# Riikliku küberturvalisuse uudiskiri

2022-03/04

Majandus- ja kommunikatsiooniministeerium

## Riik investeerib küberturvalisuse kiireloomulisse tõstmisse 30 miljonit eurot

Majandus- ja kommunikatsiooniministeerium

## Küberturvalisuse valdkonna muudatustest

CybExer Technologies

## Tartu Ülikool ja CybExer alustasid koostööd ESTCube-2 ühendamiseks ainulaadse küberturbesüsteemiga

Majandus- ja Kommunikatsiooni-ministeerium

## Seekordses uudiskirjas


### Majandus- ja Kommunikatsiooniministeerium

Riik investeerib küberturvalisuse kiireloomulisse tõstmisse 30 miljonit eurot 3

Küberturvalisuse valdkonna muudatustest 3

Ettevõtlus- ja infotehnoloogiaminister kutsus kokku erakorralise küberjulgeoleku nõukogu 5

### CybExer Technologies

Tartu Ülikool ja CybExer alustasid koostööd ESTCube-2 ühendamiseks ainulaadse küberturbesüsteemiga 6

### E-riigi akadeemia

eGA koostas küberturbe käsiraamatu Tonga Kuningriigile 6

Majandus- ja kommunikatsiooniministeeriumi juhtimisel on valminud uus Eesti digiühiskonna 2030 arengukava. 6

### TalTech

TalTechis kaitses doktoritöö Tiia Sõmer 7

TalTechi seminarides räägiti Venemaa-Ukraina konflikti kübermõõtmest ning küberturvalisuse inimlikest aspektidest 7

Kübervõistlused noortele 7

TalTechi teadlased aitasid kokku panna lugemismaterjale koolidele 7

### Cybernetica

Cybernetica müüs oma lennujuhtimise irdtorni tehnoloogia Adacelile 8

Cybernetica laiendab oma andmevahetustehnoloogiate pakkumist teenusmudeliga 8

Uudiskirjaga liitumiseks saada soov **martin.paluoja@mkm.ee**

## Riik investeerib küberturvalisuse kiireloomulisse tõstmisse 30 miljonit eurot

Valitsus esitas Riigikogule julgeolekukriisist tuleneva lisaeelarve, millega investeeritakse oluliselt ka Eesti küberkaitse tugevdamisse. Kriis Ukrainas on muutnud ohupilti ka küberruumis, mistõttu on tarvis suurendada Eesti võimekust küberrünnakuid ära hoida ja nende mõju minimeerida.

Ettevõtlus- ja IT-minister Andres Sutt ütles, et Eesti kübervõimekuse tõstmine on muutunud hädavajalikuks tulenevalt uutest ohtudest küberruumis. „Eilne rünnak Eesti avaliku sektori veebilehtede vastu on selge näide, et ohud küberruumis meie vastu on ehtsad ja täiesti olemas ning nende kaitset tuleb tõsiselt võtta. Eelmisel sügisel eraldati riigieelarvest 30 miljonit eurot Eesti küberturvalisuse tõstmiseks ja kriitiliste nõrkuste eemaldamiseks, ilma selleta oleks viimase rünnaku mõju olnud tõenäoliselt palju suurem. See näitab, et need investeeringud tasuvad ennast ära ja on Eesti küberruumi kaitseks vajalikud. Küberriskide juhtimine peab olema iga tippjuhi prioriteet," kommenteeris Sutt.

Lisaeelarvest investeeritakse kokku 30,5 miljonit eurot Eesti küberturvalisuse ja küberkaitse võimekuse tõstmiseks, millest kaks kolmandikku läheb riigi keskse küberturvalisuse taseme tõstmiseks ning ülejäänu erinevate ministeeriumite haldusalade võimekuse tõstmisse. Investeeringute abil suurendatakse muuhulgas ka riigi oluliste veebilehtede kaitset sääraste ummistusrünnakute vastu, mida oli näha 21. aprilli õhtul. Lisaks suurendatakse riigivõrgu ja internetiühenduse toimepidevust, tõhustatakse meediakanalite ja raadioeetri seiret, suurendatakse turvatestimist üle valitsemisalade ja investeeritakse teistesse küberturvalisusega seotud tegevustesse.

Tänavusest lisaeelarvest eraldatud 30 miljonit eurot täiendab 2021. aasta sügisel riigieelarvest eraldatud 30 miljoni suurust investeeringut küberturbesse, mille abil eemaldati mitmeid kriitilisi nõrkusi Eesti küberruumist.

