VALTIOVARAINMINISTERIÖ

Sosiaalisen median tieto-turva-ohje

4/2010 VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Sosiaalisen median tietoturvaohje

Valtionhallinnon tietoturvallisuuden johtoryhmä 4/2010 VAHTI

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila/VM-julkaisutiimi

ISBN 978-952-251-143-0 (pdf)
ISSN 1798-0860 (pdf)

Helsinki 2010

VALTIOVARAINMINISTERIÖ
Hallinnon kehittämisosasto

VM/2467/00.00.00/2010
OHJE
21.12.2010

Ministeriöille, virastoille ja laitoksille

Sosiaalisen median tietoturvaohje

Valtiovarainministeriön *Sosiaalisen media tietoturvaohje* kuvaa keskeisimmät sosiaalisen median palveluihin liittyvät tietoturvallisuusuhat sekä ohjeistaa organisaatioita mahdollisista ratkaisuvaihtoehdoista. Ohjeessa otetaan huomioon sosiaalisen median palveluiden käyttöön ja tarjontaan liittyvät asiat.

Ohje on tarkoitettu ensisijaisesti organisaatioiden sosiaalisen median palveluiden ja niiden käytön suunnittelijoille (esim. viestintä ja henkilöstöala), tietohallinnolle sekä tietoturvaorganisaatiolle ja -toiminnoille.

Sosiaalisen median palveluiden käyttö tulee hallinnon organisaatioissa arvioida niiden kautta saatujen hyötyjen perusteella tasapainotettuna mahdollisiin riskeihin. Riskienhallinta on keskeinen osa palveluiden käytön suunnittelua ja toteuttamista. Sosiaalisen median palveluiden ohjeistaminen on oltava linjassa organisaation tietoturvapolitiikan kanssa.

Organisaation tulee laatia sosiaalisen median käyttöpolitiikka, jonka tulee olla johdon tahtotilan mukainen ja hyväksymä sekä sisältää sosiaalisen median tietoturvallisuuteen liittyvät keskeiset linjaukset. Henkilöstön ohjeistaminen ja koulutus sekä selkeät linjaukset osana käyttöpolitiikkaa ovat tietoturvallisuuden kannalta keskeistä. Sosiaalisen median luonteen takia palveluun voidaan laittaa ainoastaan julkista tietoa.

Organisaatio voi hyödyntää sosiaalista mediaa myös siten, että se tuottaa itse joko omaan käyttöön ja/tai myös asiakkaille tarjottavia sosiaalisen median palveluita. Tällöin organisaation tulee suunnitella huolella sosiaalisen median palveluiden tarjoaminen sekä ostettaessa palveluita toimittajalta että palvelua itse tuotettaessa. Suositellaan, että sosiaalisen median käyttöönottoprojektista huolehtivat organisaatiot käyttävät hallinnollisessa, teknisissä ja tietoturva-asioissa apunaan organisaation hallinto-, verkkoviestintä-, tietohallinto- ja tietoturvaorganisaatiota.

Hallinto- ja kuntaministeri — Tapani Tölli

Neuvotteleva virkamies — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: Sosiaalisen median tietoturvaohje (VAHTI 4/2010)

Lyhyesti VAHTIsta

Valtiovarainministeriö ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Ministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin. VAHTI käsittelee kaikki merkittävät valtionhallinnon tietoturvallisuuden linjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTI edistää hallitusohjelman, yhteiskunnan turvallisuusstrategian, valtion IT-strategian, valtioneuvoston huoltovarmuuspäätöksen, kansallisen tietoturvastrategian, valtioneuvoston periaatepäätöksen valtion tietoturvallisuuden kehittämisestä ja hallituksen muiden keskeisten linjausten toimeenpanoa kehittämällä valtion tietoturvallisuutta ja siihen liittyvää yhteistyötä.

Valtioneuvosto teki 26.11.2009 periaatepäätöksen valtionhallinnon tietoturvallisuuden kehittämisestä. Periaatepäätös korostaa VAHTIn asemaa ja tehtäviä hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elimenä. Peiaatepäätöksen mukaisesti hallinnonalat kohdistavat varoja ja resursseja tietoturvallisuuden kehittämiseen ja VAHTIssa koordinoitavaan yhteistyöhön.

VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta astaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

VAHTIn toiminnalla parannetaan valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Tuloksena on aikaansaatu yksi maailman kattavimmista yleisistä tietoturvaohjeistoista (www.vm.fi/vahti). VM:n ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita sekä laaja valtion tietoturvallisuuden kehitysohjelma.

VAHTI on saanut kolme kertaa tunnustuspalkinnon esimerkillisestä toiminnastaan Suomen tietoturvallisuuden parantamisessa.

Sisältö

1 Johdanto

Sosiaalisen median suosio on viime vuosina kasvanut merkittävästi. Sosiaalisen median palveluita käyttävät niin yritykset, valtion- ja muun julkishallinnon organisaatiot, viranomaiset, yliopistot kuin yksityiset henkilöt. Ilmiö on kuitenkin monelle organisaatiolle uusi, jonka takia sosiaalisen median palveluiden käyttökulttuuri ei ole organisaatiotasolla vielä täysin muodostunut eikä sosiaalisen median hyötyjä kuten sen riskejä vielä tiedosteta.

Sanastokeskus TSK:n julkaiseman Sosiaalisen median sanaston mukaan sosiaalinen media on tietoverkkoja ja tietotekniikkaa hyödyntävä viestinnän muoto, jossa käsitellään vuorovaikutteisesti ja käyttäjälähtöisesti tuotettua sisältöä ja luodaan ja ylläpidetään ihmisten välisiä suhteita. Käytännössä tämä tarkoittaa sitä, että jokaisella käyttäjällä tai käyttäjäryhmällä on mahdollisuus olla aktiivinen viestijä ja sisällön tuottaja. Sisällön tuotto ja jakelu perustuu monelta monelle -periaatteeseen, eikä perinteiseen yhdestä monelle, niin kuin perinteiset joukkoviestimet.

Monet organisaatiot suunnittelevat sosiaalisen median palveluiden käyttöön ottamista tai jopa tarjoamista. Oikeusministeriön teettämässä katsauksessa ”Sosiaalisen median mahdollisuudet hallinnolle” (toim. Tuija Aalto) todettiin, että on arvo sinänsä, että julkiset organisaatiot ja virkamiehet ovat läsnä samoissa palveluissa kuin kansalaiset. Käyttöönottopäätöstä ei tosin tule tehdä pelkästään sen takia, että ”kaikki muutkin ovat siellä”. Sosiaalisen median käyttöönotto on organisaation johdon tietoinen päätös, joka perustuu organisaation yhden tai useamman ydintoimintaan liittyvän tehtävän tukemiseen ja johon sitoudutaan asianmukaisin resurssein.

Myös sosiaalisen median palveluiden käyttämättä jättäminen tulee olla tietoinen päätös.

Riippumatta siitä, hyödyntääkö organisaatio sosiaalisen median palveluita omiin tarpeisiin vai ei, on suositeltavaa, että sosiaalisen median käytöstä linjataan käyttöpolitiikan muodossa. Käyttöpolitiikan tulee olla johdon tahtotilan mukainen sekä johdon hyväksymä. Käyttöpolitiikan yhteydessä tulee ottaa huomioon tietoturvallisuuden toteutumiseen liittyvät seikat. Sosiaalinen media ei sinänsä tuo uusia tietoturvahaasteita, mutta sosiaalisen median käyttötavat eroavat merkittävästi perinteisen median käyttötavoista ja perinteisistä Internet-palveluista, jonka takia tietoturvauhat ilmenevät eri tavalla. Tämä johtuu siitä, että sosiaalisessa mediassa käyttäjän toimenpiteet ovat normaalia palvelui-

den käyttöä keskeisemmässä asemassa. Tahaton hölmöily saattaa johtaa ikäviin seurauksiin, esimerkiksi organisaation tietojen vuotamiseen, henkilökohtaisen mielipiteen esittämiseen organisaation virallisena kannanottona, haittaohjelman leviämiseen tms. Henkilöstön ohjeistaminen ja selkeiden linjausten tekeminen osana käyttöpolitiikkaa on organisaation tietoturvallisuuden kannalta keskeisessä asemassa.

Tämän ohjeen tavoite on avata keskeisimmät sosiaalisen median palveluihin liittyvät tietoturvallisuusuhat sekä ohjeistaa organisaatioita mahdollisista ratkaisuvaihtoehdoista. Ohjeessa otetaan huomioon sekä sosiaalisen median palveluiden käyttöön että tarjontaan liittyvät asiat. Ohje on ensisijaisesti tarkoitettu organisaatioiden sosiaalisen median palveluiden ja niiden käytön suunnittelijoille (esim. viestintä ja henkilöstöala), tietohallinnolle sekä tietoturvallisuusorganisaatiolle.

2 Sosiaaliseen mediaan liittyvät tietoturvariskit

Sosiaalisen median tietoturvaongelmat syntyvät pääosin perinteisten tietoturvauhkien ja uusien toimintamallien ja palveluiden yhdistelmänä. Sosiaalinen media ei toistaiseksi ole tuonut varsinaisesti uusia tietoturvauhkia, mutta sosiaalisen median toimintaperiaatteen luonteesta johtuen ilmenevät tietoturvauhat eri tavalla kuin perinteisessä mediassa. Toimintaperiaatteisiin kohdistuvat tietoturvauhat korostuvat erityisesti yhteisöpalveluissa.

Keskeisimmät tietoturvauhat perustuvat sekä käyttäjän omaan toimintaan että ammattimaiseen ja suunniteltuun toimintaan, jossa rikolliset, ääriryhmät tai valtiot pyrkivät esim. saamaan haltuunsa tietoa (luottokortti- ja henkilötietoja, yrityssalaisuuksia, valtiosalaisuuksia), vaikuttamaan päätöksentekoon (kuluttajien, yritysjohdon, valtionjohdon) tai tahraamaan organisaatioiden tai ihmisten mainetta.

Ammattirikolliset hakevat taloudellista etua hyödyntämällä sosiaalisen median palveluita ja niiden kautta levitettäviä haittaohjelmia, jotka mahdollistavat esim. käyttäjän tietokoneen etähallinnan ja käyttämisen rikollisjärjestön haluamaan käyttötarkoitukseen. Rikollisjärjestön ylläpitämä, jopa (sadoista) tuhansista kaapatuista tietokoneista koostuva ns. botnet-verkko voi toimia tehokkaana roskapostipalvelinympäristönä, huijaus-verkkopalveluna, kohdistettuja palvelinestohyökkäyksiä suorittavana verkkoalustana, palveluihin eri salasanayhdistelmiä kokeilevana, tietomurtautumista yrittävänä verkostona tai salasanoja matemaattisesti murtavana laskentakeskuksena. Erityisen vaarallisia ovat sellaiset organisaatioon kohdennetut hyökkäykset, joissa käytetään tarkoitusta varteen räätälöityä haittaohjelmaa, joita organisaation käyttämät torjuntajärjestelmät eivät tunnista.

