EIOPA-BoS-19/600

Informacinių ir ryšių technologijų saugumo ir valdymo gairės

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurtas – Vokietija- Tel. + 49 69-951119-20;
faks. + 49 69-951119-19; e. paštas info@eiopa.europa.eu; interneto svetainė www.eiopa.europa.eu

Turinys

Bendra informacija **3**
Įžanga **6**
Sąvokų apibrėžtys 6
1 gairė. Proporcingumas 8
2 gairė. IRT valdymo sistemoje 8
3 gairė. IRT strategija 9
4 gairė. IRT ir saugumo rizika rizikos valdymo sistemoje 9
5 gairė. Auditas 10
6 gairė. Informacijos saugumo politika ir priemonės 10
7 gairė. Informacijos saugumo pareigūno pareigybė 10
8 gairė. Loginis saugumas 11
9 gairė. Fizinis saugumas 12
10 gairė. IRT operacijų saugumas 12
11 gairė. Saugumo stebėsena 13
12 gairė. Informacijos saugumo peržiūra, vertinimai ir testavimas 13
13 gairė. Mokymas ir informuotumas informacijos saugumo klausimais 14
14 gairė. IRT operacijų valdymas 14
15 gairė. IRT incidentų ir problemų valdymas 15
16 gairė. IRT projektų valdymas 16
17 gairė. IRT sistemų įsigijimas ir kūrimas 16
18 gairė. IRT pokyčių valdymas 16
19 gairė. Veiklos tęstinumo valdymas 17
20 gairė. Poveikio veiklai analizė 17
21 gairė. Veiklos tęstinumo planavimas 17
22 gairė. Reagavimo ir atkūrimo planai 17
23 gairė. Planų testavimas 18
24 gairė. Ryšiai krizės sąlygomis 18
25 gairė. IRT paslaugų ir IRT sistemų užsakomosios paslaugos 18
Atitiktis ir pranešimo taisyklės **20**
Baigiamoji nuostata dėl peržiūrėjimo **20**

Bendra informacija

1. Pagal Reglamento (ES) Nr. 1094/2010 16 straipsnį, siekdama nustatyti nuoseklią, veiksmingą ir efektyvią priežiūros praktiką ir užtikrinti bendrą, vienodą ir nuoseklų Sąjungos teisės taikymą, EIOPA gali skelbti kompetentingoms institucijoms ar finansų įstaigoms skirtas gaires ir rekomendacijas.

2. Vadovaudamosi minėto reglamento 16 straipsnio 3 dalimi, kompetentingos institucijos ir finansų įstaigos turi dėti visas pastangas, kad laikytųsi gairių ir rekomendacijų.

3. EIOPA nusprendė, kad būtina parengti konkrečias gaires dėl informacinių ir ryšių technologijų (IRT) saugumo ir valdymo pagal Direktyvos 2009/138/EB 41 ir 44 straipsnius, atsižvelgiant į analizę, atliktą atsakant į Europos Komisijos „FinTech" srities veiksmų planą (COM(2018) 0109 final) bei 2018–2019 m. EIOPA priežiūros konvergencijos planą[1] ir pasitarus su keliomis kitomis suinteresuotosiomis šalimis[2].

4. Kaip nurodyta Europos priežiūros institucijų bendroje rekomendacijoje Europos Komisijai, EIOPA valdymo sistemos gairės *„tinkamai neatspindi IRT rizikos (įskaitant kibernetinę riziką) valdymo priežiūros svarbos"*. Nėra gairių dėl gyvybiškai svarbių elementų, kurie visuotinai pripažįstami kaip tinkamo IRT saugumo ir valdymo dalis".

5. Atlikus dabartinės (teisėkūros) padėties ES analizę rengiant minėtą bendrą rekomendaciją, paaiškėjo, kad dauguma ES valstybių narių yra nustačiusios nacionalines IRT saugumo ir valdymo taisykles. Nors reikalavimai yra panašūs, reguliavimo sistema vis dar yra nevienoda. Be to, dabartinės priežiūros praktikos tyrimas atskleidė didelę praktikos įvairovę – nuo „jokios specialios priežiūros" iki „griežtos priežiūros" (įskaitant „patikrinimus ne vietoje" ir „patikrinimus vietoje").

6. Be to, IRT tampa vis sudėtingesnės, daugėja su IRT susijusių incidentų (įskaitant kibernetinius incidentus), auga neigiamas tokių incidentų poveikis įmonių veiklai. Dėl šios priežasties IRT ir saugumo rizikos valdymas yra labai svarbus įmonei siekiant strateginių, korporatyvinių, veiklos ir reputacijos tikslų.

7. Be to, visame draudimo sektoriuje, įskaitant tradicinius ir novatoriškus verslo modelius, vis labiau kliaujamasi IRT teikiant draudimo paslaugas ir užtikrinant įprastą įmonių veiklą, pvz., draudimo sektoriaus skaitmeninimas („InsurTech", daiktų internetas ir t. t.), taip pat telekomunikacijų kanalų (interneto, judriojo ir belaidžio ryšio ir plačiajuosčių tinklų) tarpusavio sąsajos. Dėl to įmonių veikla tampa pažeidžiama dėl saugumo incidentų, įskaitant kibernetines atakas. Todėl svarbu užtikrinti, kad įmonės būtų tinkamai pasirengusios valdyti savo IRT ir saugumo riziką.

8. Be to, pripažįstant pasirengimo kibernetinei rizikai [3] ir patikimos kibernetinio saugumo sistemos poreikį, šiose gairėse kibernetinis saugumas taip pat nagrinėjamas kaip įmonės informacijos saugumo priemonių dalis. Nors šiose gairėse pripažįstama, kad kibernetinis saugumas turėtų būti įtrauktas į bendrą įmonės grėsmių IRT ir saugumui valdymą, svarbu pabrėžti, kad kibernetinės atakos turi tam tikrų specifinių savybių, į kurias reikėtų atsižvelgti siekiant

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

[2] Ataskaitą, kurią EIOPA paskelbė kaip atsakymą į Europos Komisijos „FinTech" veiksmų planą, galima rasti čia.

[3] Kibernetinė rizika apibrėžta Finansinio stabilumo tarybos 2018 m. lapkričio 12 d. leidinyje „Cyber Lexicon" https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

užtikrinti, kad informacijos saugumo priemonės tinkamai sumažintų kibernetinę riziką:

a) kibernetines atakas dažnai yra sunkiau valdyti (t. y. jas nustatyti, nuo jų apsisaugoti, jas aptikti, į jas reaguoti ir visiškai po jų atsigauti) nei daugumą kitų IRT ir saugumo rizikos šaltinių, taip pat sunku nustatyti žalos mastą;

b) kai kurios kibernetinės atakos gali paversti bendro rizikos valdymo ir veiklos tęstinumo tvarką, taip pat veiklos atkūrimo procedūras neveiksmingomis, nes jos gali paskleisti kenkėjiškas programas atsarginėse sistemose, kad jos taptų neprieinamos, arba sugadinti atsarginės kopijos duomenis;

c) kibernetinės atakos gali būti vykdomos per paslaugų teikėjus, brokerius, patikėtinius (valdymo patikėtinius) ir tarpininkus. Greitai plintančios tyliosios grėsmės gali patekti į įmonės IRT sistemą panaudojant tarpusavio ryšius per trečiųjų šalių telekomunikacijų jungtis. Todėl susieta įmonė, kuri pati nėra labai reikšminga, gali tapti pažeidžiama ir rizikos plitimo šaltiniu ir turėti sisteminį poveikį. Laikantis silpniausios grandies principo, kibernetinis saugumas turėtų rūpėti ne tik pagrindiniams rinkos dalyviams ar kritinių paslaugų teikėjams.

