Riikliku küberturvalisuse uudiskiri

2023-01

Majandus- ja kommunikatsiooniministeerium

Küberturvalisuse valdkonna õigusloomest

Andmekaitse Inspektsioon

Andmekaitsepäeva veebiseminar "Töötaja privaatsus värbamisest uute väljakutseteni"

Eesti infotehnoloogia ja Telekommunikatsiooni Liit

ITLis allkirjastati turvalise tarkvara arendamise manifest

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Majandus- ja Kommunikatsiooniministeerium

Küberturvalisuse valdkonna õigusloomest 3

MKM kutsub tasuta kursusele omandama tarkvaraarendaja oskuseid 4

Riigi Infosüsteemi Amet

CyberWeek @LAC4 2022 5

Detsembrikuu ülevaade olukorrast küberruumis 5

EU CyberNet'i missioonid ja kogukond aastal 2022 5

CCB Mapping

Andmekaitse Inspektsioon 5

Andmekaitsepäeva veebiseminar "Töötaja privaatsus värbamisest uute väljakutseteni" 5

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit

ITLis allkirjastati turvalise tarkvara arendamise manifest 6

TalTech

Université Bretagne Sud'iga koostöö raames toimub esimene talvekool 7

Algas KüberTalendi ettevõtlusprogramm 7

Cybernetica

Cybernetica viis lõpule CyberSec4Europe uurimisprojekti 8

Cybernetica lõpetab uurimisprojekti DANCE 8

Cybernetica lõpetab SPoF2.3 uurimisprojekti 8

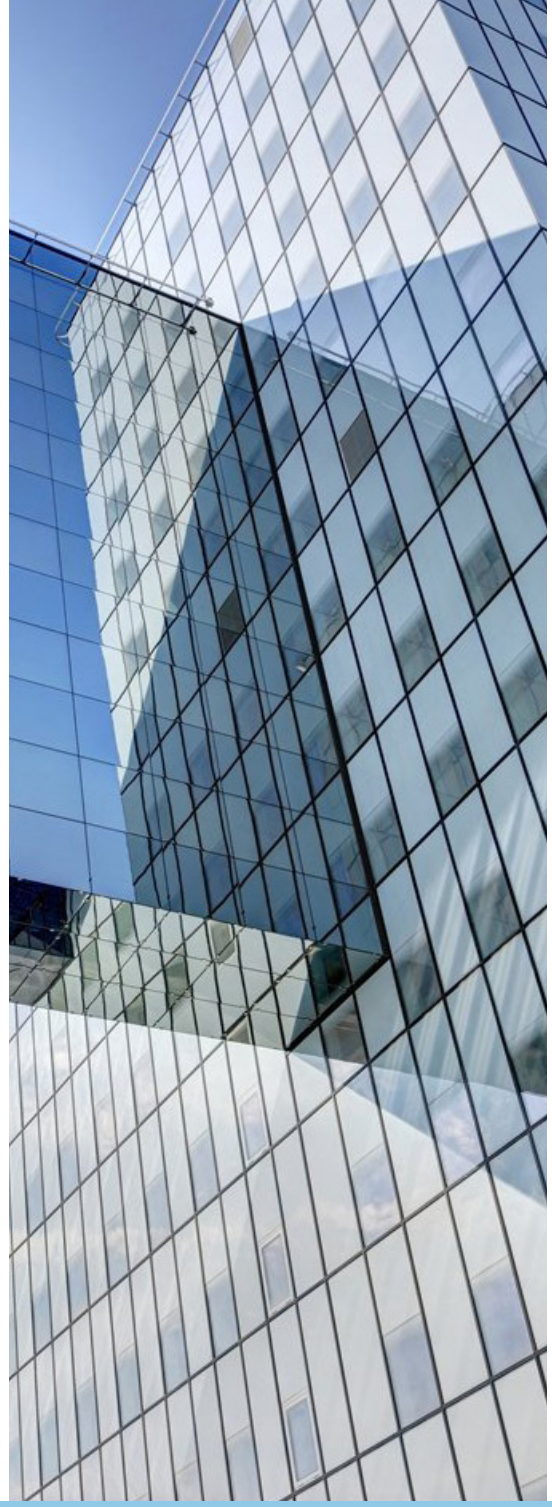
CybExer

CybExer Technologies laiendab küberharjutusväljaku kui teenuse pakkumist 9

European Telecommunications Standards Institute

Cybersecurity Standardization Conference 9

ETSI/IQC Quantum Safe Cryptography Event 9



Uudiskirjaga liitumiseks saada soov **carolyn.mets@mkm.ee**

Küberturvalisuse valdkonna õigusloomest

Möödunud aastal jõudsid lõpuni ja kehtestamisele mitmed erinevad õigusaktid nii riigisiseselt kui ka Euroopa Liidu tasandilt, mis hakkavad edaspidiselt mõjutama küberturvalisuse seaduse tähenduses teenuse osutajaid. Siinses artiklis anname ülevaate neist osadest.

