EIOPA-BoS-20/600

Info- ja kommunikatsioonitehnoloogia turbe- ja juhtimissuunised

EIOPA – Westhafen Tower, Westhafenplatz 1 – 60327 Frankfurt – Saksamaa – Tel: + 49 69-951119-20;
faks + 49 69-951119-19; e-post: info@eiopa.europa.eu veebisait: www.eiopa.europa.eu

Sisukord

Taustteave

1. Määruse (EL) nr 1094/2010 artikli 16 alusel võib EIOPA ühtsete, tõhusate ja tulemuslike järelevalvetavade kehtestamiseks ning liidu õiguse ühetaolise ja järjepideva kohaldamise tagamiseks esitada pädevatele asutustele ja finantsasutus suuniseid ja soovitusi.

2. Selle määruse artikli 16 lõike 3 kohaselt on pädevad asutused ja finantseerimisasutused kohustatud võtma mis tahes meetmeid, et kõnealuseid suuniseid ja soovitusi järgida.

3. EIOPA leidis, et seoses direktiivi 2009/138/EÜ artiklitega 41 ja 44 ning analüüsides Euroopa Komisjoni finantstehnoloogia tegevuskava (COM(2018)0109 final), EIOPA järelevalve lähenemiskava 2018–2019[1] ja mitme muu sidusrühmaga järgnevat suhtlust[2], on vaja välja töötada konkreetsed info- ja kommunikatsioonitehnoloogia (IKT) turbe- ja juhtimissuunised.

4. Nagu on esitatud Euroopa järelevalveasutuste ühises nõuandes Euroopa Komisjonile, *„ei kajasta...„* EIOPA haldussüsteemi suunised ... *„nõuetekohaselt IKT-riski (sealhulgas küberriskide) juhtimisega tegelemise olulisust*". Puuduvad suunised oluliste elementide kohta, mida loetakse üldiselt asjakohase IKT-turbe ja -juhtimise osaks.

5. ELi praeguse (seadusandliku) olukorra analüüsimine eespool osutatud ühise nõuande eesmärgil näitas, et enamik ELi liikmesriike on määratlenud IKT-turbe ja -juhtimise riiklikud eeskirjad. Ehkki nõuded on sarnased, on õigusraamistik endiselt killustunud. Peale selle selgusid praeguste järelevalvetavade uuringust väga erinevad tavad, alates „konkreetse järelevalve puudumisest" kuni „range järelevalveni" (sealhulgas „kaugkontroll" ja „kohapealne kontroll").

6. Lisaks muutub IKT aina keerukamaks ja samuti kasvab IKT-ga seotud vahejuhtumite (sealhulgas küberintsidentide) sagedus, nagu ka selliste intsidentide kahjulik mõju ettevõtjate toimimisele. Seepärast on IKT- ja turvariski juhtimine ettevõtjale oma strateegiliste, ettevõtlus-, tegevus- ja maine-eesmärkide saavutamisel ülioluline.

7. Lisaks tuginetakse kindlustussektoris (sealhulgas nii traditsioonilistes kui ka innovatiivsetes ärimudelites) kindlustusteenuste pakkumisel ja kindlustusandjate tavategevuses üha enam IKT-le, nt kindlustussektori digipööre (kindlustustehnoloogia, asjade internet jms), samuti seotus sidekanalite kaudu (internet, mobiilsed ja traadita ühendused ning Lairiba võrgud). See muudab kindlustusandjate tegevuse vastuvõtlikuks turvaintsidentidele, sealhulgas küberrünnetele. Seepärast on oluline tagada kindlustusandjate piisav ettevalmistus oma IKT- ja turvariskide juhtimiseks.

8. Tunnistades lisaks kindlustusandjate vajadust valmistuda küberriskideks[3] ja usaldusväärse küberturvalisuse raamistiku järele, käsitletakse nendes suunistes ka küberturvalisust kindlustusandja infoturbemeetmete osana. Ehkki suunistes tunnistatakse, et küberturvalisusega tuleks tegeleda kindlustusandja üldise IKT- ja turvariskide juhtimise osana, on oluline märkida, et küberrünnetel on mõni

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Aruanne, mille EIOPA avaldas vastusena Euroopa Komisjoni finantstehnoloogia tegevuskavale, on saadaval siin.

[3] Küberriski määratlust vt dokumendist „FSB Cyber Lexicon", 12. november 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

eripära, mida tuleks arvesse võtta, et tagada küberriski piisav leevendamine infoturbemeetmetega:

a) küberründeid on sageli raskem ohjata (st tuvastada, tõrjuda, avastada, neile reageerida ja nendest täielikult toibuda) kui enamikku muid IKT- ja turvariskide allikaid ning ka kahju ulatust on raske kindlaks teha;

b) mõne küberründe puhul võivad tavalised riskijuhtimis- ja talitluspidevuse meetmed ning suurõnnetusest taastumise meetmed osutuda ebatõhusaks, kuivõrd rünnetega võidakse levitada pahavara, et varundada süsteeme eesmärgiga muuta need kättesaamatuks või rikkuma varuadnmeid;

c) küberrünnete levitamise kanaliks võivad muutuda teenuseosutajad, maaklerid, (juhtiv-) agent ja -vahendajad. Ülekanduvate vargsi levivate ohtude puhul võidakse kindlustusandja IKT-süsteemi jõudmiseks kasutada kolmanda isiku sideühendusi. Seepärast võib väheoluline ühendatud kindlustusandja muutuda ohtudele vastuvõtlikuks ja riski levitamise allikaks ning viia süsteemse mõjuni. Nõrgima lüli põhimõtet järgides ei tohiks küberturvalisus olla üksnes suurimate turuosaliste või kriitiliste teenuseosutajate mure.

9. Käesolevatel suunistel on järgmine eesmärk:

a) tagada turuosalistele selgus ja läbipaistvus minimaalse oodatava teabe ja küberturbevõime, st baasturvalisuse asjus;

b) vältida võimalikku õiguslikku arbitraaži;

c) soodustada järelevalvealast ühtsust seoses IKT-turbes ja -juhtimises rakendatavate ootuste ja protsessidega, mis on IKT- ja turvariskide nõuetekohase juhtimise võti.

Info- ja kommunikatsioonitehnoloogia turbe- ja juhtimissuunised

Sissejuhatus

1. EIOPA annab kooskõlas määruse (EL) nr 1094/2010[4] artikliga 16 välja need järelevalveasutustele mõeldud suunised, et anda kindlustus- ja edasikindlustusandjatele (edaspidi kollektiivselt „kindlustusandjad") juhiseid, kuidas kohaldada direktiivis 2009/138/EÜ[5] (edaspidi „Solventsus II direktiiv") ja komisjoni delegeeritud määruses (EL) 2015/35[6] (edaspidi „delegeeritud määrus") ette nähtud juhtimisnõudeid info- ja kommunikatsioonitehnoloogia („IKT") turbe ja juhtimise kontekstis. Seepärast tuginevad käesolevad suunised Solventsus II direktiivi artiklite 41, 44, 46, 47, 132 ja 246 ning delegeeritud määruse artiklite 258–260, 266, 268–271 ja 274 juhtimissätetele. Lisaks tuginevad käesolevad suunised ka EIOPA juhtimissüsteemi suunistes (EIOPA-BoS-14/253)[7] ja suunistes pilveteenuse osutajatega tegevuse edasiandmine kohta (EIOPA-BoS-19/270)[8] esitatud juhistele.

