Riikliku küberturvalisuse uudiskiri

2023-05

Majandus- ja kommunikatsiooniministeerium

Minister Riisalo: “Tugev küberturvalisus on Eesti digitaalse eluviisi võimaldaja”

Riigi Infosüsteemi Amet

Eesti–USA ühistiim sai Locked Shieldsil teise koha

TalTech

Tehnikaülikool korraldab CySec4Psych projekti raames koolitus- ja teadlikkuse tõstmise üritusi psühholoogidele

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Majandus- ja Kommunikatsiooniministeerium

Minister Riisalo: "Tugev küberturvalisus on Eesti digitaalse eluviisi võimaldaja" 3

Küberturvalisuse kulude arvestamise mudeli tutvustus 3

Riigi Infosüsteemi Amet

EU CyberNeti uus juht on Liina Areng 4

Eesti-USA ühistiim sai Locked Shieldsil teise koha 4

Küberturbe linnalaager tõi kokku valdkonnast huvitatud tüdrukud 4

TalTech

Tehnikaülikoolis kaitses küberturbealase doktoritöö Kaur Kullman 5

Tehnikaülikool korraldab CySec4Psych projekti raames koolitus- ja teadlikkuse tõstmise üritusi psühholoogidele 5

Kood Jõhvi

kood/Jõhvi küberhäkatonil loodi 48 tunniga 15 uut lahendust virtuaalmaailma turvalisemaks muutmiseks 6

