EIOPA-BoS-20/600

Usmernenia o bezpečnosti a riadení informačných a komunikačných technológií

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

Obsah

Všeobecný kontext

1. Podľa článku 16 nariadenia (EÚ) č. 1094/2010 môže orgán EIOPA vydávať usmernenia určené príslušným orgánom a finančným inštitúciám s cieľom vytvoriť konzistentné, účinné a efektívne postupy dohľadu a zaistiť spoločné, jednotné a konzistentné uplatňovanie práva Únie.

2. V súlade s článkom 16 ods. 3 tohto nariadenia musia príslušné orgány a finančné inštitúcie vynaložiť všetko úsilie na dodržiavanie týchto usmernení a odporúčaní.

3. Orgán EIOPA identifikoval potrebu vypracovať osobitné usmernenia týkajúce sa bezpečnosti a riadenia informačných a komunikačných technológií (IKT) v súvislosti s článkami 41 a 44 smernice 2009/138/ES v kontexte analýzy vykonanej s cieľom reagovať na akčný plán Európskej komisie pre finančné technológie [COM(2018)0109 final], plán konvergencie dohľadu orgánu EIOPA na roky 2018 – 2019[1] a na základe interakcií s niekoľkými ďalšími zainteresovanými stranami[2].

4. Ako sa uvádza v spoločnom odporúčaní európskych orgánov dohľadu Európskej komisii, v usmerneniach orgánu EIOPA k systému správy a riadenia *„sa náležite nezohľadňuje dôležitosť venovania pozornosti riadeniu rizík v oblasti IKT (vrátane kybernetických rizík)*". Neexistujú usmernenia týkajúce sa dôležitých prvkov, ktoré sa vo všeobecnosti považujú za súčasť náležitej bezpečnosti a riadenia IKT."

5. Z analýzy súčasnej (legislatívnej) situácie v EÚ v súvislosti s uvedeným spoločným odporúčaním vyplynulo, že väčšina členských štátov EÚ stanovila vnútroštátne pravidlá pre bezpečnosť a riadenie IKT. Hoci sú požiadavky podobné, regulačný rámec je stále nejednotný. Okrem toho sa v prieskume súčasných postupov dohľadu odhalila široká škála postupov – od „žiadneho konkrétneho dohľadu" po „prísny dohľad" (vrátane „kontrol na diaľku" a „kontrol na mieste").

6. Navyše sa zvyšuje zložitosť IKT a zvyšuje sa aj frekvencia incidentov súvisiacich s IKT (vrátane kybernetických incidentov), ako aj škodlivý vplyv takýchto incidentov na operačné fungovanie poisťovní a zaisťovní. Z tohto dôvodu je riadenie rizík v oblasti IKT a bezpečnosti nevyhnutné na to, aby poisťovne a zaisťovne dosiahli svoje strategické, podnikové, prevádzkové ciele a ciele v oblasti dobrej povesti.

7. Okrem toho sa v sektore poisťovníctva vrátane tradičných aj inovačných obchodných modelov zvyšuje závislosť od IKT pri poskytovaní poisťovacích služieb a pri bežnom operačnom fungovaní poisťovní a zaisťovní, napr. digitalizácia sektora poisťovníctva (poistné technológie, internet vecí atď.), ako aj vzájomná prepojenosť prostredníctvom telekomunikačných kanálov (internet, mobilné a bezdrôtové pripojenie a rozsiahle siete). V dôsledku toho sú operácie poisťovní a zaisťovní zraniteľné voči bezpečnostným incidentom vrátane kybernetických útokov. Preto je dôležité zabezpečiť, aby poisťovne a zaisťovne boli primerane pripravené riadiť svoje riziká v oblasti IKT a bezpečnosti.

8. Na základe uznania potreby pripravenosti poisťovní a zaisťovní na kybernetické riziká[3] a potreby spoľahlivého rámca v oblasti kybernetickej bezpečnosti, sa tieto usmernenia navyše vzťahujú aj na kybernetickú bezpečnosť ako súčasť opatrení

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

[2] Správu, ktorú uverejnil orgán EIOPA v reakcii na akčný plán Európskej komisie pre finančné technológie, možno získať tu.

[3] Pre vymedzenie pojmu kybernetického rizika pozri dokument Rady pre finančnú stabilitu *Cyber Lexicon* z 12. novembra 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf.

poisťovní a zaisťovní v oblasti informačnej bezpečnosti. Hoci sa v týchto usmerneniach uznáva, že kybernetická bezpečnosť by sa mala riešiť ako súčasť všeobecného riadenia rizík v oblasti IKT a bezpečnosti poisťovní a zaisťovní, je dôležité zdôrazniť, že kybernetické útoky majú určité osobitné charakteristiky, ktoré by sa mali zohľadniť pri zabezpečovaní toho, že opatrenia v oblasti informačnej bezpečnosti primerane zmierňujú kybernetické riziká:

a) kybernetické útoky sa často riadia (t. j. identifikácia, ochrana, odhaľovanie, reakcia na tieto riziká a úplne zotavenie z nich) ťažšie než väčšina ostatných zdrojov rizík v oblasti IKT a bezpečnosti, a takisto sa ťažko určuje rozsah škody;

b) niektoré kybernetické útoky môžu viesť k neúčinnosti bežných opatrení na riadenie rizík a zabezpečenie kontinuity činností, ako aj postupov obnovy po havárií, pretože môže dôjsť k rozširovaniu škodlivého softvéru do záložných systémov s cieľom znemožniť ich dostupnosť alebo poškodiť záložné údaje;

c) poskytovatelia služieb, sprostredkovatelia, (riadiace) subjekty a sprostredkovatelia sa môžu stať kanálmi na šírenie kybernetických útokov. Nákazlivé tiché hrozby môžu využívať vzájomnú prepojenosť prostredníctvom telekomunikačných spojení tretích strán a prenikať tak do systémov IKT poisťovní a zaisťovní. Prepojená poisťovňa alebo zaisťovňa, ktorá sama o sebe nie je vysoko relevantná, sa preto môže stať zraniteľnou a zdrojom šírenia rizika a výsledkom môže byť systémový vplyv. Ak by sa dodržiavala zásada najslabšieho článku, kybernetická bezpečnosť by nemala byť témou len pre hlavných účastníkov trhu alebo poskytovateľov kritických služieb.

9. Cieľom týchto usmernení je:

a) poskytnúť účastníkom trhu objasnenie a transparentnosť, pokiaľ ide o minimálne očakávania týkajúce sa spôsobilosti v oblasti informačnej a kybernetickej bezpečnosti, t. j. bezpečnostný základ;

b) zabrániť potenciálnej regulačnej arbitráži;

c) podporovať konvergenciu dohľadu, pokiaľ ide o očakávania a procesy uplatniteľné v súvislosti s bezpečnosťou a riadením IKT ako kľúčový prvok riadenia rizík v oblasti IKT a bezpečnosti.

