Uradni list
Evropske unije

SL
Serija L

2024/1774

25.6.2024

DELEGIRANA UREDBA KOMISIJE (EU) 2024/1774

z dne 13. marca 2024

o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi, ki določajo orodja, metode, postopke in politike za obvladovanje tveganj na področju IKT ter poenostavljen okvir za obvladovanje tveganj na področju IKT

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 ([1]) ter zlasti člena 15, četrti pododstavek, in člena 16(3), četrti pododstavek, Uredbe,

ob upoštevanju naslednjega:

(1) Uredba (EU) 2022/2554 zajema najrazličnejše finančne subjekte, ki se razlikujejo po velikosti, strukturi, notranji organizaciji ter naravi in kompleksnosti svojih dejavnosti in ki imajo zato povečane ali zmanjšane elemente kompleksnosti ali tveganj. Za zagotovitev, da se ta raznolikost ustrezno upošteva, bi morale biti vse zahteve v zvezi z varnostnimi politikami, postopki, protokoli in orodji na področju IKT ter v zvezi s poenostavljenim okvirom za obvladovanje tveganj na področju IKT sorazmerne s to velikostjo, strukturo, notranjo organizacijo, naravo in kompleksnostjo teh finančnih subjektov ter z ustreznimi tveganji.

(2) Iz istega razloga bi morali imeti finančni subjekti, za katere velja Uredba (EU) 2022/2554, določeno prožnost pri načinu izpolnjevanja zahtev v zvezi z varnostnimi politikami, postopki, protokoli in orodji na področju IKT ter v zvezi z morebitnim poenostavljenim okvirom za obvladovanje tveganj na področju IKT. Zato bi bilo treba finančnim subjektom dovoliti, da dokumentacijo, ki jo že imajo, uporabijo za izpolnjevanje zahtev glede dokumentacije, ki izhajajo iz navedenih zahtev. Iz tega sledi, da bi bilo treba razvoj, dokumentiranje in izvajanje posebnih varnostnih politik na področju IKT zahtevati le za nekatere bistvene elemente, pri čemer bi bilo treba med drugim upoštevati vodilne sektorske prakse in standarde. Poleg tega je treba za zajetje posebnih vidikov tehnične izvedbe razviti, dokumentirati in izvajati varnostne postopke na področju IKT, da se zajamejo posebni vidiki tehnične izvedbe, vključno z upravljanjem zmogljivosti in učinkovitosti delovanja, upravljanjem ranljivosti in popravkov, varnostjo podatkov in sistemov ter beleženjem v dnevnike.

(3) Za zagotovitev, da se varnostne politike, postopki, protokoli in orodja na področju IKT iz naslova II, poglavje I, te uredbe skozi čas pravilno izvajajo, je pomembno, da finančni subjekti pravilno dodelijo in ohranjajo vse vloge in odgovornosti v zvezi z varnostjo IKT ter določijo posledice neskladnosti z varnostnimi politikami ali postopki na področju IKT.

(4) Da bi omejili tveganje nasprotij interesov, bi morali finančni subjekti pri dodeljevanju vlog in odgovornosti na področju IKT zagotoviti ločevanje nalog.

(5) Za zagotovitev prožnosti in poenostavitev okvira nadzora finančnih subjektov se od finančnih subjektov ne bi smelo zahtevati, da oblikujejo posebne določbe o posledicah neskladnosti z varnostnimi politikami, postopki in protokoli na področju IKT iz naslova II, poglavje I, te uredbe, kadar so take določbe že določene v drugi politiki ali postopku.

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

(6) V dinamičnem okolju, v katerem se tveganja na področju IKT nenehno razvijajo, je pomembno, da finančni subjekti razvijejo svoj sklop varnostnih politik na področju IKT na podlagi vodilnih praks in, kadar je primerno, standardov, kot so opredeljeni v členu 2, točka 1, Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta ([2]). To bi moralo finančnim subjektom iz naslova II te uredbe omogočiti, da ostanejo obveščeni in pripravljeni v spreminjajočem se okolju.

(7) Da bi finančni subjekti iz naslova II te uredbe zagotovili svojo digitalno operativno odpornost, bi morali v okviru svojih varnostnih politik, postopkov, protokolov in orodij na področju IKT razviti in izvajati politiko upravljanja sredstev IKT, postopke upravljanja zmogljivosti in učinkovitosti delovanja ter politike in postopke za delovanje IKT. Te politike in postopki so potrebni za zagotovitev spremljanja statusa sredstev IKT v njihovem celotnem življenjskem ciklu, da se ta sredstva učinkovito uporabljajo in vzdržujejo (upravljanje sredstev IKT). Te politike in postopki bi morali zagotoviti tudi optimizacijo delovanja sistemov IKT ter da učinkovitost delovanja sistemov in zmogljivosti IKT izpolnjuje določene poslovne cilje in cilje glede informacijske varnosti (upravljanje zmogljivosti in učinkovitosti delovanja). Nazadnje, te politike in postopki bi morali zagotoviti učinkovito in nemoteno vsakodnevno upravljanje in delovanje sistemov IKT (delovanje IKT), s čimer bi se čim bolj zmanjšalo tveganje izgube zaupnosti, celovitosti in razpoložljivosti podatkov. Te politike in postopki so torej potrebni za zagotovitev varnosti omrežij, določitev ustreznih zaščitnih ukrepov pred vdori in zlorabo podatkov ter ohranitev razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov.

(8) Za zagotovitev ustreznega upravljanja tveganja v zvezi z obstoječimi sistemi IKT bi morali finančni subjekti evidentirati in spremljati končne datume podpornih storitev tretjih oseb na področju IKT. Zaradi morebitnega vpliva, ki bi ga lahko imela izguba zaupnosti, celovitosti in razpoložljivosti podatkov, bi se morali finančni subjekti pri evidentiranju in spremljanju teh končnih datumov osredotočiti na tista sredstva ali sisteme IKT, ki so ključni za poslovanje.

(9) Kriptografske kontrole lahko zagotovijo razpoložljivost, avtentičnost, celovitost in zaupnost podatkov. Finančni subjekti iz naslova II te uredbe bi zato morali take kontrole opredeliti in izvajati na podlagi pristopa, ki temelji na tveganju. V ta namen bi morali finančni subjekti šifrirati zadevne podatke v mirovanju, med prenosom ali, kadar je potrebno, v uporabi na podlagi rezultatov dvodelnega postopka, in sicer razvrstitve podatkov in celovite ocene tveganja na področju IKT. Zaradi kompleksnosti šifriranja podatkov v uporabi bi morali finančni subjekti iz naslova II te uredbe podatke v uporabi šifrirati le, kadar bi bilo to ustrezno glede na rezultate ocene tveganja na področju IKT. Finančni subjekti iz naslova II te uredbe pa bi morali imeti možnost, da zaupnost, celovitost in razpoložljivost zadevnih podatkov zaščitijo z drugimi varnostnimi ukrepi na področju IKT, kadar šifriranje podatkov v uporabi ni izvedljivo ali je preveč kompleksno. Glede na hiter tehnološki razvoj na področju kriptografskih tehnik bi morali finančni subjekti iz naslova II te uredbe ostati seznanjeni z zadevnim razvojem kriptoanalize ter upoštevati vodilne prakse in standarde. Finančni subjekti iz naslova II te uredbe bi zato morali za soočanje z dinamičnim okoljem kriptografskih groženj, vključno z grožnjami zaradi napredka na področju kvantnega računalništva, uporabljati prožen pristop, ki temelji na zmanjševanju in spremljanju tveganja.

(10) Politike, postopki, protokoli in orodja za varnost delovanja IKT ter operativne politike, postopki, protokoli in orodja IKT so bistveni za zagotavljanje zaupnosti, celovitosti in razpoložljivosti podatkov. Eden od ključnih vidikov je strogo ločevanje produkcijskih okolij IKT od okolij, v katerih se sistemi IKT razvijajo in testirajo, ali od drugih neprodukcijskih okolij. To ločevanje bi moralo služiti kot pomemben varnostni ukrep na področju IKT proti nenamernemu in nepooblaščenemu dostopu do, spreminjanju in izbrisu podatkov v produkcijskem okolju, kar bi lahko povzročilo večje motnje v poslovanju finančnih subjektov iz naslova II te uredbe. Vendar bi bilo treba glede na sedanje prakse razvoja sistemov IKT finančnim subjektom v izjemnih okoliščinah dovoliti testiranje v produkcijskih okoljih, če to upravičijo in pridobijo potrebno odobritev.

([2]) Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L 316, 14.11.2012, str. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) Zaradi hitro spreminjajoče se narave okolja IKT, ranljivosti na področju IKT in kibernetskih groženj je potreben proaktiven in celovit pristop k prepoznavanju, ocenjevanju in odpravljanju ranljivosti na področju IKT. Brez takega pristopa so lahko finančni subjekti, njihove stranke, uporabniki ali nasprotne stranke resno izpostavljeni tveganjem, ki bi ogrozila njihovo digitalno operativno odpornost, varnost njihovih omrežij ter razpoložljivost, avtentičnost, celovitost in zaupnost podatkov, ki bi jih morale varnostne politike in postopki na področju IKT varovati. Finančni subjekti iz naslova II te uredbe bi zato morali prepoznati in odpraviti ranljivosti v svojem okolju IKT, tako finančni subjekti kot njihovi tretji ponudniki storitev IKT pa bi morali upoštevati skladen, pregleden in odgovoren okvir za upravljanje ranljivosti. Iz istega razloga bi morali finančni subjekti spremljati ranljivosti na področju IKT z uporabo zanesljivih virov in avtomatiziranih orodij ter preverjati, ali tretji ponudniki storitev IKT zagotavljajo takojšnje ukrepanje v zvezi z ranljivostmi pri zagotovljenih storitvah IKT.

(12) Upravljanje popravkov bi moralo biti ključni del tistih varnostnih politik in postopkov na področju IKT, ki so s testiranjem in uvajanjem v nadzorovanem okolju namenjeni razreševanju prepoznanih ranljivosti in preprečevanju motenj pri namestitvi popravkov.

(13) Za zagotovitev pravočasnega in preglednega obveščanja o morebitnih varnostnih grožnjah, ki bi lahko vplivale na finančni subjekt in njegove deležnike, bi morali finančni subjekti vzpostaviti postopke za odgovorno razkritje ranljivosti na področju IKT strankam, partnerjem in javnosti. Pri določanju teh postopkov bi morali finančni subjekti upoštevati dejavnike, kot so resnost ranljivosti, morebitni vpliv te ranljivosti na deležnike in razpoložljivost ukrepov za odpravo ali blažilnih ukrepov.

(14) Da se omogoči dodelitev pravic dostopa uporabnikom, bi morali finančni subjekti iz naslova II te uredbe uvesti stroge ukrepe za ugotavljanje edinstvene identifikacije posameznikov in sistemov, ki bodo dostopali do informacij finančnega subjekta. Če tega ne bi storili, bi bili finančni subjekti izpostavljeni morebitnemu nepooblaščenemu dostopu, kršitvam v zvezi s podatki in goljufivim dejavnostim, kar bi ogrozilo zaupnost, celovitost in razpoložljivost občutljivih finančnih podatkov. Medtem ko bi morala biti uporaba generičnih ali skupnih računov izjemoma dovoljena v okoliščinah, ki jih določijo finančni subjekti, bi morali finančni subjekti zagotoviti, da se ohrani odgovornost za ukrepe, sprejete prek teh računov. Brez tega zaščitnega ukrepa bi lahko morebitni zlonamerni uporabniki ovirali preiskovalne in popravne ukrepe, zaradi česar bi bili finančni subjekti izpostavljeni neodkritim zlonamernim dejavnostim ali kaznim za neskladnost.

(15) Za upravljanje hitrega napredka v okoljih IKT bi morali finančni subjekti iz naslova II te uredbe izvajati zanesljive politike in postopke vodenja projektov IKT za ohranjanje razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov. V teh politikah in postopkih vodenja projektov IKT bi morali opredeliti elemente, ki so potrebni za uspešno vodenje projektov IKT, vključno s spremembami, pridobitvami, vzdrževanjem in razvojem sistemov IKT finančnega subjekta, ne glede na metodologijo vodenja projektov IKT, ki jo izbere finančni subjekt. V okviru teh politik in postopkov bi morali finančni subjekti sprejeti prakse in metode testiranja, ki ustrezajo njihovim potrebam, pri tem pa upoštevati pristop, ki temelji na tveganju, in zagotoviti ohranjanje varnega, zanesljivega in odpornega okolja IKT. Da se zagotovi varno izvajanje projekta IKT, bi morali finančni subjekti zagotoviti, da lahko zaposleni v določenih poslovnih sektorjih ali vlogah, na katere ta projekt IKT vpliva, zagotovijo potrebne informacije in strokovno znanje. Za zagotovitev učinkovitega nadzora bi bilo treba upravljalnemu organu predložiti poročila o projektih IKT, zlasti o projektih, ki vplivajo na kritične ali pomembne funkcije, in o tveganjih, ki so povezana z njimi. Finančni subjekti bi morali pogostost in podrobnosti sistematičnih in tekočih pregledov ter poročil prilagoditi pomenu in obsegu zadevnih projektov IKT.

