Riikliku küberturvalisuse uudiskiri

2022-10

Majandus- ja kommunikatsiooniministeerium

Küberkerksuse õigusakti ettepanek

Riigi Infosüsteemi Amet

E-riik on elektrikatkestuseks valmis

Cybernetica

Cybernetica toetab Eesti e-riiki ja küberjulgeolekut uute uurimisprojektidega

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Majandus- ja Kommunikatsiooniministeerium

Küberkerksuse õigusakti ettepanek 3

Miks me teeme muutusi KüTSis pilve osas? 3

ÜRO 2022. aasta digiriigi edetabelis on Eesti avaliku sektori e-teenused maailma parimad 4

Tallinn Digital Summit 4

Küberturvalisuse poliitika nõukoda keskendus riskide- ja ohtude kaardistamisele 5

Riigi infosüsteemi Amet

E-riik on elektrikatkestuseks valmis 5

Küberrünnakud meediamajade vastu kasvasid 5

Üle-Euroopaline küberturvalisuse kuu algas teavituskampaaniaga 6

Tarbjakaitse ja Tehnilise Järelvalve Amet

ETSI kvant-turvalisuse krüptograafia töötuba 7

TalTech

Digiturvalise kooli programmi ideekava on küpsemas 7

Cybernetica

Cybernetica toetab Eesti e-riiki ja küberjulgeolekut uute uurimisprojektidega 8

Küberkerksuse õigusakti ettepanek

Septembri keskel esitas Euroopa Komisjon kauaoodatud küberkerksuse õigusakti ettepaneku, et kaitsta tarbijaid ja ettevõtjaid ebaturvaliste toodete eest.

ELi-ülese õigusakti eesmärk on nii Euroopa Liidu üldise kübeturvalisuse suurendamine kui ka lõpptarbija kaitsmine – hetkel kannavad näiteks küberrünnaku puhul peamist rahalist ja mainekahju toodete kasutajad, isegi kui rünnak oli võimalik vaid tänu valmistajapoolsele puudujäägile. Uued nõuded ja kvaliteedimärgis aitaksid lõpptarbijal toodete ostmisel ja kasutamisel paremaid valikuid teha. Ühtlasi katab eelnõu toodete küberturvalisuse nõudeid terve nende eluea jooksul, vähendades nõnda vastutuse hajumist

EL Digitoodete ja küberturvalisuse maastik on kaetud paljude õigusaktidega – mainimist vääriksid näiteks:

- NIS direktiiv,
- küberturvalisuse määrus,
- raadioseadmete direktiiv,
- üldine tooteohutuse direktiiv,
- tootja vastutuse direktiiv,
- samuti isikuandmete kaitse üldmäärus ja
- sektori-spetsiifilised õigusaktid nagu masinadirektiiv ja hetkel uuenduskuuri läbiv tehisintellekti määrus.

Küberkerksuse akt peaks aitama luua pädevatele asutustele ja turuosalistele selgust, millal mõni konkreetne õigusakt kohaldub, samuti kindlust, et erinevates õigusaktides ei ole kattuvusi.

Küberkerksuse akti eelnõu jaotab digiosadega tooted kahte kategooriasse: n-ö kõrgendatud riskiga tooted (ca 10% turust, nt brauserid, paroolihaldustarkvara, võrguhaldustarkvara, operatsioonisüsteemid) ja ülejäänud. Viimaste puhul jääks eelnõu järgi nõuetele vastavus tootja enda hinnata, kõrge riskiga tooted aga peavad läbima hindamise, kas määratud riigiasutuse või sertifitseeritud kolmanda osapoole juures. Eesti täpsemad seisukohad õigusakti osas on hetkel veel koostamisel.

MKM-i jaoks on oluline, et protsess oleks korraga läbipaistev ja tõhus ning et väiksematele või keskmistele ettevõtetele ei kehtestataks nende nõuetega liigset administratiivkoormust. Praeguses faasis tekitab küsimusi ka tulevane vastutusjaotus keerulisemate tarneahelate puhul, kus müüdav toode kujutab endast näiteks originaali modifikatsiooni. Määruse kohaldamisalast on välja jäetud teenused (nt tarkvarateenused), kuigi osad liikmesriigid on nende hõlmamist juba nõudnud.

