EIOPA-BoS-20/600

Smernice o upravljanju varnosti informacijske in komunikacijske tehnologije

EIOPA – Westhafen Tower, Westhafenplatz 1 – 60327 Frankfurt – Nemčija – tel. + 49 69-951119-20;
faks. + 49 69-951119-19; e-pošta: info@eiopa.europa.eu spletno mesto: www.eiopa.europa.eu

Kazalo

Ozadje

1. Organ EIOPA lahko za vzpostavitev doslednih, uspešnih in učinkovitih nadzornih praks ter zagotovitev skupne, enotne in usklajene uporabe prava Unije v skladu s členom 16 Uredbe (EU) št. 1094/2010 izdaja smernice in priporočila, naslovljena na pristojne organe ali finančne institucije.

2. V skladu s členom 16(3) navedene uredbe si morajo pristojni organi in finančne institucije na vsak način prizadevati za spoštovanje takih smernic in priporočil.

3. Organ EIOPA je ugotovil, da je treba oblikovati posebne smernice o upravljanju varnosti informacijske in komunikacijske tehnologije (IKT) v zvezi s členoma 41 in 44 Direktive 2009/138/ES v okviru analize, opravljene kot odziv na akcijski načrt Evropske komisije za finančno tehnologijo (COM(2018)0109 final), načrtom organa EIOPA za nadzorniško zbliževanje 2018–2019[1], in po stikih z več drugimi deležniki[2].

4. Kot je navedeno v skupnem nasvetu evropskih nadzornih organov Evropski komisiji, smernice organa EIOPA o sistemu upravljanja ne *„izražajo ustrezno pomena skrbi za obvladovanje tveganj IKT (vključno s kibernetskimi tveganji)"*. Smernic glede ključnih elementov, za katere je splošno priznano, da so del pravilnega upravljanja varnosti, ni na voljo.

5. Analiza sedanjega (zakonodajnega) stanja v EU za navedeni skupni nasvet je pokazala, da je večina držav članic EU opredelila nacionalna pravila za upravljanje varnosti IKT. Zahteve so si sicer podobne, vendar pa je regulativni okvir še vedno razdrobljen. Poleg tega je raziskava sedanjih nadzornih praks razkrila zelo različne prakse, od „nobenega posebnega nadzora" do „strogega nadzora" (vključno s „pregledi na kraju samem" in „pregledi zunaj lokacije").

6. Poleg tega postaja IKT vse bolj kompleksna, incidenti, povezani z IKT, (vključno s kibernetskimi incidenti) pa vse pogostejši, prav tako pa tudi njihov škodljiv učinek na operativno delovanje podjetij. Obvladovanje varnostnih tveganj IKT je zato za zavarovalnica in/ali pozavarovalnicae bistveno za doseganje strateških, korporativnih in operativnih ciljev ter ciljev glede ugleda.

7. Poleg tega se v zavarovalniškem sektorju, vključno s tradicionalnimi in inovativnimi poslovnimi modeli, pri izvajanju zavarovalnih storitev in pri običajnem operativnem delovanju podjetij vse bolj opirajo na IKT, na primer digitalizacija zavarovalniškega sektorja (InsurTech, IoT itd.) in medsebojno povezovanje prek telekomunikacijskih kanalov (internet, mobilne in brezžične povezave ter prostrana omrežja). Delovanje podjetij je zato izpostavljeno varnostnim incidentom, vključno s kibernetskimi napadi. Pomembno je zato zagotoviti ustrezno pripravljenost podjetij na obvladovanje njihovih varnostnih tveganj IKT.

8. Te smernice ob priznavanju, da morajo biti zavarovalnica in/ali pozavarovalnicaa pripravljena na kibernetsko tveganje[3] in imeti trden okvir za kibernetsko varnost, vključujejo tudi kibernetsko varnost kot del ukrepov podjetij za zagotavljanje informacijske varnosti. Čeprav te smernice priznavajo, da bi bilo treba kibernetsko varnost obravnavati v okviru splošnega obvladovanja varnostnih tveganj IKT v

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

[2] Poročilo, ki ga je organ EIOPA objavil kot odziv na akcijski načrt Evropske komisije za finančno tehnologijo, je na voljo tukaj.

[3] Opredelitev kibernetskega tveganja je na voljo v kibernetskem leksikonu FSB z dne 12 novembra 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf

zavarovalnica in/ali pozavarovalnicau, je pomembno poudariti, da imajo kibernetski napadi nekatere posebne značilnosti, ki bi jih bilo treba upoštevati, da bi se z ukrepi informacijske varnosti ustrezno zmanjšalo kibernetsko tveganje:

a) kibernetske napade je pogosto težje obvladovati (tj. jih opredeliti, se zavarovati pred njimi, jih odkriti, se odzvati nanje in ponovno vzpostaviti delovanje) kot večino drugih virov varnostnega tveganja IKT, prav tako je tudi težko določiti obseg škode;

b) pri nekaterih kibernetskih napadih so lahko splošne ureditve obvladovanja tveganja in neprekinjenega poslovanja ter postopki za ponovno vzpostavitev delovanja po incidentu neučinkoviti, ker ti napadi lahko prenesejo zlonamerno programsko opremo do sistemov varnostnega kopiranja, da bi preprečili njihovo razpoložljivost ali poškodovali podatke iz varnostne kopije;

c) kibernetski napadi se lahko širijo prek ponudnikov storitev, agentov, pooblaščencev (za upravljanje) in posrednikov. Kužne tihe grožnje se lahko prek medsebojne povezljivosti po telekomunikacijskih povezavah tretjih oseb prenesejo do sistema IKT zavarovalnica in/ali pozavarovalnicaa. Medsebojno povezano manj pomembno zavarovalnica in/ali pozavarovalnicae zato lahko postane ranljivo in vir širjenja tveganja, kar lahko povzroči sistemski učinek. V skladu z načelom najšibkejšega člena kibernetska varnost ni skrb samo pomembnih udeležencev na trgu ali ponudnikov kritičnih storitev.

9. Cilj teh smernic je:

a) udeležencem na trgu zagotoviti pojasnila in preglednost glede minimalnih pričakovanih informacij in zmogljivosti kibernetske varnosti, tj. varnostno izhodišče;

b) preprečiti morebitno regulativno arbitražo;

c) okrepiti nadzorniško zbliževanje glede pričakovanj in postopkov, ki se uporabljajo v zvezi z upravljanjem varnosti IKT, kot ključno za pravilno obvladovanje varnostnih tveganj IKT.

