PK-YRITYKSEN KYMMENEN TIETOTURVA-KÄSKYÄ

ALKUSANAT

Hyvä pk-yrityksen johtaja,

Tässä pk-yrityksen tietoturvaohjeessa esitettävät ns. ”kymmenen tietoturvakäskyä” on laadittu sinun ja yrityksesi käyttöön. Ohjeiden mukaan toimimalla on mahdollista turvata tehokkaasti liiketoimintanne jatkuvuus ja mahdollisimman häiriötön toiminta.

Tämän pk-yrittäjän tietoturvaohjeen laatijat ovat tietoturva-alan ammattilaisia ja itsekin pienyrittäjiä. Olemme käyttäneet kokemusperäistä harkintaamme pk-yrityksen keskeisistä tietoturvatarpeista ja sitä kautta päätyneet kymmeneen tärkeimpään asiaan, ”käskyyn”, joista pk-yrityksen kannattaa aloittaa tietoturvansa vahvistaminen. Kokemuksen lisäksi aineistoa laadittaessa on otettu huomioon useiden eri organisaatioiden näkemyksiä ja tuotoksia. Viitteitä näihin aineistoihin sekä muuta lisätietoa löytyy jokaisen käskyn lisätiedot-kohdassa.

Käskyjen sisältö on pyritty pitämään mahdollisimman tiiviinä. Tavoitteena on antaa yrityksen vastuuhenkilöille käsitys siitä, mihin kaikkiin seikkoihin tietoturvallisuutta rakennettaessa tulisi kiinnittää huomiota. Haluamme muistuttaa lukijaa siitä, että tietoturvallisuuden rinnalla myös muut turvallisuuden osa-alueet ovat yhtä keskeisiä, koska tietoturvallisuuden lonkerot ulottuvat lähes kaikkiin yritystoiminnan osa-alueisiin, eikä ainoastaan tietotekniikkaan. Näihin lukeutuvat mm. riskienhallinta, liiketoiminnan jatkuvuussuunnittelu, henkilökunnan osaaminen ja toimitilojen turvallisuus.

Tietoturvallisuudella tarkoitetaan hallinnollisia ja teknisiä järjestelyitä, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus. Tietoturvallisuuden synonyymina käytetään myös sanaa tietoturva. Muissa yhteyksissä törmäät varmasti myös termiin ICT-turvallisuus, jolla viitataan mm. tietotekniseen turvallisuuteen ja termiin kyberturvallisuus, jolla viitataan sähköisten ja verkotettujen järjestelmien turvallisuuteen.

Verkottuneessa ja yhteistyökumppaneista koostuvassa toimintaympäristössä yritys on omien tietojen lisäksi vastuussa ja riippuvainen myös kumppaneiden tietojen turvallisuudesta. Tässä ohjeessa esitetyillä tietoturvatoimenpiteillä turvataan ensisijaisesti yrityksen ja sen henkilökunnan etuja, mutta lisäksi myös yhteistyökumppaneille tärkeitä tietoja.

Tekniikan vikaantumiselle emme voi juuri muuta kuin ylläpitää järjestelmiä säännöllisesti ja varautua korjaaviin toimenpiteisiin. Ihmisen käyttäytymiseen sen sijaan voimme vaikuttaa paljonkin. Ihminen saattaa olla työssään huolimaton ja varomaton, osaamistaso voi olla puutteellinen tai asenne jatkuvaan tarkkaavaisuuteen ei ole kohdallaan.

Kuten olet varmaan huomannut, niin yrityksen toiminnan turvaaminen, liiketoiminnan jatkuvuuden varmistaminen ja niiden myötä myös tietoturvallisuuteen liittyvät asiat ovat mitä suurimmassa määrin ihmisten ja toiminnan johtamista. Toiminnan johtamisen sinä jo osaat, mutta toivomme, että lisäät johtamiskäytäntöihisi tietoturva-asiat – unohtamatta ihmisten ja toiminnan johtamista, jotka vaikuttavat myönteisellä tavalla muihin osa-alueisiin.

Näillä saatesanoilla haluamme toivottaa sinulle ja yrityksellesi entistä tietoturvallisempaa ja häiriöttömämpää liiketoimintaa.

Cybricon Oy **Tietoturvaamo Oy**

SISÄLTÖ

Alkusanat _____ 2

1 TUNNISTA SUOJATTAVA PÄÄOMA _____ 4

2 TUNNISTA RISKIT _____ 5

3 VARMISTA LIIKETOIMINNAN JATKUVUUS _____ 6

4 OMAKSU OIKEA ASENNE _____ 8

5 DOKUMENTOI JA OHJEISTA _____ 9

6 KÄYTÄ TIETOJÄRJESTELMIÄ TURVALLISESTI _____ 10

7 VARMISTA TOIMITILOJEN TURVALLISUUS _____ 12

8 HARKINTAA SOSIAALISEN MEDIAN KÄYTTÖÖN _____ 14

9 LUO OHJEET ETÄTYÖTÄ JA MATKATYÖTÄ VARTEN _____ 15

10 JALKAUTA TIETOTURVALLISUUS KÄYTÄNTÖÖN _____ 16

Lopuksi _____ 17

1 TUNNISTA SUOJATTAVA PÄÄOMA

Yrityksen kaiken toiminnan kannalta on välttämätöntä ymmärtää, mitkä toiminnot ja asiat ovat tärkeämpiä kuin muut. Tämä sääntö pätee myös turvallisuuden rakentamiseen, koska useimmiten ei ole taloudellisesti järkevää suojata kaikkea yhtä vahvasti, vaan keskittyä tärkeimpiin asioihin. Tällaisia asioita, joita myöhemmin kutsumme termeillä ”Suojattava kohde” ja ”Kriittinen resurssi tai prosessi”, voivat olla esim. seuraavat:

a. **Valmistusprosessi**

b. **Tuotekehitystieto (esim. tekniset toteutukset, patentit)**

c. **Tuotanto- ja varastotilat**

d. **Tuotteiden jakelu/logistiikka**

e. **Yrityksen avainhenkilöt**

f. **Keskeiset alihankkijat**

g. **Tietojärjestelmä (esim. toiminnanohjausjärjestelmä, laskutus, sähköposti)**

Kriittiseksi katsotun prosessin tai resurssin tunnusmerkkejä ovat, että vahingoittuessaan tai lamaantuessaan, ne aiheuttavat merkittäviä suoria ja välillisiä kustannuksia, merkittävää vahinkoa imagolle tai saattavat pahimmillaan jopa tehdä yrityksen toiminnan jatkamisen mahdottomaksi.

