TIVIA news
4/2022
TIETO- JA VIESTINTÄTEKNIIKAN AMMATTILAISET TIVIA RY

KYBERRIKOLLISUUS

VERKON RIKOLLISUUS TUTKITTAVANA

Perinteinen rikollisuus on siirtynyt voimakkaasti verkkovälitteiseksi. Kyberrikoksiin liittyvä tutkimus nostaa esille keskeiset löydökset.

LUOVUUDEN TULEVAISUUS

OHJELMAA GDPR:STÄ KYBERTURVAAN

DIGITALISAATIO ARJEN TUKENA

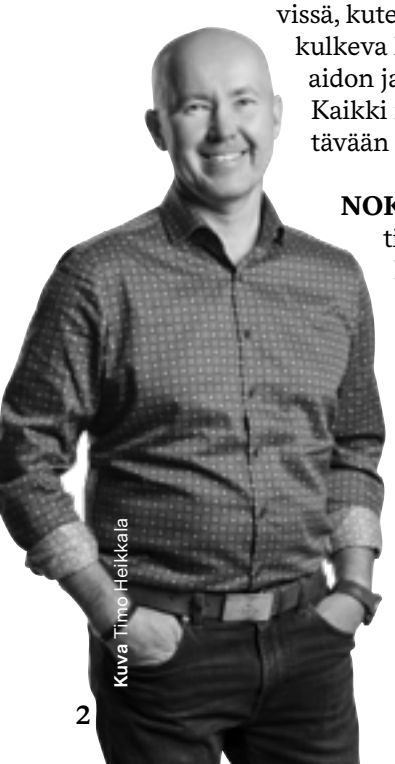
PÄÄKIRJOITUS

LUOVUUDEN TULEVAISUUS

Miljardit ihmiset käyttävät päivittäin Suomessa kehitettyjä teknologioita. Ratkaisumme ovat päätelaitteissa ja puettavassa älyssä mutta suurin osa kuitenkin käyttäjän näkymättömissä tietoliikenneverkoissa ja tukiasemien teknologiaratkaisuissa. Kun USA:n ”*one grand challenge*” oli saada ukko kuuhun, oli suomalaisten vastaava haaste mahdollistaa puhelimen käyttö langattomasti liikkuvassa kohteessa. Langaton datasiirto ja satojen muiden ratkaisujen kokonaisuus kruunasivat älypuhelinkokemuksesi. Teknologiaosaaminen yhdistettynä luovuuteen toivat meille vuosikymmenien hyvinvoinnin.

ZENIITIN SAAVUTTAMISEN jälkeen luisuimme hetkelliseen alamäkeen. Loimme kuitenkin jäljelle jääneestä teknologisesta osaamisesta uuden tulevaisuuden, jälleen kerran luovuutta ja yksittäisten ihmisten näkemyksiä ja innovatiivisuutta tukien. Syntyi startup-kulttuuri ja tuhansia uusia teknologiaorientoituneita yrityksiä. Osaaminen levisi tietoliikenneverkoista, päätelaitteista, puettavasta älystä ja tietoturvasta alustatalouteen, terveyteen, turvallisuuteen, liikenteeseen ja peliteollisuuteen. Uudistimme myös rahoituskulttuuriamme ja yritysten toimintaympäristöjä mutta suurin henkinen muutos oli startup-yrittäjän epäonnistumisen hyväksyminen.

NYT OLEMME eläneet muutaman vuoden suvannossa. Näkyviä uusia kansallisia avauksia tai innovaatio- tai yrityskulttuurin ilmiöitä ei ole nähty. Tulevaisuuden trendit ovat kyllä selkeästi nähtävissä, kuten esimerkiksi autonominen vedyllä ja sähköllä kulkeva liikenne tai metaversumin kokemukset, joissa aidon ja digitaalisen maailman raja on huomaamaton. Kaikki nämä globaalit haasteet olisi toteutettava kestävään kehitykseen perustuen.