Seuraavissa kappaleissa on katsaus niihin keskeisimpiin tietoturvariskeihin, joita sosiaalisen median palveluiden käyttämiseen tai niiden tarjoamiseen liittyy.

2.1 Tietoaineistoon liittyvät riskit

Tietoturvallisuuden keskeinen tehtävä on huolehtia tietoaineistojen luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvistä seikoista palveluiden

helppokäyttöisyyttä unohtamatta. Eräs merkittävimmistä sosiaalisen median palveluiden tietoturvallisuuden uhkakuvista on muun kuin julkisen tietoaineiston paljastuminen tai joutuminen väärin käsiin. Tämä voi aiheutua seuraavista seikoista:

1. Käyttäjä saattaa jakaa tai lähettää palveluun vahingossa tai tiedostamattaan salassa pidettäviä tietoaineistoja. Mikäli palvelu on ulkomailla tai kolmannen osapuolen ylläpitämä, saattaa aineiston poistaminen olla joko mahdotonta tai se kestää niin kauan, että tieto ehtii vuotaa ja levitä myös muualle Internet-verkon palveluihin, jolloin tietoaineisto jää ”ikuisesti” nettiin. Lisäksi tiedon poistoyritykset saattavat vain johtaa siihen, että tieto leviää entistä laajemmin.
2. Käyttäjä saattaa aiheuttaa tiedostamattaan tietovuodon siten, että vaikka hänen yksittäiset viestit eivät muodosta uhkaa, niin kerättäessä nämä eri palveluihin tuotetut viestit yhteen tai keräämällä tietoja pitemmältä aikajaksolta, saadaan muodostettua sellainen kokonaisvaltainen tilannekuva, joka johtaa luottamuksellisen tiedon menettämiseen
3. Vaikka käyttäjä ei lähetä luottamuksellista tietoa sosiaalisen median palveluun, toinen henkilö saattaa palveluun lähettämässä viestissä, valokuvissa tai videotiedostoissa paljastaa tahattomasti käyttäjää tai organisaatiota koskevia luottamuksellisia tietoja.

Useat sotilasorganisaatiot ovat ilmoittaneet ongelmaksi sen, että omat joukot kirjoittaessaan blogeja kriisialueelta paljastavat tietoja operaatiosta ja sen suunnitelmista, näin vaarantaen sekä operaation, henkilöstön että paikallisen väestön turvallisuuden.

Sosiaalista mediaa voidaan käyttää myös tietoisesti väärän tai virheellisen tiedon levittämiseen. Sähköisessä muodossa olevan tiedon leviämistä on usein mahdotonta valvoa. Tiedon eheyden takaaminen on usein mahdotonta, koska tieto saattaa muuntua merkittävästi matkalla palvelusta ja välittäjästä toiseen.

Käyttäjätunnusvarkaudet

Organisaation käyttämät käyttäjätunnukset saattavat joutua vääriin käsiin, minkä jälkeen vihamielinen toimija voi tehdä organisaation tunnukselle mitä haluaa, esim. muuttamalla palvelun sisältöä, julkistaa materiaalia organisaation nimissä, levittää haittaohjelmia tai varastaa henkilötietoja. Tämä saattaa aiheuttaa harmeja organisaation maineelle sekä aiheuttaa lisätyötä tilanteen korjaamiseksi. Tämän ohella vääriin käsiin päätynyt käyttäjätunnus ja salasana saattaa aiheuttaa salassa pidettävän tiedon päätymisen oikeudettomasti

ulkopuolisten tahojen haltuun vaarantaen tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät velvoitteet.

Identiteettiväärennökset

Käyttäjätunnusvarkauksien lisäksi esiintyy myös identiteettiväärennöksiä. Osa organisaatioista on saattanut huomata, että Internet-verkkoon on pystytetty sen toimintaa jäljitteleviä www-palveluita tai sen roolissa yritetään toimia sosiaalisen median palveluissa. Vaikka tällaiset, usein ajattelemattomuudesta tai ”pilan päin” syntyneet ideat ja palvelut saattavat vaikuttaa harmittomilta, saattaa niillä olla merkittävä vaikutus organisaation toimintaan tai sen julkisuuskuvaan.

Yksityishenkilöitä vastaan saatetaan hyökätä samalla tavalla, eli luomalla henkilön nimissä väärennetty profiili. Väärennetty profiili saattaa vaikuttaa hyvinkin aidolta jos väärentäjä on onnistunut keräämään riittävästi tietoa henkilöstä eri tietolähteistä.

Vakoilu ja tietojen kalastelu

Koska organisaatioiden henkilöstö usein käyttää sosiaalisen median palveluita, voi henkilön toiminta sosiaalisessa mediassa aiheuttaa riskejä sekä henkilölle itse että myös organisaation tietoturvallisuudelle. Erityisesti kalastelu on muodostunut merkittäväksi ongelmaksi. Käyttäjiä yritetään huijata paljastamaan tietoja itsestään tai työnantajastaan aidolta näyttävillä kyselyillä.

Sosiaalisen median palvelut tarjoavat helpomman tavan lähestyä käyttäjää, koska useat sosiaalisen median palvelut pohjautuvat avoimeen ja helposti lähestyttävään käyttötapaan. Henkilöstöä on koulutettu ja ohjeistettu olemaan lukematta ja avaamatta roskapostiviestejä tai muita epäilyttäviä linkkejä, mutta sosiaalisen median palveluissa ollaan usein varomattomampia, etenkin jos kutsu uuteen toiminnallisuuteen, palveluun tai palveluun liittyvän lisäosan asentamiseen tulee tutulta henkilöltä.

Perinteisten, sattumanvaraisten osoitelistojen sijaan suoritetaan kohdistettuja hyökkäyksiä, joiden uhrit voidaan poimia tehokkaasti käyttämällä sosiaalisen median palveluista kerättyjä tietoja.

> *Esimerkiksi keväällä 2010 Facebookissa yritettiin huijata käyttäjiä liittymään IKEA.com -sivuston faneiksi ja samalla paljastamaan suuren määrän henkilötietoja. 20 000 ensimmäiselle luvattiin tuhannen euron lahjakortti tunnettuun tavarataloon. Ongelma oli erityisen suuri Suomessa.*

Huijauksia saattaa olla mahdollista tunnistaa huolimattomasta toteutuksesta (esim. kielioppi- ja kirjoitusvirheistä), mutta asiantuntijakin saattaa langeta laadukkaasti toteutettu huijaukseen.

Sosiaaliset mediat tarjoavat yritysvakoilulle ja valtioille mahdollisuuden etsiä tarvitsemaansa tietoa ja yhdistää sitä muista lähteistä saatuihin tietoihin. Monet tutkimukset ovat osoittaneet, että ihmiset hyväksyvät helposti omaan verkostoonsa kontakteja (henkilöitä), joita he eivät tunne. Tämä yhdistettynä liialliseen luottamukseen, osaamattomuuteen ja huolimattomaan toimintaan on omiaan lisäämään organisaatioiden tietoturvariskejä.

Kontakteilla tarkoitetaan tässä esim. ystäviä, tuttuja tai muita henkilöitä tai yhteisöjä, joita palvelun käyttäjä on lisännyt palvelussa omaan verkostoon kuuluviksi, jolloin heillä on pääsy yksityiskohtaisempaan tietoon kuin muilla palvelun käyttäjillä. Jos kontaktien hyväksymisessä ei ole huolellinen, saattaa verkostoon soluttautua kontakteja, joita reaalimaailmassa ei välttämättä hyväksyisi kontakteikseen tai joita ei ole oikeasti olemassa. Tämä saattaa vaarantaa organisaation toimintaa sekä käyttäjän yksityisyyttä ja mainetta, jos soluttautuja käyttää hyväkseen verkostoa esim. vakoiluun, haittaohjelmien levittämiseen, virheellisen tiedon levittämiseen tai henkilötietojen anastamiseen.

Erään turvallisuustutkijan onnistui soluttautua Yhdysvaltojen sotilas- ja tiedusteluorganisaatioihin luomalla valeprofiilin Facebookiin, LinkedIn:iin ja Twitteriin sekä liittämällä siihen kuvan naisesta nimeltä ”Robin Sage”. Viikkojen sisään hänellä oli satoja ystäviä ja seuraajia Yhdysvaltain puolustushallinnosta, kansallisesta turvallisuusjärjestöstä NSA:sta, puolustusteollisuudesta sekä Iso-Britannian asevoimista. Hän onnistui verkostonsa kautta saamaan käsiinsä arkaluontoista tietoa, nimiä, osoitteita, pankkitilejä ja sähköposteja. Tämän lisäksi hän sai lukuisia esiintymiskutsuja. Valeprofiili sai myös kaveripyyntöjä senkin jälkeen, kun hänet oli paljastettu valheeksi.

2.2 Tekniset uhat

Merkittävimmät tekniset uhat ovat sovellushaavoittuvuudet, haittaohjelmat sekä roskapostit.

Sovellushaavoittuvuudet

Monet sekä palvelin- (server) että työasema- (client) sovellukset sisältävät haavoittuvuuksia, jotka mahdollistavat esim. käyttäjän koneen haltuunoton, haittaohjelmien levittämisen tai käyttäjän ohjaamisen saastuneille sivustoille.

Kilpailu ja tarjonta sosiaalisen median palveluissa kehittyvät nopeasti, mikä edellyttää nopeata palveluiden ja sovelluskehityksen tuotantomallia. Nopeatempoisessa sovelluskehityksessä tietoturvallisuus ja testaaminen yleensä kärsivät, jolloin palveluihin saattaa jäädä käytettävästä ohjelmointi tai sovelluspalvelinteknologiasta johtuvia haavoittuvuuksia.

Lisäksi selainohjelmistoissa ja niiden lisäohjelmistoissa saattaa esiintyä haavoittuvuuksia, jotka mahdollistavat edellä mainittujen riskien toteutumisen.

Lokakuussa 2010 julkaistiin uutinen Firefox-selaimen lisäosasta nimeltään Firesheep, joka kuuntelee verkkoliikennettä ja kaappaa sieltä sosiaalisen median palveluissa käytettäviä evästeitä mahdollistaen siten identiteettivarkaudet.

Haittaohjelmat

Koska sosiaalisen median palveluiden käyttäjämäärä kasvaa nopeasti, tarjoaa se väärinkäyttäjille otollisen alustan yrittää nopeasti levittää uusia haittaohjelmia mahdollisimman monen käyttäjän tietokoneisiin. Haittaohjelmariski koskee erityisesti sellaisia sosiaalisen median palveluita, joissa palvelun käyttäminen edellyttää www-selaimessa ohjelmakoodin suorittamista. Sen sijaan esim. pelkästä tekstisisällöstä koostuvat palvelut muodostavat pienemmän haittaohjelmariskin.