ENISA

ENISA kolmas telekommuniksatsiooni ja digitaalse infrastruktuuri turbefoorum 7

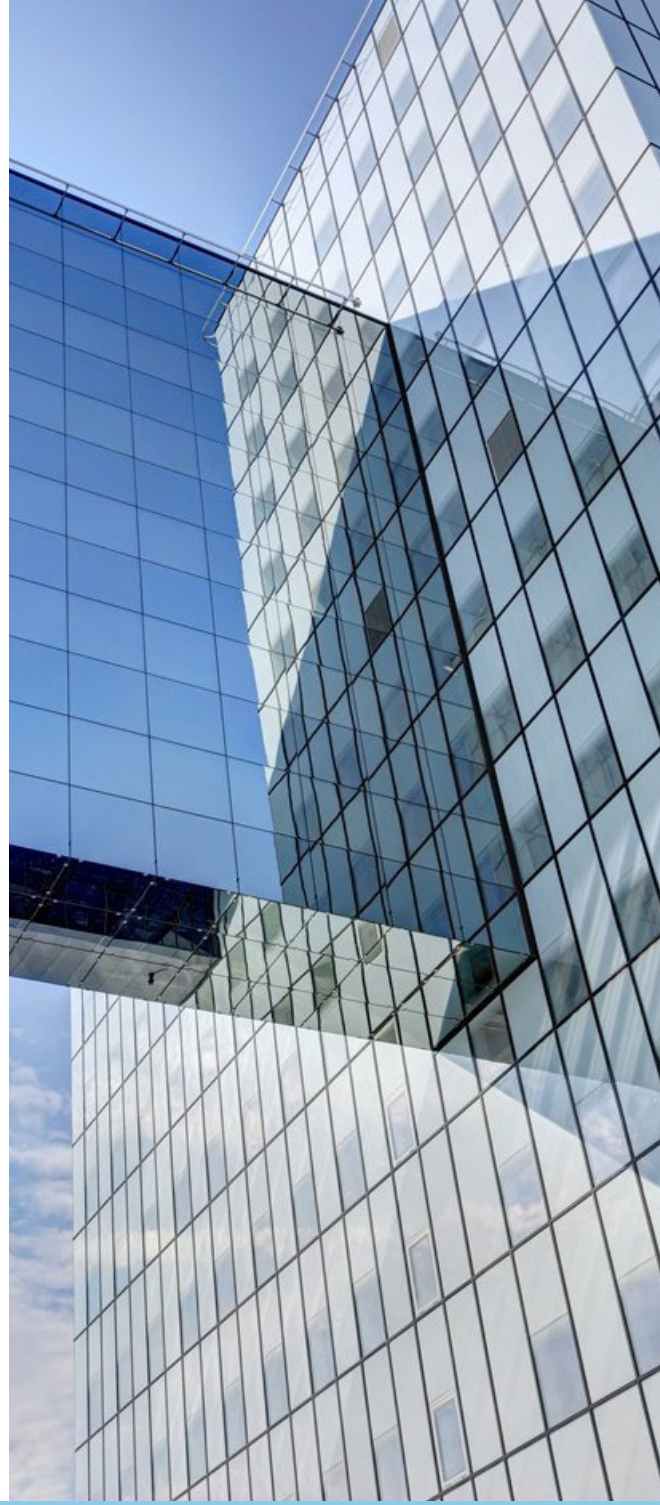
Cybernetica

Eesti ja Lõuna-Moraavia on ühendanud jõud, et toetada uudsel moel Euroopa Liidu digiühiskonna üleminekut 7

EY ja Cybernetica viivad läbi esimese üleeuroopalise digitaalsete rahakottide turu-uuringu 8

European Telecommunications Standards

ETSI Security Conference 2023 9



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

Minister Riisalo: "Tugev küberturvalisus on Eesti digitaalse eluviisi võimaldaja"

Majandus- ja infotehnoloogiaminister Tiit Riisalo sõnul on sõda Ukrainas näidanud, et küberturvalisus on riikliku julgeoleku üks nurgakivi.

Aktiivne tegevus küberruumis ei toimu ainult füüsilise sõjategevuse ajal, vaid ka eelneb ja järgneb sellele. "Kõrge küberturvalisuse taseme hoidmine nõuab pidevat tähelepanu ja pakub väljakutseid, kuid Eesti on selleks valmis. Tugev küberturvalisus on Eesti digitaalse eluviisi võimaldaja ning selle parendamine eeldab järjepidevaid investeeringuid. Küberturvalisus ei tohi olla koht, kust otsida võimalusi kokkuhoiuks. Seda enam, et riskide tuvastamine ja maandamine on oluliselt odavam kui tagajärgedega tegelemine," ütles minister.

Riisalo rõhutas, et globaalne küberohupilt muutub pidevalt ja küberrünnakute arv nii üksikisikute, ettevõtete kui ka riikide vastu kasvab globaalselt. Ta märkis, et elutähtsate teenuste üha tempokam liikumine küberruumi tähendab vajadust leida veelgi tõhusamaid viise, kuidas suurendada riiklikku kübervastupidavust. Minister ütles, et Eesti on küberrünnakute neutraliseerimisega hästi hakkama saanud ja suurem osa neist on jäänud üksnes katseteks. See tähendab, et neil pole teenustele olnud pikaajalist või tuntavat mõju. Seda hoolimata faktist, et mullused teenustõkestusründed olid näiteks võrreldes 2007. aastaga kordades intensiivsemad. "Küberrünnakute pea nähtamatu mõju Eesti inimestele on avaliku- ja erasektori tõhusa partnerluse tulemus, sest rakendatakse riski ja ohtu arvestavaid kaitsemeetmeid. Tihe koostöö ja parimate praktikate jagamine on äärmiselt oluline, sest pahalased muutuvad aina kavalamaks ja rünnakud keerulisemaks," toonitas Riisalo.

Eesti on üks arenenumaid ja uuenduslikumaid digiühiskondi maailmas. See tähendab, et iga teenuse ja andmekogu puhul tuleb hoolikalt mõelda ka infoturbe ja riskijuhtimise korraldamisele. "Jättes täna tegemata vajalikud investeeringud tõuseb märgatavalt suure mõjuga küberintsidentide oht. Selliste olukordade vältimiseks ja organisatsiooni või koguni ühiskonna toimepidevuse tagamiseks tuleb küberturvalisusest mõelda võimaldajana. Infoturve on nagu finantsaudit või toiduohutus, mille korras olemine võimaldab keskenduda oma põhitegevusele," ütles Riisalo.

Küberturvalisuse kulude arvestamise mudeli tutvustus

Olete oodatud, 23. mail Riikliku küberturvalisuse osakonna tellitud analüüsi „Küberturvalisuse kulude arvestamise mudeli loomine Majandus- ja Kommunikatsiooniministeeriumile" tulemuse tutvustusele.

Ernst&Young poolt läbiviidud analüüsi eesmärgiks oli luua põhimõtted ja juhised, millest lähtuda küberturvalisuse kulude käsitlemisel asutustes nii tehnoloogiliselt kui finantsilisest vaatenurgast. Oluline oli luua mudel, mis arvestaks tänast süsteemi ning oleks rakendatav minimaalsete muudatustega.