TUNNISTAMISEN HYÖDYT

Mahdollistaa oikeiden johtopäätösten tekemisen.

Riskienhallintaan, liiketoiminnan jatkuvuussuunnitteluun ja turvallisuuteen liittyvät toimenpiteen kyetään kohdistamaan juuri oikeisiin kohteisiin.

Hyviä käytäntöjä

- Tunnista, listaa ja priorisoi yritykselle elintärkeät toiminnot, sekä niiden sisältämät kriittiset tekijät. Tunnista myös näiden väliset riippuvuudet (Esimerkki: Mikäli asiakaskirjeiden ja markkinointimateriaalin lähettäminen on yritykselle kriittinen toiminto, ovat todennäköisesti myös sähköpostijärjestelmä, sekä materiaalin tuottamiseen ja hallintaan liittyvät järjestelmät kriittisiä).
- Dokumentoi em. asiat mahdollisuuksien mukaan ja pidä dokumentit vain tarvittavien henkilöiden saatavilla.
- Kohdista suojattaviin kohteisiin säännölliset riskien- ja jatkuvuudenhallintatoimenpiteet vähintään 2 kertaa vuodessa (näistä tarkemmin käskyissä n:ro 2 ja 3).
- Muista, että myös jotkin tukitoiminnot voivat olla kriittisiä.

KATSO LISÄTIETOJA

Yritys Suomi

https://www.yrityssuomi.fi/osaamisen-suojaaminen-ja-hallinta

2 TUNNISTA RISKIT

Säännölliset riskienhallintatoiminnot ovat jokaisen yrityksen häiriöttömän toiminnan elinehto. Onnistuessaan riskienhallinta on sulautunut yrityksen normaaliin toimintaan, eikä ole erillinen toiminto, jonka suorittaa joku ulkopuolinen kertaluonteisesti. Riskienhallinnan tulee olla säännöllistä ja ennakoivaa toimintaa.

SÄÄNNÖLLISEN RISKIENHALLINNAN HYÖDYT

Mitä vähemmän häiriöitä ja toimintakatkoksia, sitä suuremman taloudellisen ja imagollisen hyödyn yritys saa.

Taloudellinen hyöty tulee myös epäsuorasti laadukkaampina ja oikein kohdistettuina toimenpiteinä ja ratkaisuina.

Hyviä käytäntöjä

Kohdista riskienhallintatoimet ensisijassa käskyssä n:ro 1 tunnistamiisi suojattaviin kohteisiin.

Pyri hallinnoimaan yrityksen kaikkia riskejä samoilla menetelmillä (kuten operatiiviset, taloudelliset, strategiset ja vahinkoriskit), äläkä unohda tietoon kohdistuvia ja tiedosta aiheutuvia riskejä.

Noudata esim. seuraavan kaltaisia riskienhallintakäytäntöjä:

- Tunnista ja listaa suojattavaan kohteeseen liittyviä uhkia ja riskejä (”Ei-toivottuja tapahtumia”).
- Arvioi riskien suuruus (esim. kertolaskulla: Todennäköisyys x Vaikutus = Riskin suuruus) ja järjestä riskit suuruus-/tärkeysjärjestykseen.
- Suunnittele toimenpiteet suurimpien riskien hallitsemiseksi:
  a. *Keskity suurimpiin riskeihin siinä laajuudessa kuin yrityksellä on resursseja (aikaa, rahaa, henkilöstöä) huolehtia näiden riskien hallintatoimenpiteistä.*
  b. *Hallintatoimenpiteitä ovat mm. riskin poistaminen, pienentäminen ja vähentäminen.*
- Nimeä vastuullinen henkilö jokaiselle hallintatoimenpiteelle ja anna hänelle resurssit toteuttaa toimenpiteet.
- Mieti toimenpiteet myös sen varalle, että riskienhallintatoimenpiteet ”pettävät”, tai eivät ole riittävät ja riski kaikesta huolimatta toteutuu.
- Seuraa toimenpiteiden toteutumista/edistymistä ja tee muutoksia tarpeen mukaan.

Lisää riskienhallinta johtoryhmän asialistalle (säännöllisesti käsiteltäväksi asiaksi).

Ota koko henkilökunta mukaan riskienhallintatyöhön, koska et voi itse nähdä ja tietää kaikkea, vaan johtajana olet riippuvainen heidän työstään myös tässä mielessä.

Älä käytä riskin hallintaan enempää rahaa, kuin mitä riskin realisoitumisesta koituisi.

Muista, että joitakin riskejä voi ja on pakko hyväksyä.

KATSO LISÄTIETOJA

Suomen Riskienhallintayhdistys

http://srhy.fi/

http://www.pk-rh.fi

Vakuutusyhtiöiden verkkosivut

ISO 31000 -standardi

http://www.iso.org/iso/home/standards/iso31000.htm

3 VARMISTA LIIKE-TOIMINNAN JATKUVUUS

Liiketoiminnan jatkuvuudenhallinnalla tarkoitetaan varautumista erilaisiin häiriötilanteisiin. Muita termejä, joilla tarkoitetaan käytännössä samaa asiaa, ovat mm. varautuminen häiriötilanteisiin ja jatkuvuussuunnittelu.

