EIOPA-BoS-20/600

Obecné pokyny pro bezpečnost a řízení a kontrolu informačních a komunikačních technologií

EIOPA – Westhafen Tower, Westhafenplatz 1 – 60327 Frankfurt – Německo – Tel. + 49 69-951119-20;
Fax + 49 69-951119-19; e-mail: info@eiopa.europa.eu; web: www.eiopa.europa.eu

Obsah

Souvislosti

1. Podle článku 16 nařízení (EU) č. 1094/2010 může orgán EIOPA vydávat obecné pokyny a doporučení určená příslušným orgánům a finančním institucím s cílem zavést jednotné, účinné a efektivní postupy dohledu a zajistit společné, důsledné a jednotné uplatňování práva Unie.

2. V souladu s čl. 16 odst. 3 uvedeného nařízení musí příslušné orgány a finanční instituce vynaložit veškeré úsilí, aby se těmito obecnými pokyny a doporučeními řídily.

3. Orgán EIOPA zjistil, že je třeba vypracovat zvláštní pokyny pro bezpečnost a řízení a kontrolu informačních a komunikačních technologií (IKT) v souvislosti s články 41 a 44 směrnice 2009/138/ES, v rámci analýzy provedené v reakci na akční plán Evropské komise pro finanční technologie (COM(2018)0109 final), plán orgánu EIOPA pro sbližování dohledu na období 2018–2019[1] a v návaznosti na interakce s několika dalšími zúčastněnými stranami[2].

4. Jak je uvedeno ve společném doporučení evropských orgánů dohledu pro Evropskou komisi, obecné pokyny orgánu EIOPA týkající se řídícího a kontrolního systému *„náležitě neodrážejí důležitost zabývat se řízením rizik v oblasti IKT (včetně kybernetických rizik)*. Neexistují žádné pokyny týkající se zásadních prvků, které jsou obecně uznávány jako součást řádné bezpečnosti a řízení a kontroly IKT".

5. Analýza současné (legislativní) situace v EU pro výše uvedené společné doporučení ukázala, že většina členských států EU stanovila vnitrostátní pravidla pro bezpečnost a řízení a kontrolu IKT. I když jsou požadavky obdobné, regulační rámec je stále roztříštěný. Průzkum týkající se současných postupů dohledu navíc odhalil širokou škálu postupů – od „bez zvláštního dohledu" až po „důsledný dohled" (včetně „inspekcí na dálku" a „inspekcí na místě").

6. Kromě toho jsou IKT stále složitější a zvyšuje se také četnost incidentů souvisejících s IKT (včetně kybernetických incidentů) stejně jako škodlivý dopad těchto incidentů na provozní fungování podniků. Z tohoto důvodu má řízení rizik v oblasti IKT a bezpečnosti zásadní význam pro to, aby podnik dosáhl svých strategických, podnikových a provozních cílů a cílů zaměřených na dobrou pověst.

7. Napříč pojišťovnictvím, v případě tradičních i inovativních obchodních modelů, navíc roste závislost na informačních a komunikačních technologiích při poskytování pojišťovacích služeb a v běžném provozním fungování podniků, např. digitalizace pojišťovnictví (technologie pojišťovnictví, internet věcí atd.), jakož i propojenost prostřednictvím telekomunikačních kanálů (internet, mobilní a bezdrátové připojení a sítě typu WAN). V důsledku toho je provoz podniků zranitelný vůči bezpečnostním incidentům, včetně kybernetických útoků. Je proto důležité zajistit, aby byly podniky dostatečně připraveny řídit svá rizika v oblasti IKT a bezpečnosti.

8. Kromě toho tyto obecné pokyny uznávají potřebu, aby byly podniky připraveny na kybernetické riziko[3] a pevný rámec kybernetické bezpečnosti, a zahrnují rovněž kybernetickou bezpečnost jako součást opatření podniku v oblasti bezpečnosti

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

[2] Zprávu zveřejněnou orgánem EIOPA v reakci na akční plán Evropské komise pro finanční technologie lze získat zde.

[3] Definice kybernetického rizika viz FSB Cyber Lexicon, 12. listopadu 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

informací. Ačkoli tyto obecné pokyny uznávají, že kybernetická bezpečnost by měla být řešena v rámci celkového řízení rizik v oblasti IKT a bezpečnosti podniku, je důležité zdůraznit, že kybernetické útoky mají určité specifické rysy, které by měly být zohledněny, aby se zajistilo, že opatření v oblasti bezpečnosti informací kybernetické riziko odpovídajícím způsobem zmírní:

a) kybernetické útoky je v porovnání s většinou jiných zdrojů rizik v oblasti IKT a bezpečnosti často obtížnější řídit (tj. identifikovat, chránit, odhalovat, reagovat na ně a plně se z nich zotavit) a rovněž je obtížné určit rozsah škody;

b) některé kybernetické útoky mohou vést k neúčinnosti společného řízení rizik a společných opatření k zajištění kontinuity činnosti, jakož i postupů pro obnovu provozu po havárii, neboť mohou šířit škodlivý software do záložních systémů s cílem tyto systémy znepřístupnit nebo poškodit zálohovací data;

c) poskytovatelé služeb, makléři, (řídící) agenti a zprostředkovatelé se mohou stát kanály pro šíření kybernetických útoků. Nakažlivé tiché hrozby mohou k cestě do systému IKT podniku využít propojení prostřednictvím telekomunikačních spojení třetích stran. Propojený podnik, který má sám o sobě malý význam, se proto může stát zranitelným a zdrojem šíření rizik a může mít za následek systémový dopad. V souladu se zásadou nejslabšího článku by kybernetická bezpečnost neměla být pouze předmětem zájmu hlavních účastníků trhu nebo poskytovatelů kritických služeb.

9. Cílem těchto obecných pokynů je:

a) poskytnout účastníkům trhu objasnění a transparentnost, pokud jde o minimální očekávané informace a kapacity kybernetické bezpečnosti, tj. základní úroveň bezpečnosti;

b) vyhnout se případné regulatorní arbitráži;

c) podporovat sbližování dohledu, pokud jde o očekávání a postupy použitelné v souvislosti s bezpečností a řízením a kontrolou IKT, jakožto klíče k náležitému řízení rizik v oblasti IKT a bezpečnosti.

