Riikliku küberturvalisuse uudiskiri

2022-02

Majandus- ja kommunikatsiooniministeerium

Kirjad riikliku küberturvalisuse teemadel

E-riigi akadeemia

E-riigi akadeemia Ukraina meeskond jätkab tööd sõjatandril

CybExer Technologies

CybExer Technologies kaasas laienemiseks 5 miljonit

Majandus- ja Kommunikatsiooni-ministeerium

Seekordses uudiskirjas

Majandus- ja Kommunikatsiooniministeerium

Kirjad riikliku küberturvalisuse teemadel 3

IT-minister arutas elutähtsa ja olulise teenuse osutajatega küberturbe valmiduse tõstmise plaane 3

Riigi Infosüsteemi Amet ja Välisluureamet avaldasid küberturvalisust puudutavad aastaraamatud 4

Küberturvalisuse standardiseerimise veebikonverents 5

Välisministeerium

21.-22.02 toimus seminar Tallinn Workshop on International Law and Cyber Operations 5

Eesti ühines omistamise avaldusega 5

Andmekaitse Inspektsioon

Eesti osaleb üleeuroopalises avaliku sektori pilveteenuste kasutamise järelevalves 6

Startup Estonia

Startup Estonia otsib CyberTech iduettevõtluse projektijuhti. 6

E-riigi akadeemia

EGA Ukraina meeskond jätkab tööd sõjatandril 6

Eesti kübereksperdid nõustavad Kõrgõzstani ametivendi 6

TalTech

TalTech tutvustab õppimisvõimalusi küberkaitse magistriõppekaval 7

CybExer Technologies

CybExer Technologies kaasas laienemiseks 5 miljonit 7

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

Kirjad riikliku küberturvalisuse teemadel

Tulenevalt pingelisest julgeolekuolukorrast seoses Ukrainaga, mis veebruari teises pooles eskaleerus täiemahuliseks sõjaks, on ettevõtlus- ja infotehnoloogiaminister Andres Sutt ja kantsler Ando Leppiman saatnud mitmeid kirju nii riigisektori kui erasektori osapooltele, rõhutades küberturvalisuse taseme tõstmise vajalikkust ning kutsudes üles tähelepanelikkusele ohtude ja nõrkuste suhtes.

31. jaanuaril saatis kantsler Ando Leppiman kirja valitsusasutustele, põhiseaduslikele institutsioonidele ja kõigile kohalikele omavalitsustele, kus paluti kõigil osapooltel edastada kindel kontaktpunkt kriitilistest turvanõrkustest ja küberintsidentidest teavitamiseks.

2. veebruaril saatis minister Sutt kirja mitmele valitsusasutusele ja riigi IT-majale.

15. veebruaril saatis minister Sutt kirja valitsusasutustele, põhiseaduslikele institutsioonidele ja mitmele kohalikule omavalitsusele küsimustega seoses küberintsidentide lahendamise plaanidega.

15. veebruaril saatis minister Sutt kirja valitsusasutustele, põhiseaduslikele institutsioonidele, kõigile kohalikele omavalitsustele ning elutähtsate ja oluliste teenuste osutajatele, kus anti suunised pöörata kõrgendatud tähelepanu küberturvalisuse nõuete täitmisele, küberhügieeni parandamisele, intsidentide plaanide olemasolule ja tarkvara uuendamisele.

2. märtsil saatis minister Sutt kirja valitsusasutustele, põhiseaduslikele institutsioonidele ja mitmele kohalikule omavalitsusele seoses vajadustega küberturvalisuse baasvõimekuste tõstmiseks.

3. märtsil saatis minister Sutt kirja ettevõtjate liitudele, kus on välja toodud 11 nõuannet hetkeolukorda silmas pidades oma ettevõtte küberturvalisuse taseme tõstmiseks ja vastupidavuse suurendamiseks.

