VALTIOVARAINMINISTERIÖ

Julkisen hallinnon digitaalisen turvallisuuden teemaviikko – maanantai 2.10.2017

2.10.2017 Aku Hilve ja Kimmo Rousku



Koko viikon sisältö

Digitaalisen turvallisuuden teemaviikko 2017

VAHTI toteuttaa julkishallinnon organisaatioille digitaalisen turvallisuuden teemaviikon 2.–6.10.2017. Viikko on osa EU-alueen laajuista European Cyber Security Month-kokonaisuutta (ECSM).

Teemaviikon tilaisuudet:

- **Ma 2.10. Tieto- ja kyberturvallisuusluennot (verkossa).** Voit seurata esityksiä omalta koneeltasi tai katsoa niitä jälkikäteen tallenteena. Voit esittää luentojen aikana myös kysymyksiä, joihin asiantuntijamme ovat vastaamassa. Ohjelma löytyy tilaisuuden tapahtumasivulta.
- **Ti 3.10. Sähköisen asioinnin tietoturvaseminaari** – valtiovarainministeriö, Mariankatu 9, 00100 Helsinki. Ohjelma ja ilmoittautuminen löytyvät tilaisuuden tapahtumasivulta.
- **Ke 4.10. Arjen tietosuojaa – luentoja tietosuojasta (verkossa).** Voit seurata esityksiä omalta koneeltasi tai katsoa niitä jälkikäteen tallenteena. Voit esittää luentojen aikana myös kysymyksiä, joihin asiantuntijamme ovat vastaamassa. Ohjelma löytyy tilaisuuden tapahtumasivulta.
- **To 5.10. Ylimmän johdon digitaalisen turvallisuuden seminaari** – kutsuvierastilaisuus
- **Pe 6.10. Tutustu viikon aikana julkaistuihin materiaaleihin, osallistu oman organisaatiosi antamiin muihin tehtäviin ja koulutuksiin.**

Voit seurata esityksiä verkossa. Voit esittää kysymyksiä joko verkkolähetyksen alareunan Lähetä viesti -toiminnolla tai tekstiviestillä numeroon 16232. Tekstiviestin alkuun tulee laittaa tunnus A välilyönti ja tämän jälkeen viesti. Jokainen esitys tulee jäämään samalle sivustolle tallenteeksi.



Kysymyksiä

- Nyt kun seuraat tätä livenä – nettilähetyksen kautta, voit esittää kysymyksen alareunan viestiseinän avulla. Voit kirjoittaa kysymyksen joko oikealla nimelläsi / organisaatiosi tai jollain anonyymillä nimimerkillä.
- Pyrimme vastaamaan kysymyksiin tuolla samalla alueella, välttämättä emme saa kaikkiin heti vastausta - keräämme kaikki esitetyt kysymykset ja julkaisemme ne vastauksineen Digitaalisen turvallisuuden teemaviikko –sivustollamme viimeistään ensi viikon aikana
  - http://vm.fi/digitaalisen-turvallisuuden-teemaviikko
- Voit myös lähettää kysymyksiä arjen.tietosuoja@vm.fi – sekä tietoturvallisuuteen että tietosuojaan liittyen

Maanantai 2.10.2017 ohjelma 1/3

9.00 Digitaalisen turvallisuuden teemaviikko alkaa –tervetuloa!

*Tietohallintoneuvos, yksikön päällikkö **Aku Hilve**, valtiovarainministeriö*

9.15 Mitä digitaalinen turvallisuus tarkoittaa, mistä se koostuu ja miksi se on tärkeää?

Uuden MMKT-toimintamaliin esittely

*VAHTI-pääsihteeri **Kimmo Rousku**, valtiovarainministeriö*

10.00 Mitkä ovat vuoden 2017 keskeisimpiä tietoturvauhkia ja kuinka niiltä tulisi suojautua?

*Ryhmäpäällikkö **Jarna Hartikainen** Viestintävirasto, Kyberturvallisuuskeskus*

10.45 Kohdistetut tieto- ja kyberturvallisuushyökkäykset (APT)

*Tietoturva-asiantuntija **Tomi Hasu** Viestintävirasto, Kyberturvallisuuskeskus*

Maanantai 2.10.2017 ohjelma 2/3

12.45 Verkon huijaukset, petokset ja valheet - kuinka vältät verkon vaarat?
*Erityisasiantuntija **Antti Kurittu** Viestintävirasto, Kyberturvallisuuskeskus*

13.30 Millainen on hyvä salasana – muuta tunnusten ja salasanojen hallinnasta

*Riskienhallintapäällikkö **Tommi Simula**, Valtori sekä kehittämispäällikkö **Kimmo Janhunen**, Oikeusrekisterikeskus*

14.15 Kuinka tulee toimia erilaisissa häiriötilanteissa?

*Tietoturvapäällikkö **Erja Kinnunen**, Verohallinto*

15.00 Tiedätkö, olet oman elämäsi riskienhallintapäällikkö! Miten sovellat riskienhallintaa omassa työssäsi?

*ICT-tietoturvapäällikkö **Pyry Heikkinen**, Tulli*

Maanantai 2.10.2017 ohjelma 3/3

15.45 Tietoturvallisuuden huoneentaulu – miksi näin kannattaa toimia?

*Tietoturvapäällikkö **Petri Puhakainen**, Valtioneuvoston kanslia*

+ kertaus

Uuden MMKT-toimintamaliin esittely

*VAHTI-pääsihteeri **Kimmo Rousku**, valtiovarainministeriö*



Teemaviikon avaus

*Tietohallintoneuvos, yksikön päällikkö **Aku Hilve**, valtiovarainministeriö*

Tervetuloa!

- Valtiovarainministeriön ja JulkICT:n rooli
- VAHTIn tehtävät
- Odotuksiamme

Valtiovarainministeriön rooli 1/2

Valtiovarainministeriön tehtävänä on (1) julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja (2) valtionhallinnon tietoturvallisuuden ohjaus. Valtiovarainministeriön toimivalta tietoturvallisuuden ja tietohallinnon ohjauksessa ja kehittämisessä perustuu useisiin säädöksiin.