2. Käesolevaid suuniseid kohaldatakse nii üksikute kindlustusandjate kui ka *mutatis mutandis* konsolideerimisgrupi tasandil[9].

3. Pädevad asutused peaksid käesolevaid suuniseid järgides või nende täitmise üle järelevalvet tehes võtma arvesse proportsionaalsuse põhimõtet,[10] mis peaks tagama, et juhtimiskorraldus, sealhulgas IKT-turbe ja juhtimisega seotu, on vastavuses kindlustusandjatele omaste või nende võimalike riskide laadi, ulatuse ja keerukusega.

4. Käesolevaid suuniseid tuleks tõlgendada koostoimes Solventsus II direktiivi, delegeeritud määruse, EIOPA juhtimissüsteemi suuniste ja EIOPA suunistega pilveteenuse osutajatega alltöövõtulepingute sõlmimise kohta ilma, et see piiraks nende kohaldamist. Käesolevad suunised on kavandatud tehnoloogia- ja metoodikaneutraalsena.

Mõisted

5. Käesolevates suunistes määratlemata mõistetel on Solventsus II direktiivis määratletud tähendus.

6. Käesolevates suunistes kasutatakse järgmisi mõisteid:

---

4 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).

5 Euroopa Parlamendi ja nõukogu 25. novembri 2009. aasta direktiiv 2009/138/EÜ kindlustus- ja edasikindlustustegevuse alustamise ja jätkamise kohta (Solventsus II) (ELT L 335, 17.12.2009, lk 1).

6 Komisjoni 10. oktoobri 2014. aasta delegeeritud määrus (EL) 2015/35, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi 2009/138/EÜ kindlustus- ja edasikindlustustegevuse alustamise ja jätkamise kohta (Solventsus II) (ELT L 12, 17.1.2015, lk 1).

7 https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

8 https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

9 Direktiivi 2009/138/EÜ artikli 212 lõige 1.

10 Direktiivi 2009/138/EÜ artikli 29 lõige 3.

Vara omanik	Isik või üksus, kelle vastutus- ja haldusalasse kuulub teabe- ja IKT-vara.
Kättesaadavus	Volitatud üksusele kättesaadavus ja selle nõudmisel (õigeaegsus) üksuse poolt kasutatavus.
Konfidentsiaalsus	Teavet ei tehta kättesaadavaks ega avalikustata volitamata isikutele, üksustele, protsessidele ega süsteemidele.
Küberrünne	Mis tahes liiki häkkimine, mis toob kaasa ründava/pahatahtliku katse IKT-süsteemideni viiv teabevara hävitada, ohtu seada, seda muuta, see blokeerida, varastada või sellele loata juurdepääs saada või seda loata kasutada.
Küberturvalisus	Teabe- ja/või infosüsteemide konfidentsiaalsuse, tervikluse ja kättesaadavuse säilitamine küberkeskkonna kaudu.
IKT-vara	Ärikeskkonnas leiduva tarkvara või riistvara vara.
IKT-projektid	Kõik projektid või nende osad, kus IKT-süsteeme ja -teenuseid muudetakse, asendatakse või rakendatakse.
IKT-ja turvarisk	Operatiivriski allkomponendina tekkiva kahju risk, mis on tingitud konfidentsiaalsuse rikkumisest, süsteemide ja andmete usaldusväärsusega seotud tõrgetest, süsteemide ja andmete sobimatusest või mittekättesaadavusest või võimetusest muuta IKT-d mõistliku aja ja kuludega, kui keskkond või äritegevuse nõuded muutuvad (st paindlikkus). See hõlmab küberriske ja infoturberiske, mis tulenevad ebapiisavatest või nurjunud ettevõttesisestest protsessidest või -välistest sündmustest, sh küberrünnetest või ebapiisavast füüsilisest julgeolekust.
Infoturve	Teabe- ja/või infosüsteemide konfidentsiaalsuse, tervikluse ja kättesaadavuse säilitamine. Peale selle võib see hõlmata muid omadusi, nagu autentsus, vastutus, ümberlükkamatus ja usaldusväärsus.
IKT-teenused	IKT-süsteemide ja teenuseosutajate kaudu osutatavad teenused ühele või mitmele sise- või väliskasutajale.

IKT-süsteemid	Rakenduste, teenuste, infotehnoloogiavarade, IKT-varade või muude andmekäitlusvahendite kogu, mis hõlmab tegevuskeskkonda.
Teabevara	Kaitsmist vääriva konkreetse või mittekonkreetse teabe kogu.
Terviklus	Täpsus ja terviklikkus.
Operatiiv- või turvaintsident	Sündmus või mitu seotud kavandamata sündmust, mis kahjustavad või tõenäoliselt kahjustavad IKT-süsteemide ja -teenuste terviklust, kättesaadavust ja konfidentsiaalsust.
Teenuseosutaja	Kolmas isik, kes tegevuse edasiandmise lepingu alusel teostab edasiantud protsessi, teenust või tegevust või selle osa.
Ohust lähtuv läbistustestimine	Kontrollitud katse kahjustada üksuse kübervastupidavusvõimet tegelike ohusubjektide taktika, tehnika ja menetluste imiteerimisega. See põhineb sihtpäraseid ohte käsitleval luureteabel ja keskendub (minimaalse(te) eelteadmiste ja mõjuga tegevusele) üksuse inimestele, protsessidele ja tehnoloogiale.
Nõrkus	Vara või kontrollimehhanismi nõrkus, vastuvõtlikkus või viga, mida saab ühe või mitme ohu puhul ära kasutada.

7. Käesolevaid suuniseid kohaldatakse alates 1. juulist 2021.

Suunis 1. Proportsionaalsus

8. Kindlustusandjad peaksid käesolevaid suuniseid kohaldama viisil, mis on proportsionaalne nende äritegevusega seotud riskide laadi, ulatuse ja keerukusega.

Suunis 2. IKT juhtimissüsteemis

9. Haldus-, juhtimis- või järelevalveorgan peaks tagama, et kindlustusandjate juhtimissüsteemis – eelkõige riskijuhtimis- ja sisekontrollisüsteemis – juhitakse kindlustusandjate IKT- ja turvariske nõuetekohaselt.