Miks me teeme muutusi KüTSis pilve osas?

Majandus- ja Kommunikatsiooniministeerium (MKM) töötab küberturvalisuse seaduse (KüTS) määruse kallal, mis võimaldab Eesti riigi toimimise jätkumise ka siis, kui Eestis paiknevad andmekeskused ei tööta.

Majandus- ja Kommunikatsiooniministeerium (MKM) töötab küberturvalisuse seaduse (KüTS) määruse kallal, mis võimaldab Eesti riigi toimimise jätkumise ka siis, kui Eestis paiknevad andmekeskused ei tööta.

Muudatuse jõustumisel on avalikul sektoril võimalus hoida andmeid ja e-teenuseid välismaistes pilveserverites. Just analoogse lahenduse aitas Eesti ehitada kevadel Ukrainal, puuduliku seadusandluse tõttu ei ole samaväärselt kaasaegset e-lahendust olnud võimalik Eestile luua.

Ministeerium on kaalunud, kas ja kuidas võiks tulevikus lisaks andmete varundamisele toimuda andmesaatkonnast ka teenuste pakkumine, kui näiteks Eestis olevatel andmekeskustel on koormus liiga suur või kui miski on rivist väljas. Sel aastal saab Luksemburgis asuva andmesaatkonnaga sõlmitud leping läbi, kus Eesti on varasemalt juba aastaid varundanud avalike ülesannete täitmiseks olulisi andmeid. Kuigi Eesti soovib seda pikendada, otsitakse lisaks ka teisi riike, kus analoogne lahendus püsti panna ning otsitakse veel viise, kuidas tagada avaliku sektori e-teenuste töö kriisiolukorras.

MKMi IT arhitektuuri ja taristu nõuniku Allan Allmere sõnul soovib Eesti e-riigina tehnoloogia arenguga kaasas käia ning ministeerium näeb avaliku pilve kasutuselevõtmisega positiivset muutust nii teenuste käideldavusele kui ka uute teenuste väljatöötamisele. Sellega seoses on töötatud välja eelnõu KüTSi muutmiseks, mis annaks avalikule sektorile võimaluse avalike pilvetehnoloogiate kasutamiseks.

Määruse kohaselt võib välismaistes pilvsüsteemides hoiustada ka mitte-salastatud teavet, mis puudutab sõjalist riigikaitset, kuid sel juhul peavad andmed olema eelnevalt krüpteeritud. Krüpteerituna tohib pilves hoida ka asutusesiseseks kasutamiseks määratud teavet.

Tänapäeva pilvtehnoloogia pakub palju skaleerimis- ja

innovatsioonivõimalusi, millest Eesti ei soovi e-riigina ilma jääda. Arenguid peab tegema samm-sammu haaval ja pidevalt kaaluma erinevaid riskistsenaariume ning meetmeid.

Eelnõu kohaselt peab pilvteenuse kasutaja kaaluma riske, mida toob endaga kaasa pilveandmetöötlusteenuse kasutamine ehk kas ning mil määral seda teenust kasutatakse. Hetkel töötab ministeerium eelnõu sisu muudatuste kallal, seega võib enne jõustumist veel muudatusi toimuda.

ÜRO 2022. aasta digiriigi edetabelis on Eesti avaliku sektori e-teenused maailma parimad

ÜRO avalikustas 28. septembril oma 2022. aasta digiriikide edetabeli, kus Eesti avaliku sektori e-teenuseid hinnati maailma parimateks. Tallinna linna e-teenused hinnati Berliini ja Madridi järel maailmas paremuselt kolmandale kohale.

Uuringus rõhutatakse digitaalse valitsemise kasvavat rolli jätkusuutliku tuleviku loomisel ja mitmetahuliste kriisidega toimetulekul. Digitehnoloogiad mängivad viimastel aastatel järjest suuremat rolli ülemaailmse tervishoiukriisiga seotud probleemide lahendamisel ja oluliste avalike teenuste tagamisel isolatsiooni, ebakindluse ja haavatavuse perioodil.

E-teenuste puhul hinnatakse muuhulgas seda, kui suur hulk teenustest on e-teenusena kättesaadavad, aga ka nende kasutusmugavust, avaandmete kättesaadavust, töökindlust ja turvalisust. Tähtsad on ka teenuste kättesaadavus erivajadustega inimestele, kodanike kaasatus, andmete kaitse ja muu inimõigustega seonduv.