Usmernenia o bezpečnosti a riadení informačných a komunikačných technológií

Úvod

1. Orgán EIOPA v súlade s článkom 16 nariadenia (EÚ) č. 1094/2010[4] vydáva tieto usmernenia určené dozorným orgánom s cieľom poskytnúť usmernenie k tomu, ako by poisťovne a zaisťovne mali uplatňovať požiadavky na správu a riadenie stanovené v smernici 2009/138/ES[5] (ďalej len „smernica Solventnosť II") a v delegovanom nariadení Komisie (EÚ) č. 2015/35[6] (ďalej len „delegované nariadenie") v kontexte bezpečnosti a riadenia informačných a komunikačných technológií („IKT"). Tieto usmernenia vychádzajú z ustanovení o správe a riadení stanovených v článkoch 41, 44, 46, 47, 132 a 246 smernice Solventnosť II a v článkoch 258 až 260, 266, 268 až 271 a 274 delegovaného nariadenia. Okrem toho ich základ tvoria aj usmerňujúce informácie poskytnuté v usmerneniach orgánu EIOPA k systému správy a riadenia (EIOPA-BoS-14/253)[7] a usmerneniach orgánu EIOPA týkajúcich sa outsourcingu poskytovateľom cloudových služieb (EIOPA-BoS-19/270)[8].
2. Tieto usmernenia sa vzťahujú na jednotlivé poisťovne a zaisťovne a primerane teda aj na úroveň skupiny[9].
3. Príslušné orgány by pri dodržiavaní týchto usmernení alebo pri dohľade nad dodržiavaním týchto usmernení mali zohľadňovať zásadu primeranosti[10], ktorou by sa malo zabezpečiť, aby mechanizmy správy a riadenia vrátane tých, ktoré sa týkajú bezpečnosti a riadenia IKT, boli primerané povahe, rozsahu a zložitosti príslušných rizík, ktorým poisťovne a zaisťovne čelia alebo ktorým môžu čeliť.
4. Tieto usmernenia by sa mali vykladať v spojení so smernicou Solventnosť II, delegovaným nariadením, usmerneniami orgánu EIOPA k systému správy a riadenia a usmerneniami orgánu EIOPA týkajúcimi sa outsourcingu poskytovateľom cloudových služieb a bez toho, aby boli nimi dotknuté. Tieto usmernenia majú byť neutrálne z hľadiska technológie a metodiky.

Vymedzenie pojmov

5. Pokiaľ nie sú pojmy vymedzené v týchto usmerneniach, ich význam je vymedzený v smernici Solventnosť II.
6. Na účely týchto usmernení sa uplatňujú tieto vymedzenia pojmov:

[4] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1094/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov), a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/79/ES (Ú. v. EÚ L 331, 15.12.2010, s. 48).

[5] Smernica Európskeho parlamentu a Rady 2009/138/ES z 25. novembra 2009 o začatí a vykonávaní poistenia a zaistenia (Solventnosť II) (Ú. v. EÚ L 335, 17.12.2009, s. 1).

[6] Delegované nariadenie Komisie (EÚ) 2015/35 z 10. októbra 2014, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2009/138/ES o začatí a vykonávaní poistenia a zaistenia (Solventnosť II) (Ú. v. EÚ 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] Článok 212 ods. 1 smernice 2009/138/EÚ.

[10] Článok 29 ods. 3 smernice 2009/138/EÚ.

Vlastník aktíva	Osoba alebo subjekt so zodpovednosťou za informačné aktívum a aktívum v oblasti IKT a s príslušnou právomocou.
Dostupnosť	Vlastnosť charakterizovaná prístupnosťou a použiteľnosťou na žiadosť (včasnosť) oprávneného subjektu.
Dôvernosť	Vlastnosť, ktorá znamená, že informácie sa nezverejnia ani nesprístupnia neoprávneným osobám, subjektom, procesom či systémom.
Kybernetický útok	Akýkoľvek druh hackovania, ktorý vedie k útočnému/zlomyseľnému pokusu o zničenie, odhalenie, zmenu, znefunkčnenie, krádež alebo získanie neoprávneného prístupu k informačnému aktívu alebo k neoprávnenému použitiu takéhoto aktíva, so zameraním na systémy IKT.
Kybernetická bezpečnosť	Zachovanie dôvernosti, integrity a dostupnosti informácií a/alebo informačných systémov prostredníctvom počítačového média.
Aktívum v oblasti IKT	Aktívum vo forme softvéru alebo hardvéru, ktoré sa nachádza v podnikateľskom prostredí.
Projekty IKT	Každý projekt alebo jeho časť, v rámci ktorého sa menia, nahrádzajú alebo zavádzajú systémy IKT a služby v oblasti IKT.
Riziko v oblasti IKT a bezpečnosti	Ako podzložka operačného rizika, riziko strát z dôvodu porušenia dôvernosti, zlyhania integrity systémov a údajov, nevhodnosti alebo nedostupnosti systémov a údajov alebo neschopnosti v primeranom čase a pri primeraných nákladoch zmeniť IKT, ak sa zmenia požiadavky prostredia alebo obchodné požiadavky (t.j. agilita). Zahŕňa kybernetické riziká ako aj riziká v oblasti informačnej bezpečnosti vyplývajúce z neprimeraných alebo zlyhaných interných postupov alebo externých udalostí vrátane kybernetických útokov alebo z neprimeranej fyzickej bezpečnosti.
Informačná bezpečnosť	Zachovanie dôvernosti, integrity a dostupnosti informácií a/alebo informačných systémov. Môžu tu patriť aj iné vlastnosti, ako je pravosť, zodpovednosť, nespochybniteľnosť a spoľahlivosť.

Služby v oblasti IKT	Služby poskytované systémami IKT a poskytovateľmi služieb jednému alebo viacerým interným alebo externým používateľom.
Systémy IKT	Súbor aplikácií, služieb, aktív v oblasti informačných technológií, aktív v oblasti IKT alebo iných zložiek nakladania s informáciami, pričom tu patrí aj operačné prostredie.
Informačné aktívum	Súbor informácií, hmotný či nehmotný, ktorý je hodný ochrany.
Integrita	Vlastnosť správnosti a úplnosti.
Prevádzkový alebo bezpečnostný incident	Jednorazová udalosť alebo rad navzájom súvisiacich neplánovaných udalostí, ktoré majú alebo pravdepodobne budú mať nepriaznivý vplyv na integritu, dostupnosť a dôvernosť systémov IKT a služieb v oblasti IKT.
Poskytovateľ služieb	Je tretia strana, ktorá na základe dohody o outsourcingu vykonáva postup, službu alebo činnosť, alebo ich časti.
Testovanie penetrácie na základe hrozby	Kontrolovaný pokus o narušenie kybernetickej odolnosti subjektu simuláciou taktiky, techník a postupov aktérov hrozieb v reálnom živote. Vychádza z cielených spravodajských informácií o hrozbách a zameriava sa na ľudí, procesy a technológie subjektu s minimálnymi znalosťami a vplyvom na operácie.
Zraniteľnosť	Slabé miesto, citlivosť alebo chyba aktíva alebo kontroly, ktoré možno zneužiť jednou alebo viacerými hrozbami.

7. Tieto usmernenia sa uplatňujú od 1. júla 2021.

Usmernenie 1 – Primeranosť

8. Poisťovne a zaisťovne by mali uplatňovať tieto usmernenia spôsobom, ktorý je primeraný povahe, rozsahu a zložitosti rizík spojených s ich činnosťou.

Usmernenie 2 – IKT v rámci systému správy a riadenia

9. Správny, riadiaci alebo kontrolný orgán by mal zabezpečiť, aby systém správy a riadenia poisťovní a zaisťovní, najmä systém riadenia rizík a systém vnútornej kontroly, primerane riadil riziká poisťovní a zaisťovní v oblasti IKT a bezpečnosti.

