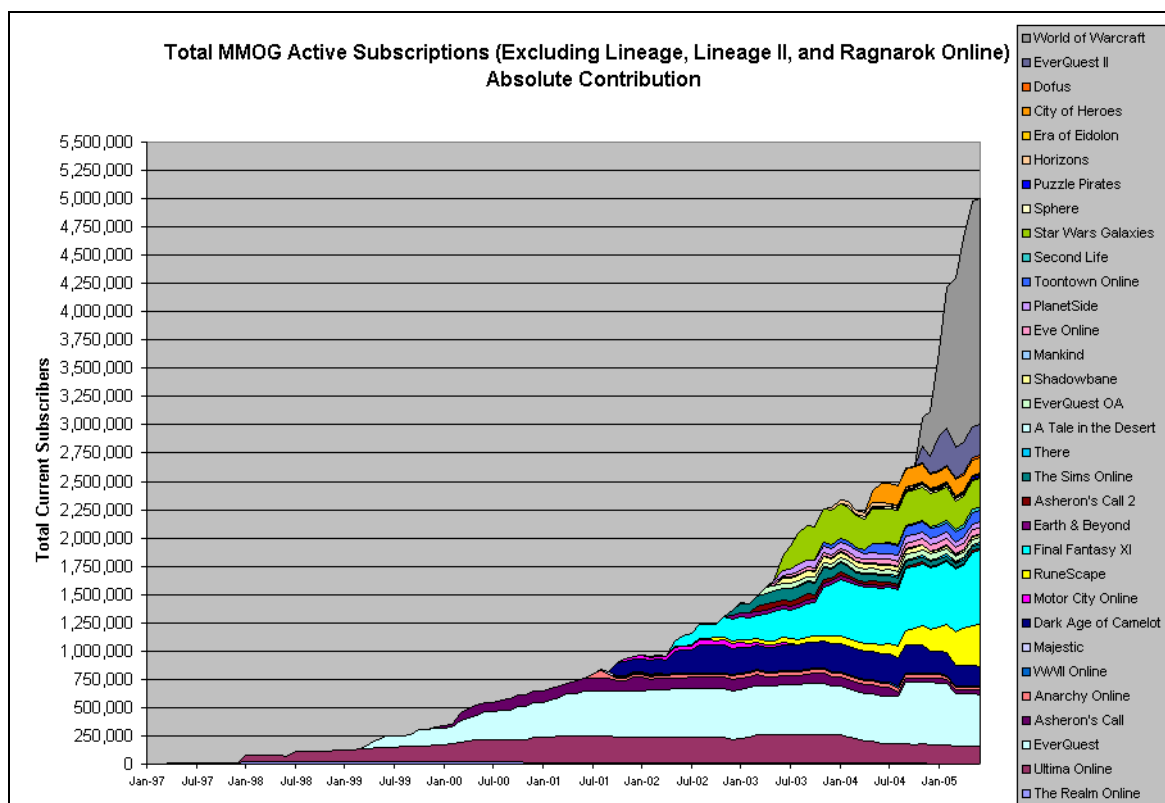
Online-pelien suosio on kovassa kasvussa

Peliteollisuutta katsellaan yleensä kokonaisuutena, joka käsittää konsoli-, tietokone- ja taskupelit sekä online-pelit. Online-pelit jakaantuvat edelleen internet-peleihin, (myös: internet game, online game, broadband game), iTV-peleihin ja mobiilipeleihin.

Online-pelit ovat rynnistäneet markkinoille vasta 2000-luvulla. Vuonna 2004 online-pelien markkinat olivat 3,8 miljardia dollaria ja luvun odotetaan viisinkertaistuvan vuoteen 2010 mennessä. Kiina on kasvamassa USA:n ohi maailman suurimpana online-pelimarkkinana.

Online-pelien suosion kasvun syynä on laajakaistaliittymien yleistyminen, ajanvietepelien (casual games) lisääntyminen ja monipelaajapelien (multiplayer games) suuri suosio sekä konsolipelien online-tuki.