Obecné pokyny pro bezpečnost a řízení a kontrolu informačních a komunikačních technologií

Úvod

1. V souladu s článkem 16 nařízení (EU) č. 1094/2010[4] vydává orgán EIOPA tyto obecné pokyny určené orgánům dohledu s cílem poskytnout pokyny k tomu, jak by pojišťovny a zajišťovny (společně dále jen „podniky") měly uplatňovat požadavky v oblasti řízení a kontroly stanovené ve směrnici 2009/138/ES[5] (dále jen „směrnice Solventnost II") a v nařízení Komise v přenesené pravomoci (EU) č. 2015/35[6] (dále jen „nařízení v přenesené pravomoci") v souvislosti s bezpečností a řízením a kontrolou informačních a komunikačních technologií (dále jen „IKT"). Za tímto účelem vycházejí tyto obecné pokyny z ustanovení o řízení a kontrole v článcích 41, 44, 46, 47, 132 a 246 směrnice Solventnost II a článcích 258 až 260, 266, 268 až 271 a 274 nařízení v přenesené pravomoci. Tyto obecné pokyny navíc vycházejí také z pokynů obsažených v obecných pokynech orgánu EIOPA týkajících se řídícího a kontrolního systému (EIOPA-BoS-14/253)[7] a v obecných pokynech orgánu EIOPA týkajících se outsourcingu u poskytovatelů cloudových služeb (EIOPA-BoS-19/270)[8].
2. Tyto obecné pokyny se vztahují jak na jednotlivé podniky, tak obdobně na skupiny[9].
3. Příslušné orgány by měly při plnění těchto obecných pokynů nebo při dohledu nad jejich dodržováním zohledňovat zásadu proporcionality[10], která by měla zajistit, aby řídící a kontrolní postupy, včetně těch, které se týkají bezpečnosti a řízení a kontroly v oblasti IKT, byly přiměřené povaze, rozsahu a komplexnosti odpovídajících rizik, jimž podniky čelí nebo mohou čelit.
4. Tyto obecné pokyny by měly být vykládány ve spojení se směrnicí Solventnost II, s nařízením v přenesené pravomoci, obecnými pokyny orgánu EIOPA týkajícími se řídícího a kontrolního systému a obecnými pokyny orgánu EIOPA týkajícími se outsourcingu u poskytovatelů cloudových služeb, aniž by tím uvedené předpisy byly dotčeny. Tyto obecné pokyny mají být technologicky a metodicky neutrální.

Definice

5. Pokud není v těchto pokynech stanoveno jinak, mají pojmy význam definovaný ve směrnici Solventnost II.
6. Pro účely těchto pokynů se použijí tyto definice:

---

[4] Nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro pojišťovnictví a zaměstnanecké penzijní pojištění), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/79/ES (Úř. věst. L 331, 15.12.2010, s. 48).

[5] Směrnice Evropského parlamentu a Rady 2009/138/ES ze dne 25. listopadu 2009 o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II), (Úř. věst. L 335, 17.12.2019, s. 1).

[6] Nařízení Komise v přenesené pravomoci (EU) 2015/35 ze dne 10. října 2014, kterým se doplňuje směrnice Evropského parlamentu a Rady 2009/138/ES o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II), (Úř. věst. L 12, 17.1.2015, s. 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] Ustanovení čl. 212 odst. 1 směrnice 2009/138/ES.

[10] Ustanovení čl. 29 odst. 3 směrnice 2009/138/ES.

Vlastník aktiv	Osoba nebo subjekt, jež mají odpovědnost a pravomoci v souvislosti s informačními aktivy a aktivy v oblasti IKT.
Dostupnost	Přístupnost a použitelnost na žádost (včasnost) oprávněného subjektu.
Důvěrnost	Skutečnost, že informace se nezpřístupňují ani nesdělují neoprávněným osobám, subjektům, pro nedovolené účely nebo systémy.
Kybernetický útok	Jakýkoli typ hackingu, který vede k útočnému/zlovolnému pokusu zničit, odkrýt, pozměnit, znepřístupnit nebo ukrást informační aktivum, získat k němu neoprávněný přístup nebo ho neoprávněně použít a který se zaměřuje na systémy IKT.
Kybernetická bezpečnost	Zachování důvěrnosti, integrity a dostupnosti informací a/nebo informačních systémů prostřednictvím kybernetického média.
Aktivum v oblasti IKT	Aktivum spočívající v softwaru nebo hardwaru, které se nachází v obchodním prostředí.
Projekty v oblasti IKT	Jakýkoli projekt nebo část projektu, v němž dochází k výměně, náhradě nebo zavádění systémů IKT a služeb v oblasti IKT.
Riziko v oblasti IKT a bezpečnosti	Jako dílčí složka operačního rizika; riziko ztráty v důsledku porušení důvěrnosti, selhání integrity systémů a dat, nevhodnosti nebo nedostupnosti systémů a dat nebo neschopnosti změnit IKT v přiměřeném čase a s přiměřenými náklady, když se mění prostředí nebo požadavky vyplývající z obchodní činnosti (tj. flexibilita). Patří sem kybernetická rizika, jakož i rizika v oblasti bezpečnosti informací vyplývající z nedostatečnosti či selhání vnitřních postupů nebo z vnějších událostí včetně kybernetických útoků či z nedostatečného fyzického zabezpečení.
Bezpečnost informací	Zachování důvěrnosti, integrity a dostupnosti informací a/nebo informačních systémů. Kromě toho mohou být zahrnuty i další prvky, jako například autenticita, odpovědnost, nepopiratelnost a spolehlivost.
Služby v oblasti IKT	Služby poskytované prostřednictvím systémů IKT a poskytovatelů služeb jednomu nebo několika interním či externím uživatelům.

Systémy IKT	Soubor aplikací, služeb, aktiv v oblasti informačních technologií, aktiv v oblasti IKT nebo jiných složek pro nakládání s informacemi, který zahrnuje provozní prostředí.
Informační aktivum	Shromážděné informace, hmotné nebo nehmotné, které je třeba chránit.
Integrita	Přesnost a úplnost.
Provozní nebo bezpečnostní incident	Jednorázová událost nebo řada souvisejících neplánovaných událostí, které mají nebo pravděpodobně budou mít nepříznivý dopad na integritu, dostupnost a důvěrnost systémů IKT a služeb v oblasti IKT.
Poskytovatel služeb	Znamená třetí stranu, která na základě ujednání o externím zajištění služeb nebo činností (outsourcingu) vykonává proces, službu nebo činnost nebo jejich část.
Penetrační testování na základě hrozeb	Řízený pokus o ohrožení kybernetické odolnosti subjektu tím, že simuluje taktiku, techniky a postupy aktérů zabývajících se reálnými hrozbami. Je založen na cíleném zpravodajství o hrozbách a zaměřuje se na lidi, procesy a technologie subjektu s minimálním povědomím a dopadem na provoz.
Zranitelnost	Slabost, vnímavost nebo vada aktiva nebo kontroly, kterou lze využít prostřednictvím jedné nebo více hrozeb.

