Riikliku küberturvalisuse uudiskiri

2023-02

Majandus- ja kommunikatsiooniministeerium

Läbivalt küberturvaline Eesti

Riigi Infosüsteemi Amet

RIA Küberturvalisuse aastaraamat 2023

Välisministeerium

Välisministeerium võttis üle NATO-Gruusia koostööpaketi küberinitsiatiivi juhtimise.

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Majandus- ja Kommunikatsiooniministeerium

Läbivalt küberturvaline Eesti 3

Majandusministeerium kutsub ettevõtteid häkatonile Ukrainale kaitselahendusi looma 4

Välisministeerium

Välisministeerium võttis üle NATO-Gruusia koostööpaketi (Substantial NATO-Georgia Package — SNGP) küberinitsiatiivi juhtimise 5

Riigi Infosüsteemi Amet

RIA küberturvalisuse aastaraamat 2023 6

Peaminister Kaja Kallas külastas RIA-t 7

Olukord küberruumis 7

Osale e-hääletamise vaatlusprogrammis 7

Andmekaitse Inspektsioon

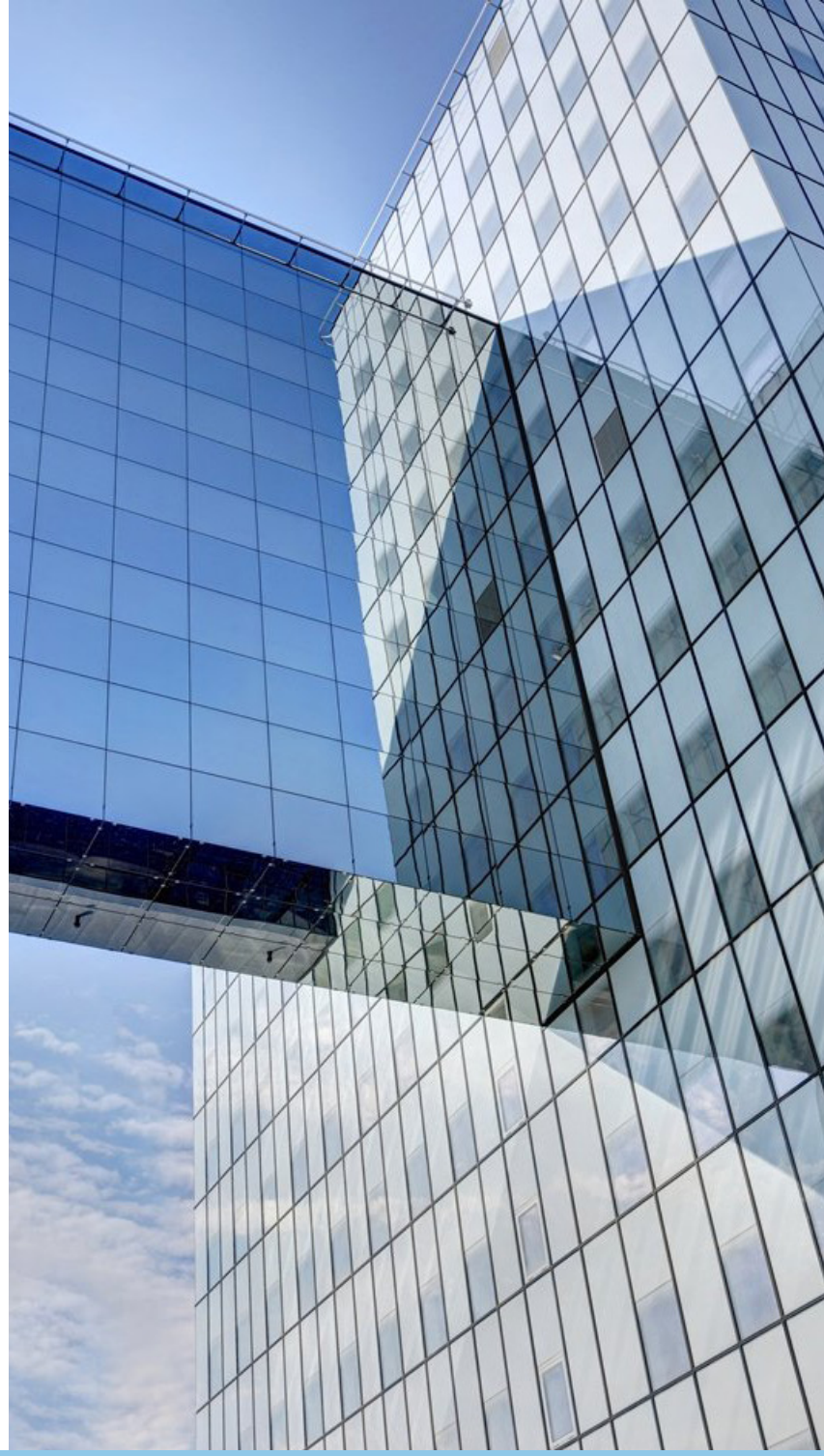
Euroopa ühisuuring tõi suuremate puudustena välja muuhulgas vähese teadlikkuse, puuduliku mõjuhindamise ning üheselt määratlemata rollid 8