Online-pelien lisäksi ajanvietettä tarjoavat erilaiset viihdepalvelut, joista on vielä toistaiseksi melko vähän tilastoja tarjolla. Alla oleva erityyppisten pelipalvelujen käyttäjä- tai tilaajamääriä kuvaava taulukko osoittaa, miten kovasta kasvusta peliteollisuudessa on kysymys.



MMOG-pelien käyttäjämäärä 1997–2005

Lähde: mmogchart.com



Interaktiivisilla TV-peleillä (iTV-pelit) tarkoitetaan digi-TV:n mahdollistamia vuorovaikutteisia pelejä, jotka on yleensä yhdistetty johonkin toiseen yhteysvälineeseen; peliä seurataan TV-ruudulta ja pelataan mm. matkapuhelimella.

Tasaisesta kasvusta huolimatta interaktiivisen television merkitys online-pelimarkkinoilla on vähäinen. Se tarvitsee rinnalleen muita yhteystapoja, jotta sillä voitaisiin laskuttaa.

Digi-TV on luonut Suomeen mahdollisuuden iTV:n hyödyntämiseen online-pelaamisessa. Toistaiseksi pelit ovat vielä kehittymättömiä ja yksinkertaisia. iTV:llä on kuitenkin mahdollisuudet kehittyä kohtuullisen kokoiseksi online-pelimarkkinaksi.

Mobiilipeleillä tarkoitetaan kaikkia sellaisia pelejä, joita pelataan mobiililaitteilla online-yhteydessä tai ne ladataan online-yhteyden kautta suoraan laitteeseen. Pääosa pelilaitteista on matkapuhelimia. Online-pelejä ovat mm. SMS-pelit, MMS-pelit, vedonlyönti- ja onnenpelit sekä Thin Client -pohjaiset, Symbian-käyttöjärjestelmälle tehdyt mobiilipelit.

Mobiilimarkkinoiden kypsyessä operaattorit pyrkivät panostamaan yhä enemmän maksullisiin lisäpalveluihin, joista pelit ovat merkittävässä asemassa. Perinteisistä operaattoreita lähellä olevista mobiiliviihdepalveluista meille ovat tuttuja lähinnä soittoäännet, logot ja taustakuvat.

Mobiilipelien alkutaival tyssäsi dot.com-kuplan puhkeamiseen joitakin vuosia sitten. Nyt mobiilipelimarkkinoilla on kuitenkin vilkasta ja uudet nopeutuvat yhteydet ja kehittyvät päätelaitestandardit mahdollistavat yhä monimutkaisempien online-pelien pelaamisen mobiilisti. Monet veikkaavatkin tämän valossa mobiilipeleille ruusuista tulevaisuutta.

Mobiilipelimarkkina on jo nyt suurin online-markkinoiden osa-alue. Sen ennustetaan kasvavan yli 11 miljardiin dollariin vuoteen 2010 mennessä. Mobiilimarkkinan potentiaali on suunnaton; maailmassa on jo lähes 2 miljardia matkapuhelinta. Merkittävimmät mobiilipelaamisen markkinat ovat Aasiassa.

Miksi palvelujen turvallisuus kiinnostaa?

Liikenne- ja viestintäministeriön LUOTI-ohjelman tavoitteena on olla mukana edistämässä luotettavien ja turvallisten sähköisten palvelujen kehitystoimintaa. Lisäksi ohjelman tavoitteena on löytää keinoja yleisen luottamuksen lisäämiseksi sähköisiä palveluja kohtaan. Siksi on ollut ensiarvoisen tärkeää tunnistaa niitä elementtejä, joiden varaan loppukäyttäjän luottamus palvelua kohtaan rakentuu. Ensimmäisenä toimintavuotena kohteeksi valittiin viihdepalvelut, koska kehitystyö niiden osalta on yleisesti kiivasta (ks. edellinen luku) ja toisaalta kehittäjäjoukko on ainakin toistaiseksi heterogeenistä. Toimintatapoja löytyy laidasta laitaan.