IT-minister arutas elutähtsa ja olulise teenuse osutajatega küberturbe valmiduse tõstmise plaane

17. veebruaril toimus ettevõtlus- ja infotehnoloogiaministri kokku kutsutud ümarlaud elutähtsate ja oluliste teenuste osutajatega, et rääkida Ukraina julgeolekukriisist tingitud küberruumi ohupildist ning võimalikest vastumeetmetest. Minister Sutt tõi välja, et võrreldes varasema küberturbe ümarlauaga möödunud aasta septembris on märgatavalt kasvanud ettevõtete huvi ja tähelepanu küberturvalisuse vastu.

Minister Sutt pani osalejatele südamele, et küberriske tuleb võtta tõsiselt. „Küberturvalisuse ohupilt on viimastel aastate jooksul oluliselt halvenenud ning Ukraina julgeolekukriis muudab olukorra veelgi keerulisemaks. Seetõttu on ülioluline, et ettevõtete ja asutuste juhid hoolitsevad oma side- ja IT-baasturvalisuse eest ning loovad varu- ja kriisiplaane. Riik on loomulikult siinkohal valmis tuge pakkuma, kuid niivõrd detsentraliseeritud süsteemi juures peab iga asutuse ja ettevõtte juht tagama kõrge küberturbe taseme ennekõike ise. Samuti on põhjust üle vaadata küberturbe investeeringute maht. Kui see jääb IT üldkulude kontekstis alla 10-15 protsendi, siis on põhjust eeldada, et süsteemid ei ole asjakohaselt kaitstud," rääkis Sutt.

Nii minister kui Riigi Infosüsteemi Amet (RIA) kinnitasid ettevõtetele, et intsidentide korral on riik kindlasti abiks nende lahendamisel.

„RIA CERT-osakonnal on 24/7 valmidus olukorda hinnata ning vajadusel intsidentide lahendamisel abistada. Kuid ennetustöö tuleb ära teha ettevõtetel endil — tuleb hoolitseda oma organisatsiooni küberturbe hügieeni eest ning valmistuda ka alternatiivide kasutusele võtmiseks, kui side- ja infosüsteemide töö on häiritud. RIA poolt antavaid suuniseid haavatavuste parandamiseks ning ohtude ennetamiseks tuleb võtta tõsiselt," märkis minister.

Fotol RIA Peadirektori asetäitja küberturvalisuse alal Gert Auväärt

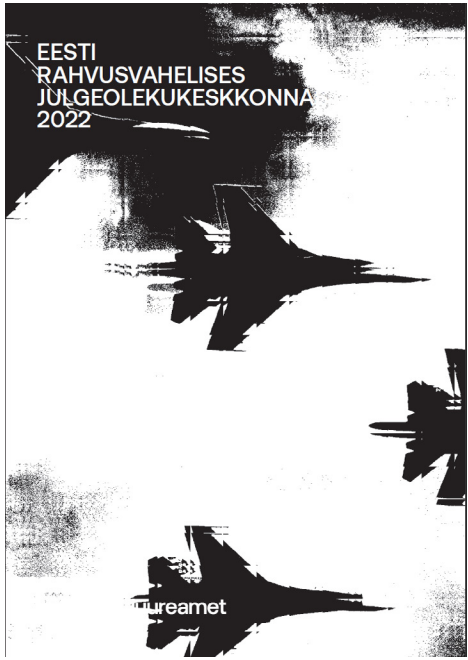
Ümarlaual andsid julgeoleku situatsioonist, küberohupildist ja riigi tegevustest ülevaate Riigi Situatsioonikeskus, Välisluureamet, Majandus- ja Kommunikatsiooniministeerium ning Riigi Infosüsteemi Amet. Ümarlaual osales üle 200 elutähtsate ja oluliste teenuste osutajate esindaja.

Lisaks toimus 18. veebruaril Küberjulgeoleku nõukogu koosolek, kus arutati julgeoleku olukorda ning saadi ülevaade riigi küberkerksuse tõstmise plaanidest.

Küberjulgeoleku nõukogu on Vabariigi Valitsuse julgeoleku komisjoni alakomisjon, mis annab suuniseid küberjulgeoleku poliitika kujundamiseks. Nõukogusse kuuluvad eri ministeeriumite ja riigiasutuste esindajad.