Cybernetica

Cybernetica ja EY hakkavad ümber kujundama EL-i rahastatud projekti raames Maksu- ja Tolliameti süsteeme 8

European Telecommunications Standards Institute

ETSI/IQC Quantum Safe Cryptography Event 9



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

Läbivalt küberturvaline Eesti

2023 on MKM-i riikliku küberturvalisuse osakonna eesmärgiks kodu korrastada, et möödunud aastal õpitut kõige paremini rakendada. Oleme palju targemad selles, kuidas riskipõhiselt parimat võimalikku küberturvet korraldada ning näinud, kuidas Ukraina suutis ka sõja raskematel hetkedel infosüsteeme kaitsta ja e-teenuseid üleval hoida. Meie jaoks on jätkuvalt kesksed küsimused riikliku küberturvalisuse korraldamisel: kuidas kaitseme oma ühiskonda — inimesi, teenuseid, infosüsteeme ja kõike nende jaoks vajalikku - võimalikult kaua ja paindlikult kriiside ja ohu korral ning milliste ohtude ja stsenaariumide jaoks peame valmis olema.

Sealjuures saab eesmärk olla ainult läbivalt küberturvaline Eesti, mis peab võimalikult hästi ja paindlikult vastu tehnoloogia arengutele ja võimalikele ohtudele. See on summa organisatsioonide tehnoloogia riskide juhtimisest ja rakendatud kohastest infoturbemeetmetest ning keskselt pakutud tehnilistest meetmetest ja nõuetest, normidest. Nii peavad digitaliseerimisest maksimaalse kasu saamiseks riskid olema juhitud ning turvalisus olema osa teenuste ja süsteemide disainist. Turvalisus pole omaette eesmärk, vaid vahend, sest ilma selleta kaob usaldus ja usalduseta kaob teenus.

Riigi küberturvamise või ükskõik millise süsteemi infoturbe korraldamise eeldus on aga koostöö. See on praktiline teadmine, et vabas ühiskonnas ei saa keegi üksi turvalisuse korraldamisega hakkama. Selleks peab koos praktiliselt ja ühiste eesmärkide nimel tegutsema. Sel aastal tahame kokku leppida ja vastu võtta riikliku küberturvalisuse strateegilise raamistiku aastateks 2023—2027, et sõidusuund enda kaitsmiseks oleks ühiselt selge. Riikliku küberturvalisuse meeskonna jaoks tähendab see ennekõike, et ootame kaasuma - teeme protsesse koostöös ja koostöiselt, kaasates ja konsulteerides.

Olenemata sellest, milliseks kujuneb aasta 2023 geopoliitikas ja maailma tehnoloogia arengutes, on Eesti ühiskonna ja ökosüsteemi liikmed küberohtude eest kõige paremini kaitstud ühiselt. Seega palume, et oleksite avatud kutsetele tulla arutlema, kaasa mõtlema ja koos Eestit turvalisemaks tegema!

Liisa Past

Riikliku küberturvalisuse juht

Foto: Meeli Küttim

MAJANDUS- JA KOMMUNIKATSIOONI-MINISTEERIUM

Majandusministeerium kutsub ettevõtteid häkatonile Ukrainale kaitselahendusi looma

Majandus- ja Kommunikatsiooniministeerium korraldab koos Garage48-ga häkatoni „Garage48 Defence for Ukraine", mis keskendub kaitsevaldkonnaga seotud tarkvara- ja riistvaralahenduste loomisele Ukraina jaoks.

Ettevõtlus- ja infotehnoloogiaminister Kristjan Järvani sõnul on kaitsevaldkond tavapäraselt väga reguleeritud, mistõttu võivad innovatsiooni pidurdada bürokraatia ja seadusandlus. „Ukraina vajab täna uudseid ja kiiresti rakendatavaid kaitselahendusi ning selle häkatoni eesmärk ongi viia kokku tehnoloogiasektor ja kaitsetööstus, et edendada koostööd ja töötada välja kaitselahendusi, mida saaks ka reaalselt Ukraina abistamiseks kasutada," rääkis Järvan.