Katkoksia liiketoimintaan voivat aiheuttaa hyvin erilaiset teknisistä ongelmista, ihmisistä ja luonnonilmiöistä johtuvat tahalliset, sekä tahattomat viat ja häiriöt. Esimerkkejä näistä ovat vialliset tuotteet/ tuotteen takaisinvedot, alihankkijan konkurssi, tietovuoto tai -varkaus, saastunut tietojärjestelmä, verkkohyökkäys, järjestelmän tai tietoverkon vikaantuminen, lakko, pandemia, ilkivalta, murto/ varkaus, sähkökatkos, tulipalo, vesivahinko, tulva tai hallin katolla olleen lumikuorman aiheuttama rakenteiden romahtaminen.

Jatkuvuudenhallinta koostuu sekä etukäteen suunnitelluista, että häiriöstä toipumisen aikana ja toipumisen päätyttyä tehtävistä toimenpiteistä, joiden avulla pyritään vähentämään liiketoimintaa häiritsevien tekijöiden vaikutusta, lyhentämään häiriöstä toipumiseen kuluvaa aikaa, sekä minimoimaan vahingot.

Jatkuvuuden hallinnassa toimiva, säännöllinen ja luotettava varmuuskopiointi on olennaisen tärkeä asia, jotta tietoja voidaan tarvittaessa palauttaa. Olennaisia ovat myös muut ennakkoon tehtävät järjestelyt, kuten sopimus tietojärjestelmien varaympäristöistä, varatiloista, varahenkilöiden kouluttaminen sekä tarvittavan varaosavaraston ylläpito.

JATKUVUUDENHALLINNAN HYÖDYT

Ennakolta varautuminen voi pelastaa yrityksen merkittäviltä taloudellisilta tappioilta tai jopa toiminnan lopettamiselta koska suojattavat kohteet (= elintärkeät toiminnot = kriittiset resurssit) voidaan pitää tuotantokäytössä mahdollisimman tehokkaasti.

Voidaan ainakin osittain pienentää tai rajoittaa asiakkaille aiheutuvaa vahinkoa (esim. toimitusten tai palvelun katkeamisesta johtuva).

Hyviä käytäntöjä

- Suunnittele yksityiskohtaisemmat toimenpiteet häiriötilanteiden varalle mahdollisimman aikaisessa vaiheessa.
- Dokumentoi suunnitelmat, mikäli ne ovat yhtä riviä pidemmät ja pidä ne vain niitä tarvitsevien saatavilla.

Huomaa, että suunnitelmia kannattaa olla ainakin kahdenlaisia, joista ensimmäisen tarkoitus on varautua ennakolta ja jälkimmäinen tarkoitettu tilanteeseen kun häiriö on jo tapahtunut:

- Laadi jatkuvuussuunnitelma kuvaamaan, miten liiketoimintaa jatketaan tilapäisillä menetelmillä, kunnes häiriö on poistettu. Huomioi ainakin häiriöt, jotka kohdistuvat toimitiloihin, avainhenkilöihin, tietojärjestelmiin, tietoon ja tuotantojärjestelmiin tai -laitteisiin.
- Laadi toipumissuunnitelma kuvaamaan ne toimenpiteet, joilla kriittinen järjestelmä (esim. tuotantolinjan ohjausjärjestelmä tai myyntireskontra) saadaan osittain tai kokonaan toimintakuntoon (hankitaan ja asennetaan) esim. savu- tai vesivahingon jälkeen.

Harjoittele ja testaa suunnitelmien toimivuutta sekä ”paperiharjoituksina” että mahdollisimman todenmukaisissa tilanteissa ainakin kerran vuodessa.

Luo joko erillinen kriisiviestintäsuunnitelma tai sisällytä viestintään liittyvät toimenpiteet muihin suunnitelmiin. Harjoittele myös viestinnän toimintaa.

Katselmoi suunnitelmat säännöllisesti ja päivitä aina kun jokin tieto muuttuu.

Varmista inventaarion toimivuus/luotettavuus (mm. koneet, tietojärjestelmät, ohjelmistot, käyttöoikeuslisenssit).

Huolehdi, että varmuuskopiointi toimii luotettavasti ja, että kopiot säilytetään turvallisesti.

Edellytä, että kopiolta palauttamisen toimivuutta testataan säännöllisesti. Tämä on yhtä tärkeää kuin varmuuskopioiden ottaminen.

Päätä (ja hanki sekä ylläpidä), minkä suojattavan kohteen varaosia tai raaka-ainetta tulee olla varastossa häiriöiden varalle.

Mikäli saatat tarvita toimitilaa häiriötilanteen seurauksena, kartoita tilannetta ja neuvottele järjestelyistä ennakolta.

Luo suhteet, ja tarvittaessa sopimukset, huolto- ja ylläpitoyritysten kanssa ennakolta.

Tietoturvapoikkeamat ovat myös eräänlaisia häiriöitä. Suunnittele ja harjoittele toimintaa myös näissä häiriötilanteissa ennakolta. Erityisen tärkeää on ymmärtää:

- Kuinka verkkohyökkäystapauksissa toimitaan ja mistä saat apua (dokumentoi näiden tahojen yhteyshenkilöt puhelinnumeroineen).
- Kuinka virusepidemian laajeneminen pysäytetään ja miten virusten kanssa yleensä toimitaan.
- Miten palomuurin, palvelinten ja työasemien tapahtuma-/lokitietoja seurataan sekä miten kyseisiä järjestelmiä päivitetään ja korjataan.
- Kenelle tietovuoto- tai varkaustapauksessa viestitään ja miten muuten toimitaan.
- Missä vaiheessa kannattaa olla yhteydessä viranomaisiin.

Mikäli jokin prosessi tai resurssi tuotetaan alihankkijan tai muun ulkoisen toimittajan toimesta, vaadi heiltä riittävät/vastaavat suunnitelmat. Sopikaa tarkasti myös vasteajoista, toipumisajoista ja vastaavista kirjallisesti.