9. Šiomis gairėmis siekiama:

a) aiškiau ir skaidriau rinkos dalyviams paaiškinti apie būtiniausią pageidaujamą informacijos ir kibernetinio saugumo pajėgumą, t. y. bazinį saugumo lygį;

b) išvengti galimo reglamentavimo arbitražo;

c) skatinti priežiūros konvergenciją, susijusią su lūkesčiais ir procesais, taikomais IRT saugumo ir valdymo srityje, nes tai raktas į tinkamą IRT ir saugumo rizikos valdymą.

Informacinių ir ryšių technologijų saugumo ir valdymo gairės

Įžanga

1. Pagal Reglamento (ES) Nr. 1094/2010[4] 16 straipsnį EIOPA rengia šias priežiūros institucijoms skirtas gaires, kuriose draudimo ir perdraudimo įmonėms (toliau kartu – „įmonės“) pateikiamos rekomendacijos, kaip reikia taikyti Direktyvoje 2009/138/EB[5] (toliau – direktyva „Mokumas II“) ir Komisijos deleguotajame reglamente (ES) Nr. 2015/35[6] (toliau – deleguotasis reglamentas) nustatytus valdymo reikalavimus informacinių ir ryšių technologijų (toliau – IRT) saugumo ir valdymo srityje. Tuo tikslu šios gairės grindžiamos valdymo nuostatomis, išdėstytomis direktyvos „Mokumas II“ 41, 44, 46, 47, 132 ir 246 straipsniuose ir deleguotojo reglamento 258–260, 266, 268–271 ir 274 straipsniuose. Be to, šios gairės taip pat grindžiamos gairėmis, pateiktomis EIOPA valdymo sistemos gairėse (EIOPA-BoS-14/253)[7] ir EIOPA debesijos paslaugų teikėjų užsakomųjų paslaugų gairėse (EIOPA-BoS-19/270)[8].
2. Gairės taikomos ir pavienėms įmonėms, ir, *mutatis mutandis*, įmonių grupėms[9].
3. Kompetentingos institucijos, laikydamosi šių gairių arba prižiūrėdamos, kaip jų laikomasi, turėtų atsižvelgti į proporcingumo principą[10], kuris turėtų užtikrinti, kad valdymo tvarka, įskaitant su IRT saugumu ir valdymu susijusią tvarką, būtų taikoma atsižvelgiant į atitinkamos rizikos, su kuria susiduria arba gali susidurti įmonės, pobūdį, mastą ir sudėtingumą.
4. Šios gairės turėtų būti aiškinamos kartu su direktyva „Mokumas II“, deleguotuoju reglamentu, EIOPA valdymo sistemos gairėmis ir EIOPA naudojimosi užsakomosiomis paslaugomis, kurias teikia debesijos paslaugų teikėjai, gairėmis ir jų nepažeidžiant. Šios gairės turėtų būti neutralios technologijų ir metodikos požiūriu.

Sąvokų apibrėžtys

5. Šiose gairėse neapibrėžtos sąvokos turi būti suprantamos taip, kaip jos apibrėžtos direktyvoje „Mokumas II“.
6. Šiose gairėse taikomos šios sąvokų apibrėžtys:

[4] 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1094/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos draudimo ir profesinių pensijų institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/79/EB (OL L 331, 2010 12 15, p. 48).

[5] 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/138/EB dėl draudimo ir perdraudimo veiklos pradėjimo ir jos vykdymo (Mokumas II) (OL L 335, 2019 12 17, p. 1).

[6] 2014 m. spalio 10 d. Komisijos deleguotasis reglamentas (ES) 2015/35, kuriuo papildoma Europos Parlamento ir Tarybos direktyva 2009/138/EB dėl draudimo ir perdraudimo veiklos pradėjimo ir jos vykdymo (Mokumas II), (OL L 12, 2015 1 17, p. 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] Direktyvos 2009/138/EB 212 straipsnio 1 dalis.

[10] Direktyvos 2009/138/EB 29 straipsnio 3 dalis.

Išteklių savininkas	Asmuo arba subjektas, kuriam priskirta atsakomybė bei įgaliojimai informacinių ir IRT išteklių atžvilgiu.
Prieinamumas	Tokia ypatybė, kuri sudaro galimybę įgaliotam subjektui pasiekti ir naudoti išteklius pagal pareikalavimą (iškart).
Konfidencialumas	Tokia ypatybė, kuri informacijos nepadaro prieinama ir neatskleidžiama leidimo neturintiems asmenims, subjektams, procesams ar sistemoms.
Kibernetinė ataka	Bet kokios rūšies į IRT nukreiptas įsilaužimas, agresyviais (kenkėjiškais) veiksmais bandant sunaikinti, atskleisti, pakeisti, sugadinti, pavogti ar neteisėtai panaudoti informacinius išteklius arba neteisėtai įgyti prieigą prie jų.
Kibernetinis saugumas	Informacijos ir (arba) informacinių sistemų konfidencialumo, vientisumo ir prieinamumo išsaugojimas naudojant kibernetinę terpę.
IRT ištekliai	Programinė arba aparatinė įranga, naudojama verslo aplinkoje.
IRT projektai	Bet koks projektas (arba jo dalis), kurį vykdant keičiamos, pakeičiamos arba įgyvendinamos IRT sistemos ir paslaugos.
IRT ir saugumo rizika	Operacinės rizikos smulkusis komponentas; rizika patirti nuostolių dėl konfidencialumo pažeidimo, sistemų ir duomenų nevientisumo, sistemų ir duomenų netinkamumo ar jų nebuvimo arba dėl nesugebėjimo per pagrįstą laiką pakeisti IRT, kai pasikeičia aplinka ar verslo poreikiai (t. y. operatyvumas). Tai apima kibernetinę riziką bei informacijos saugumo riziką, kylančią dėl netinkamų ar nevykusių vidaus procesų arba išorės įvykių, įskaitant kibernetines atakas arba nepakankamą fizinį saugumą.
Informacijos saugumas	Informacijos ir (arba) informacinių sistemų konfidencialumo, vientisumo ir prieinamumo išsaugojimas. Be to, gali būti įtrauktos ir kitos ypatybės, pvz., autentiškumas, atskaitomybė, atsakomybės prisiėmimas ir patikimumas.
IRT paslaugos	Per IRT sistemas ir paslaugų teikėjus vienam ar keliems vidaus arba išorės naudotojams teikiamos paslaugos.