ÜRO uuringutulemuste raport sisaldab hinnangut e-valitsuse kohta kõigi 193 ÜRO liikmesriigi suurima rahvaarvuga linnades.

Tallinn Digital Summit

Tallinn Digital Summit (TDS) on kujunenud iga-aastaseks digitaalseks lipulaevaks, mis toob kaasa uusimat tipptasemel inimkeskset digipoliitikat ja pakub edukat platvormi uute teemade käivitamiseks globaalsel areenil.

TDS toob kokku juhid sarnaselt mõtlevatest ja digitaalselt arenenud riikidest, rahvusvahelistest organisatsioonidest ja erasektorist, et tegeleda tänaste ja homsete kõige pakilisemate probleemidega. Tuginedes Eestis omandatud praktilistele kogemustele ja mõttekaaslastele, püüame lükata dialoogi, partnerlussuhteid ja praktilisi projekte läbipaistvama, turvalisema ja vastutustundlikuma väärtustel põhineva tuleviku poole.

Selle aasta tippkohtumisel keskendutakse usaldusväärse ühenduvuse pakkumisele usaldusväärsete partnerluste kaudu. Tippkohtumisel luuakse sillad erinevate ühenduvusalgatuste vahel ja selgitatakse välja, milline on usaldusväärne ja turvaline digitaalne ühiskond. Samuti antakse valitsustele, finantsasutustele, rahvusvahelistele organisatsioonidele, tehnilistele ekspertidele ja erasektorile konkreetseid samme, et tagada meie demokraatlike väärtuste, inimvabaduse ja inimväärikuse ning reeglitepõhise rahvusvahelise korra valitsemine.

MAJANDUS- JA KOMMUNIKATSIOONI-MINISTEERIUM

RIIGI INFOSÜSTEEMI AMET

Riigi infosüsteemi Amet

Küberturvalisuse poliitika nõukoda keskendus riskide- ja ohtude kaardistamisele

Septembrikuu keskel toimus taaskordne Majandus- ja Kommunikatsiooniministeeriumi Riikliku küberturvalisuse osakonna (RKO) kogukonnakaasamise üritus - küberturvalisuse poliitika nõukoda (KPN).

Kohtumisel jagati MKM ja haldusalade poolt infot hetkel käimasolevate protsesside kohta ning tekitati diskusiooniga võimalus ühiselt valdkondlike teemasid arutada.

Lisaks kaardistati küberturvalisusega seotud ohte ja riske. Antud sisendi protsessiga läheb RKO edasi ning koondatud ideid võetakse sisendiks edasiste plaanide seadmisel ja olemasolevate arengukavade ja plaanidega sidumiseks.

Oleme tänulikud RKO juures olevale koostoimivale võrgustikule, tänu millele saame sisulist koostööd teha erinevate osapooltega ning läbi selle ühiste väärtuste eest seista.

E-riik on elektrikatkestuseks valmis

E-riigi toimimise eest vastutav MKM haldusalas riigi infosüsteemi amet (RIA) on peadirektor Margus Noormaa kinnitusel potentsiaalseks mitmetunniseks elektrikatkestuseks valmis suutes sellises olukorras digiriigi toimimise tagada.

RIA suudab enamus lahendusi hoida töös veel 24-tundi pärast elektrikatkestuse algust ning osadel juhtudel isegi veelgi kauem. Digiriigi baaskomponentide ehk riigivõrgu, autentimise ja X-tee töö on samuti tagatud. Autentimisteenuste ehk ID-kaardi ja mobiil-ID töö osas on RIA suhelnud SK ID Solutionsi esindajatega, kellelt on saadud veendumus, et kõik on kontrolli all ja tagatud ka elektrikatkestuse korral.

Pikaajalise elektrikatkestuse ohu korral käivitab RIA kriisistaabi töö, kuhu kutsutakse olulised partnerid kohale. Füüsilise staabi moodustamine võtab RIA juhi sõnul paar tundi aega. Kõik eeldused ja valmisolek on selleks loodud ja seda on õppuste käigus harjutanud. Läbi RIA pakutakse riigivõrgu kaudu internetiühendust kriitilistele teenusepakkujatele nagu näiteks haiglatele ja piiripunktidele.

