Riikliku küberturvalisuse uudiskiri

2023-07

Majandus- ja kommunikatsiooniministeerium

Küberturvalisuse valdkonna revisjon: kärajad ja edasine tegevus

Riigi Infosüsteemi Amet

Küberturbe parandamiseks saab toetust taotleda nüüdsest suurem hulk ettevõtjaid

CCDCOE

CyConist võttis osa 600 inimest enam kui 60 riigist

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Majandus- ja Kommunikatsiooniministeerium

Küberturvalisuse valdkonna revisjon: kärajad ja edasine tegevus 3

Riigi Infosüsteemi Amet

Küberturbe parandamiseks saab toetust taotleda nüüdsest suurem hulk ettevõtjaid 3

RIA kutsub inimesi üles oma IT-vaatlikkust testima 4

RIA avaldas uuendatud krüptoalgoritmide uuringu 5

NATO küberkaitsekoostöö keskus

CyConist võttis osa 600 inimest enam kui 60 riigist 5

e-Riigi Akadeemia

eGA jätkab Lääne-Balkani küberturvalisuse parendamist 6

Presidendid väisasid eGA ja Cybexeri korraldatavat õppust Albaanias 6

#TSSCD võõrustas 53 küberdiplomaati 6

Küberturvalisuse õppus kasvatas Moldova vastupanuvõimet küberohtudele 6

TalTech

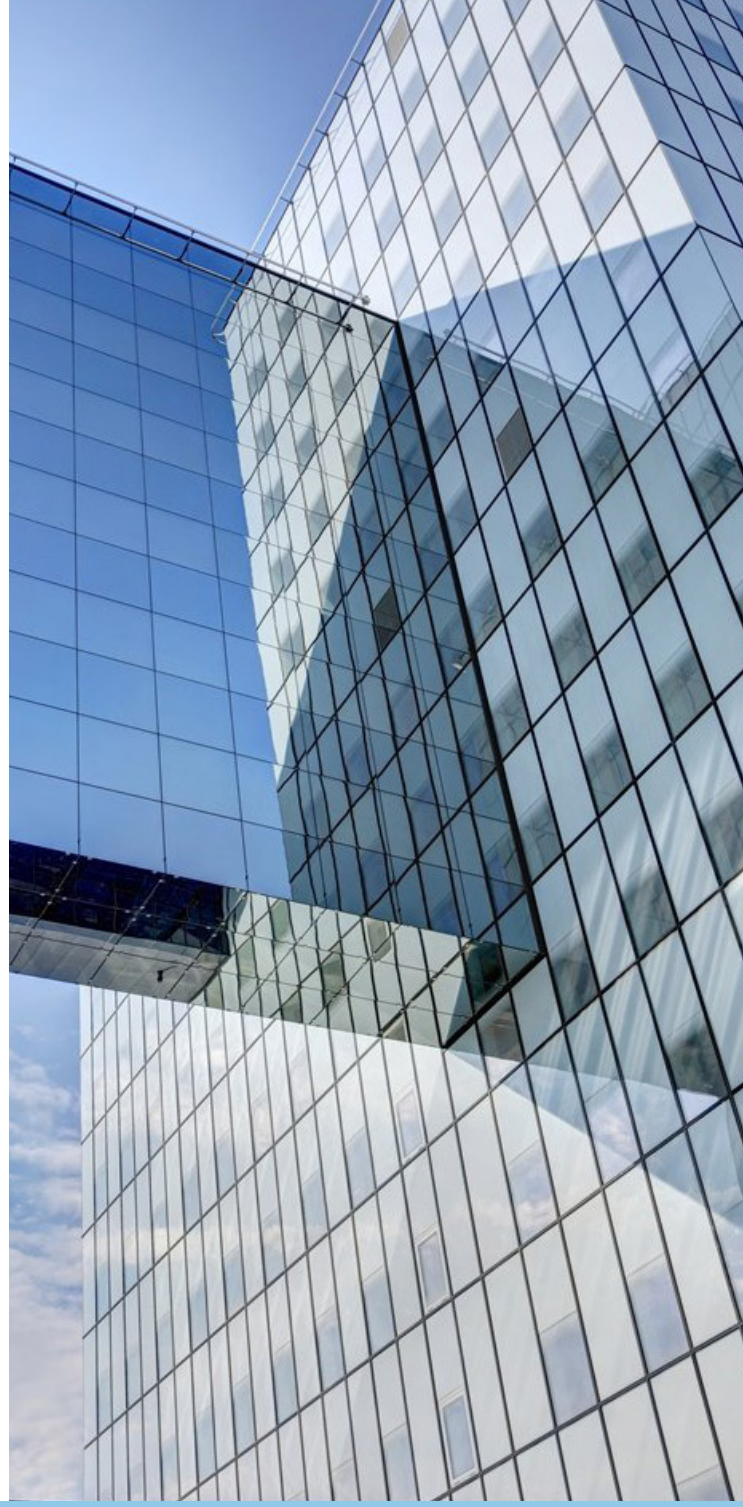
Tallinna Tehnikaülikoolis anti üle diplomid küberkaitse magistritele 7

