SANOMALEHTIYLIOPISTO

Digitalisaation vaikutukset ihmisen elämään

Sanomalehtiyliopisto on opintomuoto, jonka avoin yliopisto järjestää yhteistyössä Pohjalaisen, Ilkan ja Vaasan yliopiston kanssa.
Opintojakso: Digitalisaation vaikutukset ihmisen elämään
Koodi: TITE1150
Laajuus: 5 op
Sisältö: Opintojakso tutustuttaa opiskelijan digitalisaation vaikutuksiin yhteiskuntaan, työelämään ja ihmisten arkeen. Opintojaksolla käsitellään digitalisaatiota ja sen vaikutuksia eri näkökulmista, kuten esimerkiksi robotisaatiota, digitaalista viestintää ja kyberturvallisuutta.
Osaamistavoite: Opintojakson suoritettuaan opiskelija tuntee digitalisaation käsitteen ja osaa arvioida digitalisaation vaikutusta yhteiskuntaan.
Suoritustapa: Etätehtävä, joka on palautettava sähköpostitse tentaattorille timo.mantere@uva.fi viimeistään 30.11.2015.
Oppimateriaali: – Sanomalehtiyliopiston artikkelit (Pohjalainen ja Ilkka) 5.10., 12.10., 19.10., 26.10. ja 2.11.
– Seppo Kangaspunta (2015): Näkökulmia digitaaliseen maailmaan. TEM-analyyseja 63/2015. Työ- ja elinkeinoministeriö.
– Lakkala, Harri, Timo Raini, Jari Jussila, Hannu Kärkkäinen, Olli Pirttilä, Marko Seppänen & Tero Peltola (2015). Teollisuusyrityksen digipolku. Katsaus digitalisaatioon teollisuusyritysten näkökulmasta. Tekes 2015.
Arviointi: 1–5, hylätty.
Vastuuhenkilö: Timo Mantere.
Lisätiedot kurssista: Opiskelijapalvelut p. 029 449 8190, e-mail: avoinyo@uva.fi. Tarkat kurssitiedot: http://www.uva.fi/fi/sites/open/opintotarjonta/sanomalehtiyliopisto/
Ilmoittautuminen: https://uva.ilpa.oodi.fi/ilpa/
Hinta: 65 €

Vanhentunut ohjelma on tietoturvariski

Kyberhyökkääjä voi päästä käsiksi työpaikkasi tietoihin sinun kauttasi. Hyökkäyksiltä voi kuitenkin suojautua yksinkertaisin keinoin huolehtimalla esimerkiksi ohjelmistojen ajantasaisuudesta ja salasanojen vahvuudesta.

JARMO PANULA

VAASA Oman tietokoneen ja omien tietojen suojaaminen rakentuu pienten ja arkisten yksityiskohtien varaan, valistavat Vaasan yliopiston opettajat **Hannu K. Niinimäki** ja **Laura Lappalainen**. Asianmukaisesta suojauksesta kiittää myös työnantaja.

– Monet ihmiset ajattelevat, että he eivät ole hyökkääjiä kiinnostava kohde. Saattaa kuitenkin olla, että hyökkääjä on kiinnostunut esimerkiksi yrityksestä, jossa ihminen työskentelee, Laura Lappalainen sanoo.

– Omaa läppäriään työasioissa käyttävän laite muuttuu tietourkkijalle mielenkiintoiseksi kohteeksi, koska sen avulla voi päästä käsiksi yrityksen tietoihin.

Kenen tahansa tietokone voi olla kiinnostava kohde myös identiteettivarkaille, kiristäjille tai niille, jotka haluavat valjastaa tietokoneen osaksi suurempaa hyökkäystä.

Kiristäjät saattavat esimerkiksi lukita tärkeitä henkilökohtaisia tietoja laitteelta ja vapauttaa ne vasta maksua vastaan.

Hyökkäykseen tietokoneen valjastavien tavoitteena on usein esimerkiksi jonkin verkkopalvelun tekeminen toimintakyvyttömäksi sivuston ruuhkauttamisella.

Tällaisia hyökkäyksiä on kohdistettu tänä vuonna muun muassa verkkopankkeihin.

Hannu K. Niinimäki ja Laura Lappalainen toteavat, että verkossa liikuttaessa ja sen suojauksesta huolehdittaessa avainasia on terveen järjen käyttö. Riittävän vahvat salasanat, virusturvan käyttö ja ajan tasalla olevat ohjelmat ovat hyvä lähtökohta vahvaa tietoturvaa rakennettaessa. KUVA: MINNA HIRVELÄ

Hannu K. Niinimäki toteaa tyytyväisenä, että netinkäyttäjille alkaa olla iskostunut mieleen, että tietokoneella on oltava virusturva ja palomuuri. Muissa asioissa tietoturvaosaaminen vaihtelee valtavasti.

