Riikliku küberturvalisuse uudiskiri

2022-11

Riigikantselei

Kriisideks valmisolekust: ülevaade kriisideks valmisoleku seadusest (VOS)

NATO

NATO loob kontrollmehhanismi tehisintellekti ja andmete vastutustundliku arendamise ning kasutamise jaoks

Cybernetica

Cybernetica hakkab juhtima suurprojekti, mis edendab vägede ja sõjatehnika liikumist Euroopa Liidus

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Riigikantselei

Kriisideks valmisolekust: ülevaade kriisideks valmisoleku seadusest (VOS) 3

Riigi infosüsteemi Amet

Teavituskampaania „Kontrolli üle!“ 5

Välisministeerium

III Tallinna rahvusvahelise õiguse ja küberoperatsioonide töötuba 5

Singapuri rahvusvaheline kübernädal 2022 5

OSCE küberjulgeoleku konverents 5

Andmekaitse Inspektsioon

Andmekaitse Inspektsioon andis välja maksehäirete avaldamise juhendi 6

Balti riikide isikuandmete kaitse järelevalveasutuste kohtumine 6

Andmekaitse Inspektsioon avaldas andmeladude seire kokkuvõtte 6

Tarbjakaitse ja Tehnilise Järelvalve Amet

Eesti on maailmas internetivabaduses teisel kohal! 6

NATO

NATO loob kontrollmehhanismi tehisintellekti ja andmete vastutustundliku arendamise ning kasutamise jaoks 7

TalTech

Tehnikaülikool avas registreerimise Eesti suurimale noorte küberkaitse võistlusele KüberNaaskel 7

E-riigi Akadeemia

eGA toetab Ukraina digiriigi toimimist Euroopa Liidu 10-miljonilises abiprojektis 8

E-riigi Akadeemia tugevdab koostöös ELiga Lääne-Balkani riikide küberkerksust 8

Cybernetica

Andmevahetusplatvorm Malaisia valitsusele 8

Cybernetica hakkab juhtima suurprojekti, mis edendab vägede ja sõjatehnika liikumist Euroopa Liidus 8

Cybernetica võitis lepingu Rumeenia mereväeameti raadiosidetehnoloogia uuendamiseks 9

Cybexer Technologies

CybExer Technologies siseneb SaaS pakkumisega Poola küberturbeturule 9

Kriisideks valmisolekust: ülevaade kriisideks valmisoleku seadusest (VOS)

Kokkuvõtte koostas: Kristi Purtsak, Riigikantselei

Riigikantselei valmistab koostöös ministeeriumite, nende allasutuste, kohalike omavalitsuse üksuste ja teiste asjassepuutuvate asutustega ette kriisideks valmisoleku seadust (edaspidi nimetame VOS).

Tegemist on kriisideks valmistumise ja suurte kriiside lahendamise nö katusseadusega. VOS-i kehtima hakkamisega muutuvad kehtetuks hädaolukorra seadus, riigikaitseseadus ja erakorralise seisukorra seadus.

VOS toob endaga kaasa ka paljude muude seaduste muudatused, kuna asutustel peavad olema võimalused reageerida sündmustele nende tekkimisel, mitte alles siis kui Vabariigi Valitsus või Riigikogu on otsustanud mõne erikorra välja kuulutada (erikorrad on eriolukord, erakorraline seisukord ja sõjaseisukord). Seetõttu on äärmiselt oluline, et asutused analüüsiksid nende vastutada olevaid eriseaduseid ja vaataksid, kas on olemas kõik vajalikud tööriistad erinevate olukordadega toimetulekuks.

Majandus- ja kommunikatsiooniministeeriumi (MKM) vastutada olevatest seadusest on VOSi protsessi hõlmatud kindlasti küberturvalisuse seadus (KüTS) aga ka kõik elutähtsate teenuste osutamist puudutavad seadused. Lisaks olemasolevate elutähtsate teenuste korraldamisele lisanduvad MKMi korraldada uute elutähtsate teenustena lennuväljade toimimine, aeronavigatsiooniteenuse toimimine, avaliku raudtee toimimine, raudteeveo toimimine ja sadamate toimimine.