Riigi Infosüsteemi Amet ja Välisluureamet avaldasid küberturvalisust puudutavad aastaraamatud

15. veebruaril avaldas Välisluureamet oma aastaraamatu „Eesti rahvusvahelises julgeolekukeskkonnas 2022," milles puudutatakse mitmeid küberjulgeolekuga seotud aspekte. Lähemalt kirjutatakse Venemaa küberluurest ning selle mõjudest Eestis ja mujal. Aastaraamatuga saab tutvuda vastavas veebiportaalis või PDF dokumendina.



16. veebruaril avaldas Riigi Infosüsteemi Amet enda Küberturvalisuse aastaraamatu 2022, milles võeti kokku eelnev aasta küberturvalisuse

Välisministeerium

võtmes, sealhulgas olulisemad intsidendid 2021. aastast nii Eestis kui mujal maailmas, trendid küberruumis ja arenevad tehnoloogilised ohud ning palju muud olulist. Aastaraamatuga saab tutvuda siin.

Küberturvalisuse standardiseerimise veebikonverents

Euroopa standardiorganisatsioonid CEN, CENELEC ja ETSI peavad 15. märtsil koostöös Euroopa Liidu Küberturvalisuse Ametiga veebikonverentsi küberturvalisuse standardiseerumise teemal. Tegemist on järjestikku kuuenda konverentsiga ning seekordsel konverentsil arutatakse tehisintellekti, Euroopa digiidentiteeditaskute, infrastruktuuri ja tarneahelate ning andmekaitse teemadel. Ürituse veebisait (sh registreerimisinfo) on leitav siit.

21.–22.02 toimus seminar Tallinn Workshop on International Law and Cyber Operations

Tegemist on seminaride sarja esimese töötoaga. Kahepäevase virtuaalse kohtumise vältel keskenduti kolmele teemale küberoperatsioonide kontekstis. Esimesel päeval vaidluste rahumeelse lahendamise kohustusele olukorras, mil on tekkinud osapoolte vahel vaidlus teatud tegevuse suhtes. Teisel päeval suveräänsusele küberruumis — peamiselt, kas suveräänsus küberruumis on rahvusvahelise õiguse siduv reegel või põhimõte, millest mitmed teised siduvad reeglid (nt sekkumise keeld) tulenevad. Sellega seoses käsitletigi kolmanda ja seminari viimase teemana sekkumise keelu kohustust. Seda peamiselt siseasjadesse sekkumise keelu kontekstis - mida tähendab sekkumise keelu puhul selle keelu rikkumiseks vajalik sunnielement, mida tähendab domaine réservé ning kas küberruumis tegutsemine on mõjutanud nendest õguslikest põhimõtetest arusaamist ja nende rakendamist praktikas. Järgmine töötuba on plaanis korraldada 6.- 7. juunil riigivastutuse ja omistamise teemal.

Eesti ühines omistamise avaldusega

22.02 ühines Eesti USA, Ühendkuningriigi ja Austraalia avaldustega omistada 15.—16. veebruaril 2022 toimunud küberrünnakud Ukraina finantssektori vastu Venemaa sõjaväeluurele (GRU)

Välisminister Eva-Maria Liimetsa sõnul saame teadaolevale informatsioonile tuginedes suure tõenäosusega väita, et rünnakute taga oli Venemaa sõjaväeluure (GRU). „Küberründed elutähtsa taristu vastu lähevad vastuollu rahvusvahelise õigusega ja mõistame seega need üheselt hukka," ütles välisminister Liimets. „Kindlasti peame aitama rahvusvahelises koostöös tugevdada Ukraina küberjulgeolekualaseid oskuseid, et Ukraina suudaks oma taristut küberrünnakute eest senisest tõhusamalt kaitsta," lisas ta.