Riigiasutused on valmisolekuga tegelenud pikalt, osapooled on kõikidest kriisidest väga palju õppinud ja püütakse kogu aeg oma valmisolekut ja võimekust vastavalt suurendada. Viimane elektrikatkestuste stsenaariumi õppus leidis aset septembri lõpus, ning sujus plaanipäraselt.

Küberrünnakud meediamajade vastu kasvasid

Riigi infosüsteemi amet (RIA) koostas neile teatatud andmete põhjalt ülevaate Eesti meediaportaale tabanud küberrünnakutest. Võrreldes kahe eelmise aastaga on mõjuga küberrünnakute arv tõusnud.

Augusti lõpus sattusid Eesti meediaportaalid küberrünnakute alla – rünnati nii Ekspress Gruppi, Postimehe kui ka Õhtulehe veebiportaale. Ekspress Grupi juhi sõnul olid rünnakud augustis nende vastu intensiivsemad kui varem ja neid on rünnatud viimastel aastatel pidevalt. Rünnakute kasvu näitas RIA analüüsi- ja ennetusosakonna ülevaade, mis võrdles viimase kolme aasta teavitusi meediaportaalide vastu suunatud küberrünnakutest.

Kui 2020. aastal registreeris küberintsidentide käsitlemise osakond CERT-EE 13 intsidenti, millest kuuel oli mõju ja 2021. aastal 11 intsidenti, millest seitsmel oli mõju, siis 2022. aasta augusti lõpu seisuga oli teada 27 intsidenti, millest 18 olid mõjuga intsidendid. Selle aasta esimese kaheksa kuuga on meediamajadega seotud intsidentide arv juba kahekordistunud võrreldes terve 2020. või 2021. aastaga.

„Kasvu üheks põhjuseks on kindlasti suurem teadlikkus – inimesed ja ettevõtted annavad meile aasta-aastalt aina enam küberrünnakutest teada. Tõusu taga on ka kindlasti see, et Eesti meediamajad on praeguses geopoliitilises olukorras ja Venemaa sõda taunides Kremli-meelsete küberründajate sihtmärgiks. Rünnetest on saanud välispoliitiline mõjutusvahend, mida kasutatakse, kui ründajate silmis langetatakse ebapopulaarne otsus," ütles RIA CERT-EE osakonna juhataja Tõnu Tammer.

Kasvutrendi analüüsides näeme, et sellele on kaasa aidanud hajusate ummistusrünnete (DDoS-rünnete) tõus. Samuti luuakse rohkem meediaportaale jäljendavaid petulehti. Selliseid petulehti kasutatakse üldiselt finantspettusteks – uudistelehe sümboolika lisamisega üritatakse potentsiaalses ohvris tekitada suuremat usaldust.

Seevastu on hajusate ummistusrünnete eesmärk konkreetse serveri, teenuse või süsteemi kasutuskõlbmatuks muutmine, ummistades sihtmärki suure võrguliiklusega. „Serveri ülekoormamist võime ette kujutada olukorrana, kus 10 000 inimest soovib korraga kaubamajja siseneda. Ostukeskus pole nii suureks külastuseks valmis, see suletakse ning seeläbi ei saa inimesed teenuste juurde," tõi Tammer näite.

Portaalide vastu suunatud rünnakutega proovitaksegi enneköike nende tööd häirida. Seda tüüpi ründeid on ka suhteliselt lihtne teostada. „Kui rünne õnnestub, on see kohe kõikidele kasutajatele näha, sest veebileht ei ole enam kättesaadav. Seega on DDoS-rünnakute puhul potentsiaalne mõju suhteliselt ulatuslik," lisas CERT-EE juhataja.

Nii RIA kodulehelt kui ka blogist leiab abistavaid juhendeid, soovitusi ja postitusi. Amet soovitab liituda CERT-EE uudiskirjaga, mis annab igal hommikul lugejale kõige värskemad ja asjakohasemad kübervaldkonnaga seotud uudised nii Eestist kui ka laiast maailmast. Libalehtede eest aitab nutiseadmeid kaitsta CERT-EE lahendus.