Augustis jõustus küberturvalisuse seaduse ja teiste seaduste muutmise seadus, mille tulemusena tunnistati kehtetuks avaliku teabe seaduses (AvTS) riigi infosüsteemide turvameetmete süsteemi ehk ISKE määruse volitusnorm ning loodi uus volitusnorm Eesti Infoturbestandardiga (E-ITS) seotud määruste kehtestamiseks. Tolle eelnõuga tehti ka täiendusi küberturvalisuse seaduses (KüTS) seoses kahe Euroopa Liidu ja nõukogu määrustega (nr 2021/887 ning nr 2019/881). Määruse nr 2021/887 tõttu sätestati KüTS-is, et Riigi Infosüsteemi Amet hakkab täitma riikliku koordineerimiskeskuse ülesandeid, mis on seotud Eesti küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute teemadega. Määruse nr 2019/881 tõttu määrati Tarbijakaitse ja Tehnilise Järelevalve Amet (TTJA) riiklikuks küberturvalisuse sertifitseerimise asutuseks, sh kehtestati selle valdkonnaga seotud järelevalve ja väärteokoosseisud ning seotud menetluslikud sätted. Sama õigusaktiga tehti seadustes muudatusi seoses Eesti Rahvusringhäälinguga, mis jõustuvad 2027. aasta 1. jaanuaril. Riigikogus toimunud menetluse käigus lisati samasse eelnõusse ka infoühiskonna teenuse seaduse muudatus, millega TTJA sai õiguse piirata infoühiskonna teenust, kui infoühiskonna teenuse kaudu üldsusele levitatud teabega kihutatakse vihkamisele, vägivallale või diskrimineerimisele kodakondsuse, etnilise päritolu, keele, usutunnistuse või muude Eesti Vabariigi põhiseaduse §-s 12 nimetatud asjaolude tõttu, õhutatakse sõda või õigustatakse sõjakuritegusid ning kui see on vajalik riigi julgeoleku tagamiseks ja sellise teabe levitamise lõpetamiseks ning ohu tõrjumiseks puuduvad muud tõhusad võimalused.

E-ITS'iga seotud määrused (nii Vabariigi Valitsuse kui ka ettevõtlus- ja infotehnoloogiaministri määrused) jõustusid detsembris, mille tulemusena on määrusena kehtestatud E-ITS'i järgimise kohustus. E-ITS asendab edaspidiselt ISKE-t, kuid KüTS-i teenuse osutajad võivad E-ITS'i asemel rakendada ka rahvusvahelist standardit ISO/IEC 27001. Ministri määrusega kehtestati E-ITS'i 2022 versioon ning edaspidiselt hakatakse E-ITS'i igal aastal täiendama, kaasates E-ITS'i rakendajaid kui ka muid huvitatud osapooli. Kui E-ITS'i tekstile soovitakse anda tagasisidet ja sisendit, siis RIA ootab seda aadressile standard@ria.ee. Mainitud Vabariigi Valitsuse määruses säilitati ISKE määrusest AvTS-i tähenduses andmekogudele mõeldud erinõuded, mis on seotud andmete turvaklassi KTS määramisega. Lisaks sellele määratleti avalike ülesannete täitmist oluliselt mõjutavate võrgu- ja infosüsteemide nimekiri ja nõuded nende varundamiseks välisriigis asuvasse turvalisse andmekeskusesse. Samast määrusest jäi välja avalikul kooskõlastusringil olnud eelnõu versioonis olevad sätted pilveteenuste kasutamise kohta, mis kehtinuks ainult avalikule sektorile (vt KüTS § 3 lõiget 4). Tegeleme nn pilvemääruse sätetega edasi 2023. aastal, et need viia täiendustena ka samasse Vabariigi Valitsuse määrusesse.

Detsembri viimastel päevadel avaldati Euroopa Liidu Teatajas Euroopa Parlamendi ja nõukogu õigusaktid, mis tuleb ka Eesti õigusesse üle võtta. Nendeks on küberturvalisuse 2. direktiiv ehk NIS2 direktiiv, finantssektori digitaalse tegevuskerksusega seotud direktiiv (DORA) ja määrus ning elutähtsa teenuse osutajate toimepidevusega seotud direktiiv ehk CER direktiiv. Kõik mainitud õigusaktid jõustuvad 16. jaanuaril 2023. a. See omakorda tähendab, et peatselt hakkavad pihta tegevused eelmainitud direktiivide üle võtmiseks. NIS2 direktiiviga seonduvalt on kavas teha eraldi küberturvalisuse valdkonna revisjon, mis toimub koostöös huvitatud osapoolte, kehtiva KüTS-i teenuse osutajate kui ka NIS2-ga lisanduvate sektorite esindajatega. NIS2 direktiivi siseriiklikusse õigusesse ülevõtmise tähtaeg on 21 kuud ehk hiljemalt 17. oktoober 2024. a.

Ülevaate koostajad:

Raavo Palu, MKM

Silver Lusti, RIA

Majandus- ja Kommunikatsiooni-ministeerium

MKM kutsub tasuta kursusele omandama tarkvaraarendaja oskuseid

Majandus- ja Kommunikatsiooniministeerium ootab kandideerima programmi, mis annab tervikpildi tarkvaraarenduse protsessist ning elutsüklist.

Majandus- ja Kommunikatsiooniministeeriumi IT oskuste valdkonna juht Karl-Andreas Sprenk tõi välja, et nõudlus IT spetsialistide ning arendajate järele on hüppeliselt kasvanud pea kõigis majandussektorites. Sellele on täiendavat hoogu andnud COVID-19 pandeemia ja vajadus toetada majanduse digitaliseerimist. "Spetsialistide puudujäägi leevendamiseks oleme käivitanud programmi, mille raames koolitame 100 juunior back-end tarkvaraarendajat, keda nii era- kui ka avalik sektor pikisilmi tööturule ootab," ütles Sprenk.

