Euroopa Liidu
Teataja

ET
L-seeria

2024/1774

25.6.2024

KOMISJONI DELEGEERITUD MÄÄRUS (EL) 2024/1774,

13. märts 2024,

millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 seoses regulatiivsete tehniliste standarditega, millega määratakse kindlaks IKT-riski juhtimise vahendid, meetodid, protsessid ja põhimõtted ning lihtsustatud IKT-riski juhtimise raamistik

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrust (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011, ([1]) eriti selle artikli 15 neljandat lõiku ja artikli 16 lõike 3 neljandat lõiku,

ning arvestades järgmist:

(1) Määrus (EL) 2022/2554 hõlmab mitmesuguseid finantssektori ettevõtjaid, kes erinevad suuruse, struktuuri, sisemise korralduse ning tegevuse laadi ja keerukuse poolest, mistõttu on raskused ja riskid, millega nad kokku puutuvad, suuremad või väiksemad. Et tagada selle mitmekesisuse nõuetekohane arvessevõtmine, peaksid kõik nõuded, mis käsitlevad IKT turvalisuse põhimõtteid, menetlusi, protokolle ja vahendeid ning lihtsustatud IKT-riski juhtimise raamistikku, olema proportsionaalsed finantssektori ettevõtjate suuruse, struktuuri, sisemise korralduse, tegevuse laadi ja keerukuse ning vastavate riskidega.

(2) Samal põhjusel tuleks finantssektori ettevõtjatele, kelle suhtes kohaldatakse määrust (EL) 2022/2554, võimaldada teatav paindlikkus IKT turvalisuse põhimõtteid, menetlusi, protokolle ja vahendeid ning lihtsustatud IKT-riski juhtimise raamistikku käsitlevate nõuete täitmisel. Seetõttu peaks finantssektori ettevõtjatel olema lubatud kasutada nendest nõuetest tulenevate dokumenteerimisnõuete täitmisel kõiki juba olemas olevaid dokumente. Seega tuleks eraldi IKT turvalisuse põhimõtete väljatöötamist, dokumenteerimist ja rakendamist nõuda ainult teatavate oluliste elementide puhul, võttes muu hulgas arvesse valdkonna juhtivaid tavasid ja standardeid. Lisaks on vaja välja töötada ja dokumenteerida IKT turvalisuse menetlused, et hõlmata konkreetsed tehnilised rakendusaspektid, sealhulgas võimsuse ja jõudluse haldus, nõrkuse- ja paigahaldus, andmete ja süsteemide turvalisus ning logimine, ja neid menetlusi rakendada.

(3) Et tagada käesoleva määruse II jaotise I peatükis osutatud IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite nõuetekohane rakendamine aja jooksul, on oluline, et finantssektori ettevõtjad määraksid ja säilitaksid nõuetekohaselt kõik IKT turvalisusega seotud rollid ja vastutusvaldkonnad ning näeksid ette kõnealuste põhimõtete või menetluste järgimata jätmise tagajärjed.

(4) Huvide konflikti riski maandamiseks peaksid finantssektori ettevõtjad tagama IKTga seotud rollide ja vastutusvaldkondade määramisel ülesannete lahususe.

(5) Et tagada paindlikkus ja lihtsustada finantssektori ettevõtjate kontrolliraamistikku, ei tohiks finantssektori ettevõtjaid kohustada välja töötama erisätteid käesoleva määruse II jaotise I peatükis osutatud IKT turvalisuse põhimõtete, menetluste ja protokollide järgimata jätmise tagajärgede kohta, kui sellised sätted on mõnes kehtestatud korras või menetluses juba olemas.

([1]) ELT L 333, 27.12.2022, lk 1, ELI: https://eur-lex.europa.eu/eli/reg/2022/2554/oj?locale=et.

(6) Dünaamilises keskkonnas, kus IKT-riskid pidevalt muutuvad, on tähtis, et käesoleva määruse II jaotises osutatud finantssektori ettevõtjad tugineksid oma IKT turvalisuse põhimõtete väljatöötamisel juhtivatele tavadele ning vajaduse korral Euroopa Parlamendi ja nõukogu määruse (EL) nr 1025/2012 ([2]) artikli 2 punktis 1 määratletud standarditele. See peaks võimaldama neil olla muutuval maastikul pidevalt informeeritud ja ette valmistatud.

(7) Käesoleva määruse II jaotises osutatud finantssektori ettevõtjad peaksid digitaalse tegevuskerksuse tagamiseks töötama oma IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite osana välja IKT-varade haldamise põhimõtted, võimsuse ja jõudluse haldamise menetlused ning põhimõtted ja menetlused IKT-toimingute jaoks ning neid rakendama. Need põhimõtted ja menetlused on vajalikud, et tagada IKT-varade seisundi seire kogu nende olelusringi jooksul, nii et neid varasid kasutataks ja hooldataks tõhusalt (IKT-varade haldus). Kõnealused põhimõtted ja menetlused peaksid ka tagama IKT-süsteemide toimimise optimeerimise ning selle, et IKT-süsteemide võimsus ja jõudlus vastavad kehtestatud äri- ja infoturbe eesmärkidele (võimsuse ja jõudluse haldus). Lisaks peaksid need põhimõtted ja menetlused tagama IKT-süsteemide tõhusa ja sujuva igapäevase haldamise ja toimimise (IKT-toimingud), minimeerides seeläbi andmete konfidentsiaalsuse, tervikluse ja kättesaadavuse vähenemise riski. Kõnealused põhimõtted ja menetlused on seega vajalikud, et tagada võrkude turvalisus, näha ette piisavad kaitsemeetmed sissetungi ja andmete väärkasutamise vastu ning säilitada andmete kättesaadavus, autentsus, terviklus ja konfidentsiaalsus.

(8) Et tagada IKT pärandsüsteemidega seotud riski nõuetekohane juhtimine, peaksid finantssektori ettevõtjad registreerima kolmandate isikute osutatavate toetavate IKT-teenuste lõppkuupäevad ja neid seirama. Andmete konfidentsiaalsuse, tervikluse ja kättesaadavuse vähenemise võimaliku mõju tõttu peaksid finantssektori ettevõtjad nende lõppkuupäevade registreerimisel ja seiramisel keskenduma IKT-varadele või -süsteemidele, mis on äritegevuse seisukohast kriitilise tähtsusega.

(9) Andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse võivad tagada krüptokontrollid. Seepärast peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad sellised kontrollid kindlaks määrama ja neid rakendama, lähtudes riskipõhisest lähenemisviisist. Sellega seoses peaksid finantssektori ettevõtjad krüptima asjaomased andmed jõudeoleku, edastamise või vajaduse korral kasutamise ajal, tuginedes kaheosalise protsessi, nimelt andmete liigitamise ja põhjaliku IKT-riski hindamise tulemustele. Võttes arvesse kasutatavate andmete krüptimise keerukust, peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad krüptima need andmed üksnes juhul, kui see on asjakohane IKT-riski hindamise tulemusi arvesse võttes. Kui kasutatavate andmete krüptimine ei ole teostatav või on liiga keeruline, peaks käesoleva määruse II jaotises osutatud finantssektori ettevõtjatel olema siiski võimalik kaitsta asjaomaste andmete konfidentsiaalsust, terviklust ja kättesaadavust muude IKT-turvameetmete abil. Võttes arvesse krüptimistehnoloogia kiiret arengut, peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad pidama sammu asjakohaste krüptoanalüüsi valdkonna suundumustega ning võtma arvesse juhtivaid tavasid ja standardeid. Seega peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad rakendama riskide maandamisel ja seirel põhinevat paindlikku lähenemisviisi, et tulla toime krüptimisega seotud muutuvate ohtudega, sealhulgas ohtudega, mis tulenevad kvanttehnoloogia arengust.

(10) IKT-toimingute turvalisus ning tegevuspõhimõtted, menetlused, protokollid ja vahendid on olulised, et tagada andmete konfidentsiaalsus, terviklus ja kättesaadavus. Väga tähtis on hoida IKT tootmise keskkonnad rangelt lahus keskkondadest, kus IKT-süsteeme arendatakse ja testitakse, või muudest tootmisega mitteseotud keskkondadest. Selline eraldamine on oluline IKT-turvameede, võimaldades ära hoida soovimatu ja loata juurdepääsu andmetele ning andmete muutmise ja kustutamise tootmiskeskkonnas, mis võib põhjustada suuri häireid käesoleva määruse II jaotises osutatud finantssektori ettevõtjate äritegevuses. Võttes arvesse praeguseid IKT-süsteemide arendamise tavasid, peaks finantssektori ettevõtjatel erandlikel asjaoludel olema siiski lubatud testida süsteeme tootmiskeskkonnas, tingimusel et nad põhjendavad sellist testimist ja saavad selleks nõutava heakskiidu.

([2]) Euroopa Parlamendi ja nõukogu 25. oktoobri 2012. aasta määrus (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ (ELT L 316, 14.11.2012, lk 12, ELI: https://eur-lex.europa.eu/eli/reg/2012/1025/oj?locale=et).

(11) IKT maastiku kiire arengu ning IKT nõrkuste ja küberohtude tõttu on vaja ennetavat ja terviklikku lähenemisviisi IKT nõrkuste kindlakstegemiseks, hindamiseks ja kõrvaldamiseks. Ilma sellise lähenemisviisita võivad finantssektori ettevõtjad, nende kliendid, kasutajad või vastaspooled olla märkimisväärselt avatud riskidele, mis seavad ohtu nende digitaalse tegevuskerksuse ja võrkude turvalisuse ning selliste andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse, mida IKT turvalisuse põhimõtted ja menetlused peaksid kaitsma. Seepärast peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad tegema kindlaks oma IKT keskkonna nõrkused ja need kõrvaldama ning nii finantssektori ettevõtjad kui ka nende kolmandast isikust IKT-teenuste osutajad peaksid järgima sidusat, läbipaistvat ja vastutustundlikku nõrkusehaldusraamistikku. Samal põhjusel peaksid finantssektori ettevõtjad IKT nõrkusi seirama, kasutades usaldusväärseid ressursse ja automatiseeritud vahendeid, veendumaks, et kolmandast isikust IKT-teenuste osutajad võtavad osutatavate IKT-teenuste nõrkuste kõrvaldamiseks viivitamata meetmeid.

(12) IKT turvalisuse põhimõtetes ja menetlustes, mille eesmärk on kontrollitud keskkonnas testimise ja rakendamise teel kõrvaldada kindlakstehtud nõrkused ja ära hoida paikade installimisest tulenevad häired, peaks olema tähtsal kohal paigaldus.

(13) Et tagada õigeaegne ja läbipaistev teavitamine võimalikest turvaohtudest, mis võivad mõjutada finantssektori ettevõtjat ja tema sidusrühmi, peaksid finantssektori ettevõtjad kehtestama menetlused IKT nõrkuste vastutustundlikuks avalikustamiseks klientidele, vastaspooltele ja üldsusele. Nende menetluste kehtestamisel peaksid finantssektori ettevõtjad muu hulgas arvesse võtma selliseid tegureid nagu nõrkuse tõsidus ja võimalik mõju sidusrühmadele ning valmidus võtta parandus- või leevendusmeetmeid.

(14) Et oleks võimalik anda kasutaja pääsuõigusi, peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad kehtestama tugevad meetmed, mis võimaldavad tagada finantssektori ettevõtja teabele juurdepääsu saavate isikute ja süsteemide kordumatu identifitseerimise. Selle tegemata jätmine võib kaasa tuua loata juurdepääsu finantssektori ettevõtjate andmetele, andmetega seotud rikkumised ja pettuse ning seega ohustada tundlike finantsandmete konfidentsiaalsust, terviklust ja kättesaadavust. Kuigi üld- või jagatud kontode kasutamine peaks olema finantssektori ettevõtjate kindlaks määratud asjaoludel erandkorras lubatud, peaksid finantssektori ettevõtjad tagama, et säilib vastutus nende kontode kaudu toimuva tegevuse eest. Ilma selle kaitsemeetmeta saaksid võimalikud pahatahtlikud kasutajad takistada uurimis- ja parandusmeetmete võtmist ning finantssektori ettevõtjad muutuksid avastamata pahatahtliku tegevuse eest kaitsetuks ja nende suhtes võidakse kehtestada karistusi.

(15) IKT keskkonna kiire arenguga sammu pidamiseks peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad rakendama töökindlaid IKT-projektide juhtimise põhimõtteid ja menetlusi, et säilitada andmete kättesaadavus, autentsus, terviklus ja konfidentsiaalsus. Neis põhimõtetes ja menetlustes tuleks kindlaks määrata elemendid, mis on vajalikud IKT-projektide edukaks juhtimiseks, sealhulgas finantssektori ettevõtja IKT-süsteemide muutmine, soetamine, hooldamine ja arendamine, olenemata finantssektori ettevõtja valitud IKT-projektide juhtimise metoodikast. Nende põhimõtete ja menetluste rakendamisel peaksid finantssektori ettevõtjad kasutama oma vajadustele vastavaid testimistavasid ja -meetodeid, järgides samal ajal riskipõhist lähenemisviisi ning tagades turvalise, usaldusväärse ja vastupidava IKT keskkonna säilimise. Et tagada IKT-projekti turvaline rakendamine, peaksid finantssektori ettevõtjad kandma hoolt selle eest, et töötajad, kes on pärit konkreetsetest ärisektoritest või täidavad konkreetseid rolle, mida asjaomane IKT-projekt mõjutab, saavad pakkuda vajalikku oskus- ja muud teavet. Tõhusa järelevalve tagamiseks tuleks juhtorganile esitada IKT-projektide kohta – eelkõige kriitilise tähtsusega või olulisi funktsioone mõjutavate projektide ja nendega seotud riskide kohta – aruandeid. Finantssektori ettevõtjad peaksid kohandama süstemaatilise ja pideva läbivaatamise ning aruannete sagedust ja üksikasju vastavalt asjaomaste IKT-projektide tähtsusele ja mahule.

(16) On vaja tagada, et käesoleva määruse II jaotises osutatud finantssektori ettevõtjate soetatavad ja arendatavad tarkvarapaketid integreeritakse tõhusalt ja turvaliselt olemasolevasse IKT keskkonda kooskõlas kindlaksmääratud äri- ja infoturbe eesmärkidega. Seepärast peaksid finantssektori ettevõtjad selliseid tarkvarapakette põhjalikult hindama. Sel eesmärgil ning samuti selleks, et teha kindlaks nõrkused ja võimalikud turvalüngad nii tarkvarapakettides kui ka IKT-süsteemides laiemalt, peaksid finantssektori ettevõtjad IKT turvalisust testima. Et hinnata tarkvara terviklust ja tagada, et tarkvara kasutamine ei põhjusta IKT turvalisuse riske, peaksid finantssektori ettevõtjad samuti läbi vaatama soetatud tarkvara lähtekoodid, sealhulgas (võimaluse korral) kolmandast isikust IKT-teenuste osutajate pakutud, omandiõigusega kaitstud tarkvara lähtekoodid, kasutades nii staatilisi kui ka dünaamilisi testimismeetodeid.

(17) Muudatused, olenemata nende ulatusest, toovad kaasa riske ning võivad märkimisväärselt ohustada andmete konfidentsiaalsust, terviklust ja kättesaadavust ning seega põhjustada tõsiseid talitlushäireid. Et kaitsta finantssektori ettevõtjaid võimalike IKT nõrkuste eest, mis võivad tekitada neile märkimisväärseid riske, on vaja ranget kontrolliprotsessi, veendumaks, et kõik muudatused vastavad vajalikele IKT turvanõuetele. Seepärast peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad kehtestama oma IKT turvalisuse põhimõtete ja menetluste olulise osana usaldusväärsed IKT-muudatuste juhtimise põhimõtted ja menetlused. Et säilitada IKT-muudatuste juhtimise protsessi objektiivsus ja tõhusus, ära hoida huvide konfliktid ning tagada IKT-muudatuste objektiivne hindamine, tuleb muudatuste heakskiitmise eest vastutajad lahus hoida muudatuste taotlejatest ja rakendajatest. Et saavutada tõhus üleminek ja IKT-muudatuste kontrollitud rakendamine ning võimalikult vähe häirida IKT-süsteemide toimimist, peaksid finantssektori ettevõtjad määrama selged rollid ja vastutusvaldkonnad, eesmärgiga tagada IKT-muudatuste kavandamine, piisav testimine ja kvaliteet. Et tagada IKT-süsteemide jätkuvalt tõhus toimimine ja luua endale turvavõrk, peaksid finantssektori ettevõtjad samuti välja töötama ja kasutusele võtma varumenetlused. Finantssektori ettevõtjad peaksid need varumenetlused selgelt kindlaks määrama ning määrama ühtlasi vastutusvaldkonnad, et tagada ebaõnnestunud IKT-muudatuste korral kiire ja tõhus reageerimine.