Sotsiaalministeeriumi vastutusalas on elutähtsa teenuse osutajateks edaspidi üldarstiabi teenuse osutajad, apteekide pidajad ja ravimite hulgimüüjad. Maaeluministeeriumi vastutusalas on suuremad toidukäitlejad.

Oluline on, et kõikidele nendele teenuseosutajatele hakkavad edaspidi laienema ka KüTS-i nõuded. Kehtivatele elutähtsa teenuse osutajatele, lennunduse ja raudtee-ettevõtetele, samuti sadamatele, perearstidele ei ole tegemist uue nõudega. Küll on tegemist täiesti uue nõudega apteekidele, ravimite hulgimüüjatele ja toiduettevõtetele. Hetkel on veel avatud ülemineku aja pikkus nendele ettevõtetele, kuid seaduse väljatöötamisel üritatakse tagada mõistlik aeg uute nõuete ja muudatustega kohanemiseks.

VOSi koostamise protsess on tõstatanud ka nö saartalituse nõude (hädaolukorra seaduse § 41 lõige 2) otstarbekuse küsimuse. MKMi ja RIA eestvedamisel analüüsitakse, kui vajalik selline nõue Ukraina kriisi kogemust arvestades on.

Üldised muudatused, mis kriisideks valmisoleku seadusega Eesti õiguskorras ja kriisideks valmistumisel ja nende lahendamisel muutub:

1. Luuakse terviklik õigusruum, kus kõikideks, nii tsiviil- kui riigikaitsekriisideks valmistutakse ühtsetel alustel ja mille abil lahendatakse kõiki suure mõjuga kriise Vabariigi Valitsuse ja peaministri kui kriisiolukorra juhi, juhtimisel. Kriisiolukorra vahetut lahendamist juhib lahendav valitsusasutus, Eesti Pank või Finantsinspektsioon. Lahendavad asutused määratakse ülesannete jäävuse põhimõttel üldjuhul Vabariigi Valitsuse kriisiplaanis. Nimetatud plaanist tehakse ka avalik kokkuvõte, et oleks kõigil üldpilt, mis asutus kriisis mille eest vastutab ja milleks valmistuma peab.

2. Koondatakse ühte seadusesse eriolukorraks, erakorraliseks seisukorraks ja sõjaseisukorraks valmistumine, nende juhtimine ning nende lahendamiseks kohaldatavad meetmed. Eesmärk on, et tekiks terviklik vaade võimalikult väikese hulga ja omavahel loogiliselt süstematiseeritud õigusaktidest. Hetkel on regulatsioonid killustunud erinevate seadusete vahele ning kriisi lahendajatel (ning neid nõustavatel) on kriitilistel hetkedel üliraske kogu kriisilahendamise süsteemi hallata ja otsustajatele adekvaatset nõu anda, samuti on hetkel õigusaktides nö halle alasid ja erinevates kriisides volitused kasutada erinevaid meetmeid. Tänapäeval, kus kriisid ei ole enam nö must-valged, korraga võib esineda mitu kriisi, tegu võib olla nö hübriidkriisiga, kus ei oskagi kohe öelda, millega või kellega tegu – on äärmiselt oluline vähendada sellisteks olukordadeks valmistumisel ja lahendamisel segadust, ebatäpsusi ja mitmetimõistetavusi.

3. Võetakse kasutusele kriisiolukorra mõiste. Selle olemasolu üle otsustab valitsus, kui eksisteerib oht või on kätte jõudnud sündmus või sündmuste ahel, millel on suur mõju. Kriisiolukorra üle saab Vabariigi Valitsus otsustada asjaomaste asutuste esitatud ohuhinnangust ja muust asjassepuutuvast teabest. Kriisiolukorra mõiste kasutuselevõtuga kaob riigikaitseseaduses olev „kõrgendatud kaitsevalmidus“, selle sisu kantakse „kriisiolukorda“ üle. Koos hädaolukorra seadusega kaob ka „hädaolukorra“ mõiste.

4. Ühtlustatakse kriisideks valmistumist ja selleks planeerimist. Plaanide koostamiseks tekib üks protsess, nii et kõigil osapooltel on võimalik koostada üks plaan nii kriisiolukorraks, erikordadeks kui nende lävendi alla

jäävateks väiksemateks sündmusteks.