Tällaisia ovat laki julkisen hallinnon tietohallinnon ohjaamisesta (634/2011), laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011), valmiuslaki (1552/2011), valtioneuvoston ohjesääntö (262/2003) ja valtioneuvoston asetus valtiovarainministeriöstä (610/2003).

Valtiovarainministeriön rooli 2/2

- Valtiovarainministeriö vastaa **turvallisuusverkkotoiminnan** yleishallinnollisesta, strategisesta, taloudellisesta ja tieto- ja viestintäteknisen **varautumisen, valmiuden ja turvallisuuden ohjauksesta ja valvonnasta**.
- Valtiovarainministeriön vastuulla on laissa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä tarkoitettujen **yhteisten palvelujen palvelutuotannon** yleishallinnollinen, strateginen sekä **tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjaus**.
- Lisäksi valtiovarainministeriön vastuulla on laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista.

Valtiovarainministeriön työjärjestys

- **10 § (19.6.2017/396)**
- **Julkisen hallinnon tieto- ja viestintätekninen osasto (JulkICT)**
- Julkisen hallinnon tieto- ja viestintätekninen osasto valmistelee asiat, jotka koskevat:
- 7) julkisen hallinnon tietohallinnon ja edellä mainittujen palvelujen ja palvelutuotannon varautumisen, valmiuden ja turvallisuuden yleistä ohjausta.

Julkisen hallinnon tieto- ja viestintätekninen osasto (JulkICT-osasto)

Julkisen hallinnon tieto- ja viestintätekninen osasto vastaa julkisen hallinnon tietohallinnon, sähköisen asioinnin ja tietovarantojen käytön yleisestä kehittämisestä, valtionhallinnon tietohallinnon ohjauksesta ja yhteisten kehittämishankkeiden yhteensovittamisesta. JulkICT-osasto edistää valtion ja kuntien välistä tietohallintoyhteistyötä, kehittää yhteisiä toiminnallisia ja teknisiä ratkaisuja ja menetelmiä sekä vastaa julkisen hallinnon tietoturvallisuuden yleisestä kehittämisestä ja valtionhallinnon tietoturvallisuuden ohjauksesta.

Julkisen hallinnon tieto- ja viestintäteknistä osastoa johtaa ICT-johtaja **Anna-Maija Karjalainen**.

JulkICT-toiminnossa on kolme yksikköä:
Tietopolitiikka - lainsäädäntöneuvos **Sami Kivivasara**
Digitalisaatio - tietohallintoneuvos **Maria Nikkilä**
Palveluiden turvallisuus ja ohjaus - tietohallintoneuvos **Aku Hilve**

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä - VAHTI

- VAHTI on **julkisen hallinnon digitaalisen turvallisuuden ohjauksen, kehittämisen ja yhteistyön elin**. Valtiovarainministeriö on asettanut VAHTIn toimimaan julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä.
- VAHTIn asema on kirjattu voimassa oleviin valtioneuvoston periaatepäätöksiin Suomen kyberturvallisuusstrategiasta 2013 ja valtionhallinnon tietoturvallisuuden kehittämisestä 2009.
  - Lisäksi VAHTIlla on keskeinen rooli kyberturvallisuus-strategian toimeenpano-ohjelman v. 2017 – 2020 toteuttamisessa.

Odotuksiamme

- Teemaviikko - toivomme
  - että jokainen pystyy esitystemme ja tilaisuuksiemme avulla kehittämään omaa ja organisaationsa toimintaa
  - sitä, että organisaatiot tulevat hyödyntämään seuraavan vuoden aikana nyt laadittuja materiaaleja ja katselemaan niitä myös verkossa
  - aktiivisuutta viikon aikana – esimerkiksi kysymysten muodossa
  - että saamme palautetta teemaviikon jälkeen ensi vuoitta ajatellen
- Haluamme luoda tästä vuosittaisen julkisen hallinnon teemaviikon, jonka avulla voimme ylläpitää ja kehittää Suomen asemaa digitaalisen turvallisuuden kärkijoukoissa kulkevana yhteiskuntana – me jokainen vaikutamme siihen omalla toiminnallamme ja käytöksellä työpaikalla, kotona ja vapaa-ajalla

Miten VAHTI-toimii?

VAHTI-pääsihteeri Kimmo Rousku, valtiovarainministeriö

VAHTIn tavoitteet

- VAHTI **tukee valtiovarainministeriön päätöksentekoa** ja sen valmistelua julkisen hallinnon digitaalista turvallisuutta koskevissa asioissa.
- VAHTI kehittää digitaalista turvallisuutta, mikä mahdollistaa julkisen hallinnon toiminnan digitalisaation ja robotisaation, toimintojen luotettavuuden, salassa pidettävien tietojen luottamuksellisuuden, tietojen ja toiminnan saatavuuden ja eheyden, toiminnan jatkuvuuden ja varautumisen häiriötilanteisiin sekä parantaa toiminnan laatua ja riskienhallintaa.