(18) IKT intsidentide avastamise ja haldamise ning nendest teatamise jaoks peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad kehtestama IKT intsidente käsitlevad põhimõtted, mis hõlmavad nende intsidentide haldamise protsessi komponente. Selleks peaksid finantssektori ettevõtjad tegema kindlaks kõik organisatsioonisisesed ja -välised isikud, kes saavad hõlbustada selle protsessi eri etappide nõuetekohast koordineerimist ja rakendamist. Et optimeerida IKT intsidentide avastamist ja neile reageerimist ning teha kindlaks nende intsidentide puhul esinevad suundumused kui väärtuslik teabeallikas, mis võimaldab finantssektori ettevõtjatel tõhusalt tuvastada ja käsitleda algpõhjusi ja probleeme, peaksid finantssektori ettevõtjad eelkõige analüüsima üksikasjalikult neid IKT intsidente, mida nad peavad kõige olulisemateks, muu hulgas nende korrapärase kordumise tõttu.

(19) Et tagada anomaalse tegevuse varajane ja tõhus avastamine, peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad koguma, seirama ja analüüsima eri allikatest pärit teavet ning määrama kindlaks seonduvad rollid ja vastutusvaldkonnad. Sisemistest teabeallikatest on äärmiselt olulised logid, kuid finantssektori ettevõtjad ei tohiks üksnes neile tugineda. Finantssektori ettevõtjad peaksid arvesse võtma laiemat teavet, mille hulka kuulub teave, mida esitavad teiste sisefunktsioonide täitjad, kes on sageli väärtuslik teabeallikas. Samal põhjusel peaksid finantssektori ettevõtjad analüüsima ja seirama välistest allikatest kogutud teavet, sealhulgas kolmandast isikust IKT-teenuste osutajate esitatud teavet intsidentide kohta, mis mõjutavad nende süsteeme ja võrke, ning teavet muudest allikatest, mida finantssektori ettevõtjad peavad asjakohaseks. Kui selline teave kujutab endast isikuandmeid, kohaldatakse liidu andmekaitseõigust. Isikuandmed peaksid piirduma sellega, mis on vajalik intsidendi avastamiseks.

(20) IKT intsidentide avastamise hõlbustamiseks peaksid finantssektori ettevõtjad säilitama tõendid intsidentide kohta. Et ühelt poolt tagada selliste tõendite säilitamine piisavalt kaua ja teiselt poolt vältida liigset regulatiivset koormust, peaksid finantssektori ettevõtjad määrama kindlaks säilitamistähtaja, võttes muu hulgas arvesse andmete kriitilist tähtsust ja liidu õigusest tulenevaid säilitamisnõudeid.

(21) Et tagada IKT intsidentide õigeaegne avastamine, ei tohiks käesoleva määruse II jaotises osutatud finantssektori ettevõtjad pidada kriteeriume, mille korral käivitatakse IKT intsidendi tuvastamise ja sellele reageerimise protsess, ammendavateks. Lisaks, ehkki finantssektori ettevõtjad peaksid kõiki neid kriteeriume arvesse võtma, ei pea kriteeriumides kirjeldatud asjaolud ilmnema samal ajal ning kõnealuse protsessi käivitamiseks tuleks asjakohaselt kaaluda mõjutatud IKT-teenuste tähtsust.

(22) IKT talitluspidevuse põhimõtete väljatöötamisel peaksid käesoleva määruse II jaotises osutatud finantssektori ettevõtjad arvesse võtma IKT-riski juhtimise olulisi elemente, sealhulgas IKT intsidentide haldamise ja kommunikatsioonistrateegiaid, IKT-muudatuste juhtimise protsessi ja kolmandast isikust IKT-teenuste osutajatega seotud riske.

(23) Tuleb kindlaks määrata stsenaariumid, mida käesoleva määruse II jaotises osutatud finantssektori ettevõtjad peaksid arvesse võtma nii IKT reageerimis- ja taastekavade rakendamisel kui ka IKT talitluspidevuse kavade testimisel. Finantssektori ettevõtjad peaksid alustuseks analüüsima iga sellise stsenaariumi asjakohasust ja usutavust ning vajadust töötada välja alternatiivsed stsenaariumid. Finantssektori ettevõtjad peaksid keskenduma nendele stsenaariumidele, mille puhul investeerimine kerksust suurendavatesse meetmetesse võiks olla tõhusam ja tulemuslikum. Analüüsides esmase IKT-taristu ning varuvõimsuse, varundusseadmete ja varurajatiste vahelisi ümberlülitusi, peaksid finantssektori ettevõtjad hindama, kas varuvõimsus, varundusseadmed ja varurajatised toimivad tõhusalt piisava aja jooksul, ning tagama, et esmase IKT-taristu tavapärane toimimine taastatakse kooskõlas taaste-eesmärkidega.

(24) Tuleb sätestada operatsiooniriski nõuded, eelkõige nõuded IKT-projektide, IKT-muudatuste ja IKT talitluspidevuse juhtimise jaoks, tuginedes nõuetele, mida juba kohaldatakse kesksete vastaspoolte, väärtpaberite keskdepositooriumide ja kauplemiskohtade suhtes Euroopa Parlamendi ja nõukogu määruste (EL) nr 648/2012, ([3]) (EL) nr 600/2014 ([4]) ja (EL) nr 909/2014 ([5]) alusel.

(25) Määruse (EL) 2022/2554 artikli 6 lõike 5 kohaselt peavad finantssektori ettevõtjad vaatama läbi oma IKT-riski juhtimise raamistiku ja esitama pädevale asutusele selle läbivaatamise kohta aruande. Et võimaldada pädevatel asutustel neis aruannetes sisalduvat teavet hõlpsasti töödelda ja tagada selle teabe nõuetekohane edastamine, peaksid finantssektori ettevõtjad esitama kõnealused aruanded otsingut võimaldavas elektroonilises vormingus.

(26) Nõuetes finantssektori ettevõtjatele, kelle suhtes kohaldatakse määruse (EL) 2022/2554 artiklis 16 osutatud lihtsustatud IKT-riski juhtimise raamistikku, tuleks keskenduda nendele olulistele valdkondadele ja elementidele, mis on kõnealuste ettevõtjate tegevusulatust, riskiprofiili, suurust ja keerukust arvesse võttes minimaalselt vajalikud, et tagada nende ettevõtjate andmete ja teenuste konfidentsiaalsus, terviklus, kättesaadavus ja autentsus. Sellega seoses peaks kõnealustel finantssektori ettevõtjatel olema sisemine juhtimis- ja kontrolliraamistik ning selgelt kindlaks määratud vastutusvaldkonnad, et tagada tõhus ja usaldusväärne riskijuhtimisraamistik. Lisaks, et vähendada halduse töökoormust, peaksid kõnealused finantssektori ettevõtjad välja töötama ja dokumenteerima ainult ühe korra, nimelt infoturbe põhimõtted, milles määratakse kindlaks kõrgetasemelised põhialused ja reeglid, mis on vajalikud kõnealuste ettevõtjate andmete ja teenuste konfidentsiaalsuse, tervikluse, kättesaadavuse ja autentsuse kaitsmiseks.

(27) Käesoleva määruse sätetes käsitletakse IKT-riski juhtimise raamistikku. Neis kirjeldatakse üksikasjalikult konkreetseid elemente, mida kohaldatakse finantssektori ettevõtjate suhtes kooskõlas määruse (EL) 2022/2554 artikliga 15, ning nähakse selle määruse artikli 16 lõikes 1 osutatud finantssektori ettevõtjate jaoks ette lihtsustatud IKT-riski juhtimise raamistik. Et tagada sidusus tavapärase ja lihtsustatud IKT-riski juhtimise raamistiku vahel ning arvestades, et nimetatud sätted peaksid muutuma kohaldatavaks samal ajal, on asjakohane esitada need sätted ühes õigusaktis.

(28) Käesolev määrus põhineb regulatiivsete tehniliste standardite eelnõudel, mille esitasid komisjonile Euroopa Pangandusjärelevalve, Euroopa Kindlustus- ja Tööandjapensionide Järelevalve ning Euroopa Väärtpaberiturujärelevalve (Euroopa järelevalveasutused), konsulteerides Euroopa Liidu Küberturvalisuse Ametiga (ENISA).

([3]) Euroopa Parlamendi ja nõukogu 4. juuli 2012. aasta määrus (EL) nr 648/2012 börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (ELT L 201, 27.7.2012, lk 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj?locale=et).

([4]) Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta määrus (EL) nr 600/2014 finantsinstrumentide turgude kohta ning millega muudetakse määrust (EL) nr 648/2012 (ELT L 173, 12.6.2014, lk 84, ELI: https://eur-lex.europa.eu/eli/reg/2014/600/oj?locale=et).

([5]) Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 909/2014, mis käsitleb väärtpaberiarvelduse parandamist Euroopa Liidus ja väärtpaberite keskdepositooriume ning millega muudetakse direktiive 98/26/EÜ ja 2014/65/EL ning määrust (EL) nr 236/2012 (ELT L 257, 28.8.2014, lk 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj?locale=et).

(29) Euroopa järelevalveasutuste ühiskomitee, millele on osutatud Euroopa Parlamendi ja nõukogu määruse (EL) nr 1093/2010 ([6]) artiklis 54, Euroopa Parlamendi ja nõukogu määruse (EL) nr 1094/2010 ([7]) artiklis 54 ja Euroopa Parlamendi ja nõukogu määruse (EL) nr 1095/2010 ([8]) artiklis 54, on korraldanud käesoleva määruse aluseks olevate regulatiivsete tehniliste standardite eelnõude teemal avalikud konsultatsioonid, analüüsinud kavandatud standardite võimalikke kulusid ja kasu ning küsinud nõu määruse (EL) nr 1093/2010 artikli 37 kohaselt loodud pangandussektori sidusrühmade kogult, määruse (EL) nr 1094/2010 artikli 37 kohaselt loodud kindlustuse ja edasikindlustuse sidusrühmade kogult ning määruse (EL) nr 1095/2010 artikli 37 kohaselt loodud väärtpaberituru sidusrühmade kogult.

(30) Kui käesolevas määruses sätestatud kohustuste täitmiseks on vaja töödelda isikuandmeid, tuleks täielikult kohaldada Euroopa Parlamendi ja nõukogu määruseid (EL) 2016/679 ([9]) ning (EL) 2018/1725 ([10]). Näiteks tuleks intsidentide asjakohase avastamise tagamiseks isikuandmete kogumisel järgida võimalikult väheste andmete kogumise põhimõtet. Käesoleva määruse eelnõu teemal on konsulteeritud ka Euroopa Andmekaitseinspektoriga,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I JAOTIS

ÜLDPÕHIMÕTTED

Artikkel 1

Üldine riskiprofiil ja keerukus

II jaotises osutatud IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite ning III jaotises osutatud lihtsustatud IKT-riski juhtimise raamistiku väljatöötamisel ja rakendamisel võetakse arvesse finantssektori ettevõtja suurust ja üldist riskiprofiili ning tema teenuste, tegevuse ja toimingute laadi ja ulatust ning nende keerukust suurendavaid või vähendavaid aspekte, sealhulgas aspekte, mis on seotud järgmisega:

a) krüptimine ja krüptograafia;

b) IKT-toimingute turvalisus;

c) võrgu turvalisus;

([6]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj?locale=et).

([7]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1094/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Kindlustus- ja Tööandjapensionide Järelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/79/EÜ (ELT L 331, 15.12.2010, lk 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj?locale=et).

([8]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1095/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Väärtpaberiturujärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/77/EÜ (ELT L 331, 15.12.2010, lk 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj?locale=et).

([9]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) IKT-projektide ja -muudatuste juhtimine;

e) IKT-riski võimalik mõju andmete konfidentsiaalsusele, terviklusele ja kättesaadavusele ning häirete võimalik mõju finantssektori ettevõtja tegevuse järjekestvusele ja teenuste kättesaadavusele.

II JAOTIS

IKT-RISKI JUHTIMISE VAHENDITE, MEETODITE, PROTSESSIDE JA PÕHIMÕTETE EDASINE ÜHTLUSTAMINE KOOSKÕLAS MÄÄRUSE (EL) 2022/2554 ARTIKLIGA 15

I PEATÜKK

IKT turvalisuse põhimõtted, menetlused, protokollid ja vahendid

1. jagu

Artikkel 2

IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite suhtes kohaldatavad üldnõuded

1. Finantssektori ettevõtjad tagavad, et nende IKT-riski juhtimise raamistik hõlmab IKT turvalisuse põhimõtteid, infoturvet ning seonduvaid menetlusi, protokolle ja vahendeid, millele on osutatud määruse (EL) 2022/2554 artikli 9 lõikes 2. Finantssektori ettevõtjad kehtestavad käesolevas peatükis sätestatud IKT turvalisuse põhimõtted, menetlused, protokollid ja vahendid, mis

a) tagavad võrkude turvalisuse;

b) sisaldavad kaitsemeetmeid sissetungi ja andmete väärkasutamise vastu;

c) aitavad muu hulgas krüptimismeetodeid kasutades säilitada andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse;

d) tagavad andmete täpse ja kiire ning ilma suuremate häirete ja põhjendamatute viivitusteta ülekandmise.

2. Finantssektori ettevõtjad tagavad lõikes 1 osutatud IKT turvalisuse põhimõtete puhul, et

a) need on kooskõlas finantssektori ettevõtja infoturbe-eesmärkidega, mis on kindlaks määratud määruse (EL) 2022/2554 artikli 6 lõikes 8 osutatud digitaalse tegevuskerksuse strateegias;

b) neisse märgitakse kuupäev, mil juhtorgan on põhimõtted ametlikult heaks kiitnud;

c) need sisaldavad näitajaid ja meetmeid, millega

i) seirata IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite rakendamist,

ii) registreerida erandid sellest rakendamisest,

iii) tagada punktis ii osutatud erandite korral oma digitaalne tegevuskerksus;

d) neis määratakse kindlaks kõigi tasandite töötajate vastutusvaldkonnad IKT turvalisuse tagamisel;

e) neis määratakse kindlaks tagajärjed finantssektori ettevõtja töötajale, kes ei järgi IKT turvalisuse põhimõtteid, kui sellekohaseid sätteid ei ole ette nähtud mõnes muus finantssektori ettevõtja kehtestatud korras;

f) neis loetletakse dokumendid, mis tuleb säilitada;

g) nendega nähakse ette ülesannete lahusus kas kolme kaitseliiniga mudeli või mõne muu sisemise riskijuhtimis- ja kontrollimudeli raames, et ära hoida huvide konfliktid;

h) neis võetakse arvesse juhtivaid tavasid ja vajaduse korral määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standardeid;

i) neis määratakse kindlaks rollid ja vastutusvaldkonnad, mida tuleb rakendada nende põhimõtete, sealhulgas seotud menetluste, protokollide ja vahendite väljatöötamisel, rakendamisel ja haldamisel;

j) need vaadatakse läbi kooskõlas määruse (EL) 2022/2554 artikli 6 lõikega 5;

k) neis võetakse arvesse finantssektori ettevõtjat puudutavaid olulisi muudatusi, sealhulgas neid, mis on seotud tema tegevuse või protsessidega, küberohtude maastikuga või kohaldatavate õiguslike kohustustega.

2. jagu

Artikkel 3

IKT-riski juhtimine

Finantssektori ettevõtjad töötavad välja ja dokumenteerivad IKT-riski juhtimise põhimõtted ja menetlused ning rakendavad neid ning need põhimõtted ja menetlused peavad sisaldama kõike järgmist:

a) märge määruse (EL) 2022/2554 artikli 6 lõike 8 punkti b kohaselt kindlaks määratud IKT-riski taluvuse taseme heakskiitmise kohta;

b) IKT-riski hindamise menetlus ja metoodika, mis hõlmavad

   i) selliste nõrkuste ja ohtude kindlaksmääramist, mis mõjutavad või võivad mõjutada toetatavaid ärifunktsioone, IKT-süsteeme ja neid funktsioone toetavaid IKT-varasid;

   ii) selliste kvantitatiivsete või kvalitatiivsete näitajate kindlaksmääramist, mille abil mõõta punktis i osutatud nõrkuste ja ohtude mõju ning tõenäosust;

c) IKT-riski käsitlemise meetmete kindlaksmääramise, rakendamise ja dokumenteerimise kord tuvastatud ja hinnatud IKT-riskide jaoks, sealhulgas selliste IKT-riski käsitlemise meetmete kindlaksmääramine, mis on vajalikud selleks, et viia IKT-risk allapoole punktis a osutatud riskitaluvustaset;

d) pärast punktis c osutatud IKT-riski käsitlemise meetmete rakendamist alles jäänud IKT-jääkriskide jaoks

   i) sätted IKT-jääkriskide kindlakstegemise kohta;

   ii) rollide ja vastutusvaldkondade määramine seoses järgmisega:

      (1) finantssektori ettevõtja punktis a osutatud riskitaluvustaset ületavate IKT-jääkriskide aktsepteerimine,

      (2) käesoleva punkti d alapunktis iv osutatud läbivaatamisprotsess;

   iii) aktsepteeritud IKT-jääkriskide loetelu koostamine, sealhulgas nende aktsepteerimise põhjendamine;

   iv) sätted, mis käsitlevad aktsepteeritud IKT-jääkriskide läbivaatamist vähemalt kord aastas, sealhulgas

      1) IKT-jääkriskide muutuste kindlakstegemist,

      2) olemasolevate riskimaandamismeetmete hindamist,

      3) selle hindamist, kas põhjused, mis õigustasid IKT-jääkriskide aktsepteerimist, on läbivaatamise kuupäeval endiselt kehtivad ja kohaldatavad;

e) sätted, mille kohaselt seirata

   i) muutusi IKT-riskide ja küberohtude maastikul;

   ii) sisemisi ja väliseid nõrkusi ning ohte;

   iii) finantssektori ettevõtja IKT-riski, et kiiresti avastada muutused, mis võivad mõjutada tema IKT-riski profiili;

f) sätted protsessi kohta, millega tagatakse finantssektori ettevõtja äristrateegiasse ja digitaalse tegevuskerksuse strateegiasse tehtud muudatuste arvesse võtmine.

