# 7.8 Kyberturvallisuusosaaminen työelämässä

*Antti Hakkala, Jouni Isoaho ja Seppo Virtanen*

Tietotekniikan kunnollinen hallinta on avainasemassa yritysten, organisaatioiden sekä työntekijöiden kilpailukyvylle. Kyberturvallisuus on tietotekniikan osaamisen kriittisimpiä ja haastavimpia osa-alueita ja se on siten keskeisessä asemassa entistä turvallisemman tietoyhteiskunnan rakentamisessa alalla kuin alalla. Kyberturvallisuuden rakentamiseen on kehitetty valtavia määriä uutta teknologiaa. Teknologia ei kuitenkaan yksin riitä, koska kokonaisvaltainen kyberturvallisuus vaatii niin ihmisten, prosessien kuin teknologian saumatonta yhteistyötä ja -toimintaa. Tietoyhteiskunnassa meidät on käytännössä lisäksi pakotettu luottamaan erilaisiin järjestelmiin ja palveluihin, joiden tietoturvaan, sen käytännön toteutukseen ja arviointiin meillä ei yksilöinä ole minkäänlaista mahdollisuutta. Täydellistä turvallisuutta ei ole olemassa, minkä takia ihmisten kyberturvallisuusosaaminen ja kyberriskien hallinta ovat avainasemassa. Yksikin huonosti toteutettu palvelu tai järjestelmä voi pahimmassa tapauksessa vaarantaa yksilön tai koko organisaation kyberturvallisuuden. Yksilöiden tiedot ja taidot heijastuvat lopulta yhteiskunnallisella tasolla kokonaisturvallisuuden tasoon, ja tämän osaamispohjan rakentumisella myös tietoturvan opetuksella ja osaamisella on vankka rooli. Tässä artikkelissa tarkastellaan lyhyesti mitä keskeisiä osaamiskokonaisuuksia kyberturvallisuuden osaamiseen kuuluu ja mitä kenenkin työelämässä olevan—ja muidenkin—tulisi osata ja tietää.

## Mitä on kyberturvallisuus?

Tieto- ja kyberturvallisuus ovat käsitteinä moniulotteisia ja vaikeasti hahmotettavia. Varsinkin aihepiiriin perehtymättömälle turvallisuuteen ja tietoturvaan liittyvät käsitteet ovat usein outoja. Puhuttaessa kyberturvallisuudesta mukaan tulee vielä epämääräisempi termi ”kyber”, jonka tarkasta merkityksestä asiantuntijatkin käyvät keskustelua. Ei siis liene ihme, että kyberturvallisuus ja siihen

liittyvät uhat näyttäytyvät monille jonkinlaisena mörkönä tai agenttitarinoiden juonenkäänteinä, vaikka todellisuudessa kyberturvallisuus on jotain, mikä koskettaa meitä kaikkia.

Lähdetään liikkeelle turvallisuudesta. Sen määrittely antaa hyvät suuntaviivat kyberturvallisuuden tarkastelulle ja sen työelämäosaamisen määrittelyssä. Mitä turvallisuus on? Se voidaan jakaa neljään osa-alueeseen. Turvallisuus on turvallisuuden tunnetta, tietoa siitä, että mahdollisten uhkien ja riskien vaikutusmahdollisuudet ovat pienet. Turvallisuus on myös tosiasioiden tunnistamista ja tilannekuvan ymmärrystä. Turvallisuuteen kuuluu myös epävarmuuden ja haitallisten tapahtumien sietokyky, *resilienssi*. Viimeisenä osa-alueena turvallisuuteen kuuluvat turvallisuutta konkretisoivat mallit sekä arvot, joiden varaan turvallisuutta rakennetaan. Näiden osa-alueiden pohjalta onkin helpompi lähteä määrittelemään kyberturvallisuutta ja sen keskeisiä osa-alueita.

