2024/1774

25.6.2024.

DELEGIRANA UREDBA KOMISIJE (EU) 2024/1774

od 13. ožujka 2024.

o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuju alati, metode, procesi i politike za upravljanje IKT rizicima te pojednostavnjeni okvir za upravljanje IKT rizicima

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 ([1]) te posebice njezin članak 15. četvrti podstavak i članak 16. stavak 3. četvrti podstavak,

budući da:

(1) Uredba (EU) 2022/2554 obuhvaća širok raspon financijskih subjekata koji se razlikuju po veličini, strukturi, unutarnjem ustrojstvu te prirodi i složenosti aktivnosti, zbog čega imaju veće ili manje elemente složenosti ili rizika. Kako bi se ta raznolikost uzela u obzir, svi zahtjevi povezani s politikama, postupcima, protokolima i alatima za sigurnost IKT-a te s pojednostavnjenim okvirom za upravljanje IKT rizicima trebali bi biti proporcionalni veličini, strukturi, unutarnjem ustrojstvu te prirodi i složenosti aktivnosti tih financijskih subjekata, kao i odgovarajućim rizicima.

(2) Financijski subjekti na koje se primjenjuje Uredba (EU) 2022/2554 iz istog bi razloga trebali imati određenu fleksibilnost pri usklađivanju sa zahtjevima povezanima s politikama, postupcima, protokolima i alatima za sigurnost IKT-a te s pojednostavnjenim okvirom za upravljanje IKT rizicima. Stoga bi se financijski subjekti trebali moći na temelju dokumentacije koju već imaju uskladiti sa zahtjevima o dokumentaciji koji proizlaze iz tih zahtjeva. Iz toga proizlazi da bi izrada, dokumentacija i provedba posebnih politika za sigurnost IKT-a trebala biti obvezna samo za određene ključne elemente, uzimajući u obzir, među ostalim, vodeće prakse i standarde u industriji. Nadalje, kako bi se obuhvatili posebni aspekti tehničke provedbe, potrebno je izraditi, dokumentirati i provesti postupke za sigurnost IKT-a kojima se obuhvaćaju posebni aspekti tehničke provedbe, među ostalim upravljanje kapacitetom i performansama, upravljanje ranjivostima i zakrpama, sigurnost podataka i sustava te evidencija.

(3) Kako bi se osigurala kontinuirana ispravna provedba politika, postupaka, protokola i alata za sigurnost IKT-a iz glave II. poglavlja I. ove Uredbe, važno je da financijski subjekti ispravno dodjeljuju i održavaju sve uloge i odgovornosti povezane sa sigurnosti IKT-a te da utvrde posljedice neusklađenosti s politikama ili postupcima sigurnosti IKT-a.

(4) Kako bi se ograničio rizik od sukoba interesa, financijski subjekti trebali bi razdvojiti dužnosti pri dodjeli uloga i odgovornosti u području IKT-a.

(5) Kako bi se osigurala fleksibilnost i pojednostavnio okvir za kontrolu financijskih subjekata, financijski subjekti ne bi trebali biti obvezni uvesti posebne odredbe o posljedicama neusklađenosti s politikama, postupcima i protokolima za sigurnost IKT-a iz glave II. poglavlja I. ove Uredbe ako su te odredbe već utvrđene u sklopu druge politike ili postupka.

([1]) SL L 333, 27.12.2022., str. 1., ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(6) U dinamičnom okruženju u kojem se IKT rizici neprestano mijenjaju važno je da financijski subjekti izrade svoj skup politika za sigurnost IKT-a na temelju vodećih praksi i, prema potrebi, standarda utvrđenih u članku 2. točki 1. Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća ([2]). Tako bi financijski subjekti iz glave II. ove Uredbe trebali ostati informirani i pripravni u promjenjivom okruženju.

(7) Kako bi se osigurala njihova digitalna operativna otpornost, financijski subjekti iz glave II. ove Uredbe trebali bi u sklopu svojih politika, postupaka, protokola i alata za sigurnost IKT-a izraditi i provesti politiku upravljanja IKT imovinom, postupke upravljanja kapacitetom i performansama te politike i postupke za operacije IKT-a. Te politike i postupci nužni su za praćenje stanja IKT imovine tijekom njezina životnog ciklusa kako bi se ta imovina učinkovito upotrebljavala i održavala (upravljanje IKT imovinom). Tim politikama i postupcima trebalo bi optimizirati rad IKT-a sustava te bi trebalo osigurati da performanse IKT sustava i kapaciteta ispunjavaju utvrđene ciljeve u području poslovanja i informacijske sigurnosti (upravljanje kapacitetom i performansama). Naposljetku, te politike i postupci trebali bi omogućiti djelotvorno i neometano upravljanje i rad IKT sustava (operacije IKT-a), čime se smanjuje rizik od gubitka povjerljivosti, cjelovitosti i dostupnosti podataka. Stoga su te politike i postupci nužni za sigurnost mreža i odgovarajuće mjere zaštite od neovlaštenih upada i zlouporabe podataka te očuvanje dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka.

(8) Za potrebe pravilnog upravljanja rizicima zastarjelih IKT sustava, financijski subjekti trebali bi evidentirati i pratiti datume isteka IKT usluga podrške treće strane. S obzirom na potencijalni učinak gubitka povjerljivosti, cjelovitosti i dostupnosti podataka, financijski subjekti trebali bi se pri evidentiranju i praćenju tih datuma isteka usredotočiti na IKT imovinu ili sustave koji su ključni za poslovanje.

(9) Dostupnost, vjerodostojnost, cjelovitost i povjerljivost podataka mogu se osigurati kriptografskim kontrolama. Stoga bi financijski subjekti iz glave II. ove Uredbe trebali utvrditi i provesti te kontrole primjenom pristupa koji se temelji na procjeni rizika. Financijski subjekti u tu bi svrhu trebali enkriptirati te podatke u mirovanju, upotrebi ili, prema potrebi, prijenosu na temelju rezultata dvostranog procesa, odnosno klasifikacije podataka i sveobuhvatne procjene IKT rizika. S obzirom na složenost enkripcije podataka u upotrebi, financijski subjekti iz glave II. ove Uredbe trebali bi enkriptirati datum u upotrebi samo ako je to primjereno na temelju rezultata procjene IKT rizika. Međutim, ako enkripcija podataka u upotrebi nije izvediva ili je presložena, financijski subjekti iz glave II. ove Uredbe trebali bi drugim mjerama za sigurnost IKT-a moći zajamčiti povjerljivost, cjelovitost i dostupnost tih podataka. Zbog brzog tehnološkog razvoja u području kriptografskih tehnika financijski subjekti iz glave II. ove Uredbe trebali bi pratiti relevantna zbivanja u području kriptoanalize te pratiti vodeće prakse i standarde. Stoga bi financijski subjekti iz glave II. ove Uredbe trebali primjenjivati fleksibilan pristup na temelju ublažavanja i praćenja rizika kako bi se nosili s dinamičnom prirodom kriptografskih prijetnji, među ostalim prijetnji koje proizlaze iz napretka u kvantnom računalstvu.

(10) Sigurnost operacija IKT-a te operativne politike, postupci, protokoli i alati iznimno su važni za povjerljivost, cjelovitost i dostupnost podataka. Iznimno je važno strogo odvajanje produkcijskih okruženja IKT-a od okruženja u kojima se IKT sustavi razvijaju i testiraju ili od drugih neprodukcijskih okruženja. To odvajanje trebalo bi biti važna mjera za sigurnost IKT-a kako bi se spriječio neželjeni i neovlašteni pristup podacima u produkcijskom okruženju, izmjena tih podataka i njihovo brisanje, što bi moglo dovesti do znatnih poremećaja u poslovanju financijskih subjekata iz glave II. ove Uredbe. Međutim, s obzirom na aktualne prakse u razvoju IKT sustava, financijski subjekti u izvanrednim bi okolnostima trebali moći provoditi testiranja u produkcijskim okruženjima, pod uvjetom da opravdaju to testiranje i dobiju potrebno odobrenje.

([2]) Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12., ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) Zbog brzog razvoja i ranjivosti u području IKT-a i kiberprijetnji, potreban je proaktivan i sveobuhvatan pristup utvrđivanju, procjeni i uklanjanju ranjivosti u području IKT-a. Financijski subjekti, njihovi klijenti, korisnici ili druge ugovorne strane bez takvog bi pristupa bili uvelike izloženi rizicima, što bi ugrozilo njihovu operativnu otpornost, sigurnost njihovih mreža te dostupnost, vjerodostojnost, cjelovitost i povjerljivost podataka koji bi se trebali zaštititi politikama za sigurnost IKT-a. Stoga bi financijski subjekti iz glave II. ove Uredbe trebali utvrditi i ukloniti ranjivosti u svojem okruženju IKT-a te bi se i financijski subjekti i njihove treće strane pružatelji IKT usluga trebali pridržavati usklađenog, transparentnog i odgovornog okvira za upravljanje ranjivostima. Iz istog razloga financijski subjekti trebali bi pratiti ranjivosti u području IKT-a pomoću pouzdanih resursa i automatiziranih alata kako bi potvrdili da treće strane pružatelji IKT usluga brzo djeluju u slučaju ranjivosti u IKT uslugama koje pružaju.

(12) Upravljanje zakrpama trebalo bi biti vrlo važan dio politika i postupaka za sigurnost IKT-a kojima se na temelju testiranja i uvođenja u kontroliranom okruženju nastoje ukloniti utvrđene ranjivosti i spriječiti poremećaji zbog instalacije zakrpa.

(13) Za potrebe pravodobnog i transparentnog informiranja o potencijalnim sigurnosnim prijetnjama koje bi mogle imati učinak na financijski subjekt i njegove dionike, financijski subjekti trebali bi uvesti postupke za odgovorno obavješćivanje klijenata, partnerskih financijskih subjekata i javnosti o IKT ranjivostima. Financijski bi subjekti pri uspostavi tih postupaka trebali uzeti u obzir, među ostalim, ozbiljnost ranjivosti, potencijalni učinak ranjivosti na dionike i spremnost popravka ili mjera za ublažavanje.

(14) Kako bi se korisnicima dodijelila prava pristupa, financijski subjekti iz glave II. ove Uredbe trebali bi uvesti stroge mjere za potvrdu jedinstvene identifikacije pojedinaca i sustava koji će pristupati podacima financijskog subjekta. U suprotnom bi financijski subjekti bili izloženi mogućem neovlaštenom pristupu, povredama podataka i prijevarnim radnjama, što bi ugrozilo povjerljivost, cjelovitost i dostupnost osjetljivih financijskih podataka. Upotrebu generičkih ili dijeljenih računa trebalo bi iznimno dopustiti u okolnostima koje utvrde financijski subjekti, ako se pobrinu da postoji odgovornost za radnje poduzete putem tih računa. Ako ne postoji ta zaštitna mjera, potencijalni zlonamjerni korisnici mogli bi otežati mjere istrage i korektivne mjere, zbog čega bi financijski subjekti bili izloženi neotkrivenim zlonamjernim radnjama ili kaznama zbog neusklađenosti.

(15) Kako bi upravljali brzim napretkom u okruženjima IKT-a, financijski subjekti iz glave II. ove Uredbe trebali bi provesti pouzdane politike i postupke za upravljanje IKT projektima te očuvanje dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka. Tim politikama i postupcima za upravljanje IKT projektima trebalo bi utvrditi elemente nužne za uspješno upravljanje IKT projektima, što uključuje promjene, preuzimanja, održavanje i razvoj IKT sustavâ financijskog subjekta, neovisno o metodologiji upravljanja projektima IKT-a koju financijski subjekt odabere. U kontekstu tih politika i postupaka financijski subjekti trebali bi uspostaviti prakse i metode testiranja koje odgovaraju njihovim potrebama, a pritom bi se trebali pridržavati postupka koji se temelji na procjeni rizika i očuvati sigurno, pouzdano i otporno okruženje IKT-a. Da bi provedba IKT projekta bila sigurna, financijski subjekti trebali bi se pobrinuti da osoblje iz određenih poslovnih sektora ili osoblje na radnim mjestima na koje utječe taj IKT projekt može dostaviti potrebne informacije i pružiti potrebno stručno znanje. Kako bi se proveo djelotvoran nadzor, upravljačkom tijelu trebalo bi dostavljati izvješća o IKT projektima, posebice o projektima koji imaju učinak na ključne ili važne funkcije i o rizicima povezanima s njima. Financijska tijela trebala bi učestalost i pojedinosti sustavnih i kontinuiranih preispitivanja i izvješća prilagoditi prema važnosti i opsegu tih IKT projekata.

(16) Važno je da se softverski paketi koje financijski subjekti iz glave II. ove Uredbe nabavljaju i razvijaju djelotvorno i sigurno integriraju u postojeće okruženje IKT-a, u skladu s utvrđenim ciljevima u području poslovanja i informacijske sigurnosti. Stoga bi financijski subjekti trebali detaljno evaluirati te softverske pakete. U tu svrhu i kako bi utvrdili ranjivosti i potencijalne sigurnosne nedostatke u softverskim paketima i širim IKT sustavima, financijski subjekti trebali bi provoditi testiranja sigurnosti IKT-a. Kako bi procijenili cjelovitost softvera i pobrinuli se da upotreba softvera ne predstavlja rizik za sigurnost IKT-a, financijski subjekti trebali bi preispitati i izvorni kod nabavljenog softvera, među ostalim, ako je izvedivo, zaštićenog softvera koji pružaju treće strane pružatelji IKT usluga, primjenom statičkih i dinamičkih metoda testiranja.

(17) Promjene, neovisno o njihovu opsegu, podrazumijevaju rizike i mogu predstavljati znatan rizik od gubitka povjerljivosti, cjelovitosti i dostupnosti podataka pa bi mogle dovesti do znatnih poremećaja u poslovanju. Kako bi se financijski subjekti zaštitili od potencijalnih ranjivosti i slabosti u području IKT-a zbog kojih bi mogli biti izloženi znatnim rizicima, nužan je strog postupak provjere kako bi se potvrdilo da sve promjene ispunjavaju potrebne zahtjeve za sigurnost IKT-a. Stoga bi financijski subjekti iz glave II. ove Uredbe trebali uspostaviti pouzdane politike i postupke upravljanja promjenama IKT-a kao ključan element svojih politika i postupaka za sigurnost IKT-a. Kako bi se očuvale objektivnost i djelotvornost procesa upravljanja promjenama IKT-a, spriječili sukobi interesa te osigurala objektivna evaluacija promjena IKT-a, važno je odvojiti funkcije odgovorne za odobrenje tih promjena od funkcija koje zahtijevaju i provode te promjene. Kako bi se postigli djelotvorni prelasci, kontrolirana provedba promjena IKT-a i najmanji mogući poremećaji u radu IKT sustava, financijski subjekti trebali bi dodijeliti jasne uloge i odgovornosti kojima se jamči da su promjene IKT-a planirane, da se primjereno testiraju i da se osigurava kvaliteta. Kako bi se zajamčio kontinuiran djelotvoran rad IKT sustavâ i sigurnosna mreža za financijske subjekte, financijski subjekti trebali bi također izraditi i provesti rezervne postupke. Trebali bi jasno utvrditi te rezervne postupke i dodijeliti odgovornosti radi brzog i djelotvornog odgovora u slučaju neuspješnih promjena IKT-a.