Esimese lõigu punkti c kohaldamisel peab nimetatud punktis osutatud menetlus tagama, et

a) seiratakse rakendatavate IKT-riski käsitlemise meetmete tõhusust;

b) hinnatakse, kas finantssektori ettevõtjale kindlaks määratud riskitaluvustase on saavutatud;

c) hinnatakse, kas finantssektori ettevõtja on vajaduse korral astunud samme nende meetmete parandamiseks või täiustamiseks.

3. jagu

IKT-varade haldamine

Artikkel 4

IKT-varade haldamise põhimõtted

1. Finantssektori ettevõtjad töötavad määruse (EL) 2022/2554 artikli 9 lõikes 2 osutatud IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite osana välja ja dokumenteerivad IKT-varade haldamise põhimõtted ning rakendavad neid.

2. Lõikes 1 osutatud IKT-varade haldamise põhimõtetega

a) nähakse ette määruse (EL) 2022/2554 artikli 8 lõike 1 kohaselt kindlaks määratud ja liigitatud IKT-varade olelusringi seire ja haldamine;

b) nähakse ette, et finantssektori ettevõtja säilitab kogu järgmise teabe:

   i) iga IKT-vara kordumatu tunnus,

   ii) kõigi IKT-varade füüsiline või loogiline asukoht,

   iii) kõigi IKT-varade määruse (EL) 2022/2554 artikli 8 lõike 1 kohane liigitus,

   iv) IKT-varade omanike identiteet,

   v) IKT-vara toetatavad ärifunktsioonid või teenused,

   vi) IKT talitluspidevuse nõuded, sealhulgas taasteaja ja taastekünnise eesmärk,

   vii) kas IKT-vara võib olla või on avatud välistele võrkudele, sealhulgas internetile,

   viii) IKT-varade ja neile tuginevate ärifunktsioonide vahelised seosed ja vastastikune sõltuvus,

   ix) vajaduse korral kuupäev, mil kolmandast isikust IKT-teenuste osutaja lõpetab regulaarsete, pikendatud ja kohandatud tugiteenuste osutamise, pärast mida ei toeta IKT-varade tarnija või kolmandast isikust IKT-teenuste osutaja enam asjaomast IKT-vara;

c) nähakse finantssektori ettevõtjate puhul, kes ei ole mikroettevõtjad, ette sellise teabe säilitamine, mis on vajalik, et hinnata kõigi IKT pärandsüsteemide IKT-riski kooskõlas määruse (EL) 2022/2554 artikli 8 lõikega 7.

Artikkel 5

IKT-varade haldamise menetlus

1. Finantssektori ettevõtjad töötavad välja ja dokumenteerivad IKT-varade haldamise menetluse ning rakendavad seda.

2. Lõikes 1 osutatud menetluses määratakse kindlaks kriteeriumid ärifunktsioone toetavate teabevarade ja IKT-varade kriitilise tähtsuse hindamiseks. Sel hindamisel võetakse arvesse järgmist:

a) asjaomaste ärifunktsioonidega seotud IKT-risk ja ärifunktsioonide sõltuvus teabevaradest või IKT-varadest;

b) kuidas mõjutaks asjaomaste teabevarade ja IKT-varade konfidentsiaalsuse, tervikluse ja kättesaadavuse vähenemine finantssektori ettevõtja äriprotsesse ja tegevust.

4. jagu

Krüptimine ja krüptograafia

Artikkel 6

Krüptimine ja krüptokontroll

1. Finantssektori ettevõtjad töötavad määruse (EL) 2022/2554 artikli 9 lõikes 2 osutatud IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite osana välja ja dokumenteerivad krüptimise ja krüptokontrolli põhimõtted ning rakendavad neid.

2. Finantssektori ettevõtjad võtavad lõikes 1 osutatud krüptimise ja krüptokontrolli põhimõtete kavandamisel aluseks heakskiidetud andmeliigituse ja IKT-riski hindamise tulemused. Kõnealused põhimõtted peavad sisaldama reegleid kõige järgmise kohta:

a) jõudeolekus ja edastatavate andmete krüptimine;

b) kasutatavate andmete krüptimine (vajaduse korral);

c) sisemiste võrguühenduste ja väliseid osalejaid hõlmava andmeedastuse krüptimine;

d) artiklis 7 osutatud krüptovõtmete haldamine, sealhulgas krüptovõtmete nõuetekohane kasutamine, kaitse ja olelusring.

Kui punkti b kohaldamisel ei ole kasutatavate andmete krüptimine võimalik, töötlevad finantssektori ettevõtjad kasutatavaid andmeid eraldatud ja kaitstud keskkonnas või võtavad samaväärseid meetmeid, mis tagavad andmete konfidentsiaalsuse, tervikluse, autentsuse ja kättesaadavuse.

3. Finantssektori ettevõtjad lisavad lõikes 1 osutatud krüptimise ja krüptokontrolli põhimõtetesse krüptomeetodite ja kasutustavade valimise kriteeriumid, võttes arvesse juhtivaid tavasid ja määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standardeid ning määruse (EL) 2022/2554 artikli 8 lõike 1 kohast asjaomaste IKT-varade liigitust. Finantssektori ettevõtjad, kes ei ole võimelised järgima juhtivaid tavasid või standardeid või kasutama kõige usaldusväärsemaid meetodeid, võtavad vastu leevendus- ja seiremeetmed, millega tagatakse vastupidavus küberohtudele.

4. Finantssektori ettevõtjad lisavad lõikes 1 osutatud krüptimise ja krüptokontrolli põhimõtetesse sätted krüptimistehnoloogia ajakohastamiseks või vajaduse korral muutmiseks krüptoanalüüsi valdkonnas toimuva arengu alusel. Selle ajakohastamise või muutmisega tagatakse, et krüptotehnoloogia jääb küberohtudele vastupidavaks, nagu on ette nähtud artikli 10 lõike 2 punktiga a. Finantssektori ettevõtjad, kes ei ole võimelised krüptotehnoloogiat ajakohastama või muutma, võtavad vastu leevendus- ja seiremeetmed, millega tagatakse vastupidavus küberohtudele.

5. Finantssektori ettevõtjad lisavad lõikes 1 osutatud krüptimise ja krüptokontrolli põhimõtetesse nõude registreerida lõigete 3 ja 4 kohaste leevendus- ja seiremeetmete rakendamine ning esitada rakendamise põhjendatud selgitus.

Artikkel 7

Krüptovõtmete haldamine

1. Finantssektori ettevõtjad lisavad artikli 6 lõike 2 punktis d osutatud krüptovõtmete haldamise põhimõtetesse nõuded, mis käsitlevad krüptovõtmete haldamist kogu nende olelusringi jooksul, sealhulgas nõuded krüptovõtmete loomise, uuendamise, talletamise, varundamise, arhiveerimise, otsimise, edastamise, kasutuselt kõrvaldamise, tühistamise ja hävitamise kohta.

2. Finantssektori ettevõtjad määravad kindlaks kontrollid, et kaitsta krüptovõtmeid kogu nende olelusringi jooksul kaotsimineku, loata juurdepääsu, avalikustamise ja muutmise eest, ning rakendavad neid kontrolle. Finantssektori ettevõtjad võtavad nende kontrollide kavandamisel aluseks heakskiidetud andmeliigituse ja IKT-riski hindamise tulemused.

3. Finantssektori ettevõtjad töötavad välja meetodid, et krüptovõti kaotsimineku, murdmise või kahjustumise korral asendada, ja rakendavad neid.

4. Finantssektori ettevõtjad loovad kõigi sertifikaatide ja nende säilitamise seadmete registri vähemalt kriitilise tähtsusega või olulisi funktsioone toetavate IKT-varade jaoks ja haldavad seda. Finantssektori ettevõtjad ajakohastavad seda registrit.

5. Finantssektori ettevõtjad tagavad sertifikaatide kiire uuendamise enne nende aegumist.

5. jagu

IKT-toimingute turvalisus

Artikkel 8

Põhimõtted ja menetlused IKT-toimingute jaoks

1. Finantssektori ettevõtjad töötavad määruse (EL) 2022/2554 artikli 9 lõikes 2 osutatud IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite osana välja ja dokumenteerivad IKT-toimingute haldamise põhimõtted ja menetlused ning rakendavad neid. Neis põhimõtetes ja menetlustes määratakse kindlaks, kuidas finantssektori ettevõtjad käitavad, seiravad, kontrollivad ja taastavad oma IKT-varasid, sealhulgas IKT-toimingute dokumenteerimine.

2. IKT-toimingute põhimõtted ja menetlused, millele on osutatud lõikes 1, peavad hõlmama kõike järgmist:

a) IKT-varade kirjeldus, sealhulgas kõik järgmine:

   i) IKT-süsteemide turvalise paigaldamise, hooldamise, konfigureerimise ja eemaldamise nõuded,

   ii) IKT-varade kasutatavate teabevarade haldamise, sealhulgas nende automatiseeritud ja käsitsi töötlemise ja käsitsemise nõuded,

   iii) IKT pärandsüsteemide kindlakstegemise ja kontrollimise nõuded;

b) IKT-süsteemide kontroll ja seire, sealhulgas kõik järgmine:

   i) IKT-süsteemide varundamise ja taastamise nõuded,

   ii) ajakava koostamise nõuded, kus on arvesse võetud IKT-süsteemide vastastikust sõltuvust,

   iii) kontrolljälje ja süsteemi logiteabe protokollid,

   iv) nõuded, millega tagatakse, et siseauditite ja muu testimise puhul minimeeritakse häired äritegevuses,

   v) nõuded, mis käsitlevad IKT tootmise keskkondade lahus hoidmist arendamis-, testimis- ja muudest tootmisega mitteseotud keskkondadest,

   vi) nõuded arendustegevuseks ja testimiseks tootmiskeskkonnast eraldatud keskkonnas,

   vii) nõuded arendustegevuseks ja testimiseks tootmiskeskkonnas;

c) IKT-süsteemide vigade käsitlemine, sealhulgas kõik järgmine:

i) vigade käsitlemise menetlused ja protokollid,

ii) tugi- ja eskalatsioonikontaktid, sealhulgas välised tugikontaktid ootamatute tegevus- või tehniliste probleemide puhuks,

iii) IKT-süsteemide taaskäivitamise, tagasikerimise ja taastamise menetlused IKT-süsteemide häirete puhuks.

Punkti b alapunkti v kohaldamisel peab lahus hoidmise nõue kehtima kõikide asjaomaste keskkondade komponentide, sealhulgas arvepidamise, andmete ja ühenduste suhtes, nagu on ette nähtud artikli 13 lõike 1 punktiga a.

Punkti b alapunkti vii kohaldamisel nähakse lõikes 1 osutatud põhimõtetes ja menetlustes ette, et juhud, mil testimine toimub tootmiskeskkonnas, peavad olema selgelt määratletud, põhjendatud ja ajaliselt piiratud ning asjaomase funktsiooni täitja peab olema need vastavalt artikli 16 lõikele 6 heaks kiitnud. Finantssektori ettevõtjad tagavad tootmiskeskkonnas toimuva arendustegevuse ja testimise ajal IKT-süsteemide ja tootmisandmete kättesaadavuse, konfidentsiaalsuse, tervikluse ja autentsuse.

Artikkel 9

Võimsuse ja jõudluse haldamine

1. Finantssektori ettevõtjad töötavad määruse (EL) 2022/2554 artikli 9 lõikes 2 osutatud IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite osana välja ning dokumenteerivad võimsuse ja jõudluse haldamise põhimõtted ja menetlused ning rakendavad neid; need põhimõtted ja menetlused töötatakse välja selleks, et

a) määrata kindaks vajalik IKT-süsteemide võimsus;

b) optimeerida ressursside kasutamist;

c) rakendada seire korda, millega säilitatakse ja muudetakse paremaks

i) andmete ja IKT-süsteemide kättesaadavus,

ii) IKT-süsteemide tõhusus,

iii) IKT-süsteemide võimsuse puudujäägi ennetamine.

2. Lõikes 1 osutatud võimsuse ja jõudluse haldamise menetlustega tagatakse, et finantssektori ettevõtjad rakendavad asjakohaseid meetmeid, millega võetakse arvesse pikkade või keerukate hanke- või heakskiitmismenetlustega IKT-süsteemide või ressursimahukate IKT-süsteemide eripära.

Artikkel 10

Nõrkuse- ja paigahaldus

1. Finantssektori ettevõtjad töötavad määruse (EL) 2022/2554 artikli 9 lõikes 2 osutatud IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite osana välja ja dokumenteerivad nõrkusehalduse menetlused ning rakendavad neid.

2. Lõikes 1 osutatud nõrkusehalduse menetlused töötatakse välja selleks, et

a) teha kindlaks asjakohased usaldusväärsed teaberessursid ja hoida need ajakohased, et muuta paremaks ja säilitada teadlikkus nõrkustest;

b) tagada IKT-varade nõrkuse automaatne skaneerimine ja hindamine sageduse ja ulatusega, mis on vastavuses määruse (EL) 2022/2554 artikli 8 lõike 1 kohase liigituse ja IKT-vara üldise riskiprofiiliga;

c) kontrollida, kas kolmandast isikust IKT-teenuste osutajad

i) tegelevad finantssektori ettevõtjale osutatavate IKT-teenuste nõrkustega,

ii) teavitavad finantssektori ettevõtjaid õigeaegselt vähemalt kriitilise tähtsusega nõrkustest ning statistikast ja suundumustest;

d) jälgida, kuidas kasutatakse

i) kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutatavaid kolmandate isikute teeke, sealhulgas avatud lähtekoodiga teeke,

ii) IKT-teenuseid, mille on välja töötanud finantssektori ettevõtja ise või mille on finantssektori ettevõtja jaoks spetsiaalselt kohandanud või välja töötanud kolmandast isikust IKT-teenuste osutaja;

e) kehtestada kord nõrkuste vastutustundlikuks teatavaks tegemiseks klientidele, vastaspooltele ja üldsusele;

f) seada paikade ja muude leevendusmeetmete kasutamine tuvastatud nõrkuste kõrvaldamisel esmatähtsaks;

g) seirata ja kontrollida nõrkuse kõrvaldamist;

h) nõuda IKT-süsteeme mõjutavate tuvastatud nõrkuste registreerimist ja nende kõrvaldamise seiret.

Punkti b kohaldamisel teevad finantssektori ettevõtjad kriitilise tähtsusega või olulisi funktsioone toetavate IKT-varade nõrkuse automaatse skaneerimise ja hindamise vähemalt kord nädalas.

Punkti c kohaldamisel nõuavad finantssektori ettevõtjad, et kolmandast isikust IKT-teenuste osutajad uuriksid asjaomast nõrkust, teeksid kindlaks selle algpõhjused ja rakendaksid asjakohaseid leevendusmeetmeid.

Punkti d kohaldamisel seiravad finantssektori ettevõtjad – asjakohasel juhul koostöös kolmandast isikust IKT-teenuste osutajaga – kolmanda isiku teeke ja nende võimalikke uuendusi. Kui tegemist on kasutusvalmis IKT-varaga või IKT-vara komponentidega, mis on soetatud ja mida kasutatakse selliste IKT-teenuste jaoks, mis ei toeta kriitilise tähtsusega või olulisi funktsioone, jälgivad finantssektori ettevõtjad nii palju kui võimalik kolmandate isikute teekide, sealhulgas avatud lähtekoodiga teekide kasutamist.

Punkti f kohaldamisel võtavad finantssektori ettevõtjad arvesse nõrkuse kriitilist tähtsust, määruse (EL) 2022/2554 artikli 8 lõike 1 kohast liigitust ja tuvastatud nõrkustest mõjutatud IKT-varade riskiprofiili.

3. Finantssektori ettevõtjad töötavad määruse (EL) 2022/2554 artikli 9 lõikes 2 osutatud IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite osana välja ja dokumenteerivad paigahalduse menetlused ning rakendavad neid.

