Riikliku küberturvalisuse uudiskiri

2023-04

Majandus- ja kommunikatsiooniministeerium

Valminud on „Eesti Infoturbestandard (E-ITS) ABC“ sissejuhatav e-kursus

Riigi Infosüsteemi Amet

RIA eestvedamisel valmis uus kübertest

Majandus- ja Kommunikatsiooniministeerium

Küberturvalisuse kulude arvestamise mudel

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Majandus- ja Kommunikatsiooniministeerium

Küberturvalisuse kulude arvestamise mudel 3

NATO innovatsioonivõrgustiku esimesed kiirendid avatakse tänavu Eestis, Itaalias, Taanis ja USAs 3

Valminud on „Eesti Infoturbestandard (E-ITS) ABC" sissejuhatav e-kursus 3

Riigi Infosüsteemi Amet

RIA eestvedamisel valmis uus kübertest 4

Algas küberkogukonnale suunatud uus üritustesari RIA CyberMeetUp 4

RIA kompetentsikeskust Dominikaanis väisasid kõrged ELi esindajad 5

RIA küberturvalisuse teenistusest sai küberturvalisuse keskus 5

ITL andis RIAle aasta teo tiitli 6

Välisministeerium

Tallinna Küberdiplomaatia Suvekool 6

ÜRO Open-Ended Working Group 7

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit

Eesti tehnoloogiasektor tunnustas aasta tegijaid, kes aitavad kriitilisel ajal kaasa julgeoleku tagamisele 7

TalTech

TalTech on astunud olulisi samme merenduse küberjulgeoleku vallas 8

Küberturvalisuse veebiseminaril räägitakse sel korral Fulbright´i programmist ja naistest tehnoloogiasektoris 8

Küberkaitse magistriõppe infotund 8

Tartu Ülikool

IT Academy Research Summit 18.-19.mail Tartus 9

Kood Jõhvi

Küberturbe häkaton 9

E-riigi Akadeemia

eGA parendab Moldova kaitsejõudude kübervõimekust 9

CybExer Technologies

CybExer Technologies korraldab Helsinkis küberõppuse Cyber Resilience Helsinki 2023 10

Cybernetica

Cybernetica ja ENISA sõlmivad eIDAS määruse raames kolmeaastase raamlepingu 10

Cybernetica vanemteadur Peeter Laud sai Eesti Teadusagentuurilt uurimisgrandi uurimaks hajusidentiteedi loomist 11

European Telecommunications Standards

ETSI IoT konverents 2023: IoT Technologies for Green and Digital Transformation 12

NIS Directive User Community

Teine NISDUC konverents: From NIS to NIS 2.0 — A path to take 12

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

Küberturvalisuse kulude arvestamise mudel

Riikliku küberturvalisuse osakonna poolt tellitud ja Ernst&Youngi meeskonna väljatöötatud küberturvalisuse kulude arvestamise mudel on peagi valmis.

Mudeli eesmärk on saada kiiresti objektiivne ülevaade valdkonna kuludest ja hinnata kui otstarbekad on kulud eesmärgi saavutamisel. Lisaks võimaldab mudel välja arvestada, milline peab olema minimaalne küberturvalisuse eelarve, et asutusel oleks tagatud minimaalne vajalik turvalisus.

31. märtsil esitles Ernst&Youngi meeskond väljatöötatud mudelit, mis muu hulgas vastab kolmele seatud võtmekriteeriumile:

- mudel arvestab praegust riigi raamatupidamissüsteemi ja võimaldab minimaalsete muudatustega saada objektiivne ülevaade küberturvalisuse kuludest;
- lahendus ei suurenda oluliselt halduskoormist ega nõua märkimisväärseid arenduskulusid;
- mudel on rakendatav kiiresti.

Järgmiste sammudena on plaanitud mudeli piloteerimine ja täiendamine, et tagada hilisem sujuv rakendamine riigiasutustes.

Paralleelselt mudeli piloteerimise ja arendamisega jätkub koostöö ENISAga, kes on kogunud sarnaseid andmeid erasektori kohta juba mitu aastat. Kogemusi arvesse võttes saame luua veelgi parem mudel ja parandada küberturvalisust.

Küberturvalisuse kulumudelit plaanime tutvustada kõigile huvilistele. Täpsem aeg on selgumisel, kuid huvilised saavad endast teada anda meilile carolyn.mets@mkm.ee.

NATO innovatsioonivõrgustiku esimesed kiirendid avatakse tänavu Eestis, Itaalias, Taanis ja USAs

NATO DIANA innovatsioonikiirendite võrgustiku esimesel pilootaastal alustab tööd viis esimest kiirendit, mille hulka osutus valituks ka Eesti. Ettevõtetel on võimalik kiirenditesse kandideerida tänavu suvel, veel enne Vilniuses toimuvat NATO tippkohtumist.

Eesti kiirendit hakkavad ellu viima Teadus- ja ärilinnak Tehnopol koos Tartu Teaduspargi ja ärikiirendi Startup Wiseguys'iga. Kiirendi eesmärk on toetada süvatehnoloogia iduettevõtteid, mis panustavad riiklikku julgeoleku ja kaitsevaldkonda, viies kokku andekad innovaatorid ja uute tehnoloogiate lõppkasutajad. Kiirendis arendatakse kahese kasutusega tehnoloogiaid, st tehnoloogiad on kasutatavad nii tsiviil- kui ka kaitseotstarbel. NATO kiirendi Eestis võimaldab eelkõige Eesti ja lähiregiooni iduettevõtjatel arendada oma toodet ja ärimudelit ning leida koostööpartnereid alliansi ülesel kaitseturul, mis on tavapäraselt suletud ja kõrge sisenemisbarjääriga.

