# Riikliku küberturvalisuse uudiskiri

2023-03

Majandus- ja kommunikatsiooniministeerium

## Küberturvalisuse valdkonna revisjonist

Riigi Infosüsteemi Amet

## Märtsis saavad ettevõtted taotleda toetust küberturvalisuse parandamiseks

Siseministeeriumi infotehnoloogia- ja arenduskeskus

## SMIT on nüüdsest sertifitseeritud ISO 27001 infoturbestandardi nõuete kohaselt

Majandus- ja Kommunikatsiooni-ministeerium

## Seekordses uudiskirjas


### Majandus- ja Kommunikatsiooniministeerium

Küberturvalisuse valdkonna revisjonist 3

### Riigi Infosüsteemi Amet

Märtsis saavad ettevõtted taotleda toetust küberturvalisuse parandamiseks 3

Veebruaris külastasid RIAt Ukraina koostööpartnerid, kes on loonud DIIA nimelise mobiiliäpi ning aitavad arendada ka mRiiki 4

Palju õnne! Liina Areng sai Eesti Vabariigi presidendilt Valgetähe IV klass teenetemärgi! 4

### Siseministeeriumi infotehnoloogia- ja arenduskeskus

Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT) on nüüdsest sertifitseeritud ISO 27001 infoturbestandardi nõuete kohaselt 5

### StartUp Estonia

Startup Estonia sTARTUp Day üritus küberkogukonnale 6

Küberturbe häkaton 6

### EASi ja KredExi ühendasutus

Eesti kosmose küberharjutusväljaku ideekorje infoseminar 6

### TalTech

TalTechis tunnustati küberjulgeolekualast õppe-, teadus- ja teavitustööd 7

Algas vastuvõtt Tallinna Tehnikaülikooli 7

Küberturvalisuse veebiseminaride sarjas esineb Ebelechukwu Nwafor Villanova ülikoolist 7

Cyber4Schools projekt kutsub koole testima uut mängu 7

### E-riigi Akadeemia

eGA tõhustab Moldova kaitsejõudude küberturvet 8

### Cybernetica

Cybernetica aitab kaasa Euroopa esimese Hydrogen Valley projekti BalticSeaH2 arendamisele 8

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

## Küberturvalisuse valdkonna revisjonist

Eelmise aasta detsembri viimastel päevadel avaldati Euroopa Liidu Teatajas Euroopa Parlamendi ja nõukogu õigusaktid, mis tuleb ka Eesti õigusaktidesse üle võtta või teha nendes muudatusi. Nendeks on küberturvalisuse 2. direktiiv ehk NIS2 direktiiv, finantssektori digitaalse tegevuskerksusega seotud direktiiv ja määrus (DORA) ning elutähtsa teenuse osutajate toimepidevusega seotud direktiiv ehk CER direktiiv. Kõik mainitud õigusaktid jõustusid 16. jaanuaril 2023. a.

Teavitasime üle-eelmises uudiskirjas, et NIS2 direktiiviga seonduvalt on kavas teha eraldi küberturvalisuse valdkonna revisjon, mis toimub koostöös huvitatud osapoolte, kehtiva küberturvalisuse seaduse teenuse osutajate kui ka NIS2-ga lisanduvate sektorite esindajatega. Samuti mainisime, et peatselt hakkavad pihta tegevused eelmainitud direktiivide üle võtmiseks.

Siinse artikliga anname uudiskirja lugejatele eelteate: soovime revisjoniga seonduvalt teha märtsis arutelu-kaasamisüritused ehk kärajad. Kärajatel soovime just Teie sisendit ja mõtteid NIS2 üle võtmiseks kui ka muude praktiliste probleemide lahendamiseks õigusloome kaudu.

Täpsem info kärajate kohta edastatakse peatselt ka eelmainitud huvigruppidele. Kärajatel osalemise huvi olemasolul võib juba praegu ühendust võtta MKM-i riikliku küberturvalisuse osakonnast Raavo Paluga. Selleks palume saata e-kiri aadressil raavo.palu@mkm.ee, lisades teemareale „KüTS-i revisjoni kärajad".

