EIOPA-BoS-20/600

Smjernice o sigurnosti i upravljanju u području informacijskih i komunikacijskih tehnologija

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Njemačka - Tel. + 49 69-951119-20;
Telefaks: + 49 69-951119-19; e-pošta: info@eiopa.europa.eu mrežno mjesto: www.eiopa.europa.eu

Sadržaj

Kontekst

1. Na temelju članka 16. Uredbe (EU) br. 1094/2010 EIOPA može izdati smjernice i preporuke upućene nadležnim tijelima i financijskim institucijama s ciljem uspostave dosljednih, učinkovitih i djelotvornih nadzornih praksi te osiguranja zajedničke, jedinstvene i dosljedne primjene prava Unije.

2. U skladu s člankom 16. stavkom 3. spomenute uredbe, nadležna tijela i financijske institucije moraju uložiti sve napore kako bi poštovali navedene smjernice i preporuke.

3. EIOPA je utvrdila da postoji potreba za razvojem konkretnih smjernica o sigurnosti i upravljanju u području informacijskih i komunikacijskih tehnologija (IKT) s obzirom na članke 41. i 44. Direktive 2009/138/EZ u kontekstu analize provedene kako bi se odgovorilo na Akcijski plan za financijske tehnologije Europske komisije (COM(2018)0109 final), EIOPA-in Plan konvergencije nadzora za razdoblje 2018. – 2019.[1] te nakon interakcije s nekoliko drugih dionika[2].

4. Kako je navedeno u Zajedničkom savjetu Europskih nadzornih tijela Europskoj komisiji, EIOPA-ine Smjernice o sustavu upravljanja *„ne odražavaju na prikladan način važnost upravljanja rizicima IKT-a (uključujući kiberrizike)*". Ne postoje smjernice u vezi s ključnim elementima za koje se općenito smatra da su dio pravilnog upravljanja i sigurnosti u području IKT-a".

5. Analiza trenutačne (zakonodavne) situacije u EU-u provedena u svrhu prethodno navedenog Zajedničkog savjeta pokazala je da većina država članica EU-a ima definirane nacionalne propise za sigurnost i upravljanje u području IKT-a. Iako su zahtjevi slični, regulatorni okvir i dalje je fragmentiran. Osim toga, anketom o trenutačnim nadzornim praksama otkriveno je da postoji širok raspon praksi - od „izostanka konkretnog nadzora" do „strogog nadzora" (uključujući „neizravne" i „izravne inspekcije").

6. Nadalje, IKT postaje sve složeniji i sve je više incidenata povezanih s IKT-om (uključujući kiberincidente) te je sve jači štetan utjecaj tih incidenata na operativno funkcioniranje društava. Zbog toga je upravljanje rizicima IKT-a i sigurnosnim rizicima ključno kako bi društva mogla ostvariti svoje strateške, korporativne, operativne ciljeve i ciljeve u vezi s ugledom.

7. Osim toga, u sektoru osiguranja, uključujući tradicionalne i inovativne poslovne modele, sve je veći stupanj oslanjanja na IKT u pružanju usluga u području osiguranja i u normalnom operativnom funkcioniranju društava, kao što su primjerice digitalizacija sektora osiguranja (InsurTech, IoT itd.) i međusobna povezanost putem telekomunikacijskih kanala (internet, mobilne i bežične veze te mreže širokog područja). Zbog toga je poslovanje društava podložno sigurnosnim incidentima, uključujući kibernapade. Stoga je važno osigurati da su društva na odgovarajući način pripremljena na upravljanje rizicima IKT-a i sigurnosnim rizicima.

8. Osim toga, u ovim se Smjernicama prepoznaje potreba da društva budu pripremljena na kiberrizike[3] i da imaju čvrst okvir u području kibersigurnosti te je

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

[2] Izvješće koje je EIOPA objavila kao odgovor na Akcijski plan Europske komisije za financijske tehnologije dostupno je ovdje.

[3] Za definiciju kiberrizika vidjeti Leksikon kibernetičkih pojmova (Cyber Lexicon) Odbora za financijsku stabilnost, 12. studenoga 2018., https://www.fsb.org/wp-content/uploads/P121118-1.pdf

kibersigurnost obuhvaćena u okviru mjera informacijske sigurnosti društva. U ovim se Smjernicama prepoznaje da bi kibersigurnost trebala biti dio cjelokupnog upravljanja rizicima IKT-a i sigurnosnim rizicima u društvima, a također je važno istaknuti da kibernapadi imaju neke specifične karakteristike koje je potrebno uzeti u obzir kako bi se osiguralo da se mjerama informacijske sigurnosti na odgovarajući način ublaže kiberrizici:

a) kibernapadima je često teže upravljati (tj. identificirati ih, otkriti, odgovoriti na njih, zaštititi se i potpuno se oporaviti od njih) nego većinom drugih izvora rizika IKT-a i sigurnosnih rizika te je raspon štete teško odrediti;

b) zbog nekih kibernapada, opći mehanizmi za upravljanje rizicima i za kontinuitet poslovanja te postupci za oporavak od katastrofe mogu postati neučinkoviti jer mogu širiti zlonamjerne programe u sustave za sigurnosne kopije kako bi oni postali nedostupni ili kako bi se oštetili podatci iz sigurnosne kopije;

c) pružatelji usluga, brokeri, agenti (za upravljanje) i posrednici mogu postati kanali za širenje kibernapada. Zarazne tihe prijetnje mogu iskoristiti međusobnu povezanost putem telekomunikacijskih veza treće strane kako bi došle do sustava IKT-a određenog društva. Stoga međusobno povezano društvo koje samo po sebi nije jako relevantno može postati ranjivo i izvor širenja rizika, što može imati utjecaj na sustav. Na temelju načela najslabije karike, kibersigurnost ne bi trebala predstavljati razlog za zabrinutost samo velikim sudionicima na tržištu ili pružateljima ključnih usluga.

9. Ciljevi ovih Smjernica su sljedeći:

a) osigurati pojašnjenja i transparentnost za sudionike na tržištu u vezi s najmanjim očekivanim kapacitetima u području informacijske sigurnosti i kibersigurnosti, tj. osnovnom razinom sigurnosti;

b) spriječiti potencijalnu regulatornu arbitražu;

c) poticati nadzornu konvergenciju s obzirom na očekivanja i postupke primjenjive u vezi s upravljanjem i sigurnosti u području IKT-a kao ključ za pravilno upravljanje sigurnosnim rizicima i rizicima IKT-a.

