Riikliku küberturvalisuse uudiskiri

2022-12

Majandus- ja Kommunikatsiooniministeerium

Riikliku küberturvalisuse aastakonverents 2022

Riigi Infosüsteemi Amet

2023. aastal lõppeb mitme olulise Microsoft tarkvara tootetugi

E-riigi akadeemia

Eesti küberlabor Ukraina relvajõududele

Majandus- ja Kommunikatsiooniministeerium

Seekordses uudiskirjas

Majandus- ja Kommunikatsiooniministeerium

Riikliku küberturvalisuse aastakonverents 2022 3

Majandus- ja Kommunikatsiooniministeerium teeb Amazon Web Services-iga koostööd avaliku sektori IT toimepidevuse parendamiseks

Riigi infosüsteemi Amet 4

President Alar Karis sai RIAs ülevaate olukorrast küberruumis 5

2023. aastal lõppeb mitme olulise Microsoft tarkvara tootetugi 5

RIA registreeris oktoobris 265 mõjuga intsidenti, mis on viimase poole aasta kõige kõrgem näitaja 6

Välisministeerium

ÜRO Peaassambleel võeti vastu Programm of Action (PoA) resolutsioon 6

O5-G5+ grupi riikide kohtumine Hollandis 6

Kutse osalema seminaril “Great Powers and Cyber Diplomacy” 6

Tarbjakaitse ja Tehnilise Järelvalve Amet

TTJA juhib üleriigilise kampaaniaga tähelepanu internetikäitumisele 6

Tallinna Tehnikaülikool

Küberolümpia projekti kübervõistlused nüüd tunnustatud Teaduse Populariseerija tunnusmärgiga 7

KüberKonverents kohtub Sõnaraamatuga 7

Küber-pealelõunad detsembris 8

Alustab KüberTalentide ettevõtluse stipendiumprogramm “Põgenemistuba”

Lastekaitse Liit 8

Targalt internetis advendikalender lastele 8

E-riigi Akadeemia

Eesti küberlabor Ukraina relvajõududele 9

eGA avas Moldovas kontori

Cybernetica 9

5 aastat Smart-ID! 9

European Telecommunications Standards Institute

ETSI veebiseminar: uuendused raadioseadmete direktiivi, küberkerksuse akti ja tehisintellekti seaduse kohta 9

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

Riikliku küberturvalisuse aastakonverents 2022

23. novembril toimus esmakordselt riikliku küberturvalisuse aastakonverents, mis keskendus laiapõhjalisele vaatele küberturvalisuses. Kuhu ja kuidas on Eesti riik teel? Millised riskid ja ohud meid varitsevad? Keskse küsimusena vaadeldi vastutust küberturvalisuse ja infoturbe eest ning mõtestati selle seoseid riigivalitsemise ja äriprotsessiga.

Konverentsi avas peaminister Kaja Kallas, kelle sõnavõtust jäi kõlama, et käimas on info- ja kübersõda. Seetõttu tuleb teenustesse järjepidevalt investeerida, et need peaksid vastu ka halvimate stsenaariumide korral. Peaministri soovitus oli läbi harjutada kõige mustemad stsenaariumid, sest praktika toetab tõhusat toimimist kriisiolukordades. Lisaks tuleb tema sõnul fookus seada valimiste turvalisusele ja usaldusväärsetele ühendustele. Ta rõhutas, et võtmetähtsusega on inimeste teadlikkuse kasvatamine küberohtudest ja küberhügieeni parendamine.

Ettevõtlus- ja infotehnoloogiaminister Kristjan Järvan kiitis kõiki, kes kübervaldkonna arengusse panustavad. Tema sõnul on aasta jooksul suudetud edukalt ära hoida suuremaid ohte ja on tegutsetud tõhusalt. Minister tõi välja, et suur võit sellel aastal on baasrahastuse saamine. Järvan toonitas kasutajamugavuse olulisust, sest pole tarvis luua uhkeid lahendusi, mida paljud inimesed kasutada ei oska. Suhtlus riigiga peab olema lihtne ja mugav igale kodanikule.