(18) Financijski subjekti iz glave II. ove Uredbe trebali bi uspostaviti politiku otkrivanja IKT incidenata koja obuhvaća sastavne dijelove procesa upravljanja IKT incidentima radi otkrivanja upravljanja i izvješćivanja o IKT incidentima. Financijski subjekti u tu bi svrhu trebali utvrditi sve relevantne kontakte unutar i izvan organizacije koji mogu olakšati pravilnu koordinaciju i provedbu različitih faza tog procesa. Kako bi se optimiziralo otkrivanje IKT incidenata i odgovor na njih te kako bi se utvrdili trendovi među tim incidentima, koji su vrijedan izvor informacija na temelju kojih financijski subjekti mogu djelotvorno utvrditi i ukloniti temeljne uzroke i probleme, financijski subjekti trebali bi posebno detaljno analizirati IKT incidente koje smatraju najznačajnijima, među ostalim zato što se redovito ponavljaju.

(19) Kako bi se rano i djelotvorno otkrile neobične aktivnosti, financijski subjekti iz glave II. ove Uredbe trebali bi prikupljati, pratiti i analizirati različite izvore informacije te dodijeliti povezane uloge i odgovornosti. Kad je riječ o unutarnjim izvorima informacija, evidencije su iznimno relevantan izvor, ali financijski subjekti ne bi se trebali oslanjati isključivo na evidencije. Umjesto toga, financijski subjekti trebali bi uzimati u obzir opširnije informacije kako bi obuhvatili izvješća drugih unutarnjih funkcija, koje su često vrijedan izvor relevantnih informacija. Financijski subjekti stoga bi trebali analizirati i pratiti informacije prikupljene iz vanjskih izvora, uključujući informacije koje dostavljaju treće strane pružatelji IKT usluga o incidentima koji utječu na njihove sustave, kao i druge izvore informacija koje financijski subjekti smatraju relevantnima. Pravo Unije o zaštiti podataka primjenjuje se ako su te informacije osobni podaci Osobne podatke trebalo bi ograničiti na ono što je nužno za otkrivanje incidenata.

(20) Kako bi se olakšalo otkrivanje IKT incidenata, financijski subjekti trebali bi čuvati dokaze o tim incidentima. Kako bi se, s jedne strane, ti dokazi čuvali dovoljno dugo i, s druge strane, smanjilo regulatorno opterećenje, financijski subjekti trebali bi odrediti razdoblje zadržavanja uzimajući u obzir, među ostalim, ključnost podataka i zahtjeve za zadržavanje koji proizlaze iz prava Unije.

(21) Kako bi se IKT incidenti otkrili na vrijeme, financijski subjekti iz glave II. ove Uredbe trebali bi smatrati da kriteriji utvrđeni za aktiviranje otkrivanja IKT incidenata i odgovora na njih nisu iscrpni. Nadalje, financijski subjekti trebali bi razmotriti svaki kriterij, ali za potrebe aktiviranja procesa otkrivanja i odgovora na IKT incidente i okolnosti opisane u kriteriju ne moraju se dogoditi istodobno i treba na primjeren način razmotriti važnost pogođenih IKT usluga.

(22) Financijski subjekti iz glave II. ove Uredbe trebali bi pri izradi politike kontinuiteta poslovanja u području IKT-a uzeti u obzir ključne sastavnice upravljanja IKT rizicima, što uključuje strategije upravljanja i informiranja o IKT incidentima, proces upravljanja promjenama IKT-a i rizike povezane s trećim stranama pružateljima IKT usluga.

(23) Važno je utvrditi skup scenarija koje bi financijski subjekti iz glave II. ove Uredbe trebali razmotriti pri provedbi planova odgovora i oporavka u području IKT-a te pri testiranju planova kontinuiteta poslovanja u području IKT-a. Ti bi scenariji financijskim subjektima trebali služiti kao početna točka u analizi relevantnosti i vjerojatnosti svakog scenarija te potrebe za izradom alternativnih scenarija. Financijski subjekti trebali bi se usredotočiti na scenarije u kojima bi ulaganje u mjere otpornosti bilo učinkovitije i djelotvornije. Financijske institucije trebale bi testiranjem prebacivanja s primarne IKT infrastrukture na redundantne kapacitete, sigurnosne kopije i redundantnu infrastrukturu procijeniti rade li ti kapaciteti, sigurnosne kopije i infrastruktura dovoljno dugo i djelotvorno i uvjeriti se da se uobičajen rad primarne IKT infrastrukture ponovno uspostavi u skladu s ciljevima oporavka.

(24) Potrebno je utvrditi zahtjeve za operativni rizik, konkretnije zahtjeve za upravljanje IKT projektima, promjenama IKT-a i kontinuitetom poslovanja u području IKT-a na temelju zahtjeva koji se već primjenjuju na središnje druge ugovorne strane, središnje depozitorije vrijednosnih papira i mjesta trgovanja u skladu s uredbama (EU) br. 648/2012 ([3]), (EU) br. 600/2014 ([4]) i (EU) br. 909/2014 ([5]) Europskog parlamenta i Vijeća.

(25) Člankom 6. stavkom 5. Uredbe (EU) 2022/2554 propisuje se da financijski subjekti preispituju svoj okvir za upravljanje IKT rizicima i izvješće o tom preispitivanju podnose nadležnom tijelu. Kako bi nadležna tijela mogla lako obraditi informacije u tim izvješćima i kako bi se te informacije odgovarajuće prenijele, financijski subjekti trebali bi ta izvješća dostavljati u pretraživom elektroničkom formatu.

(26) Zahtjevi za financijske subjekte na koje se primjenjuje pojednostavnjeni okvir za upravljanje IKT rizicima iz članka 16. Uredbe (EU) 2022/2554 trebali bi se odnositi na ključna područja i elemente koji su na temelju opsega, rizika, veličine i složenosti tih financijskih subjekata minimalno potrebni da bi podaci i usluge tih financijskih subjekata bili povjerljivi, cjeloviti, dostupni i vjerodostojni. Ti bi financijski subjekti u tom kontekstu trebali uspostaviti okvir za unutarnje upravljanje i kontrolu s jasnim odgovornostima kako bi se omogućio djelotvoran i pouzdan okvir za upravljanje rizicima. Nadalje, kako bi se smanjilo administrativno i operativno opterećenje, ti bi financijski subjekti trebali izraditi i dokumentirati samo jednu politiku, odnosno politiku informacijske sigurnosti, u kojoj se pobliže opisuju načela i pravila na visokoj razini koja su potrebna za zaštitu povjerljivosti, cjelovitosti, dostupnosti i vjerodostojnosti podataka i usluga tih financijskih subjekata.

(27) Odredbe ove Uredbe odnose se na okvir za upravljanje IKT rizicima: u njima se opisuju posebni elementi primjenjivi na financijske subjekte u skladu s člankom 15. Uredbe (EU) 2022/2554 i utvrđuje se pojednostavnjeni okvir za upravljanje rizicima za financijske subjekte iz članka 16. stavka 1. te uredbe. Kako bi se zajamčila usklađenost redovnog i pojednostavnjenog okvira za upravljanje IKT rizicima te s obzirom na to da bi te odredbe trebale početi primjenjivati istodobno, te je odredbe primjereno uključiti u isti zakonodavni akt.

(28) Ova Uredba temelji se na nacrtu regulatornih tehničkih standarda koji su Komisiji dostavili Europsko nadzorno tijelo za bankarstvo, Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje te Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala (europska nadzorna tijela) uz savjetovanje s Agencijom Europske unije za kibersigurnost (ENISA).

([3]) Uredba (EU) br. 648/2012 Europskog parlamenta i Vijeća od 4. srpnja 2012. o OTC izvedenicama, središnjoj drugoj ugovornoj strani i trgovinskom repozitoriju (SL L 201, 27.7.2012., str. 1., ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Uredba (EU) br. 600/2014 Europskog parlamenta i Vijeća od 15. svibnja 2014. o tržištima financijskih instrumenata i izmjeni Uredbe (EU) br. 648/2012 (SL L 173, 12.6.2014., str. 84., ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Uredba (EU) br. 909/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o poboljšanju namire vrijednosnih papira u Europskoj uniji i o središnjim depozitorijima vrijednosnih papira te izmjeni direktiva 98/26/EZ i 2014/65/EU te Uredbe (EU) br. 236/2012 (SL L 257, 28.8.2014., str. 1., ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Zajednički odbor europskih nadzornih tijela iz članka 54. Uredbe (EU) br. 1093/2010 Europskog parlamenta i Vijeća ([6]), članka 54. Uredbe (EU) br. 1094/2010 Europskog parlamenta i Vijeća ([7]) i članka 54. Uredbe (EU) br. 1095/2010 Europskog parlamenta i Vijeća ([8]) proveo je otvorena javna savjetovanja o nacrtu regulatornih tehničkih standarda na kojem se ova Uredba temelji, analizirao je potencijalne troškove i koristi predloženih standarda i zatražio je savjet Interesne skupine za bankarstvo osnovane u skladu s člankom 37. Uredbe (EU) br. 1093/2010, Interesne skupine za osiguranje i reosiguranje i Interesne skupine za strukovno mirovinsko osiguranje osnovane u skladu s člankom 37. Uredbe (EU) br. 1094/2010 te Interesne skupine za vrijednosne papire i tržišta kapitala osnovane u skladu s člankom 37. Uredbe (EU) br. 1095/2010.

(30) U mjeri u kojoj je obradu osobnih podataka potrebno uskladiti s obvezama utvrđenima u ovom aktu u potpunosti bi se trebale primjenjivati uredbe (EU) 2016/679 ([9]) i (EU) 2018/1725 ([10]) Europskog parlamenta i Vijeća. Na primjer, ako se radi odgovarajućeg otkrivanja incidenata prikupljaju osobni podaci, trebalo bi poštovati načelo smanjenja količine podataka. O nacrtu ovog akta zatražen je i savjet Europskog nadzornika za zaštitu podataka,

DONIJELA JE OVU UREDBU:

GLAVA I.

OPĆE NAČELO

Članak 1.

Ukupni profil rizičnosti i složenost

Pri izradi i provedbi politika, postupaka, protokola i alata za sigurnost IKT-a iz glave II. te pojednostavnjenog okvira za upravljanje IKT rizicima iz glave III. uzimaju se u obzir veličina i ukupni profil rizičnosti financijskog subjekta te priroda, opseg i elementi veće ili manje složenosti njegovih usluga, aktivnosti i poslovanja, među ostalom elementi povezani sa sljedećim:

(a) enkripcijom i kriptografijom;

(b) sigurnosti operacija IKT-a;

(c) mrežnom sigurnosti;

([6]) Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ (SL L 331, 15.12.2010., str. 12., ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Uredba (EU) br. 1094/2010 Europskog parlamenta i Vijeća od 24. studenog 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., ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Uredba (EU) br. 1095/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala), izmjeni Odluke br. 716/2009/EZ i stavljanju izvan snage Odluke Komisije 2009/77/EZ (SL L 331, 15.12.2010., str. 84., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(d) upravljanjem IKT projektima i promjenama IKT-a;

(e) potencijalnim učinkom IKT rizika na povjerljivost, cjelovitost i dostupnost podataka te potencijalnim učinkom poremećaja na kontinuitet i dostupnost aktivnosti financijskog subjekta.

GLAVA II.

DALJNJE USKLAĐIVANJE ALATA, METODA, PROCESA I POLITIKA ZA UPRAVLJANJE IKT RIZICIMA U SKLADU S ČLANKOM 15. UREDBE (EU) 2022/2554

POGLAVLJE I.

Politike, postupci, protokoli i alati za sigurnost IKT-a

Odjeljak 1.

Članak 2.

Opći elementi politika, postupaka, protokola i alata za sigurnost IKT-a

1. Financijski subjekti osiguravaju da su njihove politike za sigurnost IKT-a, politike informacijske sigurnosti te povezani postupci, protokoli i alati iz članka 9. stavka 2. Uredbe (EU) 2022/2554 ugrađeni u njihov okvir za upravljanje IKT rizicima. Financijski subjekti uspostavljaju politike, postupke, protokole i alate za sigurnost IKT-a utvrđene u ovom Poglavlju kojima se:

(a) osigurava sigurnost mreža;

(b) uspostavljaju mjere zaštite od neovlaštenih upada i zlouporabe podataka;

(c) čuvaju dostupnost, vjerodostojnost, cjelovitost i povjerljivost podataka, među ostalim pomoću kriptografskih tehnika;

(d) jamči točan i brz prijenos podataka bez znatnih poremećaja i nepotrebnih zastoja.

2. Financijski subjekti osiguravaju da politike za sigurnost IKT-a iz stavka 1.:

(a) budu usklađene s ciljevima financijskog subjekta u području informacijske sigurnosti koji su uključeni u strategiju za digitalnu operativnu otpornost iz članka 6. stavka 8. Uredbe (EU) 2022/2554;

(b) uključuju datum na koji je upravljačko tijelo službeno odobrilo politike za sigurnost IKT-a;

(c) sadržavaju pokazatelje i mjere za:

i. praćenje provedbe politika, postupaka, protokola i alata za sigurnost IKT-a;

ii. evidentiranje iznimaka od te provedbe;

iii. digitalnu operativnu otpornost financijskog subjekta u slučaju iznimki iz podtočke ii.;

(d) uključuju opis odgovornosti osoblja na svim razinama za sigurnost IKT-a financijskog subjekta;

(e) uključuju opis posljedica neusklađenosti osoblja financijskog subjekta s politikama za sigurnost IKT-a ako odredbe o tome nisu uključene u druge politike financijskog subjekta;

(f) uključuju popis dokumentacije koju je potrebno čuvati;

(g) uključuju opis aranžmana za razdvajanje dužnosti u kontekstu modela „tri crte obrane” ili drugog internog modela upravljanja rizicima i kontrole nad njima, prema potrebi, kako bi se izbjegli sukobi interesa;

(h) budu usklađene s vodećim praksama i, prema potrebi, standardima utvrđenima u članku 2. točki 1. Uredbe (EU) br. 1025/2012;

(i) uključuju opis uloga i odgovornosti za izradu, provedbu i održavanje politika, postupaka, protokola i alata za sigurnost IKT-a;

(j) budu preispitivane u skladu s člankom 6. stavkom 5. Uredbe (EU) 2022/2554;

(k) budu prilagođene bitnim promjenama koje se odnose na financijski subjekt, među ostalim bitnim promjenama aktivnosti ili procesa financijskog subjekta, prirode kiberprijetnji ili primjenjivih pravnih obveza.

Odjeljak 2.

Članak 3.

Upravljanje IKT rizicima

Financijski subjekti izrađuju, dokumentiraju i provode politike i postupke za upravljanje IKT rizicima koji sadržavaju sve sljedeće:

(a) navođenje odobrenja razine tolerancije na IKT rizik utvrđene u skladu s člankom 6. stavkom 8. točkom (b) Uredbe (EU) 2022/2554;

(b) postupak i metodologiju za provedbu procjene IKT rizika kojom se utvrđuju:

  i. ranjivosti i prijetnje koje utječu ili mogu utjecati na poslovne funkcije koje se podupiru, IKT sustave i IKT imovinu kojom se te funkcije podupiru;

  ii. kvantitativni ili kvalitativni pokazatelji za mjerenje učinka i vjerojatnosti pojave ranjivosti i prijetnji iz podtočke i.;

(c) postupak za utvrđivanje, provedbu i dokumentiranje mjera za postupanje s utvrđenim i procijenjenim IKT rizicima, što uključuje određivanje mjera za postupanje s IKT rizicima koje su nužne kako bi se IKT rizik smanjio na razinu tolerancije na rizik iz točke (a);

(d) za preostale IKT rizike koji i dalje postoje nakon provedbe mjera za postupanje s IKT rizicima iz točke (c):

  i. odredbe o utvrđivanju tih preostalih IKT rizika;

  ii. dodjelu uloga i odgovornosti u vezi s:

    1. prihvaćanjem preostalih IKT rizika koji prelaze razinu tolerancije financijskog subjekta na rizik iz točke (a);

    2. procesom preispitivanja iz podtočke iv. ove točke (d);

  iii. izradu popisa prihvaćenih preostalih IKT rizika uz obrazloženje prihvaćanja;

  iv. odredbe o preispitivanju prihvaćenih preostalih IKT rizika najmanje jedanput godišnje, uključujući:

    1. utvrđivanje svih promjena preostalih IKT rizika;

    2. procjenu dostupnih mjera za ublažavanje;

    3. procjenu toga jesu li razlozi za prihvaćanje preostalih IKT rizika i dalje valjani i primjenjivi na datum preispitivanja;

(e) odredbe o praćenju:

  i. svih promjena IKT rizika i prirode kiberprijetnji;

  ii. unutarnjih i vanjskih ranjivosti i prijetnji;

  iii. IKT rizika financijskog subjekta kojim se omogućuje brzo otkrivanje promjena koje bi mogle utjecati na njegov profil IKT rizičnosti;

(f) odredbe o procesu kojim se osigurava da se uzimaju u obzir sve promjene poslovne strategije i strategije za digitalnu operativnu otpornost financijskog subjekta.