IRT sistemos	Taikomųjų programų, paslaugų, informacinių technologijų išteklių, IRT išteklių ar kitų informacijos tvarkymo komponentų rinkinys, apimantis ir veiklos aplinką.
Informaciniai ištekliai	Materialūs ar nematerialūs informacijos rinkiniai, kuriuos verta apsaugoti.
Vientisumas	Tikslumo ir išsamumo ypatybė.
Operacinis ar saugumo incidentas	Pavienis įvykis arba tarpusavyje susiję nenumatyti įvykiai, kurie turi arba, tikėtina, turės neigiamą poveikį IRT sistemų ir paslaugų vientisumui, prieinamumui ir konfidencialumui.
Paslaugų teikėjas	Tai trečioji šalis, kuri pagal užsakomųjų paslaugų susitarimą vykdo procesą (arba jo dalį), teikia paslaugas (arba jų dalį) arba vykdo veiklą (arba jos dalį).
Grėsmėmis grindžiamas įsiskverbimų testavimas	Kontroliuojamas bandymas pakenkti subjekto kibernetiniam atsparumui imituojant tikrovišką grėsmes keliančių subjektų taktiką, metodus ir procedūras. Bandymas pagrįstas konkrečia informacija apie grėsmes, ir pagrindinis dėmesys skiriamas subjekto žmonėms, procesams ir technologijoms, o išankstinės žinios ir poveikis veiklai – minimalus.
Pažeidžiamumas	Išteklių ar kontrolės silpnoji vieta, jautrumas ar trūkumas, kuriuo gali būti pasinaudota vienai ar kelioms grėsmėms sukelti.

7. Šios gairės taikomos nuo 2021 m. liepos 1 d.

1 gairė. Proporcingumas

8. Įmonės turėtų taikyti šias gaires atsižvelgdamos į jų verslui būdingos rizikos pobūdį, mastą ir sudėtingumą.

2 gairė. IRT valdymo sistemoje

9. Administracinis, valdymo arba priežiūros organas (AVPO) turėtų užtikrinti, kad įmonių valdymo sistemoje, visų pirma rizikos valdymo ir vidaus kontrolės sistemoje, būtų tinkamai valdoma įmonių IRT ir saugumo rizika.

10. AVPO turėtų užtikrinti, kad įmonių darbuotojų skaičius ir įgūdžiai nuolat atitiktų jų IRT veiklos poreikius bei IRT ir saugumo rizikos valdymo procesus ir būtų pakankami IRT strategijai įgyvendinti. Be to, darbuotojams turėtų būti reguliariai rengiami tinkami mokymai IRT ir saugumo rizikos temomis, įskaitant informacijos saugumą, kaip nustatyta 13 gairėje.

11. AVPO turėtų užtikrinti pakankamus išteklius pirmiau nurodytiems reikalavimams įgyvendinti.

3 gairė. IRT strategija

12. AVPO yra bendrai atsakinga už rašytinės įmonių IRT strategijos, kuri yra jų bendros verslo strategijos dalis ir suderinta su ja, nustatymą ir patvirtinimą, taip pat už jos komunikacijos ir įgyvendinimo priežiūrą.

13. IRT strategijoje turėtų būti apibrėžti bent šie dalykai:

    a) kaip turėtų būti plėtojamos įmonių IRT siekiant veiksmingai remti ir įgyvendinti jų verslo strategiją, įskaitant organizacinės struktūros, verslo modelių, IRT sistemos ir pagrindinių tarpusavio priklausomybės ryšių su paslaugų teikėjais raidą;

    b) IRT architektūros, įskaitant priklausomybę nuo paslaugų teikėjų, raida;

    c) aiškūs informacijos saugumo tikslai, sutelkiant dėmesį į IRT sistemas ir paslaugas, darbuotojus ir procesus.

14. Įmonės turėtų užtikrinti, kad IRT strategija būtų laiku įgyvendinta, priimta ir apie ją pranešta visiems susijusiems darbuotojams ir paslaugų teikėjams, jei taikoma ir tinkama.

15. Įmonės taip pat turėtų parengti savo IRT strategijos veiksmingumo ir įgyvendinimo stebėsenos bei vertinimo procesus. Šis procesas turėtų būti reguliariai peržiūrimas ir atnaujinamas.

4 gairė. IRT ir saugumo rizika rizikos valdymo sistemoje

16. AVPO tenka bendra atsakomybė sukurti veiksmingą IRT ir saugumo rizikos valdymo sistemą, kuri būtų įmonės bendros rizikos valdymo sistemos dalis. Tai apima priimtinos rizikos nustatymą šios rizikos atžvilgiu pagal įmonės rizikos strategiją ir reguliarią rašytinę ataskaitą apie rizikos valdymo proceso rezultatus, skirtą AVPO.

17. Rengdamos bendrą rizikos valdymo sistemą, įmonės IRT ir saugumo rizikos atžvilgiu (apibrėždamos toliau aprašytus IRT apsaugos reikalavimus) turėtų įtraukti bent šiuos elementus:

    a) įmonės turėtų sudaryti ir reguliariai atnaujinti savo verslo procesų ir veiklos, veiklos funkcijų, vaidmenų ir išteklių (pvz., informacinių ir IRT išteklių) planus, kad nustatytų jų svarbą ir tarpusavio priklausomybės ryšius su IRT ir saugumo rizika;

    b) įmonės turėtų nustatyti ir vertinti visą susijusią IRT ir saugumo riziką, su kuria jos susiduria, ir suklasifikuoti nustatytus verslo procesus ir veiklą, veiklos funkcijas, vaidmenis ir išteklius (pvz., informacinius ir IRT išteklius) pagal svarbą. Įmonės taip pat turėtų įvertinti apsaugos reikalavimus, susijusius su bent tų verslo procesų ir veiklos konfidencialumu, vientisumu ir prieinamumu, veiklos funkcijomis, vaidmenimis ir ištekliais (pvz., informaciniais ir IRT ištekliais). Turėtų būti nurodyti išteklių savininkai, atsakingi už išteklių klasifikavimą;

    c) metodai, skirti reikalingos apsaugos svarbai ir lygmeniui nustatyti, ypač atsižvelgiant į apsaugos tikslus, susijusius su vientisumu, prieinamumu ir konfidencialumu, turėtų užtikrinti, kad nustatomi apsaugos reikalavimai būtų nuoseklūs ir išsamūs;

d) IRT ir saugumo rizika turėtų būti vertinama remiantis apibrėžtais IRT ir saugumo rizikos kriterijais, atsižvelgiant į jų verslo procesų ir veiklos svarbą, verslo funkcijas, vaidmenis ir išteklius (pvz., informacinius ir IRT išteklius), nustatyto pažeidžiamumo ir ankstesnių įmonę paveikusių incidentų mastą;

e) IRT ir saugumo rizikos vertinimas turėtų būti atliekamas ir dokumentuojamas reguliariai. Šis vertinimas taip pat turėtų būti atliekamas prieš bet kokius esminius infrastruktūros, procesų ar procedūrų, turinčių įtakos verslo procesams ir veiklai, veiklos funkcijoms, vaidmenims ir ištekliams (pvz., informaciniams ir IRT ištekliams), pokyčius;

f) remdamosi savo rizikos vertinimu, įmonės turėtų bent apibrėžti ir įgyvendinti nustatytos IRT ir saugumo rizikos mažinimo ir informacinių išteklių apsaugos priemones pagal jų klasifikavimą. Tai turėtų apimti likutinės rizikos valdymo priemonių apibrėžimą.

18. IRT ir saugumo rizikos valdymo rezultatus turėtų patvirtinti AVPO ir jie turėtų būti įtraukti į operacinės rizikos valdymo procesą kaip įmonės bendro rizikos valdymo dalis.