Eesti on teinud Ukrainaga kaua koostööd küberjulgeoleku valdkonnas ning jätkab Ukraina küberjulgeoleku ülesehitamisel oma kogemuste ja teadmiste jagamist. Koostöö hõlmab nii küberjulgeoleku, küberkaitse kui küberdiplomaatia valdkondi, näiteks arendades Ukraina e-valitsemise infrastruktuuri, e-teenuseid ja küberturvalisuse standardeid.

Fotol Anna-Maria Osula (TsalTech), Tanel Sepp ja Kerli Veski (Välisministeerium) töötoa avamisel

ANDMEKAITSE INSPEKTSIOON

Andmekaitse Inspektsioon

Eesti osaleb üleeuroopalises avaliku sektori pilveteenuste kasutamise järelevalves

Veebruaris algas Euroopa Andmekaitsenõukogu eestvedamisel esimene andmekaitsealane ühisjärelevalve — 22 andmekaitseasutust üle Euroopa võtavad ühiselt luubi alla pilveteenuste kasutamise avalikus sektoris. Ühisjärelevalves osaleb ka Eesti Andmekaitse Inspektsioon.

„Ühisalgatus viiakse läbi selleks, et saada ülevaade isikuandmete töötlemise olukorrast pilveteenuste kasutamisel," selgitas Andmekaitse Inspektsiooni tehnoloogianõunik Urmo Parm. „Meie eesmärk on kaardistada pilveteenuseid kasutavate asutuste kitsaskohad ja koostada neile konkreetsed soovitused riskide haldamiseks."

Seire tugineb kõigi osalevate riikide järelelvalveasutuste ühisele ettevalmistustööle ning selle raames kogutakse erinevates riikides eelteavet, saadetakse välja küsimustikud ning vajadusel alustatakse ka ametlike järelevalvemenetlustega. Seire küsimused on liikmesriikide üleselt ühiselt koostatud. Eelkõige uurivad järelevalveasutused, millised on avaliku sektori asutuste peamised väljakutsed ELi isikuandmete kaitse üldmääruse järgimisel pilvepõhiste teenuste kasutamisega seoses.

Ühisseire raames võetakse ühendust enam kui 80 asutusega Euroopa majanduspiirkonnas. Nende hulgas on nii Euroopa Liidu institutsioonid kui ka asutused väga erinevatest sektoritest, näiteks tervishoiu-, finants- ja haridusasutused, IT-teenuste pakkujad. Eestis on seiresse kaasatud asutusteks Transpordiamet, Eesti Haigekassa, Haridus- ja Teadusministeerium ning Tallinna Linnavalitsus, kellel tuleb inspektsiooni küsimustikule vastused saata hiljemalt aprilli lõpuks.

Ühisjärelevalve tulemusi analüüsitakse koordineeritult ning järelevalveasutused otsustavad võimalike edasiste riiklike järelevalvemeetmete üle. Lisaks koondatakse kõigi riikide tulemused kokku ühtsesse raportisse, mis annab teemast sügavama ülevaate ja võimaldab sihipäraseid järeltegevusi ELi tasandil.

STARTUP ESTONIA

Startup Estonia

Startup Estonia otsib CyberTech iduettevõtluse projektijuhti.

Võimalus teha tähendusrikast tööd ja mõjutada Eesti majanduse tulevikku. Tööpakkumisega saab tutvuda siin.

eGA e-governance academy

E-riigi akadeemia

EGA Ukraina meeskond jätkab tööd sõjatandril

E-riigi Akadeemia 21 töötajat viibivad hetkel Ukraina sõjakoldes, jätkates Ukraina andmevahetusplatvormi ja andmete kaitsmisega ning toetades IT armee tegevust. Suur tänu kõigile Eesti ettevõtetele, kes on olnud meie meeskonnale andmete kaitsmisel toeks! Rohkem meie meeskonna kohapealsest tegevusest saab kuulata-lugeda siin.