Kuva Timo Heikkala

NOKIAN MATKAPUHELINTEN jälkeen sanottiin, ettemme koskaan näe samanlaista nousua. Näimme kuitenkin tuhansien startup-yritysten synnyn ja kymmenien päätymisen globaaleiksi toimijoiksi. Tarvitsimme enemmän kuin koskaan luovuutta, jotta voimme kiihdyttää takaisin yhdeksi maailman johtavista innovaatiokeskittymistä. Tulevaisuuden trendit ja teknologiaosaaminen kohtaavat esimerkiksi **Luova Työelämä 2030 -hankkeessa**, jossa *MARKin* luotsaamana *TIVIA* ja muut merkittävät toimijat rakentavat osaltaan Suomen tulevaisuutta. ■

Janne Mustonen
toimitusjohtaja, TIVIA

TIVIA news

JULKAISIJA
Tieto- ja viestintätekniikan ammattilaiset TIVIA ry

PÄÄTOIMITTAJA
Janne Mustonen

ULKOASU
Olli Teräs

TOIMITUSKUNTA
Eija Kalliala,
Joona Haavisto, Olli Teräs

KANNEN KUVA
Shutterstock

TIVIA

YHTEYSTIEDOT
TIVIA
Lars Sonckin kaari 12
02600 Espoo
tivia@tivia.fi
tivia.fi

JÄSENASIAT
jasenasiat@tivia.fi

TEKNOLOGIA 22
3.–5.5.2022 Messukeskus Helsinki

OHJELMAA GDPR:STÄ KYBERTURVAAN

Teksti Paula Miinalainen, Joona Haavisto **Kuva** Messukeskus

Teknologia 22 -messuilla *TIVIAn* jäsenyhdistykset tuottavat osan ICT-lavan ohjelmasta. Nyt esittelemme *Tietoturva ry:n* ja *TIVIA Uusimaa ry:n* ohjelmanumerot.

TIVIA Uusimaa on lavalla 4.5.2022 aamupäivän ja alkuun on esittelyssä Digirata-hanke, jonka tavoitteena on uudistaa nykyinen ja vanhentuva junien kulunvalvontajärjestelmä uudella, digitaalisella ja EU-vaatimusten mukaisella kulunvalvontajärjestelmällä.

Jari Kenttä *AddSecurelta* kertoo, millaisia vaatimuksia talo- ja turvatekniikan turvalliseen hallintaan liittyy ja miten yleinen toiminnan kehittäminen tarpeeseen vaikuttaa.

Zero Trustista kertoo *Netumin* **Tatu Vehmas.** Kyseessä on suojausmalli, joka sopeutuu tehokkaasti nykyaikaisen ympäristön monimutkaisuuteen, kattaa hybridityöpaikan sekä suojelee käyttäjiä, laitteita, sovelluksia ja tietoja niiden sijainnista riippumatta.

GDPR ja suomalainen yritysmaailma -esityksessä johdon konsultti **Paula Miinalainen** painottaa, että GDPR tulee olla mukana yrityksen kehitystyössä hankkeen alusta loppuun. Näin tehdään tietosuojasta yritykselle vahvuus. Ennen kuin päätetään uuden teknologian hankinnasta, analysoidaan ratkaisun mahdollinen vaikutus henkilötietojen käsittelyyn, toteutusvaiheessa asetuksen vaateet huomioidaan työn edetessä ja hyvällä viestinnällä varmistetaan kilpailuetu.

Tietoturva ry ottaa ICT-lavan haltuun torstaina 5.5. aamupäivän ajaksi erittäin ajankohtaisella teemalla, sähkönjakelun kyberturvallisuus ja huoltovarmuus.

Puheenvuoroja on sähkönjakelun kaikilta kerroksilta; *Huoltovarmuuskeskukselta*, *Fortumilta*, *Fingridilta*, *Carunalta*, *Helenilta* sekä *Hitachi Energyltä*.

Sähköverkon kyberturvallisuus on aiheena sellainen, että se on, tai ainakin pitäisi olla jatkuvan mielenkiinnon kohteena. Olemme varmasti kaikki seuranneet Ukrainan tapahtumia, jossa jo ennen varsinaisia fyysisiä sotatoimia sähköverkot kaadettiin joulukuussa kyberhyökkäyksellä. ■

Hyvä järjestelmäkuvaus

10.–11.5.2022

▶ Osallistujat saavat kattavan kokonaiskuvan hyvän järjestelmäkuvauksen rakenteesta ja sisällöstä. He oppivat mm. **tietojärjestelmän koko elinkaaren** kattavan vaatimusten ja kuvausten hallinnan prosessin sekä tuottamaan asiallisia kuvauksia.