Smjernice o sigurnosti i upravljanju u području informacijskih i komunikacijskih tehnologija

Uvod

1. U skladu s člankom 16. Uredbe (EU) br. 1094/2010[4] EIOPA izdaje ove Smjernice namijenjene nadzornim tijelima kako bi pružila smjernice o načinu na koji bi društva za osiguranje i reosiguranje (zajedno „društva") trebala primjenjivati zahtjeve u vezi s upravljanjem predviđene Direktivom 2009/138/EZ[5] („Direktiva Solventnost II") i Delegiranom uredbom Komisije (EU) br. 2015/35[6] („Delegirana uredba") u kontekstu sigurnosti i upravljanja u području informacijskih i komunikacijskih tehnologija („IKT"). U tu se svrhu ove Smjernice temelje na odredbama o upravljanju iz članaka 41., 44., 46., 47., 132. i 246. Direktive Solventnost II i članaka od 258. do 260., članka 266., članaka od 268. do 271. i članka 274. Delegirane uredbe. Osim toga, ove se smjernice također temelje na EIOPA-inim Smjernicama o sustavu upravljanja (EIOPA-BoS-14/253)[7] i Smjernicama o izdvajanju poslova pružateljima usluga računalstva u oblaku (EIOPA-BoS-19/270)[8].
2. Smjernice se primjenjuju kako na pojedinačna društva, tako i, uz potrebne preinake, na razini grupe[9].
3. Nadležna tijela trebala bi, kad su usklađena s ovim Smjernicama ili kad nadziru usklađenost s njima, uzeti u obzir načelo proporcionalnosti[10], kojim bi se trebalo osigurati da sustavi upravljanja, uključujući one povezane s upravljanjem i sigurnosti u području IKT-a, budu proporcionalni s obzirom na narav, opseg i složenost odgovarajućih rizika s kojim se društva suočavaju ili bi se mogla suočiti.
4. Ove bi Smjernice trebalo tumačiti u vezi s Direktivom Solventnost II, Delegiranom uredbom, EIOPA-inim Smjernicama o sustavu upravljanja i EIOPA-inim Smjernicama o izdvajanju poslova pružateljima usluga računalstva u oblaku, ne dovodeći ih u pitanje. Ove su Smjernice neutralne s obzirom na tehnologiju i metodologiju.

Definicije

5. Pojmovi koji nisu definirani u ovim Smjernicama imaju značenje definirano u Direktivi Solventnost II.
6. Za potrebe ovih Smjernica primjenjuju se sljedeće definicije:

[4] Uredba (EU) br. 1094/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju Europskog nadzornog tijela (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje), o izmjeni Odluke br. 716/2009/EZ i o stavljanju izvan snage Odluke Komisije 2009/79/EZ (SL L 331, 15.12.2010., str. 48.).

[5] Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 335, 17.12.2019., str. 1.).

[6] Delegirana uredba Komisije (EU) 2015/35 od 10. listopada 2014. o dopuni Direktive 2009/138/EZ Europskog parlamenta i Vijeća o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 12, 17.1.2015., str. 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] Članak 212. stavak 1. Direktive 2009/138/EZ.

[10] Članak 29. stavak 3. Direktive 2009/138/EZ.

Vlasnik imovine	Osoba ili subjekt odgovoran i ovlašten za informacijsku imovinu i imovinu IKT-a.
Dostupnost	Raspoloživost i mogućnost upotrebljavanja na zahtjev (pravovremenost) ovlaštenog subjekta.
Povjerljivost	Uskraćivanje dostupnosti ili otkrivanja informacija neovlaštenim fizičkim osobama, subjektima, procesima ili sustavima.
Kibernapad	Svaka vrsta hakiranja koja vodi do ofenzivnog/zlonamjernog pokušaja da se uništi, objavi, izmjeni, onemogući, ukrade ili dobije neovlašten pristup ili da se neovlašteno upotrijebi informacijska imovina koja cilja sustave IKT-a.
Kibersigurnost	Očuvanje povjerljivosti, cjelovitosti i dostupnosti informacija i/ili informacijskih sustavâ putem kibernetičkog medija.
Imovina IKT-a	Softverska ili hardverska imovina koja se nalazi u poslovnom okruženju.
Projekti u području IKT-a	Svaki projekt ili njegov dio u kojem se sustavi i usluge IKT-a mijenjaju, zamjenjuju ili implementiraju.
Rizik IKT-a i sigurnosni rizik	Podkategorija operativnog rizika; rizik gubitaka uslijed povrede povjerljivosti, gubitka integriteta sustava i podataka, neprikladnosti ili nedostupnosti sustava i podataka ili nemogućnosti promjene IKT-a unutar razumnog roka i uz razumne troškove u slučaju promjene u okruženju ili promjene zahtjeva poslovanja (to jest prilagodljivosti). To obuhvaća kiberrizike i rizike informacijske sigurnosti koji proizlaze iz neadekvatnih ili neuspješnih internih postupaka ili vanjskih događaja, uključujući kibernapade ili neadekvatnu fizičku sigurnost.
Informacijska sigurnost	Očuvanje povjerljivosti, cjelovitosti i dostupnosti informacija i/ili informacijskih sustava. Usto može obuhvaćati i autentičnost, odgovornost, nepobitnost i pouzdanost.
Usluge IKT-a	Usluge koje se pružaju unutarnjim ili vanjskim korisnicima putem sustavâ IKT-a i pružatelja usluga.

Sustavi IKT-a	Skup aplikacija, usluga, imovine informacijske tehnologije, imovine IKT-a ili drugih komponenti za postupanje s informacijama, koji obuhvaća i radno okruženje.
Informacijska imovina	Skup informacija, materijalnih ili nematerijalnih, koje vrijedi zaštititi.
Cjelovitost	Točnost i potpunost.
Operativni ili sigurnosni incident	Jedan događaj ili niz povezanih neplaniranih događaja koji imaju ili će vjerojatno imati negativan učinak na cjelovitost, dostupnost, i povjerljivost sustava i usluga IKT-a.
Pružatelj usluga	Znači treća strana koja obavlja određeni postupak, uslugu ili aktivnost ili dijelove postupka, usluge ili aktivnosti, u okviru sporazuma o izdvajanju poslova.
Penetracijsko testiranje vođeno prijetnjama	Kontrolirani pokušaj ugrožavanja kiberotpornosti subjekta oponašanjem taktika, tehnika i postupaka stvarnih prijetećih činitelja. Temelji se na saznanjima o ciljanim prijetnjama i usredotočuje se na ljude, postupke i tehnologiju subjekta, s minimalnom sposobnosti predviđanja i minimalnim učinkom na poslovanje.
Ranjivost	Slabost, podložnost ili mana imovine ili kontrolne funkcije koju može iskoristiti jedna prijetnja ili više njih.

7. Ove se Smjernice primjenjuju od 1. srpnja 2021.

Smjernica 1. – Proporcionalnost

8. Društva bi trebala primjenjivati ove Smjernice na način koji je proporcionalan naravi, opsegu i složenosti rizika svojstvenih njihovu poslovanju.

Smjernica 2. – IKT u sustavu upravljanja

9. Upravno, upravljačko ili nadzorno tijelo trebalo bi osigurati da se pomoću sustava upravljanja društva, osobito sustava upravljanja rizicima i sustava unutarnje kontrole, na odgovarajući način upravlja rizicima IKT-a i sigurnosnim rizicima.