Selleks:

a) hakatakse koostama üleriigilist riskianalüüsi, mis hõlmab nii tsiviilkriisidega seotud riske kui riigikaitsega seotud ohte. See on aluseks Vabariigi Valitsuse kriisiplaanile ja sellest tehakse avalik kokkuvõte. Üleriigilist riskianalüüsi võtavad arvesse nii kriisiplaanide koostajad kui elutähtsa teenuse osutajad oma riskianalüüsi ja toimepidevuse plaani koostamisel.

b) Riigi kaitsetegevuse kava asemel tuleb uus planeerimisdokument - Vabariigi Valitsuse kriisiplaan, mis hõlmab valmistumist nii tsiviilkriisideks kui riigikaitsekriisideks.

c) Ministeeriumid ja Riigikantselei hakkavad seniste kaitsetegevuse kava alamkavade asemel koostama Vabariigi Valitsuse kriisiplaani alamplaani.

d) Alamplaanid annavad sisendi kriisiülesandega asutuste ja isikute plaanide tegemiseks (seniste HOLPide asemel, nt RIA hakkab koostama kriisiülesandega asutuse plaani).

Kõige olulisem on see, et kriisiülesandega asutused ja isikud teevad ühe plaani erinevate olukordade lahendamiseks või oma kriisiülesande täitmise tagamiseks. See peaks eelduslikult aitama vähendada halle alasid ja ka ressursikulu, mis läheb hetkel erinevate plaanide koostamisse.

Kriisiülesandega isiku ja asutuse plaane hakkavad koostama ka kõik kohaliku omavalitsuse üksused.

5. Võetakse kasutusele tänaste riigikaitseülesannete ja hädaolukordadeks valmistumise asemel kriisiülesanded, et lihtsustada ning muuta läbipaistvamaks ülesanded, mille täitmine on vajalik (ükskõik millise) kriisi lahendamiseks või leevendamiseks. Elutähtsa teenuse regulatsioon on edaspidi osa kriisiülesannetest. Hetkel on hädaolukorra seaduse elutähtsa teenuse katkemisel selle taastamise fookus ainult tavaolukorras (n-ö rahuajal). Elutähtsa teenuse viimine kriisiülesannete alla loob eeldused teenuste kriisiaegse toimimise sätestamiseks ka riigikaitsekriisis. Täpsemad nõuded elutähtsa teenuse osutamiseks riigikaitselistes olukordades kehtestavad elutähtsat teenust korraldavad asutused.

6. Püsiva kriisiülesandega isikutele ja asutustele, sealhulgas elutähtsa teenuste osutajatele, KOVidele ning põhiseaduslikele institutsioonidele määratakse toimepidevuse tagamise kohustus. Toimepidevus on n-ö baashügieenina osa asutuste sisemisest töökorraldusest ja selle alla käivad ka asutuste valmidustasemed ja objektikaitse regulatsioon.

7. Sätestatakse esimest korda seaduse tasemel elanikkonnakaitse, mille eesmärk on tagada elanikkonna elu ja tervise kaitse ning toimetulek kriisiolukorras. Elanikkonnakaitse hõlmab lisaks varjumisele ja evakuatsioonile asutuste ja KOVide tegevusi kriisiolukorraks valmistumisel ja selle lahendamisel, sealhulgas elanikkonna teavitamist ja nõustamist eesmärgiga suurendada nende valmisolekut kriisiolukorras ise toime tulla.

8. Senise HOSis sätestatud riski – ja kriisikommunikatsiooni asemel võetakse kasutusele „avalikkuse ja elanikkonna teavitamine“, mis koosneb nii valmistumiseks-ennetamiseks tehtavast riskikommunikatsioonist, kui lahendamisel tehtavast kriisikommunikatsioonist. Kommunikatsiooni eest vastutab iga asutus ise.

9. Eraldi sätestatakse viivitamatu ohuteate edastamine, kus esimest korda seaduse tasemel reguleeritakse ka sireenide kasutamine.