CXO-koulutusohjelma

11.8.–15.12.2022

▶ Johdon CXO-koulutusohjelmaan osallistuja saa kokonaisvaltaisen kuvan nykyajan modernista digijohtamisesta. Koulutuksen jälkeen ymmärrät millaisia mitattavia hyötyjä IT:n ja digitalisaation johtaminen organisaation johtamisjärjestelmän osana tuottaa, ja mitä tällainen johtaminen konkreettisesti tarkoittaa jokapäiväisenä tekemisenä.

Cloud Security Summit

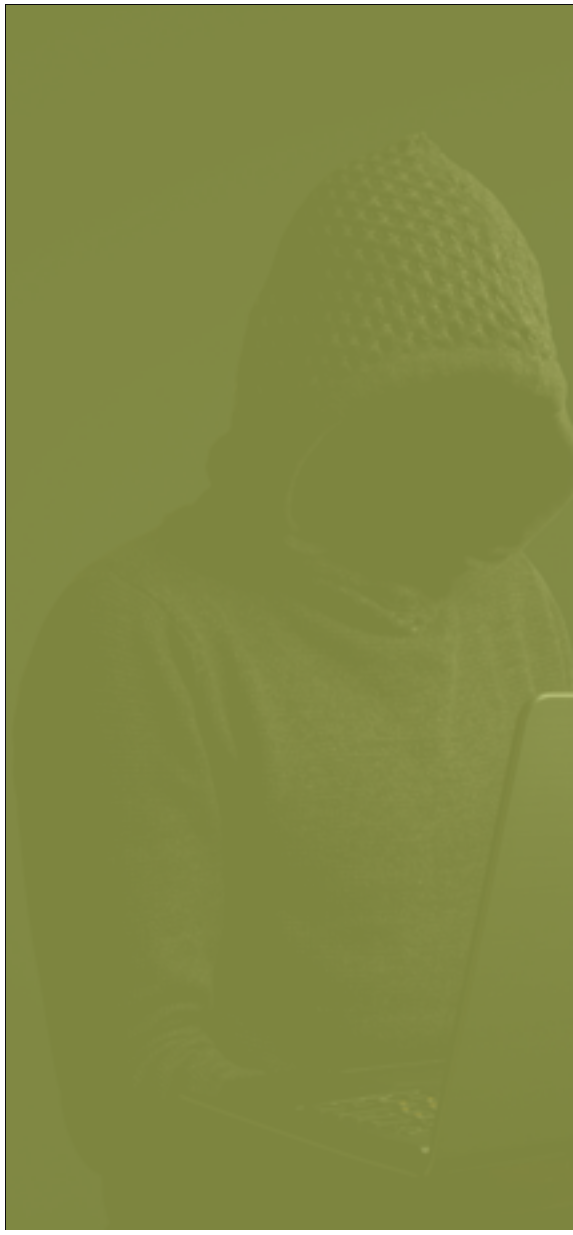
21.9.2022

▶ Tapahtumassa kuulemme tietoturvan huippuasiantuntijoilta tarinoita pilviturvallisuudesta, miten heidän organisaatioissaan **pilvipalveluiden tietoturvahaasteisiin** on varauduttu, ja mitkä ovat pilvipalveluiden kuumimmat trendit. Ilmoittautumalla 31.5. mennessä pääset hyödyntämään Early Bird -etuhinnan kaksi yhden hinnalla.

tivia.fi/koulutukset

KYBERRIKOLLISUUS

KYBERRIKOKSET TUOMIO-ISTUIMISSA



Kyberrikollisuus on nouseva rikollisuuden muoto, mitä ilmentää esimerkiksi se, että kyberrikollisuuden torjunta on noussut viime vuosina monien eurooppalaisten valtioiden turvallisuusstrategioiden keskeiseksi painopistealueeksi. Perinteinen rikollisuus on siirtynyt myös voimakkaasti verkkovälitteiseksi. Kyberrikollisuuteen liittyvä tutkimus on kuitenkin ollut vähäistä.

