4.11.2010

1 YLIOPISTOJEN TIETOTURVAPÄÄLLIKÖIDEN SUOSITUS SOSIAALISEN MEDIAN KÄYTÖSTÄ

Tämä viestintäsuositus sisältää yliopistojen tietoturvapäälliköiden kannanoton sosiaalisen median verkkosovellusten käyttöön ja pyrkii tuomaan esiin niihin liittyvät keskeiset tietoturva- ja laillisuusriskit. Suositus laadittiin 19.5.2010 pidetyn kokouksen keskustelujen ja linjausten mukaisesti yliopistojen tietoturvapäälliköiden ja Funet Cert:n, HIIT:n ja Aalto-yliopiston teknisten asiantuntijoiden kanssa.

Tietoturvasuositus luo perusedellytykset sosiaalisen median käytölle yliopistoissa sisältäen ehdot käytön aloittamiselle, tarkastelun vastuista, laillisuusperiaatteista, sopimusriskeistä ja tietoturvariskeistä. Suositusta laadittaessa on huomioitu valtionhallinnon Tietoturvatasot ohjeistus.

Vaikka yliopistot suhtautuvat myönteisesti sosiaalisen median käyttöön viestinnässä, markkinoinnissa ja tiedeviestinnässä, on myös käytön riskejä arvioita realisesti. Sosiaalisen median käyttöön liittyvät toiminnalliset, oikeudelliset, tekniset sekä taloudelliset riskit ydintoiminnalle tulee ymmärtää ennen sosiaalisen median välineiden käyttöönottoa. Sosiaalisen median palvelut otetaan käyttöön johdetusti osana yliopiston toimintaa.

Tämä dokumentti täydentää Viestintäosaston laatimaa dokumenttia: ”suositus sosiaalisesta mediasta yliopistojen viestinnässä ja markkinoinnissa”.

1.1 Perusteet sosiaalisten medioitten käyttöönotolle

Tekninen kehitys on tuonut uusia maksuttomia ja helppokäyttöisiä yhteisöllisiä verkkosovelluksia, joita nimitetään sosiaaliseksi mediaksi. Yliopistoissa on suuri tarve sosiaalisen median käyttöön, koska sosiaalisen median sovelluksia voidaan käyttää yliopistolla opetuksen apuvälineinä virtuaalisia opetusympäristöjä ja sisällöntuotannon välineitä. Myös tutkimusryhmät ovat huomanneet niiden mahdollistavan maailmanlaajuisen, tutkimustyön kannalta merkittävän kontaktiverkoston luomiseen ja nopean viestinnän. Kiinnostus sosiaalisen median käyttöön on ollut niin laaja, että käyttäjät eivät ole aina kyenneet arvioimaan sosiaalisten medioitten tuomia riskejä yliopiston toiminnalle ja yliopiston järjestelmien tietoturvallisuudelle.

4.11.2010

1.2 Käytön rajoitukset

Yliopistojen on kyettävä arvioimaan millä toiminta-alueilla ulkoiset palveluntarjoajat pystyvät tuottamaan riittävän palvelutason. Yliopiston turvaluokiteltua materiaalia, kuten laskusta, henkilöstöasioita ja muuta turvaluokiteltua aineistoa, ei tule liittää osaksi sosiaalisen median palveluja.

Sosiaalisen median toiminnan luonteesta johtuen rahoituksen perusteena oleva toiminta pitää pystyä turvaamaan varamenettelyin, jolloin opetus tai tutkimus ei saa perustua yhden palvelun varaan tai palvelun on oltava varmistettu ja saatavissa niiden vaatimusten mukaisesti jotka kyseiselle käyttötarkoitukselle ovat ehdottomia. Mitään toimintoja ei saa perustaa oletukseen että sosiaalisen median palvelu toimii varmasti.