(16) Zagotoviti je treba, da se paketi programske opreme, ki jih pridobijo in razvijejo finančni subjekti iz naslova II te uredbe, učinkovito in varno vključijo v obstoječe okolje IKT v skladu z uveljavljenimi poslovnimi cilji in cilji glede informacijske varnosti. Finančni subjekti bi zato morali take pakete programske opreme temeljito oceniti. V ta namen ter za prepoznavanje ranljivosti in morebitnih varnostnih vrzeli v paketih programske opreme in širših sistemih IKT bi morali finančni subjekti izvajati testiranje varnosti IKT. Da bi ocenili integriteto programske opreme in zagotovili, da njena uporaba ne predstavlja tveganj za varnost IKT, bi morali finančni subjekti pregledati tudi izvorne kode pridobljene programske opreme, po možnosti tudi lastniške programske opreme, ki jo zagotavljajo tretji ponudniki storitev IKT, z uporabo statičnih in dinamičnih metod testiranja.

(17) Spremembe ne glede na njihov obseg vključujejo tveganja in lahko pomenijo bistvena tveganja izgube zaupnosti, celovitosti in razpoložljivosti podatkov ter bi torej lahko povzročile resne motnje poslovanja. Za zaščito finančnih subjektov pred morebitnimi ranljivostmi in slabostmi na področju IKT, ki bi jih lahko izpostavile bistvenim tveganjem, je potreben strog postopek preverjanja, da se potrdi, da vse spremembe izpolnjujejo potrebne zahteve za varnost IKT. Finančni subjekti iz naslova II te uredbe bi zato kot bistveni element svojih varnostnih politik in postopkov na področju IKT morali imeti vzpostavljene zanesljive politike in postopke za upravljanje sprememb na področju IKT. Da bi ohranili objektivnost in učinkovitost postopka upravljanja sprememb na področju IKT, preprečili nasprotja interesov in zagotovili objektivno ocenjevanje sprememb na področju IKT, je treba funkcije, odgovorne za odobritev teh sprememb, ločiti od funkcij, ki zahtevajo in izvajajo te spremembe. Da bi dosegli učinkovite prehode, nadzorovano izvajanje sprememb na področju IKT in minimalne motnje v delovanju sistemov IKT, bi morali finančni subjekti dodeliti jasne vloge in odgovornosti, ki zagotavljajo, da so spremembe na področju IKT načrtovane in ustrezno testirane ter da je zagotovljena kakovost. Da bi zagotovili nadaljnje učinkovito delovanje sistemov IKT in vzpostavili varnostno mrežo za finančne subjekte, bi morali finančni subjekti razviti in izvajati tudi nadomestne postopke. Finančni subjekti bi morali jasno opredeliti te nadomestne postopke in dodeliti odgovornosti, da se zagotovi hiter in učinkovit odziv v primeru neuspešnih sprememb na področju IKT.

(18) Za odkrivanje in upravljanje incidentov, povezanih z IKT, ter poročanje o njih bi morali finančni subjekti iz naslova II te uredbe vzpostaviti politiko glede incidentov, povezanih z IKT, ki bi zajemala komponente postopka obvladovanja incidentov, povezanih z IKT. V ta namen bi morali finančni subjekti identificirati vse ustrezne stike znotraj in zunaj organizacije, ki lahko olajšajo pravilno usklajevanje in izvajanje različnih faz v tem postopku. Da bi optimizirali odkrivanje incidentov, povezanih z IKT, in odzivanje nanje ter ugotovili trende med temi incidenti, ki so dragocen vir informacij, ki finančnim subjektom omogoča učinkovito identifikacijo in odpravljanje temeljnih vzrokov in težav, bi morali finančni subjekti zlasti podrobno analizirati incidente, povezane z IKT, za katere menijo, da so najpomembnejši, med drugim zato, ker se redno ponavljajo.

(19) Za zagotovitev zgodnjega in učinkovitega odkrivanja neobičajnega ravnanja bi morali finančni subjekti iz naslova II te uredbe zbirati, spremljati in analizirati različne vire informacij ter dodeliti s tem povezane vloge in odgovornosti. Kar zadeva notranje vire informacij, so dnevniki izjemno pomemben vir, vendar se finančni subjekti ne bi smeli zanašati samo nanje. Namesto tega bi morali finančni subjekti upoštevati širše informacije, ki bi vključevale informacije o tem, kaj poročajo druge notranje funkcije, saj so te funkcije pogosto dragocen vir relevantnih informacij. Iz istega razloga bi morali finančni subjekti analizirati in spremljati informacije, zbrane iz zunanjih virov, vključno z informacijami, ki jih tretji ponudniki storitev IKT zagotovijo o incidentih, ki vplivajo na njihove sisteme in omrežja, ter iz drugih virov informacij, za katere finančni subjekti menijo, da so relevantni. Če so take informacije osebni podatki, se uporablja pravo Unije o varstvu podatkov. Osebni podatki bi morali biti omejeni na to, kar je potrebno za odkrivanje incidentov.

(20) Za lažje odkrivanje incidentov, povezanih z IKT, bi morali finančni subjekti hraniti dokaze o teh incidentih. Za zagotovitev, da se taki dokazi hranijo dovolj dolgo in da se hkrati prepreči pretirano regulativno breme, bi morali finančni subjekti določiti obdobje hrambe, med drugim ob upoštevanju kritičnosti podatkov in zahtev glede hrambe, ki izhajajo iz prava Unije.

(21) Za zagotovitev pravočasnega odkrivanja incidentov, povezanih z IKT, bi morali finančni subjekti iz naslova II te uredbe merila, opredeljena za sprožitev odkrivanja incidentov, povezanih z IKT, in odzivanja nanje, obravnavati kot neizčrpna. Poleg tega, čeprav bi morali finančni subjekti upoštevati vsako od teh meril, za sprožitev postopkov odkrivanja incidentov, povezanih z IKT, in odzivanja nanje ni treba, da okoliščine, opisane v merilih, nastopijo hkrati, ustrezno pa bi bilo treba upoštevati tudi pomen prizadetih storitev IKT.

(22) Pri oblikovanju politike neprekinjenega poslovanja na področju IKT bi morali finančni subjekti iz naslova II te uredbe upoštevati bistvene komponente obvladovanja tveganj na področju IKT, vključno s strategijo obvladovanja incidentov, povezanih z IKT, in komunikacijsko strategijo v zvezi z njimi, postopkom upravljanja sprememb na področju IKT in tveganji, povezanimi s tretjimi ponudniki storitev IKT.

(23) Določiti je treba sklop scenarijev, ki bi jih morali finančni subjekti iz naslova II te uredbe upoštevati pri izvajanju načrtov odzivanja in okrevanja IKT ter testiranju načrtov neprekinjenega poslovanja na področju IKT. Ti scenariji bi morali za finančne subjekte predstavljati izhodišče pri analizi ustreznosti in verjetnosti vsakega scenarija ter potrebe po razvoju alternativnih scenarijev. Finančni subjekti bi se morali osredotočiti na scenarije, v katerih bi lahko bile naložbe v ukrepe za odpornost učinkovitejše in uspešnejše. S testiranjem preklopov med primarno infrastrukturo IKT in morebitno redundantno zmogljivostjo, rezervnimi sistemi in redundantnimi obrati bi morale finančne institucije oceniti, ali ta zmogljivost, rezervni sistem in ti obrati učinkovito delujejo dovolj dolgo, ter zagotoviti, da se normalno delovanje primarne infrastrukture IKT obnovi v skladu s cilji obnovitve.

(24) Določiti je treba zahteve za operativno tveganje in zlasti zahteve za vodenje projektov IKT in upravljanje sprememb na področju IKT ter upravljanje neprekinjenega poslovanja na področju IKT na podlagi tistih, ki se že uporabljajo za centralne nasprotne stranke, centralne depotne družbe in mesta trgovanja v skladu z uredbami (EU) št. 648/2012 ([3]), (EU) št. 600/2014 ([4]) oziroma (EU) št. 909/2014 ([5]) Evropskega parlamenta in Sveta.

(25) Člen 6(5) Uredbe (EU) 2022/2554 od finančnih subjektov zahteva, da pregledajo svoj okvir za obvladovanje tveganj na področju IKT in svojemu pristojnemu organu predložijo poročilo o tem pregledu. Da bi pristojnim organom omogočili enostavno obdelavo informacij v teh poročilih in zagotovili ustrezen prenos teh informacij, bi morali finančni subjekti ta poročila predložiti v elektronski obliki, ki omogoča iskanje.

(26) Zahteve za finančne subjekte, za katere velja poenostavljen okvir za obvladovanje tveganj na področju IKT iz člena 16 Uredbe (EU) 2022/2554, bi morale biti osredotočene na tista bistvena področja in elemente, ki so glede na obseg, tveganje, velikost in kompleksnost navedenih finančnih subjektov minimalno potrebni za zagotovitev zaupnosti, celovitosti, razpoložljivosti in avtentičnosti podatkov in storitev teh finančnih subjektov. V tem kontekstu bi morali imeti ti finančni subjekti vzpostavljen okvir notranjega upravljanja in nadzora z jasnimi odgovornostmi, da se omogoči učinkovit in zanesljiv okvir za obvladovanje tveganj. Poleg tega bi morali ti finančni subjekti za zmanjšanje upravnega in operativnega bremena razviti in dokumentirati samo eno politiko, tj. politiko informacijske varnosti, ki določa načela in pravila na visoki ravni, potrebna za zaščito zaupnosti, celovitosti, razpoložljivosti in avtentičnosti podatkov in storitev teh finančnih subjektov.

(27) Določbe te uredbe se nanašajo na področje okvira za obvladovanje tveganj na področju IKT s podrobno opredelitvijo posebnih elementov, ki se uporabljajo za finančne subjekte v skladu s členom 15 Uredbe (EU) 2022/2554, in z oblikovanjem poenostavljenega okvira za obvladovanje tveganj na področju IKT za finančne subjekte iz člena 16(1) navedene uredbe. Za zagotovitev skladnosti med običajnim in poenostavljenim okvirom za obvladovanje tveganj na področju IKT ter ob upoštevanju, da bi se morale te določbe začeti uporabljati hkrati, je primerno te določbe vključiti v en sam zakonodajni akt.

(28) Ta uredba temelji na osnutku regulativnih tehničnih standardov, ki so ga Komisiji predložili Evropski bančni organ, Evropski organ za zavarovanja in poklicne pokojnine ter Evropski organ za vrednostne papirje in trge (evropski nadzorni organi) v posvetovanju z Agencijo Evropske unije za kibernetsko varnost (ENISA).

([3]) Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov (UL L 201, 27.7.2012, str. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) Uredba (EU) št. 600/2014 Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov in spremembi Uredbe (EU) št. 648/2012 (UL L 173, 12.6.2014, str. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) Uredba (EU) št. 909/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o izboljšanju ureditve poravnav vrednostnih papirjev v Evropski uniji in o centralnih depotnih družbah ter o spremembi direktiv 98/26/ES in 2014/65/EU ter Uredbe (EU) št. 236/2012 (UL L 257, 28.8.2014, str. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Skupni odbor evropskih nadzornih organov iz člena 54 Uredbe (EU) št. 1093/2010 Evropskega parlamenta in Sveta ([6]), člena 54 Uredbe (EU) št. 1094/2010 Evropskega parlamenta in Sveta ([7]) ter člena 54 Uredbe (EU) št. 1095/2010 Evropskega parlamenta in Sveta ([8]) je organiziral odprta javna posvetovanja o osnutku regulativnih tehničnih standardov, na katerem temelji ta uredba, analiziral morebitne stroške in koristi predlaganih standardov ter zaprosil za nasvet interesno skupino za bančništvo, ustanovljeno v skladu s členom 37 Uredbe (EU) št. 1093/2010, interesno skupino za zavarovanja in pozavarovanja ter interesno skupino za poklicne pokojninske sklade, ustanovljeni v skladu s členom 37 Uredbe (EU) št. 1094/2010, ter interesno skupino za vrednostne papirje in trge, ustanovljeno v skladu s členom 37 Uredbe (EU) št. 1095/2010.

(30) V obsegu, v katerem je obdelava osebnih podatkov potrebna za izpolnitev obveznosti iz tega akta, bi se morali v celoti uporabljati Uredba (EU) 2016/679 ([9]) in Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta ([10]). Pri zbiranju osebnih podatkov za zagotovitev ustreznega odkrivanja incidentov bi bilo treba na primer upoštevati načelo najmanjšega obsega podatkov. O osnutku besedila tega akta je bilo opravljeno tudi posvetovanje z Evropskim nadzornikom za varstvo podatkov –

SPREJELA NASLEDNJO UREDBO:

NASLOV I

SPLOŠNO NAČELO

Člen 1

Splošni profil tveganja in kompleksnost

Pri razvoju in izvajanju varnostnih politik, postopkov, protokolov in orodij na področju IKT iz naslova II in poenostavljenega okvira za obvladovanje tveganj na področju IKT iz naslova III se upoštevajo velikost in splošni profil tveganja finančnega subjekta ter narava, obseg in elementi povečane ali zmanjšane kompleksnosti njegovih storitev, dejavnosti in poslovanja, vključno z elementi, ki se nanašajo na:

(a) šifriranje in kriptografijo;

(b) varnost delovanja IKT;

(c) varnost omrežja;

([6]) Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

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

([8]) Uredba (EU) št. 1095/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za vrednostne papirje in trge) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/77/ES (UL L 331, 15.12.2010, str. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj)

(d) vodenje projektov IKT in upravljanje sprememb na področju IKT;

(e) morebitni vpliv tveganja na področju IKT na zaupnost, celovitost in razpoložljivost podatkov ter motenj na neprekinjenost in razpoložljivost dejavnosti finančnega subjekta.