10. Kriisiülesannetega seotakse ka kriisiülesannetega ameti- ja töökohad, mis on rakendatavad nii tsiviil- kui riigikaitselises kriisis.

Need olid ainult peamised muudatused, mida eelnõu endaga kaasa toob.

Hetkel käib koos ministeeriumite ja nende allasutustega kogu paketi viimane lihv, et see ametlikule kooskõlastusele saata. Seega tuleb antud kirjatükki suhtuda reservatsiooniga, et kõik võib veel muutuda ja tegu ei ole lõplike lahendustega enne, kui neid Riigi Teatajast lugeda ei saa.

Teavituskampaania „Kontrolli üle!“

Eesti elanike küberteadlikkuse tõstmiseks alustas Riigi Infosüsteemi Amet teavituskampaaniat „Kontrolli üle!“, mis rõhutab küberhügieeni algtõdesid.

Statistikaameti uuringu „Infotehnoloogia leibkonnas“ järgi on inimeste küberteadlikkus viimaste aastate jooksul paranenud, ent küberkurjategijate lõksu langevad siiski igapäevaselt arvuteid ja nutiseadmeid kasutavad inimesed. Teavituskampaania keskendub Eestis levinumate petu- ja kuriteoskeemidele, mille tagajärjel jäävad sajad ettevõtted ja inimesed ilma rahast, andmetest ja kontodest.

Kampaania kutsub üles harjumuspärast käitumist internetis teadlikumalt jälgima – näiteks millisele lingile klõpsad, kas kasutad tugevat parooli ja kuhu seda sisestad, kas oled veendunud, et sõbralt saadud e-kiri on just sõbra saadetud ning kas see, mida internetist alla laed ja arvutisse paigaldad on turvaline ning vajalik. Need on küll teada-tuntud ja väikesed asjad, ent turvalisuse vaatest väga olulised.

„Kontrolli üle!“ kampaania kestab 20. novembrini ning häid soovitusi kohtab nii tänavapildis kui ka meediakanalites.

III Tallinna rahvusvahelise õiguse ja küberoperatsioonide töötuba

3.-4.10.2022 toimus III Tallinna rahvusvahelise õiguse ja küberoperatsioonide töötuba. Kokku osales üritusel 55 eksperti 24-st erinevast riigist.

Töötoa raames käsitleti vastumeetmete, jõukasutuse, enesekaitse ja vajalikkuse teemasid küberruumis. Lisaks analüüsiti praktilisi küberoperatsioone ja riikide reaktsioone kajastavaid stsenaariume.

Töötoa juhatasid sisse oma valdkonnas kõrgelt hinnatud eksperdid – prof. Duncan Hollis Temple ülikoolist ja dr. Francois Delerue IE ülikoolist.

Eelnevad kaks Välisministeeriumi poolt korraldatud rahvusvahelise õiguse töötuba keskendusid muuhulgas suveräänsusele, mittesekkumise printsiibile ning vaidluste rahumeelsele lahendamisele.

Järgmine töötuba on planeeritud 2023. aasta kevadesse.

Singapuri rahvusvaheline kübernädal 2022

18.-20.10.2022 osales Eesti kübersaadik Tanel Sepp Singapuri rahvusvahelisel kübernädalal.

Eesti seisukohtade tutvustamine ja selgitamine meile olulistes küsimustes (küber, demokraatia, Ukraina) on endiselt hädavajalik ja möödapääsmatu. Juhul, kui Eesti ei kasuta rahvusvahelistes foorumites oma häält, et seista rahvusvahelisel õigusel tugineva vaba, avatud ja turvalise küberruumi eest, täidab tühja ruumi kiiresti Venemaa narratiiv.

Eesti ja samameelsete riikide huvides on, et mittedemokraatlik narratiiv ei jääks rahvusvahelistel kohtumistel kõlama ja et ka geograafiliselt kaugemal paiknevad riigid (nn Global South) mõistaksid Eesti seisukohti.

OSCE küberjulgeoleku konverents

20.-21.10.2022 osales Digi- ja küberdiplomaatia osakond (DKO) Poolas toimunud OSCE küberjulgeoleku konverentsil. Konverentsil käsitleti kübervastupidavust, OSCE usaldusmeetmeid ja kodanikuhariduse rolli küberjulgeoleku tagamisel.