4. Lõikes 3 osutatud paigahalduse menetlused töötatakse välja selleks, et

a) teha võimalikult suures ulatuses kindlaks olemasolevad tark- ja riistvarapaigad ja uuendused ning neid hinnata, kasutades automatiseeritud vahendeid;

b) määrata kindlaks hädaolukorras rakendatav IKT-varade paikamise ja ajakohastamise kord;

c) testida ja kasutada artikli 8 lõike 2 punkti b alapunktides v, vi ja vii osutatud tark- ja riistvarapaiku ja uuendusi;

d) kehtestada tark- ja riistvarapaikade installeerimise ja uuendamise tähtajad ning eskalatsioonimenetlused, kui neist tähtaegadest ei ole võimalik kinni pidada.

Artikkel 11

Andmete ja süsteemide turvalisus

1. Finantssektori ettevõtjad töötavad määruse (EL) 2022/2554 artikli 9 lõikes 2 osutatud IKT turvalisuse põhimõtete, menetluste, protokollide ja vahendite osana välja ja dokumenteerivad andmete ja süsteemide turvalisuse menetluse ning rakendavad seda.

2. Lõikes 1 osutatud andmete ja süsteemide turvalisuse menetlus peab hõlmama kõiki järgmisi andmete ja IKT-süsteemide turvalisusega seotud elemente kooskõlas määruse (EL) 2022/2554 artikli 8 lõike 1 kohase liigitusega:

a) käesoleva määruse artiklis 21 osutatud pääsupiirangud, mis toetavad vastava liigitustaseme kaitsenõudeid;

b) IKT-varade turvalise konfigureerimise lähtealuse kindlaksmääramine nii, et minimeeritakse varade avatust küberohtudele, ning meetmed, millega kontrollitakse korrapäraselt, kas neid lähtealuseid kasutatakse tõhusalt;

c) selliste turvameetmete kindlaksmääramine, millega tagatakse, et IKT-süsteemidesse ja lõppseadmetesse installitakse ainult lubatud tarkvara;

d) ründekoodide vastaste turvameetmete kindlaksmääramine;

e) selliste turvameetmete kindlaksmääramine, millega tagatakse, et finantssektori ettevõtja andmete edastamiseks ja säilitamiseks kasutatakse ainult lubatud andmekandjaid, süsteeme ja lõppseadmeid;

f) järgmised nõuded, et tagada kaasaskantavate lõppseadmete ja mittekaasaskantavate isiklike lõppseadmete turvaline kasutamine:

   i) nõue kasutada juhtimislahendust lõppseadmete kaugjuhtimiseks ja finantssektori ettevõtja andmete kaugkustutamiseks,

   ii) nõue kasutada turvamehhanisme, mida töötajad või kolmandast isikust IKT-teenuste osutajad ei saa loata muuta, eemaldada või vältida,

   iii) nõue kasutada eemaldatavaid andmesalvestusseadmeid üksnes juhul, kui IKT-jääkrisk jääb allapoole finantssektori ettevõtja artikli 3 esimese lõigu punktis a osutatud riskitaluvustaset;

g) protsess, millega kustutatakse turvaliselt finantssektori ettevõtja ruumides või mujal säilitatavad andmed, mida finantssektori ettevõtjal ei ole enam vaja koguda või säilitada;

h) protsess, millega turvaliselt likvideeritakse või kõrvaldatakse kasutusest finantssektori ettevõtja ruumides või mujal asuvad konfidentsiaalset teavet sisaldavad andmesalvestusseadmed;

i) selliste turvameetmete kindlaksmääramine ja rakendamine, millega välditakse süsteemide ja lõppseadmete puhul andmekadu ja -leket;

j) turvameetmete rakendamine tagamaks, et kaugtöö ja isiklike lõppseadmete kasutamine ei kahjusta finantssektori ettevõtja IKT turvalisust;

k) kolmandast isikust IKT-teenuste osutaja käitatavate IKT-varade või -teenuste puhul digitaalse tegevuskerksuse säilitamist käsitlevate nõuete kindlaksmääramine ja rakendamine kooskõlas andmeliigituse ja IKT-riski hindamise tulemustega.

Punkti b kohaldamisel võetakse nimetatud punktis osutatud turvalise konfigureerimise lähtealuse puhul arvesse juhtivaid tavasid ja määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standardites sätestatud asjakohaseid meetodeid.

Punkti k kohaldamisel võtavad finantssektori ettevõtjad arvesse järgmist:

a) teenuseosutaja soovitatud seadete rakendamine enda käitatavate elementide puhul;

b) infoturbe rollide ja vastutusvaldkondade selge jaotus finantssektori ettevõtja ja kolmandast isikust IKT-teenuste osutaja vahel kooskõlas määruse (EL) 2022/2554 artikli 28 lõike 1 punktis a sätestatud põhimõttega, mille kohaselt finantssektori ettevõtjal lasub täielik vastutus oma kolmandast isikust IKT-teenuste osutaja eest, ning selle määruse artikli 28 lõikes 2 osutatud finantssektori ettevõtjate puhul kooskõlas finantssektori ettevõtja kehtestatud kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamise põhimõtetega;

c) vajadus tagada ja säilitada finantssektori ettevõtja piisav pädevus kasutatava teenuse haldamiseks ja turvalisuse tagamiseks;

d) tehnilised ja korralduslikud meetmed, et minimeerida kolmandast isikust IKT-teenuste osutaja teenuste jaoks kasutatava taristuga seotud riske, võttes arvesse juhtivaid tavasid ja määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standardeid.

Artikkel 12

Logimine

1. Finantssektori ettevõtjad töötavad sissetungi ja andmete väärkasutamise vastaste kaitsemeetmete osana välja ja dokumenteerivad logimise menetlused, protokollid ja vahendid ning rakendavad neid.

2. Lõikes 1 osutatud menetlused, protokollid ja vahendid peavad hõlmama kõike järgmist:

a) logitavate sündmuste kindlaksmääramine, logide säilitamisaeg ning logiandmete turvalisuse tagamise ja käitlemise meetmed, võttes arvesse logide loomise otstarvet;

b) logide üksikasjalikkuse vastavusse viimine nende otstarbe ja kasutamisega, et võimaldada tõhusalt avastada anomaalne tegevus, nagu on ette nähtud artikliga 24;

c) nõue logida sündmused, mis on seotud kõige järgmisega:

   i) artiklis 21 osutatud loogilise ja füüsilise pääsu reguleerimine ning identiteedihaldus,

   ii) võimsuse haldamine,

   iii) muudatuste juhtimine,

   iv) IKT-toimingud, sealhulgas tegevus IKT-süsteemides,

   v) võrguliiklus, sealhulgas IKT-võrgu jõudlus;

d) meetmed, millega kaitstakse logimissüsteeme ja logiandmeid rikkumise, kustutamise ja loata juurdepääsu eest andmete jõudeoleku, edastamise ja vajaduse korral kasutamise ajal;

e) meetmed logimissüsteemide tõrgete avastamiseks;

f) ilma et see piiraks liidu või liikmesriigi õiguses sätestatud asjakohaste regulatiivsete nõuete kohaldamist, finantssektori ettevõtja kõigi IKT-süsteemide kellaaegade sünkroniseerimine, tuginedes dokumenteeritud usaldusväärsele võrdlusajale.

Punkti a kohaldamisel määravad finantssektori ettevõtjad kindlaks säilitamistähtaja, võttes arvesse äri- ja infoturbe eesmärke, sündmuse logis registreerimise põhjust ja IKT-riski hindamise tulemusi.

6. jagu

Võrgu turvalisus

Artikkel 13

Võrgu turvalisuse haldamine

Finantssektori ettevõtjad töötavad võrgu turvalisuse tagamiseks kehtestatavate sissetungi ja andmete väärkasutamise vastaste kaitsemeetmete osana välja ja dokumenteerivad võrgu turvalisuse haldamise põhimõtted, menetlused, protokollid ja vahendid, mis peavad hõlmama kõike järgmist:

a) IKT-süsteemide ja võrkude eraldamine ja segmentimine, võttes arvesse

   i) asjaomaste IKT-süsteemide ja võrkude toetatavate funktsioonide kriitilist tähtsust või olulisust,

   ii) määruse (EL) 2022/2554 artikli 8 lõike 1 kohast liigitust,

   iii) neid IKT-süsteeme ja võrke kasutavate IKT-varade üldist riskiprofiili;

b) finantssektori ettevõtja kõigi võrguühenduste ja andmevoogude dokumenteerimine;

c) eraldi ja spetsiaalse võrgu kasutamine IKT-varade haldamiseks;

d) võrkupääsu reguleerimise kindlaksmääramine ja rakendamine, et ära hoida ja avastada ühendused finantssektori ettevõtja võrguga pääsuloata seadme või süsteemi kaudu või mis tahes lõpp-punkti kaudu, mis ei vasta finantssektori ettevõtja turvanõuetele;

e) kasutatavate sideprotokollide jaoks sisevõrke, üldkasutatavaid võrke, riigisiseseid võrke, kolmandate isikute võrke ja traadita võrke läbivate võrguühenduste krüptimine, võttes arvesse heakskiidetud andmeliigituse ja IKT-riski hindamise tulemusi ning artikli 6 lõikes 2 osutatud võrguühenduste krüptimist;

f) võrgu projekteerimine kooskõlas finantssektori ettevõtja kehtestatud IKT turvanõuetega, võttes arvesse juhtivaid tavasid, et tagada võrgu konfidentsiaalsus, terviklus ja kättesaadavus;

g) sisevõrgu ning interneti ja muude välisühenduste vahelise võrguliikluse turvalisuse tagamine;

h) tulemüüri reeglite ja ühendusfiltrite kindlaksmääramiseks, rakendamiseks, heakskiitmiseks, muutmiseks ja läbivaatamiseks rollide ja vastutusvaldkondade ning etappide kindlaksmääramine;

i) võrguarhitektuuri ja võrgu sisseprojekteeritud turbe meetmete läbivaatamine kord aastas ning mikroettevõtjate puhul perioodiliselt, et teha kindlaks võimalikud nõrkused;

j) meetmed, et vajaduse korral ajutiselt isoleerida alamvõrgud ning võrgukomponendid ja -seadmed;

k) kõigi võrgukomponentide turvalise konfigureerimise lähtealuse rakendamine ning võrgu ja võrguseadmete tugevdamine kooskõlas teenuseosutaja juhistega, määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standarditega (kui see on asjakohane) ja juhtivate tavadega;

l) menetlused süsteemi- ja kaugseansside piiramiseks, lukustamiseks ja lõpetamiseks pärast kindlaksmääratud jõudeolekuperioodi möödumist;

m) võrguteenuste lepingute puhul

   i) IKT-turvameetmete ja infoturbe meetmete, teenustasemete ja juhtimisnõuete kindlaksmääramine ja täpsustamine kõigi võrguteenuste puhul,

   ii) teave selle kohta, kas neid teenuseid osutab kontsernisisene IKT-teenuste osutaja või osutavad neid kolmandast isikust IKT-teenuste osutajad.

Punkti h kohaldamisel vaatavad finantssektori ettevõtjad tulemüüri reeglid ja ühendusfiltrid korrapäraselt läbi, võttes arvesse määruse (EL) 2022/2554 artikli 8 lõike 1 kohast liigitust ja asjaomaste IKT-süsteemide üldist riskiprofiili. Kriitilise tähtsusega või olulisi funktsioone toetavate IKT-süsteemide puhul kontrollivad finantssektori ettevõtjad kehtivate tulemüüri reeglite ja ühendusfiltrite asjakohasust vähemalt iga kuue kuu tagant.

Artikkel 14

Edastatava teabe turve

1. Finantssektori ettevõtjad töötavad andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse säilitamiseks kehtestatavate kaitsemeetmete osana välja ja dokumenteerivad edastatava teabe kaitsmise põhimõtted, menetlused, protokollid ja vahendid ning rakendavad neid. Finantssektori ettevõtjad tagavad eelkõige kõik järgmise:

a) andmete kättesaadavus, autentsus, terviklus ja konfidentsiaalsus võrguedastuse ajal ning menetluste kehtestamine, et hinnata nende nõuete täitmist;

b) andmelekete ennetamine ja avastamine ning teabe turvaline edastamine finantssektori ettevõtja ja väliste isikute vahel;

c) nii finantssektori ettevõtja kui ka kolmandate isikute töötajatele ette nähtud finantssektori ettevõtja teabe kaitsmise vajadust kajastavate konfidentsiaalsusnõuete või mitteavalikustamise korra dokumenteerimine, rakendamine ja korrapärane läbivaatamine.

2. Finantssektori ettevõtjad võtavad lõikes 1 osutatud edastatava teabe kaitsmise põhimõtete, menetluste, protokollide ja vahendite kavandamisel aluseks heakskiidetud andmeliigituse ja IKT-riski hindamise tulemused.

7. jagu

IKT-projektide ja -muudatuste juhtimine

Artikkel 15

IKT-projektide juhtimine

1. Finantssektori ettevõtjad töötavad andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse säilitamiseks kehtestatavate kaitsemeetmete osana välja ja dokumenteerivad IKT-projektide juhtimise põhimõtted ning rakendavad neid.

2. Lõikes 1 osutatud põhimõtetes määratakse kindlaks elemendid, mis tagavad finantssektori ettevõtja IKT-süsteemide soetamise, hooldamise ja vajaduse korral arendamisega seotud IKT-projektide tõhusa juhtimise.

3. Lõikes 1 osutatud põhimõtted peavad hõlmama kõike järgmist:

a) IKT-projektide eesmärgid;

b) IKT-projektide juhtimine, sealhulgas rollid ja vastutusvaldkonnad;

c) IKT-projektide kavandamine, ajakava ja etapid;

d) IKT-projektide riskihindamine;

e) asjakohased vahe-eesmärgid;

f) muudatuste juhtimise nõuded;

g) kõigi nõuete, sealhulgas turvanõuete testimine ning vastav heakskiitmismenetlus, kui IKT-süsteem võetakse kasutusele tootmiskeskkonnas.

4. Lõikes 1 osutatud põhimõtetega tagatakse IKT-projektide turvaline rakendamine, hankides vajalikku oskus- ja muud teavet IKT-projektist mõjutatud ärivaldkonnast või funktsioonide täitjatelt.

5. Seoses lõike 3 punktis d osutatud IKT-projektide riskihindamisega nähakse lõikes 1 osutatud IKT-projektide juhtimise põhimõtetes ette, et finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone mõjutavate IKT-projektide käivitamisest ja edenemisest ning nendega seotud riskidest teatatakse juhtorganile

a) eraldi või koos, sõltuvalt IKT-projektide tähtsusest ja mahust;

b) korrapäraselt ja vajaduse korral sündmuspõhiselt.

Artikkel 16

IKT-süsteemide soetamine, arendamine ja hooldamine

1. Finantssektori ettevõtjad töötavad andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse säilitamiseks kehtestatavate kaitsemeetmete osana välja ja dokumenteerivad IKT-süsteemide soetamise, arendamise ja hooldamise põhimõtted ning rakendavad neid. Neis põhimõtetes

a) määratakse kindlaks IKT-süsteemide soetamise, arendamise ja hooldamisega seotud turbetavad ja metoodika;

b) sätestatakse kohustus määrata kindlaks

   i) määruse (EL) nr 1025/2012 artikli 2 punktides 4 ja 5 määratletud tehniline spetsifikatsioon ja IKT tehniline spetsifikatsioon,

   ii) IKT-süsteemide soetamise, arendamise ja hooldamisega seotud nõuded, pöörates erilist tähelepanu IKT turvanõuetele ja nende heakskiitmisele asjaomase ärifunktsiooni täitja ja IKT-vara omaniku poolt kooskõlas finantssektori ettevõtja sisemise juhtimiskorraga;

c) määratakse kindlaks meetmed eesmärgiga maandada riski, et IKT-süsteeme nende arendamise või hooldamise või tootmiskeskkonnas kasutuselevõtu ajal tahtmatult muudetakse või et nendega sel ajal tahtlikult manipuleeritakse.

2. Finantssektori ettevõtjad töötavad välja, dokumenteerivad ja rakendavad IKT-süsteemide soetamise, arendamise ja hooldamise menetlused, et testida artikli 8 lõike 2 punkti b alapunktide v, vi ja vii kohaselt kõiki IKT-süsteeme ja need heaks kiita enne nende kasutamist ja pärast nende hooldamist. Testimise tase peab olema vastavuses asjaomaste äriprotsesside ja IKT-varade kriitilise tähtsusega. Testimine tuleb kavandada nii, et selle käigus tehakse kindlaks, kas uued IKT-süsteemid on ettenähtud viisil kasutamiseks piisavad, ja kontrollitakse ettevõttes arendatud tarkvara kvaliteeti.