Sosiaalisessa mediassa haittaohjelmien levittäminen on helpompaa seuraavista syistä:

1. Mikäli henkilö saa viestin sosiaalisen median kautta ystävältään, työtoveriltaan tai muuten tutunoloiselta lähettäjältä, se saatetaan kuvitella turvallisemmaksi kuin suoraan sähköpostitse saapuva vastaavanlainen, muuten tietosisällöltään epäilyttävä viesti. Tämä koskee erityisesti yhteisöpalveluita

2. Useissa palveluissa viitataan uutisiin tai muihin keskusteluissa esillä oleviin asioihin käyttämällä url-osoitteen lyhennyspalveluita kuten bit.ly tai tinyurl.com. Näiden tarkoitus on säästää tilaa niissä sosiaalisen median palveluissa, joissa päivityksen merkkimäärä on rajoitettu (esim. Twitter). Haittapuolena on se että linkkiä napauttava ei pysty näkemään ennen osoitteessa vierailua, mihin osoitteeseen hänet johdatetaan. Tällöin on myös vaikea arvioida millaisia mahdollisia haittaohjelmia kyseiseltä www-sivulta yritetään koneelle upottaa
    - On myös huomattava että url-osoitteen lyhennyspalvelun luotettavuuteen tulee kiinnittää huomiota. Väärinkäyttäjä voi muuttaa aiemmin turvallisen ja oikean linkin ohjautumaan haitalliseen osoitteeseen.

3. Sosiaalisen median palveluntarjoaja ei välttämättä ole kiinnittänyt tarpeeksi huomiota oman palvelun tietoturvallisuuteen ja palvelussa voi olla tietoturva-aukkoja, jotka mahdollistavat käyttäjän koneen saastuttamisen.

4. Perinteisten haittaohjelmien rinnalle on noussut kokonaan uusi uhka, joka on käytetyimpien sosiaalisen median palveluita taidokkaasti hyödyntävät haittaohjelmat. Niiden tarkoituksena on ohjata käyttäjä hyökkääjän ylläpitämään palveluun käyttäen hyväksi henkilön luottamusta omaan verkostoon.

Organisaation maine saattaa kärsiä merkittävän kolauksen, jos käy ilmi, että sen palvelun kautta on ohjattu käyttäjiä haittaohjelmasivuille tai että organisaation tuottamaan palveluun on saatu upotettua haittaohjelma.

Url-lyhennyspalvelut mahdollistavat pitkien tai muuten hankalasti muistettavien linkkien tallentamisen lyhemmiksi, helpommin muistettaviksi url-osoitteiksi.

Roskaposti

Roskaposti on muodostunut ongelmalliseksi myös sosiaalisen median palveluissa. Ominaista sosiaalisen median palveluiden kautta välitetyistä roskaposteista on hakukoneiden mahdollistama roskapostien kohdentaminen tietyille käyttäjäryhmille tai suosittujen sivustojen tai ryhmien hyödyntäminen viestien lähettämiseen. Viestit saattavat sisältää linkkejä esim. tuotemyyntisivustoille tai pornograafisiin sivustoihin. Roskapostin estäminen on usein hankalaa vaikka monella palveluntarjoajalla tarjoaa raportointimahdollisuuden: roskapostittajat tyypillisesti vaihtavat lähdeosoitettaan säännöllisesti.

Sosiaalisen median palvelut tarjoavat esimerkiksi satunnaista roskapostitusta tehokkaamman ja nopeamman tavan yrittää huijata rahaa. Syksyllä 2010 Facebook-verkkopalvelussa levisi viesti, josta ”pitämällä” (like) huijausviesti pääsee käsiksi käyttäjän profiilitietoihin ja mm. saa selville käyttäjän mahdollisen matkapuhelinnumeron. Huijauksen seurauksena käyttäjän matkapuhelinlaskuun saattaa tulla 19 € lisämaksu ylimääräisestä palvelusta.

2.3. Muut uhkakuvat

Palveluiden epäselvät ja/tai muuttuvat sopimusehdot

Organisaation tulisi sosiaalisen median palveluita käyttöön ottaessaan lukea ja seurata huolellisesti palvelun käyttöön liittyviä sopimus- ja palveluehtoja. Useissa palveluissa keskeinen haaste on toimittajan ja palvelun sijainti pelkästään ulkomailla, jolloin palvelun tarjoaja ei ole halukas muuttamaan sopimusta pienen ulkomaisen asiakkaan toiveiden vuoksi. Ulkomailla sijaitsevien sosiaalisen median palvelujen tarjoajat eivät ole Suomen lainsäädännön piirissä, jolloin sopimusehtojen lisäksi noudatettavat lainsäädännön vaatimukset voivat poiketa merkittävästi Suomessa totutuista. Suomalaisilla viranomaisilla ei esim. ole automaattisesti toimivaltaa poistaa laitonta aineistoa ulkomaisesta palvelusta.

Tärkeä huomioon otettava seikka koskee sitä, millaiset oikeudet palvelua ylläpitävä toimittaja saa asiakkaan palveluun tallentamaan tietoon. Pahimmillaan toimittaja pidättää itsellään kaikki oikeudet, mikä mahdollistaa tietojen levittämisen ja edelleen välittämisen tai myymisen myös kolmansille osapuolille.

> *Ote erään suositun sosiaalisen median palvelun palvelusopimuksesta: "License and warrant your submissions: You do not have to submit anything to us, but if you choose to submit something (including any User generated content, ideas, concepts, techniques and data), you must grant, and you actually grant by concluding this Agreement, a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicenseable, fully paid up and royaltyfree right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, and use and commercialize, in any way now known or in the future discovered, anything that you submit to us, without any further consent, notice and/or compensation to you or to any third parties…".*

Monet suositut sosiaalisen median palvelut on tarkoitettu ainoastaan yksityishenkilöiden käyttöön, jolloin niiden käyttäjäehdoissa asetetut velvoitteet ja vastuut voivat olla ristiriidassa käyttäjän oman organisaation sääntöjen kanssa. Käyttäjä voidaan velvoittaa esim. puolustamaan palveluntarjoajaa ulkopuolisten tahojen, kuten käyttäjän oman organisaation, oikeusvaatimuksia vastaan.

Palvelun ja tietoaineistojen sijaintiin ja tietoturvallisuuden tilaan liittyvät epäselvyydet

Sosiaalisen median palveluissa, kuten muissakin Internet-palveluissa, yleistyvät jaettua kapasiteettia eli palvelinvirtualisointia ja pilvipalvelua (cloud computing) hyödyntävät tuotantomallit. Näiden mallien suurimpia haasteita ovat tietoaineistojen sijaintiin liittyvät kysymykset, palveluiden käytettävyys nor-

maaliolojen häiriötilanteissa sekä epätietoisuus palvelun tietoturvallisuuden todellisesta tilasta.

Sosiaalisen median palveluun siirretty tieto saattaa sijaita maassa, jonka lainsäädäntö tietoturvaan tai tietosuojaan liittyvissä asioissa poikkeaa merkittävästi Suomen lainsäädännöstä. Joissain tapauksissa (esim. henkilötiedot) Suomen lainsäädäntö rajoittaa tietoaineiston siirtoa maahan, jossa tietosuoja- tai tietoturvasäännökset ovat Suomen tasoa heikompia. Mahdolliset ristiriitatilanteet ratkotaan useimmiten palvelun tarjoajan toimintamaan oikeudessa ja kyseessä olevan maan lainsäädännön mukaisesti. Lisätietoja löytyy tietosuojavaltuutetun toimiston www-sivuilta (kts. Liite 3: Lähteet).

Mikäli palvelu sijaitsee kokonaisuudessaan Suomen ulkopuolella, se ei ole käytettävissä kansainvälisten tietoliikenneyhteyksien ollessa poikki. Koska sosiaalisen median palvelut eivät tyypillisesti ole kriittisiä organisaation toiminnalle, tämän ei pitäisi muodostua ongelmaksi. Kuitenkin uusien, etenkin ryhmätyö- ja viestintäpalveluiden yleistyessä saattaa näiden palveluiden kriittisyysluokka nousta korkeammaksi kuin perinteisten sosiaalisen median palveluiden. Tämä tulee ottaa huomioon palveluiden jatkuvuus- ja toipumissuunnittelussa ja tarvittaessa suunnitella riittävät varajärjestelyt.

Lisäksi on otettava huomioon, että ulkomailla sijaitsevan palveluntarjoajan tietoturvallisuutta on yleensä mahdotonta tarkistaa (auditoida). Sosiaalisen median palvelun käyttöön ottaminen on tällöin aina riski.

Henkilöturvallisuus

Jotkut henkilöt kertovat hyvin avoimesti tietoja itsestään ja omasta elämästään sosiaalisen median palveluissa. Osa palveluista on rakennettu siten, että hakukoneet, esimerkiksi Google, pystyvät hakemaan henkilöön liittyviä tietoja omaan tietokantaansa, jolloin tiedot ovat julkisesti löydettävissä ja nähtävissä. Henkilöön liittyvien tietojen joutuminen vääriin käsiin saattaa pahimmassa tapauksessa aiheuttaa henkilölle ja hänen lähipiirilleen fyysistä uhkaa.

> *Erään tietoturvayrityksen johtaja kertoi, että ei käytä vapaa-ajan yhteisöpalveluita oman ja perheensä fyysisen turvallisuutensa takia. Tietoturvayrityksen toiminta hankaloittaa ammattirikollisten liiketoimintaa, mikä saattaa asettaa kyseisen henkilön fyysiseen vaaraan. Riskiä ei kannata suurentaa paljastamalla itsestään liian paljon tietoja Internetissä ja erityisesti sosiaalisen median palveluissa.*

Henkilön elämään voi myös päästä vaikuttamaan kiusaamalla tai uhkailemassa sosiaalisen median kautta. Esimerkiksi väärennetyn profiiliin avulla väärinkäyttäjä pystyy kirjoittamaan kohteestaan perättömiä tai valheellisia viestejä sekä julkaisemaan muuta sellaista tietoa, mikä aikaisemmin olisi ollut

hankalampaa. Henkilöön kohdistuva epäasiallinen käytös saattaa häiritä sekä työtehtävää että henkilön hyvinvointia laajemminkin.

Sosiaalisiin medioihin liittyy myös muita henkilöä tai organisaation ja/tai henkilön omaisuutta koskevia väärinkäyttömahdollisuuksia. Seuraamalla henkilön sosiaalisen verkostoon tuottamia viestejä ja tilatietojen päivityksiä, voidaan yrittää päätellä, missä ja milloin henkilö on ja kenen muiden henkilöiden seurassa.