## Küberturvalisuse valdkonna muudatustest

Kehtiv küberturvalisuse seadus ning selle esimene muutmine

Küberturvalisuse seadus jõustus 2018. aasta 23. mail ning sellega võeti üle Euroopa võrgu ja infoturbe direktiiv (EL) 2016/1148, mille lühendiks on NIS. Seadusega kehtestati teatud teenuste osutajatele turvameetmete rakendamise ja küberintsidentidest teavitamise nõuded. Samuti täpsustati küberturvalisuse tagamise koordineerimisel ja piiriülese koostöö korraldamisel riikliku järelevalveasutuse ehk Riigi Infosüsteemi Ameti ülesandeid. Seaduse eesmärgiks on tugevdada ühiskonna jaoks määrava tähtsusega teenuste osutamisel ning riigi ja kohaliku omavalitsuse üksuste võrgu- ja infosüsteemide kaitset. Avalikus sektoris oli enne seda seadust kohustus rakendada avaliku teabe seadusest tulenevaid turvameetmeid infosüsteemide kolmeastmelise etalonturbe süsteemi ehk ISKE näol üksnes infosüsteemidele, mis on andmekogud avaliku teabe seaduse tähenduses. Küberturvalisuse seaduse jõustumisega laienes avalikus sektoris (sh kohaliku omavalitsuse üksustes) kohustus rakendada ISKE-st tulenevaid infoturbe meetmeid ka muudele võrgu- ja infosüsteemidele — näiteks meiliserveritele, failiserveritele ja dokumendihaldussüsteemidele.

Vahepeal on Euroopa Liit vastu võtnud uusi õigusakte ning ka Eesti õiguskorras on tekkinud vajadus uuendada küberturvalisuse tagamise nõudeid. Sellest johtuvalt toimub ka küberturvalisuse seaduse esimene muutmine, mis on oma olemuselt ka nö esimene samm revisjoni läbi viimiseks. Esimene muutmine toimub küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seadus 531 SE-ga.

Seaduse eesmärgiks on tugevdada ühiskonna jaoks määrava tähtsusega teenuste osutamisel ning riigi ja kohaliku omavalitsuse üksuste võrgu- ja infosüsteemide kaitset.

Küberturvalisuse seaduse I muutmise eelnõul on kolm peamist eesmärki:

1. ajakohastada küberturvalisuse

seadust, et oleks võimalik kehtestada Eesti infoturbestandard ehk E-ITS ja muud ajakohastatud võrgu- ja infosüsteemide küberturvalisuse nõuded ning seeläbi suurendada nende küberturvalisust;

2. määratleda küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute riiklik koordineerimiskeskuse ülesandeid täitev asutus ning selle ülesannete täitmise korraldus;

3. määratleda riiklik küberturvalisuse sertifitseerimise asutus, selle asutuse järelevalvevolitused ning kehtestada Euroopa küberturvalisuse sertifitseerimise raamistike ja sertifitseerimise kavade rikkumise korral kohaldatavad karistusnormid.

E-ITS on infoturbe halduse kogum, mis tulevikus vahetab välja ISKE. See on ennekõike mõeldud avalikule sektorile, sh elutähtsate ning oluliste teenuste osutajatele, kuid sellest võib eeskuju võtta ka muu erasektor. Teises punktis toodud ülesande saab Riigi Infosüsteemi Amet ning kolmandas punktis oleva ülesande saab Tarbijakaitse ja Tehnilise Järelevalve Amet.

## Küberturvalisuse valdkonna II muutmine ehk revisjon

Kõigepealt — miks muudetakse küberturvalisuse seadusesse suhteliselt lühikese aja jooksul kaks korda? Selleks on erinevad põhjused:

peamiseks põhjuseks on asjaolu, et eelnevalt mainitud teemade reguleerimine ei saa oodata revisjoni teostamist, sh on need seotud Euroopa Liidu õiguse rakendamisega;

küberturvalisuse seaduse aluseks olev NIS-i esimene direktiiv tunnistatakse peatselt kehtetuks ning selle asemele tuleb uues sõnastuses kehtestatud NIS2 direktiiv — hetkel on NIS2 poliitilistes triloogides ning on ootus, et see võetakse sel aastal vastu;

lisaks sellele on Euroopa Liidus ja nõukogus ette valmistamisel ka muid õigusakte, mis tuleb kas üle võtta Eesti õigusesse või teha muudatusi Eesti seadustes, et neid saaks õiguspäraselt rakendada.