Sosiaalisen median sovelluksia ei voida käyttää etätyön välineenä, sillä työhön liittyvässä materiaalissa on usein ei-julkista materiaalia. Sosiaalisia medioita ei ole sallittua käyttää tietokoneilta, joissa käsitellään valtionhallinnon ohjeistuksen mukaisen turvaluokan II ja III mukaisia tietoja. Turvaluokan II tieto sisältää kansalliseen turvallisuuteen, varautumiseen ja viranomaistoimintaan liittyviä tietoja. Turvaluokan III asiakirja sisältää salassa pidettävää tietoa, kuten potilastietoja, liikesalaisuuksia kuten patentti- ja keksintötietoja, sekä perusrekistereitä ja arkaluontoisia henkilötietoja.

1.3 Sallittu käyttö

Yliopisto voi käyttää sosiaalisen median palveluita ja toimia sen välityksellä yliopiston markkinoinnissa, rekrytoinnissa ja sidosryhmien kommunikoinnin mahdollistajana luonteeltaan julkisissa asioissa. Sosiaalista mediaa voidaan käyttää:

- Harkittuun suunnattuun tiedottamiseen, ei tiedon tallentamiseen
- Asiakaspalvelun täydentävänä kanavana, esimerkiksi asiakastyytyväisyys / palautekyselyissä joissa ei käsitellä henkilötietoja.
- Yhteistyökumppaneiden ja muiden sidosryhmien kanssa tapahtuvaan viestintään julkiseksi luokiteltavien asioiden osalta
- Viestittäessä julkisia asioita yliopiston toiminnasta
- Rekrytoinnin apuna
- Yliopiston toiminnan markkinoinnissa esimerkiksi blogien avulla
- Rajoitetulta osin poikkeustilaviestinnän tiedottamisen apuvälineenä täydentämässä muita viestintävälineitä, mutta ko. viestintään liittyvä vastuutaho on määriteltävä yksikäsitteisesti. On huomattava että osa kriisiviestinnästä ei ole julkista eikä se saa päätyä ulkopuolisen tietoon.

- Yliopiston toiminnan esittelyyn Youtubessa tai sen kaltaisissa palveluissa. Kuitenkin palvelun käytön aiheuttama mahdollinen kuormitus tietoliikenteelle tulee kyetä ennalta arvioimaan niin, ettei se hidasta normaalia toimintaa.
- Sellaisen julkisen materiaalin jakoon, jonka tekijänoikeudet on varmistettu

2 Suositeltu käyttöönottomalli

Yliopistojen tulisi sallia käyttöön vain sellaisia soisaalisen median palveluita, joihin liittyvät riskit ovat yliopistojen kannalta kohtuullisen pienet ja hallittavissa. Ennen kunkin palvelun uuden palvelun käytön aloittamista tulee siihen liittyvät riskit arvioida yhdessä liopiston lakimiesten ja tietoturva-asiantuntijoiden kanssa. Viestintä konsultoi sosiaalisen median tavoitteellisessa käytössä.

Sosiaalisen median käyttö yliopiston työvälineenä tulee huomioida laadittaessa yliopiston tietohallintostrategiaa ja tietoturvaohjeita. Työasemilta joissa käsitellään korkean turvaluokan tietoa (TL III, II eli potilatiedot, henkilötiedot, rahavirtatiedot)ei tule käyttää sosiaalisen median palveluita.

Lisäksi ennen uuden palvelun käyttöönottoa

- Ulkoistetun palvelun käyttöönotto edellyttää hyvää sopimusosaamista.
- Viralliseen käyttöön tulevasta palvelusta on syytä solmia kirjallinen sopimus aina. Ilman erillistä sopimusta palveluntarjoaja voi muuttaa käyttöehtoja kuulematta asiakasta; huolella tehdyn kirjallisen sopimuksen ehtojen muuttaminen vaatii neuvotteluja sopimuskumppanin kanssa.
- On kyettävä arvioimaan palvelun ylläpitovaatimukset, sekä arvioitava millaisia ruuhkapiikkejä palvelujen käytöstä voi kantautua. Päätöksenteon tueksi tarvitaan tilastoja käytöstä.
- Tarvitaan budjetti perehdyttämiseen ja henkilöstön tietoturvakoulutukseen
- Tarvitaan tietoturva- ja käyttösääntöjen hyväksymislomake jossa kuvataan laillisuusnäkökulmasta käyttäjän vastuu, sallittu käyttö/tiedottaminen, toiminta ongelmatilanteessa
- Rajoituksista on tiedotettava (rajoittamaton tietoliikenne ei ole perusoikeus)
- Kunkin yliopiston tulee arvioida miten pilvipalvelut tulevat muokkaamaan omaa tietoturvan hallintaa ja miten se vaikuttaa toimintaan poikkeustiloissa.
- Kukin sosiaalista mediaa käyttävä työntekijä vastaa itse palvelujen tietoturva-asetuksista

