



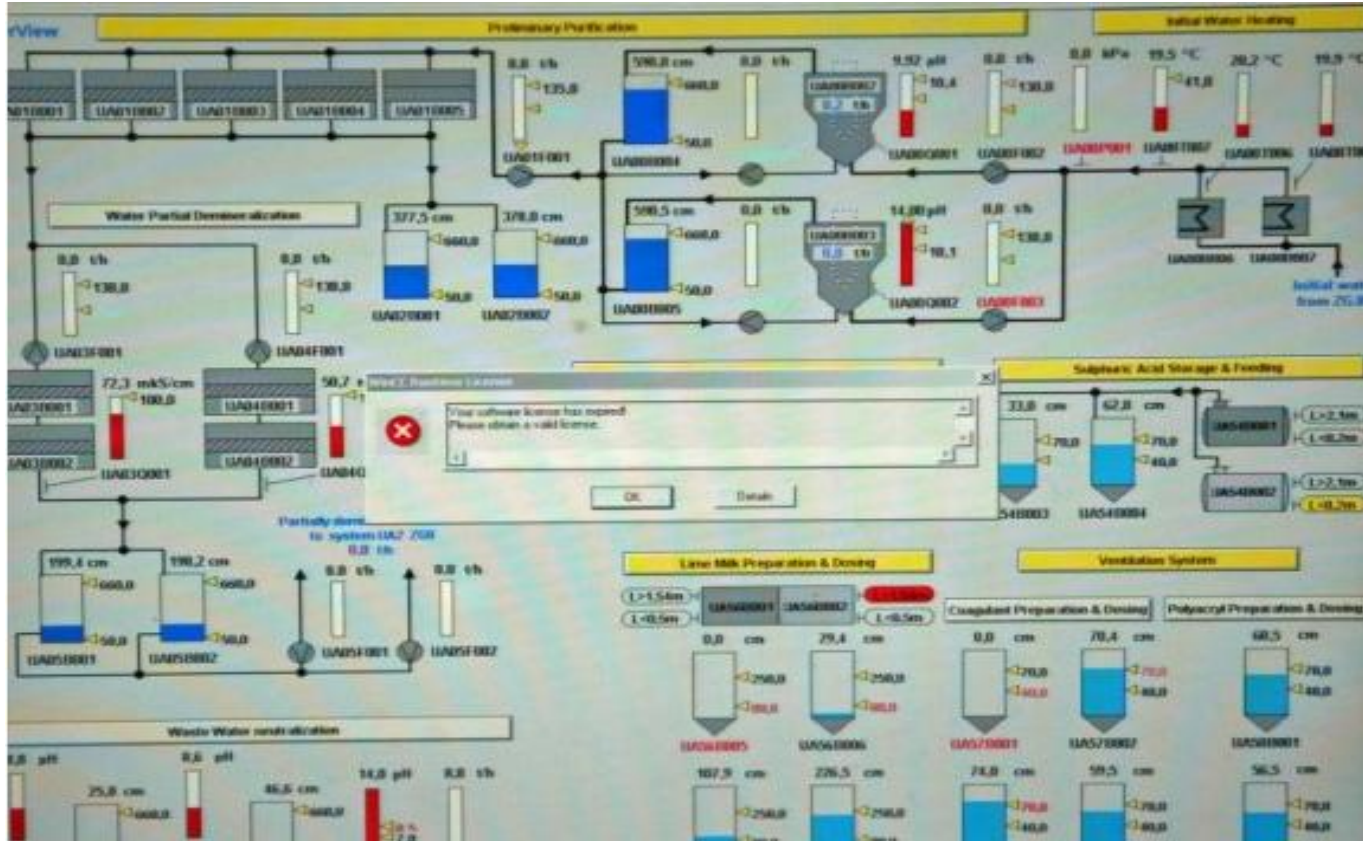
# Ajankohtaista tietoturvallisuudessa – valtionhallinnossa ja muualla