KATSO LISÄTIETOJA

Valtiovarainministeriö, Vaatimukset jatkuvuuden hallinnalle ja tiedon turvaamiselle

https://www.vahtiohje.fi/web/guest/liite-3-vaatimukset-jatkuvuuden-hallinnalle-ja-tiedon-turvaamiselle

Huoltovarmuuskeskus

http://www.huoltovarmuus.fi

ISO 22301 ja 22313 -standardit

http://www.iso.org

4 OMAKSU OIKEA ASENNE

Tietoturvallisuus on kaikkien yhteinen asia – jokainen yrityksen IT-järjestelmien ja -laitteiden käyttäjä on omalta osaltaan vastuussa tietoturvakäytäntöjen noudattamisesta ja sitä kautta tietojärjestelmien häiriöttömän toimivuuden, palvelukyvyn ja eheyden toteutumisesta.

Tietoturvallisuuteen liittyvät asiat, kuten sen rakentaminen, ylläpito ja kehittäminen ovat pääosin johtamista ja vain murto-osaltaan teknologiaa. Hyvä ja toimiva tietoturvallisuus on tulos oikeasta asenteesta, niin johdon kuin käyttäjien tasolla, mutta ennen kaikkea se on tulos onnistuneesta johtamisesta. Epäonnistuminen turvallisuuden johtamisessa voi pahimmillaan mitätöidä turvallisuusjärjestelyt ja siten vaarantaa yrityksen kriittiset prosessit ja resurssit.

OIKEASTA ASENTEESTA SAATAVAT HYÖDYT

Turvallisuuden rakentaminen on huomattavasti sujuvampaa ja edullisempaa, kun koko henkilöstön asenteen ovat myönteiset.

Yrityksen tietoturvakäytännöt onnistutaan jalkauttamaan koko organisaatioon.

Hyviä käytäntöjä

- Johda tietoturvallisuutta samoin kuin johdat yrityksen muitakin toimintoja, kuten vaikkapa taloutta ja myyntiä.
- Lisää henkilökunnan tilaisuuksissa pitämiisi esityksiin ja puheisiin aina jokin turvallisuuteen, riskienhallintaan tai jatkuvuudenhallintaan liittyvä teema.
- Älä vähättele tai aliarvioi tietoturvatyön tärkeyttä, äläkä oleta, että mikrotukihenkilösi kykenee kantamaan kaiken vastuun tai, että virustorjunta estää paperisen tiedon joutumisen vääriin käsiin.
- Jos ulkoistat tietoteknisen turvallisuuden, vaadi alihankkijalta järjestelmällistä toimintaa, seuraa heidän tekemisiään (mm. vahvojen käyttäjätunnusten hallinta) ja vaadi säännöllistä raportointia/yhteydenpitoa.
- Tietoturvallisuus syntyy ihmisten asenteesta, huolellisuudesta ja osaamisesta – kannusta ja ohjaa omaa henkilökuntaasi. Näytä esimerkkiä henkilöstölle, motivoi heitä turvalliseen toimintaan ja edellytä jokaiselta samojen pelisääntöjen noudattamista.
- Johtajana sinun tulee toimia esimerkkinä henkilökunnalle. Jos itse toimit ”turvattomasti” voit olla varma, että myös henkilökunta tekee samoin.
- Koko henkilökunnan tulee olla yhtä motivoitunut toimimaan tietoturvallisesti.

KATSO LISÄTIETOJA

Wikipedia (Työmotivaatio)

http://fi.wikipedia.org/wiki/Ty%C3%B6motivaatio

Työterveyslaitos

http://www.ttl.fi/partner/tepsi/hyvat_kaytannot/teknologiateollisuus/sivut/arvot.aspx

5 DOKUMENTOI JA OHJEISTA

Ajan tasalla oleva ja kattava dokumentaatio on eittämättä eräs yrityksen suojattavista kohteista.

Dokumentaatio on tärkeässä roolissa perehdytettäessä ja koulutettaessa henkilöstöä. Kirjallinen ohjeistus auttaa ja opastaa koko henkilö-kuntaa, ja tarvittaessa myös yhteistyökumppaneita, jotta he toimivat turvallisella tavalla ja noudattavat yrityksen laatimia tietoturvakäytäntöjä ja oheistuksia.

Kenties vielä tärkeämmässä roolissa dokumentit ovat häiriötilanteissa. Kuvittele tilanne, missä tietojärjestelmävastuullinen on lomamatkalla Kauko-Idässä ja ulkopuolisen toimijan pitäisi asentaa ja konfiguroida sähköpostijärjestelmänne uudelleen – mielellään vielä täsmälleen samalla tavalla kuin rikkoutunut järjestelmänne oli.

DOKUMENTOINNIN HYÖDYT
Osaavampi henkilöstö ja sitä kautta turvatumpi toimintaympäristö.
Yhteneväiset ja yhdenmukaiset käytännöt ja toiminta.
Mahdollistaa omalta osaltaan nopeamman häiriöstä toipumisen

Hyviä käytäntöjä

Laadi seuraavat dokumentit ja huolehdi niiden jatkuvasta kouluttamisesta koko henkilökunnalle:

- Tietoturvapolitiikka (tai turvallisuuspolitiikka): Linjaukset ja periaatteet, tietoturvatavoitteet, roolit ja vastuut, jne.
- Tiedon käsittelyohje: Kuinka tietoa käsitellään ja luokitellaan tietoturvallisesti eri tilanteissa ja tiedon elinkaaren vaiheissa (laadinta, tallennus ja arkistointi, lähettäminen fyysisenä- tai sähköpostina, kopiointi, poistaminen/tuhoaminen).
- Seuraavat osa-alueet joko erillisinä ohjeina tai esim. yrityksen Turvallisuuskäsikirjaan koottuna: Hälytys-, kulunvalvonta- ja lukitusjärjestelmien sekä avainten ja kulku-/henkilökorttien käyttö, vierailutilanteet, sidosryhmien kanssa työskentely, yhteystietolistat häiriötilanteita varten, Internetin ja SOME:n käyttö, sekä muut tämän ohjeen käskyihin sisältyvät ohjeet.

Dokumentoi myös seuraavat asiat ja saata ne tarvittavien tahojen tietoon:

- Tietojärjestelmien sekä muiden teknisten järjestelmien kokoonpanotiedot, mukaan lukien laitteistot ja ohjelmistot.
- Riskienhallintakäytännöt, mukaan lukien tietoon liittyvät riskit
- Liiketoiminnan jatkuvuudenhallintaan liittyvät dokumentit (kts. käsky n:ro 3).