Revisjoni käigus on soov korrastada mitmeid teemasid. Toome ülevaate revisjoni teemadest ehk nö kontsentraadi märksõnadena:

valdkondlike õigusaktide ülevaatus ehk:

- siinne muudatus on ka ettevalmistus uue NIS2 direktiivi üle võtmiseks;
- arvestame võimalikul määral ka muid Euroopa Liidus olevate õigusakte ja nende algatusi (nt EIDAS2, DORA, CER jne);
- küberturvalisuse seadusele viitavate õigusaktide ning ka muude õigusaktide (seadused, Vabariigi Valitsuse ja ministrite määrused) üle vaatamine ning vajadusel täiendamine;

üle vaadata/hinnata küberturvalisuse seaduse subjektide ring (nt hõlmata ka riigi asutatud äriühinguid + teadaolevalt toob NIS2 uusi valdkondi juurde);

5G turvalisuse tagamise nõuete eeskujul viime küberturvalisuse seadusesse elektroonilise side seadusesse lisatud nn 12 punkti tarneahelate turvalisuse tagamiseks + sarnased nõuded tekitame ka riigihanke protsessis;

Küberjulgeoleku Nõukogu määratlemine seaduse tasandil;

kriisihalduse reguleerimine (see osa, mis ei lähe tulevasse valmisolekuseadusesse);

järelevalve süsteemi ja —meetmete ning rahatrahvide suuruste üle vaatamine — rahatrahvide suuruste üle vaatamine on tingitud NIS2 direktiivist ning teatavas osas ka küberturvalisuse määrusest;

uurime/mõtleme järgmistel teemadel (kas või kuidas reguleerida/edendada): väiksemate organisatsioonide küberturbe konsolideerimine; white-hat'de tegevuse edendamine; bug-bounty reguleerimine; riigivõrgu kasutamise suurendamine; riigi pakutavad monitooringu seadmed; RTIX kasutamise suurendamine; küberhügieeni testide kohustuslikkus riigiasutustes jne.

Eelnõu koostajate eesmärk on saata revisjoni eelnõu väljatöötamiskavatsus ametlikule kooskõlastusringile käesoleva aasta III kvartaliks ning eelnõu ise ametlikule kooskõlastusringile hiljemalt selle aasta lõpuks.

## Ettevõtlus- ja infotehnoloogiaminister kutsus kokku erakorralise küberjulgeoleku nõukogu

Ettevõtlus- ja Infotehnoloogiaminister Andres Sutt kutsus märtsis kokku erakorralise küberjulgeoleku nõukogu, et arutada Eesti küberkaitse tugevdamist Ukraina-Venemaa sõja kontekstis. Küberjulgeoleku nõukogu keskendus muutunud küberohupildile ja erinevate valitsemisalade tegevustele, mis aitavad tõsta riigi küberturvalisuse taset.

Minister Andres Sutt lausus kohtumisel, et kuigi Eestile otsene sõjaline oht puudub, siis käib Ukrainas konventsionaalse sõjapidamise kõrval ka väga aktiivne sõjategevus Ukraina ja Venemaa küberruumides ning see mõjutab ka Eesti küberruumi ohuhinnangut. „On näha, et Venemaa sõjaline rünnak Ukraina vastu on takerdunud ning iga kaotatud tank ja lennuk kahandab Venemaa sõjapidamise võimekust veelgi. See aga ei mõjuta Venemaa võimekust küberruumis rünnakuid läbi viia ning seetõttu on oluline, et Eesti küberkaitse vastaks samuti ohupildile," ütles Sutt. Minister lisas, et küberrünnakute ja intsidentide kasv ei ole seni olnud ülemäära suur, ent kuna küberruumis puudub eelhoiatus võib see alati hetkega muutuda ning selleks peab ka valmis olema.

Riigi Infosüsteemi Ameti peadirektori asetäitja küberturvalisuse alal Gert Auväärti sõnul on RIA olnud juba nädalaid tõstetud valmisolekus ning CERT-EE jälgib 24/7 küberruumis toimuvat. „Oleme suunanud lisajõudu ettevõtete ja asutuste turvanõrkuste avastamisele ja neist ettevõtetele ja asutustele teada andmisele, et nad saaksid oma IT-süsteemid paigata enne, kui ründaja seda ära kasutab. Samas rõhutan, et RIA ei jõua seda teha kõigi eest ning iga ettevõtte ja asutuse vastutus on oma süsteemid korras hoida," rääkis Auväärt.