25.5.2011

Erja Kinnunen VK/VIP

[erja.kinnunen@valtiokonttori.fi](mailto:erja.kinnunen@valtiokonttori.fi)

# Vuoden 2010 ilmiöitä



# STUXNET

Haittaohjelma (mato), jonka tehtävänä oli hyökätä tietynlaisia teollisuusautomaatiojärjestelmiä vastaan



## Vuoden 2010 ilmiöitä

### Päätoimittajilta



### Wikileaks: Totuus solmiosta

Noin viikko sitten selvisi, että Ylen on mahdollista saada Wikileaksilta haltuunsa Suomea koskevat noin tuhat diplomaattisähköä. Ne olivat otos kuuluisasta jättivuodosta: Yhdysvaltain ulkoasiainhallinnosta paljastussivustolle vuotaneista noin 250 000 sähköestä.

# Vuoden 2011 ilmiöitä

## Microsoft Security Advisory (2524375) Fraudulent Digital Certificates Could Allow Spoofing

Published: March 23, 2011

**Version: 1.0**

TIETOTURVA ■ Niclas Storås, MikroPC, 29.3.2011, 16:45

### Varmana pidetyt sirukortit murtuvat

Tutkijat ovat löytäneet uuden tavan sirukorttien pin-koodin varastamiseen: koodi voidaan kaivaa sirulta. Asiasta kertoo [the H Security](#) -verkkosivusto.

Aikaisemmin pankkikorttien pin-koodeja on varastettu muun muassa pankkiautomaattien näppäimien päälle asetettavan laitteen avulla. Vanhanaikaisempi konsti on ollut vakoilla koodi näppäilyn yhteydessä.

Uudella keinolla pin-koodin varastaminen käy suoraan sirulta. Koodi kaivetaan esiin kortinlukijaan asetetun piirin avulla.

Home > Programs

### Open Letter to RSA Customers



Arthur W. Coviello, Jr.

Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products. While at

this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations.

# Eräs merkittävimmistä tietomurroista



Etusivu > Tietoturva nyt! > 2011 > Huhtikuu > CERT-FI varoitus 01/2011 PlayStation Network -palvelun tietomurrosta on päivitetty

## Tietoturva nyt!

28.4.2011

### CERT-FI varoitus 01/2011 PlayStation Network -palvelun tietomurrosta on päivitetty

Palvelussa on 330 000 suomalaista käyttäjää. Luottokorttitiedot on säilytetty salattuna.

CERT-FI on julkaissut varoituksen Sony PlayStation Network -palvelun tietomurrosta. Tietomurron yhteydessä maailmanlaajuisesti 77 miljoonan käyttäjän järjestelmään syöttämät henkilötiedot anastettiin. Palvelussa on 330 000 suomalaista käyttäjää. Järjestelmään tallennetut luottokorttitiedot on säilytetty salattuna eikä niiden anastamisesta ole näyttöä.

#### Lisätietoa

<http://www.cert.fi/varoitukset/2011/varoitus-2011-01.html>

» Lue uutinen mobiilisivustolla

## Miljoonien Playstation-käyttäjien tiedot varastettiin

27.4.2011 00:32 Sony myöntää PlayStation Network -palvelun käyttäjätietojen vuotaneen murtautujalle. Edelleenkin ei ole aikataulua palvelujen palauttamiselle.



Kuva: Niko Jylhä

Sony antoi lisää tietoa PlayStation Network - ja Qriocity-palvelut [sulkeneesta](#) hyökkäyksestä. [Yhtiön mukaan](#) käyttäjätiedot näyttävät joutuneen murtaujan haltuun 17.-19. huhtikuuta tapahtuneessa tunkeutumisessa, mutta [hvökkävksen vksitvskohdat](#) ovat vielä tutkinnan alla.

- Taloudelliset ja imago-vaikutukset vähintään merkittäviä!