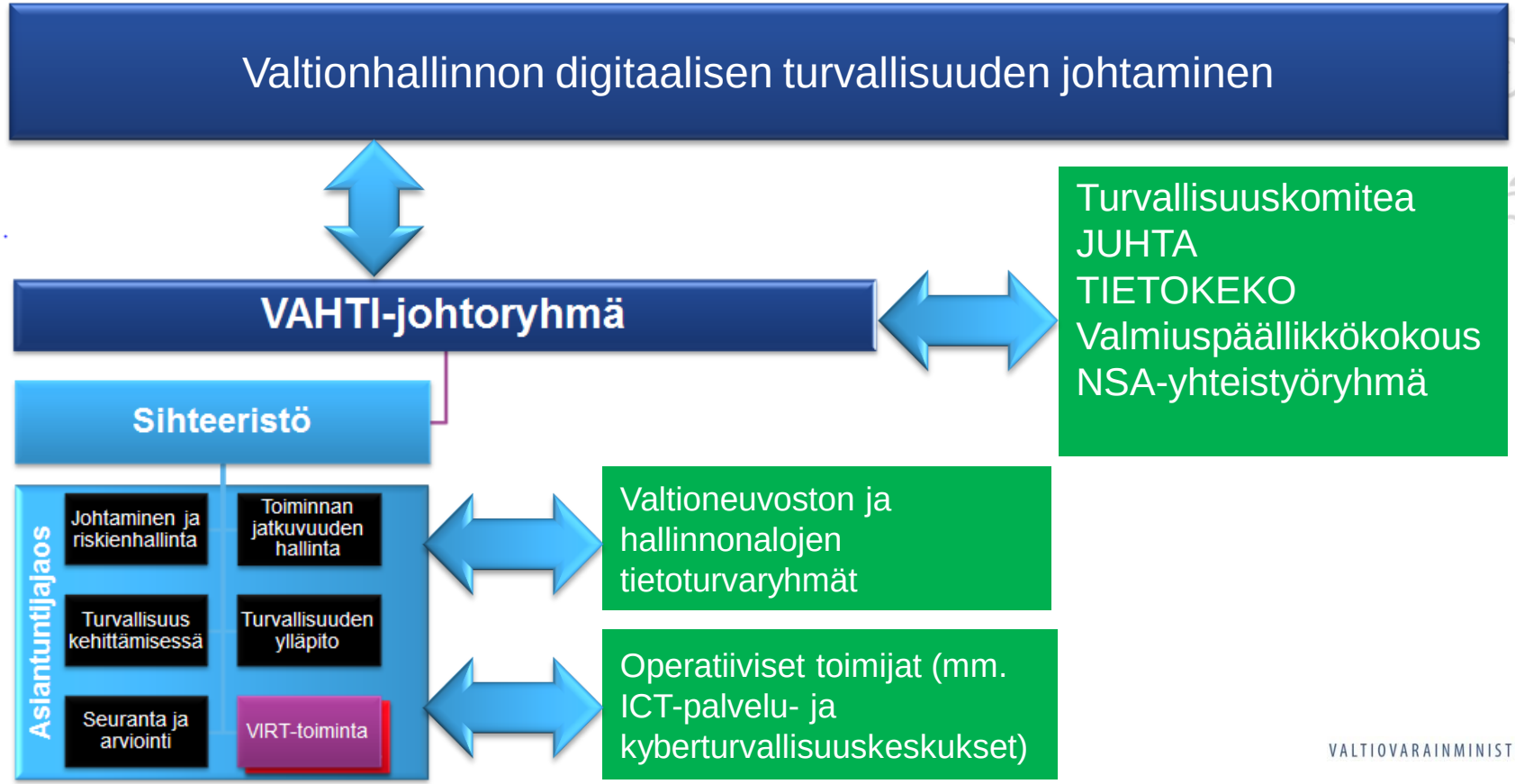
VAHTI-johtoryhmä – tehtävät 1/2

- VAHTI on julkisen hallinnon digitaalisen turvallisuuden ohjauksen, kehittämisen ja yhteistyön elin. VAHTI
  - **valmistelee ja sovittaa yhteen** valtiovarainministeriön linjauksia julkisen hallinnon digitaalisesta turvallisuudesta sekä **seuraa ja edistää** niiden toimeenpanoa
  - **käsittelee** julkisen hallinnon digitaalista turvallisuutta koskevat säädökset, ohjeet, suositukset sekä muut tieto- ja kyberturvallisuuden linjaukset
  - **edistää** julkisen hallinnon tietoturvakulttuuria ja henkilöstön tietoturvatietoisuutta
  - **edesauttaa** tietosuojan toteutumista osana digitaalisen turvallisuuden kehittämistä

VAHTI-johtoryhmä – tehtävät 1/2

- **toteuttaa** digitaalista turvallisuutta koskevia kyselyitä ja barometrejä sekä **julkaisee** näistä raportteja sekä havainnoista koostettuja kehittämissuunnitelmia
- **mittaa, kokoaa ja ylläpitää kokonaiskuvaa** julkisenhallinnon digitaalisen turvallisuuden tilanteesta sekä raportoi tästä valtiovarainministeriön johdolle
- **ohjaa, valmistelee ja sovittaa yhteen** julkisen hallinnon digitaaliseen turvallisuuteen liittyviä kehittämisohjelmia ja hankkeita sekä niiden toimeenpanoa
- **kehittää** digitaalisen turvallisuuden operatiivista häiriötilanteiden hallintaa osana VIRT-toimintamallia
- **käsittelee ja sovittaa yhteen** julkisen hallinnon kansainvälisen tietoturvayhteistyön linjauksia ja vaikuttamista kansainvälisessä tietoturvatyössä.

Kyber- ja tietoturvallisuuden kehittäminen, ohjaus ja yhteistyö



VAHTIn toiminta

- Mukana toiminnassa >50 organisaatiota, noin 130 johtajaa, esimiestä ja asiantuntijaa johtoryhmä, sihteeristö ja viidessä asiantuntijaryhmissä
  - Valtionhallinnon organisaatiot
  - Kuntien edustajat
  - Sairaanhoitopiirien edustajat
  - Yliopistojen edustajat
- VAHTI järjestää vuosittain useampia seminaari-/ koulutustilaisuuksia, loppuvuodesta juhlistetaan 20. toimintavuotta

Viimeaikaisia aikaansaannoksiamme

Yhteistyö!