Smernice o upravljanju varnosti informacijske in komunikacijske tehnologije

Uvod

1. Organ EIOPA v skladu s členom 16 Uredbe (EU) št. 1094/2010[4] izdaja te smernice, naslovljene na nadzorne organe, da bi zagotovil smernice o tem, kako bi morale zavarovalnice in pozavarovalnice (skupno „zavarovalnica in/ali pozavarovalnicaa") upoštevati zahteve glede upravljanja iz Direktive 2009/138/ES[5] („direktiva Solventnost II") in Delegirane uredbe Komisije (EU) št. 2015/35[6] („Delegirana uredba") pri upravljanju varnosti informacijske in komunikacijske tehnologije („IKT"). Te smernice zato temeljijo na določbah o upravljanju členov 41, 44, 46, 47, 132 in 246 direktive Solventnost II ter členov 258 do 260, 266, 268 do 271 in 274 Delegirane uredbe. Temeljijo tudi na smernicah organa EIOPA o sistemu upravljanja (EIOPA-BoS-14/253)[7] in smernicah organa EIOPA o oddajanju storitev v izvajanje zunanjim ponudnikom storitev v oblaku (EIOPA-BoS-19/270)[8].
2. Smernice se uporabljajo za posamezna zavarovalnica in/ali pozavarovalnicaa in smiselno na ravni skupine[9].
3. Pristojni organi bi morali pri zagotavljanju ali nadzoru skladnosti s temi smernicami upoštevati načelo sorazmernosti[10], ki bi moralo zagotoviti, da je ureditev upravljanja, vključno z ureditvijo, povezano z upravljanjem varnosti IKT, sorazmerna z naravo, obsegom in zapletenostjo ustreznih tveganj, ki so jim ali so jim lahko izpostavljena zavarovalnica in/ali pozavarovalnicaa.
4. Te smernice se berejo v povezavi in brez poseganja v direktivo Solventnost II, delegirano uredbo, smernice organa EIOPA o sistemu upravljanja in smernice organa EIOPA o oddajanju storitev v izvajanje zunanjim ponudnikom storitev v oblaku. Te smernice naj bi bile tehnološko in metodološko nevtralne.

Opredelitve pojmov

5. Izrazi, ki v teh smernicah niso opredeljeni, imajo pomen iz direktive Solventnost II.
6. Za namene teh smernic se uporabljajo naslednje opredelitve pojmov:

[4] Uredba (EU) št. 1094/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za zavarovanja in poklicne pokojnine) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/79/ES (UL L 331, 15.12.2010, str. 48).

[5] Direktiva 2009/138/ES Evropskega parlamenta in Sveta z dne 25. novembra 2019 o začetku opravljanja in opravljanju dejavnosti zavarovanja in pozavarovanja (Solventnost II) (UL L 335, 17.12.2009, str. 1).

[6] Delegirana uredba Komisije (EU) 2015/35 z dne 10. oktobra 2014 o dopolnitvi Direktive 2009/138/ES Evropskega parlamenta in Sveta o začetku opravljanja in opravljanju dejavnosti zavarovanja in pozavarovanja (Solventnost II) (UL L 12, 17.1.2015, str. 1).

[7] https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa_guidelines_on_system_of_governance_sl.pdf

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

[9] Člen 212(1) Direktive 2009/138/ES.

[10] Člen 29(3) Direktive 2009/138/ES.

Lastnik sredstva	Oseba ali subjekt, odgovoren in pristojen za informacijsko sredstvo in sredstvo IKT.
Razpoložljivost	Lastnost biti dostopen in uporaben na zahtevo (pravočasnost) pooblaščenega subjekta.
Zaupnost	Lastnost, da se informacije ne dajo na voljo in ne razkrivajo nepooblaščenim posameznikom, subjektom, postopkom ali sistemom.
Kibernetski napad	Katera koli vrsta vdora v računalniški sistem, ki pripelje do napadalnega/zlonamernega poskusa uničiti, izpostaviti, spremeniti, onesposobiti ali ukrasti informacijsko sredstvo, pridobiti nepooblaščen dostop do njega ali ga nepooblaščeno uporabiti ter ki je usmerjen v sisteme IKT.
Kibernetska varnost	Ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij ter/ali informacijskih sistemov prek kibernetskega sredstva.
Sredstvo IKT	Sredstvo, ki je lahko programska ali strojna oprema in se uporablja v poslovnem okolju.
Projekti IKT	Kateri koli projekt ali njegov del, pri katerem se sistemi in storitve IKT spremenijo, nadomestijo ali izvedejo.
Varnostno tveganje IKT	Kot podelement operativnega tveganja; tveganje izgube zaradi kršitve zaupnosti, necelovitosti sistemov in podatkov, neustreznosti ali nerazpoložljivosti sistemov in podatkov ali nezmožnosti spremeniti IKT v razumnem času in z razumnimi stroški, kadar se spremenijo okoljske ali poslovne zahteve (tj. prožnost). To vključuje kibernetska in informacijska varnostna tveganja, ki so posledica neustreznih ali neučinkovitih notranjih postopkov ali zunanjih dogodkov, vključno s kibernetskimi napadi ali neustrezno fizično varnostjo.
Informacijska varnost	Ohranjanje zaupnosti, celovitosti in razpoložljivosti informacij ter/ali informacijskih sistemov. Vključuje lahko tudi druge lastnosti, kot so avtentičnost, odgovornost, neizvrševanje in zanesljivost.
Storitve IKT	Storitve, ki jih ponudniki storitev prek sistemov IKT zagotavljajo enemu ali več notranjim ali zunanjim uporabnikom.

Sistemi IKT	Sklop aplikacij, storitev, sredstev informacijske tehnologije, sredstev IKT ali drugih sestavnih delov, ki obravnavajo informacije, kar vključuje operativno okolje.
Informacijsko sredstvo	Zbirka opredmetenih ali neopredmetenih informacij, ki jih je treba zavarovati.
Celovitost	Lastnost točnosti in popolnosti.
Operativni ali varnostni incident	Enkratni dogodek ali niz povezanih nenačrtovanih dogodkov, ki imajo ali bodo verjetno imeli negativen učinek na celovitost, razpoložljivost in zaupnost sistemov in storitev IKT.
Ponudnik storitev	Pomeni tretjo osebo, ki v celoti ali delno izvaja postopek, storitev ali dejavnost na podlagi dogovora o zunanjem izvajanju.
Penetracijsko testiranje ob upoštevanju groženj	Nadzorovan poskus ogroziti kibernetsko odpornost subjekta s simuliranjem taktike, tehnik in postopkov za resnične grožnje. Temelji na ciljno usmerjenih obveščevalnih podatkih o grožnjah ter je osredotočen na osebje, postopke in tehnologijo subjekta, z minimalnimi predhodnimi informacijami in vplivom na operacije.
Ranljivost	Šibka točka, dovzetnost ali pomanjkljivost sredstva ali nadzora, ki jih lahko izkoristi ena ali več groženj.

7. Te smernice se začnejo uporabljati 1. julija 2021.

Smernica 1 – Sorazmernost

8. Zavarovalnica in/ali pozavarovalnicaa bi morala te smernice uporabljati na način, sorazmeren z naravo, obsegom in zapletenostjo tveganj, katerim so izpostavljena pri opravljanju svoje dejavnosti.

Smernica 2 – IKT v okviru sistema upravljanja

9. Upravni, upravljalni ali nadzorni organ bi moral zagotoviti, da zavarovalnica in/ali pozavarovalnicaa s svojimi sistemi upravljanja, predvsem s sistemom obvladovanja tveganja in notranjega nadzora, ustrezno obvladujejo svoja varnostna tveganja IKT.