KATSO LISÄTIETOJA

VAHTI Henkilöstön tietoturvaohje

https://www.vahtiohje.fi/web/guest/4/2013-henkiloston-tietoturvaohje

VAHTI Johdon tietoturvaopas

https://www.vahtiohje.fi/web/guest/2/2011-johdon-tietoturvaopas

VAHTI Tietoturvasanasto

https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto

VM:n tietoturvaohjeita ja julkaisuja

https://www.vahtiohje.fi/web/guest/487

6 KÄYTÄ TIETO-JÄRJESTELMIÄ TURVALLI-SESTI

Tietojärjestelmissä, mobiililaitteissa ja tallennusvälineissä on todennäköisesti yrityksellesi korvaamatonta tietoa. Nimitämme niitä kaikkia tässä yhteydessä tietojärjestelmiksi.

Tietojärjestelmien osalta on tärkeää muistaa, että niiden turvallinen käyttö sekä suojaaminen tulee ulottaa yrityksen toimitilojen lisäksi myös niiden ulkopuolella suoritettavaan käyttöön – niin kotiin, kauppaan kuin matkoille.

Jossain määrin ”toimitilojen ulkopuolella” tapahtuvaa käyttöä ovat sosiaalisessa mediassa, Internetissä, yhteistyökumppaneiden tietojärjestelmissä ja pilvipalveluissa tehtävä työ, sekä henkilökohtaiset toimenpiteet. Näistä kerromme tarkemmin käskyssä n:ro 8.

TIETOJÄRJESTELMIEN TURVALLISESTA KÄYTÖSTÄ SAATAVA HYÖTY

Käyttämällä tietojärjestelmiä oikein ja mahdollisimman turvallisesti, yritys mm. säästää hankinnoissa (laitteisto, ohjelmisto, lisenssit), kohtaa vähemmän vikatilanteita, saa vähemmän roskapostia ja kykenee turvaamaan omat ja asiakkaidensa tiedot luotettavammin.

Hyviä käytäntöjä

- Muista, että tietoa on tietokoneiden lisäksi mm. paperilla, tuotteissa ja palveluissa, keskusteluissa sekä henkilökunnan muistissa.
- Yrityksen sisäisiä tietoja sisältävät tulosteet ja asiakirjat on suojattava ulkopuolisilta.
- Vältä turhaa tulostamista ja kopiointia, koska ylimääräiset kopiot lisäävät vääriin käsiin

joutumisen vaaraa, aiheuttavat lisäkustannuksia sekä kasvattavat ympäristöjalanjälkeä.

- Muille kuuluvien tietojen urkkiminen, käyttäminen ja lähettäminen on kielletty.

- Laittoman tai hyvän tavan vastaisen materiaalin julkaiseminen, välittäminen tai jakelu yrityksen tietojärjestelmissä, ja muutenkin, on kielletty.

- Käyttäjän pitää säilyttää saamansa IT-laitteet turvallisessa paikassa kun niitä ei käytetä.

- Tallennettava aineisto on mahdollisuuksien mukaan aina tallennettava palvelimelle, missä IT-yksikkö varmistaa tiedot.

- Tilannetta, että aineisto on ainoastaan omalla työkoneella, pitää välttää, jottei kaikkea tietoa menetetä esim. kiintolevyn hajotessa koska tieto on yhtiön omaisuutta.

- Estä tietojärjestelmien väärinkäyttö ja saastuminen (tunnuksien ja salasanojen luonti sekä hallinta, varovaisuus verkossa, vaaralliset liitetiedostot ja linkit, luottamuksellisen tiedon käsittely).

- Pidä kaikkein tärkeimmät tiedot sisältävät laitteet irti tietoverkoista. Vain tällä tavoin voit varmistua, että strategiaa, hinnoittelumalleja tai asiakastietoja ei anasteta ainakaan tietoverkon välityksellä.

- Lukitse em. laitteet luotettavaan tilaan tai kassakaappiin aina kun et niitä tarvitse.

- Huolehdi siitä, että käyttöjärjestelmäpäivitykset ja työvälineohjelmistot on päivitetty ajan tasalle.

- Huolehdi siitä, että palomuuri ja haittaohjelmien torjuntaohjelmistot ovat käytössä ja ajan tasalla.

- Ohjeista muistikorttien, pilvipalveluiden, omien laitteiden ja verkkoyhteyksien käyttö siten, että ne ovat yrityksen tietoturvakäytäntöjen mukaisia.

- Yrityksen laitteita ja järjestelmiä ei tule käyttää asiattomaan toimintaan.

- Ohjeista toimintatavat ja vastuut ongelmatilanteiden ratkaisemiseksi.

KATSO LISÄTIETOJA

Viestintävirasto (Laitteen turvallinen käyttö)

https://www.viestintavirasto.fi/tietoturva/laitteenturvallinenkaytto.html

Viestintävirasto (muut tietoturvaohjeet)

https://www.viestintavirasto.fi/tietoturva/tietoturvaohjeet.html

Aalto yliopisto

http://tietoturva.tkk.fi/fi/tietotekniikan_kaytto/kayttopolitiikka.htm

Finanssialan keskusliitto

https://www.fkl.fi/teemasivut/pankkiturvallisuus/kuluttajalle/Sivut/tietoturva.aspx

VAHTI-ohje

https://www.vahtiohje.fi/web/guest/291

7 VARMISTA TOIMITILOJEN TURVALLISUUS

Toimitilojen turvallisuudella on keskeinen vaikutus sekä tietoturvallisuuteen että muihin turvallisuuden osa-alueisiin. Toimitilojen turvaamiseen ja suojaamiseen käytettävät resurssit mitoitetaan riskienhallinnan tulosten perusteella (huomioiden mm. alueen rikostilanne, rakenteiden vahvuus, etäisyys viranomaisiin ja vartiointiliikkeeseen, toimitaanko tiloissa 24/7 vai vähemmän).

