EIOPA-BoS-20/600

Informācijas un komunikācijas tehnoloģiju drošības un pārvaldības pamatnostādnes

EAAPI – *Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Germany* - Tālr. *+ 49 69-951119-20;*
fakss: + 49 69-951119-19; e-pasts: info@eiopa.europa.eu vietne: www.eiopa.europa.eu

Saturs

Konteksts 3
Ievads 6
Definīcijas 6
1. pamatnostādne. Samērīgums 8
2. pamatnostādne. IKT pārvaldes sistēmā 8
3. pamatnostādne. IKT stratēģija 9
4. pamatnostādne. IKT un drošības riski riska pārvaldības sistēmā 9
5. pamatnostādne. Revīzija 10
6. pamatnostādne. Informācijas drošības politika un pasākumi 10
7. pamatnostādne. Informācijas drošības funkcija 11
8. pamatnostādne. Loģiskā drošība 11
9. pamatnostādne. Fiziskā drošība 12
10. pamatnostādne. IKT operacionālā drošība 12
11. pamatnostādne. Drošības uzraudzība 13
12. pamatnostādne. Informācijas drošības pārskati, novērtējums un testēšana 13
13. pamatnostādne. Informācijas drošības apmācība un izpratne 14
14. pamatnostādne. IKT darbības vadība 14
15. pamatnostādne. IKT incidentu un problēmu pārvaldība 15
16. pamatnostādne. IKT projektu vadība 16
17. pamatnostādne. IKT sistēmu apguve un izstrāde 16
18. pamatnostādne. IKT pārmaiņu vadība 17
19. pamatnostādne. Darbības nepārtrauktības pārvaldība 17
20. pamatnostādne. Darbības ietekmes analīze 17
21. pamatnostādne. Darbības nepārtrauktības plānošana 17
22. pamatnostādne. Reaģēšanas un atjaunošanas plāni 18
23. pamatnostādne. Plānu testēšana 18
24. pamatnostādne. Krīzes saziņa 19
25. pamatnostādne. IKT pakalpojumu un IKT sistēmu ārpakalpojumi 19
Atbilstība un ziņošanas noteikumi 20
Nobeiguma noteikums par pārskatīšanu 20

Konteksts

1. Saskaņā ar Regulas (ES) Nr. 1094/2010 16. pantu EAAPI ir tiesīga izdot pamatnostādnes un ieteikumus kompetentām iestādēm un finanšu iestādēm, lai ieviestu konsekventu, efektīvu un konstruktīvu uzraudzības praksi un nodrošinātu kopēju, vienveidīgu un konsekventu Savienības tiesību aktu piemērošanu.

2. Atbilstīgi minētās regulas 16. panta 3. punktam kompetentām iestādēm un finanšu iestādēm jādara viss iespējamais, lai ievērotu šādas pamatnostādnes un ieteikumus.

3. EAAPI identificēja nepieciešamību izstrādāt īpašas vadlīnijas informācijas un komunikācijas tehnoloģiju (IKT) drošībai un pārvaldībai attiecībā uz Direktīvas 2009/138/EK 41. un 44. pantu saistībā ar analīzi, kas veikta, atbildot uz Eiropas Komisijas FinTech rīcības plānu (COM(2018)0109 *final*), EAAPI uzraudzības konverģences plānu 2018.–2019. gadam[1] un pēc saskarsmes ar vairākām citām ieinteresētajām personām[2].

4. Kā norādīts Eiropas uzraudzības iestāžu kopīgajā ieteikumā Eiropas Komisijai, EAAPI Pamatnostādnēs par pārvaldības sistēmu "nav pienācīgi atspoguļots, cik svarīgi ir rūpēties par IKT riska pārvaldību (tostarp kiberriskiem)". Trūkst vadlīnijas attiecībā uz vitāli svarīgiem elementiem, kas parasti tiek atzīti par pareizas IKT drošības un pārvaldības sastāvdaļu".

5. Pašreizējās (likumdošanas) situācijas analīze ES saistībā ar iepriekš minēto kopīgo ieteikumu parādīja, ka lielākā daļa ES dalībvalstu ir valsts noteikumi par IKT drošību un pārvaldību. Lai gan prasības ir līdzīgas, tiesiskais regulējums joprojām ir sadrumstalots. Turklāt aptauja par pašreizējo uzraudzības praksi atklāja ļoti dažādas prakses — no "nav īpašas uzraudzības" līdz "stingrai uzraudzībai" (tostarp "attālinātas pārbaudes" un "pārbaudes uz vietas").

6. Turklāt pieaug IKT sarežģītība, un pieaug arī ar IKT saistīto incidentu (tostarp kibernoziegumu) biežums, kā arī šādu incidentu nelabvēlīgā ietekme uz uzņēmumu operatīvo darbību. Šī iemesla dēļ IKT un drošības risku pārvaldība ir būtiska, lai uzņēmums varētu sasniegt savus stratēģiskos, korporatīvos, darbības un reputācijas mērķus.

7. Turklāt visā apdrošināšanas nozarē, iekļaujot gan tradicionālos, gan novatoriskos uzņēmējdarbības modeļus, apdrošināšanas pakalpojumu sniegšanā un uzņēmumu parastās operatīvās darbības nodrošināšanā arvien vairāk paļaujas uz IKT, piemēram, apdrošināšanas nozares digitalizācija (InsurTech, IoT utt.), kā arī savstarpēja savienojamība, izmantojot telekomunikāciju kanālus (internetu, mobilos un bezvadu savienojumus un platjoslas tīklus). Tā rezultātā uzņēmējdarbība ir neaizsargāta pret drošības incidentiem, tostarp kiberuzbrukumiem. Tāpēc ir svarīgi nodrošināt, ka uzņēmumi ir pietiekami sagatavoti savu IKT un drošības risku pārvaldīšanai.

8. Turklāt, atzīstot uzņēmumu nepieciešamību sagatavoties kiberriskam[3] un pēc stipras kiberdrošības sistēmas, šajās pamatnostādnēs kiberdrošība ir ietverta arī kā daļa no uzņēmuma informācijas drošības pasākumiem. Kaut arī šajās pamatnostādnēs ir atzīts, ka kiberdrošība būtu jārisina uzņēmuma vispārējās IKT

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

[2] EIOPA ziņojumu, atbildot uz Eiropas Komisijas FinTech rīcības plānu, var iegūt šeit.

[3] Kiberriska definīciju, lūdzu, skatiet FSB 2018. gada 12. novembra kiberleksikonā, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

un drošības risku pārvaldības ietvaros, ir svarīgi norādīt, ka kiberuzbrukumiem ir dažas raksturīgas iezīmes, kuras būtu jāņem vērā, lai nodrošinātu, ka informācijas drošības pasākumi pienācīgi mazina kiberdrošību risku:

a) kiberuzbrukumus bieži ir grūtāk pārvaldīt (t. i., identificēt, aizsargāt, atklāt, reaģēt uz tiem un pilnībā no tiem atgūties) nekā lielāko daļu citu IKT un drošības riska avotu, kā arī ir grūti noteikt kaitējuma apmēru;

b) daži kiberuzbrukumi var padarīt neefektīvus kopējus riska pārvaldības un darbības nepārtrauktības pasākumus, kā arī negadījumu seku novēršanas procedūras, jo tie var izplatīt ļaunprātīgu programmatūru dublējumu sistēmās, padarot tās nepieejamas vai sabojājot dublējumu datus;

c) pakalpojumu sniedzēji, brokeri, (pārvaldošie) aģenti un starpnieki var kļūt par kiberuzbrukumu izplatīšanas kanāliem. Lipīgi klusie apdraudējumi var izmantot savstarpēju savienojamību caur trešo personu telekomunikāciju saitēm, tādējādi nonākot uzņēmuma IKT sistēmā. Tāpēc savstarpēji saistīts uzņēmums, kas atsevišķi ir maznozīmīgs, var kļūt viegli ievainojams un kļūt par riska izplatīšanas avotu, kā arī radīt sistēmisku ietekmi. Ievērojot vājākā posma principu, par kiberdrošību vajadzētu domāt ne tikai galvenajiem tirgus dalībniekiem vai kritisko pakalpojumu sniedzējiem.