Kyberrikollisuuteen liittyvä kansainvälinen tutkimus on lisääntynyt viime vuosina. Tutkimus on kuitenkin tekniikkaan ja insinööritieteisiin painottunutta. Kyberrikollisuutta koskeva kotimainen kriminologinen ja rikosoikeudellinen tutkimus on ollut hyvin vähäistä, vaikka kyberrikosten sääntely on lisääntynyt voimakkaasti viime vuosien aikana. Rikoslaissa keskeisenä on *38 luku*, jossa säädetään tieto- ja viestintärikoksista. Kyberrikoksia koskevia säännöksiä sisältyy myös muihin rikoslain lukuihin. Olemme tehneet kyberrikoksiin liittyvän tutkimuksen (**Paasonen**, **Aaltonen** & **Luomala** 2021), joka on julkaistu *Defensor Legisissä* (4/2021). Tässä tuodaan esille keskeiset tutkimustulokset.

POLIISIN TIETOON TULLEET RIKOKSET JA TUOMIOT

Poliisiin tietoon tulleiden tieto- ja viestintärikosten määrä on kasvanut selvästi 2010-luvulla. Vuonna 2010 poliisin tietoon tuli yhteensä 717 rikosta, vuonna 2019 peräti 5 202 rikosta (taulukko 1). Valtaosan tästä kasvusta selittää identiteettivarkauden kriminalisointi vuonna 2015. Muiden nimikkeiden yhteenlaskettu määrä on kasvanut vuosien 2010–2019 aikana maltillisemmin, mutta kuitenkin noin 80 prosenttia.

Tietoon tulleiden rikosten määrään suhteutettuna tieto- ja viestintärikoksista käräjäoikeuksissa tuomittujen rangaistusten määrä on varsin matala: vuosina 2015–2019 tuomittujen henkilöiden määrä (yhteensä 206 henkilöä) on ollut vuosittain korkeimmillaan 48. Koska tuomiotilastot laaditaan päärikosperustaisesti, suora vertailu kaikki rikosepäilyt erikseen laskeviin poliisitilastoihin on harhaanjohtava. Paremmin vertailukelpoinen, tuomioissa syyksi luettujen rikosten määrä onkin selvästi korkeampi, viime vuosina keskimäärin vajaat 500 kappaletta.

Eroa päärikospohjaiseen tuomittujen määrään selittää erityisesti rangaistusasteikoltaan vakavampien rikosten oheisrikoksena esiintyvien identiteettivarkauksien suuri määrä viime vuosina. Tästä rikostilastointiin liittyvästä seikasta huolimatta tieto- ja viestintärikoksista tuomittujen määrää voidaan pitää yllättävän alhaisena. Esimerkiksi vuonna 2018

Vuosina 2010–2019 poliisin tietoon tulleet tieto- ja viestintärikokset

Taulukko 1 | rikoslain 38 luku

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Salassapitorikos 38:1§1/1–2	29	55	43	49	39	47	41	45	59	51
Salassapitorikkomus 38:2§1–2	17	22	16	14	14	13	20	7	16	20
Viestintäsalaisuuden loukkaus 38:3§1/1–2	293	295	232	279	294	291	406	352	304	254
Viestintäsalaisuuden loukkauksen yritys 38:3§2	1	0	1	0	0	1	3	1	0	0
Törkeä viestintäsalaisuuden loukkaus 38:4§1/1–3	1	1	4	3	4	0	3	1	5	0
Tietoliikenteen häirintä 38:5§1	24	79	47	93	54	84	67	61	32	39
Tietoliikenteen häirinnän yritys 38:5§2	0	1	1	0	0	1	0	0	0	1
Törkeä tietoliikenteen häirintä 38:6§1/1–6	2	4	7	13	6	3	10	15	14	8
Lievä tietoliikenteen häirintä 38:7§1	8	3	5	9	5	6	9	6	3	11
Tietoliikenteen lievän häirinnän yritys 38:7§2	0	1	0	0	0	0	0	1	0	0
Tietojärjestelmän häirintä 38:7a§1	4	3	9	11	10	30	38	23	20	9
Tietojärjestelmän häirinnän yritys 38:7a§2	0	0	0	0	1	4	0	0	0	0
Törkeä tietojärjestelmän häirintä 38:7b§1/ 1–5	0	0	0	0	3	7	16	14	9	5
Tietomurto 38:8§1–2	292	403	462	582	339	342	410	395	477	772
Tietomurron yritys 38:8§3	8	11	10	5	14	40	13	17	22	16
Törkeä tietomurto 38:8a§1/1–2	1	8	14	5	6	3	8	19	8	6
Törkeän tietomurron yritys 38:8a§2	0	0	0	0	0	0	0	8	0	0
Suojauksen purkujärjestelmärikos 38:8b§	0	0	0	0	2	0	0	0	0	0
Tietosuojarikos 38:9§1/1–3	37	90	135	116	484	108	103	91	75	82
Identiteettivarkaus 38:9a§1	0	0	0	0	0	530	3 308	3 964	3 810	3 928
YHTEENSÄ	717	976	986	1 179	1 275	1 510	4 405	5 020	4 854	5 202

