Viestiliikenne- ja tietoverkkoturvallisuus KYBERUHKAT

KYBER

- ”Kyber" sanaa käytetään lähes poikkeuksetta yhdyssanan etuliitteenä. Sanan merkityssisältö liittyy yleensä sähköisessä muodossa olevan informaation käsittelyyn.
- ”Kybertoimintaympäristö” on sähköisessä muodossa olevan informaation käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä ja tietoverkosta muodostuva toimintaympäristö.
- ”Kyberaseet” ovat käytännössä haittaohjelmat ja palvelunestohyökkäykset.

Ajankohtaista

- **STUXNET, kyberase jolla hyökättiin Iranin ydinvoimaloita vastaan uudelleen ohjelmoimalla tietojärjestelmiä. Stuxnet-iskun arvellaan hidastaneen Iranin ydinohjelmaa.**
- **STUXNET -verkkomato aloitti kyberturvallisuuden osalta uuden aikakauden v. 2010. Se on ensimmäinen mato, joka vakoilee ja uudelleen ohjelmoi (sabotoi laitteistoa) teollisuusjärjestelmiä.**
- **Stuxnetin pääsy Iranin Natanzin rikastuslaitoksen järjestelmään tapahtui luultavasti muistitikuilla, koska tietokoneita ei ollut kytketty turvallisuussyistä Internetiin.**
- **Bradley E. Manning**, korpraali, US ARMY, vuosi Wikileaks -järjestölle noin 700 000 asiakirjaa. Tietovuoto paljasti Yhdysvalloille kiusallisia yksityiskohtia sotavankien kohtelusta ja siviiliuhrien lukumäärästä. Mm. ”Collateral Murder” – videon sekä noin 260 000 arkaluontoista diplomaattisähkettä Wikileaksiin. Hänet vangittiin toukokuussa 2010 ja tuomittiin elokuussa 2013 35 vuodeksi vankeuteen.
- **Edward Snowden**, NSA:n urkintakohu. Kesäkuussa 2013 Snowden luovutti The Guardian ja The Washington Post -lehdille NSA:n salaiseksi luokiteltua tietoa, joissa käsiteltiin erityisesti maailmanlaajuisesti toimivaa PRISM-ohjelmaa, joka kerää mm. verkkopalveluiden käyttäjien yhteystietoja, niiden sisältöä, ihmisten puhelu- ja tekstiviestien tietoja.
- Myöhemminhän vielä selvisi että US government on pakottanut takaportit yhdysvaltalaisiin käyttöjärjestelmiin, ohjelmistoihin ja laitteisiin.
- **NSA uutisointia:**
  - Obama tiesi Merkelin puhelinurkinnasta. NSA on saattanut urkkia Saksan liittokanslerin Angela Merkelin puhelinliikennettä jo vuodesta 2002 (HS 27.10.2013)
  - Pohjolan **johtajat ymmällään** USA:n vakoilusta (HS 29.10.2013)
  - Kesällä alkanut urkintaskandaali hiertää liittolaisten suhteita (HS 29.10.2013)
  - The NSA's problem? Too much data (Washington Post 10/2013)
  - Ranska kovistelee USA:ta vakoilusta (mtv3.fi 21.10.2013)

- **Tietomurtajilta eivät konstit lopu: Jopa hiiren kautta voi hyökätä (IT -viikko 10.10.2013)**
- **Suosion taakka: Android -haittaohjelmat puskivat yli miljoonan (IT -viikko 7.10.2013)**
  - Tämän vuoden alussa Androidille oli tehty 425 000 tuholaista. Syyskuussa haittaohjelmien määrä rikkoi miljoonan rajan.
- **Älypuhelinten suojaus täysin retuperällä: Vaaraa ei tajuta (IT -viikko 7.10.2013)**
  - Yli 80 prosenttia yritysten ja kuluttajien älypuhelimista on avoimia haittaohjelmille ja hyökkäyksille, selviää Juniper Researchin uudesta raportista.

Suomen kyberturvallisuusstrategia

- Valtioneuvosto antoi 24.1.2013 periaatepäätöksen Suomen kyberturvallisuusstrategiasta
- Kyberturvallisuusstrategiassa **määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin** ja varmistetaan sen toimivuus.
- **Ministeriöiden johdolla on laadittu erilliset toimeenpano-ohjelmat** (Turvallisuuskomitea hyväksyi toimeenpano-ohjelman11.3.2014)**,** jotka sisältävät kyseisten hallinnonalojen ja hallinnonalaan liittyvien keskeisten toimijoiden konkreettiset, käytännön toimenpiteet, **joilla luodaan edellytykset kyberturvallisuusstrategian** linjausten ja siihen liittyvän taustamuistion antamien perusteiden **toteutumiseksi vuoteen 2016 mennessä**.

Suomen kyberturvallisuusstrategia, miksi?

- Yhteiskunnan turvallisuudesta huolehtiminen on valtiovallan keskeisimpiä tehtäviä ja yhteiskuntamme elintärkeät toiminnot on pystyttävä turvaamaan kaikissa tilanteissa.
- **Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille**.