Eesti ja samameelsete huvi on, et küberjulgeoleku tagamine toimuks läbi kõiki sidusrühmi kaasava lähenemise. Sealjuures tuleb tõhustada rahvusvahelist koostööd, jagada toimivaid praktikaid ja edendada OSCE usaldusmeetmete rakendamist.

Kübervastupidavus on nagu turvavöö – kui regulatsioonid ja süsteemid küberrünnakutega tegelemiseks on paigas, on võimalik õnnetuste

negatiivset mõju oluliselt vähendada.

Andmekaitse Inspektsioon andis välja maksehäirete avaldamise juhendi

Andmekaitse Inspektsioon andis oktoobri alguses välja uuendatud maksehäirete avaldamise juhendi.

Juhend selgitab maksehäireandmete avaldamisega seotud õigusi ja kohustusi, mis tulenevad ELi isikuandmete kaitse üldmäärusest ja isikuandmete kaitse seadusest.

Juhend "Maksehäirete avaldamine" on praktiliseks abimaterjaliks kõigile, kes puutuvad kokku võlaandmetega. Juhendist saavad nõu nii maksehäireandmete avaldajad kui ka nende andmete saajad-küsijad, samuti nii võlausaldajad kui ka võlgnikud.

Loe lähemalt siit.

Avaliku teabe päeva ettekanded on Andmekaitse Inspektsiooni veebilehel järelvaadatavad

Septembri lõpus tähistatakse igal aastal rahvusvahelist avaliku teabe päeva. Sel päeval juhivad avaliku teabe asutused üle maailma tähelepanu riigi läbipaistvusega seotud teemadele.

Andmekaitse Inspektsioon korraldas sel aastal avaliku teabe päeva tähistamiseks veebipõhise teabepäeva. Teabepäev toimus 30. septembril veebipõhise sündmusena ning oli suunatud riigi- ja kohaliku omavalitsuse asutustele ning Andmekaitse Inspektsiooni avaliku teabe nõukogule.

Teabepäeva juhatas avasõnadega sisse Andmekaitse Inspektsiooni jurist Elve Adamson. Tarbijakaitse ja Tehnilise Järelevalve Ameti digiligipääsetavuse ekspert Harri Puskar rääkis avaliku sektori digiligipääsetavusest. Põhjaliku ülevaate muutuvast Euroopa Liidu õigusruumist andmete taaskasutuse vaates andis Majandus- ja Kommunikatsiooniministeeriumi andmete taaskasutuse programmijuht Nele Nisu. Teabepäeva viimase ettekandena tutvustas Arenguseire Keskuse ekspert Johanna Vallistu olulisemaid leidusid keskuse uuringust, milles võeti vaatluse alla avaliku teabe kasutamise võimalused.

Teabepäeva saab järele vaadata siin.

Ilmus eestikeelne kokkuvõte Euroopa Andmekaitsenõukogu 2021. aasta aastaraamatust

Ilmunud on Euroopa Andmekaitsenõukogu 2021. aasta aastaraamatu lühikokkuvõte eesti keeles.

Aastaraamatust saab põhjaliku ülevaate nõukogu möödunud aasta tööst, vastuvõetud suunistest, olulisematest menetlustest nii piiriüleselt kui liikmesriigiti ja veel paljust muust, mis andmekaitsemaailma ka edaspidi mõjutab.

Loe eestikeelset kokkuvõtet siit.

Balti riikide isikuandmete kaitse järelevalveasutuste kohtumine

20.-21. oktoobril toimus Vilniuses Balti riikide andmekaitse järelevalveasutuste iga-aastane koostöökohtumine.

Kohtumise peamiseks eesmärgiks oli omavahelise koostöö tugevdamine ning parimate praktikate vahetamine. Kohtumisel võeti kokku Balti riikide selle aasta ühisjärelevalve vahetulemused ning lepiti kokku 2023. aasta sektoripõhise ühisseire järgmised sammud.

Loe lähemalt siit.

Andmekaitse Inspektsioon avaldas andmeladude seire kokkuvõtte

Andmekaitse Inspektsioon viis perioodil suvi 2021 kuni kevad 2022 riigi valitsussektoris läbi andmeladude seire.