Eesti kübereksperdid nõustavad Kõrgõzstani ametivendi

2021. sügisel alanud kaheaastase Euroopa Liidu mestimisprojekti raames nõustavad Eesti kübereksperdid Kõrgõzstani ametivendi EL Võrgu- ja infoturbe direktiiviga kooskõlas oleva seaduse ettevalmistamisel. Järgmiste tegevustena asume arendama sealset küberturvalisuse intsidentide ja olukorra monitoorimise valdkonda. Kõrgõzstan on loonud riikliku CERT üksuse ning plaanib ka riigiasutuste CERTi asutamist ning on väga huvitatud Eesti ekspertide kogemusest uue operatsioonikeskuse (Security Operations Centre e SOC) kavandamisel. Peamised koostööpartnerid Kõrgõzstanis on Riikliku Julgeolekukomitee Küberturvalisuse Koordinatsioonikeskus ning Digitaalarengu Ministeerium.

Fotol Eesti eksperdid Bishkekis

TalTech

TalTech tutvustab õppimisvõimalusi küberkaitse magistriõppekaval

TalTechi küberkriminalistika ja küberjulgeoleku keskus viib läbi virtuaalse infotunni sisseastujatele, kus tutvustatakse küberkaitse magistriõppekava.

Infotund toimub 9. märtsil algusega kell 18 Teams'is Tallinna Tehnikaülikooli magistriõppe infonädala raames. Õppekava tutvustab programmijuht Rain Ottis. Infotund toimub inglise keeles. Täpsem teave infotunni kohta ja Teams´i link siin.

Magistriõppe infonädala info leiad siit. Loe õppekava ja kandideerimise kohta lähemalt siit.

Küberkaitse magistrikava on Tallinna Tehnikaülikooli ja Tartu Ülikooli ühendõppekava, kus tudengid võtavad kursuseid mõlemast ülikoolist. Küberkaitse ja digitaalse ekspertiisi peaerialade õpe toimub valdavalt Tallinnas ning krüptograafia peaeriala õpe toimub valdavalt Tartus. Õppekava eesmärk on anda laiapõhjalised teadmised infosüsteemide turvalisusest ning erialased oskused vastavalt valitud peaerialale.

CybExer Technologies

CybExer Technologies kaasas laienemiseks 5 miljonit

CybExer Technologies kaasas Eesti ja Soome investoritelt 5 miljonit eurot, et jätkata üha kasvavate küberrünnakute ajal era- ja riigisektorile realistlike küberõppuste harjutusväljakute arendamist.

Ettevõtte esimese investeerimisvooru käigus liitusid CybExer Technologies meeskonnaga riskikapitalifondid Karma Ventures, First Fellow Partners ja Specialist VC ja ingelinvestorid, kellel on suur kogemus küberturvalisuse valdkonnas.

"Järjest keerulisemate küberrünnakute tõttu on üle maailma kasvanud vajadus tõsta õppuste- ja koolitustega küberteadlikkust ja valmisolekut. Klientide tagasiside näitab, et tänu meie realistlike küberrünnakute stsenaariumite kogule, lihtsale ja mugavale funktsionaalsusele ja väljanägemisele on meie treeningplatvormist kasu nii era- kui riigisektorile. Kuna nõudlus meie toodete ja teenuste vastu järjest kasvab, siis oli aeg kaasata asjatundlike investorite rühm, kelle teadmised küberturvalisusest ja selle edendamise vajadusest maailmas on CybExeri kasvu katalüsaatoriks," ütles Andrus Kivisaar, Cybexer Technologies'e tegevjuht.

First Fellow Partners juhi Risto Siilasmaa sõnul „pole kahtlust, et küberharjutusväljaku tehnoloogia mängib üle maailma era- ja riigisektori kübervastupidavuse loomisel olulist rolli ja me ei taha sellest maha jääda. Meile on väga muljet avaldanud nii CybExeri meeskond kui ka nende loodud tehnoloogia."

Fotol Andrus Kivisaar, Cybexer Technologies kaas-asutaja ja tegevjuht

CybExer hindab tänase küberharjutusväljakute turu suuruseks üle 5 miljardi euro aastas ja lähtuvalt klientide huvi kasvust on turg kasvutrendis.

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