KYBERTURVALLISUUDEN JOHTAMINEN JA KANSALLINEN KOORDINAATIO

- Johtamisen ylimmän tason muodostaa valtioneuvosto
- Kunkin ministeriön tulee toimivaltansa mukaisesti huolehtia siitä, että tavoitetilojen perusteella määritetyt strategiset tehtävät toteutetaan.

Suomen kyberturvallisuusstrategia

Strategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus.

Strategiassa kuvataan kyberturvallisuuden:

- **visio,**
- **toimintamalli ja**
- **strategiset linjaukset**.

Suomen kyberturvallisuusstrategia: VISIO

Vision toteutumisen puolestapuhujia ovat mm:

- vahva osaaminen
- pitkä yhteistyön perinne sekä julkisen hallinnon sisällä että Julkisen ja yksityisen sektorin välillä sekä
- selkeät turvallisuusvastuut eri toimijoiden kesken

Suomen kyberturvallisuuden toimintamalli rakentuu 8 periaatteen varaan:

1. Kyberturvallisuuden **asiat kuuluvat pääsääntöisesti valtioneuvoston toimivaltaan**.
   Kukin ministeriö vastaa toimialallaan kyberturvallisuuteen liittyvien asioiden valmistelusta ja hallinnon asianmukaisesta järjestämisestä.
2. Kyberturvallisuus on **kiinteä osa yhteiskunnan kokonaisturvallisuutta ja sen toimintamalli noudattaa Yhteiskunnan turvallisuusstrategiassa (YTS) määritettyjä periaatteita ja toimintatapoja.**
3. Kyberturvallisuus perustuu **koko yhteiskunnan tietoturvallisuuden järjestelyihin.**
4. Kyberturvallisuuden toimintamalli **perustuu** tehokkaaseen ja laaja-alaiseen **tiedon hankinta-, analysointi- ja keruujärjestelmään**, yhteiseen ja jaettuun **tilannetietoisuuteen** sekä kansalliseen ja kansainväliseen **yhteistoimintaan** varautumisessa.
5. Kyberturvallisuuden **järjestelyissä noudatetaan** viranomaisten, yritysten ja järjestöjen välillä **vastuunjakoa**, joka perustuu säädöksiin ja sovittuun yhteistyöhön. Tarve sopeutua nopeisiin muutoksiin, kyky hyödyntää uusia mahdollisuuksia ja reagoida yllättäviin tilanteisiin vaatii toimijoilta strategisen ketteryyden periaatteiden ymmärtämistä ja noudattamista kyberturvallisuuteen tähtäävien toimien kehittämisessä ja johtamisessa.
6. Kyberturvallisuutta rakennetaan toiminnallisten ja teknisten vaatimusten perusteella sekä kansallisesti että kansainvälisesti
7. Kyberturvallisuuden **kehittämisessä panostetaan** voimakkaasti kybertoimintaympäristön **tutkimukseen, koulutukseen, työllistymiseen ja tuotekehitykseen**, jotta Suomi voisi kehittyä yhdeksi kyberturvallisuuden johtavista maista.
8. Kyberturvallisuuskehityksen varmistamiseksi **huolehditaan** siitä, että **lainsäädäntö ja kannustimet ovat kunnossa.**

STRATEGISET LINJAUKSET:

Kansallista kyberturvallisuutta kehitetään strategisten linjausten (10) mukaisesti. Linjauksilla luodaan edellytykset kyberturvallisuuden kansallisen vision toteutumiselle.

1. Yhteistoimintamalli
   Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden **toimijoiden välinen tehokas yhteistoimintamalli**
2. Tilannetietoisuus, kyberturvallisuuskeskus
   Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen **osallistuvien** keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden **tilannetietoisuutta ja tilanneymmärrystä perustamalla kyberturvallisuuskeskus.**
3. Yhteiskunnan elintärkeiden toimintojen turvaaminen ja jatkuvuuden hallinta
   Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden **kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat** ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa
4. Kyberrikollisuuden torjunta
   Huolehditaan, että **poliisilla on tehokkaat edellytykset ennalta ehkäistä**, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä **rikoksia.**
5. Kyberpuolustus osana kansallista puolustuskykyä
   Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.
6. Aktiivinen kansainvälinen yhteistoiminta
   Vahvistetaan kansallista kyberturvallisuutta **osallistumalla** aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten **kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan.**
7. Osaaminen ja yhteinen ymmärrys
   Parannetaan kaikkien yhteiskunnan toimijoiden **kyberosaamista ja -ymmärrystä.**

8. Ajantasainen lainsäädäntö on kyberturvallisuuden edellytys
   Kansallisella **lainsäädännöllä varmistetaan** tehokkaan kyberturvallisuuden **toteuttamisen edellytykset**.
9. Kyberturvallisuustehtävät ja palvelumallit
   Määritellään viranomaisille ja elinkeinoelämän **toimijoille** kyberturvallisuutta koskevat **tehtävät** ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle.
10. Toimeenpano ja seuranta
    Strategian **toimeenpanoa valvotaan** ja **toteumaa seurataan**.

