TIVIA | 10/2025 news

KYBER-VARAUTUMINEN

DIGITALISAATION KOLIKKO

KYBERRIKOLLISUUS JA TEKOÄLYN VARJOPUOLET

STRIDE UHKAMALLINNUKSEEN JA RISKIENHALLINTAAN

PÄÄKIRJOITUS

TEKOÄLY RISKIENHALLINNAN MOOTTORINA

Tekoäly on mullistanut riskienhallinnan tarjoamalla tehokkaita tapoja tunnistaa, analysoida ja hallita riskejä. Se pystyy käsittelemään valtavia datamääriä, tunnistamaan piileviä riskitekijöitä ja havaitsemaan poikkeamia esimerkiksi talousdatan, tuotannon tai käyttäytymisen perusteella. Tämä mahdollistaa nopean reagoinnin ja tarkemmat ennusteet.

Reaaliaikainen valvonta on tekoälyn merkittävä etu: se voi seurata markkinoita, toimitusketjuja tai kyberturvallisuushälytyksiä ja antaa välittömiä varoituksia. Visuaaliset tilannekuvat ja simulaatiot tukevat päätöksentekoa ja auttavat arvioimaan riskien todennäköisyyksiä ja vaikutuksia, myös taloudellisesta näkökulmasta.

Tekoäly tehostaa riskienhallintaprosessia optimoimalla resurssien käyttöä ja nopeuttamalla päätöksentekoa. Se voi analysoida laajoja dokumenttiaineistoja, priorisoida olennaiset uhkat ja auttaa organisaatioita keskittymään kriittisiin riskeihin.

Myös ympäristöriskien hallinnassa tekoäly on hyödyllinen. Sääennusteiden ja ilmastomallien avulla se voi ennustaa esimerkiksi myrskyjä tai tulvia sekä arvioida niiden vaikutuksia toiminta-ympäristöön. Maineenhallinnassa tekoäly seuraa sosiaalista mediaa, tunnistaa negatiivisia keskustelutrendejä ja varoittaa niistä.

Petosten ja väärinkäytösten ehkäisyssä tekoäly tunnistaa epäilyttävää toimintaa, automatisoi tarkastuksia ja vahvistaa sisäistä valvontaa. Lisäksi se tukee koulutusta esimerkiksi riskisimulaatioiden avulla.

Tekoäly ei korvaa ihmisten tekemää päätöksentekoa, mutta toimii tehokkaana työkaluna, joka vahvistaa riskien tunnistamista, analysointia ja hallintaa.

Jyri Paasonen
turvallisuusoikeuden
apulaisprofessori, Vaasan yliopisto
Tietoturva ry:n hallituksen jäsen

JULKAISIJA
TIVIA ry

PÄÄTOIMITTAJA
Juha Lappi

TOIMITUSKUNTA
Timo Piiparinen

ULKOASU JA TAITTO
Visionomi

YHTEYSTIEDOT
TIVIA ry
c/o TIVIA Infuture Oy
Firdonkatu 2 T 63
00520 Helsinki
tivia@tivia.fi
tivia.fi

Etusivun kuva: Philipp Katzenberger, Unsplash

DIGITALISAATION KOLIKKO Mahdollisuus vai uhka

Teksti: Jyri Paasonen

Teollinen vallankumous 1700-1800 -lukujen taitteessa mullisti maailman pysyvästi. Koneet korvasivat käsityön, syntyi tehdasteollisuus ja sähkötekniikka kehittyi. Ihmisten arki ja yhteiskunta muuttuivat perusteellisesti - harva ilmiö on muokannut historiaa yhtä syvästi.

Nyt elämme digitalisaation vallankumousta. Oma sukupolveni on kokenut sen lähietäisyydeltä: Commodore64 -harjoituksista ja kasettiasemista siirryttiin korppuihin, 8-bittinen Nintendo valtasi olohuoneet, Nokian puhelimet täyttivät taskut ja internet muutti koko elämänpiirin. Digitalisaatio on helpottanut arkea, mutta samalla se on synnyttänyt uuden uhan - kyberrikollisuuden.