Tarbijakaitse- ja Tehnilise Järelevalve Ameti sideosakonna juhataja Oliver Gailan andis kohtumisel ülevaate meediakanalite piiramisest. „Tänaseks on ettevõtjate ja teiste riigiasutuste koostöös piiratud ligipääs ligi 40 telekanalile, mille sisu kihutas vihkamisele ja vägivallale, kutsus üles õigusrikkumistele või milledele rakendusid EL sanktsioonid. Sellega oleme suurema osa inforuumist kaitsnud, kuid samas tasub meeles pidada, et tänapäeva ühiskonnas pole võimalik kõiki info edastamise kanaleid lõpuni kinni panna." tõdes Gailan, kelle sõnul jätkab TTJA Eesti meediaruumi seiret.

Küberjulgeoleku nõukogus anti ka ülevaade Eesti kiireloomulistest küberturbe võimekuse tõstmise vajadustest. „Juba enne Ukraina sõja algust alustasime valitsemisalade ülese kaardistusega, et tuvastada võimelünki ning võimalikke tegevusi Eesti küberturvalisuse taseme tõstmiseks. Oleme kõige kriitilisemad tegevused paika saanud ja nende rahastamisotsused teeme valitsuses järgmistel nädalatel lisaeelarve arutelude raames," lisas Sutt.

Kohtumise lõpetuseks tunnustas minister kõiki asutusi ja ettevõtteid, kes on seni õigeaegselt ja korrektselt oma süsteeme korras hoidnud, uuendanud ning jaganud vajalikku infot nii MKMi, TTJA kui RIAga. „Eriline tänu ka sideettevõtetele, kes on olnud heaks partneriks vaenu õhutavate kanalite piiramisel," lõpetas Sutt.

MAJANDUS- JA KOMMUNIKATSIOONI-MINISTEERIUM

## Majandus- ja kommunikatsiooniministeeriumi juhtimisel on valminud uus Eesti digiühiskonna 2030 arengukava

Arengukava eesmärgiks on omada pikaajalist strateegiat väge täis Eesti digiühiskonna edu tagamiseks, kus kõik inimesed saavad parima digikogemuse. Arengukava on jaotatud kolmeks valdkonnaks: digiriik, ühenduvus ning küberturvalisus.

Arengukava detailsem nn tegevusplaan on Eesti digiühiskonna programm. See annab täpsema ülevaate, sh täisülevaate tegevustest ja meetmete ning tegevuste mõõdikutest ja vastutajatest. Programm luuakse neljaks aastaks ning uuendatakse kord aastas. See annab digiriigile vajaliku paindlikkuse ning kiire reageerimisvõimaluse.

Arengukava lähtub suunistes Eesti 2035 pikaajalisest strateegiast. Peamiseks suunanäitajaks on strateegias seatud eesmärk, et avalikud teenused on kvaliteetsed, etteaimavad ja kättesaadavad igas piirkonnas, tagades inimeste põhiõigused.

Arengukavaga (ka selle ingliskeelse versiooniga) saab tutvuda lähemalt siin.

CYBEXER TECHNOLOGIES

CybExer Technologies

## Tartu Ülikool ja CybExer alustasid koostööd ESTCube-2 ühendamiseks ainulaadse küberturbesüsteemiga

Tartu Ülikooli observatooriumi ja CybExeri koostöös on plaanis luua ESTCube-2 baasil satelliidi juhtimissüsteemist digitaalne kaksik. Kaksikul on samad funktsioonid, mida kasutatakse satelliidi juhtimisel, aga nende rakendamine ei mõjuta ESTCube-2 tööd. Kaksiku peal on võimalik katsetada ja arendada süsteemi vastupanu küberrünnetele ning täiustada saadud kogemuste põhjal originaaljuhtimissüsteemi. Samuti saab seda kasutada satelliitide operaatorite treenimisel.

Poolteist aastat kestev koostööprojekt on maailmas ainulaadne ja ESTCube-2-le lisanduv kloonitav küberturberakendus muudab selle veel huvitavamaks. Pikemas vaates võimaldab poolte ühine teadus- ja arendustöö luua uusi küberturbetööriistu ja -tooteid, mida saab kasutada satelliitjuhtimissüsteemides kogu maailmas. Koostöö loob mitmesuguseid uusi ja põnevaid jätkuprojektide võimalusi ka Eesti kosmoseklastrile.