5 gairė. Auditas

19. Įmonių valdymo, sistemų ir procesų, susijusių su IRT ir saugumo rizika, auditą pagal įmonių audito planą[11] turėtų periodiškai atlikti auditoriai, turintys pakankamai žinių, įgūdžių ir patirties IRT ir saugumo rizikos srityje, kad galėtų nepriklausomai užtikrinti savo veiksmingumą AVPO. Tokio audito dažnis ir sritis turėtų būtų proporcingi atitinkamai IRT ir saugumo rizikai.

6 gairė. Informacijos saugumo politika ir priemonės

20. Įmonės turėtų nustatyti AVPO patvirtintą rašytinę informacijos saugumo politiką, kurioje turėtų būti apibrėžti aukšto lygio principai ir taisyklės įmonių informacijos konfidencialumui, vientisumui ir prieinamumui apsaugoti, siekiant paremti IRT strategijos įgyvendinimą.

21. Į politiką reikėtų įtraukti pagrindinių informacijos saugumo valdymo srities funkcijų ir pareigų aprašymą, joje reikėtų nustatyti saugumo reikalavimus darbuotojams, procesams bei technologijai, pažymint, kad už įmonių informacijos saugumą atsako visų lygmenų darbuotojai.

22. Apie politiką turėtų būti pranešta pačioje įmonėje ir ji turėtų būti taikoma visiems darbuotojams. Kai taikytina ir svarbu, apie informacijos saugumo politiką arba jos dalis turėtų būti pranešta ir paslaugų teikėjams ir jos turėtų būti jiems taikomos.

23. Remdamosi šia politika, įmonės turėtų nustatyti ir įgyvendinti konkretesnes informacijos saugumo procedūras ir informacijos saugumo priemones, kad, *inter alia*, sumažintų joms kylančią IRT ir saugumo riziką. Šios procedūros ir informacijos saugumo priemonės turėtų apimti visus šiose gairėse aprašytus procesus, kai taikytina.

7 gairė. Informacijos saugumo pareigūno pareigybė

24. Įmonės savo valdymo sistemoje ir laikydamosi proporcingumo principo turėtų įsteigti informacijos saugumo pareigūno pareigybę ir paskirti asmenį vykdyti šias pareigas. Įmonė turėtų užtikrinti informacijos saugumo pareigūno

[11] Deleguotojo reglamento 271 straipsnis.

nepriklausomumą ir objektyvumą, tinkamai atribodamos jį nuo IRT plėtros ir veiklos procesų. Pareigūnas turėtų būti atskaitingas AVPO.

25. Informacijos saugumo pareigūno užduotys paprastai yra šios:

    a) padėti AVPO nustatyti ir vykdyti įmonių informacijos saugumo politiką ir kontroliuoti jos įgyvendinimą;

    b) reguliariai ir *ad hoc* pagrindu pranešti ir konsultuoti AVPO apie informacijos saugumo būklę ir jos pokyčius;

    c) stebėti ir peržiūrėti informacijos saugumo priemonių įgyvendinimą;

    d) užtikrinti, kad naudojantis teikiamomis paslaugomis būtų laikomasi informacijos saugumo reikalavimų;

    e) užtikrinti, kad visi darbuotojai ir paslaugų teikėjai, turintys prieigą prie informacijos ir sistemų, būtų tinkamai informuoti apie informacijos saugumo politiką, pavyzdžiui, rengiant informacijos saugumo mokymus ir informacinius kursus;

    f) koordinuoti operacinių ar saugumo incidentų nagrinėjimą ir pranešti apie svarbius incidentus AVPO.

8 gairė. Loginis saugumas

26. Įmonės turėtų apibrėžti, dokumentuoti ir įgyvendinti loginės prieigos kontrolės arba loginio saugumo (tapatybės ir prieigos valdymo) procedūras pagal 4 gairėje apibrėžtus apsaugos reikalavimus. Šios procedūros turėtų būti įgyvendinamos, kontroliuojamos, stebimos ir reguliariai peržiūrimos, taip pat turėtų apimti anomalijų stebėsenos kontrolės priemones. Tokiose procedūrose turėtų būti įgyvendinti bent toliau išvardyti elementai (terminas „vartotojas“ apima ir techninius vartotojus):

    a) būtinybė žinoti, mažiausios privilegijos ir pareigų atskyrimas: įmonės turėtų valdyti prieigos teises, įskaitant nuotolinę prieigą prie informacinių išteklių ir jų pagalbinių sistemų, remdamosi principu „būtina žinoti“. Vartotojams turėtų būti suteikiamos minimalios prieigos teisės, reikalingos jų būtinoms pareigoms įvykdyti („mažiausios privilegijos“ principas), t. y. siekiant užkirsti kelią nepagrįstai prieigai prie duomenų arba prieigos teisių derinių paskirstymui, kuriuo gali būti naudojamasi siekiant išvengti kontrolės priemonių („pareigų atskyrimo“ principas);

    b) vartotojų atskaitomybė: įmonės turėtų kuo labiau riboti bendrų ir pasidalijamų vartotojų paskyrų naudojimą ir užtikrinti, kad visada būtų galima nustatyti vartotojus ir atsekti už IRT sistemose atliktus veiksmus atsakingą fizinį asmenį ar leistą atlikti užduotį;

    c) privilegijuotos prieigos teisės: įmonės turėtų įgyvendinti griežtas privilegijuotos prieigos prie sistemos kontrolės priemones, griežtai ribodamos ir įdėmiai stebėdamos padidintas prieigos prie sistemos teises turinčias paskyras (pvz., administratorių paskyras).

    d) nuotolinė prieiga: siekiant užtikrinti saugų ryšį ir sumažinti riziką, nuotolinę administracinę prieigą prie kritinių IRT sistemų reikėtų suteikti tik pagal principą „būtina žinoti“ ir naudojant patikimus autentiškumo patvirtinimo sprendimus;

    e) vartotojo veiksmų įrašymas į žurnalą: įvertinus riziką, į žurnalą turėtų būti įrašomi ir stebimi bent privilegijuotų vartotojų veiksmai. Siekiant užkirsti kelią

nesankcionuotam duomenų pakeitimui arba ištrynimui prieigos registracijos žurnalus reikėtų saugoti tiek, kiek proporcinga atsižvelgiant į nustatytų veiklos funkcijų, pagalbinių procesų ir informacinių išteklių svarbą, nepažeidžiant ES ir nacionalinės teisės aktuose nustatytų informacijos saugojimo reikalavimų. Įmonės turėtų naudoti šią informaciją siekdamos palengvinti anomalios veiklos, pastebėtos teikiant paslaugas, nustatymą ir tyrimą;

f) prieigos valdymas: prieigos teises reikėtų suteikti, atšaukti arba keisti laiku, remiantis iš anksto nustatytais patvirtinimo darbo procesais, kuriuose dalyvauja atitinkamų informacinių išteklių savininkas. Jei prieiga nebereikalinga, prieigos teisės turėtų būti nedelsiant panaikintos;

g) prieigos vertinimas: prieigos teises reikėtų reguliariai peržiūrėti siekiant užtikrinti, kad vartotojai neturėtų pernelyg didelių privilegijų ir kad prieigos teisės būtų atšauktos (panaikintos), kai jų nebereikia;

h) prieigos teisių suteikimas, keitimas, panaikinimas turėtų būti įformintas dokumentais taip, kad būtų lengviau tai suprasti ir analizuoti;

i) autentiškumo patvirtinimo būdai: įmonės turėtų naudoti autentiškumo patvirtinimo būdus, kurie būtų pakankamai patikimi, kad būtų galima tinkamai ir veiksmingai užtikrinti prieigos kontrolės politikos ir procedūrų laikymąsi. Autentiškumo patvirtinimo būdai turi atitikti IRT sistemų, informacijos ar proceso, prie kurio prieinama, svarbą. Tai turėtų būti bent sudėtingi slaptažodžiai arba patikimesni autentiškumo patvirtinimo būdai (kaip antai dviejų pakopų autentiškumo patvirtinimas) atsižvelgiant į atitinkamą riziką.