7. Tyto obecné pokyny se použijí od 1. července 2021.

Obecný pokyn 1 – Proporcionalita

8. Podniky by měly tyto obecné pokyny uplatňovat způsobem, který je přiměřený povaze, rozsahu a komplexnosti rizik spojených s jejich činností.

Obecný pokyn 2 – IKT v rámci řídícího a kontrolního systému

9. Správní, řídící nebo kontrolní orgán by měl zajistit, aby řídící a kontrolní systém podniků, zejména systém řízení rizik a vnitřní kontroly, vhodně řídil rizika podniků v oblasti IKT a bezpečnosti.

10. Správní, řídící nebo kontrolní orgán by měl zajistit, aby počet zaměstnanců podniků a jejich dovednosti byly přiměřené pro průběžnou podporu jejich provozních potřeb v oblasti IKT a jejich postupů pro řízení rizik v oblasti IKT a bezpečnosti a pro zajištění realizace jejich strategie v oblasti IKT. Kromě toho by zaměstnanci měli pravidelně absolvovat odpovídající odbornou přípravu v oblasti IKT a

bezpečnostních rizik, včetně bezpečnosti informací, jak je stanoveno v obecném pokynu 13.

11. Správní, řídicí nebo kontrolní orgán by měl zajistit, aby přidělené zdroje byly přiměřené pro splnění výše uvedených požadavků.

Obecný pokyn 3 – Strategie v oblasti IKT

12. Správní, řídicí nebo kontrolní orgán nese celkovou odpovědnost za stanovení a schválení písemné strategie podniků v oblasti IKT jako součásti jejich celkové obchodní strategie a v souladu s ní, jakož i za dohled nad jejím oznámením a prováděním.

13. Strategie v oblasti IKT by měla definovat alespoň:

    a) jak by se měly IKT podniků vyvíjet, aby účinně podporovaly a realizovaly jejich obchodní strategii, včetně vývoje organizační struktury, obchodních modelů, systému IKT a klíčových vztahů závislosti s poskytovateli služeb;

    b) vývoj architektury IKT, včetně vztahů závislosti s poskytovateli služeb, a

    c) jasné cíle v oblasti bezpečnosti informací se zaměřením na systémy a služby, zaměstnance a procesy v oblasti IKT.

14. Podniky by měly zajistit, aby strategie v oblasti IKT byla včas provedena, přijata a sdělena všem příslušným zaměstnancům, a případně příslušným poskytovatelům služeb.

15. Podniky by také měly zavést postup sledování a měření účinnosti provádění jejich strategie v oblasti IKT. Tento postup by měl být pravidelně přezkoumáván a aktualizován.

Obecný pokyn 4 – IKT a bezpečnostní rizika v rámci systému řízení rizik

16. Správní, řídicí nebo kontrolní orgán nese celkovou odpovědnost za vytvoření účinného systému řízení rizik v oblasti IKT a bezpečnosti v rámci celkového systému řízení rizik podniku. To zahrnuje určení tolerance pro tato rizika v souladu se strategií podniku v oblasti rizik a pravidelnou písemnou zprávu o výsledku procesu řízení rizik určenou správnímu, řídicímu nebo kontrolnímu orgánu.

17. V rámci svého celkového systému řízení rizik by podniky měly v souvislosti s riziky v oblasti IKT a bezpečnosti (při definování požadavků na ochranu IKT, jak je popsáno níže) zvážit alespoň tyto aspekty:

    a) podniky by měly vytvořit a pravidelně aktualizovat mapování svých obchodních procesů a činností, obchodních funkcí, úloh a aktiv (např. informačních aktiv a aktiv v oblasti IKT) s cílem určit jejich význam a vzájemnou závislost na rizicích v oblasti IKT a bezpečnosti;

    b) podniky by měly určit a měřit všechna příslušná rizika v oblasti IKT a bezpečnosti, kterým jsou vystaveny, a klasifikovat určené obchodní procesy a činnosti, obchodní funkce, úlohy a aktiva (např. informační aktiva a aktiva v oblasti IKT) z hlediska kritičnosti. Podniky by měly rovněž posoudit alespoň požadavky na ochranu důvěrnosti, integrity a dostupnosti těchto obchodních procesů a činností, obchodních funkcí, úloh a aktiv (např. informačních aktiv a aktiv v oblasti IKT). Měli by být určeni vlastníci aktiv, kteří jsou odpovědní za klasifikaci aktiv;

c) metody používané k určení kritičnosti a požadované úrovně ochrany, zejména s ohledem na cíle ochrany integrity, dostupnosti a důvěrnosti, by měly zajistit, aby výsledné požadavky na ochranu byly jednotné a komplexní;

d) měření rizik v oblasti IKT a bezpečnosti by mělo být prováděno na základě stanovených kritérií rizik v oblasti IKT a bezpečnosti s přihlédnutím ke kritičnosti jejich obchodních procesů a činností, obchodních funkcí, úloh a aktiv (např. informačních aktiv a aktiv v oblasti IKT), k rozsahu známých zranitelností a předchozím incidentům, které měly dopad na podnik;

e) posouzení rizik v oblasti IKT a bezpečnosti by mělo být prováděno a dokumentováno pravidelně. Toto posouzení by mělo být rovněž provedeno před jakoukoli významnou změnou infrastruktury, procesů nebo postupů, která má vliv na obchodní procesy a činnosti, obchodní funkce, úlohy a aktiva (např. informační aktiva a aktiva v oblasti IKT);

f) na základě svého posouzení rizik by podniky měly alespoň vymezit a provést opatření k řízení zjištěných rizik v oblasti IKT a bezpečnosti a chránit informační aktiva v souladu s jejich klasifikací. To by mělo zahrnovat vymezení opatření k řízení zbytkových rizik.

18. Výsledky procesu řízení rizik v oblasti IKT a bezpečnosti by měly být schváleny správním, řídicím nebo kontrolním orgánem a měly by být zahrnuty do procesu řízení provozního rizika jako součást celkového řízení rizik podniků.