Yleisesti Suomessa voidaan todeta, että palveluja kohtaan ei ole olemassa suurta epäluuloa tai luottamuspulaa. Silti jokapäiväinen kirjoittelu käyttöjärjestelmien tietoturva-aukoista sekä erilaisista luottokortin käyttäjiä kohtaan kohdistuvista hyökkäyksistä pitää loppukäyttäjät varpaillaan. Nythän on ensimmäisen kerran kohdistunut myös vakavasti otettava phishing-hyökkäys luotettavina pidettyjä suomalaisia pankkipalveluja kohtaan.

Luottamuksella on siis palvelujen käytön ja yleistymisen kannalta suuri rooli. Uusien palvelujen käyttöönotto on aina hidasta ja tällaiset seikat vaikuttavat yleensä kaikkien sähköisten palvelujen käyttöönottoon – toimialasta riippumatta.

Tyyntä myrskyn edellä?

Useimmat tavatuista yritysten edustajista pitävät Suomea jonkinlaisena lintukotona. Pienenä markkinana Suomi ei ole perinteisesti ollut kiinnostava kohde tietoturvaloukkauksille tai –rikkomuksille. Suomesta saatava huomioarvo on kohtuullisen pientä ja palvelujen piirissä liikkuvat pienet rahat eivät houkuttele tietoturvarikollisia. Suomessa toimivat yritykset kehittävät kuitenkin palveluja ja pelejä ennen kaikkea globaaleille markkinoille, joten uhkaa on osattava tarkastella laajemmin ja sen vuoksi asiaa ei lähdetä vähättelemään. Toisaalta meitä lähellä olevat itänaapurit ovat jo osoittaneet ”kiinnostuksensa” suomalaisia online-käyttäjiä kohtaan suuntaamalla huijausyrityksiään suoraan suomalaisille loppukäyttäjille.

Tietoturvaan on suhtauduttava tosissaan ja varauksella. Tässä on oikeastaan kyse ainakin kahdesta tekijästä. Ensinnäkin tietoturva ei ole Suomesta käsin hoidettava ongelma. Jos jotain tapahtuu muualla, heijastuu se nopeasti meillemme. Tästä on esimerkkinä vaikkapa maailmanlaajuisesti käytössä olevat käyttöjärjestelmien tai selainten tietoturva-aukot päivityksineen. Toiseksi Suomi voi erottautua turvallisilla ja luotettavilla palveluilla, niin kuin se oikeastaan on jo joillain osa-alueilla onnistunut tekemään. Turvallisten palvelujen kehittämisessä voi piillä kilpailukykytekijöitä kilpaillessamme maailman mahtiyritysten kanssa samoilla markkinoilla.

Ovatko maassamme tapahtuneet vähäiset tietoturvaloukkaukset silti vain tyyntä myrskyn edellä? Sitä moni haastatelluista pohti tosissaan. Suomesta käsin on jatkuvasti kyettävä seuraamaan, mitä maailmalla tapahtuu ja reagoimaan asioihin niiltä osin kuin se on meiltä mahdollista. Kyse on enemmänkin sellaisten toimintatapojen kehittämisestä, joilla voidaan parantaa ennakoivia tulevia riskejä kohtaan. Tästä toiminnasta hyvänä esimerkkinä mainittakoon Viestintäviraston CERT-FI-yksikkö sekä sen verkosto ja toiminta.



Palvelunkehittäjien huomiot kiinnittyvät käyttötapauksiin

Palvelujen kehittäjät listasivat käyttötilanteet ja niiden aiheuttamien tietoturvariskien tunnistamisen tällä hetkellä palvelukehitysprosessin ykköσαιheiksi puhuttaessa turvallisten palvelujen kehittämisestä. Palvelujen luotettavuus ja turvallisuus on monelle yritykselle liiketoiminnan elinehto.

”Palvelujen luotettavuus ja turvallisuus on monelle yritykselle liiketoiminnan elinehto.”