2.1 Käyttäjäryhmät ja keskeiset käyttötapaukset

Työnantajan tulee ottaa kantaa sosiaalisen median käyttöön työtehtävissä – se voi kieltää sosiaalisten medioitten käytön tai osoittaa sen yhdeksi työvälineeksi osana työtehtävien hoitoa. Työnantajan ei kuitenkaan pidä velvoittaa työntekijää palvelun käyttöön omalla nimellä, sen tulee perustua vapaaehtoisuuteen tai käytön suositellaan tapahtuvan ryhmätunnuksen kautta.

Yliopistojen kannattaa miettiä, miten palveluista tiedotetaan ja miten niitä markkinoidaan sidosryhmille. ja mitä käyttäjät voivat sanoa yliopiston nimissä. Edelläoleva tulisi kirjata viestintäpolitiikkaan ja henkilöiden toimenkuviin. Tapaus- ja palvelukohtaisesti tulee miettiä, onko syytä rajata ne käyttäjät ja ryhmät, jotka saavat edustaa työnantajaansa. Suositellaan ryhmien muodostamista, joilla on lupa esiintyä yliopiston nimissä (esimerkiksi viestintä, tietohallinto, teknologiapalvelut, ServiceDesk) ja jotka saavat ”esitellä” tai tiedottaa omaa toimintaansa. Yliopiston työtehtäviä ei saa hoitaa ykistyishenkilön tunnuksella, koska on jokaisen edun mukaista pitää työ- ja ykistysprofiili erillisenä. Näin ei pääse syntymään työntekijän omia, työhön liittymättömiä mielipiteitä.

Yliopiston virallisena edustajana esiinnyttäessä tulee pyrkiä käyttämään ryhmätunnusta ja organisaatio-osoitteita, kuten ”Aalto viestintä”. Muussa tapauksessa työnantaja on vastuussa esimerkiksi työntekijän henkilötunnuksien (HETU) luovuttamiseen liittyvissä asioissa. Yksityishenkilö ei saa esiintyä yliopiston nimissä, vaan työnantajaa edustettaessa tulee nimen lisäksi esittää myös työhön liittyvä tehtävänimike. Riskien minimoimiseksi työnantajan tulee ottaa huomioon muun muassa varahenkilöjärjestelyt, henkilövaihdokset ja tietojen luovutukset. Vääränlainen varomaton viestintä voi aiheuttaa työnantajan nolaamisen tai maineen menetyksen. Myös työnantajan ja työntekijän arvostelu sekä palautteen antaminen sosiaalisten medioitten kautta on kiellettyä. Työnantajalla on oikeus seurata työkäytössä olevaa sosiaalisten medioitten viestintää.

3 Sosiaalisten medioitten laillisuusriskit

Suositellaan, että yliopisto arvioi kukin sosiaalisen median palvelun kohdalla laillisuus- ja tekijänoikeusnäkökulmat lakimiehen avustuksella ja kyseisen palvelun tietoturvariskit tietoturva-asiantuntijoiden kanssa. Ennen käyttöä on mietittävä myös riskien realisoitumisen todennäköisyys, niiden hallinta ja realisoitumisesta koituvat vahingot.

3.1 Tutkimusdatan käsittely

- Tutkimusdataa ei saa julkaista, jos tietoon on jaetut oikeudet, tai julkaisija ei ole tiedon yksinomainen omistaja
- Tutkimusdata ei ole julkista ennen virallista julkaisua
- On huomioitava, että tutkimusdatassa voi olla turvaluokiteltua tai erikseen salassa pidettäväksi materiaaliksi luokiteltavaa tietoa kuten potilasdataa tai tutkimukseen liittyvän kolmannen osapuolen sopimusvelvoitteita.