„Garage48 Defence for Ukraine" on Makeathon, mis keskendub reaalsete kaitsega seotud tarkvara- ja riistvaralahenduste loomisele Ukraina jaoks. Makeathonil luuakse prototüübid, mis on päriselt kasutatavad. „Eestil on väga tugev kaitsetööstuse potentsiaal, kuna meil on keskmisest suurem osakaal elanikkonnast militaarteemadega kokku puutunud ning me võtame ka ohte realistlikult — kui sinna juurde lisada Eesti iduettevõtete kogemuspagas, siis võime oodata tulevikus sellest sektorist palju edulugusid," märkis minister.

„Ukraina on Eestile väga tänulik Venemaa invasiooni algusest saadik antud enneolematu sõjalise abi eest. Venemaa jõhker agressioon on oht kogu Euroopa julgeolekuarhitektuurile," rõhutas Ukraina suursaadik Eestis Mariana Betsa. Tema sõnul tuleks lisaks relvadele panustada ka uuenduslikesse kaitsega seotud lahendustesse ja tehnoloogiatesse, et tulla toime Venemaa agressioonist tingitud julgeolekuprobleemidega. „Hindame kõrgelt Eesti olulist rolli IT- ja innovaatiliste tehnoloogiate vallas ning usume, et kaitsehäkaton "Garage48 Defence for Ukraine" aitab panustada Ukraina kaitsesse ning aidata Ukrainal sõda võita," lisas Betsa.

Tartus 17.-19. veebruarini 2023 toimuvale kaitsehäkatonile oodatakse tiime, kuhu kuuluvad kaitsevaldkonna eksperdid, arendajad, disainerid, programmeerijad, riistvaraspetsialistid ja insenerid, üliõpilased, meeskonnajuhid, visionäärid ja ettevõtjad. Häkaton annab võimaluse ka Baltikumi ja Skandinaavia sõjaväe- ja kaitsekoolidele, tehnoloogiaettevõtetele ja avalikule kaitsesektorile, et omavahel seguneda ja suhelda, jagada ideid ja teadmisi ning leida uusi koostöövõimalusi ja luua uusi kaitselahendusi. Ürituse lõppedes valib žürii välja parimad, kellele on ka rahalised auhinnad.

Ideede esitamine ja registreerimine tiimina oli avatud 3. veebruarini. Registreerimine individuaalselt on avatud 10. veebruarini. Tiimidele tagatakse kõik vajaminevad materjalid, ruumid ja ekspertiis, et 48 tunni jooksul lahendus valmis saaks.

Häkatoni korraldavad Majandus- ja Kommunikatsiooniministeerium koostöös Garage48.

Lisainfo ürituse kohta siin.

Välisministeerium võttis üle NATO-Gruusia koostööpaketi (Substantial NATO-Georgia Package – SNGP) küberinitsiatiivi juhtimise

SNGP sai heakskiidu 2014. aasta Walesi tippkohtumisel. Programmi eesmärk on toetada Gruusiat (GE) võimearenduses, NATO-ga koostöövõimelisuse saavutamises ja alliansi liikmeks astumisel tulevikus.

Programmil on 17 töövaldkonda, millest igaühel on juht- ja doonorriigid. Alates 2015. aastast on Eesti juhtinud Kaitseministeeriumi eestvedamisel SNGP küberkaitse valdkonda (cyber defence iniative), mille raames on toimunud GE-EE küberekspertide koostöö ja mentorlus.

2023. aasta veebruaris toimuval NATO kaitseministrite kohtumisel arutatakse SNGP muudatusi, mis puudutab ka programmi kübervaldkonda. Initsiatiivi skoop muutub laiapindsemaks, liikudes küberkaitse (cyber defence) aspektilt küberturvalisuse (cyber security) tõstmisele GE ühiskonnas laiemalt. Prioriteetsed tegevused on seotud edaspidi GE digi- ja küberturbe arendamisega (kriitilise taristu kaitse, ühiskondliku küberteadlikkuse ja -hügieeni tõstmine, ekspertide väljaõpe, rahvusvahelised koostööõppused jms). Muutuste tuules võttis Eesti poolelt SNGP juhtrolli üle Välisministeerium, mis koordineerib initsiatiivi raames edasisi GE küberturvalisuse tõstmiseks suunatud tegevusi.