Seire eesmärk oli saada ülevaade valitsussektori andmeladudest, selgitada välja peamised probleemid ning nende põhjused. Seire küsimustele vastas 20 asutust. Vastustest tuvastas inspektsioon 28 andmelao tunnustega andmetöötluskeskkonda. Seire kokkuvõtet ja tehtud järeldusi saab lugeda inspektsiooni kodulehel.

Eesti on maailmas internetivabaduses teisel kohal!

USA mõttekoda Freedom House avaldas raporti, milles analüüsiti 70 riigi inimeste õigusi ja vabadusi avalikus veebiruumis.

Raportis on välja toodud ka TTJA tegevused 5G sageduslubade jagamisel ning vaenu ja sõda õhutavate meediakanalite piiramisel.

Tutvu raportiga siin.

NATO

NATO loob kontrollmehhanismi tehisintellekti ja andmete vastutustundliku arendamise ning kasutamise jaoks

NATO kaitseministrid leppisid kokku, et luuakse ülevaatusnõukogu, mis juhiks tehisintellekti ja andmete vastutustundlikku arendamist ja kasutamist NATO-s.

Esimeseks ülesandeks on välja töötada kasutajasõbralik vastutustundliku tehisintellekti sertifitseerimisstandard, mis hõlmab kvaliteedikontrolli ja riskide maandamist, mis aitab viia uued tehisintellekti ja andmeprojektid vastavusse 2021. aasta oktoobris heaks kiidetud NATO vastutustundliku kasutamise põhimõtetega.

Ainulaadne platvorm parimate tavade vahetamiseks, uuendajate ja operatiivsete lõppkasutajate juhendamiseks kogu arendusfaasis, aidates seeläbi kaasa usalduse loomisele innovatsioonikogukonnas.

Praegu katsetab NATO tehisintellekti erinevates valdkondades nagu küberkaitse, kliimamuutused ja pildianalüüs. Vastuseks 2022. aasta strateegilise kontseptsiooni üleskutsele kiirendada digitaalset ümberkujundamist, kiitsid NATO liitlased heaks ka NATO esimese digitaalse ümberkujundamise visiooni. Aastaks 2030 võimaldab NATO digitaalne ümberkujundamine alliansil viia läbi mitmeid valdkonda hõlmavaid operatsioone, tagada koostalitlusvõime kõigis valdkondades, suurendada olukorrateadlikkust ning hõlbustada poliitilisi konsultatsioone ja andmepõhist otsuste tegemist.

Lisainfo NATO kodulehel.

TalTech

Tehnikaülikool avas registreerimise Eesti suurimale noorte küberkaitse võistlusele KüberNaaskel

Tallinna Tehnikaülikool ja Kaitseministeerium kutsuvad kõiki 14-25aastaseid häkkereid registreeruma Eesti küberkaitse talentide suurvõistlusele KüberNaaskel. Võistluse eelvoor toimub 2.-3. detsembril ning põhivoor 10. detsembril.

Selleaastase võistluse süžee viib meid tagasi 2007. aasta Pronksiöö sündmustesse. Stsenaariumikohaselt on peategelane Kaitseliidu Küberkaitseüksuse salajane abiline, kes kutsutakse eksperdina appi nii riigile kui ka ettevõtetele. Ülesandeks on hoida üleval vajalikud teenused, paigata serverid ja leida süsteemides olevad pahalased.

Võistluse parimatele on välja pandud erinevad auhinnad, sealhulgas võimalus tulla tehnikaülikooli õppima ning osaleda KüberLaagrites Eestis ja Norras. Registreerumine on avatud kuni 27. novembrini võistluse kodulehel.

Täpsem info võistluse kohta või kui soovid toetajana kaasa lüüa: Birgy Lorenz.

KüberNaaskli võistlust toetab Kaitseministeerium ja projekti viib ellu Tallinna Tehnikaülikool. Võistluse tehniliseks partneriks on Eesti küberturbe ettevõte CTF Tech.