NASLOV II

NADALJNJE USKLAJEVANJE ORODIJ, METOD, POSTOPKOV IN POLITIK ZA OBVLADOVANJE TVEGANJ NA PODROČJU IKT V SKLADU S ČLENOM 15 UREDBE (EU) 2022/2554

POGLAVJE I

Varnostne politike, postopki, protokoli in orodja na področju IKT

Oddelek 1

Člen 2

Splošni elementi varnostnih politik, postopkov, protokolov in orodij na področju IKT

1. Finančni subjekti zagotovijo, da so njihove varnostne politike, informacijska varnost ter povezani postopki, protokoli in orodja na področju IKT iz člena 9(2) Uredbe (EU) 2022/2554 vključeni v njihov okvir za obvladovanje tveganj na področju IKT. Finančni subjekti vzpostavijo varnostne politike, postopke, protokole in orodja na področju IKT iz tega poglavja, ki:

(a) zagotavljajo varnost omrežij;

(b) vsebujejo zaščitne ukrepe pred vdori in zlorabo podatkov;

(c) ohranjajo razpoložljivost, avtentičnost, celovitost in zaupnost podatkov, tudi z uporabo kriptografskih tehnik;

(d) zagotavljajo natančen in hiter prenos podatkov brez večjih motenj in nepotrebnih zamud.

2. Finančni subjekti za varnostne politike na področju IKT iz odstavka 1 zagotovijo, da:

(a) so usklajene s cilji glede informacijske varnosti finančnega subjekta, vključenimi v strategijo za digitalno operativno odpornost iz člena 6(8) Uredbe (EU) 2022/2554;

(b) vsebujejo datum uradne odobritve varnostnih politik na področju IKT s strani upravljalnega organa;

(c) vsebujejo kazalnike in ukrepe za:

(i) spremljanje izvajanja varnostnih politik, postopkov, protokolov in orodij na področju IKT;

(ii) evidentiranje izjem od tega izvajanja;

(iii) zagotavljanje, da je v primeru izjem iz točke (ii) zagotovljena digitalna operativna odpornost finančnega subjekta;

(d) določajo odgovornosti zaposlenih na vseh ravneh, da se zagotovi varnost finančnega subjekta na področju IKT;

(e) določajo posledice neizpolnjevanja varnostnih politik na področju IKT s strani zaposlenih v finančnem subjektu, kadar določbe v zvezi s tem niso določene v drugih politikah finančnega subjekta;

(f) navajajo dokumentacijo, ki jo je treba hraniti;

(g) določajo ureditev ločevanja nalog v okviru modela treh obrambnih linij ali drugega notranjega modela obvladovanja in nadzorovanja tveganj, kot je ustrezno, da se prepreči nasprotja interesov;

(h) upoštevajo vodilne prakse in, kadar je ustrezno, standarde, kot so opredeljeni v členu 2, točka 1, Uredbe (EU) št. 1025/2012;

(i) opredelijo vloge in odgovornosti za razvoj, izvajanje in vzdrževanje varnostnih politik, postopkov, protokolov in orodij na področju IKT;

(j) se pregledujejo v skladu s členom 6(5) Uredbe (EU) 2022/2554;

(k) upoštevajo pomembne spremembe v zvezi s finančnim subjektom, vključno s pomembnimi spremembami dejavnosti ali postopkov finančnega subjekta, okolja kibernetskih groženj ali veljavnih pravnih obveznosti.

Oddelek 2

Člen 3

Obvladovanje tveganj na področju IKT

Finančni subjekti razvijejo, dokumentirajo in izvajajo politike in postopke za obvladovanje tveganj na področju IKT, ki vsebujejo vse naslednje:

(a) navedbo odobritve tolerančne ravni tveganja za tveganje na področju IKT, določene v skladu s členom 6(8), točka (b), Uredbe (EU) 2022/2554;

(b) postopek in metodologijo za izvedbo ocene tveganja na področju IKT, v katerih so opredeljeni:

  (i) ranljivosti in grožnje, ki vplivajo ali bi lahko vplivale na podprte poslovne funkcije, sisteme IKT in sredstva IKT, ki podpirajo te funkcije;

  (ii) kvantitativni ali kvalitativni kazalniki za merjenje učinka in verjetnosti ranljivosti in groženj iz točke (i);

(c) postopek za opredelitev, izvajanje in dokumentiranje ukrepov za obravnavo tveganj na področju IKT za identificirana in ocenjena tveganja na področju IKT, vključno z določitvijo ukrepov za obravnavo tveganj na področju IKT, potrebnih za uskladitev tveganja na področju IKT s tolerančno ravnjo tveganja iz točke (a);

(d) za preostala tveganja na področju IKT, ki so še vedno prisotna po izvajanju ukrepov za obravnavo tveganj na področju IKT iz točke (c):

  (i) določbe o identifikaciji teh preostalih tveganj na področju IKT;

  (ii) dodelitev vlog in odgovornosti v zvezi s:

    (1) sprejetjem preostalih tveganj na področju IKT, ki presegajo tolerančno raven tveganja finančnega subjekta iz točke (a);

    (2) postopkom pregleda iz točke (iv) te točke (d);

  (iii) pripravo popisa sprejetih preostalih tveganj na področju IKT, vključno z utemeljitvijo njihovega sprejetja;

  (iv) določbe o pregledu sprejetih preostalih tveganj na področju IKT vsaj enkrat letno, vključno z:

    (1) identifikacijo vseh sprememb preostalih tveganj na področju IKT;

    (2) oceno razpoložljivih blažilnih ukrepov;

    (3) oceno, ali so razlogi, ki upravičujejo sprejetje preostalih tveganj na področju IKT, še vedno veljavni in se uporabljajo na datum pregleda;

(e) določbe o spremljanju:

  (i) vseh sprememb tveganja na področju IKT in okolja kibernetskih groženj;

  (ii) notranjih in zunanjih ranljivosti in groženj;

  (iii) tveganja finančnega subjekta na področju IKT, ki omogoča hitro odkrivanje sprememb, ki bi lahko vplivale na njegov profil tveganja na področju IKT;

(f) določbe o postopku za zagotovitev, da se upoštevajo vse spremembe poslovne strategije in strategije za digitalno operativno odpornost finančnega subjekta.

Za namene prvega odstavka, točka (c), postopek iz navedene točke zagotavlja:

(a) spremljanje učinkovitosti izvedenih ukrepov za obravnavo tveganj na področju IKT;

(b) oceno, ali so bile dosežene določene tolerančne ravni tveganja finančnega subjekta;

(c) oceno, ali je finančni subjekt sprejel ukrepe za popravek ali izboljšanje navedenih ukrepov, kadar je potrebno.

Oddelek 3

Upravljanje sredstev IKT

Člen 4

Politika upravljanja sredstev IKT

1. Finančni subjekti v okviru varnostnih politik, postopkov, protokolov in orodij na področju IKT iz člena 9(2) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo politiko upravljanja sredstev IKT.

2. Politika upravljanja sredstev IKT iz odstavka 1:

(a) predpisuje spremljanje in upravljanje življenjskega cikla sredstev IKT, identificiranih in razvrščenih v skladu s členom 8(1) Uredbe (EU) 2022/2554;

(b) predpisuje, da finančni subjekt vodi evidenco o vsem naslednjem:

(i) edinstvenem identifikatorju vsakega sredstva IKT;

(ii) informacijah o fizični ali logični lokaciji vseh sredstev IKT;

(iii) razvrstitvi vseh sredstev IKT v skladu s členom 8(1) Uredbe (EU) 2022/2254;

(iv) identiteti lastnikov sredstev IKT;

(v) poslovnih funkcijah ali storitvah, ki jih podpira sredstvo IKT;

(vi) zahtevah glede neprekinjenega poslovanja na področju IKT, vključno s cilji glede časa okrevanja in točke obnovitve;

(vii) ali je sredstvo IKT lahko ali je izpostavljeno zunanjim omrežjem, vključno z internetom;

(viii) povezavah in soodvisnostih med sredstvi IKT in poslovnimi funkcijami, ki uporabljajo vsako sredstvo IKT;

(ix) kadar je ustrezno, za vsa sredstva IKT o končnih datumih rednih in razširjenih podpornih storitev ter podpornih storitev po meri tretjega ponudnika storitev IKT, po katerih ponudnik ali tretji ponudnik storitev IKT teh sredstev IKT ne podpira več;

(c) za finančne subjekte, ki niso mikropodjetja, predpisuje, da ti finančni subjekti vodijo evidenco informacij, potrebnih za izvedbo posebne ocene tveganja na področju IKT za vse obstoječe sisteme IKT iz člena 8(7) Uredbe (EU) 2022/2554.

Člen 5

Postopek za upravljanje sredstev IKT

1. Finančni subjekti razvijejo, dokumentirajo in izvajajo postopek za upravljanje sredstev IKT.

2. Postopek za upravljanje sredstev IKT iz odstavka 1 določa merila za izvedbo ocene kritičnosti informacijskih sredstev in sredstev IKT, ki podpirajo poslovne funkcije. Pri tej oceni se upošteva:

(a) tveganje na področju IKT, povezano s temi poslovnimi funkcijami in njihovimi odvisnostmi od informacijskih sredstev ali sredstev IKT;

(b) kako bi izguba zaupnosti, celovitosti in razpoložljivosti takih informacijskih sredstev in sredstev IKT vplivala na poslovne procese in dejavnosti finančnih subjektov.

Oddelek 4

Šifriranje in kriptografija

Člen 6

Šifriranje in kriptografske kontrole

1. Finančni subjekti v okviru svojih varnostnih politik, postopkov, protokolov in orodij na področju IKT iz člena 9(2) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo politiko o šifriranju in kriptografskih kontrolah.

2. Finančni subjekti politiko o šifriranju in kriptografskih kontrolah iz odstavka 1 oblikujejo na podlagi rezultatov odobrene razvrstitve podatkov in ocene tveganja na področju IKT. Ta politika vsebuje pravila za vse naslednje:

(a) šifriranje podatkov v mirovanju in med prenosom;

(b) šifriranje podatkov v uporabi, kadar je potrebno;

(c) šifriranje notranjih omrežnih povezav in prometa z zunanjimi strankami;

(d) upravljanje kriptografskih ključev iz člena 7, ki določa pravila o pravilni uporabi, zaščiti in življenjskem ciklu kriptografskih ključev.

Kadar šifriranje podatkov v uporabi ni mogoče, finančni subjekti za namene točke (b) obdelujejo podatke v uporabi v ločenem in zaščitenem okolju ali sprejmejo enakovredne ukrepe za zagotovitev zaupnosti, celovitosti, avtentičnosti in razpoložljivosti podatkov.

3. Finančni subjekti v politiko o šifriranju in kriptografskih kontrolah iz odstavka 1 vključijo merila za izbiro kriptografskih tehnik in praks uporabe, pri čemer upoštevajo vodilne prakse in standarde, kot so opredeljeni v členu 2, točka 1, Uredbe (EU) št. 1025/2012, ter razvrstitev ustreznih sredstev IKT, določeno v skladu s členom 8(1) Uredbe (EU) 2022/2554. Finančni subjekti, ki ne morejo upoštevati vodilnih praks ali standardov ali uporabljati najzanesljivejših tehnik, sprejmejo blažilne ukrepe in ukrepe za spremljanje, ki zagotavljajo odpornost proti kibernetskim grožnjam.

4. Finančni subjekti v politiko o šifriranju in kriptografskih kontrolah iz odstavka 1 vključijo določbe za posodabljanje ali spreminjanje kriptografske tehnologije, kadar je potrebno, na podlagi razvoja kriptoanalize. S temi posodobitvami ali spremembami se zagotovi, da kriptografska tehnologija ostane odporna proti kibernetskim grožnjam, kot se zahteva v členu 10(2), točka (a). Finančni subjekti, ki ne morejo posodabljati ali spreminjati kriptografske tehnologije, sprejmejo blažilne ukrepe in ukrepe za spremljanje, ki zagotavljajo odpornost proti kibernetskim grožnjam.

5. Finančni subjekti v politiko o šifriranju in kriptografskih kontrolah iz odstavka 1 vključijo zahtevo po evidentiranju sprejetja blažilnih ukrepov in ukrepov za spremljanje, sprejetih v skladu z odstavkoma 3 in 4, ter po predložitvi utemeljene obrazložitve za njihovo sprejetje.

Člen 7

Upravljanje kriptografskih ključev

1. Finančni subjekti v politiko upravljanja kriptografskih ključev iz člena 6(2), točka (d), vključijo zahteve za upravljanje kriptografskih ključev v njihovem celotnem življenjskem ciklu, vključno z ustvarjanjem, obnavljanjem, hrambo, varnostnim kopiranjem, arhiviranjem, priklicem, prenosom, umikom, preklicem in uničenjem teh kriptografskih ključev.

2. Finančni subjekti opredelijo in izvajajo kontrole za zaščito kriptografskih ključev pred izgubo, nepooblaščenim dostopom, razkritjem in spreminjanjem v njihovem celotnem življenjskem ciklu. Finančni subjekti te kontrole oblikujejo na podlagi rezultatov odobrene razvrstitve podatkov in ocene tveganja na področju IKT.

3. Finančni subjekti razvijejo in izvajajo metode za nadomestitev kriptografskih ključev v primeru izgube, ogroženosti ali okvare teh ključev.

4. Finančni subjekti vzpostavijo in vzdržujejo register vseh potrdil in naprav za shranjevanje potrdil vsaj za sredstva IKT, ki podpirajo kritične ali pomembne funkcije. Finančni subjekti ta register posodabljajo.

5. Finančni subjekti zagotovijo pravočasno obnovitev potrdil pred iztekom njihove veljavnosti.

Oddelek 5

Varnost delovanja IKT

Člen 8

Politike in postopki za delovanje IKT

1. Finančni subjekti v okviru varnostnih politik, postopkov, protokolov in orodij na področju IKT iz člena 9(2) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo politike in postopke za upravljanje delovanja IKT. Te politike in postopki določajo, kako finančni subjekti upravljajo, spremljajo, nadzirajo in obnavljajo svoja sredstva IKT, vključno z dokumentiranjem delovanja IKT.

2. Politike in postopki za delovanje IKT iz odstavka 1 vsebujejo vse naslednje:

(a) opis sredstev IKT, vključno z vsem naslednjim:

  (i) zahtevami glede varne namestitve, vzdrževanja, konfiguracije in odstranitve sistema IKT;

  (ii) zahtevami glede upravljanja informacijskih sredstev, ki jih uporabljajo sredstva IKT, vključno z njihovo obdelavo in obravnavo, tako avtomatizirano kot ročno;

  (iii) zahtevami v zvezi z identifikacijo in nadzorom obstoječih sistemov IKT;

(b) kontrole in spremljanje sistemov IKT, vključno z vsem naslednjim:

  (i) zahtevami za varnostno kopiranje in obnovitev sistemov IKT;

  (ii) zahtevami glede časovnega razporejanja ob upoštevanju soodvisnosti med sistemi IKT;

  (iii) protokoli za informacije o revizijski sledi in sistemskem dnevniku;

  (iv) zahtevami za zagotovitev, da izvajanje notranje revizije in drugega testiranja čim bolj zmanjša motnje v poslovanju;

  (v) zahtevami glede ločevanja produkcijskih okolij IKT od razvojnih, testnih in drugih neprodukcijskih okolij;

  (vi) zahtevami za izvajanje razvoja in testiranja v okoljih, ki so ločena od produkcijskega okolja;

  (vii) zahtevami za izvajanje razvoja in testiranja v produkcijskih okoljih;

(c) obravnavanje napak v zvezi s sistemi IKT, vključno z vsem naslednjim:

(i) postopki in protokoli za obravnavanje napak;

(ii) stiki za podporo in prenos na višjo raven, vključno s stiki za zunanjo podporo v primeru nepričakovanih operativnih ali tehničnih težav;

(iii) postopki za ponovni zagon, povrnitev prejšnjega stanja in obnovitev sistema IKT za uporabo v primeru motenj v sistemu IKT.

Za namene točke (b)(v) se pri ločevanju upoštevajo vse komponente okolja, vključno z računi, podatki ali povezavami, kot se zahteva v členu 13(1), točka (a).

Za namene točke (b)(vii) politike in postopki iz odstavka 1 določajo, da so primeri, v katerih se testiranje izvaja v produkcijskem okolju, jasno opredeljeni, utemeljeni, časovno omejeni in odobreni s strani ustrezne funkcije v skladu s členom 16(6). Finančni subjekti zagotovijo razpoložljivost, zaupnost, celovitost in avtentičnost sistemov IKT in produkcijskih podatkov med razvojnimi in testnimi dejavnostmi v produkcijskem okolju.

Člen 9

Upravljanje zmogljivosti in učinkovitosti delovanja

1. Finančni subjekti v okviru varnostnih politik, postopkov, protokolov in orodij na področju IKT iz člena 9(2) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo postopke upravljanja zmogljivosti in učinkovitosti delovanja za naslednje:

(a) opredelitev zahtev glede zmogljivostih svojih sistemov IKT;

(b) uporabo optimizacije virov;

(c) postopke spremljanja za vzdrževanje in izboljševanje:

(i) razpoložljivosti podatkov in sistemov IKT;

(ii) učinkovitosti sistemov IKT;

(iii) preprečevanja pomanjkanja zmogljivosti IKT.

2. Postopki upravljanja zmogljivosti in učinkovitosti delovanja iz odstavka 1 zagotavljajo, da finančni subjekti sprejmejo ukrepe, ki so primerni za upoštevanje posebnosti sistemov IKT z dolgimi ali zapletenimi postopki nabave ali odobritve ali sistemi IKT, ki zahtevajo veliko virov.

Člen 10

Upravljanje ranljivosti in popravkov

1. Finančni subjekti v okviru varnostnih politik, postopkov, protokolov in orodij na področju IKT iz člena 9(2) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo postopke upravljanja ranljivosti.

2. S postopki upravljanja ranljivosti iz odstavka 1 se:

(a) identificirajo in posodabljajo ustrezni in zaupanja vredni informacijski viri za krepitev in ohranjanje ozaveščenosti o ranljivostih;

(b) zagotovi izvajanje avtomatiziranega pregledovanja in ocenjevanja ranljivosti sredstev IKT, pri čemer sta pogostost in obseg teh dejavnosti sorazmerna z razvrstitvijo, določeno v skladu s členom 8(1) Uredbe (EU) 2022/2554, in splošnim profilom tveganja sredstva IKT;

(c) preveri, ali:

(i) tretji ponudniki storitev IKT obravnavajo ranljivosti, povezane s storitvami IKT, ki jih opravljajo za finančni subjekt;

(ii) ti ponudniki storitev finančnemu subjektu pravočasno poročajo vsaj o kritičnih ranljivostih ter statističnih podatkih in trendih;

(d) spremlja uporaba:

(i) knjižnic tretjih oseb, vključno z odprtokodnimi knjižnicami, ki jih uporabljajo storitve IKT, ki podpirajo kritične ali pomembne funkcije;

(ii) storitev IKT, ki jih je razvil finančni subjekt sam ali jih je za finančni subjekt posebej prilagodil ali razvil tretji ponudnik storitev IKT;

(e) vzpostavijo postopki za odgovorno razkritje ranljivosti strankam, nasprotnim strankam in javnosti;

(f) daje prednost uvajanju popravkov in drugih blažilnih ukrepov za odpravo prepoznanih ranljivosti;

(g) spremlja in preverja sanacijo ranljivosti;

(h) zahteva evidentiranje vseh odkritih ranljivosti, ki vplivajo na sisteme IKT, in spremljanje njihovega razreševanja.

Za namene točke (b) finančni subjekti vsaj enkrat tedensko izvajajo avtomatizirano pregledovanje in ocenjevanje ranljivosti sredstev IKT za sredstva IKT, ki podpirajo kritične ali pomembne funkcije.

Za namene točke (c) finančni subjekti od tretjih ponudnikov storitev IKT zahtevajo, da raziščejo zadevne ranljivosti, določijo temeljne vzroke in izvedejo ustrezne blažilne ukrepe.

Za namene točke (d) finančni subjekti, kadar je primerno v sodelovanju s tretjim ponudnikom storitev IKT, spremljajo različico in morebitne posodobitve knjižnic tretjih oseb. V primeru za uporabo pripravljenih (komercialnih) sredstev IKT ali komponent sredstev IKT, pridobljenih in uporabljenih pri delovanju storitev IKT, ki ne podpirajo kritičnih ali pomembnih funkcij, finančni subjekti v največji možni meri spremljajo uporabo knjižnic tretjih oseb, vključno z odprtokodnimi knjižnicami.

Za namene točke (f) finančni subjekti upoštevajo kritičnost ranljivosti, razvrstitev, določeno v skladu s členom 8(1) Uredbe (EU) 2022/2554, in profil tveganja sredstev IKT, ki jih prizadenejo prepoznane ranljivosti.

3. Finančni subjekti v okviru varnostnih politik, postopkov, protokolov in orodij na področju IKT iz člena 9(2) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo postopke upravljanja popravkov.

4. S postopki upravljanja popravkov iz odstavka 3 se:

(a) v največji možni meri identificirajo in ocenijo razpoložljivi popravki in posodobitve programske in strojne opreme z uporabo avtomatiziranih orodij;

(b) opredelijo postopki za namestitev popravkov in posodabljanje sredstev IKT v nujnih primerih;

(c) testirajo in uvajajo popravki in posodobitve programske in strojne opreme iz člena 8(2), točke (b)(v), (vi) in (vii);

(d) določijo roki za namestitev popravkov in posodobitev programske in strojne opreme ter postopki prenosa na višjo raven, če teh rokov ni mogoče upoštevati.

Člen 11

Varnost podatkov in sistemov

1. Finančni subjekti v okviru varnostnih politik, postopkov, protokolov in orodij na področju IKT iz člena 9(2) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo postopek za varnost podatkov in sistemov.

2. Postopek za varnost podatkov in sistemov iz odstavka 1 vsebuje vse naslednje elemente v zvezi z varnostjo podatkov in sistemov IKT v skladu z razvrstitvijo, določeno v skladu s členom 8(1) Uredbe (EU) 2022/2554:

(a) omejitve dostopa iz člena 21 te uredbe, ki podpirajo zahteve glede zaščite za vsako stopnjo razvrstitve;

(b) opredelitev osnove varne konfiguracije za sredstva IKT, ki čim bolj zmanjšuje izpostavljenost teh sredstev IKT kibernetskim grožnjam, in ukrepe za redno preverjanje, ali se te osnove učinkovito uporabljajo;

(c) opredelitev varnostnih ukrepov za zagotovitev, da se v sisteme IKT in končne naprave namesti samo odobrena programska oprema;

(d) opredelitev varnostnih ukrepov proti zlonamernim kodam;

(e) opredelitev varnostnih ukrepov za zagotovitev, da se za prenos in shranjevanje podatkov finančnega subjekta uporabljajo samo odobrene naprave za shranjevanje podatkov, sistemi in končne naprave;

(f) naslednje zahteve za varno uporabo prenosnih končnih naprav in zasebnih neprenosnih končnih naprav:

  (i) zahtevo po uporabi rešitve za upravljanje, ki omogoča upravljanje končnih naprav na daljavo in brisanje podatkov finančnega subjekta na daljavo;

  (ii) zahtevo po uporabi varnostnih mehanizmov, ki jih zaposleni ali tretji ponudniki storitev IKT ne morejo nepooblaščeno spremeniti, odstraniti ali obiti;

  (iii) zahtevo, da se odstranljive naprave za shranjevanje podatkov uporabljajo le, kadar je preostalo tveganje na področju IKT v mejah tolerančne ravni tveganja finančnega subjekta iz člena 3, prvi pododstavek, točka (a);

(g) postopek za varno brisanje podatkov, prisotnih v prostorih finančnega subjekta ali hranjenih zunaj njih, ki jih finančnemu subjektu ni več treba zbirati ali hraniti;

(h) postopek za varno odstranitev ali razgradnjo naprav za shranjevanje podatkov, prisotnih v prostorih finančnega subjekta ali hranjenih zunaj njih, ki vsebujejo zaupne informacije;

(i) opredelitev in izvajanje varnostnih ukrepov za preprečevanje izgube in uhajanja podatkov za sisteme in končne naprave;

(j) izvajanje varnostnih ukrepov za zagotavljanje, da delo na daljavo in uporaba zasebnih končnih naprav ne vplivata negativno na varnost IKT finančnega subjekta;

(k) za sredstva ali storitve IKT, ki jih upravlja tretji ponudnik storitev IKT, opredelitev in izvajanje zahtev za ohranjanje digitalne operativne odpornosti v skladu z rezultati razvrstitve podatkov in ocene tveganja na področju IKT.

Za namene točke (b) se pri osnovi varne konfiguracije iz navedene točke upoštevajo vodilne prakse in ustrezne tehnike, določene v standardih, kot so opredeljeni v členu 2, točka 1, Uredbe (EU) št. 1025/2012.

Za namene točke (k) finančni subjekti upoštevajo naslednje:

(a) izvedbo nastavitev za elemente, ki jih upravlja finančni subjekt, kot jih priporoča prodajalec;

(b) jasno razdelitev vlog in odgovornosti na področju informacijske varnosti med finančnim subjektom in tretjim ponudnikom storitev IKT v skladu z načelom, da je finančni subjekt v celoti odgovoren za svojega tretjega ponudnika storitev IKT, iz člena 28(1), točka (a), Uredbe (EU) 2022/2554, in v skladu s politiko finančnega subjekta o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, za finančne subjekte iz člena 28(2) navedene uredbe;

(c) potrebo po zagotavljanju in ohranjanju ustreznih kompetenc znotraj finančnega subjekta na področju upravljanja in varnosti uporabljene storitve;

(d) tehnične in organizacijske ukrepe za zmanjšanje tveganj, povezanih z infrastrukturo, ki jo tretji ponudnik storitev IKT uporablja za svoje storitve IKT, na najnižjo možno raven ob upoštevanju vodilnih praks in standardov, kot so opredeljeni v členu 2, točka 1, Uredbe (EU) št. 1025/2012.