10. Upravno, upravljačko ili nadzorno tijelo trebalo bi osigurati da su broj članova osoblja društva i njihove vještine prikladni za pružanje podrške njihovim operativnim potrebama u području IKT-a i postupcima upravljanja rizicima IKT-a te sigurnosnim rizicima na kontinuiranoj osnovi te kako bi se osigurala provedba njihove strategije IKT-a. Osim toga, osoblju bi se redovito trebalo pružati

odgovarajuće osposobljavanje o rizicima IKT-a i sigurnosnim rizicima te o informacijskoj sigurnosti, kako je navedeno u Smjernici 13.

11. Upravno, upravljačko ili nadzorno tijelo trebalo bi osigurati da su dodijeljena sredstva prikladna za ispunjavanje prethodno navedenih zahtjeva.

Smjernica 3. – Strategija IKT-a

12. Upravno, upravljačko ili nadzorno tijelo odgovorno je za uspostavu i odobrenje pisane strategije IKT-a društava, koja je dio njihove cjelokupne poslovne strategije i s njome je usklađena, te za nadzor njezina priopćavanja i provedbe.

13. Strategijom IKT-a trebalo bi se definirati barem sljedeće:

    a) način na koji bi se informacijske i komunikacijske tehnologije društava trebale razvijati kako bi se pomoću njih učinkovito provodila njihova poslovna strategija i pružila joj se podrška, uključujući razvoj organizacijske strukture, poslovnih modela, sustava IKT-a i ključne ovisnosti s pružateljima usluga;

    b) razvoj arhitekture IKT-a, uključujući ovisnosti o pružateljima usluga; i

    c) jasni ciljevi u pogledu informacijske sigurnosti, s naglaskom na sustave i usluge IKT-a, osoblje i postupke.

14. Društva bi trebala osigurati da se strategija IKT-a, ondje gdje je to primjenjivo i relevantno, pravodobno provede, donese i priopći svim relevantnim članovima osoblja i pružateljima usluga.

15. Društva bi trebala uspostaviti postupak za praćenje i mjerenje učinkovitosti provedbe strategije IKT-a. Taj bi se postupak trebao redovito preispitivati i ažurirati.

Smjernica 4. – Rizici IKT-a i sigurnosni rizici u sustavu upravljanja rizikom

16. Upravno, upravljačko ili nadzorno tijelo odgovorno je za uspostavu učinkovitog sustava za upravljanje rizicima IKT-a i sigurnosnim rizicima u okviru cjelokupnog sustava društva za upravljanje rizikom. To uključuje utvrđivanje tolerancije na rizik za te rizike, u skladu sa strategijom rizika društva, i redovito pisano izvješće o rezultatu postupka upravljanja rizikom, upućeno upravnom, upravljačkom ili nadzornom tijelu.

17. Kao dio svojeg cjelokupnog sustava upravljanja rizikom, društva bi trebala, s obzirom na rizike IKT-a i sigurnosne rizike (prilikom utvrđivanja zahtjeva u pogledu zaštite IKT-a kako je opisano u nastavku) razmotriti barem sljedeće:

    a) društva bi trebala uspostaviti i redovito ažurirati mapiranje svojih poslovnih procesa i aktivnosti, poslovnih funkcija, uloga i imovine (npr. informacijske imovine i imovine IKT-a) kako bi utvrdila njihovu važnost i njihovu međusobnu ovisnost s obzirom na rizike IKT-a i sigurnosne rizike;

    b) društva bi trebala utvrditi i izmjeriti sve relevantne rizike IKT-a i sigurnosne rizike kojima su izložena i klasificirati utvrđene poslovne procese i aktivnosti, poslovne funkcije, uloge i imovinu (npr. informacijsku imovinu i imovinu IKT-a) s obzirom na kritičnost. Društva bi također trebala procijeniti zahtjeve u pogledu zaštite barem povjerljivosti, cjelovitosti i dostupnosti tih poslovnih procesa i aktivnosti, poslovnih funkcija, uloga i imovine (npr. informacijske imovine i imovine IKT-a). Potrebno je identificirati vlasnike imovine koji su odgovorni za klasifikaciju imovine;

c) metodama koje se upotrebljavaju za utvrđivanje kritičnosti i potrebne razine zaštite, osobito u pogledu ciljeva zaštite cjelovitosti, dostupnosti i povjerljivosti, trebalo bi osigurati da su zahtjevi u pogledu zaštite dosljedni i sveobuhvatni;

d) mjerenje rizika IKT-a i sigurnosnih rizika trebalo bi provesti na temelju utvrđenih kriterija za rizike IKT-a i sigurnosne rizike, uzimajući u obzir kritičnost poslovnih procesa i aktivnosti, poslovnih funkcija, uloga i imovine (npr. informacijske imovine i imovine IKT-a), razmjer utvrđenih ranjivosti i prethodnih incidenata koji su utjecali na društvo;

e) procjenu rizika IKT-a i sigurnosnih rizika potrebno je redovito provoditi i dokumentirati. Ta bi se procjena također trebala provesti prije svih većih promjena infrastrukture, procesa i postupaka koji utječu na poslovne procese i aktivnosti, poslovne funkcije, uloge i imovinu (npr. informacijsku imovinu i imovinu IKT-a);

f) na temelju svoje procjene rizika društva bi trebala barem definirati i provoditi mjere za upravljanje utvrđenim rizicima IKT-a i sigurnosnim rizicima te zaštititi informacijsku imovinu u skladu s njezinom klasifikacijom. To bi trebalo obuhvaćati definiranje mjera za upravljanje preostalim rizicima.

18. Rezultate postupka upravljanja rizicima IKT-a i sigurnosnim rizicima trebalo bi odobriti upravno, upravljačko ili nadzorno tijelo i trebalo bi ih uključiti u postupak upravljanja operativnim rizicima, kao dio cjelokupnog upravljanja rizicima društva.

Smjernica 5. – Revizija

19. Upravljanje, sustave i postupke društva povezane s rizicima IKT-a i sigurnosnim rizicima trebali bi, u skladu s planom revizije društva,[11] periodično revidirati revizori koji imaju dovoljno znanja, vještina i stručnosti u području rizika IKT-a i sigurnosnih rizika kako bi upravnom, upravljačkom ili nadzornom tijelu mogli osigurati neovisno jamstvo u vezi s njihovom učinkovitosti. Učestalost i usmjerenost takvih revizija trebale bi biti razmjerne relevantnim rizicima IKT-a i sigurnosnim rizicima.

Smjernica 6. – Politika i mjere informacijske sigurnosti

20. Društva bi trebala utvrditi pisanu politiku informacijske sigurnosti koju odobrava upravno, upravljačko ili nadzorno tijelo, kojom bi se trebala definirati načela i pravila na visokoj razini za zaštitu povjerljivosti, cjelovitosti i dostupnosti informacija društva s ciljem pružanja podrške provedbi strategije IKT-a.