Za potrebe prvog stavka točke (c) postupkom iz te točke osigurava se:

(a) praćenje djelotvornosti provedenih mjera za postupanje s IKT rizicima;

(b) procjena toga jesu li postignute utvrđene razine tolerancije financijskog subjekta na rizik;

(c) procjena toga je li financijski subjekt prema potrebi poduzeo mjere za ispravak ili poboljšanje tih mjera.

Odjeljak 3.

Upravljanje IKT imovinom

Članak 4.

Politika upravljanja IKT imovinom

1. Financijski subjekti u sklopu politika, postupaka, protokola i alata za sigurnost IKT-a iz članka 9. stavka 2. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode politiku upravljanja IKT imovinom.

2. Politikom upravljanja IKT imovinom iz stavka 1.:

(a) predviđa se praćenje i upravljanje životnim ciklusom IKT imovine utvrđene i klasificirane u skladu s člankom 8. stavkom 1. Uredbe (EU) 2022/2554;

(b) predviđa se da financijski subjekt vodi evidenciju o svemu sljedećem:

i. jedinstvenom identifikatoru sve IKT imovine;

ii. informacijama o fizičkoj ili logičkoj lokaciji sve IKT imovine;

iii. klasifikaciji sve IKT imovine u skladu s člankom 8. stavkom 1. Uredbe (EU) 2022/2254;

iv. identitetu vlasnika IKT imovine;

v. poslovnim funkcijama ili uslugama koje se podupiru IKT imovinom;

vi. zahtjevima za kontinuitet poslovanja u području IKT-a, među ostalim ciljnom vremenu oporavka i ciljnoj točki oporavka;

vii. izloženosti ili mogućoj izloženosti IKT imovine vanjskim mrežama, među ostalim internetu;

viii. vezama i međuovisnostima među IKT imovinom i poslovnim funkcijama za koje se upotrebljava sva IKT imovina;

ix. prema potrebi, za svu IKT imovinu, datumima isteka redovnih, proširenih i prilagođenih usluga podrške trećih strana pružatelja IKT usluga nakon kojih dobavljač ili treća strana pružatelj IKT usluga više ne pruža podršku za tu IKT imovinu;

(c) predviđa se da financijski subjekti koji nisu mikropoduzeća vode evidenciju o informacijama potrebnima za provedbu posebne procjene IKT rizika za sve zastarjele IKT sustave iz članka 8. stavka 7. Uredbe (EU) 2022/2554.

Članak 5.

Postupak upravljanja IKT imovinom

1. Financijski subjekti izrađuju, dokumentiraju i provode postupak za upravljanje IKT imovinom.

2. Postupkom za upravljanje IKT imovinom iz stavka 1. utvrđuju se kriteriji za provedbu procjene ključnosti informacijske imovine i IKT imovine kojom se podupiru poslovne funkcije. U toj se procjeni uzimaju u obzir:

(a) IKT rizik povezan s tim poslovnim funkcijama i njihova ovisnost o informacijskoj imovini ili IKT imovini;

(b) utjecaj mogućeg gubitka povjerljivosti, cjelovitosti i dostupnosti te informacijske imovine i IKT imovine na poslovne procese i aktivnosti financijskih subjekata.

Odjeljak 4.

Enkripcija i kriptografija

Članak 6.

Enkripcija i kriptografske kontrole

1. Financijski subjekti u sklopu svojih politika, postupaka, protokola i alata za sigurnost IKT-a iz članka 9. stavka 2. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode politiku enkripcije i kriptografskih kontrola.

2. Financijski subjekti osmišljavaju politiku enkripcije i kriptografskih kontrola iz stavka 1. na temelju rezultata odobrene klasifikacije podataka i procjene IKT rizika. Ta politika sadržava pravila o svemu sljedećem:

(a) enkripciji podataka u mirovanju i prijenosu;

(b) enkripciji podataka u upotrebi, prema potrebi;

(c) enkripciji unutarnjih mrežnih veza i prometa s vanjskim stranama;

(d) upravljanju kriptografskim ključevima iz članka 7., kojim se utvrđuju pravila o ispravnoj upotrebi, zaštiti i životnom ciklusu kriptografskih ključeva.

Za potrebe točke (b) ako nije moguća enkripcija podataka u upotrebi, financijski subjekti ih obrađuju u odvojenom i zaštićenom okruženju ili poduzimaju jednakovrijedne mjere kako bi osigurali njihovu povjerljivost, cjelovitost, vjerodostojnost i dostupnost.

3. Financijski subjekti u politiku enkripcije i kriptografskih kontrola iz stavka 1. uključuju kriterije za odabir kriptografskih tehnika i praksi upotrebe, pri čemu uzimaju u obzir vodeće prakse i standarde u skladu s člankom 2. točkom 1. Uredbe (EU) br. 1025/2012 te klasifikaciju relevantne IKT imovine utvrđenu u skladu s člankom 8. stavkom 1. Uredbe (EU) 2022/2554. Financijski subjekti koji se ne mogu pridržavati vodećih praksi ili standarda ili ne mogu primjenjivati najpouzdanije tehnike donose mjere za ublažavanje i praćenje radi otpornosti na kiberprijetnje.

4. Financijski subjekti u politiku enkripcije i kriptografskih kontrola iz stavka 1. uključuju odredbe o ažuriranju ili promjeni, prema potrebi, kriptografske tehnologije na temelju napretka u području kriptoanalize. Zahvaljujući tim ažuriranjima ili promjenama kriptografska tehnologija ostaje otporna na kiberprijetnje u skladu s člankom 10. stavkom 2. točkom (a). Financijski subjekti koji ne mogu ažurirati ili promijeniti kriptografsku tehnologiju donose mjere za ublažavanje i praćenje radi otpornosti na kiberprijetnje.

5. Financijski subjekti u politiku enkripcije i kriptografskih kontrola iz stavka 1. uključuju zahtjev za evidentiranje donošenja mjera za ublažavanje i praćenje koje se donose u skladu sa stavcima 3. i 4. i za obrazloženo objašnjenje njihova donošenja.

Članak 7.

Upravljanje kriptografskim ključevima

1. Financijski subjekti u politiku upravljanja kriptografskim ključevima iz članka 6. stavka 2. točke (d) uključuju zahtjeve za upravljanje kriptografskim ključevima tijekom njihova cijelog životnog ciklusa, što uključuje njihovo generiranje, obnovu, pohranu, sigurnosno kopiranje, arhiviranje, dohvaćanje, prijenos, povlačenje, opoziv i uništenje.

2. Financijski subjekti utvrđuju i provode kontrole za zaštitu kriptografskih ključeva od gubitka, neovlaštenog pristupa, otkrivanja i izmjene tijekom njihova cijelog životnog ciklusa. Te kontrole osmišljavaju na temelju rezultata odobrene klasifikacije podataka i procjene IKT rizika.

3. Financijski subjekti izrađuju i provode metode za zamjenu kriptografskih ključeva u slučaju njihova gubitka, ugroženosti ili oštećenosti.

4. Financijski subjekti uspostavljaju i održavaju registar svih certifikata i uređaja na kojima su certifikati pohranjeni barem za IKT imovinu kojom se podupiru ključne ili važne funkcije. Taj registar ažuriraju.

5. Financijski subjekti trebaju se pobrinuti da se istekli certifikati brzo obnove.

Odjeljak 5.

Sigurnost operacija IKT-a

Članak 8.

Politike i postupci za operacije IKT-a

1. Financijski subjekti u sklopu politika, postupaka, protokola i alata za sigurnost IKT-a iz članka 9. stavka 2. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode politike i postupke za upravljanje operacijama IKT-a. Tim se politikama i postupcima utvrđuje kako financijski subjekti upotrebljavaju, prate, kontroliraju i obnavljaju svoju IKT imovinu, što uključuje dokumentiranje operacija IKT-a.

2. Politike i postupci za operacije IKT-a iz stavka 1. sadržavaju sve sljedeće:

(a) opis IKT imovine, koji uključuje sve sljedeće:

   i. zahtjeve povezane sa sigurnom instalacijom, održavanjem, konfiguracijom i deinstalacijom IKT sustava;

   ii. zahtjeve za upravljanje informacijskom imovinom koja se upotrebljava za IKT imovinu, među ostalim njezinu automatiziranu i ručnu obradu i upotrebu;

   iii. zahtjeve za utvrđivanje i kontrolu zastarjelih IKT sustava;

(b) kontrole i praćenje IKT sustava, što uključuje sve sljedeće:

   i. zahtjeve za sigurnosno kopiranje i ponovnu uspostavu IKT sustavâ;

   ii. zahtjeve za izradu rasporeda, pri čemu se uzimaju u obzir međuovisnosti među IKT sustavima;

   iii. protokole za revizijski postupak i podatke u evidenciji sustava;

   iv. zahtjeve da se unutarnjim revizijama i drugim testiranjima smanje mogući poremećaji u poslovanju;

   v. zahtjeve za odvajanje produkcijskih okruženja IKT-a od okruženja u kojima se IKT sustavi razvijaju i testiraju te od drugih neprodukcijskih okruženja;

   vi. zahtjeve za razvoj i testiranje u okruženjima odvojenima od produkcijskog okruženja;

   vii. zahtjeve za razvoj i testiranje u produkcijskim okruženjima;

(c) postupanje s greškama u IKT sustavima, što uključuje sve sljedeće:

i. postupke i protokole za postupanje s greškama;

ii. kontakte za podršku i eskalaciju, među ostalim vanjske kontakte za podršku u slučaju neočekivanih operativnih ili tehničkih problema;

iii. postupke za ponovno pokretanje, vraćanje na prethodnu verziju i oporavak IKT sustava u slučaju poremećaja u IKT sustavu.

Za potrebe točke (b) podtočke v. odvajanje se odnosi na sve sastavne dijelove okruženja, među ostalim račune, podatke ili veze u skladu s člankom 13. prvim stavkom točkom (a).

Za potrebe točke (b) podtočke vii. politikama i postupcima iz stavka 1. predviđa se da su slučajevi u kojima se testiranje provodi u produkcijskom okruženju jasno utvrđeni, obrazloženi i vremenski ograničeni te da ih je odobrila relevantna funkcija u skladu s člankom 16. stavkom 6. Financijski subjekti osiguravaju dostupnost, povjerljivost, cjelovitost i vjerodostojnost IKT sustavâ i produkcijskih podataka tijekom aktivnosti razvoja i testiranja u produkcijskom okruženju.

Članak 9.

Upravljanje kapacitetom i performansama

1. Financijski subjekti u sklopu politika, postupaka, protokola i alata za sigurnost IKT-a iz članka 9. stavka 2. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode postupke za upravljanje kapacitetom i performansama za sljedeće:

(a) utvrđivanje zahtjeva za kapacitet svojih IKT sustava;

(b) primjenu optimizacije resursa;

(c) postupke praćenja za održavanje i unaprjeđenje:

i. dostupnosti podataka i IKT sustavâ;

ii. učinkovitosti IKT sustavâ;

iii. sprječavanja manjka kapaciteta IKT-a.

2. Postupcima upravljanja kapacitetom i performansama iz stavka 1. osigurava se da financijski subjekti poduzimaju mjere koje su primjerene specifičnostima IKT sustavâ s dugim ili složenim procesima nabave ili odobrenja ili IKT sustava za koje je potrebno mnogo resursa.

Članak 10.

Upravljanje ranjivostima i zakrpama

1. Financijski subjekti u sklopu politika, postupaka, protokola i alata za sigurnost IKT-a iz članka 9. stavka 2. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode postupke upravljanja ranjivostima.

2. Postupcima upravljanja ranjivostima iz stavka 1.:

(a) utvrđuju se i ažuriraju relevantni i pouzdani izvori informacija za povećanje i održavanje razine informiranosti o ranjivostima;

(b) osiguravaju se performanse automatiziranog skeniranja i procjena ranjivosti IKT imovine, pri čemu su učestalost i opseg tih aktivnosti razmjerni klasifikaciji utvrđenoj u skladu s člankom 8. stavkom 1. Uredbe (EU) 2022/2554 i ukupnom profilu rizičnosti IKT imovine;

(c) provjerava se sljedeće:

i. obrađuju li treće strane pružatelji IKT usluga ranjivosti povezane s IKT uslugama koje pružaju financijskom subjektu;

ii. izvješćuju li pravodobno ti pružatelji usluga financijski subjekt barem o ključnim ranjivostima te statističkim podacima i trendovima;

(d) prati upotreba sljedećeg:

i. knjižnica treće strane, među ostalim knjižnica otvorenog koda, koje se upotrebljavaju za IKT usluge kojima se podupiru ključne ili važne funkcije;

ii. IKT usluga koje je financijski subjekt sam razvio ili koje je treća strana pružatelj IKT usluga posebno prilagodio ili razvio za financijski subjekt;

(e) utvrđuju se postupci za odgovorno obavješćivanje klijenata, partnerskih financijskih subjekata i javnosti o ranjivostima;

(f) daje se prioritet uvođenju zakrpi i drugim mjerama za ublažavanje kako bi se uklonile utvrđene ranjivosti;

(g) prati se i provjerava uklanjanje ranjivosti;

(h) zahtijeva se evidentiranje svih otkrivenih ranjivosti koje utječu na IKT sustave i praćenje njihova saniranja.

Za potrebe točke (b) financijski subjekti barem jednom tjedno provode automatizirano skeniranje i procjenu ranjivosti IKT imovine za IKT imovinu kojom se podupiru ključne ili važne funkcije.

Za potrebe točke (c) financijski subjekti zahtijevaju da treće strane pružatelji IKT usluga istražuju relevantne ranjivosti, utvrđuju njihove temeljne uzroke i poduzimanju odgovarajuće mjere za ublažavanje.

Za potrebe točke (d) financijski subjekti, prema potrebi u suradnji s trećom stranom pružateljem IKT usluga, prate verziju i moguća ažuriranja knjižnica treće strane. U slučaju gotove (spremna za upotrebu) IKT imovine koja je nabavljena i upotrebljava se za rad IKT usluga kojima se ne podupiru ključne ili važne funkcije ili sastavnih dijelova te IKT imovine, financijski subjekti u najvećoj mogućoj mjeri prate upotrebu knjižnica treće strane, među ostalim knjižnica otvorenog koda.

Za potrebe točke (f) financijski subjekti uzimaju u obzir ključnost ranjivosti, klasifikaciju utvrđenu u skladu s člankom 8. stavkom 1. Uredbe (EU) 2022/2554 i profil rizičnosti IKT imovine na koju utječu utvrđene ranjivosti.