Paneeli „Laiapindne küberjulgeolek: mida me teame täna, mida ei teadnud aasta tagasi?“ arutelus osalesid Eesti suursaadik Ukrainas Kaimo Kuusk, välisluureameti peadirektor Kaupo Rosin, PPA peadirektori asetäitja arenduse alal Krista Aas ja seda modereeris E-riigi Akadeemia küberturvalisuse valdkonna juht Merle Maigre. Vestlus keskendus suuresti Ukraina sõjale, seal hangitud õppetundidele ja koostööle erinevate riikide vahel. Samuti rõhutati, et ohuhinnangute täiendamine eri asutuste poolt on äärmiselt oluline.

CERT-EE juht Tõnu Tammer ja CYBERS tegevjuht Jürgen Erm avasid koostööd erasektori ning riigi vahel. Märgiti, et ettevõtjad tunnevad sageli hirmu intsidentidest teavitamisel ja paraku hakatakse küberturvalisusele tihti mõtlema alles siis, kui probleem on juba käes. Siiski pööratakse küberturvalisusele üha rohkem tähelepanu ja nagu ettekandes rõhutati, siis „selle peale peab ehitama!“.

Teine paneel kandis nime „Riskijuhtimine ja infoturve dünaamiliste ohtude maailmas“. Vestluses osalesid Telia Eesti tehnoloogiajuht Andre Visse, RIA juhtiv küberturbe ekspert Mari Seeba ja Eesti Panga president Madis Müller. Paneeli juhtis digiarengu asekantsler Luukas Kristjan Ilves. Arutelust jäi kõlama, et kõikides tegevustes ja otsustes on riskid ning juht peab seda teadvustama. Seetõttu on tähtis, et riskide kaardistamine, maandamine ja mõtestamine on osa igapäevasest tööst. Ehkki on valdkondi, kus risk saab olla positiivne, siis kübervaldkonnas see nii pole. Tuleb mõista, et küberrisk on alati negatiivne ja selle riski juhtimiseks tuleb tööd

Fotod: Meeli Küttim

teha. Paneelis osalejad tõid välja, et valmisolek küberohtudele reageerimiseks on aasta jooksul paranenud, kuid endiselt on väga oluline panna paika strateegiline liikumine kogu kübervaldkonnas.

Aastakonverentsi teine osa oli pühendatud küberstrateegiale. Riikliku küberuturvalisuse juht Liisa Past tegi ettekande „Küberturvaline riik 2022+", millele järgnes paneel „Küberturvaline Eesti 2022+". Paneelis osales veel Cybernetica juhatuse esimees Oliver Väärtnõu ja vestlust modereeris Karl-Alari Varma. Selle paneeli puhul oli publikul võimalus kaasa rääkida arutelu algusest saati. Ettekanne avas riiklikku suunda küberturvalisuse valdkonnale ja ühtlasi tõi Past välja, et valmimas on riikliku kübeturvalisuse strateegia. Paneelis keskenduti suuresti haridus- ja teaduspoliitikale. Leiti, et vaja on tekitada diskussiooni riigi ja erasektori vahel, et avatult rääkida probleemidest ning võimalikest lahendustest.

Täpsemalt on võimalik aastakonverentsi paneele ja esitlusi vaadata siit: Riikliku küberturvalisuse aastakonverents - YouTube

Täname kõiki esinejaid, osalejaid ja korraldajaid. Esimene riikliku küberturvalisuse konverents andis mõista, et vajadus antud formaadi järele on keskkonnas olemas. Seega anname endast parima, et juba uuel aastal uute teemadega teie ette tulla!

Konverentsi korraldas Majandus- ja Kommunikatsiooniministeerium koostöös Riigi Infosüsteemi Ametiga Euroopa Liidu struktuuritoetuse toetusskeemist "Infoühiskonna teadlikkuse tõstmine", mida rahastab Euroopa Regionaalarengu Fond. Üritust aitas korraldada Conference Expert / Reisiekspert.

Majandus- ja Kommunikatsiooniministeerium teeb Amazon Web Services-iga koostööd avaliku sektori IT toimepidevuse parendamiseks

Majandus- ja Kommunikatsiooniministeerium teeb ettevõttega Amazon Web Services (AWS) koostööd pilvepõhise lahenduse arendamisel, mis võimaldab riikidel üle maailma kaitsta kriiside vältel tõhusalt enda digitaalseid varasid ning avalikke digiteenuseid.