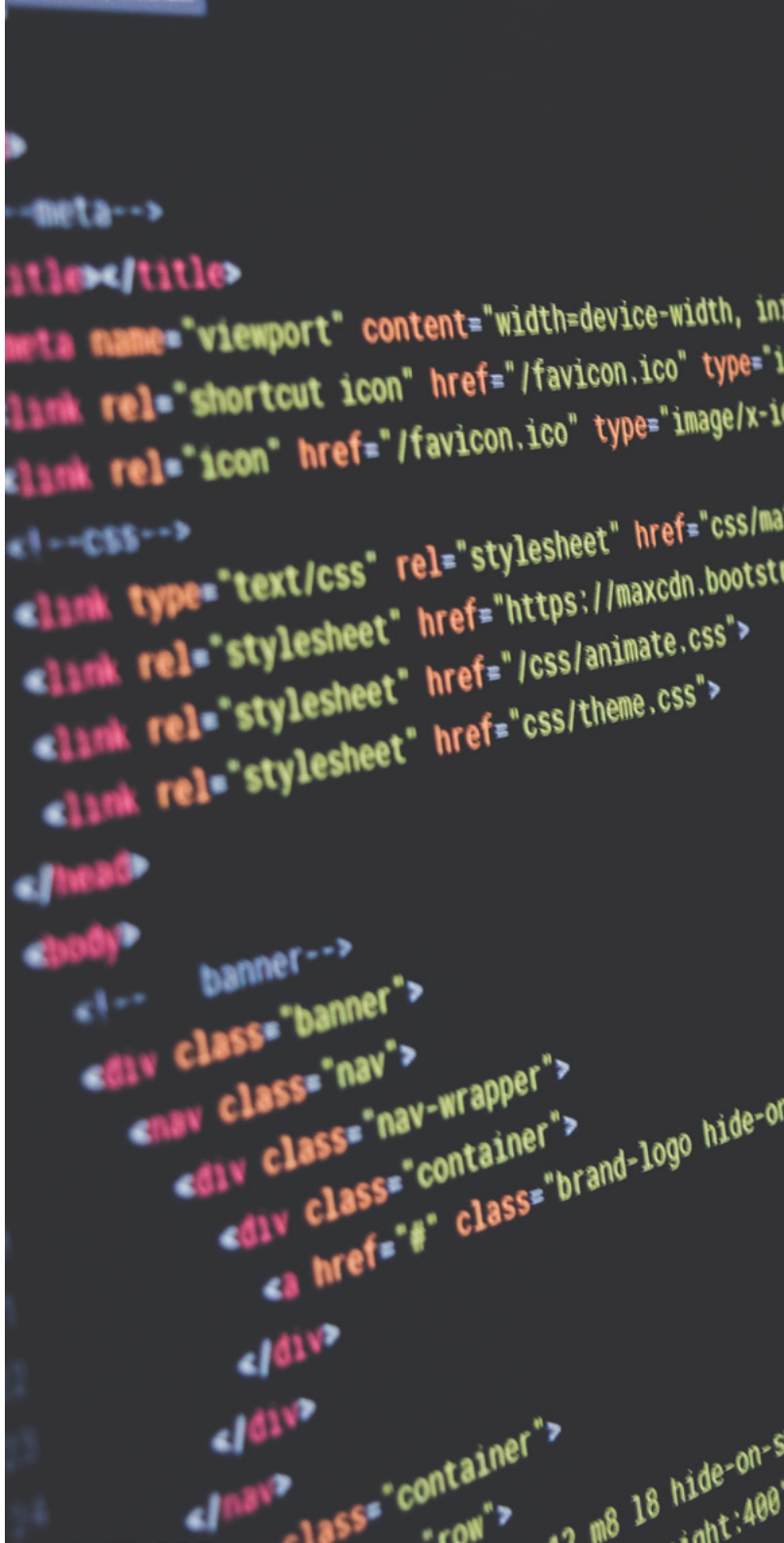
27. märtsil algav kursus on mõeldud töötavale täiskasvanule, kes kaalub karjääripöörde tegemist. See on täies mahus läbitav e-õppena ja ülesandeid on võimalik sooritada olenemata kellaajast ning asukohast. "Programm võimaldab paindlikult ühildada töö- ja eraelu. Ühtlasi toetab õppijat kogu perioodi vältel mentor, kes aitab lahendada tekkivaid küsimusi ja mõtleb kaasa karjääriplaneerimise protsessis," märkis Sprenk. Ta täpsustas, et 5 kuud kestev koolitusprogramm hõlmab iseseisvat õppimist, interaktiivseid loenguid, praktilisi harjutusi ja ülesandeid ning virtuaalseid kohtumisi lektorite ja mentoritega. Kokku läbitakse kaheksa e-õppe moodulit.