– Omien tietojen levittäminen tämän päivän sosiaalisessa mediassa on aivan villiä. Ihmisten identiteeteistä on saatavilla hirveän paljon tietoa. Myös tietojen varmuuskopioinnista huolehtiminen vaihtelee.

Tärkeimmäksi yksityishenkilön tietoturvan rakennuspalikaksi Niinimäki nostaa ohjelmistopäivitykset.

– Hyökkääjät etsivät vanhentuneita ohjelmia, joissa on tietoturva-aukkoja. Näiden vanhentuneiden ohjelmien kautta päästään luikertelemaan sisään laitteisiin.

– Suurin osa eri ohjelmien päivityksistä on nimenomaan tietoturvapäivityksiä. Vain pienen osan tarkoitus on kehittää ohjelman toimintaa.

Tämän päivän yhteiskunnassa tietoverkkojen suojaaminen liittyy Niinimäen ja Lappalaisen mukaan oleellisesti myös digitaalisuudesta riippuvaisten toimintojen turvaamiseen.

– Nykyään lähes kaikki yhteiskunnan elintärkeät toiminnot, kuten veden ja energian jakelu, rahaliikenne sekä ruokahuolto ovat riippuvaisia digitaalisen ympäristön toimintakyvystä.

Eri toimintojen digitalisoituminen tuo mukanaan kyberuhkia, sillä rikollisuus verkossa on edullista ja helppoa, jos tekijällä on osaamista.

Kyberrikolliset tavoittelevat rahaa tai resursseja, kybervakoilijat urkkivat yritysten ja valtioiden salaisuuksia, ja kyberterrorismi laajentaa terrorismin toimintakenttää.

Niinimäen ja Lappalaisen mukaan sodankäynnin luonteen muuttuminen asettaa valtionhallinnon ja puolustusvoimat uusien haasteiden eteen, kun käytössä on esimerkiksi kauko-ohjattavia ja automatisoituja asejärjestelmiä sekä informaatiosodankäynnin mahdollisuuksia.

– Kyberympäristössä koko sodankäynnin käsite joutuu täysin uuden tarkastelun alle. Voiko maan valloittaa pelkästään informaatiosodankäynnin keinoin kansalaismielipiteisiin vaikuttamalla?

Hannu K. Niinimäki

■ Tietotekniikan opettaja Vaasan yliopistossa

■ Erityisalana informaatioyhteiskunnan ilmiöt ja salausmenetelmät

Laura Lappalainen

■ Tietojärjestelmätieteiden opettaja Vaasan yliopistossa

■ Erityisalana tietojärjestelmien kehittäminen ja käyttäjälähtöisyys

Vaikka tietoverkoissa liikutetaan 2010-luvulla valtavasti tärkeää tietoa, Lappalainen ei koe, että maailma olisi muuttunut digitalisaation myötä aiempaa turvattomammaksi.

Digitalisaatio on luonut erinomaiset mahdollisuudet tehokkaaseen toimintaan eri elämän osa-alueilla.

Uhkaavalta kuulostavasta kyberterrorismista keskusteltaessakin on muistettava oleellinen asia: terrorismi vaatii terroristeilta motiivin.

Mittava hyökkäys esimerkiksi sähkönjakeluun ei ole Suomessa todennäköistä, joskin suojauksen kestävyydestä on silti pidettävä huolta.

– Suomessa on ryhdytty panostamaan turvallisuuteen näissä asioissa. Lisäksi hyökkäyksen tekeminen on todella työlästä ja se vaatii mittavan valmistelemisen lisäksi myös järjestelmien haavoittuvuutta. Jos kaikki on hyvin suojattu ja ajan tasalla, järjestelmiin on hyvin hankalaa päästä käsiksi, Niinimäki vakuuttaa.

Monilla työpaikoilla olisi kuitenkin vielä tehtävää henkilöstön tietoturvatietoisuuden parantamiseksi.

– Useat yritykset tarjoavat tietoturvamateriaalia saataville, mutta eivät kovin aktiivisesti. Tietoturvakoulutusta ei ehkä nähdä yrityksissä niin tärkeänä asiana kuin pitäisi, Lappalainen toteaa.

Juttusarja päättyy.

Huoltovarmuus panee suojautumaan

Energian ja veden jakelu on Suomessa pääosin automatisoitua. Ei ole poissuljettua, että jakelua päästäisiin häiritsemään haavoittuvien tietoliikenneyhteyksien kautta, mutta yhtiöissä on myös suojauduttu tällaisilta uhilta.