# Tietomurto maksaa 7 miljoonaa dollaria

Matias Mäki



Tietomurron keskihinta on paisunut jo yli seitsemään miljoonaan dollariin Yhdysvalloissa. Kasvulle ei näy loppua.



Tuomas Linnake

8.3.2011 17:00

3

Yritysten kärsimät tappiot tietomurroista olivat keskimäärin 7,2 miljoonaa dollaria eli 5,1 miljoonaa euroa viime vuonna Yhdysvalloissa. Luvut kertoi tietoturvayhtiö Symantec, joka maksoi Ponemon Institutelle selvityksen tekemisestä.

Hinta kasvoi jo viidettä vuotta peräkkäin ja oli viime vuonna 214 dollaria murettua tietotalletusta kohti. Vuonna 2009 vastaava luku oli 204 dollaria.

Suosittelen 2

1

Kommentoi

Lähetä

Tulosta (HTML)

Tallenna (PDF)

Del.icio.us

Facebook

Twitter

Miksi rahaa löytyy tilanteen korjaamiseen vasta jälkikäteen? Riskienhallinta!

# Yli 150 ministeriön tietokoneesta löytyi vakoiluohjelma

Ensio Ilmonen / Lehtikuva



Ranskan valtiovarainministeriön noin 150 tietokoneesta löytyi vakoiluohjelma. Ranskassa epäillään, että vakoojat keräsivät tietoa Ranskan isännöimästä G20-

huippukokouksesta.



Perttu Pitkänen

7.3.2011 16:39

20

Ranskan valtiovarainministeriö vahvistaa, että sen tietokoneista on paljastunut poikkeuksellisen laaja vakoiluyritys. Verkkorikolliset ovat päässeet yli 150 ministeriön tietokoneeseen, [kertoo asiantuntija Graham Cluley](#) tietoturvayhtiö Sophosin blogissa.

KYBERUHKAT ■ Suvi Korhonen, 24.3.2011, 15:04

## Kyberhyökkäys iski EU-komissioon huippukokouksen alla

Euroopan komissio ilmoittaa joutuneensa poikkeuksellisen vakavan kyberiskun kohteeksi ennen EU-kokousta. Hyökkäys sattui vain tunteja ennen kokousta, jossa käsitellään Libyan tilannetta, euroalueen lainakriisiä ja ydinturvallisuutta, [kertoo uutistoimisto AFP](#).

Komission työntekijöille ilmoitettiin keskiviikkona aamulla, että sähköpostin etäkäyttö ei ollut enää mahdollista ja työntekijöitä

iksi Euroopan unionin  
n External Action Servicen

kkäys ei sinänsä ole  
ko usein.

DRI

# Kukaan ei ole suojassa, etenkin kohdistetuilta hyökkäyksiltä!

## U.S. Spy Agency Is Said to Focus Decrypting Skills on Nasdaq Cyber Attack

25.5.2011 Erja Kinnunen

By Michael Riley - Mar 30, 2011 6:03 PM GMT+0300

# Vuoden 2011 ilmiöitä

TERVEYS ■ Emma Kauppi, 10:27

## HS: Häiriö tietoverkoissa riesasi eilen sairaaloita

Tietoverkkohäiriö häiritsi merkittävästi potilaiden hoitoa keskiviikkona Varsinais-Suomen sairaanhoitopiirin sairaaloissa, [kirjoittaa](#) Helsingin Sanomat.

Yksikään potilas ei kuitenkaan vaarantunut vakavasti, vaikka pahimman häiriön aikana muun muassa potilaiden laboratoriotuloksia ja lääkitystietoja ei saatu käyttöön.

Tietojärjestelmät toimivat keskiaamuna hitaasti ja pysähtyivät kahdelta iltapäivällä lähes kokoaan kahdeksi tunniksi.

Varsinais-Suomen sairaanhoitopiirin sairaaloissa on noin 2000 potilasta, joista noin puolet on vuodeosastoilla.