3.2 Sopimusriskit

- On huomioitava että oikeudet omiin materiaaleihin yleensä menetetään, kun ne julkaistaan sosiaalisten medioitten palveluissa (maininta palvelun tarjoajan sopimuksissa).
- Tiedon omistajuus yleensä siirtyy palveluntarjoajalle. Sopimuksista on tarkastettava vaatiiko palveluntarjoaja vapaan käsittelyoikeuden dataan. On vaikea varmistua siitä onko dataa luettu jos palveluntarjoajan tietovarannot ovat Suomen aluerajojen ulkopuolella.
- Tietojen poistaminen palvelusta jälkikäteen on yleensä mahdotonta
- Palvelut saattavat olla käyttöönotettaessa maksuttomia, mutta voivat muuttua maksulliseksi myöhemmin.
- Sopimustarkastelu ennen palvelun käyttöönottoa on tärkeä varmistuksineen miten tieto saadaan takaisin.
- Palveluntarjoajan kokoluokka ja vakavaraisuus tulee varmistaa sekä se missä tiedot tulevat sijaitsemaan, mikä on palvelun siirrettävyys ja arkistointitapa.
- Sopimusjuridiikkaan liittyy palvelusopimuksen, sen luotettavuuden ja jatkuvuussitoumuksen tarkastelu
- On selvitettävä minkä maan lainsäädännön alaisia palvelut ja sopimus ovat, tämä ratkaisee millaiset mahdollisuudet on taistella datasta tarvittaessa (vaikuttavatko esimerkiksi maan poliittiset epävakaudet asiaan)
- Kokonaisvastuun ajattelu huomioitava: täytyy ymmärtää onko palveluissa tarvetta muun muassa käytettävyyteen mobiililla päätelaitteella, jolloin tietoturvallisuus tulee huomioida myös älypuhelintasolla.
- Palvelua käyttöönotettaessa on syytä huomioida, että palveluntarjoaja ei yleensä vastaa datan tietoturvasta. Suomesta tarjotun palvelun kohdalla tulee varmistua siitä, että palveluntarjoaja vastaa datan, henkilötietojen ja sähköisen viestinnän tunnistamistietojen suojaamisesta lainsäädännön asettamien vaatimusten mukaan.
- Palveluntarjoaja on sitoutettava toipumisprosesseihin ennen kuin mitään tapahtuu.
- Kriisitilanteessa on mahdollista että palveluntarjoaja estää pääsyn palveluun talletettuihin tietoihin. Erimielisyyksien selvittäminen lakiteitse voi tulla hyvin kalliiksi.
- Sopimuksessa tulisi estää palveluntarjoajan oikeus asiakkaan tallettaman tiedon analysointiin.

- Palveluntarjoaja voi halutessaan luovuttaa kansalliselle turvallisuusviranomaiselle kaiken. On yrityssidonnaista suojeleeko sopimusoikeus tällaiselta.
- Yrityskäyttäjän sopimus ja ehdot voi muuttua
- Yliopiston vastuulla on että sopimusta noudatetaan, työnantaja on vastuussa työvälineistä jota työntekijälle on annettu.
- Yhteys salasanapolitiikkaan (ei samaa tunnusta)
- Työnantajalla on lista kenellä lupa edustaa työnantajaansa

4 Sosiaalisten medioitten tietoturvallisuus

Koska sosiaalisen median palvelut tulevat muokkaamaan yliopiston omaa tietoturvan hallintaa (esimerkiksi toiminta poikkeustiloissa), ennen palvelun käyttöönottoa tietoturvapäällikkö tekee arvion palvelukohtaisesti, ovatko riskit liian suuria ulkoisen palvelutarjoajan käyttämiseksi. Tämä arvio sisältää riskien realisoitumisen todennäköisyyden, sekä arvion siitä, estääkö riskit koko palvelun käyttöönoton. Laillisuusnäkökulmaan liittyvät riskit tulisi arvioida lakimiehen kanssa.

Riskit muuttuvat säännönmukaisesti joten niiden säännöllinen arviointi on paikallaan. Jos muuttunut uusi riski vaarantaa organisaation toiminnan merkittävästi, tietoturvapäälliköllä on oikeus estää palvelun käyttö tilapäisesti tai kokonaan. Tämä tulee huomioida jotta tiedottamista tai muuta palvelua ei suunnitella pelkästään yhden palvelun varaan.