Cybernetica

Cybernetica ühendab Kataloonia tippülikoolid turvaliseks andmevahetuseks 7

European Telecommunications Standard

ETSI turvakonverents 2023 8



Uudiskirja sisendi andmiseks või liitumiseks kirjuta **carolyn.mets@mkm.ee**

Küberturvalisuse valdkonna revisjon: kärajad ja edasine tegevus

Majandus- ja Kommunikatsiooniministeerium (MKM) viis läbi 22. ja 26. juunil esimesed kärajad erasektori ja avaliku sektori esindajatega.

Kärajatel anti lühiülevaade, mida toob endaga kaasa Euroopa Parlamendi ja nõukogu direktiiv nr 2022/2555 ehk NIS 2 direktiiv, tutvustati revisjoniga seotud ajakava ning arutati NIS2 direktiivi üle võtmisega kui ka muid kübervaldkonnaga seotud küsimusi ja teemasid, mis on revisjoni ettevalmistamise käigus tekkinud. Kärajate peamiseks eesmärgiks oli kärajate jaoks ette saadetud küsimuste ja teemade arutelu, et neid valideerida või ümber lükata ning saada osalejatelt täiendavaid mõtteid, soovitusi ja kommentaare, mida saaks revisjoni sisse võtta.

Kärajate käigus ja selle järel saadud kirjaliku sisendi põhjal valmistab MKM ette revisjoniga seotud eelnõu teksti. MKM-il on ka soov teha käesoleva aasta sügisel (eelduslikult septembris või oktoobris) täiendavad kärajad, et arutada tolle hetke seisuga kokku kirjutatud eelnõu kavandit. MKM planeerib saata revisjoniga seotud eelnõu Eelnõude Infosüsteemi kaudu avalikule kooskõlastusele 2023. a lõpus. Vabariigi Valitsuse tegevusplaani kohaselt tuleb eelnõu esitada Vabariigi Valitsusse aprillis 2024. a ning siseriiklikud sätted peavad olema kohaldatavad alates 18. oktoobrist 2024. a.

Küberturbe parandamiseks saab toetust taotleda nüüdsest suurem hulk ettevõtjaid

Märtsis avas Riigi Infosüsteemi Amet (RIA) koostöös EAS ja Kredex ühendasutusega toetusprogrammi, et aidata ettevõtetel tõsta oma küberturvalisuse taset. Juunis laienes tegevusalade ring, kes saavad küsida kuni 60 000 euro suurust toetust. Nende hulgas on perearstikeskused, elektrienergia tootjad, majutus- ja toitlustusettevõtted ja paljud teised.