Juhtrolli ülevõtmise raames on toimunud kohtumised peamiste GE küberjulgeolekuga tegelevate asutuste ja doonoritega, kaardistatud nende ootusi, võimalusi ja murekohti, et liikuda efektiivselt tulemuste suunas. Initsiatiivi juhina on Välisministeeriumi eesmärk vahendada Eesti küberkogemust ja toetada GE asutuste püüdlusi ühiskonna küberturvalisuse tõstmisel.

Jätkub töö GE-EE eksperttaseme kohtumiste planeerimisel - eesmärk korraldada lühiajalisi seminare/töötubasid teemadel, mis GE jaoks on eriti aktuaalsed. Koostöö planeerimisel ootame tõhusat ja praktilist suhtlust Eesti kübervaldkonna asutustega!

RIA küberturvalisuse aastaraamat 2023

2022. aastal toimus Eesti küberruumis 2672 küberintsidenti, mis mõjutasid Eesti inimesi, ettevõtteid ja teenuseid. Suurima kasvu tegid ummistusrünnakud, mida kasutatakse aina enam välispoliitilise mõjutusvahendina.

Ettevõtlus- ja infotehnoloogiaminister Kristjan Järvani sõnul tuletas möödunud aasta meelde, et vabadus, sõltumatus ning turvatunne pole enesestmõistetavad.

„Sõda Ukrainas on valusal viisil näidanud, et küberturvalisus on riikliku julgeoleku üks nurgakivi. Aktiivne tegevus küberruumis ei toimu ainult füüsilise sõjategevuse ajal, vaid ka eelneb ja järgneb sellele. Tuhandete inimeste igapäevase pingutuse tulemusena on Eestist saanud üks arenenumaid digiriike maailmas, mis pakub sadu kõrge kvaliteediga e-teenuseid. Ometi muudab see meid ka ainulaadseks sihtmärgiks," ütles Järvan.

Minister lisas, et seisame küberruumis silmitsi pidevalt muutuva ohupildiga, mis tähendab riskipõhist reageerimist nii organisatsioonide infoturbes kui ka riigi julgeolekus.

Ta tõi välja, et mullu toimus Eesti vastu suunatud küberrünnakute intensiivsuses hüppeline kasv, kuid Eesti on hästi hakkama saanud ja suurem osa rünnakutest on jäänud üksnes katseteks.

"Meie eesmärk peab olema läbivalt küberturvaline Eesti, mis suudab tõhusalt kohaneda tehnoloogia arengute ja uute võimalike ohtudega. Seetõttu on täiendavate investeeringute suunamine küberturvalisuse valdkonda ja koostöö parendamine võtmetähtsusega. Selle hea näide on valitsuse otsus eraldada baaseelarvesse vahendid iga aasta 42 miljoni euro ulatuses. Oluline on õppida ja õigel ajal märgata, kohaneda ning reageerida, sest ründajad teevad täpselt sama," rõhutas minister.

„Aasta tagasi ennustasime, et kui Venemaa ründab Ukrainat, siis muutub Eesti küberruum palju tulisemaks. Kahjuks pidas nii sõjaennustus kui ka meie prognoos paika. Oleme pärast 24. veebruari praktiliselt kübersõjas, kus pea iga päev või nädal toimuvad ründed ja nende katsed. Nägime väga mitmel korral, et teenuste häirimiseks mõeldud ründed käisid käsikäes Eesti riigijuhtide ja poliitikute sõnavõttude ja seisukohtadega. Augustis, kui Narvast teisaldati tank, sooritati Eesti vastu rekordilised 66 ummistusrünnakut. Hea ettevalmistuse tõttu ei olnud neil tuntavat mõju, kuigi ründajad õppisid ja arenesid kogu aasta. Aasta alguses ja lõpus toimunud rünnete vahel on selge kontrast," ütles RIA peadirektor Margus Noormaa.

Ta lisas sarnaseid tõuse oli näha ka siis, kui Riigikogu kuulutas Venemaa terroristlikuks riigiks ning Ukraina president esines video teel rahvasaadikutele. Rünnakute mõju Eesti organisatsioonidele, asutustele ja ettevõtetele oli marginaalne, kuid katkestusi esines.

„Tänu valitsuse rahasüstile suutsime ründajatest ühe sammu ees olla ning suutsime napilt enne massilisi ründeid kaitselahendused püsti seada. Täiendavate meetmeteta olnuks pilt sootuks

teine," rõhutas Noormaa. Sarnased ründed jätkuvad ka tänavu ning viimane suurem laine algas 23. jaanuaril, kui sihikule võeti finants- ja kindlustussektor.