DIANA kiirendite võrgustikuga ühendatakse mitu siinset uute tehnoloogiate testimiskeskkonda: Tartu Ülikool, TalTech, sihtasutus CR14, Kaitseväe Akadeemia, ettevõte Milrem Robotics, Lennuakadeemia ja Sisekaitseakadeemia. Samuti saavad kõik kiirendis osalevad ettevõtted kasutada ligi sadat NATO riikide testimiskeskust.

Esimesel pilootaastal valitakse kõikide kiirendite peale välja mõnikümmend iduettevõtjat, kes saavad NATO-lt rahalise toetuse oma idee arendamiseks. DIANA kiirendiprogramm koosneb kahest kuuekuulisest etapist. Poole aasta järel jätkavad igas kiirendis vaid kõige lootustandvamad idufirmad, kes saavad selleks täiendavat toetust.

Eelmise aasta lõpus kinnitas NATO DIANA direktorite kogu strateegilised fookusvaldkonnad aastaks 2023, milleks on energia varustuskindlus, turvaline andmevahetus, tuvastamine ja seire. Suve alguses kuulutatakse iduettevõtetele välja konkurss neis fookusvaldkondades lahenduste pakkumiseks, suve jooksul valitakse välja parimad, kellel on sügisest võimalik alustada tööd kiirendiprogrammides.

Valminud on „Eesti Infoturbestandard (E-ITS) ABC" sissejuhatav e-kursus

Millised on infoturbe eesmärgid? Kuidas Eesti Infoturbestandard (E-ITS) aitab asutuse ärieesmärkide saavutamisel? Millal hakata infoturvet planeerima? "Eesti

Infoturbestandardi (E-ITS) ABC" e-kursus vastab just nendele aga ka paljudele teistele olulistele küsimustele.

Avaliku sektori töötajatele ja olulise teenuse osutajatele peab E-ITSi kasutamine saama tööprotsessi loomulikuks osaks. MKM ja RIA koostöös valminud sissejuhatav e-kursus pakub võimaluse omandada esmane arusaam standardi olemusest, portaalist ja annab vajalikud suunised alustamiseks.

Kursuse läbimine võtab kuni 60 minutit ning on kõigile huvilistele tasuta.

Rohkem infot Digiriigi Akadeemia lehelt.

RIA eestvedamisel valmis uus kübertest

Märtsi lõpus valmis uus kübertest.

Kübertest jaguneb sisult kaheks. Esmalt tuleb kasutajal läbi töötada koolituse osa, mis katab 12 olulisemat teemat. Nende juurest leiab ka hoiatavaid näiteid päriselust, sh õngitsuskirju ja pettuseid, mida on CERT-EE meeskonnale uurimiseks saadetud.

Kursuse lugemismaterjalide lugemise järel tuleb sooritada test, pärast mida saab iga kasutaja teada oma punktisumma ning tagasiside õigete ja valede vastuste kohta.

Kursusel saab vastused küsimustele, kuidas tunda ära õngitsuslehti ja -kirju, millised on levinumad petuskeemid, kuidas seadistada turvaliselt kodune WiFi-võrk, teha turvaliselt kaugtööd jmt. Kõik need igapäevased teemad tasub aeg-ajalt üle korrata ja kübertest on selleks hea võimalus.

Kübertesti eelkäija, Cybexeri arendatud digitest, oli viimane avaliku sektori ja olulise teenuse pakkujatele (nt meditsiinitöötajad) mõeldud õppeplatvorm, mille abil said kasutajad testida enda teadmisi. Läinud aasta juunis lõppes RIA ja digitesti arendaja koostööleping, mille järel otsustasime ise RIAs testi sisusse panustada ja selle koos arendajaga välja töötada.

Test on kohustuslik riigiasutustele. Elutähtsa teenuse pakkujatele, perearstidele ja teistele organisatsioonidele on test soovituslik.

Kui soovite Kübertesti kasutusele võtta, tuleb täita Kübertesti kasutamise taotlus. Asutuse esindusõigusliku isiku digiallkirjastatud taotlus tuleb edastada Riigi Infosüsteemi Ametile.

Koos taotlusega tuleb saata ka asutuse töötajate nimekiri, kes hakkavad Kübertesti kasutama.

Test asub Moodle´i keskkonnas.

Kõik Kübertesti teemalised päringud või küsimused, sh täidetud Kübertesti kasutamise taotlused saab edastada aadressile: kybertest@kybertest.ee

Algas küberkogukonnale suunatud uus üritustesari RIA CyberMeetUp

21. märtsil toimus Tallinnas Palo Alto klubis uue üritustesarja RIA CyberMeetUp avapauk. Esimesel kokkusaamisel räägiti, milline on viimane seis Eesti küberruumis ning tutvustati uusi algatusi ja projekte.

RIA CyberMeetUp on kogukonnaüritus, mis on mõeldud inimestele, kes panustavad küberturbesse ükskõik, mis moel. Selle eestvedajaks on RIA teaduse ja arenduse koordineerimisosakonna juht Lauri Tankler. "Meie jaoks on oluliseks märksõnaks avatus. Et igaüks, kes tunneb, et ta on Eesti küberkogukonna liige, leiaks endale sõpru ja liitlasi, koostööpartnereid ja lahingukaaslasi," ütles Lauri. "See tähendab ka, et me oleme avatud ingliskeelsele seltskonnale, humanitaar-, äri-, ja sotsiaalteaduste taustaga küberentusiastidele ja nendele, kes on alles varbaga kübervaldkonna vett katsumas."