„Turvalisust ei ole kunagi liga palju, eriti küberruumis. Täna ei pruugi kõik ettevõtted enda teenuse ja süsteemide kaitsmiseks piisavalt ressurssi leida, mistõttu tuleme teenusepakkujatele appi ja jagame küberturvalisuse taseme tõstmiseks toetusi. Esimesed taotlused on saanud EAS ja Kredex ühendasutuselt positiivsed vastused, kuid ootame veelgi rohkem ettevõtteid, kellele toetust anda," ütles RIA küberekspert, teaduse ja koordinatsiooniosakonna juhataja Lauri Tankler.

Toetuse taotlemiseks vajaminev informatsioon ja juhised on leitavad EAS ja Kredexi ühendasutuse kodulehel. Lisaküsimuste korral kirjutage tak@ria.ee.

Toetust saavad taotleda Eesti äriregistrisse kantud väikesed ja keskmise suurusega ettevõtjad, kelle tegevusala kuulub järgmistesse EMTAK tegevusalade jagudesse:

- **B – mäetööstus**
- **C – töötlev tööstus**
- **D – elektrienergia, gaasi, auru ja konditsioneeritud õhuga varustamine**
- **E – veevarustus, kanalisatsioon, jäätme- ja saastekäitlus**
- **F – ehitus**
- **G – hulgi- ja jaekaubandus, välja arvatud mootorsõidukite ja mootorrataste remont**
- **H – veondus ja laondus**
- **I – majutus ja toitlustus**
- **J – info ja side**
- **M – kutse-, teadus- ja tehnikaalane tegevus**
- **N – haldus- ja abitegevused**
- **Q – tervishoid ja sotsiaalhoolekanne**

Küberturbe parandamiseks mõeldud toetuse andmine on osa Euroopa Liidu Digital Europe programmi pilootprojektist, millega kasvatatakse väikese ja keskmise suurusega ettevõtjate võimekusi tulla toime küberrünnakutega ja ennetada neist tulenevaid majanduskahjusid.

Programm on kaheastmeline, mille esimene tegevussuund on oma küberturvalisuse hetkeseisu hindamine ning teine parandamist vajavate arendustegevuste elluviimine.

Küberpööret kaasrahastatakse läbi Euroopa

Liidu Digital Europe programmi ja Euroopa küberpädevuskeskuse. Toetusteks ettenähtud kogusumma on 865 000 eurot.

Taotlemise tingimuste kohta leiab täpsema ülevaate veebilehelt.

RIA kutsub inimesi üles oma IT-vaatlikkust testima

Riigi Infosüsteemi Amet (RIA) pöörab juulis aset leidva küberteadlikkuse tõstmise kampaaniaga tähelepanu ohtudele, mis Eesti inimesi küberruumis varitsevad ning mille tõttu meie ettevõtted ja inimesed võivad jäävad ilma olulistest andmetest, kontodest ja rahast.

Kampaaniaga kutsutakse inimesi üles oma harjumuspärast käitumist teadlikumalt jälgima ning testima oma IT-teadmisi IT- vaatliku kodulehel.

"Teated sellest, kuidas keegi on jäänud internetis ilma oma rahast, on muutunud igapäevaseks. Need summad ei ole väikesed, ulatudes teinekord tuhandete eurodeni. Kahjuks teevad inimesed oma hooletuse või teadmatusega tihti küberkurjategijate elu väga palju lihtsamaks. Oleme mitme aasta vältel näinud, et suurem teadlikkus küberruumis varitsevatest ohtudest aitab kaitsta nii inimest ennast kui ka terveid süsteeme," märkis RIA analüüsi- ja ennetusosakonna juht Märt Hiietamm.

Alates juunist on kõigile kättesaadav küberteadlikkuse test. Kaasahaaravate ja praktiliste õppevideote abil selgitatakse, kuidas ennast levinumate küberohtude eest kaitsta ning enda teadmisi saab proovile panna läbides 12 küsimusega testi. Test on jõukohane kõigile, ka neile, kes igapäevaselt internetis ei toimeta.