Üritus toimub ministeeriumite ühishoone Tamme saalis 23.05 kell 10:00–12:00.

Osaleda võib MKMis Tamme saalis või siis üle Teamsi virtuaalselt.

Palun registreerida siin, kohtade arv on piiratud!

EU CyberNeti uus juht on Liina Areng

Alates aprilli lõpust juhib RIA EU CyberNeti projekti senine CyberNeti regionaalse programmi juht Liina Areng. Võrgustiku endise juhi Erkki Leego viimane tööpäev RIAs oli 21. aprillil.

Küberturvalisuse keskuse juht Gert Auväärti sõnul on projekti töö saavutanud viimase kahe aasta jooksul täiesti teise taseme, sh on ekspertide hulk pidevas kasvutrendis. „See, et EL-i kõrge esindaja Borrell käis hiljuti LAC4 keskust avamas ei ole mingi iseenesest mõistetav nähtus, vaid on päriselt väga kõrge tunnustus projekti edule ja tiimi ennastsalgavale tööle," tõdes Auväärt.

„EU CyberNeti pall ei kuku selle muudatuse pinnalt maha, vaid vastutuse võtab üle projektiga ühes vereringes pikalt olnud Liina Areng, kes seda rolli kindlasti väärikalt edasi kannab. Soovin edu nii Erkkile kui Liinale uute väljakutsetega," lisas keskuse juht Gert Auväärt.

Eesti-USA ühistiim sai Locked Shieldsil teise koha

21. aprillil lõppes Tallinnas NATO küberkaitsekoostöö keskuse korraldatud küberõppus Locked Shields, mille võitis Rootsi-Islandi ühistiim. Auväärse teise koha pälvis Eesti-USA ühistiim, kuhu kuulusid ka paljud RIAkad. Kolmandaks tuli Poola meeskond.

"Locked Shieldsil ei ole kaotajaid. Ka teine koht on võit," sõnas RIA küberturvalisuse keskuse osakonnajuhataja Raimo Peterson, kes oli nädala jagu kestnud õppusel Eesti-USA tiimi juht. „Pakkusime 155 Eesti eksperdile väga suure arenguhüppe ja koolituse, mida kuskilt mujalt ei saa."

Locked Shields on ligi 3000 osalisega maailma suurim omataoline küberõppus, mis võimaldab osalejatel kaitsta päris arvutisüsteeme reaalajas toimuvate rünnakute eest ning mängida läbi, kuidas langetada aegkriitilises situatsioonis nii taktikalisi kui ka strateegilisi otsuseid.

Seekordsest õppusest võttis osa 24 tiimi 32 erinevast riigist, sh Eestist. Õppust on korraldatud alates 2010. aastast.

Küberturbe linnalaager tõi kokku valdkonnast huvitatud tüdrukud

Reedel, 28. aprillil korraldas RIA koos Kaitseliiduga kodutütardele küberturvalisuse teemalise linnalaagri.

Tegemist oli esimese taolise laagriga, kus kodutütardele näidati praktiliselt küberruumis valitsevaid ohte ja kuidas ennast nende vastu kaitsta. Teemadena võeti läbi võrgu skänneerimine, Kali Linux, paroolid ning räsid, turvanõrkuste otsimine ja eetika.

Noored võtsid oma kogemused kokku järgmiselt:

Liisbet: „See on huvitav, et siin näeme seda maailma, kuidas need asjad programmides sees käivad, kuidas neid asju lahti võetakse ja milliseid koode selleks kasutatakse. Hakkasin mõtlema, et see oleks huvitav valdkond, kus töötada."

Cristel: "See on hea, et seletatakse lahti, mis on mis. Varasemalt oleme ka erinevatel koolitustel käinud, kus on selliseid asju näidatud, aga see on alati väga põgusalt olnud. Nüüd saame ise läbi proovida ja küsida, mis kuidas käib."

Laager toimus küberkaitseüksuse ruumides Männikul ning sellest võtsid osa 17 kodutütart.

Tehnikaülikoolis kaitses küberturbealase doktoritöö Kaur Kullman

25. aprillil kaitses Kaur Kullman oma doktoritööd „Interaktiivsed, ruumiliselt tajutavad, mitmemõõtelised andmekuvad küberturbele“ („Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity“).