Ettevõtlus- ja infotehnoloogiaminister Kristjan Järvani sõnul on sõda Ukrainas näidanud, et digitaalne toimepidevus on kriiside puhkedes riikliku julgeoleku üks nurgakivi. "Eesti juhib avaliku sektori digitaliseerimise innovatsiooni maailmas. Võimalus teha AWS-iga koostööd lahenduse loomisel, mis toetab riikide digitaalset toimepidevust ka kõige keerulisematel hetkedel kinnitab, et Eesti on digisiirde teemal usaldusväärne ning hinnatud partner," ütles minister.

"Koostöö Majandus- ja Kommunikatsiooniministeeriumiga on aidanud meil paremini mõista Eesti digiriigi vajadusi ning väljakutseid. Koostööl põhinev lähenemine on oluline uudsete tehnoloogiliste lahenduste loomisel, et tagada infotehnoloogiline järjepidevus. Eesti on paljudele riikidele nende digisiirde teekonnal eeskuju ja oleme uhked, et saame teha koostööd," sõnas Amazon Web Services valitsuste digisiirde juht Liam Maxwell.

Eestile on digiriigi toimepidevus ja kriisikindluse kasvatamine prioriteet ning varundame juba täna riiklikult olulisi andmekogusid Luksemburgis asuvas andmesaatkonnas. "Eesti digiriik on kompleksne ja mitmekihiline. Eesmärgiga tagada valmisolek ka kõige kriitilisemateks stsenaariumideks on tähtis erinevate lahenduste kombineerimine üheks tugevaks tervikuks. Pilvepõhistel lahendustel on seejuures oluline roll," ütles Järvan.

Ministri sõnul ootavad inimesed, et avalikud digiteenused on alati kättesaadavad. "Riigi digitaalsed varad peavad kriiside puhkemisel olema turvaliselt kaitstud, et säilitada võimalikult harjumuspärane elukorraldus. Suur osa kriitilisest teabest asub juba täna võrgus ja häiringud selle töös avaldavad laiapõhjalist mõju kogu ühiskonnale. Riikidel tuleb üha rohkem mõelda enda kübertagala kindlustamisele," rõhutas minister.

Ta tõi välja, et valitsused üle maailma otsivad aktiivselt võimalusi riskide maandamiseks, millele annab hoogu geopoliitilise ebakindluse kasv. "Olgu teemaks energiakriis, küberrünnakute hüppeline kasv või hoopis nõrkused taristus - arutelud on muutunud intensiivsemaks. Öeldakse, et teisi õpetades õpid ise kõige paremini ja koostöö AWS-iga on aidanud ka meil märgata järele aitamist vajavaid kohti. Seega on kasu mõlemapoolne," märkis minister. Ta sõnas, et Eestil on lisaks AWS-ile laiapõhjaline koostöö ka mitmete teiste globaalsete tehnoloogiaettevõtetega, kellega toimub pidev suhtlus Eesti digiriigi arengu tagamiseks ja kriisikindluse suurendamiseks.

President Alar Karis sai RIAs ülevaate olukorrast küberruumis

9. novembril külastas RIAt Eesti Vabariigi president Alar Karis koos delegatsiooniga. President sai põhjaliku ülevaate olukorrast küberruumist ja ülevaate järgmise aasta plaanidest.

Põhjalikumalt peatuti Ukraina teemal, mis on olnud selle aasta läbivaks teemaks. Küberturvalisuse teenistuse juht Gert Auväärt rõhutas, et ka sõja lõppedes, ei saa prognoosida, et küberruumis läheks rahulikumaks. Vastupidi — tuleb kogu aeg valvel olla, valmistuda ning olla küberruumi kaitsmisel ülesannete kõrgusel.

Arutelul peatuti ka valimiste turvalisusel. Päev enne RIAsse tulekut kirjutas Alar Karis alla otsusele, mille kuulutas Riigikogu valimispäevaks tuleva aasta 5. märtsi. RIA juht Margus Noormaa kinnitas presidendile, et RIA on valimiste turvalisusega tegelenud väga põhjalikult ning ollakse järgmise aasta Riigikogu valimisteks valmis.