Jo ennen varsinaista kyberaikaa rikollisuudessa nähtiin muutos. 1990-luvun alussa länsimaissa perinteiset omaisuus- ja väkivaltarikokset vähenivät, mutta syitä “crime drop” -ilmiölle ei ole yksiselitteisesti selitetty. Yksi teoria on, että digitaalinen murros muutti arkea ja ajankäyttöä, avaten samalla uusia rikollisuuden muotoja ja tarjoten perinteiselle rikollisuudelle uusia mahdollisuuksia.

Kyberrikollisuus näkyy arjessa konkreettisesti: kalasteluviestejä tulvii sähköposteihin, palvelunestohyökkäykset kaatavat järjestelmiä ja yksi haavoittuvuus voi lamauttaa kokonaisen organisaation. Digitaalinen jälki mahdollistaa kuitenkin myös rikosten selvittämisen. Vastaamon tietomurto kuvastaa rikosten massoittumista, kun taas FBI:n Greenlight-operaatio osoittaa, että kansainvälisellä yhteistyöllä kyberrikollisuutta voidaan torjua tehokkaasti.

Haasteena on, että kyberrikollisuudesta ei ole luotettavaa kokonaiskuvaa. Yhtenäiset oikeudelliset määritelmät puuttuvat, kansainväliset tilastot ovat hajanaisia,
ja kriminologinen tutkimus on keskittynyt perinteisiin rikoksiin. Ilman tarkkoja mittareita päätöksenteko ja resurssien kohdentaminen jäävät vajaiksi.

Kyberrikollisuus kasvaa ja skaalautuu globaalisti. Yksikin rikollinen voi tavoittaa hetkessä tuhansia uhreja, ja kiinnijäämisriski on usein pieni. Tämä haastaa rikosoikeusjärjestelmät ja rikosvastuun toteutumisen.

Ratkaisuja haetaan kansallisesti ja EU-tasolla. Sääntelyä on tiukennettu, viranomaisten kyvykkyyksiä vahvistettu ja kriittisille toimijoille asetettu uusia velvoitteita. Silti on muistettava, että kyberturvallisuus ei ole ensisijaisesti viranomaisten, vaan yritysten vastuulla. Yritykset hallitsevat järjestelmät, prosessit ja datan - ja siten suurin osa riskienhallinnan ratkaisuista on niiden käsissä.

Tarvitsemme selkeitä määritelmiä, parempia mittareita ja laadukkaampaa dataa. Sääntelyn tulee kannustaa oikeisiin tekoihin, kuten haavoittuvuuksien hallintaan, toimitusketjujen turvaamiseen ja jatkuvuudenhallintaan. Yrityksille on tarjottava ymmärrettävä, riskiin suhteutettu velvoitekehikko ja tilaa innovoida. Kun kannusteet ja käytännöt tukevat toisiaan, kyberturvallisuus voi olla kilpailuetu, ei pelkkä kustannus.

Digitalisaation kolikko ei ole hyvä tai paha - se on voima, joka muokkaa yhteiskuntaa. Meidän tehtävämme on varmistaa, että kyvykkyys, vastuut ja kannusteet kohtaavat. Vasta silloin vallankumouksen hyödyt voivat ylittää sen riskit.

KYBERRIKOLLISUUS JA TEKOÄLYN

Teksti: Jyri Paasonen

Tekoäly on noussut arjen työkalusta myös rikollisuuden vipuvarreksi. Europolin vuonna 2024 julkaisema analyysi kuvaa 821 EU:ssa toimivaa rikollisverkostoa ja yli 25 000 jäsentä, joiden toimintaa leimaa kansainvälisyys ja kyvykkyys hyökätä useissa maissa samanaikaisesti. Kyberhyökkäyksiin erikoistuneissa verkostoissa tyypillinen malli on “ransomware-as-a-service”: ydinryhmä tarjoaa haittaohjelman ja hoitaa lunnasneuvottelut, kun kumppanit toteuttavat iskut ja jakavat tuotot. Tämä työnjako laskee kynnystä osallistua ja kasvattaa rikollisen toiminnan mittakaavaa.

Kielimallien turvatoimet eivät sulje riskejä: epäsuorat tai vaiheistetut pyynnöt voivat ohittaa suojauksia, ja mallit tuottavat idiomaattista, uskottavaa tekstiä millä tahansa kielellä. Se tekee sosiaalisesta manipuloinnista ja tietojenkalastelusta aiempaa vaikeammin tunnistettavaa, mahdollistaa massakohdennuksen ja tarjoaa välineet disinformaation, propagandan ja identiteetin jäljittelyn tehostamiseen. Kun viestit näyttävät ja tuntuvat ”oikeilta”, uhrin erehtymisen todennäköisyys kasvaa - ja tekoälyn nopeus sekä skaalautuvuus moninkertaistavat vaikutuksen.