Noormaa lisas, et RIA aitab tagada digiriigi toimimise riigisektoris ning igale poole ei jõuta.

„Meie seire leiab päevas sadu nõrkuste või viirusega nakatunud seadmeid. Selle info edastame kohe teenusepakkujatele, kelle kliendid on ohus. Minu tungiv palve on, et see info haavatavustest edastatakse kliendile. Oluliselt odavam on õppida teiste, mitte oma vigadest. Kui meie hoiatustele jäetakse reageerimata, siis pole tavatu, et meie nõu küsitakse siis, kui küberintsident on juba ettevõtet laastanud," lausus RIA peadirektor.

RIA sai mullu info 2672 mõjuga küberintsidendi kohta (seda on ca viiendiku võrra enam kui 2021. aastal). Kõige rohkem tuvastati ja anti teada inimeste andmeid koguvatest õngitsuslehtedest (1206), teenusekatkestustest (344) ja kasutajakontode ülevõtmisest (236). Pettustest teavitati 224-l ning kontode kompromiteerimistest 164 korral. RIA-le anti mullu teada 302 ummistusrünnakust, millest 100 olid mõjuga, ning 21 lunavararünnakust.

RIA küberturvalisuse aastaraamat keskendub Eesti küberruumi juhtumitele ja statistikale. Juttu tuleb ummistusrünnakutest, Venemaa küberrünnakutest Ukraina asutuste ja ettevõtete

vastu, lunavararünnakutest, turvanõrkustest, valimiste kaitsmisest ja netipettustest. Lugusid leiab ka sellest, kuidas muuta Eesti läbivalt küberturvaliseks ning millised olid möödunud aasta suurimad küberintsidendid mujal maailmas.

Küberturvalisuse aastaraamatut saab alla laadida RIA kodulehelt.

Peaminister Kaja Kallas külastas RIA-t

Infot on alati hea saada allikale võimalikult lähedalt.

Sestap oligi rõõm rääkida 26. jaanuaril peaminister Kaja Kallasele otse, millega Riigi Infosüsteemi Amet tegeleb. Esmalt andis juhtkond ülevaate nendest kümnetest olulistest teenustest, mis RIA õlul ja vastutada on, edasi suunduti maja peale väikesele ringkäigule.

Foto: Riigi Infosüsteemi Amet

Peaminister kuulis CERT-EE tiimi ekspertidelt, kuidas ja mida nad seiravad Eesti küberruumis ning mis moodi lahendatakse küberintsidente. Seejärel kohtus ta analüüsi- ja ennetusosakonna analüütikutega, kes kirjutavad ka peaministri lauale jõudvaid küberruumi ohuhinnanguid ja ülevaateid.

Juttu tuli ka valimistest ja nende toimumiseks hädavajalike infosüsteemide arendamistest. Edasi liiguti Riigivõrgu osakonda. Sealne tiim vastutab selle eest, et Eesti riigiasutustel oleks olemas andmeside ja internet.

Olukord küberruumis

Jaanuaris avaldas RIA ülevaate 2022. aasta IV kvartali trendidest ja tähelepanekutest küberruumis.

Eelmise aasta viimast kolme kuud iseloomustavad suured õngitsuslained, veebikestad, mis ohustavad kaitsetuid veebilehti, suur hulk ummistusründed ning Eestis toimunud unikaalne küberõppus.

Täpsemat ülevaadet loe RIA koduleheküljelt rubriigist olukord küberruumis.

Osale e-hääletamise vaatlusprogrammis

Riigi valimisteenistus pakub Riigikogu valimiste eel võimalust osaleda koolitusel, kus selgitatakse ja tehakse läbi elektroonilise hääletamise toimingud. Koolituse eesmärk on anda e-hääletamise vaatlemisest huvitatutele protsessi paremaks mõistmiseks vajalikud teadmised.

Elektroonilise hääletamise koolitus toimub seminari vormis nädal enne valimisi. Selle käigus tehakse läbi kõik e-hääletamise protseduurid, räägitakse lahti süsteemi turvalisust tagavad meetmed ja vastatakse osalejate küsimustele.

Koolituse käigus toimub ka elektroonilise hääletamise esimene vaatlusvoor, kus luuakse hääletamise salajasust tagav krüptovõtmete paar. Koolituse viimasel päeval toimub e-hääletamise süsteemi täielik kontroll ehk prooviläbimine.