10. Haldus-, juhtimis- või järelevalveorgan peaks tagama, et kindlustusandjate töötajate arv ja oskused on piisavad nende IKT-alaste tegevusvajaduste, IKT- ja turvariski juhtimise protsesside järjepidevaks toetamiseks ning IKT-strateegia rakendamise tagamiseks. Peale selle tuleks töötajatele pakkuda IKT- ja turvariskide , sealhulgas infoturbe alal regulaarselt piisavat koolitust, nagu on osutatud suunises 13.

11. Haldus-, juhtimis- või järelevalveorgan peaks tagama, et eraldatud vahendid on eespool osutatud nõuete täitmiseks piisavad.

Suunis 3. IKT-strateegia

12. Haldus-, juhtimis- või järelevalveorganil lasub üldvastutus kindlustusandjate kirjaliku IKT-strateegia loomise ja heakskiitmise eest nende üldise äristrateegia osana ja sellega kooskõlas, samuti sellest teavitamise ja selle rakendamise järelevalve eest.

13. IKT-strateegias tuleks kindlaks määrata vähemalt järgmine:

    a) kuidas kindlustusandjate IKT peaks arenema, et oma äristrateegiat tõhusalt toetada ja rakendada, hõlmates nende organisatsioonilist struktuuri, ärimudelit, IKT-süsteemide arengut ja peamist sõltuvust teenuseosutajatest;

    b) IKT-arhitektuuri areng, sealhulgas sõltuvus teenuseosutajatest, ning

    c) selged infoturbe eesmärgid, mis keskenduvad IKT-süsteemidele ja -teenustele, töötajatele ja protsessidele.

14. Kindlustusandjad peaksid tagama IKT-strateegia õigeaegse rakendamise, vastuvõtmise ja kõikide asjaomaste töötajate ja teenuseosutajate teavitamise sellest vastavalt kehtivatele ja asjakohastele nõudmistele.

15. Kindlustusandjad peaksid kehtestama korra oma IKT-strateegia tõhususe ja rakendamise seireks ning mõõtmiseks. Seda korda tuleks regulaarselt läbi vaadata ja ajakohastada.

Suunis 4. IKT- ja turvariskid riskijuhtimissüsteemis

16. Haldus-, juhtimis- või järelevalveorganil lasub üldvastutus IKT- ja turvariskide tõhusa juhtimissüsteemi sisseseadmise eest kindlustusandja üldise riskijuhtimissüsteemi osana. See hõlmab nende riskide puhul riskitaluvuspiiri kindlaksmääramist vastavalt kindlustusandja riskistrateegiale ning regulaarset kirjalikku aruannet haldus-, juhtimis- või järelevalveorganile riskijuhtimisprotsessi tulemuse kohta.

17. Kindulustusandja peaksid oma üldise riskijuhtimissüsteemi osana seoses IKT- ja turvariskidega (määrates vastavalt allpool kirjeldatule kindlaks IKT kaitsenõuded) võtma arvesse vähemalt järgmist:

    a) kindlustusandjad peaksid kaardistama ja ajakohastama regulaarselt oma äriprotsesse ja tegevust, äritoiminguid, ülesandeid ja varasid (nt teabevarad ja IKT-varad), et selgitada välja nende tähtsus ja sõltuvus IKT- ja turvariskidest;

    b) kindlustusandjad peaksid välja selgitama ja ära mõõtma kõik olulised IKT- ja turvariskid, millega nad kokku puutuvad, ning liigitama tuvastatud äriprotsessid ja tegevused, äritoimingud, ülesanded ja varad (nt teabevarad ja IKT-varad) kriitilisuse alusel. Kindlustusandjad peaksid ühtlasi hindama vähemalt nende äriprotsesside ja -tegevuste, äritoimingute, ülesannete ja varade (nt teabevarad ja IKT-varad) konfidentsiaalsuse, tervikluse ja kättesaadavuse kaitsenõudeid. Tuleks tuvastada varade liigitamise eest vastutavad vara omanikud;

    c) meetodid, mida kasutatakse kriitilisuse ja samuti vajaliku kaitse taseme kindlaksmääramiseks eelkõige seoses tervikluse, kättesaadavuse ja

konfidentsiaalsuse kaitse eesmärkidega, peaksid tagama kaitsenõuete järjepidevuse ja terviklikkuse;

d) IKT- ja turvariske tuleks mõõta määratletud IKT- ja turvariskikriteeriumide alusel, võttes arvesse nende äriprotsesside ja -tegevuste, äritoimingute, ülesannete ja varade (nt teabevarade ja IKT-varade) kriitilisust, teadaolevate nõrkuste ulatust ja varasemaid intsidente, mis kindlustusandjat mõjutasid;

e) IKT- ja turvariske tuleks regulaarselt hinnata ja dokumenteerida. Selline hindamine tuleks korraldada ka enne mis tahes suurt infrastruktuuri, protsesside või korra olulisemat muutmist, mis mõjutab äriprotsesse ja -tegevusi, äritoiminguid, ülesandeid ja varasid (nt teabevarad ja IKT-varad);

f) kindlustusandjad peaksid oma riskihinnangu põhjal vähemalt määrama kindlaks ja rakendama meetmeid tuvastatud IKT- ja turvariskide juhtimiseks ning infovarade kaitsmiseks vastavalt nende liigitusele. See peaks hõlmama meetmete kindlaksmääramist ülejäänud riskide juhtimiseks.

18. IKT-ja turvariskide juhtimise protsessi tulemused peaks heaks kiitma haldus-, juhtimis- või järelevalveorgan ja need tuleks kindlustusandja üldise riskijuhtimise osana kaasata operatiivriski juhtimise protsessi.

Suunis 5. Audit

19. Kindlustusandjate juhtimist, süsteeme ning nende IKT-ja turvariskide protsesse peaksid perioodiliselt auditeerima vastavalt kindlustusandjate auditikavale[11] piisavate teadmiste, oskuste ning IKT- ja turvariskide oskusteadmistega audiitorid, et kinnitada sõltumatult nende tõhusust haldus-, juhtimis- või järelevalveorganile. Nende auditite sagedus ja fookus peaksid olema võrdelised asjakohaste IKT- ja turvariskidega.

Suunis 6. Infoturbepoliitika ja -meetmed

20. Kindlustusandjad peaksid kehtestama kirjaliku ning haldus-, juhtimis- või järelevalveorgani heakskiidetud infoturbepoliitika, milles tuleks määratleda kõrgetasemelised põhimõtted ja eeskirjad kindlustusandjate teabe konfidentsiaalsuse, tervikluse ja kättesaadavuse kaitseks, et toetada IKT-strateegia rakendamist.

21. Poliitika peaks kirjeldama infoturbe juhtkonna peamisi ülesandeid ja kohustusi ning selles tuleks sätestada infoturbega seotud töötajatele, protsessidele ja tehnoloogiale kehtivad nõuded, pidades silmas, et kõigi taseme töötajatel on kohustus tagada kindlustusandjate infoturve.