21. Politika bi trebala sadržavati opis glavnih uloga i odgovornosti za upravljanje informacijskom sigurnošću te bi njome trebali biti utvrđeni zahtjevi za osoblje, postupke i tehnologiju u vezi s informacijskom sigurnošću, pri čemu je utvrđeno da osoblje na svim razinama ima odgovornosti u osiguravanju informacijske sigurnosti društva.

22. Politiku bi trebalo priopćiti unutar društva i trebala bi se primjenjivati na sve članove osoblja. Politiku informacijske sigurnosti ili njezine dijelove također bi, prema potrebi, trebalo priopćiti pružateljima usluga i trebala bi se na njih primjenjivati.

23. Društva bi na temelju te politike trebala uspostaviti i provesti konkretnije postupke i mjere u području informacijske sigurnosti kako bi, *među ostalim*, smanjila rizike IKT-a i sigurnosne rizike kojima su izložena. Ti postupci i mjere u području

[11] Članak 271. Delegirane uredbe.

informacijske sigurnosti trebali bi, prema potrebi, obuhvaćati svaki postupak opisan u ovim Smjernicama.

Smjernica 7. – Služba za informacijsku sigurnost

24. Društva bi, unutar svojeg sustava upravljanja i u skladu s načelom proporcionalnosti, trebala uspostaviti službu za informacijsku sigurnost i dodijeliti odgovornosti imenovanoj osobi. Društvo bi trebalo osigurati neovisnost i objektivnost službe za informacijsku sigurnost na način da je na prikladan način izdvoji iz postupaka u vezi s informacijskim i komunikacijskim tehnologijama i njezinim razvojem. Služba bi trebala podnositi izvješća upravnom, upravljačkom ili nadzornom tijelu.

25. Zadaće službe za informacijsku sigurnost u pravilu su sljedeće:

    a) pružanje podrške upravnom, upravljačkom ili nadzornom tijelu prilikom utvrđivanja i održavanja politike informacijske sigurnosti za društva i kontroliranje njezine primjene;

    b) redovito savjetovanje i izvješćivanje upravnog, upravljačkog ili nadzornog tijela na *ad hoc* osnovi o stanju informacijske sigurnosti i njezinu razvoju;

    c) praćenje i preispitivanje provedbe mjera informacijske sigurnosti;

    d) osiguravanje da se prilikom upotrebljavanja pružatelja usluga poštuju zahtjevi u pogledu informacijske sigurnosti;

    e) osiguravanje da su svi zaposlenici i pružatelji usluga koji pristupaju informacijama i sustavima primjereno obaviješteni o politici informacijske sigurnosti, primjerice putem osposobljavanja i sastanaka za informiranje o informacijskoj sigurnosti;

    f) koordiniranje ispitivanja operativnih i sigurnosnih incidenata i izvješćivanje o relevantnim incidentima upravnom, upravljačkom ili nadzornom tijelu.

Smjernica 8. – Logička sigurnost

26. Društva bi trebala definirati, dokumentirati i provoditi postupke za logičku kontrolu pristupa ili logičku sigurnost (upravljanje identitetima i pristupom) u skladu sa zahtjevima u pogledu zaštite navedenima u Smjernici 4. Te bi postupke trebalo provoditi, izvršavati, pratiti i periodički preispitivati i oni bi također trebali obuhvaćati kontrole za praćenje anomalija. Tim bi postupcima trebalo barem provesti sljedeće elemente, pri čemu pojam „korisnik” također obuhvaća tehničke korisnike:

    a) načelo nužnosti pristupa informacijama, načelo najmanjih povlastica i razdvajanja dužnosti: društva bi trebala upravljati pravima pristupa, uključujući pristup na daljinu informacijskoj imovini i njezinim sustavima za podršku na temelju načela nužnosti pristupa informacijama. Korisnicima bi trebalo dodijeliti najmanja prava pristupa koja su strogo potrebna za izvršavanje njihovih dužnosti (načelo „najmanjih povlastica”), odnosno radi sprečavanja neopravdanog pristupa podatcima ili sprečavanja dodjele kombinacija prava pristupa koja se mogu upotrebljavati za izbjegavanje kontrola (načelo „razdvajanja dužnosti”);

    b) odgovornost korisnika: društva bi trebala, u mjeri u kojoj je to moguće, ograničiti upotrebu generičkih i zajedničkih korisničkih računa te osigurati da se korisnici u svakom trenutku mogu identificirati ili povezati s odgovornom

fizičkom osobom ili ovlaštenim zadatkom za radnje koje se izvršavaju u sustavima IKT-a;

c) prava povlaštenog pristupa: društva bi trebala provoditi snažne kontrole povlaštenog pristupa sustavu na način da strogo ograniče i pomno nadziru račune s povećanim pravima na pristup sustavu (npr. administratorski računi);

d) pristup na daljinu: kako bi se osigurala sigurna komunikacija i smanjili rizici, administrativni pristup na daljinu kritičnim sustavima IKT-a trebalo bi se odobravati samo na temelju načela nužnosti pristupa informacijama i ako se upotrebljavaju jaka rješenja za autentifikaciju;

e) evidentiranje aktivnosti korisnika: aktivnosti korisnika trebale bi se evidentirati i pratiti na način koji je proporcionalan riziku i obuhvaća barem aktivnosti povlaštenih korisnika. Evidencije pristupa trebalo bi osigurati na način da se spriječe neovlaštene izmjene ili brisanje te ih čuvati tijekom razdoblja koje je razmjerno kritičnosti utvrđenih poslovnih funkcija, procesa za podršku i informacijske imovine, ne dovodeći u pitanje zahtjeve u pogledu čuvanja podataka utvrđene pravom EU-a i nacionalnim pravom. Društva bi te informacije trebala upotrebljavati radi olakšavanja utvrđivanja i istraživanja neuobičajenih aktivnosti koje su otkrivene tijekom pružanja usluga;

f) upravljanje pristupom: prava pristupa potrebno je pravovremeno dodijeliti, ukinuti ili izmijeniti, u skladu s prethodno utvrđenim procedurama odobravanja kad je uključen relevantni vlasnik informacijske imovine. Kad pristup više nije potreban, prava pristupa trebalo bi odmah oduzeti;

g) procjena pristupa: prava pristupa trebalo bi periodički preispitivati kako bi se osiguralo da korisnici ne posjeduju prevelike povlastice te da su prava pristupa povučena/ukinuta kad više nisu potrebna.

h) dodjelu, izmjenu i oduzimanje prava pristupa trebalo bi dokumentirati na način kojim se olakšavaju razumijevanje i analiza; i

i) Metode autentifikacije: društva bi trebala provoditi metode autentifikacije koje su dovoljno pouzdane za primjereno i učinkovito osiguravanje usklađenosti s politikama i postupcima za kontrolu pristupa. Metode autentifikacije trebale bi biti razmjerne kritičnosti sustava IKT-a, informacija ili procesa kojima se pristupa. To bi trebalo uključivati barem jake lozinke ili snažnije metode autentifikacije (kao što je autentifikacija na temelju dvaju elemenata) na temelju relevantnog rizika.