„Võimalike turvaintsidentide aegsaks tuvastamiseks ja leidude mitigeerimiseks peavad keerukate süsteemide kaitsjad neid süsteeme järjepidevalt seirama: tuvastama anomaaliad, eristama valepositiivsed, delegeerima leiud pädevale kolleegile, kes intsidendi lahendamise eest hoolitseks.”

“Keeruka süsteemi kaitsmise eelduseks on selle kaitsjate hea arusaam sellest süsteemist, selle komponentidest, nende omavahelistest ja välistest seostest, komponentide ootuspärasest käitumisest, süsteemi kasutajate harjumustest jm — süsteemi mentaalne mudel.”

“Kuigi keerukate süsteemide topoloogia visualiseerimine kahemõõtmelise kujutisena lamedal ekraanil võib süsteemi mõistmisel kasuks tulla, on rohkema kui kolme mõõtme samaaegne visualiseerimine lamedal ekraanil kohmakas selle hoomamatu ruumilisuse tõttu — kuvatu ruumilisus pole paberilt ega lamedalt ekraanilt lihtsasti tajutav: see doktoritöö keskendub nende probleemide võimalikele lahendustele.“

Doktoritöö juhendaja oli prof. Olaf Maennel (Adelaide’i Ülikool/Tallinna Tehnikaülikool) ning kaasjuhendajad prof. Don Engel (Marylandi Ülikool) ja prof. Stefan Sütterlin (Tallinna Tehnikaülikool).

Doktoritöö on avaldatud tehnikaülikooli raamatukogu digikogus.

Tehnikaülikool korraldab CySec4Psych projekti raames koolitus- ja teadlikkuse tõstmise üritusi psühholoogidele

Euroopa Liidu rahastatud projekti CySec4Psych (Cyber Security for Psychology) raames korraldab Tallinna Tehnikaülikool sel kevadel ja varasuvel koolitus- ja teadlikkuse tõstmise üritusi. Üritused on suunatud psühholoogiatudengitele, kes soovivad tutvuda küberkaitse valdkonnaga.

Projekti peamised eesmärgid on luua küberturvalisuse valdkonna karjäärivalik psühholoogia eriala lõpetajatele läbi teadlikkuse tõstmise ja koolitustegevuse, vähendada küberturvalisuse oskuste lõhet, luues õpetamis- ja koolitusmaterjale ning uurimis- ja koolituskava, töötada välja rahvusvahelised tipptasemel moodulid, mis vastaks hariduse ja tööturu vajadustele. Pikaajaliseks eesmärgiks on käivitada ja arendada kogu Euroopas küberturvalisuse psühholoogide võrgustik.

Projekti meeskonna moodustavad rahvusvahelise taustaga koolitatud psühholoogid Saksamaa Saarlandi Ülikoolist, Tallinna Tehnikaülikoolist, Hollandi Leideni Ülikoolist ja Helmholtzi Infoturbe keskust CISPA Saksamaalt, kes kõik töötavad IT-turvalisuse valdkonnas. Meeskonna huvivaldkonnad ulatuvad küberteadlikkuse täiendõppest keerulistes organisatsioonides, küberkuritegevusest kuni sooritusteni sõjalise küberkaitses, meeskondade rollist sotsiaal-tehnilistes süsteemides kuni küberjulgeoleku rollini poliitilises desinformatsioonis.

- 25.-26. mail toimub Tallinna Tehnikaülikooli korraldusel täielikult veebis Researchathon, mis annab psühholoogia ja teiste käitumisteaduse üliõpilastele edasi põhitõdesid ja näiteid selle kohta, kuidas käitumisteadused võivad aidata kaasa turvaprobleemide paremale käsitlemisele.
- 12.- 16. juunil toimub Tallinnas CySec4Psych suvekool.

Kontakt: prof. Stefan Sütterlin (stefan.sutterlin@taltech.ee).

kood/Jõhvi küberhäkatonil loodi 48 tunniga 15 uut lahendust virtuaalmaailma turvalisemaks muutmiseks

Nädalavahetusel Jõhvis toimunud küberturvalisuse häkatonil osales üle 100 küberentusiasti üle Eesti, et leida uuenduslikke lahendusi küberturvalisusega seotud probleemidele ja väljakutsetele. Startup Estonia ja kood/Jõhvi poolt ellu kutsutud häkaton kestis 48 tundi ja selle käigus arendasid 15 tiimi uuenduslikke ideid, mis lahendasid nii levinud õngitsusrünnakutega seotud probleeme, kui ka küberturbealase teadlikkuse suurendamise ning tehisintellekti ja süvavõltsinguid puudutavaid probleeme.