27. Elektroninė taikomųjų programų prieiga prie duomenų ir IRT sistemų turėtų būti kuo labiau ribojama ir suteikiama tik kai tai būtina tam tikrai paslaugai teikti.

9 gairė. Fizinis saugumas

28. Siekiant apsaugoti įmonių patalpas, duomenų centrus ir jautrias zonas nuo nesankcionuotos prieigos ir aplinkos pavojų, turėtų būti apibrėžtos, dokumentuotos ir įgyvendinamos įmonių fizinio saugumo priemonės (pvz., apsauga nuo elektros tiekimo sutrikimų, gaisro, vandens ir neleistinos fizinės prieigos).

29. Fizinė prieiga prie IRT sistemų turėtų būti leidžiama tik įgaliotiems asmenims. Įgaliojimai turėtų būti suteikiami atsižvelgiant į asmens užduotis ir atsakomybės sritis ir tik asmenims, kurie yra tinkamai apmokyti ir prižiūrimi. Siekiant užtikrinti, kad nereikalingos prieigos teisės būtų greitai atšauktos (panaikintos), fizinę prieigą reikėtų reguliariai peržiūrėti.

30. Tinkamos apsaugos nuo aplinkos pavojų priemonės turėtų atitikti pastatų svarbą ir tuose pastatuose vykdomų operacijų ar esančių IRT sistemų svarbą.

10 gairė. IRT operacijų saugumas

31. Įmonės turėtų įgyvendinti procedūras, užtikrinančias IRT sistemų ir IRT paslaugų konfidencialumą, vientisumą ir prieinamumą, kad atitinkamai būtų sumažintas saugumo problemų poveikis IRT paslaugų teikimui. Šios procedūros pagal poreikį turėtų apimti:

a) galimo pažeidžiamumo, kurį reikėtų įvertinti ir ištaisyti, nustatymą užtikrinant savalaikį IRT sistemų atnaujinimą, įskaitant programinę įrangą, kurią įmonės tiekia savo vidaus ir išorės vartotojams, diegiant kritinius saugumo atnaujinimus, įskaitant antivirusinių programų apibrėžčių atnaujinimą, arba kompensuojamąsias kontrolės priemones;

b) saugios visų kritinių komponentų, kaip antai operacinių sistemų, duomenų bazių, maršrutizatorių ar jungiklių, bazinės konfigūracijos įgyvendinimą;

c) tinklo suskirstymą į segmentus, duomenų nutekėjimo prevencijos sistemas ir tinklo srauto šifravimą (atsižvelgiant į informacinių išteklių klasifikaciją);

d) galinių įrenginių, įskaitant serverius, kompiuterizuotas darbo vietas ir mobiliuosius prietaisus, apsaugos įgyvendinimą; Prieš suteikdama galiniam įrenginiui prieigą prie įmonės tinklo, įmonė turėtų įvertinti, ar jis atitinka įmonės nustatytus saugumo standartus;

e) užtikrinimą, kad būtų įdiegti IRT sistemų vientisumo patikrinimo mechanizmai;

f) saugomų ir perduodamų duomenų šifravimą (pagal informacinių išteklių klasifikaciją).

11 gairė. Saugumo stebėsena

32. Įmonės turėtų nustatyti ir įgyvendinti procedūras ir procesus, skirtus nuolat stebėti veiklą, darančią poveikį įmonių informacijos saugumui. Stebimi turėtų būti bent:

    a) vidaus ir išorės veiksniai, įskaitant veiklos ir IRT administracines funkcijas;

    b) paslaugų teikėjų, kitų subjektų ir vidaus naudotojų sandoriai;

    c) galimos vidaus ir išorės grėsmės.

33. Remdamosi stebėsena, įmonės turėtų plėtoti tinkamus ir veiksmingus gebėjimus nustatyti neįprastą veiklą ir grėsmes, pvz., fizinį ar loginį įsibrovimą, informacijos išteklių slaptumo, vientisumo ir prieinamumo pažeidimus, kenkėjišką kodą ir viešai žinomas programinės ir kompiuterinės įrangos pažeidžiamas vietas, apie jas pranešti ir į jas reaguoti.

34. Saugumo stebėsenos pranešimai turėtų padėti įmonėms suprasti operacinių arba saugumo incidentų pobūdį, nustatyti tendencijas ir padėti įmonėms atlikti vidaus tyrimus bei priimti atitinkamus sprendimus.

12 gairė. Informacijos saugumo peržiūra, vertinimai ir testavimas

35. Įmonės turėtų atlikti įvairias informacijos saugumo peržiūras, vertinimus ir testavimą, siekdamos užtikrinti veiksmingą IRT sistemų ir paslaugų pažeidžiamumo nustatymą. Pavyzdžiui, įmonės gali atlikti spragų analizę vadovaudamosi informacijos saugumo standartais, atitikties peržiūromis, vidaus ir išorės informacinių sistemų auditu arba fizinio saugumo peržiūromis.

36. Įmonės turėtų sukurti ir įdiegti informacijos saugumo testavimo sistemą, kurioje būtų patvirtinamas jų informacijos saugumo priemonių patikimumas ir veiksmingumas, ir užtikrinti, kad sistemoje būtų nagrinėjamos grėsmės ir pažeidžiamumas, nustatyti grėsmių stebėsenos ir IRT ir saugumo rizikos vertinimo procese.

37. Testavimas turėtų būti atliekamas saugiai ir patikimai, jį turėtų atlikti nepriklausomi tikrintojai, turintys pakankamai žinių, įgūdžių ir patirties testuojant informacijos saugumo priemones.

38. Įmonės testavimą turėtų atlikti reguliariai. Testavimo apimtis, dažnumas ir metodas (pvz., įskaitant, kai būtina ir tinkama, grėsmėmis grindžiamą įsiskverbimų testavimą) turėtų būti proporcingi nustatytam rizikos lygiui. Kritinių IRT sistemų bandymai ir pažeidžiamumo testavimas turėtų būti atliekamas kasmet.

39. Įmonės turėtų užtikrinti, kad saugumo priemonių testavimai būtų atliekami pasikeitus infrastruktūrai, procesams ar procedūroms ir atlikus pakeitimus dėl svarbių operacinių ar saugumo incidentų arba pradėjus naudoti naujas ar iš esmės pakeistas kritines taikomąsias programas. Įmonės turėtų stebėti ir vertinti saugumo testavimo rezultatus ir atitinkamai atnaujinti savo saugumo priemones, nepagrįstai nedelsdamos, kai tai susiję su kritinėmis IRT sistemomis.