10. Správny, riadiaci alebo kontrolný orgán by mal zabezpečiť, aby počet a zručnosti zamestnancov poisťovní a zaisťovní boli primerané na priebežnú podporu ich

prevádzkových potrieb v oblasti IKT, postupov riadenia rizík v oblasti IKT a bezpečnosti a zabezpečenie vykonávania stratégie v oblasti IKT. Okrem toho by zamestnanci mali pravidelne absolvovať primeranú odbornú prípravu o rizikách v oblasti IKT a bezpečnosti vrátane informačnej bezpečnosti, ako sa stanovuje v usmernení 13.

11. Správny, riadiaci alebo kontrolný orgán by mal zabezpečiť, aby pridelené zdroje boli primerané na splnenie uvedených požiadaviek.

Usmernenie 3 – Stratégia v oblasti IKT

12. Správny, riadiaci alebo kontrolný orgán má celkovú zodpovednosť za stanovenie a schvaľovanie písomnej stratégie poisťovní a zaisťovní v oblasti IKT v rámci ich celkovej obchodnej stratégie a v súlade s ňou, ako aj za dohľad nad komunikáciou o nej a jej vykonávaním.

13. V stratégii v oblasti IKT by sa malo vymedziť aspoň:

    a) ako by sa malo vyvíjať IKT poisťovní a zaisťovní, aby účinne podporovalo a realizovalo ich obchodnú stratégiu vrátane vývoja organizačnej štruktúry, obchodných modelov, systémov IKT a kľúčových prípadov závislosti od poskytovateľov služieb;

    b) vývoj architektúry IKT vrátane závislosti od poskytovateľov služieb; a

    c) jasné ciele informačnej bezpečnosti so zameraním na systémy IKT a služby v oblasti IKT, zamestnancov a postupy.

14. Poisťovne a zaisťovne by v relevantných prípadoch mali zabezpečiť včasné vykonávanie a prijatie stratégie v oblasti IKT a jej komunikáciu všetkým príslušným zamestnancom a poskytovateľom služieb.

15. Poisťovne a zaisťovne by mali stanoviť postupy na monitorovanie a meranie účinnosti vykonávania stratégie v oblasti IKT. Tento postup by sa mal pravidelne preskúmavať a aktualizovať.

Usmernenie 4 – Riziká v oblasti IKT a bezpečnosti v rámci systému riadenia rizík

16. Správny, riadiaci alebo kontrolný orgán má celkovú zodpovednosť za vytvorenie účinného systému riadenia rizík v oblasti IKT a bezpečnosti v rámci celkového systému riadenia rizík. To zahŕňa určenie tolerancie rizík pre tieto riziká v súlade s rizikovou stratégiou poisťovní a zaisťovní a pravidelnú písomnú správu o výsledku procesu riadenia rizík určenú správnemu, riadiacemu alebo kontrolnému orgánu.

17. Poisťovne a zaisťovne by v rámci svojho celkového systému riadenia rizík mali vo vzťahu k rizikám súvisiacim s IKT a bezpečnosťou (pri vymedzovaní požiadaviek na ochranu IKT ako sa uvádza ďalej) zvážiť aspoň tieto aspekty:

    a) poisťovne a zaisťovne by mali vytvoriť a pravidelne aktualizovať mapovanie svojich obchodných procesov a činností, obchodných funkcií, úloh a aktív (napr. informačných aktív a aktív v oblasti IKT) s cieľom určiť ich význam a vzájomné závislosti vo vzťahu k rizikám v oblasti IKT a bezpečnosti;

    b) poisťovne a zaisťovne by mali identifikovať a merať všetky relevantné riziká v oblasti IKT a bezpečnosti, ktorým sú vystavené, a klasifikovať identifikované obchodné procesy a činnosti, obchodné funkcie, úlohy a aktíva (napr. informačné aktíva a IKT aktíva) z hľadiska kritickosti. Poisťovne a zaisťovne by takisto mali posúdiť požiadavky na ochranu aspoň z hľadiska dôvernosti,

integrity a dostupnosti týchto obchodných procesov a činností, obchodných funkcií, úloh a aktív (napr. informačné aktíva a aktíva v oblasti IKT). Mali by sa identifikovať vlastníci aktív, ktorí zodpovedajú za klasifikáciu aktív;

c) metódy použité na určenie kritickosti, ako aj úrovne požadovanej ochrany, najmä pokiaľ ide o ciele ochrany integrity, dostupnosti a dôvernosti, by mali zabezpečiť, aby výsledné požiadavky na ochranu boli konzistentné a komplexné;

d) meranie rizík v oblasti IKT a bezpečnosti by sa malo vykonávať na základe vymedzených kritérií rizika v oblasti IKT a bezpečnosti, pričom by sa mala zohľadniť kritickosť ich obchodných procesov a činností, obchodných funkcií, úloh a aktív (napr. informačných aktív a aktív v oblasti IKT), rozsah známych zraniteľností a predchádzajúce incidenty, ktoré mali na poisťovňu a zaisťovňu vplyv;

e) hodnotenie rizík v oblasti IKT a bezpečnosti by sa malo vykonávať a dokumentovať pravidelne. Toto posúdenie by sa malo vykonať aj pred každou významnou zmenou infraštruktúry, procesov alebo postupov ovplyvňujúcich obchodné procesy a činnosti, obchodné funkcie, úlohy a aktíva (napr. informačné aktíva a aktíva v oblasti IKT);

f) poisťovne a zaisťovne by na základe svojho posúdenia rizika mali prinajmenšom vymedziť a zaviesť opatrenia na riadenie identifikovaných rizík v oblasti IKT a bezpečnosti a na ochranu informačných aktív v súlade s ich klasifikáciou. Malo by tu patriť vymedzenie opatrení na riadenie zostávajúcich zvyškových rizík.

18. Výsledky procesu riadenia rizík v oblasti IKT a bezpečnosti by mal schvaľovať správny, riadiaci alebo kontrolný orgán a mali by sa zahrnúť do procesu riadenia operačného rizika ako súčasť celkového riadenia rizík poisťovní a zaisťovní.

Usmernenie 5 – Audit

19. Správu a riadenie, systémy a procesy poisťovní a zaisťovní v súvislosti s ich rizikami v oblasti IKT a bezpečnosti by mali pravidelne kontrolovať audítori s dostatočnými vedomosťami, zručnosťami a odbornými znalosťami v oblasti rizík v oblasti IKT a bezpečností v súlade s plánom auditu[11] poisťovní a zaisťovní, s cieľom poskytnúť správnemu, riadiacemu alebo kontrolnému orgánu nezávislé uistenie o ich účinnosti. Frekvencia a zameranie týchto auditov by malo byť primerané príslušným rizikám v oblasti IKT a bezpečnosti.

Usmernenie 6 – Politika a opatrenia v oblasti informačnej bezpečnosti

20. Poisťovne a zaisťovne by mali zaviesť písomnú politiku v oblasti informačnej bezpečnosti schválenú správnym, riadiacim alebo kontrolným orgánom, v ktorej by sa mali vymedziť zásady a pravidlá na vysokej úrovni na ochranu dôvernosti, integrity a dostupnosti informácií poisťovní a zaisťovní s cieľom podporiť vykonávanie stratégie v oblasti IKT.