Pühapäeva õhtul toimunud lõpuüritusel tutvustas häkatoni žuriile oma valminud ideid ja prototüüpe kaheksa tiimi. Häkatoni võidutiim StealthSyntax võttis fookusesse viimase aja vaieldamatult kõige suurema tähelennuga tehisintellekti ChatGPT turvalisuse, pakkudes võimalust kasutajate jagatud sisendinfo turvamiseks. "11% ChatGPT-le kasutajate poolt sisestatud infost on konfidentsiaalne ja keegi ei saa olla praegusel hetkel kindel, mis juhtub tundlike andmetega pärast nende jagamist," selgitasid tiimiliikmed ise enda lahendatavat lähteprobleemi. Tiimi lahendus aitab kasutajate sisestatud infot maskeerida, muutes selle jõudmise kolmandate osapoolte kätte võimatuks. Auhinnatud said lisaks StealthSyntaxile veel kaks potentsiaalikat ideed - süvavõltsingute ja autoriõiguste rikkumise vastu võitlev Arrjee ja õngitsusrünnakute ennetusega tegelev Webiify.

Kogu häkatoni jooksul olid tiimidele nõuga abiks 16 mentorit. "Esmalt tiimidega probleemi kirjeldamine ja ideede väljatöötamine ning seejärel erakordse kiirusega arendustegevuse käivitamine oli võrratu kogemus," jagas üks häkatoni mentoritest, kaitseliidu vabatahtlik ja Swedbanki scrum master Talis Pähn. "Häkaton tõestas taaskord, et väikese julgustuse ja nõuannetega suudavad motiveeritud inimesed saavutada kõike, mida nad soovivad," lisas Pähn.

Foto: Hanna Luisa Grosberg

Seda kinnitab ka võitjatiimi StealthSyntax liige Kaspar Johannes Pärtel. "Esimene häkatoni kogemus oli võimas, väga palju on võimalik päriselt ära teha 48 tunniga, kui ennast täielikult ühele asjale pühendada. Annab tohutult enesekindlust oma edasiste projektide elluviimiseks. Soovitan häkatonil osalemist kindlasti kõigile, see on hea võimalus viia ennast mugavustsoonist välja ja koguda erakordselt väärtuslikke kontakte."

Žürii liige, Startup Estonia kübertehnoloogia valdkonna juht Kati Pärn tõi välja, et võistkondade energia laval oli väga hoogne ning presentatsioonid sisukad. "Initsiatiividega saab rahul olla, kuna küberturvalisuse teemad on tänapäeva geopoliitilist olukorda ja tehisintellekti arengut arvestades äärmiselt olulised ning kõik tiimid olid teinud väga head tööd. Kolm võitjatiimi näitasid oma leidlikkust probleemide lahendamisel, millele lõpuhindamine andis väikest pinget juurde," lisas Kati Pärn.

Häkatoni korraldaja kood/Jõhvi ja koodikoolis õppijate jaoks oli tegu nende esimese taolise üritusega. "Oleme tulemustega väga rahul, sest kokku tuli väga mitmekülgne seltskond osalejaid ja mentoreid," rõõmustas kood/Jõhvi koolijuht Karin Künnapas. "Häkatonil osalejatest üle poole olid kood/Jõhvi õppijad, kes said väga väärtusliku kogemuse osaliseks ja meie suureks heameeleks mitmed neist ka jätkavad oma ideede

kood / Jõhvi

arendusega. Ka kood/Jõhvi plaanib häkatonide ellukutsumise ja korraldamisega jätkata."

kood/Jõhvi küberturbe häkaton toimus vahemikus 21.-23. aprillil Jõhvis. Häkatoni eesmärk oli leida uuenduslikke lahendusi konkreetsetele küberturbe väljakutsetele, 48 tunni jooksul pidid tiimid valmis ehitama ja esitlema töötavat prototüüpi või lahendust. Häkatoni elluviimist toetasid Startup Estonia, Kredex, EAS, Tehnopol, Cybers, Telia, LHV, Miltton, Latitude59, NFTTallinn, sTARTUp Day, Guardtime, k-Space, Rangeforce, TalTech, Küberväejuhatus, Objekt, FFF.