Projektiga tähistatakse Tartu Ülikooli ja CybExer Technologies OÜ pikemaajalise koostöö algust küberturbevaldkonnas. Selle kinnituseks allkirjastati ka ühiste kavatsuste protokoll.

Projekti abil saab CybExer Technologies OÜ avardada enda loodud küberharjutusväljaku kasutamise viise. Harjutusväljak on IT-süsteemide simuleerimist võimaldav lahendus, mille abil saab katsetada eri süsteemide vastupidavust küberrünnakutele ja kaitset nende vastu.

eGA e-governance academy

E-riigi akadeemia

## eGA koostas küberturbe käsiraamatu Tonga Kuningriigile

Aprillis valmis eGA ekspertide koostatud küberturbe käsiraamat Tonga Kuningriigile, mis aitab tongalastel oma IT-süsteeme ja keskkonda analüüsida ning selle põhjal valida sobivaid kaitsemeetmed. Pärast veealuse internetikaabli jõudmist saareriiki on digiteenused hoogsalt arenenud, kuid kasvanud on ka ohud. Erinevalt Eestist on seal väga suur risk looduskatastoofideks.

Käsiraamatu mõte on juhatad asutusi süstemaatiliselt turvet haldama ja riske hindama. Arvestades Tonga väiksust (rahvaarv on sarnane Tartu linnaga), oli vajalik lihtsustada tuntud rahvusvahelisi raamistikke, samas säilitades kõik oluline. Käsiraamatu kasutamise koolitused seisavad veel ees. Käsiraamatu valmimist toetas Maailmapank projekti „ Tonga küberturbealane konsulteerimine“ raames.

## TalTechis kaitses doktoritöö Tiia Sõmer

TalTechi tarkvarateaduse instituudi doktorant Tiia Sõmer kaitses 3. mail oma doktoritöö "Modelling Financially Motivated Cyber Crime" ("Finantsiliselt motiveeritud küberkuritegevuse modelleerimine").

"Doktoritöös pakutakse rahaliselt motiveeritud küberkuritegevuse mudeldamiseks uus definitsioon ja taksonoomia, ning välja on töötatud JMAP mudel küberkuritegevuse kui protsessi kirjeldamiseks."

Juhendajad: Prof Rain Ottis (Tallinna Tehnikaülikool) ning Dr. Patrick Voss de Haan.

Oponendid: kaasprofessor Hervé Borrion (Londoni Ülikooli Kolledž, Suurbritannia) ja lektor Matti Näsi (Helsingi Ülikool, Soome)

Lähemalt doktoritöö kohta saab lugeda siit.

## TalTechi seminarides räägiti Venemaa-Ukraina konflikti kübermõõtmest ning küberturvalisuse inimlikest aspektidest

TalTechi küberkriminalistika ja küberjulgeoleku keskuse ja USA Eesti saatkonna koostöös on toimunud kaks veebiseminari.

16. märtsil pidas Tuftsi Ülikooli (USA) professor Josephine Wolff veebiloengu Venemaa-Ukraina konflikti kübermõõtmest. Professor Wolff vaatles oma loengus varasemaid näiteid Venemaa küberrünnakutest Eestis, Gruusias ja Ukrainas. Samuti rääkis ta, kuidas kasutavad Venemaa, Ukraina koos teiste riikide ja eraettevõtetega oma kübervõimekust käimasoleva konflikti käigus ning viisidele, mil määral nad käituvad varasematest küberkonfliktidest erinevalt. Loengut on võimalik järele vaadata siit.

20. aprillil  arutleti küberturvalisuse inimlike aspektide üle, mis on muutunud IT maailmas üliloluliseks, et päriselt edukas olla. Lisaks räägiti ka IT ja küberturbe valdkonna võimaluste üle kõikidele ühiskonna liikmetele. Vestlusringis osalesid Dr Wayne Patterson, Catlyn Kirna, Prof Kaido Kikkas ja Dr Birgy Lorenz.

## Kübervõistlused noortele

TalTechi eestvedamisel toimusid mitmed suured kübervõistlused noortele.