3. Financijski subjekti u sklopu politika, postupaka, protokola i alata za sigurnost IKT-a iz članka 9. stavka 2. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode postupke upravljanja zakrpama.

4. Postupcima upravljanja zakrpama iz stavka 3.:

(a) u najvećoj mogućoj mjeri utvrđuju se i procjenjuju dostupne zakrpe i ažuriranja softvera i hardvera s pomoću automatskih alata;

(b) utvrđuju se hitni postupci za krpanje i ažuriranje IKT imovine;

(c) testiraju se i uvode zakrpe i ažuriranja softvera i hardvera iz članka 8. stavka 2. točke (b) podtočaka v., vi. i vii.;

(d) utvrđuju se rokovi za instalaciju zakrpa i ažuriranja softvera i hardvera te postupci eskalacije ako se ti rokovi ne mogu ispuniti.

Članak 11.

Sigurnost podataka i sustava

1. Financijski subjekti u sklopu politika, postupaka, protokola i alata za sigurnost IKT-a iz članka 9. stavka 2. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode postupak za sigurnost podataka i sustava.

2. Postupak za sigurnost podataka i sustava iz stavka 1. sadržava sve sljedeće elemente povezane sa sigurnosti podataka i IKT sustavâ u skladu s klasifikacijom iz članka 8. stavka 1. Uredbe (EU) 2022/2554:

(a) ograničenja pristupa iz članka 21. ove Uredbe, kojima se podupiru zahtjevi za zaštitu za svaku razinu klasifikacije;

(b) utvrđivanje polazne sigurne konfiguracije za IKT imovinu kojom se izloženost te IKT imovine kiberprijetnjama svodi na najmanju moguću mjeru i mjera za redovitu provjeru toga jesu li te polazne konfiguracije djelotvorno provedene;

(c) utvrđivanje sigurnosnih mjera kako bi se osiguralo da se u IKT sustave i na krajnje uređaje instalira samo ovlašteni softver;

(d) utvrđivanje sigurnosnih mjera protiv zlonamjernih kodova;

(e) utvrđivanje sigurnosnih mjera kako bi se osiguralo da se za prijenos i pohranu podataka financijskog subjekta upotrebljavaju samo ovlašteni mediji za pohranu podataka, sustavi i krajnji uređaji;

(f) sljedeće zahtjeve za sigurnu upotrebu prijenosnih krajnjih uređaja i privatnih neprijenosnih krajnjih uređaja:

   i. zahtjev za upotrebu rješenja za upravljanje za daljinsko upravljanje krajnjim uređajima i daljinsko brisanje podataka financijskog subjekta;

   ii. zahtjev za upotrebu sigurnosnih mehanizama koje članovi osoblja ili treće strane pružatelji IKT usluga ne mogu na neovlašteni način promijeniti, ukloniti ili premostiti;

   iii. zahtjev za upotrebu prijenosnih uređaja za pohranu podataka samo ako unutar razine tolerancije financijskog subjekta na rizik postoji preostali IKT rizik iz članka 3. prvog stavka točke (a);

(g) proces za sigurno brisanje podataka koji se nalaze u prostorima financijskog subjekta ili su vanjski pohranjeni, a koje financijski subjekt više ne treba prikupljati ili pohranjivati;

(h) proces za sigurno odlaganje ili stavljanje izvan funkcije uređaja za pohranu podataka koji se nalaze u prostorima financijskog subjekta ili su vanjski pohranjeni, a koji sadržavaju povjerljive informacije;

(i) utvrđivanje i provedbu sigurnosnih mjera za sprječavanje gubitka i curenja podataka za sustave i krajnje uređaje;

(j) provedbu sigurnosnih mjera kako rad na daljinu i upotreba privatnih krajnjih uređaja ne bi negativno utjecali na sigurnost IKT-a financijskog subjekta;

(k) za IKT imovinu ili usluge kojima upravlja treća strana pružatelj IKT usluga, utvrđivanje i provedbu zahtjeva za održavanje digitalne operativne otpornosti u skladu s rezultatima klasifikacije podataka i procjene IKT rizika.

Za potrebe točke (b) za polaznu sigurnu konfiguraciju iz te točke uzimaju se u obzir vodeće prakse i primjerene tehnike utvrđene u standardima iz članka 2. točke 1. Uredbe (EU) br. 1025/2012.

Za potrebe točke (k) financijski subjekti razmatraju sljedeće:

(a) primjenu postavki koje preporučuje dobavljač na elementima kojima upravlja financijski subjekt;

(b) jasnu raspodjelu uloga i odgovornosti za informacijsku sigurnost između financijskog subjekta i treće strane pružatelja IKT usluga u skladu s načelom potpune odgovornosti financijskog subjekta za treću stranu pružatelja IKT usluga iz članka 28. stavka 1. točke (a) Uredbe (EU) 2022/2554 i za financijske subjekte iz članka 28. stavka 2. te uredbe i u skladu s politikom financijskog subjekta o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije;

(c) nužnost pružanja i održavanja odgovarajućih kompetencija unutar financijskog subjekta za upravljanje uslugom koja se upotrebljava i njezinu sigurnost;

(d) tehničke i organizacijske mjere za smanjenje rizika povezanih s infrastrukturom koju treća strana pružatelj IKT usluga upotrebljava za svoje IKT usluge, uzimajući u obzir vodeće prakse i standarde utvrđene u članku 2. točki 1. Uredbe (EU) br. 1025/2012.

Članak 12.

Evidentiranje

1. Financijski subjekti u sklopu mjera zaštite od neovlaštenih upada i zlouporabe podataka izrađuju, dokumentiraju i provode postupke, protokole i alate za evidentiranje.

2. Postupci, protokoli i alati za evidentiranje iz stavka 1. sadržavaju sve sljedeće:

(a) utvrđivanje događaja koji se evidentiraju, razdoblja čuvanja evidencije te mjere za zaštitu i obradu podataka iz evidencije, pri čemu se uzima u obzir svrha za vođenje evidencije;

(b) usklađivanje razine detaljnosti evidencije s njezinom svrhom i upotrebom za potrebe djelotvornog otkrivanja neobičnih aktivnosti kako je navedeno u članku 24.;

(c) zahtjeve za evidentiranje događaja koji se odnose na sve sljedeće:

i. kontrolu logičkog i fizičkog pristupa, kako je navedeno u članku 21., i upravljanje identitetom;

ii. upravljanje kapacitetom;

iii. upravljanje promjenama;

iv. operacije IKT-a, što uključuje aktivnosti u IKT sustavu;

v. aktivnosti mrežnog prometa, što uključuje performanse IKT mreže;

(d) mjere za zaštitu sustavâ za evidentiranje i podataka u evidenciji od neovlaštenog mijenjanja, brisanja i neovlaštenog pristupa u mirovanju, prijenosu ili, prema potrebi, upotrebi;

(e) mjere za otkrivanje prekida sustavâ za evidenciju;

(f) ne dovodeći u obzir primjenjive regulatorne zahtjeve iz prava Unije ili nacionalnog prava, sinkronizaciju satova svakog IKT sustava financijskog subjekta s dokumentiranim pouzdanim referentnim izvorom vremena.

Za potrebe točke (a) financijski subjekti utvrđuju razdoblje čuvanja, pri čemu uzimaju u obzir ciljeve u području poslovanja i informacijske sigurnosti, razlog evidentiranja događaja u evidenciji i rezultate procjene IKT rizika.

Odjeljak 6.

Mrežna sigurnost

Članak 13.

Upravljanje mrežnom sigurnosti

Financijski subjekti u sklopu mjera zaštite mreža od neovlaštenih upada i zlouporabe podataka izrađuju, dokumentiraju i provode politike, postupke, protokole i alate za upravljanje mrežnom sigurnosti, što uključuje sve sljedeće:

(a) razdvajanje i segmentaciju IKT sustavâ i mreža, pri čemu se uzimaju u obzir:

i. ključnost ili važnost funkcije koja se podupire IKT sustavima i mrežama;

ii. klasifikacija utvrđena u skladu s člankom 8. stavkom 1. Uredbe (EU) 2022/2554;

iii. ukupni profil rizičnosti IKT imovine za koju se ti IKT sustavi i mreže upotrebljavaju;

(b) dokumentiranje svih mrežnih veza i tokova podataka financijskog subjekta;

(c) upotrebu zasebne namjenske mreže za upravljanje IKT imovinom;

(d) utvrđivanje i provedbu kontrole pristupa mreži kako bi se spriječilo i otkrilo povezivanje neovlaštenih uređaja ili sustava na mrežu financijskog sustava ili krajnje točke koje ne ispunjavaju zahtjeve financijskog subjekta za sigurnost;

(e) enkripciju mrežnih veza koje prolaze kroz korporativne mreže, javne mreže, domaće mreže, mreže treće strane i bežične mreže u pogledu komunikacijskih protokola koji se upotrebljavaju, pri čemu se uzimaju u obzir rezultati odobrene klasifikacije podataka, rezultati procjene IKT rizika i enkripcija mrežnih veza iz članka 6. stavka 2.;

(f) oblikovanje mreža u skladu sa zahtjevima za sigurnost IKT-a koje utvrdi financijski subjekt, pri čemu se uzimaju u obzir vodeće prakse kako bi se osigurala povjerljivost, cjelovitost i dostupnost mreže;

(g) zaštitu mrežnog prometa između unutarnjih mreža i interneta te drugih vanjskih veza;

(h) utvrđivanje uloga i odgovornosti te koraka za određivanje, provedbu, odobrenje, promjenu i preispitivanje pravila za vatrozid i filtara veza;

(i) provedbu preispitivanja mrežne strukture i oblikovanja mrežne sigurnosti jedanput godišnje, a periodički za mikropoduzeća, kako bi se utvrdile potencijalne ranjivosti;

(j) mjere za privremenu izolaciju, prema potrebi, podmreža te mrežnih komponenata i uređaja;

(k) provedbu polazne sigurne konfiguracije svih mrežnih komponenata te povećanje sigurnosti mreže i mrežnih uređaja u skladu s uputama dobavljača te, prema potrebi, primjenjivim standardima kako su definirani u članku 2. točki 1. Uredbe (EU) br. 1025/2012 i vodećim praksama;

(l) postupke za ograničavanje, zaključavanje i prekid rada sustava i daljinskih sesija nakon određenog razdoblja neaktivnosti;

(m) za ugovore o mrežnim uslugama:

i. utvrđivanje i specifikaciju mjera za sigurnost IKT-a i informacijsku sigurnost, razina usluge i zahtjeva za upravljanje za sve mrežne usluge;

ii. pruža li te usluge pružatelj IKT usluga unutar grupe ili treća strana pružatelj IKT usluga.

Za potrebe točke (h) financijski subjekti redovito provode preispitivanje pravila za vatrozid i filtara veza u skladu s klasifikacijom iz članka 8. stavka 1. Uredbe (EU) 2022/2554 i ukupnim profilnom rizičnosti uključenih IKT sustava. Za IKT sustave kojima se podupiru ključne ili važne funkcije, financijski subjekti barem svakih šest mjeseci provjeravaju primjerenost postojećih pravila za vatrozid i filtara veza.

Članak 14.

Zaštita podataka u prijenosu

1. Financijski subjekti u sklopu zaštitnih mjera za očuvanje dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka izrađuju, dokumentiraju i provode politike, postupke, protokole i alate za zaštitu podataka u prijenosu. Financijski subjekti posebice osiguravaju sve navedeno:

(a) dostupnost, vjerodostojnost, cjelovitost i povjerljivost podataka tijekom mrežnog prijenosa te uspostavu postupaka za procjenu usklađenosti s tim zahtjevima;

(b) sprječavanje i otkrivanje curenja podataka te siguran prijenos podataka između financijskog subjekta i vanjskih strana;

(c) provedbu, dokumentiranje i redovito preispitivanje zahtjevâ za povjerljivost ili ugovorâ o povjerljivosti podataka koji odražavaju potrebe financijskog subjekta za zaštitu podataka, što obuhvaća i osoblje financijskog subjekta i treće strane.

2. Financijski subjekti osmišljavaju politike, postupke, protokole i alate za zaštitu podataka u prijenosu iz stavka 1. na temelju rezultata odobrene klasifikacije podataka i procjene IKT rizika.

Odjeljak 7.

Upravljanje IKT projektima i promjenama IKT-a

Članak 15.

Upravljanje IKT projektima

1. Financijski subjekti u sklopu zaštitnih mjera za očuvanje dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka izrađuju, dokumentiraju i provode politiku upravljanja IKT projektima.

2. Politikom upravljanja IKT projektima iz stavka 1. utvrđuju se elementi za djelotvorno upravljanje IKT projektima povezanima s nabavom, održavanjem i, prema potrebi, razvojem IKT sustavâ financijskog subjekta.

3. Politika upravljanja IKT projektima iz stavka 1. sadržava sve sljedeće:

(a) ciljeve IKT projekta;

(b) vođenje IKT projekta, uključujući uloge i odgovornosti;

(c) planiranje, rokove i korake IKT projekta;

(d) procjenu rizika IKT projekta;

(e) relevantne ključne etape;

(f) zahtjeve za upravljanje promjenama;

(g) testiranje svih zahtjeva, među ostalim zahtjeva za sigurnost, i odgovarajući proces odobrenja pri uvođenju IKT sustava u produkcijsko okruženje.

4. Politikom upravljanja IKT projektima iz stavka 1. predviđa se sigurna provedba IKT projekta na temelju potrebnih informacija i stručnog znanja iz poslovnog područja ili funkcija na koje utječe taj IKT projekt.

5. U skladu s procjenom IKT rizika iz stavka 3. točke (d), politikom upravljanja IKT projektima iz stavka 1. predviđa se da se upravljačko tijelo izvješćuje o uspostavi i napretku IKT projekata koji utječu na ključne ili važne funkcije financijskog subjekta i njihovim povezanim rizicima na sljedeći način:

(a) pojedinačno ili skupno, ovisno o važnosti i opsegu IKT projekata;

(b) periodički i, prema potrebi, u slučaju važnih događaja.

Članak 16.

Nabava, razvoj i održavanja IKT sustavâ

1. Financijski subjekti u sklopu zaštitnih mjera za očuvanje dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka izrađuju, dokumentiraju i provode politiku o nabavi, razvoju i održavanju IKT sustava. Tom se politikom:

(a) utvrđuju sigurnosne prakse i metodologije povezane s nabavom, razvojem i održavanjem IKT sustavâ;

(b) zahtijeva utvrđivanje:

i. tehničkih specifikacija i tehničkih specifikacija IKT-a, kako je definirano u članku 2. točkama 4. i 5. Uredbe (EU) br. 1025/2012;

ii. zahtjeva za nabavu, razvoj i održavanje IKT sustavâ uz poseban fokus na zahtjeve za sigurnost IKT-a i njihovo odobrenje koje daju relevantna poslovna funkcija i vlasnik IKT imovine u skladu s aranžmanima za unutarnje upravljanje financijskog subjekta;

(c) utvrđuju mjere za smanjenje rizika od nenamjerne izmjene IKT sustavâ ili njihove namjerne manipulacije tijekom razvoja, održavanja i uvođenja tih IKT sustava u produkcijsko okruženje.

2. Financijski subjekti izrađuju, dokumentiraju i provode postupak za nabavu, razvoj i održavanje IKT sustavâ koji se odnosi na testiranje i odobrenje svih IKT sustava prije njihove upotrebe i nakon održavanja u skladu s člankom 8. stavkom 2. točkom (b) podtočkama v., vi. i vii. Razina testiranja razmjerna je ključnosti relevantnih poslovnih postupaka i IKT imovine. Testiranje se osmišljava za provjeru jesu li novi IKT sustavi primjereni za predviđeni rad, što uključuje provjeru kvalitete softvera razvijenog unutar samog subjekta.