Ongelma pahenee entisestään, jos viesteihin, materiaaliin tai tilatietojen päivityksessä hyödynnetään paikkatietoja. Uudet teknologiat, päätelaitteet ja palvelut hyödyntävät gps- ja 3G-laitteiden kautta myös matkapuhelinverkkojen tarjoamaa a-gps-teknologiaa, joka mahdollistaa päätelaitteen paikallistamisen muutaman metrin tarkkuudella. Tämän ohella toisena keinona paikantamiseen on tullut wlan-tukiasemapaikannus, jota voidaan käyttää myös ilman gps-ominaisuutta. Samoja teknologioita tullaan hyödyntämään myös muissa elektroniikkalaitteissa ja digikameroissa, joten paikkatiedoista on tulossa yksi uusi de facto -ominaisuus päätelaitteisiin. Tämä tulisi ottaa huomioon sosiaalisen median palveluiden ohella muissa tietojärjestelmissä ja tietoaineistoissa ja huolehtia siitä, että organisaatio ei paljasta suotta käyttäjiin tai asiakirjoihin liittyviä paikkatietoja esimerkiksi tietoaineistojen metatiedoissa. Paikkatiedot mahdollistavat sekä asiakirjan että henkilöiden paikantamisen ja tämä tulisi huomioida riskien arvioinnissa.

Internetissä pyöri jonkin aikaan verkkosivu PleaseRobMe, joka keräsi Twitteriin ilmoitetut lomailmoitukset ja julkaisi ne keskitetysti. Verkkosivuston tarkoitus oli huumorimielessä herättää ihmisiä ilmiselvään ongelmaan, mutta ikävä tosiasia on, että murtovarkaat ovat hyödyntäneet sosiaalisen median palveluissa paljastettuja poissaolotietoja selvittääkseen tyhjillään olevia kotitalouksia. Murtovarkaita helpottavat lisäksi erilaiset karttapalvelut, joilla potentiaalisia kohteita voidaan etsiä ja parhaan tarkkuuden omaavilla karttapalveluilla voidaan jopa selvittää kohteessa käytössä olevia hälytys- tai muita turvajärjestelmiä.

Yksityisyyden suoja

Sosiaalisen median palveluita kehitettäessä ei käyttäjien yksityisyyden suoja ole ollut pääasia. Päinvastoin, monen sosiaalisen median palvelun liiketoimintamalli perustuu siihen, että käyttäjien tiedot ovat mahdollisimman julkisia. Samaan aikaan sosiaalinen normi yksityisyydestä on muuttumassa ja julkisen ja yksityisen välinen raja on hämärtymässä. Sosiaaliset mediat ovat ilmiönä niin uusi, että niihin ei ole osattu vielä suhtautua järkiperäisesti; erityisesti yksityisyyteen liittyvät asiat tulevat ajankohtaisiksi vasta siinä vaiheessa, kun usein on liian myöhäistä.

Esimerkkinä mainittakoon kuuluisaksi muodostunut tapaus, josta uutisoitiin laajasti kesällä 2009 Iso-Britanniassa. Tapaus koski Facebookissa olevaa sivustoa, joka aiheutti kansallisen turvallisuusriskin. Maan tiedustelupalvelun (MI6) johtajan vaimo kertoi avoimesti Facebook –sivustollaan hyvinkin henkilökohtaisia asioita perheestään, julkaisi valokuvia sekä paljasti kotiosoitteensa. Viattomalta vaikuttava sivusto oli kuitenkin kaikkien lontoolaisten verkostoon kuuluville avoin. Tilanne aiheutti riskin niin valtiotasolla kuin perheellekin.

Vaikka käyttäjä kuvittelee tekevänsä kaiken omasta mielestään oikein ja laittaa päälle keskeiset yksityisyyden suojaa koskevat asetukset ja noudattaa parhaita käytäntöjä palveluita käyttäessään, mikään ei takaa sitä, ettei joku toinen hänen verkostossaan oleva henkilö aiheuta omalla tahattomalla toiminnallaan ongelmia, jotka johtavat käyttäjän omien tietojen leviämiseen. Erityisesti valokuvat ja niiden ”taggaus” saattavat muodostaa käyttäjästä kattavan profiilin. Lisäksi valokuvien taustoilla näkyvät muut yksityiskohdat, kuten autojen rekisteritunnukset, talonumerot jne. yhdistettynä paikkatietoon paljastavat käyttäjästä yllättävän paljon. Myös sovelluskehityksessä tapahtuvat viat saattavat paljastaa käyttäjien henkilökohtaisia tietoja, eivätkä tiedot sen jälkeen ole enää helposti poistettavissa, mikäli ne ovat ehtineet levitä Internetissä.

Kevennys: Täysin turvallisia sosiaaliset mediat eivät onneksi ole rikollisillekaan. Keväällä 2010 Italian poliisi sai kiinni henkilön, jota syytetään useista murhista, huumerikoksista ja yhteydestä mafiaan. Henkilön piilopaikka jäljitettiin hänen Facebookin selaamiseen käyttämän 3G-mokkulayhteyden avulla.

Maineen hallinta

Myös organisaatioon kohdistuu joitain samanlaisia uhkia kuin yksittäiseen henkilöön. Yhä useammassa palvelussa arvioidaan kaupallisten yritysten ja kauppaliikkeiden sekä palveluiden mainetta sekä muuta toimivuutta. Tällaisten arviointien toimintaan voidaan yrittää vaikuttaa väärennettyjen käyttäjäprofiilien avulla. Vaikka jokin organisaatio tai toimittaja, liike tai palvelu olisi saanut hyvät arvosanat jossakin palvelussa, on siihen voitu vaikuttaa valheellisilla arvosteluilla, jos arvostelijoiden määrä on pieni.

Valtaosa julkisista sosiaalisen median palveluista rahoittaa toimintaansa mainoksilla. Organisaatio ei voi vaikuttaa siihen, millaisia mainoksia heidän yhteisö- tai verkkopalvelunsivuillaan esitetään. Organisaation uskottavuus saattaa heikentyä, jos sen sosiaalisen median palvelusivuilla mainostetaan jotain sellaista, joka ei sovi organisaation imagoon.

Organisaation maineen mustaamisen ohella väärennettyjen tai kaapattujen profiilien avulla on myös mahdollista hyökätä yksittäistä käyttäjää vastaan.

Pahimmillaan tällainen omasta verkostosta suuntautuva mustamaalaus saattaa näyttää ulkopuolisesta erittäin uskottavalta ja menetetyn maineen palauttamiseen kuluu aikaa tai maineen palauttaminen on mahdotonta.

Lisäksi organisaation mainetta ja uskottavuutta saattavat haitata työntekijöiden varomattomasti esittämät mielipiteet tai väärät tiedot, erityisesti jos ei ole ilmiselvää, että kerrottu ”tieto” tai esitetty mielipide on henkilön oma eikä organisaation virallinen kanta. Pahimmassa tapauksessa organisaatio saattaa joutua juridiseen ja taloudelliseen vastuuseen työntekijän julkaisemasta asiasta.

”Öisin vapaa-ajan viestejä lähettävä työntekijä Taavi Tavallinen” on tapauksena hyvinkin erilainen kuin ”öisin vapaa-ajan viestejä lähettävä yksityishenkilö Taavi Tavallinen”. Mikäli Taavi ehdottomasti haluaa lähettää kavereilleen huomiota herättäviä viestejä öisin, tulee Taavin selvästi harkita, mitä hän julkaisee, missä hän julkaisee ja kenelle hän julkaisee. Vaikka Taavi esiintyykin yksityishenkilönä, häntä koskevat edelleen työntekijään liittyvät velvollisuudet.

3 Tietoturvallisuuden toteuttaminen palveluita käytettäessä

Sosiaalisen median palveluiden käyttö tulee arvioida niiden kautta saatujen hyötyjen perusteella tasapainotettuna mahdollisiin riskeihin. Riskienhallinta tulisi toimia keskeisenä osana palveluiden käyttöä suunniteltaessa. Lähtökohta on, että organisaatiolla on selkeä tavoite sosiaalisen median hyödyntämisessä sekä riittävästi resursseja tavoitteen saavuttamiseksi. Sosiaalisen median palveluiden ohjeistaminen tulee olla linjassa organisaation tietoturvapolitiikan kanssa. On suositeltavaa, että organisaatio laatii sosiaalisen median käyttöpolitiikan, joka ohjaa sekä organisaation että henkilöstön toimintaa sosiaalisen median palveluiden käytössä.

Palveluita käytettäessä tulee määrittää palveluissa sallitut verkkoidentiteetit. Verkkoidentiteettejä on kolmenlaisia:

1. Organisaatiotunnus: palveluun kirjaudutaan roolipohjaisella (sähköposti)tunnuksella tai organisaation tarjoamalla, henkilökohtaisella (sähköposti)tunnuksella. Palvelun käyttäjä edustaa organisaatiotaan.

   Organisaation sosiaalisen median palvelua päivittävät henkilöt kirjautuvat palveluun organisaation henkilökohtaista sähköpostitunnusta (etu.suku@organisaatio.fi) tai roolipohjaista tunnusta (tiedottaja@organisaatio.fi) käyttäen. Tällöin työnantajalla on täysi oikeus määrätä, mitä tällaisella tunnuksella voidaan tehdä ja millaisiin keskusteluihin sillä voidaan osallistua.

2. Hybridi: palveluun kirjaudutaan joko organisaation tarjoamalla henkilökohtaisella (sähköposti)tunnuksella tai omalla yksityisellä (sähköposti) tunnuksella. Palvelun käyttäjä mainitsee työnantajansa, mutta toimii palvelussa asiantuntijaroolissa yksityishenkilönä.

   LinkedIn on ammattimaiseen verkostoitumiseen tarkoitettu yhteisöpalvelu, jota verkostoitumisen lisäksi hyödynnetään oman osaamisen kehit-

tämiseen seuraamalla omien verkostojensa ja ryhmiensä viestejä ja keskusteluja. Käyttö perustuu kuitenkin harvoin organisaation suositukseen hyödyntää palvelua; tunnuksen luominen ja ylläpito on perustunut henkilön omatoimiseen päätökseen ottaa palvelu käyttöön. Osa palvelua käyttävistä kirjautuu palveluun organisaation sähköpostitunnuksella ja osa vapaa-ajan tunnuksella. Työnantajan mahdollisuus ohjeistaa hybridinomainen osallistuminen on hyvin rajattu. Organisaation tarjoaman sähköpostitunnuksen käyttö voidaan halutessaan kieltää ja työntekijää sitoo edelleen työntekijään liittyvät velvoitteet, mutta muilta osin henkilön toiminta sosiaalisen median palvelussa on henkilön itse päätettävissä oleva asia.

3. Täysin yksityinen identiteetti: palveluun kirjaudutaan omalla henkilökohtaisella (sähköposti)tunnuksella. Palvelun käyttäjä toimii täysin yksityishenkilönä.