27. Elektronički pristup podatcima i sustavima IKT-a putem aplikacija trebao bi biti ograničen na najmanju mjeru potrebnu za pružanje odgovarajuće usluge.

Smjernica 9. – Fizička sigurnost

28. Društva bi trebala definirati, dokumentirati i provoditi mjere fizičke sigurnosti (npr. zaštita od prekida napajanja energijom, požara, vode i neovlaštenog fizičkog pristupa) radi zaštite svojih prostorija, podatkovnih centara i osjetljivih područja od neovlaštenog pristupa i opasnosti povezanih s okolišem.

29. Fizički pristup sustavima IKT-a trebalo bi dopustiti samo ovlaštenim pojedincima. Ovlaštenja bi trebalo dodjeljivati u skladu sa zadatcima i odgovornostima pojedinaca te bi ona trebala biti ograničena na osobe koje su primjereno osposobljene i koje se primjereno prati. Fizički pristup trebalo bi redovito preispitivati kako bi se osiguralo brzo povlačenje/ukidanje nepotrebnih prava pristupa.

30. Odgovarajuće mjere za zaštitu od opasnosti povezanih s okolišem trebale bi biti razmjerne važnosti zgrada i kritičnosti operacija ili sustava IKT-a koji se nalaze u tim zgradama.

Smjernica 10. – Sigurnost IKT operacija

31. Društva bi trebala uvesti postupke radi osiguranja povjerljivosti, cjelovitosti i dostupnosti sustavâ i usluga IKT-a kako bi se smanjio utjecaj sigurnosnih problema na pružanje usluga IKT-a. Ti postupci trebaju na odgovarajući način uključivati sljedeće mjere:

    a) utvrđivanje potencijalnih ranjivosti koje bi trebalo ocijeniti i sanirati na način da je osigurano da su sustavi IKT-a ažurirani, uključujući softver koji društva pružaju svojim unutarnjim i vanjskim korisnicima, primjenom kritičnih sigurnosnih zakrpa, uključujući ažuriranje antivirusnog programa, ili provedbom kompenzacijskih kontrola;

    b) provedbu osnovnih sigurnosnih postavki za sve kritične komponente poput operativnih sustava, baza podataka, usmjerivača ili sklopki;

    c) provedbu segmentiranja mreže, sustava sprečavanja propuštanja podataka i enkripcije mrežnog prometa (u skladu s klasifikacijom informacijske imovine);

    d) provedbu zaštite krajnjih točaka, uključujući poslužitelje, radne stanice i mobilne uređaje. Društva bi trebala procijeniti ispunjava li krajnja točka definirane sigurnosne standarde prije nego što joj se odobri pristup korporativnoj mreži;

    e) provjeru uspostave mehanizama za provjeru cjelovitosti radi provjere cjelovitosti sustavâ IKT-a;

    f) enkripciju podataka u mirovanju i u prijenosu (u skladu s klasifikacijom informacijske imovine).

Smjernica 11. – Praćenje sigurnosti

32. Društva bi trebala utvrditi i provesti postupke i procese za kontinuirano praćenje aktivnosti koje utječu na informacijsku sigurnost društava. Praćenjem je potrebno obuhvatiti barem sljedeće:

    a) unutarnje i vanjske čimbenike, uključujući poslovne funkcije i administrativne funkcije IKT-a;

    b) transakcije pružatelja usluga, drugih subjekata i unutarnjih korisnika; i

    c) potencijalne unutarnje i vanjske prijetnje.

33. Društva bi na temelju praćenja trebala osigurati odgovarajuće i učinkovite kapacitete za otkrivanje neuobičajenih aktivnosti i prijetnji, izvještavanje o njima i pružanje odgovora na njih, poput fizičkog ili logičkog neovlaštenog ulaza, kršenja povjerljivosti, cjelovitosti i dostupnosti informacijske imovine, zlonamjernog kôda i javno poznatih ranjivosti za softver i hardver.

34. Izvještavanje na temelju praćenja sigurnosti trebalo bi pomoći društvima da razumiju prirodu operativnih i sigurnosnih incidenata, da utvrde trendove i da pruže podršku svojim internim istragama te da donesu odgovarajuće odluke.

Smjernica 12. – Preispitivanje, procjenjivanje i testiranje informacijske sigurnosti

35. Društva bi trebala provoditi različita preispitivanja, procjenjivanja i testiranja informacijske sigurnosti kako bi se osiguralo učinkovito utvrđivanje ranjivosti u njihovim sustavima IKT-a i uslugama IKT-a. Primjerice, društva mogu provoditi analizu nedostataka u pogledu standarda za informacijsku sigurnost, preispitivanja usklađenosti, internih i vanjskih revizija informacijskih sustava ili preispitivanja fizičke sigurnosti.

36. Društva bi trebala uspostaviti i provoditi okvir za testiranje informacijske sigurnosti kojim se potvrđuju pouzdanost i učinkovitost njihovih mjera informacijske sigurnosti i osigurati da se tim okvirom uzimaju u obzir prijetnje i ranjivosti utvrđene praćenjem prijetnji te postupkom procjene rizika IKT-a i sigurnosnih rizika.

37. Testiranje bi na siguran način trebali provoditi neovisni ispitivači koji imaju dovoljno znanja, vještina i stručnosti u testiranju mjera informacijske sigurnosti.

38. Društva bi trebala redovito provoditi testiranja. Opseg, učestalost i metode testiranja (poput penetracijskog testiranja, uključujući penetracijsko testiranje vođeno prijetnjama) trebali bi biti razmjerni razini utvrđenog rizika. Testiranje kritičnih sustava IKT-a i ispitivanje ranjivosti trebalo bi provoditi svake godine.

39. Društva bi trebala osigurati da se testovi sigurnosnih mjera provode u slučaju promjena infrastrukture, procesa ili postupaka te ako su izmjene provedene zbog većih operativnih ili sigurnosnih incidenata ili zbog objave novih ili znatno izmijenjenih kritičnih aplikacija. Društva bi trebala pratiti i procjenjivati ishode testiranja sigurnosti i u skladu s njima ažurirati svoje sigurnosne mjere, a u slučaju kritičnih sustava IKT-a to bi trebale činiti bez odgađanja.