Kuvat Shutterstock

poliisi kirjasi lähes 500 tietomurtoepäilyä, mutta seuraavana vuonna tuomittiin ainoastaan kaksi henkilöä tietomurrosta, ja syyksi luettiin viisi rikosta.

Vuonna 2010 poliisin tietoon tuli yhteensä 717 rikosta, vuonna 2019 peräti 5 202 rikosta

Selvästi yleisin seuraamus on tuomioistuimessa määrätty sakko (taulukko 2), joka oli seuraamuslajina noin neljässä viidestä tuomiosta. Näiden lisäksi vuosina 2015–19 annettiin 17 rangaistusmääräystä. Yhteensä 7 henkilöä tuomittiin viiden vuoden aikana ehdottomaan vankeusrangaistukseen. Näistä kolmessa tapauksessa päärikoksena oli tietoliikenteen häirintä, neljässä törkeä tietoliikenteen häirintä.

TEONPIIRTEET VUOSIEN 2015–2019 KÄRÄJÄOIKEUSAINEISTOSSA

Kaikkien tuomioiden osalta voidaan yleishavaintona todeta, että edistyneempiä ”hakkerointitaitoja” ilmentävät rikokset ovat aineistossa vähemmistössä. Noin 80 prosenttia rikoksista tehtiin menetelmin, joka vastaavat tietojärjestelmän normaalia käyttöä, kuten esimerkiksi toisen henkilön käyttäjätunnuksen ja salasanan hyödyntämistä järjestelmään kirjautuessa (tietomurto). Haittaohjelmaa tai algoritmia käytettiin ainoastaan 12 tapauksessa.

Yleisin syyksi luettu tieto- ja viestintärikos tuomioaineistossamme on viestintäsalaisuuden loukkaus. Tietoliikenteen häirintärikoksissa (perusmuotoinen tai törkeä) korostuvat puolestaan aiheettomat hätäkeskussoitot. Noin 80 %:ssa tuomioista oli kyse tällaisesta teosta. Pahimmissa tapauksissa soittoja oli tehty useita satoja kertoja.

Tietosuojarikoksia puolestaan dominoivat potilastietojen asiattomat katselut, ja mukana on lisäksi useita tapauksia, joissa poliisi tuomittiin samalla virkavelvollisuuden rikkomisesta Poliisiasiain tietojärjestelmän tietojen perusteettomasta käytöstä.

Törkeissä tietomurroissa tekoko- ▶

Tieto- ja viestintärikoksista käräjäoikeuksissa vuosina 2015–2019 tuomitut rangaistukset

Taulukko 2

Ehdoton vankeusrangaistus	0	2	1	4	0	3 %
Yhdyskuntapalvelu	0	0	1	0	0	0 %
Ehdollinen vankeusrangaistus	3	8	10	1	1	11 %
Sakko	29	33	34	42	28	81 %
Aikaisempi rangaistus riittävä seuraamus	0	1	0	0	0	0 %
Tuomitsematta jättäminen	1	3	2	0	2	4 %
YHTEENSÄ	33	47	48	47	31	100 %