10. Upravni, upravljalni ali nadzorni organ bi moral zagotoviti, da so število ter znanja in spretnosti zaposlenih v zavarovalnica in/ali pozavarovalnicaih ustrezni za nenehno podporo operativnim potrebam IKT in postopkom obvladovanja varnostnih tveganj IKT ter zagotavljajo izvajanje strategije IKT. Poleg tega bi se moral i zaposleni redno ustrezno usposabljati o varnostnih tveganjih IKT, vključno z varnostjo informacij, v skladu s smernico 13.

11. Upravni, upravljalni ali nadzorni organ bi morali zagotoviti, da so dodeljeni viri ustrezni za izpolnjevanje zgornjih zahtev.

Smernica 3 – Strategija IKT

12. Upravni, upravljalni ali nadzorni organ je na splošno odgovoren za določitev in odobritev pisne strategije IKT podjetij, ki je sestavni del njihove splošne poslovne strategije in je z njo usklajena, ter za nadzor obveščanja o njej in njenega izvajanja.

13. V strategiji IKT se opredelijo vsaj:

    a) kako bi se morala razvijati IKT podjetij za učinkovito podporo in izvajanje njihove poslovne strategije, vključno z razvojem organizacijske strukture, poslovnih modelov, sistema IKT in ključnih odvisnosti od ponudnikov storitev;

    b) razvoj arhitekture IKT, vključno z odvisnostmi od ponudnikov storitev; ter

    c) jasni cilji glede informacijske varnosti, s poudarkom na sistemih, storitvah, zaposlenih in postopkih IKT.

14. Zavarovalnica in/ali pozavarovalnicaa bi morala zagotoviti, da se strategija IKT izvaja in sprejme ter da so o njej pravočasno obveščeni vsi zadevni zaposleni in ponudniki storitev, kot je potrebno in ustrezno.

15. Zavarovalnica in/ali pozavarovalnicaa bi morala vzpostaviti tudi postopek za spremljanje in merjenje uspešnosti izvajanja svoje strategije IKT. Ta postopek se redno pregleduje in posodablja.

Smernica 4 – Varnostna tveganja IKT v okviru sistema obvladovanja tveganja

16. Upravni, upravljalni ali nadzorni organ je na splošno odgovoren za vzpostavitev učinkovitega sistema za obvladovanje varnostnih tveganj IKT v okviru splošnega sistema zavarovalnica in/ali pozavarovalnicaa za obvladovanje tveganja. To vključuje določitev dopustnega tveganja za navedena tveganja v skladu s strategijo zavarovalnica in/ali pozavarovalnicaa za obvladovanje tveganja in redno pisno poročilo o rezultatu postopka obvladovanja tveganja, naslovljeno na upravni, upravljalni ali nadzorni organ.

17. Zavarovalnica in/ali pozavarovalnicaa bi morala v okviru svojega splošnega sistema obvladovanja tveganja (pri opredelitvi zahtev glede zaščite IKT, kot so opisane spodaj) upoštevati vsaj naslednje:

    a) zavarovalnica in/ali pozavarovalnicaa vzpostavijo in redno posodabljajo shematsko razporeditev svojih poslovnih procesov in dejavnosti, poslovnih funkcij, vlog in sredstev (npr. informacijska sredstva in sredstva IKT), da bi opredelila njihov pomen ter soodvisnosti od IKT in varnostnih tveganj;

    b) zavarovalnica in/ali pozavarovalnicaa opredelijo in merijo vsa pomembna varnostna tveganja IKT, ki so jim izpostavljena, ter razvrstijo opredeljene poslovne procese in dejavnosti, poslovne funkcije, vloge in sredstva (npr. informacijska sredstva in sredstva IKT) z vidika kritičnosti. Oceniti bi morala tudi vsaj zahteve glede varstva zaupnosti, celovitosti in razpoložljivosti navedenih poslovnih procesov in dejavnosti, poslovnih funkcij, vlog in sredstev (npr. informacijskih sredstev in sredstev IKT). Opredeliti bi bilo treba lastnike sredstev, odgovorne za njihovo razvrstitev;

    c) z metodami, uporabljenimi za določitev kritičnosti, in zahtevano ravnjo varstva, predvsem v zvezi s cilji glede varstva celovitosti, razpoložljivosti in

zaupnosti, bi se morala zagotoviti skladnost in celovitost tako določenih zahtev;

d) varnostna tveganja IKT bi se morala meriti na podlagi opredeljenih meril varnostnih tveganj IKT ob upoštevanju kritičnosti njihovih poslovnih procesov in dejavnosti, poslovnih funkcij, vlog in sredstev (npr. informacijskih sredstev in sredstev IKT), obsega znanih ranljivosti in predhodnih incidentov, ki so vplivali na zavarovalnica in/ali pozavarovalnicae;

e) varnostna tveganja IKT bi se moreala redno ocenjevati in dokumentirati. Ta ocena bi se morala opraviti tudi pred vsako večjo spremembo infrastrukture, procesov ali postopkov, ki vpliva na poslovne procese in dejavnosti, poslovne funkcije, vloge in sredstva (npr. informacijska sredstva in sredstva IKT);

f) zavarovalnica in/ali pozavarovalnicaa bi morala na podlagi svoje ocene tveganja opredeliti in izvajati vsaj ukrepe za obvladovanje opredeljenih varnostnih tveganj IKT in varstvo informacijskih sredstev v skladu z njihovo razvrstitvijo. Sem bi bilo treba vključiti tudi opredelitev ukrepov za obvladovanje preostalih tveganj.

18. Rezultate postopka obvladovanja varnostnih tveganj IKT bi moral odobriti upravni, upravljalni ali nadzorni organ, vključiti pa jih je treba v postopek obvladovanja operativnega tveganja v okviru splošnega obvladovanja tveganj v zavarovalnica in/ali pozavarovalnicaih.

Smernica 5 – Revizija

19. Upravljanje, sisteme in postopke podjetij za varnostna tveganja IKT bi moral v skladu z njihovim revizijskim načrtom[11] redno pregledovati revizorji, ki imajo dovolj znanja, spretnosti in izkušenj s področja varnostnih tveganj IKT, da upravnemu, upravljalnemu ali nadzornemu organu zagotovijo neodvisno zagotovilo o njihovi učinkovitosti. Pogostost in osredotočenost takih revizij morata biti sorazmerni z zadevnimi varnostnimi tveganji IKT.

Smernica 6 – Politika in ukrepi informacijske varnosti

20. Zavarovalnica in/ali pozavarovalnicaa bi morala določiti pisno politiko informacijske varnosti, ki jo odobri upravni, upravljalni ali nadzorni organ ter v kateri bi morala biti opredeljena načela in pravila na visoki ravni za varstvo zaupnosti, celovitosti in razpoložljivosti informacij podjetij, da bi se podprlo izvajanje strategije IKT.

21. Politika bi morala vključiti opis glavnih vlog in odgovornosti za upravljanje informacijske varnosti, v njej pa opredeliti določene zahteve za osebje, postopke in tehnologijo v zvezi z informacijsko varnostjo, ob priznavanju, da so za zagotavljanje informacijske varnosti podjetij odgovorni zaposleni na vseh ravneh.