   Työntekijää koskettaa edelleen työntekijän velvoitteet (esim. virkavelvoite), mutta työnantajalla ei ole oikeutta sanella työntekijän vapaa-ajan toimintaa sosiaalisen median palvelussa. On kuitenkin myönteistä, jos organisaation tietoturvaohjeistus tukee henkilöä toiminaan tietoturvallisesti myös vapaa-ajan toiminnoissaan.

3.1 Yleistä - sosiaalisen median käyttöpolitiikka

Käyttöpolitiikassa tulee ottaa kantaa yleisiin sosiaaliseen mediaan liittyviin menettelyihin sekä organisaation että henkilöstön osalta. On suositeltavaa, että sosiaalisen median tietoturvallisuuteen liittyvät linjaukset liitetään osaksi organisaation sosiaalisen median käyttöpolitiikkaa.

Keskeinen kysymys on myös organisaation suhtautuminen sosiaalisen median palveluiden käyttöön työpaikalta ja työaikana. Organisaation tulee linjata, sallitaanko minkä tahansa sosiaalisen median palvelun käyttö vai rajataanko käyttö vain ammattimaiseen toimintaan. Kysymys liittyy sekä henkilöstöhallintoon (työajan käyttö) että tietohallintoon (työnantajan tietohallintopalveluiden käyttö), mutta sillä saattaa olla myös turvallisuuteen liittyviä vaikutuksia.

Käyttöpolitiikassa tulee määritellä:

1. Mitä organisaation ydintoimintaa liittyvää tehtävää sosiaaliseen mediaan osallistuminen tukee? Mikä on sosiaalisen median käytön tavoite?
2. Mitä sosiaalisen median palveluita otetaan käyttöön, ylläpidetään ja seurataan?

    1. Kuka päättää käyttöönotosta?
    2. Kuka vastaa osallistumisesta ja palveluiden ylläpidosta?
    3. Kuka seuraa palvelusopimusten muutoksia ja arvioi organisaation käytön jatkuvuuden?
    4. Miten työvälineet, käyttö, läsnäolo ja seuranta resursoidaan ja toteutetaan? Mistä ja millä laitteilla?
    5. Millä tavoin henkilöstö osallistuu palvelun toimintaan? Kuka vastaa ja kommentoi sosiaalisessa mediassa käytävää, organisaatiota koskevaa keskustelua? Mitkä ovat käytettävät verkkoidentiteetit?
3. Sosiaalisen median käyttö työpaikalta
    1. On/ei ole suositeltavaa?
    2. On mahdollistettu/rajoitettu/estetty työpaikalta
4. Sosiaalisen median käytön koulutus
    1. Sisällöntuottajille
    2. Ylläpitäjille
    3. Henkilöstölle
5. Tietoturvallisuus
    1. Riskien hallinta
        1) Kuka vastaa riskien arvioimisesta, toimenpiteiden suunnittelusta ja tietoturvallisuuden seurannasta?
        2) Kuinka usein riskejä arvioidaan?
    2. Tietoaineistojen suojaaminen
        1) Miten varmistetaan, että salassa pidettävä tieto ei vuoda sosiaaliseen mediaan?
        2) Miten hallitaan oikeudet palveluun tallennettaviin tietoaineistoihin?
    3. Tietojenkäsittely-ympäristöjen suojaaminen
        1) Jos sosiaalisen median palvelua käytetään työpaikalta, mitä saa ja ei saa tehdä?
        2) Miten estetään haittaohjelmien leviäminen organisaation tietojenkäsittely-ympäristöön?
        3) Millaisia teknisiä ratkaisuja löytyy sosiaalisen median palveluiden tietoturvallisen käytön parantamiseksi?
    4. Maineen hallinta
        1) Mikä on asiallista käytöstä sosiaalisessa mediassa?
        2) Miten reagoidaan valeprofiileihin ja tunnuksiin tai jos organisaation tunnuksia kaapataan?
    5. Henkilöturvallisuus
        1) Miten reagoidaan häirintään ja uhkailuun?
    6. Yksityisyyden suoja

Liitteessä 2 on käyttöpolitiikan malliesimerkki, jossa määritellään organisaation kannanotto sosiaalisen median palveluiden käytön suhteen

3.2 Ohjeistus ja koulutus

Ohjeistus ja koulutus ovat keskeisessä asemassa sosiaalisen median käytön yleistyessä ja käyttökulttuurin kehittyessä. Ohjeistusta ja koulutusta on annettava koko henkilöstölle, koska henkilöstö saattaa käyttää sosiaalista mediaa yksityishenkilöinä riippumatta siitä, esiintyykö työnantaja sosiaalisessa mediassa vai ei. Mikäli organisaatio itse tarjoaa tai käyttää sosiaalisen median palveluita, ohjeistusta tulee antaa siitä, miten henkilöstön tulee toimia organisaation edustajana kyseisissä palveluissa. Ohjeistuksen tulee perustua organisaation hyväksyttyyn käyttöpolitiikkaan.

Ohjeissa ja koulutuksissa on tehtävä selväksi se, missä määrin organisaation asioita saa käsitellä sosiaalisessa mediassa. Esimerkiksi organisaation hallussa olevia salassa pidettäviä tietoja ja yrityssalaisuuksia ei tule käsitellä sosiaalisessa mediassa millään tavalla.

> *Ei ole sallittua, että työntekijä päivittelee sosiaalisessa mediassa kavereilleen, kuinka on osallistumassa miljoonan euron suuruiseen hankkeeseen, jonka kilpailutukseen osallistuvat yritykset X, Y ja Z.*

> *Kertominen osallistumisesta julkiseen seminaariin tuskin vaarantaa organisaation tietoturvallisuutta, esimerkiksi: "Terveisiä Ateenasta, jossa osallistun mielenkiintoiseen seminaariin. Aurinko paistaa ja esityksetkin ovat hyviä!"*

Organisaation ohjeistuksessa ja koulutuksessa tulisi neuvoa, miten henkilö voi erottaa esiintymisen yksityishenkilönä tai työntekijänä (esim. virkamiehenä). Ensisijainen ohje on, että henkilöstö käyttää harkintaa keskustellessaan vapaa-ajan sosiaalisen median palveluissa työpaikkaansa liittyvistä asioista eikä esim. julkaise tai käytä työpaikan sähköpostiosoitetta. Tämä on tärkeää, koska osa palveluista edelleen välittää ja myy sähköpostiosoitteita kolmansille osapuolille. Ongelmaksi voi muodostua myös se, että henkilön vaihtaessa työnantajaa, hänen saattaa olla hankala muistaa lopettaa, perua tai vaihtaa sähköpostiosoitetta kaikkiin niihin palveluihin, joissa hän on käyttänyt työnantajan sähköpostiosoitetta.

Ohjeistuksessa ja koulutuksessa tulee käydä läpi keskeiset käyttöpolitiikassa määritellyt asiat sekä kiinnittää huomiota esim. seuraaviin asioihin:

- Verkkoidentiteettien käyttäminen
- Mitä organisaatioon toimintaan liittyvää saa kertoa ja mitä ei?
- Mitkä ovat yleiset käyttäytymissäännöt?
- Suositukset liittyen palveluiden yksityisyysasetuksiin (privacy settings)
- Käyttöehtojen lukemisen tärkeys

- Salasanaturvallisuus
  - Hyvän salasanan luominen
  - Eri salasanojen käyttö eri palveluissa
- Suositus etsiä hakukoneilla omalla nimellä mahdollisten identiteettivarkauksien löytämiseksi
- Kehotus huolellisuuteen verkostoiduttaessa ja kontaktien hyväksymisessä
- Kehotus varomaan haittaohjelmia
- Kehotus olemaan varuillaan kun napsuttelee lyhennettyjä url-osoitteita
- Tiedota kalasteluviestien yleispiirteistä ja kehota olla vastaamatta niihin
- Kerro kolmannen osapuolen sovelluksista ja niiden riskeistä, kehotus käyttämään harkintaa

Henkilöstön on hyvä tiedostaa ne tilanteet, jolloin työroolia on syytä olla mainitsematta, koska paljastuminen saattaisi vaarantaa hänen tehtävänsä tai turvallisuutensa.

Esimerkiksi terveydenhuolto- tai muilla palvelualoilla toimivien tulee harkita, miten suhtautua asiakkaiden kanssa verkostoitumiseen yksityisprofiilin kautta.

On suositeltavaa, että sosiaalinen media otetaan mukaan henkilöstölle suunnattuun tietoturvallisuus-koulutukseen. Esimerkiksi verkkopohjaisiin oppimisympäristöihin on helppo tuottaa osio sosiaalisesta mediasta osana muuta tietoturvallisuuskoulutusta.

Liitteessä 1 on ”Käyttäjän 10 ohjetta”, jotka voidaan tarvittaessa purkaa auki ja syventää

3.3 Tietoaineistoturvallisuus

Tietoaineistojen suojaamisessa lähtökohtana on, että sosiaalisen median palveluun ei tule laittaa muuta kuin julkista tietoa. On myös otettava huomioon, että yksittäiset julkiset tiedot saattavat muodostaa kokonaisuuden, joka ei ole enää julkinen. Näin ollen organisaatioiden tulee määritellä käyttöpolitiikassaan se, ketkä saavat julkaista organisaatioon liittyviä tietoja sosiaaliseen mediaan sekä mitä tietoja ja mihin palveluihin niitä julkaistaan.

Mikäli organisaation tavoitteena on tarjota sellaisia sosiaalisen median palveluita, joissa on tarkoitus tallentaa salassa pidettäviä tietoaineistoja, tulee kiinnittää huomiota käytettävän teknisen ympäristön toteutustavan valintaan. Sosiaalisen median palvelua tulee kehittää kuten mitä tahansa palvelua ja huolehtia tietoturvallisuuden ottamisesta huomioon kokonaisvaltaisesti hankkeen koko elinkaaren ajan.

Jos sosiaalisessa mediassa käytävä keskustelu muuttuu julkisesta salassa pidettäväksi, pitää se siirtää riittävän suojaustason omaavaan palveluun. Käyttäjille tulee lisäksi tiedottaa mihin käyttötarkoitukseen sosiaalisen median palvelu on tarkoitettu ja ohjata muu asiointi asianmukaisesti.

Tallennettaessa tietoja organisaation ulkopuoliseen palveluun tulisi ohjeistaa, miten tietoaineistoista voidaan poistaa siihen tallentuneet metatiedot.

3.4 Tekniset ratkaisut

Jos sosiaalisen median palveluita käytetään organisaation välineillä ja/tai organisaation tietojenkäsittely-ympäristöistä, tulee käytettävät työvälineet ja tietojenkäsittely-ympäristöt suojata asianmukaisin teknisin keinoin.