Kukapa haluaisi pelata sellaista verkkopeliä, jonka kautta menetät omat käyttäjätietosi ulkopuoliselle ja mahdollisesti kohtaat vielä taloudellisiakin tappioita? Tällaisten palvelujen piiristä katoavat käyttäjät hyvinkin nopeasti.

Palvelujen kehittämisen kannalta tämä on edellyttänyt uudenlaisten toimintamallien omaksumista. Tietoturva astuu kuvaan entistä varhaisemmassa vaiheessa – palveluja suunniteltaessa. Alkuvaiheessa huomio kiinnittyy käyttöprosessin kuvaamiseen. Minkälaisia erilaisia tilanteita palvelun piirissä voi päästä syntymään? Käyttötapauskuvausten kautta voidaan arvioida erilaisia riskejä ja niiden toteutumista. Rakennetun riskianalyysin avulla voidaan tehdä yksityiskohtaisempia tietoturvasuunnitelmia riskien välttämiseksi. Tietoturvasuunnitelma toimii useassa tapauksessa vaatimusmäärittelydokumenttina mm. alihankkijoita valittaessa ja ohjeistettaessa. Se toimii myös ohjelistana sopimusdokumentteja kirjoitettaessa tilaajan ja toimittajan välillä.

Käyttötilanteiden kuvaaminen saattaa vaatia myös vilkasta mielikuvitusta, sillä useimmiten turva-aukot löytyvät paikoista, joita palvelunkehittäjät eivät huomaa ajatella. Työ on siksi hyvinkin vaativaa ja kaikkien aukkojen tukkiminen etukäteen on lähes mahdotonta.

Aukottoman palvelun rakentaminen tarkoittaa yleensä tinkimistä käytettävyydestä. Myös tämän vuoksi aukkojen täydellinen tukkiminen ei tunnu järkevältä. Palvelujen kehittäjät pyrkivät arvioimaan realistisista lähtökohdista, mitkä uhat ovat todellisia ja millä tasolla näihin pitää suhtautua.

Case: Internet-pokeri

PAF lanseerasi multiplayer internet-pokerin kesällä 2005. Multiplayer-pelissä online-pelaajat pelaavat toisiaan, eivät konetta vastaan. Tällöin huijaamisen mahdollisuus on suurempi. Pelin kehityksessä on jouduttu paneutumaan käyttäjien suorittaman huijaamisen tunnistukseen teknisten tietoturvatekijöiden lisäksi.

Markku Reiss kirjoitti PAFin Stefan Petterssonin haastattelusta kesällä 2005 Digitodayssa seuraavasti: ”Pelien lanseerausta on jo odotettu, koska nettipokerit ovat juuri nyt kovassa nousussa. Samalla olemme PAFissa yllättyneet siitä, että alalla ja mediassa ei ole lainkaan keskusteltu internet-pokerin kääntöpuolesta eli siitä



ilmeisestä riskistä, että tavalliset pelaajat häviävät rahojaan pelissä fuskaaville pelaajille”, sanoo PAFin internet-pelien johtaja Stefan Pettersson.

PAF kertoo valinneensa huolella luotettavan yhteistyökumppanin. ”PokerNetworkilla on pitkälle kehitetty järjestelmä, jolla estetään fuskaaminen, eli toisin sanoen järjestelmä pystyy jäljittämään pelaajat, jotka pelaavat yhteistyössä toistensa kanssa. Yritys on myös hakenut patenttia ohjelmistolle”, painottaa Pettersson.”

*”Merkittävimmät tietoturva-
loukkaukset kohdistuvat
käyttäjien väliseen
keskinäiseen toimintaan,
ts. huijaamiseen.”*

Kuten haastattelu osoittaa, pelien kehityksessä joudutaan yhä enemmän ottamaan huomioon käyttäjien mahdolliset tahalliset väärinkäytökset palvelua kohtaan. Tämä tekee palvelukehityksestä haastavampaa, kun joudutaan kuvaamaan erilaisia käyttö- tai oikeammin väärinkäyttötapauksia sekä tekemään niiden mukaan varautumissuunnitelmia.