9. Šo pamatnostādņu mērķis ir:

a) nodrošināt skaidrību un pārredzamību tirgus dalībniekiem attiecībā uz minimālām sagaidāmajām informācijas un kiberdrošības iespējām, t. i., drošības atsauces scenāriju;

b) izvairīties no iespējamās regulējuma arbitrāžas;

c) veicināt uzraudzības konverģenci attiecībā uz cerībām un procesiem saistībā ar IKT drošību un pārvaldību kā pareizas IKT un drošības risku pārvaldības atslēgu.

Informācijas un komunikācijas tehnoloģiju drošības un pārvaldības pamatnostādnes

Ievads

1. Saskaņā ar Regulas (ES) Nr. 1094/2010[4] 16. pantu EAAPI izdod šīs pamatnostādnes, kas adresētas uzraudzības iestādēm, lai sniegtu norādījumus par to, kā apdrošināšanas un pārapdrošināšanas sabiedrībām (turpmāk tekstā kopā saukti "uzņēmumi") jāpiemēro Direktīvā 2009/138/EK[5] (Direktīva "Maksātspēja II") un Komisijas Deleģētajā regulā (ES) Nr. 2015/35[6] ("Deleģētā regula") paredzētās pārvaldības prasības informācijas un komunikācijas tehnoloģiju ("IKT") drošības un pārvaldības kontekstā. Šim nolūkam šīs pamatnostādnes balstās uz noteikumiem par pārvaldību, kas paredzēti Direktīvas "Maksātspēja II" 41., 44., 46., 47., 132. un 246. pantā un Deleģētās regulas 258. līdz 260., 266., 268. līdz 271. un 274. pantā. Turklāt šīs pamatnostādnes ir balstītas arī norādījumos, kas sniegti EAAPI Pamatnostādnēs par pārvaldības sistēmu (EIOPA-BoS-14/253)[7] un EAAPI Pamatnostādnēs par ārpakalpojumiem ar mākoņdatošanu saistītajiem pakalpojumu sniedzējiem[8] (EIOPA-BoS-19/270).
2. Pamatnostādnes piemērojamas gan atsevišķiem uzņēmumiem, gan *mutatis mutandis* grupas līmenī[9].
3. Kompetentajām iestādēm, ievērojot šīs pamatnostādnes vai uzraugot to ievērošanu, būtu jāņem vērā samērīguma princips[10], kam būtu jānodrošina, lai pārvaldības pasākumi, tostarp tie, kas saistīti ar IKT drošību un pārvaldību, būtu proporcionāli attiecīgo uzņēmumu uzņēmējdarbībai raksturīgo vai iespējamo risku veidam, pakāpei un sarežģītībai.
4. Šīs pamatnostādnes būtu jālasa kopā ar Direktīvu "Maksātspēja II", Deleģēto regulu, EAAPI Pamatnostādnēm par pārvaldības sistēmu un EAAPI Pamatnostādnēm par ārpakalpojumiem ar mākoņdatošanu saistītajiem pakalpojumu sniedzējiem, neskarot tajās ietvertos nosacījumus. Šīs pamatnostādnes ietur neitrālu pozīciju attiecībā uz tehnoloģiju un metodiku.

Definīcijas

5. Ja termini šajās pamatnostādnēs nav definēti, tiem ir tāda nozīme, kā noteikts Direktīvā "Maksātspēja II".
6. Šajās pamatnostādnēs izmanto šādas definīcijas.

---

[4] Eiropas Parlamenta un Padomes Regula (ES) Nr. 1094/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Apdrošināšanas un aroda pensiju iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/79/EK (OV L 331, 15.12.2010., 48. lpp).

[5] Eiropas Parlamenta un Padomes Direktīva 2009/138/EK (2009. gada 25. novembris) par uzņēmējdarbības uzsākšanu un veikšanu apdrošināšanas un pārapdrošināšanas jomā (Maksātspēja II) (OV L 335, 17.12.2009., 1. lpp.).

[6] Komisijas Deleģētā regula (ES) 2015/35 (2014. gada 10. oktobris), ar ko papildina Eiropas Parlamenta un Padomes Direktīvu 2009/138/EK par uzņēmējdarbības uzsākšanu un veikšanu apdrošināšanas un pārapdrošināšanas jomā (Maksātspēja II) (OV L 12, 17.1.2015., 1. lpp.).

[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] Direktīvas 2009/138/EK 212. panta 1. punkts.

[10] Direktīvas 2009/138/EK 29. panta 3. punkts.

Aktīvu īpašnieks	Persona vai organizācija, kurai ir atbildība un pilnvaras attiecībā uz informāciju un IKT aktīviem.
Pieejamība	Īpašība, kas nozīmē tiesības piekļūt un izmantot pēc pilnvarotas organizācijas pieprasījuma (savlaicīgums).
Konfidencialitāte	Īpašība, kas nozīmē, ka informācija nav pieejama vai nav izpaužama personām, organizācijām, procesiem vai sistēmām, kuriem nav atbilstoša pilnvarojuma.
Kiberuzbrukums	Jebkura veida uzlaušana, kas vērsta uz IKT sistēmām un kas noved pie pārkāpjoša/ļaunprātīga mēģinājuma iznīcināt, atklāt, mainīt, atspējot, nozagt vai iegūt nesankcionētu piekļuvi informācijas aktīvam vai to izmantot neatļautā veidā.
Kiberdrošība	Informācijas un/vai informācijas sistēmu konfidencialitātes, integritātes un pieejamības saglabāšana, izmantojot kiberlīdzekli.
IKT aktīvs	Programmatūras vai aparatūras aktīvs, kas atrodams uzņēmumdarbības vidē.
IKT projekti	Jebkurš projekts vai tā daļa, kurā IKT sistēmas un pakalpojumi tiek mainīti, aizstāti vai ieviesti.
IKT un drošības risks	Kā operacionālā riska apakškomponente; risks, kas rodas saistībā ar konfidencialitātes pārkāpumu, sistēmu un datu integritātes zudumu, sistēmu un datu neatbilstību vai nepieejamību, kā arī gadījumā, kad, mainoties vides vai uzņēmējdarbības prasībām (t. i., ātrumam), saprātīgā laikposmā un ar saprātīgām izmaksām nav bijis iespējams mainīt IKT. Tas ietver kiberriskus, kā arī informācijas drošības riskus, ko izraisa neatbilstīgi vai nepilnvērtīgi iekšējie procesi vai ārējie notikumi, tostarp kiberuzbrukumi vai neatbilstīga fiziskā drošība.
Informācijas drošība	Informācijas un/vai informācijas sistēmu konfidencialitātes, integritātes un pieejamības saglabāšana. Turklāt var būt iesaistītas arī citas īpašības, piemēram, autentiskums, atbildība, nenoliedzamība un uzticamība.
IKT pakalpojumi	Pakalpojumi, kurus IKT sistēmas un pakalpojuma sniedzēji nodrošina vienam vai vairākiem iekšējiem vai ārējiem lietotājiem.