TOIMITILOJEN TURVALLISUUDESTA SAATAVA HYÖTY

Tietoturvallisuuden ”ympärille” saadaan toimitilajärjestelyillä suojaava lisäkerros, mikä vaikeuttaa mm. tiedon varastamista ja järjestelmien fyysistä vahingoittamista. Samat järjestelyt suojaavat myös muuta omaisuutta ja ennen kaikkea henkilökuntaa.

Hyviä käytäntöjä

- Varmista, että ovet ja ikkunat vastaavat sitä murtoluokkaa, jota tarvitsette. Käyttäkää niitä oikein pitämällä ne kiinni/lukittuina sekä huoltamalla säännöllisesti.
- Järjestä avaintenhallinta (metalliavaimet, kulkukortit ja -napit yms.) niin, että avaimen haltijalla on pääsy vain työtehtäviensä edellyttämiin tiloihin. Pidä kirjaa kaikista avaimista.
- Ota käyttöön hälytys- ja valvontajärjestelmät tarvittavassa laajuudessa. Tällaisia ovat mm. murto- ja palohälyttimet, kamera- ja kulunvalvonta, sekä erilaiset toimitilojen tekniikkaan liittyvät hälytykset (vesi, lämpötila, kosteus).

- Varmista, ettei suojattavien kohteiden (erityisesti tietojärjestelmien) kanssa samassa tai yläpuolisissa tiloissa ole haavoittuvia vesi- tai viemäriputkia. Tarvittaessa nosta arkisto-, tietojärjestelmä-, tuotekehitys- tai varastotilojen suojausta ja valvontaa korkeammalle kuin toimistotilojen.

- Mikäli yrityksen koko edellyttää, ota käyttöön kuvalliset henkilökortit ja edellytä koko henkilökunnan käyttävän niitä.

- Älä jätä suojattavia kohteita ulkopuolisten nähtäville tai saataville (sijoittelu, sälekaihtimet kiinni).

- Muista myös paloturvallisuus, kuten oikeantyyppinen sammutuskalusto ja palo-osastoinnit.

- Huolehdi, että hätäpoistumistiet pysyvät aina esteettöminä ja, että henkilöstö tietää lähimmän hätäpoistumistien sijainnin.

- Varmistu, että henkilökunnassa on riittävästi ensiaputaitoisia.

- Tee tarvittaessa sopimus tilojen vartioinnista. Älä kuitenkaan anna vartijoille avaimia tärkeimpiin tiloihin – riittää kun he vartioivat ulkotiloja sekä yleisiä toimitiloja ja pystyvät tarvittaessa, eli häiriötilanteessa, pääsemään myös suojatuille alueille.

- Varmista, että koko henkilökunta osaa toimia vierailijoiden suhteen oikeaoppisesti. Isännän tehtävä on huolehtia, ettei vieraat pääse heille kuulumattomiin tiloihin, neuvottelutiloihin ei jää luottamuksellista tietoa/materiaalia, vieraat eivät saa kytkeä tietokoneitaan yrityksen sisäiseen tietoverkkoon eikä heitä jätetä yksin mihinkään tiloihin jne.

KATSO LISÄTIETOJA

Yrittäjä, Kiinteistö- ja toimitilaturvallisuus

http://www.yrittajat.fi/fi-FI/pohjois-pohjanmaanyrittajat/raahe/yleista/turvanurkka/kiinteisto-ja-toimitilaturvallisuus/

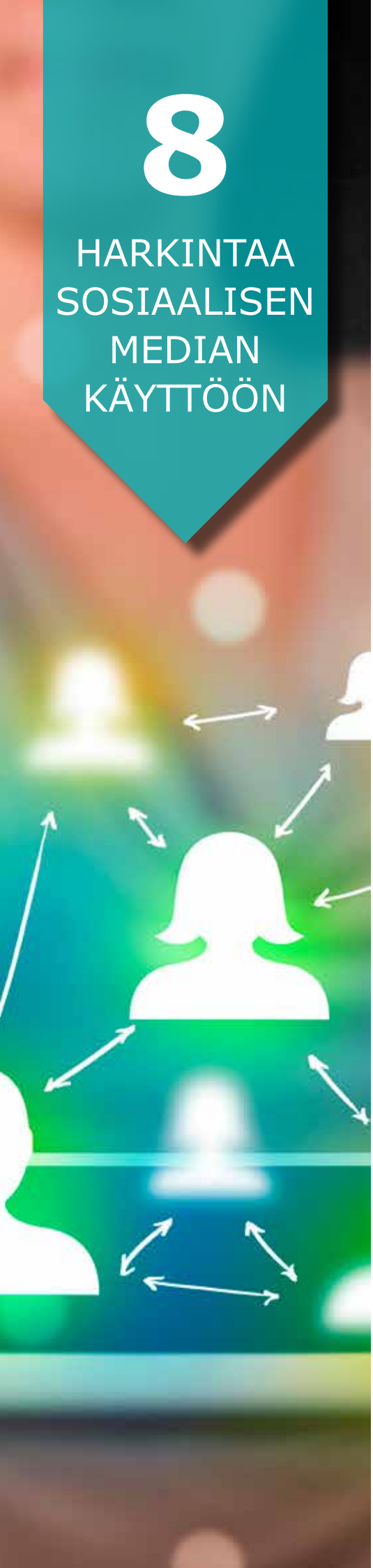
Finanssialan keskusliitto (Vahingontorjunnan ohjeet)

https://www.fkl.fi/materiaalipankki/ohjeet/Sivut/default.aspx

Huoltovarmuuskeskus (Julkaisut)

http://www.huoltovarmuuskeskus.fi/julkaisut/

8 HARKINTAA SOSIAALISEN MEDIAN KÄYTTÖÖN



Sosiaalisen median (SOME) suosio ja käyttö (Facebook, Twitter, Blogit, LinkedIn jne.) on kasvanut yrityksissä merkittävästi. Monelle yritykselle tämä on kuitenkin vielä suhteellisen uusi asia ja näissä yrityksissä ei vielä ole omaa sosiaalisen median kulttuuria, eikä kaikkia sosiaalisen mediaan liittyviä liiketoiminta- ja tietoturvariskejä tunnisteta. Tällaisia riskejä ovat esim. tietovuoto seurauksena siitä, että tiedon jakaja ei ole ymmärtänyt jakamansa aineiston luottamuksellista luonnetta tai mainevahinko siitä, että joku levittää tahallisesti väärää ja virheellistä tietoa tavoitteenaan aiheuttaa yritykselle vahinkoa.