Koolitus on jaotatud kolmele päevale, 14. veebruarist 16. veebruarini. Osaleda on võimalik veebi teel ja piiratud arvul inimestel ka kohapeal.

Koolitusele tuleb registreeruda hiljemalt **7. veebruaril,** andes oma soovist e-kirjaga märku aadressil vaatlemine@valimised.ee.

Detailsem info koolitusprogrammi kohta on leitav valimiste veebilehelt.

ANDMEKAITSE INSPEKTSIOON

Andmekaitse Inspektsioon

Euroopa ühisuuring tõi suuremate puudustena välja muuhulgas vähese teadlikkuse, puuduliku mõjuhindamise ning üheselt määratlemata rollid

Euroopa Andmekaitsenõukogu eestvedamisel läbiviidud esimene andmekaitse ühisjärelevalve, mis võttis luubi alla pilveteenuste kasutamise avalikus sektoris.

Ühisjärelvalve leidis, et suurematekskitsaskohtadeks uuritavates asutustes olid vähene teadlikkus sellest, kas ja milliseid isikuandmeid pilvteenustes töödeldakse. Valdavalt puudusid asutustel andmekaitseliste mõjude hindamised, puudulikult olid ka määratletud andmetöötlusega seotud rollid asutuste ja pilveteenuse osutaja vahel.

Kokku osales uuringus 22 andmekaitseasutust üle Euroopa, nende hulgas Andmekaitse Inspektsioon. Inspekteeriti ligi 100 Euroopa Liidu ja riikide avaliku halduse institutsiooni, mis tegelevad tervishoiu, rahanduse, hariduse, transpordi ja infotehnoloogiaga. Uuringu aluseks oli liikmesriikide ühiselt koostatud küsimustik, mida sai vastavalt vajadusele ka kohandada. Eelkõige uurisid järelevalveasutused, millised on avaliku sektori asutuste peamised väljakutsed isikuandmete kaitse üldmääruse järgimisel pilvepõhiste teenuste kasutamisel. Eestis olid seiresse kaasatud Transpordiamet, Eesti Haigekassa, Haridus- ja Teadusministeerium ning Tallinna Linnavalitsus.

Lisaks kolmele väljatoodud sagedasemale puudusele tõi uuring organisatsioonide puhul välja veel puudulikku teadmist pilveteenuse alltöötlejast, diagnostika ja telemeetria andmete töötlusest ja rahvusvahelisest andmeedastusest. Ka ei vastanud lepingud alati isikuandmete kaitse üldmääruse artikkel 28 nõuetele.

"Meie eesmärk oli kaardistada pilveteenuseid kasutavate asutuste kitsaskohad ja koostada neile soovitused probleemide ületamiseks ning riskide haldamiseks. Ikka selleks, et avalike pilveteenuste kasutamisel oleks isikuandmed kaitstud," märkis Andmekaitse Inspektsiooni tehnoloogia valdkonnajuht Urmo Parm. Ühiselt kokkupandud soovitused on plaanis avaldada lähiajal, lisaks soovituste avaldamisega on kavas seires osalenud asutustele avastatud kitsaskohti ja edasisi soovitusi ka eraldi tutvustada.

EuroStati andmetel on pilveteenuste kasutamine ettevõtetes viimastel aastatel kogu Euroopa Liidus mitmekordistunud. Koroonapandeemia tõi kaasa organisatsioonide ümberkujundamise ning ka paljud avaliku sektori asutused on asunud kasutama üha enam pilvepõhiseid tehnoloogiaid. Seejuures võib aga riigi- ja kohaliku omavalitsuse asutustel olla keerukas leida tooteid ja teenuseid, mis vastavad ELi andmekaitsereeglitele.

Ühisalgatuse laiem eesmärk oli ühtlustada ja tugevdada andmekaitselast järelevalvet Euroopas ning tõhustada andmekaitseasutuste rahvusvahelist koostööd.

Pilveteenuste seire kokkuvõtet on võimalik lugeda siit.

CYBERNETICA

Cybernetica

Cybernetica ja EY hakkavad ümber kujundama EL-i rahastatud projekti raames Maksu- ja Tolliameti süsteeme

Cybernetica koostöös EY-ga (endine Ernst & Young) hakkavad tegema eeltööd loomaks plaani Eesti Maksu- ja Tolliameti (MTA) maksukohustuslaste registri välja vahetamiseks.

Tegemist on Euroopa Liidu reformide ettevalmistamise rahastust (TSI) finantseeritud projektiga, mille viib ellu EY koostöös Cyberneticaga, kes osaleb projektis allhankijana, ning Euroopa Komisjoni struktuurireformide toe peadirektoraadiga (DG REFORM).