Kärajate järel tegeletakse kaasatud osapooltega ühiselt eelnõu kirjutamisega, et eelnõu tekst saada kokku 2023. aasta sügiseks (eelistatult septembris). Seejärel edastatakse eelnõu eelnõude infosüsteemi vahendusel ka avalikule kooskõlastusele.

NIS2 direktiivi siseriiklikusse õigusesse ülevõtmise tähtaeg on 21 kuud ehk see tuleb üle võtta hiljemalt 17. oktoobriks 2024. a.



## Märtsis saavad ettevõtted taotleda toetust küberturvalisuse parandamiseks

Riigi Infosüsteemi Amet ja EAS/Kredex ühendasutus hakkavad märtsi esimeses pooles jagama toetusi mitme sektori väikese- ja keskmise suurusega ettevõtetele. Toetust saavad taotleda tööstusettevõtjad, hulgi- ja jaekaubandusettevõtjad, ehitusettevõtjad, veondus ja laondusettevõtjad ning info- ja sideettevõtjad.

Toetuse abil saavad Eesti väikese ja keskmise suurusega tööstusettevõtjad välise nõustaja kaasabil hinnata IT-süsteemide küberturvalisuse taset ja astuda esimesi samme kaitsmaks ettevõtet küberrünnakute ja nendega kaasnevate kahjude vastu.

„Küberintsidendid teevad ettevõtetele haiget, rünnakud võivad tööstusettevõtte tootmise katkestada või arvepettuse järel rahalist kahju tekitada. Seetõttu soovime Euroopa Liidu toel katsetada, kas digi- ja rohepöörde kõrval võiks üks küberpöörde toetus innustada väiksemaid ettevõtteid panustama enese küberturbesse. Küberpööre on esimeseks sammuks ettevõtetele küberturvalisuse teel," ütles RIA teaduse- ja koordineerimisosakonna juhataja Lauri Tankler.

Ta lisas, et küberpöörde pilootprojekt on kaheastmeline. „Esimese tegevussuunana pakume ettevõtetele kuni 10 000 euro suurust süsti, et nad kaardistaksid ära oma küberturvalisuse hetkeseisu ning saaksid ülevaate kõige põletavamatest puudustest ja parandusettepanekutest. Kui see faas on läbitud, siis avaneb neil võimalus taotleda kuni 50 000 eurot, et teise tegevussuuna osana neile tehtuid soovitusi päriselt ellu viia. Ehk siis tuleb esmalt lasta hinnata oma küberturvalisust ja siis juba astuda konkreetseid samme selle parendamiseks," lausus Tankler.

Selleks, et toetusele vastavaid tööstusettevõtteid aidata, leiab RIA kodulehelt infot Eestis tegutsevatest küberturvalisuse ettevõtetest, kelle abil vastav hindamine ehk teekaart luua. RIA veebist leiab ka näidise ja juhendi, mida peab küberturvalisuse hindamise

teenust osutavad pakkujad seda tehes silmas pidama ja millist metoodikat kasutama.

Mõlema toetuse taotlemisel on toetus taotlevate ettevõtete omafinantseeringu osakaal 50%.

Millised ettevõtted saavad toetus taotleda?

- Ettevõtjad, kes soovivad tõsta küberturvalisuse alast teadlikkust ning juurutada lahendusi, mis aitavad kaitsta küberrünnakute ja nendest tingitud kahjude eest.

- Toetust saavad taotleda Eesti äriregistrisse kantud väikesed- ja keskmise suurusega ettevõtjad: tööstusettevõtjad (EMTAK B, C), hulgi- ja jaekaubandusettevõtjad (EMTAK G), ehitusettevõtjad (EMTAK F), veondus ja laondusettevõtjad (EMTAK H), info- ja sideettevõtjad (EMTAK J).

- Ettevõtja taotluse esitamisele eelneva kahe majandusaasta keskmine müügitulu vastavalt äriregistrile esitatud majandusaasta aruannetele on taotleja põhitegevusalal Eestis vähemalt 200 000 eurot.