Mitään yliopiston palvelua- tai toimintoa ei tule rakentaa pelkästään sosiaalisen median tai pilvipalvelun varaan vaan toiminnalle pitää löytyä palvelun käyttöönottajan toimesta varamenettely ja se tulee kuvata toipumissuunnitelmissa. Jos sosiaalisen median palvelu ei ole käytettävissä, on arvioitava etukäteen miten se vaikuttaa toimintaan.

Sosiaalisen median palvelun käytettävyyteen ja tietoturvaan liittyvät kysymykset tulee voida postittaa ServiceDeskiin ja tietoturvan osalta yliopistojen tietoturvahenkilöstölle. Tietomurtotapausten selvittäminen on yleensä haasteellista ja työasematurvallisuuden merkitys korostuu.

Lisäksi suositellaan valtionhallinnon Tietoturvatasot määrittelyjen mukaisia teknisiä rajoitteita käyttöönotettavaksi yliopistoille soveltuvin osin. Tällaisia ovat esimerkiksi vaatimus tietoturva-arkkitehtuurin toteutumisesta muun muassa verkon segmentoinnilla ja palomuureilla, jotta haittaohjelman leviäminen hidastuu, sovellusten asentamisen esto työasemille (vakioimagen käyttö) ja organisaation tietoliikennettä analysoivien tekniikoiden käyttö.

4.1 Tietoturvariskit

Sosiaalisen median käyttöön liittyy yliopiston kannalta huomattava määrä riskejä:

- On mahdotonta valvoa mitä tietoa organisaatiosta liikkuu ulos
- Yksityisyysasetuksien säädöissä on oltava tarkkana. Palvelun välitysmekanismi voi sallia useita asetuksia aina yleisestä julkiseen vastaukseen ja yksityiseen vastaukseen
- Palveluiden tarjoajat ovat hitaita reagoimaan hyökkäyksiin
- Sosiaalisen median tilin irtisanominen on hankalaa, palveluun syötettyjä tietoja ei saa takaisin eikä yleensä täysin poistettuakaan.
- Haittakoodi leviää sosiaalisten medioitten kautta tehokkaasti, saastuneiden linkkien lähettäminen muille käyttäjille on helppoa. Ongelman muodostavat lyhennetyt URL -osoitteet, joista ei tiedä, minne käyttäjä päätyy.
- Vastapuolen tunnistaminen luotettavasti hankalaa, jolloin väärän identiteetin käyttö on helppoa. Myös identiteettivarkaudet ovat yleistyneet.
- Väärennetyt kirjautumissivut ovat käyttäjän uhkana
- Saman salasanan käyttäminen useissa järjestelmissä on ongelma. Jos ulkopuolisen palvelun salasanat saadaan haltuun esimerkiksi tietomurron kautta, niiden avulla voidaan päästä tunkeutumaan myös yliopiston järjestelmiin.
- Palveluun syötettyjen henkilöön liittyvien tietojen perusteella on mahdollista profiloida käyttäjiä hyvinkin tarkasti
- Tietoturvattomien sovellusten asentaminen muiden käyttäjien sivuilla olevista linkeistä on mahdollista
- Käyttäjien tiedot kerätään palveluntarjoajan arkistoon
- Tietoturvalliset käyttöasetukset vaativat perehtymistä
- Suurin osa käyttäjistä hyväksyy sellaiset kontaktit joita ei tunne
- Suurin osa käyttäjistä jakaa yksityisiä tiedostojaan
- Palvelut eivät tarjoa tietoturvaohjeita käyttäjilleen
- Käyttäjä luovuttaa helposti nimi ja osoitetietoja
- Tiedon jakaminen muiden käyttäjien kanssa oltava tarkasti rajattua
- Tietoturvattomien sovellusten asentaminen muiden käyttäjien sivuilla olevista linkeistä on riski.
- Huijarit lähettävät Facebook -sovelluspyyntöjä. Haittasovellus saattaa varastaa kaikki käyttäjän sivuilla olevat tiedot.