Tietojenkäsittely-ympäristön tietoturvallisuusrakenteiden tulee perustua muun muassa seuraaviin vaatimuksiin:

- 621/1999 Laki viranomaisen toiminnan julkisuudesta
- 681/2010 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa
- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010
- Sisäverkko-ohje, VAHTI 3/2010
- muut VAHTI-ohjeet soveltuvin osin

3.5 Muut ratkaisut

Palveluiden sopimusehdot

Liityttäessä sosiaalisen median palveluiden käyttäjäksi organisaatio sitoutuu noudattamaan palvelun tarjoajan laatimaa palvelusopimusta. Palvelusopimuksessa määritellään käytön ehdot, palveluun tuotetun sisällön omistajuus sekä palvelun tarjoajan oikeudet sisältöön, palvelun tarjoajan oikeudet muuttaa palvelusopimusta, ja niin edelleen. Sosiaalisen median palveluiden sopimusehtoihin tulee perehtyä huolellisesti etukäteen ja niiden muutoksia tulee seurata ja arvioida organisaation kannalta jatkuvasti.

Immateriaalioikeuksiin liittyviin seikkoihin tulee perehtyä huolellisesti ennen kuin tuottaa palveluun sisältöä. Monet suositut sosiaalisen median palvelut edellyttävät, että käyttäjä luovuttaa palvelun tarjoajalle oikeudet kopioida, muuttaa, julkaista, poistaa ja kaupallistaa palveluun tuotetut tiedot ilman käyttäjän suostumusta tai edes että käyttäjä on asiasta tietoinen.

Sopimuksia hyväksyttäessä tulee huomioida myös mitä organisaation tiedoille tapahtuu kun sopimus umpeutuu eikä palvelun käyttöä haluta enää jat-

kaa tai mitä tiedoille tapahtuu jos palveluntarjoaja päättää lopettaa palvelun tarjoamisen.

Henkilöturvallisuus

Henkilön toimiessa organisaation kannalta sellaisessa tehtävässä, että hänen läsnäolonsa sosiaalisen median palvelussa on syytä harkita (tai vähintään rajoittaa täysin yksityiseen käyttöön), on suositeltavaa, että henkilö kehottaa perheenjäseniään ja ystäviään huolellisuuteen. Tulee harkita, kannattaako esim. perheen koti- ja lomatietoja kuvineen julkistaa ja olla erityisen tarkkana yksityisasetuksista sekä perusteista, ketkä hyväksyy verkostoonsa. Mitä paremmin työntekijän merkittävä rooli tai asema on julkisesti tiedossa, sitä suurempi vaara on siinä, että hänen identiteettiään vastaan suunnataan kohdistettu hyökkäys.

Organisaation on varauduttava sosiaalisen median palveluiden kautta tapahtuvaan kiusaamiseen tai uhkailuun. Mahdolliset kiusaamistapaukset voivat olla hyvin henkilökohtaisia, esim. työntekijän aiempien kiusaajien toteuttamia tai kasvottomia herjauksia tai uhkauksia. Työntekijällä tulee olla selkeät ohjeet miten toimia, jos kokee netissä kiusaamista tai uhkailuja. Perusohjeena on, että organisaatio ryhtyy välittömästi käyttöpolitiikan mukaisiin toimenpiteisiin esim. käyttäen palvelun tarjoamia mahdollisuuksia (esim. uhkaajan käyttäjätilin lukitseminen). Asiasta tulee tehdä tarvittaessa rikosilmoitus. Sosiaalisessa mediassa kannattaa myös mainita, että organisaatio ei hyväksy henkilöstöönsä kohdistuvaa kiusaamista tai uhkailua ja ryhtyy asianmukaisiin toimenpiteisiin, mikäli kiusaamista tai uhkailua esiintyy.

Yksityisyyden suoja

Yksityisyyden suoja on usein jätetty sosiaalisen median palvelun käyttäjän vastuulle. Tämän takia käyttäjän tulee heti rekisteröitymisen jälkeen muuttaa yksityisyyden suoja-asetukset halutulle tasolle.

Henkilöstöä voi ohjeistaa huolehtimaan yksityisyyden suojastaan esim. seuraavilla seikoilla:

1. Identiteettivarkauksien hankaloittamiseksi kannattaa tutustua tarkkaan käytettävän palvelun tarjoamiin yksityisyyden suoja-asetuksiin ja useimmissa tapauksissa säätää ne oletusasetuksia tiukemmiksi
2. Julkiset sosiaalisen median palvelut sisältävät erilaisia mekanismeja unohdetun salasanan palauttamiseen. Tulee miettiä tarkkaan, millaisia keinoja sallii salasanan palauttamiseksi. Esimerkiksi salasanan palauttamisen mahdollistavassa menetelmässä pitää välttää kysymyksiä tyyliin ”Mikä on lemmikkisi nimi?”, koska vastaus saattaa löytyä suoraan

henkilön palvelussa kertomista tiedoista. Suositeltavampaa on käyttää salasanan palauttamista lähettämällä sen muuttamisen mahdollistava linkki käyttäjän oletussähköpostiosoitteeseen.

3. Tulee miettiä, kannattaako esim. omaa syntymäaikaa, -paikkaa ja muita osoitetietoja kertoa, koska todennäköisesti ne henkilöt, jotka kyseisiä tietoja tarvitsevat, tietävät ne muutenkin
4. Sosiaalisen median palveluihin kerrottavaa tietoa kannattaa harkita kuten suunniteltaessa työaseman vakiointia ja ohjelmistokannan minimointia (eli sallia työasemassa käytettäväksi vain ne sovellukset joita tarvitaan); sosiaalisen median palvelussa kerrotaan vain se, mikä on välttämätöntä palvelun toiminnan kannalta
5. Valokuvia julkaistaessa kannattaa kiinnittää huomio kuviin mahdollisesti liitettyihin paikkatietoihin.

Kaikista varotoimenpiteistä huolimatta sosiaaliseen mediaan tallentamat tiedot voivat päätyä kolmansien osapuolien haltuun tai levitä hallitsemattomasti muissa Internetin palveluissa.

Maineen hallinta

Organisaatio voi vaikuttaa maineen hallintaan liittyviin uhkiin toimimalla itse aktiivisesti sosiaalisessa mediassa ja tarjoamalla omassa profiilissa oikeaa informaatiota proaktiivisesti tai reaktiivisesti kommentoimalla ja korjaamalla muualla esiintyvää väärää tietoa. On kuitenkin oltava huolellinen, missä tilanteessa ja missä määrin ja millä asenteella korjaa itseään koskevaa tietoa. Keskustelukanavaa saatetaan helposti mieltää ”yksityiseksi”, jolloin esim. viranomaisen läsnäoloa viranomaisena ei pidetä toivottuna.

Mikäli sosiaalisen median palveluita otetaan käyttöön, tulee varata riittävästi resursseja asianmukaiseen läsnäoloon. Palvelun ylläpidon on oltava säännöllistä ja jatkuvaa. Tämä edellyttää uusien, pitkäjänteisen toiminnan edellyttämien toimintakulttuurien, prosessien ja henkilöstörakenteiden luomista. Esimerkkinä mainittakoon virkatöiden sovittamineen sosiaalisen median nopeaan ja erityistilanteissa ympärivuorokautiseen rytmiin. Kun palvelussa ollaan läsnä, odotetaan reaktioita nopeasti.

Valtaosa julkisista sosiaalisen median palveluista rahoittaa toimintaansa mainoksilla eikä organisaatio voi vaikuttaa siihen, millaisia mainoksia heidän yhteisö- tai verkkopalvelun kohdalla palvelussa esitetään. Tämän takia tulisi selvittää saatavilla olevat palvelut ja niissä käytettävät mainosmekanismit, ennen kuin organisaatio sitoutuu niitä käyttämään oman sosiaalisen palvelunsa alustana.

4 Tietoturvallisuuden toteuttaminen sosiaalisen median palveluita tarjottaessa

Organisaatio voi hyödyntää sosiaalista mediaa myös siten, että se tuottaa itse joko omaan käyttöön ja/tai myös asiakkaille tarjottavia sosiaalisen median palveluita. Tällaista palvelutarjontaa suunniteltaessa kehittämishanke poikkeaa muiden tietojärjestelmien kehittämishankkeista siinä, kuinka organisaatio pystyy välttämään ne ongelmat, joita sosiaalisen median palveluiden käyttöön yleisesti liittyy ja jotka on kuvattu tarkemmin tämän ohjeen edellisissä luvuissa.

Sosiaalisen median palvelut voidaan jaotella palveluiden tuotantomallin mukaan esimerkiksi seuraavasti:

1) Globaaleissa pilvipalveluissa tuotetut palvelut
   - palvelut voidaan tuottaa mistä tahansa maapallolta
2) Suomessa tuotetut palvelut
   - palvelut tuotetaan tyypillisesti käyttäen virtualisoituja, useammalle asiakkaalle tarkoitettuja palvelinympäristöjä käyttäen, ns. toimittajan asiakkaiden kesken jakama ”pilvipalvelu”.
3) Itse tuotetut palvelut tai toimittajalta hankitut dedikoidut palvelut
   - tällöin palvelu on mahdollista toteuttaa siten, että se täyttää esim. tietoturvatasojen ja ICT-varautumisen edellyttämät vaatimukset jolloin palvelussa voidaan käsitellä salassa pidettäviä tietoaineistoja

4.1 Sosiaalisen median palveluiden tarjoaminen

Organisaation tulee suunnitella huolella sosiaalisen median palveluiden tarjoaminen sekä ostettaessa valmiita palveluita toimittajalta että palvelua itse tuotettaessa. Tärkein organisaation johdon päätös on, millaisia palveluita tuotetaan ja miten huolehditaan tarvittavasta resursoinnista. Käyttöönottopäätöksen ei tulisi perustua pelkästään tietoturvallisuuteen, mutta tietoturvallisuus on hyvä ottaa huomioon sekä myönteisessä että kielteisessä päätöksessä.

On suositeltavaa, että sosiaalisen median käyttöönottoprojektista huolehtivat organisaation kyseisestä ydintoiminnasta vastaavat yksiköt käyttäen hallinnollisessa, teknisissä ja tietoturva-asioissa apunaan organisaation verkkoviestintä-, tietohallinto- ja tietoturvaorganisaatiota. Sosiaalinen media tulee nähdä organisaation toimintaa ja suorituskykyä kehittävänä prosessina ja palveluna samalla tavalla kuin muut niin sisäistä tai ulkoista toimintaa kehittävät prosessit ja palvelut. Sosiaalisen median palveluiden luontaisena omistajana toimii yleensä organisaation viestinnästä ja tiedottamisesta vastaava yksikkö. Yksikön tulee nimetä selvästi vastuuhenkilö(t) (omistaja, toimivaltainen virkamies), jotka päättävät sosiaalisen median palveluiden tarjoamiseen liittyvistä linjauksista ja kysymyksistä.