# EMME OLE ONGELMIEMME YKSIN!

30.03.2011 8.58 Emma Kauppi

## Nasan tietoturva kyläkaupan tasoa

Nasan tarkastaja Paul Martin havaitsi turva-aukot auditoinnissaan. Avaruusvirasto suostui laatutarkastukseen jo viime vuonna, mutta se suoritettiin vasta nyt.

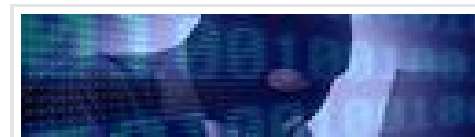


# AI MITEN NIIN RIKOLLISET MATKIVAT MEITÄ?

29.03.2011 8.37 Niko Rinta

## Verkkorikollisille myydään omia pilvipalveluita

Verkkorikollisuus hyödyntää pilvipalvelumalleja toiminnassaan. Hämärillä aikeilla olevat voivat ostaa krakkerointipaketin ja maksaa siitä ajan perusteella.

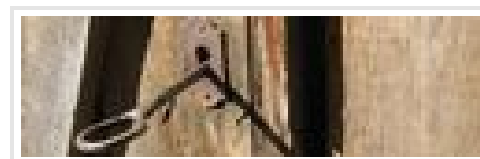


# APT?

28.03.2011 16.06 Emma Kauppi

## Varo apt-iskuja! Siis mitä?

Monet organisaatiot eivät oikein tiedä, mikä advanced persistent threat -isku on. Tämä vaikeuttaa niiltä suojautumista.



Tämä oli nimenomaan apt-isku, jossa hyökkääjät soluttautuvat yrityksen tietojärjestelmiin asentamalla haittaohjelman esimerkiksi selaimen tai sähköpostiohjelman kautta. Hyökkääjät ovat kärsivällisiä, taitavia ja varakkaita.

Tällaisten hyökkäysten viesti on selvä: jopa kehittyneimpien toimijoiden tietoihin voidaan murtautua. Se taas ei ole selvää, mitä tietoturvapääalliköiden pitäisi tehdä apt-hyökkäyksille.

### **Pelkkä markkinointikikka?**

Jotkut näkevät apt:n markkinointina. "Apt on fud-markkinointia (fear, uncertainty, doubt) ja osaksi vain yritys tehdä hyökkäyksestä pelottavampi, kuin se on", sanoo tutkimusyhtiö **Spire Securityn** tutkimusjohtaja **Pete Lindstrom**.

"Ei ole niin noloa joutua apt-hyökkäyksen kuin oman turva-aukon aiheuttaman hyökkäyksen kohteeksi."

Lindstrom jatkaa, että apt-kohu on nostanut tietoturvatietoutta hänen yhtiössään, mutta budjetti ei ole muuttunut miksiäkään eikä uusia työkaluja ole otettu käyttöön.

"Tämä on apt:n pieni likainen salaisuus. Puolustautuja ei tee mitään muuta eri tavalla kuin ennen, paitsi yrittää olla parempi siinä, missä pitäisi jo olla hyvä", hän summaa.

# VARASTETUT SSL-VARMENTEET

NETTIRIKOLLISUUS ■ Emma Kauppi, 28.3.2011, 11:39

## Iranin kybersota jatkuu: varmennevaras antoi itsensä ilmi

Digitaalisia varmenteita myyvä **Comodo Group** kertoi perjantaina, että sen kumppanin **InstantSSL:n** järjestelmään hyökättiin ja niistä varastettiin ssl-varmenteita. Vaarantuneet sivut olivat kirjautumissivut **Googlen** Gmailiin, **Microsoftin** Hotmailiin, **Yahoo** Mailiin sekä **Skype**-nettipuhelimeen. Lisäksi **Mozillan** Firefox-lisäosien sivujen varmenne anastettiin.

Tapaus on huolestuttava, sillä Comodon myymät ssl-salausvarmenteet ovat tärkeä osa internetiä suojaavaa infrastruktuuria. Varmenteet kertovat selaimelle, että se on yhteydessä oikeaan sivustoon eikä valesivuille. Ssl-suojaus ehkäisee myös kalasteluhyökkäyksiä.