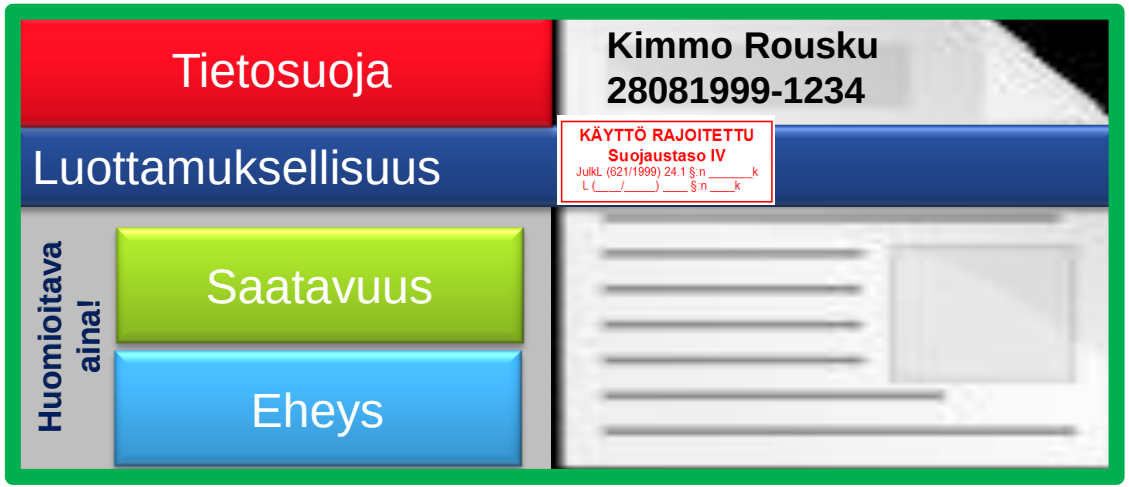
- **Tämä teemaviikko**
- VAHTI-tietoturvabarometri henkilöstölle ja johdolle käynnissä
  - >108 organisaatiota osallistuu, organisaatiot ehtivät vielä tänään ilmoittautua!
  - Viime vuonna saimme 13915 vastausta – kiitos!
- Teemme yhteistyötä julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) asettaman tietoturva, tietosuoja ja varautumisen asiantuntijaryhmän kanssa heidän yhteishankkeissa
  - www.arjentietosuoja.fi sekä JUHTA/VAHTI-yhteishankkeet tietosuojan osoitusvelvollisuutta edistäviin yhteishankkeisiin
- www.vahtiohje.fi sivustolle tuotetut ohjeet ja tukimateriaalit

Digitaalinen turvallisuus on digitalisaation mahdollistaja

#luottamus #turvallisuus #yhteistyö
- mahdollistaa - #menestys

Tietoturvallisuus

- **Tietoturvallisuus** = tiedon saatavuus + eheys + luottamuksellisuus ja mikäli mukana henkilötietoja, huomioitava **tietosuoja**
  - **Tietoturvallisuus on tietosuojan mahdollistaja**