Üle-Euroopaline küberturvalisuse kuu algas teavituskampaaniaga

Kogu oktoober on ENISA eestvedamisel küberturvalisuse ja küberteadlikkuse kuu. Ka RIA korraldab sel puhul mitmeid üritusi. Neist suurim on 3. oktoobril alanud küberturvalisuse teavitus- ja ennetuskampaania, mille eesmärk on juhtida inimeste tähelepanu ohtudele, mis kaasnevad hooletu käitumisega arvutis või nutiseadmes.

Kampaania „Kontrolli üle!" keskendub levinumate petu- ja kuriteoskeemidele, mille tagajärjel jäävad sajad ettevõtted ja inimesed ilma olulistest andmetest, kontodest ja rahast. Lisaks osaletakse nakatunud seadmete kaudu enda teadmata pahavara levitamises, tuues sellega kaasa veel suuremaid kuritegude laineid ning takistusi infosüsteemide töös.

RIA analüüsi- ja ennetusosakonna juhi Märt Hiietamme sõnul on Eesti inimeste teadlikkus erinevate uuringute ja küsitluste järgi aastate jooksul kasvanud, ent ahnete kelmide lõksu langevad ka igapäevaselt nutiseadmetega tööd tegevad inimesed, sest kurjategijad kasutavad ära iga väiksemagi libastumise – valele lingile vajutamise, hooletu paroolidega ümberkäimise või petukirjale vastamise.

„"Kontrolli üle" kutsub üles juba harjumuspärast käitumist veelgi teadlikumalt jälgima – näiteks millisele lingile vajutad, kas kasutad tugevat parooli ja kuhu seda sisestad, kas oled ikka veendunud, et sõbralt saadud e-kiri on ikka sõbra saadetud ning kas see, mida internetist alla laed ja arvutisse paigaldad on turvaline ning vajalik. Need on küll elementaarsed ja väikesed asjad, ent turvalisuse vaatest väga olulised," ütles Hiietamm.

Tänavune kampaania on üles ehitatud juba tuttavale „Ole IT-vaatlik" kampaania visuaalile ning võimendab küberhügieeni algtõdesid, mille rakendamine aitab hoida arvutist ja telefonist eemal pahavara ning kaitsta arvutikasutajaid küberkurjategijate ohvriks langemise eest.

Kampaania kestab kuni 18. novembrini ning kogu selle aja jooksul on nii tänavapildis kui ka erinevates meediakanalites näha ja kuulda mitmesuguseid hoiatavaid ja õpetlikke plakateid, lugusid ning heli- ja videoklippe, mille eesmärk on muuta inimeste käitumist veelgi turvalisemaks.

Kampaania on rahastatud riigi eelarvest ning selle kogumaksumus on veidi üle 200 000 euro. RIA partnerid kampaania elluviimisel on kommunikatsiooni- ja turundusagentuurid Nobel, Arena Media ning Agenda PR. Kampaania korraldamist vedas analüüsi- ja ennetusosakond.

Kampaania materjalid ning soovitused leiab IT-vaatliku kodulehelt.

Tarbijakaitse ja Tehnilise Järelvalve Amet

ETSI kvant-turvalisuse krüptograafia töötuba

ETSI (European Telecommunications Standards Institute) ja IQC (Institute for Quantum Computing) on 9. korda korraldamas kvant-turvalisuse krüptograafia üritust.

Töötuba toimub 13.-15. veebruar 2023. aastal ETSI peakontoris Sophia Antipolises, Lõuna-Prantsusmaal.

Sündmus toob kokku erinevad osalejad kvant-turvalise küberjulgeoleku kogukonnas, et hõlbustada teadmiste vahetamist ja koostööd, mis on vajalik küber infrastruktuuride ja äripraktikate üleminekuks, et muuta need kvantarvutite ajastul turvaliseks.

Ürituse täpsem ajakava avalikustatakse detsembris.

Rohkem infot siit.