Presidendi küsimusele, kui teadlikud on noored küberohtudest vastas Gert Auväärt, et noorte küberteadlikkus peaks olema oluliselt suurem ning küberhügieeni võiks koolides õpetada. RIA on panustanud sel aastal Tagasi Kooli projekti jaoks mitmete küberloengutega ning tegelenud laiema avalikkuse küberhügieeniga läbi IT-vaatliku kampaania ja venekeelse ennetuskampaania. Näiteks tõusis IT-vaatliku venekeelse kodulehe külastatavus tänu kampaaniale 4000 % võrra.

2023. aastal lõppeb mitme olulise Microsoft tarkvara tootetugi

2023. aastal lõppeb mitme olulise Microsoft tarkvara tootetugi, mille tõttu ei ole teenused enam turvalised ning RIA ei soovita neid kasutada.

Outlook 2013, Office 2013, Exchange Server 2013 ning Excel 2013 on vaid käputäis Microsofti programme ja tooteid, mille tehniline tugi järgmisel aastal lõppeb. Pärast tootetoe lõppu ei saa neid tarkvarasid turvaliseks pidada.

Microsoft peatab 2023. aastal turvauuenduste väljastamise kokku 53 teenusele ja tarkvarale. Kui kasutaja või asutus kasutab neid teenuseid edasi, siis ajapikku kasvab küberintsidendi toimumise tõenäosus ning oht langeda küberrünnaku- või kuriteo ohvriks.

Loetelu kõikides toe kaotavatest Microsofti programmidest ja teenustest leiab RIA blogist. Blogist leiab ka stsenaariumid, mis võivad täituda, kui kasutusel on aegunud tarkvara.

Näiteks võib ründajal õnnestuda aegunud tarkvara tõttu siseneda või üle võtta ettevõtte meili-ja/või veebiserver, varastada töötajate e-kirjad või saada ligipääs arvutis olevatele andmete. Samuti saab aegunud tarkvara turvaaukude kaudu süsteemides levitada pahavara ja saata korda lunavararünnakuid.

Microsoft lõpetab teenuste toe järk-järgult 2023. aasta neljal kuupäeval. Windows 7, Windows 8.1 ning Windows Server 2008 R2 tugi lõppeb juba järgmise aasta 10. jaanuaril. Eestis laialt levinud meiliserveri Exchange Server 2013, Skype for Business 2015 ning MS Office 2013 tugi saab punkti 11. aprillil. MS SQL Server 2008 ning BizTalk 2013 ei saa turvauuendusi 11. juulist. Outlook 2019 for Mac, Word 2019 for Mac, PowerPoint 2019 for Mac ja mitmed teised Macile mõeldud tooted kaotavad toe 10. oktoobril 2023.

Pärast toe kadumist ei väljasta Microsoft tarkvaras leitud turvaaukudele paikasid ning iga päevaga suureneb risk, et tarkvara ei pruugi enam korralikult töötada, sest ülejäänud süsteeme arendatakse edasi. Nende toodete asemel kasutada alternatiive, millel tootetugi on olemas.

„Nii nagu sõidukid vajavad hooldust, tuleb ka programme kõpitseda, muidu need lagunevad. Tarkvara kasutamise käigus tulevad välja puudused, mida tarkvaratootjad uuendustega kõrvaldavad. Kuna need enam kui poolsada toodet kaovad Microsofti sortimendist, siis need lahendused rohkem uuendusi ei saa. See tähendab, et programmid ei pruugi enam korralikult töötada. Lisaks hakkavad küberkurjategijad haavatavusi ära kasutades süsteeme ründama, tuues sellega kaasa rahalist kahju ja ebamugavusi," ütles RIA küberintsidentide käsitlemise osakonna CERT-EE juhataja Tõnu Tammer.

RIA soovitab ettevõtetel tutvuda Eesti Infoturbestandardiga. Standard annab asutustele ja ettevõtetele detailse ülevaate, kuidas organisatsiooni eri laadi küberohtude eest kaitsta.