Tieto- ja kyberturvallisuudelle on olemassa useita erilaisia määritelmiä, riippuen siitä, mistä näkökulmasta tarkastelija haluaa aihetta käsitellä. Voidaan ajatella vain abstraktisti tiedon turvaamista riippumatta sen olomuodoista, tietoa tallentavien tai siirtävien laitteiden teknistä suojaamista, yrityksen liiketoimintaprosessien suunnittelua, matemaattista salakirjoitusta, tai kaikkea tältä väliltä. Kyberturvallisuus voidaan määritellä kattamaan kaikki nämä osa-alueet tiedon abstraktin esitysmuodon suojaamisesta yrityksen liiketoimintaprosessien ja aineellisten sekä aineettomien resurssien ja intressien suojaamiseksi tieto- ja viestintäteknologiaa käyttävien uhkien aiheuttamilta riskeiltä. Haittaohjelmien avulla mahdollinen hyökkääjä kykenee vaikuttamaan myös fyysisen maailman kohteisiin ja liiketoiminnalle keskeisiin prosesseihin. Vuonna 2017 haittaohjelmahyökkäykset muun muassa vaikuttivat terveydenhuollon toimintaan ja potilasturvallisuuteen Isossa-Britanniassa ja keskeyttivät useiden satamien toiminnan. Kyberturvallisuus on siis yrityksen näkökulmasta tällaisten tapahtumien ennaltaehkäisyä, kokonaisvaltaista tiedon, resurssien, laitteiden, ihmisten ja intressien suojaamista.

## Kyberturvallisuuden rakentaminen

Hyvä lähtökohta kyberturvallisuuden rakentamiselle on, että täydellistä tai absoluuttista turvallisuutta ei ole olemassa, ei fyysisessä eikä kybermaailmassa. Lähtökohtaisesti on oletettava, että kaikki järjestelmät ovat murrettavissa ja kaikki turvatoimet ovat kierrettävissä. Sotastrategian klassikkoteoksissa puolustajien epäkiitollinen osa suhteessa hyökkääjään on tunnistettu jo satoja, ellei tuhansia vuosia sitten, ja kyberturvallisuus ei muodosta tähän poikkeusta. Puolustajan on ennakoitava kaikki mahdolliset hyökkäysskenaariot ja haavoittuvaiset palvelut, kun taas hyökkääjälle riittää yksi onnistunut hyökkäys. Lisäksi kyberympäristö uhkineen ja riskeineen muuttuu jatkuvasti. Näiden tosiasioiden valossa kyberturvallisuus nähdäänkin usein jatkuvana prosessina eikä yksittäisenä toimenpiteenä tai joukkona erillisiä suoritteita. Tieto- ja kyberturvallisuutta ei voi ostaa valmiina ratkaisuna, vaan sen kanssa on tehtävä jatkuvasti töitä.

Tänä päivänä järjestelmät ovat harvoin täysin suljettuja, vaan niitä käytetään ajasta ja paikasta riippumattomasti, monilta eri teknologia-alustoilta. Erityises-

ti etäkäyttöalustoja, kuten älypuhelimia, tabletti-, ja kannettavia tietokoneita, käytetään usein huonosti suojatuissa ympäristöissä ja moniin eri käyttötarkoituksiin. Tällöin kyberturvallisuusriskit muodostuvat usein erittäin vaikeasti hallittaviksi.

Kyberturvallisuuden rakentaminen voidaan nähdä kolmen tasoisena tekemisenä:

1) Tekninen taso - Valitaan lähtökohtaisesti mahdollisimman tietoturvallisia teknologisia ratkaisuja. Käytetään viimeisintä tietoturvateknologiaa. Pidetään järjestelmät päivitettyinä.

2) Sosiaalinen taso - Kehitetään ja opetetaan hyviä tietoturvallisia käytänteitä kaikkeen tekemiseen. Kasvatetaan ihmisten tietoisuutta mahdollisista uhista ja riskeistä sekä teknologian rajoitteista. Rakennetaan yhteisvastuullista kyberturvakulttuuria. Tietoturvapolitiikka ulotetaan kattamaan kaikki tekniset alustat.

3) Riskien hallinnan taso - Haetaan ratkaisuja riskien hallintaan ja mahdollisten seuraamusten minimointiin. Tulos-panos –suhde tietorikollisessa toiminnassa marginalisoidaan.