MKM koostööpartneri BCS Koolitus AS projektijuhi Maria Mang sõnas, et esimene pilootgrupp alustas möödunud aasta oktoobris ja kursusel osalejate õppeedukus on silmapaistev. "Kahtlemata on e-kursuse puhul peamine väljakutse päevase õppekoormuse reguleerimine, mis nõuab suurt sihikindlust. Oleme loonud keskkonnad, kus õppijad saavad aktiivselt oma väljakutseid ja edusamme teistega jagada ning seeläbi üksteisele toeks olla. Samuti on motivatsiooni säilitamisel määrava tähtsusega lektori oskuslik lähenemine, abi ja tugi õpiharjumuste kinnistamisel. Peagi avame veel kaks õppegruppi ja kui tunnete, et olete sobiv kandidaat, on viimane aeg kandideerida. Kandideerimise protsess võtab veidi aega, kuid annab parema võimaluse olla kindel oma sobivuses tarkvaraarendajaks," ütles Mang.

Programmi on oodatud kandideerima kõik vähemalt 21-aastased, kes omavad keskharidust, kehtivat töösuhet ja kellel puudub varasem IT valdkonna tasemeharidus. "IT sektor pakub ohtralt põnevaid väljakutseid. Meie kursusega liitumine on suurepärane võimalus astuda esimesed sammud selles maailmas ja hakata rajama uut karjääriteed," ütles Sprenk.

Täiendav teave programmi kohta ja ankeet registreerimiseks on leitavad siit.

Programmi toetatakse Euroopa Liidu struktuuritoetuse toetusskeemist „Digitaalse kirjaoskuse suurendamine", mida rahastab Euroopa Sotsiaalfond.



CyberWeek @LAC4 2022

LAC4 on EU CyberNeti loodud küberkompetentsi keskus Ladina-Ameerika ja Kariibi mere piirkonnas.

Novembrikuus toimus esmakordselt CyberWeek 2022, kus olid kohal 27 riigi esindajad. Nädala jooksul toimus 5 paralleelset üritust küberturvalisuse võimekuse kasvatamise teemadel.

1. GFCE LAC Regional Meeting 2022
2. FIRST-LAC4 Technical Colloquium
3. EU CyberNet LAC Regional Priorities Discussion
4. Communication — a Key Pillar in Solving Any (Cyber)crisis
5. Caribbean Regional Cybersecurity Exercise "CyberCrabs 2022"

Rohkem infot leiab siit.

Detsembrikuu ülevaade olukorrast küberruumis

CERT-EE regstreeris detsembris 233 mõjuga intsidenti, mis on viimase poole aasta keskmisest veidi madalam näitaja.

Detsembris jätkusid DDoS-ründed riigiasutuste ja ettevõtete pihta. Taas oli mitmeid teenusekatkestusi ning Eesti inimesi tabas erinevate õngitsuskirjade laine. Loe täpsemalt RIA detsembrikuu olukorrast küberruumis.

Loe edasi siit.

EU CyberNet'i missioonid ja kogukond aastal 2022

2022. aastal liitus EU CyberNeti ekspertide kogukonnaga 100 uut küberturvalisuse asjatundjat.

Nüüd on EU CyberNet'il kokku 275 eksperti üle Euroopa, kellel on väga erinevad oskused ja kogemused küberturvalisuse valdkonnast, et osaleda edukalt ülemaailmselt toimuvatel missioonidel.

Ülevaate erinevatest missioonidest, mille EU CyberNet 2022. aasta jooksul ellu viis, leiab siit.

CCB Mapping

Möödunud aasta lõpuks koostas EU CyberNet kaardistuse Euroopa Liidu rahastatud välistest kübervõimekuse projektidest.

Kaardistuse eesmärk on anda üksikasjalik ülevaade sellest, millised projektid ja millistes piirkondades väliskoostöö suunal aset leiavad. Kaardistusele leiab ligipääsu siit.

Andmekaitsepäeva veebiseminar "Töötaja privaatsus värbamisest uute väljakutseteni"

28. jaanuaril tähistatakse üle maailma andmekaitsepäeva. Rahvusvaheline andmekaitsepäev on pühendatud andmekaitsealaste õiguste tutvustamisele ja andmetöötlusega seotud riskide teadvustamisele.

Andmekaitse Inspektsioon korraldab sel puhul kolmapäeval, 25. jaanuaril kell 11.00-14.00 teabepäeva, mida saab jälgida otseülekandena inspektsiooni kodulehel, YouTube'i kanalis või Facebooki lehel.

Teabepäeval võtakse sedapuhku fookusesse andmekaitse töösuhetes. Räägitakse töötaja privaatsusest kogu töösuhte elukaare vältel alates värbamisprotsessist kuni töölt lahkumiseni. Korratakse üle põhimõtted, mida pidada silmas kandidaatide andmete kogumisel.

Veebiseminari on oodatud vaatama kõik huvilised. Põnevat infot ja uusi teadmisi saavad kindlasti nii töötajad kui tööandjad, personalijuhid, värbajad ja ka andmespetsialistid. Osalemine on kõigile tasuta.

Lisainfo Andmekaitse kodulehel.

EESTI INFOTEHNOLOOGIA JA TELEKOMMUNIKATSIOONI LIIT

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit

ITLis allkirjastati turvalise tarkvara arendamise manifest

Ajal, mil digitaliseerimine on saanud normiks pea kõigis valdkondades, on vaja tõsiselt tähelepanu pöörata ka digiruumi turvalisusele.

Eesti IT-ettevõtete liidu ITL-i liikmeks olevad arendusettevõtted soovivad võtta suurema rolli ja vastutuse nende poolt loodava tarkvara turvalisel arendamisel ning on allkirjastanud manifesti ehk turvalise tarkvara arendamise hea tava.