Lisainfo RIA kodulehel.

Riigi Infosüsteemi Amet

RIA registreeris oktoobris 265 mõjuga intsidenti, mis on viimase poole aasta kõige kõrgem näitaja

Oktoobris toimus järjekordne suurem ummistusrünnete laine Eesti riigiasutuste ja ettevõtete vastu.

- RIA algatas üleriigilise küberturvalisuse teavitus- ja ennetuskampaania, mille eesmärgiks on juhtida tähelepanu küberohtudele. Lisaks toimus RIA aastaseminar koostööpartneritele.

- Austraalia tervisekindlustust pakkuv ettevõte ja USA üks suurimaid haiglakette said pihta lunavararünnakuga.

Täpsemalt saab lugeda siit.

Välisministeerium

Välisministeerium

ÜRO Peaassambleel võeti vastu Programm of Action (PoA) resolutsioon

3. novembril võeti ÜRO Peaassambleel ülekaalukalt vastu Programme of Action (PoA) resolutsioon, mille eesmärgiks on välja töötada alaline globaalne formaat kübervaldkonna julgeolekualaste teemade arutamiseks

Resolutsiooni hääletus näitas algatusele väga suurt poolehoidu: 157 poolt, vastu 6 ja erapooletuid 14, oluline on kaalukate riikide (India, LAV) poolthääl. Venemaa hääletas resolutsiooni vastu, sest nende arvates PoA õõnestab Venemaa algatatud Open Ended Working Group (OEWG) formaati. PoA täpsema sisu ja formaadi üle jätkub arutelu ÜRO OEWG töögrupis.

O5-G5+ grupi riikide kohtumine Hollandis

17.-18. novembril toimus Hollandis Haagis O5-G5+ grupi riikide (US, UK, CAN, AUS, NZ ja FR, DE, NL, SE, DK, EE) kohtumine, kus peamiste teemadena arutati küberruumi ohupilti, omavahelise koordinatsiooni ja kommunikatsiooni parendamist ning arenguid ÜRO-s ning teistes rahvusvahelistes organisatsioonides. Kaalume tõsiselt, et 2024.a võiks ühe selle formaadi kohtumise korraldada Eesti.

Kutse osalema seminaril "Great Powers and Cyber Diplomacy"

13. detsembril korraldab TalTech rahvusvahelise projekti CYDIPLO raames seminari "Great Powers and Cyber Diplomacy".

Seminari avasõnavõtu teeb DKO peadirektor, Eesti küberdiplomaatia erisaadik Tanel Sepp. Täpsem info töötoa kohta on leitav siit. Osalemisesoovi ja täiendavate küsimuste korral palun anda märku Anna-Maria Osulale.

Kõik huvilised on oodatud!

Tarbijakaitse ja Tehnilise Järelvalve Amet

Tarbijakaitse ja Tehnilise Järelvalve Amet

TTJA juhib üleriigilise kampaaniaga tähelepanu internetikäitumisele

Tarbijakaitse ja Tehnilise Järelvalve Amet (TTJA) on käivitanud üleriigilise kampaania „Ära kliki endale liigseid kohustusi!", mille eesmärgiks on juhtida tähelepanu internetikäitumisele ning veebikeskkonnas levivatele ohtudele ja pettustele.

„Oleme jõudnud oma tarbimisharjumustega ajastusse, kus internetis poodlemine ning erinevate lepingute sõlmimine on igapäevane nähtus. Näiliselt ohutud klikkamised võivad aga hooletule internetikasutajale kaasa tuua hulgaliselt probleeme ning finantskahju. Leiame, et teadlikkuse tõstmine internetis tehtavate klikkide osas on oluline, nii oskavad inimesed suuremat tähelepanu pöörata lepingulõksudele ja võimalikele pettustele ning vältida vigu nii e-ostlemisel kui ka investeerimisotsuste tegemisel," selgitab TTJA tarbijate ja ettevõtjate nõustamise osakonna juhataja Kristina Tammaru.