22. O politiki se obvešča v okviru zavarovalnica in/ali pozavarovalnicaa in se uporablja za vse zaposlene. O politiki informacijske varnosti ali njenih delih bi bilo treba, po potrebi in kadar je primerno, obvestiti tudi ponudnike storitev ter jih uporabljati tudi zanje.

23. Zavarovalnica in/ali pozavarovalnicaa bi morala na podlagi politike vzpostaviti in izvajati bolj specifične postopke in ukrepe informacijske varnosti, da bi med drugim zmanjšala varnostna tveganja IKT, katerim so izpostavljena. Ti postopki in ukrepi

[11] Člen 271 Delegirane uredbe.

informacijske varnosti bi morala po potrebi vključevati vse postopke, opisane v teh smernicah.

Smernica 7 – Funkcija informacijske varnosti

24. Zavarovalnica in/ali pozavarovalnicaa bi morala v skladu z načelom sorazmernosti v okviru svojega sistema upravljanja vzpostaviti funkcijo informacijske varnosti z odgovornostmi, dodeljenimi imenovani osebi. Neodvisnost in nepristranskost funkcije informacijske varnosti bi se morala zagotoviti z njeno ustrezno ločitvijo od postopkov razvoja in delovanja IKT. Funkcija poroča upravnemu, upravljalnemu ali nadzornemu organu.

25. Naloge funkcije informacijske varnosti so običajno:

    a) podpiranje upravnega, upravljalnega ali nadzornega organa pri opredelitvi in ohranjanju politike informacijske varnosti za zavarovalnica in/ali pozavarovalnicaa ter nadzor njene uporabe;

    b) redno in ad hoc poročanje in obveščanje upravnega, upravljalnega ali nadzornega organa o stanju informacijske varnosti in njenem razvoju;

    c) spremljanje in pregled izvajanja ukrepov informacijske varnosti;

    d) zagotavljanje upoštevanja zahtev glede informacijske varnosti pri uporabi ponudnikov storitev;

    e) zagotavljanje, da so vsi zaposleni in ponudniki storitev, ki imajo dostop do informacij in sistemov, dobro obveščeni o politiki informacijske varnosti, na primer prek usposabljanja in ozaveščanja o informacijski varnosti;

    f) usklajevanje preučevanja operativnega ali varnostnega incidenta in sporočanje pomembnih incidentov upravnemu, upravljalnemu ali nadzornemu organu.

Smernica 8 – Logična varnost

26. Zavarovalnica in/ali pozavarovalnicaa bi morala opredeliti, dokumentirati in izvajati postopke za nadzor logičnega dostopa ali logične varnosti (upravljanje identitete in dostopa) v skladu z zahtevami glede varstva iz smernice 4. Ti postopki bi se morali vzpostaviti, izvajati, spremljati in redno pregledovati, vključevati pa bi morala tudi nadzor spremljanja nepravilnosti. S temi postopki bi se morali izvajati vsaj naslednji elementi, pri čemer izraz „uporabnik" vključuje tudi tehnične uporabnike:

    a) potreba po seznanitvi, najmanjši privilegij in ločitev nalog: zavarovalnica in/ali pozavarovalnicaa upravljajo pravice dostopa, vključno z dostopom na daljavo, do informacijskih sredstev in njihovih podpornih sistemov na podlagi „potrebe po seznanitvi". Uporabnikom bi se morale dodeliti minimalne pravice dostopa, nujno potrebne za izvajanje njihovih nalog (načelo „najmanjšega privilegija"), tj. da se prepreči neupravičen dostop do podatkov ali da bi se dodeljena kombinacija pravic dostopa lahko uporabila za izogibanje nadzoru (načelo „ločitve nalog");

    b) odgovornost uporabnikov: zavarovalnica in/ali pozavarovalnicaa bi morala v največji možni meri omejiti uporabo generičnih in skupnih uporabniških računov ter zagotoviti, da je vedno mogoče uporabnike identificirati in jim slediti do odgovorne fizične osebe ali pooblaščene naloge za dejanja, izvedena v sistemih IKT;

c) pravice privilegiranega dostopa: zavarovalnica in/ali pozavarovalnicaa bi morala izvajati dosleden nadzor nad privilegiranim dostopom do sistemov, tako da se strogo omeji in skrbno nadzoruje račune z večjimi pravicami dostopa do sistemov (npr. skrbniške račune);

d) dostop na daljavo: da bi se zagotovila varna komunikacija in zmanjšalo tveganja, bi se moral oddaljeni skrbniški dostop do kritičnih sistemov IKT odobriti samo na podlagi potrebe po seznanitvi in ob uporabi rešitev stroge avtentikacije;

e) beleženje uporabniških dejavnosti: dejavnosti uporabnikov bi se morale beležiti in spremljati sorazmerno s tveganjem, kar vključuje vsaj dejavnosti privilegiranih uporabnikov. Dnevniki dostopov bi se morali zavarovati, da se prepreči nedovoljeno spreminjanje ali izbris, ter biti shranjeni za obdobje, ki je sorazmerno s kritičnostjo opredeljenih poslovnih funkcij, podpornih procesov in informacijskih sredstev, brez poseganja v zahteve glede hrambe, ki jih določata zakonodaja EU in nacionalna zakonodaja. Uporabniki bi morali te informacije uporabiti za lažje prepoznavanje in preiskovanje nenavadnih dejavnosti, ugotovljenih pri izvajanju storitev;

f) upravljanje dostopa: pravice dostopa bi se morale pravočasno dodeliti, preklicati ali spremeniti po vnaprej določenih običajnih postopkih za odobritev, če je vključen lastnik zadevnega informacijskega sredstva. Če dostop ni več potreben, bi se morale pravice dostopa nemudoma preklicati;

g) presoja dostopa: pravice dostopa bi se morale redno pregledovati, da se zagotovi, da uporabniki nimajo prevelikih privilegijev in da se pravice dostopa prekličejo/ukinejo, ko niso več potrebne;

h) dodelitev, sprememba in preklic pravic dostopa bi se morale dokumentirati na način, ki omogoča razumevanje in analizo; ter

i) metode avtentikacije: zavarovalnica in/ali pozavarovalnicaa bi morala izvajati metode avtentikacije, ki so dovolj zanesljive, da ustrezno in dejansko zagotavljajo upoštevanje politik in postopkov glede nadzora dostopa. Metode avtentikacije bi morale biti sorazmerne s kritičnostjo sistemov, informacij ali procesa IKT, do katerih je mogoč dostop. To bi moralo vključevati vsaj zapletena gesla ali strožje metode avtentikacije (npr. dvofaktorsko avtentikacijo), ki temeljijo na zadevnem tveganju.

27. Elektronski dostop do podatkov in sistemov IKT prek aplikacij bi moral biti omejen na nujno potrebno za izvajanje zadevne storitve.

Smernica 9 – Fizična varnost

28. Zavarovalnica in/ali pozavarovalnicaa bi morala opredeliti, dokumentirati in izvajati ukrepe fizične varnosti (npr. zavarovanje pred izpadom električne energije, požarom, vodo in nepooblaščenim fizičnim dostopom) za zavarovanje svojih prostorov, podatkovnih centrov in občutljivih območij pred nepooblaščenim dostopom in okoljskimi nevarnostmi.