„Projekti eesmärk on kaardistada vundamendi seisukorda, millele toetuvad riigi jaoks elutähtsad teenused. Nii saame teada, milliseid samme on vaja astuda, et tagada maksumaksjatele lihtsad ja mugavad teenused ning nende areng ka tulevikus," ütles Maksu- ja Tolliameti äriarhitekt Anni Uibu. „Ootame projekti raames koostööpartnerilt tegevuskava, vajalikke mõjuanalüüse ning riskihinnanguid, mille pealt oleks MTA-l võimalik edaspidiseid otsuseid teha."

Maksukohustuslaste registrit hakati ehitama juba 1998. aastal. Selle eesmärgiks on andmete kogumine maksuseadustest ja teistest seadustest tulenevate ülesannete täitmiseks, arvestuse pidamine maksude tasumise õigsuse kontrollimiseks, maksude määramiseks ja sissenõudmiseks. „Tänaseks on sellest saanud

keerukas ja mahukas register, mis koondab erinevaid IT süsteeme ja alamregistreid ehk suur monoliitne süsteem. EY ülesanne on analüüsida kogu seda süsteemi tervikuna nii ärilisest kui ka infotehnoloogilisest vaatest ning teha kindlaks, kas kõik seal olevad protsessid ja andmed on ka täna kasutuses. Lõppeesmärk oleks leida lahendus ühe suure monoliitse süsteemi jaotamiseks väiksemateks tükkideks ehk modulaarseks, mikroteenustel põhinevaks lahenduseks. Tänu sellisele legoklotsidest koosnevale arhitektuurile, saab tulevane süsteem agiilsem ja kasutajasõbralikum, samas kohanemisvõimeline pidevalt muutuvate oludega," ütles Raivo Ruusalepp EY Eesti konsultatsiooniosakonnast. EY on projekti vedaja ja analüüsib registri ümber kujundamise ärilist vaadet.

„Meie pikaajalise ja eduka koostöö käigus Eesti Maksu- ja Tolliametiga oleme saanud hea ülevaate kliendi süsteemidest ja vajadustest, mis hõlbustab meil seda projekti teostada," kommenteeris Cybernetica maksu- ja tolliinfosüsteemide osakonna projektijuht Urmo Braun. „Projekti sisuks on maksukohustuslaste registri analüüs. Cybernetica analüüsib MTA äriobjektide omavahelisi seoseid ning pakub välja monoliitse infosüsteemi tükeldamise kava ja strateegia ning uue infosüsteemide arhitektuuri," rääkis Braun.

Cybernetica üle kahekümneaastane kogemus tolli infosüsteemide arendamises on loonud hea pinnase olemaks Maksu- ja Tolliameti süsteemide arenduspartner.

Projekt viiakse ellu DG REFORMi toel, mille eesmärk on aidata EL-i liikmesriikidel kujundada ja rakendada struktuurireforme. Töö valmib 2024. aasta septembriks.

Cybernetical on pikaajaline kogemus keeruliste, tugevate turvanõuetega infosüsteemide arendamiseks, mille kompetentsi kuulub terve tarkvaraarendus: nii eel-, äri- kui ka süsteemianalüüs, arendus, testimine, juurutus ning hooldus. EY Eesti konsultatsiooniosakonnal on suur kogemus digiriigi teenuste disainimisel ning oma äritegevust kasvatada ja optimeerida soovivate ettevõtete nõustamisel.