Internetis leviv lepingulõks võib seisneda ühekordses toote või teenuse pakkumises, auhinna loosimises osalemises või tasuta prooviperioodiga liitumises. Lepingulõks võib näida kui tavaline reklaam, sest tegu on internetis, eriti sotsiaalmeedias levivate pakkumistega, kus tasuta prooviperioodile või ühekordsele ostule

järgneb ootamatu maksekohustus. Tarbija klikib ja teeb tellimuse, teadmata, et seob ennast pikemaajalise lepingu või maksekohustusega. Reeglina on teave täiendavate maksete kohta pakkumises küll esitatud, kuid on raskesti märgatav, kuna kasutatakse kas muust tekstist oluliselt väiksemat kirjasuurust, vähem märgatavaid värve või paigutust.

Sellistele pakkumistele on iseloomulikud kirjeldused „olematu risk", „otsusta kiiresti", „100% garantii", mistõttu toob lepingulõksu sattumine omakorda kaasa eksitavate tingimustega nõustumise. E-poe tippdomeen .ee või lehe eestikeelne sisu ei anna alati alust arvata, et tegemist on Eesti ettevõttega. Samuti veebipoed, mille veebiaadressis sisaldub näiteks .lv või .de, ei pruugi olla Läti või Saksamaa ettevõtted ning veebilehel kasutatud keele järgi ei saa hinnata kauplejate päritolu.

Lisaks kogub aina enam populaarsust investeerimine. Teema, mis aga palju kõlapinda pole saanud, on see, kui palju kaasneb sellega pettusi, millega võivad inimesed kaotada väga suuri summasid. Internetis on mitmeid lehekülgi, kus külastajale lubatakse investeerimisel suurt intressi, kuid tehtud klikk teenusega liitudes võib kaasa tuua enda raske vaevaga teenitud rahast ilma jäämise. Magus müügijutt ja kiire ning hõlpsa tulu teenimise võimalus võib ratsionaalse mõtlemise tagaplaanile jätta, kuid tegelikkuses kehtib põhimõte „mis tundub liiga hea, et olla tõsi, see ei olegi tõsi".

Kampaania materjalid ning tarbijate kogemuslood leiab TTJA kodulehelt.

Tallinna Tehnikaülikool

Küberolümpia projekti kübervõistlused nüüd tunnustatud Teaduse Populariseerija tunnusmärgiga

Teaduse populariseerimise auhinnaga pärjatud Birgy Lorenzi jaoks on oluline noorte turvaline käitumine internetis. Auhind anti kätte 11. novembri teaduskommunikatsiooni konverentsil "Teaduskommunikatsioon liigutab...".

Tallinna Tehnikaülikooli IT-teadlase ja õppejõu Birgy Lorenzi fookus on noorte ja koolide toetamine IT-õppes ning õpilaste küberturvalise käitumise edendamine. Kümneid tuhandeid noori harinud teadur on öelnud, et teda vaimustab noorte küberkäitumise uurimine ja selle mõjutamine. Lorenzit käivitab interaktiivne õpetamine, milles kõik õpetajad ja õppejõud tahaksid olla edukad ning eetiline käitumine nii teadlase kui inimesena.

Just tema vedamisel ja Kaitseministeeriumi toetusel toimub detsembri alguses kooliõpilaste võistlus KüberNaaskel. Lisaks KüberNaasklile korraldab Birgy teisigi võistlusi ning viie aasta jooksul on võistlustel ja programmides osalenud 75 tuhat noort. Samuti loob ta ainekavasid, õppematerjale ja -mänge ning juhib TalTechis IT-didaktikakeskust ja akadeemilise eetika komisjoni. Ta on Eesti Informaatikaõpetajate Seltsi asutaja ja juhatuse liige, Eesti Andmekaitse Liidu juhatuses, Pelgulinna Gümnaasiumi õpetaja ja IT-arendusjuht. Aastaid on ta viinud Eesti talente välisvõistlustele nagu European Cyber Security Challenge, Cyber Patriot (USA), Magic CTF (USA).

Põhjalikuma ülevaate Birgy Lorenzi tegemistest saab Eesti Teadus-infosüsteemist.