22. Poliitika peaks kindlustusandja ettevõttesiseselt teatavaks tegema ja seda tuleks kohaldada kõikide töötajate suhtes. Asjakohastel ja olulistel puhkudel tuleks infoturbepoliitikast või selle osadest teavitada ka teenuseosutajaid ja kohaldada poliitikat nende suhtes.

23. Poliitika kohaselt peaksid kindlustusandjad kehtestama ja rakendama konkreetsemaid infoturbemenetlusi ja infoturbemeetmeid, et leevendada muu hulgas IKT- ja turvariske, millega nad kokku puutuvad. Menetlused ja infoturbemeetmed peaksid asjakohastel puhkudel hõlmama kõiki käesolevates suunistes kirjeldatud protsesse.

[11] Delegeeritud määruse artikkel 271.

Suunis 7. Infoturbe funktsioon

24. Kindlustusandjad peaksid oma haldussüsteemis ja vastavalt proportsionaalsuse põhimõttele seadma sisse infoturbe funktsiooni koos määratud isikule antud kohustustega. Kindlustusandja peaks tagama infoturbe funktsiooni sõltumatuse ja erapooletuse, hoides seda nõuetekohaselt lahus IKT-arendusest ja tööprotsessidest. Funktsiooni kohta tuleks aru anda haldus-, juhtimis- või järelevalveorganile.

25. Infoturbe funktsiooni tüüpülesanded on järgmised:

    a) toetada haldus-, juhtimis- või järelevalveorganit kindlustusandjatele infoturbepoliitika kindlaksmääramisel ja säilitamisel ning kontrollida selle rakendamist;

    b) anda haldus-, juhtimis- või järelevalveorganile regulaarselt ja sihtotstarbeliselt aru ja nõu infoturbe ning selle arengu kohta;

    c) jälgida infoturbemeetmete rakendamist ja vaadata see läbi;

    d) tagada infoturbenõuete järgimine teenuseosutajate kasutamisel;

    e) tagada kõigi töötajate ja teenuseosutajate, kellel on teabele ja süsteemidele juurdepääs, piisav teavitamine infoturbepoliitikast, näiteks infoturbe koolituse ja teadlikkuse tõstmise seminaride abil;

    f) koordineerida operatiiv- või turvaintsidentide uurimist ja teatada olulistest intsidentidest haldus-, juhtimis- või järelevalveorganile.

Suunis 8. Loogiline turvalisus

26. Kindlustusandjad peaksid vastavalt suunises 4 määratletud kaitsenõuetele määrama kindlaks, dokumenteerima ja rakendama loogilise andmetele juurdepääsu kontrolli või loogilise turvalisuse (identiteedi- ja juurdepääsuhalduse) korra. Seda korda tuleks rakendada, jõustada, jälgida ja perioodiliselt läbi vaadata ning see peaks hõlmama ka anomaaliate jälgimise kontrolli. Selles korras tuleks rakendada vähemalt järgmisi elemente, kus mõiste „kasutaja" hõlmab ka tehnilisi kasutajaid:

    a) teadmisvajadus, privileegide piiratus ja ülesannete lahusus: kindlustusandjad peaksid piirama teabevaradele ja nende tugisüsteemidele juurdepääsu õigusi (sealhulgas kaugjuurdepääs teabevaradele) „teadmisvajaduse" põhimõtet kasutades. Kasutajatele tuleks anda tööülesannete täitmiseks rangelt vajalikud minimaalsed juurdepääsuõigused („privileegide piiratuse" põhimõte), st et ennetada põhjendamatut juurdepääsu andmetele või selliste juurdepääsuõiguste kombinatsiooni määramist, mida võidakse kasutada kontrollidest hoidumiseks („ülesannete lahususe" põhimõte);

    b) kasutajate vastutus: kindlustusandjad peaksid võimaluste piires piirama üld- ja ühiste kasutajakontode kasutamist ning tagama võimaluse kasutajaid alati tuvastada ja jälgida neid vastutava füüsilise isikuni või IKT-süsteemides tehtud toimingu volitatud ülesandeni;

    c) privilegeeritud juurdepääsuõigused: kindlustusandjad peaksid rakendama süsteemi privilegeeritud juurdepääsule rangeid kontrollimehhanisme, piirates rangelt süsteemile suurema juurdepääsuga kontosid (nt administraatori kontod) ja pidades nende üle hoolikalt järelevalvet;

    d) kaugjuurdepääs: turvalise side tagamiseks ja riski vähendamiseks tuleks halduslik kaugjuurdepääs kriitilise tähtsusega IKT-süsteemidele anda ainult teadmisvajaduse põhjal ja tugevate autentimislahenduste kasutamisel;

e) kasutajate tegevuse logimine: kasutajate tegevust tuleks logida ja jälgida riskile vastaval viisil, mis peaks hõlmama vähemalt privilegeeritud kasutajate tegevust. Juurdepääsulogisid tuleks kaitsta lubamatu muutmise või kustutamise eest ja nende säilitusaeg peaks olenema äritoimingute, tugiprotsesside ja teabevarade tuvastatud kriitilisusest, ilma et see piiraks Euroopa Liidu ja riiklikus õiguses sätestatud säilitamisnõuete kohaldamist. Kindlustusandjad peaksid kasutama seda teavet teenuste osutamisel tuvastatud anomaalsete tegevuste väljaselgitamise ja uurimise soodustamiseks;

f) juurdepääsu haldamine: juurdepääsuõigusi tuleks anda, ära võtta ja muuta õigeaegselt vastavalt varem kindlaksmääratud heakskiitmise korrale, juhul kui on tegemist kehtiva teabevara omanikuga. Kui juurdepääsu ei ole enam vaja, tuleks juurdepääsuõigused kohe tühistada;

g) juurdepääsu hindamine: juurdepääsuõigused tuleks perioodiliselt üle vaadata tagamaks, et kasutajatel ei ole liigseid privileege ja et juurdepääsuõigused võetakse tagasi/tühistatakse, kui neid enam vaja ei ole;

h) juurdepääsuõiguste andmist, muutmist ja tühistamist tuleks dokumenteerida arusaadaval ja analüüsi hõlbustaval viisil ning

i) autentimismeetodid: kindlustusandjad peaksid kasutama piisavalt stabiilseid autentimismeetodeid, mis võimaldavad piisavalt ja tõhusalt tagada juurdepääsukontrolli korra ja menetluste järgimise. Autentimismeetodid peaksid vastama juurdepääsetava(te) IKT-süsteemide, -teabe või -protsessi kriitilisusele. See peaks asjakohase riski põhiselt hõlmama vähemalt keerulisi paroole või tugevamaid autentimismeetodeid (näiteks kaheastmeline autentimine).