Središnje druge ugovorne strane uz zahtjeve utvrđene u prvom podstavku u osmišljavanje i provedbu testiranja iz prvog podstavka prema potrebi uključuju:

(a) članove sustava poravnanja i klijente;

(b) interoperabilne središnje druge ugovorne strane;

(c) druge zainteresirane strane.

Središnji depozitoriji vrijednosnih papira uz zahtjeve utvrđene u prvom podstavku u osmišljavanje i provedbu testiranja iz prvog podstavka prema potrebi uključuju:

(a) korisnike;

(b) pružatelje ključnih javnih i drugih usluga;

(c) druge središnje depozitorije vrijednosnih papira;

(d) druge tržišne infrastrukture;

(e) sve ostale institucije s kojima su središnji depozitoriji vrijednosnih papira utvrdile međuovisnosti u politici kontinuiteta poslovanja.

3. Postupci iz stavka 2. uključuju provedbu preispitivanja izvornog koda koja obuhvaćaju statičko i dinamičko testiranje. To uključuje testiranje sigurnosti sustava i aplikacija izloženih internetu u skladu s člankom 8. stavkom 2. točkom (b) podtočkama v., vi. i vii. Financijski subjekti:

(a) utvrđuju i analiziraju ranjivosti i neobične pojave u izvornom kodu;

(b) donose akcijski plan za otklanjanje tih ranjivosti i neobičnih pojava;

(c) prate provedbu tog akcijskog plana.

4. Postupak iz stavka 2. uključuje testiranje softverskih paketa najkasnije u fazi integracije u skladu s člankom 8. stavkom 2. točkom (b) podtočkama v., vi. i vii.

5. Postupkom iz stavka 2. osigurava se sljedeće:

(a) u neprodukcijskim okruženjima pohranjuju se samo anonimizirani, pseudonimizirani ili randomizirani produkcijski podaci;

(b) financijski subjekti osiguravaju cjelovitost i povjerljivost podataka u neprodukcijskim okruženjima.

6. Odstupajući od stavka 5., postupkom iz stavka 2. može se predvidjeti da se produkcijski podaci pohranjuju samo za određena testiranja, na ograničeno vrijeme i nakon odobrenja relevantne funkcije i prijave tog testiranja funkciji za upravljanje IKT rizikom.

7. Postupak iz stavka 2. obuhvaća provedbu kontrola za zaštitu cjelovitosti izvornog koda IKT sustava koji su razvijeni unutar subjekta ili koje je razvila i financijskom subjektu pruža treća strana pružatelj IKT usluga.

8. Postupkom iz stavka 2. predviđa se da se zaštićeni softver i, ako je moguće, izvorni kod koji pružaju treće strane pružatelji IKT usluga ili koji potječe iz projekata otvorenog koda analiziraju i testiraju u skladu sa stavkom 3. prije uvođenja u produkcijsko okruženje.

9. Stavci od 1. do 8. ovog članka primjenjuju se i na IKT sustave koje razvijaju ili kojima upravljaju korisnici izvan IKT funkcije uz primjenu pristupa koji se temelji na procjeni rizika.

Članak 17.

Upravljanje promjenama IKT-a

1. Financijski subjekti u sklopu zaštitnih mjera za očuvanje dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka u postupke upravljanja promjenama IKT-a iz članka 9. stavka 4. točke (e) Uredbe (EU) 2022/2554 u vezi sa svim promjenama softvera, hardvera, komponenata ugrađenog softvera, sustava ili sigurnosnih parametara uključuju sve sljedeće elemente:

(a) provjeru ispunjenosti zahtjeva za sigurnost IKT-a;

(b) mehanizme za neovisnost funkcija koje odobravaju promjene i funkcija odgovornih za zahtijevanje i provedbu tih promjena;

(c) jasan opis uloga i odgovornosti kako bi se osiguralo:

  i. da se promjene definiraju i planiraju;

  ii. da se utvrdi primjereni prelazak;

  iii. da se promjene kontrolirano testiraju i dovrše;

  iv. da postoji djelotvorno osiguranje kvalitete;

(d) dokumentiranje pojedinosti o promjenama i obavješćivanje o njima, među ostalim o:

  i. svrsi i opsegu promjene;

  ii. rokovima za provedbu promjene;

  iii. očekivanim ishodima;

(e) utvrđivanje rezervnih postupaka i odgovornosti, što uključuje postupke i odgovornosti za odustajanje od promjena ili oporavak od neuspješno provedenih promjena;

(f) postupke, protokole i alate za upravljanje hitnim promjenama s odgovarajućim zaštitnim mjerama;

(g) postupke za dokumentiranje, ponovnu evaluaciju, procjenu i odobrenje hitnih promjena nakon njihove provedbe, što uključuje zaobilazna rješenja i zakrpe;

(h) utvrđivanje potencijalnog učinka promjene na postojeće mjere za sigurnost IKT-a i procjenu je li zbog te promjene potrebno donijeti dodatne mjere za sigurnost IKT-a.

2. Središnje druge ugovorne strane i središnji depozitoriji vrijednosnih papira nakon znatnih promjena u IKT sustavima te sustave strogo testiranu simulirajući visoko opterećenje.

Središnje druge ugovorne strane u osmišljavanje i provedbu testiranja iz prvog podstavka prema potrebi uključuju:

(a) članove sustava poravnanja i klijente;

(b) interoperabilne središnje druge ugovorne strane;

(c) druge zainteresirane strane.

Središnji depozitoriji vrijednosnih papira u osmišljavanje i provedbu testiranja iz prvog podstavka prema potrebi uključuju:

(a) korisnike;

(b) pružatelje ključnih javnih i drugih usluga;

(c) druge središnje depozitorije vrijednosnih papira;

(d) druge tržišne infrastrukture;

(e) sve ostale institucije s kojima su središnji depozitoriji vrijednosnih papira utvrdile međuovisnosti u politici kontinuiteta poslovanja u području IKT-a.

Odjeljak 8.

Članak 18.

Fizička i okolišna sigurnost

1. Financijski subjekti u sklopu zaštitnih mjera za očuvanje dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka utvrđuju, dokumentiraju i provode politiku fizičke i okolišne sigurnosti. Financijski subjekti tu politiku izrađuju s obzirom na prirodu kiberprijetnji, u skladu s klasifikacijom iz članka 8. stavka 1. Uredbe (EU) 2022/2554 i na temelju ukupnog profila rizičnosti IKT imovine i dostupne informacijske imovine.

2. Politika fizičke i okolišne sigurnosti iz stavka 1. sadržava sve sljedeće:

(a) upućivanje na odjeljak politike o kontroli pravâ upravljanja pristupom iz članka 21. prvog stavka točke (g);

(b) mjere za zaštitu prostora i podatkovnih centara financijskog subjekta te područja koje je financijski subjekt odredio kao osjetljiva, a u kojima se nalazi IKT imovina i informacijska imovina, od napada, nesreća te okolišnih opasnosti i prijetnji;

(c) mjere za zaštitu IKT imovine unutar i izvan prostora financijskog subjekta, pri čemu se uzimaju u obzir rezultati procjene IKT rizika za relevantnu IKT imovinu;

(d) mjere za osiguranje dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti IKT imovine, informacijske imovine i uređaja za kontrolu fizičkog pristupa financijskog subjekta na temelju odgovarajućeg održavanja;

(e) mjere za očuvanje dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka, uključujući:

i. politiku praznog stola za papire;

ii. politiku praznog zaslona za prostore u kojima se obrađuju podaci.

Za potrebe točke (b) mjere za zaštitu od okolišnih opasnosti i prijetnji razmjerne su važnosti prostora, podatkovnih centara, područja određenih kao osjetljivih i ključnosti operacija ili IKT sustava koji se u njima nalaze.

Za potrebe točke (c) politika fizičke i okolišne sigurnosti iz stavka 1. sadržava mjere za odgovarajuću zaštitu IKT imovine koja se ostavlja bez nadzora.

POGLAVLJE II.

Politika ljudskih resursa i kontrola pristupa

Članak 19.

Politika ljudskih resursa

Financijski subjekti u svoju politiku ljudskih resursa ili druge relevantne politike uključuju sve sljedeće elemente povezane sa sigurnosti IKT-a:

(a) utvrđivanje i dodjelu svih posebnih odgovornosti za sigurnost IKT-a;

(b) sljedeće zahtjeve za osoblje financijskog subjekta i treće strane pružatelje IKT usluga koji upotrebljavaju IKT imovinu financijskog subjekta ili joj pristupaju:

i. da budu informirani o politikama, postupcima i protokolima financijskog subjekta za sigurnost IKT-a te da ih se pridržavaju;

ii. da budu upoznati s kanalima za prijavljivanje koje je financijski subjekt uspostavio u svrhu otkrivanja neobičnog ponašanja, među ostalim, prema potrebi, kanala za prijavljivanje koji su uspostavljeni u skladu s Direktivom (EU) 2019/1937 Europskog parlamenta i Vijeća ([11]);

iii. da osoblje nakon prestanka radnog odnosa financijskom subjektu vrati svu IKT imovinu i materijalnu informacijsku imovinu koju posjeduje, a pripada financijskom subjektu.

Članak 20.

Upravljanje identitetom

1. Financijski subjekti u sklopu svoje kontrole pravâ upravljanja pristupom izrađuju, dokumentiraju i provode politike i postupke za upravljanje identitetom kojima se osigurava jedinstvena identifikacija i autentifikacija fizičkih osoba i sustava koji pristupaju podacima financijskih subjekata kako bi se prava pristupa dodijelila korisnicima u skladu s člankom 21.

2. Politike i postupci za upravljanje identitetom iz stavka 1. sadržavaju sve sljedeće:

(a) ne dovodeći u pitanje članak 21. prvi stavak točku (c), svakom članu osoblja financijskog subjekta ili osoblja treće strane pružatelja IKT usluga koji pristupa informacijskoj imovini i IKT imovini financijskog subjekta dodjeljuje se jedinstveni identitet koji odgovara jedinstvenom korisničkom računu;

(b) proces upravljanja životnim ciklusom za identitete i račune kojim se upravlja izradom, promjenama, preispitivanjem i ažuriranjem, privremenom deaktivacijom i ukidanjem svih računa.

Za potrebe točke (a) financijski subjekti vode evidenciju o svim dodjelama identiteta. Ta se evidencija čuva nakon reorganizacije financijskog subjekta ili nakon završetka ugovornog odnosa, ne dovodeći u pitanje zahtjeve za zadržavanje utvrđene u primjenjivom pravu Unije i nacionalnom pravu.

Za potrebe točke (b) financijski subjekti, ako je izvedivo i prema potrebi, uvode automatizirana rješenja za proces upravljanja životnim ciklusom identiteta.

Članak 21.

Kontrola pristupa

Financijski subjekti u sklopu svoje kontrole pravâ upravljanja pristupom izrađuju, dokumentiraju i provode politiku koja sadržava sve sljedeće:

(a) dodjelu prava pristupa IKT imovini na temelju načela nužne informiranosti, nužne upotrebe i najmanjih povlastica, među ostalim za daljinski i hitni pristup;

(b) razdvajanje dužnosti kako bi se spriječio neopravdani pristup ključnim podacima ili kako bi se spriječila dodjela kombiniranih prava pristupa kojima se mogu zaobići kontrole;

(c) odredbu o odgovornosti korisnika, što uključuje maksimalno ograničavanje upotrebe generičkih i dijeljenih korisničkih računa i omogućivanje u svakom trenutku utvrđivanja identiteta korisnika koji u IKT sustavima izvršavaju pojedine aktivnosti;

([11]) Direktiva (EU) 2019/1937 Europskog parlamenta i Vijeća od 23. listopada 2019. o zaštiti osoba koje prijavljuju povrede prava Unije (SL L 305, 26.11.2019., str. 17., ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

(d) odredbu o ograničenjima pristupa IKT imovini, što uključuje utvrđivanje kontrola i alata za sprečavanje neovlaštenog pristupa;

(e) postupke za upravljanje računima kojima se dodjeljuju, mijenjaju ili opozivaju prava pristupa za korisničke i generičke račune, među ostalim generičke administratorske račune, što uključuje odredbu o svemu sljedećem:

i. dodjeli uloga i odgovornosti za dodjelu, preispitivanje i opoziv pravâ pristupa;

ii. dodjeli povlaštenog, hitnog i administratorskog pristupa na osnovi nužne informiranosti ili na *ad hoc* osnovi za sve IKT sustave;

iii. povlačenju pravâ pristupa bez nepotrebne odgode po prestanku radnog odnosa ili kad pristup više nije nužan;

iv. ažuriranju pravâ pristupa ako su potrebne promjene i barem jedanput godišnje za sve IKT sustave, osim IKT sustava kojima se podupiru ključne ili važne funkcije i barem svakih šest mjeseci za IKT sustave kojima se podupiru ključne ili važne funkcije;

(f) metode autentifikacije, što uključuje sve sljedeće:

i. primjenu metoda autentifikacije koje su razmjerne klasifikaciji utvrđenoj u skladu s člankom 8. stavkom 1. Uredbe (EU) 2022/2554 i ukupnom profilu rizičnosti IKT imovine te uzimajući u obzir vodeće prakse;

ii. upotrebu pouzdanih metoda autentifikacije u skladu s vodećim praksama i tehnikama za daljinski pristup mreži financijskog subjekta, za povlašteni pristup, za pristup IKT imovini kojom se podupiru ključne ili važne funkcije ili javno dostupnoj IKT imovini;

(g) mjere za kontrolu fizičkog pristupa, što uključuje:

i. utvrđivanje identiteta i evidentiranje fizičkih osoba koje su ovlaštene za pristup prostorima, podatkovnim centrima i područjima koje je financijski subjekt odredio kao osjetljiva, a u kojima se nalazi IKT imovina i informacijska imovina;

ii. dodjelu pravâ fizičkog pristupa ključnoj IKT imovini isključivo ovlaštenim osobama, u skladu s načelima nužne informiranosti i najmanjih povlastica te na *ad hoc* osnovi;

iii. praćenje fizičkog pristupa prostorima, podatkovnim centrima i područjima koje je financijski subjekt odredio kao osjetljiva, a u kojima se nalaze IKT imovina i informacijska imovina;

iv. preispitivanje pravâ fizičkog pristupa kako bi se pravodobno opozvala prava pristupa koja nisu nužna.

Za potrebe točke (e) podtočke i. financijski subjekti utvrđuju razdoblje čuvanja, pri čemu uzimaju u obzir ciljeve u području poslovanja i informacijske sigurnosti, razloge evidentiranja događaja u evidenciji i rezultate procjene IKT rizika.

Za potrebe točke (e) podtočke ii. financijski subjekti, ako je moguće, upotrebljavaju zasebne račune za obavljanje administrativnih zadaća u IKT sustavima. Ako je izvedivo i primjereno, financijski subjekti uvode automatizirana rješenja za upravljanje povlaštenim pristupom.

Za potrebe točke (g) podtočke i. utvrđivanje identiteta i evidentiranje razmjerni su važnosti prostora, podatkovnih centara, područja određenih kao osjetljivih i ključnosti operacija ili IKT sustava koji se u njima nalaze.

Za potrebe točke (g) podtočke iii. praćenje je razmjerno klasifikaciji utvrđenoj u skladu s člankom 8. stavkom 1. Uredbe (EU) 2022/2554 i ključnosti područja kojem se pristupa.

POGLAVLJE III.

Otkrivanje i odgovora na IKT incidente

Članak 22.