29. Fizičen dostop do sistemov IKT bi moral biti dovoljen samo pooblaščenim posameznikom. Pooblastilo bi se moralo dodeliti v skladu s posameznikovimi nalogami in odgovornostmi ter omejiti na posameznike, ki so ustrezno usposobljeni in nadzorovani. Fizični dostop bi se moral redno pregledovati, s čimer se zagotovi, da se nepotrebne pravice dostopa nemudoma prekličejo/ukinejo.

30. Ustrezni ukrepi za zavarovanje pred okoljskimi nevarnostmi bi morali biti sorazmerni s pomenom stavb in kritičnostjo operacij ali sistemov IKT v teh stavbah.

Smernica 10 – Varnost operacij IKT

31. Zavarovalnica in/ali pozavarovalnicaa bi morala izvajati postopke za zagotavljanje zaupnosti, celovitosti in razpoložljivosti sistemov in storitev IKT, da bi čim bolj zmanjšala vpliv varnostnih vprašanj na izvajanje storitev IKT. Ti postopki bi morali ustrezno vključevati naslednje ukrepe:

    a) opredelitev morebitnih ranljivosti, ki se ocenijo in odpravijo s posodabljanjem sistemov IKT, vključno s programsko opremo, ki jo zavarovalnica in/ali pozavarovalnicaa zagotovijo notranjim in zunanjim uporabnikom, z uporabo kritičnih varnostnih popravkov, vključno s posodobitvami opredelitev protivirusnih programov, ali z izvajanjem nadomestnih kontrol;

    b) izvajanje varnih konfiguracijskih izhodišč za vse kritične komponente, kot so operativni sistemi, podatkovne zbirke, usmerjevalniki in stikala;

    c) izvajanje omrežne segmentacije, sistemov za preprečevanje uhajanja podatkov in šifriranje omrežnega prometa (v skladu z razvrstitvijo informacijskih sredstev);

    d) izvajanje zaščite končnih točk, vključno s strežniki, delovnimi postajami in mobilnimi napravami. Zavarovalnica in/ali pozavarovalnicaa bi morala preveriti, ali končne točke izpolnjujejo varnostne standarde, ki so jih opredelila, preden so jim odobrila dostop do svojega omrežja;

    e) zagotovitev, da so vzpostavljeni mehanizmi za preverjanje celovitosti sistemov IKT;

    f) šifriranje podatkov v mirovanju in v prenosu (v skladu z razvrstitvijo informacijskih sredstev).

Smernica 11 – Spremljanje varnosti

32. Zavarovalnica in/ali pozavarovalnicaa bi morala vzpostaviti ter izvajati postopke in procese za nenehno spremljanje dejavnosti, ki vplivajo na njihovo informacijsko varnost. Spremljanje bi moralo vključevati vsaj:

    a) notranje in zunanje dejavnike, vključno s poslovnimi in upravnimi funkcijami IKT;

    b) transakcije ponudnikov storitev, drugih subjektov in notranjih uporabnikov ter

    c) morebitne notranje in zunanje grožnje.

33. Zavarovalnica in/ali pozavarovalnicaa bi morala na podlagi spremljanja vzpostaviti primerne in učinkovite zmogljivosti za odkrivanje, poročanje in odzivanje na nenavadne dejavnosti in grožnje, kot so fizični ali logični vdori, kršitve zaupnosti, celovitosti in razpoložljivosti informacijskih sredstev, zlonamerna koda ter javno znane ranljivosti programske in strojne opreme.

34. Poročanje na podlagi spremljanja varnosti bi moralo zavarovalnica in/ali pozavarovalnicaem pomagati razumeti naravo operativnih ali varnostnih incidentov za prepoznavanje trendov in podporo zavarovalnica in/ali pozavarovalnicaem pri notranjih preiskavah ter jim omogočiti sprejetje ustreznih odločitev.

Smernica 12 – Pregledi, ocena in preskušanje informacijske varnosti

35. Zavarovalnica in/ali pozavarovalnicaa bi morala izvajati različne preglede, ocene in preskuse informacijske varnosti, da zagotovijo učinkovito prepoznavanje ranljivosti v svojih sistemih in storitvah IKT. Opravijo lahko na primer analizo vrzeli glede na standarde informacijske varnosti, preglede skladnosti, notranje in zunanje revizije informacijskih sistemov ali preglede fizične varnosti.

36. Zavarovalnica in/ali pozavarovalnicaa bi morala vzpostaviti in izvajati okvir za preskušanje informacijske varnosti, s katerim potrdijo zanesljivost in učinkovitost ukrepov informacijske varnosti, ter zagotoviti, da ta okvir upošteva grožnje in ranljivosti, opredeljene s spremljanjem groženj in oceno varnostnih tveganj IKT.

37. Preskušanje bi morali varno izvajati neodvisni preskuševalci, ki imajo dovolj znanja, spretnosti in izkušenj s preskušanjem ukrepov informacijske varnosti.

38. Zavarovalnica in/ali pozavarovalnicaa bi morala preskuse izvajajo redno. Obseg, pogostost in metoda preskušanja (npr. penetracijsko testiranje, vključno s penetracijskim testiranjem ob upoštevanju grožnje) bi morali biti sorazmerni z ravnjo opredeljenega tveganja. Preskusi kritičnih sistemov IKT in pregledi ranljivosti bi se morali izvajati letno.

39. Zavarovalnica in/ali pozavarovalnicaa bi morala zagotoviti, da se preskusi varnostnih ukrepov izvedejo pri spremembah infrastrukture, procesov ali postopkov ali pri spremembah, sprejetih zaradi večjih operativnih ali varnostnih incidentov ali zaradi izdaje novih ali pomembno spremenjenih kritičnih aplikacij. Spremljati in vrednotiti bi morala rezultate varnostnih preskusov ter in v skladu z njimi nemudoma posodobiti svoje varnostne ukrepe v primeru kritičnih sistemov IKT.

Smernica 13 – Usposabljanje in ozaveščanje o informacijski varnosti

40. Zavarovalnica in/ali pozavarovalnicaa bi morala vzpostaviti programe usposabljanja o informacijski varnosti za vse osebje, vključno z upravnim, upravljalnim ali nadzornim organom, za zagotovitev njihove usposobljenosti za opravljanje nalog ter odgovornosti za zmanjšanje človeških napak, kraj, goljufij, zlorab ali izgub. Zagotoviti bi morala, da program usposabljanja redno zagotavlja usposabljanje za vse osebje.

41. Zavarovalnica in/ali pozavarovalnicaa bi morala vzpostaviti in izvajati občasne programe ozaveščanja o varnosti za izobraževanje svojega osebja, vključno z upravnim, upravljalnim ali nadzornim organom, o tem, kako morajo obravnavati tveganja, povezana z informacijsko varnostjo.