27. Rakenduste elektrooniline juurdepääs andmetele ja IKT-süsteemidele peaks olema piiratud miinimumini, mida on vaja asjakohase teenuse osutamiseks.

Suunis 9. Füüsiline julgeolek

28. Kindlustusandjate füüsilise julgeoleku meetmed (nt kaitse elektrikatkestuste, tulekahju, veeavarii või loata füüsilise juurdepääsu eest) tuleks kindlaks määrata, dokumenteerida ja neid tuleks rakendada, et kaitsta ruume, andmekeskusi ja tundlikke piirkondi loata juurdepääsu ja keskkonnaohtude eest.

29. Füüsiline juurdepääs IKT-süsteemidele peaks olema lubatud ainult volitatud isikutele. Volitused peaksid olema määratud isiku ülesannete ja kohustuste järgi ning piirduma isikutega, kellel on asjakohane väljaõpe ja kelle üle on tagatud järelevalve. Füüsiline juurdepääs tuleks regulaarselt üle vaadata, tagamaks tarbetute juurdepääsuõiguste kohene tagasivõtmine/tühistamine.

30. Keskkonnaohtude eest kaitsmiseks mõeldud piisavad meetmed peaksid vastama hoonete olulisusele ning nendes hoonetes tehtavate toimingute või seal asuvate IKT-süsteemide kriitilisusele.

Suunis 10. IKT-tegevuse turvalisus

31. Kindlustusandjad peaksid rakendama IKT-süsteemide ja IKT-teenuste konfidentsiaalsuse, tervikluse ja kättesaadavuse tagamise korda, et vähendada vastavalt turbeküsimuste mõju IKT-teenuste osutamisele. See kord peaks asjakohastel puhkudel hõlmama järgmisi meetmeid:

a) võimalike nõrkuste väljaselgitamine, mida tuleks hinnata ja parandada, tagades IKT-süsteemide ajakohasuse, sh tarkvara, mille kindlustusandjad annavad oma sise- ja väliskasutajatele, kohaldades kriitilisi turvavärskendusi, sealhulgas viirusetõrje signatuuride uuendused, või rakendades kompenseerivaid kontrollimehhanisme;

b) turvaliste aluskonfiguratsioonide rakendamine kõikide kriitiliste komponentide puhul, nagu operatsioonisüsteemid, andmebaasid, ruuterid või kommutaatorid;

c) võrgu segmenteerimise, andmekao ennetussüsteemide ja võrguliikluse krüpteerimise rakendamine (vastavuses teabevara liigitusega);

d) lõppsõlmede, sealhulgas serverite, tööjaamade ja mobiilseadmete kaitse rakendamine. Kindlustusandjad peaksid hindama, kas lõppsõlm vastab nende määratud turbestandarditele, enne kui sellele antakse juurdepääs kindlustusandja võrgustikule;

e) selle tagamine, et on kasutusel tervikluse kontrollimise mehhanismid IKT-süsteemide tervikluse kontrollimiseks;

f) andmete krüpteerimine nii säilitamisel kui edastamisel (vastavuses teabevara liigitusega).

Suunis 11. Turvaseire

32. Kindlustusandjad peaksid kehtestama korra ja menetlused kindlustusandjate infoturvet mõjutavate tegevuste pidevaks seiramiseks ning neid rakendama. Seire peaks hõlmama vähemalt järgmist:

    a) sise- ja välistegureid, sealhulgas äri- ja IKT-haldustoiminguid;

    b) teenuseosutajate, muude üksuste ja sisekasutajate tehinguid ning

    c) võimalikke sise- ja välisohte.

33. Seire alusel peaksid kindlustusandjad rakendama asjakohaseid ja tõhusaid vahendeid anomaalsete tegevuste ja ohtude – nagu füüsiline või loogiline sekkumine, teabevara konfidentsiaalsuse, tervikluse ja kättesaadavuse rikkumine, tark- ja riistvara ründekood ja üldsusele teadaolevad nõrkused – tuvastamiseks, neist teatamiseks ja neile reageerimiseks.

34. Turbeseire aruanded peaksid aitama kindlustusandjatel mõista nii operatiiv- kui ka turvaintsidentide laadi, selgitada välja suundumusi ning toetada kindlustusandjate siseuurimisi ja võimaldada neil teha asjakohaseid otsuseid.

Suunis 12. Infoturbe ülevaatused, hindamine ja testimine

35. Kindlustusandjad peaksid tegema erinevaid infoturbe ülevaatuseid, hindamisi ja testimisi, et tagada oma IKT-süsteemide ja IKT-teenuste nõrkuste tõhus tuvastamine. Kindlustusandjad võivad näiteks võrrelda vajaduste analüüsiga teabes olevaid lünki infoturbe standarditega, teha nõuete täitmise kontrolle, infosüsteemide sise- ja välisauditeid või füüsilise turvalisuse kontrolle.

36. Kindlustusandjad peaksid kehtestama infoturbe testimise raamistiku, millega kinnitatakse nende infoturbemeetmete stabiilsust ja tõhusust, ja seda rakendama ning veenduma, et selles raamistikus arvestatakse ohtude seire ning IKT- ja turvariskide hindamise protsessi käigus tuvastatud ohtude ja nõrkustega.

37. Testima peaksid ohutul ja turvalisel viisil sõltumatud testijad, kellel on infoturbemeetmete testimise alal piisavad teadmised, oskused ja oskusteave.

38. Kindlustusandjad peaksid teste tegema regulaarselt. Testimise (nagu läbistustestimise, sealhulgas ohust lähtuva läbistustestimise) ulatus, sagedus ja meetod peaksid vastama tuvastatud riski tasemele. Kord aastas tuleks testida kriitilisi IKT-süsteeme ja teha nõrkuste kontrolle.

39. Kindlustusandjad peaksid tagama, et turvameetmete teste tehakse taristu, protsesside või korra muudatuste korral ja kui muudatusi tehakse oluliste operatiiv- või turvaintsidentide või uute või märkimisväärselt muudetud kriitiliste rakenduste avaldamise tõttu. Kindlustusandjad peaksid jälgima ja hindama turvatestide tulemusi ning ajakohastama nende alusel viivitusteta oma turvameetmeid kriitilise tähtsusega IKT-süsteemide korral.

Suunis 13. Infoturbekoolitus ja -teadlikkus

40. Kindlustusandjad peaksid kasutusele võtma infoturbekoolitusprogrammid kõikidele töötajatele, sealhulgas haldus-, juhtimis- või järelevalveorganile, et tagada töötajate koolitamine oma ülesannete ja kohustuste täitmiseks, et vähendada inimlikku eksimust, vargusi, pettusi, väärkasutust või kahju. Kindlustusandjad peaksid tagama koolitusprogrammi raames kõikide töötajate regulaarse koolitamise.

41. Kindlustusandjad peaksid kehtestama regulaarsed turvateadlikkuse programmid ja neid rakendama, et koolitada oma töötajaid (sealhulgas haldus-, juhtimis- või järelevalveorganit), kuidas käsitleda infoturbe riske.