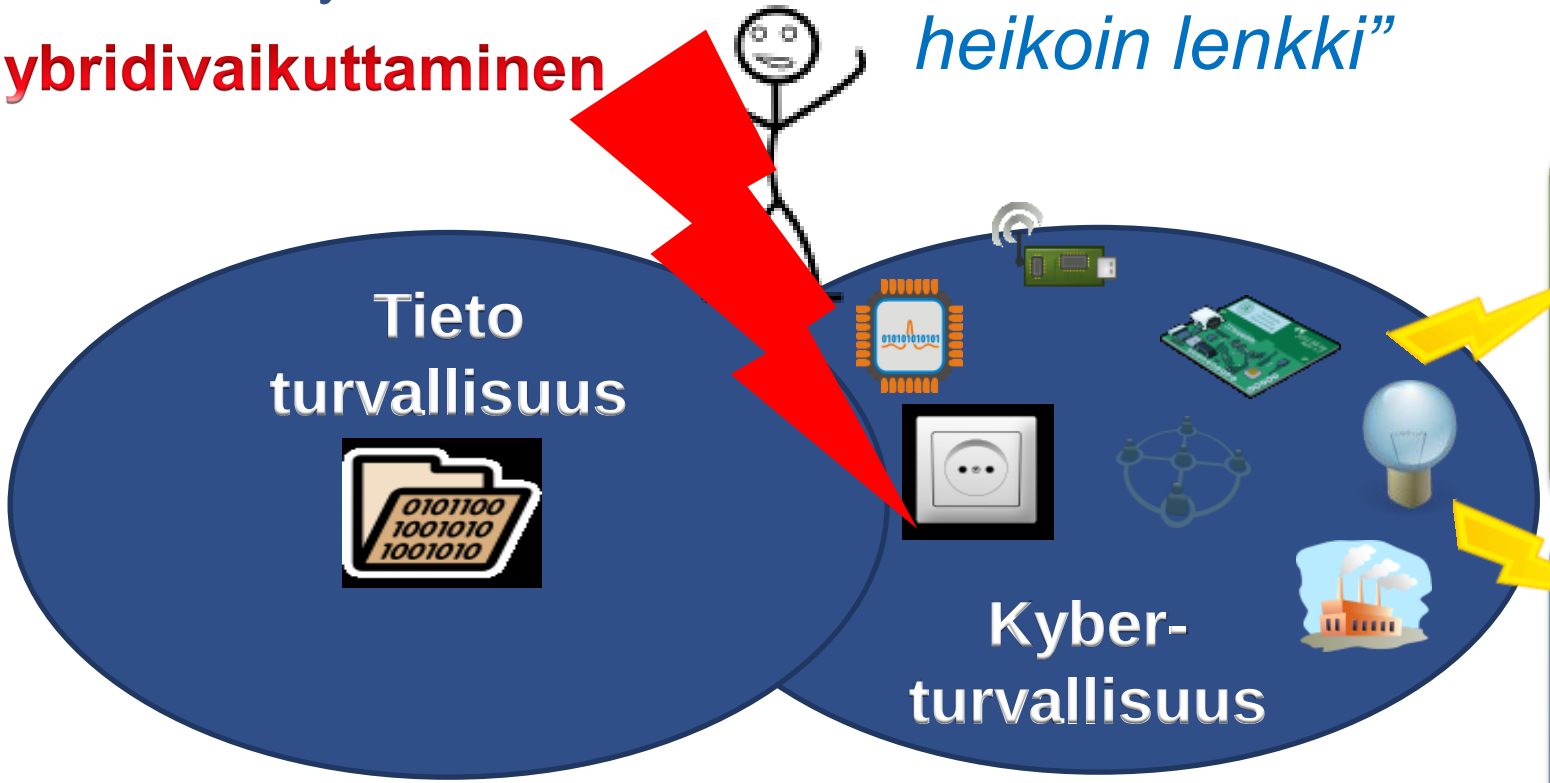
Kyberturvallisuus

- Tietoturvallisuus näyttäytyy hyvin vahvasti **tietojen**, osin tietojärjestelmien näkökulmasta
  - Tietoturvauhka
- Kyberturvallisuus tarkoittaa laaja-alaisesti digitaalisen toimintaympäristön (virtuaalinen bitti / ICT-maailma mutta myös fyysinen maailma) **toiminnan turvaamista**, johon kuuluu myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet (konesalit, sähkönjakelu, henkilöstö jne).
- Digitaalisesta maailmasta voidaan vaikuttaa sekä digitaaliseen maailmaan (kyberavaruus) sekä analogiseen, meidän ympärillä toimivaan yhteiskuntaan
- Kyberturvallisuutta on myös **kyky sietää näitä uhkia (resilienssi)**.
  - Kyberturvallisuuteen voidaan vaikuttaa useilla erilaisilla keinoilla, tietoturvauhan lisäksi myös hybridivaikuttamisen keinoin

Tieto vs kyberturvallisuus

Hybridivaikuttaminen

”Ihminen on xxx:n heikoin lenkki”




LIVE
breakyourownnews.com
BREAKING NEWS
TIETOSUOJA ON HANKALAA?
VAHTI-pääsihteeri
Erityisasiantuntija
7:50
VOIKO TÄMÄ OLLA TODELLAKIN OIKEA UUTINEN?

Tietosuoja



- **Tietosuojalla** tarkoitetaan yksilön (rekisteröity) **yksityisyyden ja luottamuksen turvaamista**; esimerkiksi henkilötietojen oikeaoppista käsittelyä ja niiden suojaamista luvattomalta käytöltä ja muulta käsittelyltä.
- Tietosuojan tarkoituksena on näin ollen turvata tiedon kohteen yksityisyys sekä edut, oikeudet ja vapaudet sekä oikeusturva.
  - Ja on siis eräs myös Euroopan unionin keskeisistä perusoikeuksista => EU:n yleinen tietosuoja-asetus keskeisessä roolissa
  - Suomen perustuslaki - Yksityiselämän suoja;
    - Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.
    - Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

Toiminnan jatkuvuus

- Eikö tämä ole kaikkien organisaatioiden kenties kaikista tärkein kysymys?
- Kuinka varautua toimintaa uhkaaviin häiriöihin ennakoivasti, joista osa liittyy tieto- ja kyberturvallisuuteen sekä tietosuojaan
  - Miten
    - A) Kehitetään suojautumis- ja reagointikykyä
    - B) entäs kun häiriö pääsee toteutumaan - toipuminen
    - C) ja kyvykkyys palautua takaisiin normaaliin toimintaan sen kriittisyyden mukaisesti ?


Toimintaan kohdistuvat tieto- ja kyberturvauhat
Toiminnan johtaminen
Riskienhallinta
Varautuminen häiriötilanteisiin
Tekninen turvallisuus
Tietoturvallisuus
Kaiken toiminnan ja tiedon saatavuuden ja eheyden turvaaminen
Henkilötiedot – tietosuoja
Salassa pidettävä tieto – luottamuksellisuus
Hallinnollinen turvallisuus
Henkilöstö
Suojattava tieto | kohde | toiminta
Toiminnan mittaaminen ja vaatimusten hallinta sekä arviointi
Toimintaan kohdistuvat vaatimukset

Miten organisaatiosi | Sinä voitte kehittää digitaalista turvallisuutta?

MMKT

- toimintamalli turvalliseen työskentelyyn

MMKT-malli?

YHTEINEN TIEDONANTO EUROOPAN PARLAMENTILLE JA NEUVOSTOLLE Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle

http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

”Noin 95 prosenttia kyberturvallisuuspoikkeamista väitetään olevan sellaisia, jotka on mahdollistanut jonkinlainen – tarkoituksellinen tai tahaton – **inhimillinen virhe**”

- Tähän auttaa:
  - Tekniset keinot
  - Henkilöstön ohjeistus, koulutus
  - Tietoturva-asenne ja kulttuuri sekä johdon esimerkki

Inhimillisiä virheitä?



- Meistä jokainen on tehnyt ja tulee tekemään inhimillisiä – **tahattomia** virheitä
- Uusien teknologisten laitteiden ja palveluiden (toiminnan digitalisaatio) myötä myös näiden inhimillisten virheiden määrä kasvaa
  - Samalla tulee koskemaan toimimattomia, tai virheellisesti toimivia ICT-järjestelmiä, laitteita ja palveluita
- Teknologian puolelle
  - Lisää automaatiota, keinoälyä huolehtimaan turvallisuudesta
- Entäs ihmisten toiminnan osalta?