Smernica 14 – Upravljanje operacij IKT

42. Zavarovalnica in/ali pozavarovalnicaa bi morala upravljati svoje operacije IKT na podlagi strategije IKT. V dokumentih bi morala opredeliti, kako zavarovalnica in/ali pozavarovalnicae upravlja, spremlja in nadzoruje sisteme in storitve IKT, vključno z dokumentiranjem kritičnih procesov, postopkov in operacij IKT.

43. Zavarovalnica in/ali pozavarovalnicaa bi morala za kritične operacije IKT izvajati postopke beleženja in spremljanja, da se omogočijo odkrivanje, analiza in popravek napak.

44. Zavarovalnica in/ali pozavarovalnicaa bi morala voditi popis svojih sredstev IKT, ki ga sproti posodabljajo. Popis sredstev IKT bi moral biti dovolj podroben, da omogoča takojšnjo identifikacijo sredstva IKT, njegove lokacije, varnostne razvrstitve in lastništva.

45. Zavarovalnica in/ali pozavarovalnicaa bi morala spremljati in upravljati življenjski cikel sredstev IKT za zagotovitev, da ta še naprej izpolnjujejo in podpirajo poslovne zahteve in zahteve za obvladovanje tveganja. Na podlagi dokumentiranega postopka bi morala zavarovalnica in/ali pozavarovalnicaa spremljati, ali sredstva IKT podpirajo njihovi dobavitelji ali notranji razvijalci ter ali se uporabljajo vsi ustrezni popravki in posodobitve. Tveganja, ki izhajajo iz zastarelih ali nepodprtih sredstev IKT, bi se morala oceniti in zmanjšati. Razgrajena sredstva IKT bi se morala varno predelati in odstraniti.

46. Zavarovalnica in/ali pozavarovalnicaa bi morala izvajati postopke načrtovanja učinkovitosti in zmogljivosti ter spremljanja za pravočasno preprečevanje, odkrivanje in odzivanje na pomembna vprašanja glede učinkovitosti sistemov IKT in premajhnih zmogljivosti IKT.

47. Zavarovalnica in/ali pozavarovalnicaa bi morala opredeliti in izvajati postopke za varnostno kopiranje in obnovitev podatkov in sistemov IKT, da se po potrebi lahko obnovijo. Obseg in pogostost varnostnega kopiranja bi se morala določiti v skladu z zahtevami za obnovitev delovanja ter kritičnostjo podatkov in sistemov IKT, ovrednotenih v skladu z opravljeno oceno tveganja. Postopki varnostnega kopiranja in obnovitve bi se morali redno preskušati.

48. Zavarovalnica in/ali pozavarovalnicaa bi morala zagotoviti, da se varnostne kopije podatkov in sistemov IKT hranijo na eni ali več lokacij zunaj prvotne lokacije, ki so varne in dovolj oddaljene od prvotne lokacije, da niso izpostavljene enakim tveganjem.

Smernica 15 – Obvladovanje incidentov in odpravljanje težav IKT

49. Zavarovalnica in/ali pozavarovalnicaa bi morala vzpostaviti in izvajati postopek obvladovanja incidentov in odpravljanja težav, da se spremljajo in beležijo operativni in varnostni incidenti ter da se zavarovalnica in/ali pozavarovalnicaem omogoči nadaljnje izvajanje ali ponovna vzpostavitev kritičnih poslovnih funkcij in procesov, kadar se pojavijo motnje.

50. Zavarovalnica in/ali pozavarovalnicaa bi morala določiti ustrezna merila in prage za razvrstitev dogodka med operativne ali varnostne incidente ter zgodnje opozorilne znake, ki bi jih bilo treba uporabljati kot opozorilo, ki omogoča zgodnje odkrivanje teh incidentov.

51. Zavarovalnica in/ali pozavarovalnicaa bi morala za zmanjšanje učinka škodljivih dogodkov in pravočasno obnovitev delovanja vzpostaviti ustrezne postopke in organizacijske strukture za dosledno in celovito spremljanje, obravnavanje in nadaljnje ukrepanje ob operativnih in varnostnih incidentih, da se opredelijo in obravnavajo temeljni vzroki ter sprejmejo popravljalni ukrepi za preprečitev ponovitve incidentov. Postopek obvladovanja incidentov in odpravljanja težav bi moral določati vsaj:

    a) postopke za opredelitev, spremljanje, beleženje in razvrstitev incidentov po pomembnosti, ki jo je določilo zavarovalnica in/ali pozavarovalnicae na podlagi njihove kritičnosti za neprekinjeno delovanje in pogodb o izvajanju storitev;

    b) vloge in odgovornosti za različne scenarije incidentov (npr. napake, nepravilno delovanje, kibernetski napadi);

    c) postopek za odpravljanje težav, da se opredeli, analizira in odpravi temeljni vzrok enega ali več incidentov; zavarovalnica in/ali pozavarovalnicaa bi morala analizirati operativne ali varnostne incidente, ki so bili opredeljeni ali

so se zgodili v organizaciji in/ali zunaj nje, ter proučiti ključna spoznanja, pridobljena na podlagi teh analiz, in ustrezno posodobiti varnostne ukrepe;

d) načrte učinkovite notranje komunikacije, vključno s postopkoma za obveščanje o incidentih in stopnjevanje, kar vključuje tudi pritožbe strank v zvezi z varnostjo, da se zagotovi, da:

   i. se o incidentih z morebitnim velikim škodljivim vplivom na kritične sisteme in storitve IKT poroča pristojnemu višjemu vodstvu;

   ii. je upravni, upravljalni ali nadzorni organ pri pomembnih incidentih na ad hoc podlagi obveščen vsaj o vplivu, odzivu in dodatnih kontrolah, opredeljenih zaradi incidentov;

e) postopke za odzivanje na incidente, da se zmanjša vpliv, povezan z incidenti, ter zagotovi, da storitev pravočasno začne delovati in postane varna;

f) specifične načrte zunanje komunikacije za kritične poslovne funkcije in procese za:

   i. sodelovanje z zadevnimi deležniki pri učinkovitem odzivu in obnovitvi delovanja po incidentu;

   ii. zagotavljanje pravočasnih informacij, vključno s poročanjem o incidentih, zunanjim osebam (npr. strankam, drugim udeležencem na trgu, zadevnim (nadzornim) organom, kot je potrebno in v skladu z ureditvijo, ki se uporablja).

Smernica 16 – Upravljanje projektov IKT

52. Zavarovalnica in/ali pozavarovalnicaa bi morala izvajati metodologijo za upravljanje projektov IKT (vključno z upoštevanjem neodvisnih varnostnih zahtev) z ustreznim postopkom upravljanja in vodenjem izvajanja projekta za učinkovito podporo izvajanju strategije IKT prek projektov IKT.

53. Zavarovalnica in/ali pozavarovalnicaa bi morala ustrezno spremljati in zmanjšati tveganja, ki izhajajo iz portfelja projektov IKT, pri čemer bi morala upoštevati tudi tveganja, ki lahko izhajajo iz soodvisnosti med različnimi projekti in odvisnosti več projektov od istih virov in/ali strokovnega znanja.