21. Táto politika by mala obsahovať opis hlavných úloh a povinností riadenia informačnej bezpečnosti a mali by v nej byť stanovené požiadavky na zamestnancov, procesy a technológiu v súvislosti s informačnou bezpečnosťou,

[11] Článok 271 delegovaného nariadenia.

pri zohľadnením toho, že zamestnanci na všetkých úrovniach majú povinnosti pokiaľ ide o zabezpečovanie informačnej bezpečnosti poisťovní a zaisťovní.

22. Táto politika by sa mala komunikovať v rámci poisťovní a zaisťovní a mala by sa vzťahovať na všetkých zamestnancov. Ak je to vhodné a relevantné, politika v oblasti informačnej bezpečnosti alebo jej časti by sa mali komunikovať aj poskytovateľom služieb a vzťahovať sa aj na nich.

23. Na základe tejto politiky by poisťovne a zaisťovne mali zaviesť a vykonávať špecifickejšie postupy a opatrenia v oblasti informačnej bezpečnosti s cieľom okrem iného zmierniť riziká v oblasti IKT a bezpečnosti, ktorým sú vystavené. Tieto postupy a opatrenia v oblasti informačnej bezpečnosti by, podľa potreby mali zahŕňať každý proces opísaný v týchto usmerneniach.

Usmernenie 7 – Funkcia informačnej bezpečnosti

24. Poisťovne a zaisťovne by mali v rámci svojho systému správy a riadenia a v súlade so zásadou primeranosti vytvoriť funkciu informačnej bezpečnosti s povinnosťami pridelenými určenej osobe. Poisťovne a zaisťovne by mali zabezpečiť nezávislosť a objektivitu tejto funkcie informačnej bezpečnosti jej náležitým oddelením od postupov vývoja a prevádzky IKT. O tejto funkcii by sa mali podávať správy správnemu, riadiacemu alebo kontrolnému orgánu.

25. V rámci funkcie informačnej bezpečnosti sa zvyčajne plnia tieto úlohy:

    a) podpora správneho, riadiaceho alebo kontrolného orgánu pri vymedzovaní a udržiavaní politiky v oblasti bezpečnosti informácií pre poisťovne a zaisťovne a kontrola jej zavádzania;

    b) pravidelné a *ad hoc* podávanie správ správnemu, riadiacemu alebo kontrolnému orgánu o stave informačnej bezpečnosti a jej vývoji;

    c) monitorovanie a preskúmanie vykonávania opatrení v oblasti informačnej bezpečnosti;

    d) zabezpečenie aby sa pri využívaní poskytovateľov služieb dodržiavali požiadavky na informačnú bezpečnosť;

    e) zabezpečenie, aby všetci zamestnanci a poskytovatelia služieb, ktorí majú prístup k informáciám a systémom, boli primerane informovaní o politike v oblasti informačnej bezpečnosti, napríklad prostredníctvom odbornej prípravy v oblasti informačnej bezpečnosti a zvyšovania informovanosti;

    f) koordinácia preskúmania prevádzkových alebo bezpečnostných incidentov a nahlasovanie relevantných incidentov správnemu, riadiacemu alebo kontrolnému orgánu.

Usmernenie 8 – Logická bezpečnosť

26. Poisťovne a zaisťovne by mali vymedziť, zdokumentovať a zaviesť postupy logickej kontroly prístupu alebo logickej bezpečnosti (správa totožnosti a prístupu) v súlade s požiadavkami na ochranu, ako sú vymedzené v usmernení 4. Tieto postupy by sa mali vykonávať, presadzovať, monitorovať a pravidelne preskúmavať a mali by zahŕňať aj kontroly monitorovania anomálií. V rámci týchto postupov by sa mali zavádzať minimálne nasledujúce prvky, pričom pojem používateľ zahŕňa aj technických používateľov:

    a) zásada „need-to-know“, minimálnych práv a oddelenia funkcií: poisťovne a zaisťovne by mali spravovať prístupové práva vrátane vzdialeného prístupu

k informačným aktívam a ich podporným systémom na základe zásady „need-to-know". Používateľom by mali byť udelené minimálne prístupové práva, ktoré sú striktne nevyhnutné na vykonávanie ich povinností (zásada minimálnych práv), t. j. aby sa zabránilo neodôvodnenému prístupu k údajom alebo aby sa zabránilo prideleniu kombinácií prístupových práv, ktoré je možné využiť na obchádzanie kontrol (zásada oddelenia funkcií);

b) zodpovednosť používateľov: poisťovne a zaisťovne by mali v čo najväčšej miere obmedziť používanie všeobecných a spoločných používateľských účtov a zabezpečiť, aby bolo možné používateľov kedykoľvek identifikovať a spätne vysledovať k zodpovednej fyzickej osobe alebo povolenej úlohe pre činnosti vykonávané v systémoch IKT;

c) práva privilegovaného prístupu: poisťovne a zaisťovne by mali uplatňovať silné kontroly nad privilegovaným prístupom do systémov prísnym obmedzovaním a dôsledným dohľadom nad kontami so zvýšenými oprávneniami na prístup do systémov (napr. kontá správcov);

d) vzdialený prístup: s cieľom zabezpečiť bezpečnú komunikáciu a znižovať riziko by sa mal vzdialený správcovský prístup ku kritickým systémom IKT poskytovať iba na základe zásady „need-to-know" a pri použití riešení silnej autentifikácie;

e) zaznamenávanie činností používateľov: činnosti používateľov by sa mali zaznamenávať a monitorovať spôsobom primeraným riziku, ktorý zahŕňa prinajmenšom činnosti privilegovaných používateľov. Záznamy o prístupe by mali byť zabezpečené, aby sa zabránilo nepovolenej úprave alebo vymazaniu, a uchovávané počas obdobia zodpovedajúceho kritickosti identifikovaných obchodných činností, podporných procesov a informačných aktív, bez toho, aby boli dotknuté požiadavky na uchovávanie stanovené v práve Únie a vo vnútroštátnom práve. Poisťovne a zaisťovne by mali tieto informácie použiť na uľahčenie identifikácie a vyšetrovania nezvyčajných činností zistených pri poskytovaní služieb;

f) správa prístupu: prístupové práva by sa mali udeľovať, odstraňovať a upravovať včas podľa vopred stanovených postupov schvaľovania, ak ide o príslušného vlastníka informačného aktíva. V prípade, že prístup už nie je potrebný, prístupové práva by sa mali okamžite zrušiť;

g) posúdenie prístupu: prístupové práva by mali byť pravidelne preskúmané s cieľom zabezpečiť, aby používatelia nemali nadmerné privilégiá a aby boli prístupové práva zrušené/odstránené, ak už nie sú potrebné;

h) udelenie, zmena a zrušenie prístupových práv by sa mali zdokumentovať spôsobom, ktorý uľahčuje pochopenie a analýzu; a

i) metódy autentifikácie: poisťovne a zaisťovne by mali presadzovať metódy autentifikácie, ktoré sú dostatočne odolné, aby sa primerane a účinne zabezpečilo, že sa dodržiavajú politiky a postupy na kontrolu prístupu. Metódy autentifikácie by mali byť primerané kritickej povahe systémov IKT, informácií alebo postupov, ku ktorým sa uskutočňuje prístup. Toto by malo zahŕňať minimálne silné heslá alebo silnejšie metódy autentifikácie (napríklad dvojstupňová autentifikácia) podľa príslušného rizika.