ITL-i president Juhan-Madis Pukk rõhutab, et ühiseid väärtusi jagavate ettevõtete algatus annab positiivse tõuke küberturvalisuse teema olulisuse esiletõstmiseks ühiskonnas ning toob kasu ka kogu sektorile. „Kui näiteks arhitekt asub ehitajaga koostöös hoonet planeerima, siis ei huvita ehitajat see, millise tarkvara abil arhitekt oma tööd teeb — jäägu erialaspetsiifika spetsialistide jaoks. Aga oluline on, et nii eraettevõtetes kui ka avalikus sektoris oleks normiks turvaliselt töötav tarkvara. ITL-i hea tavaga liitunud ettevõtte töötajad ning nende kliendid saavad kinnituse, et organisatsiooni jaoks on turvalisusse investeerimine oluline ning kasutusel on parimad praktikad loodavate lahenduste turvalisuse tagamiseks."

Ühisalgatuse taga on paljud suurettevõtted, kes näevad praegu digitaliseerimise järsku kasvu.

Liidus oli üheks hea tava initsiaatoriks ITL-i juhatuse liige ja Nortal AS tegevjuht Ats Albre. "Oleme huvitatud, et Eestis loodud tarkvara oleks turvalisuse mõõdupuu kogu maailmas. Manifestiga liitumise otsus nõuab liitujalt kriitilist hinnangut enda tegelikule võimekusele, sest vastutuse võtame nii enda kui oma klientide ees. Meie jaoks on liitumine kvaliteedimärk ja lubadus oma klientidele, et tarkvaraarenduse turvalisuse tagamine on tõesti juhitud, integreeritud, arenev ja vastutustundlik."

"Ainult analüütikud, arhitektid ja programmeerijad ei saa turvalist tarkvara arendada — turvakaalutlused peavad olema ka ettevõtte omaniku prioriteedid," sõnas Cybernetica arendusjuht Arne Ansper.

Sama oluline kui IT-ettevõtte lubadus olla turvalisi tarkvaralahendusi pakkuv partner, on klientide ehk teenuse ostjate teadlikkus ja oskus turvalist tarkvara tellida.

ITL-i hea tavaga turvalise tarkvara arendamisel on liitunud hetkel 23 arendusettevõtet-organisatsiooni.

IT-ettevõtjad kutsuvadki üles kõiki tarkvara arendusettevõtteid head tava järgima: ettevõtjad-tellijad, võiksid osata küsida turvalist tarkvara arendust ning kindlustama oma tagala, et tulevikus ei oleks nende ärikriitilised protsessid haavatavad; hankijad, võiksid lisada hanketingimustesse turvalise tarkvara arendamise hea tava järgimise nõude.

Hea tava ning sellega liitunud ettevõtted ITL koduleheküljel.

TalTech

Université Bretagne Sud'iga koostöö raames toimub esimene talvekool

9. - 20. jaanuaril viibivad TalTechis 23 küberkaitse magistritudengit Prantsusmaalt.

CYBERUS Erasmus Mundus on kaheaastane ühine magistriprogramm, kus tudengid võtavad kursuseid kolmest ülikoolist Université Bretagne Sud (Prantsusmaa), Université Libre de Belgique (Belgia) ja Université du Luxembourg (Luksemburg) ning osalevad esimese semestri lõpus TalTechi poolt korraldatavas talvekoolis teemal „The Cyberlandscape: Cyberthreats and Cyberactors". Kursusel uuritakse küberruumi rolli riiklike ja valitsusväliste osalejate tegevusvaldkonnana.

Programmi on koostanud Dr Adrian Venables küberkriminalistika ja küberjulgeoleku keskusest kaasates loenguid andma teadlasi ja eksperte nii keskusest kui ka TalTechist laiemalt. Samuti külastavad talvekooli osalejad mitmeid Eesti küberkaitse organisatsioone ja ettevõtteid ning kohtuvad kohalike üliõpilastega.

Lähemalt on programmi ning TalTechi osaluse kohta võimalik lugeda siit.

Algas KüberTalendi ettevõtlusprogramm

12.01.2023 kogunesid 40 noort (15-30 aastast) küberturvalisuse huvilist, et õppida looma üheskoos erinevaid põgenemistube.