Politika upravljanja IKT incidentima

Financijski subjekti u sklopu mehanizama za otkrivanje neobičnih aktivnosti, što uključuje probleme s performansama IKT mreže i IKT incidente, izrađuju, dokumentiraju i provode politiku o IKT incidentima u kojoj:

(a) dokumentiraju proces upravljanja IKT incidentima iz članka 17. Uredbe (EU) 2022/2554;

(b) utvrđuju popis relevantnih kontakata s unutarnjim funkcijama i vanjskim dionicima koji su izravno uključeni u sigurnost operacija IKT-a, među ostalim u:

i. otkrivanje i praćenje kiberprijetnji;

ii. otkrivanje neobičnih aktivnosti;

iii. upravljanje ranjivostima;

(c) utvrđuju, provode i upotrebljavaju tehničke, organizacijske i operativne mehanizme kako bi poduprli proces upravljanja IKT incidentima, uključujući mehanizme za brzo otkrivanje neobičnih aktivnosti i ponašanja u skladu s člankom 23. ove Uredbe;

(d) čuvaju sve dokaze povezane s IKT incidentima tijekom razdoblja koje nije dulje od nužnog za potrebe za koje se podaci prikupljaju, razmjerno ključnosti pogođenih poslovnih funkcija, potpornih procesa te IKT imovine i informacijske imovine u skladu s [člankom 15. Delegirane uredbe Komisije (EU) 2024/1772 ([12]) i svim primjenjivim zahtjevima za čuvanje iz prava Unije;

(e) utvrđuju i provode mehanizme za analiziranje znatnih IKT incidenata ili IKT incidenata koji se ponavljaju te uzoraka u broju i pojavi IKT incidenata.

Za potrebe točke (d) financijski subjekti na siguran način čuvaju dokaze iz te točke.

Članak 23.

Otkrivanje neobičnih aktivnosti te kriteriji za otkrivanje i odgovor na IKT incidente

1. Financijski subjekti određuju jasne uloge i odgovornosti za djelotvorno otkrivanje i odgovor na IKT incidente i neobične aktivnosti.

2. Mehanizam za brzo otkrivanje neobičnih aktivnosti, što uključuje probleme s performansama IKT mreže i IKT incidente, kako je navedeno u članku 10. stavku 1. Uredbe (EU) 2022/2554, financijskim subjektima omogućuje:

(a) prikupljanje, praćenje i analizu svega sljedećeg:

i. unutarnjih i vanjskih čimbenika, što uključuje barem evidenciju prikupljenu u skladu s člankom 12. ove Uredbe, informacije koje dostavljaju poslovne i IKT funkcije te probleme koje prijavljuju korisnici financijskog subjekta;

ii. potencijalnih unutarnjih i vanjskih kiberprijetnji, pri čemu se uzimaju u obzir scenariji koje akteri prijetnje često upotrebljavaju i scenariji koji se temelje na saznanjima o prijetnjama;

([12]) Delegirana uredba Komisije (EU) 2024/1772 od 13. ožujka 2024. o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuju kriteriji za klasifikaciju IKT incidenata i kiberprijetnji, pragovi značajnosti i pojedinosti izvješća o značajnim incidentima (OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii. obavijesti o IKT incidentu koju dostavi treća strana pružatelj IKT usluga financijskog subjekta u vezi s incidentom otkrivenim u IKT sustavima i mrežama treće strane pružatelja IKT usluga, a koji bi mogao utjecati na financijski subjekt;

(b) utvrđivanje neobičnih aktivnosti i ponašanja te provedbu alata koji šalju upozorenja na neobične aktivnosti i ponašanja barem za IKT imovinu i informacijsku imovinu kojom se podupiru ključne ili važne funkcije;

(c) određivanje prioriteta upozorenja iz točke (b) kako bi se omogućilo upravljanje otkrivenim IKT incidentima unutar očekivanog roka saniranja, koji određuju financijski subjekti, tijekom i izvan radnog vremena;

(d) automatsko ili ručno evidentiranje, analiziranje i evaluaciju svih relevantnih informacija o svim neobičnim aktivnostima i ponašanju.

Za potrebe točke (b) alati iz te točke sadržavaju alate koji šalju automatska upozorenja na temelju unaprijed definiranih pravila za utvrđivanje neobičnih aktivnosti koje utječu na potpunost i cjelovitost izvora podataka ili evidencije.

3. Financijski subjekti štite evidentiranje neobičnih aktivnosti od neovlaštenog mijenjanja i neovlaštenog pristupa u mirovanju, prijenosu i, prema potrebi, upotrebi.

4. Financijski subjekti evidentiraju sve relevantne informacije za svaku otkrivenu neobičnu aktivnosti, čime se omogućuje:

(a) utvrđivanje datuma i vremena pojave neobične aktivnosti;

(b) utvrđivanje datuma i vremena otkrivanja neobične aktivnosti;

(c) utvrđivanje vrste neobične aktivnosti.

5. Financijski subjekti za aktiviranje procesa otkrivanja i odgovora na IKT incidente iz članka 10. stavka 2. Uredbe (EU) 2022/2554 uzimaju u obzir sve sljedeće kriterije:

(a) pokazatelje da je u IKT sustavu ili mreži možda izvršena zlonamjerna aktivnost ili da su IKT sustav ili mreža možda ugroženi;

(b) otkrivene gubitke podataka u pogledu dostupnosti, vjerodostojnosti, cjelovitosti i povjerljivosti podataka;

(c) otkriveni štetan učinak na transakcije i operacije financijskog subjekta;

(d) nedostupnost IKT sustava i mreže.

6. Za potrebe stavka 5. financijski subjekti uzimaju u obzir i ključnost pogođenih usluga.

POGLAVLJE IV.

Upravljanje kontinuitetom poslovanja u području IKT-a

Članak 24.

Sastavnice politike kontinuiteta poslovanja u području IKT-a

1. Financijski subjekti u svoju politiku kontinuiteta poslovanja u području IKT-a iz članka 11. stavka 1. Uredbe (EU) 2022/2554 uključuju sve sljedeće:

(a) opis:

i. ciljeva politike kontinuiteta poslovanja u području IKT-a, među ostalim međusobnog odnosa IKT-a i općeg kontinuiteta poslovanja, pri čemu se uzimaju u obzir rezultati analize učinka na poslovanje (BIA) iz članka 11. stavka 5. Uredbe (EU) 2022/2554;

ii. opsega aranžmana, planova, postupaka i mehanizama za kontinuitet poslovanja u području IKT-a, među ostalim ograničenja i izuzeća;

iii. vremenskog okvira aranžmana, planova, postupaka i mehanizama za kontinuitet poslovanja u području IKT-a;

iv. kriterija za aktiviranje i deaktiviranje planova kontinuiteta poslovanja u području IKT-a, planova odgovora i oporavka u području IKT-a i planova komunikacije u krizi;

(b) odredbe o:

i. upravljanju i organizaciji za provedbu politike kontinuiteta poslovanja u području IKT-a, što uključuje uloge, odgovornosti i postupke eskalacije kojima se osigurava dostupnost dostatnih resursa;

ii. usklađivanju planova kontinuiteta poslovanja u području IKT-a i općih planova kontinuiteta poslovanja, što se odnosi barem na sljedeće:

1. potencijalne scenarije prekida, među ostalim scenarije iz članka 26. stavka 2. ove Uredbe;

2. ciljeve oporavka, pri čemu financijski subjekt nakon poremećaja može unutar ciljnog vremena oporavka obnoviti svoje ključne ili važne funkcije na ciljnu točku oporavka;

iii. izradi planova kontinuiteta poslovanja u području IKT-a za znatne poremećaje u poslovanju u sklopu tih planova te određivanju prioriteta mjera za kontinuitet poslovanja u području IKT-a na temelju pristupa koji se temelji na procjeni rizika;

iv. izradi, testiranju i preispitivanju planova odgovora i oporavka u području IKT-a u skladu s člancima 25. i 26. ove Uredbe;

v. preispitivanju i djelotvornosti provedenih aranžmana, planova, postupaka i mehanizama za kontinuitet poslovanja u području IKT-a u skladu s člankom 26. ove Uredbe;

vi. usklađivanju politike kontinuiteta poslovanja u području IKT-a sa sljedećim:

1. komunikacijskom politikom iz članka 14. stavka 2. Uredbe (EU) 2022/2554;

2. komunikacijskim mjerama i komunikacijskim mjerama u krizi iz članka 11. stavka 2. točke (e) Uredbe (EU) 2022/2554.

2. Središnje druge ugovorne strane uz zahtjeve iz stavka 1. osiguravaju da njihova politika kontinuiteta poslovanja u području IKT-a:

(a) sadržava najdulje vrijeme oporavka ključnih funkcija koje nije dulje od dva sata;

(b) uzima u obzir vanjske povezanosti i međuovisnosti unutar financijskih infrastruktura, što uključuje mjesta trgovanja na kojima se poravnanje provodi putem središnje druge ugovorne strane, sustave namire vrijednosnih papira i platne sustave te kreditne institucije kojima se koristi središnja druga ugovorna strana ili povezana središnja druga ugovorna strana;

(c) zahtijeva uspostavu mehanizama za:

i. osiguranje kontinuiteta ključnih ili važnih funkcija središnje druge ugovorne strane na temelju scenarija katastrofe;

ii. održavanje sekundarnog mjesta za obradu kojim se može osigurati kontinuitet ključnih ili važnih funkcija središnje druge ugovorne strane jednak primarnome mjestu;

iii. održavanje sekundarnog poslovnog mjesta ili neposredan pristup tom mjestu kako bi osoblju moglo osigurati kontinuitet usluge ako primarno poslovno mjesto nije dostupno;

iv. razmatranje potrebe za dodatnim mjestima za obradu, posebno ako zbog različitosti profila rizičnosti primarnog i sekundarnog mjesta nije dovoljno pouzdano da će ciljevi kontinuiteta poslovanja središnje druge ugovorne strane biti ispunjeni u svim scenarijima.

Za potrebe točke (a) središnje druge ugovorne strane u svim okolnostima dovršavaju postupke i plaćanja na kraju dana u traženom roku i na traženi dan.

Za potrebe točke (c) podtočke i. aranžmanima iz te točke uređuju se barem raspoloživost odgovarajućih ljudskih resursa, najdulje vrijeme nefunkcioniranja ključnih funkcija te prijelaz na sekundarno mjesto i oporavak poslovanja na tome mjestu.

Za potrebe točke (c) podtočke ii. sekundarno mjesto za obradu iz te točke ima profil geografske rizičnosti koji je različit od onog primarnog mjesta.

3. Središnji depozitoriji vrijednosnih papira uz zahtjeve iz stavka 1. osiguravaju da se njihovom politikom kontinuiteta poslovanja u području IKT-a:

(a) uzima u obzir vanjske povezanosti i međuovisnosti s korisnicima, ključnim pružateljima službi i usluga, drugim središnjim depozitorijima vrijednosnih papira i drugim tržišnim infrastrukturama;

(b) zahtijeva da se aranžmanima za kontinuitet poslovanja u području IKT-a omogućuje ciljno vrijeme oporavka ključnih ili važnih funkcija koje nije dulje od dva sata.

4. Mjesta trgovanja uz zahtjeve iz stavka 1. osiguravaju da se njihovom politikom kontinuiteta poslovanja u području IKT-a jamči:

(a) da se trgovanje može nastaviti u roku od dva sata od incidenta koji uzrokuje poremećaj ili malo kasnije;

(b) da je najveća količina podataka koji se mogu izgubiti iz svake IT usluge mjesta trgovanja nakon incidenta koji uzrokuje poremećaj blizu nuli.

Članak 25.

Testiranje planova kontinuiteta poslovanja u području IKT-a

1. Financijski subjekti pri testiranju planova kontinuiteta poslovanja u području IKT-a u skladu s člankom 11. stavkom 6. Uredbe (EU) 2022/2554 uzimaju u obzir analizu učinka na poslovanje (BIA) i procjenu IKT rizika iz članka 3. stavka 1. točke (b) ove Uredbe.

2. Financijski subjekti testiranjem planova kontinuiteta poslovanja u području IKT-a iz stavka 1. procjenjuju mogu li osigurati kontinuitet svojih ključnih ili važnih funkcija. To testiranje:

(a) provodi se na temelju testnih scenarija kojima se simuliraju potencijalni poremećaji, a uključuju odgovarajući niz ozbiljnih, ali vjerojatnih scenarija;

(b) prema potrebi, uključuje testiranje IKT usluga koje pružaju treće strane pružatelji IKT usluga;

(c) za financijske subjekte osim mikropoduzeća, kako je navedeno u članku 11. stavku 6. drugom podstavku Uredbe (EU) 2022/2554, uključuje scenarije prebacivanja s primarne IKT infrastrukture na redundantne kapacitete, sigurnosne kopije i redundantnu infrastrukturu;

(d) osmišljeno je radi preispitivanja pretpostavki na kojima se temelje planovi kontinuiteta poslovanja, među ostalim aranžmani za upravljanje i planovi komunikacije u krizi;

(e) uključuju postupke za provjeru sposobnosti osoblja financijskih subjekata, trećih strana pružatelja IKT usluga, IKT sustava i IKT usluga da primjereno odgovore na scenarije utvrđene u skladu s člankom 26. stavkom 2.

Za potrebe točke (a) financijski subjekti u testiranje uvijek uključuju scenarije koji su uzeti u obzir pri izradi planova kontinuiteta poslovanja.

Za potrebe točke (b) financijski subjekti, prema potrebi, uzimaju u obzir scenarije povezane s nesolventnosti ili prekidima trećih strana pružatelja IKT usluga ili političkim rizicima u jurisdikcijama u kojima se nalaze treće strane pružatelji IKT usluga.

Za potrebe točke (c) testiranjem se provjerava mogu li se barem ključne ili važne funkcije dovoljno dugo održati na odgovarajući način i može li se ponovno uspostaviti uobičajen rad.

3. Središnje druge ugovorne strane uz zahtjeve iz stavka 2. u testiranje planova kontinuiteta poslovanja u području IKT-a iz stavka 1. uključuju:

(a) članove sustava poravnanja;

(b) vanjske pružatelje usluga;

(c) relevantne institucije u financijskoj infrastrukturi s kojima središnje druge ugovorne strane imaju međuovisnosti utvrđene u politici kontinuiteta poslovanja.

4. Središnji depozitoriji vrijednosnih papira uz zahtjeve iz stavka 2. u testiranje planova kontinuiteta poslovanja u području IKT-a iz stavka 1. uključuju:

(a) korisnike središnjih depozitorija vrijednosnih papira;

(b) pružatelje ključnih javnih i drugih usluga;

(c) druge središnje depozitorije vrijednosnih papira;

(d) druge tržišne infrastrukture;

(e) sve ostale institucije s kojima su središnji depozitoriji vrijednosnih papira utvrdile međuovisnosti u politici kontinuiteta poslovanja.

5. Financijski subjekti dokumentiraju rezultate testiranja iz stavka 1. Svi nedostaci utvrđeni na temelju tog testiranja analiziraju se, otklanjaju i prijavljuju upravljačkom tijelu.

Članak 26.

Planovi odgovora i oporavka u području IKT-a

1. Financijski subjekti pri izradi planova odgovora i oporavka u području IKT-a iz članka 11. stavka 3. Uredbe (EU) 2022/2554 uzimaju u obzir rezultate svoje analize učinka na poslovanje (BIA). Ti planovi odgovora i oporavka u području IKT-a:

(a) uključuju opis uvjeta za njihovu aktivaciju ili deaktivaciju te sve iznimke povezane s tom aktivacijom i deaktivacijom;

(b) uključuju opis mjera koje se poduzimaju za osiguranje dostupnosti, cjelovitosti, kontinuiteta i oporavka barem IKT sustava i usluga kojima se podupiru ključne ili važne funkcije financijskog subjekta;

(c) osmišljeni su tako da se pomoću njih ostvaruju ciljevi oporavka operacija financijskih subjekata;

(d) dokumentiraju se i stavljaju na raspolaganje osoblju uključenom u izvršenje planova odgovora i oporavka u području IKT-a te su lako dostupni u hitnim slučajevima;

(e) uključuju mogućnosti kratkoročnog i dugoročnog oporavka, među ostalim djelomičan oporavak sustava;

(f) uključuju ciljeve planova odgovora i oporavka u području IKT-a te uvjete za utvrđivanje uspješnog izvršenja tih planova.