Smjernica 13. – Osposobljavanje i podizanje razine svijesti o informacijskoj sigurnosti

40. Društva bi trebala uspostaviti programe osposobljavanja o informacijskoj sigurnosti za sve članove osoblja, uključujući upravna, upravljačka ili nadzorna tijela, kako bi se osiguralo da su osposobljeni za izvršavanje svojih dužnosti i odgovornosti radi smanjenja mogućnosti ljudske greške, krađe, prijevare, zlouporabe ili gubitka. Društva bi trebala osigurati da se putem programa osposobljavanja redovito pruža osposobljavanje svim članovima osoblja.

41. Društva bi trebala organizirati i provesti periodičke programe za podizanje razine svijesti o sigurnosti radi obrazovanja članova osoblja, uključujući osoblje upravnog, upravljačkog ili nadzornog tijela, o tome kako postupati s rizicima povezanim s informacijskom sigurnosti.

Smjernica 14. – Upravljanje IKT operacijama

42. Društva trebale bi upravljati IKT operacijama na temelju svoje strategije IKT-a. U dokumentima bi se trebalo definirati na koji način društva upotrebljavaju, prate i nadziru sustave IKT-a usluge IKT-a, uključujući dokumentiranje kritičnih IKT procesa, postupaka i operacija.

43. Društva bi trebala provoditi postupke evidentiranja i praćenja za kritične IKT operacije kako bi se omogućilo otkrivanje, analiza i ispravljanje pogrešaka.

44. Društva bi trebala ažurirati popis svoje imovine IKT-a. Popis imovine IKT-a trebao bi biti dovoljno detaljan kako bi se omogućila brza identifikacija imovine IKT-a, njezine lokacije, sigurnosne klasifikacije i vlasništva.

45. Društva bi trebala pratiti životni ciklus imovine IKT-a i upravljati njome kako bi se osiguralo da i dalje ispunjava zahtjeve u pogledu poslovanja i upravljanja rizicima te da im pruža podršku. Društva bi trebala pratiti podržavaju li njihovi dobavljači ili interni razvojni inženjeri njihovu imovinu IKT-a te jesu li primijenjene sve relevantne zakrpe i nadogradnje na temelju dokumentiranog postupka. Potrebno je procijeniti i smanjiti rizike koji proizlaze iz zastarjele ili nepodržane imovine IKT-a. Imovinu IKT-a koja je povučena iz upotrebe potrebno je sigurno obraditi i ukloniti.

46. Društva bi trebala provoditi postupke planiranja i praćenja rada i sposobnosti kako bi pravodobno spriječila, otkrila i odgovorila na važna pitanja u pogledu rada sustava IKT-a i manjka kapaciteta IKT-a.

47. Društva bi trebala definirati i provoditi postupke za izradu sigurnosnih kopija i ponovnu uspostavu podataka i sustava IKT-a kako bi se osiguralo da ih se, ako je to potrebno, može ponovno uspostaviti. Opseg i učestalost izrade sigurnosnih kopija trebali bi se utvrditi u skladu sa zahtjevima poslovanja za oporavak i s kritičnošću podataka i sustava IKT-a te se trebaju procjenjivati u skladu s provedenom procjenom rizika. Testiranje postupaka izrade sigurnosnih kopija i ponovne uspostave trebalo bi redovito provoditi.

48. Društva bi trebala osigurati da se podatci i sigurnosne kopije sustava IKT-a pohranjuju na jednoj lokaciji ili više lokacija koje su izvan primarnog mjesta i koje su sigurne i dovoljno udaljene od primarnog mjesta kako ne bi bile izložene istim rizicima.

Smjernica 15. – Upravljanje incidentima i problemima u području IKT-a

49. Društva bi trebala uspostaviti i provoditi postupak upravljanja incidentima i problemima radi praćenja i evidentiranja operativnih i sigurnosnih incidenata te kako bi se društvima omogućilo da u slučaju poremećaja nastave ili ponovno krenu obavljati kritične poslovne funkcije i procese.

50. Društva bi trebala odrediti primjerene kriterije i pragove za klasifikaciju događaja kao operativnog ili sigurnosnog incidenta te rane pokazatelje opasnosti koji bi trebali služiti kao upozorenje kako bi se omogućilo rano otkrivanje tih incidenata.

51. Kako bi se smanjio utjecaj štetnih događaja i kako bi se omogućio pravovremeni oporavak, društva bi trebala uspostaviti odgovarajuće postupke i organizacijske strukture kako bi se osiguralo dosljedno i integrirano praćenje operativnih i sigurnosnih incidenata, njihovo rješavanje i daljnje postupanje te kako bi se osiguralo da su glavni uzroci utvrđeni i uklonjeni i da su poduzete korektivne radnje/mjere kako bi se spriječio ponovni nastanak incidenta. Postupkom upravljanja incidentima i problemima trebalo bi se utvrditi barem sljedeće:

    a) postupci za utvrđivanje, praćenje, evidentiranje, kategorizaciju i klasifikaciju incidenata u skladu s prioritetom koji određuje društvo i na temelju kritičnosti u pogledu poslovanja te sporazuma o uslugama;

    b) uloge i odgovornosti za različite scenarije incidenta (npr. pogreške, neispravan rad, kibernapadi);

    c) postupak upravljanja problemom za utvrđivanje, analizu i rješavanje glavnih uzroka jednog ili više incidenata; društva bi trebala analizirati operativne ili sigurnosne incidente koji su utvrđeni ili su nastali u okviru organizacije i/ili izvan nje te bi trebala razmotriti ključne pouke stečene iz tih analiza i u skladu s njima ažurirati sigurnosne mjere;

d) učinkoviti interni komunikacijski planovi, uključujući postupke obavješćivanja o incidentima i postupcima eskalacije, koji obuhvaćaju i pritužbe klijenata povezane sa sigurnošću, kako bi se osiguralo sljedeće:

   i. incidenti s potencijalno visokim negativnim učinkom na kritične sustave IKT-a i usluge IKT-a prijavljeni su odgovarajućem višem rukovodstvu;

   ii. upravno, upravljačko ili nadzorno tijelo obavještava se na *ad hoc* osnovi u slučaju većih incidenata i barem je obaviješteno o učinku, odgovoru i dodatnim kontrolama koje je potrebno definirati zbog nastanka incidenata.

e) postupci za odgovor na incidente kako bi se ublažili učinci povezani s incidentima i kako bi se osiguralo da usluga pravodobno postane operativna i sigurna;

f) posebni planovi za vanjsku komunikaciju za kritične poslovne funkcije i procese u svrhu:

   i. suradnje s relevantnim dionicima kako bi se učinkovito odgovorilo na incident i oporavilo od njega;

   ii. pružanja pravodobnih informacija, uključujući izvještavanje o incidentima, vanjskim stranama (npr. kupcima, drugim sudionicima na tržištu, relevantnim (nadzornim) tijelima, kako je to potrebno i u skladu s primjenjivim propisima).

Smjernica 16. – Upravljanje IKT projektima

52. Društva bi trebala uvesti metodologiju za IKT projekte (uključujući neovisno razmatranje sigurnosnih zahtjeva) s odgovarajućim postupkom upravljanja i vodstvom za provedbu projekta kako bi se na učinkovit način pružila podrška provedbi strategije IKT-a putem IKT projekata.