Člen 12

Beleženje v dnevnike

1. Finančni subjekti v okviru zaščitnih ukrepov pred vdori in zlorabo podatkov razvijejo, dokumentirajo in izvajajo postopke, protokole in orodja za beleženje v dnevnike.

2. Postopki, protokoli in orodja za beleženje v dnevnike iz odstavka 1 vsebujejo vse naslednje:

(a) opredelitev dogodkov, ki jih je treba zabeležiti v dnevnike, obdobje hrambe dnevnikov ter ukrepe za zaščito in obravnavo podatkov iz dnevnikov, ob upoštevanju namena, za katerega so dnevniki ustvarjeni;

(b) usklajenost ravni podrobnosti dnevnikov z njihovim namenom in uporabo, da se omogoči učinkovito odkrivanje neobičajnega ravnanja iz člena 24;

(c) zahtevo po beleženju dogodkov v zvezi z vsem naslednjim v dnevnike:

  (i) nadzorom logičnega in fizičnega dostopa iz člena 21 ter upravljanjem identitete;

  (ii) upravljanjem zmogljivosti;

  (iii) upravljanjem sprememb;

  (iv) delovanjem IKT, vključno z dejavnostmi sistema IKT;

  (v) dejavnostmi v zvezi z omrežnim prometom, vključno z zmogljivostjo omrežja IKT;

(d) ukrepe za zaščito sistemov beleženja v dnevnike in informacij iz dnevnikov pred nedovoljenim spreminjanjem, brisanjem in nepooblaščenim dostopom v mirovanju, med prenosom in, kadar je primerno, v uporabi;

(e) ukrepe za odkrivanje odpovedi v sistemih beleženja v dnevnike;

(f) brez poseganja v morebitne veljavne regulativne zahteve v skladu s pravom Unije ali nacionalnim pravom, uskladitev ur vsakega od sistemov IKT finančnega subjekta na podlagi dokumentiranega zanesljivega referenčnega časovnega vira.

Za namene točke (a) finančni subjekti določijo obdobje hrambe ob upoštevanju poslovnih ciljev in ciljev glede informacijske varnosti, razloga za zabeleženje dogodka v dnevnik in rezultatov ocene tveganja na področju IKT.

Oddelek 6

Varnost omrežja

Člen 13

Upravljanje varnosti omrežja

Finančni subjekti v okviru zaščitnih ukrepov, ki zagotavljajo varnost omrežij pred vdori in zlorabo podatkov, razvijejo, dokumentirajo in izvajajo politike, postopke, protokole in orodja za upravljanje varnosti omrežja, vključno z vsem naslednjim:

(a) ločevanjem in segmentacijo sistemov in omrežij IKT ob upoštevanju:

  (i) kritičnosti ali pomembnosti funkcije, ki jo podpirajo ti sistemi in omrežja IKT;

  (ii) razvrstitve, določene v skladu s členom 8(1) Uredbe (EU) 2022/2554;

  (iii) splošnega profila tveganja sredstev IKT, ki uporabljajo te sisteme in omrežja IKT;

(b) dokumentacijo vseh omrežnih povezav in podatkovnih tokov finančnega subjekta;

(c) uporabo ločenega in namenskega omrežja za upravljanje sredstev IKT;

(d) opredelitvijo in izvajanjem nadzora dostopa do omrežja, da se preprečijo in odkrijejo povezave katere koli nepooblaščene naprave ali sistema ali katere koli končne točke, ki ne izpolnjuje varnostnih zahtev finančnega subjekta, z omrežjem finančnega subjekta;

(e) šifriranjem omrežnih povezav, ki se potekajo prek korporativnih omrežij, javnih omrežij, domačih omrežij, omrežij tretjih strani in brezžičnih omrežij, za uporabljene komunikacijske protokole ob upoštevanju rezultatov odobrene razvrstitve podatkov, rezultatov ocene tveganja na področju IKT in šifriranja omrežnih povezav iz člena 6(2);

(f) zasnovo omrežij v skladu z zahtevami za varnost IKT, ki jih določi finančni subjekt, ob upoštevanju vodilnih praks za zagotavljanje zaupnosti, celovitosti in razpoložljivosti omrežja;

(g) zagotavljanjem omrežnega prometa med notranjimi omrežji ter internetom in drugimi zunanjimi povezavami;

(h) opredelitvijo vlog, odgovornosti in korakov za določitev, izvajanje, odobritev, spremembo in pregled pravil za požarni zid in filtrov povezav;

(i) izvajanjem pregledov arhitekture omrežja in varnostne zasnove omrežja enkrat letno, za mikropodjetja pa redno, da se prepoznajo morebitne ranljivosti;

(j) ukrepi za začasno osamitev podomrežij ter omrežnih komponent in naprav, kadar je potrebno;

(k) izvajanjem osnove varne konfiguracije vseh omrežnih komponent ter utrjevanjem varnosti omrežja in omrežnih naprav v skladu z morebitnimi navodili prodajalca, standardi, kot so opredeljeni v členu 2, točka 1, Uredbe (EU) št. 1025/2012, kadar je ustrezno, in vodilnimi praksami;

(l) postopki za omejitev, zaklepanje in prekinitev sistema in sej na daljavo po določenem obdobju neaktivnosti;

(m) za pogodbe o omrežnih storitvah:

  (i) opredelitvijo in določitvijo ukrepov za varnost IKT in informacijsko varnost, ravni storitev in zahtev glede upravljanja vseh omrežnih storitev;

  (ii) ali te storitve opravlja ponudnik storitev IKT znotraj skupine ali tretji ponudniki storitev IKT.

Za namene točke (h) finančni subjekti redno pregledujejo pravila za požarni zid in filtre povezav v skladu z razvrstitvijo, določeno v skladu s členom 8(1) Uredbe (EU) 2022/2554, in splošnim profilom tveganja zadevnih sistemov IKT. Za sisteme IKT, ki podpirajo kritične ali pomembne funkcije, finančni subjekti vsaj vsakih šest mesecev preverijo ustreznost obstoječih pravil za požarni zid in filtrov povezav.

Člen 14

Varovanje informacij med prenosom

1. Finančni subjekti v okviru zaščitnih ukrepov za ohranitev razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov razvijejo, dokumentirajo in izvajajo politike, postopke, protokole in orodja za zaščito informacij med prenosom. Finančni subjekti zlasti zagotovijo vse naslednje:

(a) razpoložljivost, avtentičnost, celovitost in zaupnost podatkov med prenosom v omrežju ter vzpostavitev postopkov za ocenjevanje skladnosti s temi zahtevami;

(b) preprečevanje in odkrivanje uhajanja podatkov ter varen prenos informacij med finančnim subjektom in zunanjimi strankami;

(c) da se izvajajo, dokumentirajo in redno pregledujejo zahteve glede zaupnosti ali dogovori o nerazkrivanju informacij, ki odražajo potrebe finančnega subjekta po zaščiti informacij, tako za zaposlene v finančnem subjektu kot za zaposlene v tretjih osebah.

2. Finančni subjekti politike, postopke, protokole in orodja za zaščito informacij med prenosom iz odstavka 1 oblikujejo na podlagi rezultatov odobrene razvrstitve podatkov in ocene tveganja na področju IKT.

Oddelek 7

Vodenje projektov IKT in upravljanje sprememb na področju IKT

Člen 15

Vodenje projektov IKT

1. Finančni subjekti v okviru zaščitnih ukrepov za ohranitev razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov razvijejo, dokumentirajo in izvajajo politiko vodenja projektov IKT.

2. Politika vodenja projektov IKT iz odstavka 1 določa elemente, ki zagotavljajo učinkovito vodenje projektov IKT, povezanih s pridobitvijo, vzdrževanjem in, kadar je ustrezno, razvojem sistemov IKT finančnega subjekta.

3. Politika vodenja projektov IKT iz odstavka 1 vsebuje vse naslednje:

(a) cilje projektov IKT;

(b) upravljanje projektov IKT, vključno z vlogami in odgovornostmi;

(c) načrtovanje, časovni okvir in korake projektov IKT;

(d) oceno tveganja projektov IKT;

(e) ustrezne mejnike;

(f) zahteve glede upravljanja sprememb;

(g) testiranje vseh zahtev, vključno z varnostnimi zahtevami, in zadevni postopek odobritve pri uvajanju sistema IKT v produkcijsko okolje.

4. Politika vodenja projektov IKT iz odstavka 1 zagotavlja varno izvajanje projektov IKT z zagotavljanjem potrebnih informacij in strokovnega znanja s poslovnega področja ali funkcij, na katere projekt IKT vpliva.

5. V skladu z oceno tveganja projektov IKT iz odstavka 3, točka (d), politika vodenja projektov IKT iz odstavka 1 določa, da se o vzpostavitvi in napredku projektov IKT, ki vplivajo na kritične ali pomembne funkcije finančnega subjekta, ter o tveganjih, povezanih z njimi, poroča upravljalnemu organu, kot sledi:

(a) posamično ali združeno, odvisno od pomena in obsega projektov IKT;

(b) redno in po potrebi na podlagi dogodkov.

Člen 16

Pridobitev, razvoj in vzdrževanje sistemov IKT

1. Finančni subjekti v okviru zaščitnih ukrepov za ohranitev razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov razvijejo, dokumentirajo in izvajajo politiko, ki ureja pridobitev, razvoj in vzdrževanje sistemov IKT. S to politiko se:

(a) opredeli varnostne prakse in metodologije v zvezi s pridobitvijo, razvojem in vzdrževanjem sistemov IKT;

(b) zahteva opredelitev:

(i) tehničnih specifikacij in tehničnih specifikacij IKT, kot so opredeljene v členu 2, točki 4 in 5, Uredbe (EU) št. 1025/2012;

(ii) zahtev v zvezi s pridobitvijo, razvojem in vzdrževanjem sistemov IKT, s posebnim poudarkom na zahtevah za varnost IKT in njihovi odobritvi s strani ustrezne poslovne funkcije in lastnika sredstev IKT v skladu z ureditvami notranjega upravljanja finančnega subjekta;

(c) določi ukrepe za zmanjšanje tveganja nenamerne spremembe ali namerne manipulacije sistemov IKT med razvojem, vzdrževanjem in uvajanjem teh sistemov IKT v produkcijsko okolje.

2. Finančni subjekti razvijejo, dokumentirajo in izvajajo postopek pridobitve, razvoja in vzdrževanja sistemov IKT za testiranje in odobritev vseh sistemov IKT pred njihovo uporabo in po vzdrževanju v skladu s členom 8(2), točka (b), točke (v), (vi) in (vii). Raven testiranja je sorazmerna s kritičnostjo zadevnih poslovnih postopkov in sredstev IKT. Testiranje je zasnovano tako, da se preveri, ali so novi sistemi IKT ustrezni za predvideno delovanje, vključno s kakovostjo notranje razvite programske opreme.

Centralne nasprotne stranke poleg zahtev iz prvega pododstavka v zasnovo in izvajanje testiranja iz prvega pododstavka vključijo, kot je primerno:

(a) klirinške člane in stranke;

(b) interoperabilne centralne nasprotne stranke;

(c) druge zainteresirane strani.

Centralne depotne družbe poleg zahtev iz prvega pododstavka v zasnovo in izvajanje testiranja iz prvega pododstavka vključijo, kot je primerno:

(a) uporabnike,

(b) izvajalcev ključnih javnih in drugih storitev;

(c) druge centralne depotne družbe;

(d) druge tržne infrastrukture;

(e) vse druge institucije, s katerimi so centralne depotne družbe ugotovile soodvisnosti v svoji politiki neprekinjenega poslovanja.

3. Postopek iz odstavka 2 vsebuje izvajanje pregledov izvorne kode, ki zajemajo statično in dinamično testiranje. To testiranje vključuje varnostno testiranje za sisteme in aplikacije, ki so izpostavljeni spletu, v skladu s členom 8(2), točka (b), točke (v), (vi) in (vii). Finančni subjekti:

(a) prepoznajo in analizirajo ranljivosti in nepravilnosti v izvorni kodi;

(b) sprejmejo akcijski načrt za odpravo teh ranljivosti in nepravilnosti;

(c) spremljajo izvajanje tega akcijskega načrta.

4. Postopek iz odstavka 2 vsebuje varnostno testiranje paketov programske opreme najpozneje v fazi integracije v skladu s členom 8(2), točke (b)(v), (vi) in (vii).

5. Postopek iz odstavka 2 določa, da:

(a) se v neprodukcijskih okoljih shranjujejo samo anonimizirani, psevdonimizirani ali randomizirani produkcijski podatki;

(b) morajo finančni subjekti varovati celovitost in zaupnost podatkov v neprodukcijskih okoljih.

6. Z odstopanjem od odstavka 5 se lahko s postopkom iz odstavka 2 določi, da se produkcijski podatki hranijo le za posebne primere testiranj, za omejena časovna obdobja ter po odobritvi s strani ustrezne funkcije in da se o takih primerih poroča funkciji obvladovanja tveganj na področju IKT.

7. Postopek iz odstavka 2 vključuje izvajanje kontrol za zaščito celovitosti izvorne kode sistemov IKT, ki so notranje razviti ali ki jih razvije in finančnemu subjektu zagotovi tretji ponudnik storitev IKT.

8. Postopek iz odstavka 2 določa, da je treba lastniško programsko opremo in, kadar je to izvedljivo, izvorno kodo, ki jo zagotovijo tretji ponudniki storitev IKT ali izvira iz odprtokodnih projektov, pred uvedbo v produkcijskem okolju analizirati in testirati v skladu z odstavkom 3.

9. Odstavki 1 do 8 tega člena se uporabljajo tudi za sisteme IKT, ki jih razvijejo ali upravljajo uporabniki zunaj funkcije IKT, z uporabo pristopa, ki temelji na tveganju.

Člen 17

Upravljanje sprememb na področju IKT

1. Finančni subjekti v okviru zaščitnih ukrepov za ohranitev razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov v postopke upravljanja sprememb na področju IKT iz člena 9(4), točka (e), Uredbe (EU) 2022/2554 v zvezi z vsemi spremembami komponent programske opreme, strojne opreme, strojne programske opreme ter sistemskih ali varnostnih parametrov vključijo vse naslednje elemente:

(a) preverjanje, ali so zahteve za varnost IKT izpolnjene;

(b) mehanizme za zagotavljanje neodvisnosti funkcij, ki odobrijo spremembe, in funkcij, odgovornih za zahtevanje in izvajanje teh sprememb;

(c) jasen opis vlog in odgovornosti za zagotovitev, da:

  (i) so spremembe so določene in načrtovane;

  (ii) je zasnovan ustrezen prehod;

  (iii) se spremembe nadzorovano testirajo in zaključijo;

  (iv) se učinkovito zagotavlja kakovost;

(d) dokumentiranje in sporočanje podrobnosti o spremembi, vključno z:

  (i) namenom in obsegom spremembe;

  (ii) časovnim okvirom uvedbe spremembe;

  (iii) pričakovanimi rezultati;

(e) opredelitev nadomestnih postopkov in odgovornosti, vključno s postopki in odgovornostmi za prekinitev sprememb ali obnovitev po spremembah, ki niso bile uspešno izvedene;

(f) postopke, protokole in orodja za upravljanje nujnih sprememb, ki zagotavljajo ustrezne zaščitne ukrepe;

(g) postopke za dokumentiranje, ponovno oceno, oceno in odobritev nujnih sprememb po njihovi izvedbi, vključno z obhodnimi rešitvami in popravki;

(h) opredelitev morebitnega učinka spremembe na obstoječe varnostne ukrepe na področju IKT in oceno, ali taka sprememba zahteva sprejetje dodatnih varnostnih ukrepov na področju IKT.

2. Potem ko centralne nasprotne stranke in centralne depotne družbe bistveno spremenijo svoje sisteme IKT, na njih opravijo strogo testiranje s simulacijo stresnih pogojev.

Centralne nasprotne stranke v zasnovo in izvajanje testiranja iz prvega pododstavka vključijo, kot je primerno:

(a) klirinške člane in stranke;

(b) interoperabilne centralne nasprotne stranke;

(c) druge zainteresirane strani.

Centralne depotne družbe v zasnovo in izvajanje testiranja iz prvega pododstavka vključijo, kot je primerno:

(a) uporabnike,

(b) izvajalce ključnih javnih in drugih storitev;

(c) druge centralne depotne družbe;

(d) druge tržne infrastrukture;

(e) vse druge institucije, s katerimi so centralne depotne družbe ugotovile soodvisnosti v svoji politiki neprekinjenega poslovanja na področju IKT.

Oddelek 8

Člen 18

Fizična varnost in varnost okolja

1. Finančni subjekti v okviru zaščitnih ukrepov za ohranitev razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov določijo, dokumentirajo in izvajajo politiko fizične varnosti in varnosti okolja. Finančni subjekti to politiko oblikujejo glede na okolje kibernetskih groženj v skladu z razvrstitvijo, določeno v skladu s členom 8(1) Uredbe (EU) 2022/2554, ter ob upoštevanju splošnega profila tveganja sredstev IKT in dostopnih informacijskih sredstev.

2. Politika fizične varnosti in varnosti okolja iz odstavka 1 vključuje vse naslednje:

(a) sklic na oddelek politike o nadzoru pravic upravljanja dostopa iz člena 21, prvi odstavek, točka (g);

(b) ukrepe za zaščito prostorov, podatkovnih centrov finančnega subjekta ter občutljivih namenskih območij, ki jih določi finančni subjekt, kjer so nameščena sredstva IKT in informacijska sredstva, pred napadi, nesrečami ter okoljskimi grožnjami in nevarnostmi;

(c) ukrepe za zavarovanje sredstev IKT v prostorih finančnega subjekta in zunaj njih ob upoštevanju rezultatov ocene tveganja na področju IKT v zvezi z zadevnimi sredstvi IKT;

(d) ukrepe za zagotovitev razpoložljivosti, avtentičnosti, celovitosti in zaupnosti sredstev IKT, informacijskih sredstev in naprav za nadzor fizičnega dostopa finančnega subjekta z ustreznim vzdrževanjem;

(e) ukrepe za ohranitev razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov, vključno s:

(i) politiko prazne mize za dokumente;

(ii) politiko praznega zaslona za prostore, kjer se obdelujejo informacije.

Za namene točke (b) so ukrepi za zaščito pred okoljskimi grožnjami in nevarnostmi sorazmerni s pomembnostjo prostorov, podatkovnih centrov in občutljivih namenskih območij ter kritičnostjo operacij ali sistemov IKT, ki se nahajajo v njih.

Za namene točke (c) politika fizične varnosti in varnosti okolja iz odstavka 1 vsebuje ukrepe za zagotovitev ustrezne zaščite nenadzorovanih sredstev IKT.

POGLAVJE II

Kadrovska politika in nadzor dostopa

Člen 19

Kadrovska politika

Finančni subjekti v svojo kadrovsko politiko ali druge ustrezne politike vključijo vse naslednje elemente, povezane z varnostjo IKT:

(a) opredelitev in dodelitev morebitnih posebnih odgovornosti na področju varnosti IKT;

(b) zahteve za zaposlene v finančnem subjektu in pri tretjih ponudnikih storitev IKT, ki uporabljajo sredstva IKT finančnega subjekta ali dostopajo do njih, da:

(i) so obveščeni o varnostnih politikah, postopkih in protokolih finančnega subjekta na področju IKT ter jih upoštevajo;

(ii) so seznanjeni s kanali za prijavo, ki jih je vzpostavil finančni subjekt za odkrivanje neobičajnega ravnanja, vključno s kanali za prijavo, vzpostavljenimi v skladu z Direktivo (EU) 2019/1937 Evropskega parlamenta in Sveta ([11]), kadar je ustrezno;

(iii) zaposleni ob prenehanju zaposlitve finančnemu subjektu vrnejo vsa sredstva IKT in oprijemljiva informacijska sredstva, ki jih imajo v posesti in pripadajo finančnemu subjektu.

Člen 20

Upravljanje identitete

1. Finančni subjekti v okviru svojega nadzora pravic upravljanja dostopa razvijejo, dokumentirajo in izvajajo politike in postopke upravljanja identitete, ki zagotavljajo edinstveno identifikacijo in avtentikacijo fizičnih oseb in sistemov, ki dostopajo do informacij finančnih subjektov, da se omogoči dodelitev pravic dostopa uporabnikom v skladu s členom 21.

2. Politike in postopki za upravljanje identitete iz odstavka 1 vsebujejo vse naslednje:

(a) brez poseganja v členu 21, prvi odstavek, točka (c), se vsakemu zaposlenemu v finančnem subjektu ali zaposlenemu pri tretjem ponudnikov storitev IKT, ki dostopa do informacijskih sredstev in sredstev IKT finančnega subjekta, dodeli edinstvena identiteta, ki ustreza edinstvenemu uporabniškemu računu;

(b) postopek upravljanja življenjskega cikla za identitete in račune, s katerim se upravlja ustvarjanje, spreminjanje, pregled in posodobitev, začasna deaktivacija in zaprtje vseh računov.

Za namene točke (a) finančni subjekti vodijo evidence o vseh dodelitvah identitet. Te evidence se hranijo po reorganizaciji finančnega subjekta ali po koncu pogodbenega razmerja brez poseganja v zahteve glede hrambe, določene v veljavnem pravu Unije in nacionalnem pravu.

Za namene točke (b) finančni subjekti, kadar je to izvedljivo in ustrezno, uvedejo avtomatizirane rešitve za postopek upravljanja življenjskega cikla za identitete.

Člen 21

Nadzor dostopa

Finančni subjekti v okviru svojega nadzora pravic upravljanja dostopa razvijejo, dokumentirajo in izvajajo politiko, ki vsebuje vse naslednje:

(a) dodelitev pravic dostopa do sredstev IKT na podlagi načel potrebe po seznanitvi, potrebe po uporabi in delovanja ob najmanjših privilegijih, vključno za oddaljeni dostop in dostop v sili;

(b) ločevanje nalog, zasnovano za preprečevanje neupravičenega dostopa do kritičnih podatkov ali preprečevanje dodelitve kombinacij pravic dostopa, ki se lahko uporabijo za izogibanje kontrolam;

(c) določbo o sledljivosti aktivnosti uporabniškega računa, tako da se čim bolj omeji uporaba generičnih in skupnih uporabniških računov ter zagotovi, da je uporabnike vedno mogoče prepoznati za dejanja, ki se izvajajo v sistemih IKT;

([11]) Direktiva (EU) 2019/1937 Evropskega parlamenta in Sveta z dne 23. oktobra 2019 o zaščiti oseb, ki prijavijo kršitve prava Unije (UL L 305, 26.11.2019, str. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

(d) določbo o omejitvah dostopa do sredstev IKT, ki določa kontrole in orodja za preprečevanje nepooblaščenega dostopa;

(e) postopke za upravljanje računov za podelitev, spremembo ali preklic pravic dostopa za uporabniške in generične račune, tudi za generične skrbniške račune, vključno z določbami o vsem naslednjem:

(i) dodelitvi vlog in odgovornosti za podeljevanje, pregled in preklic pravic dostopa;

(ii) dodelitvi prednostnega, nujnega in skrbniškega dostopa na podlagi potrebe po uporabi ali na priložnostni podlagi za vse sisteme IKT;

(iii) odvzemu pravic dostopa brez nepotrebnega odlašanja ob prenehanju delovnega razmerja ali ko dostop ni več potreben;

(iv) posodobitvi pravic dostopa, kadar so potrebne spremembe in vsaj enkrat letno za vse sisteme IKT, razen sistemov IKT, ki podpirajo kritične ali pomembne funkcije, in vsaj vsakih šest mesecev za sisteme IKT, ki podpirajo kritične ali pomembne funkcije;

(f) metode avtentikacije, vključno z vsem naslednjim:

(i) uporabo metod avtentikacije, ki so sorazmerne z razvrstitvijo, določeno v skladu s členom 8(1) Uredbe (EU) 2022/2554, in splošnim profilom tveganja sredstev IKT ter ob upoštevanju vodilnih praks;

(ii) uporabo metod močne avtentikacije za oddaljeni dostop do omrežja finančnega subjekta, za prednostni dostop, za dostop do sredstev IKT, ki podpirajo kritične ali pomembne funkcije, ali sredstev IKT, ki so javno dostopna, v skladu z vodilnimi praksami in tehnikami;

(g) ukrepe za nadzor fizičnega dostopa, ki vključujejo:

(i) identifikacijo in evidentiranje fizičnih oseb, ki so pooblaščene za dostop do prostorov, podatkovnih centrov in občutljivih namenskih območij, ki jih določi finančni subjekt, kjer so nameščena sredstva IKT in informacijska sredstva;

(ii) podelitev pravic fizičnega dostopa do ključnih sredstev IKT samo pooblaščenim osebam v skladu z načelom potrebe po seznanitvi in načelom delovanja ob najmanjših privilegijih ter na priložnostni podlagi;

(iii) spremljanje fizičnega dostopa do prostorov, podatkovnih centrov in občutljivih namenskih območij, ki jih določi finančni subjekt, kjer so nameščena sredstva IKT in informacijska sredstva ali oboje;

(iv) pregled pravic fizičnega dostopa, da se zagotovi takojšen preklic nepotrebnih pravic dostopa.

Za namene točke (e)(i) finančni subjekti določijo obdobje hrambe, pri čemer upoštevajo poslovne cilje in cilje glede informacijske varnosti, razloge za zabeleženje dogodka v dnevnike in rezultate ocene tveganja na področju IKT.

Za namene točke (e)(ii) finančni subjekti, kadar je to mogoče, uporabljajo namenske račune za izvajanje skrbniških nalog v zvezi s sistemi IKT. Kadar je to izvedljivo in primerno, finančni subjekti uvedejo avtomatizirane rešitve za upravljanje prednostnega dostopa.

Za namene točke (g)(i) sta identifikacija in evidentiranje sorazmerna s pomembnostjo prostorov, podatkovnih centrov in občutljivih namenskih območij ter kritičnostjo operacij ali sistemov IKT, ki se nahajajo v njih.