## Kyberturvallisuus ja tietoyhteiskunnan muutoksen asettamat haasteet

Tietoyhteiskunnan kehittyminen vaikuttaa työelämään kokonaisvaltaisesti. Tietoyhteiskunnalla tarkoitetaan yleisesti ottaen sellaista yhteiskuntaa, jossa tieto toimii keskeisenä moottorina yhteiskunnan taloudellisessa ja sosiaalisessa kehityksessä ja aktiivisesti muokkaa yhteiskunnan rakenteita. Nykyinen yhteiskuntamme on selkeästi jo siirtynyt kohti verkottunutta tietoyhteiskuntaa, jossa tiedon keskeistä roolia korostaa yhteiskunnan verkottuminen ja tiedon käsittelyn, siirtämisen ja varastoinnin helppous ja kustannustehokkuus.

Tietoyhteiskuntakehitys ei tuo mukanaan vain positiivisia puolia, jotka ovat olleet luonteeltaan jopa mullistavia, vaan tietoyhteiskunnalla—ja erityisesti verkottuneella sellaisella—on myös varjopuolensa. Kun tiedon arvo korostuu, aiemmin merkityksettömänkin tuntuisesta tiedonmurusesta voi tulla arvokasta, tallentamisen ja jopa varastamisen arvoista. Internetin keskeinen ominaisuus—se ei unohda mitään—muodostuu tässä tapauksessa myös uhaksi yhteiskunnan jäsenille tavoilla, joita vielä muutama vuosikymmen sitten ei osattu edes kuvitella.

Kansainväliset tietoverkot mahdollistavat globaalin viestinnän lisäksi myös globaalin valvonnan. Joukkovalvonnan ongelmat ovat olleet esillä korostuneesti viimeisen viiden vuoden aikana. Vaikka keskustelu joukkovalvonnan tarpeellisuudesta ja laajuudesta ei ole vielä tuottanut yhtenäistä lopputulosta—mitä tuskin ikinä nähtäneenkään—on se omalta osaltaan ollut keskeinen tekijä tiedon arvon, merkityksen ja omistajuuden ongelmien esille tuomisessa sekä tavallisen kansalaisen että yrityksen näkökulmassa. Tiedotusvälineet käsittelevät tietoturva- ja tietosuoja-asioita arkipäiväisinä aiheina muiden joukossa ja kes-

kivertokansalainenkin on jo todennäköisesti törmännyt tietoturvaohjeisiin ja -vinkkeihin.

## Sosiaalinen media

Sosiaalinen media muodostaa kokonaisuuden, johon jokainen osallistuja vapaaehtoisesti lisää koko ajan tietoa itsestään, ajatuksistaan, toiminnastaan, ja elämästään. Sosiaalinen media on monelle yritykselle keskeinen markkinointi- ja toimintakanava, ja siellä tapahtuvat asiat voivat vaikuttaa merkittävästi niin yksityisen ihmisen kuin yrityksenkin toimintaan.

Kyberturvallisuuden kannalta sosiaalinen media tuo mukanaan useita ongelmia. Tiedon arvo, julkisuus ja mahdolliset käyttökohteet eivät ole aina täysin selviä kaikille, jolloin sosiaaliseen mediaan jaettava tieto saattaa sisältää turvallisuuteen haitallisesti vaikuttavia osia. Esimerkiksi jaetaan yksityisyyden suojaamaa materiaalia tai tietoa, jota on mahdollista käyttää vääriin tarkoituksiin—vaikka tieto itsessään vaikuttaisikin harmittomalta tai arvottomalta, ei tiedon kriittisyyttä ja arvoa osata aina tunnistaa. Sosiaalinen media tuo mukanaan myös ihmisen toimintaan ja käytökseen liittyviä riskejä, jotka on otettava huomioon etenkin yritysmaailmassa.

## Tietosuoja

Tietosuojan merkitys on korostunut nykyisessä kyberturvallisuuden ilmastossa. EU:n tietosuoja-asetus GDPR on viimeistään tuonut tiedonhallinnan ja tietosuojan kysymykset jokaisen tietoisuuteen. Yritysten on otettava toiminnassaan tietosuoja-asiat vakavasti, ja yksityishenkilöidenkin on ainakin kiinnitettävä asiaan huomiota, jotta pahimmilta ongelmilta vältytään.