27. Elektronický prístup prostredníctvom aplikácií k údajom a systémom IKT by sa mal obmedziť na minimum, ktoré je potrebné na poskytovanie príslušnej služby.

Usmernenie 9 – Fyzická bezpečnosť

28. Opatrenia poisťovní a zaisťovní v oblasti fyzickej bezpečnosti (napr. ochrana pred výpadkom energie, požiarom, vodou a neoprávneným fyzickým prístupom) by sa mali vymedziť, zdokumentovať a vykonávať s cieľom chrániť ich priestory, dátové centrá a citlivé oblasti pred neoprávneným prístupom a nebezpečenstvami prostredia.

29. Fyzický prístup k systémom IKT by sa mal povoliť iba oprávneným osobám. Oprávnenie by sa malo prideliť v súlade s úlohami a povinnosťami jednotlivca a obmedziť na osoby, ktoré sú primerane vyškolené a monitorované. Fyzický prístup by sa mal pravidelne preskúmať s cieľom zaistiť, aby boli prístupové práva, ktoré nie sú nevyhnutné, ihneď zrušené/odstránené.

30. Primerané opatrenia na ochranu pred nebezpečenstvami prostredia by mali byť úmerné dôležitosti budov a kritickej povahe operácií alebo systémov IKT nachádzajúcich sa v týchto budovách.

Usmernenie 10 – Bezpečnosť operácií IKT

31. Poisťovne a zaisťovne by mali zaviesť postupy na zabezpečenie dôvernosti, integrity a dostupnosti systémov IKT a služieb v oblasti IKT s cieľom minimalizovať vplyv bezpečnostných problémov na poskytovanie služieb v oblasti IKT. Tieto postupy by mali obsahovať nasledujúce opatrenia:

    a) identifikácia možných zraniteľností, ktoré by mali byť vyhodnotené a napravené zabezpečením aktuálnosti systémov IKT vrátane softvéru, ktorý poisťovne a zaisťovne poskytujú svojim interným a externým používateľom, a to využívaním kritických bezpečnostných opráv vrátane aktualizácie antivírusových definícií alebo vykonávaním kompenzačných kontrol;

    b) zavedenie bezpečných základných konfigurácií pre všetky kritické komponenty, ako sú operačné systémy, databázy, smerovače alebo spínače;

    c) zavedenie sieťovej segmentácie, systémov na prevenciu úniku údajov a šifrovanie sieťovej prevádzky (v súlade s klasifikáciou informačných aktív);

    d) zavedenie ochrany koncových bodov vrátane serverov, pracovných staníc a mobilných zariadení. Poisťovne a zaisťovne by mali posúdiť, či koncové body spĺňajú bezpečnostné normy, ktoré vymedzili, predtým, ako sa im udelí prístup do podnikovej siete;

    e) zabezpečenie toho, aby boli zavedené mechanizmy kontroly integrity na overenie integrity systémov IKT;

    f) šifrovanie údajov v pokoji a v tranzite (v súlade s klasifikáciou informačných aktív).

Usmernenie 11 – Monitorovanie bezpečnosti

32. Poisťovne a zaisťovne by mali zaviesť a vykonávať postupy a procesy na nepretržité monitorovanie činností, ktoré majú vplyv na informačnú bezpečnosť poisťovne a zaisťovne. Monitorovanie by malo zahŕňať prinajmenšom:

    a) interné a externé faktory vrátane obchodných funkcií a správcovských funkcií v oblasti IKT;

    b) transakcie poskytovateľov služieb, iných subjektov a interných používateľov; a

c) potenciálne vnútorné a vonkajšie hrozby.

33. Na základe monitorovania by poisťovne a zaisťovne mali zaviesť primerané a účinné kapacity na odhaľovanie, nahlasovanie a reakciu na neobvyklé činnosti a hrozby, ako sú fyzické alebo logické vniknutie, narušenie dôvernosti, integrity a dostupnosti informačných aktív, škodlivé kódy a verejne známe zraniteľnosti softvéru a hardvéru.

34. Nahlasovanie na základe monitorovania bezpečnosti by malo poisťovniam a zaisťovniam pomôcť pochopiť povahu prevádzkových ako aj bezpečnostných incidentov, identifikovať trendy a podporiť interné vyšetrovania poisťovní a zaisťovní a umožniť im prijímať primerané rozhodnutia.

Usmernenie 12 – Preskúmania, posúdenie a testovanie informačnej bezpečnosti

35. Poisťovne a zaisťovne by mali vykonávať množstvo rôznych preskúmaní, posúdení a testovaní informačnej bezpečnosti na zabezpečenie účinnej identifikácie zraniteľností vo svojich systémoch IKT a službách v oblasti IKT. Poisťovne a zaisťovne môžu napríklad vykonávať analýzu nedostatkov v porovnaní s normami informačnej bezpečnosti, preskúmania dodržiavania súladu s predpismi, vnútorné a externé audity informačných systémov alebo preskúmania fyzickej bezpečnosti.

36. Poisťovne a zaisťovne by mali stanoviť a zaviesť rámec pre testovanie informačnej bezpečnosti, ktorým sa potvrdí spoľahlivosť a účinnosť ich opatrení v oblasti informačnej bezpečnosti a zabezpečí sa, že sú v tomto rámci zohľadnené hrozby a zraniteľnosti, ktoré sú identifikované prostredníctvom monitorovania hrozieb a postupu posúdenia rizík v oblasti IKT a bezpečnosti.

37. Testovanie by sa malo vykonávať bezpečným a zabezpečeným spôsobom a nezávislými testovacími pracovníkmi s dostatočnými vedomosťami, zručnosťami a odbornými znalosťami z testovania opatrení v oblasti informačnej bezpečnosti.

38. Poisťovne a zaisťovne by mali vykonávať testy pravidelne. Rozsah, frekvencia a metóda testovania (napr. testovanie penetrácie vrátane testovania penetrácie na základe hrozby) by mali byť úmerné úrovni zisteného rizika. Testovanie kritických systémov IKT a skenovanie zraniteľností by sa malo vykonávať každoročne.

39. Poisťovne a zaisťovne by mali zabezpečiť, aby sa testy bezpečnostných opatrení vykonávali v prípade zmien infraštruktúry, procesov alebo postupov, a v prípade, že sa vykonajú zmeny z dôvodu zásadných prevádzkových alebo bezpečnostných incidentov alebo z dôvodu vydania nových alebo významne zmenených kritických aplikácií. Poisťovne a zaisťovne by mali monitorovať a vyhodnocovať výsledky bezpečnostných testov a aktualizovať podľa toho svoje bezpečnostné opatrenia v prípade kritických systémov IKT bez zbytočného odkladu.

Usmernenie 13 – Odborná príprava a informovanosť v oblasti informačnej bezpečnosti

40. Poisťovne a zaisťovne by mali vytvoriť programy odbornej prípravy v oblasti informačnej bezpečnosti pre všetkých zamestnancov vrátane správnych, riadiacich a kontrolných orgánov s cieľom zabezpečiť, aby boli vyškolení na plnenie svojich úloh a povinností s cieľom znížiť ľudský faktor, krádeže, podvody, zneužitie alebo stratu. Poisťovne a zaisťovne by mali zabezpečiť, aby program odbornej prípravy poskytoval pravidelné školenie pre všetkých zamestnancov.