IKT sistēmas	Lietojumprogrammu, pakalpojumu, informācijas tehnoloģiju aktīvu, IKT aktīvu vai citu informācijas apstrādes komponentu kopums, kas ietver darbības vidi.
Informācijas aktīvs	Materiālas vai nemateriālas informācijas kopums, kuru ir vērts aizsargāt.
Integritāte	Īpašība, kas norāda uz precizitāti un pilnīgumu.
Operacionālais vai drošības incidents	Vienreizējs notikums vai vairāki saistīti, neplānoti notikumi, kuri negatīvi ietekmējuši vai, iespējams, ietekmēs IKT sistēmu un pakalpojumu integritāti, pieejamību un konfidencialitāti.
Pakalpojumu sniedzējs	Trešā persona, kas saskaņā ar vienošanos par ārpakalpojumu izmantošanu kā ārpakalpojumu pilnīgi vai daļēji īsteno procesu, sniedz pakalpojumu vai veic darbību.
Draudos balstīta ielaušanās testēšana	Kontrolēts mēģinājums apdraudēt subjekta kiberizturību, simulējot reālu apdraudējuma dalībnieku taktiku, paņēmienus un procedūras. Tā ir balstīta uz mērķtiecīgas apdraudējumu izlūkošanas datiem un pievēršas organizācijas cilvēkiem, procesiem un tehnoloģijām ar minimālām priekšzināšanām un ietekmi uz darbību.
Ievainojamība	Aktīva vai kontroles vājums, uzņēmība vai trūkums, ko var izmantot viens vai vairāki apdraudējumi.

7. Šīs pamatnostādnes piemēro no 2021. gada 1. jūlija.

1. pamatnostādne. Samērīgums

8. Uzņēmumiem šīs pamatnostādnes būtu jāpiemēro proporcionāli to darbībai raksturīgo risku veidam, pakāpei un sarežģītībai.

2. pamatnostādne. IKT pārvaldes sistēmā

9. Pārvaldes, vadības vai uzraudzības struktūrai (*AMSB*) būtu jānodrošina, ka uzņēmumu pārvaldības sistēma, jo īpaši riska pārvaldības un iekšējās kontroles sistēma, pienācīgi pārvalda uzņēmumu IKT un drošības riskus.

10. *AMSB* būtu jānodrošina, ka uzņēmumu darbinieku skaits un prasmes ir piemērotas, lai pastāvīgi atbalstītu IKT operatīvās vajadzības un IKT un drošības riska pārvaldības procesus, kā arī nodrošinātu to IKT stratēģijas ieviešanu. Turklāt darbiniekiem regulāri būtu jāsaņem atbilstoša apmācība par IKT un drošības riskiem, tostarp informācijas drošību, kā noteikts 13. pamatnostādnē.

11. *AMSB* būtu jānodrošina, ka piešķirtie resursi ir piemēroti, lai izpildītu iepriekš minētās prasības.

3. pamatnostādne. IKT stratēģija

12. *AMSB* ir kopējā atbildība par uzņēmumu rakstiskas IKT stratēģijas izveidošanu un apstiprināšanu to vispārējās uzņēmējdarbības stratēģijas ietvaros, un saskaņojot ar to, kā arī par informēšanas par stratēģiju un tās ieviešanas uzraudzību.

13. IKT stratēģijā būtu jānosaka vismaz:

    a) kā ir jāattīstās uzņēmumu IKT, lai efektīvi atbalstītu un ieviestu to uzņēmējdarbības stratēģijā, ietverot organizatoriskās struktūras attīstību, uzņēmējdarbības modeļus, IKT sistēmu un būtiskos atkarības faktorus no pakalpojumu sniedzējiem;

    b) IKT arhitektūras attīstība, tostarp atkarības faktorus no pakalpojumu sniedzējiem; un

    c) skaidri informācijas drošības mērķi, koncentrējoties uz IKT sistēmām un pakalpojumiem, personālu un procesiem.

14. Uzņēmumiem būtu jānodrošina IKT stratēģijas savlaicīga ieviešana, pieņemšana un visu attiecīgo darbinieku un pakalpojumu sniedzēju informēšana.

15. Uzņēmumiem būtu jāizveido procesi, kas vajadzīgi, lai uzraudzītu un izmērītu IKT stratēģijas ieviešanas efektivitāti. Šis process regulāri būtu jāpārskata un jāatjaunina.

4. pamatnostādne. IKT un drošības riski riska pārvaldības sistēmā

16. *AMSB* ir kopējā atbildība par efektīvas sistēmas izveidi IKT un drošības risku pārvaldībai uzņēmuma vispārējās riska pārvaldības sistēmas ietvaros. Tas ietver sevī riska tolerances noteikšanu šādiem riskiem saskaņā ar uzņēmuma riska stratēģiju un regulāru rakstisku ziņojumu *AMSB* par riska pārvaldības procesa rezultātu.

17. Vispārējās riska pārvaldības sistēmas ietvaros uzņēmumiem saistībā ar IKT un drošības riskiem (vienlaikus nosakot turpmāk aprakstītās IKT aizsardzības prasības) būtu jāņem vērā vismaz šādi aspekti:

    a) uzņēmumiem būtu jāizveido un regulāri jāatjaunina savu uzņēmējdarbības procesu un darbību, uzņēmējdarbības funkciju, lomu un aktīvu (piemēram, informācijas aktīvu un IKT aktīvu) kartējums, nosakot to nozīmi un savstarpējo atkarību no IKT un drošības riskiem;

    b) uzņēmumiem būtu jāidentificē un jānovērtē visi attiecīgie IKT un drošības riski, kuri var tos skart, un jāklasificē identificētie uzņēmējdarbības procesi un darbības, uzņēmējdarbības funkcijas, lomas un aktīvi (piemēram, informācijas aktīvi un IKT aktīvi) pēc to nozīmīguma pakāpes. Uzņēmumiem arī būtu jāizvērtē aizsardzības prasības vismaz attiecībā uz šo uzņēmējdarbības procesu un darbību konfidencialitāti, integritāti un pieejamību, uzņēmējdarbības funkcijām, lomām un aktīviem (piemēram, informācijas aktīvi un IKT aktīvi). Jāidentificē par aktīvu klasifikāciju atbildīgie aktīvu īpašnieki;

    c) metodēm, ko izmanto, lai noteiktu nepieciešamās aizsardzības nozīmīgumu un līmeni, jo īpaši attiecībā uz integritātes, pieejamības un konfidencialitātes

aizsardzības mērķiem, būtu jānodrošina izrietošo aizsardzības prasību konsekvence un to visaptverošais raksturs;

d) IKT un drošības risku mērīšana būtu jāveic, pamatojoties uz definētajiem IKT un drošības riska kritērijiem, ņemot vērā to uzņēmējdarbības procesu un darbību, uzņēmējdarbības funkciju, lomu un aktīvu (piemēram, informācijas aktīvu un IKT aktīvu) nozīmīgumu, zināmos ievainojamības faktorus un iepriekšējos incidentus, kas skāruši uzņēmumu;

e) regulāri būtu jāveic un jādokumentē IKT un drošības risku novērtējums. Šis novērtējums būtu jāveic arī pirms jebkādām būtiskām izmaiņām infrastruktūrā, procesos vai procedūrās, kas skar uzņēmējdarbības procesus un darbības, uzņēmējdarbības funkcijas, lomas un aktīvus (piemēram, informācijas aktīvi un IKT aktīvi);

f) pamatojoties uz savu riska novērtējumu uzņēmumiem būtu vismaz jānosaka un jāīsteno pasākumi identificēto IKT un drošības risku pārvaldīšanai un informācijas aktīvu aizsardzībai atbilstoši to klasifikācijai. Tajā jāiekļauj pasākumu definīcija atlikušo pārējo risku pārvaldībai.

18. IKT un drošības risku pārvaldības procesa rezultātus būtu jāapstiprina *AMSB* un jāiekļauj operacionālā riska pārvaldības procesā uzņēmuma vispārējās riska pārvaldības ietvaros.

5. pamatnostādne. Revīzija

19. Uzņēmumu pārvaldības, sistēmu un procesu attiecībā uz IKT un drošības riskiem periodisku revīziju saskaņā ar uzņēmumu revīzijas plānu[11] veic revidenti, kuriem ir pietiekamas zināšanas, prasmes un kompetence IKT un drošības risku jomā, lai sniegtu *AMSB* objektīvas garantijas par to efektivitāti. Šādu revīziju biežumam un mērķim vajadzētu būt samērīgam ar attiecīgajiem IKT un drošības riskiem.

6. pamatnostādne. Informācijas drošības politika un pasākumi

20. Uzņēmumiem būtu jāizveido *AMSB* apstiprināta rakstiska informācijas drošības politika, kurā nosaka vispārējus principus un noteikumus uzņēmumu informācijas konfidencialitātes, integritātes un pieejamības aizsardzībai IKT stratēģijas ieviešanas nolūkiem.

21. Šajā politikā būtu jāiekļauj informācijas drošības pārvaldības galveno lomu un atbildības apraksts, un tajā ir jāizklāsta prasības darbiniekiem, procesiem un tehnoloģijām attiecībā uz informācijas drošību, nosakot, ka visu līmeņu darbiniekiem ir pienākums nodrošināt uzņēmumu informācijas drošību.

22. Uzņēmumā būtu jāsniedz informācija par politiku, un tai būtu jāattiecas uz visiem darbiniekiem. Attiecīgā gadījumā par informācijas drošības politiku vai tās daļām būtu jāinformē un tās jāpiemēro arī pakalpojumu sniedzējiem.

23. Pamatojoties uz politiku, uzņēmumiem būtu jāizveido un jāievieš konkrētākas informācijas drošības procedūras un informācijas drošības pasākumi, lai cita starpā mazinātu IKT un drošības riskus, kuri tos skar. Šajās procedūrās un informācijas drošības pasākumos būtu jāiekļauj katrs šajās pamatnostādnēs attiecīgi aprakstītais process.

[11] Deleģētās regulas 271. pants.

7. pamatnostādne. Informācijas drošības funkcija

24. Uzņēmumiem savā pārvaldības sistēmā un saskaņā ar samērīguma principu būtu jāizveido informācijas drošības funkcija, uzticot pienākumus nozīmētajai personai. Uzņēmumam būtu jānodrošina šīs informācijas drošības neatkarība un objektivitāte, pienācīgi nodalot to no IKT attīstības un operāciju procesiem. Funkcijai būtu jāatskaitās *AMSB*.

25. Informācijas drošības funkcijas uzdevumi parasti ir šādi:

    a) sniegt atbalstu *AMSB*, nosakot un uzturot informācijas drošības politiku uzņēmumiem, un kontrolējot tās izvietošanu;

    b) regulāri un *ad hoc* informēt un konsultēt *AMSB* par informācijas drošības stāvokli un tā attīstību;

    c) pārraudzīt un pārskatīt informācijas drošības pasākumu īstenošanu;

    d) nodrošināt, ka, izmantojot pakalpojumu sniedzējus, tiek ievērotas informācijas drošības prasības;

    e) nodrošināt, ka visi darbinieki un pakalpojumu sniedzēji, kuriem ir piekļuve informācijai un sistēmām, ir pienācīgi informēti par informācijas drošības politiku, piemēram, organizējot informācijas drošības apmācības un informatīvās sesijas;

    f) koordinēt operacionālo un drošības incidentu pārbaudi un par būtiskajiem informēt *AMSB*.

8. pamatnostādne. Loģiskā drošība

26. Uzņēmumiem būtu jānosaka, jādokumentē un jāievieš procedūras loģiskai piekļuves kontrolei vai loģiskai drošībai (identitātes un piekļuves pārvaldībai) atbilstīgi aizsardzības prasībām, kā noteikts 4. pamatnostādnē. Šīs procedūras būtu jāievieš, jāpiemēro, jāuzrauga un periodiski jāpārskata, un tajās jāiekļauj arī anomāliju uzraudzības pārbaudes. Šajās procedūrās būtu jāīsteno vismaz šādi elementi, ja termins "lietotājs" ietver arī tehniskos lietotājus:

    a) nepieciešamība zināt, mazākā privilēģija un pienākumu nošķiršana: uzņēmumiem būtu jāpārvalda piekļuves tiesības, tostarp attālinātu piekļuvi informācijas aktīviem un to atbalsta sistēmām, pamatojoties uz "nepieciešamību zināt". Lietotājiem būtu jāpiešķir minimālās piekļuves tiesības, kas ir nepārprotami nepieciešamas viņu pienākumu veikšanai ("mazāko privilēģiju" princips), t. i, lai novērstu nepamatotu piekļuvi datiem vai piekļuves tiesību kombināciju piešķiršanu, ko var izmantot, lai apietu kontroles pasākumus ("pienākumu nošķiršanas" princips);

    b) lietotāju atbildība: uzņēmumiem pēc iespējas būtu jāierobežo vispārīgo un koplietojamo lietotāju kontu izmantošana un jānodrošina, lai lietotāji vienmēr varētu tikt identificēti un izsekoti līdz atbildīgai fiziskai personai vai autorizētam uzdevumam attiecībā uz IKT sistēmās veiktajām darbībām;

    c) privileģētas piekļuves tiesības: uzņēmumiem būtu jāīsteno stingri kontroles pasākumi attiecībā uz privileģētu piekļuvi sistēmai, stingri ierobežojot un cieši uzraugot kontus ar paaugstinātām piekļuves tiesībām sistēmai (piemēram, administratora kontus).

    d) attālināta piekļuve: lai nodrošinātu drošu saziņu un samazinātu risku, attālinātā administratīvā piekļuve kritiski svarīgām IKT sistēmām būtu

jāpiešķir tikai, pamatojoties uz "nepieciešamību zināt", un ja tiek izmantoti spēcīgi autentifikācijas risinājumi;

e) lietotāju darbību reģistrēšana: lietotāju darbības būtu jāreģistrē un jāuzrauga proporcionāli riskam, ietverot vismaz priviliģēto lietotāju darbības. Piekļuves žurnāli būtu jāglabā, lai novērstu neatļautu datu modifikāciju vai dzēšanu, un to glabāšanas ilgumam vajadzētu būt atbilstīgam konstatēto darbības funkciju, atbalsta procesu un informācijas aktīvu kritiskumam, neskarot ES un valsts tiesību aktos noteiktās saglabāšanas prasības. Uzņēmumiem būtu jāizmanto šī informācija, lai sekmētu maksājumu pakalpojumu sniegšanā konstatēto netipisku darbību identifikāciju un izmeklēšanu;

f) piekļuves pārvaldība: piekļuves tiesības būtu jāpiešķir, jānoņem un savlaicīgi jānomaina saskaņā ar iepriekš noteikto apstiprināšanas kārtību, ja ir iesaistīts attiecīgā informācijas aktīva īpašnieks. Gadījumā, kad piekļuve vairs nav nepieciešama, piekļuves tiesības būtu nekavējoties jāatceļ;

g) piekļuves novērtējums: piekļuves tiesības būtu periodiski jāpārskata, lai pārliecinātos, ka lietotājiem nav pārmērīgu privilēģiju un ka piekļuves tiesības tiek atsauktas/liegtas, kad tās vairs nav vajadzīgas;

h) piekļuves tiesību piešķiršana, grozīšana un atsaukšana būtu jādokumentē veidā, kas atvieglo izpratni un analīzi; un

i) autentifikācijas metodes: uzņēmumiem būtu jāīsteno autentifikācijas metodes, kas ir pietiekami spēcīgas, lai atbilstoši un efektīvi nodrošinātu atbilstību piekļuves kontroles politikai un procedūrām. Autentifikācijas metodēm vajadzētu būt samērīgām ar IKT sistēmu, informācijas vai piekļuves procesa kritisko svarīgumu. Tam vismaz būtu jāietver spēcīgas paroles vai spēcīgākas autentifikācijas metodes (piemēram, tādu kā divu faktoru autentifikācija), pamatojoties uz attiecīgu risku.

27. Lietojumprogrammu elektroniskā piekļuve datiem un sistēmām būtu jāierobežo līdz minimālajam līmenim, kas nepieciešams attiecīgā pakalpojuma nodrošināšanai.

9. pamatnostādne. Fiziskā drošība

28. Uzņēmumu fiziskās drošības pasākumi (piemēram, aizsardzība pret strāvas padeves pārtraukumiem, ugunsgrēku, plūdiem un neatļautu fizisku piekļuvi) būtu jānosaka, jādokumentē un jāīsteno uzņēmuma telpu, datu centru un jutīgo zonu aizsardzībai pret nesankcionētu piekļuvi un vides apdraudējumiem.

29. Fizisku piekļuvi IKT sistēmām būtu jāatļauj tikai atļauju saņēmušām personām. Atļauja būtu jāpiešķir saskaņā ar personas uzdevumiem un pienākumiem, un — tikai personām, kuras ir atbilstīgi apmācītas un uzraudzītas. Fiziskā pieeja būtu regulāri jāpārskata, lai nodrošinātu, ka nevajadzīgas piekļuves tiesības tiek nekavējoties atsauktas/liegtas.

30. Pienācīgiem pasākumiem aizsardzībai pret vides apdraudējumiem vajadzētu būt samērīgiem ar ēku nozīmi un šajās ēkās izvietoto operāciju vai IKT sistēmu kritisko svarīgumu.

10. pamatnostādne. IKT operacionālā drošība

31. Uzņēmumiem būtu jāievieš procedūras IKT sistēmu un IKT pakalpojumu konfidencialitātes, integritātes un pieejamības nodrošināšanai, lai attiecīgi samazinātu drošības jautājumu ietekmi uz IKT pakalpojumu sniegšanu. Šajās procedūrās būtu atbilstoši jāietver šādi pasākumi:

a) potenciālo ievainojamību identificēšana, kuras būtu jānovērtē un jānovērš, nodrošinot mūsdienīgas IKT sistēmas, tostarp programmatūras, ko uzņēmumi nodrošina saviem iekšējiem un ārējiem lietotājiem, paredzot kritiski svarīgus drošības "programmatūras ielāpus", iekļaujot pretvīrusu definēšanas atjauninājumus vai īstenojot kompensējošus kontroles pasākumus;

b) drošu konfigurācijas bāzlīniju ieviešana visiem nozīmīgajiem komponentiem, piemēram, operētājsistēmām, datu bāzēm, maršrutētājiem un slēdžiem;

c) tīkla segmentēšanas, datu noplūdes novēršanas sistēmu un tīkla plūsmas šifrēšanas ieviešana (saskaņā ar informācijas aktīvu klasifikāciju);

d) galapunktu, tostarp serveru, darbstaciju un mobilo ierīču, aizsardzības ieviešana. Uzņēmumiem būtu jānovērtē, vai galapunkts atbilst to definētajiem drošības standartiem, pirms tam tiek piešķirta piekļuve korporatīvajam tīklam;

e) nodrošināt integritātes pārbaudes mehānismu ieviešanu, pārbaudot IKT sistēmu integritāti;

f) datu, kas ir neaktīvi dati, datu pārsūtīšanas procesā vai aktīvā lietojumā esošu datu šifrēšana (saskaņā ar informācijas aktīvu klasifikāciju).

11. pamatnostādne. Drošības uzraudzība

32. Uzņēmumiem būtu jāizveido un jāievieš procedūras un procesi nepārtrauktai darbību, kuras skar uzņēmumu informācijas drošību, uzraudzībai. Šai uzraudzībai būtu jāaptver vismaz:

    a) iekšējie un ārējie faktori, tostarp uzņēmējdarbības un IKT administratīvās funkcijas;

    b) pakalpojumu sniedzēju, citu organizāciju un iekšējo lietotāju darījumi; un

    c) iespējamie iekšējie un ārējie apdraudējumi.

33. Pamatojoties uz uzraudzību, uzņēmumiem būtu jāievieš piemērotas un efektīvas iespējas atklāt, ziņot un reaģēt uz anomālām darbībām un apdraudējumiem, piemēram, fizisku vai loģisku ielaušanos, informācijas līdzekļu konfidencialitātes, integritātes un pieejamības pārkāpumiem, ļaunprātīgu kodu un publiski zināmām programmatūras un datoraparatūras ievainojamības vietām.

34. Drošības uzraudzības ziņojumiem vajadzētu palīdzēt uzņēmumiem izprast gan operacionālo, gan drošības incidentu būtību, noteikt tendences un sniegt atbalstu uzņēmumu iekšējā izmeklēšanā, kā arī palīdzēt viņiem pieņemt atbilstošus lēmumus.

12. pamatnostādne. Informācijas drošības pārskati, novērtējums un testēšana

35. Uzņēmumiem būtu jāveic dažādi atšķirīgi informācijas drošības pārskati, novērtējumi un testi, lai nodrošinātu savu IKT sistēmu un pakalpojumu ievainojamības aspektu identificēšanu. Piemēram, uzņēmumi var veikt atbilstības analīzi, izmantojot salīdzinājumu ar informācijas drošības standartiem, atbilstības pārskatus, informācijas sistēmu iekšējās un ārējās revīzijas vai fiziskās drošības pārskatus.

36. Uzņēmumiem būtu jāizveido un jāievieš informācijas drošības testēšanas sistēma, kas apstiprinātu informācijas drošības pasākumu stabilitāti un efektivitāti, un būtu jānodrošina, ka šajā sistēmā tiek ņemti vērā apdraudējumi un ievainojamības

faktori, kas identificēti, izmantojot apdraudējumu uzraudzību un IKT un drošības risku novērtēšanas procesu.

37. Testēšana būtu jāveic drošā un uzticamā veidā, un to veic neatkarīgi testētāji, kuriem ir pietiekamas zināšanas, prasmes un kompetence informācijas drošības pasākumu testēšanā.

38. Uzņēmumiem būtu regulāri jāveic testi. Testēšanas tvērumam, biežumam un metodei (piemēram, ielaušanās testēšanai, ieskaitot draudos balstītai ielaušanās testēšanai) vajadzētu būt samērīgiem ar identificēto riska līmeni. Nozīmīgo IKT sistēmu testēšana un ievainojamības skenēšana būtu jāveic katru gadu.

39. Uzņēmumiem būtu jānodrošina, ka drošības pasākumu testi tiek veikti gadījumos, kad notiek izmaiņas infrastruktūrā, procesos vai procedūrās un ja izmaiņas tiek veiktas nopietnu operacionālo vai drošības incidentu dēļ, vai arī tādēļ, ka tirgū tiek laistas jaunas vai būtiski mainītas kritiski svarīgas lietojumprogrammas. Uzņēmumiem būtu jāuzrauga un jāizvērtē drošības testu rezultāti un attiecīgi jāatjaunina savi drošības pasākumi atbilstošā veidā un bez nepamatotas kavēšanās attiecībā uz kritiski svarīgām IKT sistēmām.