13 gairė. Mokymas ir informuotumas informacijos saugumo klausimais

40. Įmonės visiems darbuotojams, įskaitant AVPO darbuotojus, turėtų parengti informacijos saugumo mokymo programas, siekdamos užtikrinti jų pasirengimą vykdyti savo funkcijas ir pareigas mažinant žmonių klaidų, vagystės, sukčiavimo, piktnaudžiavimo ar praradimo atvejų skaičius. Įmonės turėtų užtikrinti, kad mokymo programoje būtų numatytas nuolatinis visų darbuotojų mokymas.

41. Įmonės turėtų parengti ir įgyvendinti periodines informuotumo apie saugumą didinimo programas, skirtas išmokyti jų darbuotojus, įskaitant AVPO darbuotojus, spręsti su informacijos saugumu susijusios rizikos klausimus.

14 gairė. IRT operacijų valdymas

42. Įmonės turėtų valdyti savo IRT operacijas remdamosi IRT strategija. Dokumentuose turėtų būti apibrėžta, kaip įmonės naudoja, stebi ir valdo IRT sistemas ir IRT paslaugas, įskaitant kritinių IRT procesų, procedūrų ir operacijų dokumentavimą.

43. Įmonės turėtų įgyvendinti kritinių IRT operacijų įrašymo į žurnalą ir stebėsenos procedūras, kad būtų galima nustatyti, analizuoti ir ištaisyti klaidas.

44. Įmonės turėtų nuolat atnaujinti savo IRT išteklių sąrašą. IRT išteklių sąrašas turėtų būti pakankamai išsamus, kad būtų galima greitai nustatyti IRT išteklių, jo buvimo vietą, saugumo klasifikaciją ir savininką.

45. Įmonės turėtų stebėti ir valdyti IRT išteklių gyvavimo ciklus, siekdamos užtikrinti, kad jie ir toliau atitiktų veiklos ir rizikos valdymo reikalavimus ir padėtų juos įgyvendinti. Įmonės turėtų stebėti, ar jų IRT išteklius ir toliau palaiko jų tiekėjai ar įmonėje dirbantys kūrėjai, tai pat ar remiantis dokumentuotu procesu atliekami visi patobulinimai ir atnaujinimai. Su pasenusiais ar nepalaikomais IRT ištekliais susijusią riziką reikėtų vertinti ir mažinti. Nebenaudojami IRT ištekliai turėtų būti saugiai apdoroti ir pašalinti.

46. Siekdamos laiku užkirsti kelią svarbioms su IRT sistemomis ir nepakankamais IRT pajėgumais susijusių veiklos rezultatų problemoms, jas nustatyti ir į jas reaguoti, įmonės turėtų įgyvendinti veiklos rezultatų ir pajėgumų planavimo ir stebėsenos procesus.

47. Įmonės turėtų sukurti ir įgyvendinti duomenų ir IRT sistemų atsarginio kopijavimo ir atstatymo procedūras, kad prireikus jas būtų galima atkurti. Atsarginio kopijavimo mastą ir dažnį reikėtų nustatyti remiantis veiklos atkūrimo reikalavimais ir atsižvelgiant į duomenų ir IRT sistemų svarbą, nustatytą remiantis atliktu rizikos įvertinimu. Reikėtų reguliariai atlikti atsarginio kopijavimo ir atstatymo procedūrų testavimą.

48. Įmonės turėtų užtikrinti, kad duomenų ir IRT sistemų atsarginės kopijos būtų saugomos vienoje ar keliose vietose už pagrindinės buvimo vietos ribų, kurios yra saugios ir pakankamai toli nuo pagrindinės buvimo vietos, kad joms nekiltų tokia pati rizika.

15 gairė. IRT incidentų ir problemų valdymas

49. Įmonės turėtų sukurti ir įgyvendinti incidentų ir problemų valdymo procesą, kurį taikant būtų stebimi ir į žurnalą įrašomi operaciniai ir saugumo IRT incidentai, o sutrikimų atveju įmonės galėtų tęsti arba laiku vėl pradėti vykdyti kritines veiklos funkcijas ir procesus.

50. Įmonės turėtų nustatyti tinkamus kriterijus ir ribines vertes, kuriomis remiantis įvykį būtų galima pripažinti operaciniu ar saugumo incidentu, taip pat išankstinio įspėjimo rodiklius, sudarančius galimybę iš anksto nustatyti tokius incidentus.

51. Siekdamos kuo labiau sumažinti neigiamų įvykių poveikį ir laiku užtikrinti atkūrimą, įmonės turėtų sukurti tinkamus procesus ir organizacines struktūras, kad būtų užtikrinta nuosekli kompleksinė operacinių ir saugumo incidentų stebėsena, valdymas ir tolesni veiksmai, siekiant užtikrinti, kad būtų nustatytos ir įvertintos pagrindinės priežastys ir imtasi ištaisomųjų veiksmų (priemonių), kad tokie incidentai nepasikartotų. Incidentų ir problemų valdymo procese reikėtų nustatyti bent:

    a) procedūras, skirtas incidentams nustatyti, atsekti, įrašyti į žurnalą, suskirstyti į kategorijas ir klasifikuoti pagal įmonės apibrėžtą prioritetą, pagrįstą veiklos svarba ir paslaugų sutartimis;

    b) funkcijas ir pareigas pagal įvairius incidentų scenarijus (pvz., susijusius su klaidomis, triktimis, kibernetinėmis atakomis);

    c) problemų valdymo procedūrą, naudojamą siekiant nustatyti, analizuoti ir pašalinti pagrindinę vieno ar kelių incidentų priežastį; įmonės turėtų analizuoti operacinius ar saugumo incidentus, kurie buvo nustatyti ir (arba) įvyko organizacijos viduje ir (arba) už jos ribų, ir turėtų apsvarstyti pagrindines pamokas, įgytas atlikus šią analizę, ir atitinkamai atnaujinti saugumo priemones;

    d) veiksmingus vidaus komunikacijos planus, įskaitant pranešimo apie incidentus ir problemų sprendimo procedūras, apimančias ir su saugumu susijusius klientų skundus, siekiant užtikrinti, kad:

        i. apie incidentus, galinčius padaryti didelį neigiamą poveikį kritinėms IRT sistemoms ir IRT paslaugoms, būtų pranešama atitinkamai vyresniajai vadovybei;

        ii. *ad hoc* pagrindu AVPO būtų pranešama apie didelius incidentus ir bent jau apie poveikį, reagavimą ir papildomas kontrolės priemones, kurias reikia nustatyti dėl incidentų;

    e) reagavimo į incidentus procedūras siekiant sumažinti su incidentais susijusį poveikį ir užtikrinti, kad paslaugos būtų vėl teikiamos laiku ir saugiai;

    f) konkrečius išorės komunikacijos planus, susijusius su kritinėmis veiklos funkcijomis ir procesais, siekiant:

        i. bendradarbiauti su atitinkamais suinteresuotaisiais subjektais, kad į incidentą būtų sureaguota veiksmingai ir atsigauta po jo;

        ii. laiku pateikti reikiamą informaciją, taip pat ir apie incidentus, išorės šalims (pvz., klientams, kitiems rinkos dalyviams, atitinkamoms (priežiūros) institucijoms), laikantis taikytinų normų).