Pärast Lauri sissejuhatust astus hubase Palo Alto

klubi lavale analüüsi- ja ennetusosakonna juht Märt Hiietamm, kes andis ülevaate olukorrast küberruumis. Seejärel võttis mikrofoni üle külalisesineja Carry Kangur, kes veab NATO küberkaitsekoostöökeskuses maailma suurima küberõppuse Locked Shieldsi korraldamist. Carry rääkis, mida tänavuselt õppuselt oodata.

Tunniajase esitluste osa võttis kokku uuesti Lauri Tankler, kes kõneles ligi 60 kohaletulnule Euroopa küberkompetentsikeskuse Eesti rakukese (NCC-EE) tegevustest ehk kuidas jagab RIA koos EASi ja KredExi ühendasutusega kübertoetusi ja kavatseb panustada taoliste ürituste, aga ka koolituste, laagrite, uuringute ja muude tegevustega Eesti kübersektori arengusse.

Üritustesari toimub inglise keeles ja hakkab toimuma kord kuus, seda kaasrahastab Euroopa Liit ja Euroopa küberkompetentsikeskus. **Järgmine CyberMeetUp toimub 13. aprillil samuti Palo Alto klubis. Ürituse info on leitav Facebookis.**

RIA kompetentsikeskust Dominikaanis väisasid kõrged ELi esindajad

Märtsi lõpus külastas ELi välisasjade ja julgeolekupoliitika kõrge esindaja Josep Borrell Fontelles RIA küberkompententsi keskust (LAC4) Dominikaani Vabariigis.

Kõrgetasemelisel kohtumisel osalesid lisaks Borrellile Eesti RIA küberturvalisuse keskuse juht Gert Auväärt ja Dominikaani Vabariigi peaminister Joel Santos.

Borrell märkis, et LAC4 keskus näitab Euroopa Liidu pühendumust koostööle Ladina-Ameerika ja Kariibi mere piirkonna riikidega. „Mul on hea meel öelda, et tegu on regiooni esimese küberkompetentsi keskusega, mille EL on loonud. Keskuse sünd ilmestab, et siinsed riigid, eriti Dominikaani Vabariik, digitaliseeruvad kiiresti ning see toob kaasa innovatsiooni ja hüved ühiskonnale ning demonstreerib, et jagame samu väärtusi. Ta lisas, et küberkeskus on heades kätes, sest kui keegi maailmas teab midagi küberturvalisusest, siis nendeks on eestlased.

RIA peadirektori asetäitja Gert Auväärt märkis, et küberturvalisusele rõhumine on aina vajalikum ning see on ka Eesti sõnum olnud. „Mul ja kogu RIA-l on hea meel, et meil on võimalus nii lähedalt ja suurelt panustada Ladina-Ameerika ja Kariibi mere piirkonna küberturbe tõstmisesse ning ise samal ajal juurde õppida.”

LAC4 aitab kaasa küberjulgeolekualase hariduse ja võimekuse parandamisele, parandab koostalitlusvõimet, küberruumi võimekust, teadus- ja arendustegevust ning loob riiklikud küberjulgeolekustandardid Ladina-Ameerika ja Kariibi mere piirkonna riikides. Keskust viib ellu EU CyberNet projekt, mida rahastab Euroopa Liit. EU CyberNeti projekti elluviija on RIA.

RIA küberturvalisuse teenistusest sai küberturvalisuse keskus

RIA põhimääruse muudatuse tulemusel kannab küberturvalisuse teenistus nüüdsest küberturvalisuse keskuse nime.

Muudatus on pigem vormiline kui sisuline ning üksus jätkab oma seniste ülesannete täitmisega, samuti koosseisuga. Keskus küll kasvab, kuid uusi ülesandeid, kompetentse või struktuurimuudatusi praegune nimemuutus kaasa ei too.

Küberturvalisuse keskus ehk inglise keeles

National Cyber Security Centre (lühidalt NCSC) on riigi kesksete küberasutuste tähiseks. Need on asutused, mis tegelevad oma riigi avaliku sektori ja kriitilise infrastruktuuri küberturvalisusega ning on võrgu- ja infosüsteemide turbe direktiivi (NIS) mõistes küberturvalisuse pädevad asutused ja kontaktpunktid — nii nagu seda on Eestis RIA, sh küberturvalisuse keskus.

Selliseid asutusi on Euroopaski mitu ning Eesti oli seni üks väheseid riike, kus keskuse mõiste veel kasutusel ei olnud. Selle aasta alguses alustas Läti kaitseministeeriumi allasutusena tööd CERT-LVIe baseeruv küberturvalisuse keskus, mis hakkab tegelema lisaks intsidentide haldamisega ka muude valdkonna teemadega. Sarnase ülesehitusega ja ülesannetega keskused on veel Leedus, Soomes, Rootsis ja Taanis.

„Küberturvalisuse teenistuse ümbernimetamine keskuseks on mõistlik just seetõttu, et oleksime selgemalt pildis valdkonna omaniku ja kompetentsikeskusena nii Eestis kui ka väljaspool. Selline lähenemine annab rahvusvahelises suhtluses parema selguse ning lisab nimena ka väärtust selle töö sisule, mida igapäevaselt teeme," ütles RIA juht Margus Noormaa.