Obecný pokyn 5 – Audit

19. Řízení a kontrola, systémy a procesy podniků, pokud jde o jejich rizika v oblasti IKT a bezpečnosti, by měly být v souladu s auditním plánem podniků[11] pravidelně kontrolovány auditory, kteří mají dostatečné znalosti, dovednosti a dostatečnou odbornost, co se týče rizik v oblasti IKT a bezpečnosti, aby správnímu, řídicímu nebo kontrolnímu orgánu poskytli nezávislé ujištění o jejich účinnosti. Četnost a zaměření těchto auditů by měly odpovídat příslušným rizikům v oblasti IKT a bezpečnosti.

Obecný pokyn 6 – Politika a opatření v oblasti bezpečnosti informací

20. Podniky by měly zavést písemnou politiku bezpečnosti informací schválenou správním, řídicím nebo kontrolním orgánem, která by měla vymezovat nejdůležitější zásady a pravidla na ochranu důvěrnosti, integrity a dostupnosti informací podniků s cílem podpořit provádění strategie v oblasti IKT.

21. Politika by měla zahrnovat popis hlavních úloh a povinností v oblasti řízení bezpečnosti informací a měla by stanovit požadavky na zaměstnance, procesy a technologie v souvislosti s bezpečností informací a uznat, že zaměstnanci na všech úrovních mají při zajišťování bezpečnosti informací podniků určité povinnosti.

22. Tato politika by měla být oznámena v rámci podniku a měla by se vztahovat na všechny zaměstnance. V příslušném případě, a je-li to relevantní, by politika bezpečnosti informací nebo její části měly být oznámeny poskytovatelům služeb a vůči nim uplatňovány.

23. Na základě této politiky by podniky měly zavést a provádět konkrétnější postupy a opatření v oblasti bezpečnosti informací mimo jiné s cílem zmírnit rizika v oblasti IKT a bezpečnosti, jimž jsou vystaveny. Tyto postupy a opatření v oblasti

[11] Článek 271 nařízení v přenesené pravomoci.

bezpečnosti informací by měly zahrnovat každý proces popsaný v těchto obecných pokynech.

Obecný pokyn 7 – Funkce bezpečnosti informací

24. Podniky by měly v rámci svého řídícího a kontrolního systému a v souladu se zásadou proporcionality zřídit funkci bezpečnosti informací, která bude plnit úkoly svěřené určené osobě. Podnik by měl zajistit nezávislost a objektivitu této funkce bezpečnosti informací tak, že ji vhodným způsobem oddělí od procesů vývoje a provozu IKT. Tato funkce by měla být podřízena správnímu, řídicímu nebo kontrolnímu orgánu.

25. Úkolem funkce bezpečnosti informací je obvykle:

    a) podporovat správní, řídicí nebo kontrolní orgán při vymezování a udržování politiky bezpečnosti informací pro podniky a kontrolovat její uplatňování;

    b) pravidelně a *ad hoc* podávat zprávy a poskytovat poradenství správnímu, řídicímu nebo kontrolnímu orgánu o stavu bezpečnosti informací a o jejím vývoji;

    c) sledovat a přezkoumávat provádění opatření v oblasti bezpečnosti informací;

    d) zajistit, aby při využívání poskytovatelů služeb byly dodržovány požadavky na bezpečnost informací;

    e) zajistit, aby všichni zaměstnanci a poskytovatelé služeb, kteří mají přístup k informacím a systémům, byli odpovídajícím způsobem informováni o politice bezpečnosti informací, například prostřednictvím školení a informačních akcí v oblasti bezpečnosti informací;

    f) koordinovat posuzování provozních nebo bezpečnostních incidentů a o významných incidentech podávat zprávy správnímu, řídicímu nebo kontrolnímu orgánu.

Obecný pokyn 8 – Logická bezpečnost

26. Podniky by měly vymezit, zdokumentovat a provádět postupy kontroly logického přístupu nebo logické bezpečnosti (řízení totožnosti a přístupu) v souladu s požadavky na ochranu, jak je vymezeno v obecném pokynu 4. Tyto postupy by měly být prováděny, vymáhány, sledovány a pravidelně přezkoumávány a jejich součástí by měly být i kontroly za účelem sledování anomálií. Tyto postupy by měly zavést alespoň dále uvedené prvky, přičemž výraz „uživatel" zahrnuje i technické uživatele:

    a) vědět jen to potřebné, zásada minimálních práv a oddělení funkcí: podniky by měly práva přístupu, včetně vzdáleného přístupu, k informačním aktivům a ke svým podpůrným systémům spravovat na základě zásady „vědět jen to potřebné". Uživatelům by měla být udělena minimální přístupová práva, která jsou nezbytně nutná k plnění jejich povinností (zásada „minimálních práv"), aby se zabránilo neoprávněnému přístupu k datům nebo přidělení kombinací přístupových práv, které lze použít k obcházení kontrolních prvků (zásada „oddělení funkcí");

    b) odpovědnost uživatele: podniky by měly co nejvíce omezit používání obecných a sdílených uživatelských účtů a u akcí prováděných v systémech IKT by měly zajistit možnost uživatele kdykoliv identifikovat a vysledovat ho zpět k odpovědné fyzické osobě nebo pověřenému úkolu;

c) privilegovaná přístupová práva: podniky by měly zavést přísné prvky kontroly privilegovaných přístupů do systému pomocí přísného omezení účtů se zvýšenými právy přístupu k systému (např. účtů administrátora) a měly by nad těmito účty zajišťovat pečlivý dohled;

d) vzdálený přístup: aby byla zajištěna bezpečná komunikace a snížena rizika, měl by být vzdálený administrativní přístup ke kritickým systémům IKT poskytován pouze na základě zásady „vědět jen to potřebné" a měla by být používána účinná řešení pro ověřování identity;

e) je třeba zajistit vedení auditních záznamů a monitorování činností uživatelů zahrnující přinejmenším činnosti privilegovaných uživatelů, a to způsobem přiměřeným rizikům. Záznamy o přístupu by měly být zabezpečeny tak, aby se předešlo jejich neoprávněným úpravám nebo výmazu, a měly by být uloženy po dobu odpovídající kritičnosti identifikovaných obchodních funkcí, podpůrných procesů a informačních aktiv, aniž by byly dotčeny požadavky na uchovávání údajů stanovené v unijních a vnitrostátních právních předpisech. Podniky by měly tyto informace používat k usnadnění identifikace a vyšetřování neobvyklých činností, které byly zjištěny při poskytování služeb;

f) řízení přístupu: přístupová práva by měla být udělována, odebírána a upravována včas, a to v souladu s předem stanovenými postupy schvalování, pokud se jedná o vlastníka příslušného informačního aktiva. V případě, že přístup již není nutný, měla by být přístupová práva okamžitě zrušena;

g) posuzování přístupu: přístupová práva by měla být pravidelně přezkoumávána s cílem zajistit, aby uživatelé nepožívali nadměrných výsad a aby byla přístupová práva odebrána, jakmile již nebudou zapotřebí;

h) udělení, úprava nebo odebrání přístupových práv by měly být zdokumentovány způsobem, který usnadňuje porozumění a analýzu, a

i) metody ověření: podniky by měly prosazovat metody ověření, které jsou dostatečně robustní, aby přiměřeně a účinně zajistily dodržování zásad a postupů kontroly přístupu. Metody ověření by měly odpovídat kritičnosti systémů IKT, informací nebo procesu, k nimž se přistupuje. Měly by zahrnovat přinejmenším silná hesla nebo silnější metody ověření (například dvoufaktorové ověření) podle příslušného rizika.