41. Poisťovne a zaisťovne by mali vytvoriť a vykonávať pravidelné programy zvyšovania povedomia o bezpečnosti s cieľom vzdelávať svojich zamestnancov vrátane správnych, riadiacich a kontrolných orgánov o tom, ako riešiť riziká súvisiace s informačnou bezpečnosťou.

Usmernenie 14 – Riadenie operácií IKT

42. Poisťovne a zaisťovne by mali riadiť svoje operácie IKT na základe stratégie v oblasti IKT. V dokumentoch by sa malo vymedziť, ako poisťovne a zaisťovne prevádzkujú, monitorujú a kontrolujú systémy IKT a služby v oblasti IKT vrátane zdokumentovania kritických procesov, postupov a operácií IKT.

43. Poisťovne a zaisťovne by mali zaviesť postupy zaznamenávania a monitorovania v prípade kritických operácií IKT, aby sa umožnilo zisťovanie, analýza a oprava chýb.

44. Poisťovne a zaisťovne by mali viesť aktuálny súpis svojich aktív v oblasti IKT. Súpis aktív v oblasti IKT by mal byť dostatočne podrobný, aby umožnil rýchlu identifikáciu aktíva v oblasti IKT, jeho umiestnenia, bezpečnostnú klasifikáciu a vlastníctvo.

45. Poisťovne a zaisťovne by mali monitorovať a riadiť životný cyklus aktív v oblasti IKT s cieľom zabezpečiť, aby naďalej spĺňali a podporovali obchodné požiadavky a požiadavky na riadenie rizík. Poisťovne a zaisťovne by mali monitorovať, či sú ich aktíva v oblasti IKT podporované ich predajcami a internými vývojovými pracovníkmi a či sa uplatnili všetky príslušné opravy a modernizácie na základe zdokumentovaného procesu. Mali by sa posúdiť a zmierniť riziká vyplývajúce z neaktuálnych alebo nepodporovaných aktív v oblasti IKT. Vyradené aktíva v oblasti IKT by sa mali bezpečne spracovať a zlikvidovať.

46. Poisťovne a zaisťovne by mali realizovať plánovanie výkonnosti a kapacity a procesy monitorovania s cieľom predísť dôležitým problémom vo výkonnosti systémov IKT a nedostatkom kapacity IKT, odhaliť ich a reagovať na ne včas.

47. Poisťovne a zaisťovne by mali vymedziť a realizovať zálohovanie údajov a systémov IKT a postup obnovy s cieľom zabezpečiť, aby mohli byť obnovené podľa potreby. Rozsah a frekvencia zálohovania by mali byť stanovené v súlade s obchodnými požiadavkami na obnovu a kritickou povahou údajov a systémov IKT a hodnotené podľa vykonaného posúdenia rizík. Pravidelne by sa malo vykonávať testovanie postupov zálohovania a obnovy.

48. Poisťovne a zaisťovne by mali zabezpečiť, aby sa zálohy údajov a systémov IKT uchovávali na jednom alebo viacerých miestach mimo primárnej lokality, ktoré sú bezpečné a dostatočne vzdialené od primárnej lokality, aby sa zabránilo vystaveniu rovnakým rizikám.

Usmernenie 15 – Riadenie incidentov a problémov v oblasti IKT

49. Poisťovne a zaisťovne by mali zaviesť a realizovať postup riadenia incidentov a problémov na monitorovanie a zaznamenávanie prevádzkových alebo bezpečnostných incidentov a aby umožnili poisťovniam a zaisťovniam pokračovať alebo znovu obnoviť kritické obchodné funkcie a procesy v prípade výskytu narušení.

50. Poisťovne a zaisťovne by mali určiť vhodné kritériá a prahové hodnoty na klasifikáciu udalosti ako prevádzkového alebo bezpečnostného incidentu, ako aj indikátory včasného varovania, ktoré by mali slúžiť ako upozornenie, aby bolo možné včas odhaliť tieto incidenty.

51. S cieľom minimalizovať vplyv nepriaznivých udalostí a umožniť včasnú obnovu by poisťovne a zaisťovne mali stanoviť vhodné procesy a organizačné štruktúry na zabezpečenie jednotného a integrovaného monitorovania, zaobchádzania a nadväzných opatrení pokiaľ ide o prevádzkové a bezpečnostné incidenty a na zabezpečenie identifikácie a riešenia základných príčin a prijatia nápravných opatrení, aby sa zabránilo opätovnému výskytu incidentu. V procese riadenia incidentov a problémov by sa mali prinajmenšom stanoviť:

    a) postupy na identifikáciu, sledovanie, zaznamenávanie, kategorizovanie a klasifikovanie incidentov podľa priority definovanej poisťovňou alebo zaisťovňou a na základe obchodnej kritickej povahy a dohôd o poskytovaní služieb;

    b) úlohy a zodpovednosti za rôzne scenáre incidentov (napr. chyby, nesprávne fungovanie, kybernetické útoky);

    c) postup riadenia problémov na identifikovanie, analyzovanie a riešenie základnej príčiny jedného alebo viacerých incidentov — poisťovňa alebo zaisťovňa by mala vždy analyzovať prevádzkové alebo bezpečnostné incidenty, ktoré boli identifikované alebo sa vyskytli v rámci organizácie a/alebo mimo nej, a mala by zvážiť hlavné poznatky získané z týchto analýz a zodpovedajúcim spôsobom aktualizovať bezpečnostné opatrenia;

    d) účinné plány internej komunikácie vrátane postupov oznamovania a incidentov a eskalačných postupov — vzťahujúce sa aj na sťažnosti klienta týkajúce sa bezpečnosti — s cieľom zabezpečiť:

        i. aby incidenty s potenciálne veľkým nepriaznivým vplyvom na kritické systémy IKT a služby v oblasti IKT boli nahlasované príslušnému vrcholovému manažmentu;

        ii. aby správny, riadiaci alebo kontrolný orgán bol informovaný na báze *ad hoc* v prípade významných incidentov a aby bol informovaný minimálne o vplyve, reakcii a dodatočných kontrolách, ktoré sa vymedzia v dôsledku incidentov;

    e) postupy reakcie na incidenty s cieľom zmierniť vplyv spojený s incidentmi a zabezpečiť, aby sa služba včas stala prevádzkyschopnou a bezpečnou;

    f) osobitné plány externej komunikácie pre kritické obchodné funkcie a procesy s cieľom:

        i. spolupracovať s príslušnými zainteresovanými stranami v záujme účinnej reakcie a obnovy po incidente;

        ii. poskytnúť včas informácie vrátane hlásenia incidentov externým stranám [napr. klientom, iným účastníkom trhu, relevantnému (dozornému) orgánu tak, ako je to vhodné, a v súlade s platnou reguláciou].

Usmernenie 16 – Riadenie projektov IKT

52. Poisťovne a zaisťovne by mali zaviesť metodiku projektov IKT (vrátane nezávislých bezpečnostných požiadaviek) s primeraným procesom správy a riadenia a vedením realizácie projektu s cieľom účinne podporiť vykonávanie stratégie v oblasti IKT prostredníctvom projektov IKT.