Suurin muutos näkyy sosiaalisessa manipuloinnissa ja tietojenkalastelussa. Kielimallit tuottavat idiomaattista, virheetöntä tekstiä ja pystyvät omaksumaan organisaation tai yksittäisen henkilön kirjoitustyylin. Kun viestit näyttävät ja tuntuvat oikeilta, uhrin erehtymisen todennäköisyys kasvaa. Samalla automaatio mahdollistaa nopean skaalaamisen: viestejä voidaan kohdentaa suurille joukoille, muokata eri kielille ja sovittaa kontekstiin.

Tämä laskee rikoksen tekemisen kynnystä ja kasvattaa yritysten, julkisen sektorin ja yksityishenkilöiden altistusta. Sama mekanismi tukee myös disinformaation ja propagandan levittämistä. Tekoälyllä voidaan tuottaa suuria määriä toisiaan vahvistavaa sisältöä, ylläpitää haluttua kertomusta monikanavaisesti ja hämärtää rajanvetoa luotettavan ja epäluotettavan tiedon välillä. Yleisölle välittyy sujuvaa, tyylillisesti uskottavaa tekstiä, jonka alkuperä ja tarkoitus jäävät helposti piiloon.

Teknisessä mielessä kielimallit eivät ole itsessään haittaohjelmatehtaita, mutta niiden kyky selittää perusmekanismeja ja jäsentää ongelmia madaltaa aloittelijoiden kynnystä. Mallit voivat auttaa hahmottamaan rakenteita, jotka liittyvät esimerkiksi verkkoympäristön heikkouksiin, ja tuottaa yksinkertaisia komponentteja, joiden varaan osaava tekijä voi rakentaa lisää.

Turvaominaisuudet pyrkivät estämään suoran avun antamisen haitallisiin tarkoituksiin, mutta järjestelmien toiminta perustuu edelleen kielelliseen tulkintaan, joka on altis harhauttamiselle. Tyyliä mukaileva teksti ja synteettinen media - teksti, ääni, kuva ja video - mahdollistavat lisäksi henkilö- ja ryhmäimitoinnin. Kun viesti kuulostaa ”oikealta” ihmiseltä tai viranomaiselta, luottamuksen väärinkäyttö helpottuu.

Riskit kasvavat erityisesti mittakaavan, nopeuden ja tyylinmukautuvuuden vuoksi. Automaatio tekee kohdentamisesta halpaa ja nopeaa, ja kun syvää tek-

Kuva: Pixabay

Kuva: Παύλος, Pixabay

VARJOPUOLET

nistä osaamista ei aina tarvita, potentiaalisten tekijöiden määrä kasvaa. Turvasuojien rajallisuus korostaa tarvetta yhdistää tekniset kontrollit, prosessit ja ihmisten osaaminen. Tällä hetkellä ei ole olemassa yleiskäyttöistä ja varmaa työkalua, joka kykenisi luotettavasti toteamaan, onko teksti ihmisen vai tekoälyn tuottamaa. Siksi pelkkiin teknisiin tunnistusratkaisuihin nojaaminen on riittämätöntä.

Organisaatioiden näkökulmasta keskeistä on nostaa tietoisuutta ja osaamista. Henkilöstölle on annettava valmiudet tunnistaa epätyypilliset pyynnöt, tyylivirheet tai kontekstista poikkeavat viestit ja käyttää kaksoisvarmistuksia esimerkiksi maksujen hyväksymisessä tai tunnustietojen luovuttamisessa.

Tietoisuuden rinnalla on rakennettava selkeä hallintamalli tekoälyn käytölle: määriteltävä hyväksyttävät käyttötarkoitukset, roolit ja vastuut sekä pidettävä kirjaa siitä, missä ja miten tekoälyä hyödynnetään. Kolmansien osapuolten hallinta on olennaista, sillä mallipalvelut ja integraatiot ovat usein ulkoisia: sopimusehtoihin on sisällytettävä päivityskäytännöt, lokitus ja tietoturvavaatimukset. Jatkuvuudenhallinnan näkökulmasta tarvitaan harjoituksia, toimivia varasuunnitelmia ja selkeä viestintäketju poikkeustilanteiden varalle.