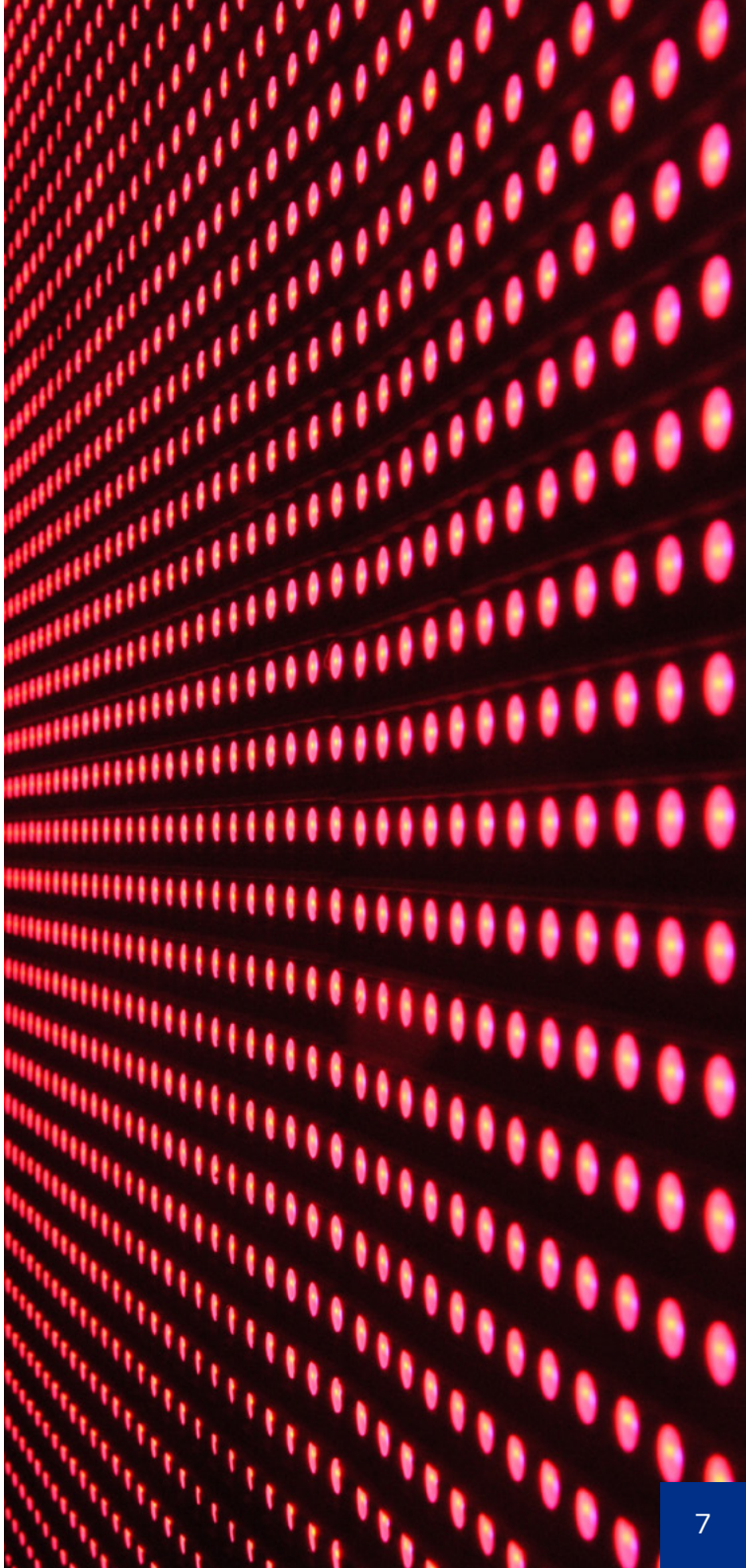
Põgenemistoa teenus on reaalajas või digikanali toel toimuv mänguline koolitus, milles tuleb lahendada nutikaid ülesandeid, leida ülesannetele lahendusi või saladustele vastused.

Programmi jooksul toimub vähemalt neli koolitust (teemadel: teaduslik mõtteviis, ettevõtlus, küberturvalisus, teenusedisain, kohtumised ettevõtjatega).

Stipendiumi eesmärgiks on toetada ja tunnustada kübertalente ja suunata neid omandama pädevusi teadusliku mõtteviisi, küberturvalisuse ja ettevõtluse valdkonnas; propageerida ja soodustada Eesti noori ja ka laiemat üldsust looma küberturvalisuse teadlikkust tõstvaid ja tehnilisi oskuseid arendavaid tegevusi, mida on noortel võimalik hiljem enda loodud ettevõtetel toodete või teenusena turundada.

Lõpuüritusel märtsis jagatakse välja stipendiumid kolmele parimale Põgenemistoa ideekavale 800 EUR, mille otsustab zürii. Stipendiumi toetaja 2022-2023 aastal on Startup Estonia, EAS ja Kredex. Kaasatud ettevõtjad on RangeForce, CTF Tech, CyberWiseSpace, Helmes ja Vespia. Tegevus on toetatud Startup Estonia tegevusest "CyberTech ökosüsteemi arendavad tegevused" ja tegevusi viib ellu Tallinna Tehnikaülikool.

Loe lähemalt siit.



Cybernetica viis lõpule CyberSec4Europe uurimisprojekti

CyberSec4Europe on Bukarestis tekkinud Euroopa küberturvalisuse kompetentsikeskuse ja küberturvalisuse ekspertiisi võrgustiku uurimis- ja innovatsiooni pilootprojekt.

Projekti 43 partnerit 22 ELi liikmesriigist ja assotsieerunud riigist töötavad selle nimel, et ühtlustada teekonda tarkvarakomponentide väljatöötamisest, mis vastaksid lühi- ja pikaajaliste tegevuskavade alusel määratletud nõuetele. Need on seotud projekti tegelike näidiskasutusjuhtumitega, mis käsitlevad küberjulgeoleku väljakutseid digitaalse infrastruktuuri, rahanduse, hariduse, arukate linnade, tervishoiu ja meretranspordi sektorites. Töö tulemusena koostatakse rida soovitusi peamiste küberturvalisuse valdkondade ja kriitiliste tehnoloogia-/rakenduselementide kohta.