Lisaks esimeses lõigus sätestatud nõuete täitmisele kaasavad kesksed vastaspooled vajaduse korral esimeses lõigus osutatud testimise kavandamisse ja elluviimisesse

a) kliirivaid liikmeid ja kliente;

b) koostalitlusvõimelisi keskseid vastaspooli;

c) teisi huvitatud isikuid.

Lisaks esimeses lõigus sätestatud nõuete täitmisele kaasavad väärtpaberite keskdepositooriumid vajaduse korral esimeses lõigus osutatud testimise kavandamisse ja elluviimisesse

a) kasutajaid;

b) kriitilise tähtsusega teenuste osutajaid;

c) muid väärtpaberite keskdepositooriume;

d) muid turutaristuid;

e) mis tahes muid asutusi, kellega väärtpaberite keskdepositooriumil on talitluspidevuse põhimõtete kohaselt kindlaks tehtud vastastikune sõltuvus.

3. Lõikes 2 osutatud menetlus peab sisaldama lähtekoodi ülevaatust, mis hõlmab nii staatilist kui ka dünaamilist testimist. Testitakse internetile avatud süsteemide ja rakenduste turvalisust kooskõlas artikli 8 lõike 2 punkti b alapunktidega v, vi ja vii. Finantssektori ettevõtjad

a) teevad kindlaks lähtekoodi nõrkused ja anomaaliad ning analüüsivad neid;

b) võtavad vastu tegevuskava nõrkuste ja anomaaliate kõrvaldamiseks;

c) seiravad selle tegevuskava rakendamist.

4. Lõikes 2 osutatud menetlus peab hõlmama tarkvarapakettide turvalisuse testimist hiljemalt integreerimisetapis kooskõlas artikli 8 lõike 2 punkti b alapunktidega v, vi ja vii.

5. Lõikes 2 osutatud menetlusega tagatakse, et

a) tootmisega mitteseotud keskkondades säilitatakse üksnes anonüümitud, pseudonüümitud või randomeeritud tootmisandmeid;

b) finantssektori ettevõtjad kaitsevad tootmisega mitteseotud keskkondades andmete terviklust ja konfidentsiaalsust.

6. Erandina lõikest 5 võib lõikes 2 osutatud menetlusega ette näha, et tootmisandmeid säilitatakse ainult konkreetse testimise jaoks, piiratud aja jooksul ja pärast asjaomase funktsiooni täitjalt heakskiidu saamist ning et IKT-riski juhtimise funktsiooni täitjat teavitatakse sellistest juhtumitest.

7. Lõikes 2 osutatud menetlus peab hõlmama kontrolle, et kaitsta finantssektori ettevõtja välja töötatud IKT-süsteemide või kolmandast isikust IKT-teenuste osutaja välja töötatud ja finantssektori ettevõtjale edastatud IKT-süsteemide lähtekoodi terviklust.

8. Lõikes 2 osutatud menetlusega nähakse ette, et omandiõigusega kaitstud tarkvara ja, kui see on teostatav, kolmandast isikust IKT-teenuste osutajate esitatud või avatud lähtekoodiga projektidest saadud lähtekoodi analüüsitakse ja testitakse kooskõlas lõikega 3 enne kasutuselevõttu tootmiskeskkonnas.

9. Käesoleva artikli lõikeid 1–8 kohaldatakse ka selliste IKT-süsteemide suhtes, mille on välja töötanud või mida haldavad riskipõhist lähenemisviisi järgides kasutajad, kes ei ole IKT-funktsiooni täitjad.

Artikkel 17

IKT-muudatuste juhtimine

1. Finantssektori ettevõtjad lisavad andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse säilitamiseks kehtestatavate kaitsemeetmete osana IKT-muudatuste juhtimisse määruse (EL) 2022/2554 artikli 9 lõike 4 punktis e osutatud menetlused kõigi tarkvaras, riistvaras, püsivara komponentides, süsteemides või turvaparameetrites tehtavate muudatuste jaoks kõik järgmise:

a) IKT turvanõuete täitmise kontrollimine;

b) mehhanismid, millega tagatakse muudatuste heakskiitjate ning nende muudatuste taotlejate ja rakendajate sõltumatus;

c) rollide ja vastutusvaldkondade selge kirjeldus, kandmaks hoolt selle eest, et

   i) muudatused määratakse täpselt kindlaks ja kavandatakse,

   ii) kavandatakse asjakohane üleminek,

   iii) muudatusi testitakse ja viimistletakse kontrollitud viisil;

   iv) toimub tõhus kvaliteedi tagamine;

d) muudatuse üksikasjade dokumenteerimine ja edastamine, mis hõlmab

   i) muudatuse eesmärki ja ulatust,

   ii) muudatuse rakendamise ajakava,

   iii) oodatavaid tulemusi;

e) varumenetlused ja vastutusvaldkonnad, sealhulgas menetlused ja vastutusvaldkonnad muudatuse tegemisest loobumise puhuks või taastumiseks muudatustest, mille rakendamine ebaõnnestus;

f) hädaolukorras tehtavate muudatuste haldamise menetlused, protokollid ja vahendid, millega tagatakse piisavad kaitsemeetmed;

g) menetlused hädaolukorras tehtavate muudatuste dokumenteerimiseks, ümberhindamiseks, hindamiseks ja heakskiitmiseks pärast nende rakendamist, sealhulgas hädalahendused ja paigad;

h) muudatusest olemasolevatele IKT-turvameetmetele tuleneva võimaliku mõju kindlakstegemine ning muudatuse tõttu täiendavate IKT-turvameetmete võtmise vajaduse hindamine.

2. Kesksed vastaspooled ja väärtpaberite keskdepositooriumid testivad pärast seda, kui nad on teinud oma IKT-süsteemidesse olulisi muudatusi, oma IKT-süsteeme rangelt, simuleerides stressiolukorda.

Kesksed vastaspooled kaasavad vajaduse korral esimeses lõigus osutatud testimise kavandamisse ja elluviimisesse

a) kliirivaid liikmeid ja kliente;

b) koostalitlusvõimelisi keskseid vastaspooli;

c) teisi huvitatud isikuid.

Väärtpaberite keskdepositooriumid kaasavad vajaduse korral esimeses lõigus osutatud testimise kavandamisse ja elluviimisesse

a) kasutajaid;

b) kriitilise tähtsusega teenuste osutajaid;

c) muid väärtpaberite keskdepositooriume;

d) muid turutaristuid;

e) mis tahes muid asutusi, kellega väärtpaberite keskdepositooriumil on IKT talitluspidevuse põhimõtete kohaselt kindlaks tehtud vastastikune sõltuvus.

8. jagu

Artikkel 18

Füüsiline ja keskkonnaturve

1. Finantssektori ettevõtjad määravad andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse säilitamiseks kehtestatavate kaitsemeetmete osana kindlaks ja dokumenteerivad füüsilise ja keskkonnaturbe põhimõtted ning rakendavad neid. Finantssektori ettevõtjad võtavad nende põhimõtete väljatöötamisel arvesse küberohtude maastikku, määruse (EL) 2022/2554 artikli 8 lõike 1 kohast liigitust, IKT-varade üldist riskiprofiili ja juurdepääsetavaid teabevarasid.

2. Lõikes 1 osutatud füüsilise ja keskkonnaturbe põhimõtted peavad hõlmama kõike järgmist:

a) viide sellele põhimõtete osale, kus käsitletakse artikli 21 esimese lõigu punktis g osutatud pääsuhalduse õiguste reguleerimist;

b) meetmed, millega kaitstakse finantssektori ettevõtja ruume ja andmekeskusi ning finantssektori ettevõtja kindlaks määratud tundlikke alasid, kus asuvad IKT- ja teabevarad, rünnete, õnnetuste ning keskkonnaohtude eest;

c) meetmed, millega tagatakse IKT-varade turvalisus nii finantssektori ettevõtja ruumides kui ka neist väljaspool, võttes arvesse asjaomaste IKT-varadega seotud IKT-riski hindamise tulemusi;

d) meetmed, millega tagatakse asjakohase hoolduse kaudu finantssektori ettevõtja IKT-varade ja teabevarade ning samuti füüsilise pääsu reguleerimise seadmete kättesaadavus, autentsus, terviklus ja konfidentsiaalsus;

e) meetmed, millega säilitatakse andmete kättesaadavus, autentsus, terviklus ja konfidentsiaalsus, sealhulgas

   i) puhta-laua-põhimõte,

   ii) tühja-ekraani-põhimõte teabetöötlusseadmete jaoks.

Punkti b kohaldamisel peavad meetmed, mille eesmärk on kaitsta keskkonnaohtude eest, olema vastavuses ruumide, andmekeskuste ja kindlaksmääratud tundlike alade ning seal tehtavate toimingute või asuvate IKT-süsteemide kriitilise tähtsusega.

Punkti c kohaldamisel peavad lõikes 1 osutatud füüsilise ja keskkonnaturbe põhimõtted hõlmama meetmeid, millega tagatakse järelevalveta jäetud IKT-varade asjakohane kaitse.

II PEATÜKK

Personalipoliitika ja pääsu reguleerimine

Artikkel 19

Personalipoliitika

Finantssektori ettevõtjad lisavad oma personalipoliitikasse või muudesse asjakohastesse põhimõtetesse kõik järgmised IKT turvalisusega seotud elemendid:

a) IKT turvalisusega seotud vastutusvaldkondade kindlaksmääramine ja nende eest vastutajate määramine;

b) nõuded, et finantssektori ettevõtja töötajad ja kolmandast isikust IKT-teenuste osutaja töötajad, kes kasutavad finantssektori ettevõtja IKT-varasid või kellel on nendele varadele juurdepääs, peavad

   i) olema kursis finantssektori ettevõtja IKT turvalisuse põhimõtete, menetluste ja protokollidega ning neid järgima,

   ii) olema teadlikud teavituskanalitest, mille finantssektori ettevõtja on loonud anomaalse käitumise avastamiseks, sealhulgas asjakohasel juhul teavituskanalitest, mis on loodud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/1937 ([11]) kohaselt,

   iii) tagastama töösuhte lõppemisel finantssektori ettevõtjale kõik enda valduses olevad IKT-varad ja materiaalsed teabevarad, mis kuuluvad finantssektori ettevõtjale.

Artikkel 20

Identiteedihaldus

1. Finantssektori ettevõtjad töötavad pääsuhalduse õiguste reguleerimise osana välja ja dokumenteerivad identiteedihalduse põhimõtted ja menetlused, millega tagatakse finantssektori ettevõtja teabele ligi pääsevate füüsiliste isikute ja süsteemide kordumatu identifitseerimine ja autentimine, et oleks võimalik anda kasutaja pääsuõigusi kooskõlas artikliga 21, ning rakendavad neid põhimõtteid ja menetlusi.

2. Lõikes 1 osutatud põhimõtted ja menetlused peavad hõlmama kõike järgmist:

a) ilma et see piiraks artikli 21 esimese lõigu punkti c kohaldamist, kordumatule kasutajakontole vastava kordumatu identiteedi määramine igale finantssektori ettevõtja või kolmandast isikust IKT-teenuste osutaja töötajale, kellel on juurdepääs finantssektori ettevõtja teabevaradele ja IKT-varadele;

b) identiteetide ja kontode olelusringi haldamise protsess, mis hõlmab kõigi kontode loomist, muutmist, läbivaatamist ja ajakohastamist, ajutist deaktiveerimist ja lõplikku sulgemist.

Punkti a kohaldamisel säilitavad finantssektori ettevõtjad andmed kõigi identiteetide määramiste kohta. Need andmed hoitakse alles ka pärast finantssektori ettevõtja ümberkorraldamist või lepingulise suhte lõppemist, ilma et see piiraks kohaldatavas liidu ja siseriiklikus õiguses sätestatud säilitamisnõuete kohaldamist.

Punkti b kohaldamisel võtavad finantssektori ettevõtjad identiteetide olelusringi haldamise protsessi jaoks kasutusele automatiseeritud lahendused, kui see on teostatav ja asjakohane.

Artikkel 21

Pääsu reguleerimine

Finantssektori ettevõtjad töötavad pääsuhalduse õiguste reguleerimise osana välja ja dokumenteerivad põhimõtted, mis peavad hõlmama kõike järgmist, ning rakendavad neid:

a) IKT-varadele juurdepääsu õiguste, sealhulgas kaugpääsu ja hädaolukorras pääsu õiguse andmine, lähtudes teadmisvajadusest, kasutusvajadusest ja minimaalõiguste printsiibist;

b) ülesannete lahusus, et ära hoida põhjendamatu juurdepääs kriitilise tähtsusega andmetele või sellise pääsuõiguste kombinatsiooni tekkimine, mida võidakse kasutada kontrollist kõrvalehoidmiseks;

c) säte kasutaja vastutuse kohta, millega piiratakse nii palju kui võimalik üldkontode ja jagatud kasutajakontode kasutamist ning tagatakse, et kasutajad on IKT-süsteemides tehtavate toimingute puhul alati tuvastatavad;

([11]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2019. aasta direktiiv (EL) 2019/1937 liidu õiguse rikkumisest teavitavate isikute kaitse kohta (ELT L 305, 26.11.2019, lk 17, ELI: https://eur-lex.europa.eu/eli/dir/2019/1937/oj?locale=et).

d) säte IKT-varadele juurdepääsu piiramise kohta, millega nähakse ette kontrollid ja vahendid loata juurdepääsu ärahoidmiseks;

e) kontohaldusmenetlused kasutaja- ja üldkontode, kaasa arvatud üldiste administraatorikontode pääsuõiguste andmiseks, muutmiseks või tühistamiseks, sealhulgas sätted kõige järgmise kohta:

   i) rollide ja vastutusvaldkondade määramine pääsuõiguste andmiseks, läbivaatamiseks ja tühistamiseks,

   ii) kõikidele IKT-süsteemidele eelis-, hädaolukorras või administraatori pääsu andmine kasutusvajaduse korral või vajaduspõhiselt,

   iii) pääsuõiguste tühistamine põhjendamatu viivituseta, kui töösuhe lõpeb või kui pääs ei ole enam vajalik,

   iv) pääsuõiguste ajakohastamine, kui on vaja teha muudatusi, ning kriitilise tähtsusega või olulisi funktsioone toetavate IKT-süsteemide puhul vähemalt kord kuue kuu jooksul ning kõigi muude IKT-süsteemide puhul vähemalt kord aastas;

f) autentimismeetodid, sealhulgas kõik järgmine:

   i) autentimismeetodite kasutamine viisil, mis on vastavuses määruse (EL) 2022/2554 artikli 8 lõike 1 kohase liigitusega ja IKT-varade üldise riskiprofiiliga, ning võttes arvesse juhtivaid tavasid,

   ii) tugevate autentimismeetodite kasutamine finantssektori ettevõtja võrgule kaugpääsu, eelispääsu, kriitilise tähtsusega või olulisi funktsioone toetavatele IKT-varadele juurdepääsu või üldsusele kättesaadavatele IKT-varadele juurdepääsu andmisel kooskõlas juhtivate tavade ja meetoditega;

g) füüsilise pääsu reguleerimise meetmed, sealhulgas

   i) selliste füüsiliste isikute identifitseerimine ja nende toimingute logimine, kellel on õigus siseneda finantssektori ettevõtja ruumidesse ja andmekeskustesse ning finantssektori ettevõtja kindlaks määratud tundlikele aladele, kus asuvad IKT- ja teabevarad,

   ii) kriitilise tähtsusega IKT-varade puhul füüsilise pääsu õiguse andmine üksnes volitatud isikutele kooskõlas teadmisvajaduse ja minimaalõiguste printsiibiga ning vajaduspõhiselt,

   iii) finantssektori ettevõtja ruumidesse ja andmekeskustesse ning finantssektori ettevõtja kindlaks määratud tundlikele aladele, kus asuvad IKT- ja teabevarad, füüsilise pääsu seire,

   iv) füüsilise pääsu õiguste läbivaatamine, et tagada tarbetute pääsuõiguste viivitamatu tühistamine.

Punkti e alapunkti i kohaldamisel määravad finantssektori ettevõtjad kindlaks säilitamistähtaja, võttes arvesse äri- ja infoturbe eesmärke, sündmuse logis registreerimise põhjust ja IKT-riski hindamise tulemusi.

Punkti e alapunkti ii kohaldamisel kasutavad finantssektori ettevõtjad IKT-süsteemidega seotud haldusülesannete täitmiseks võimaluse korral spetsiaalseid kontosid. Kui see on teostatav ja asjakohane, võtavad finantssektori ettevõtjad eelispääsu haldamiseks kasutusele automatiseeritud lahendused.

Punkti g alapunkti i kohaldamisel peavad identifitseerimine ja logimine olema vastavuses ruumide, andmekeskuste ja kindlaksmääratud tundlike alade ning seal tehtavate toimingute või asuvate IKT-süsteemide kriitilise tähtsusega.

Punkti g alapunkti iii kohaldamisel peab seire olema vastavuses määruse (EL) 2022/2554 artikli 8 lõike 1 kohase liigitusega ja juurdepääsetava ala kriitilise tähtsusega.