Tekniset suojaukset täydentävät kokonaisuutta. Sähköposti- ja verkkosuodatus, monivaiheinen tunnistautuminen ja vähiten oikeuksien periaate ehkäisevät vahinkojen syntymistä ja leviämistä. Lokitus ja poikkeamien havainnointi auttavat havaitsemaan epätavalliset viestintäkuviot, massalähdöt tai oikeuksien äkilliset muutokset. Tietojen luokittelu, salaus ja vuodonestojärjestelmät tukevat kriittisen tiedon suojaa, ja sisältöjen alkuperämerkintöihin perustuvat ratkaisut voivat tulevaisuudessa helpottaa luottamuksen rakentamista digitaalisissa ympäristöissä. Kokonaisuutta on jatkuvasti päivitettävä, koska uhkakenttä kehittyy tekniikan mukana.

Lainvalvonnan on pysyttävä kehityksessä mukana. Tämä tarkoittaa sekä omien kyvykkyyksien vahvistamista että tiivistä yhteistyötä teknologiayritysten, CERT-toimijoiden ja muiden viranomaisten kanssa. Tekoäly voi tukea analytiikkaa ja tutkintaa laillisuuden ja perusoikeuksien rajoissa, mutta yhtä tärkeää on yhteinen kieli uhkailmiöiden kuvaamiseen ja tiedonvaihdon nopeuttamiseen. Kun havaintoja voidaan jakaa rakenteisesti ja nopeasti, väärinkäytösten elinkaari lyhenee.

Kokonaisuutena tekoäly ei ole itsessään hyvä tai paha, vaan voimakas väline, jonka vaikutus riippuu käyttöyhteydestä, kannustimista ja valvonnasta. Väärinkäytösten kirjo on vasta hahmottumassa, ja menetelmät monimutkaistuvat tekniikan kehittyessä. Siksi vastauksen on oltava kokonaisvaltainen: ihmisten osaaminen, selkeät prosessit, tarkoituksenmukaiset tekniset kontrollit ja kehittyvä sääntely on kytkettävä toisiinsa. Kun kyvykkyydet, kannusteet ja vastuut ovat linjassa, tekoälyn hyötyjä voidaan kasvattaa ja riskit pitää hallittavina - myös silloin, kun rikollinen toiminta pyrkii hyödyntämään samoja teknologioita.

STRIDE tuo systemaattisuutta uhkamallinnukseen ja riskienhallintaan

Teksti: Jyri Paasonen

Modernien digitaalisten palveluiden kehittämisessä tietoturva on oltava mukana alusta asti - ei vasta sitten, kun järjestelmä on jo käytössä ja ensimmäiset haavoittuvuudet ilmenevät. STRIDE on yksi tunnetuimmista uhkamallinnusmenetelmistä, joka tarjoaa systemaattisen tavan tunnistaa ja analysoida erilaisia uhkia järjestelmän eri osissa.

Menetelmä on kehitetty Microsoftin toimesta, ja sen nimi muodostuu kuudesta keskeisestä uhkakategoriasta: Spoofing (identiteetin väärentäminen), Tampering (tietojen manipulointi), Repudiation (kiistettävyys), Information Disclosure (tietovuoto), Denial of Service (palvelunestohyökkäys) ja Elevation of Privilege (oikeuksien laajentaminen).

STRIDE ei ole pelkkä lista mahdollisista hyökkäyksistä, vaan käytännön työkalu, jota voidaan käyttää esimerkiksi ohjelmistokehityksen yhteydessä, kun suunnitellaan järjestelmäarkkitehtuuria ja halutaan ymmärtää, missä kohdin suojausratkaisuja tarvitaan. Menetelmä toimii erityisen hyvin, kun käytössä on järjestelmästä visuaalinen esitys, kuten data flow -kaavio. Tällöin voidaan tarkastella järjestelmän jokaista komponenttia - palvelimia, käyttäjiä, tietovirtoja ja rajapintoja - ja arvioida niitä yksitellen STRIDE-kategorioiden kautta.