Senine teenistus keskusena jätkab samade ülesannete täitmisega, milleks on küberruumi 24/7 seire intsidentide käsitlemine, DDoS rünnakute ja riigivõrgu kaitse, analüüs, ohuteavitus, ennetus, järelevalve, standard, teadus ja arendustegevus, kriitilise infra kaitse, koolituses ja õppused, kriisi haldamine ja küberreservi võimekuse tagamine. Keskust juhib RIA peadirektori asetäitja Gert Auväärt.

ITL andis RIAle aasta teo tiitli

23. märtsil kuulutas Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) välja aasta tunnustuse saajad, kes on aidanud kriitilisel ajal kaasa julgeoleku tagamisele. Aasta teo tiitli pälvis RIA küberturbe meeskond Eesti küberjulgeoleku tagamise eest.

Lisainfo RIA koduleheküljel.

Välisministeerium

Töötuba Rahvusvahelise Õiguse ja Küberoperatsioonide teemal

30.–31.03 toimus IV Tallinna Töötuba Rahvusvahelise Õiguse ja Küberoperatsioonide teemal.

Töötoas võtsid sõna rahvusvahelise humanitaarõiguse eksperdid Dr Kubo Mačák Rahvusvahelisest Punasest Ristist (ICRC) ja Dr Heather Dinniss Rootsi Kaitseülikoolist. Lisaks ettekannetele ja diskussioonidele arutati ka praktilisi stsenaariumeid.

Üritusel osales 58 inimest 26 riigist. Töötoa raames käsitleti järgnevaid teemasid: rünnaku mõiste; objektid: kahesugune kasutus (dual use) ja andmed; relvastatud konfliktide ajal sõjategevuses osalenud isikute kategooriad. Töötoas osalenud olid ühel meelel, et rahvusvaheline sõjaõigus kehtib ka küberruumis ning ei soodusta sealjuures küberruumi militariseerimist.

Tallinna Küberdiplomaatia Suvekool

12.–16.06 korraldab Välisministeerium koostöös eGA, ESTDEV-i ja DG INTPA-ga neljanda Tallinna Küberdiplomaatia Suvekooli.

Suvekool koosneb mitmetahulisest õppeprogrammist 50 osalejale, kellest pooled on nn. globaalse lõuna ja pooled lääneriikide esindajad. Viiepäevase programmi käigus käsitletakse laia ringi teemasid:

- digitaliseerimine,
- rahvusvaheline küberjulgeolek ja riikide vastutustundlik käitumine,
- küberjulgeoleku raamistike jõustamine,
- kübervõime arendus ja küberkerksuse parandamine,
- küberõppus.

Koostöös eGA ja ESTDEV´iga on käimas kontseptsiooni välja töötamine, võimalike esinejate kaardistamine ning korralduslike aspektide kokku leppimine.

ÜRO Open-Ended Working Group

6.-10.03 toimus ÜRO Open-Ended Working Group (OEWG), kus üheks olulisemaks uueks aspektiks on üha suurenev riikide aktiivne osalemine — ohtude teemal võttis sõna umbes 60 ja rahvusvahelise õiguse teemal umbes 40 riiki.

Eesti korraldas koos Indoneesia, Rwanda ja Šveitsiga eduka veereürituse rahvusvahelise humanitaarõiguse teemal, mis kujunes ootamatult nii populaarseks, et saal oli puupüsti täis. OEWG raames oli märkimisväärne, et Venemaa pani lauale küberjulgeoleku õiguslikult siduva rahvusvahelise lepingu maketi. Eesti on seisukohal, et eelkõige tuleb kohaldada olemasolevat rahvusvahelist õigust ja konventsiooni läbirääkimisteks ei ole aeg veel küps.

Eesti tehnoloogiasektor tunnustas aasta tegijaid, kes aitavad kriitilisel ajal kaasa julgeoleku tagamisele

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) kuulutas välja sektori aasta tunnustuse saajad.

Aasta Tegu 2022 on Eesti küberjulgeoleku tagamine — saajaks Riigi Infosüsteemi Ameti (RIA) küberturbe meeskond; Aasta Tegija 2022 tiitleid anti kaks: Tarbijakaitse ja Tehnilise Järelevalve Ametile (TTJA) otsustava tegutsemise eest Eesti inforuumi kaitsmisel ning maailmanäituse Dubai EXPO 2020 meeskonnale Eesti eduka esindatuse tagamise eest; Aasta Läbimurdja 2022 tiitli sai kõrgtehnoloogiaga tegelev idufirma GScan.

ITL-il on kombeks oma sünnipäeval tunnustada sektori auhinnaga neid inimesi, kelle ideed, algatus või tegevus on oluliselt mõjutanud meie valdkonda Eestis või Eesti elu laiemalt.

ITL-i Aasta Tegu tähistab konkreetset algatust, millega vastaval aastal IT-valdkonda positiivselt üllatati. Tunnustuse sai RIA küberturbe meeskond Eesti digiökosüsteemi probleemideta toimimas hoidmise eest olukorras, kus küberründed on mitmekordistunud

ITL-i „Aasta Tegija 2022“ tunnustuse sai TTJA otsustava tegutsemise eest Eesti inforuumi kaitsmisel Venemaa sõjapropaganda eest koostöös oma partneritega.

ITL-i „Aasta Tegija 2022“ tunnustuse sai Dubai EXPO 2020 meeskond Eesti eduka esindatuse tagamise eest maailmanäitusel Dubai EXPO 2020.

ITL-i „Aasta Läbimurdja 2022“ tunnustuse sai GScan äriarenduse ja teadusinnovatsiooni sümbioosis tekkinud kõrgtehnoloogilise lahenduse eest, mille potentsiaal on nii sektorite ülesena kui ka globaalses mastaabis suurem kui praegu arvatagi oskame. Selleks on looduslikul müüonkiirgusel põhinev tomograaf, mille abil on näiteks piiripunktides võimalik tuvastada pagasis olevaid keelatud ning ohtlikke esemeid ja aineid.

Aasta auhindade kandidaate said esitada ITL-i liikmed ning koostööpartnerid, lõpliku otsuse tegi ITL-i juhatus.

ITL on info- ja kommunikatsioonitehnoloogiaga tegelevaid ettevõtteid ja organisatsioone ühendav erialaliit. Liidu peamine eesmärk on soodustada IKT sektori äri Eestis, pakkuda lisandväärtust Eesti majandusele ning hõlbustada ettevõtete vahelist koostööd.

Varasemad auhinnasaajad.

Lisainfo ITL koduleheküljel.

Foto: Sadu Photo

TalTech on astunud olulisi samme merenduse küberjulgeoleku vallas

Tallinna Tehnikaülikooli Eesti Mereakadeemia on asutanud merenduse küberturbe keskuse, mis on oluline samm turvalisema merendussektori suunas.

Keskuse eesmärk on teha tipptasemel merenduse küberjulgeoleku alast teadustööd ja pakkuda väljaõpet, et tagada ohutu ja turvaline merendustegevus.

Merenduse küberturbe keskus loodi, et adresseerida kasvavat vajadust küberturvalisuse järele merenduses, mis suuresti toetub tehnoloogiale — sidelahendused, navigeerimine ja lasti käitlemine. Kuid aina suurem sõltuvus tehnoloogiast on muutnud sektori ka küberohtude suhtes haavatavaks.

Keskus kutsuti ellu pikalt kavandatud idee tulemusena ja sellesse on kaasatud juba väljakujunenud IT- ja küberjulgeolekualased uurimisvõimalused TalTechis ning Mereakadeemia merendusalased teadmised. Eesti tugev kohalolek ja maine mõlemas valdkonnas ning keskuse loomine annab tunnistust Eesti pühendumusest tegeleda küberjulgeoleku väljakutsetega ka merenduses.

Merenduse küberturbe keskus teeb tihedat koostööd TalTechi küberkriminalistika ja küberjulgeoleku keskusega. Kahe keskuse koostöö aitab ületada lõhet kahe valdkonna vahel ning pakkuda terviklikku ja kohandatud lähenemisviisi merenduse küberjulgeoleku valdkonnale.

Keskus hakkab toimima uurimis-, haridus- ja koolituskeskusena, et arendada merendusspetsialistide ning tulevaste ja juba töötavate meremeeste küberjulgeolekualaseid oskusi ja teadmisi. Samuti keskendub keskus strateegiate väljatöötamisele, et kaitsta infrastruktuuri, laevu ja sadamaid küberrünnakute eest, tagades merenduse ohutus ja turvalisus tulevikus. Lisaks loob keskus koostöösidemeid erasektoriga, et tagada teadustöö ja koolituse vastavus sektori vajadustele.

Keskust juhtima asuv uus professor asub peagi Mereakadeemias tööle. Väljavalitud kandidaat toob kaasa laialdased teadmised ja kogemused nii merenduse kui ka küberjulgeoleku vallas, võimaldades keskusel saavutada oma eesmärgid ja kujuneda rahvusvaheliselt tunnustatud teaduskeskuseks.

Lähem info MariCybERA projekti kohta siit.

Küberturvalisuse veebiseminaril räägitakse sel korral Fulbright´i programmist ja naistest tehnoloogiasektoris

11. aprillil algusega kell 15 esineb küberturvalisuse veebiseminaride sarjas Fulbright'i programmi külalisteadur Julia Garrard ettekandega teemal: "Fulbright Program and Personal Experience as a Woman in a STEM field".

Täpsem info ja registreerimine siin.

Veebiseminare korraldab Tallinna Tehnikaülikool koostöös USA saatkonnaga Eestis projekti „Roadmap for Inclusive Cybersecurity" raames.

Küberkaitse magistriõppe infotund

TalTechi küberkriminalistika ja küberjulgeoleku keskus viib läbi virtuaalse infotunni sisseastujatele, kus tutvustatakse küberkaitse magistriõppekava.

Infotund toimub 21. aprillil kell 16-17. Õppekava tutvustab programmijuht Rain Ottis. Infotund toimub inglise keeles ja Teamsis. Salvestust ei toimu.

Loe õppekava ja kandideerimise kohta siin.

Infotundi on ennast võimalik registreerida Fienta keskonnas.

Küberkaitse õppekava infotund toimub magistriõppe infonädala raames, mis kestab 17.-21. aprillini. Ülikooli vastuvõtutingimuste infotund toimub 17. aprillil kell 18-19 Tallinna Tehnikaülikooli peahoone (Ehitajate tee 5) aulas.

Tartu Ülikool

IT Academy Research Summit 18.–19. mail Tartus

IT Akadeemia teadusprogrammi (2018-2023) lõpu tähistamisega seotult korraldatakse Akadeemia teaduste tippkohtumine.
Ühel üritusel on võimalik kohtuda kõigi uurimisrühmadega, mis on loodud kolmes tehisintellekti, suurandmete ja robootika valdkondades.

Oluline info:

- Millal? 18.-19. mai Tartu Ülikoolis Delta keskuses
- Kes on kutsutud? Ettevõtete ja avaliku sektori teadlased ja juhid, doktorandid ja magistrandid ning IT-uuringutest ja rakendustest huvitatud laiem avalikkus
- Osalemine: Tasuta
- Registreerimine siin (ASAP, hiljemalt 11. maiks)

Veebileht ja täisprogramm on leitav siit.

Kood Jõhvi

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.

Otsime arendajaid, disainereid (tootedisainerid, kunstnikud, arhitektid, UI/UX jne), programmeerijaid (tarkvara, robootika jne), riistvaraspetsialiste ja insenere (mehaanika, elektroonika, 3D printimine jne), tudengeid, meeskonnajuhte, visionääre ja ärimehi, kellel on või ei ole küberturvalisuse kogemusi.

Kui oled huvitatud anna endas teada, registreerides siin.

E-riigi Akadeemia

eGA parendab Moldova kaitsejõudude kübervõimekust

E-riigi Akadeemia (eGA) sõlmis Moldova Vabariigi kaitseministeeriumiga 27. märtsil 2023 vastastikuse mõistmise memorandumi (MOU), et tugevdada Moldova relvajõudude küberkaitse võimekust Euroopa rahutagamisrahastu (EPF) toel.

Loe täpsemalt eGA koduleheküljelt.

CybExer Technologies

CybExer Technologies korraldab Helsinkis küberõppuse Cyber Resilience Helsinki 2023

4.-5. mail 2023 toimub Helsinkis Threat Hunting (ohutuvastus) tüüpi küberõppus Soome ja Eesti ettevõtete kübertiimidele ning kübertiimide liikmetele.

CybExer Technologiese küberharjutusväljak pakub kahel järjestikusel päeval võimalust Eesti ja Soome era- ja avalike organisatsioonide IT-süsteemidega töötajatele võimalust harjutada ühiselt küberrünnakute tuvastamist ning süsteemide kaitset.

Cyber Resilience Helsinki peamine eesmärk on anda osalejatele intensiivsetele küberrunnakutele reageerimise kogemus. Kaitsemeeskondade peamine ülesanne on tuvastada ründajad ja jälgida nende liikumist eelseadistatud IT-süsteemides. Üritus toimub võistlusena, kus selgitatakse välja edukaimad tiimid.

Sündmus on mõeldud IT-turvalisuse ja küberkaitsega tegelevatele tehnilistele töötajatele. Harjutuse eesmärk on tuua osalejad välja mugavustsoonist ja anda võimalus tegeleda nende jaoks ootamatute väljakutsetega stressiolukorras.

Registreerimine on avatud nii 4-6 liikmelistele küberkaitsetiimidele kui ka individuaalsetele osalejatele, kes saavad koha mõnes tiimis. Tegemist on suurepärase osalemisvõimalusega ka Eesti ettevõtetele/organisatsioonidele.

Registreerimise ja lisaküsimuste korral: sales@cybexer.com

Lisainfo CybExeri kodulehelt.

Cybernetica

Cybernetica ja ENISA sõlmivad eIDAS määruse raames kolmeaastase raamlepingu

Cybernetica ja Euroopa Liidu Küberturvalisuse Agentuur (ENISA) sõlmisid kolmeaastase raamlepingu eIDAS määruse ülevaatamise raames. Cybernetica hakkab pakkuma laia valikut nõustamisteenuseid seoses digikukru ja elektroonilise identifitseerimisega.

Raamlepingu eesmärgiks on toetada ENISA tööd elektroonilise identifitseerimise, digikukrute ja usaldusteenuste valdkonnas aastatel 2023—2025. Tegelikud projektid sõltuvad eIDASe läbivaatuse lõpptekstist ja tööriistakasti protsessi väljundist Euroopa digiidentiteedi raamistiku koordineeritud lähenemisviisi jaoks. Peale selle lisandub NIS2 direktiivi ja eIDASe ülevaatuse koosmõju, mis hõlmab küberturvalisuse ja juhtimisnõudeid.

eIDAS määrus jõustus 2016. aastal ja see asendas elektrooniliste allkirjade direktiivi 1999/93/EC. eIDAS käsitleb 1999. aasta direktiivi probleeme ja laiendab selle reguleerimisala. Määruse eesmärgiks on hõlbustada kaubandust ELis läbipaistvuse, turvalisuse, tehnilise neutraalsuse, koostöö ja koostalitlusvõime kaudu.

Nende väärtuste jõustamiseks eIDAS:

- standardiseerib elektroonilise isikutuvastuse (eID) kasutamise;
- määratleb uue elektrooniliste usaldusteenuste (eTS) klassi;
- selgitab ja tagab digiallkirjade õigusliku kehtivuse;
- loob Euroopa Liidus elektrooniliste usaldusteenuste jaoks Euroopa siseturu.