Suunis 14. IKT-tegevuste juhtimine

42. Kindlustusandjad peaksid juhtima oma IKT-tegevusi IKT-strateegia alusel. Dokumentides tuleks määrata, kuidas kindlustusandjad IKT-süsteeme ja IKT-teenuseid käitavad, jälgivad ja kontrollivad, hõlmates kriitiliste IKT-protsesside, -menetluste ja -toimingute dokumenteerimist.

43. Kindlustusandjad peaksid kriitiliste IKT-tegevuste menetlusi logima ja jälgima, et võimaldada vigade tuvastamist, analüüsi ja parandamist.

44. Kindlustusandjad peaksid pidama oma IKT-varade kohta ajakohastatud registrit. IKT-varade register peaks olema piisavalt detailne, et võimaldada IKT-vara, selle asukohta, turvaliigitust ja kuuluvust kiirelt tuvastada.

45. Kindlustusandjad peaksid jälgima ja juhtima IKT-varade olelusringi tagamaks, et need vastavad jätkuvalt äri- ja riskijuhtimise nõuetele ning toetavad neid. Kindlustusandjad peaksid jälgima, et nende tarnijad või sisearendajad toetavad nende IKT-varasid ning et kõiki asjakohaseid paikasid ja värskendusi tehakse dokumenteeritud korra kohaselt. Vananenud või ilma toeta IKT-varadest tulenevaid riske tuleks hinnata ja leevendada. Kasutusest kõrvaldatud IKT-varad tuleks ohutult töödelda ja ära visata.

46. Kindlustusandjad peaksid rakendama tulemuslikkuse ja võime planeerimise ning seireprotsesse IKT-süsteemide oluliste toimimisprobleemide ja IKT-võimekuse puudujääkide ajakohaseks ennetamiseks, tuvastamiseks ja leevendamiseks.

47. Kindlustusandjad peaksid määrama kindlaks ja rakendama andme- ja IKT-süsteemide varundamise ja taastamise korra tagamaks, et neid saab vajaduse korral taastada. Varundamise ulatus ja sagedus tuleb panna paika äri taastamisnõuetest ning andme- ja IKT-süsteemide kriitilisusest lähtuvalt ning seda

tuleb hinnata kooskõlas tehtud riskihindamisega. Varundamise ja taaste korda tuleks regulaarselt testida.

48. Kindlustusandjad peaksid tagama varundatud andme- ja IKT-süsteemide säilitamise ühes või mitmes peamisest tegevuskohast erinevas kohas, mis on turvalised ja peamisest tegevuskohast samade riskide vältimiseks piisavalt kaugel.

Suunis 15. IKT-intsident ja probleemilahendus

49. Kindlustusandjad peaksid kehtestama intsidentide ja probleemide lahendamise korra ja seda rakendama, et jälgida ja logida operatiiv- ja turvaintsidente ning võimaldada katkestuste esinemisel kindlustusandjatel kriitiliste äritoimingute ja -protsessidega uuesti jätkata.

50. Kindlustusandjad peaksid kindlaks määrama asjakohased kriteeriumid ja läved (et liigitada sündmused operatiiv- või turvaintsidendiks), samuti varajase hoiatuse indikaatorid, mis peaksid toimima hoiatusteatena intsidentide varase tuvastamise võimaldamiseks.

51. Kahjulike sündmuste mõju minimeerimiseks ja kiire taastumise võimaldamiseks peaksid kindlustusandjad kehtestama nõuetekohase korra ja organisatsioonilised struktuurid, mis tagavad operatiiv- ja turvaintsidentide järjepideva ning integreeritud seire, käsitlemise ja järelmeetmete rakendamise, et tagada algpõhjuste tuvastamine ja kõrvaldamine ning see, et korduvate intsidentide esinemise ennetamiseks võetakse parandusmeetmed. Intsidendi- ja probleemijuhtimise korras tuleks kehtestada vähemalt järgmine:

    a) kord intsidentide tuvastamiseks, jälgimiseks, logimiseks, liigitamiseks ja prioriteetsuse alusel klassifitseerimiseks, lähtudes kindlustusandja määratletud prioriteedist ning tuginedes äri kriitilisusele ja teenuslepingutele;

    b) ülesanded ja kohustused erinevate intsidentide stsenaariumite jaoks (nt vead, talitlushäired, küberründed);

    c) probleemijuhtimise kord ühe või mitme intsidendi algpõhjuse tuvastamiseks, analüüsimiseks ja lahendamiseks – kindlustusandjad peaksid analüüsima operatiiv- või turvaintsidente, mis on tuvastatud või esinenud organisatsioonis ja/või sellest väljaspool, ning võtma arvesse nendest analüüsidest saadud peamisi õppetunde ja turvameetmeid vastavalt ajakohastama;

    d) tõhusad ettevõttesisesed kommunikatsiooniplaanid, sh intsidentidest teavitamine ja eskalatsioonimenetlused – mis hõlmavad ka klientidelt saabuvaid turvalisusega seotud kaebusi – tagamaks, et:

        i. asjaomast kõrgemat juhtkonda teavitatakse intsidentidest, mis võivad avaldada kriitilise tähtsusega IKT-süsteemidele ja IKT-teenustele väga kahjulikku mõju;

        ii. haldus-, juhtimis- või järelevalveorganit hoitakse vastavalt vajadusele kursis oluliste intsidentidega ning teda teavitatakse vähemalt intsidentide tõttu määratletud mõjust, vastumeetmest ja lisakontrollidest.

    e) intsidentidele reageerimise kord, millega leevendatakse intsidentidega seotud mõju ja tagatakse teenuse õigeaegne ja turvaline kasutus;

    f) konkreetsed väliskommunikatsiooniplaanid kriitiliste äritoimingute ja -protsesside jaoks, et:

i. teha intsidendile tõhusalt reageerimisel ja sellest taastumisel koostööd asjakohaste sidusrühmadega;

ii. anda välistele pooltele (nt klientidele, teistele turuosalistele, asjaomastele (järelevalve)asutusele) ajakohast teavet, sealhulgas intsidentidest ettekandmine (mis on kohaldatava määruse seisukohast nõuetekohane ja sellega kooskõlas).

Suunis 16. IKT-projektide juhtimine

52. Kindlustusandjad peaksid rakendama IKT-projektide metoodikat (sealhulgas sõltumatud turvanõudega seotud kaalutlused) koos asjakohase haldusprotsessi ja projekti rakendamise juhtimisega, et toetada tõhusalt IKT-strateegia rakendamist IKT-projektide kaudu.

53. Kindlustusandjad peaksid nõuetekohaselt jälgima ja leevendama oma IKT-projektide portfellist tulenevaid riske, arvestades ühtlasi riskidega, mis võivad tuleneda erinevate projektide omavahelistest seostest ja projektide sõltuvusest samadest ressurssidest ja/või oskusteabest.