KüberNaaskel CyberSpike

E-riigi Akadeemia

eGA toetab Ukraina digiriigi toimimist Euroopa Liidu 10-miljonilises abiprojektis

Alates Venemaa täiemahulise agressiooni algusest Ukrainas on Euroopa Liit pakkunud Ukraina ametiasutustele kiiret abi küberturvalisuse ja andmeturbe vajaduste täitmiseks, et hoida avalikud teenused sõja ajal kättesaadavana. E-riigi Akadeemia (eGA) vastutab Euroopa Liidu (EL) üle 10 miljoni euro suuruse abi kohalejõudmise eest.

Lisainfo.

E-riigi Akadeemia tugevdab koostöös ELiga Lääne-Balkani riikide küberkerksust

Vastusena sagenenud küberrünnakutele on Euroopa Liit suurendanud küberturvalisuse alast koostööd Lääne-Balkani riikidega. Esmalt tugevdatakse Albaania, Montenegro ja Põhja-Makedoonia küberkerksust, mis hõlmab küberturvalisuse seadusandluse kohandamist ja küberintsidentidele reageerimise meeskondade (CERT) erialase ettevalmistuse tugevdamist. Projekti viib ellu E-riigi Akadeemia.

Lisainfo.

Cybernetica

Andmevahetusplatvorm Malaisia valitsusele

Cybernetica rakendas Malaisia valitsuse jaoks Unified eXchange Platformi (UXP), et tagada turvaline koostalitlusvõime, dokumentide ja teenuste vahetamine valitsusasutuste vahel, moderniseerides tõhusalt oma e-valitsemise infrastruktuuri, et hõlbustada digitaalset transformatsiooni.

Kui Malaisias oli juba varem olemas keskne andmevahetuslahendus nimega Malaysian Government Central Data Exchange (MyGDX), siis projekti põhieesmärk oli pakkuda MyGDX-ile uusi võimalusi ja funktsioone, värskendades seda Cybernetica UXP-tehnoloogia uusimale versioonile.

Andmevahetustehnoloogiate juht Maksim Ovtšinnikov ja andmevahetustehnoloogiate müügi- ja partnerlussuhete juht Adhele Tuulas külastasid Malaisiat ning kohtusid partneri, HLA Groupi, MAMPU ja riikliku registriosakonnaga. „Malaisia valitsusel on koostalitlusvõime süsteemi osas ambitsioonikad plaanid. Järgmise 5 aasta jooksul kavatsevad nad UXP-d kasutusele võtta 400+ valitsusorganisatsioonis ja pakkuda süsteemi mõnele Malaisia osariigile“ kommenteeris Ovtšinnikov.

„Me valmistame praegu ette MAMPU visiiti Eestisse. Oleme edasise koostöö suhtes väga optimistlikud ja rakendame praegu Malaisia suurimates agentuurides UXP-d, mis on aluseks edasistele arengutele“ ütles Adhele Tuulas.

Lisainfo.

Cybernetica hakkab juhtima suurprojekti, mis edendab vägede ja sõjatehnika liikumist Euroopa Liidus

Cybernetica juhib alates detsembrist Euroopa Kaitsefondist (EDF) rahastatavat konsortsiumiprojekti “Secure Digital Military Mobility System (SDMMS)”, mida viib läbi 11 Euroopa ettevõtet.

Projekti eesmärk on luua tarkvara, mis soodustaks Euroopa riikide väeosade piiriülest liikumist Euroopa piires, arvestades peamisi ette tulla võivaid kitsaskohti. Koostööpartnerite loodud tarkvaraplatvorm tagab tõhusama töökorralduse väeosade liikumisel üle riigipiiride, lihtsustades nii piiriülest infojagamist kui ka piiriületuslubade küsimist. Projekti raames vastutab Cybernetica konsortsium üldise haldamise, platvormi arhitektuuri loomise ja arendamise eest.

“Meie jaoks on äärmiselt oluline panustada kogu Euroopa julgeolekusse, eriti tänases olukorras. Cybernetica jaoks on tegemist strateegilise algatusega, millesse soovime panustada pikaajaliselt,” ütles Cybernetica tegevjuht Oliver Väärtnõu.