Sosiaalisen median palveluiden tarjoamisessa tulee ottaa huomioon esim. seuraavia asioita:

- **Palvelusopimuksen ja käyttöehtojen luominen palveluiden tarjoamiseen**
  - Palvelusopimuksessa linjataan esimerkiksi:
    - mihin käyttöön organisaatio tarjoaa sosiaalisen median palveluita
    - mitkä ovat palveluiden tuottamiseen liittyvät keskeiset periaatteet
    - palvelutasoluokat (SLA)
    - miten asiakas saa palveluita käyttää
    - mahdolliset laskutusperusteet
  - Palvelusopimuksessa tulee ottaa huomioon tietoturvallisuuteen liittyvät asiat pyrkien ratkaisemaan niitä ongelmia, joita on kuvattu tämän ohjeen luvussa 2.
- **Käyttäjien ohjeistaminen ja kouluttaminen palveluiden käyttöön**
  - Palvelun käyttäjille tulee tarjota asianmukaiset käyttöohjeet
  - Asiakasorganisaation kanssa on sovittava koulutusjärjestelyistä
- **Teknisen tietoturvallisuuden toteuttaminen**
  - Palvelun tekninen tietoturvallisuus tulee vastata palvelulle asetettua tietoturvatasovaatimusta
  - Palvelua tulee toteuttaa organisaation (tietoturva)arkkitehtuurin mukaiseksi
- Auditointi
  - mitä tärkeämmästä ja kriittisemmästä palvelusta on kyse, sitä tärkeämmäksi tulee huolellinen auditoiti hankkeen aikana sekä palvelun siirtyessä tuotantoon
- Jatkuvuudenhallinta / varautuminen

4.2 Suosituksia ja hyviä käytäntöjä palveluiden tarjoamista suunniteltaessa

Organisaation tulee ottaa huomioon Ohjeessa tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010) olevat vaatimukset koskien tietoaineistojen käsittelyä ulottaen sen myös palveluiden tarjoamiseen. Mikäli palvelu hankintaan ulkopuoliselta toimittajalta tai se toteutetaan itse omana palveluna, tulee palvelua suunniteltaessa ottaa huomioon palvelussa käsiteltävä tietoaineisto, jonka perusteella pitää määrittää palvelun edellyttämä tietoturvataso. Tämän ohella palvelua suunniteltaessa tulee selvittää, kuinka kriittinen se on organisaation toiminnalle ja ottaa tämä huomioon palvelun ICT-varautumiseen liittyviä vaatimuskriteereitä mietittäessä. Käyttöönottoa suunniteltaessa tulee huolehtia tarvittavista riskienhallintaprosesseista eri vaiheissa.

Sosiaalisen median palvelun tietoturvallisuusrakenteet tulee perustua esim. seuraaviin vaatimuksiin:

- Laki viranomaisten toiminnan julkisuudesta (621/1999
- 681/2010 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa
- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010

Lisäksi on suositeltavaa tarkastella seuraavan kriteeristön vaatimuksia:
- Kansallinen turvallisuusauditointikriteeristö (KATAKRI)

Kun organisaatio käynnistää sosiaalisen median palvelun hankinta- tai käyttöönottohankkeen, hankkeen tulisi noudattaa muita tietojärjestelmien hankinnassa ja käyttöönotossa noudatettavia hyviä käytäntöjä, esimerkiksi ”JHS 173 ICT-palvelujen kehittäminen: Vaatimusmäärittely suosituksessa esitettyjä suosituksia”.

ICT-hankintojen tietoturvallisuutta on käsitelty tarkemmin VAHTIn tulevassa ICT-hankintojen tietoturvallisuus-ohjeessa.

Hankkeen eri vaiheisiin tulee sisällyttää tarpeellinen määrä tietoturvallisuuteen liittyviä auditointeja esim. riskienarvioinnin, vaatimusmäärittelyn, mahdollisen pilotin ja/tai lopullisen tuotantopalvelun osalta. Käyttöönotettava, mahdollisesti myös asiakkaille tarjottava palvelu tulee saattaa osaksi organisaation tietojärjestelmien tietoturvallisuuden vuosikello-prosessia ja toteuttaa sen mukaiset riskienarvioinnit ja muut vuosikelloon kuvatut elinkaarenhallinnan osa-alueet.

Liitteet

Liite 1. Käyttäjän 10 ohjetta

Yleisenä ohjeena voidaan todeta, että ”älä hölmöile!”. Sosiaalisessa mediassa tapahtunut hölmöily voi kostautua myöhemmin elämässä, myös sen jälkeen kun välitön savu on laskeutunut. Hölmöily saattaa rikkoa ihmissuhteita, työsuhteita tai tyhjentää pankkitilin. Terveen järjen käyttö on sallittua ja suositeltavaa sosiaalisten medioiden käytössä.

Seuraavassa 10 yleisohjetta:

1. Selvitä ja noudata organisaatiosi sosiaalisten medioiden käyttöpolitiikkaa. Osallistu organisaation järjestämään tietoturvakoulutukseen.
2. Jos epäilet, että olet joutunut huijatuksi tai muun hyökkäyksen kohteeksi, älä epäröi pyytää apua. Älä jätä tekemättä asiasta rikosilmoitusta, vaikka taloudellinen menetys saattaa osaltasi jäädä vaatimattomaksi.
3. Jos mainitset sosiaalisen median palvelun henkilöprofiilissasi työnantajasi, esiinnyt tällöin organisaatiosi (epävirallisena) edustajana. Muista käyttäytyä sen mukaisesti!
4. Älä käytä samaa salasanaa eri palveluissa. Älä käytä samoja käyttäjätunnuksia ja salasanoja työ- ja vapaa-ajan palveluissa. Huolehdi salasanasi laadusta käyttämällä vain vahvoja salasanoja.
5. Varo syöttämästä liian henkilökohtaista tai yksityiskohtaista tietoa, valokuvia tai muuta materiaalia itsestäsi. Huomaa, että palvelun tarjoaja voi hyödyntää profiiliisi syöttämiäsi tietoja laajasti. Tutustu huolellisesti käyttämiesi palveluiden sopimusehtoihin.
6. Tarkista käyttäjäprofiilin yksityisyyden suojaa koskevat asetukset ja muuta niitä tarvittaessa siten, että tietosi eivät leviä laajemmalle kuin haluamallesi käyttäjäjoukolle.
7. Kunnioita perheesi ja ystäviesi suhtautumista sosiaalisiin medioihin. Vaikka olisit itse niistä innostunut, eivät kaikki sitä kuitenkaan ole. Jos kanssaihmisesi eivät halua sinun laittavan kuvia tai tietoa heistä sosiaaliseen mediaan, noudata heidän toiveitaan.
8. Älä hyväksy tuntemattomia yhteydenottoyrityksiä verkostoosi äläkä napsauta vieraita, hämäräperäisiä linkkejä.
9. Älä keskustele työasioista muissa kuin työtehtäviin hyväksytyissä sosiaalisissa medioissa. Ole erityisen huolellinen salassa pidettävän tiedon suhteen. Muista, että palvelun ylläpitäjät pääsevät teknisesti käsiksi kaikkeen

palveluun talletettuun ja myös vain keskustelun osapuolten väliseksi tarkoitettuun tietoon.

10. Huolehdi siitä, että tietokoneesi käyttöjärjestelmäpäivitykset ja työvälineohjelmistot on päivitetty ajan tasalle ja että siinä on tarvittavat palomuuri- ja haittaohjelmien torjuntaohjelmistot käytössä ja että ne päivittyvät automaattisesti.

Liite 2. Esimerkki sosiaalisen median käyttöpolitiikasta

Sosiaalisen median käyttöpolitiikka

Tässä asiakirjassa määritetään <organisaatio X>:n sosiaalisen median käyttöpolitiikka.

Tavoite

Sosiaalisen median osallistuminen tukee seuraavia <organisaatio X>:n ydintoimintoja

- Toiminta 1
- Toiminta 2

Sosiaalisen median palveluiden käytön tavoitteet ovat:

- Tavoite 1
- Esimerkiksi ajankohtaisista asioista tiedottaminen kansalaisille
- Esimerkiksi palautteen kerääminen lakiesityksistä
- Esimerkiksi nuorison tavoittaminen nuorison käyttämissä palveluissa

Sosiaalisen median palvelut

<Organisaatio X> ottaa käyttöön seuraavat palvelut:

<Palvelu 1>:

Palvelu mahdollistaa tehokkaan tiedottamiskanavan ja tavoittaa halutut kohderyhmät muita vastaavia palveluita paremmin. Palvelusopimus on <organisaatio X>:n kannalta hyväksyttävissä.

Tehtävään osoitettu henkilöstö osallistuu palveluun organisaatiotunnuksia käyttäen.

<Palvelu 2>:

Palvelu tavoittaa nuorison ja muodostaa luontevan keskustelukanavan heidän kanssaan. Palvelusopimus on osittain ongelmallinen, mutta ongelmat pienennetään ohjeistamalla henkilökuntaa palvelun käyttöön. Tehtävään osoitettu henkilöstö osallistuu palveluun henkilökohtaisilla virkamiestunnuksilla.

Muita palveluita harkitaan tapauskohtaisesti tarpeen vaatiessa.

<Organisatio X:n johtaja Y> tekee päätöksen sosiaalisen median palvelun käyttöön otosta sekä käytön laajuudesta. <Ydintoiminnasta> vastaa osallistumisen toteuttamisesta, palvelun ylläpidosta ja sen resurssoimisesta sekä arvioi yhdessä <lakiosaston> kanssa palvelusopimuksen muutoksista johtuvat vaikutukset. Merkittäviin muutoksiin johtuvat vaikutukset tulee hyväksyttää <johtaja Y:llä>.

Osallistumisen periaatteet

Sosiaalisen median palveluissa käsitellään vain julkista tietoa.

Julkaistu aineisto sekä käytävät keskustelut tulee luonteeltaan olla objektiivisia, neutraaleja ja asiallisia. Organisaatio ei osallistu väittelyihin eikä ota kantaa mahdollisiin omiin tai muiden ristiriitatilanteisiin. Provokatiivisiin organisaatioille osoitettuihin viesteihin ei reagoida. Laittomat, siveettömät, aggressiiviset sekä loukkaavat viestit pyritään poistamaan palvelusta siitä erikseen tiedottamatta.

Henkilöstön osallistuminen sosiaalisen median palveluihin

<Organisaatio X> suhtautuu myönteisesti/neutraalisti/varovaisesti työntekijöiden osallistumiseen sosiaaliseen mediaan palveluihin.

<Organisaatio X>:n näkemys on, että työntekijä mainitessaan työnantajansa edustaa työnantajaa julkaistessaan sisältöä tai käydessään keskusteluja työnantajastaan.

Virkamiehen tulee ottaa huomioon, että virkamiesvastuu on voimassa riippumatta siitä, mainitseeko virkamies työnantajansa sosiaalisen median palveluissa vai ei.

Työntekijä saa/ei saa käyttää työsähköpostiosoitetta sosiaalisen median palveluissa, jos käyttö liittyy työntekijän ammattimaiseen verkostoitumiseen tai ammattitaidon kehittämiseen. Täysin vapaa-ajan sosiaalisen median palveluissa työntekijä ei saa käyttää työsähköpostiosoitetta.