### Yhtiö syyttää Irania

Comodon mukaan hyökkäys oli taitavasti suoritettu, mutta havaittiin

epäili vahvasti Iranin hallitusta. "Kaikki viittaa Iranin hallitukseen ja sen juuri perustamaan kybersodankäynnin yksikköön", sanoi Comodon

pääjohtaja **Memor Abdulmuyyid** uutistoimisto **ignis.me** perjantaina. Hän uskoi valtion hyötyvän hyökkäyksestä keräämällä käyttäjätietoja ja saamalla pääsyn sähköpostitileille.

## SUOMESSA YTS

Strategiassa kuvatut uhkamallit ovat:

- » voimahuollon vakavat häiriöt
- » tietoliikenteen ja tietojärjestelmien vakavat häiriöt - kyberuhkat

# Tietoturvallisuus valtionhallinnossa

Ei tietoturvallisuutta koskevaa erillislakia

Julkisuuslakiin 621/1999 liittyvät määräykset

- Hyvä tiedonhallintatapa 18§
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999
- Tietoturvallisuusasetus 681/2010



Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä (VAHTI 7/2009)

- Hyväksytty 26.11.2009, voimaan 1.12.2009

# Muu tietoturvalainsäädäntö

- Henkilötietolaki (523/1999)
- Laki valtioneuvostosta (175/2003)
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Valmiuslaki (1080/1991)
- Laki valtion talousarviosta (423/1988)
- Asetus valtion talousarviosta (1243/1992)
- Hallinnonala-/virastokohtaiset säädökset



# Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä



## Tietoturvallisuuden kehittämisperiaatteet

- Vastuullisuus
- Laillisuus
- Osaaminen
- Yhteistyö ja synergiaedut
- Integrointi
- Kansainvälinen yhteistyö

## Kehittämisen painopisteet

- Johtaminen
- Kokonaisvaltaisuus ja läpäisy
- Ennaltaehkäisy ja varautuminen
- Tiedon ja sen arvon suojaaminen

# Valtioneuvoston periaatepäätös valtiorhallinnon tietoturvallisuuden kehittämistä



Hallinnossa tulee varmistaa **tietoturvallisuuden perustason toteutuminen koko valtiorhallinnossa ja korotetun / korkean tason toteutuminen yhteiskunnan elintärkeissä toiminnoissa**. Jokaisen hallinnon organisaation on saavutettava vähintään tietoturvallisuuden perustaso. VM antaa lähiaikoina ohjeen tietoturvasoista ja niiden vaatimuksista. Tietoturvasojen ja varautumisen toimeenpanoa tehostetaan yhteishankkeiden avulla.

# Valtionhallinnon tietoturvallisuuden kehitysohjelma 2010-2015

- Kehittämisen painopisteenä toimintamallin ja johtamisen muutos
  - Konzernimainen toimintatapa ja tietoturvaohjaus
  - Tietoturvallisuuden tulosohjaus, mittaaminen, raportointi ja arvioinnit
  - Tietoturvaosaaminen ja koulutus
  - Riskienhallinta ja varautuminen
  - Tietoturvalainsäädännön kehittäminen
  - Tietoturvaressurit ja budjetointi
- Yksittäiset kehityskohteet
  - Turvalliset sähköiset palvelut
  - Tiedon ja sen arvon suojaaminen elinkaaren eri vaiheissa
  - Käyttövaltuuksien hallinnan kehittäminen
  - Turvallisten ja yhteen toimivien palveluiden integrointi
  - Konzernin tietoturvapalveluiden kehittäminen ja käyttöönotto
  - Operatiivisen reagointikyvyn kehittäminen



# Tietoturvallisuusasetus

Vaikutusarviokierros keväällä 2010

[http://www.vm.fi/vm/fi/04\\_julkaisut\\_ja\\_asiakirjat/03\\_muut\\_asiakirjat/20100510Tietot/name.jsp](http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20100510Tietot/name.jsp)