16 gairė. IRT projektų valdymas

52. Įmonės turėtų įgyvendinti IRT projektų metodiką (nepriklausomai įvertinant saugumo reikalavimus), tinkamai valdydamos procesą ir vadovaudamos projektų įgyvendinimui, kad IRT projektais veiksmingai paremtų IRT strategijos įgyvendinimą.

53. Įmonės turėtų tinkamai stebėti ir mažinti IRT projektų portfelyje kylančią riziką, kartu atsižvelgdamos į riziką, kuri gali kilti dėl įvairių projektų tarpusavio priklausomybės ryšių ir daugelio projektų priklausomybės nuo tų pačių išteklių ir (arba) ekspertų.

17 gairė. IRT sistemų įsigijimas ir kūrimas

54. Įmonės turėtų sukurti ir įgyvendinti IRT sistemų įsigijimo, kūrimo ir palaikymo valdymo procesą, siekiant užtikrinti, kad tvarkomų duomenų konfidencialumas, vientisumas, prieinamumas būtų visapusiškai užtikrintas ir būtų laikomasi nustatytų apsaugos reikalavimų. Šis procesas turėtų būti sukurtas remiantis rizika pagrįstu metodu.

55. Įmonės turėtų užtikrinti, kad prieš įsigyjant ar sukuriant sistemas būtų aiškiai apibrėžti funkciniai ir nefunkciniai reikalavimai (įskaitant informacijos saugumo reikalavimus) ir techniniai uždaviniai.

56. Įmonės turėtų būti parengusios priemones, užkertančias kelią netyčiniam IRT sistemų keitimui ar tyčiniam manipuliavimui jomis jas kuriant.

57. Įmonėse turėtų būti įdiegta IRT sistemų, IRT paslaugų ir informacijos saugumo priemonių testavimo ir patvirtinimo metodika.

58. Įmonės turėtų tinkamai atlikti IRT sistemų, IRT paslaugų ir informacijos saugumo priemonių testavimą, kad nustatytų galimus saugumo trūkumus, pažeidimus ir incidentus.

59. Įmonės turėtų užtikrinti gamybos aplinkos atskyrimą nuo kūrimo, testavimo ir kitos ne gamybos aplinkos.

60. Įmonės turėtų įgyvendinti priemones, skirtas apsaugoti IRT sistemų pirminių kodų vientisumą (jei yra). Siekdamos sumažinti nereikalingą priklausomybę nuo konkrečių sričių ekspertų, jos taip pat turėtų išsamiai dokumentuoti IRT sistemų kūrimą, įgyvendinimą, veikimą ir (arba) konfigūravimą.

61. Įmonėje įdiegti IRT sistemų įsigijimo ir kūrimo procesai taip pat turėtų būti taikomi IRT sistemoms, kurias, taikydami rizika pagrįstą metodą, kuria arba valdo IRT organizacijai nepriklausantys galutiniai veiklos funkcijos vartotojai (pvz., verslo valdymo taikomosios programos arba galutinių vartotojų skaičiavimo programos). Įmonės turėtų pildyti tokių taikomųjų programų, palaikančių kritines veiklos funkcijas ar procesus, registrą.

18 gairė. IRT pokyčių valdymas

62. Siekdamos užtikrinti, kad visi IRT sistemų pakeitimai būtų registruojami, vertinami, testuojami, patvirtinami, leidžiami ir įdiegiami kontroliuojamu būdu, įmonės turėtų sukurti ir įgyvendinti IRT pokyčių valdymo procesą. Skubūs ar neatidėliotini IRT pokyčiai turėtų būti atsekami ir apie juos turėtų būti *ex post* pranešama atitinkamam turto savininkui *ex post* analizei atlikti.

63. Įmonės turėtų vertinti, ar dabartinės veiklos aplinkos pokyčiai turi įtakos turimoms saugumo priemonėms arba reikalauja papildomų susijusios rizikos mažinimo priemonių. Tokie pokyčiai turėtų atitikti įmonių oficialų pokyčių valdymo procesą.

19 gairė. Veiklos tęstinumo valdymas

64. Pagal bendrą įmonės veiklos tęstinumo politiką AVPO yra atsakingas už įmonės IRT tęstinumo politikos nustatymą ir patvirtinimą. Apie IRT tęstinumo politiką turėtų būti tinkamai informuojama įmonėse ir ji turėtų būti taikoma visiems susijusiems darbuotojams ir atitinkamais atvejais paslaugų teikėjams.

20 gairė. Poveikio veiklai analizė

65. Vykdydamos patikimą veiklos tęstinumo valdymą, įmonės turėtų atlikti poveikio veiklai analizę, kad įvertintų joms kylančią rimtų veiklos sutrikimų riziką, taip pat kiekybiškai ar kokybiškai įvertintų galimą jų poveikį, remdamosi vidaus ir (arba) išorės duomenimis ir scenarijų analize. Atliekant poveikio veiklai analizę taip pat reikėtų atsižvelgti į nustatytų ir klasifikuotų verslo procesų ir veiklos, verslo funkcijų, vaidmenų ir išteklių (pvz., informacinių ir IRT išteklių) svarbą ir jų tarpusavio priklausomybės ryšius pagal 4 gairę.

66. Įmonės turėtų užtikrinti, kad jų IRT sistemos ir IRT paslaugos būtų sukurtos atsižvelgiant į poveikio veiklai analizę, pavyzdžiui, numatant tam tikrų kritinių komponentų dubliavimą siekiant užkirsti kelią sutrikimams dėl įvykių, darančių poveikį tiems komponentams.

21 gairė. Veiklos tęstinumo planavimas

67. Įmonių bendruose veiklos tęstinumo planuose (VTP) turėtų būti įvertinta reikšminga rizika, kuri galėtų neigiamai paveikti IRT sistemas ir IRT paslaugas. Planais turi būti remiami tikslai apsaugoti ir prireikus atkurti įmonių verslo procesų bei veiklos, verslo funkcijų, vaidmenų ir išteklių (pvz., informacinių ir IRT išteklių) konfidencialumą, vientisumą ir prieinamumą. Rengdamos tokius planus, įmonės, kai tinkama, turėtų tai koordinuoti su atitinkamomis vidaus ir išorės suinteresuotosiomis šalimis.

68. Įmonės turėtų įgyvendinti VTP siekdamos užtikrinti savo gebėjimą tinkamai reaguoti į galimų sutrikimų scenarijus neviršijant nustatyto atkūrimo termino (t. y. didžiausio laikotarpio, per kurį sistemą ar procesą būtina atkurti po incidento) ir nustatyto atkūrimo momento (t. y. didžiausio laikotarpio, per kurį incidento atveju duomenų praradimas laikomas priimtinu pagal iš anksto nustatytą paslaugų lygį).

69. Savo VTP įmonės turėtų išnagrinėti įvairius scenarijus, įskaitant kraštutinius, bet įmanomus, taip pat kibernetinės atakos scenarijus, ir įvertinti galimą tokių scenarijų poveikį. Remdamosi tokiais scenarijais, įmonės turėtų aprašyti, kaip užtikrinamas IRT sistemų ir paslaugų tęstinumas ir įmonių informacijos saugumas.