53. Društva bi trebala na odgovarajući način pratiti i smanjivati rizike koji proizlaze iz njihova portfelja projekata u području IKT-a, također uzimajući u obzir rizike koji mogu proizaći iz međuovisnosti različitih projekata i ovisnosti višestrukih projekata o istim sredstvima i/ili stručnosti.

Smjernica 17. – Nabava i razvoj sustavâ IKT-a

54. Društva bi trebala razviti i provoditi postupak kojim se uređuje nabava, razvoj i održavanje sustavâ IKT-a kako bi se osiguralo da su povjerljivost, cjelovitost i dostupnost podataka koji se trebaju obraditi sveobuhvatno osigurani i da su ispunjeni zahtjevi u pogledu zaštite. Taj bi postupak trebao biti osmišljen na temelju pristupa koji se temelji na procjeni rizika.

55. Društva bi trebala osigurati da se prije nabave ili razvoja sustava jasno definiraju funkcionalni i nefunkcionalni zahtjevi (uključujući zahtjeve u pogledu informacijske sigurnosti) i tehnički ciljevi.

56. Društva bi trebala osigurati da su uspostavljene mjere za sprečavanje nenamjerne promjene ili namjerne manipulacije sustavima IKT-a tijekom razvoja.

57. Društva bi trebala imati metodologiju za testiranje i odobravanje sustava IKT-a, usluga IKT-a i mjera informacijske sigurnosti.

58. Društva bi trebala na odgovarajući način testirati sustave IKT-a, usluge IKT-a i mjere informacijske sigurnosti radi utvrđivanja mogućih sigurnosnih slabosti, prekršaja i incidenata.

59. Društva bi trebala osigurati odvajanje produkcijskih okruženja od razvojnih, testnih i drugih neprodukcijskih okruženja.

60. Društva bi trebala provesti mjere za zaštitu cjelovitosti izvornog koda (kad je to moguće) sustavâ IKT-a. Također bi trebala na sveobuhvatan način dokumentirati razvoj, implementaciju, rad i/ili konfiguraciju sustavâ IKT-a kako bi se smanjila nepotrebna ovisnost o stručnjacima za tu tematiku.

61. Postupak nabave i razvoja sustava IKT-a društava također bi se trebao primjenjivati i na sustave IKT-a koje razvijaju ili kojima upravljaju krajnji korisnici poslovne funkcije izvan organizacije IKT-a (npr. aplikacije prilagođene poslovanju ili računalne aplikacije za krajnje korisnike) primjenom pristupa koji se temelji na procjeni rizika. Društva bi trebala voditi registar aplikacija kojima se podupiru kritične poslovne funkcije ili postupci.

Smjernica 18. – Upravljanje promjenama IKT-a

62. Društva bi trebala uspostaviti i provoditi postupak upravljanja promjenama IKT-a kako bi se osiguralo da se sve promjene sustavâ IKT-a bilježe, testiraju, procjenjuju, odobravaju, ovlašćuju i implementiraju na kontrolirani način. Promjene tijekom izvanrednih situacija ili hitne promjene IKT-a trebale bi se moći pratiti i trebalo bi ih se moći *ex post* priopćiti odgovarajućem vlasniku imovine radi *ex post* analize.

63. Društva bi trebala utvrditi utječu li promjene u postojećem operativnom okruženju na postojeće sigurnosne mjere te je li potrebno donošenje daljnjih mjera za smanjivanje povezanih rizika. Te bi promjene trebale biti u skladu s formalnim postupkom upravljanja promjenama društva.

Smjernica 19. – Upravljanje kontinuitetom poslovanja

64. Kao dio cjelokupne politike društva u vezi s upravljanjem kontinuitetom poslovanja, upravno, upravljačko ili nadzorno tijelo odgovorno je za uspostavu i odobravanje politike kontinuiteta IKT-a društava. Politiku kontinuiteta IKT-a potrebno je na primjeren način priopćiti unutar društva i trebala bi se primjenjivati na sve članove osoblja te, prema potrebi, pružatelje usluga.

Smjernica 20. – Procjena učinka na poslovanje

65. U okviru dobrog upravljanja kontinuitetom poslovanja, društva bi trebala provesti procjenu učinka na poslovanje kako bi ocijenila izloženost društva znatnijim prekidima poslovanja i njihov potencijalan učinak, kvantitativno i kvalitativno, upotrebom unutarnjih i/ili vanjskih podataka i analize scenarija. U okviru procjene učinka na poslovanje također bi se trebala uzeti u obzir kritičnost utvrđenih i klasificiranih poslovnih procesa i aktivnosti, poslovnih funkcija, uloga i imovine (npr. informacijske imovinu i imovine IKT-a) i njihove međuovisnosti, u skladu sa Smjernicom 4.

66. Društva bi trebala osigurati da su njihovi sustavi IKT-a i usluge IKT-a osmišljeni i usklađeni s njihovom procjenom učinka na poslovanje, primjerice s redundantnošću određenih kritičnih komponenti kako bi se spriječili poremećaji izazvani događajima koji utječu na te komponente.

Smjernica 21. – Planiranje kontinuiteta poslovanja

67. U okviru planova kontinuiteta poslovanja društva bi trebala razmotriti bitne rizike koji bi mogli imati negativan učinak na sustave i usluge IKT-a. Planovima bi se trebala pružiti podrška ciljevima u pogledu zaštite i, ako je potrebno, ponovno

uspostaviti povjerljivost, cjelovitost i dostupnost poslovnih procesa i aktivnosti, poslovnih funkcija, uloga i imovine društava (npr. informacijske imovine i imovine IKT-a). Ako je to potrebno, tijekom uspostave tih planova, društva bi se trebala koordinirati s relevantnim unutarnjim i vanjskim dionicima.

68. Društva bi trebala uspostaviti planove kontinuiteta poslovanja kako bi osigurala da mogu primjereno reagirati na moguće scenarije propasti unutar ciljanog vremena oporavka (najdulje razdoblje unutar kojeg se sustav ili proces mora ponovno uspostaviti nakon incidenta) i ciljane točke oporavka podataka (najdulje vremensko razdoblje tijekom kojeg je prihvatljivo da su podatci izgubljeni u slučaju incidenta na razini prethodno definirane usluge).

69. Društva bi u svojem planu kontinuiteta poslovanja trebala razmotriti čitav niz različitih scenarija, uključujući ekstremne, ali moguće scenarije, i kibernapade, te procijeniti potencijalni učinak koji bi ti scenariji mogli imati. Na temelju tih scenarija društva bi trebala opisati kako se osiguravaju kontinuitet sustava i usluga IKT-a te informacijska sigurnost društva.