- Hallinnonalan edellytykset ja valmiudet toimeenpanoon
- Hyödyt ja haitat
- Toimeenpanon edellyttämät resurssit
- Resurssi- ja kustannusvaikutukset



Asetus hyväksyttiin valtioneuvostossa 1.7.2010

Voimaan 1.10.2010

Asetusta tukevat VAHTI-ohjeet

- [Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010](#)
- [Sisäverkko-ohje 3/2010](#)

# Miksi asetusta tarvitaan?

- Tietoturvallisuuteen liittyviä asioita on ripoteltu lainsäädännössä useaan eri paikkaan, tietoturvallisuusasetus tulee toimimaan keskeisessä roolissa.
- TTA on viranomaisille ehdottomasti tärkein velvoite huolehtia tietoturvallisuudesta entisten (julkisuuslaki, henkilötietolaki, laki yksityisyyden suojasta työelämässä, sähköisen viestinnän tietosuojalaki) ohella.
- Eräs tärkeimmistä syistä saattaa asetus voimaan liittyä **kansainvälisten luokiteltujen tietoaineistojen käsittelyyn**
  - Suomi ei ole kaikissa asioissa ollut mallioppilas
  - Jos Suomen maine / luotettavuus / uskottavuus käsitellä kansainvälisiä turvallisuusluokiteltuja tietoaineistoja ei ole vakuuttava, emme saa sitä tietoa, jota tarvitsemme!



# Mitä uutta tietoturva-asetus toi mukanaan?



- **Tietoturvallisuuden perustason** määrittämisen asetuksessa
- Neliportainen **asteikko** suojaustasojen ja turvallisuusluokiteltavien tietoaaineistojen luokittelun toteuttamiseksi
- Vaatimuksen luokiteltujen tietoaaineistojen käsittelyn edellyttämän **tietoturvallisuustason** täyttymisestä
  - Asetuksessa ei määritetä perustason vaatimuksien ohella muita vaatimuksia, vaan ne määritellään täytäntöönpanoa koskevassa VAHTI-ohjeessa

## VIRANOMAISEN TIEDOT JA ASIAKIRJAT

- Viranomaisen luomat tiedot ja asiakirjat
- Viranomaisen vastaanottamat tiedot ja asiakirjat
- Viranomaisen valmisteltavana olevat tiedot ja asiakirjat

### Viranomaisen asiakirjojen tietoturvaluokittelu

Salassa pidettävä, viranomaisharkinta, käyttötarkoitussidonnaisuus

#### Suojaustasomerkintä

Suojaustaso I

Suojaustaso II

Suojaustaso III

Suojaustaso IV

TiTuA 681/2010, 9 §  
JulkL 621/1999 24.1 § 3-6, 11-33 k  
Hetil 523/1999 11 §  
Muu lainsäädäntö

#### Turvallisuusluokitusmerkintä

ERITTÄIN SALAINEN

SALAINEN

LUOTTAMUKSELLINEN

KÄYTTÖ RAJOITETTU

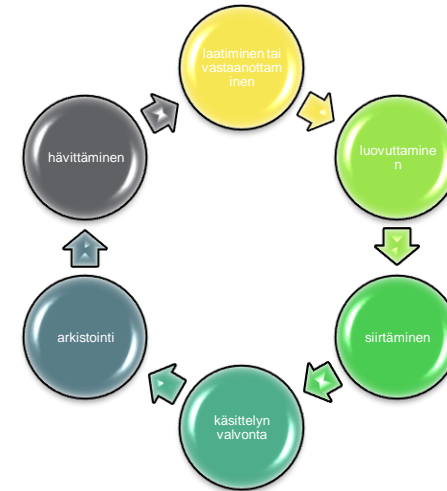
TiTuA 681/2010, 11 §  
JulkL 621/1999 24.1 § 2, 7- 10 k  
KansVälTiTuL 588/2004, 8 §