"Väga paljud pettused ja muud küberintsidendid oleks olemata, kui inimesed järgiks küberhügieeni põhireegleid. Just nende selgitamiseks ja kinnistamiseks ongi videod ja test mõeldud," sõnas Märt Hiietamm.

Kampaania kestab 4. augustini ning kampaania sõnumeid kohtab nii tänavapildis kui ka meediakanalites. Lisaks stardib 3. juulil ka 10-osaline küberturvalisuse saatesari nimega „Ohtlik klikk", mis läheb igal esmaspäeval eetrisse Kuku Raadios. Saatesarja eesmärk on teavitada elanikke ohtudest ja murekohtadest küberruumis ning isiklikust vastutusest küberintsidentide ennetamisel ja tagajärgedega tegelemisel.

Selle aasta esimese viie kuu jooksul registreeris RIA ca 550 õngitsuslehte, mille kaudu petavad kelmid inimestelt välja pangakaardi andmeid ja PIN-koode.

Registreerisime ka ca 1200 intsidenti, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele ja käideldavusele, ning tuvastasime ca 5000 seadet, mis olid pahavaraga nakatunud.

Mõned näited küberrünnakutest:

- Mais teavitati CERT-EE-d rohkelt erinevate teenusepakkujate nimel saadetud sõnumitest, milles olev link viis kurjategijate loodud andmeid koguvale lehele. Eriti tihti tehti seda postiteenuste pakkujate nimel. Aasta alguses oli senisest enam ka Smart-ID kasutajaandmete õngitsusi.

- Kasvab e-posti või sotsiaalmeedia kontode ülevõtmine. Üldjuhul ei saa kasutaja enam ise enda kontole ligi, sest seotud e-posti aadress ja parool on ära vahetatud ning ligipääsu taastamine on küllalt keeruline. Tihti on e-posti kontoga seotud paljude teiste keskkondade paroolide taastamine, mis annab ründajale võimaluse ka need salasõnad ära muuta.

- Mais sattus küberrünnaku ohvriks tuntud tehnoloogiatootja veebipood, mille käigus paigaldati lehele pahaloomuline skript. Rünnak oli võimalik, sest ohver ei olnud uuendanud tarkvara.

- Ülikoolide nimel saadetakse kirju, millele oli lisatud manusena troojan-tüüpi pahavaraga nakatunud DOCX-failid, mille avamisel on ründajal võimalik saada ligipääs kasutaja seadmele.

- Märtsis tabas üht Tallinnas asuvat

mööblitootjat arvepettus, kui nende välismaal asuvale kliendile saadeti nende meilikonto alt kurjategijate pangarekvisiitidega arve.

• Märtsis tuvastasime mitusada Eesti veebilehte, mis võisid olla RedStealer-nimelise nuhkvaraga nakatunud. Antud pahavara eesmärgiks on varastada ohvri kasutajatunnuseid ja muid tundlikke andmeid.

• Veebruaris toimus ühe IT teenusepakkuja vastu lunavararünnak, mille käigus krüpteeriti serverites ja töökohaarvutites olnud andmed ning varukoopiad. Ründe tõttu katkes töö kahes ettevõttes, kellele rünnaku alla sattunud IT-firma teenuseid osutab.

RIA avaldas uuendatud krüptoalgoritmide uuringu

Riigi Infosüsteemi Ameti (RIA) tellimusel koostasid Cybernetica teadlased värske ülevaate krüptograafiliste vahendite kasutamise hetkeseisust.

Uuringuaruanne kuulub samasse seeriasse varasemate aruannetega, mis valmisid aastatel 2011-2018. Regulaarne uuring on välja kasvanud vajadusest omada ülevaadet krüptograafiliste vahendite ja nende kasutamise turvatasemest. Seekord on suurt rõhku pandud kvantarvutikindlale krüptograafiale ning selle kasutuselevõtu hetkeseisule.