Kaiken tämän takana on tiedon korostunut arvo ja rooli palveluiden, prosessien ja yhteiskunnan rakenteen muokkaajana. Tieto on valtaa, ja tähän todellisuuteen on nyt herätty. Tietosuoja-asioiden laiminlyönti voi johtaa ikäviin, yrityksen kannalta jopa kohtalokkaisiin seuraamuksiin. Tämän vuoksi myös tiedon suojaaminen, tiedon kriittisyyden ja arvon huomioon ottaminen ja ymmärtäminen ovat keskeisiä osa-alueita kyberturvallisuuden osaamisessa meille jokaiselle.

## Osaamisprofiilit nykyajan työelämässä

Kyberturvallisuudesta on tullut erottamaton osa nykyajan yhteiskuntaa ja työelämää, sillä tiedon merkityksen korostuminen ja sen jatkuvasti palveluita ja prosesseja muokkaava luonne koskettavat yhteiskunnan jokaista osa-aluetta. Tätä taustaa vasten onkin tärkeää, että jokainen tietoyhteiskunnan jäsen omaa tietyt perustiedot ja -taidot—kyberturvallisuuden kansalaistaidot—joiden avulla luoviminen kyberkarikoissa on ainakin, jos ei helppoa, niin ainakin mahdollista. Mutta mitä näihin kyberturvallisuuden kansalaistaitoihin kuuluu? Tätä kysymystä olemme lähteneet ratkomaan määrittelemällä kyberturvallisuuden osaamisprofiilit erilaisille ja -tasoisille toimijoille.

Perustasolla (taso 1) henkilöllä on sellaiset tiedot ja taidot, jotka antavat valmiudet toimia tietoyhteiskunnassa täysivaltaisesti ja samalla täyttävät modernin työelämän perusvaatimukset kyberturvallisuuden suhteen. Tällä tasolla kyetään sekä henkilökohtaisessa että työelämässä kohdatessa tunnistamaan mahdollisia kyberturvallisuusriskejä, uhkia ja uhkaskenaarioita, sekä raportoimaan niistä eteenpäin oikealle taholle. Yksilön näkökulmasta tähän kuuluvat riskien ja uhkien tunnistaminen, hallinta sekä turvalliset käytänteet kaikessa tietoteknisessä toiminnassa. Näiden asioiden oppiminen tulisi aloittaa jo siinä vaiheessa, kun tietotekniikkaa aletaan käyttämään. Tämä tulisi integroida vahvasti jo alakouluopetukseen.

Asiantuntijatasolla (taso 2) henkilö on selkeästi asiantuntijaroolissa ja omalta osaltaan vastaa tiedon käsittelystä, tallentamisesta, uuden tiedon luomisesta ja tiedon soveltamisesta. Asiantuntijan on ymmärrettävä oman sovellusalueensa käsitteet ja substanssi syvällisesti, mutta mikäli asiantuntijuus ei suoranaisesti liity kyberturvallisuutta lähellä olevaan aiheeseen, jonkin verran perustasoa syvällisempi ymmärrys ja osaaminen riittävät. Tietyissä asiantuntijarooleissa syvällisempi ymmärrys ja osaaminen ovat kuitenkin tarpeen. Esimerkiksi perusasteen tai lukion opettajan tulisi osata perustason lisäksi opettaa ja ohjata oppilaitaan saavuttamaan perustason tiedot ja taidot sekä luomaan kyberturvallisuuden kulttuuria. Toisaalta esimerkiksi tietoliikenneinsinöörin tulisi osata suunnitella ja toteuttaa oman alansa järjestelmiä niin, että kaikki kyberturvallisuuden osa-alueet on suunnittelu- ja toteutusvaiheessa otettu huomioon, näin ehkäisten järjestelmien haavoittuvuuksia. Asiantuntijatason osaaminen tulisi integroida osaksi toisen ja kolmannen asteen opintoja. Kyberosuuden laajuus ja sisältö riippuu asiantuntijan alasta.