Teknisten aukkojen etsintä on siirtymässä palvelukehitysprosessin alkupäähän

Monien peliyritysten mukaan kehittyneet tuotekehitysmenetelmät ja talojen kovan luokan osaaminen on yksi tärkeimmistä menetelmistä luotettavia ja turvallisia palveluja rakennettaessa. Suomen ongelma on lähinnä osaamisen kehittämisessä. Monesti yritykset ovat se taho, joka varmistaa oman henkilöstönsä osaamisen erilaisten koulutusten ja toisaalta oikeanlaisen henkilövalinnan avulla. Suomalaiset oppilaitokset eivät ole kyenneet vastaamaan tietotekniikka-alojen huutavaan pulaan kovanluokan osaajista. Yhä useammin osaajat on rekrytoitava maailmalta.

Hyvätasoisella osaamisella varmistetaan oman palvelu- ja pelialustan turvallisuus. Se mihin ei voida vaikuttaa, on luonnollisesti internet-alustat (mm. selaimet) ja näiden turvallisuus. Sen vuoksi ollaan myös muista riippuvaisia.

Yhä useammin omassa tuotekehitystyössä pyritään oman alustan tekniset aukot tunnistamaan jo varhaisessa vaiheessa. Tällöin ollaan omalta osalta varmistamassa luotettavan palvelun rakentumista. Palvelun luotettavuus on yksi keskeinen elementti yrityksen uskottavuuden rakentamisessa. Uskottavuudella on puolestaan suuri merkitys rynnistettäessä kansainvälisille markkinoille. Turvallisuus ei ole kuitenkaan merkittävin uskottavuuden elementti, vaan oikeastaan se on välttämätön pakko. Uskottavuus rakentuu monen tekijän summana, josta mm. aiemmin mainittu yrityksen kaupallinen ja tekninen osaaminen näyttelee suurta roolia.



Case Habbo-hotelli

Sulake Corporationin Habbo-hotelli on loistava esimerkki paitsi uskottavuuden merkityksestä yrityksen kasvua vauhdittavana tekijänä, myös palvelun luotettavuuden merkityksestä käytön kasvua kiihdyttävänä elementtinä. Sulakkeelle luotettavuus ja turvallisuus ovat saaneet erityisen merkityksen, koska palvelun tai pelin kohderyhmään kuuluvat lapset ja nuoret käyttäjät.

Monista käytännön asioista onkin sovittu eri viranomaistahojen kanssa tämän monelle vaikutukselle alttiin kohderyhmän suojelemiseksi. Mm. maksamisesta ja hinnoittelusta on sovittu yhteisesti viranomaistahojen kanssa. Siltikään ei voida olettaa, että vastuu siirrettäisiin tällaisin menettelyin palveluja kehittäville yrityksille. Vanhempien vastuuta ei voida lähteä ulkoistamaan.

Sulake sanoo edellä mainitun lisäksi haasteekseen kovasti kasvavan käyttäjäryhmän ja palvelun käyttöasteen kasvamisen hallittavuuden. Käyttäjäryhmään kuuluu tänä päivänä toistakymmentä miljoonaa käyttäjää eripuolilla maailmaa ja luonnollisesti tähän joukkoon mahtuu käyttäjiä laidasta laitaan. On luonnollista, että miljoonien käyttäjien joukkoon mahtuu edistyksellisiä "lapsineroja", jotka kokeilevat palvelun piirissä paitsi omia niin myös toisten käyttäjien rajoja. Sulake on rakentanut palvelualustaan kehittyneitä kontrollointimekanismeja erilaisten väärinkäytösten ehkäisemiseksi. Tässä on onnistuttu erinomaisesti, mutta Sulake myöntää, että tällä saralla on oltava aina aktiivinen.