- Projekti tegevused peavad toimuma Euroopa Liidu liikmesriigis või Euroopa Majanduspiirkonna riikides (Norra, Island, Liechtenstein). Taotleja ettevõtja üle kontrolli omav ettevõtja peab samuti olema registreeritud EL või EEA piirkonnas.

- Sektorid, mille ettevõtted toetust taotleda ei saa.

RIA ja EAS/Kredex korraldavad toetuse vastu huvi tundvatel ettevõtetele infotunni, kus tutvustatakse toetuse taotlemise protsessi ja tingimusi. Infotund toimub märtsi alguses. Täpsem info on peatselt leitav kübertoetuse kodulehelt.

## Veebruaris külastasid RIAt Ukraina koostööpartnerid, kes on loonud DIIA nimelise mobiiliäpi ning aitavad arendada ka mRiiki

Koostöö RIA ja Ukraina ettevõtte vahel algas juba 2022. aasta kevadel, kui Eestis oli mRiigi arendus juba hoo sisse saanud. Ukraina ettevõttega jagati äpi arendamise *know how-d* ja teadmisi toimivatest praktikatest. Siiani on koostöö olnud virtuaalne ja seekordse kohtumise eesmärk oli tugevdada sidemeid, viia kokku ekraani taga olevate inimeste näod ja nimed ning teha koos erinevaid töötubasid.

Eesti riikliku mobiilirakenduse mRiigi kaudu jõuavad digiteenused ja -lahendused ühiskonnani ning paraneb kahesuunaline kommunikatsioon ja viis, kuidas riigiteenuseid tarbitakse. Tulevikus saab läbi loodava platvormi rakendada nutivõimekust paremate riigiteenuste pakkumiseks kodanikele ja edaspidi ka asutustele. Ühiselt TEHIKu ja MKMi esindajatega käidi läbi ka teisi IT-majasid ning arutleti Eesti IT-maastiku üle.

## Palju õnne! Liina Areng sai Eesti Vabariigi presidendilt Valgetähe IV klass teenetemärgi!

Foto: Riigi Infosüsteemi Amet

Üheksa aastat on Liina aidanud maailmale rääkida ja tutvustada e-Eesti edulugu. On äärmiselt tore, et Liina panust on märgatud. Viimase viie aasta jooksul on ta aidanud käivitada Euroopa Liidu esimesed suured projektid nagu Cyber4Dev ning EU CyberNet. Liina eestvedamisel avas RIA mullu kevadel küberturvalisuse keskuse (LAC4) Dominikaani Vabariigis, mis sisuliselt töötab kui e-Eesti saatkond Kariibi ja Ladina-Ameerika piirkonnas.

"Liina on sellise tunnustuse, äramärkimise auga välja teeninud. Ta teeb tööd suure pühendumusega ning on alati väga positiivne ning inspireeriv. „Kes teeb, see jõuab", Liina ilmestab sellist vana ütlust suurepäraselt," ütles RIA peadirektor Margus Noormaa.

"Olen hämmingus, üllatunud. Ma ei osanud seda kuidagi oodata. Sain ise teenetemärgist teada ühtäkki laekuma hakanud sõnumite ja kõnede järgi. Olen väga tänulik ja liigutatud. See teenetemärk kuulub kogu minu tiimile, kellega koos olen saanud olulisi asju ellu viia, kogu RIAle," sõnas värske teenetemärgi omanik, Liina Areng.

## Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT) on nüüdsest sertifitseeritud ISO 27001 infoturbestandardi nõuete kohaselt

Eesti riigi suurima IT-arenduskeskusena tuntud Siseministeeriumi infotehnoloogia- ja arenduskeskus (SMIT) on nüüdsest sertifitseeritud ISO 27001 infoturbestandardi nõuete kohaselt.

SMITi peadirektori Mart Nielseni sõnul on ISO 27001 kvaliteedimärk, mis kinnitab et nende infoturve vastab kõrgeimatele rahvusvahelistele standarditele ning et digiriik püsib tugeval vundamendil. „SMITi jaoks on see suur tunnustus, sest infoturve on meie toodete ja teenuste alustala."