Projekti põhieesmärk oli katsetada Euroopa demokraatia ja digitaalse ühtse turu terviklikkuse tagamiseks ja säilitamiseks vajalike küberjulgeoleku võimete konsolideerimist ja tulevast kavandamist. CyberSec4Europe on muutnud selle laia eesmärgi mõõdetavateks ja konkreetseteks sammudeks: kolm poliitilist eesmärki, kolm tehnilist eesmärki ja kaks innovatsioonieesmärki.

Lisainfo siit.

Cybernetica lõpetab uurimisprojekti DANCE

Isikuandmete kaitse üldmäärus (GDPR) ei võimalda testida infosüsteeme isikuandmete põhjal. See takistab innovatsiooni ja uute andmepõhiste teenuste (sh tehisintellekti) arendamist.

Mitmed Euroopa andmekaitseasutused on märkinud, et sünteetilised andmed ei ole GDPR-i põhjenduse 26 tähenduses tuvastatavad ja neid saab kasutada IT-süsteemide testimiseks. Sünteetilised andmed peavad siiski olema originaaliga sarnased.

Uusi andmeid saab sünteesida olemasolevate andmete põhjal. Organisatsioonidel aga puudub pädevus ja nad on valmis seda teenust ostma. Selline süntees nõuab algandmete töötlemist. Selleks on vaja seaduslikku alust ja usaldust, mistõttu on raske allhanget hankida.

Antud projektis katsetati andmete sünteesi turvalise arvutustehnoloogia abil, mis kaitseb teenusepakkuja algandmeid nii, et süntees võib olla isegi pilveteenus, mis ei suuda lähteandmete väärtusi lekkida.

Lisainfo projekti kohta siit.

Cybernetica lõpetab SPoF2.3 uurimisprojekti

SPoF (Single Point of Failure) oli esialgne uuring, mis viidi läbi aastatel 2019-2020. See tõrketaluvuse analüüs osutas eID infrastruktuuri nõrkadele lülidele Eesti eID ökosüsteemis, mis võisid mõjutada paljusid kasutajaid. Peamine nõrkus oli Eestis kasutusel olevate erinevate autentimisprotokollide hulk.

Pärast selle leidmist viidi läbi kaks täiendavat uuringut. SPoF2.1 uuris Eestis kasutatavaid autentimistööriistu ja -teenuseid, et selgitada välja, kas nende API-sid oleks võimalik ühtlustada ning kuidas vältida *man-in-the-middle* rünnakuid. SPoF2.2 uuris, kuidas vähendada sõltuvust kehtivuskinnitusteenusest ja tagada funktsionaalsus olukorras, kus kehtivuskinnitusteenus ei tööta.

See viib meid SPoF2.3 juurde. Projekt koosnes kahest osast — analüüsist ja soovitusest. Esimeses osas koguti ja süstematiseeriti materjali sertifitseerimisasutustega seotud kriiside, usaldusahelate, usaldusnimekirjade kohta ning analüüsiti usaldusmudelite erinevusi nende tehnilistest ja juriidilistest aspektidest lähtuvalt. Teises osas töötati välja soovitused Eestile sobivaks eID usaldusmudeliks koos kõigi vajalike tehniliste kirjeldustega.

Lisainfo projekti kohta siit.

CybExer

CybExer Technologies laiendab küberharjutusväljaku kui teenuse pakkumist

Seoses kasvava nõudlusega laiendab CybExer Technologies küberharjutusväljaku kui teenuse (Software as a Service — SaaS) pakkumist.

Algselt pigem kaitse- ja julgeolekuklientide teenindamiseks välja töötatud küberharjutusväljaku järele on kiiresti tekkinud nõudlus erasektoris. Sellest tulenevalt on CybExer töötanud välja kolmeastmelise tellimuspõhise tarkvarapakkumise, mis on suunatud finantsasutuste, akadeemiliste organisatsioonide, hallatavate turvateenuste pakkujate (MSSP) ja küberturbetööstuse klientidele.

CybExeri tegevjuhi Andrus Kivisaare sõnul pakub see turule paindlikumat, ligipääsetavamat ja usaldusväärsemat lahendust. See tähendab väga kiiret juurutusaega, nõudmisel kureeritud sisu ja oma sisu loomise võimalust küberharjutusväljakule.

Tootejuht Tomi Helkearo lisab, et turul on nõudmine, et pääseda kiiresti ligi kogu tehnoloogiapaketile, võtmata seda tehes liigset finantsriski või tegemata selleks liigsuuri investeeringuid.

Pakkumine on suunatud ka nutikatele linnadele (Smart Cities) ja tehisintellektiuuringutele. „Cyber Range'i turg on kasvav turg. Näeme seda tüüpi teenuste järele suuremat vajadust erinevatel elualadel. SaaS-i pakkumine võimaldab nutikatel linnadel küberohtude vastu testida kriitilisi digitaalseid lahendusi, millele meie igapäevaelus üha enam tugineme, samas kui tehisintellekti uurimisrühmad vajavad oma algoritmide koolitamiseks stabiilseid, skaleeritavaid ja juurdepääsetavaid keskkondi," lisab Andrus Kivisaar.

Nii pakutakse klientidele, partneritele ja laiemale küberturvalisuse kogukonnale uusi võimalusi ettevõtete ja teenuste kübervastupidavuse standardite parandamiseks.

Loe täpsemalt siit.

Andrus Kivisaar, CybExeri tegevjuht

European Telecommunications Standards

Cybersecurity Standardization Conference

Konverents toimub 7. veebruar 2023 hübriid üritusena.