Uuring on vajalik igapäevases kasutuses olevate infosüsteemide turvaliseks arenguks.

Lisainfo ja uuring on leitavad RIA koduleheküljelt.

CyConist võttis osa 600 inimest enam kui 60 riigist

30. maist 2. juunini toimus maailmas ainulaadne küberkonverents CyCon. NATO küberkaitsekoostöö keskuse (CCDCOE) konverents keskendus sellele, kuidas küberkonfliktid mõjutavad sõjapidamist ja ühiskondi. Valdkondadeülene suurkonverents tõi Eestisse kübersõja tippeksperdid erasektorist, ülikoolidest ja julgeolekuasutustest.

Konverentsi avas president Alar Karis. "Aasta pärast Venemaa agressioonisõda Ukraina vastu näeme selgelt, et peame palju sügavamalt mõistma küberkonflikte ja nende mõju meie ühiskonnale. On aeg teiste kogemustest õppida, õpitut jagada ja leida lahendusi, mis suurendavad nii üksikinimese kui ka meie kollektiivset säilenõtkust küberruumis," ütles Alar Karis.

President rõhutas, et nii avalik kui ka erasektor, aga ka ühiskond tervikuna, peavad kübervastupidavuse suurendamiseks rohkem korda saatma. "Seda on kergem öelda kui teha. Enamik inimesi ei kuluta aega, et näha seoseid järjekordse tarkvarauuenduse ning kahjuliku küberintsidendi vahel. Seetõttu peame keskenduma sellele, et tõsta teadlikkust kõikidel tasanditel. Küberkonverents CyCon on üks parimaid näiteid, kuidas eri valdkonnad saavad koostööd edendada," lisas Karis.

NATO CCDCOE direktor Mart Noorma rõhutas, et kõik CCDCOE 39 liikmesriiki teevad koostööd küberruumi turvalisemaks muutmiseks.

"Meie peamine eesmärk on aidata sarnaselt mõtlevatel riikidel ühiseid eesmärke saavutada. CyCon pakub suurepärast platvormi avalikule ja erasektorile, sõjalistele organisatsioonidele ja akadeemilistele ringkondadele, et tulla kokku ja võidelda küberprobleemidega ühtse meeskonnana," ütles Noorma.

Nelja päeva jooksul võtsid sõna ja arutasid küberkonfliktide ning küberturvalisuse teemadel ca poolsada esinejat. Rääkijate seas olid muuhulgas NATO asepeasekretär David van Weel, Valge Maja kübervaldkonna direktor Kemba Eneas Walden, Cambridge'i ülikooli professor Ross J. Anderson ning Euroopa Liidu küberturvalisuse ameti (ENISA) juht Juhan Lepassaar.

CyCon tõi Tallinnasse ka Saksamaa, Austraalia, USA, Suurbritannia, Poola, Kanada ja kümnete teiste liikmesriikide küberväejuhatuse ja kaitseväe esindajad. Sõna võtsid teadlased ja professorid tippülikoolidest, nagu Cambridge, Cornell ja Oxford. Nendega jagasid lava ka suurettevõtete nagu Microsoft, Fortinet ja Palo Alto Networks esindajad.

CyConi eesmärk on tuua ühte ruumi poliitikud, teadlased ning erasektori ja militaarorganisatsioonide kõrged esindajad, et arutada, kuidas uued tehnoloogiad nagu tehisintellekt, käimasolevad konfliktid, rahvusvaheline seadusandlus ja kümned muud faktorid muudavad küberkonfliktide olemust ning mida peaks rahvusvaheline üldsus tegema, et end küberruumis paremini kaitsta.

CyCon 2023 kestis 30. maist 2. juunini ning ingliskeelse konverentsi peateema oli “Meeting Reality”. CyConist võttis osa 600 inimest enam kui 60 riigist.

Küberkonfliktide üle arutlevat konverentsi korraldab NATO küberkaitsekoostöö keskus. Tallinnas asuv NATO oivakeskus on NATO poolt akrediteeritud rahvusvaheline mõttekoda ja väljaõppeasutus.