TalTech

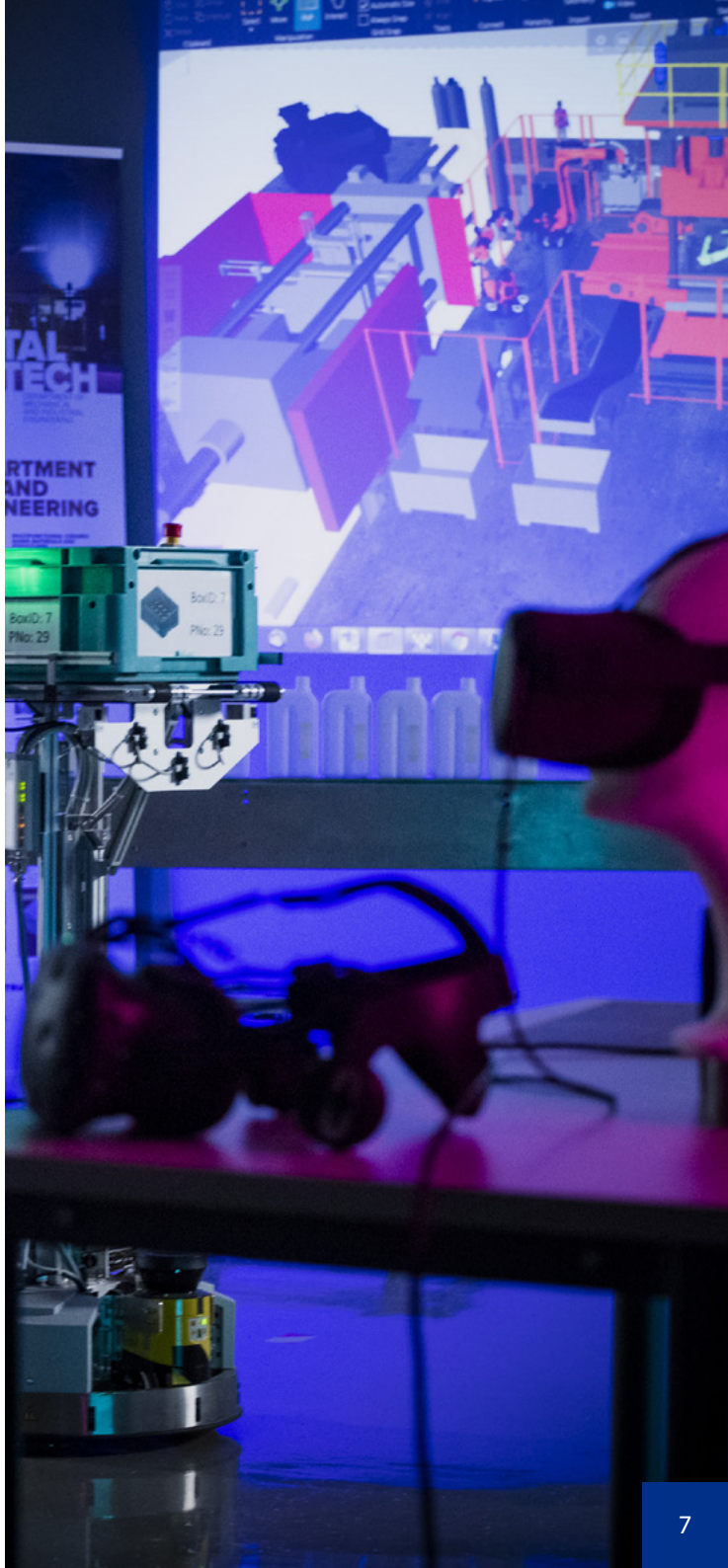
Digiturvalise kooli programmi ideekava on küpsemas

Tallinna Tehnikaülikool viib Majandus- ja Kommunikatsiooniministeeriumi tellimusel ellu enesehindamisvahendi loomist, millega koolid saavad hinnata oma küberturvalisuse olukorda neljas moodulis: dokumentatsioon, keskkond, õppetöö ja inimesed koolis. Ideekava peaks valmis saama detsembriks.

Juba juunist on toimunud koostöö koolide ja ekspertide vahel, et hindamistööriist välja töötada, koolidele arenduslahendusi pakkuda ning arutada, kuidas parimaid näiteid tunnustada ja laiemalt tutvustada. Suurimad mured on koolidel täna Eesti inforturbestandardi (E-ITS) rakendamisega. Sageli ei ole koolides teema eest vastutajat, mistõttu on tegevused selles vallas juhuslikud. Samuti ei viida läbi enesekontrolliteste ning nii õpetajate kui lapsevanemate küberhügieeniteadmised vajavad uuendamist. Välja on toodud ka küberturvalisusele keskendunud huviringide vähesust.