**JULKINEN TIETO**

# Luokituksen toteuttaminen

- Tietoturvatyökalut on suunniteltava ja toteutettava siten, että ne kattavat asiakirjan kaikki käsittelyvaiheet

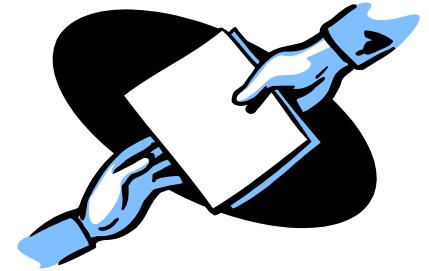
- laatiminen tai vastaanottaminen
- luovuttaminen
- siirtäminen
- käsittelyn valvonta
- arkistointi
- hävittäminen



## ELINKAAREN HALLINTA!

- Jos valtionhallinnon viranomainen on päättänyt luokitella asiakirjansa tietoturvallisuuden toteuttamiseksi, luokittelussa on noudatettava tietoturva-asetuksen 3. luvussa säädettyjä perusteita.
- Luokitusta ei saa ulottaa sellaiseen asiakirjaan tai asiakirjan osiin, joissa käsittelyvaatimusten noudattaminen ei suojattavan edun vuoksi ole tarpeen.
- **Merkinnän tarpeellisuus ja sen osoittama suojaustaso vaatimus on tarkistettava viimeistään silloin, kun viranomainen on antamassa asiakirjan ulkopuoliselle.**

# Julkinen vs. salassa pidettävä tieto



- **Julkinen tieto**

- Ei julkisuuslain tai muun säädöksen perusteella ole määritetty salassa pidettäväksi
- Muu kuin laissa määritelty tieto, jos tiedon paljastumiselle ulkopuolisille ei ole haitallisia seuraamuksia

- **Salassa pidettävä tieto**

- Lainsäädännöllinen peruste tai tiedon paljastumisella ulkopuolisille on eri asteisia haitallisia seuraamuksia
  - Esim. salassa pidettävät henkilötiedot ja liike- sekä ammattisalaisuudet

**SALASSA PIDETTÄVÄ**  
**Suojaustaso** \_\_

Julkl (621/1999) 24.1 §:n \_\_\_\_k  
Lain (\_\_\_\_/\_\_\_\_) \_\_\_\_ §:n \_\_\_\_k

**ERITTÄIN SALAINEN**  
**Suojaustaso I**

Julkl (621/1999) 24.1 §:n \_\_\_\_k  
L (\_\_\_\_/\_\_\_\_) \_\_\_\_ §:n \_\_\_\_k

**SALAINEN**  
**Suojaustaso II**

Julkl (621/1999) 24.1 §:n \_\_\_\_k  
L (\_\_\_\_/\_\_\_\_) \_\_\_\_ §:n \_\_\_\_k

**LUOTTAMUKSELLINEN**  
**Suojaustaso III**

Julkl (621/1999) 24.1 §:n \_\_\_\_k  
L (\_\_\_\_/\_\_\_\_) \_\_\_\_ §:n \_\_\_\_k

**KÄYTTÖ RAJOITETTU**  
**Suojaustaso IV**

Julkl (621/1999) 24.1 §:n \_\_\_\_k  
L (\_\_\_\_/\_\_\_\_) \_\_\_\_ §:n \_\_\_\_k

# Käsittelyn rajoitukset

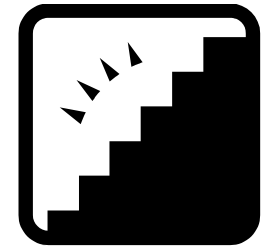
- Linjaukset asetuksessa, tarkemmat ohjeet VAHTI-ohjeistuksessa
- Suojaustason I ja II asiakirjoille tiukat vaatimukset
  - tulevat edellyttämään korkean tietoturvatason vaatimusten täyttymistä
- Suojaustason III asiakirja voi siirtää viranomaisen ylläpitämässä käyttörajoitetussa tietoverkossa, jos tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät korotetun tietoturvallisuuden tason vaatimukset.
- Sama koskee suojaustasoa IV edellyttävää arkaluonteisia henkilötietoja tai biometrisiä tunnistetietoja sisältävää henkilörekisteriin talletettua asiakirjaa.
- Suojaustason IV asiakirjan saa siirtää valtionhallinnon viranomaisen päättämällä tavalla