Strateginen linjaus 5. Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään

(Suomen sotilaallinen puolustaminen, muiden viranomaisten tukeminen ja osallistuminen kansainväliseen kriisinhallintaan):

- **Tavoitteena on**, **että suorituskyky mitoitetaan sellaiseksi, että se mahdollisimman tehokkaasti tukee puolustusvoimien toimintaa** alueellisen koskemattomuuden turvaamiseksi ja maan puolustamiseksi.
- Uskottava **suorituskyky rakennetaan yhteistyössä muiden viranomaisten, yritysten sekä yliopistojen kanssa.**
- Normaaliaikoina suorituskykyä kehitetään verkostoitumalla, tiedonvaihdolla, yhteisillä hankkeilla sekä osallistumalla kansallisiin ja kansainvälisiin työryhmiin ja harjoituksiin. **Poikkeusoloissa tai erilaisissa häiriötilanteissa toiminnan perusratkaisut eivät muutu.**
- Puolustusvoimat **suojaa omat järjestelmänsä ja verkkonsa siten, että se kykenee suoriutumaan lakisääteisistä tehtävistään** huolimatta kybertoimintaympäristön uhkista.
- Kyberuhkien syntyminen on kyettävä havaitsemaan ajoissa ja kybermaailman tapahtumia seurattava reaaliajassa. Edellyttää **kybertilannekuvan muodostamista**.
- Puolustusvoimien **kybertilannekuva**a muodostettaessa toimitaan **yhteistyössä** perustettavan **kansallisen Kyberturvallisuuskeskuksen kanssa.**
- Kyberpuolustuksen **suorituskykyä kehitetään** kansallisella tasolla **yhteistyössä** muiden viranomaisten, elinkeinoelämän, tiedeyhteisön ja muiden toimijoiden kanssa
- **Kansainvälistä** kyberpuolustukseen liittyvää **yhteistyötä** tiivistetään edelleen keskeisten toimijoiden kanssa. Yhteistoiminta perustuu kahdenvälisiin sopimuksiin sekä monikansalliseen yhteistyöhön.
- Puolustusvoimat antaa kyberuhkien aiheuttamissa häiriötilanteissa **virka-apua muille viranomaisille**. Tarvittaessa puolustusvoimat saa tukea muilta viranomaisilta omia kyberpuolustustehtäviä toteuttaessaan.

Haittaohjelmat

- **Haittaohjelmat** aiheuttavat monenlaisia harmeja tietokoneen käytölle. Koneen käyttö saattaa hidastua sekä verkkosurffailu ja sähköpostin käyttö voivat hankaloitua merkittävästi. Ohjelmistojen toiminnassa saattaa esiintyä häiriöitä ja kone saattaa käynnistyä itsestään ilman käyttäjän toimenpiteitä. Muita ongelmia ovat tietojen häviäminen tai muuttuminen, selaimen kotisivun muuttuminen sekä muut käyttöhäiriöt. Hankalimmissa tapauksissa operaattori saattaa sulkea liittymän, jos tietokone käyttäjän tietämättä lähettää häiriöliikennettä verkkoon tai toimii roskapostin välitystoimistona.

- Tyypillisesti **viruksia** saadaan koneelle sähköpostin kautta, ladattaessa tiedostoja internetistä, vertaisverkon kautta tai pikaviestinohjelman välityksellä. Virukset leviävät myös levykkeiden, cd- ja dvd-levyjen sekä muistitikkujen välityksellä.

- **Verkkomadot**, etsivät verkkoon kytkettyjä koneita, joihin ei ole asennettu viimeisimpiä korjauspäivityksiä. Madot leviävät viruksia huomattavasti nopeammin suoraan koneelta toiselle.

- **Troijan hevoseksi** kutsutaan haittaohjelmaa, joka naamioidaan vaikkapa viattoman näköiseksi peliksi tai muuksi hyötyohjelmaksi. Troijan hevonen voi sisältää mitä hyvänsä toimintoja ja pahimmillaan se voi tuhota tietokoneen kovalevyn sisällön.

- **Takaportiksi** kutsutaan ohjelmaa, joka avaa ulkoisen tietoliikenneyhteyden suojaamattomaan tietokoneeseen. Takaportin kautta voidaan mm. varastaa käyttäjän henkilökohtaisia tietoja koneesta.

- **Vakoiluohjelmiksi** kutsutaan ohjelmia, jotka keräävät tietoa koneen tai ohjelmistojen käyttötavoista, käyttäjän tallentamista tiedoista ja vaikkapa näppäinpainalluksista. Vakoiluohjelma voi lähettää tiedon automaattisesti eteenpäin tai vakoiluohjelma voi avata pääsyn tietokoneeseen verkon kautta asentamalla koneeseen takaportin.