Smernica 17 – Nakup in razvoj sistemov IKT

54. Zavarovalnica in/ali pozavarovalnicaa bi morala razviti in izvajati postopek upravljanja nakupa, razvoja in vzdrževanja sistemov IKT, da bi se zaupnost, celovitost in razpoložljivost podatkov razumljivo zavarovali ter izpolnile opredeljene zahteve glede varstva. Ta postopek bi se moral oblikovati na podlagi pristopa, ki temelji na tveganju.

55. Zavarovalnica in/ali pozavarovalnicaa bi morala zagotoviti, da se pred nakupom ali razvojem sistema jasno opredelijo funkcionalne in nefunkcionalne zahteve (vključno z zahtevami glede informacijske varnosti) ter tehnični cilji.

56. Zavarovalnica in/ali pozavarovalnicaa bi morala zagotoviti, da se vzpostavijo ukrepi za preprečitev nenamernih sprememb ali namerne zlorabe sistemov IKT med razvojem.

57. Zavarovalnica in/ali pozavarovalnicaa bi morala imeti vzpostavljeno metodologijo za preskušanje in odobritev sistemov in storitev IKT ter ukrepov informacijske varnosti.

58. Zavarovalnica in/ali pozavarovalnicaa bi morala ustrezno preskusiti sisteme in storitve IKT ter ukrepe informacijske varnosti za ugotovitev morebitnih varnostnih pomanjkljivosti, kršitev in incidentov.

59. Zavarovalnica in/ali pozavarovalnicaa bi morala zagotoviti ločitev proizvodnih okolij od razvojnega, preizkusnega in drugih neproizvodnih okolij.

60. Zavarovalnica in/ali pozavarovalnicaa bi morala izvajati ukrepe za varstvo celovitosti izvorne kode (če je na voljo) sistemov IKT. Poleg tega bi morala celovito dokumentirati razvoj, izvajanje, upravljanje in/ali konfiguracijo sistemov IKT, da zmanjšajo nepotrebno odvisnost od področnih strokovnjakov.

61. Postopki podjetij za nakup in razvoj sistemov IKT bi se morali uporabljati tudi za sisteme IKT, ki jih razvijejo ali upravljajo končni uporabniki poslovne funkcije zunaj organizacije IKT (npr. za aplikacije, ki jih upravlja zavarovalnica in/ali pozavarovalnicae, ali računalniške aplikacije končnih uporabnikov), in sicer na podlagi pristopa, ki temelji na tveganju. Zavarovalnica in/ali pozavarovalnicaa bi morala voditi register teh aplikacij, ki podpirajo kritične poslovne funkcije ali procese.

Smernica 18 – Upravljanje sprememb IKT

62. Zavarovalnica in/ali pozavarovalnicaa bi morala vzpostaviti in izvajati postopek upravljanja sprememb IKT za zagotovitev, da se vse spremembe sistemov IKT nadzorovano beležijo, ocenijo, preskusijo, odobrijo, dovolijo in izvedejo. Nujne spremembe ali spremembe v izrednih razmerah bi morale biti sledljive, o njih pa bi moral biti naknadno obveščen lastnik zadevnega sredstva zaradi naknadne analize.

63. Zavarovalnica in/ali pozavarovalnicaa bi morala ugotoviti, ali spremembe v obstoječem operativnem okolju vplivajo na vzpostavljene varnostne ukrepe in ali je treba zaradi njih sprejeti dodatne ukrepe za zmanjšanje prisotnih tveganj. Te spremembe bi morale biti v skladu s formalnim postopkom podjetij za upravljanje sprememb.

Smernica 19 – Upravljanje neprekinjenega poslovanja

64. Upravni, upravljalni ali nadzorni organ je v okviru splošne politike neprekinjenega poslovanja podjetij odgovoren za določitev in odobritev politike podjetij za neprekinjeno delovanje IKT. O politiki zagotavljanja neprekinjenega delovanja IKT bi bilo treba v okviru podjetij ustrezno obveščati, uporabljati pa bi se morala za vse zadevno osebje in po potrebi ponudnike storitev.

Smernica 20 – Analiza poslovnega učinka

65. Zavarovalnica in/ali pozavarovalnicaa bi morala v okviru dobrega upravljanja neprekinjenega poslovanja izvesti analizo poslovnega učinka za oceno svoje izpostavljenosti resnim motnjam poslovanja ter kvantitativno in kvalitativno oceno njihovega morebitnega učinka na podlagi notranjih in/ali zunanjih podatkov in analize scenarijev. Pri analizi poslovnega učinka bi se morala upoštevati tudi kritičnost opredeljenih in razvrščenih poslovnih procesov in dejavnosti, poslovnih funkcij, vlog in sredstev (npr. informacijskih sredstev in sredstev IKT) ter njihovih soodvisnosti v skladu s smernico 4.

66. Zavarovalnica in/ali pozavarovalnicaa bi morala zagotoviti, da so njihovi sistemi in storitve IKT zasnovani v skladu z analizo poslovnega učinka, na primer ob upoštevanju nepotrebnosti nekaterih kritičnih komponent, da se preprečijo motnje, ki jih povzročijo dogodki, ki vplivajo na te komponente.

Smernica 21 – Načrtovanje neprekinjenega poslovanja

67. Splošni načrti podjetij za neprekinjeno poslovanje bi morali upoštevati pomembna tveganja, ki bi lahko škodljivo vplivala na sisteme in storitve IKT. Načrti bi morali podpirati cilje glede varstva ter po potrebi ponovne vzpostavitve zaupnosti, celovitosti in razpoložljivosti poslovnih procesov in dejavnosti, poslovnih funkcij, vlog in sredstev podjetij (npr. informacijskih sredstev in sredstev IKT). Zavarovalnica in/ali pozavarovalnicaa bi se morala med pripravo teh načrtov po potrebi usklajevaati z zadevnimi notranjimi in zunanjimi deležniki.

68. Zavarovalnica in/ali pozavarovalnicaa bi morala sprejeti načrte neprekinjenega poslovanja, da se lahko ustrezno odzovejo na scenarije morebitnega izpada delovanja v skladu s ciljnim časom obnovitve delovanja (najdaljši čas, v katerem je treba po incidentu sistem ali proces ponovno vzpostaviti) in ciljno točko obnovitve delovanja (najdaljši čas, v katerem je ob incidentu sprejemljiva izguba podatkov na vnaprej določeni ravni storitve).

69. Zavarovalnica in/ali pozavarovalnicaa bi morala v načrtih neprekinjenega poslovanja upoštevati različne scenarije, tudi skrajne, a verjetne, vključno s scenariji kibernetskega napada, in oceniti morebitni vpliv takih scenarijev. Na podlagi teh scenarijev bi morala opisati, kako se zagotavljata neprekinjenost delovanja sistemov in storitev IKT ter informacijska varnost v zavarovalnica in/ali pozavarovalnicaih.