Za potrebe točke (d) financijski subjekti jasno određuju uloge i odgovornosti.

2. Planovima odgovora i oporavka u području IKT-a iz stavka 1. utvrđuju se relevantni scenariji, među ostalim scenariji znatnih poremećaja u poslovanju i povećane vjerojatnosti pojave poremećaja. U tim se planovima osmišljavaju scenariji na temelju aktualnih informacija o prijetnjama i iskustva stečenog tijekom prethodnih poremećaja poslovanja. Financijski subjekti uzimaju u obzir sve sljedeće scenarije:

(a) kibernetičke napade i prebacivanja s primarne IKT infrastrukture na redundantne kapacitete, sigurnosne kopije i redundantnu infrastrukturu;

(b) scenarije u kojima kvaliteta pružanja ključne ili važne funkcije opada do neprihvatljive razine ili pružanje te funkcije nije moguće, pri čemu razmatraju mogući učinak nesolventnosti ili drugih oblika prekida relevantne treće strane pružatelja IKT usluga;

(c) djelomični ili potpuni prekid prostora, među ostalim ureda i poslovnih prostora te podatkovnih centara;

(d) znatan prekid IKT imovine ili komunikacijske infrastrukture;

(e) nedostupnost ključnog broja osoblja ili članova osoblja odgovornih za kontinuitet poslovanja;

(f) učinak klimatskih promjena i događaja povezanih s degradacijom okoliša, prirodnih katastrofa, pandemija i fizičkih napada, među ostalim neovlaštenih upada i terorističkih napada;

(g) unutarnje napade;

(h) političku i društvenu nestabilnost, među ostalim, prema potrebi, u jurisdikciji u kojoj se nalaze treća strana pružatelj IKT usluga te na lokaciji na kojoj se pohranjuju i obrađuju podaci;

(i) opsežne nestanke struje.

3. Ako primarne mjere oporavka nisu kratkoročno izvedive zbog troškova, rizika, logistike ili nepredviđenih okolnosti, u planovima odgovora i oporavka u području IKT-a iz stavka 1. razmatraju se alternativne mogućnosti.

4. Financijski subjekti u sklopu planova odgovora i oporavka u području IKT-a iz stavka 1. razmatraju i provode mjere kontinuiteta za ublažavanje prekida trećih strana pružatelja IKT usluga kojima se podupiru ključne ili važne funkcije financijskog subjekta.

POGLAVLJE V.

Izvješće o preispitivanju okvira za upravljanje IKT rizicima

Članak 27.

Format i sadržaj izvješća o preispitivanju okvira za upravljanje IKT rizicima

1. Financijski subjekti u pretraživom elektroničkom formatu dostavljaju izvješće o preispitivanju okvira za upravljanje IKT rizicima iz članka 6. stavka 5. Uredbe (EU) 2022/2554.

2. Financijski subjekti u izvješće iz stavka 1. uključuju sve sljedeće informacije:

(a) uvodni odjeljak u kojem se:

i. jasno utvrđuje identitet financijskog subjekta koji je predmet izvješća i, prema potrebi, opisuje struktura njegove grupe;

ii. opisuje kontekst izvješća u smislu prirode, opsega i složenosti usluga, aktivnosti i operacija financijskog subjekta, njegove organizacije, utvrđenih ključnih funkcija, strategije, velikih tekućih projekata ili aktivnosti, odnosa i njegove ovisnosti o unutarnjim i ugovornim IKT uslugama i sustavima ili posljedica koje bi potpun gubitak ili znatno oštećenje tih sustava imalo na ključne ili važne funkcije i učinkovitost tržišta;

iii. sažeto opisuju glavne promjene u okviru za upravljanje IKT rizicima u odnosu na prethodno podneseno izvješće;

iv. sažeto opisuju trenutačni i kratkoročni profil IKT rizičnosti, prirodu prijetnji, procijenjenu djelotvornost kontrola i sigurnosni položaj financijskog subjekta;

(b) datum na koji je upravljačko tijelo financijskog subjekta odobrilo izvješće;

(c) opis razloga za preispitivanje okvira za upravljanje IKT rizicima u skladu s člankom 6. stavkom 5. Uredbe (EU) 2022/2554;

(d) datum početka i završetka razdoblja preispitivanja;

(e) funkciju odgovornu za preispitivanje;

(f) opis glavnih promjena i unaprjeđenja okvira za upravljanje IKT rizicima od prethodnog preispitivanja;

(g) sažetak nalaza preispitivanja te detaljnu analizu i procjenu ozbiljnosti slabosti, nedostataka i odstupanja u okviru za upravljanje IKT rizicima tijekom razdoblja preispitivanja;

(h) opis mjera za otklanjanje utvrđenih slabosti, nedostataka i odstupanja, što uključuje sve sljedeće:

i. sažetak mjera poduzetih kako bi se otklonile utvrđene slabosti, nedostaci i odstupanja;

ii. očekivani datum provedbe mjera i datume povezane s unutarnjom kontrolom provedbe, što uključuje informacije o napretku provedbe tih mjera na datum izrade nacrta izvješća uz obrazloženje, prema potrebi, postoji li rizik od nepoštivanja rokova;

iii. alate koji se upotrebljavaju i utvrđivanje funkcija odgovornih za provedbu mjera, što uključuje pojedinosti o tome radi li se o unutarnjim ili vanjskim alatima i funkcijama;

iv. opis učinka promjena predviđenih u sklopu mjera na proračunske, ljudske i materijalne resurse financijskog subjekta, među ostalim resurse namijenjene za provedbu korektivnih mjera;

v. informacije o procesu za informiranje nadležnog tijela, prema potrebi;

vi. ako utvrđene slabosti, nedostaci ili odstupanja nisu podložni korektivnim mjerama, detaljno obrazloženje kriterija upotrijebljenih za analizu učinka tih slabosti, nedostataka ili odstupanja kako bi se procijenio povezani preostali IKT rizik te učinka kriterija upotrijebljenih za prihvaćanje povezanog preostalog rizika;

(i) informacije o planiranoj daljnjoj razradi okvira za upravljanje IKT rizicima;

(j) zaključke iz preispitivanja okvira za upravljanje IKT rizicima;

(k) informacije o prošlim preispitivanjima, među ostalim:

i. popis prošlih preispitivanja;

ii. prema potrebi, stanje provedbe korektivnih mjera utvrđenih u prethodnom izvješću;

iii. ako se pokazalo da predložene korektivne mjere iz prošlih preispitivanja nisu djelotvorne ili su dovele do neočekivanih poteškoća, opis načina na kojim bi se te korektivne mjere mogle poboljšati ili opis tih neočekivanih poteškoća;

(l) izvore informacija upotrijebljenih za pripremu izvješća, među ostalim:

i. za financijske subjekte osim mikropoduzeća, kako je navedeno u članku 6. stavku 6. Uredbe (EU) 2022/2554, rezultate unutarnjih revizija;

ii. rezultate procjena usklađenosti;

iii. rezultate testiranja digitalne operativne otpornosti i, prema potrebi, rezultate naprednog testiranja IKT alata, sustava i procesa putem penetracijskog testiranja vođenog prijetnjama (TLPT);

iv. vanjske izvore.

Za potrebe točke (c), ako je preispitivanje pokrenuto na temelju uputa nadzornog tijela ili zaključaka iz relevantnog testiranja operativne otpornosti ili revizijskih procesa, izvješće sadržava izričita upućivanja na te upute ili zaključke kako bi se mogao utvrditi razlog za pokretanje preispitivanja. Ako je preispitivanje pokrenuto zbog IKT incidenata, izvješće sadržava popis svih IKT incidenata i analizu temeljnih uzroka incidenata.

Za potrebe točke (f) opis sadržava analizu učinka promjena na strategiju za digitalnu operativnu otpornost financijskog subjekta, na okvir unutarnje kontrole IKT-a financijskog subjekta i na upravljanje IKT rizicima financijskog subjekta.

GLAVA III.

POJEDNOSTAVNJENI OKVIR ZA UPRAVLJANJE IKT RIZICIMA ZA FINANCIJSKE SUBJEKTE IZ ČLANKA 16. STAVKA 1. UREDBE (EU) 2022/2554

POGLAVLJE I.

Pojednostavnjeni okvir za upravljanje IKT rizicima

Članak 28.

Upravljanje i organizacija

1. Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 uspostavljaju okvir za unutarnje upravljanje i kontrolu kojim se osigurava djelotvorno i razborito upravljanje IKT rizicima kako bi se postigla visoka razina digitalne operativne otpornosti.

2. Financijski subjekti iz stavka 1. u sklopu svojeg pojednostavnjenog okvira za upravljanje IKT rizicima osiguravaju da njihovo upravljačko tijelo:

(a) snosi opću odgovornost za to da se pojednostavnjenim okvirom za upravljanje IKT rizicima provodi poslovna strategija financijskog subjekta u skladu s njegovom sklonošću preuzimanju rizika i da se u tom kontekstu uzima u obzir IKT rizik;

(b) utvrđuje jasne uloge i odgovornosti za sve zadaće povezane s IKT-om;

(c) utvrđuje jasne ciljeve u području informacijske sigurnosti i zahtjeve u području IKT-a;

(d) odobrava, nadzire i periodički preispituje:

  i. klasifikaciju informacijske imovine financijskog subjekta kako je navedeno u članku 30. stavku 1. ove Uredbe, popis glavnih utvrđenih rizika i analizu učinka na poslovanje te povezane politike;

  ii. planove kontinuiteta poslovanja financijskog subjekta te mjere odgovora i oporavka iz članka 16. stavka 1. točke (f) Uredbe (EU) 2022/2554;

(e) izrađuje i barem jednom godišnje preispituje proračun nužan za ispunjavanje potreba financijskog subjekta u pogledu digitalne operativne otpornosti, i to za sve vrste resursa, što uključuje relevantne programe za podizanje svijesti o sigurnosti u području IKT-a i osposobljavanja o digitalnoj operativnoj otpornosti te stjecanje vještina u području IKT-a za sve članove osoblja;

(f) utvrđuje i provodi politike i mjere iz poglavlja I., II. i III. ove glave kako bi utvrdilo i procijenilo IKT rizik kojem je financijski subjekt izložen te upravljalo tim rizikom;

(g) utvrđuje i provodi postupke, IKT protokole i alate koji su potrebni za zaštitu sve informacijske imovine te IKT imovine;

(h) osigurava da osoblje financijskog subjekta osvježava znanje i vještine koji su im dostatni kako bi mogli razumjeti i procijeniti IKT rizik i njegov učinak na poslovanje financijskog subjekta, razmjerno IKT riziku kojim se upravlja;

(i) uspostavlja aranžmane za izvješćivanje, među ostalim učestalost, oblik i sadržaj izvješća o informacijskoj sigurnosti i digitalnoj operativnoj otpornosti za upravljačko tijelo.

3. Financijski subjekti iz stavka 1. mogu, u skladu sa sektorskim pravom Unije i nacionalnim sektorskim pravom, eksternalizirati zadaće provjeravanja usklađenosti sa zahtjevima za upravljanje IKT rizicima pružateljima IKT usluga unutar grupe ili trećim stranama pružateljima IKT usluga. U slučaju takve eksternalizacije financijski subjekti ostaju u potpunosti odgovorni za provjeru usklađenosti sa zahtjevima za upravljanje IKT rizicima.

4. Financijski subjekti iz stavka 1. osiguravaju odgovarajuće razdvajanje i neovisnost kontrolnih funkcija i funkcija unutarnje revizije.

5. Financijski subjekti iz stavka 1. osiguravaju da njihov pojednostavnjeni okvir za upravljanje IKT rizicima podliježe unutarnjoj reviziji koju revizori provode u skladu s planom revizije financijskog subjekta. Revizori moraju imati dostatno znanje, vještine i stručno znanje u području IKT rizika te moraju biti neovisni. Učestalost i težište revizija u području IKT-a moraju biti razmjerni IKT riziku financijskog subjekta.

6. Financijski subjekti iz stavka 1. na temelju ishoda revizije iz stavka 5. osiguravaju pravodobnu provjeru i ispravljanje ključnih nalaza revizije u području IKT-a.

Članak 29.

Politika i mjere informacijske sigurnosti

1. Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode politiku informacijske sigurnosti u kontekstu pojednostavnjenog okvira za upravljanje IKT rizicima. U toj politici informacijske sigurnosti utvrđuju se načela i pravila na visokoj razini koja su potrebna za zaštitu povjerljivosti, cjelovitosti, dostupnosti i vjerodostojnosti podataka i usluga koje pružaju ti financijski subjekti.

2. Financijski subjekti iz stavka 1. na temelju politike informacijske sigurnosti iz stavka 1. utvrđuju i provode mjere za sigurnost IKT-a kako bi ublažili svoju izloženost IKT riziku, što uključuje mjere za ublažavanje koje provode treće strane pružatelji IKT usluga.

Mjere za sigurnost IKT-a uključuju sve mjere iz članaka od 30. do 38.

Članak 30.

Klasifikacija informacijske imovine i IKT imovine

1. U sklopu pojednostavnjenog okvira za upravljanje IKT rizicima iz članka 16. stavka 1. točke (a) Uredbe (EU) 2022/2554 financijski subjekti iz stavka 1. tog članka utvrđuju, razvrstavaju i dokumentiraju sve ključne ili važne funkcije, informacijsku imovinu i IKT imovinu kojima se one podupiru te njihove međuovisnosti. Financijski subjekti prema potrebi preispituju to utvrđivanje i klasifikaciju.

2. Financijski subjekti iz stavka 1. utvrđuju sve ključne ili važne funkcije koje podupiru treće strane pružatelji IKT usluga.

Članak 31.

Upravljanje IKT rizicima

1. Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 u svoj pojednostavnjeni okvir za upravljanje IKT rizicima uključuju sve sljedeće:

(a) određivanje razina tolerancije na rizik za IKT rizik u skladu sa sklonošću financijskog subjekta preuzimanju rizika;

(b) utvrđivanje i procjenu IKT rizika kojima je izložen financijski subjekt;

(c) utvrđivanje strategija ublažavanja barem za IKT rizike koji nisu unutar razina tolerancije na rizik financijskog subjekta;

(d) praćenje djelotvornosti strategija ublažavanja iz točke (c);

(e) utvrđivanje i procjenu svih IKT rizika i rizika za informacijsku sigurnost koji proizlaze iz svake velike promjene IKT sustava ili IKT usluga, procesa ili postupaka, iz rezultata testiranja IKT sigurnosti i nakon svakog znatnog IKT incidenta.

2. Financijski subjekti iz stavka 1. periodički provode i dokumentiraju procjenu IKT rizika, razmjerno profilu IKT rizičnosti financijskih subjekata.

3. Financijski subjekti iz stavka 1. kontinuirano prate prijetnje i ranjivosti relevantne za njihove ključne ili važne funkcije te informacijsku imovinu i IKT imovinu te redovito preispituju scenarije rizika koji utječu na te ključne ili važne funkcije.

4. Financijski subjekti iz stavka 1. utvrđuju pragove za upozorenja i kriterije za aktiviranje i pokretanje procesa odgovora na IKT incidente.

Članak 32.