Za namene točke (g)(iii) je spremljanje sorazmerno z razvrstitvijo, določeno v skladu s členom 8(1) Uredbe (EU) 2022/2554, in kritičnostjo območja, do katerega se dostopa.

POGLAVJE III

ODKRIVANJE INCIDENTOV, POVEZANIH Z IKT, IN ODZIVANJE NANJE

Člen 22

Politika obvladovanja incidentov, povezanih z IKT

Finančni subjekti v okviru mehanizmov za odkrivanje neobičajnega ravnanja, vključno s težavami v zvezi z zmogljivostjo omrežja IKT in incidenti, povezanimi z IKT, razvijejo, dokumentirajo in izvajajo politiko glede incidentov, povezanih z IKT, s katero:

(a) dokumentirajo postopek obvladovanja incidentov, povezanih z IKT, iz člena 17 Uredbe (EU) 2022/2554;

(b) pripravijo seznam ustreznih stikov z notranjimi funkcijami in zunanjimi deležniki, ki so neposredno vključeni v varnost delovanja IKT, vključno z:

  (i) odkrivanjem in spremljanjem kibernetskih groženj;

  (ii) odkrivanjem neobičajnega ravnanja;

  (iii) upravljanjem ranljivosti;

(c) vzpostavijo, izvajajo in upravljajo tehnične, organizacijske in operativne mehanizme za podporo postopku obvladovanja incidentov, povezanih z IKT, vključno z mehanizmi, ki omogočajo takojšnje odkrivanje neobičajnega ravnanja in vedenja v skladu s členom 23 te uredbe;

(d) hranijo vse dokaze v zvezi z incidenti, povezanimi z IKT, za obdobje, ki ni daljše, kot je potrebno za namene, za katere se zbirajo podatki, sorazmerno s kritičnostjo prizadetih poslovnih funkcij, podpornih postopkov ter sredstev IKT in informacijskih sredstev, v skladu s členom 15 Delegirane uredbe Komisije (EU) 2024/1772 ([12]), in vsemi veljavnimi zahtevami glede hrambe v skladu s pravom Unije;

(e) vzpostavijo in izvajajo mehanizme za analizo pomembnih ali ponavljajočih se incidentov, povezanih z IKT, ter vzorcev v številu in pojavljanju incidentov, povezanih z IKT.

Za namene točke (d) finančni subjekti varno hranijo dokaze iz navedene točke.

Člen 23

Odkrivanje neobičajnega ravnanja ter merila za odkrivanje incidentov, povezanih z IKT, in odzivanje nanje

1. Finančni subjekti določijo jasne vloge in odgovornosti za učinkovito odkrivanje incidentov, povezanih z IKT, ter neobičajnega ravnanja in odzivanje nanje.

2. Mehanizem za takojšnje odkrivanje neobičajnega ravnanja, vključno s težavami v zvezi z zmogljivostjo omrežja IKT in incidenti, povezanimi z IKT, iz člena 10(1) Uredbe (EU) 2022/2554, finančnim subjektom omogoča, da:

(a) zbirajo, spremljajo in analizirajo vse naslednje:

  (i) notranje in zunanje dejavnike, vključno z vsaj dnevniki, zbranimi v skladu s členom 12 te uredbe, informacijami iz poslovnih funkcij in funkcij IKT ter vsemi težavami, ki jih sporočijo uporabniki finančnega subjekta;

  (ii) morebitne notranje in zunanje kibernetske grožnje, pri čemer upoštevajo scenarije, ki jih običajno uporabljajo akterji groženj, in scenarije, ki temeljijo na obveščevalnih podatkih o grožnjah;

([12]) Delegirana uredba Komisije (EU) 2024/1772 z dne 13. Marca 2024 o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi o določitvi meril za razvrščanje incidentov, povezanih z IKT, in kibernetskih groženj, ter pragov pomembnosti in podrobnosti poročil o večjih incidentih (UL L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(iii) obvestila o incidentih, povezanih z IKT, s strani tretjega ponudnika storitev IKT finančnega subjekta, ki se odkrijejo v sistemih in omrežjih IKT tretjega ponudnika storitev IKT in lahko vplivajo na finančni subjekt;

(b) prepoznajo neobičajno ravnanje in vedenje ter uporabljajo orodja, ki ustvarjajo opozorila o neobičajnem ravnanju in vedenju, vsaj za sredstva IKT in informacijska sredstva, ki podpirajo kritične ali pomembne funkcije;

(c) dajejo prednost opozorilom iz točke (b), da se omogoči upravljanje odkritih incidentov, povezanih z IKT, v pričakovanem času razreševanja, kot ga določijo finančni subjekti, tako med delovnim časom kot zunaj njega;

(d) samodejno ali ročno evidentirajo, analizirajo in ovrednotijo vse pomembne informacije o vsem neobičajnem ravnanju in vedenju.

Za namene točke (b) orodja iz navedene točke vsebujejo orodja, ki zagotavljajo avtomatizirana opozorila na podlagi vnaprej določenih pravil za prepoznavanje nepravilnosti, ki vplivajo na popolnost in celovitost virov podatkov ali zbiranja dnevnikov.

3. Finančni subjekti zaščitijo vsako evidenco neobičajnega ravnanja pred nedovoljenim spreminjanjem in nepooblaščenim dostopom v mirovanju, med prenosom in, kadar je primerno, v uporabi.

4. Finančni subjekti v dnevnikih zabeležijo vse ustrezne informacije za vsako odkrito neobičajno ravnanje, ki omogočajo:

(a) opredelitev datuma in časa pojava neobičajnega ravnanja;

(b) opredelitev datuma in časa odkritja neobičajnega ravnanja;

(c) opredelitev vrste neobičajnega ravnanja.

5. Finančni subjekti upoštevajo vsa naslednja merila za sprožitev postopkov odkrivanja incidentov, povezanih z IKT, in odzivanja nanje iz člena 10(2) Uredbe (EU) 2022/2554:

(a) znake, da se je v sistemu ali omrežju IKT morda izvajala zlonamerna dejavnost ali da sta bila tak sistem ali omrežje IKT morda ogrožena;

(b) izgube podatkov, odkrite v zvezi z razpoložljivostjo, avtentičnostjo, celovitostjo in zaupnostjo podatkov;

(c) odkrit škodljiv vpliv na transakcije in poslovanje finančnega subjekta;

(d) nerazpoložljivost sistemov in omrežij IKT.

6. Za namene odstavka 5 finančni subjekti upoštevajo tudi kritičnost prizadetih storitev.

POGLAVJE IV

Upravljanje neprekinjenega poslovanja na področju IKT

Člen 24

Komponente politike neprekinjenega poslovanja na področju IKT

1. Finančni subjekti v svojo politiko neprekinjenega poslovanja na področju IKT iz člena 11(1) Uredbe (EU) 2022/2554 vključijo vse naslednje:

(a) opis:

(i) ciljev politike neprekinjenega poslovanja na področju IKT, vključno z medsebojnim razmerjem med neprekinjenim poslovanjem na področju IKT in splošnim neprekinjenim poslovanjem ter ob upoštevanju rezultatov analize vpliva na poslovanje iz člena 11(5) Uredbe (EU) 2022/2554;

(ii) obsega ureditev, načrtov, postopkov in mehanizmov neprekinjenega poslovanja na področju IKT, vključno z omejitvami in izključitvami;

(iii) časovnega okvira, ki ga zajemajo ureditve, načrti, postopki in mehanizmi neprekinjenega poslovanja na področju IKT;

(iv) meril za aktivacijo in deaktivacijo načrtov neprekinjenega poslovanja na področju IKT, načrtov odzivanja in okrevanja IKT ter načrtov obveščanja o kriznih razmerah;

(b) določbe o:

(i) upravljanju in organizaciji izvajanja politike neprekinjenega poslovanja na področju IKT, vključno z vlogami, odgovornostmi in postopki prenosa na višjo raven, ki zagotavljajo, da so na voljo zadostni viri;

(ii) usklajenosti načrtov neprekinjenega poslovanja na področju IKT in splošnih načrtov neprekinjenega poslovanja vsaj v zvezi z vsem naslednjim:

(1) potencialnimi scenariji odpovedi, vključno s scenariji iz člena 26(2) te uredbe;

(2) cilji obnovitve, ki določajo, da mora biti finančni subjekt sposoben po motnjah obnoviti delovanje svojih kritičnih ali pomembnih funkcij v okviru ciljev glede časa okrevanja in točke obnovitve;

(iii) razvoju načrtov neprekinjenega poslovanja na področju IKT za resne motnje poslovanja v okviru teh načrtov in prednostnem razvrščanju ukrepov za neprekinjeno poslovanje na področju IKT z uporabo pristopa, ki temelji na tveganju;

(iv) razvoju, testiranju in pregledu načrtov odzivanja in okrevanja IKT v skladu s členoma 25 in 26 te uredbe;

(v) pregledu učinkovitosti izvedenih ureditev, načrtov, postopkov in mehanizmov neprekinjenega poslovanja na področju IKT v skladu s členom 26 te uredbe;

(vi) usklajenosti politike neprekinjenega poslovanja na področju IKT s:

(1) politiko obveščanja iz člena 14(2) Uredbe (EU) 2022/2554;

(2) komunikacijskimi ukrepi in ukrepi za obvladovanje kriz iz člena 11(2), točka (e), Uredbe (EU) 2022/2554.

2. Poleg zahtev iz odstavka 1 centralne nasprotne stranke zagotovijo, da njihova politika neprekinjenega poslovanja na področju IKT:

(a) vsebuje najdaljši čas okrevanja za njihove kritične funkcije, ki ni daljši od dveh ur;

(b) upošteva zunanje povezave in soodvisnosti znotraj finančnih infrastruktur, vključno z mesti trgovanja, za katere kliring opravlja centralna nasprotna stranka, sistemi poravnave vrednostnih papirjev in plačilnimi sistemi ter kreditnimi institucijami, ki jih uporablja centralna nasprotna stranka ali povezana centralna nasprotna stranka;

(c) zahteva, da so vzpostavljene ureditve, da se:

(i) zagotovi neprekinjenost kritičnih ali pomembnih funkcij centralne nasprotne stranke na podlagi scenarijev nesreč;

(ii) vzdržuje sekundarna lokacija za obdelavo, ki lahko zagotovi neprekinjenost kritičnih ali pomembnih funkcij centralne nasprotne stranke, enako kot primarna lokacija;

(iii) vzdržuje sekundarna lokacija poslovanja ali je možen takojšen dostop do nje, da lahko zaposleni zagotovijo neprekinjenost storitve, če primarna lokacija poslovanja ni na voljo;

(iv) upošteva potreba po dodatnih lokacijah za obdelavo, zlasti če razlika med profiloma tveganja primarne in sekundarne lokacije ne zagotavlja zadostne gotovosti, da bodo cilji neprekinjenega poslovanja centralne nasprotne stranke doseženi v vseh scenarijih.

Za namene točke (a) centralne nasprotne stranke zaključijo postopke in plačila ob koncu dneva ob zahtevanem času in na zahtevani dan v vseh okoliščinah.

Za namene točke (c)(i) ureditve iz navedene točke obravnavajo razpoložljivost ustreznih človeških virov, najdaljši čas izpada kritičnih funkcij ter samodejni preklop in obnovitev na sekundarni lokaciji.

Za namene točke (c)(ii) ima sekundarna lokacija za obdelavo iz navedene točke geografski profil tveganja, ki se razlikuje od profila primarne lokacije.

3. Poleg zahtev iz odstavka 1 centralne depotne družbe zagotovijo, da njihova politika neprekinjenega poslovanja na področju IKT:

(a) upošteva vse povezave in soodvisnosti z uporabniki, izvajalci ključnih javnih in drugih storitev, drugimi centralnimi depotnimi družbami in drugimi tržnimi infrastrukturami;

(b) zahteva, da njene ureditve neprekinjenega poslovanja na področju IKT zagotovijo, da cilj glede časa okrevanja za njihove kritične ali pomembne funkcije ni daljši od dveh ur.

4. Poleg zahtev iz odstavka 1 mesta trgovanja zagotovijo, da njihova politika neprekinjenega poslovanja na področju IKT zagotavlja, da:

(a) se lahko trgovanje ponovno vzpostavi v dveh urah ali približno dveh urah od incidenta, ki povzroči motnjo;

(b) je največja količina podatkov, ki se lahko izgubijo iz katere koli storitve IT mesta trgovanja po incidentu, ki povzroči motnjo, blizu nič.

Člen 25

Testiranje načrtov neprekinjenega poslovanja na področju IKT

1. Finančni subjekti pri testiranju načrtov neprekinjenega poslovanja na področju IKT v skladu s členom 11(6) Uredbe (EU) 2022/2554 upoštevajo svojo analizo vpliva na poslovanje in oceno tveganja na področju IKT iz člena 3(1), točka (b), te uredbe.