13. pamatnostādne. Informācijas drošības apmācība un izpratne

40. Uzņēmumiem būtu jāizveido informācijas drošības apmācības programmas visam personālam, tostarp *AMSB*, lai nodrošinātu, ka viņi ir saņēmuši nepieciešamo apmācību, lai pildītu tiem uzticētos pienākumus un uzdevumus, samazinātu cilvēku kļūdas, zādzības, krāpšanu, ļaunprātīgu izmantošanu vai zaudējumus. Uzņēmumiem būtu jānodrošina, ka apmācības programma regulāri sniedz apmācības visiem darbiniekiem.

41. Uzņēmumiem būtu jāizveido un jāievieš periodiskas drošības izpratnes programmas, lai izglītotu savus darbiniekus, tostarp *AMSB*, par ar informācijas drošību saistīto risku novēršanu.

14. pamatnostādne. IKT darbības vadība

42. Uzņēmumiem būtu jāpārvalda sava IKT darbība, pamatojoties uz IKT stratēģiju. Dokumentos būtu jādefinē, kā uzņēmumi darbojas, uzrauga un kontrolē IKT sistēmas un IKT pakalpojumus, tostarp jādokumentē nozīmīgie IKT procesi, procedūras un darbības.

43. Uzņēmumiem būtu jāievieš reģistrēšanas un uzraudzības procedūras kritiski svarīgām IKT operācijām, kas ļautu atklāt, analizēt un labot kļūdas.

44. Uzņēmumiem būtu jāuztur atjaunināta savu IKT aktīvu uzskaite. IKT aktīvu uzskaitei vajadzētu būt pietiekami detalizētai, lai varētu ātri identificēt IKT aktīvu, tā atrašanās vietu, drošības klasifikāciju un īpašumtiesības.

45. Uzņēmumiem būtu jāuzrauga un jāpārvalda IKT aktīvu aprites cikli, lai nodrošinātu, ka tie arvien ir atbilstīgi un atbalsta uzņēmējdarbības un risku pārvaldības prasības. Uzņēmumiem būtu jāuzrauga, vai ārējie piegādātāji un iekšējie izstrādātāji atbalsta to IKT aktīvus un vai visi attiecīgie programmatūras ielāpi un jauninājumi tiek piemēroti, pamatojoties uz dokumentētiem procesiem. Ir jānovērtē un jāsamazina riski, ko rada novecojuši vai neatbalstīti IKT aktīvi. Norakstītie IKT aktīvi būtu jāapstrādā drošā veidā un jāiznīcina.

46. Uzņēmumiem būtu jāievieš veiktspējas un jaudas plānošanas un uzraudzības procesi, lai savlaicīgi novērstu, atklātu un reaģētu uz svarīgiem IKT sistēmu veiktspējas jautājumiem un IKT jaudas trūkumu.

47. Uzņēmumiem būtu jānosaka un jāievieš datu un IKT sistēmu dublēšanas un atjaunošanas procedūras, lai nodrošinātu, ka datus var atgūt pēc vajadzības. Dublējumu apjoms un biežums būtu jānosaka atbilstoši uzņēmējdarbības atjaunošanas prasībām un datu un IKT sistēmu kritiskajam svarīgumam un jānovērtē saskaņā ar veikto riska novērtējumu. Regulāri jāveic dublēšanas un atjaunošanas procedūru testēšana.

48. Uzņēmumiem būtu jānodrošina, ka datu un IKT sistēmu dublējumkopijas tiek glabātas vienā vai vairākās vietās ārpus primārās atrašanās vietas, kas ir drošas un pietiekami tālu no primārās atrašanās vietas, lai izvairītos no vieniem un tiem pašiem riskiem.

15. pamatnostādne. IKT incidentu un problēmu pārvaldība

49. Uzņēmumiem būtu jāizveido un jāievieš incidentu un problēmu pārvaldības process, lai uzraudzītu un reģistrētu operacionālos vai drošības incidentus un kas dotu iespēju uzņēmumiem turpināt vai atsākt kritiski svarīgās uzņēmējdarbības funkcijas un procesus gadījumos, kad rodas traucējumi.

50. Uzņēmumiem būtu jānosaka piemēroti kritēriji un robežvērtības, lai notikumu klasificētu kā operacionālo vai drošības incidentu, kā arī agrīnas brīdināšanas rādītāji, kam jābrīdina, lai dotu iespēju agrīni atklāt šādus incidentus.

51. Lai samazinātu nelabvēlīgu notikumu ietekmi un ļautu savlaicīgi atgūt datus, uzņēmumiem būtu jāizveido piemēroti procesi un organizatoriskās struktūras, kas nodrošinātu konsekventu un integrētu operacionālo un drošības incidentu uzraudzību, pārvaldību un kontroli un pārliecinātos, ka cēloņi tiek identificēti, risināti un ir īstenotas koriģējošas darbības pasākumi, lai novērstu atkārtotu incidentu rašanos. Incidentu un problēmu pārvaldības procesā vajadzētu noteikt vismaz:

    a) procedūras, lai identificētu, izsekotu, reģistrētu, kategorizētu un klasificētu incidentus pēc uzņēmuma definētajām prioritātēm, pamatojoties uz uzņēmējdarbības kritisko svarīgumu un pakalpojumu līgumiem;

    b) lomas un atbildību dažādiem incidentu scenārijiem (piemēram, kļūdas, darbības traucējumi, kiberuzbrukumi);

    c) problēmu pārvaldības procedūra, lai identificētu, analizētu un atrisinātu viena vai vairāku incidentu pamatcēloni; uzņēmumiem būtu jāanalizē operacionālie vai drošības incidenti, kuri ir identificēti vai notikuši organizācijā un/vai ārpus tās, un būtu jāapsver nozīmīgākā pieredze, kas gūta šajās analīzēs, un attiecīgi jāatjaunina drošības pasākumi;

    d) efektīvus iekšējās saziņas plānus, ietverot paziņojumus par incidentiem un eskalācijas procedūras- attiecībā uz klientu sūdzībām, kas saistītas ar drošību, lai nodrošinātu, ka:

        i. par incidentiem, kas, iespējams, ļoti nelabvēlīgi ietekmē kritiski svarīgās IKT sistēmas un IKT pakalpojumus, tiek ziņots attiecīgajai augstākajai vadībai;

        ii. *AMSB* tiek *ad-hoc* informēta nopietnu incidentu gadījumā un vismaz tiek informēta par ietekmi, reaģēšanu un papildu kontroles pasākumiem, kas jānosaka incidentu rezultātā.

    e) procedūras reaģēšanai uz incidentiem, lai mazinātu ar incidentiem saistīto ietekmi un nodrošinātu, ka pakalpojums laikus kļūst pieejams un ir drošs;

f) īpašus ārējās saziņas plānus kritiski svarīgām uzņēmējdarbības funkcijām un procesiem, lai:

i. sadarbotos ar attiecīgajām ieinteresētajām personām nolūkā efektīvi reaģēt uz incidentu un atgūt tā radītos zaudējumus;

ii. savlaicīgi sniegtu informāciju, tostarp ziņojumus par incidentiem, ārējām personām (piemēram, klientiem, citiem tirgus dalībniekiem, attiecīgajām (uzraudzības) iestādēm, attiecīgā gadījumā un saskaņā ar piemērojamiem noteikumiem).