Rohkem infot CyConi kohta leiab siit.

Konverentsi galeriid leiab siit.

o: Kristi Sits

eGA jätkab Lääne-Balkani küberturvalisuse parendamist

Uue projekti eesmärk on suurendada Lääne-Balkani küberkerksust kooskõlas ELi acquis’ga ja parimate tavadega, parandades küberjulgeoleku ennetamist, valmisolekut ja reageerimist asjaomaste avaliku ja erasektori sidusrühmade jaoks Lääne-Balkani riikides.

Tegevused viiakse läbi kolme aasta jooksul 5 miljoni euro ulatuses. Projektist lähemalt siit.

Lisaks on eGAl käsil “Küberturvalisuse kiirreageerimisprojekt Albaaniale, Montenegrole ja Põhja-Makedooniale”.

Presidendid väisasid eGA ja Cybexeri korraldatavat õppust Albaanias

6.-9. juunil toimunud “elava tule” küberõppuse eesmärk on parandada Lääne- Albaania, Montenegro ja Põhja-Makedoonia küberrünnakutele reageerimise võimekust ning riikide küberkerksust.

Õppuse korraldasid eGA ja Cybexer Technologies EL-i rahastatud Lääne-Balkani kiirreageerimisprojekti raames.

Loe edasi siit.

#TSSCD võõrustas 53 küberdiplomaati

12. –16.06 Tallinnas toimunud küberdiplomaatia suvekool võõrustas 43 riigi küberdiplomaate, et edendada rahvusvahelist koostööd turvalisema küberruumi nimel.

Ürituse korraldasid koostöös Euroopa Liidu Rahvusvahelise Partnerluse Peadirektoraat (INTPA), Välisministeerium, eGA ja Eesti Rahvusvahelise Arengukoostöö Keskus (ESTDEV).

Fotod ürituselt eGA Flickris.

Küberturvalisuse õppus kasvatas Moldova vastupanuvõimet küberohtudele

14.–16. juunil Chişinăus toimunud kolmepäevane küberturvalisuse õppus oli järjekordne oluline samm Moldova valitsusametnike ja elutähtsate teenuste osutajate küberturvalisuse alase valmisoleku suurendamisel. Õppusel osales üle 30 kübereksperdi avalikust ja erasektorist.

eGA ja CybExer Technologiesi korraldatud

õppuse eesmärk oli tugevdada avaliku sektori asutuste ja elutähtsate teenuste osutajate vastupanuvõimet ning kompetentsi ja suurendada teadlikkust küberjuhtumite võimalike mõjude kohta.

Loe edasi siit.

TalTech

Tallinna Tehnikaülikoolis anti üle diplomid küberkaitse magistritele

21. juunil toimunud Tallinna Tehnikaülikooli Infotehnoloogia teaduskonna pidulikul lõpuaktusel anti üle diplomid 12-le küberkaitse magistrikava lõpetajale, nendest kaks lõpetas õpingud cum laude. Aktust on võimalik järele vaadata TalTechi Youtube kanalil.

Kõikide 2022/2023. õppeaasta lõpetajate nimed on ära toodud TalTechi ajakirja Mente et Manu juunikuises numbris.

Cybernetica

Cybernetica ühendab Kataloonia tippülikoolid turvaliseks andmevahetuseks

Cybernetica ja Kataloonia tippülikoolid sõlmisid lepingu uue koostalitlusplatvormi arendamiseks ja juurutamiseks, et hõlbustada andmevahetust ülikoolide vahel.

Platvorm CAMINS võtab aluseks Cybernetica saadud kogemused Eesti koostalitlusvõime raamistiku ning ettevõtte enda koostalitlusplatvormi toote Unified eXchange Platfrom (UXP) arendamisel. Loodava platvormi põhiomadused on detsentraliseeritus, skaleeritavus ja privaatsuse säilitamine. Projekti rahastab EL-i üksus NextGenerationEU.