III PEATÜKK

IKT intsidentide avastamine ja neile reageerimine

Artikkel 22

IKT intsidentide haldamise põhimõtted

Finantssektori ettevõtjad töötavad anomaalse tegevuse, sealhulgas IKT-võrgu jõudluse probleemide ja IKT intsidentide avastamise mehhanismide osana välja ja dokumenteerivad IKT intsidentide haldamise põhimõtted ning rakendavad neid ning teevad nende kohaselt järgmist:

a) dokumenteerivad määruse (EL) 2022/2554 artiklis 17 osutatud IKT intsidentide haldamise protsessi;

b) koostavad loetelu asjakohaste sisefunktsioonide täitjatest ja väliste sidusrühmade esindajatest, kes on otseselt seotud IKT-toimingute turvalisusega, sealhulgas järgmisega:

   i) küberohtude avastamine ja seire,

   ii) anomaalse tegevuse avastamine,

   iii) nõrkusehaldus;

c) loovad, võtavad kasutusele ja käitavad IKT intsidentide haldamise protsessi toetavaid tehnilisi, korralduslikke ja tegevusmehhanisme, sealhulgas mehhanisme, mis võimaldavad kiiresti avastada anomaalse tegevuse ja käitumise kooskõlas käesoleva määruse artikliga 23;

d) kooskõlas komisjoni delegeeritud määruse (EL) 2024/1772 ([12]) artikliga 15 ja liidu õiguses sätestatud kohaldatavate säilitamisnõuetega säilitavad kõik IKT intsidentidega seotud tõendid, mis on vastavuses mõjutatud ärifunktsioonide, toetavate protsesside ning IKT- ja teabevarade kriitilise tähtsusega, ajavahemiku jooksul, mis ei ole pikem kui on vajalik andmete kogumise eesmärgi saavutamiseks;

e) loovad mehhanismid, et analüüsida olulisi või korduvaid IKT intsidente ning nende intsidentide arvu ja esinemisega seotud suundumusi, ning rakendavad neid mehhanisme.

Punkti d kohaldamisel säilitavad finantssektori ettevõtjad nimetatud punktis osutatud tõendeid turvalisel viisil.

Artikkel 23

Anomaalse tegevuse avastamine ning IKT intsidentide avastamise ja neile reageerimise kriteeriumid

1. Finantssektori ettevõtjad määravad kindlaks selged rollid ja vastutusvaldkonnad, et tõhusalt avastada IKT intsidente ja anomaalset tegevust ning neile tõhusalt reageerida.

2. Määruse (EL) 2022/2554 artikli 10 lõikes 1 osutatud mehhanism, mis võimaldab kohe avastada anomaalse tegevuse, sealhulgas IKT-võrgu jõudluse probleemid ja IKT intsidendid, peab andma finantssektori ettevõtjatele võimaluse

a) koguda, seirata ja analüüsida kõike järgmist:

   i) sisemised ja välised tegurid, sealhulgas vähemalt käesoleva määruse artikli 12 kohaselt kogutud logid, teave äri- ja IKT-funktsioonide täitjatelt ning finantssektori ettevõtja kasutajate teatatud probleemid,

   ii) võimalikud sisemised ja välised küberohud, võttes arvesse stsenaariume, mille kasutamine on levinud ohusubjektide seas, ja stsenaariume, mis põhinevad ohuteadmusel,

([12]) Komisjoni 13. märtsi 2024. aasta delegeeritud määrus (EL) 2024/1772, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 regulatiivsete tehniliste standarditega, millega määratakse kindlaks IKT intsidentide ja küberohtude liigitamise kriteeriumid, kehtestatakse olulisuse läved ja täpsustatakse tõsiste intsidentide kohta esitatavate raportite üksikasju (ELT L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) finantssektori ettevõtja kolmandast isikust IKT-teenuste osutaja teatatud IKT intsidendid, mis on avastatud asjaomase teenuseosutaja IKT-süsteemides ja -võrkudes ning mis võivad mõjutada finantssektori ettevõtjat;

b) teha kindlaks anomaalne tegevus ja käitumine ning rakendada vahendeid, mis annavad sellise tegevuse ja käitumise kohta hoiatusi, vähemalt kriitilise tähtsusega või olulisi funktsioone toetavate IKT-varade ja teabevarade puhul;

c) seada punktis b osutatud hoiatusteated esmatähtsaks, et avastatud IKT intsidendi puhul oleks võimalik leida lahendus finantssektori ettevõtja kindlaks määratud eeldatava lahendusaja jooksul nii tööajal kui ka väljaspool tööaega;

d) automaatselt või käsitsi registreerida, analüüsida ja hinnata asjakohast teavet kogu anomaalse tegevuse ja käitumise kohta.

Punkti b kohaldamisel peavad nimetatud punktis osutatud vahendite hulka kuuluma vahendid, mis annavad eelnevalt kindlaks määratud reeglite alusel automaatseid hoiatusteateid, mis võimaldab kindlaks teha anomaalia, mis mõjutab andmeallikate täielikkust ja terviklust või logide kogumist.

3. Finantssektori ettevõtjad kaitsevad anomaalse tegevuse registreerimise andmeid rikkumise ja loata juurdepääsu eest andmete jõudeoleku, edastamise ja vajaduse korral kasutamise ajal.

4. Finantssektori ettevõtjad registreerivad iga avastatud anomaalse tegevuse kohta kogu asjakohase teabe, mis võimaldab kindlaks teha

a) anomaalse tegevuse toimumise kuupäeva ja kellaaja;

b) anomaalse tegevuse avastamise kuupäeva ja kellaaja;

c) anomaalse tegevuse laadi.

5. Finantssektori ettevõtjad võtavad määruse (EL) 2022/2554 artikli 10 lõikes 2 osutatud IKT intsidendi tuvastamise ja sellele reageerimise protsessi käivitamisel arvesse kõike järgmist:

a) märgid sellest, et IKT-süsteemis või -võrgus võib olla toimunud pahatahtlik tegevus või et IKT-süsteem või -võrk võib olla ohtu seatud;

b) avastatud andmekaod, mis mõjutavad andmete kättesaadavust, autentsust, terviklust ja konfidentsiaalsust;

c) avastatud kahjulik mõju finantssektori ettevõtja tehingutele ja tegevusele;

d) IKT-süsteemid ja -võrk ei ole enam kättesaadavad.

6. Lõike 5 kohaldamisel võtavad finantssektori ettevõtjad arvesse ka mõjutatud teenuste kriitilist tähtsust.

IV PEATÜKK

IKT talitluspidevuse juhtimine

Artikkel 24

IKT talitluspidevuse põhimõtted

1. Finantssektori ettevõtjad lisavad määruse (EL) 2022/2554 artikli 11 lõikes 1 osutatud IKT talitluspidevuse põhimõtetesse kõik järgmise:

a) kirjeldus järgmise kohta:

i) IKT talitluspidevuse põhimõtete eesmärgid, sealhulgas IKT talitluspidevuse ja üldise talitluspidevuse vahelised seosed, võttes arvesse määruse (EL) 2022/2554 artikli 11 lõikes 5 osutatud talitlusmõju analüüsi tulemusi;

ii) IKT talitluspidevuse korra, kavade, menetluste ja mehhanismide ulatus, sealhulgas piirangud ja erandid;

iii) IKT talitluspidevuse korra, kavade, menetluste ja mehhanismide rakendamise tähtajad;

iv) IKT talitluspidevuse kavade, IKT reageerimis- ja taastekavade ning kriisikommunikatsioonikavade aktiveerimise ja deaktiveerimise tingimused;

b) sätted järgmise kohta:

i) IKT talitluspidevuse põhimõtete rakendamise juhtimine ja korraldus, sealhulgas rollid, vastutusvaldkonnad ja eskalatsioonimenetlused, millega tagatakse piisavate vahendite olemasolu;

ii) IKT talitluspidevuse kavade ja üldiste talitluspidevuse kavade kooskõla, sealhulgas vähemalt kogu järgmine teave:

1) võimalikud tõrkestsenaariumid, sealhulgas käesoleva määruse artikli 26 lõikes 2 osutatud stsenaariumid,

2) taaste-eesmärgid, mille kohaselt finantssektori ettevõtja peab olema suuteline taastama pärast talitlushäiret oma kriitilise tähtsusega või olulised funktsioonid kooskõlas taasteaja ja taastekünnise eesmärgiga;

iii) nende kavade osana IKT talitluspidevuse kavade väljatöötamine tõsiste talitlushäirete puhuks ning IKT talitluspidevuse meetmete esmatähtsaks seadmine, kasutades riskipõhist lähenemisviisi;

iv) IKT reageerimis- ja taastekavade väljatöötamine, testimine ja läbivaatamine kooskõlas käesoleva määruse artiklitega 25 ja 26;

v) rakendatava IKT talitluspidevuse korra, kavade, menetluste ja mehhanismide tulemuslikkuse läbivaatamine kooskõlas käesoleva määruse artikliga 26;

vi) IKT talitluspidevuse põhimõtete kooskõlastamine

1) määruse (EL) 2022/2554 artikli 14 lõikes 2 osutatud kommunikatsioonipoliitikaga,

2) määruse (EL) 2022/2554 artikli 11 lõike 2 punktis e osutatud kommunikatsiooni- ja kriisijuhtimismeetmetega.

2. Kesksed vastaspooled tagavad lisaks lõikes 1 osutatud nõuete täitmisele, et nende IKT talitluspidevuse põhimõtetes

a) kehtestatakse kriitilise tähtsusega funktsioonide maksimaalseks taasteajaks kuni kaks tundi;

b) võetakse arvesse väliseid seoseid ja vastastikust sõltuvust finantstaristutes, sealhulgas keskse vastaspoole kliiritavates kauplemiskohtades, väärtpaberiarveldus- ja maksesüsteemides ning keskse vastaspoole või seotud keskse vastaspoole kasutatavates krediidiasutustes;

c) esitatakse järgmised nõuded:

i) kehtestada avariistsenaariumidel põhinev kord, et tagada keskse vastaspoole kriitilise tähtsusega või oluliste funktsioonide talitluspidevus,

ii) omada varutöötluskohta, et tagada keskse vastaspoole kriitilise tähtsusega või oluliste funktsioonide edasitoimimine samal viisil kui peamises töötluskohas,

iii) omada kohest juurdepääsu varutöötluskohale, et töötajad saaksid tagada teenuste jätkumise, kui ligipääs peamisele tegevuskohale puudub,

iv) kaaluda täiendavate töötluskohtade vajadust, eelkõige juhul, kui peamise ja varutöötluskoha riskiprofiil ei erine nii palju, et oleks piisavalt kindel, et keskse vastaspoole talitluspidevuse eesmärgid täidetakse kõigi stsenaariumide korral.

Punkti a kohaldamisel teevad kesksed vastaspooled päevalõpu protseduurid ja maksed igas olukorras ettenähtud ajal ja päeval.

Punkti c alapunkti i kohaldamisel nähakse nimetatud punktis osutatud korraga ette piisavate inimressursside kättesaadavus, kriitilise tähtsusega funktsioonide maksimaalne seisuaeg ning varutöötluskohale üleminek ja taaste.

Punkti c alapunkti ii kohaldamisel peab nimetatud punktis osutatud varutöötluskoha geograafiline riskiprofiil erinema peamise töötluskoha riskiprofiilist.

3. Väärtpaberite keskdepositooriumid tagavad lisaks lõikes 1 osutatud nõuete täitmisele, et nende IKT talitluspidevuse põhimõtetes

a) võetakse arvesse mis tahes seoseid ja vastastikust sõltuvust kasutajate, kriitilise tähtsusega teenuste osutajate, teiste väärtpaberite keskdepositooriumide ja muude turutaristutega;

b) nähakse ette, et IKT talitluspidevuse kord peab tagama, et kriitilise tähtsusega või oluliste funktsioonide taasteaja eesmärk ei ületa kaht tundi.

4. Kauplemiskohad tagavad lisaks lõikes 1 osutatud nõuete täitmisele oma IKT talitluspidevuse põhimõtetega, et

a) kauplemist saab jätkata kahe tunni või peaaegu kahe tunni jooksul pärast häirivat intsidenti;

b) suurim andmehulk, mis võib kauplemiskoha IT-teenuse kaudu häire korral kaduma minna, on nullilähedane.

Artikkel 25

IKT talitluspidevuse kavade testimine

1. IKT talitluspidevuse kavade testimisel vastavalt määruse (EL) 2022/2554 artikli 11 lõikele 6 võtavad finantssektori ettevõtjad arvesse oma talitlusmõju analüüsi ja käesoleva määruse artikli 3 lõike 1 punktis b osutatud IKT-riski hindamist.

2. Finantssektori ettevõtjad hindavad lõikes 1 osutatud testimise teel, kas nad suudavad tagada oma kriitilise tähtsusega või oluliste funktsioonide talitluspidevuse. Kõnealune testimine

a) peab põhinema testimisstsenaariumidel, kus simuleeritakse võimalikke häireid, sealhulgas piisaval hulgal tõsistel, kuid usutavatel stsenaariumidel;

b) peab hõlmama vajaduse korral kolmandast isikust teenuseosutajate IKT-teenuste testimist;

c) peab hõlmama finantssektori ettevõtjate puhul, kes ei ole mikroettevõtjad, esmase IKT-taristu ning varuvõimsuse, varundusseadmete ja varurajatiste vahelise ümberlülituse stsenaariume, nagu on osutatud määruse (EL) 2022/2554 artikli 11 lõike 6 teises lõigus;

d) kavandatakse eesmärgiga seada kahtluse alla talitluspidevuse kavade aluseks olevad eeldused, sealhulgas juhtimiskord ja kriisikommunikatsioonikavad;

e) peab hõlmama menetlusi, millega kontrollida finantssektori ettevõtja töötajate, kolmandast isikust IKT-teenuste osutajate, IKT-süsteemide ja IKT-teenuste suutlikkust asjakohaselt reageerida artikli 26 lõike 2 kohaselt arvesse võetud stsenaariumidele.

Punkti a kohaldamisel testivad finantssektori ettevõtjad alati stsenaariume, mida võeti arvesse talitluspidevuse kavade väljatöötamisel.

Punkti b kohaldamisel võtavad finantssektori ettevõtjad nõuetekohaselt arvesse stsenaariume, mis on seotud kolmandast isikust IKT-teenuste osutajate maksejõuetuse või muude tõrgetega või poliitiliste riskidega kolmandast isikust IKT-teenuste osutajate jurisdiktsioonides, kui see on asjakohane.

Punkti c kohaldamisel kontrollitakse testimise käigus, kas vähemalt kriitilise tähtsusega või olulised funktsioonid toimivad nõuetekohaselt piisava aja jooksul ning kas on võimalik taastada tavapärane toimimine.

3. Lisaks lõikes 2 osutatud nõuete täitmisele kaasavad kesksed vastaspooled lõikes 1 osutatud IKT talitluspidevuse kavade testimisse

a) kliirivaid liikmeid;

b) väliseid teenuseosutajaid;

c) finantstaristu asjaomaseid asutusi, kellega kesksetel vastaspooltel on talitluspidevuse põhimõtete kohaselt kindlaks tehtud vastastikune sõltuvus.

4. Lisaks lõikes 2 osutatud nõuete täitmisele kaasavad väärtpaberite keskdepositooriumid vajaduse korral lõikes 1 osutatud IKT talitluspidevuse kavade testimisse

a) väärtpaberite keskdepositooriumide kasutajaid;

b) kriitilise tähtsusega teenuste osutajaid;

c) muid väärtpaberite keskdepositooriume;

d) muid turutaristuid;

e) mis tahes muid asutusi, kellega väärtpaberite keskdepositooriumil on talitluspidevuse põhimõtete kohaselt kindlaks tehtud vastastikune sõltuvus.

5. Finantssektori ettevõtjad dokumenteerivad lõikes 1 osutatud testimise tulemused. Testimise käigus tuvastatud puudusi analüüsitakse, need kõrvaldatakse ja neist teatatakse juhtorganile.

Artikkel 26

IKT reageerimis- ja taastekavad

1. Määruse (EL) 2022/2554 artikli 11 lõikes 3 osutatud IKT reageerimis- ja taastekavade väljatöötamisel võtavad finantssektori ettevõtjad arvesse oma talitlusmõju analüüsi tulemusi. IKT reageerimis- ja taastekavade suhtes kehtivad järgmised nõuded:

a) kavades tuleb kindlaks määrata tingimused, mille korral kava aktiveeritakse või deaktiveeritakse, ning neist tehtavad erandid;

b) kavades tuleb kirjeldada, milliseid meetmeid peab võtma, et tagada vähemalt finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone toetavate IKT-süsteemide ja -teenuste kättesaadavus, terviklus, järjekestvus ja taastamine;

c) kavad tuleb koostada eesmärgiga saavutada finantssektori ettevõtja taaste-eesmärgid;

d) kavad tuleb dokumenteerida ning teha kättesaadavaks IKT reageerimis- ja taastekavade elluviimises osalevatele töötajatele ning kavad peavad olema hädaolukorras kergesti kättesaadavad;

e) kavades tuleb ette näha nii lühi- kui ka pikaajalised taastevõimalused, sealhulgas süsteemide osaline taastamine;

f) kavades tuleb kindlaks määrata kava eesmärgid ning kava elluviimise õnnestunuks tunnistamise tingimused.