Suunis 17. IKT-süsteemide omandamine ja arendamine

54. Kindlustusandjad peaksid välja töötama IKT-süsteemide omandamise, arendamise ja haldamise korra ning seda rakendama, et tagada igakülgselt töödeldavate andmete konfidentsiaalsus, terviklus ja kättesaadavus ning kindlaksmääratud kaitsenõuete täitmine. Korra kavandamisel tuleb lähtuda riskipõhisest lähenemisest.

55. Kindlustusandjad peaksid tagama, et enne süsteemi omandamist või arendamist määratakse selgelt kindlaks funktsionaalsed ja mittefunktsionaalsed nõuded (sealhulgas infoturbenõuded) ning tehnilised eesmärgid.

56. Kindlustusandjad peaksid tagama, et IKT-süsteemide tahtmatu muutmise või nendega tahtliku manipuleerimise ennetamiseks süsteemide arendamise käigus on kehtestatud meetmed.

57. Kindlustusandjatel peaks olema kehtestatud metodoloogia IKT-süsteemide, IKT-teenuste ja infoturbemeetmete testimiseks ja heakskiitmiseks.

58. Kindlustusandjad peaksid nõuetekohaselt testima IKT-süsteeme, IKT-teenuseid ja infoturbemeetmeid, et tuvastada turvalisuse võimalikke puudujääke, rikkumisi ja intsidente.

59. Kindlustusandjad peaksid tagama tootmiskeskkondade lahutamise arendus-, test- ja muudest tootmisega mitteseotud keskkondadest.

60. Kindlustusandjad peaksid rakendama meetmeid IKT-süsteemide lähtekoodi (kui see on kättesaadav) tervikluse kaitseks. Lisaks peaksid nad põhjalikult dokumenteerima IKT-süsteemide arendamist, rakendamist, käitamist ja/või seadistamist, et vähendada tarbetut sõltuvust valdkonnaekspertidest.

61. Kindlustusandjate IKT-süsteemide soetamise ja arendamise kord peaks ühtlasi kehtima IKT-süsteemidele, mida arendavad või juhivad IKT-organisatsiooni välised äritoimingu lõppkasutajad (nt äriühingute hallatavad rakendused või lõppkasutaja andmetöötlusrakendused), kasutades riskipõhist lähenemist. Kindlustusandjad peaksid pidama kriitilise tähtsusega äritoiminguid või -protsesse toetavate rakenduste registrit.

Suunis 18. IKT-muutuste juhtimine

62. Kindlustusandjad peaksid kehtestama IKT-muutuste juhtimise korra ja seda rakendama tagamaks, et kõik IKT-süsteemide muudatused salvestatakse ja kiidetakse heaks ning neid hinnatakse, testitakse, lubatakse ja rakendatakse kontrollitud viisil. Kiirete või hädaolukorras tehtud IKT-muudatuste ajal tehtud muudatused peaksid olema jälgitavad ja neist tuleks muudatuse tegemise järel teatada järelanalüüsi tarvis asjaomasele varaomanikule.

63. Kindlustusandjad peaksid välja selgitama, kas nende tegevuskeskkonna muutused mõjutavad olemasolevaid turvameetmeid või kas on kaasnevate riskide leevendamiseks vaja võtta täiendavaid meetmeid. Need muudatused peaksid olema vastavuses kindlustusandjate ametliku muutuste juhtimise korraga.

Suunis 19. Talitluspidevuse juhtimine

64. Kindlustusandjate üldise talitluspidevuspoliitika osana vastutab haldus-, juhtimis- või järelevalveorgan kindlustusandjate IKT talitluspidevuspoliitika määratlemise ja heakskiitmise eest. IKT talitluspidevuse poliitika peaks kindlustusandja tegema ettevõttesiseselt nõuetekohaselt teatavaks ning seda tuleks kohaldada kõikide asjaomaste töötajate ja asjakohastel puhkudel teenuseosutajate suhtes.

Suunis 20. Tegevuse mõju analüüs

65. Usaldusväärse talitluspidevuse juhtimise osana peaksid kindlustusandjad tegevuse mõju analüüsima, et hinnata kvantitatiivselt ja kvalitatiivselt kindlustusandja kokkupuudet äritegevuse suurte häirete ja nende võimaliku mõjuga, kasutades sise- ja/või välisandmete ja stsenaariumi analüüsi. Tegevuse mõju analüüsis tuleks ka arvesse võtta tuvastatud ja liigitatud äriprotsesside ja -tegevuste, äritoimingute, ülesannete ja varade (nt teabevara ja IKT-vara) kriitilisust ning nende vastastikust sõltuvust kooskõlas suunisega 4.

66. Kindlustusandjad peaksid tagama, et nende IKT-süsteeme ja IKT-teenuseid kavandatakse tegevuse mõju analüüsi kohaselt ja kooskõlastatakse sellega, näiteks teatud kriitilise tähtsusega komponentide liiasuse puhul, et ennetada neid komponente mõjutavate sündmuste põhjustatud häireid.

Suunis 21. Talitluspidevuse kavandamine

67. Kindlustusandjate üldistes talitluspidevuse kavades tuleks arvesse võtta olulisi riske, mis võivad IKT-süsteeme ja IKT-teenuseid kahjustada. Kavades tuleks toetada eesmärki kaitsta kindlustusandjate äriprotsesside ja -tegevuste, ärifunktsioonide, rollide ja vara (nt teabevara ja IKT-vara) konfidentsiaalsust, terviklust ja kättesaadavust ning need vajaduse korral taastada. Kindlustusandjad peaksid asjakohastel puhkudel kavade kehtestamist asjakohaste siseste ja väliste sidusrühmadega kavade koostamise ajal kooskõlastama.

68. Kindlustusandjad peaksid kehtestama talitluspidevuse kavad, et reageerida ettenähtud taastumisaja (maksimumaeg, mille jooksul tuleb süsteem või protsess pärast intsidenti taastada) ja ettenähtud taastekünnise (maksimumaeg, mille jooksul andmed võivad varem määratletud teenusetaseme intsidendi jooksul kaotsi minna) raames asjakohaselt võimalikele rikkestsenaariumidele.

69. Kindlustusandjad peaksid talitluspidevuskavade puhul kaaluma mitut eri stsenaariumi, sealhulgas äärmuslikke, kuid teostatavaid stsenaariume ja küberründe stsenaariume, ning hindama selliste stsenaariumide võimalikku mõju.

Nende stsenaariumide põhjal peaksid kindlustusandjad kirjeldama, kuidas tagatakse IKT-süsteemide ja -teenuste pidevus ning ka kindlustusandjate infoturve.