Otetaan esimerkiksi yksinkertainen verkkopalvelu, jossa käyttäjät voivat kirjautua sisään, tallentaa tietoja ja jakaa niitä muille. Spoofing-uhka syntyy, jos hyökkääjä pystyy esiintymään toisena käyttäjänä. Tämän torjumiseksi tarvitaan vahva tunnistautuminen, kuten kaksivaiheinen kirjautuminen. Tampering-uhka tarkoittaa, että asiakirjoja tai muuta tietoa voidaan muuttaa luvattomasti, ja se voidaan estää käyttämällä salattua tiedonsiirtoa sekä digitaalista allekirjoitusta.

Repudiation liittyy tilanteisiin, joissa käyttäjä voi kiistää toimineensa tietyllä tavalla. Tämän estämiseksi on tärkeää lokittaa toiminnot ja säilyttää lokeja turvallisesti. Information Disclosure tarkoittaa sitä, että asiattomat saavat pääsyn luottamuksellisiin tietoihin. Sitä voidaan ehkäistä tiedon salauksella ja käyttöoikeuksien huolellisella hallinnalla.

Denial of Service -uhat uhkaavat palvelun saatavuutta, ja niitä vastaan voidaan suojautua muun muassa liikenteen rajoituksilla, kuormantasaajilla ja palvelun jatkuvalla valvonnalla. Elevation of Privilege taas tarkoittaa, että hyökkääjä saa korkeammat käyttöoikeudet kuin kuuluisi, ja sitä voidaan ehkäistä esimerkiksi käyttöoikeuksien tiukalla valvonnalla ja roolipohjaisella käyttöoikeusmal-

	UHKA	RIKOTTUOMAISUUS	UHAN MÄÄRITELMÄ
S	Spoofing (Indentiteetin väärentäminen)	Todennus (Autentikointi)	Esittäytyminen joksikin tai joksikin muuksi kuin itse on.
T	Tampering (Tietojen manipulointi)	Eheys	Järjestelmän, verkon tai tallennusmedian tietojen luvaton muuttaminen.
R	Repudiation (Kiistettävyys)	Kiistämättömyys	Toiminnan kieltäminen tai vastuusta irtisanoutuminen.
I	Information Disclosure (Tietovuoto)	Luottamuksellisuus	Tiedon paljastaminen henkilölle, jolla ei ole oikeutta päästä siihen käsiksi.
D	Denial of Service (Palvelunestohyökkäys)	Saatavuus	Palvelun vaatimat resurssit käytetään, jolloin se ei ole käytettävissä.
E	Elevation of Priviledge (Oikeuksien laajentaminen)	Valtuutus (Autorisointi)	Henkilö saa oikeuksia, joita hänelle ei ole tarkoitettu.

lilla.

STRIDE tuo selkeyttä ja ennakoitavuutta tietoturvan suunnitteluun. Sen avulla uhkia ei tarvitse arvailla tai käsitellä jälkikäteen, vaan niitä voidaan käsitellä järjestelmällisesti osana kehitysprosessia. Samalla se parantaa yhteistyötä kehittäjien, tietoturva-asiantuntijoiden ja muiden sidosryhmien välillä, kun kaikilla on yhteinen viitekehys uhkien tunnistamiseen ja niiden hallintaan.

Tietoturva ei ole yksittäinen ominaisuus tai lisämoduuli, vaan se on osa järjestelmän rakennetta ja toiminnallisuutta. STRIDE auttaa varmistamaan, että tämä rakenne on vahva ja kestää nykyaikaiset kyberturvahaasteet.

STRIDE-mallia voidaan lisäksi hyödyntää erinomaisena pohjana sekä riskien arvioinnissa että tietosuojan vaikutustenarvioinnissa. Vaikka STRIDE on alun perin kehitetty teknisten tietoturvauhkien tunnistamiseen, sen systemaattinen lähestymistapa toimii hyvin myös laajemmassa kontekstissa, kuten tietosuojavaatimusten täyttämisessä ja riskienhallinnan tukena.

Riskien arviointi edellyttää, että tunnistetaan mahdolliset uhat, arvioidaan niiden todennäköisyys ja vaikutus sekä määritellään hallintakeinot. STRIDE tarjoaa valmiin rakenteen uhkien kategorisointiin ja toimii samalla uhkakirjastona, joka helpottaa riskiarvion kattavuutta ja loogisuutta. Jokainen STRIDE-kategoria voidaan yhdistää konkreettisiin uhkaskenaarioihin ja liittää niihin tekniset ja hallinnolliset torjuntakeinot.