Erikoisasiantuntija (taso 3) on tieto- ja kyberturvallisuuden erikoisasiantuntija, joka kykenee itsenäiseen toimintaan kyberturvallisuuden kentällä ja osaa analysoida, tutkia ja tarvittaessa rakentaa uusia ratkaisuja tietoturvan eri osa-alueilla. Organisaatiotasolla nämä henkilöt ovat usein vastuussa muiden jäsenten, koko organisaation, tai jopa valtiotason kyberturvallisuusosaamisesta, -koulutuksesta ja teknisistä ratkaisuista. Kyberturvallisuuden erikoisasiantuntijat koulutetaan erillisissä tutkinto-ohjelmissa. Tällä hetkellä Suomessa tällaisia ohjelmia on Turun ja Jyväskylän yliopistoilla.

Osaamisprofiilien yhdistäminen työntekijän toimenkuvaan tai työn sisältöön on luonnollisesti vaikeasti yleistettävissä, koska jokaisen yhteisön, yrityksen ja yksilön tarpeet, vastuut ja toimintakenttä vaikuttavat vaadittuun kybertuvallisuuden osaamiseen.

## Kyberturvallisuuden temaattiset kokonaisuudet

Seuraavaksi esitellään kyberturvallisuudelle keskeiset temaattiset kokonaisuudet ja niiden sisällöt. Jokainen kokonaisuus muodostaa itsenäisen osaamisalueensa, joiden hallinta on tärkeää nykypäivän työelämässä—ja laajemmin ajateltuna tietoyhteiskunnan osana turvallisesti toimimisessa.

***Haavoittuvuudet, uhat ja hyökkäykset:*** Ohjelmiston, laitteiston ja ihmisen toiminnan luomat haavoittuvuudet sekä sen, miten näitä haavoittuvuuksia käyte-

tään hyväksi. Haittaohjelmat, niiden luokittelu ja toiminnallisuus. Erilaiset hyökkäysmenetelmät, uhkatekijät ja toimijat, sekä näiden toiminnan tavoitteet ja motivaatiot. Ihmiselementtiin perustuvien haavoittuvuuksien hyödyntäminen.

***Tietoturvaprotokollat, -mekanismit ja -politiikat:*** Abstraktit tietoturvakäsitteet, kuten tietoturvaprotokollat, tietoturvan perusperiaatteet (luottamuksellisuus-eheys-autenttisuus) ja näiden laajennukset, riskienhallinta ja analysointi, uhkien tunnistaminen, kategorisointi ja niihin vastaaminen, kyberturvallisuus, kybersodankäynti, kriittinen infrastruktuuri ja asiaan liittyvä lainsäädäntö.

***Vastatoimet:*** ”Perinteiset” tietoturvakäsitteet ja työkalut, kuten palomuurit, tunkeutumisen havainnointi- ja estojärjestelmät, matemaattinen salakirjoitus (kryptografia), salasanaturvallisuus, tekniset ratkaisut ja suojamenetelmät.

***Tietoturva ja tiedon kriittisyys:*** Erilaisten sovellusalueiden tuottaman tiedon ominaisuuksien, arvon ja käyttökohteiden ymmärtäminen, tiedonhallinnan ja varastoinnin menetelmät, metatiedon käsite ja sen merkityksen ymmärtäminen, valvonta ja yksityisyys.

## Osaamisprofiilit ja temaattiset alueet

Yhdistämällä osaamisprofiilit ja temaattiset kokonaisuudet saadaan kokonaiskuva siitä, mitkä kyberturvallisuuden käsitteet ja osaamiskokonaisuudet korostuvat kussakin osaamisprofiilissa. Koska kyberturvallisuuden kenttä on niin laaja, ei ole tarkoituksenmukaista, tai edes mahdollista, että jokainen organisaation tai yhteiskunnan jäsen on kyberturvallisuuden asiantuntija. Tärkeämpää on se, että jokaisella perustason ymmärrys kyberturvallisuuden eri osa-alueista.