SOME:N HYÖDYT

Sosiaalinen media tuo oikein käytettynä ja hyödynnettynä yrityksille erinomaisen mahdollisuuden tavoittaa uusia asiakkaita, palvella olemassa olevia asiakkaita ja lisätä myyntiä. Yritys voi käyttää SOME:a huolehtiakseen asiakastyytyväisyydestä, rakentaakseen imagoaan, jakaakseen tietoa ja tiedottaakseen arvoistaan.

Sosiaalinen media on yritykselle uusi myynti- ja markkinointikanava, siis mahdollisuus.

Turvallisen SOME:n käytön hyötynä on vähemmän käyttäjien aiheuttamia tietovuotoja ja muita imagoa vahingoittavia häiriöitä.

Hyviä käytäntöjä

- Harkitse SOME:n käyttöä ja listaa siitä haettavat lisäarvot, ellei sitä jo käytetä.
- Laadi yrityksesi SOME:n käyttöpolitiikkaa ja ohjeistus.
- Järjestä henkilökunnalle SOME:en liittyvää tietoturvakoulutusta tai sisällytä se muun turvallisuuskoulutuksen yhteyteen.
- Eri palveluissa tulee käyttää eri salasanoja ja ne pitää olla ns. vahvoja salasanoja.
- Älä julkaise SOME:ssa tietoa, josta kilpailijasi hyötyvät äläkä varsinkaan mitään ei-julkista tietoa.
- Älä julkaise SOME:ssa kilpailijoita loukkaavaa tietoa, koska seuraukset voivat olla arvaamattomat ja hallitsemattomat.
- Huolehdi siitä, että käyttöjärjestelmäpäivitykset ja työvälineohjelmistot on päivitetty ajan tasalle.
- Huolehdi siitä, että palomuuri ja haittaohjelmien torjuntaohjelmistot ovat käytössä ja ajan tasalla.
- Muista – SOME:ssa leviävä palaute, varsinkin negatiivinen, on vaikea taltuttaa ja se voi olla hyvin vahingollista maineelle ja liiketoiminnalle.
- Harjoittele etukäteen, miten toimia ja kommentoida, mikäli SOME:ssa liikkuu tietoa, jota haluat korjata.

KATSO LISÄTIETOJA

Valtiovarainministeriö, Sosiaalisen media tietoturvaohje

https://www.vahtiohje.fi/web/guest/johdanto27

Intosome Oy

http://www.intosome.fi/wp-content/uploads/2011/08/sosiaalisen-median-toimintaohje.pdf

Sosiaalinenmedia.org

http://wiki.eoppimiskeskus.fi/display/someorg/Some-ohjeistuksia

9 LUO OHJEET ETÄTYÖTÄ JA MATKATYÖTÄ VARTEN

Etä- ja matkatyö on muualla kuin vakituisessa toimipisteessä tehtävää työtä ja tämän työmuodon laajuus kasvaa kasvamistaan tämän päivän globalisoituneessa maailmassa. Se luo samalla uusia tarpeita yrityksen tietoturvan ylläpitämiselle ja asettaa siten uusia vaatimuksia tietoturvaratkaisuille ja käytännöille. Tyypillinen etätyö on kotoa tai matkoilla tehtävää toimistotyötä, jolloin käytön taustaympäristöt vaihtelevat.

Etätyöntekijän omilla toimenpiteillä ja menettelytavoilla on suuri merkitys tietoturvamielessä, mutta vähintään yhtä suuri merkitys on turvallisilla tietoliikenneyhteyksillä yrityksen sisäverkosta sen ulkopuolelta tuleviin sallittuihin yhteyspyyntöihin.

ETÄTYÖN JA MATKATYÖN SUOJAAMISESTA SAATAVA HYÖTY

Parempi työn tuottavuus ja tehokkuus koska työtä voi tehdä siellä missä tekijäkin on.

Hyviä käytäntöjä etätyön osalta

- Luo selvät ohjeet ja käytännöt etätyöskentelyä varten.
- Salli etätyö vain erillisellä sopimuksella, missä kuvataan sovitut säännöt etätyön suhteen.
- Tunnista työtehtävät, joita ei voi/ei saa tehdä etätyönä.
- Hanki teknologia, joka mahdollista turvallisen etäyön ja jolla etätyö on sallittu. Peruslähtökohtana on käyttää vähintään ns. tunneloitua yhteyttä (VPN-yhteyttä) etäyhteyksissä ja huolehtia, että kaikki tietovälineet on luotettavasti salattu (mm. muistitikut ja kannettavien tietokoneiden kiintolevyt).
- Muista ohjeistaa, että yrityksen etälaitteiden käyttö on sallittu vain yrityksen työntekijöille – ei perheenjäsenille.
- Etätyössä tulee muistaa tietoaineiston luokitus ja samalla tulee minimoida mukana kuljetettavan fyysisen aineiston määrä yrityksen ulkopuolelle (silloinkin hyvin ja asianmukaisesti suojattuna).
- Myös etätyössä tulee muistaa tietojen säännöllinen varmistaminen.

Hyviä käytäntöjä matkatyön osalta

- Käyttäjän pitää tehdä kaikkensa, ettei näytöllä oleva tieto näy sivullisille esim. matkoilla tai julkisilla paikoilla.
- Matkoilla pitää muistaa olla puhumatta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä (kuten kaupoissa, junassa, bussissa, lentokentillä).
- Esim. bussissa tai junassa pitää varmistua, etteivät kanssamatkustajat pysty kurkistamaan ja näkemään käsittelemiäsi tietoja ja asiakirjoja. Kaikkein turvallisinta on, kun keskityt matkustamisen aikana matkustamiseen ja unohdat työn tekemisen.
- Tieto ja laitteet pitää aina pitää valvottuna ja niitä pitää säilyttää lukitussa paikassa kun niitä ei käytä.
- Paperitulosteiden käyttämistä pitää välttää julkisilla paikoilla.
- Julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin pitää ehdottomasti välttää.