Smjernica 22. – Planovi za odgovor i oporavak

70. Na temelju procjene učinka na poslovanje i mogućih scenarija društva bi trebala izraditi planove za odgovor i oporavak. Tim bi se planovima trebalo utvrditi koji uvjeti mogu potaknuti aktiviranje planova i koje bi se radnje trebale poduzeti kako bi se osigurali cjelovitost, dostupnost, kontinuitet i oporavak barem kritičnih sustava IKT-a, usluga IKT-a i podataka društava. Cilj planova za odgovor i oporavak trebao bi biti postizanje ciljeva oporavka poslovanja društava.

71. U planovima za odgovor i oporavak trebale bi se razmotriti kratkoročne i, prema potrebi, dugoročne mogućnosti oporavka. Planovi bi trebali biti barem:

    a) usmjereni na oporavak operacija važnih usluga IKT-a, poslovnih funkcija, procesa za podršku, informacijske imovine i njihove međuovisnosti kako bi se izbjegli štetni učinci na funkcioniranje društva;

    b) dokumentirani i stavljeni na raspolaganje poslovnim jedinicama i jedinicama za podršku te lako dostupni u izvanrednim situacijama, uključujući jasno definirane uloge i odgovornosti; i

    c) stalno ažurirani u skladu s iskustvima stečenima na temelju incidenata, testiranja, novih utvrđenih rizika i prijetnji te promijenjenih ciljeva i prioriteta za oporavak.

72. U planovima bi se također trebale razmotriti alternativne mogućnosti u slučajevima u kojima oporavak možda neće biti izvediv u kratkoročnom razdoblju zbog troškova, rizika, logistike ili nepredviđenih okolnosti.

73. U okviru planova za odgovor i oporavak društva bi trebala razmotriti i provoditi mjere za osiguranje kontinuiteta kako bi ublažila slučajeve propasti pružatelja usluga, koji su od ključne važnosti za kontinuitet pružanja usluga IKT-a društava (u skladu s odredbama EIOPA-inih Smjernica o sustavu upravljanja i Smjernica o izdvajanju poslova pružateljima usluga računalstva u oblaku).

Smjernica 23. – Testiranje planova

74. Društva bi trebala testirati svoje planove kontinuiteta poslovanja i osigurati da se funkcioniranje njihovih kritičnih poslovnih procesa i aktivnosti, poslovnih funkcija, uloga i imovine (npr. informacijske imovine) i imovine IKT-a te njihova

međuovisnost (uključujući onu koju pružaju pružatelji usluga) redovito testiraju na temelju profila rizičnosti društva.

75. Planove kontinuiteta poslovanja potrebno je redovito ažurirati, na temelju rezultata testiranja, aktualnih saznanja o prijetnjama i lekcija naučenih iz prethodnih događanja. Sve važne promjene ciljeva oporavka (uključujući ciljano vrijeme oporavka i ciljanu točku oporavka) i/ili promjene poslovnih procesa i aktivnosti, poslovnih funkcija, uloga i imovine (npr. informacijske imovine i imovine IKT-a) također bi se trebale uključiti.

76. Na temelju testiranja planova kontinuiteta poslovanja potrebno je pokazati da mogu osigurati održivost poslovanja sve dok se ponovno ne uspostave kritične operacije na razini prethodno definirane usluge ili tolerancije utjecaja.

77. Rezultate testiranja treba dokumentirati, a sve utvrđene nedostatke koji proizlaze iz testiranja treba analizirati, obraditi i o njima izvijestiti upravno, upravljačko ili nadzorno tijelo.

Smjernica 24. – Komuniciranje u kriznim situacijama

78. U slučaju prekida poslovanja ili izvanredne situacije, a tijekom provedbe planova kontinuiteta poslovanja, društva bi trebala osigurati postojanje učinkovitih mjera za komuniciranje u kriznim situacijama tako da svi relevantni unutarnji i vanjski dionici, uključujući relevantna nadzorna tijela, ako to zahtijevaju nacionalni propisi, te relevantne pružatelje usluga, budu pravodobno i primjereno obaviješteni.

Smjernica 25. – Izdvajanje poslova u vezi s uslugama IKT-a i sustavima IKT-a

79. Ne dovodeći u pitanje EIOPA-ine Smjernice o izdvajanju poslova pružateljima usluga računalstva u oblaku, društva bi trebala osigurati da su, prilikom izdvajanja poslova u području usluga IKT-a i sustava IKT-a, ispunjeni odgovarajući zahtjevi za uslugu IKT-a ili sustav IKT-a.

80. U slučaju izdvajanja poslova u vezi s kritičnim ili važnim funkcijama, društva bi trebala osigurati da ugovorne obveze pružatelja usluga (npr. ugovor, sporazumi o razini usluga, odredbe o raskidu u relevantnim ugovorima) uključuju barem sljedeće:

    a) odgovarajuće i proporcionalne ciljeve i mjere u pogledu informacijske sigurnosti, uključujući zahtjeve poput minimalnih zahtjeva u pogledu informacijske sigurnosti, specifikacije životnog ciklusa podataka društava, prava revizije i pristupa i sve zahtjeve u vezi sa lokacijom podatkovnih centara i enkripcijom podataka, mrežnom sigurnosti i postupcima praćenja sigurnosti;

    b) sporazume o razini usluga, kako bi se osigurao kontinuitet usluga IKT-a i sustava IKT-a i ciljevi u pogledu izvedbe u normalnim okolnostima te onih koje se pružaju na temelju planova za napredvidive situacije u slučaju prekida usluge; i

    c) postupke rješavanja operativnih i sigurnosnih incidenata, uključujući postupke eskalacije i izvještavanja.

81. Društva bi trebala pratiti razinu usklađenosti tih pružatelja usluga sa sigurnosnim ciljevima, mjerama i ciljevima u pogledu izvedbe te tražiti jamstva u pogledu te usklađenosti.

Pravila o usklađenosti i izvještavanju

82. Ovaj dokument sadržava Smjernice izdane u skladu s člankom 16. Uredbe (EU) br. 1094/2010. U skladu s člankom 16. stavkom 3. spomenute uredbe, nadležna tijela i društva moraju uložiti sve napore kako bi poštovali navedene smjernice i preporuke.

83. Nadležna tijela koja su usklađena ili se namjeravaju uskladiti s ovim Smjernicama trebaju ih na primjeren način uvrstiti u svoj regulatorni ili nadzorni okvir.

84. Nadležna tijela trebaju potvrditi EIOPA-i jesu li usklađena s ovim Smjernicama ili se namjeravaju s njima uskladiti te navesti razloge za neusklađenost u roku od dva mjeseca nakon izdavanja prevedenih verzija.

85. U slučaju da nadležna tijela ne odgovore u navedenom roku, smatrat će se da nisu usklađena s pravilima izvještavanja te će kao takva biti prijavljena.

Završna odredba o pregledu

86. Ove Smjernice podliježu EIOPA-inu pregledu.