# Tietoturvasot

- VMn asettamat yhtenäiset vaatimukset koko hallinnolle tietoturvallisuuden toteuttamiseksi
- Vahvistaa hallinnon tietoturvaosaamista ja -kulttuuria
- Mahdollistavat toimittaja- ja alihankkijaketjun tietoturvallisuuden varmistamisen
- Mahdollistaa turvallisen verkottumisen
- Mahdollistaa hallinnon hyvät, laadukkaat ja turvalliset palvelut
- Saattaa hallinnon ja palvelut yhtenäiselle perusturvasolalle
- Vähentää hallinnon päällekkäistä työtä
- Organisaatioiden turvallisuus on mitattavissa ja auditoitavissa yhtenäisin kriteerein

# Tietoturvasojen toteutus

- Perustaso toteutettava koko valtionhallinnossa 30.9.2013 mennessä
- Jotkin hallinnonalat tai virastot toteuttavat etupainotteisesti
  - MMM hallinnonalan yhteishanke
  - SMn OPK päätös joulukuussa 2009; koko hallinnonalalla korotettu taso 2012
  - VIPin ministeriö-asiakkaiden THK-hanke
- Suurin osa käynnistää toteutuksen VMn yhteishakkeissa
  - Ilmoittautuminen päättyi 6.5.2011
  - Käynnistyvät kesällä 2011
  - 2-3 hanketta, joissa kussakin n. 20-30 virastoa
  - VIP toimii hankkeiden vetäjänä ja koordinaattorina
  - Tavoitteena perus- tai korotettu taso 2013 mennessä



# VAHTI-ohjeet



**VAHTI 2/2010**  
Purkaa auki tietoturvallisuusasetuksen ja sisältää tietoturvasojen vaatimukset



**VAHTI 4/2010**  
Suositeltava kun organisaatio ottaa SOMEn käyttöön



**VAHTI 3/2010**  
Määrittelee tietoturvasot sisäverkoissa



[www.vahtiohje.fi](http://www.vahtiohje.fi)

# Tulevat VAHTI-ohjeet

Tietotekniikka-  
ympäristön  
tietoturvaohje

## VAHTI x/2011

Tuleva ohje, joka antaa yksityiskohtaiset vaatimukset siitä, miten tietoturvasojen vaatimukset voidaan toteuttaa nykyaikaisilla välineillä ja teknologioilla

ICT-  
hankintojen  
tietoturvaohje

## VAHTI x/2011

Miten tietoturvasuus tulisi toteuttaa hankinnoissa?  
Miten TTT ja ICT-varautuminen pitäisi ottaa huomioon hankinnoissa?

Yhteinen turvallisuussopimusmalli valtionhallintoon

Päätelaitteiden  
tietoturvaohje

## VAHTI x/2011

Päivitys vuoden 2006 Älypuhelinten tietoturvasuusohjeen laajennus päätelaitteisiin; pöytäkoneet, kannettavat, tabletit, älypuhelimet

ICT-  
varautumisen  
vaatimukset

## VAHTI x/2011

ICT-varautumisen 12.15.2009 vaatimusten viimeistely ja julkaisu

# Kysymyksiä ?



**TIETOTURVA.VIP@VALTIOKONTTORI.FI**

**VIP.TIETOTURVA@VALTIOKONTTORI.FI**

**WWW.VALTIOKONTTORI.FI/TTT**

Valtiokonttori  
Statskontoret  
State Treasury