Lähde: Tilastokeskus, Syytetyt, tuomitut ja rangaistukset

konaisuudet olivat huomattavasti laajempia ja tekotavoiltaan teknisesti vaativampia, mutta toisaalta näitä tuomioita oli aineistossa ainoastaan kaksi kappaletta viiden vuoden aikana. Törkeiden tietomurtojen lisäksi edistyneempiä kyberrikoksia aineistossa edustavat tietojärjestelmä häirintärikokset. Törkeistä tietomurroista tuomitut tuomittiin myös törkeästä tietojärjestelmän häirinnästä.

Palvelunestohyökkäykset ovat keskeinen tekotapa näissä rikoksissa, ja yhtä tapausta lukuun ottamatta muissa tuomiossa, joissa syyksi luettiin joko perusmuotoinen tai törkeä tietojärjestelmän häirintä, kyseessä oli nimenomaan tällainen teko. Ainoastaan seitsemän tuomioita sisälsi vähintään yhden tällaisen teon, joten näidenkin rikosten voidaan todeta olevan vielä varsin harvinaisia tuomioistuimissa.

JOHTOPÄÄTÖKSIÄ

Tuomioistuinaineistomme analyysin perusteella vaikuttaa siltä, että keskeinen syy suhteellisen lievään rangaistuskäytäntöön tieto- ja viestintärikoksissa on se, että tällä hetkellä tuomioon saakka päätyvät rikokset edustavat verrattain lieviä tekomuotoja. Vaikka onkin todennäköistä, että rikosilmoituksiksi päätyy vain pieni osa kaikista kyberrikoksista, on tietoon tulleiden rikostenkin empiirisessä tutkimuksessa paljon tehtävää, joka voisi hyödyttää rikoksentorjuntaa.

Suuri ero tietoon tulleiden rikosten ja syyksi luettujen tieto- ja viestintärikosten lukumäärässä viittaa siihen, että valtaosa rikosepäilyistä päättyy joko esitutkintaan tai syyteharkintaan, mutta syitä tähän ei tunneta. Toisaalta on selvää, ettei viranomaisten tietoon tulleen kyberrikollisuuden koko kuvaa saada selville keskittymällä ainoastaan rikoslain 38 luvun mukaisiin rikosepäilyihin tai -tuomioihin, vaan rikosilmoituksia ja tuomioita tulisi käydä laajemmin läpi useampien sellaisten rikoslajien osalta, joissa on todennäköisesti kyberrikollisuuden elementtejä. Tällaisia rikoslajeja ovat muun muassa huumausainerikokset, petosrikokset, laittomat uhkaukset sekä yksityiselämää koskevan tiedon levittäminen.

Kyberrikokset ovat tällä hetkellä merkittävä haaste rikosoikeusjärjestelmälle ja sitä kautta rikosvastuun toteutumiselle. Vaikuttaa selvältä, että lisäpanostukset kyberrikollisuuden torjuntaan ja paljastamiseen ovat tarpeen. Kyberturvallisuuden kehittämistoimia on tehty kansallisesti ja EU-tasolla. Näissä korostuu vahvasti julkisen sektorin rooli ja erilaiset sääntelyratkaisut. Kyberturvallisuuden kannalta olennaista on kuitenkin elinkeinoelämän rooli ja yritysten riskienhallinta, jonka takia eri sääntelyratkaisuiden kannustinvaikutuksiin ja tehokkuuteen pitäisi kiinnittää nykyistä enemmän huomiota. Tämän takia olisi tärkeää, että aihetta tutkittaisiin monipuolisesti, kun kyberrikollisuus kasvaa voimakkaasti. Kyberrikollisuuden laajuus voi olla paljon suurempi kuin tiedetään, ja taloudellisten vahinkojen arviointi on tästä syystä haastavaa. Tämän takia olisi tärkeää kehittää myös kyberrikosten mittaamista ja seurantaa. ■

Artikkelin kirjoittaja OTT **Jyri Paasonen** on turvallisuusalan tutkija ja dosentti.