Kansainvälisessä ympäristössä toimiminen asettaa omat haasteensa hallittavuudelle myös lainsäädännöllisestä näkökulmasta. Monikansallisessa ympäristössä lainsäädännöt vaihtelevat ja Sulake on joutunut tekemään monia maakohtaisia ratkaisuja. Tämä edellyttää myös maakohtaisia neuvotteluja kohdemaan viranomaistahojen kanssa siitä, mitä saa tehdä ja mikä on kiellettyä.

Käytettävyys määrää turvallisuuden rajan

Vaikka turvallisuuden merkitystä ei voi vähätellä, muistavat monet viihdepalvelu- ja peliyritykset mainita käytettävyyden rajoja rakentavana tekijänä. Käytettävyys määrittää monesti sen, missä tietoturvallisuuden raja kulkee. Käytettävyys on kuitenkin palvelujen käytön "mittari". Korkea käytettävyys ruokkii käyttöä, huono käytettävyys tappaa palvelun.

"Korkea käytettävyys ruokkii käyttöä, huono käytettävyys tappaa palvelun."

Palvelukehityksessä on pidettävä jalat maassa ja mietittävä, mitkä ovat todellisia uhkia ja mitkä sci-fi-elokuvien tasoisia uhkilla pelottelua. Tosiasia kuitenkin on se, että ongelmia on toistaiseksi ollut hyvin vähän, varsinkin Suomessa.

Turvallisuudella on myös hintansa. Jos tähän peliin lähtee liian kovalla intohimolla mukaan, unohtaen käytettävyystekijät ja realistisuuden, saattaa palvelukehittäminen



tulla kalliiksi. Viimeisimpien teknologioiden käyttöönotto kun tuppaa olemaan paitsi työlästä (osaamisen puute), myös kallista puuhaa.

Kansainväliset markkinat ovat ainoa tie kasvuun

Suomen markkinoiden pienuus ja silti kohtuullinen kilpailun taso vähäisistä asiakkaista on kääntänyt palveluja ja pelejä kehittävien yritysten katseet ulkomaille heti alkumetreilla. Suomen rajojen ulkopuolella ei luonnollisestikaan ole yhtään sen helpompaa, mutta korkeasta osaamistasostaan tunnetut yritykset ovat osoittaneet, että kansainvälisillä markkinoilla pärjääminen ei ole mahdoton tehtävä.

Suomalaiset yritykset ovat olleet tunnettuja turvallisten palvelujen kehittäjinä. Haastatellut eivät ole osanneet mainita yksiselitteistä syytä tähän. Ehkä tämä mielikuva syntyy myös Suomi-kuvan kautta. Suomi tunnetaan maailmalla turvallisena ympäristönä, jossa on kehittyntä toimintaa tietoyhteiskuntakehityksen saralla.

Yhteenvedona edellä mainituista voidaan sanoa, että suomalaisten yritysten on pystyttävä kasvattamaan erinomaisen teknisen osaamisen rinnalle myös kaupallista osaamista pärjätäkseen kansainvälisillä markkinoilla. Tästä on puhuttu laajalla rintamalla mm. Neogames-peliklusterin piirissä. Neogames on pienenä toimijana tehnyt erinomaista työtä suomalaisten yritysten viemiseksi maailmalle. Muitakin vienninedistäjätahoja on ollut kuvassa mukana, kuten esimerkiksi Finpro ja Tekes.

LUOTI-OHJELMA

Luottamus ja tietoturva sähköisissä palveluissa (LUOTI) -ohjelma on liikenne- ja viestintäministeriön tietoturvaohjelma vuosille 2005–2006. Sen tavoitteena on uusien monikanavaisten sähköisten palvelujen tietoturvan kehittäminen. LUOTI tuo yhteen yritysten uudet tarpeet ja tietoturva-alan osaamisen. LUOTI-ohjelman ensimmäinen pilotointialue oli viihde.

Tavoitteena on käytännön hankkeiden avulla kehittää uutta toimintamallia, jossa tietoturva otetaan sähköisiin palveluihin mukaan jo niiden kehittämisen alkuvaiheessa. Lopullisena tavoitteena on kuluttajien luottamuksen lisääminen sähköisiin palveluihin.