KüberKonverents kohtub Sõnaraamatuga

Tallinna Tehnikaülikool ja Eesti Informaatikaõpetajate Selts kutsuvad kõiki osalema 10. detsembril 2022 toimuval veebikonverentsil "Sõnaraamat ja kübermöll".

Selleaastane veebiküberkonverents pakub nii töötube, mõtisklemist terminite ja mõistete üle informaatikas kui ka tutvustab koolidele enesehindamise võimalusi küberturvalises, et valmistuda Eesti Infoturbestandardi rakendamiseks. Samuti jagame ideid, kuidas talente paremini toetada ja päeva lõpuks selguvad parimad KüberNaasklid.

Lisainfo ja päevakava

Registreerimine on avatud kuni 07.12.2022.

Konverentsi ja tutvustavaid tegevusi toetavad Kaitseministeerium, Majandus- ja Kommunikatsiooniministeerium, Haridusministeerium, Eesti Keele Instituut, Eesti Interneti Sihtasutus, Riigi Infosüsteemi Amet ja Eesti Informaatikaõpetajate Selts.

Küber-pealelõunad detsembris

Tallinna Tehnikaülikool koostöös Ameerika suursaatkonnaga Eestis korraldavad miniprojekti „Roadmap for Inclusive Cybersecurity" raames kaks ingliskeelset veebinari, kus astuvad üles küberturvalisuse eksperdid Ameerikast.

19. detsembril kell 15:00 „Kuidas küberturvalisuse mõtteviisi muutus tagab küberjulgeoleku valdkonna jätkusuutlikkuse?" Prof. Augustine Orgah.

05.12 toimus veebinar „Kuidas jõuda küberturvalisuses inimlike aspektideni? How to Arrive at 'Behavioral Cybersecurity' - personal story of Wayne Patterson PhD".

Täpsem info ja registreerumine.

Alustab KüberTalentide ettevõtluse stipendiumprogramm "Põgenemistuba"

Tallinna Tehnikaülikool kuulutas välja stipendiumiprogrammi leidmaks 18-30aastaseid kübertalente, kes soovivad ennast edasi arendada ettevõtluse valdkonnas.

Stipendiumi eesmärgiks on toetada ja tunnustada kübertalente ja suunata neid omandama pädevusi teadusliku mõtteviisi, küberturvalisuse ja ettevõtluse valdkonnas; propageerida ja soodustada Eesti noori ja ka laiemat üldsust looma küberturvalisuse teadlikkust tõstvaid ja tehnilisi oskuseid arendavaid tegevusi, mida on noortel võimalik hiljem enda loodud ettevõtetel toodete või teenusena turundada.

Statuut ja info.

Registreerumine programmi on avatud kuni 22.12.2022.

Projekti toetab Startup Estonia, EAS ja Kredex. Partneritena osalevad ka RangeForce, CTF Tech, CyberWise, Helmes ja Vespia.

Lastekaitse Liit
Estonian Union for Child Welfare

Lastekaitse Liit

Targalt internetis advendikalender lastele

Alates 1. detsembrist on avatud Targalt internetis advendikalender lastele, millest leiab diginippe ja -trikke nutiseadmete targemaks ja turvalisemaks kasutamiseks.

Igal päeval avaneb üks uus aken, millest leiab teavet ja harivaid ning ka lõbusaid ülesandeid erinevatel nutiseadmete kasutamisega seotud teemadel, näiteks paroolid, puhkusenipid, suhtlemine, postitamine, pildistamine, digikoristus jne. Kalendris on praktilised nõuanded, mille saab kohe kasutusse võtta. Esimene ülesanne testib soojenduseks kasutaja kiirust ja osavust.

Advendikalender Targalt internetis kodulehel.

Advendikalendri koostas Lastekaitse Liit projekti Targalt internetis raames. Targalt internetis projekti eesmärk on laste, lapsevanemate ja õpetajate targem interneti- ja nutiseadme kasutus. Projekti toetab sotsiaalministeerium ja on kaasrahastanud Euroopa Liit.

E-riigi Akadeemia

Eesti küberlabor Ukraina relvajõududele

Euroopa Liidu Euroopa rahurahastu poolt Ukrainale antava toetuse raames paigaldasid E-riigi Akadeemia ja CybExer Technologies Ukraina relvajõudude küberkaitseüksustele küberlabori.