European Telecommunications Standards

ETSI/IQC Quantum Safe Cryptography Event

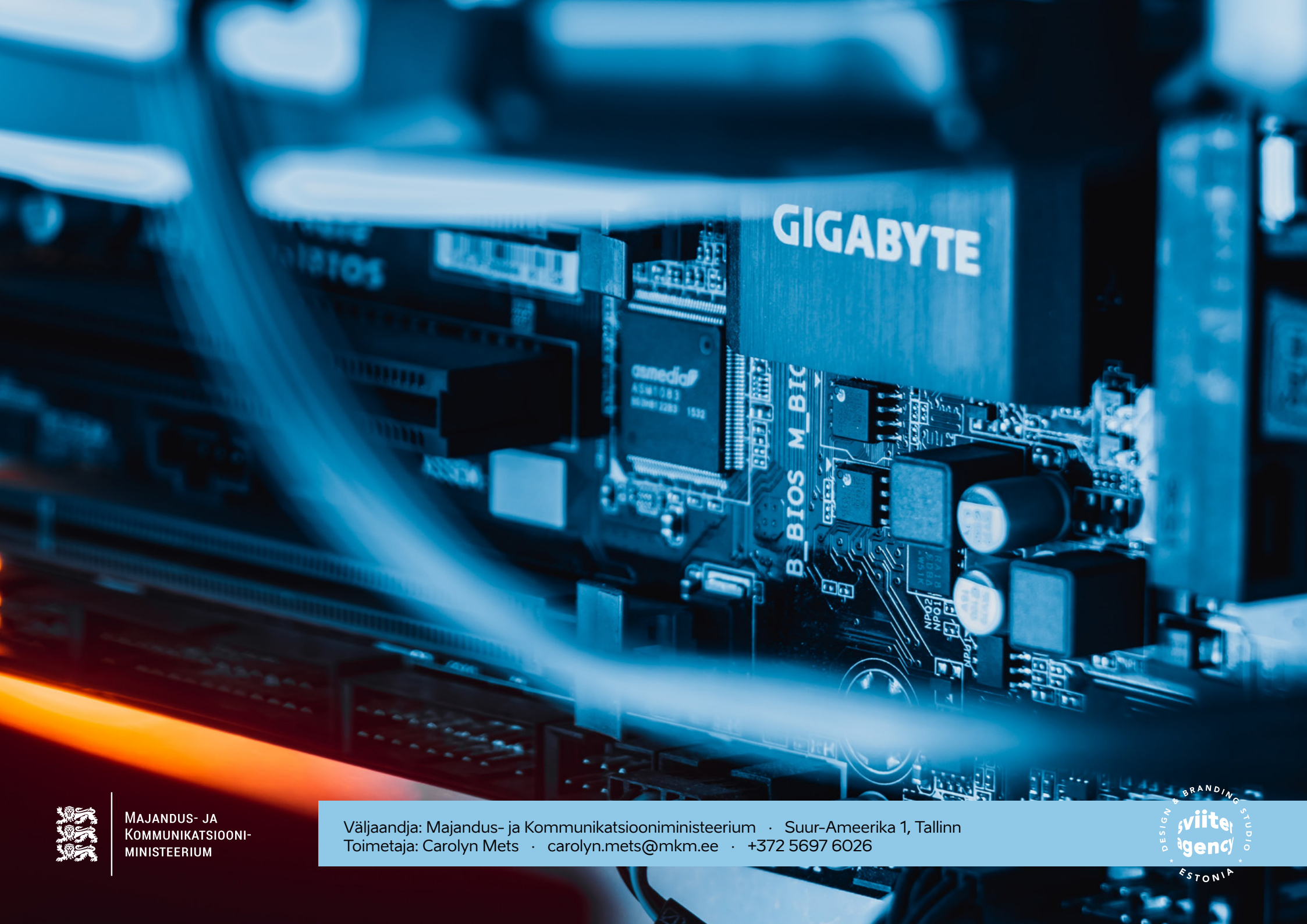
ETSI-l ja Institute for Quantum Computing-il on hea meel teid teavitada 9. Quantum Safe Cryptography Event'ist, mis toimub 13.-15. veebruar füüsiliselt Prantsusmaal.

13. veebruar — An Executive Track: mõeldud ettevõtete juhtidele, sealhulgas tegevjuhtidele, CTO-dele ja CISO-dele. Seal on võimalus kõrgetasemeliste paneeldiskussioonide kaudu saada rohkem teavet riikide tegevuste ja poliitikasuundade kohta, kuulda infosüsteemide pakkujatelt kvantohutu migratsiooni perspektiividest ja viimasena kuulda kvantohutute lahenduste kasutuselevõtust.

14.—15. veebruar — A Technical Track: mis uurib täpsemalt ohutuid kvant tegevusi kogu maailmas, PQC ja QKD integratsiooni, migratsiooni lähenemisviise, migratsiooni ja jõudluse väljakutseid, haavatavust, valideerimist, testimist ja sertifitseerimist.

See tulevikku vaatav üritus toob kokku kvantturvalise küberjulgeoleku kogukonna osalejad üle kogu maailma ning hõlbustab teadmiste vahetamist ja koostööd, mis on vajalik küberinfrastruktuuride ja äri tavade üleminekuks ning nende turvaliseks muutmiseks kvantarvutite ajastul. Kogu üritus on tasuta.

Registreerimine ja lisainfo siin.



Majandus- ja Kommunikatsiooni-
ministeerium

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

Design & Branding Studio sviite agency Estonia