22 gairė. Reagavimo ir atkūrimo planai

70. Remdamosi poveikio veiklai analize ir įmanomais scenarijais, įmonės turėtų parengti reagavimo ir atkūrimo planus. Tokiuose planuose reikėtų nurodyti, kokiomis sąlygomis planai gali būti taikomi ir kokių veiksmų reikėtų imtis siekiant užtikrinti bent kritinių įmonėse įdiegtų IRT sistemų, IRT paslaugų ir duomenų vientisumą, prieinamumą, tęstinumą ir atkūrimą. Reagavimo ir atkūrimo planais turėtų būti siekiama įgyvendinti įmonių operacijų atkūrimo tikslus.

71. Reagavimo ir atkūrimo planuose reikėtų apsvarstyti trumpalaikius ir, prireikus, ilgalaikius atkūrimo variantus. Planai turėtų būti bent:

a) parengti daugiausia dėmesio skiriant svarbių IRT paslaugų operacijų, veiklos funkcijų pagalbinių procesų, informacinių išteklių ir jų tarpusavio priklausomybės ryšių atkūrimui, siekiant išvengti neigiamo poveikio įmonės veikimui;

b) įforminti dokumentais, kuriais galėtų naudotis veiklos ir pagalbiniai skyriai ir kuriuos būtų galima skubiai pritaikyti iškilus nenumatytam atvejui, aiškiai nustačius vaidmenis bei atsakomybę;

c) atnaujinami atsižvelgiant į incidentų bei testavimo patirtį, naujai nustatytą riziką bei grėsmes ir pasikeitusius atkūrimo tikslus ir prioritetus.

72. Planuose taip pat turėtų būti vertinamos alternatyvos, kai trumpalaikis atkūrimas gali būti neįmanomas dėl sąnaudų, rizikos, logistikos ar nenumatytų aplinkybių.

73. Reagavimo ir atkūrimo planuose įmonės turėtų apsvarstyti ir įgyvendinti tęstinumo priemones, kad sumažintų trečiųjų šalių tiekėjų, kurie yra itin svarbūs įmonės IRT paslaugų tęstinumui, problemas (laikantis EIOPA valdymo sistemos gairių ir EIOPA debesijos paslaugų teikėjų užsakomųjų paslaugų gairių nuostatų).

23 gairė. Planų testavimas

74. Įmonės turėtų testuoti savo VTP ir užtikrinti, kad jų ypatingos svarbos verslo procesai ir veikla, veiklos funkcijos, vaidmenys ir ištekliai (pvz., informaciniai ištekliai) bei IRT ištekliai ir jų tarpusavio priklausomybės ryšiai (įskaitant paslaugų teikėjų teikiamus išteklius) būtų reguliariai testuojami remiantis įmonės rizikos pobūdžiu.

75. VTP reikėtų atnaujinti reguliariai, remiantis testavimų rezultatais, surinktais duomenimis apie grėsmes ir su ankstesniais įvykiais susijusia patirtimi. Taip pat reikia įtraukti bet kokius atkūrimo tikslų (įskaitant nustatytą atkūrimo terminą ir nustatytą atkūrimo momentą) pakeitimus ir (arba) verslo procesų ir veiklos, veiklos funkcijų, vaidmenų ir išteklių (pvz. informacinių ir IRT išteklių) pakeitimus.

76. Atliekant VTP testavimą, turi būti įrodyta, kad jie tinkami siekiant išlaikyti veiklos gyvybingumą, kol bus atkurtos kritinės operacijos pagal anksto nustatytą paslaugų lygį ar leistiną poveikį.

77. Testavimo rezultatai turėtų būti dokumentuojami; visus per testavimus nustatytus trūkumus reikėtų išnagrinėti ir pašalinti bei apie juos pranešti AVPO.

24 gairė. Ryšiai krizės sąlygomis

78. Sutrikus veiklai arba iškilus nenumatytai situacijai, taip pat įgyvendindamos VTP, įmonės turėtų būti įdiegusios veiksmingas informavimo krizės atveju priemones, kad visi svarbūs vidaus ir išorės suinteresuotieji subjektai, įskaitant atitinkamas priežiūros institucijas, kai to reikalaujama nacionalinės teisės aktuose, ir išorės paslaugų teikėjus, būtų laiku ir tinkamai informuoti.

25 gairė. IRT paslaugų ir IRT sistemų užsakomosios paslaugos

79. Nepažeidžiant EIOPA debesijos paslaugų teikėjų užsakomųjų paslaugų gairių, įmonės turėtų užtikrinti, kad tais atvejais, kai IRT paslaugos ir IRT sistemos yra užsakomos, būtų laikomasi atitinkamų IRT paslaugai arba IRT sistemai taikomų reikalavimų.

80. Kai iš paslaugų tiekėjo užsakomos kritinės ar svarbios funkcijos, įmonės turėtų užtikrinti, kad į paslaugų teikėjo sutartinius įsipareigojimus (pvz., sutartis,

susitarimus dėl paslaugų lygio, atitinkamų sutarčių nutraukimo nuostatas) būtų įtraukti bent šie dalykai:

a) tinkami ir proporcingi su informacijos saugumu susiję tikslai ir priemonės, įskaitant reikalavimus, kaip antai minimaliuosius informacijos saugumo reikalavimus, specifikacijas dėl įmonės duomenų gyvavimo ciklo, visus reikalavimus dėl duomenų centrų buvimo vietos, duomenų šifravimo, tinklo saugumo ir saugumo stebėsenos procesų;

b) susitarimai dėl paslaugų lygio, siekiant užtikrinti IRT paslaugų ir IRT sistemų tęstinumą ir tikslinius veiklos rodiklius įprastomis aplinkybėmis, taip pat susitarimus, numatytus nenumatytų atvejų planuose paslaugų nutraukimo atveju;

c) operacinių ir saugumo incidentų valdymo procedūros, įskaitant problemų sprendimo ir informavimo procedūras.

81. Įmonės turėtų vykdyti stebėseną ir siekti užtikrinti, kad tie paslaugų teikėjai laikytųsi nustatytų saugumo tikslų, priemonių ir veiklos rezultatų tikslų.

Atitiktis ir pranešimo taisyklės

82. Šiame dokumente pateiktos pagal Reglamento (ES) Nr. 1094/2010 16 straipsnį parengtos gairės. Vadovaudamosi to reglamento 16 straipsnio 3 dalimi, kompetentingos institucijos ir įmonės turi dėti visas pastangas, kad laikytųsi gairių ir rekomendacijų.

83. Kompetentingos institucijos, kurios laikosi arba ketina laikytis šių gairių, turėtų atitinkamai įtraukti jas į savo reguliavimo ar priežiūros sistemą.

84. Kompetentingos institucijos per 2 mėnesius nuo šių gairių vertimų paskelbimo turi Europos draudimo ir profesinių pensijų institucijai patvirtinti, ar jos laikosi arba ketina laikytis šių gairių, ir, jeigu nesilaiko, nurodyti nesilaikymo priežastis.

85. Jeigu iki šio termino pabaigos atsakymas nebus gautas, bus laikoma, kad kompetentingos institucijos nesilaiko pranešimo reikalavimo, ir apie tai bus pranešta.

Baigiamoji nuostata dėl peržiūrėjimo

86. Šias gaires peržiūri EIOPA.