<Organisaatio X> kehottaa kuitenkin seuraavissa tehtävissä olevia työntekijöitä käyttämään harkintaa sosiaalisen median palveluiden käytössä: <sellaiset tehtävät, joiden turvallisuus voi vaarantua tai jonka tehtävänhoitajan henkilöturvallisuus voi vaarantua, jos tehtävästä tai tehtävänhoitajasta paljastuu liian paljon arkaluonteista tietoa>. Tehtävän hoitajan tulee tiedottaa lähipiiriään sosiaalisen median palveluiden käyttöperiaatteista edellä mainittujen työntekijöiden kohdalla.

Sosiaalisen median palveluita saa/saa pääsääntöisesti/ei saa käyttää <organisaatio X>:n tietojenkäsittely-ympäristöstä.

Työnantajan sosiaalisen median palvelua saa / ei saa päivittää työpaikan ulkopuolelta.

Työntekijää saa/saa työtehtävien hoitamisen tueksi/ei saa käyttää sosiaalisen median palveluita työaikana. Palveluiden käyttöön suhtaudutaan myönteisesti, jos käyttö tukee esim. ammattimaista verkostoitumista tai työtehtävää. Henkilökohtaista viestintää sallitaan/tulee rajoittaa vain välttämättömään/on kielletty.

Koulutus

<Organisaatio X:n taho Z> vastaa sosiaalisen median palveluiden koulutuksen koordinoimisesta sisällöntuottajille, ylläpitäjille sekä henkilöstölle. <Tietoturvavastaava> vastaa edellä mainittujen koulutusosioiden tietoturvallisuusosista.

Koulutus toteutetaan <verkkokoulutuksena/erilliskoulutuksena/…>.

Tietoturvallisuus

<Tietoturvavastaava> vastaa riskien arvioimisesta, toimenpiteiden suunnittelusta ja tietoturvallisuuden seurannasta. Riskejä arvioidaan säännöllisesti, kerran vuodessa tai tarvittaessa useammin. <Tietoturvavastaava> esittää riskiarvioinnin <johtaja Y:lle> osana <johtaja Y:n> päätöksentekoa palveluiden käyttöönotosta.

Tietoaineistoja suojataan ohjeistamalla henkilöstö sekä huolehtimalla siitä, että tietojenkäsittely-ympäristön tekninen tietoturva on asianmukaisella tasolla. Mikäli sosiaaliseen mediaan tuotetaan sisältöä <organisaatio Y>:n tietojenkäsittely-ympäristön ulkopuolelta, tulee tarkoitukseen käyttää työasemaa, jossa ei ole salassa pidettäviä tai muita arkaluonteisia tietoja.

<Organisaatio X>:n tietojenkäsittely-ympäristö tulee täyttää perustason/korotetun tason tietoturvavaatimuksia.

Kaikkia työntekijöitä koulutetaan sosiaalisen median tietoturvallisuuden osalta (ks. kohta koulutus).

<Organisaatiotaho> vastaa palvelusopimusehtojen vaikutusten arvioimisesta.

Maineen hallinta

<Organisaatio X> toteuttaa maineen hallinnan seuraamalla organisaatiosta julkaistua tietoa tai siitä käytävää keskustelua seuraavissa sosiaalisen median palveluissa: … Seurannasta vastaa <organisaatiotaho>.

Mikäli organisaatio havaitsee epäasiallista viestintää, siihen puututaan seuraavasti:

- Organisaation sivuilla tapahtuvaan viestintään puututaan poistamalla epäasiallisuudet. Virheellisiä käsityksiä pyritään oikaisemaan.
- Muualla esiintyvä virheellisiin tietoihin käytävään keskusteluun ei puututa.

- Organisaation nimissä julkaistu sisältö pyritään poistamaan ottamalla yhteyttä palvelun tarjoajaan.

Henkilöturvallisuus

Sosiaalisen median palveluun lisätään tiedote, jossa kerrotaan <organisaatio X>:n suhtautumisesta henkilöstöön kohdistuvaan kiusaamiseen, häirintään tai uhkailuihin sekä todetaan, että <organisaatio X> ryhtyy asianmukaisiin toimenpiteisiin, mikäli tällaista toimintaa esiintyy.

Henkilö tulee <kääntyä esimiehen puoleen>, jos kokee joutuneensa kiusaamisen, häirinnän tai uhkailun kohteeksi tai jos muusta syystä kokee, että hänen turvallisuutensa on vaarantunut.

Esimies tulee ryhtyä toimenpiteisiin asian selvittämiseksi:

- <Organisaatiotaho> vastaa yhteydenotosta palvelun tarjoajan kanssa
- <Organisaatiotaho> vastaa mahdollisen rikosilmoituksen tekemisestä
- <Organisaatiotaho> vastaa turvallisuusjärjestelyistä
- <Terveydenhuolto> tukee, jos kiusaaminen, häirintä tai uhkailu johtanut henkiseen ahdinkoon.

Liite 3. Lähteet

Oikeusministeriö – Sosiaalisen median mahdollisuudet hallinnolle -katsaus
http://www.kansanvalta.fi/Etusivu/Tutkimusjakehitys/Sosiaalisenmedianmahdollisuudethallinnollepa

Liikenne- ja viestintäministeriö – Sosiaalisen median ohjeet (LVM:n sisäisiä julkaisuja 4/2010) http://www.lvm.fi/web/fi/julkaisu/view/1182548

Centre for the Protection of National Infrastructure - Good practice Guide; Online Social Networking, heinäkuu/2010
http://www.cpni.gov.uk/Docs/Online_Social_Networking-Good_Practice_Guide.pdf

Department of Defence Social Media Hub
http://socialmedia.defense.gov/

Gartner Industry Research, Andrea Di Maio - Comparing Social-Media Policies for Government, 11.12.2009

Gartner Industry Research, Carol Rozwell - Policy Is Not Enough: Educate Employees About Social Media Use, 10.2.2010

Gartner Industry Research, Andew Walls, Andrea Di Maio - New U.S. Government Security Guidelines for Social Media Are a Start, but Only a Start, 5.10.2009

Gartner Industry Research, Andrew Walls - How to Win Arguments About the Security of Social Software, 1.2.2010

Gartner Industry Research, Andrea Di Maio, Government Employees on Social Networks: Reversing the Burden of Proof, 16.9.2009

Sophos - Social media security toolkit
http://www.sophos.com/lp/threatbeaters/

SAK:n sosiaalisen median ohjeistus
http://www.sak.fi/suomi/ajankohtaista.jsp?lang=fi&location1=1&id=33935&print=1

Tietosuojavaltuutetun toimiston ohjeet
http://www.tietosuoja.fi/9230.htm
http://www.tietosuoja.fi/uploads/fqfq98_1.pdf
JHS 173 ICT-palvelujen kehittäminen: Vaatimusmäärittely suosituksessa esitettyjä suosituksia.
http://docs.jhs-suositukset.fi/jhs-suositukset/JHS173/JHS173.pdf)

LIITE 4. Ohjeen valmistelleen VAHTIn alaisen työryhmän kokoonpano

Tämä ohje on laadittu Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTIn alaisena ja ohjaamana.

Ohjeen laatineen VAHTIn alaisen Sosiaalisen median tietoturvatyöryhmän jäseninä olivat:

Catharina Candolin (pj), Pääesikunta
Kimmo Rousku, Valtion IT-palvelukeskus
Kim Lukin, Helsingin yliopisto
Mats Kommonen, Turun yliopisto
Terja Ketola, Valtioneuvoston kanslia
Lauri Äijälä, Ulkoasianministeriö
Samuli Bergström, Poliisihallitus
Erja Saraste, Huoltovarmuuskeskus
Outi Jousi, Hansel Oy
Lauri Karppinen, Tietosuojavaltuutetun toimisto
Mikael Ratschinskij, Jyväskylän kaupunki

Ohjeen luonnos oli avoimella ja laajalla lausuntokierroksella sekä otakantaa.fi-keskustelussa syksyllä 2010. Saadut lausunnot ja kommentit käsiteltiin työryhmän kokouksissa ja otettiin huomioon ohjeen lopulliseen versioon.

VAHTI hyväksyi ohjeen ja päätti sen julkistamisesta joulukuussa 2010 pidetyssä kokouksessa.

Liite 5. Valtiovarainministeriön antamia tietoturvaohjeita

Alla on lueteltu voimassaolevat VAHTI-ohjeet.

- Sosiaalisen median tietoturvaohje, VAHTI 4/2010
- Sisäverkko-ohje, VAHTI 3/2010
- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010
- Lokiohje, VAHTI 3/2009
- ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin, VAHTI 2/2009
- Hankkeen tietoturvaohje, VAHTI 9/2008
- Valtionhallinnon tietoturvasanasto, VAHTI 8/2008
- Informationssäkerhetsanvisning för personalen, VAHTI 7/2008
- Valtionhallinnon salauskäytäntöjen tietoturvaohje VAHTI 3/2008
- Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008
- Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007
- Älypuhelimien tietoturvallisuus - hyvät käytännöt, VAHTI 2/2007
- Osallistumisesta vaikuttamiseen - valtionhallinnon haasteet kansainvälisessä tietoturvatyössä, VAHTI 1/2007
- Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006
- Tietoturvakouluttajan opas, VAHTI 11/2006
- Henkilöstön tietoturvaohje, VAHTI 10/2006
- Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006
- Tietoturvallisuuden arviointi valtionhallinnossa, VAHTI 8/2006
- Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi, VAHTI 7/2006
- Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006
- Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006
- Electronic Mail-handling Instruction for State Government, VAHTI 2/2006
- Tietoturvapoikkeamatilanteiden hallinta, VAHTI 3/2005
- Valtionhallinnon sähköpostien käsittelyohje, VAHTI 2/2005

- Information Security and management by Results, VAHTI 1/2005
- Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004
- Datasäkerhet och resultatstyrning, VAHTI 4/2004
- Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004
- Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004
- Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006, VAHTI 1/2004
- Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
- Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003
- Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003
- Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003
- Valtionhallinnon etätyön tietoturvallisuusohje, VAHTI 3/2002
- Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002
- Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001
- Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001

Ohjeita laaditaan, päivitetään ja uudistetaan tarpeiden mukaan.

Voimassa oleva VAHTI-ohjeisto löytyy VM:n verkkosivuilta www.vm.fi/vahti. Tuossa osoitteessa on myös tietoa VAHTIn muusta toiminnasta ja hankkeista ohjeiden lisäksi. Lisäksi verkossa on olemassa ensimmäinen versio rakenteistetusta VAHTI-ohjeistosta osoitteessa www.vahtiohje.fi.

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 Valtioneuvosto
Puhelin 09 160 01
Telefaksi 09 160 33123
www.vm.fi

4/2010
VAHTI
Joulukuu 2010

ISSN 1798-0860 (pdf)
ISBN 978-952-251-143-0 (pdf)