MMKT-toimintamalli turvalliseen toimintaan

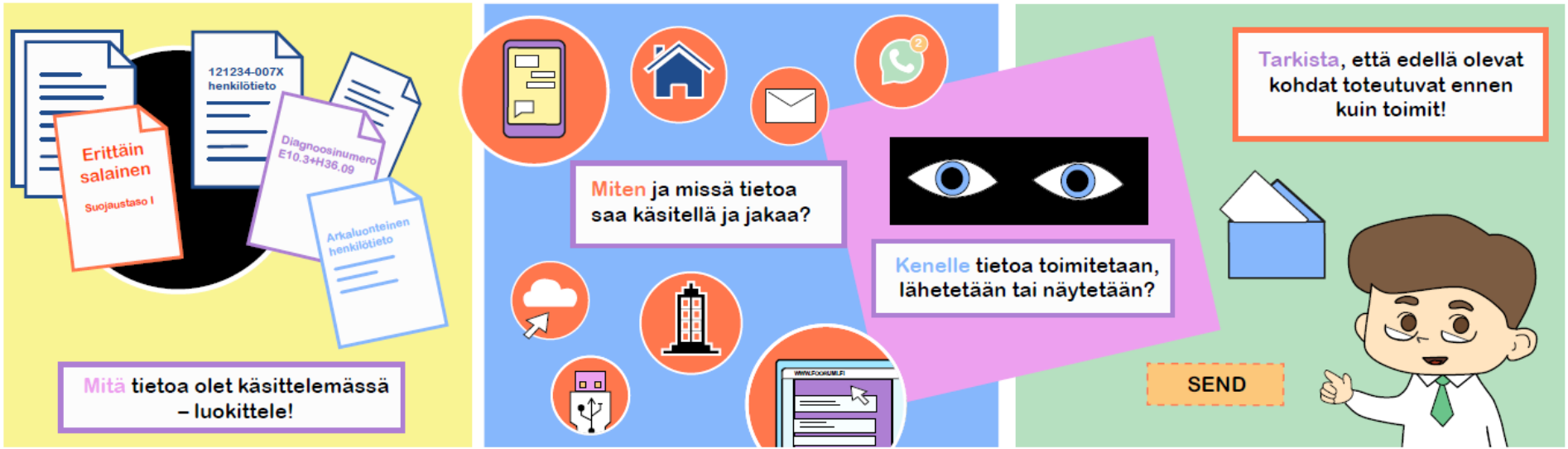
M Millaisia tietoja käsittelet? Luokittele tiedot.

M Miten | millä välineillä sekä missä tietoja käsittelet?

K Kenelle tietoja luovutat?

T Tarkista ennen kuin toimit!

M-M-K-T –toimintamalli tietojenkäsittelyyn



MMKT tarkemmin

Mitä tietoa olet käsittelemässä - esimerkiksi tallentamassa | lähettämässä | jakamassa | näyttämässä tai hävittämässä?

- **Luokittele** julkinen | salassa pidettävä | henkilötieto | arkaluonteinen henkilötieto

Miten ja **missä** tietoa käsitellään sen luokituksen mukaisesti?

- tekstiviesti | puhelinsoitto | pikaviestipalvelu | sähköposti | videoneuvottelu | salattu sähköposti / turvaposti | ryhmätyötila | usb-muisti | pilvipalvelu | sosiaalinen media | muu julkinen tai turvallinen palvelu tai menetelmä … ?
  - työpaikalla | etätöissä | julkinen tila

MMKT tarkemmin

K **Kenelle** tietoa toimitetaan | lähetetään tai näytetään?

- Julkinen tieto saa levitä kaikkialle
- Salassa pidettävä tai henkilötieto - onko vastaanottajalla oikeus saada tieto?

T **Tarkista!**

- Jos käytät esimerkiksi sähköpostia, katso vielä kerran viesti ja ovatko vastaanottajat oikeat ennen kuin napautat **Lähetä** tai muuten jaat tietoa
- Sovita työskentelysi muuten fyysiseen ympäristöön

Toinen näkökulma – MMKT –palveluita käytettäessä

Lähettäjä:

Lähetetty: su 1.10.2017 22:41

Vastaanottaja: Rousku Kimmo VM

Kopio:

Aihe: Valokuvia viime yön aika villeistä juhlista :-)

Hei,

Olipas upeat juhlat meillä, kiitos kun pääsit osallistumaan. Julkaisin tuonne muutaman parhaista otoksista, joissa olet kanssa keskeisessä roolissa mukana. Ethän jaa noita kuvia kuitenkaan edelleen ....

https://picturedatabank.organisaatio.fi/PGrated/viime_yon_juhlat

M&M

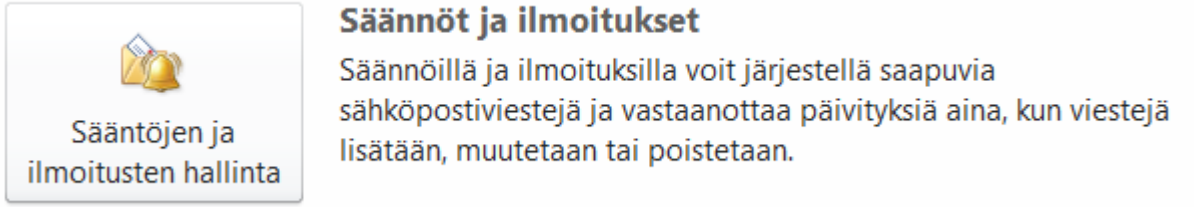
Mieti **M**itä **K**likkaat **T**urvallisesti