53. Poisťovne a zaisťovne by mali náležite monitorovať a zmierňovať riziká vyplývajúce z portfólia projektov IKT so zreteľom aj na riziká, ktoré môžu vyplývať

zo vzájomných závislostí medzi rôznymi projektami a zo závislostí viacerých projektov od rovnakých zdrojov a/alebo odborných znalostí.

Usmernenie 17 – Obstarávanie a vývoj systémov IKT

54. Poisťovne a zaisťovne by mali vypracovať a zaviesť proces, ktorým sa riadi obstarávanie, vývoj a údržba systémov IKT s cieľom zabezpečiť, aby dôvernosť, integrita, dostupnosť údajov, ktoré sa majú spracovať, boli komplexne zabezpečené a aby boli splnené vymedzené požiadavky na ochranu. Tento proces by mal byť navrhnutý pomocou prístupu založeného na rizikách.

55. Poisťovne a zaisťovne by mali zabezpečiť, aby pred obstaraním alebo vývojom systému boli jasne vymedzené požiadavky na funkčnosť a požiadavky nesúvisiace s funkčnosťou (vrátane požiadaviek na informačnú bezpečnosť) a technické ciele.

56. Poisťovne a zaisťovne by mali zabezpečiť zavedenie opatrení na zabránenie neúmyselnej zmene alebo úmyselnej manipulácii so systémami IKT počas vývoja.

57. Poisťovne a zaisťovne by mali mať zavedenú metodiku na testovanie a schvaľovanie systémov IKT, služieb v oblasti IKT a opatrení v oblasti informačnej bezpečnosti.

58. Poisťovne a zaisťovne by mali primerane testovať systémy IKT, služby v oblasti IKT a opatrenia informačnej bezpečnosti s cieľom identifikovať potenciálne bezpečnostné slabé stránky, narušenia a incidenty.

59. Poisťovne a zaisťovne by mali zabezpečiť oddelenie produkčných prostredí od vývojových, testovacích a iných neprodukčných prostredí.

60. Poisťovne a zaisťovne by v prípade potreby mali zaviesť opatrenia na ochranu integrity zdrojového kódu systémov IKT. Mali by takisto komplexným spôsobom dokumentovať vývoj, realizáciu, prevádzku a/alebo konfiguráciu systémov IKT, aby sa znížila závislosť na odborníkoch v danej oblasti, ktorá nie je nevyhnutná.

61. Procesy poisťovní a zaisťovní týkajúce sa obstarávania a vývoja systémov IKT by sa mali vzťahovať aj na systémy IKT vyvinuté alebo riadené koncovými používateľmi obchodnej funkcie mimo organizácie IKT (napr. podnikovo riadené aplikácie alebo počítačové aplikácie koncových používateľov) prostredníctvom prístupu na základe rizík. Poisťovne a zaisťovne by mali viesť register týchto aplikácií, ktoré podporujú kritické obchodné funkcie alebo procesy.

Usmernenie 18 – Riadenie zmien IKT

62. Poisťovne a zaisťovne by mali stanoviť a vykonávať proces riadenia zmien IKT s cieľom zabezpečiť, aby boli všetky zmeny IKT systémov zaznamenané, posúdené, testované, schválené, overené a vykonané kontrolovaným spôsobom. Zmeny počas naliehavých alebo núdzových zmien IKT by mali byť vysledovateľné a následne oznámené príslušnému vlastníkovi aktív na účely analýzy *ex post*.

63. Poisťovne a zaisťovne by mali určovať, či zmeny v existujúcom prevádzkovom prostredí ovplyvňujú existujúce bezpečnostné opatrenia alebo si vyžadujú prijatie dodatočných opatrení na zmiernenie príslušných rizík. Tieto zmeny by mali byť v súlade s formálnym procesom riadenia zmien v poisťovniach a zaisťovniach.

Usmernenie 19 – Riadenie kontinuity činnosti

64. V rámci celkovej politiky kontinuity činností poisťovní a zaisťovní má správny, riadiaci alebo kontrolný orgán zodpovednosť za stanovenie a schválenie politiky poisťovní a zaisťovní v oblasti kontinuity IKT. Politika kontinuity IKT by sa mala v rámci poisťovní a zaisťovní primerane komunikovať a mala by sa vzťahovať na

všetkých príslušných zamestnancov a v v prípade potreby na poskytovateľov služieb.

Usmernenie 20 – Analýza vplyvu na činnosť

65. V rámci riadneho riadenia kontinuity činností by poisťovne a zaisťovne mali vykonať analýzu vplyvu na činnosť s cieľom posúdiť pravdepodobnosť vážnych narušení činnosti poisťovní a zaisťovní a ich potenciálny vplyv, z kvantitatívneho aj kvalitatívneho hľadiska, pri využití interných a/alebo externých údajov a analýzy scenára. V analýze vplyvu na činnosť by sa mala zohľadniť aj kritická povaha identifikovaných a klasifikovaných obchodných procesov a činností, obchodných funkcií, úloh a aktív (napr. informačných aktív a aktív v oblasti IKT) a ich vzájomná závislosť v súlade s usmernením 4.

66. Poisťovne a zaisťovne by mali zabezpečiť, aby ich systémy IKT a služby v oblasti IKT boli navrhnuté a zosúladené s ich analýzou vplyvu na činnosť, napríklad s redundanciou určitých kritických zložiek, aby sa zabránilo narušeniam spôsobeným udalosťami, ktoré ovplyvňujú uvedené zložky.

Usmernenie 21 – Plánovanie kontinuity činnosti

67. V plánoch na zabezpečenie kontinuity činností poisťovní a zaisťovní by sa mali zohľadniť významné riziká, ktoré by mohli mať nepriaznivý vplyv na systémy IKT a služby v oblasti IKT. V týchto plánoch by sa mali podporovať ciele zamerané na ochranu a v prípade potreby obnovenie dôvernosti, integrity a dostupnosti obchodných procesov a činností, obchodných funkcií, úloh a aktív (napr. informačných aktív a aktív v oblasti IKT) poisťovní a zaisťovní. Poisťovne a zaisťovne by sa mali počas vytvárania týchto plánov podľa potreby koordinovať s príslušnými internými a externými zainteresovanými stranami.

68. Poisťovne a zaisťovne by mali zaviesť plány na zabezpečenie kontinuity činnosti s cieľom zabezpečiť, že budú môcť primerane reagovať na možné scenáre zlyhania v rámci cieľového času obnovy (maximálny čas, v rámci ktorého musí byť systém alebo proces obnovený po incidente) a cieľového bodu obnovy (maximálne obdobie, za ktoré sa v prípade incidentu môžu stratiť údaje na vopred určenej úrovni poskytovania služby).

69. Poisťovne a zaisťovne by mali vo svojich plánoch na zabezpečenie kontinuity činnosti zvážiť celý rad rôznych scenárov vrátane extrémnych, ale realistických scenárov a scenárov kybernetického útoku a posúdiť potenciálny vplyv takýchto scenárov. Na základe týchto scenárov by poisťovňa alebo zaisťovňa mala opísať, ako je zabezpečená kontinuita systémov IKT a služieb v oblasti IKT, ako aj informačná bezpečnosť poisťovní a zaisťovní.

Usmernenie 22 – Plány reakcie a obnovy

70. Na základe analýz vplyvu na činnosť a pravdepodobných scenárov by poisťovne a zaisťovne mali vyvinúť plány reakcie a obnovy. V týchto plánoch by sa mali stanovovať podmienky, ktoré môžu vyžadovať aktivovanie týchto plánov a aké kroky by sa mali prijať na zabezpečenie integrity, dostupnosti, kontinuity a obnovy aspoň kritických systémov IKT a služieb v oblasti IKT poisťovní a zaisťovní. Cieľom plánov reakcie a obnovy by malo byť splnenie cieľov obnovy operácií poisťovní a zaisťovní.

71. Plány reakcie a obnovy by, ak je to potrebné, mali zohľadňovať krátkodobé, ako aj dlhodobé možnosti obnovy. Plány by sa mali prinajmenšom:

a) zamerať na obnovu prevádzky dôležitých služieb v oblasti IKT, obchodných funkcií, podporných procesov, informačných aktív a ich vzájomnej závislosti s cieľom zabrániť nepriaznivým účinkom na fungovanie poisťovní a zaisťovní;

b) zdokumentovať a sprístupniť obchodným a podporným jednotkám a byť ľahko dostupné v prípade núdze vrátane jasného vymedzenia úloh a zodpovedností; a

c) mali neustále aktualizovať v súlade so skúsenosťami získanými z incidentov, testov, novo identifikovanými rizikami a hrozbami, ako aj so zmenenými cieľmi a s prioritami obnovy.

72. V týchto plánoch by takisto mali byť zohľadnené alternatívne možnosti, ak nie je možné zrealizovať obnovu v krátkodobom horizonte z dôvodu nákladov, rizík, logistiky či nepredvídaných okolností.

73. V rámci plánov reakcie a obnovy by poisťovne a zaisťovne mali zvážiť a zaviesť opatrenia na zabezpečenie kontinuity s cieľom zmierniť zlyhanie poskytovateľov služieb, ktorí majú kľúčový význam pre kontinuitu služieb v oblasti IKT poisťovní a zaisťovní (v súlade s ustanoveniami usmernení orgánu EIOPA k systému správy a riadenia a usmernení týkajúcimi sa outsourcingu poskytovateľom cloudových služieb).

Usmernenie 23 – Testovanie plánov

74. Poisťovne a zaisťovne by mali otestovať svoje plány na zabezpečenie kontinuity činnosti a zabezpečiť, aby sa fungovanie ich kritických obchodných procesov a činností, obchodných funkcií, úloh a aktív (napr. informačné aktíva) a aktív v oblasti IKT a ich vzájomná závislosť (vrátane tých, ktoré poskytujú poskytovatelia služieb) pravidelne testovalo na základe rizikového profilu poisťovní a zaisťovní.

75. Plány na zabezpečenie kontinuity činností by sa mali aktualizovať pravidelne, na základe výsledkov testovania, súčasných spravodajských informácií o hrozbách a poznatkov získaných z predchádzajúcich udalostí. Mali by sa zahrnúť aj všetky relevantné zmeny cieľov obnovy (vrátane cieľového času obnovy a cieľového bodu obnovy) a/alebo zmeny v obchodných procesoch a činnostiach, obchodných funkciách, úlohách a aktívach (napr. informačné aktíva a aktíva v oblasti IKT).

76. Testovaním plánov na zabezpečenie kontinuity činnosti by sa malo preukázať, že sú schopné udržať životaschopnosť poisťovní a zaisťovní dovtedy, kým sa obnovia kritické operácie na vopred určenej úrovni služby alebo v rámci tolerancie vplyvu.

77. Výsledky testov by mali byť zdokumentované a všetky identifikované nedostatky vyplývajúce z testov by mali byť analyzované, riešené a nahlásené správnemu, riadiacemu alebo kontrolnému orgánu.

Usmernenie 24 – Krízová komunikácia

78. V prípade prerušenia prevádzky alebo núdzového stavu a počas vykonávania plánov na zabezpečenie kontinuity činností by poisťovne a zaisťovne mali zabezpečiť, aby boli zavedené účinné opatrenia krízovej komunikácie tak, aby boli všetky príslušné interné a externé zainteresované strany vrátane príslušných dozorných orgánov, ak si to vyžaduje vnútroštátna úprava, ako aj príslušných poskytovateľov služieb včas a primerane informované.

Usmernenie 25 – Outsourcing služieb v oblasti IKT a systémov IKT

79. Bez toho, aby boli dotknuté usmernenia orgánu EIOPA týkajúce sa outsourcingu poskytovateľom cloudových služieb, by poisťovne a zaisťovne mali zabezpečiť, aby v prípade outsourcingu služieb v oblasti IKT a systémov IKT boli splnené príslušné požiadavky na služby v oblasti IKT alebo systémy IKT.

80. V prípade outsourcingu kritických alebo dôležitých funkcií by poisťovne a zaisťovne mali zabezpečiť, aby zmluvné záväzky poskytovateľa služieb (napr. zmluva, dohody o úrovni poskytovaných služieb, ustanovenia o ukončení v príslušných zmluvách) zahŕňali aspoň:

    a) vhodné a primerané ciele a opatrenia v oblasti informačnej bezpečnosti vrátane požiadaviek, ako sú minimálne požiadavky na informačnú bezpečnosť, špecifikácie životného cyklu údajov poisťovní a zaisťovní, práva na audit a prístup a všetky požiadavky týkajúce sa umiestnenia dátových centier a požiadaviek na šifrovanie údajov, procesov monitorovania bezpečnosti sietí a bezpečnosti;

    b) dohody o úrovni poskytovaných služieb s cieľom zabezpečiť kontinuitu služieb v oblasti IKT a systémov IKT a výkonnostné ciele za normálnych okolností, ako aj ciele, ktoré sa stanovujú v pohotovostných plánoch v prípade prerušenia poskytovania služby; a

    c) postupy na riešenie prevádzkových a bezpečnostných incidentov vrátane eskalácie a podávania správ.

81. Poisťovne a zaisťovne by mali monitorovať a overovať, do akej miery títo poskytovatelia služieb dodržiavajú ich bezpečnostné ciele, bezpečnostné opatrenia a výkonnostné ciele.

Pravidlá dodržiavania odporúčaní a podávania správ

82. Tento dokument obsahuje usmernenia vydané v zmysle článku 16 nariadenia (EÚ) č. 1094/2010. V súlade s článkom 16 ods. 3 tohto nariadenia musia príslušné orgány a poisťovne a zaisťovne vynaložiť všetko úsilie na dodržiavanie usmernení a odporúčaní.

83. Príslušné orgány, ktoré dodržiavajú alebo majú v úmysle dodržiavať tieto usmernenia, by ich mali vhodným spôsobom začleniť do regulačného rámca alebo rámca dohľadu.

84. Príslušné orgány musia do dvoch mesiacov od dátumu vydania preložených verzií potvrdiť orgánu EIOPA, či usmernenia dodržiavajú alebo majú v úmysle dodržiavať, a v prípade, že usmernenia nedodržiavajú, uvedú dôvody.

85. V prípade neposkytnutia odpovede do tohto termínu sa príslušné orgány budú považovať za orgány, ktoré nedodržiavajú povinnosť informovať, a táto skutočnosť bude zverejnená.

Záverečné ustanovenie o preskúmaní

86. Tieto odporúčania budú predmetom preskúmania orgánom EIOPA.