Cybernetica aastatepikkune kogemus missioonikriitiliste tehnoloogiate väljatöötamisel ja juurutamisel on loonud vajaliku võimekuse võtta juhtrolli rahvusvahelistes suure mõjuga konsortsiumiprojektides. Sõjalise mobiilsuse edendamiseks vajalik andmevahetus Euroopa Liidu liikmesriikide vahel toimub Cybernetica arendatud ja erinevates kontekstides kasutatava tehnoloogia UXP (Unified eXchange Platform) abil. Cybernetical on ligi kahekümneaastane kogemus tolliinfosüsteemide arendamisel, mis võimaldavad kaupade tõhusat piiriülest liikumist Euroopa Liidu piires.

Lisainfo.

Cybernetica võitis lepingu Rumeenia mereväeameti raadiosidetehnoloogia uuendamiseks

Cybernetica võitis lepingu Rumeenia mereväeameti (RNA) hankeks, et uuendada riigi siseveeteedel kasutatavat raadiosidesüsteemi. Uuendusega täiendatakse olemasolev raadiolahendus kaasaegseks VHF-sidesüsteemiks, mis koosneb uudsest süsteemiarhitektuurist ja tipptasemel seadmetest. Rumeenias on Doonau jõe pikim lõik ja kogu selle pikkuses riigis katab Cybernetica raadiosidesüsteem.

Seiresüsteemide osakonna juhataja Martin Linki sõnul aitab uus raadiosidesüsteem korraldada liiklust veeteel ja tagada kõikidele laevadele ohutus. „Uus lahendus võimaldab kõrge võimekusega laevaliikluse juhtimist raadio teel igal hetkel 24/7, mis tähendab kõrgemat olukorrateadlikkust, mis omakorda toob efektiivsust ning vähendab võimalikke ohte ja vigu. See on abiks ka päästetegevuse tõhusaks koordineerimiseks, kui seda peaks vaja minema," selgitas Link.

Tööd teostatakse Rumeenia mereväe ameti jaoks, mis on Rumeenia transpordiministeeriumi alluvuses spetsialiseerunud rakendusasutus, mis tagab navigatsiooniohutuse. See on projekt, mis tähistab professionaalse ja rahuldava koostöö jätku.

Lisainfo.

Cybexer Technologies

CybExer Technologies siseneb SaaS pakkumisega Poola küberturbeturule

CybExer Technologies ja Poola küberturbeettevõte LabSecure PSA allkirjastasid 26. oktoobril Monsis NATO Kommunikatsiooni- ja Teabeagentuuri konverentsil NATO Edge 2022 vastastikuse mõistmise kokkuleppe, et hakata pakkuma Poola turul küberturvalisuse treeninguid, mis kasutavad CybExeri küberharjutusväljaku (cyber range) tehnoloogiat.

LabSecure'i tegevjuht Jacek Czech ütles, et Poolas kehtivad olulised regulatiivsed nõuded tuhandetele riigiasutuste, ettevõtete – riigi- ja eraettevõtete töötajatele ning peamiselt kohalike omavalitsuste küberjulgeoleku töötajatele pideva koolitustsükli läbimiseks ja sertifitseerimisnõuete täitmiseks. „Meil on hea meel teha koostööd CybExer Technologies'ga ja kasutada selle väljakutse lahendamiseks ennast tõestanud küberharjutusväljakut," lisas Czech.

CybExer Technologies tegevjuhi Andrus Kivisaare sõnul on leping järjekordne tõestus CybExeri SaaS-i pakkumise atraktiivsusest. „Meie missiooniks on teha kübeharjutusväljaku tehnoloogia kättesaadavaks küberturvalisuse koolituste ja treeningute pakkujatele, kellel on teadmine kohalikust turust ja hea ligipääs klientidele. Soovime olla hea partner ja võimaldada koolituse pakkujatel kohandada oma sisu kohalike vajadustega. Meil on väga hea meel sõlmida LabSecure'iga kokkulepe, et suurendada Poola avaliku sektori ja ettevõtete vastupidavust küberohtudele. See verstapost tähistab meie jaoks sisenemist 40-miljonilise riigi turule ja aitab kaasa meie tehnoloogia laiemale levikule," lisas Kivisaar.

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