Töö on osa Euroopa rahurahastu küberkaitse valdkonna toetusest Ukrainale. Selle elluviimist juhib E-riigi Akadeemia.

Lisainfo eGA kodulehelt.

eGA avas Moldovas kontori

Sealse kontori tööd juhib Epp Maaten, kes koos meeskonnaga ja Moldova valitsusega viivad ellu Euroopa Liidu toetatud küberkerksuse projekti.

Projekt aitab Moldova riigiasutustel viia oma tegevused kooskõlla EL võrgu- ja infoturbe direktiivi nõuetega.

Lisainfo projekti kohta siit.

Cybernetica

5 aastat Smart-ID!

Uute arenduste poole lükkas vajadus turvalise mugavuse järele.

Sel aastal tähistas Smart-ID oma 5. aastapäeva. 2017. aastal käivitatud ja Cybernetica patenteeritud SplitKey tehnoloogial töötav Smart-ID on kiiresti kasvatanud Baltikumis ja Islandil enam kui 3 miljonist kasutajast koosnevaks kasutajabaasiks, turvalise ja märgivaba autentimismeetodi jaoks, mida kasutavad laialdaselt pangad, e-kaubanduse ettevõtted ja valitsusasutused ja teised. Igas sekundis sooritatakse 80 tehingut. Seega on mõju ettevõtetele, valitsusasutustele, aga ka tavapärastele ostjatele ja kodanikele olnud tohutu.

Loomise ajal kehtestas Euroopa Keskpank eeskirju klientide tugevama autentimise kohta. Seetõttu otsisid pangad lahendust, mis võiks asendada olemasolevad omandipõhised autentimisfaktorid, nagu füüsilised ühekordsed koodikaardid, millegi raskemini kopeeritava, varastatava ja paljundatavaga.

Lisaks soovisid pangad, et nende klientidel oleks endiselt mugav kasutuskogemus ja kaasataks protsessidesse nutitelefone. Kuid tootjad ise ei usaldanud ega ole siiani täielikult usaldanud nutitelefonidele omamisteguri elementide pakkumist. Meie partner SK ID Solutions usaldas Cyberneticale alternatiivsete lahenduste otsimise, mis lahendaksid pankade väljakutsed.

Saime proovida huvitavat krüptotehnikat, mis uurib olukordi, kus kontroll krüptovõtme üle on jagatud või krüptovõti ise on jagatud mitme osapoole vahel. Seda nimetatakse läve krüptosüsteemiks ja see on iseenesest tuntud idee sõjaliste rakenduste algusaegadest saadik ning seda on edasi arendatud 90ndatel.

Cybernetica rakendas seda veidi teistsuguses olukorras ja ühendati teadmistepõhine autentimisfaktor (ainult kasutajale teadaolevad PIN-koodid) ja valduspõhine autentimisfaktor (kasutaja nutitelefon) üheks uudsete turvaomadustega krüptosüsteemiks. Nii sündis meie patenteeritud SplitKey tehnoloogia. See võeti kohe Smart-ID sees kasutusele autentimise ja elektroonilise allkirja tehnoloogia alusena.

Loe edasi Smart-ID loomisest siin.

European Telecommunications Standards

ETSI veebiseminar: uuendused raadioseadmete direktiivi, küberkerksuse akti ja tehisintellekti seaduse kohta

ETSI-l on hea meel kutsuda osalema veebiseminaril: Raadioseadmete direktiivi, küberkerksuse akti ja tehisintellekti seaduse oleku värskendus, mis toimub 15. detsembril 2022.

Veebiseminar annab ülevaate Euroopa Komisjoni praegustest algatustest, mis juhivad standardimise seisukohast mitmeid olulisi poliitilisi algatusi, mis on seotud küberturvalisuse, privaatsuse, pettustevastase kaitse ja tehisintellektiga. Sellega seoses kehtestatakse uued olulised nõuded, mida seadmete tootjad peavad täitma, et säilitada jätkuv juurdepääs ühtsele Euroopa turule.

Lisainfo ja registreerimine 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 ESTONIA