KATSO LISÄTIETOJA

Valtiovarainministeriö, Liikkuva työ, etätyö ja matkatyö

https://www.vahtiohje.fi/web/guest/liikkuva-tyo-etatyo-ja-matkatyo

Tietoalan Toimihenkilöt

http://www.tietoala.fi/tyoehtosopimus/liitteet/liite-9-etatyoohje/

Motiva

http://www.motiva.fi/files/1996/Etatyoopas_tyonantajille.pdf

Finlex

http://www.finlex.fi/data/normit/20917-A132004TM.pdf

10 JALKAUTA TIETO-TURVALLI-SUUS KÄYTÄNTÖÖN

Tietoturvallisuuden jalkauttaminen, sulauttaminen tai istuttaminen yrityksen arkeen on jatkuvaa toimintaa ja edellyttää kaikkien organisaatiotasojen osallistumista – yrityksen johdon määrittelemällä tavalla. Kuten ohjeen alussa korostettiin, turvallisuutta on johdettava aktiivisesti koko ajan, jotta se palvelee tarkoitustaan.

Jalkauttaminen tarkoittaa mm. viestintää henkilöstölle ja yhteistyökumppaneille, kouluttamista sekä uuden toimintamallin, tietojärjestelmän, palomuurijärjestelmän tai ohjeen käyttöönottoa.

JALKAUTTAMISEN HYÖDYT

Onnistuneella ja johdetulla jalkauttamisella voidaan tehdyt päätökset siirtää käytäntöön koko organisaation laajuisesti.

Huolella määritelty jalkauttaminen mahdollistaa toivottujen tulosten ja käytöstapojen saavuttamisen.

Koko organisaatio toimii samojen käytäntöjen mukaisesti ja yhtenäisesti pienentäen tietoturvariskejä merkittävästi.

Hyviä käytäntöjä

- Tuloksellinen jalkauttaminen lähtee yrityksen ylimmästä johdosta ja heidän ohjaamana.
- Joka kerta kun teette pienenkin muutoksen tietoturvakokonaisuuteen, huolehtikaa tiedottamisesta tarvittaville tahoille, dokumentoinnista ja seuratkaa muutoksen toimivuutta käytännössä.
- Viestintä ja koulutus ovat tehokkaita jalkautusmenetelmiä, joten käyttäkää niitä säännöllisesti.
- Informoi koko henkilökuntaa yrityksen tietoturvaohjeista, niiden tarkoituksesta, sijainnista ja vastuuhenkilöistä sekä ohjeiden noudattamisen tärkeydestä.
- Huolehdi siitä, että jokainen työntekijä tuntee omat tietoturvavastuunsa ja toimii niiden mukaisesti. Laadi työtehtäväkohtainen tietoturvakortti ja mielellään myös yhteenveto yrityksen yhteisistä tietoturvaperiaatteista.
- Järjestä säännöllisiä tietoturvatilaisuuksia ja -koulutuksia työntekijöille (1-2 kertaa vuodessa) sekä rohkaise työntekijöitä osallistumaan niihin aktiivisesti.

KATSO LISÄTIETOJA

Six Sigma

http://www.isixsigma.com/dictionary/deming-cycle-pdca/

Wikipedia

http://fi.wikipedia.org/wiki/PDCA

LOPUKSI

Hanki apua ja luotettavat yhteistyökumppanit hyvissä ajoin – Kysy aina apua ellet itse osaa! Apua on saatavilla.

Tietoturvallisuutta voi rakentaa ja ylläpitää useilla erilaisilla, mutta samaan lopputulokseen pyrkivillä, menetelmillä ja malleilla. Yleisesti voi todeta, että kaikki kotimaiset ja kansainvälisen mallit (standardit, kriteeristöt sekä hyvät käytännöt) ovat kattavia opastamaan yrityksesi hyvälle perustasolle sekä tietoturvallisuuden että muiden turvallisuuden osa-alueiden hallinnan suhteen.

Kun valitset yhteistyökumppania, muista ainakin seuraavat:

- Kysy referenssejä, ole heihin yhteydessä ja arvioi saamaasi palautetta.
- Tee sopimus aina kirjallisesti äläkä unohda turvallisuusasioita:
  - Salassapitosopimus
  - Toimitus- ja palveluajat/-tasot
  - Nimetty yhteyshenkilö
  - Yrityksesi tietojen turvallinen käsittely
  - Noudatettavat sopimusehdot
  - Sopimusrikkomukset, seuraamukset ja korvausvelvollisuus
- Valitse ”itsesi kokoinen” ja mieluusti paikallinen toimija:
  - Palvelun nopeus, joustavuus ja henkilökohtaisuus ovat keskeisiä valintakriteereitä
  - Yrityksesi turvallisuuspuutteista ja turvallisuuden kehittämisestä on parempi keskustella saman pöydän ääressä
- Vältä vuosien mittaisen kumppanuuden solmimista heti alussa – tilaa ensin pieni ja hallittava ”paketti” ja laajempia kokonaisuuksia tai jatkuva sopimus vasta kun olet saavuttanut luottamuksen.
- Ellet ole tyytyväinen, vaihda välittömästi.
- Muista, että voit myös vertailla ja kilpailuttaa toimittajia.

sandesign 2015

CYBRICON

Cybricon Oy

www.cybricon.fi

info@cybricon.fi

tietoturvaamo
TURVALLISUUSNEUVONANTAJASI

Tietoturvaamo Oy

www.tietoturvaamo.fi

tt@tietoturvaamo.fi

KIRKKONUMMI
KYRKSLÄTT

www.kirkkonummi.fi/yritykset