kood/Jõhvi on uudne programm täiskasvanutele, mis pakub 21. sajandi lähenemist programmeerimise õppimisele, et vähendada tarkvaraarendajate puudust ja võimaldada teistest valdkondadest pärit inimestele uusi ja huvitavaid võimalusi elus. Kooli rahastavad üle 30 ettevõtte, sealhulgas paljud idufirmad ja ükssarvikud, kes on valmis pärast kaheaastase programmi lõppemist õppijaid tööle võtma.

Lisalugemist blogipostituses.

ENISA

ENISA kolmas telekommuniksatsiooni ja digitaalse infrastruktuuri turbefoorum

ENISA kolmas telekommunikatsiooni ja digitaalse infrastruktuuri turbefoorum kolmapäeval, 24. mail Lissabonis hotellis Epic Sana Marquês (ainult füüsiline).

Sündmus pakub elektroonilise side pakkujatele, digitaalse infrastruktuuri üksustele ja riiklikele ametiasutustele platvormi, kus jagada häid tavasid ja kogemusi uusimate turvaohtudega toimetulekuks, hõlmates selliseid teemasid nagu marsruutimise turvalisus, satelliitside, merekaablite turvalisus, null-usaldusarhitektuurid, 5G turvalisus, RAN-turve, telekommunikatsiooni ja energia vastastikused sõltuvused, telekommunikatsioon kui kilp, Interneti killustatus. Arutatakse viimastest seadusandlikest algatustest, nagu NIS2 direktiiv, tulenevaid muudatusi ja vahetada arvamusi tuvastatud väljakutsete ja võimaluste üle.

Registreerumine ja lisainfo siin.

Cybernetica

Eesti ja Lõuna-Moraavia on ühendanud jõud, et toetada uudsel moel Euroopa Liidu digiühiskonna üleminekut

Küberturvalisuse tippkeskus Eestis ja Lõuna-Moravias (CHESS), mis valiti välja 102 taotluse hulgast, püüab ületada lõhet teaduse ja innovatsiooni vahel, tuues kokku fundamentaalteadlased majanduse ja ühiskonna ärakasutajatega

Selle EL-i rahastatava projekti raames teeb Eesti, kes on tugeva e-valitsuse taristuga digiühiskonna liider maailmas, tihedat koostööd Lõuna-Moraviaga, Tšehhi IKT-tööstuse ja hariduse jõujaamaga, keskendudes tugevalt küberturvalisusele.

CHESS projekti raames töötatakse välja ühine piiriülene küberjulgeolekualaste teadusuuringute ja innovatsiooni strateegia, mis keskendub kuuele väljakutsevaldkonnale:

- turvaliste asjade internet;
- turvasertifikaat;
- usaldusväärse tarkvara kontrollimine;
- turvalisuse säilitamine plokiahelas;
- postkvantkrüptograafia;
- küberturvalisuse inimkesksed aspektid.

"Strateegia väljatöötamisele aitab kaasa

pilootprojektide elluviimine, mis tugevdavad piirkondadevahelist koostööd, kaasavad piirkondlikke innovatsiooni ökosüsteeme ja koguvad tõendeid tulevaste projektide jaoks," ütles Masaryki ülikooli prof Vashek Matyas.

Cybernetica vanemteadurid vastutavad kvantijärgse väljakutse valdkonna juhtimise ja turvasertifikaadi väljakutsete valdkonna kaasjuhtimise eest. Cybernetica CHESSi projekti juhtivteadur Liina Kamm ütles: "Nii Lõuna-Moraavia kui ka Eesti IKT vundament on veidi erinevate fookustega, nii et koostöö aitab meil üksteiselt õppida ja seeläbi meie digitaalset ühiskonda paremaks muuta."

Lõppkokkuvõttes avaldab CHESS projekt osalevatele institutsioonidele kasulikku mõju, suurendades nende nähtavust, atraktiivsust ja potentsiaali luua uuenduslikke ja kasutatavaid uurimistulemusi. Kuid lisaks loob see ainulaadse suhtlusvõrgustiku väljaspool oma konsortsiumi, ühendades Lõuna-Moravia tugevad küljed sertifitseerimise ja inimkeskse uurimistöö vallas Eesti teadmistega plokiahela, postkvantkrüptograafia ja e-valitsemise vallas, et hõlbustada turvalist üleminekut täielikule mastaapsed digitaalsed ühiskonnad.