„Kliendid, partnerid ja järelevalveasutused saavad olla kindlad, et SMITil on kõrgeimal tasemel süsteemid riskide tuvastamiseks, juhtimiseks ja maandamiseks," selgitas ta. „Ja ka iga Eesti inimene saab olla kindel, et meie teenused on turvalised — olgu selleks rahvastikuregistri andmed, juriidilised toimingud või isikut tõendavad dokumendid".

Mis on edu võti? Eelkõige on sellise üle-ettevõttelise projekti puhul oluline juhtkonna ja töötajate toetus, sh koostöö. ISO infoturbestandard ei hõlma üksnes infoturbe või infosüsteemidega seotud teemasid, vaid tegelikult kogu organisatsiooni alates personalist ja hangetest lõpetades ruumide füüsilise turvalisusega. Sinna vahele jäävad kõik muud teemad, nagu varahaldus, juurdepääsud ja logimine, seadmete haldus, arendus jne.

Nielsen tõi välja, et infoturbestandardi sertifikaadi taotlemine oli kogu organisatsiooni ühine saavutus. „Tegemist oli aasta läbi väldanud protsessiga, mis päädis auditi eduka läbimisega. Audiitorid kiitsid meie organisatsiooni küpsust ja ettevalmistust ning tegid ka täiendavaid ettepanekuid, mille abil infoturbe korraldus veelgi paremaks saada," kirjeldas peadirektor.

„Küberkuritegevus on tõusuteel ja kurikaelte meetodid muutuvad samm sammult kavalamateks — peame iga päev selle nimel pingutama, et pidevalt sammuke eespool olla. Tööprotsesside lihvimine, tehniliste vahendite arendamine ja inimeste kompetentside tõstmine on selle lahutamatuks eelduseks," märkis Nielsen.

Selle aasta alguses vahetas aastaid kehtinud ISKE standardi välja uus Eesti infoturbestandard (E-ITS), mille Eesti avaliku sektori asutused peavad rakendama. Valitsuse määruse kohaselt tohivad aga asutused E-ITSi asemel rakendada ka rahvusvahelist ISO/IEC 27001 infoturbestandardit. ISO on ulatuslikum ja rakendamine suuremat pingutust nõudev, samas SMITi teenuste kriitilisus kallutas kaalukeele just ISO standardi kasuks.

StartUp Estonia

## Startup Estonia sTARTUp Day üritus küberkogukonnale

Paneeldiskussioon “Cybersecurity for businesses — what do we need to be ready for in 2023?”

16. märtsil algusega kell 14.45 toimub sTARTUp Day ürituse raames paneeldiskussioon teemal “Cybersecurity for businesses — what do we need to be ready for in 2023?” Lydia Hotel sündmuskeskuses.

Tänapäeva küberturvalisuse maailm on pidevalt muutuv. Ettevõtted seisavad silmitsi uute küberturvalisuse ohtudega peaaegu iga päev, rõhutades selgelt kõrgemate turvameetmete vajadust, üksikasjalikke riskihinnanguid ja pädevate spetsialistide kaasamist.

Arutelu alla tulevad erinevad teemad nagu ennetavad meetmeted, kuidas leevendada riski kõrgemal tasemel ja integreerida küberturvalisus igapäevases äris? Mis juhtub, kui ettevõtet rünnatakse ja kuidas lahendada kahju minimaalse rahalise ja mainekaotusega? Kuidas on loodud usaldus alustavate ettevõtete ja ettevõtete suhtes, kes pakuvad küberturbeteenuseid ja teadmisi ning kuidas saaks Eesti iduettevõtted edendada veelgi rohkem usaldust?

Paneelis osalevad: Taavi Veskimägi (Elering), Andrus Kivisaar (CybExer Technologies), Jürgen Erm (Cybers).

Moderaator on Gert Jervan (TalTech)

Lisainfo siit.

## Küberturbe häkaton

21.-23.04 toimub kood/Jõhvi uhiuues õppehoones kood/Jõhvi ja Startup Estonia koostöös korraldatav küberturbe häkaton.

Ürituse eesmärk on meie ühise küberruumi kindlustamine läbi erinevate valdkonna probleemide lahendamise ning 48 tunni jooksul jõuda prototüüpideni.