16. pamatnostādne. IKT projektu vadība

52. Uzņēmumiem būtu jāievieš IKT projektu metodika (tostarp neatkarīgu drošības prasību apsvērumi) ar atbilstošu pārvaldības procesu un projektu īstenošanas vadību, lai efektīvi nodrošinātu IKT stratēģijas īstenošanu, izmantojot IKT projektus.

53. Uzņēmumiem būtu pienācīgi jāuzrauga un jāsamazina riski, kas rodas no IKT projektu portfeļa, ņemot vērā arī riskus, kas var rasties dažādu projektu savstarpējas atkarības faktoru dēļ un vairāku projektu atkarības faktoru dēļ no tiem pašiem resursiem un/vai kompetences.

17. pamatnostādne. IKT sistēmu apguve un izstrāde

54. Uzņēmumiem būtu jāizstrādā un jāievieš process, kas regulē IKT sistēmu iegādi, attīstību un uzturēšanu, lai nodrošinātu, ka apstrādājamo datu konfidencialitāte, integritāte un pieejamība ir visaptveroši nodrošināta un tiek ievērotas noteiktās aizsardzības prasības. Šis process būtu jāizstrādā, izmantojot uz risku balstītu pieeju.

55. Uzņēmumiem būtu jānodrošina, ka pirms sistēmas iegādes vai attīstības darbībām tiek skaidri definētas funkcionālās un nefunkcionālās prasības (tostarp informācijas drošības prasības) un tehniskie mērķi.

56. Uzņēmumiem būtu jānodrošina tādu pasākumu īstenošana, kas izstrādes laikā novērstu netīšas izmaiņas vai tīšu manipulāciju ar IKT sistēmām.

57. Uzņēmumiem vajadzētu būt ieviestai metodikai IKT sistēmu, IKT pakalpojumu un informācijas drošības pasākumu testēšanai un apstiprināšanai.

58. Uzņēmumiem būtu atbilstoši jātestē IKT sistēmas, IKT pakalpojumi un informācijas drošības pasākumi, lai identificētu iespējamās drošības nepilnības, pārkāpumus un incidentus.

59. Uzņēmumiem būtu jānodrošina ražošanas vides nodalīšana no izstrādes, testēšanas un citas vides, kas nav saistīta ar ražošanu.

60. Uzņēmumiem būtu jāīsteno pasākumi IKT sistēmu pirmkodu (ja tādi ir) integritātes aizsardzībai. Tiem būtu arī visaptveroši jādokumentē IKT sistēmu izstrāde, ieviešana, darbība un/vai konfigurēšana, lai samazinātu nevajadzīgu atkarību no attiecīgo jomu ekspertiem.

61. Uzņēmumu procesi IKT sistēmu iegādei un izstrādei būtu jāpiemēro arī attiecībā uz IKT sistēmām, kuras izstrādā vai pārvalda uzņēmējdarbības funkcijas galalietotāji ārpus IKT organizācijas (piemēram, uzņēmējdarbības pārvaldītas lietojumprogrammas vai galalietotāju skaitļošanas lietojumprogrammas), izmantojot uz risku balstītu pieeju. Uzņēmumiem būtu jāuztur tādu lietojumprogrammu reģistrs, kuras atbalsta kritiski svarīgas uzņēmējdarbības funkcijas vai procesus.

18. pamatnostādne. IKT pārmaiņu vadība

62. Uzņēmumiem būtu jāizveido un jāievieš IKT izmaiņu pārvaldības process, lai nodrošinātu, ka visas izmaiņas IKT sistēmās tiek reģistrētas, novērtētas, testētas, apstiprinātas, atļautas un īstenotas kontrolētā veidā. Izmaiņām, kas veiktas steidzamu vai ārkārtas IKT izmaiņu gaitā, vajadzētu būt izsekojamām un par tām *ex post* jāinformē attiecīgais aktīvu īpašnieks *ex post* analīzes nolūkiem.

63. Uzņēmumiem būtu jānosaka, vai izmaiņas esošajā darbības vidē ietekmē esošos drošības pasākumus, vai jāpieņem papildu pasākumi, lai mazinātu saistītos riskus. Šīm izmaiņām vajadzētu būt saskaņā ar uzņēmumu oficiālo pārmaiņu vadības procesu.

19. pamatnostādne. Darbības nepārtrauktības pārvaldība

64. Uzņēmumu vispārējās darbības nepārtrauktības politikas ietvaros *AMSB* atbild par uzņēmumu IKT nepārtrauktības politikas izveidošanu un apstiprināšanu. Par IKT nepārtrauktības politiku uzņēmumos atbilstoši būtu jāinformē, un tai būtu jāattiecas uz visiem attiecīgajiem darbiniekiem un, attiecīgā gadījumā, uz pakalpojumu sniedzējiem.

20. pamatnostādne. Darbības ietekmes analīze

65. Pareizas darbības nepārtrauktības pārvaldības ietvaros uzņēmumiem būtu jāveic darbības ietekmes analīze, kvantitatīvi un kvalitatīvi izvērtējot, cik lielā mērā uzņēmumu skar nopietni darbības traucējumi, un to iespējamo ietekmi, izmantojot iekšējos un/vai ārējos datus un scenāriju analīzi. Darbības ietekmes analīzē būtu jāņem vērā arī identificēto un klasificēto uzņēmējdarbības procesu un darbību, uzņēmējdarbības funkciju, lomu un aktīvu (piemēram, informācijas aktīvu un IKT aktīvu) nozīmīgums un to savstarpējā atkarība saskaņā ar 4. pamatnostādni.

66. Uzņēmumiem būtu jānodrošina, ka to IKT sistēmas un IKT pakalpojumi ir izstrādāti un saskaņoti ar to darbības ietekmes analīzi, piemēram, veidojot dažu kritiski svarīgu komponentu rezervi, lai novērstu traucējumus, ko izraisa notikumi, kas ietekmē šos komponentus.

21. pamatnostādne. Darbības nepārtrauktības plānošana

67. Uzņēmumu darbības nepārtrauktības plānos (DNP) būtu jāņem vērā materiālie riski, kas varētu nelabvēlīgi ietekmēt IKT sistēmas un IKT pakalpojumus. Plāniem būtu jāatbalsta mērķi aizsargāt un nepieciešamības gadījumā atkārtoti izveidot uzņēmējdarbības procesu un darbību, kā arī uzņēmējdarbības funkciju, lomu un aktīvu (piemēram, informācijas aktīvu un IKT aktīvu) konfidencialitāti, integritāti un pieejamību. Šo plānu izstrādes laikā, ja vajadzīgs, uzņēmumiem būtu jāveic saskaņošana ar attiecīgām iekšējām un ārējām ieinteresētajām personām.

68. Uzņēmumiem būtu jāievieš DNP, lai nodrošinātu, ka tie var atbilstoši reaģēt uz iespējamiem atteices scenārijiem atjaunošanas laika mērķa (maksimālais laika periods, kādā sistēma vai process jāatjauno pēc incidenta) un atjaunošanas punkta mērķa (maksimālais laika periods, kurā dati var tikt zaudēti incidentā iepriekš noteiktā pakalpojumu līmenī) ietvaros.

69. Uzņēmumiem savos DNP būtu jāapsver virkne dažādu scenāriju, tostarp ārkārtēji, bet iespējami scenāriji un kiberuzbrukumu scenāriji, un jānovērtē šādu scenāriju iespējamā ietekme. Pamatojoties uz šiem scenārijiem, uzņēmumam būtu jāapraksta, kā tiek nodrošināta IKT sistēmu un pakalpojumu nepārtrauktība, kā arī uzņēmuma informācijas drošība.