| | **Taso 1 – Perustaso** | **Taso 2 – Alakohtainen osaaminen** | **Taso 3 – Erikois-asiantuntijat** |
|---|---|---|---|
| **Haavoittuvuudet, uhat ja hyökkäykset** | Tiedostaa olemassaolon ja osaa tunnistaa kohdattaessa | Ymmärtää peruspe-riaatteet sekä käytännön toiminnan. | Kykenee analysoimaan ja/tai toisintamaan tarvittaessa, toiminnan syvällinen ymmärrys |
| **Tietoturva-protokollat, -mekanismit ja -politiikat** | Ymmärtää sovellusalan ja tarkoituksen. Osaa arvioida noudattaako toiminta protokollia ja määräyksiä. Ymmärtää riskinhallinnan ajattelumallin ja ihmisen toiminnan vaikutuksen. | Kykenee soveltamaan politiikkoja ja protokollia omassa työssään. | Kykenee arvioimaan ja suunnittelemaan protokollia, käytänteitä ja prosesseja, sekä valvomaan näiden käyttöä. Syvällinen ymmärrys ihmisen aiheuttamista kyberturvallisuushaasteista. |
| **Vastatoimet** | Ymmärtää peruskäsitteet, toiminnot ja näiden rajoitteet. | Syvällisempi ymmärrys toiminnasta ja kyky soveltaa olemassa olevia vastatoimia uusiin tilanteisiin käytännössä. | Kykenee hallinnoimaan, analysoimaan ja suunnittelemaan uusia vastatoimia. |
| **Tietoturva, -suoja ja tiedon kriittisyys** | Ymmärtää tiedon kriittisyyden käsitteen, tiedon sijainnin merkityksen, ja turvaamisen tärkeyden. Osaa erottaa henkilökohtaisen ja työperäisen tiedon. | Osaa suojata kriittisen datan ja osaa soveltaa tietosuojan periaatteita omaan työhönsä. Ymmärtää tiedon arvon ja tiedon suojaamisen tekniset rajoitteet. | Osaa arvioida tiedon suojamekanismeja ja hallita toiminnan kannalta kriittistä tietoa. Kykenee suunnittelemaan uusia tiedon suojaamisen menetelmiä. |

## Yhteenveto

Kyberturvallisuuden osaaminen on keskeinen taito, jonka merkitys nykyisessä verkottuneessa tietoyhteiskunnassa vain kasvaa. Jotta olemme yhdessä yhteiskuntana valmiina kohtaamaan tulevaisuuden työelämän haasteet, on meidän jokaisen saavutettava tietty perusymmärrys kyberturvallisuuteen liittyvistä asioista. Mitä enemmän elämme maailmassa, jonka lainalaisuuksia emme ymmärrä, olemme vain pakotettuja luottamaan muiden tekemiin ratkaisuihin ja elämään kasvavassa epävarmuudessa. Tämän kaltainen pakotettu luottamus on haitallista yhteiskunnan kokonaisturvallisuudelle, koska turvallisuus osaltaan edellyttää tilannekuvan hallintaa ja ymmärrystä vallitsevista lainalaisuuk-

sista. Edellä esitetyn kaltainen kyberturvallisuuden käsitteiden jaottelun ja osaamisprofiilien määrittelyn hyödyntäminen yhdistettynä organisaaton tarpeiden tunnistamiseen ja, mikä tärkeintä, näiden tietojen ja taitojen tehokkaaseen koulutukseen tarjoaa mahdollisuuden kohdata verkottuneeseen tietoyhteiskuntaan kohdistuvat kyberturvallisuuden haasteet hyvin varustautuneena.

## Lähteitä

Euroopan komissio 2018. Data protection. Saatavissa: https://ec.europa.eu/info/law/law-topic/data-protection_en

Gnostech Inc. Maritime Blog 2018. Petya and Maersk: One Year Later. Saatavissa: http://www.gnostech.com/maritime-blog/petya-maersk-one-year-later/

Hakkala A 2017. On Security and Privacy for Networked Information Society— Observations and Solutions for Security Engineering and Trust Building in Advanced Societal Processes. Väitöskirja, TUCS Dissertations 225. Turun yliopisto.

Limnéll J, Majewski K & Salminen M 2014. Kyberturvallisuus. Docendo.

Schneier B 2003. Beyond fear: thinking sensibly about security in an uncertain world. Copernicus books.

Smart W 2018. Lessons learned review of the WannaCry Ransomware Cyber Attack. UK Department of Health & Social Care. Saatavissa: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

von Solms R & van Niekerk J 2013. From information security to cyber security. Computers & Security, 38, 97–102.

*”Hyvä lähtökohta kyberturvallisuuden rakentamiselle on, että täydellistä tai absoluuttista turvallisuutta ei ole olemassa, ei fyysisessä eikä kybermaailmassa.”*