Suunis 22. Reageerimis- ja taastekavad

70. Kindlustusandjad peaksid tegevuse mõju analüüsi ja teostatavate stsenaariumide alusel töötama välja reageerimis- ja taastekavad. Nendes kavades tuleb täpsustada kavade käivitamise tingimused ja meetmed, mis tuleb võtta vähemalt kindlustusandjate kriitilise tähtsusega IKT-süsteemide, IKT-teenuste ja andmete tervikluse, kättesaadavuse, talitluspidevuse ja taastamise tagamiseks. Reageerimis- ja taastekavade eesmärk peaks olema kindlustusandjate tegevuste taaste-eesmärkide täitmine.

71. Reageerimis- ja taastekavades tuleks arvestada nii lühi- kui ka (vajaduse korral) pikaajaliste taastetegevustega. Vähemalt tuleks kavade puhul teha järgmist:

    a) keskenduda neis oluliste IKT-teenuste toimingute, ärifunktsioonide, tugiprotsesside, teabevarade ja nende vastastikuse sõltuvuse taastamisele, et vältida kahjulikku mõju kindlustusandja tegevusele;

    b) need dokumenteerida ning teha äri- ja tugiüksustele teatavaks ja kergesti kättesaadavaks hädaolukorras (sealhulgas määratleda selgesti ülesanded ja kohustused) ning

    c) neid pidevalt ajakohastada intsidentide, testide, hiljuti tuvastatud riskide ja ohtude põhjal saadud kogemuste ning muudetud taastamiseesmärkide ja prioriteetide alusel.

72. Kavades tuleks arvestada ka alternatiivsete võimalustega, kus taastamine pole kulu, riskide, logistika või ettenägematute asjaolude tõttu lähiajal teostatav.

73. Reageerimis- ja taastekavade osana peaksid kindlustusandjad kaaluma ja rakendama talitluspidevuse meetmeid tõrgete leevendamiseks teenuseosutajate puhul, kes on kindlustusandjate IKT-teenuste talitluspidevuse jaoks väga olulised (kooskõlas EIOPA juhtimissüsteemi suuniste ja EIOPA suunistega pilveteenuse osutajatega alltöövõtulepingute sõlmimise kohta sätetega).

Suunis 23. Kavade testimine

74. Kindlustusandjad peaksid oma talitluspidevuse kavasid testima ning tagama oma kriitiliste protsesside ja toimingute, ärifunktsioonide, ülesannete ja varade (nt teabevarad), samuti IKT-varade ja nende vastastikuse sõltuvuse (sealhulgas teenuseosutajate pakutu) regulaarse testimise kindlustusandja riskiprofiili alusel.

75. Talitluspidevuse kavasid tuleks regulaarselt testimistulemuste, ohte käsitleva värske luureteabe ja varasematest sündmustest saadud õppetundide alusel ajakohastada. Samuti tuleks kaasata kõik asjaomased taastamiseesmärkide (sealhulgas ettenähtud taastumisaja ja ettenähtud taastekünnise) muutused ja/või äriprotsesside ja tegevuste, ärifunktsioonide, ülesannete ja varade (nt teabevarad ja IKT-varad) muutused.

76. Talitluspidevuse kavade testimine peaks näitama, et nende abil on võimalik säilitada äritegevuse toimimine kuni kriitiliste toimingute taastamiseni varem määratletud teenusetasemel või lubatud kõrvalekalde piires.

77. Testi tulemusi tuleb dokumenteerida ning testidest tulenevaid tuvastatud puudujääke tuleb analüüsida, nendega tegeleda ning haldus-, juhtimis- või järelevalveorganit neist teavitada.

Suunis 24. Teabevahetus kriisiolukorras

78. Tegevuste katkestuse korral või hädaolukorras ning talitluspidevuse kavade rakendamisel peaksid kindlustusandjad tagama, et neil oleksid olemas tõhusad meetmed teabe vahetamiseks kriisiolukorras, et kõik sisesed ja välised sidusrühmad (sealhulgas asjaomased järelevalveasutused, kui riigi õigusaktidega seda nõutakse, ning asjakohased teenuseosutaja) saaksid teavet õigeaegselt ja asjakohasel viisil.

Suunis 25. IKT-teenuste ja IKT-süsteemide allhanked

79. Ilma et see piiraks EIOPA suuniste pilveteenuse osutajatega alltöövõtulepingute sõlmimise kohta kohaldamist peaksid kindlustusandjad tagama, et IKT-teenuste ja IKT-süsteemide allhangete korral täidetakse IKT-teenuse või IKT-süsteemi asjaomaseid nõudeid.

80. Kriitiliste või oluliste funktsioonide allhanke korral peaksid kindlustusandjad tagama, et teenuseosutaja lepingulised kohustused (nt leping, teenusetaseme kokkulepped, asjaomaste lepingute lõpetamise sätted) sisaldavad vähemalt järgmist:

    a) asjakohaseid ja proportsionaalseid infoturbe eesmärke ja meetmeid, sealhulgas selliseid nõudeid nagu näiteks minimaalse infoturbe nõuded, kindlustusandjate andmete olelusringi, auditi ja juurdepääsuõiguste kirjeldust ning andmekeskuste mis tahes asukohanõudeid ja krüpteerimisnõudeid, võrguturbe ja turbeseire korda;

    b) teenusetaseme kokkuleppeid, et tagada IKT-teenuste ja IKT-süsteemide talitluspidevus ning tulemuseesmärgid tavaolukorras, samuti hädaolukorra lahendamise plaaniga hõlmatud kokkuleppeid teenuse katkemise korral ning

    c) operatiiv- ja turvariskide juhtimise korda, sh teavitamine ja aruandlus.

81. Teenuseosutajad peaksid jälgima ja veenduma, kuidas ja mis tasemel järgivad sellised teenuseosutajad neid turvaeesmärke, -meetmeid ja tulemuseesmärke.

Järgimis- ja aruandlusnõuded

82. Käesolev dokument sisaldab määruse (EL) nr 1094/2010 artikli 16 kohaselt väljaantud suuniseid. Selle määruse artikli 16 lõike 3 kohaselt on pädevad asutused ja kindlustusandjad kohustatud võtma mis tahes meetmeid, et kõnealuseid suuniseid ja soovitusi järgida.

83. Pädevad asutused, kes käesolevaid suuniseid järgivad või kavatsevad hakata neid järgima, peaksid lisama need asjakohasel viisil oma reguleerimis- või järelevalveraamistikku.

84. Pädevad asutused peavad kinnitama EIOPA-le, kas nad järgivad või kavatsevad hakata järgima käesolevaid suuniseid, ning esitama mittejärgimise põhjused kahe kuu jooksul pärast tõlgete avaldamist.

85. Kui osutatud tähtajaks ei vastata, peetakse pädevaid asutusi aruandlusnõudeid mittetäitvaks ja nendest teatatakse.

Läbivaatamise lõppsäte

86. Käesolevad suunised vaatab läbi EIOPA.