„Meil on väga hea meel, et Cybernetica kogemus koostalitlusplatvormide arendamisel on leidnud järjekordse tunnustuse, seekord hariduse valdkonnas. Kataloonia regiooni loodav andmevahetuse ökosüsteem annab tugeva ja skaleeritava aluse Hispaania ülikoolisüsteemi edasiseks digitaliseerimiseks," leiab Cybernetica tegevjuht Oliver Väärtnõu.

Cybernetica andmevahetustehnoloogiate osakonna juhataja Maksim Ovtšinnikov toob välja, et loodava koostalitlusvõime platvormi abil saab lihtsamalt jagada üliõpilaste, õppejõudude ja teeninduspersonali andmeid. „Andmevahetuse automatiseerimine aitab ülikoolidel efektiivsemalt töötada ühiste eesmärkide nimel ning ühendada seni eraldi seisnud protsessid. Esialgu keskendub projekt seitsmele koostalitlusvõime kasutusjuhule, et edendada platvormi kasutuselevõttu ja näitlikustada selle väärtust erinevate sidusrühmade jaoks," selgitab Ovtšinnikov.

Projektis osalevad mitmed Kataloonia riiklikud ülikoolid, ent projekti tellija ja peakoordinaator on rahvusvaheliselt tunnustatud Rovira i Virgili ülikool. Lisaks eelnimetatud ülikoolile võtavad platvormi CAMINS kasutusele veel neli ülikooli: Barcelona autonoomne ülikool, Barcelona ülikool, Girona ülikool ja Kataloonia polütehniline ülikool. Kaks ülikooli — Lleida ülikool ja Kataloonia avatud ülikool — ühinevad projektiga vaatlejatena. Kohalikku tehnilist tuge ja infrastruktuuri hooldust hakkab pakkuma Kataloonia ülikoolide teeninduskeskus.

Cybernetica on üle 25-aastase e-valitsuse tehnoloogiate juurutamise kogemusega Eesti üks juhtivaid IKT-ettevõtteid. Muuhulgas on Cybernetica arendatud Eesti e-riigi põhiline andmevahetuse platvorm X-tee, digiidentiteedi üks alustehnoloogiaid SplitKey ning interneti hääletamise rakendus. Ettevõte on üle 10 aasta eksportinud oma tehnoloogiaid ja juurutanud e-riigi projekte paljudes riikides, sh Ukrainas, Jaapanis, Beninis, Tuneesias, Bahamadel, Gröönimaal ja mujal.

European Telecommunications Standard

ETSI turvakonverents 2023

Konverentsi keskpunktiks on teadusuuringud ja innovatsioon. Avatud on registreerimine ja päevakava on avalikustatud!