Tietosuojan vaikutustenarvioinnissa STRIDE auttaa erityisesti teknisten riskien tunnistamisessa, jotka voivat johtaa tietosuojaloukkauksiin. Spoofing voi johtaa henkilötietojen paljastumiseen väärälle taholle, Information Disclosure suoraan tietovuotoon, Tampering tietojen virheellisyyteen ja Repudiation vastuullisuuden puutteeseen. Myös Denial of Service ja Elevation of Privilege voivat estää rekisteröidyn oikeuksien toteutumisen. Tämän vuoksi STRIDE tukee olennaisesti tietosuojan vaatimuksia ja auttaa osoittamaan, että riskit on tunnistettu ja niihin on varauduttu.

Yhteenvetona voidaan todeta, että STRIDE ei yksin kata kaikkia tietosuojan tai liiketoimintariskien osa-alueita, mutta se on erinomainen tekninen työkalu riskien systemaattiseen tunnistamiseen ja torjuntakeinojen suunnitteluun. Se toimii käytännössä sillanrakentajana tietoturvan, riskienhallinnan ja tietosuojan välillä.

Kuva: ThisIsEngineering, Pexels

Organizational Testing Leadership
27.8.-14.11.2025, Helsinki

In this tutorial, we explain the fundamentals of test leadership and have practical exercises to understand it. We discuss what leadership means in different scenarios, where effective test leadership is needed, and where leadership is all too often missing.

ISTQB Sertifioitu testaaja - Perustaso
13.-15.10.2025, Helsinki
8.-10.12.2025, Helsinki

Koulutuksessa opit ohjelmistotestauksen suomenkielisen perusterminologian ja saat valmiudet käyttää eri testaustekniikoita käytännön testausprojekteissa. Kurssin avulla hallitset testausprosessin, standardit sekä käytössä olevien työkalujen perusasiat.

Koulutus valmistaa sinua suorittamaan vuoden 2018 syllabuksen mukaisen ISTQB Foundation -sertifikaatin, joka on osoitus henkilökohtaisesta testausosaamisestasi.

BBST® Foundations
26.10.2025, Helsinki

The Black-Box Software Testing Foundations course is one of the most eye-opening and in-depth online course on the fundamental concepts in software testing and its critical challenges.

The course includes video lectures, quizzes, homework of various kinds, and a final exam. All of the homework, and the exam, are reviewed by instructors, and individual or class-wide feedback is provided.

Testing Assembly 2025 Tutorial
21.11.2025, Helsinki

Holistic Testing: Strategies for Agile Teams. This is a workshop for testing & QA professionals. Tutorial is facilitated by Alexandra Schladebeck.

tivia.fi/tapahtumat

GreenICT kiertue 2025
- Ratkaisuja kestävään tulevaisuuteen

Green ICT -tapahtumat keräävät yhteen alueen kiinnostavimmat yritykset ja toimijat, jotka haluavat olla mukana toteuttamassa ICT -alan vihreää siirtymää. Kiertueen tapahtumat ovat osa kansallisesti toteutettava Green ICT VISIIRI -hanketta.

Green ICT VISIIRI -hanke kasvattaa tietoisuutta ICT-alan vihreästä siirtymästä sekä auttaa löytämään ratkaisuja kohti kestävämpää tulevaisuutta.

Tapahtumasta jää käteen kattava ymmärrys Green ICT:n nykytilasta ja tavoitteista sekä konkreettisia työkaluja vihreän siirtymän toteuttamiseen. Päivän aikana syntyy myös arvokas verkosto samanhenkisten yritysten edustajista, jotka jakavat yhteisen vision kestävästä tulevaisuudesta. Lisäksi päivä tarjoaa mahdollisuuden viettää aikaa rennossa ilmapiirissä ICT-alan huippuosaajien seurassa.

Tulevat tapahtumapäivämäärät:

7.10.2025	Joensuu	30.10.2025	Jyväskylä
8.10.2025	Mikkeli	4.11.2025	Helsinki
7.10.2025	Vaasa	18.11.2025	Lappeenranta
29.10.2025	Tampere		

Kaikki tapahtumat ovat osallistujille maksuttomia.
https://tivia.fi/green-ict-kiertue-2025