CHESSi konsortsiumi kuulub üheksa partnerit ja kolm assotsieerunud partnerit, sealhulgas Masaryki Ülikool, Tartu Ülikool, Brno Tehnikaülikool, Tallinna Tehnikaülikool, Cybernetica, Red Hat, Guardtime, Eesti Infosüsteemi Amet, Küberturvalisuse keskus, National Cyber ja Infoturbeagentuur, Lõuna-Moravia Innovatsioonikeskus ja Eesti Infoturbe Liit.

Lisainfo Cybernetica koduleheküljel.

Projekti rahastab Euroopa Liit toetuslepingu nr 101087529 alusel. Selles projektis väljendatud seisukohad ja arvamused on ainult autori(te) omad ega pruugi kajastada Euroopa Liidu või Euroopa Teadusuuringute Rakendusagentuuri omasid.

EY ja Cybernetica viivad läbi esimese üleeuroopalise digitaalsete rahakottide turu-uuringu

Euroopa Komisjoni informaatika peadirektoraat tellis esimese üleeuroopalise digitaalsete rahakottide turu-uuringu, et uurida erinevaid digitaalseid rahakotte ja nende pakkujaid ning mille lõppeesmärk on suurendada digitaalse identiteedi rahakottide kasutuselevõttu kogu Euroopas.

Projekti "C2G ja C2B usaldusmudelid ja turuanalüüsi konsultatsiooniteenused" viib läbi EY uuringumeeskond, keda toetavad mitmed digitaalsete rahakottide ja identiteedi valdkonna asjatundjad, sh Cybernetica.

Uuringu põhifookuses on digitaalsete rahakottide pakkujad — nii turujuhendi sihtrühmana kui ka oma digitaalsete rahakottide kohta teabe pakkujana turujuhendi toiteks. Projekt hõlmab liikmesriikide rahakoti rakendusraamistikke, arhitektuuri viiteraamistikku, erasektori algatusi, tarbijalt valitsusele (C2G) ja tarbijalt ettevõttele (C2B) teenuseid. Uuring annab läbilõike Euroopa digitaalsete rahakottide turust analüüsi tegemise ajal. Nii palju kui võimalik, käsitletakse uuringus olukorda kõigis 27 ELi liikmesriigis, kuigi digitaalsete rahakottide parimaid tavasid võidakse tutvustada ka teistest piirkondadest.

Cybernetica põhiülesanne on pakkuda nõustamisteenuseid, et toetada, nõustada ja kinnitada EY läbiviidavat uuringuanalüüsi, jagades ekspertarvamusi ja kogemusi olemasolevate regulatiivsete raamistike kohta nii Euroopa kui ka riiklikul tasandil digitaalsete rahakottide, rahvusvaheliste ja Euroopa standardite, turvalisuse kohta. aspekte, krüptoalgoritme ja protokolle ning paljusid muid valdkondi, mis puudutavad digitaalse identiteedi rahakotte.

Rohkem infot ja edasi lugemine Cybernetica koduleheküljelt.