Punkti d kohaldamisel määravad finantssektori ettevõtjad selgelt kindlaks rollid ja vastutusvaldkonnad.

2. Lõikes 1 osutatud IKT reageerimis- ja taastekavades määratakse kindlaks asjakohased stsenaariumid, sealhulgas tõsiste talitlushäirete stsenaariumid ja häirete esinemise tõenäosuse suurenemise stsenaariumid. Neis kavades esitatavate stsenaariumide väljatöötamisel võetakse aluseks olemasolev teave ohtude kohta ja varasemate talitlushäiretega seotud kogemused. Finantssektori ettevõtjad võtavad nõuetekohaselt arvesse kõike järgmist:

a) küberründed ning esmase IKT-taristu ja varuvõimsuse, varundusseadmete ja varurajatiste vahelised ümberlülitused;

b) stsenaariumid, kus kriitilise tähtsusega või olulise funktsiooni täitmise kvaliteet halveneb vastuvõetamatu tasemeni või viib ebaõnnestumiseni, arvestades hoolikalt asjaomaste kolmandast isikust IKT-teenuste osutajate maksejõuetuse või muude tõrgete võimalikku mõju;

c) ruumide, sealhulgas kontori- ja äriruumide ning andmekeskuste osaline või täielik kasutuskõlbmatuks muutumine;

d) IKT-varade või sidetaristu märkimisväärne rike;

e) kriitilise arvu töötajate või talitluspidevuse tagamise eest vastutavate töötajate puudumine;

f) kliimamuutuste ning keskkonnaseisundi halvenemisega seotud sündmuste, loodusõnnetuste, pandeemiate ja füüsiliste rünnete, sealhulgas sissetungi ja terrorirünnakute mõju;

g) siseründed;

h) poliitiline ja sotsiaalne ebastabiilsus, sealhulgas asjakohasel juhul kolmandast isikust IKT-teenuste osutaja jurisdiktsioonis ning andmete säilitamise ja töötlemise kohas;

i) ulatuslikud elektrikatkestused.

3. Kui esmased taastemeetmed ei ole kulude, riskide, logistika või ettenägematute asjaolude tõttu lühikeses perspektiivis teostatavad, kaalutakse lõikes 1 osutatud IKT reageerimis- ja taastekavades alternatiivseid võimalusi.

4. Finantssektori ettevõtjad kaaluvad ja rakendavad lõikes 1 osutatud IKT reageerimis- ja taastekavade raames talitluspidevuse meetmeid, millega leevendada tõrkeid selliste kolmandast isikust teenuseosutajate tegevuses, kes osutavad finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid.

V PEATÜKK

IKT-riski juhtimise raamistiku läbivaatamise aruanne

Artikkel 27

IKT-riski juhtimise raamistiku läbivaatamise aruande vorm ja sisu

1. Finantssektori ettevõtjad esitavad otsingut võimaldavas elektroonilises vormingus määruse (EL) 2022/2554 artikli 6 lõikes 5 osutatud IKT-riski juhtimise raamistiku läbivaatamise aruande.

2. Finantssektori ettevõtjad lisavad lõikes 1 osutatud aruandesse kõik järgmise:

a) sissejuhatav osa, milles on

   i) selgelt nimetatud finantssektori ettevõtja, kelle kohta aruanne esitatakse, ja vajaduse korral kirjeldatud tema kontserni struktuuri,

   ii) kirjeldatud aruande tausta: finantssektori ettevõtja teenuste, tegevuse ja toimingute laad, ulatus ja keerukus, organisatsiooniline struktuur, kindlaksmääratud kriitilise tähtsusega funktsioonid, strateegia, olulised käimasolevad projektid või tegevused, seosed, sõltuvus ettevõttesisestest ja lepingulistest IKT-teenustest ja -süsteemidest või mõju, mida selliste süsteemide toimimise lõppemine või märkimisväärne halvenemine avaldaks kriitilise tähtsusega või olulistele funktsioonidele ja turu tõhususele,

   iii) esitatud kokkuvõte peamistest muudatustest, mis on tehtud IKT-riski juhtimise raamistikus pärast eelmise aruande esitamist,

   iv) esitatud kõrgetasemeline ülevaade finantssektori ettevõtja praegusest ja lähiaja IKT-riski profiilist, ohumaastikust, finantssektori ettevõtja kontrollide hinnatud tõhususest ja tema turvaolekust;

b) kuupäev, mil finantssektori ettevõtja juhtorgan aruande heaks kiitis;

c) IKT-riski juhtimise raamistiku määruse (EL) 2022/2554 artikli 6 lõike 5 kohase läbivaatamise põhjuste kirjeldus;

d) läbivaatamisperioodi algus- ja lõppkuupäev;

e) teave läbivaatamise eest vastutaja kohta;

f) IKT-riski juhtimise raamistikus pärast eelmist läbivaatamist tehtud oluliste muudatuste ja täiustuste kirjeldus;

g) läbivaatamise tulemuste kokkuvõte ning läbivaatamisperioodil IKT-riski juhtimise raamistikus esinenud nõrkuste, puuduste ja lünkade tõsiduse üksikasjalik analüüs ja hinnang;

h) tuvastatud nõrkuste, puuduste ja lünkade kõrvaldamise meetmete kirjeldus, sealhulgas kõik järgmine:

   i) tuvastatud nõrkuste, puuduste ja lünkade kõrvaldamiseks võetud meetmete kokkuvõte,

   ii) meetmete rakendamise eeldatav kuupäev ja rakendamise sisekontrolliga seotud kuupäevad, sealhulgas teave kõnealuste meetmete rakendamise seisu kohta aruande koostamise kuupäeva seisuga, ning vajaduse korral selgitus selle kohta, kas on olemas oht, et tähtaegadest ei peeta kinni,

   iii) meetmete rakendamiseks kasutatavad vahendid ja meetmete rakendamise eest vastutavate isikute kindlaksmääramine koos täpsustusega selle kohta, kas need vahendid ja isikud on sisemised või välised,

   iv) meetmetes kavandatud muudatuste mõju finantssektori ettevõtja eelarve-, inim- ja materiaalsetele ressurssidele, sealhulgas parandusmeetmete rakendamiseks ette nähtud vahenditele,

   v) vajaduse korral teave pädeva asutuse teavitamise korra kohta,

   vi) kui tuvastatud nõrkuste, puuduste või lünkade suhtes ei kohaldata parandusmeetmeid, üksikasjalik selgitus nõrkuste, puuduste või lünkade mõju analüüsimisel või IKT-jääkriski hindamisel kasutatud kriteeriumide kohta ja seonduva jääkriski aktsepteerimise kriteeriumide kohta;

i) teave IKT-riski juhtimise raamistiku kavandatud edasiarendamise kohta;

j) IKT-riski juhtimise raamistiku läbivaatamise järeldused;

k) teave varasema läbivaatamise kohta, sealhulgas

   i) varasemate läbivaatamiste loetelu,

   ii) vajaduse korral viimases aruandes kindlaks määratud parandusmeetmete rakendamise seis,

   iii) kui varasema läbivaatamise käigus kavandatud parandusmeetmed on osutunud ebatõhusaks või tekitanud ootamatuid probleeme, kirjeldus selle kohta, kuidas neid parandusmeetmeid saaks täiustada, või nende ootamatute probleemide kirjeldus;

l) aruande koostamisel kasutatud teabeallikad, sealhulgas kõik järgmine:

   i) finantssektori ettevõtjate puhul, kes ei ole mikroettevõtjad, määruse (EL) 2022/2554 artikli 6 lõikes 6 osutatud siseauditite tulemused,

   ii) vastavushindamise tulemused,

   iii) IKT-vahendite, -süsteemide ja -protsesside digitaalse tegevuskerksuse testimise tulemused ning vajaduse korral ohuteabel põhinevale läbistustestimisele tugineva süvatestimise tulemused,

   iv) välised allikad.

Punkti c kohaldamisel, juhul kui läbivaatamine algatati pärast järelevalvejuhiste saamist või digitaalse tegevuskerksuse testimisel või asjaomaste auditite raames tehtud järelduste põhjal, peab aruanne sisaldama selgeid viiteid neile juhistele või järeldustele, et oleks võimalik kindlaks teha läbivaatamise algatamise põhjus. Kui läbivaatamine algatati pärast IKT intsidente, peab aruanne sisaldama kõigi IKT intsidentide loetelu koos nende algpõhjuste analüüsiga.

Punkti f kohaldamisel peab kirjeldus sisaldama analüüsi selle kohta, millist mõju avaldavad muudatused finantssektori ettevõtja digitaalse tegevuskerksuse strateegiale, IKT sisekontrolli raamistikule ja IKT-riski juhtimisele.

III JAOTIS

LIHTSUSTATUD IKT-RISKI JUHTIMISE RAAMISTIK MÄÄRUSE (EL) 2022/2554 ARTIKLI 16 LÕIKES 1 OSUTATUD FINANTSSEKTORI ETTEVÕTJATELE

I PEATÜKK

Lihtsustatud IKT-riski juhtimise raamistik

Artikkel 28

Juhtimine ja korraldus

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjatel peab olema sisemine juhtimis- ja kontrolliraamistik, mis tagab IKT-riski tulemusliku ja usaldusväärse juhtimise, et saavutada digitaalse tegevuskerksuse kõrge tase.

2. Lõikes 1 osutatud finantssektori ettevõtjad tagavad oma lihtsustatud IKT-riski juhtimise raamistiku osana, et nende juhtorgan

a) kannab üldist vastutust selle eest, et lihtsustatud IKT-riski juhtimise raamistik võimaldab ellu viia finantssektori ettevõtja äristrateegia kooskõlas tema riskivalmidusega, ning tagab, et selle raames võetakse arvesse IKT-riski;

b) määrab kõigi IKTga seotud ülesannete jaoks kindlaks selged rollid ja vastutusvaldkonnad;

c) kehtestab infoturbe-eesmärgid ja IKT-nõuded;

d) kiidab heaks, vaatab korrapäraselt läbi ning teeb järelevalvet järgmise üle:

   i) finantssektori ettevõtja teabevarade liigitus, millele on osutatud käesoleva määruse artikli 30 lõikes 1, peamiste tuvastatud riskide loetelu ning talitlusmõju analüüs ja sellega seotud põhimõtted,

   ii) finantssektori ettevõtja talitluspidevuse kavad ning reageerimis- ja taastemeetmed, millele on osutatud määruse (EL) 2022/2554 artikli 16 lõike 1 punktis f;

e) näeb ette ja vaatab vähemalt kord aastas läbi eelarve, mis on vajalik finantssektori ettevõtja digitaalse tegevuskerksuse vajaduste rahuldamiseks, pidades silmas igat liiki ressursse, sealhulgas asjakohaseid IKT-turbe alase teadlikkuse suurendamise programme ja digitaalse tegevuskerksuse koolitusi ning kõigi töötajate IKT-oskusi;

f) määrab kindlaks käesoleva jaotise I, II ja III peatükis sätestatud põhimõtted ja meetmed, millega tehakse kindlaks, hinnatakse ja juhitakse finantssektori ettevõtja IKT-riski, ning rakendab neid;

g) määrab kindlaks menetlused, IKT-protokollid ja -vahendid, mis on vajalikud kõigi teabevarade ja IKT-varade kaitsmiseks, ning rakendab neid;

h) tagab, et finantssektori ettevõtja töötajatel on piisavad ja ajakohased teadmised ja oskused, mis võimaldavad mõista ja hinnata IKT-riski ning selle mõju finantssektori ettevõtja tegevusele, proportsionaalselt juhitava IKT-riskiga;

i) kehtestab aruandluskorra, sealhulgas määrab kindlaks juhtorganile teabeturbe ja digitaalse tegevuskerksuse kohta esitatavate aruannete sageduse, vormi ja sisu.

3. Lõikes 1 osutatud finantssektori ettevõtjad võivad kooskõlas liidu ja liikmesriigi valdkondliku õigusega anda IKT-riski juhtimise nõuete täitmise kontrollimise ülesanded edasi kontsernisisestele või kolmandast isikust IKT-teenuste osutajatele. Ülesannete edasiandmise korral vastutab IKT-riski juhtimise nõuete täitmise kontrollimise eest täielikult finantssektori ettevõtja.

4. Lõikes 1 osutatud finantssektori ettevõtjad tagavad, et kontrollifunktsioonid ja siseauditifunktsioonid on sobivalt eraldatud ja sõltumatud.

5. Lõikes 1 osutatud finantssektori ettevõtjad tagavad, et audiitorid teevad nende lihtsustatud IKT-riski juhtimise raamistikule siseauditeid kooskõlas finantssektori ettevõtjate auditikavaga. Audiitoritel peavad olema piisavad teadmised, oskused ja asjatundlikkus IKT-riski valdkonnas ning nad peavad olema sõltumatud. IKT-auditite sagedus ja fookus peavad olema vastavuses finantssektori ettevõtja IKT-riskiga.

6. Lõikes 1 osutatud finantssektori ettevõtjad tagavad lõikes 5 osutatud IKT-auditite kriitilise tähtsusega tulemuste õigeaegse kontrollimise ja parandamise.

Artikkel 29

Infoturbe põhimõtted ja meetmed

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad töötavad lihtsustatud IKT-riski juhtimise raamistiku osana välja ja dokumenteerivad infoturbe põhimõtted ning rakendavad neid. Neis põhimõtetes määratakse kindlaks kõrgetasemelised põhialused ja reeglid, et kaitsta andmete ja finantssektori ettevõtjate osutatavate teenuste konfidentsiaalsust, terviklust, kättesaadavust ja autentsust.

2. Lõikes 1 osutatud finantssektori ettevõtjad kehtestavad oma lõikes 1 osutatud infoturbe põhimõtetele tuginedes IKT-riski maandamiseks IKT-turvameetmed ning rakendavad neid; kõnealused põhimõtted hõlmavad ka kolmandast isikust IKT-teenuste osutajate rakendatavaid riskimaandamismeetmeid.

IKT-turvameetmed peavad hõlmama kõiki artiklites 30–38 osutatud meetmeid.

Artikkel 30

Teabevarade ja IKT-varade liigitamine

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad teevad selle lõike punktis a osutatud lihtsustatud IKT-riski juhtimise raamistiku osana kindlaks, liigitavad ja dokumenteerivad kõik kriitilise tähtsusega või olulised funktsioonid, neid toetavad teabevarad ja IKT-varad ning nende vastastikuse sõltuvuse. Finantssektori ettevõtjad vaatavad selle kindlakstegemise ja liigitamise vajaduse korral läbi.

2. Lõikes 1 osutatud finantssektori ettevõtjad teevad kindlaks kõik kriitilise tähtsusega või olulised funktsioonid, mida toetavad kolmandast isikust IKT-teenuste osutajad.

Artikkel 31

IKT-riski juhtimine

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad lisavad oma lihtsustatud IKT-riski juhtimise raamistikku kõik järgmised toimingud:

a) IKT-riski taluvuse taseme kindlaksmääramine kooskõlas finantssektori ettevõtja riskivalmidusega;

b) finantssektori ettevõtja IKT-riski kindlakstegemine ja hindamine;

c) riskimaandamisstrateegiate kindlaksmääramine vähemalt selliste IKT-riskide jaoks, mis ületavad finantssektori ettevõtja riskitaluvuse taset;

d) punktis c osutatud riskimaandamisstrateegiate tulemuslikkuse seire;

e) IKT-süsteemi, -teenuste, -protsesside või -menetluste olulistest muudatustest tulenevate ning IKT turvalisuse testimise tulemustes kajastatud IKT- ja infoturberiskide tuvastamine ja hindamine ning IKT- ja infoturberiskide tuvastamine ja hindamine pärast igat suurt IKT intsidenti.

2. Lõikes 1 osutatud finantssektori ettevõtjad teevad ja dokumenteerivad korrapäraselt IKT-riski hindamise vastavalt oma IKT-riski profiilile.

3. Lõikes 1 osutatud finantssektori ettevõtjad seiravad pidevalt ohte ja nõrkusi, mis on olulised nende kriitilise tähtsusega või oluliste funktsioonide ning teabevarade ja IKT-varade seisukohast, ning vaatavad korrapäraselt läbi kriitilise tähtsusega või olulisi funktsioone mõjutavad riskistsenaariumid.

4. Lõikes 1 osutatud finantssektori ettevõtjad määravad kindlaks alarmiläved ja -kriteeriumid, mille korral käivitatakse ja algatatakse IKT intsidendile reageerimise protsess.