Need standardid kehtivad nii EL-i liikmesriikides kui ka piirideüleselt.

eIDAS määrus on praegu ülevaatamisel ja ENISA jätkab oma tööd avalik-õiguslike ja eraasutuste toetamisel määruse rakendamisel, käsitledes

tehnoloogilisi aspekte ja usaldusteenuste, elektroonilise identiteedi ja digikukrute ehitusplokke. Euroopa Komisjon tegi 3. juunil 2021 ettepaneku eIDAS määruse (EL) nr 910/2014 muutmiseks. Selle eesmärk on Euroopa elektroonilise identiteedi ja usaldusteenuste maastik uuesti määratleda, jõustada veelgi rangemat integratsiooni. Lisaks luuakse sellega Euroopa digikukrute uus raamistik ja võetakse kasutusele kolm uut usaldusteenust (elektrooniliste arhiveerimisteenuste, elektrooniliste pearaamatute pakkumine ning elektrooniliste allkirjade ja pitsati loomise seadmete haldamine). Need muudatused suurendavad turu perspektiivi ja avaldavad mõju küberturvalisuse nõuetele.

Alates 2013. aastast on ENISA toetanud eIDAS määruse rakendamist, andes turvasoovitusi usaldusteenuste korrektseks rakendamiseks, kaardistades tehnilisi ja regulatiivseid nõudeid, edendades kvalifitseeritud usaldusteenuste kasutuselevõttu Euroopas, tõstes seotud osapoolte ja lõppkasutajate teadlikkust elektrooniliste tehingute turvalisusest kasutades usaldusteenuseid.

Lisainfo siin.

Cybernetica vanemteadur Peeter Laud sai Eesti Teadusagentuurilt uurimisgrandi uurimaks hajusidentiteedi loomist

Eesti Teadusagentuur väljastas Cybernetica vanemteadur Peeter Lauale neljaks aastaks 769 600 euro suuruse uurimisgrandi. Laud hakkab juhtima kolmest uurimissuunast koosnevat teadusprojekti, mis keskendub digitaalse identiteedi tõendite nõrkadele lülidele.

„Digitaalsed identiteedisüsteemid on meie ühiskonna nurgakivi. Selliste süsteemide funktsionaalsuste võimalikult laiaulatuslik levitamine võimaldab meil eemaldada nõrgad lülid ja parandada süsteemi privaatsusomadusi. Lisaks võib see võimaldada identiteete paremini digitaliseerida," kommenteeris Laud.

Eesti Teadusagentuuri uurimistoetuste valdkonna juht Helen Post selgitas, et uurimistoetuste eesmärk on toetada kõrgetasemeliste teadus- ja arendusprojektide läbi viimist ning taotlusi hindavad rahvusvahelised eksperdikomisjonid. „Hea meel on tõdeda, et Eestis on maailmatasemel teadlasi, nagu Peeter Laud, kes panustavad teadusse arengusse just uurimistoetuse abil," lisas ta.

Grandiprojektis on kolm peamist uurimissuunda. Esimeses uuritakse, kuidas digitõendeid on võimalik välja anda ja kasutada viisidel, mis on kasutajate jaoks võimalikult privaatsed. Selleks kasutatakse krüptograafilisi tehnoloogiaid, eriti nullteadmustõestusi, et kasutajal oleks võimalik sõltuvale osapoolele (s.t. serverile) avaldada enda kohta ainult seda, mis sõltuva osapoole jaoks oluline on. „Usume, et nende tehnoloogiate loomisel on palju kasu nullteadmustõestuste kompilaatorist, mille loomise ja arendamisega oleme Cyberneticas juba ligi kolm aastat tegelenud," ütles Laud.

Laud koos meeskonnaga töötavad grandiprojektis välja protokollid, milles osalemiseks peab kasutaja mingil hetkel rakendama oma privaatvõtit. Nende võtmete haldamine on mittetriviaalne ning õiged viisid selleks võivad sõltuda konkreetsest protokollist. Võtmete turvalisemaks haldamiseks võib kasutada lävikrüptograafiat, s.t. SplitKey-ga sarnanevaid meetodeid. Grandiprojekti teine uurimissuund keskendubki nende meetodite väljapakkumisele, seda muuhulgas postkvantturvaliste protokollide jaoks. Cybernetica poolt patenteeritud SplitKey tehnoloogia on kasutusel näiteks Smart-ID-s.

Grandiprojekti kolmas suund uurib, kuidas isiku identiteet kujuneb ja kuidas elektroonilise identiteedi haldus saab neid kujunemisviise ära kasutada. „Toetudes mõttele, et identiteet on atribuutide kogum, arutame, kuidas need kogumid saavad üksteise kohta midagi väita ja kuidas nende väidete tõeväärtust hinnata," sõnas Peeter Laud.

Lisainfo koduleheküljel.

European Telecommunications Standards

ETSI IoT konverents 2023: IoT Technologies for Green and Digital Transformation

ETSI iga-aastane lipulaev naaseb 2023. aastal. ETSI IoT konverents 2023— IoT tehnoloogiad roheliseks ja digitaalseks ümberkujundamiseks toimub 4.—6. juulil 2023 ETSI ruumides Sophia Antipolises Prantsusmaal.

Üritus hõlmab ETSI IoT konverentsi ja esitlusi, mis tutvustavad IoT kasutusjuhtumeid ja tehnoloogiaid rohelise ja digitaalse ümberkujundamise toetamiseks. Üritus pakub osalejatele võimalust jagada kogemusi seoses asjade interneti tehnoloogiate, teenuste, tegevuste, nõuetega, vaadates praegust ja tulevast standardimistööd.