Selle tunnustatud konverentsi 2023. aasta programmis on spetsiaalsed istungid standardiseerimise kohta valdkondades, mis on seotud tekkivate ELi õigusaktidega:

- Küberkerksuse akt

- eIDAS määrus

- RED direktiiv, kavandatav EL kiibimäärus, andmemäärus, tehisintellekti määrus ja teised.

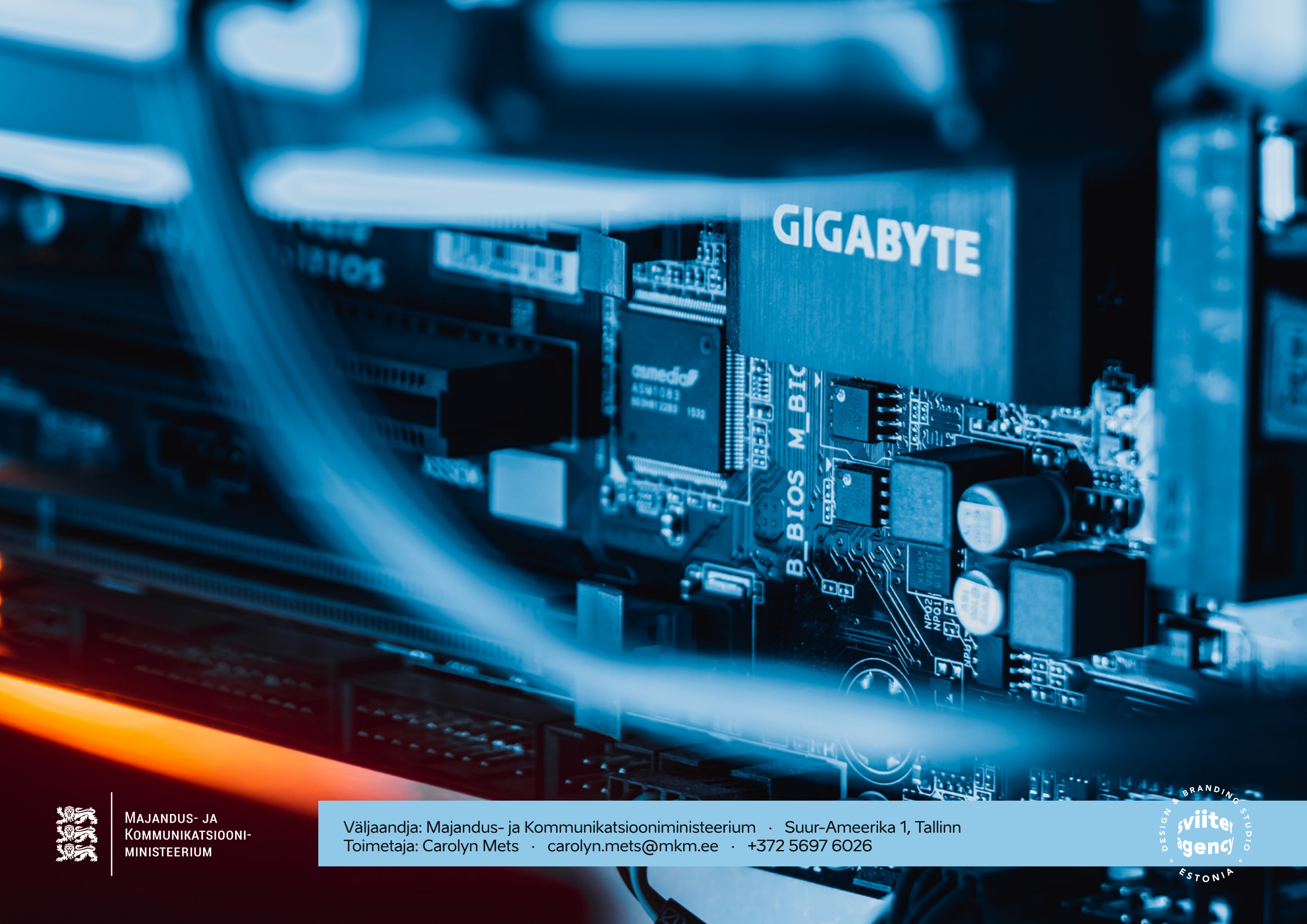
Lisainfo ja registreerimine siin.

ETSI/IQC Quantum Safe Cryptography Event

ETSI-l ja kvantarvutite instituudil on hea meel teatada 9. kvantturvalise krüptograafia üritusest, mis toimub 13.-15. veebruaril 2023 ETSI ruumides Lõuna-Prantsusmaal.

Üritus toob kokku kvantturvalise küberjulgeoleku kogukonna osalejad üle kogu maailma ning hõlbustab teadmiste vahetamist ja koostööd, mis on vajalik küberinfrastruktuuride ja äritavade üleminekuks ning nende turvaliseks muutmiseks kvantarvutite ajastul.

Lisainfo ja registreerimine siin.



Majandus- ja Kommunikatsiooni-
ministeerium

Väljaandja: Majandus- ja Kommunikatsiooniministeerium · Suur-Ameerika 1, Tallinn
Toimetaja: Carolyn Mets · carolyn.mets@mkm.ee · +372 5697 6026

Design & Branding Studio sviite agency Estonia