TEKOÄLY JA METAVERSUMI. Esityksessään Risto Linturi yhdessä digitaalisten kaksostensa ja tekoälyn voimaannuttamien virtuaaliapulaistensa kanssa kuvaa viestinnän ja vuorovaikutuksen tulevaisuutta tekoälyn, virtuaalitodellisuuden, digitaalisten kaksosten ja metaversumin maailmassa.

DIGITALISAATIO ARJEN TUKENA

Teksti Paula Miinalainen, Joona Haavisto **Kuva** Risto Linturi

Lähityöstä siirryttiin hybridityöhön nopealla tahdilla, tuoden viestintään murrosta ja johtamiseen ketteryyttä. *TIVIA Uusimaa* ja *AKVA-verkostomme* järjestävät seminaarin 13.–14. toukokuuta Sannäsin kartanolla Porvoossa. Tervetuloa mukaan keskustelemaan digitalisaation murroksesta ja verkostoitumaan upeissa maisemissa.

Osittainen etätyö tuli jäädäkseen ja tarvitsee uutta johtamistapaa, palautteen antamista ja palautumista. Digitaalinen turvallisuus on ajankohtaisempi ja herkempi asia kuin se on ollut milloinkaan. Näistä teemoista kertovat seminaarin asiantuntijamme.

Risto Linturi, tulevaisuudentutkija

Tekoäly ja metaversumi: Digitaalisen viestinnän radikaali murros alkaa nyt!

Kimmo Rousku, tietokirjailija, johtava erityisasiantuntija, VAHTI-pääsihteeri Digi- ja väestötietovirastossa

Digitaalinen turvallisuus mahdollistaa digitalisaation.

Nina Nissilä, johtaja, Kela

Digitalisaatio Kelassa – ketterästi kohti uutta.

Katrina Harjuhahto-Madetoja, toimitusjohtaja, Innovaltti Oy

Johtamisen uusi normaali – lähityöstä hybridityöhön

Pia Ek, asianajaja, osakas Castrén & Snellman

Digiloikka juristin silmin

Joona Haavisto, Senior Software Developer & People Person at Gofore

Ketteryyskokemuksia

Merja Mattsson, projektipäällikkö, CGI

Palautumisen ja palautteen merkitys asiantuntijan arjessa.

Paula Miinalainen, johdon konsultti, Arbor Vitae – Finland Oy ■

EU:n tietosuoja-asetus kehitystyössä.

Lauantai-illan vietämme saunaosastolla rentoutuen, syöden ja toisiimme tutustuen.

Miten digitalisaatiosta tulee arjen tuki
13.–14.5.2022
Sannäsin kartano, Porvoo

Tilaisuuden ohjelma ja ilmoittautuminen TIVIA Uusimaan nettisivuilla.

▶ tiviauusimaa.fi

AJANKOHTAISTA


Kuva: Shutterstock

Merkitykselliset projektit onnistuvat

21.4.2022

▶ Tule mukaan merkityksen löytöretkelle *PM Clubin* webinaariin 21.4. Mailan varressa webinaarissa Kumuran **Mikko Saastamoinen** ja **Merja Galler**. Webinaari on maksuton ja pidetään Zoom-sovelluksella. Webinaarin jälkeen on mahdollisuus jäädä linjoille keskustelemaan.

Teknologia 22

3.–5.5.2022

▶ Teknologia 22 on Pohjois-Euroopan johtava teknologian ja teollisuuden messutapahtuma. Teknologia-messukokonaisuus koostuu useista eri osa-alueista, joita ovat mm. **elektroniikka**, **robotiikka** ja **ICT**. *TIVIA* ja jäsenyhdistyksistä *TIVIA Uusimaa*, *ICT Leaders Finland, Tietoturva* ja *Sytyke* vastaavat messujen ICT-lavana toimivan TIVIA Stagen ohjelmasta. Tapahtuman teemana on tänä vuonna "Kestävän huomisen ratkaisut".

Current trends in German automotive industry

17.5.2022

▶ This *TIVIA* webinar will illustrate recent developments in **Germany's automotive and mobility sector** with a special focus on the region of Baden-Württemberg. It will illustrate current challenges and opportunities as well as potential fields of cooperation with technology developers and suppliers.

tivia.fi/tapahtumat