27. Elektronický přístup prostřednictvím aplikací k datům a systémům IKT by měl být omezen na minimum, které je nutné k poskytování příslušné služby.

Obecný pokyn 9 – Fyzická bezpečnost

28. Je třeba vymezit, zdokumentovat a provádět opatření pro fyzické zabezpečení (např. ochrana před výpadkem proudu, požárem, vodou a neoprávněným fyzickým přístupem) podniků na ochranu jejich prostor, datových center a citlivých oblastí před neoprávněným přístupem a před riziky okolního prostředí.

29. Fyzický přístup k systémům IKT by měl být povolen pouze oprávněným osobám. Oprávnění by mělo být přiděleno v souladu s úkoly a povinnostmi dané osoby a mělo by být omezeno na osoby, které jsou řádně proškoleny a sledovány. Fyzický přístup by měl být pravidelně přezkoumáván, aby bylo v případě potřeby zajištěno neprodlené odebrání nepotřebných přístupových práv.

30. Přiměřená opatření na ochranu před riziky okolního prostředí by měla být úměrná důležitosti budov a kritičnosti operací nebo systémů IKT umístěných v těchto budovách.

Obecný pokyn 10 – Bezpečnost provozu IKT

31. Podniky by měly zavést postupy k zajištění důvěrnosti, integrity a dostupnosti systémů IKT a služeb v oblasti IKT s cílem minimalizovat dopad bezpečnostních incidentů na poskytování služeb v oblasti IKT. Tyto postupy by měly odpovídajícím způsobem zahrnovat následující opatření:

    a) identifikace potenciálních zranitelností, které by měly být vyhodnoceny a napraveny zajištěním aktualizace systémů IKT, včetně softwaru, který podniky poskytují svým interním a externím uživatelům, provedením kritických bezpečnostních oprav, včetně aktualizací virových definic, nebo zavedením kompenzačních kontrol;

    b) zavedení požadavků na bezpečnostní konfigurace všech kritických komponent, jako jsou operační systémy, databáze, směrovače nebo přepínače;

    c) zavedení segmentace sítě, systémů prevence úniků dat a šifrování síťového provozu (v souladu s klasifikací informačních aktiv);

    d) zavedení ochrany koncových bodů včetně serverů, pracovních stanic a mobilních zařízení. Podniky by měly vyhodnotit, zda koncový bod splňuje jimi vymezené bezpečnostní standardy, než bude těmto bodům umožněn přístup do podnikové sítě;

    e) zajištění toho, aby byly zavedeny mechanismy pro ověření integrity systémů IKT;

    f) šifrování uložených dat a přenášených dat (v souladu s klasifikací informačních aktiv).

Obecný pokyn 11 – Bezpečnostní monitorování

32. Podniky by měly zavést a provádět postupy a procesy pro průběžné sledování činností, které mají dopad na bezpečnost informací podniků. Sledování by mělo přinejmenším zahrnovat:

    a) interní a externí faktory, včetně obchodních a správcovských funkcí v systému informačních a komunikačních technologií;

    b) transakce prováděné poskytovateli služeb, jinými subjekty a interními uživateli a

    c) potenciální interní a externí hrozby.

33. Na základě sledování by podniky měly zavést vhodné a účinné kapacity pro odhalování a oznamování neobvyklých činností a hrozeb, jako jsou fyzické nebo logické narušení, narušení důvěrnosti, integrity a dostupnosti informačních aktiv, škodlivý kód a veřejně známé zranitelnosti softwaru a hardwaru, a pro reakci na ně.

34. Podávání zpráv z bezpečnostního monitorování by mělo podnikům pomoci pochopit povahu provozních nebo bezpečnostních incidentů, určit trendy a podpořit vnitřní vyšetřování podniků a umožnit jim přijímat vhodná rozhodnutí.

Obecný pokyn 12 – Přezkumy, hodnocení a testování bezpečnosti informací

35. Podniky by měly provádět nejrůznější přezkumy, hodnocení a testování bezpečnosti informací, aby zajistily účinnou identifikaci zranitelností ve svých systémech IKT a službách v oblasti IKT. Podniky mohou například provádět diferenční analýzu podle

standardů bezpečnosti informací, přezkumy dodržování předpisů, interní a externí audity informačních systémů nebo kontroly fyzického zabezpečení.

36. Podniky by měly stanovit a provádět rámec pro testování bezpečnosti informací, který ověřuje spolehlivost a účinnost opatření v oblasti bezpečnosti informací, a měly by zajistit, aby tento rámec zohledňoval hrozby a zranitelnosti identifikované prostřednictvím sledování hrozeb a procesu posouzení rizik v oblasti IKT a bezpečnosti.

37. Testování by mělo být prováděno bezpečným a zabezpečeným způsobem a nezávislými testovacími subjekty s dostatečnými znalostmi, dovednostmi a dostatečnou odborností v oblasti testování opatření pro bezpečnost informací.

38. Podniky by měly testy provádět pravidelně. Rozsah, četnost a metoda testování (např. penetrační testy, včetně penetračního testování na základě hrozeb) by měly být úměrné úrovni zjištěného rizika. Testování kritických systémů IKT a kontroly zranitelností by měly být prováděny každoročně.

39. Podniky by měly zajistit, aby byly testy bezpečnostních opatření prováděny v případě změn infrastruktury, procesů nebo postupů a v případě, že dojde ke změnám v důsledku závažných provozních nebo bezpečnostních incidentů nebo v důsledku vydání nových nebo výrazně změněných kritických aplikací. Podniky by měly sledovat a vyhodnocovat výsledky bezpečnostních testů a odpovídajícím způsobem aktualizovat svá bezpečnostní opatření, v případě kritických systémů IKT bez zbytečného prodlení.