2023. aasta konverents keskendub:

- IoT roheliseks ja digitaalseks ümberkujundamiseks
- IoT-tehnoloogiatele, sealhulgas (kuid mitte ainult) ontoloogiad, digitaalsed kaksikud, servtöötlus, asjade Interneti turvalisus, SAREF, oneM2M
- Horisontaalsed asjade Interneti standardid vertikaalsete ärisektorite jaoks, sealhulgas, kuid mitte ainult, arukad linnad, energia ja võrk, nutikas põllumajandus ja täppispõllumajandus, liftid ja hooned, mereteenused.

Lisainfo ja registreerimine.

NIS Directive User Community

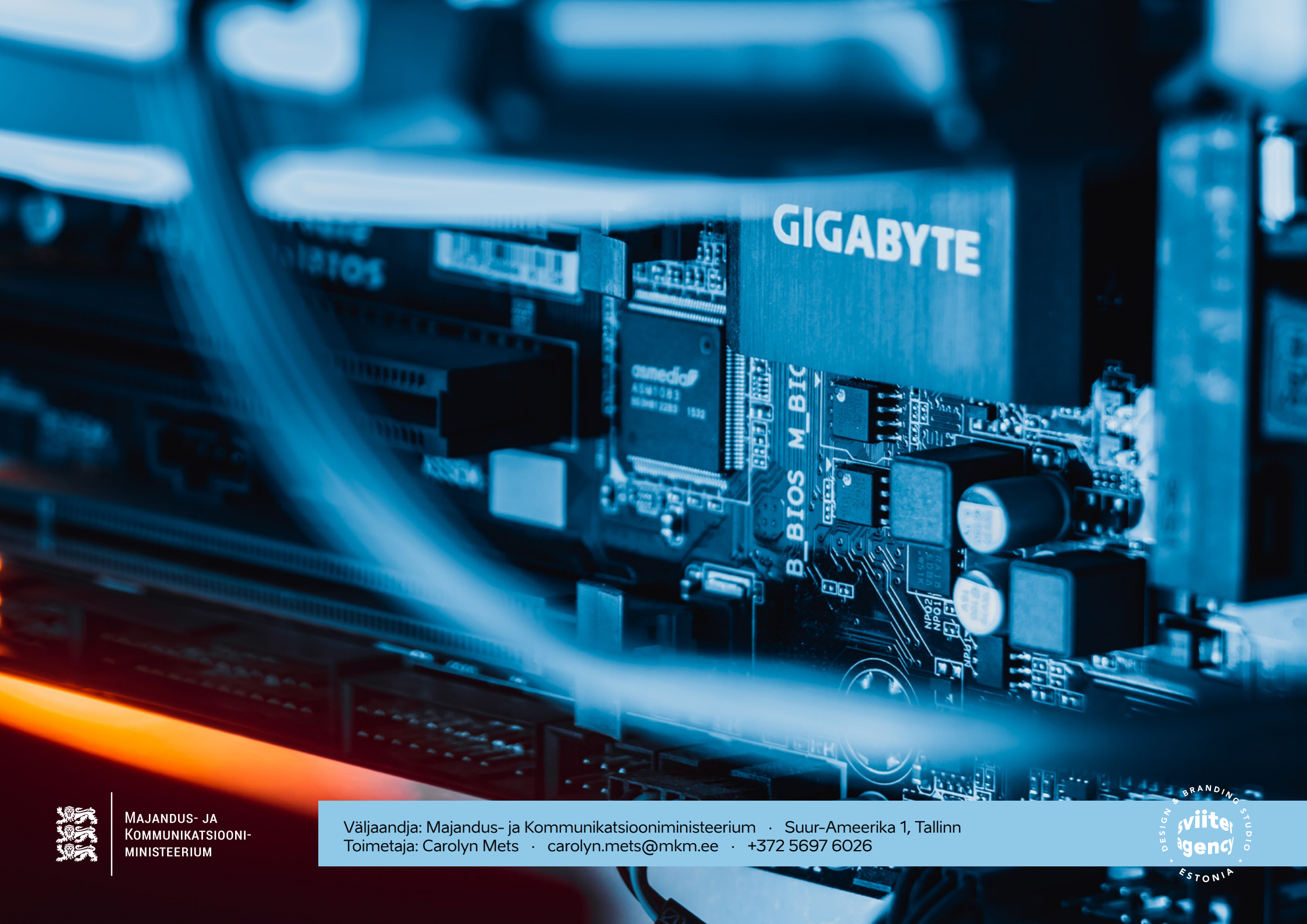
Teine NISDUC konverents: From NIS to NIS 2.0 — A path to take

Belgia postiteenuste ja telekommunikatsiooni instituut (BIPT), Belgia küberturvalisuse keskus (CCB) ja Luxembourgeois de Régulationi instituut (ILR) koos Luksemburgi teaduse ja tehnoloogia instituudiga (LIST) ja Luksemburgi küberturvalisuse majaga (LHC), korraldavad 25.-26. aprillil 2023 Belgias Brüsselis teise NISDUC konverentsi.

Konverentsi eesmärk on arendada võrgu- ja infoturbe direktiivi praktikate kogukonda, jagada teadmisi ja tavasid ning saada kogemusi koolitustel.

Kahepäevasele tasuta konverentsile on oodatud oluliste teenuste operaatorid, digiteenuste pakkujad, riiklikud asutused, arvutiturbeintsidentidele reageerimise meeskonnad, valdkondlikud ühendused, küberjulgeolekuasutused ja muud asjassepuutuvad inimesed.

Lisainfo ja registreerimine.



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