Näistä saat lisätietoa ja esimerkkejä päivän muissa esityksissä

Vinkki sähköpostin turvallisuuden parantamiseksi

Kimmon oma vinkki – Outlookin katumusviive

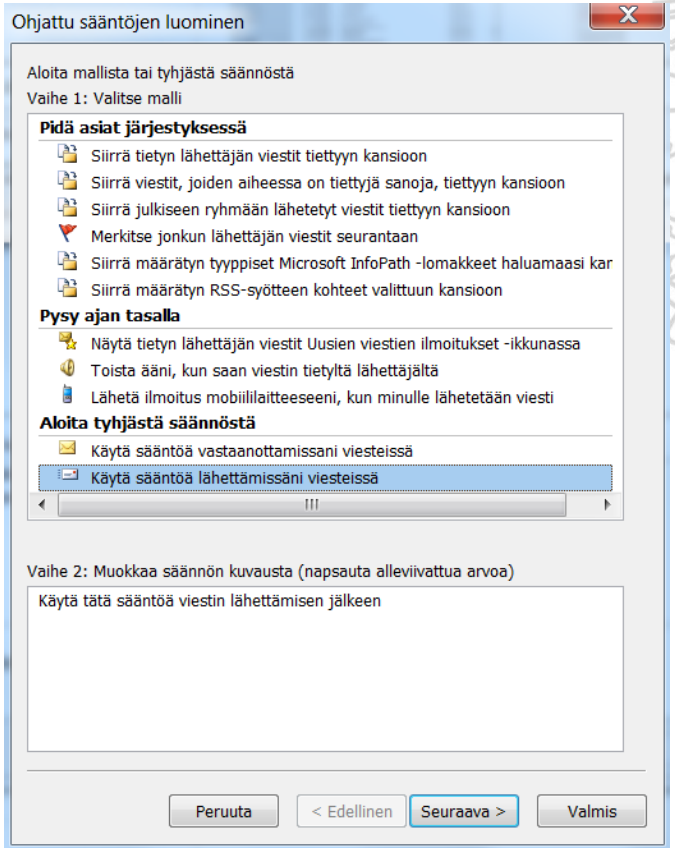
- Miten itse vältän inhimilliset erehdykset? Olen asettanut minuutin katumusviiveen kaikkeen lähteviin sähköposteihini
  - Väärä vastaanottaja, vastaanottaja puuttui, liite unohtui, ai niin … tai just tuli uusi viesti, jossa jotain lisätietoa,
- Tiedosto |



- Uusi sääntö |

Kimmon oma vinkki – Outlookin katumusviive

- Valitse **”Käytä sääntöä lähettämissäni viesteissä”**

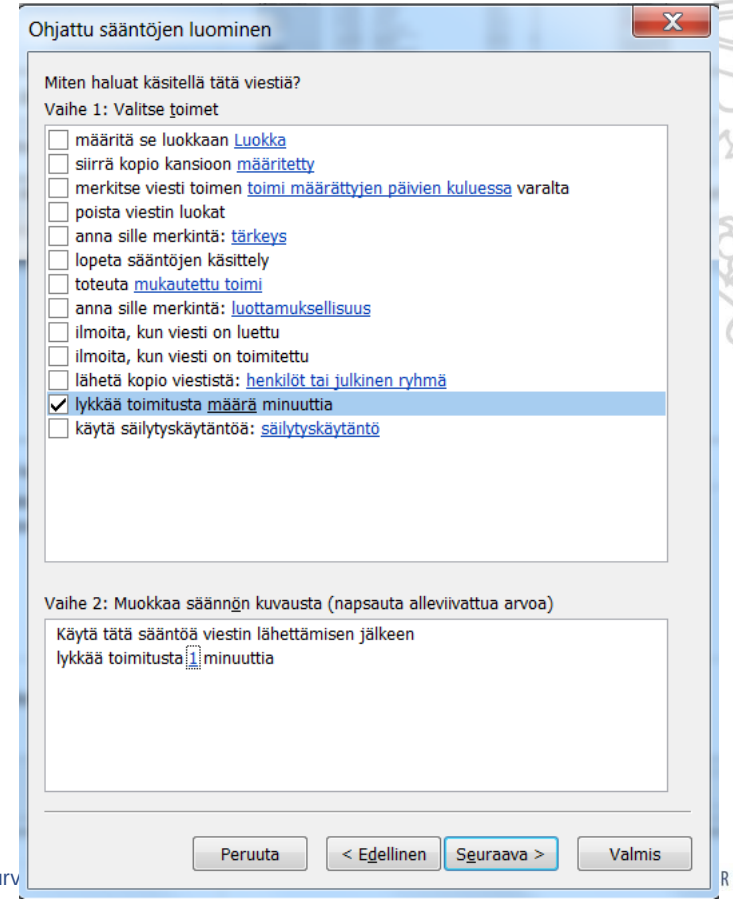


napauta Seuraava

(jos tulee jokin ilmoitus, napauta Ok)

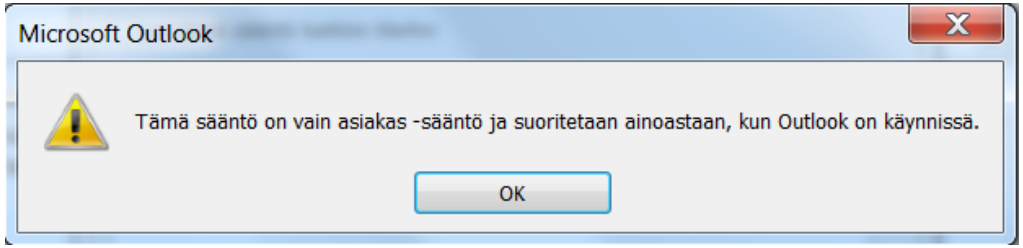
Kimmon oma vinkki – Outlookin katumusviive

- Valitse **”lykkää toimitusta määrä minuuttia”**
  - Itse käytän 1 minuuttia, voi olla toki suurempi, mutta harvoin ollut tarve pitemmälle aikaviiveelle
- napauta **Seuraava**
  - Tähän voi tehdä myös poikkeuksia
- napauta **Seuraava**

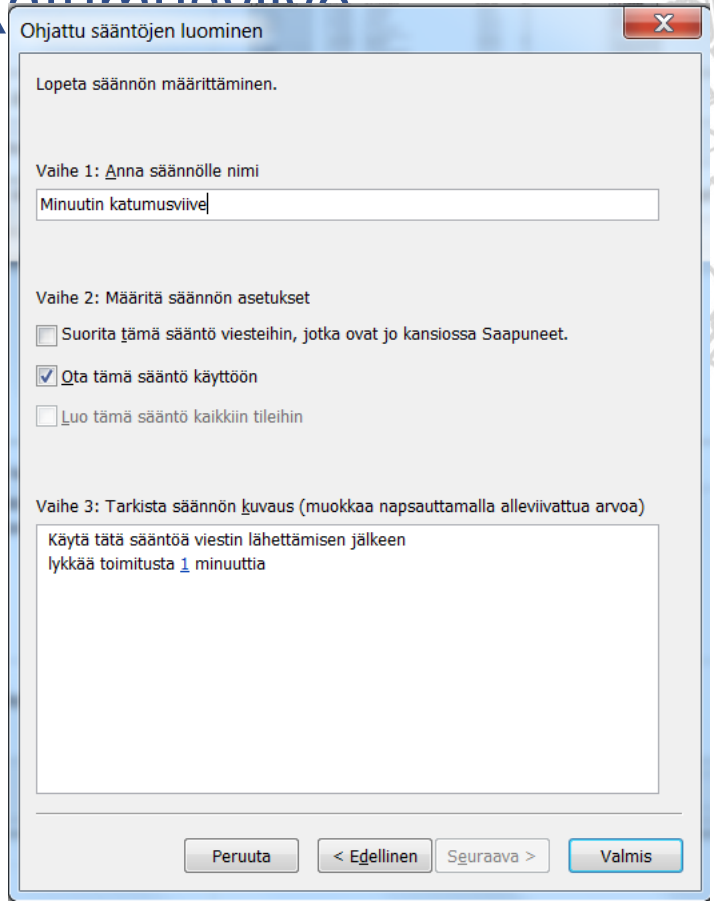


Kimmon oma vinkki – Outlookin katumusviive

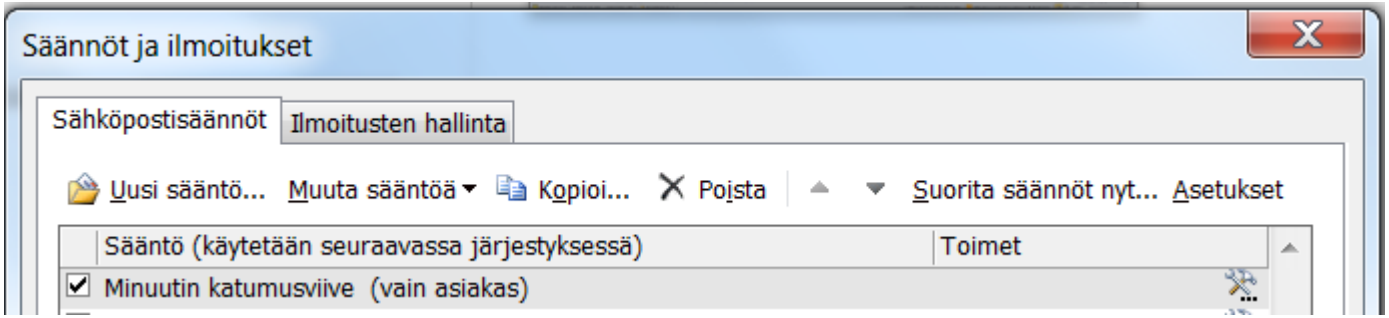
- Anna säännölle kuvaava nimi ja napauta **Valmis**.



- Hyväksy asiaan kuuluva ilmoitus ok.

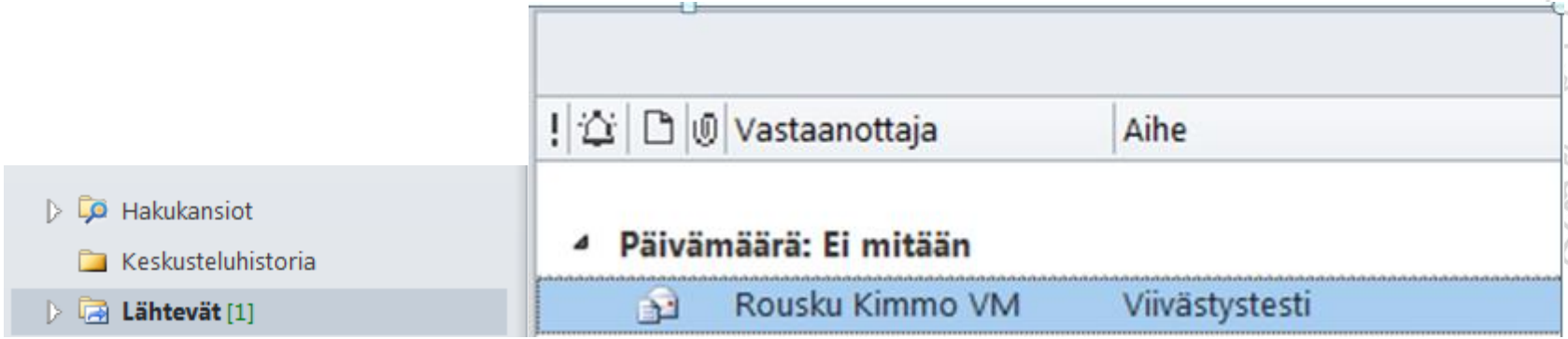


Kimmon oma vinkki – Outlookin katumusviive



- Edellisen toimenpiteen seurauksena sinulle nyt uusi sääntö, joka viivästyttää jokaista lähettämääsi viestiä minuutilla. Huomaa, tämä ei koske kännykästä lähetettäviä sähköpostejasi.
- Miten pääset muokkaamaan viestiä, jos huomaat että jotain pitääkin muuttaa? Lähetä testiviesti – voit lähettää sen vaikka itsellesi.

Kimmon oma vinkki – Outlookin katumusviive



- Etsi Outlookin kansiorakenteesta **Lähtevät** (Outbox) –kansio. Siellä on yksi viesti – juuri lähettämäsi testiviesti. Se pysyy Lähtevät kansiossa minuutin, jonka jälkeen viesti lähtee, ellet ala sitä ennen sitä muokkaamaan.
- Voit siis avata viestin normaalisti ja muokata viestiä – kun lähetät sen uudelleen, lähtee se muutostesi jälkeen kun napautat Lähetä

VALTIOVARAINMINISTERIÖ

Kimmo Rousku
VAHTI-pääsihteeri
Puh. 02955 30140
Lisätieto: kimmo.rousku@vm.fi vahti@vm.fi
www.vm.fi/vahti – www.vahtiohje.fi –
www.arjentietosuoja.fi