Smernica 22 – Načrti odzivanja in obnovitve delovanja

70. Zavarovalnica in/ali pozavarovalnicaa bi morala na podlagi analize poslovnega učinka in verjetnih scenarijev pripraviti načrte odzivanja in obnovitve delovanja. V teh načrtih bi morali biti navedeni pogoji, pod katerimi se lahko zahteva aktivacija načrta, ter ukrepi, ki jih je treba sprejeti za zagotovitev celovitosti, razpoložljivosti, neprekinjenosti in obnovitve vsaj kritičnih sistemov in storitev IKT ter podatkov podjetij. Načrti odzivanja in obnovitve delovanja bi morali biti usmerjeni k doseganju ciljev glede obnovitve delovanja podjetij.

71. V načrtih odzivanja in obnovitve delovanja bi bilo treba preučiti možnosti kratko- in po potrebi dolgoročne obnovitve. Načrti bi morali biti najmanj:

    a) osredotočeni na obnovitev delovanja pomembnih storitev IKT, poslovnih funkcij, podpornih procesov, informacijskih sredstev in njihovih soodvisnosti, da se preprečijo škodljivi učinki na delovanje zavarovalnica in/ali pozavarovalnicaa;

    b) dokumentirani in dani na voljo poslovnim in podpornim enotam ter v nujnem primeru lahko dostopni, vključevati pa jasno opredelitev vlog in odgovornosti, ter

    c) nenehno posodabljani v skladu s spoznanji, pridobljenimi iz incidentov, preskusi, na novo opredeljenimi tveganji in grožnjami ter spremenjenimi cilji in prednostnimi nalogami glede obnovitve delovanja.

72. V načrtih bi se morale upoštevati tudi alternativne možnosti, kadar obnovitev delovanja morda kratkoročno ni izvedljiva zaradi stroškov, tveganj, logistike ali nepredvidenih okoliščin.

73. Zavarovalnica in/ali pozavarovalnicaa bi morala v okviru načrtov odzivanja in obnovitve delovanja upoštevati in izvajati ukrepe za neprekinjenost, da se ublaži izpad ponudnikov storitev, ki so ključne za neprekinjenost storitev IKT v zavarovalnica in/ali pozavarovalnicau (v skladu z določbami smernic organa EIOPA

o sistemu upravljanja in smernicami o oddajanju storitev v izvajanje zunanjim ponudnikom storitev v oblaku).

Smernica 23 – Preskušanje načrtov

74. Zavarovalnica in/ali pozavarovalnicaa bi morala preskusiti svoje načrte neprekinjenega poslovanja ter zagotoviti, da se delovanje njihovih kritičnih poslovnih procesov in dejavnosti, poslovnih funkcij, vlog in sredstev (npr. informacijskih sredstev) ter sredstev IKT in njihove soodvisnosti (vključno s tistimi, ki jih zagotovijo ponudniki storitev) redno preskušajo na podlagi profila tveganja zavarovalnica in/ali pozavarovalnicaa.

75. Načrti neprekinjenega poslovanja bi se morali redno posodabljati na podlagi rezultatov preskušanj, obveščevalnih podatkov o trenutnih grožnjah in spoznanj, pridobljenih iz predhodnih dogodkov. Vključiti bi bilo treba tudi vse pomembne spremembe ciljev glede obnovitve (vključno s ciljnim časom in ciljno točko obnovitve delovanja) ter/ali spremembe poslovnih procesov in dejavnosti, poslovnih funkcij, vlog in sredstev (npr. informacijskih sredstev in sredstev IKT).

76. Zavarovalnica in/ali pozavarovalnicaa bi morala s preskušanjem načrtov neprekinjenega poslovanja dokazati, da so sposobna vzdrževati uspešno poslovanje do ponovne vzpostavitve kritičnih operacij na vnaprej določeni ravni storitve ali odpornost na učinek incidentov.

77. Rezultate preskusov bi bilo treba dokumentirati, vsaka pomanjkljivost, opredeljena na podlagi preskusov, pa bi morala biti analizirana, odpravljena in o njej bi bilo treba poročati upravnemu, upravljalnemu ali nadzornemu organu.

Smernica 24 – Krizno komuniciranje

78. Zavarovalnica in/ali pozavarovalnicaa bi morala v primeru motenj ali v izrednih razmerah in med izvajanjem načrtov neprekinjenega poslovanja zagotoviti, da imajo vzpostavljene učinkovite ukrepe za krizno komuniciranje, tako da so vsi zadevni notranji in zunanji deležniki, vključno z zadevnimi nadzornimi organi, če to zahteva nacionalna ureditev, ter zadevni ponudniki storitev pravočasno in ustrezno obveščeni.

Smernica 25 – Oddajanje storitev in sistemov IKT v izvajanje zunanjim ponudnikom

79. Če se storitve in sistemi IKT oddajo v izvajanje zunanjim ponudnikom, bi morala zavarovalnica in/ali pozavarovalnicaa brez poseganja v smernice organa EIOPA o oddajanju storitev v izvajanje zunanjim ponudnikom storitev v oblaku zagotoviti, da so izpolnjene zadevne zahteve za te storitve.

80. Če so oddane v izvajanje zunanjim ponudnikom kritične ali pomembne funkcije, bi morala zavarovalnica in/ali pozavarovalnicaa zagotoviti, da pogodbene obveznosti ponudnika storitve (npr. pogodba, sporazumi o ravni storitve, določbe o prenehanju v zadevnih pogodbah) vključujejo vsaj:

    a) ustrezne in sorazmerne cilje in ukrepe informacijske varnosti, vključno z zahtevami, kot so minimalne zahteve glede informacijske varnosti, specifikacij življenjskega cikla podatkov podjetij, revizije in pravic dostopa ter zahteve glede lokacije podatkovnih centrov in šifriranja podatkov, omrežne varnosti in postopkov spremljanja varnosti;

b) sporazume o ravni storitev za zagotovitev neprekinjenosti storitev in sistemov IKT ter cilje glede učinkovitosti v običajnih okoliščinah in iz kriznega načrta v primeru prekinitve storitve, ter

c) postopke za obravnavanje operativnih in varnostnih incidentov, vključno s stopnjevanjem in poročanjem.

81. Zavarovalnica in/ali pozavarovalnicaa bi morala spremljati in zahtevati zagotovilo glede ravni skladnosti takih ponudnikov storitev z njihovimi varnostnimi cilji, ukrepi in cilji glede učinkovitosti.

Pravila glede upoštevanja in poročanja

82. Ta dokument vsebuje smernice, izdane v skladu s členom 16 Uredbe (EU) št. 1094/2010. V skladu s členom 16(3) navedene uredbe si morajo pristojni organi in zavarovalnica in/ali pozavarovalnicaa na vsak način prizadevati za upoštevanje smernic in priporočil.

83. Pristojni organi, ki upoštevajo ali nameravajo upoštevati te smernice, jih ustrezno vključijo v svoj regulativni ali nadzorni okvir.

84. Pristojni organi morajo organu EIOPU potrditi, ali upoštevajo oziroma ali nameravajo upoštevati te smernice, pri tem pa navesti razloge za neupoštevanje, in sicer v dveh mesecih po objavi prevedenih različic.

85. Če pristojni organi v tem roku ne bodo odgovorili, se bo štelo, da pravil glede poročanja ne upoštevajo, in se bo o njih tako tudi poročalo.

Končna določba glede pregleda

86. Za pregled teh smernic je pristojen organ EIOPA.