Üritusele registeerimine avaneb 12. märtsil ning osalema oodatakse huvilisi mitmetelt elualadelt: arendajad, disainerid, programmeerijad, äriarendajad, turundajad, visionäärid ja küberturbe huvilised - kõik on oodatud.

Kui soovid häkatonil osaleda partnerina, kirjuta karin@kood.tech

EASi ja KredExi ühendasutus

## Eesti kosmose küberharjutusväljaku ideekorje infoseminar

6. märtsil kell 14-16 toimub Eesti kosmose küberharjutusväljaku ideekorje infoseminar!

Tänu Eesti osalemisele ESA valikprogrammis ARTES 4.0 ja Space Systems for Safety & Security (4S) programmiliinis, avanevad meile uued võimalused kosmose küberjulgeoleku valdkonnas. ESA ja kosmosekogukond vajavad Eestisse rajatava uue kosmose küberharjutusväljaku näol uusi tehnoloogiaid nii kosmosevarade ja -andmete kaitsmiseks, kui õppuste ja harjutuste läbiviimiseks.

Ideede ja kontseptuaalsete lahenduste kogumiseks uue kosmose küberharjutusväljaku jaoks avab Eesti Kosmosebüroo ideekorje.

Registreeri end 6.märtsil toimuvale infoseminarile juba täna aadressil kosmos@eas.ee.

## TalTechis tunnustati küberjulgeolekualast õppe-, teadus- ja teavitustööd

Eesti Vabariigi 105. aastapäeva aktusel tunnustas Tallinna Tehnikaülikool 2022. aasta parimaid teadlasi, õppejõude, tugitöötajaid ning märkis ära parimad teadusartiklite autorid ja tudengid ning kuulutas välja aasta kultuuri-, spordi- ja tudengiteo. Eelmise aasta parimate õppejõudude hulgas märgiti ära küberkaitse professor Olaf Maennel.

Samuti tunnustas vabariigi aastapäeva eel oma aasta töötajaid IT-teaduskond. Aasta teadlased on professor Hayretdin Bahsi, kelle teadustöö keskendub masinõppe rakendamisele küberkaitses ja digitaalsele ekspertiisile ning professor Ahto Buldas, kelle teadustöö keskendub plokiaheltehnoloogiale ja selle rakendamisvõimalustele. Aasta õppejõud on õppeaine monitooringulahendused küberkaitses õppejõud dr Risto Vaarandi.

Aasta programmijuht on küberkaitse magistikava juht professor Rain Ottis.

Samuti tunnustati tänukirjaga TalTech IT Kolledži vanemteadurit Birgy Lorenzit silmapaistva panuse eest küberturvalisuse valdkonna populariseerimisel noorte seas.

## Algas vastuvõtt Tallinna Tehnikaülikooli

1. märtsil algas sisseastumisavalduse vastuvõtt Tallinna Tehnikaülikooli, kus küberturvalisusealane õpe toimub nii bakalaureuse- kui ka magistritasemel.

Küberturbe tehnoloogiad (Cyber Security Engineering) on bakalaureusetaseme õppekava TalTech IT Kolledžis. Õppekava on laiapõhjaline ja praktilise suunitlusega, mistõttu on kõik ainetes omandatavad teoreetilised teadmised tugevalt toetatud praktilise õppega. Küberkaitse (Cybersecurity) on Tallinna Tehnikaülikooli ja Tartu Ülikooli ühine magistritaseme õppekava, kus tudengid võtavad kursuseid mõlemast ülikoolist. Küberkaitse ja digitaalse ekspertiisi peaerialade õpe toimub valdavalt Tallinnas ning krüptograafia peaeriala õpe toimub valdavalt Tartus. Õppekava koordineerib TalTech küberkriminalistika ja küberjulgeoleku keskus.

Mõlemal õppekaval on õppekeel inglise keel ning nominaalkoormusega õpe on tasuta. Vastuvõtt 2023/2024. õppeaastaks on avatud kuni 4. juulini kl 12.