Fizička i okolišna sigurnost

1. Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 utvrđuju i provode mjere za fizičku sigurnost osmišljene na temelju prirode prijetnji i u skladu s klasifikacijom iz članka 30. stavka 1. ove Uredbe, ukupnim profilom rizičnosti IKT imovine i dostupnom informacijskom imovinom.

2. Mjerama iz stavka 1. štite se prostori financijskih subjekata i, prema potrebi, podatkovni centri financijskih subjekata u kojima se nalaze IKT imovina i informacijska imovina od neovlaštenog pristupa, napada i nesreća te okolišnih opasnosti i prijetnji.

3. Zaštita od okolišnih opasnosti i prijetnji razmjerna je važnosti predmetnog prostora i, prema potrebi, podatkovnih centara te ključnosti operacija ili IKT sustava koji se u njima nalaze.

POGLAVLJE II.

Dodatni elementi sustava, protokola i alata kojima se učinak IKT rizika svodi na najmanju moguću mjeru

Članak 33.

Kontrola pristupa

Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode postupke za kontrolu logičkog i fizičkog pristupa te primjenjuju, prate i periodički preispituju te postupke. Ti postupci sadržavaju sljedeće elemente kontrole logičkog i fizičkog pristupa:

(a) pravima pristupa informacijskoj imovini, IKT imovini i funkcijama koje one podupiru te pravima pristupa ključnim lokacijama poslovanja financijskog subjekta upravlja se na temelju načela nužne informiranosti, nužne upotrebe i najmanjih povlastica, među ostalim za daljinski i hitni pristup;

(b) odgovornost korisnika, kojom se omogućuje utvrđivanje identiteta korisnika koji izvršavaju pojedine radnje u IKT sustavima;

(c) postupke za upravljanje računima kojima se dodjeljuju, mijenjaju ili opozivaju prava pristupa za korisničke i generičke račune, među ostalim generičke administratorske račune;

(d) metode autentifikacije razmjerne klasifikaciji iz članka 30. stavka 1. i ukupnom profilu rizičnosti IKT imovine, koje se temelje na vodećim praksama;

(e) prava pristupa periodički se preispituju i povlače kad više nisu potrebna.

Za potrebe točke (c) financijski subjekt dodjeljuje povlašteni, hitni i administratorski pristup na osnovi nužne informiranosti ili na *ad hoc* osnovi za sve IKT sustave te se on evidentira u skladu s člankom 34. prvim stavkom točkom (f).

Za potrebe točke (d) financijski subjekti primjenjuju pouzdane metode autentifikacije koje se temelje na vodećim praksama za daljinski pristup mreži financijskih subjekata, povlašteni pristup i pristup IKT imovini kojom se podupiru ključne ili važne funkcije koje su javno dostupne.

Članak 34.

Sigurnost operacija IKT-a

Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 u sklopu svojih sustava, protokola i alata te u pogledu sve IKT imovine:

(a) prate i upravljaju životnim ciklusom sve IKT imovine;

(b) prate podupiru li IKT imovinu treće strane pružatelji IKT usluga financijskih subjekata, prema potrebi;

(c) utvrđuju zahtjeve za kapacitet svoje IKT imovine te mjere za održavanje i povećanje dostupnosti i učinkovitosti IKT sustavâ te sprečavaju manjak kapaciteta IKT-a prije nego što do njega dođe;

(d) provode automatizirano skeniranje i procjenu ranjivosti IKT imovine razmjerne njihovoj klasifikaciji u skladu s člankom 30. stavkom 1. i ukupnom profilu rizičnosti IKT imovine te uvode zakrpe kako bi otklonili utvrđene ranjivosti;

(e) upravljaju rizicima povezanima sa zastarjelom ili nepodržanom IKT imovinom;

(f) evidentiraju događaje povezane s kontrolom logičkog i fizičkog pristupa, operacijama IKT-a, među ostalim aktivnostima sustava i mrežnog prometa, i upravljanjem promjenama IKT-a;

(g) utvrđuju i provode mjere za praćenje i analiziranje informacija o neobičnim aktivnostima i ponašanju za ključne ili važne operacije IKT-a;

(h) provode mjere za praćenje relevantnih i aktualnih informacija o kiberprijetnjama;

(i) provode mjere za utvrđivanje mogućih curenja informacija, zlonamjernog koda i drugih sigurnosnih prijetnji, kao i javno poznatih ranjivosti softvera i hardvera te provjeravaju postoje li odgovarajuća nova sigurnosna ažuriranja.

Za potrebe točke (f) financijski subjekti usklađuju razinu detaljnosti evidencije s njihovom svrhom i upotrebom IKT imovine koja se koristi za izradu evidencije.

Članak 35.

Sigurnost podataka i sustava te mrežna sigurnost

Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 u sklopu svojih sustava, protokola i alata izrađuju i provode zaštitne mjere kojima se mreže štite od neovlaštenih upada i zlouporabe podataka te održava dostupnost, vjerodostojnost, cjelovitost i povjerljivost podataka. Konkretno, uzimajući u obzir klasifikaciju iz članka 30. stavka 1. ove Uredbe, financijski subjekti uspostavljaju sve sljedeće:

(a) utvrđivanje i provedbu mjera za zaštitu podataka u upotrebi, prijenosu i mirovanju;

(b) utvrđivanje i provedbu sigurnosnih mjera povezanih s upotrebom softvera, medija za pohranu podataka, sustava i krajnjih uređaja za prijenos i pohranu podataka financijskog subjekta;

(c) utvrđivanje i provedbu mjera za sprečavanje i otkrivanje neovlaštenih povezivanja na mrežu financijskog subjekta, kao i za zaštitu mrežnog prometa između unutarnjih mreža financijskog subjekta i interneta te drugih vanjskih veza;

(d) utvrđivanje i provedbu mjera kojima se osigurava dostupnost, vjerodostojnost, cjelovitost i povjerljivost podataka tijekom mrežnog prijenosa;

(e) proces za sigurno brisanje podataka koji se nalaze u prostorima financijskog subjekta ili su vanjski pohranjeni, a koje financijski subjekt više ne treba prikupljati ili pohranjivati;

(f) proces za sigurno odlaganje ili stavljanje izvan funkcije uređaja za pohranu podataka koji se nalaze u prostorima ili su vanjski pohranjeni, a koji sadržavaju povjerljive informacije;

(g) utvrđivanje i provedbu mjera kako rad na daljinu i upotreba privatnih krajnjih uređaja ne bi negativno utjecali na sposobnost financijskog subjekta da obavlja ključne aktivnosti na odgovarajući, pravodoban i siguran način.

Članak 36.

Testiranje sigurnosti IKT-a

1. Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 uspostavljaju i provode plan za testiranje sigurnosti IKT-a kako bi provjerili djelotvornost mjera za sigurnost IKT-a razvijenih u skladu s člancima 33., 34., 35., 37. i 38. ove Uredbe. Financijski subjekti osiguravaju da se u planu uzmu u obzir prijetnje i ranjivosti utvrđene u sklopu pojednostavnjenog okvira za upravljanje IKT rizicima iz članka 31. ove Uredbe.

2. Financijski subjekti iz stavka 1. preispituju, procjenjuju i testiraju mjere za sigurnost IKT-a, pri čemu uzimaju u obzir ukupni profil rizičnosti IKT imovine financijskog subjekta.

3. Financijski subjekti iz stavka 1. prate i procjenjuju rezultate testiranja sigurnosti te u skladu s njima ažuriraju svoje sigurnosne mjere bez nepotrebne odgode u slučaju IKT sustava kojima se podupiru ključne ili važne funkcije.

Članak 37.

Nabava, razvoj i održavanja IKT sustavâ

Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554, prema potrebi, osmišljavaju i provode postupak kojim se uređuju nabava, razvoj i održavanje IKT sustavâ na temelju pristupa koji se temelji na procjeni rizika. Tim se postupkom:

(a) osigurava da se prije svake nabave ili razvoja IKT sustava jasno odrede funkcionalni i nefunkcionalni zahtjevi, među ostalim zahtjevi za informacijsku sigurnost, te da relevantna poslovna funkcija odobri te zahtjeve;

(b) osigurava testiranje i odobrenje IKT sustava prije njihove prve upotrebe i prije mijenjanja produkcijskog okruženja;

(c) određuju mjere za smanjenje rizika od nenamjerne izmjene IKT sustava ili njihove namjerne manipulacije tijekom razvoja i uvođenja u produkcijsko okruženje.

Članak 38.

Upravljanje IKT projektima i promjenama IKT-a

1. Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 izrađuju, dokumentiraju i provode postupak za upravljanje IKT projektima te utvrđuju uloge i odgovornosti za njegovu primjenu. Taj postupak obuhvaća sve faze IKT projekata od pokretanja do završetka.

2. Financijski subjekti iz stavka 1. izrađuju, dokumentiraju i provode postupak za upravljanje promjenama IKT-a kako bi se sve promjene IKT sustavâ evidentirale, testirale, procijenile, provele i provjerile na kontroliran način i uz odgovarajuće mjere zaštite radi očuvanja digitalne operativne otpornosti financijskog subjekta.

Poglavlje III.

UPRAVLJANJE KONTINUITETOM POSLOVANJA U PODRUČJU IKT-a

Članak 39.

Sastavnice plana kontinuiteta poslovanja u području IKT-a

1. Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 izrađuju svoje planove kontinuiteta poslovanja u području IKT-a uzimajući u obzir rezultate analize izloženosti znatnim poremećajima u poslovanju i njihova potencijalnog učinka te scenarije kojim bi mogla biti izložena njihova IKT imovina kojom se podupiru ključne ili važne funkcije, uključujući scenarij kibernetičkog napada.

2. Za planove kontinuiteta poslovanja u području IKT-a iz stavka 1. vrijedi sljedeće:

(a) odobrava ih upravljačko tijelo financijskog subjekta;

(b) dokumentiraju se i lako su dostupni u hitnim ili kriznim slučajevima;

(c) u njima se dodjeljuju dostatni resursi za njihovo izvršenje;

(d) u njima se utvrđuju planirane razine oporavka i vremenski okviri za oporavak i nastavak rada funkcija te ključnih unutarnjih i vanjskih ovisnosti, što uključuje treće strane pružatelje IKT usluga;

(e) u njima se utvrđuju uvjeti na temelju kojih se mogu aktivirati planovi kontinuiteta poslovanja u području IKT-a te mjere koje se poduzimaju kako bi se osigurali dostupnost, kontinuitet i oporavak IKT imovine financijskih subjekata kojom se podupiru ključne ili važne funkcije;

(f) u njima se utvrđuju mjere ponovne uspostave i oporavka za ključne ili važne poslovne funkcije, potporne procese, informacijsku imovinu i njihove međuovisnosti kako bi se izbjegli štetni učinci na funkcioniranje financijskih subjekata;

(g) u njima se utvrđuju postupci i mjere za sigurnosno kopiranje kojima se određuju opseg podataka koji su podložni sigurnosnom kopiranju i minimalna učestalost sigurnosnog kopiranja na temelju ključnosti funkcije za koju se ti podaci upotrebljavaju;

(h) u njima se razmatraju alternativne mogućnosti ako primarne mjere oporavka nisu kratkoročno izvedive zbog troškova, rizika, logistike ili nepredviđenih okolnosti;

(i) u njima se utvrđuju aranžmani za unutarnju i vanjsku komunikaciju, među ostalim planovi za eskalaciju;

(j) ažuriraju se u skladu s iskustvom stečenim na temelju incidenata, testiranja, novih rizika, utvrđenih prijetnji, promijenjenih ciljeva oporavka, znatnih promjena organizacije financijskog subjekata te IKT imovine kojom se podupiru ključne ili poslovne funkcije.

Za potrebe točke (f) mjerama iz te točke predviđa se ublažavanje prekida ključnih trećih strana pružatelja.

Članak 40.

Testiranje planova kontinuiteta poslovanja

1. Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 testiraju svoje planove kontinuiteta poslovanja iz članka 39. ove Uredbe, uključujući scenarije iz tog članka, barem jedanput godišnje u vezi s postupcima sigurnosnog kopiranja i ponovne uspostave ili nakon svake znatne promjene plana kontinuiteta poslovanja.

2. Testiranjem planova kontinuiteta poslovanja iz stavka 1. dokazuje se da financijski subjekti iz tog stavka mogu održati svoje poslovanje do ponovne uspostave ključnih operacija i utvrđuju se svi nedostaci u tim planovima.

3. Financijski subjekti iz stavka 1. dokumentiraju rezultate testiranja planova kontinuiteta poslovanja i svi nedostaci utvrđeni na temelju tog testiranja analiziraju se, otklanjaju i prijavljuju upravljačkom tijelu.

POGLAVLJE IV.

Izvješće o preispitivanju pojednostavnjenog okvira za upravljanje IKT rizicima

Članak 41.

Format i sadržaj izvješća o preispitivanju pojednostavnjenog okvira za upravljanje IKT rizicima

1. Financijski subjekti iz članka 16. stavka 1. Uredbe (EU) 2022/2554 u pretraživom elektroničkom formatu dostavljaju izvješće o preispitivanju okvira za upravljanje IKT rizicima iz stavka 2. tog članka.

2. Izvješće iz stavka 1. sadržava sve sljedeće informacije:

(a) uvodni odjeljak koji uključuje:

i. opis konteksta izvješća u smislu prirode, opsega i složenosti usluga, aktivnosti i operacija financijskog subjekta, organizacije financijskog subjekta, utvrđenih ključnih funkcija, strategije, velikih tekućih projekata ili aktivnosti i odnosa te ovisnosti financijskog subjekta o unutarnjim i eksternaliziranim IKT uslugama i sustavima ili posljedica koje bi potpun gubitak ili znatno oštećenje tih sustava imalo na ključne ili važne funkcije i učinkovitost tržišta;

ii. sažeti opis trenutačnih i kratkoročnih utvrđenih IKT rizika, prirode prijetnji, procijenjene djelotvornosti kontrola i sigurnosnog položaja financijskog subjekta;

iii. informacije o području o kojem se izvješćuje;

iv. sažeti opis glavnih promjena u okviru za upravljanje IKT rizicima u odnosu na prethodno izvješće;

v. sažetak i opis učinka glavnih promjena u pojednostavnjenom okviru za upravljanje IKT rizicima u odnosu na prethodno izvješće;

(b) prema potrebi, datum na koji je upravljačko tijelo financijskog subjekta odobrilo izvješće;

(c) opis razloga za preispitivanje, što uključuje:

i. ako je preispitivanje pokrenuto na temelju uputa nadzornog tijela, dokaz o tim uputama;

ii. ako je preispitivanje pokrenuto zbog IKT incidenata, popis svih tih IKT incidenata i analizu temeljnih uzroka incidenata;

(d) datum početka i završetka razdoblja preispitivanja;

(e) osobu odgovornu za preispitivanje;

(f) sažetak nalaza i samoprocjenu ozbiljnosti slabosti, nedostataka i odstupanja utvrđenih u okviru za upravljanje IKT rizicima tijekom razdoblja preispitivanja, uključujući njihovu detaljnu analizu;

(g) utvrđene korektivne mjere za otklanjanje slabosti, nedostataka i odstupanja pojednostavnjenog okvira za upravljanje IKT rizicima te očekivani datum provedbe tih mjera, među ostalim daljnjih mjera povezanih sa slabostima, nedostacima i odstupanjima utvrđenima u prethodnim izvješćima ako te slabosti, nedostaci i odstupanja još nisu otklonjeni;

(h) opće zaključke preispitivanja pojednostavnjenog okvira za upravljanje IKT rizicima, uključujući sve daljnje planirane razvoje događaja.

GLAVA IV.

ZAVRŠNE ODREDBE

Članak 42.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 13. ožujka 2024.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN