VALTIOVARAINMINISTERIÖ

VAHTI-tilannekatsaus sekä VAHTI 2/2015 Ohje salauskäytännöistä -tilaisuus ICT-toimittajille

15.3.2016 Kimmo Rousku

Tilaisuuden ohjelma

Ohjelma:

8.45 Ilmoittautuminen

9.00 Tervetuloa! - Aku Hilve, VM

9.10 VAHTI Salausohjeen esittely - Kimmo Rousku, VM

9.40 Lyhyt oppimäärä - Mistä salauksessa on kyse? – Risto Hakala, Viestintävirasto

10.10 Kahvitauko

10.30 Mitkä ovat tietojen salauksen keskeiset haasteet?

Miten toimittajien pitäisi ottaa ohje huomioon? - Aki Tauriainen, Viestintävirasto

11.00 Muuta ajankohtaista VAHTI-toiminnassa – Kimmo Rousku, VM

11.45 Keskustelu sekä kysymyksiä ja vastauksia –osio

12.15 Tilaisuus päättyy

Tervetuloa!

Yksikön päällikkö, VAHTIn puheenjohtaja **Aku Hilve**

Esityksessäni

- VAHTI?
- Miksi salaus on tärkeää?
- Muuttunut uhkatilanne
- Salaus on mahdollistaja
- Ohjeen esittely

JulkICT-osasto

Valtiovarainministeriön Julkisen hallinnon tieto- ja viestintätekninen (ICT) -osasto vastaa julkisen hallinnon tietohallinnon, sähköisen asioinnin ja tietovarantojen käytön yleisestä kehittämisestä, valtionhallinnon tietohallinnon ohjauksesta ja yhteisten kehittämishankkeiden yhteensovittamisesta.

JulkICT-toiminto 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.

VAHTI

- VAHTI toimii siten julkisen hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä.
- VAHTIn tavoitteena on tieto- ja kyberturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista.
- Tavoitteena on myös edistää tieto- ja kyberturvallisuuden sekä ICT-varautumisen saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta sekä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa ja käyttöä.

VAHTI

- VAHTIn hankkeisiin kootaan eri hallinnonaloilta kohteeseen parhaiten sopiva asiantuntemus. VAHTI osallistuu tarvittaessa valtionhallinnon näkökulmasta kansallista ja kansainvälistä tietoturvallisuutta kehittävien yhteistyöryhmien toimintaan sekä valmistelee tai valmisteluttaa näiden kanssa mahdollisesti valtionhallinnolle annettavat linjaukset.
- **Suomen kyberturvallisuusstrategian mukaisesti VAHTI käsittelee ja yhteen sovittaa valtionhallinnon keskeiset tieto- ja kyberturvallisuuden linjaukset.**

VM:n ohjausrooli

Laki julkisen hallinnon tietohallinnon ohjauksesta (2011)

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (2011) 5§

Valmiuslaki (2013) §105

Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013)

Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015

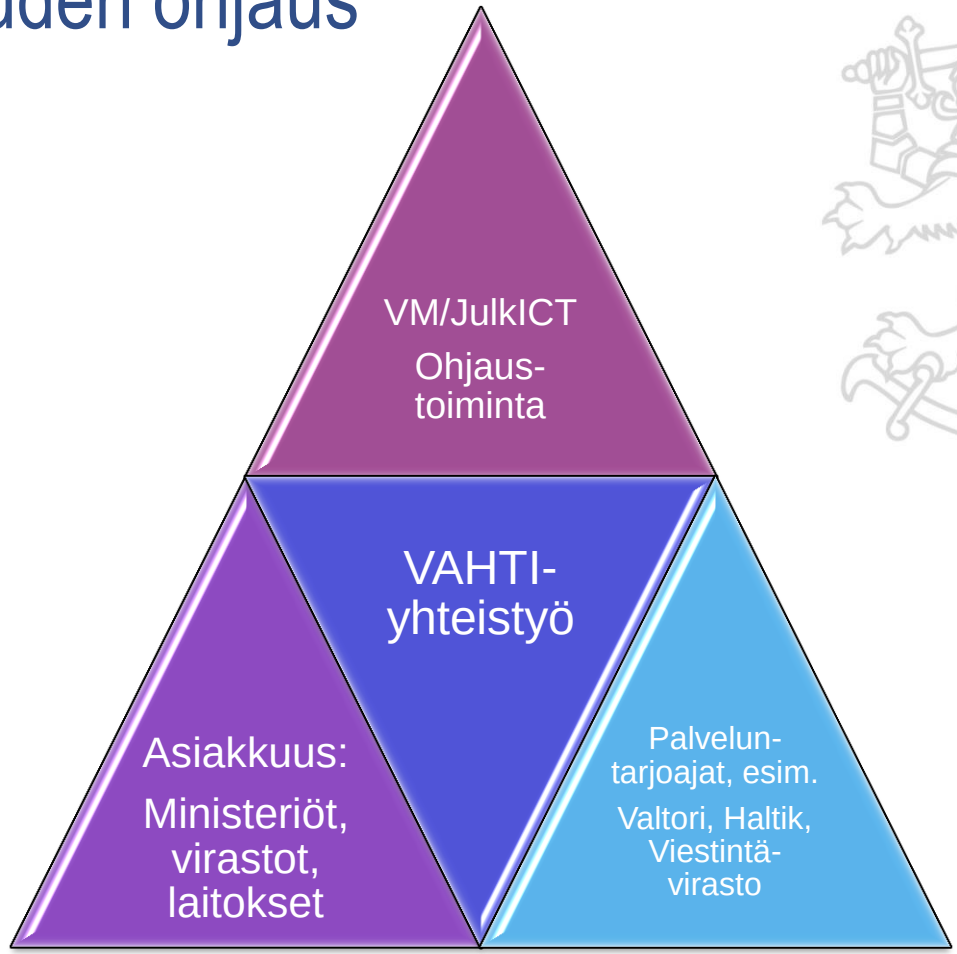
Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä valtionhallinnossa (2009)

Yhteiskunnan turvallisuusstrategia (2010)

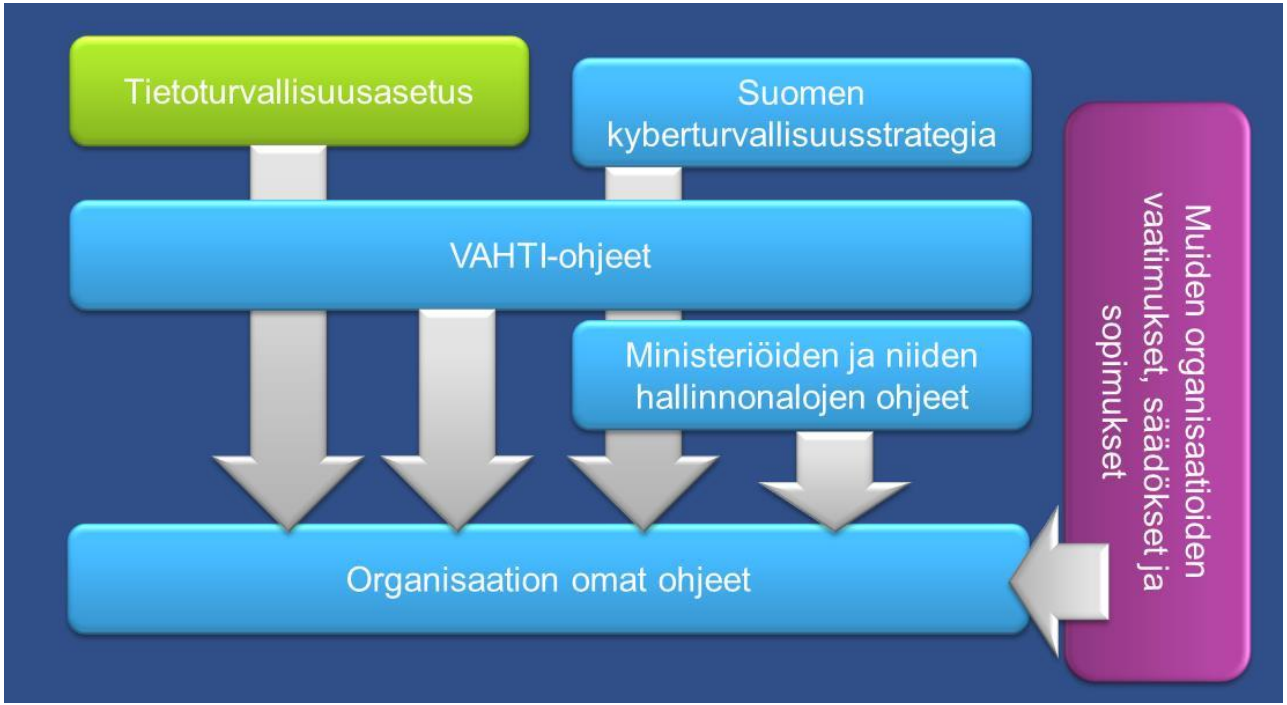
Kansallinen kyberturvallisuusstrategia (2013)

Tieto- ja kyberturvallisuuden ohjaus valtionhallinnossa

- Kuten kaikessa toiminnassa, erityisesti **luottamusta** edellyttävässä tieto- ja kyberturvallisuudessa yhteistyön merkitys on keskeinen

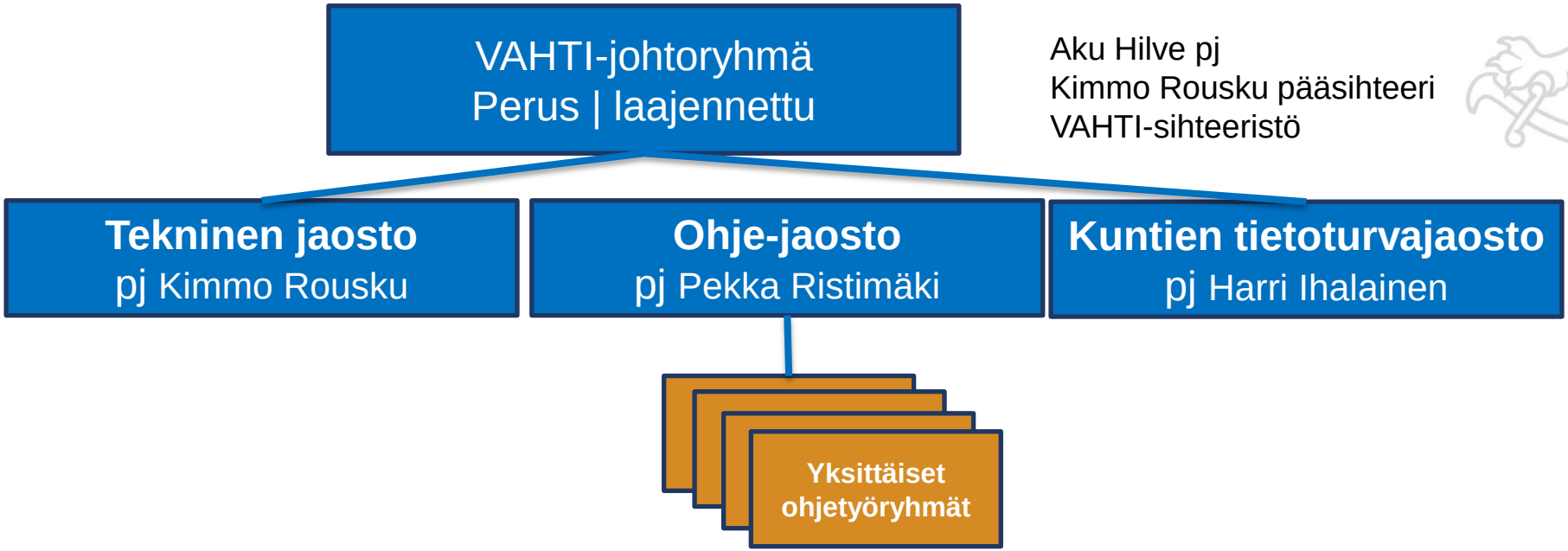


Tieto- ja kyberturvallisuuden ohjaus valtionhallinnossa



Toiminta

- VAHTI johtoryhmä




Ohje salauskäytännöistä
Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
– VAHTI 2/2015
Julkisen hallinnon ICT

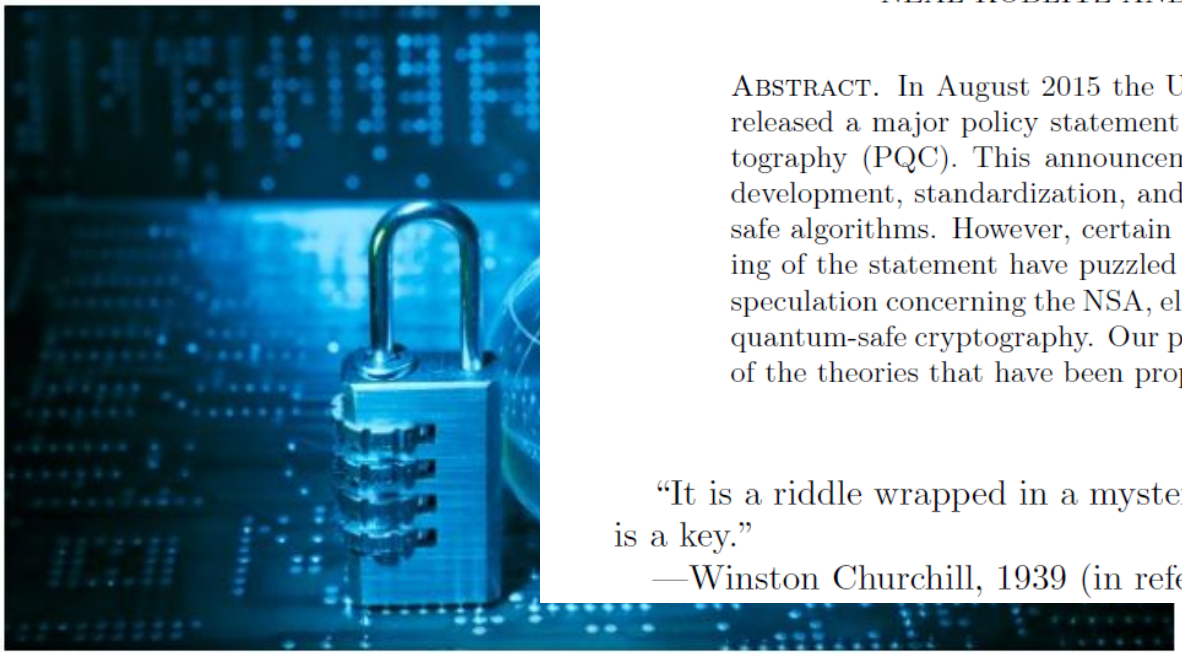
Miksi salaus on tärkeää? > osa riskienhallintaa !

- Suojaus, sen puute tai huono toteutus päätyvät säännöllisesti myös uutisiin. Kenties yleisin esimerkki on tietomurto verkkopalveluun, jonka käyttäjätietokannassa olevat salasanat ovat vuotaneet murtautujalle; väärällä tavalla salatut salasanat puretaan ja murtautuja julkaisee ne selväkielisinä.
- Edellisten lisäksi nopeasti kasvava uhka on yritysten maksuliikenne- tai muihin talousjärjestelmiin murtautuminen ja asiakas- tai luottokorttitietojen varastaminen sekä niiden hyödyntäminen rikollisesti.
- Kaikki edellä olevat esimerkit ovat sellaisia, jotka uhkaavat myös julkishallinnon toimintaa ja tietoja. Tiedon salaaminen liittyy osittain kaikkiin edellä mainittuihin esimerkkeihin.
- Eräs tämän vuosikymmenen loppupuolen keskeisiä suuntauksia tuleekin olemaan tiedon salauksen merkityksen kasvu ja sen käytön laajentuminen

Muuttunut uhkatilanne

Is the NSA trying to warn us that cryptography is de

By Graham Templeton on October 27, 2015 at 9



A RIDDLE WRAPPED IN AN ENIGMA

NEAL KOBLITZ AND ALFRED J. MENEZES

ABSTRACT. In August 2015 the U.S. National Security Agency (NSA) released a major policy statement on the need for post-quantum cryptography (PQC). This announcement will be a great stimulus to the development, standardization, and commercialization of new quantum-safe algorithms. However, certain peculiarities in the wording and timing of the statement have puzzled many people and given rise to much speculation concerning the NSA, elliptic curve cryptography (ECC), and quantum-safe cryptography. Our purpose is to attempt to evaluate some of the theories that have been proposed.

"It is a riddle wrapped in a mystery inside an enigma; but perhaps there is a key."

—Winston Churchill, 1939 (in reference to the Soviet Union)

Muuttunut uhkatilanne

Edward Snowden: we may never spot space aliens thanks to encryption

And extraterrestrials may never notice us, either, if our technology is sufficiently sophisticated, whistleblower tells Neil deGrasse Tyson

Former intelligence contractor Edward Snowden says encryption could get in the way of any communication with aliens. Photograph: Frederick Florin/AFP/Getty Images

Will NSA whistleblower Snowden release proof of alien visitations to Earth?

UFO chasers hope NSA whistleblower Edward Snowden may be on the brink of releasing a string of confidential US files proving the existence of aliens after he talked turkey about extra terrestrials for the first time.

Muuttunut uhkatilanne

Laskentatehon nopea kehittyminen heikentää salausta

Tiedon salaaminen pohjautuu matemaattisiin algoritmeihin. Erilaisten laskenta-alustojen suorituskyvyn kehittyminen Mooren lain mukaisesti vaikuttaa käytettävissä olevien salausteknologioiden luotettavuuteen. Esimerkiksi 1980- tai 1990-luvulla kuviteltu avaimen pituus ei ole enää turvallinen, koska käytettävät teknologiat ovat kehittyneet ja sitä myötä avainten auki purkamiseen kuluva aika on oleellisesti lyhentynyt. Myös pilviteknologia tuo uusia ja helpommin saatavilla olevia hyökkäystapoja esimerkiksi salasanojen murtamiseen. Mitä kriittisemmästä ja pitkäaikaisemmasta säilytyksestä on kyse, sitä tärkeämpää on huolehtia käytettävien avainten pituudesta siten, että ne turvaavat tiedot koko niiden salassapidolta edellytettävän ajan. Lisätietoa tiedon salaamisesta viranomaiskäytössä antaa kyberturvallisuuskeskus (ncsa@ficora.fi).

Salaus on mahdollistaja

- Hyvä esimerkki salaustarpeesta on pilvipalvelu, jossa salassa pidettävät tiedot sijaitsevat organisaation ulkopuolella, mahdollisesti ulkomailla, ja niitä käytetään internet-verkon ylitse. Pilvipalveluiden käyttöä voidaan laajentaa siinä vaiheessa kun niissä on mahdollista käyttää asiakkaan tarkastamaa ja hyväksymää tiedon salausratkaisua. Lisäksi salaukseen liittyvä avaintenhallinta tulee toteuttaa siten, että myös se täyttää kaikki asiakkaan edellyttämät vaatimukset.
- Kuten kaikessa toiminnassa, myös salauksen suunnittelussa, toteutuksessa, käyttöönotossa ja ylläpidossa tulee hyödyntää riskienhallintaa sekä ottaa huomioon lakisääteiset ja organisaation liike- tai ydintoiminnan vaatimukset sekä mahdolliset haasteet, joita käytettävä salaus saattaa sille asettaa.
- Tietojen salaus tulee huomioida myös organisaation arkkitehtuurisuunnittelussa ja -toteutuksessa siten, että organisaatio kehittää ja hyödyntää salausteknologiaa suunnitelmallisesti osana arkkitehtuurinsa kehittämistä.

Salaus on mahdollistaja

- digitalisoinnin kasvava tarve; yhä useampi toiminto on sähköistetty ja kehitys tulee tältä osin vielä kiihtymään laajamittaisen, kokonaisia toimintaketjuja koskevan digitalisoinnin myötä
- ajasta ja paikasta riippumaton työskentely sekä julkishallinnossa että julkishallinnon palveluita käyttävien asiakkaiden ja kansalaisten keskuudessa uusien päätelaitteiden ja langattomien tietoliikenneyhteyksien kehittyminen
- uudenlaiset palveluiden tuotantotavat, palveluiden virtualisoiminen, jaetut kapasiteettipalvelut sekä pilvipalvelut

Ohjeemme sisältö

Sisällysluettelo

Haastava kokonaisuus!

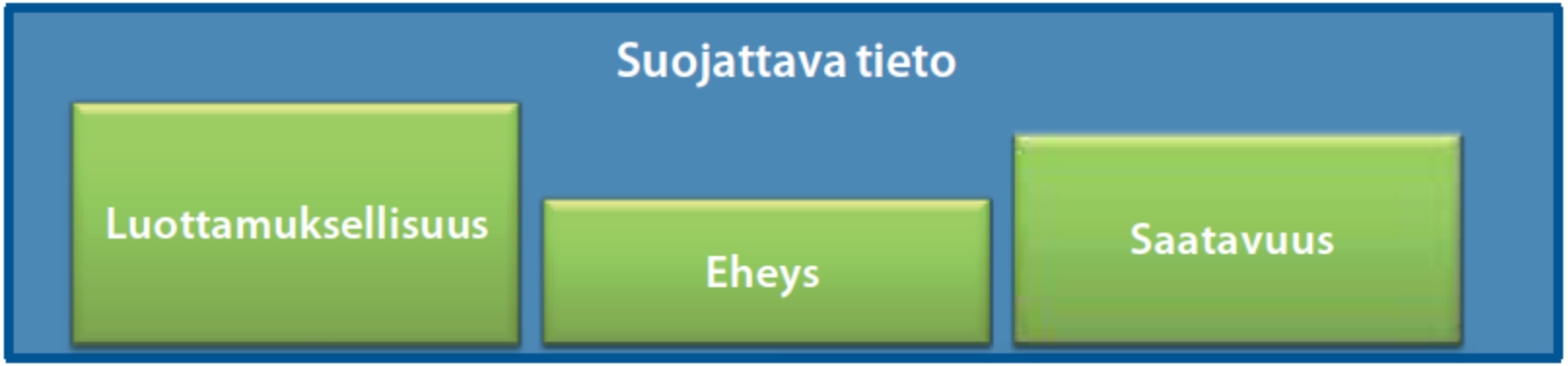
Tämä on ollut ehdottomasti haastavin ohje, jossa olen ollut missään muodossa mukana viimeisen vajaan kymmenen vuoden aikana, mitä olen VAHTI-ohjeiden osalta mukana ollut!

Erityisesti itselleni tämä on avannut silmät meidän keskeisen haasteen osalta, kansallisen krypto-osaamisen ja tuote-kehityksen tärkeyden ja merkityksen

Yksittäisiä nostoja

L – E – S (CIA)

Kuvio 1. Luottamuksellisuus, eheys ja saatavuus; tietoturvallisuuden osa-alueiden merkitys vaihtelee suojattavan kohteen mukaan.



- Etenkin toiminnan digitalisaatio edellyttää tietoturvallisuuden kaikkien osa-alueiden huomioimista ja näiden osa-alueiden riskienhallintaa – VAHTIn ohjejaoston meneillään olevat ohjetyöryhmät julkaisevat ensi vuonna tätä kokonaisuutta tukevia ohjeita

Ohjeen tavoite – et tajua kaikkea – **HYVÄ!**

1.3 Ohjeen tavoite

Tämän ohjeen tavoitteena on:

- kertoa tiedon salauksesta yleisellä tasolla siten, että lukija saa käsityksen myös aihekokonaisuuteen liittyvistä haasteista ja salauksen tulevaisuudennäkymistä
- ohjeistaa, kuinka salaus tulisi ottaa huomioon organisaatioiden eri toiminnoissa
- antaa ohjeita ja tietoa siitä, miten ja mistä salaukseen liittyvää lisätietoa on saatavilla
- päivitettävien, verkossa sijaitsevien liitetiedostojen avulla määrittää valtionhallinnossa käytettäviä teknisiä salaukseen liittyviä vaatimuksia

On salausta (placebo, turvallisuuden tunne), ja on oikeaa salausta
- Tässä tarvitaan oikeaa asiantuntemusta

Ohjeen kohderyhmä – ei sellaisenaan käyttäjille!

1.4 Ohjeen kohderyhmä

Tämä ohje on tarkoitettu organisaatiossa kaikille niille tahoille, joiden tehtävänä on vastata organisaation

- ICT-arkkitehtuurista
- ICT-palveluista
- järjestelmien suunnittelusta ja kehittämisestä
- järjestelmien operatiivisesta palvelutuotannosta
- tietoturvallisuudesta

Ohje ei ole tarkoitettu sellaisenaan jaettavaksi organisaation henkilöstölle. Ohje tulee ottaa huomioon suunniteltaessa ja kehitettäessä tietojärjestelmiä tai muita tiedon salausta edellyttäviä kohteita.

1.5 Ohjeen rakenne

Tämä ohje jakautuu kuuteen lukuun ja kahteen (2) liitteeseen. Lukujen keskeinen sisältö on seuraava:

1. Tausta ja tavoite; kertoo mikä on salauksen merkitys osana tietojen luottamuksellisuuden takaamista, joka on yksi kolmesta tietoturvallisuuden kulmakivestä
2. Tiivistelmä – tarkistuslistat; kuvaa salauksen näkökulmasta tärkeimmät asiat organisaatiolle ja henkilöstölle sekä sisältää huoneentaulut em. ryhmille
3. Tietoturvallisuusasetus, tietoturvatasot ja muut viitekehykset; listaa keskeisimmät aihepiiriin liittyvät valtionhallinnon viitekehykset sekä kuvaa, miten tietojen salausta on käsitelty ja millaisia vaatimuksia on erityisesti tietoturvallisuusasetuksessa sekä sen täytäntöönpanoa tukevissa VAHTI-ohjeissa
4. Tiedon salaaminen – tekninen viitekehys; teknologiset asiat ja termit, jotka jokaisen salausasioiden kanssa työskentelevän henkilön tulisi hallita
5. Avaintenhallinta; keskeinen osa-alue, koska jopa hyvin toteutettu salauskokonaisuus voi sortua huonosti tai virheellisesti toteutetun avaintenhallinnan vuoksi
6. Salausratkaisun valinta ja käyttöönotto; kuvaa mihin asioihin salausratkaisun valinnassa ja käyttöönotossa tulee kiinnittää huomiota sekä erilaisia käyttötapauksia salausten toteuttamisesta

2.1 Huoneentaulu – organisaatio

1. Luokittele tiedot oikeaoppisesti! Tietoaineistojen oikeaoppinen luokittelu; mikäli luokittelu tehdään väärin tai tarpeettoman laajasti tietojärjestelmän eri ympäristöihin (esim. kehitys-, testiympäristöt tai muut tietojärjestelmän osat), se aiheuttaa joko ylimääräisiä kustannuksia (yliluokiteltu) tai vaarantaa salassa pidettävän tiedon luottamuksellisuuden (aliluokittelu).

2. Salaa tarpeen mukaan! Tarve-analyysi; kartoittakaa mihin tietojen salausta tarvitaan ja mitkä ovat ne vaatimukset, joihin tiedon salaaminen perustuu.

3. Ole erityisen huolellinen kansainvälisiä salassa pidettävien tietojen käsittelyä suunniteltaessa ja toteutettaessa! Kansainvälisten salassa pidettävien tietojen käsittelyvaatimukset poikkeavat vastaavista kansallisista vaatimuksista.

4. Määritä tarpeet ja vaatimukset! Käytettävien salaustuotteiden määrittely ja valinta; usein toteutuksia tai palveluita hankittaessa todetaan riittäväksi, että siinä on jokin salaus. Tässä ohjeessa pyritään tuomaan esille se, että on olemassa myös salauksia, joita ei ole aina toteutettu huolellisesti ja vaatimusten mukaisesti.

5. Ota tuote käyttöön oikeaoppisesti! Salaustuote sellaisenaan ei riitä, vaan tulee myös selvittää tuotteen kyseiseen käyttötarkoitukseen soveltuvat ominaisuudet, asetukset ja konfiguraatio (esim. että vahingossa ei sallita käyttöön vanhentuneita tai heikommin turvattuja ominaisuuksia, protokollia tai vastaavia asetuksia tai toimintoja).

6. Suunnittele avaintenhallinta! Vaikka salaus olisi muuten toteutettu huolellisesti ja oikeaoppisesti, kaikki vaatimukset huomioiden ja täyttäen, ratkaisu voidaan pilata puutteellisesti suunnitellulla avaintenhallinnalla.

7. Toteuta avaintenhallinta suunnitelman mukaisesti! Vaikka kaikki olisi suunniteltu huolellisesti, erityisesti avaintenhallinnan osalta pitää esimerkiksi auditointien ja tarkastusten avulla varmistua siitä, että suunnitelmat on myös toteutettu sovitulla tavalla ja vaatimustenmukaisesti.

8. Hallitse varmenteita! Salausjärjestelmiin liittyy yleensä varmenteita, joilla on voimassaoloaika. Organisaatioiden tulee huolehtia varmenteiden uusimisesta hyvissä ajoin ennen niiden vanhenemista. Tämä pitää vastuuttaa ja keskittää siten, että käytettävistä varmenteista on olemassa ajantasainen tieto ja prosessi niiden hallitsemiseksi.

9. Salaa kiintolevyt! Organisaation on syytä salata kaikkien työasemien kovalevyt. Internetistä löytyy helposti lukuisia helppokäyttöisiä ohjeita, joiden avulla voidaan päästä kiinni salaamattoman työaseman tietoihin. Hyvä kiintolevyn salaustuote pienentää tätä riskiä.

10. Muista auditoida! Kokonaisuuden auditoiminen; kaikkia palveluita tai tietojärjestelmiä ei ole tarkoituksenmukaista tai järkevää auditoida. Oleellista on se, että organisaatiolla on suunnitelma, joka kuvaa, mitkä ovat auditointia edellyttäviä palveluita tai tietojärjestelmiä ja kuinka auditoinnit toteutetaan. Käytännössä suunnitelma voi olla esimerkiksi osa palvelun tietoturvallisuuden vuosikelloa.

11. Toteuta monikerroksinen suojausratkaisu! Salaus on vain yksi osa organisaation monikerroksista suojautumista. Se ei yksinään riitä, mutta se on tärkeä osa ns. sipulimaisessa tietoturva-arkkitehtuurissa. Monikerroksisen rakenteen avulla varaudutaan siihen, että yksittäisen osa-alueen pettäessä tai murtautujan päästessä yhdestä kerroksesta läpi, seuraavat kerrokset suojaavat edelleen tietoa.

12. Muista vastuut! Omistajan vastuu; organisaatio on aina itse vastuussa omistamistaan tiedoista ja käytössään olevista tietojärjestelmistä, vaikka niiden toteuttamisesta vastaisi jokin ulkopuolinen taho, joko valtionhallinnon organisaatio tai kaupallinen toimittaja. Vastuuta ei ole mahdollista ulkoistaa.

2.2 Huoneentaulu – käyttäjä

1. Opettele luokittelemaan tiedot oikein! Tietoaineistojen oikeaoppinen luokittelu; vaikka organisaatio olisi toteuttanut tietojärjestelmät ja niiden salausratkaisut oikeaoppisesti, se ei auta, mikäli henkilöstö ei osaa luokitella tietoa ja käyttää luokituksen mukaisia tietojärjestelmiä oikein läpi tiedon koko elinkaaren.

2. Käytä salassa pidettävän tietojen käsittelyyn niitä varten tarkoitettuja ohjelmia ja palveluita! Henkilöstön tulee käyttää määrättyjä työvälineitä ohjeistetulla tavalla, mukaan luettuna tiedon salausratkaisut sähköpostin käsittelyssä, päätelaitteiden käytössä sekä tiedon kuljettamisessa ulkoisilla apumuisteilla (usb- ja muut muistit). Nämä tulee huomioida toimittaessa työpaikalla, työmatkalla tai etätöissä.

3. Toimimme vaatimustenmukaisesti! Valtionhallintoon kohdistuu usein tiukemmat turvallisuusvaatimukset kuin yksityisiin yrityksiin. Tämän takia tulee huomata, että kaikkia yksityisellä puolella käytössä olevia palveluita tai toimintatapoja ei ole välttämättä mahdollista käyttää valtionhallinnossa, johtuen esimerkiksi tietojen salassapitoon tai salaukseen liittyvistä vaatimuksista.

4. Noudata annettuja ohjeita! Vaikka digitalisoimme toimintojamme kiihtyvällä tahdilla, tietoaineistoja käsitellään jatkossakin usein tavoin, jotka eivät kaikki ole sähköisiä. Esimerkiksi keskusteluissa tai paperimuotoisissa aineistoissa tietojen salaaminen ei ole mahdollista samalla tavoin kuin tietojärjestelmissä tai tietoliikenteessä. Tietojen käsittelyssä on noudatettava organisaation antamia ohjeita turvallisesta työskentelystä.

5. Ole aktiivinen, ilmoita poikkeamista! Henkilöstön velvoitteena on kysyä ja kyseenalaistaa asioita silloin kun herää epäilys, että jokin asia ei ole niin kuin sen pitäisi olla tai että asiassa vaikuttaisi olevan jotain outoa. Esimerkiksi jos käyttäjä saa sähköpostitse salassa pidettävää tietoa, jota ei ole millään lailla salattu. Samoin jos www-sivusto huomauttaa siitä, että sen käyttämä varmenne ei ole toimiva, tulee ottaa yhteyttä joko palvelua tuottavan tai oman organisaation palvelupisteeseen ja pyytää korjaamaan asia tai muuten selvittämään sitä.

Muita tähän liittyviä materiaaleja!

LIITE 1

Liite 1. Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot

Liitettä ylläpidetään ja säilytetään viestintäviraston sivustolla osoitteessa https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/ncsa-fi.html

Kohdasta asiakirjat:

Kryptografiset vahvuusvaatimukset - kansalliset suojaustasot.pdf. Lisäksi linkki asiakirjaan löytyy tämän ohjeen www-sivulta osoitteesta www.vahtiohje.fi.

Seuraavaksi kaksi Viestintäviraston Kyberturvallisuuskeskuksen esitystä, joiden välissä on

VAHTI-ajankohtaiskatsaus

Tekninen jaosto

- TUKIMATERIAALI: tarkastusten ja auditointien suorittaminen ja niihin valmistautuminen
  - Julkaistaan kesälomien jälkeen
  - Seminaari myös toimittajille osana muuta ajankohtaisseminaaria

Kuntien tietoturvajaosto

- Jalkautamme VAHTI-työssä kehitettyjä toimintamalleja, parhaita käytäntöjä ja ohjeita kuntien käyttöön
  - Kesällä / syksyllä 2015 toteutimme kuntien tieto- ja kyberturvallisuuskyselyn, osin samalla mallilla millä valtionhallintoon
  - 93 vastausta eli noin 30% vastausprosentti
  - Eroja valtionhallintoon on, johtuen todellla laaaaajasta kultakentästä ja ääripäät kuntakentällä merkittävästi laajemmat mitä valtionhallinnon organisaatioiden kesken

Ohjejaosto – meneillään olevat hankkeet

- **VAHTI-ohje 2/2016 Toiminnan jatkuvuuden hallinta**
  - **Pj Riitta Gröhn, Aalto-yliopisto**
- https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=908454ca-81bb-4ea1-8165-2e25b4b7b603
  - Suosittelen tutustumaan, ennen kaikkea vaikutusanalyysityökalu (BIA)
- **Sähköisen asioinnin tietoturvallisuus**
  - Pj Kimmo Janhunen, ORK
- **Tietoturvapoikkeamien hallinta**
  - Pj Juha Ilkka, VNK
- **VAHTIn tieto- ja kyberturvallisuuden hallintarakenteen päivittämisen hankeryhmä**
  - Pj Kirsi Janhunen

Johtaminen ja riskienhallinta	**Turvallisuustoiminnan johtaminen ja organisointi** tietoturvallisuuden hallintajärjestelmä (ISMS) riskienhallinta henkilöstöturvallisuus hankinnat ja sopimukset viestintä
Tiedon ja suojattavien kohteiden turvallisuuden hallinta	**Kehittäminen ja toteuttaminen** suojattavien kohteiden tunnistaminen/hallinta tietojen luokittelu suojausten määrittely, suunnittelu ja toteutus riippuvuuksien tunnistaminen?
Toimintaympäristön turvallisuuden hallinta	**Operatiiviset toimenpiteet** käyttöturvallisuus ja prosessit fyysinen ja ympäristön turvallisuus poikkeamatilanteista toipuminen
Toiminnan jatkuvuuden hallinta	**Suunnittelu ja varautuminen** valmiussuunnittelu jatkuvuussuunnittelu ICT-varautuminen toipumissuunnittelu harjoittelu ja testaaminen
Seuranta ja arviointi	**Vaatimustenmukaisuuden varmistaminen** itsearvioinnit ulkoiset auditoinnit

Ohjejaosto – meneillään olevat hankkeet

- **VAHTI-portaali**
  - Jossa julkaistaan uusittu hallintarakenne, muu materiaali, päivitetyt, uudet VAHTI-ohjeet sekä erilliset vaatimukset
- **Lainsäädännön uudistaminen**
  - Asetetaan uusi ryhmä huhtikuun VAHTI-ryhmä
    - Osa arkistolain uudistuksen yhteydessä suunniteltua tietojenhallinnan ja tietojenkäsittelyn lakikokonaisuutta, jonka valmisteluvastuussa on valtiovarainministeriö
    - Selkiyttää tietoturvallisuusasetuksen osalta havaittuja kehittämistä vaativia osa-alueita, purkaa normeja, helpottaa kaikkien meidän työtä
  - HE valmis v 2017, laki voimaan v 2018
    - Järjestämme tästä erillisiä kuulemistilaisuuksia mm nykytilan kuvaamisen osalta (VM:n vastuuhenkilönä toimii Saana Seppänen)

Ohjejaosto – meneillään olevat hankkeet

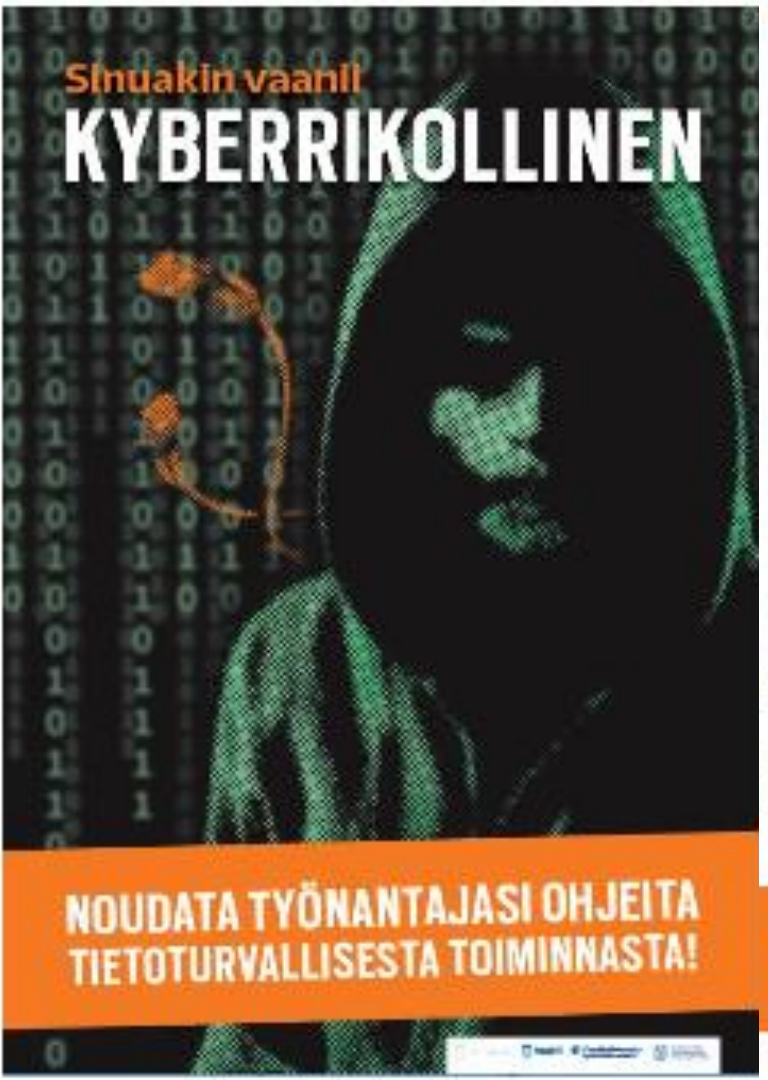
- **EU-tietosuoja-asetusryhmä**
  - Raportti lainsäädäntökokonaisuuden vaikutuksista tieto- ja kyberturvallisuuden näkökulmasta – **toukokuu 2016**
    - Sekä tähän liittyviä seminaareja myös syksyllä
    - Raportin päivitys v 2016-2017

Muuta

- **VAHTI-toimintakertomus vuodelle 2015**
  - Julkaistaan huhtikuussa – sisältää mm. tarkemmat tulokset meidän kyselyistä
- **VAHTI-salausohjeen englanninkielinen versio**
  - Julkaistaan huhti/toukokuussa
- **Digital Security Risk Management for Economic and Social Prosperity**
  - Julkaistaan huhti/toukokuussa suomenkielisenä
- **Henkilöstön tietoturvakysely**
  - Tarkoitus mahdollistaa kysely julkishallinnon osalta kesälomien jälkeen

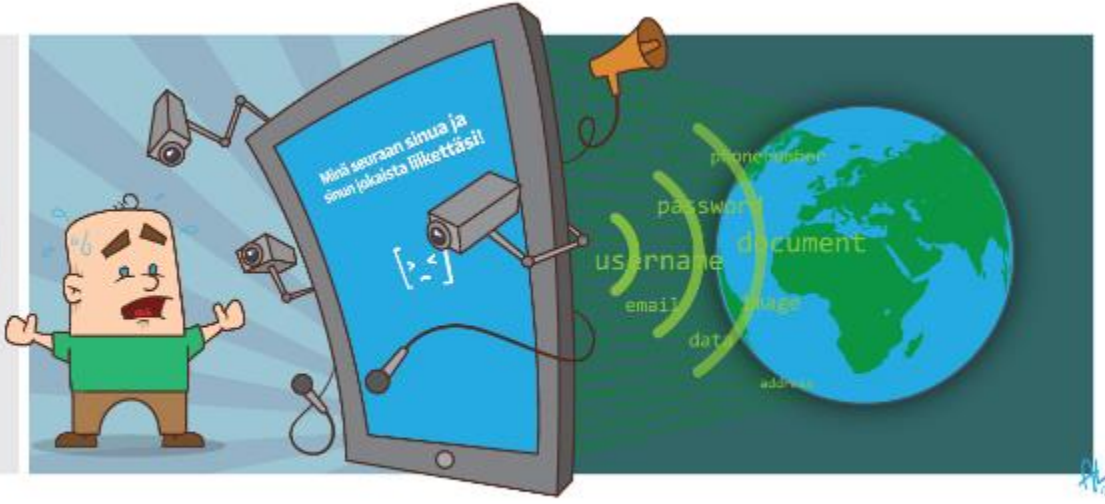
Julkishallinnon tietoturvaviikon aktiviteetit

- Toteutimme 8-12.2.2016 viikolla tieto- ja kyberturvatietoisuutta edistäneen kampanjan, jossa julkaisimme viisi sarjakuvaa sekä kolme julistetta
- Vapaasti hyödynnettävissä https://www.vahtiohje.fi/web/guest/tieto-ja-kyberturvallisuus-viikko-2016


Sinuakin vaanii
KYBERRIKOLLINEN
NOUDATA TYÖNANTAJASI OHJEITA
TIETOTURVALLISESTA TOIMINNASTA!


Kyberturvallisuuden avulla huolehdimme
yhteiskunnan toiminnasta kaikissa olosuhteissa
NOUDATA TYÖNANTAJASI OHJEITA TIETOTURVALLISESTA TOIMINNASTA,
TOIMI TURVALLISESTI MYÖS VAPAA-AJALLA!

www.vahtiohje.fi



Ennen kuin asennat laitteellesi Appseja tai muita sovelluksia, tarkista millaisia oikeuksia se edellyttää toimiakseen.

Ennen Q&A-osiota, erillinen esitys SecICT-hankkeen tilanteesta – VIRT-toiminnan johtaja Kirsi Janhunen

Kysymyksiä ja vastauksia läpikäydyistä tai muista tuntemattomista aiheista ☺ ?

VALTIOVARAINMINISTERIÖ

Kimmo Rousku
VAHTI-pääsihteeri
Puh. 02955 30140
Lisätieto: etunimi.sukunimi@vm.fi
www.vm.fi

Kiitos!