## Küberturvalisuse veebiseminaride sarjas esineb Ebelechukwu Nwafor Villanova ülikoolist

7. märtsil algusega kell 17 esineb Ebelechukwu Nwafor Villanova ülikoost teemal „Social Engineering Attacks". Ettekanne uurib erinevaid sotsiaalse manipulatsiooni tüüpe ja rünnakutes kasutatavad tehnikad. Samuti käsitletakse, kuidas rünnakuid tuvastada, ennetada ning paremini end ja oma organisatsiooni kaitsta. Veebiseminar toimub Teamsis ja on ingliskeelne.

Täpsem info ja registreerimine siin.

## Cyber4Schools projekt kutsub koole testima uut mängu

TalTech ja Pelgulinna Gümnaasium Eestist osalevad partneritena Euroopa Liidu Erasmus+ projektis Cyber4Schools. Koostöö raames luuakse veebimäng õpilastele, mille eesmärk on harida lapsi ja noori küberturvalisuse alal. Projekt kutsub üles õpetajaid, koolitajaid ja didaktikuid osalema veebimängu testimisel.

Rohkem infot projekti kodulehel.

Kontakt: birgy.lorenz@taltech.ee

E-riigi Akadeemia

## eGA tõhustab Moldova kaitsejõudude küberturvet

E-riigi Akadeemia panustab läbi Euroopa Rahurahastu (EPF) Moldova kaitsejõudude küberkaitseõpesse viies läbi vastavaid õppuseid tuvastamaks infosüsteemidesse tungimist ja tõrjumaks küberrünnakuid. Projekti raames hangitakse ja tarnitakse ka vajalikke küberturvalisust parendavaid seadmeid.

EGA tegevusi Moldovas kajastas Aktuaalne Kaamera 27. veebruaril.

Lisainfo siit.

Cybernetica

## Cybernetica aitab kaasa Euroopa esimese Hydrogen Valley projekti BalticSeaH2 arendamisele

Sellest aastast algab Läänemere ümber viieaastane Hydrogen Valley projekt (BalticSeaH2) 44 partneri vahel: üle Balti riikide, Soome, Rootsi, Taani, Norra, Poola, Saksamaa ja Prantsusmaa. Projekti kaasrahastab EL Horizon Europe programm kogueelarvega 33 miljonit eurot. Projekti eesmärk on luua Euroopas esimene oluline piiriülene vesinikuorg, mis võimaldab vähendada erinevate tööstusharude CO2 emissiooni ja piirkonna isemajandamist.