Katsed on läbi viidud 75 kooliga, kus digiturvalisuse teemadega varasemalt tegeletud on ja tegevustel on silma peal hoidnud haridustehnoloog ja/või IT-juht/arvutiõpetaja. Koolides, kus hindamistööriista katsetanud on, hinnati selle läbi viimist kogu meeskonnas oluliseks ning valiti välja tähtsamad arendusteemad. Murekohtadena ja ühiste arendusvajadustena on esile toodud reeglite loomet, teavitustööd peredele, vajadust õppematerjalide ja koolituste järele, jms.

Lisainfo programmi ja enesehindamisvahendiga tutvumiseks: birgy.lorenz@taltech.ee.



CYBERNETICA

Cybernetica toetab Eesti e-riiki ja küberjulgeolekut uute uurimisprojektidega

2022. aasta on olnud edukas aasta Cybernetica osalemiseks teadus- ja arendusprogrammis European Horizon.

Cybernetica Infoturbe Instituut alustab aasta lõpus kolme uue projektiga, mis kõik aitavad kaasa andmepõhiste teenuste arendamisele ning tugevamate küberturvalisuse ja andmekaitsetehnoloogiate loomisele avaliku ja erasektori kasutamiseks.

Projekt nimega TEADAL (Trustworthy, Energy-Aware Federated Data Lakes Along the Computing Continuum) uurib, kuidas tulevikus töödelda andmeid, mida jagatakse erinevate kasutajate mobiilseadmete ja erinevate teenusepakkujate andmekeskuste vahel. Sel viisil levitatud andmeid tuleb töödelda teatud viisil, et mitte lekkida volitamata isikutele. Andmekeskused on järjest suuremad energiatarbijad, mistõttu TEADAL projektis pööratakse tähelepanu andmetöötluse energiatõhususele. TEADAL arendab tehnoloogiaid ja nende valikumeetodeid ning katsetab neid tervishoius, põllumajanduses, rahanduses, tööstuses ja keskkonnakaitses.

Projekt LAGO (Lessen Data Access and Governance Obstacles) toob kokku Euroopa justiits- ja õiguskaitseorganid ning teadlased, et leida paremaid lahendusi andmete kasutamiseks kuritegevuse ja terrorismivastases võitluses. Projektiga uuritakse, kuidas eetiliselt, ohutult ja seaduslikult jagada andmeid (sh isikuandmeid) teadusuuringuteks, tehisintellekti mudelite arendamiseks ja riskianalüüsiks, mis tugevdaks Euroopa kodanike turvalisust.

Cybernetica ülesanne mõlemas projektis on uurida tõhusaid viise turvaliste andmepõhiste teenuste loomiseks, tuginedes ettevõtte aastatepikkusele uurimis- ja arendustegevusele privaatsuskaitsetehnoloogiate vallas. “Tänapäeva X-tee saab pakkuda kodanikule lihtsat teenust, mille taha on peidetud hajutatud andmebaasid. Meie tulevik on tehisintellekt ja uued andmepõhised teenused. Peame õppima ehitama uusi teenuseid nii, et need kaitseksid hajutatud andmeid ja samal ajal kasutaks energiat säästlikult,” selgitas Cybernetica teadusjuht Dan Bogdanov.

Lisaks andmekaitsele tuleb tagada ka süsteemide kaitse. Seetõttu on Cybernetical au teha koostööd Tšehhi ja Eesti teaduspartneritega uues projektis CHESS (Cyber-security Excellence Hub in Estonia and South Moravia). CHESS uurib küberturvalisuse tulevikutehnoloogiaid. Näiteks postkvantkrüptograafia algoritmide uurimine aitab meil tagada kinnisvara valmisoleku, kui kvantarvutitel õnnestub meie tänapäevane krüptograafia murda. „Õpime küberturvalahendusi paremini analüüsima, testima ja sertifitseerima, seetõttu suudame paremini valida tehnoloogiaid tulevase ID-kaardi, mobiil-ID, Smart ID ja ka X-tee jaoks,“ kommenteerib vanemteadur Liina Kamm.

Majandus- ja Kommunikatsiooni-
ministeerium

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

viite agency
DESIGN & BRANDING STUDIO
ESTONIA