Obecný pokyn 13 – Odborná příprava a povědomí týkající se bezpečnosti informací

40. Podniky by měly zavést programy odborné přípravy v oblasti bezpečnosti informací pro všechny zaměstnance, včetně správního, řídicího nebo kontrolního orgánu, aby zajistily, že zaměstnanci budou proškoleni k plnění svých úkolů a povinností, s cílem omezit lidské chyby, krádeže, podvody, zneužití nebo ztráty. Podniky by měly zajistit, aby program odborné přípravy pravidelně zajišťoval školení pro všechny zaměstnance.

41. Podniky by měly zavést a provádět pravidelné programy pro zvyšování povědomí o bezpečnosti s cílem vzdělávat své zaměstnance, včetně správního, řídicího nebo kontrolního orgánu, ohledně způsobu řešení rizik souvisejících s bezpečností informací.

Obecný pokyn 14– Řízení provozu IKT

42. Podniky by měly řídit svůj provoz IKT na základě strategie v oblasti IKT. Dokumenty by měly vymezit, jak podniky provozují, sledují a kontrolují systémy IKT a služby v oblasti IKT, včetně dokumentování kritických procesů, postupů a operací v oblasti IKT.

43. Podniky by měly u kritických částí provozu IKT zavést postupy logování a sledování, které umožní odhalit, analyzovat a opravit chyby.

44. Podniky by měly udržovat aktuální soupis svých aktiv v oblasti IKT. Soupis aktiv v oblasti IKT by měl být dostatečně podrobný, aby umožnil okamžitou identifikaci aktiva v oblasti IKT, jeho umístění, bezpečnostní klasifikace a odpovědnosti za aktivum.

45. Podniky by měly sledovat a řídit životní cykly aktiv v oblasti IKT, aby zajistily, že aktiva budou i nadále splňovat a podporovat požadavky týkající se obchodu a řízení

rizik. Podniky by měly sledovat, zda jejich dodavatelé nebo interní vývojáři podporují jejich aktiva v oblasti IKT a zda jsou všechny příslušné opravy a aktualizace prováděny na základě zdokumentovaného procesu. Je třeba posuzovat a zmírňovat rizika vyplývající ze zastaralých nebo nepodporovaných aktiv v oblasti IKT. Aktiva v oblasti IKT vyřazená z provozu by měla být bezpečně zpracována a zlikvidována.

46. Podniky by měly zavést procesy plánování a monitorování výkonnosti a kapacity, aby včas předešly závažným problémům v oblasti výkonnosti systémů IKT a nedostatkům kapacity v oblasti IKT a aby tyto problémy včas zjišťovaly a reagovaly na ně.

47. Podniky by měly vymezit a provádět postupy zálohování a obnovy dat a systémů IKT, aby bylo zajištěno, že tato data a systémy bude možné v případě potřeby obnovit. Rozsah a četnost záloh by měly být stanoveny podle požadavků na obnovení činnosti a kritičnosti dat a systémů IKT a měly by být hodnoceny podle provedeného posouzení rizik. Pravidelně by mělo být prováděno testování postupů zálohování a obnovy.

48. Podniky by měly zajistit, aby zálohy dat a systémů IKT byly uloženy mimo primární místo na jednom nebo více místech, která jsou bezpečná a dostatečně vzdálená od primárního místa, díky čemuž nebudou vystaveny stejným rizikům.

Obecný pokyn 15 – Řízení incidentů a problémů v oblasti IKT

49. Podniky by měly stanovit a provádět proces řízení incidentů a problémů s cílem sledovat a zaznamenávat provozní a bezpečnostní incidenty a umožnit podnikům pokračování nebo obnovení kritických obchodních funkcí a procesů v případě narušení.

50. Podniky by měly stanovit příslušná kritéria a prahové hodnoty ke klasifikaci události jako provozního nebo bezpečnostního incidentu a také indikátory včasného varování, které by měly sloužit jako upozornění umožňující tyto incidenty včas odhalit.

51. Aby minimalizovaly dopad nepříznivých událostí a umožnily včasnou obnovu, měly by podniky stanovit vhodné postupy a organizační struktury, které zajistí jednotné a integrované sledování, řešení a návazné sledování provozních a bezpečnostních incidentů a zabezpečí, aby byly identifikovány a odstraněny hlavní příčiny a byla přijata nápravná opatření / opatření, aby se předešlo výskytu opakovaných incidentů. Postup řízení incidentů a problémů by měl stanovit alespoň:

    a) postupy pro identifikaci, zpětné sledování, zaznamenávání, kategorizaci a klasifikaci incidentů podle priority definované podnikem a na základě kritičnosti z hlediska obchodní činnosti a dohod o službách;

    b) úlohy a povinnosti pro různé scénáře incidentů (např. chyby, poruchy, kybernetické útoky);

    c) postupy řízení problémů s cílem identifikovat, analyzovat a vyřešit hlavní příčinu jednoho nebo více incidentů; podniky by měly analyzovat provozní nebo bezpečnostní incidenty, které byly identifikovány nebo se vyskytly uvnitř nebo vně organizace, a měly by zvážit hlavní poznatky získané z těchto analýz a odpovídajícím způsobem aktualizovat bezpečnostní opatření;

    d) účinné plány interní komunikace včetně postupů pro oznamování incidentů a jejich předání na vyšší úroveň řízení (zahrnující i stížnosti zákazníků související s bezpečností), které zajistí:

i. aby byly incidenty s potenciálně velkým nepříznivým dopadem na kritické systémy IKT a služby v oblasti IKT oznamovány příslušnému vrcholovému vedení;

ii. aby byl v případě závažných incidentů správní, řídicí nebo kontrolní orgán informován *ad hoc* a aby byl vyrozuměn přinejmenším o dopadu, reakci a dodatečných kontrolách, které mají být stanoveny v důsledku incidentů;

e) postupy reakce na incidenty ke zmírnění dopadů souvisejících s incidenty a zajištění včasného obnovení činnosti a bezpečnosti služby;

f) specifické plány externí komunikace pro kritické obchodní funkce a procesy s cílem:

i. spolupracovat s příslušnými zainteresovanými subjekty za účelem účinné reakce na incident a obnovy po incidentu;

ii. poskytnout včasné informace, včetně oznámení incidentu, externím stranám (např. zákazníkům, ostatním účastníkům trhu, příslušnému orgánu dohledu) podle potřeby a v souladu s platnými předpisy.

Obecný pokyn 16 – Řízení projektů v oblasti IKT

52. Podniky by měly zavést metodiku pro projekty v oblasti IKT (včetně nezávislého zvážení bezpečnostních požadavků) s odpovídajícím procesem řízení a kontroly a vedením při realizaci projektů, aby bylo prostřednictvím projektů IKT účinně podporováno provádění strategie v oblasti IKT.

53. Podniky by měly náležitě sledovat a zmírňovat rizika vyplývající z jejich portfolia projektů v oblasti IKT a brát v úvahu také rizika, která mohou vyplývat ze vzájemných závislostí mezi různými projekty a ze závislostí více projektů na týchž zdrojích nebo odborných znalostech.

Obecný pokyn 17 – Pořizování a vývoj systémů IKT

54. Podniky by měly vyvinout a zavést postup upravující pořízení, vývoj a údržbu systémů IKT s cílem zajistit, aby byla srozumitelně zajištěna důvěrnost, integrita a dostupnost zpracovávaných údajů a byly splněny stanovené požadavky na ochranu. Tento postup by měl být navržen pomocí přístupu založeného na riziku.

55. Podniky by měly zajistit, aby před provedením jakéhokoli nákupu nebo vývoje systému byly jasně vymezeny funkční a jiné než funkční požadavky (včetně požadavků na bezpečnost informací) a technické cíle.

56. Podniky by měly zajistit, aby byla zavedena opatření, která zabrání nezáměrné změně nebo záměrnému zmanipulování systémů IKT během vývoje.

57. Podniky by měly mít zavedenu metodiku testování a schvalování systémů IKT, služeb v oblasti IKT a opatření pro bezpečnost informací.

58. Podniky by měly odpovídajícím způsobem testovat systémy IKT, služby v oblasti IKT a opatření pro bezpečnost informací tak, aby identifikovaly možná slabá místa, narušení a incidenty v oblasti bezpečnosti.

59. Podniky by měly zajistit oddělení produkčních prostředí od vývojových, testovacích a ostatních neprodukčních prostředí.

60. Podniky by měly zavést opatření na ochranu integrity zdrojového kódu (je-li k dispozici) systémů IKT. Měly by také komplexně dokumentovat vývoj, zavádění,

provoz nebo konfiguraci systémů IKT, aby se snížila jakákoli nadbytečná závislost na odbornících v dané oblasti.

61. Postupy podniků pro pořízení a vývoj systémů IKT by se měly vztahovat i na systémy IKT vyvinuté nebo řízené koncovými uživateli obchodních funkcí mimo organizaci IKT (např. podnikové aplikace nebo počítačové aplikace koncových uživatelů) s využitím přístupu založeného na riziku. Podnik by měl vést evidenci aplikací, které podporují kritické obchodní funkce nebo procesy.

Obecný pokyn 18 – Řízení změn v oblasti IKT

62. Podniky by měly stanovit a zavést proces řízení změn v oblasti IKT, aby zajistily, že všechny změny systémů IKT budou zaznamenávány, posuzovány, testovány, schvalovány, prováděny a ověřovány kontrolovaným způsobem. Naléhavé nebo mimořádné změny v oblasti IKT by měly být dohledatelné a měly by být následně oznámeny vlastníkovi příslušného aktiva pro účely následné analýzy.

63. Podniky by měly průběžně zjišťovat, zda změny stávajícího provozního prostředí ovlivňují stávající bezpečnostní opatření nebo vyžadují přijetí dalších opatření, aby se zmírnila příslušná rizika. Tyto změny by měly být v souladu s formálním procesem podniků pro řízení změn.

Obecný pokyn 19 – Řízení kontinuity činnosti

64. V rámci celkové politiky podniků v oblasti kontinuity činnosti má správní, řídicí nebo kontrolní orgán odpovědnost za stanovení a schválení politiky podniků v oblasti kontinuity IKT. Politika kontinuity IKT by měla být v rámci podniků náležitě oznámena a měla by se vztahovat na všechny příslušné zaměstnance, a případně na poskytovatele služeb.

Obecný pokyn 20 – Analýza dopadu na podnikatelskou činnost

65. V rámci řádného řízení kontinuity činnosti by podniky měly provádět analýzu dopadu na podnikatelskou činnost, aby bylo možné posoudit vystavení podniků závažným narušením činnosti a jejich možný dopad, a to kvantitativně i kvalitativně, za použití analýzy interních a/nebo externích údajů a scénářů. Analýza dopadu na podnikatelskou činnost by také měla zvážit kritičnost identifikovaných a klasifikovaných obchodních procesů a činností, obchodních funkcí, úloh a aktiv (např. informačních aktiv a aktiv v oblasti IKT) a jejich vzájemné závislosti v souladu s obecným pokynem 4.

66. Podniky by měly zajistit, aby jejich systémy IKT a služby v oblasti IKT byly navrženy a sladěny s jejich analýzou dopadu na podnikatelskou činnost, například pokud jde o redundanci určitých kritických složek, aby se zabránilo narušením způsobeným událostmi, které mají na tyto složky dopad.

Pokyn 21 – Plánování kontinuity činnosti

67. Celkové plány kontinuity činnosti podniků by měly zohledňovat podstatná rizika, která by mohla nepříznivě ovlivnit systémy IKT a služby v oblasti IKT. Plány by měly podporovat cíle týkající se ochrany a v případě potřeby obnovy důvěrnosti, integrity a dostupnosti obchodních procesů a činností podniků, obchodních funkcí, úloh a aktiv (např. informačních aktiv a aktiv v oblasti IKT). Podniky by měly při sestavování těchto plánů podle potřeby koordinovat svou činnost s příslušnými interními a externími zainteresovanými stranami.

68. Podniky by měly zavést plány kontinuity činnosti, aby zajistily, že budou moci přiměřeně reagovat na případné scénáře selhání v rámci cílové doby obnovy (maximální doba, během níž musí být po incidentu obnoven systém nebo proces) a cílového bodu obnovy (maximální lhůta, během níž je přijatelná ztráta dat v případě incidentu na předem definované úrovni služeb).

69. Podniky by měly ve svých plánech kontinuity činnosti zvážit řadu různých scénářů, včetně extrémních, ale věrohodných scénářů a scénářů kybernetických útoků, a posoudit potenciální dopad těchto scénářů. Na základě těchto scénářů by podniky měly popsat, jak je zajištěna kontinuita systémů IKT a služeb v oblasti IKT, jakož i bezpečnost informací podniků.