22. pamatnostādne. Reaģēšanas un atjaunošanas plāni

70. Pamatojoties uz darbības ietekmes analīzi un ticamiem scenārijiem, uzņēmumiem būtu jāizstrādā reaģēšanas un atjaunošanas plāni. Šajos plānos būtu jāprecizē, kādos apstākļos var būt nepieciešama plāna aktivizēšana un kādas darbības ir jāveic, lai nodrošinātu vismaz uzņēmumu kritiski svarīgo IKT sistēmu un IKT pakalpojumu integritāti, pieejamību, nepārtrauktību un atjaunošanu. Reaģēšanas un atjaunošanas plāniem vajadzētu būt vērstiem uz uzņēmumu operāciju atjaunošanas mērķu sasniegšanu.

71. Reaģēšanas un atjaunošanas plānos attiecīgos gadījumos būtu jāapsver gan īstermiņa, gan ilgtermiņa atjaunošanās iespējas. Plānos būtu vismaz:

    a) jāpievēršas svarīgu IKT pakalpojumu, uzņēmējdarbības funkciju, atbalsta procesu, informācijas aktīvu un to savstarpējās atkarības darbību atjaunošanai, lai izvairītos no nelabvēlīgas ietekmes uz uzņēmuma darbību;

    b) jādokumentē un jānodrošina, ka tie ir pieejami darbības un atbalsta vienībām un tiem ir viegli piekļūt avārijas gadījumā, iekļaujot skaidras lomu un atbildību definīcijas; un

    c) jāatjaunina, ņemot vērā incidentos, testos gūto pieredzi, nesen konstatētie riski, kā arī apdraudējumi un atjaunošanas mērķi un prioritātes, kam bijušas izmaiņas.

72. Plānos būtu jāapsver arī alternatīvas iespējas, ja izmaksu, risku, loģistikas vai neparedzētu apstākļu dēļ atjaunošana īstermiņā var nebūt iespējama.

73. Reaģēšanas un atjaunošanas plānu ietvaros uzņēmumiem būtu jāapsver un jāīsteno nepārtrauktības nodrošināšanas pasākumi, lai mazinātu pakalpojumu sniedzēju atteices ietekmi, kas ir ļoti svarīgi uzņēmumu IKT pakalpojumu nepārtrauktībai (saskaņā ar EAAPI Pamatnostādnēm par pārvaldības sistēmu un par ārpakalpojumiem ar mākoņdatošanu saistītajiem pakalpojumu sniedzējiem)

23. pamatnostādne. Plānu testēšana

74. Uzņēmumiem būtu jātestē savi DNP un jānodrošina, ka to nozīmīgo uzņēmējdarbības procesu un darbību, uzņēmējdarbības funkciju, lomu un aktīvu (piemēram, informācijas aktīvu) un IKT aktīvu un to savstarpējās atkarības (tostarp pakalpojumu sniedzēju nodrošinātās) tiek regulāri testētas, pamatojoties uz uzņēmumu riska profilu.

75. DNP būtu regulāri jāatjaunina, pamatojoties uz testēšanas rezultātiem, jaunāko informāciju par apdraudējumiem un pieredzi, kas gūta no iepriekšējiem notikumiem. Jāiekļauj arī visas attiecīgās izmaiņas atjaunošanas mērķos (tostarp atjaunošanas laika mērķī un atjaunošanas punkta mērķī) un/vai izmaiņas uzņēmējdarbības procesos un darbībās, uzņēmējdarbības funkcijās, lomās un aktīvos (piemēram, informācijas aktīvos un IKT aktīvos).

76. DNP testēšanas rezultātiem vajadzētu pierādīt spēju uzturēt uzņēmuma dzīvotspēju līdz brīdim, kad kritiski svarīgās darbības tiek atjaunotas iepriekš noteiktā pakalpojumu līmenī, vai to triecienizturību.

77. Testu rezultāti būtu jādokumentē, kā arī visas identificētās nepilnības, kas izriet no testiem, būtu jāanalizē, jārisina un jāziņo *AMSB*.

24. pamatnostādne. Krīzes saziņa

78. Uzņēmumiem būtu jānodrošina, ka traucējumu vai ārkārtas situācijas gadījumā, kā arī darbības nepārtrauktības plānu īstenošanas laikā tiem vajadzētu būt sagatavotiem efektīviem krīzes saziņas pasākumiem, lai visas attiecīgās iekšējās un ārējās ieinteresētās personas, tostarp attiecīgās uzraudzības iestādes gadījumos, kad to prasa valsts tiesību akti, kā arī būtiskie pakalpojumu sniedzēji tiktu savlaicīgi un atbilstošā veidā informēti.

25. pamatnostādne. IKT pakalpojumu un IKT sistēmu ārpakalpojumi

79. Neskarot EAAPI Pamatnostādnes par ārpakalpojumiem ar mākoņdatošanu saistītajiem pakalpojumu sniedzējiem, uzņēmumiem būtu jānodrošina, ka gadījumos, kad IKT pakalpojumi un IKT sistēmas tiek uzticēti ārpakalpojumu sniedzējiem, tiek izpildītas attiecīgās prasības attiecībā uz IKT pakalpojumu vai IKT sistēmu.

80. Ārpakalpojumu izmantošanas gadījumā attiecībā uz nozīmīgām vai svarīgām funkcijām uzņēmumiem būtu jānodrošina, lai pakalpojumu sniedzēja līgumsaistības (piemēram, līgums, pakalpojumu līmeņa nolīgumi, izbeigšanas noteikumi attiecīgajos līgumos) ietvertu vismaz:

    a) atbilstošus un samērīgus informācijas drošības mērķus un pasākumus, tostarp tādas prasības kā minimālās informācijas drošības prasības, uzņēmuma datu dzīves cikla specifikācijas, revīzija un piekļuves tiesības un jebkādas prasības attiecībā uz datu centru atrašanās vietu un datu šifrēšanas prasībām, tīkla drošību un drošības uzraudzības procesiem;

    b) pakalpojumu līmeņa nolīgumi, lai nodrošinātu IKT pakalpojumu un IKT sistēmu un darbības mērķu nepārtrauktību normālos apstākļos, kā arī ārkārtas rīcības plānos paredzētajos pakalpojumu nodrošināšanas pārtraukuma gadījumā; un

    c) operacionālo un drošības incidentu apstrādes procedūras, tostarp eskalācija un ziņošana.

81. Uzņēmumiem būtu jāuzrauga šo pakalpojumu sniedzēju atbilstības līmenis un jāpārliecinās, ka tas ir atbilstīgs to drošības mērķiem, pasākumiem un darbības mērķiem.

Atbilstība un ziņošanas noteikumi

82. Šajā dokumentā ir izklāstītas pamatnostādnes, kas izdotas saskaņā ar Regulas (ES) Nr. 1094/2010 16. pantu. Atbilstīgi minētās regulas 16. panta 3. punktam kompetentajām iestādēm un uzņēmumiem jādara viss iespējamais, lai ievērotu pamatnostādnes un ieteikumus.

83. Kompetentajām iestādēm, kuras ievēro vai plāno ievērot šīs pamatnostādnes, tās būtu pienācīgi jāiekļauj savā regulatīvajā vai uzraudzības sistēmā.

84. Kompetentajām iestādēm ir jāapstiprina EAAPI, vai tās ievēro vai plāno ievērot šīs pamatnostādnes, norādot neievērošanas iemeslus, divu mēnešu laikā no tulkoto versiju izdošanas.

85. Ja minētajā termiņā atbilde nebūs saņemta, tiks uzskatīts, ka kompetentās iestādes neievēro ziņošanas noteikumus un par to tiks attiecīgi ziņots.

Nobeiguma noteikums par pārskatīšanu

86. Šo pamatnostādņu pārskatīšanu veiks EAAPI.