European Telecommunications Standards

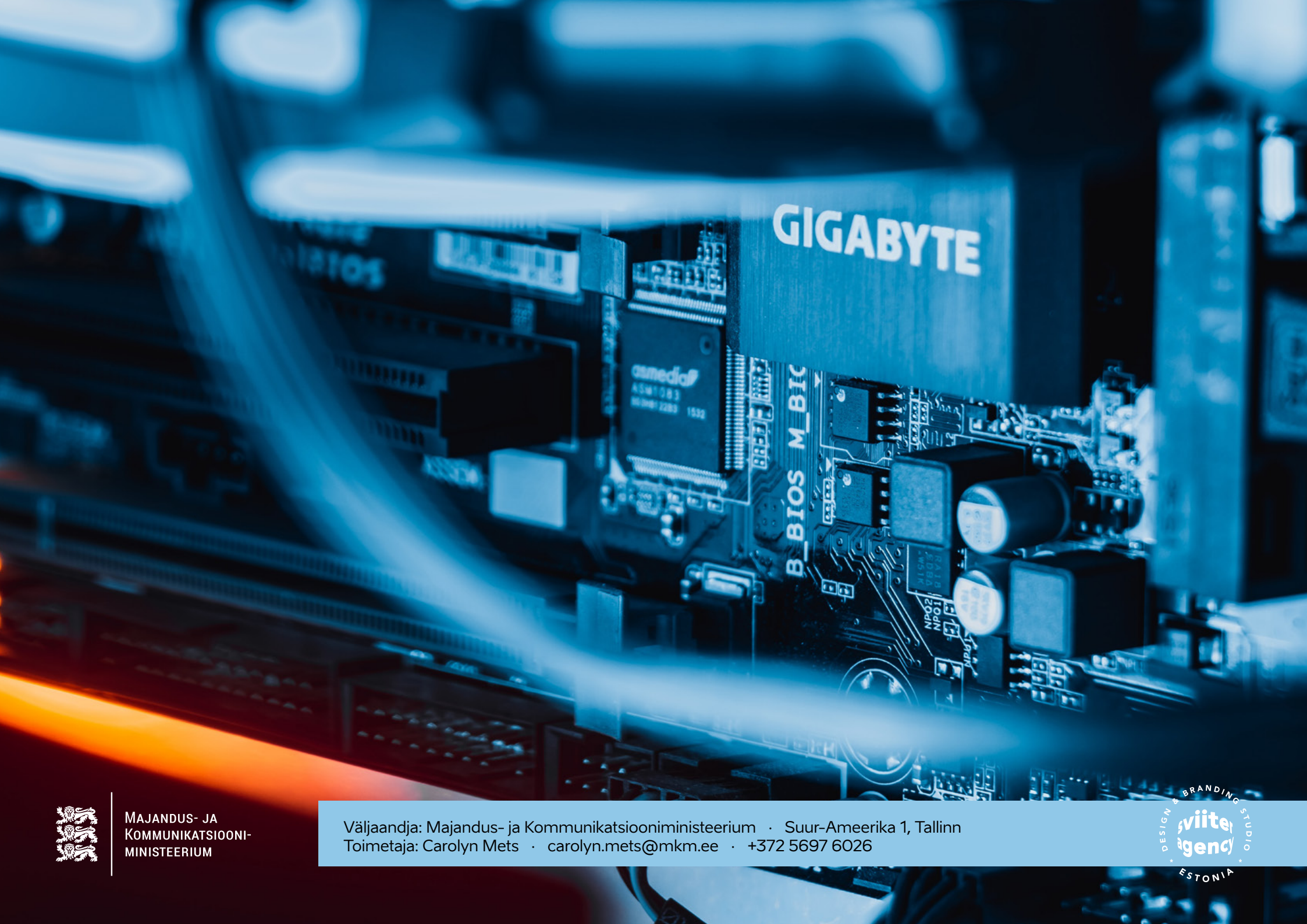
ETSI Security Conference 2023

ETSI konverentsi fookuses on sellel aastal teadusuuringud ja innovatsioon. Esitluste kutse on avatud 31. maini.

ETSI iga-aastane küberturvalisuse lipulaev ETSI turvakonverents toimub 16.–19. oktoobril 2023 Prantsusmaal ETSI-s Sophia Antipolises.

Sündmus langeb kokku 2023. aasta Euroopa küberjulgeoleku kuuga. Selle aasta programm hõlmab selliseid teemasid nagu:
• Ülemaailmsed määrused
• „5G looduses" — 2023: saabuvad pilvepõhised, 5G tuuma, vertikaalid ja API-d.
• Sertifitseerimine (5G, IoT, GSMA NESAS, mobiiltelefon, pilv)
• IoT värskendamine — TS 103 645, sundjuhtimise leevendamine, vertikaalid (sh nutikad lukud ja hääleassistendid), e-tervis.
• 6G futuurid
• Zero trust
• AI (sh Open AI ja GPT).
• Avatud lähtekood
• Avage RAN
• Mitte-maapealsed võrgud (NTN) — rakendused, riskid ja kasutusjuhtum
• Tarneahela turvalisus
• Post Quantum "State of the Nation" — NIST, GSMA PQTN, Migration, AI, mida kasutatakse Quantumi vastu suunatud rünnakuteks, ETSI QSC.
• Liitreaalsus

Lisainfo ja kontaktid ETSI koduleheküljelt.



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