Artikkel 32

Füüsiline ja keskkonnaturve

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad määravad kindlaks füüsilise turbe meetmed ja võtavad nende väljatöötamisel arvesse ohumaastikku, käesoleva määruse artikli 30 lõikes 1 osutatud liigitust ning IKT-varade üldist riskiprofiili ja juurdepääsetavaid teabevarasid, ning rakendavad neid meetmeid.

2. Lõikes 1 osutatud meetmetega kaitstakse finantssektori ettevõtjate ruume ja vajaduse korral andmekeskusi, kus asuvad IKT- ja teabevarad, loata juurdepääsu, rünnete ja õnnetuste ning keskkonnaohtude eest.

3. Kaitse keskkonnaohtude eest peab olema vastavuses asjaomaste ruumide ja vajaduse korral andmekeskuste ning seal tehtavate toimingute või asuvate IKT-süsteemide kriitilise tähtsusega.

II PEATÜKK

Süsteemide, protokollide ja vahendite muud elemendid IKT-riski mõju minimeerimiseks

Artikkel 33

Pääsu reguleerimine

Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad töötavad välja ja dokumenteerivad loogilise ja füüsilise pääsu reguleerimise menetlused ja rakendavad neid ning tagavad nende menetluste järgimise, seire ja korrapärase läbivaatamise. Need menetlused peavad sisaldama sisaldavad järgmisi loogilise ja füüsilise pääsu reguleerimise elemente:

a) finantssektori ettevõtja teabevaradele, IKT-varadele ja nendega toetatavatele funktsioonidele ning elutähtsatele tegevuskohtadele juurdepääsu õiguste, sealhulgas kaugpääsu ja hädaolukorras pääsu õiguste haldamine, lähtudes teadmisvajadusest, kasutusvajadusest ja minimaalõiguste printsiibist;

b) kasutajate vastutus, millega tagatakse, et IKT-süsteemis toimingu teinud kasutaja on võimalik tuvastada;

c) kontohaldusmenetlused kasutaja- ja üldkontode, sealhulgas üldiste administraatorikontode pääsuõiguste andmiseks, muutmiseks või tühistamiseks;

d) autentimismeetodid, mis on vastavuses artikli 30 lõikes 1 osutatud liigitusega ja IKT-varade üldise riskiprofiiliga ning põhinevad juhtivatel tavadel;

e) pääsuõiguste korrapärane läbivaatamine ja tühistamine, kui neid ei ole enam vaja.

Punkti c kohaldamisel võimaldab finantssektori ettevõtja kõikidele IKT-süsteemidele eelis-, hädaolukorras või administraatori pääsu kasutusvajaduse korral või vajaduspõhiselt ning see pääs logitakse kooskõlas artikli 34 lõike 1 punktiga f.

Punkti d kohaldamisel kasutavad finantssektori ettevõtjad oma võrgule kaugpääsu, eelispääsu ning kriitilise tähtsusega või olulisi funktsioone toetavatele üldsusele kättesaadavatele IKT-varadele juurdepääsu andmisel juhtivatel tavadel põhinevaid tugevaid autentimismeetodeid.

Artikkel 34

IKT-toimingute turvalisus

Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad teevad oma süsteemide, protokollide ja vahendite rakendamise raames kõigi IKT-varade puhul järgmist:

a) seiravad ja haldavad kõigi IKT-varade olelusringi;

b) vajaduse korral kontrollivad, kas nende IKT-varasid toetavad kolmandast isikust IKT-teenuste osutajad;

c) teevad kindlaks oma IKT-varade ja -meetmete vajamineva võimsuse, mis võimaldab säilitada ja muuta paremaks IKT-süsteemide kättesaadavuse ja tõhususe ning ennetada IKT võimsuse puudujääki;

d) teevad IKT-varade nõrkuse automaatse skaneerimise ja hindamise, mis on vastavuses artikli 30 lõikes 1 osutatud liigitusega ja IKT-vara üldise riskiprofiiliga, ning võtavad kasutusele paigad tuvastatud nõrkuste kõrvaldamiseks;

e) juhivad aegunud, toetamata või IKT pärandvaraga seotud riske;

f) logivad sündmusi, mis on seotud loogilise ja füüsilise pääsu reguleerimisega, IKT-toimingutega, sealhulgas süsteemi- ja võrguliiklusega, ning IKT-muudatuste juhtimisega;

g) määravad kindlaks meetmed, millega seirata ja analüüsida kriitilise tähtsusega või oluliste IKT-toimingutega seotud anomaalset tegevust ja käitumist käsitlevat teavet;

h) rakendavad meetmeid, millega seirata küberohte käsitlevat asja- ja ajakohast teavet;

i) rakendavad meetmeid, millega teha kindlaks võimalikud teabelekked, ründekoodid ja muud turvaohud, samuti tarkvara ja riistvara üldteada nõrkused ning kontrollida vastavaid turvauuendeid.

Punkti f kohaldamisel viivad finantssektori ettevõtjad logide üksikasjalikkuse vastavusse logide otstarbega ja neid logisid tootva IKT-vara kasutamisega.

Artikkel 35

Andmete, süsteemide ja võrgu turvalisus

Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad töötavad oma süsteemide, protokollide ja vahendite osana välja sissetungi ja andmete väärkasutamise vastased kaitsemeetmed, millega tagatakse võrkude turvalisus ning säilitatakse andmete kättesaadavus, autentsus, terviklus ja konfidentsiaalsus, ning rakendavad neid meetmeid. Eelkõige näevad finantssektori ettevõtjad käesoleva määruse artikli 30 lõikes 1 osutatud liigitust arvesse võttes ette kõik järgmise:

a) kasutatavate, edastatavate ja jõudeolekus andmete kaitsmise meetmete kindlaksmääramine ja rakendamine;

b) finantssektori ettevõtja andmete edastamiseks ja säilitamiseks kasutatava tarkvara, andmekandjate, süsteemide ja lõppseadmete kasutamisega seotud turvameetmete kindlaksmääramine ja rakendamine;

c) selliste meetmete kindlaksmääramine ja rakendamine, millega hoitakse ära ja avastatakse loata ühendused finantssektori ettevõtja võrguga ning tagatakse finantssektori ettevõtja sisevõrgu ning interneti ja muude välisühenduste vahelise võrguliikluse turvalisus;

d) selliste meetmete kindlaksmääramine ja rakendamine, mis tagavad andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse võrguedastuse ajal;

e) selliste finantssektori ettevõtja ruumides või väljaspool säilitatavate andmete turvalise kustutamise protsess, mida finantssektori ettevõtjal ei ole enam vaja koguda või säilitada;

f) finantssektori ettevõtja ruumides või mujal asuvate konfidentsiaalset teavet sisaldavate andmesalvestusseadmete turvalise likvideerimise või kasutusest kõrvaldamise protsess;

g) selliste meetmete kindlaksmääramine ja rakendamine, millega tagatakse, et kaugtöö ja isiklike lõppseadmete kasutamine ei kahjusta finantssektori ettevõtja suutlikkust teha asjakohaselt, õigeaegselt ja turvaliselt oma kriitilise tähtsusega toiminguid.

Artikkel 36

IKT turvalisuse testimine

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad koostavad IKT turvalisuse testimise kava, mille alusel kontrollida käesoleva määruse artiklite 33, 34, 35, 37 ja 38 kohaselt välja töötatud IKT-turvameetmete tõhusust, ning rakendavad seda. Finantssektori ettevõtjad tagavad, et selles kavas võetakse arvesse ohte ja nõrkusi, mis on kindlaks tehtud käesoleva määruse artiklis 31 osutatud lihtsustatud IKT-riski juhtimise raamistiku raames.

2. Lõikes 1 osutatud finantssektori ettevõtjad vaatavad IKT-turvameetmed läbi ning hindavad ja testivad neid, võttes arvesse oma IKT-varade üldist riskiprofiili.

3. Lõikes 1 osutatud finantssektori ettevõtjad seiravad ja hindavad turvalisustestide tulemusi ning ajakohastavad vastavalt nendele oma turvameetmeid ning kriitilise tähtsusega või olulisi funktsioone toetavate IKT-süsteemide turvameetmeid põhjendamatu viivituseta.

Artikkel 37

IKT-süsteemide soetamine, arendamine ja hooldamine

Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad koostavad IKT-süsteemide soetamise, arendamise ja hooldamise korra, järgides riskipõhist lähenemisviisi, ning vajaduse korral rakendavad seda. Selle korraga

a) tagatakse, et enne IKT-süsteemide soetamist või arendamist on täpselt kindlaks määratud funktsionaalsed ja mittefunktsionaalsed nõuded, sealhulgas infoturbenõuded, ning asjaomase funktsiooni täitja on need heaks kiitnud;

b) tagatakse IKT-süsteemide testimine ja heakskiitmine enne nende esmakordset kasutamist ja enne nende muutmist tootmiskeskkonnas;

c) määratakse kindlaks meetmed maandamaks riski, et IKT-süsteeme nende tootmiskeskkonnas arendamise ja rakendamise ajal tahtmatult muudetakse või et nendega sel ajal tahtlikult manipuleeritakse.

Artikkel 38

IKT-projektide ja -muudatuste juhtimine

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad töötavad välja ja dokumenteerivad IKT-projektide juhtimise menetluse ja rakendavad seda ning määravad selle rakendamise jaoks kindlaks rollid ja vastutusvaldkonnad. See menetlus peab hõlmama kõiki IKT-projektide etappe alates projektide algatamisest kuni nende lõpetamiseni.

2. Lõikes 1 osutatud finantssektori ettevõtjad töötavad välja ja dokumenteerivad IKT-muudatuste juhtimise menetluse, millega tagatakse, et kõigi IKT-süsteemidesse tehtavate muudatuste registreerimine, testimine, hindamine, heakskiitmine, rakendamine ja kontrollimine toimub kontrollitud viisil ja rakendades piisavaid kaitsemeetmeid, et säilitada finantssektori ettevõtja digitaalne tegevuskerksus, ning rakendavad seda menetlust.

III PEATÜKK

IKT talitluspidevuse juhtimine

Artikkel 39

IKT talitluspidevuse kavad

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad töötavad välja IKT talitluspidevuse kavad, võttes arvesse tulemusi, milleni on jõutud, analüüsides tõsiste talitlushäirete riski ja nende häirete võimalikku mõju ning kriitilise tähtsusega või olulisi funktsioone toetavate IKT-varadega seotud võimalikke stsenaariume, sealhulgas küberründe stsenaariumi.

2. Lõikes 1 osutatud kavade puhul kehtivad järgmised nõuded:

a) finantssektori ettevõtja juhtorgan peab kavad heaks kiitma;

b) kavad tuleb dokumenteerida ning need peavad olema häda- või kriisiolukorras kergesti kättesaadavad;

c) kavadega tuleb ette näha piisavad vahendid nende rakendamiseks;

d) kavad peavad sisaldama tasemeid ja tähtaegu funktsioonide ning peamise sisemise ja välise sõltuvuse taastamiseks ja jätkumiseks, sealhulgas seoses kolmandast isikust IKT-teenuste osutajatega;

e) kavades tuleb kindlaks määrata tingimused, mis võivad kaasa tuua kava aktiveerimise, ning meetmed, mida tuleb võtta, et tagada finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone toetavate IKT-varade kättesaadavus, järjekestvus ja taastamine;

f) kavades tuleb kindlaks määrata kriitilise tähtsusega või oluliste ärifunktsioonide, tugiprotsesside, teabevarade ja nende vastastikuse sõltuvuse ennistamise ja taastamise meetmed, et vältida kahjulikku mõju finantssektori ettevõtjate toimimisele;

g) kavades tuleb kindlaks määrata varundusmenetlused ja -meetmed, milles täpsustatakse varundatavate andmete maht ja minimaalne varundamissagedus, lähtudes neid andmeid kasutava funktsiooni kriitilisest tähtsusest;

h) kavades tuleb kaaluda alternatiivseid võimalusi juhuks, kui taastamine ei ole kulude, riskide, logistika või ettenägematute asjaolude tõttu lühikeses perspektiivis teostatav;

i) kavades tuleb kindlaks määrata sise- ja välissuhtluse kord, sealhulgas eskalatsioonikava;

j) kavu tuleb ajakohastada, võttes arvesse intsidentidega seotud kogemusi, testimist, kindlakstehtud uusi riske ja ohte, muudetud taaste-eesmärke ning olulisi muudatusi finantssektori ettevõtja korralduses ja kriitilise tähtsusega või ärifunktsioone toetavates IKT-varades.

Punkti f kohaldamisel nähakse meetmetega ette kriitilise tähtsusega kolmandast isikust teenuseosutajate tõrgete leevendamine.

Artikkel 40

Talitluspidevuse kavade testimine

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad testivad oma käesoleva määruse artiklis 39 osutatud talitluspidevuse kavades kindlaks määratud varundus- ja taastemenetlusi, sealhulgas selles artiklis osutatud stsenaariume, vähemalt kord aastas ja iga kord, kui talitluspidevuse kavas tehakse oluline muudatus.

2. Lõikes 1 osutatud talitluspidevuse kavade testimisega tõendatakse, et lõikes 1 osutatud finantssektori ettevõtjad suudavad jätkata oma äritegevust seni, kuni kriitilise tähtsusega toimingud on taastatud, ning tehakse kindlaks nendes kavades esinevad puudused.

3. Lõikes 1 osutatud finantssektori ettevõtjad dokumenteerivad talitluspidevuse kavade testimise tulemused ning analüüsivad kõiki testimise käigus tuvastatud puudusi, kõrvaldavad need ja teatavad neist juhtorganile.

IV PEATÜKK

Lihtsustatud IKT-riski juhtimise raamistiku läbivaatamise aruanne

Artikkel 41

Lihtsustatud IKT-riski juhtimise raamistiku läbivaatamise aruande vorm ja sisu

1. Määruse (EL) 2022/2554 artikli 16 lõikes 1 osutatud finantssektori ettevõtjad esitavad otsingut võimaldavas elektroonilises vormingus selle artikli lõikes 2 osutatud lihtsustatud IKT-riski juhtimise raamistiku läbivaatamise aruande.

2. Lõikes 1 osutatud aruanne peab sisaldama kõike järgmist:

a) sissejuhatav osa, milles on

   i) aruande tausta kirjeldus: finantssektori ettevõtja teenuste, tegevuse ja toimingute laad, ulatus ja keerukus, organisatsiooniline struktuur, kindlaksmääratud kriitilise tähtsusega funktsioonid, strateegia, olulised käimasolevad projektid või tegevused, seosed, sõltuvus ettevõttesisestest ja lepingulistest IKT-teenustest ja -süsteemidest või mõju, mida selliste süsteemide toimimise lõppemine või märkimisväärne halvenemine avaldaks kriitilise tähtsusega või olulistele funktsioonidele ja turu tõhususele,

   ii) ülevaade finantssektori ettevõtja praegusest ja lähiaja tuvastatud IKT-riskist, ohumaastikust, finantssektori ettevõtja kontrollide hinnatud tõhususest ja tema turvaolekust,

   iii) teave valdkonna kohta, mille kohta aru antakse,

   iv) kokkuvõte olulistest muudatustest, mis on tehtud lihtsustatud IKT-riski juhtimise raamistikus pärast eelmise aruande esitamist,

   v) lihtsustatud IKT-riski juhtimise raamistikus pärast eelmise aruande esitamist tehtud oluliste muudatuste mõju kirjeldus;

b) asjakohasel juhul kuupäev, mil finantssektori ettevõtja juhtorgan aruande heaks kiitis;

c) lihtsustatud IKT-riski juhtimise raamistiku läbivaatamise põhjuste kirjeldus, sealhulgas

   i) kui läbivaatamine algatati pärast järelevalvejuhiste saamist, tõendid nende juhiste kohta,

   ii) kui läbivaatamine algatati pärast IKT intsidente, kõigi intsidentide loetelu koos nende algpõhjuste analüüsiga;

d) läbivaatamisperioodi algus- ja lõppkuupäev;

e) läbivaatamise eest vastutav isik;

f) läbivaatamise tulemuste kokkuvõte ning enesehinnang läbivaatamisperioodil lihtsustatud IKT-riski juhtimise raamistikus esinenud nõrkuste, puuduste ja lünkade tõsiduse kohta, sealhulgas nende üksikasjalik analüüs;

g) parandusmeetmed lihtsustatud IKT-riski juhtimise raamistikus tuvastatud nõrkuste, puuduste ja lünkade kõrvaldamiseks ning nende meetmete rakendamise eeldatav kuupäev, sealhulgas järelmeetmed varasemates aruannetes tuvastatud nõrkuste, puuduste ja lünkade jaoks, kui neid ei ole veel kõrvaldatud;

h) lihtsustatud IKT-riski juhtimise raamistiku läbivaatamise üldised järeldused, sealhulgas teave selle raamistiku kavandatud edasiarendamise kohta.

IV JAOTIS

LÕPPSÄTTED

Artikkel 42

Jõustumine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 13. märts 2024

Komisjoni nimel
president
Ursula VON DER LEYEN