Obecný pokyn 22 – Plány reakce a obnovy

70. Na základě analýzy dopadu na podnikatelskou činnost a věrohodných scénářů by podniky měly vypracovat plány reakce a obnovy. Tyto plány by měly specifikovat, jaké podmínky mohou vyžadovat aktivaci plánu a jaká opatření by měla být přijata k zajištění integrity, dostupnosti, kontinuity a obnovy přinejmenším kritických systémů IKT a služeb v oblasti IKT provozovaných podniky. Cílem plánů reakce a obnovy by mělo být splnění cílů obnovy operací podniků.

71. Plány reakce a obnovy by měly zohledňovat krátkodobé a v případě potřeby dlouhodobé možnosti obnovy. Tyto plány by přinejmenším měly být:

    a) zaměřeny na obnovu činnosti důležitých služeb v oblasti IKT, obchodních funkcí, podpůrných procesů, informačních aktiv a jejich vzájemných závislostí, aby se zabránilo nepříznivým dopadům na fungování podniku;

    b) zdokumentovány a zpřístupněny obchodním a podpůrným útvarům a snadno dostupné v případě mimořádné situace, včetně jasného vymezení úloh a povinností, a

    c) průběžně aktualizovány v souladu s poznatky získanými z incidentů, testování, s nově identifikovanými riziky a hrozbami a se změněnými cíli a prioritami obnovy.

72. Plány by také měly zvážit alternativní možnosti v případech, kdy obnova nemusí být z krátkodobého hlediska proveditelná z důvodu nákladů, rizik, logistiky nebo nepředvídaných okolností.

73. V rámci plánů reakce a obnovy by podniky měly zvážit a provádět opatření pro kontinuitu činnosti, aby zmírnily selhání poskytovatelů služeb, kteří mají klíčový význam pro kontinuitu služeb podniků v oblasti IKT (v souladu s ustanoveními obecných pokynů orgánu EIOPA týkajících se řídícího a kontrolního systému a obecných pokynů týkajících se outsourcingu u poskytovatelů cloudových služeb).

Obecný pokyn 23 – Testování plánů

74. Podniky by měly své plány kontinuity činnosti testovat a zajistit, aby provoz jejich kritických obchodních procesů a činností, obchodních funkcí, úloh a aktiv (např. informačních aktiv) a aktiv v oblasti IKT a jejich vzájemné závislosti (včetně těch, které poskytli poskytovatelé služeb) byly pravidelně testovány na základě rizikového profilu podniků.

75. Plány kontinuity činnosti by se měly pravidelně aktualizovat na základě výsledků testování, aktuálních informací o hrozbách a zkušeností získaných z předchozích událostí. Měly by být rovněž zahrnuty veškeré relevantní změny cílů obnovy (včetně cílové doby obnovy a cílového bodu obnovy) nebo změny v obchodních procesech a

činnostech, obchodních funkcích, úlohách a aktivech (např. informačních aktivech a aktivech v oblasti IKT).

76. Testování plánů kontinuity činnosti by mělo prokázat, že tyto plány jsou schopny zachovat životaschopnost podniku, dokud nebudou obnoveny kritické operace na předem stanovenou úroveň služeb nebo toleranci dopadu.

77. Výsledky testů by měly být zdokumentovány a veškeré zjištěné nedostatky vyplývající z testů by měly být analyzovány, řešeny a oznámeny správnímu, řídicímu nebo kontrolnímu orgánu.

Obecný pokyn 24 – Krizová komunikace

78. V případě narušení nebo mimořádné situace a během provádění plánů kontinuity činnosti by měly podniky zajistit, aby byla zavedena účinná komunikační opatření pro případ krize, aby byly včas a vhodným způsobem informovány všechny příslušné interní i externí zainteresované strany, včetně příslušných orgánů dohledu, pokud to vyžadují vnitrostátní právní předpisy, jakož i příslušných poskytovatelů služeb.

Obecný pokyn 25 – Outsourcing služeb v oblasti IKT a systémů IKT

79. Aniž jsou dotčeny obecné pokyny orgánu EIOPA týkající se outsourcingu u poskytovatelů cloudových služeb, měly by podniky zajistit, aby v případech, kdy jsou služby v oblasti IKT a systémy IKT zajišťovány externě, byly splněny příslušné požadavky na službu v oblasti IKT nebo systém IKT.

80. V případě outsourcingu kritických nebo důležitých funkcí by podniky měly zajistit, aby smluvní povinnosti poskytovatele služeb (např. smlouva, dohody o úrovni služeb, ustanovení o ukončení v příslušných smlouvách) zahrnovaly alespoň:

    a) vhodné a přiměřené cíle a opatření související s bezpečností informací, včetně požadavků, jako jsou minimální požadavky na bezpečnost informací, specifikace životního cyklu dat podniků, práva na audit a přístupová práva a veškeré požadavky týkající se umístění datových center a požadavků na šifrování dat, procesů zabezpečení sítě a sledování bezpečnosti;

    b) dohody o úrovni služeb, aby se zajistila kontinuita služeb v oblasti IKT a systémů IKT a výkonnostní cíle za běžných okolností, jakož i cíle stanovené v pohotovostních plánech v případě přerušení služby a

    c) postupy řešení provozních a bezpečnostních incidentů včetně předávání na vyšší úroveň řízení a podávání zpráv.

81. Podniky by měly sledovat, zda tito poskytovatelé služeb zajišťují správnou úroveň bezpečnostních cílů, opatření a provozních úkolů podniku, a měly by se snažit získat v tomto ohledu dostatečné ujištění.

Pravidla pro dodržování předpisů a oznamování

82. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení Evropského parlamentu a Rady (EU) č. 1094/2010. V souladu s čl. 16 odst. 3 uvedeného nařízení musí příslušné orgány a podniky vynaložit veškeré úsilí, aby se obecnými pokyny a doporučeními řídily.

83. Příslušné orgány, které se těmito obecnými pokyny řídí nebo hodlají řídit, by je měly vhodným způsobem začlenit do svého rámce regulace nebo dohledu.

84. Příslušné orgány musí orgánu EIOPA potvrdit, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě uvést důvody, proč se jimi neřídí nebo nehodlají řídit, a to do dvou měsíců od vydání přeložených znění doporučení.

85. Pokud v této lhůtě nebude obdržena odpověď, bude se mít za to, že příslušné orgány nedodržely oznamovací povinnost, a budou jako takové vykazovány.

Závěrečné ustanovení o přezkoumání

86. Tyto obecné pokyny podléhají přezkoumání ze strany orgánu EIOPA.