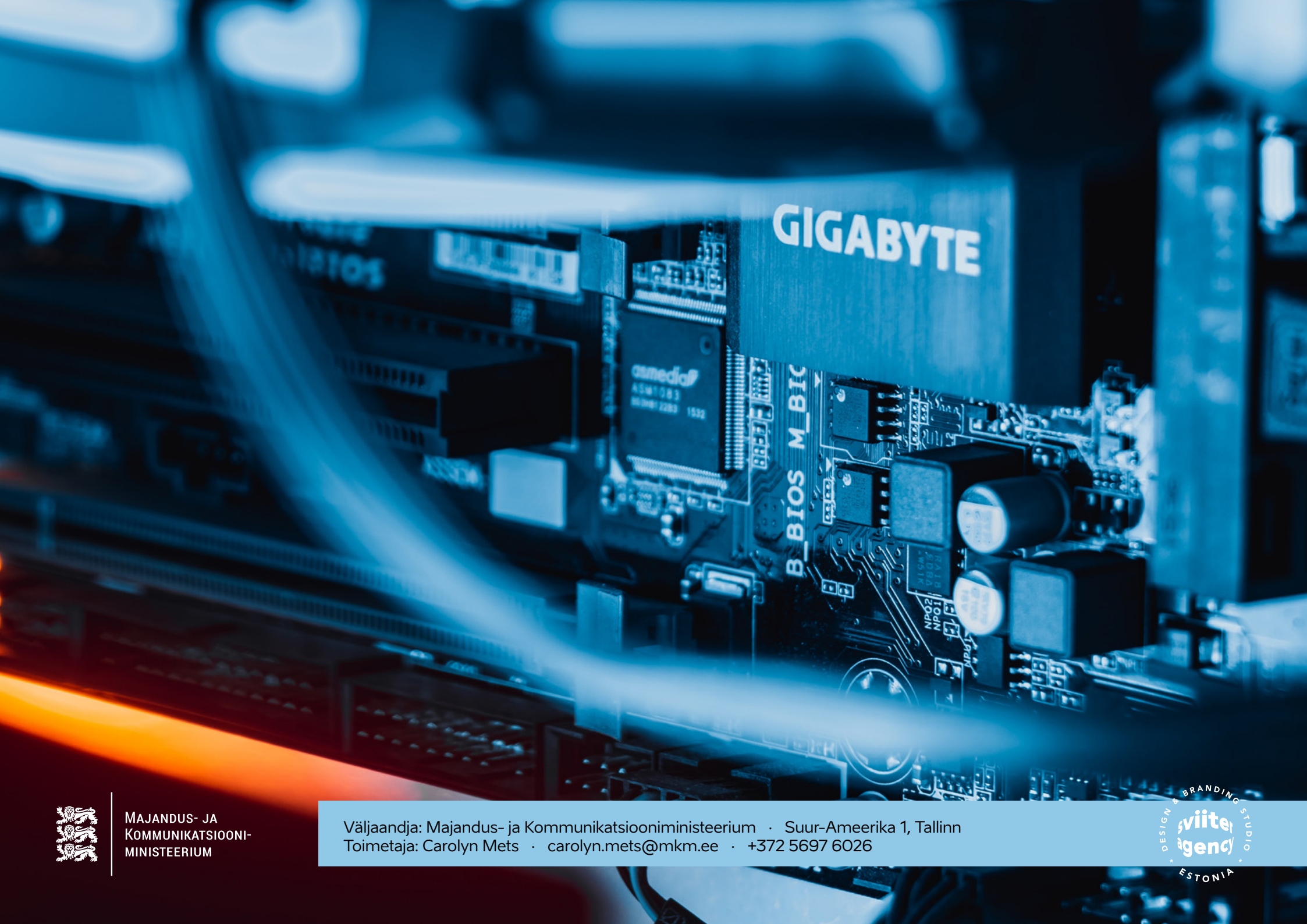
ETSI iga-aastane küberturvalisuse lipulaev ETSI turvakonverents toimub 16.–19. oktoobril 2023 Prantsusmaal ETSI-s Sophia Antipolises. Sündmus langeb kokku 2023. aasta Euroopa küberjulgeoleku kuuga.

Sel aastal keskendub üritus turvauuringutele ja ülemaailmsetele turvastandarditele. Arutatud tehnoloogiavaldkondade hulgas käsitletakse spetsiaalsetel seanssidel zero-trust, tarneahelat, asjade internetti (IoT), kvantandmetöötlust, 5G/6G ja tehisintellekti (AI).

Eksperdid jagavad oma kogemusi ka laiematest aspektidest, nagu küberturvalisuse standardimise järgmise põlvkonna spetsialistide leidmine ja VKEde toetamine.

See eksklusiivne üritus annab turvakogukonnale ainulaadse võimaluse tulla kokku, et suhelda ekspertidega, suhelda kaaslastega ning jagada teadmisi ja arvamusi küberturvalisuse standardimise teemal. Ärge jätke kasutamata võimalust kogukonnaga kohtuda ja suhelda!

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 ESTONIA