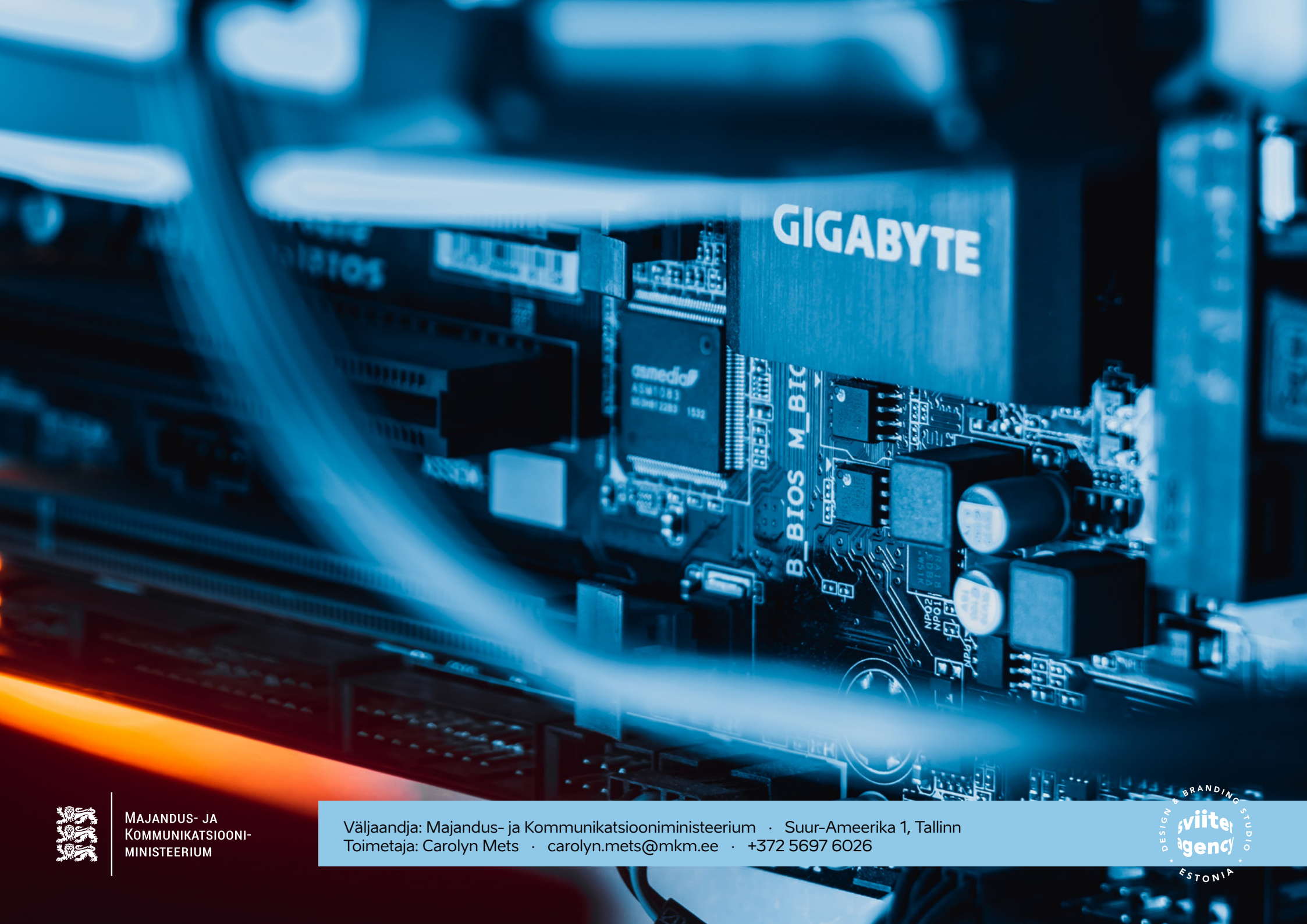
Cybernetica töötab välja vesiniku veebituru kontseptsiooni H2Pool: veebiplatvormi kontseptsioonina, mis on vesiniku sidusrühmade jaoks ressurss. *Secure-by-Design* arhitektuur on välja töötatud platvormi jaoks, mis sisaldab krüptograafilisi turvatehnoloogiaid konfidentsiaalsuse (krüptimine, turvaline andmetöötlus), terviklikkuse ja töökindluse tagamiseks. Süsteemi ülesehituse kinnitamiseks kasutatakse olemasolevate andmete analüüsil ja modelleerimisel põhinevate süsteemi katseandmete loomiseks andmete sünteesi tehnikaid.

“See on ambitsioonikas projekt, millel on mõjukad tulemused,” kommenteeris Cybernetica energeetikasektori juht Marko Petron. “Cybernetica kasutab oma pikaajalist kogemust tarkvara, privaatsus- ja küberjulgeolekulahenduste loomisel energiavaldkonnas ning tugineb oma töös olemasolevale elektri paindlikkuse turu lahendusele,” ütles Petron.

Cybernetica on energialahendusi arendanud üle 10 aasta ning panustanud paljudesse kõrgetasemelistesse mõõtmisandmeid kasutavatesse projektidesse — nt Elering Estfeed süsteem ja e-Eleringi portaal. Globaalsed projektid hõlmavad tehnilisi lahendusi üleeuroopalistele elektri paindlikkuse turu konsortsiumidele INTERRFACE (kaasatud 5 riiki, eelarve 20 miljonit eurot) ja OneNet (kaasatud 23 riiki, eelarve 28 miljonit eurot).

Cybernetica eesmärk on luua energiasektoris uuenduslikke digitaalseid lahendusi, mis kasutavad turvalise e-riigi kontseptsioone ning teadus- ja arendusressursse.

Lisainfo Cybernetica kodulehel.




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 ESTONIA