KüberNaaskel/CyberSpike on üleriigiline Capture The Flag tüüpi võistlus noortele vanuses 14-25 eluaastat, ning on ühtlasi ka Eesti eelvoor osalemaks European Cyber Security Challenge'l. Kvalifikatsiooni esimene voor oli kuni 29. aprillini avatud kõikidele. Teine voor toimub kutsetega kuni 17. juunini. KüberNaaskel/CyberSpike on osa Euroopa Liidu Küberturvalisuse Agentuuri (ENISA) algatusest European Cyber Security Challenge (ECSC). Täpsem info siit.

Samuti toimus 30. aprillil noortele algajatele küberturbe huvilistele Magic CTF kübervõistlus.

## TalTechi teadlased aitasid kokku panna lugemismaterjale koolidele

Targalt Internetis projekti raames on loodud lugemismaterjal ja juhtumite arutelude näited, mis aitavad koolidel mõista, kuidas isikuandmetega koolis paremini ringi käia. Lisaks sellele antakse soovitusi, kuidas vähendada digiprügi ja tõsta seeläbi turvalisust. TalTech ja teised materjali kokkupanekus osalenud eksperdid leiavad, et selline lugemisvara aitab koolidel teha isikuandmete kaitsmiseks paremaid otsuseid. Materjali leiab siit.

CYBERNETICA



## Cybernetica müüs oma lennujuhtimise irdtorni tehnoloogia Adacelile

Cybernetica astus strateegilise sammu oma põhitegevuste teravamaks fokuseerimiseks e-valitsemise tehnoloogiate, turvalise tarkvara- ja tootearenduse ning küberturvalisuse teenuste suunal ning müüs irdtorni tehnoloogia globaals ele lennuliikluse juhtimise tehnoloogia- ja teenusepakkujale Adacel.

Tehinguga omandas Adacel Cybernetica loodud irdtorni tehnoloogia ning võttis üle selle arendamise. Irdtorn võimaldab 24/7 turvalist lennujuhtimist distantsilt. Hetkel on selle tehnoloogia peamine klient Eestis Lennuliiklusteeninduse AS ning esimene irdtorn on paigaldatud Kuressaare lennuväljale.

Cybernetica juhatuse esimehe Oliver Väärtnõu sõnul on Cybernetica tuumiktugevus e-valitsemise ning infoturbe alane ekspertteadmus. "Arvestades tänast nõudlust usaldusväärse e-valitsemise tehnoloogiapartneri järele, on meie jaoks mõistlik samm oma tegevuste fookus suunatagi rohkem meie põhilistele väärtuspakkumistele digitaalse identiteedi, andmevahetuse, privaatsuse ja turvalisuse tehnoloogiate vallas."

## Cybernetica laiendab oma andmevahetustehnoloogiate pakkumist teenusmudeliga

Cybernetica andmevahetusplatvorm Unified eXchange Platform ehk UXP on tänapäeval kasutusel mitmetes eri kohtades üle maailma nagu Jaapanis, Ukrainas, Tuneesias, Namiibias, Gröönimaal ja mitmelpool mujal. Traditsiooniline UXPi lahendus on sobilik hästi riikidele ja suurtele organisatsioonidele, kellel on piisavalt vahendeid ning tehnoloogilist küpsust platvormi oma taristus rakendada ning investeerida ka selle jätkusuutlikkusse.

Nüüd pakub Cybernetica ka uut interoperability as a service lähenemist ehk Managed UXP, kus klient ei pea ise hoolitsema teenuse rakendamise, töös hoidmise ning tehniliste uuenduste eest. Tegemist on eriti sobiva lahendusega näiteks olukorras, kui puuduvad piisavad ressursid - näiteks ei ole piisavalt tehnilist tööjõudu.

Suuremahuline digitaliseerimine ning seda võimaldavad tehnoloogiad võivad olla üpriski keerukad, samas on turvaline andmevahetus iga digiülemineku tugevaks vundamendiks. Esmakordselt pakub Cybernetica klientidele võimalust andmevahetust Managed UXP teenusena ka enne rakendamist ise katsetada.

MAJANDUS- JA KOMMUNIKATSIOONI-MINISTEERIUM

Väljaandja: Majandus- ja Kommunikatsiooniministeerium · Suur-Ameerika 1, Tallinn
Toimetaja: Martin Paluoja · martin.paluoja@mkm.ee · +372 639 7685

DESIGN & BRANDING STUDIO viite agency ESTONIA