JARMO PANULA

VAASA Vaasan Sähköverkko Oy:n toimitusjohtaja **Juha Rintamäki** toteaa yhtiön sähköverkkojen toiminnan olevan täysin tietoverkkojen varassa. Rintamäen mukaan sähköverkon keskeisimpiä osia on ohjattu tietoliikenneyhteyksien kautta jo 1970-luvulta alkaen.

Onko verkon toimintaa mahdollista häiritä kyberhyökkäyksellä?

– Onhan se mahdollista, vaikka tekisi mieli väittää muuta, Rintamäki myöntää.

Verkko on kuitenkin huolellisesti suojattu. Toimivat sähköverkot ovat osa yhteiskunnan huoltovarmuutta, Rintamäki muistuttaa. Esimerkiksi huoltovarmuuskeskuksella on tehtynä tarkastusluettelo, jonka avulla suojauksen tasoa yhtiöissä voi kartoittaa.

– Energiayhtiöiden tietoturvariskejä on kartoitettu tutkimuksilla myös toimialan sisällä. Parhaita käytäntöjä on haettu.

Kaikkea avoimessa verkossa olevaa liikennettä voidaan yrittää häiritä erityyppisin kyberhyökkäyksin, toteaa Anvian IT-palveluiden johtaja **Ari Jaatinen**.

Jaatinen kertoo Anvian suhtautuvan tietoturvallisuuteen vakavasti kaikessa toiminnassaan.

Onko kysymys siitä, että joku haluaisi häiritä yhteyksienne toimintaa, ylipäätään mielestäsi oleellinen tänä päivänä?

– Kysymys ei välttämättä ole siitä, että jokin taho haluaisi erityisesti häiritä juuri Anviaa tai sen asiakkaita. Pikemminkin kyse on siitä, että kun häirintä kerran on mahdollista avoimissa tietoverkoissa, siihen on myös varauduttava ja häirinnältä on suojauduttava.

– Oman kehitys- ja valvontatyön lisäksi seuraamme aktiivisesti eri tahojen, muun muassa kyberturvallisuuskeskuksen, suosituksia ja ohjeistuksia.

Seinäjoen Vesi Oy:n toimitusjohtaja **Juha Santtila** toteaa, että kyberuhat ovat olleet kasvava puheenaihe myös vesihuollon huoltovarmuudesta keskusteltaessa.

– Asia on ollut paljon esillä. Teemme jatkuvasti parannuksia järjestelmiimme ja niihin pääsy on pyritty tekemään mahdollisimman hankalaksi. Tietoturva-aukkoja on etsitty tietoisesti ja niitä on tukittu, Santtila kertoo.

Veden jakelun keskeyttäminen kyberhyökkäyksellä ei ole yksinkertaista.

– Arvelen, että hakkerit pystyvät aiheuttamaan ehkä lähinnä laiterikkoja.

Digitalisaatio ja automaatio ovat muuttaneet myös veden jakelua. KUVA: MARIA MÄKI

Teemme jatkuvasti parannuksia järjestelmiimme ja niihin pääsy on pyritty tekemään mahdollisimman hankalaksi. Tietoturva-aukkoja on etsitty tietoisesti ja niitä on tukittu.
Juha Santtila, Seinäjoen Vesi Oy:n toimitusjohtaja

Iltapäiväseminaari torstaina

Sanomalehtiyliopiston iltapäiväseminaari järjestetään torstaina 5.11. Vaasan yliopiston Wolff-auditoriossa Tervahovirakennuksessa osoitteessa Wolffintie 34.

Ohjelma:
■ klo 15.00 Seminaarin avaus. Koulutuspäällikkö Reetta Kungsbacka, Avoin yliopisto

■ klo 15.10 Digin mahdollisuudet perinteisessä sanomalehdessä. Päätoimittaja Toni Viljanmaa, sanomalehti Pohjalainen

■ klo 15.30 Digitalisaation rakenteelliset jännitteet. Professori Tero Vartiainen

■ klo 16.00 Kahvit tarjoaa sanomalehti Pohjalainen

■ klo 16.30 Digitaalisuus tietotyössä. Professori Tanja Sihvonen, Vaasan yliopisto

■ klo 17.00 Internet of things nykypäivänä ja tulevaisuudessa. Toimitusjohtaja Pasi Tuominen, Wapice Oy

■ klo 17.30 Loppukeskustelu ja päätössanat. Professori Tero Vartiainen

■ Seminaari on maksuton ja avoin kaikille. Ilmoittautumiset kahvitarjoilun vuoksi viimeistään tänään 2.11.2015 puhelimitse: 029 449 8190 tai sähköpostitse: avoinyo@uva.fi

■ Tilaisuuden hashtag: #digivaikutukset