2. Finančni subjekti s testiranjem svojih načrtov neprekinjenega poslovanja na področju IKT iz odstavka 1 ocenijo, ali so sposobni zagotoviti neprekinjenost kritičnih ali pomembnih funkcij finančnega subjekta. To testiranje:

(a) se izvede na podlagi testnih scenarijev, ki simulirajo morebitne motnje, vključno z ustreznim nizom resnih, vendar verjetnih scenarijev;

(b) vključuje testiranje storitev IKT, ki jih opravljajo tretji ponudniki storitev IKT, kadar je ustrezno;

(c) za finančne subjekte, ki niso mikropodjetja, kot je navedeno v členu 11(6), drugi pododstavek, Uredbe (EU) 2022/2554, vključuje scenarije preklopa s primarne infrastrukture IKT na redundantno zmogljivost, rezervne sisteme in redundantne obrate;

(d) je zasnovano tako, da izpodbija predpostavke, na katerih temeljijo načrti neprekinjenega poslovanja, vključno z ureditvami upravljanja in načrti obveščanja o kriznih razmerah;

(e) vsebuje postopke za preverjanje sposobnosti zaposlenih v finančnih subjektih, tretjih ponudnikov storitev IKT, sistemov IKT in storitev IKT, da se ustrezno odzovejo na scenarije, ki se ustrezno upoštevajo v skladu s členom 26(2).

Za namene točke (a) finančni subjekti v testiranje vedno vključijo scenarije, ki se upoštevajo pri pripravi načrtov neprekinjenega poslovanja.

Za namene točke (b) finančni subjekti ustrezno upoštevajo scenarije, povezane z insolventnostjo ali prenehanjem delovanja tretjih ponudnikov storitev IKT ali povezane s političnimi tveganji v jurisdikcijah tretjih ponudnikov storitev IKT, kadar je to ustrezno.

Za namene točke (c) se s testiranjem preveri, ali lahko vsaj kritične ali pomembne funkcije ustrezno delujejo dovolj dolgo in ali je mogoče obnoviti normalno delovanje.

3. Poleg zahtev iz odstavka 2 centralne nasprotne stranke v testiranje svojih načrtov neprekinjenega poslovanja na področju IKT iz odstavka 1 vključijo:

(a) klirinške člane;

(b) zunanje ponudnike;

(c) ustrezne institucije v finančni infrastrukturi, s katerimi so centralne nasprotne stranke ugotovile soodvisnosti v svojih politikah neprekinjenega poslovanja.

4. Poleg zahtev iz odstavka 2 centralne depotne družbe v testiranje svojih načrtov neprekinjenega poslovanja na področju IKT iz odstavka 1 vključijo, kot je ustrezno:

(a) uporabnike centralnih depotnih družb;

(b) izvajalce ključnih javnih in drugih storitev;

(c) druge centralne depotne družbe;

(d) druge tržne infrastrukture;

(e) vse druge institucije, s katerimi so centralne depotne družbe ugotovile soodvisnosti v svoji politiki neprekinjenega poslovanja.

5. Finančni subjekti dokumentirajo rezultate testiranja iz odstavka 1. Vse prepoznane pomanjkljivosti na podlagi tega testiranja se analizirajo, odpravijo in sporočijo upravljalnemu organu.

Člen 26

Načrti odzivanja in okrevanja IKT

1. Finančni subjekti pri pripravi načrtov odzivanja in okrevanja IKT iz člena 11(3) Uredbe (EU) 2022/2554 upoštevajo rezultate svoje analize vpliva na poslovanje. Načrti odzivanja in okrevanja IKT:

(a) določajo pogoje za njihovo aktivacijo ali deaktivacijo in vse izjeme za tako aktivacijo ali deaktivacijo;

(b) opisujejo, katere ukrepe je treba sprejeti za zagotovitev razpoložljivosti, celovitosti, neprekinjenosti in okrevanja vsaj sistemov in storitev IKT, ki podpirajo kritične ali pomembne funkcije finančnega subjekta;

(c) so oblikovani tako, da izpolnjujejo cilje obnovitve poslovanja finančnih subjektov;

(d) so dokumentirani in dani na voljo zaposlenim, vključenim v izvajanje načrtov odzivanja in okrevanja IKT, ter so zlahka dostopni v izrednih razmerah;

(e) določajo kratkoročne in dolgoročne možnosti okrevanja, vključno z delnim okrevanjem sistemov;

(f) določajo cilje načrtov odzivanja in okrevanja IKT ter pogoje, da se izvedba teh načrtov razglasi za uspešno.

Za namene točke (d) finančni subjekti jasno opredelijo vloge in odgovornosti.

2. V načrtih odzivanja in okrevanja IKT iz odstavka 1 se opredelijo ustrezni scenariji, vključno s scenariji resnih motenj poslovanja in povečane verjetnosti pojava motnje. V teh načrtih se razvijejo scenariji, ki temeljijo na trenutnih informacijah o grožnjah in izkušnjah, pridobljenih pri preteklih pojavov motenj poslovanja. Finančni subjekti ustrezno upoštevajo vse naslednje scenarije:

(a) kibernetske napade in preklope med primarno infrastrukturo IKT in redundantno zmogljivostjo, rezervnimi sistemi in redundantnimi obrati;

(b) scenarije, v katerih se kakovost zagotavljanja kritične ali pomembne funkcije poslabša na nesprejemljivo raven ali odpove in se ustrezno upošteva morebitni vpliv insolventnosti ali drugih vrst prenehanja delovanja katerega koli zadevnega tretjega ponudnika storitev IKT;

(c) delno ali popolno neuporabnost prostorov, vključno s pisarniškimi in poslovnimi prostori, ter podatkovnih centrov;

(d) znatno odpoved sredstev IKT ali komunikacijske infrastrukture;

(e) nerazpoložljivost kritičnega števila zaposlenih ali zaposlenih, odgovornih za zagotavljanje neprekinjenega delovanja;

(f) vpliv dogodkov, povezanih s podnebnimi spremembami in degradacijo okolja, naravnih nesreč, pandemij in fizičnih napadov, vključno z vdori in terorističnimi napadi;

(g) notranje napade;

(h) politično in socialno nestabilnost, tudi, kjer je ustrezno, v jurisdikciji tretjega ponudnika storitev IKT in na lokaciji, kjer se podatki shranjujejo in obdelujejo;

(i) razširjene izpade električne energije.

3. Kadar primarni ukrepi okrevanja kratkoročno morda niso izvedljivi zaradi stroškov, tveganj, logistike ali nepredvidenih okoliščin, se v načrtih odzivanja in okrevanja IKT iz odstavka 1 preučijo alternativne možnosti.

4. Finančni subjekti v okviru načrtov odzivanja in okrevanja IKT iz odstavka 1 preučijo in izvajajo ukrepe za neprekinjenost, da bi ublažili prenehanje delovanja tretjih ponudnikov storitev IKT, ki podpirajo kritične ali pomembne funkcije finančnega subjekta.

POGLAVJE V

Poročilo o pregledu okvira za obvladovanje tveganj na področju IKT

Člen 27

Oblika in vsebina poročila o pregledu okvira za obvladovanje tveganj na področju IKT

1. Finančni subjekti predložijo poročilo o pregledu okvira za obvladovanje tveganj na področju IKT iz člena 6(5) Uredbe (EU) 2022/2554 v elektronski obliki, ki omogoča iskanje.

2. Finančni subjekti v poročilo iz odstavka 1 vključijo vse naslednje informacije:

(a) uvodni del, v katerem:

(i) je jasno opredeljen finančni subjekt, ki je predmet poročila, in po potrebi opisana struktura njegove skupine;

(ii) je opisan kontekst poročila v smislu narave, obsega in kompleksnosti storitev, dejavnosti in poslovanja finančnega subjekta, njegove organizacije, identificiranih kritičnih funkcij, strategije, velikih tekočih projektov ali dejavnosti, odnosov in njegove odvisnosti od notranjih in pogodbenih storitev in sistemov IKT ali posledic, ki bi jih imela popolna izguba ali resna degradacija takih sistemov v smislu kritičnih ali pomembnih funkcij in učinkovitosti trga;

(iii) so povzete večje spremembe okvira za obvladovanje tveganj na področju IKT od prejšnjega predloženega poročila;

(iv) je predstavljen povzetek trenutnega in kratkoročnega profila tveganja na področju IKT, okolja groženj, ocenjene učinkovitosti njegovih kontrol in varnostnega stanja finančnega subjekta;

(b) datum, ko je upravljalni organ finančnega subjekta odobril poročilo;

(c) opis razloga za pregled okvira za obvladovanje tveganj na področju IKT v skladu s členom 6(5) Uredbe (EU) 2022/2554;

(d) začetni in končni datum obdobja pregleda;

(e) navedbo funkcije, odgovorne za pregled;

(f) opis večjih sprememb in izboljšav okvira za obvladovanje tveganj na področju IKT od prejšnjega pregleda;

(g) povzetek ugotovitev pregleda ter podrobno analizo in oceno resnosti slabosti, pomanjkljivosti in vrzeli v okviru za obvladovanje tveganj na področju IKT v obdobju pregleda;

(h) opis ukrepov za odpravo identificiranih slabosti, pomanjkljivosti in vrzeli, vključno z vsem naslednjim:

(i) povzetkom ukrepov, sprejetih za sanacijo identificiranih slabosti, pomanjkljivosti in vrzeli;

(ii) pričakovanim datumom za izvedbo ukrepov in datumi, povezanimi z notranjo kontrolo izvajanja, vključno z informacijami o napredku pri izvajanju teh ukrepov na datum priprave poročila, pri čemer se pojasni, kadar je ustrezno, ali obstaja tveganje, da roki ne bodo upoštevani;

(iii) orodji, ki se bodo uporabila, in opredelitvijo funkcije, odgovorne za izvajanje ukrepov, z navedbo, ali so orodja in funkcije notranji ali zunanji;

(iv) opisom učinka sprememb, predvidenih v ukrepih, na proračunske, človeške in materialne vire finančnega subjekta, vključno z viri, namenjenimi izvajanju morebitnih popravnih ukrepov;

(v) informacijami o postopku obveščanja pristojnega organa, kadar je primerno;

(vi) če identificirane slabosti, pomanjkljivosti ali vrzeli niso predmet popravnih ukrepov, podrobno razlago meril, uporabljenih za analizo učinka teh slabosti, pomanjkljivosti ali vrzeli za oceno povezanega preostalega tveganja na področju IKT, in meril, uporabljenih za sprejetje povezanega preostalega tveganja;

(i) informacije o načrtovanem nadaljnjem razvoju okvira za obvladovanje tveganj na področju IKT;

(j) sklepe, dosežene na podlagi pregleda okvira za obvladovanje tveganj na področju IKT;

(k) informacije o preteklih pregledih, vključno s:

(i) seznamom dosedanjih preteklih pregledov;

(ii) kadar je ustrezno, stanjem izvajanja popravnih ukrepov, določenih v zadnjem poročilu;

(iii) če so se v preteklih pregledih predlagani popravni ukrepi izkazali za neučinkovite ali so povzročili nepričakovane izzive, opisom, kako bi bilo te popravne ukrepe mogoče izboljšati, ali opisom teh nepričakovanih izzivov;

(l) vire informacij, uporabljene pri pripravi poročila, vključno z vsem naslednjim:

(i) za finančne subjekte, ki niso mikropodjetja, iz člena 6(6) Uredbe (EU) 2022/2554 rezultati notranjih revizij;

(ii) rezultati ocen skladnosti;

(iii) rezultati testiranja digitalne operativne odpornosti in, kadar je ustrezno, rezultati naprednega testiranja orodij, sistemov in postopkov IKT, ki temelji na penetracijskem testiranju, na podlagi analize groženj;

(iv) zunanjimi viri.

Za namene točke (c), kadar se je pregled začel po nadzorniških navodilih ali sklepih, ki izhajajo iz ustreznih postopkov testiranja ali revizije digitalne operativne odpornosti, poročilo vsebuje izrecne sklice na taka navodila ali sklepe, kar omogoča opredelitev razloga za začetek pregleda. Kadar se je pregled začel po incidentih, povezanih z IKT, poročilo vsebuje seznam vseh incidentov, povezanih z IKT, skupaj z analizo temeljnih vzrokov incidentov.

Za namene točke (f) opis vsebuje analizo učinka sprememb na strategijo finančnega subjekta za digitalno operativno odpornost, na okvir notranjega nadzora finančnega subjekta na področju IKT in na upravljanje finančnega subjekta z obvladovanjem tveganj na področju IKT.

NASLOV III

POENOSTAVLJEN OKVIR ZA OBVLADOVANJE TVEGANJ NA PODROČJU IKT ZA FINANČNE SUBJEKTE IZ ČLENA 16(1) UREDBE (EU) 2022/2554

POGLAVJE I

POENOSTAVLJEN OKVIR ZA OBVLADOVANJE TVEGANJ NA PODROČJU IKT

Člen 28

Upravljanje in organizacija

1. Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 imajo vzpostavljen okvir notranjega upravljanja in nadzora, ki zagotavlja učinkovito in skrbno obvladovanje tveganj na področju IKT, da se doseže visoka raven digitalne operativne odpornosti.

2. Finančni subjekti iz odstavka 1 kot del svojega poenostavljenega okvira za obvladovanje tveganj na področju IKT zagotovijo, da njihov upravljalni organ:

(a) nosi splošno odgovornost za zagotavljanje, da poenostavljen okvir za obvladovanje tveganj na področju IKT omogoča doseganje poslovne strategije finančnega subjekta v skladu z nagnjenostjo tega finančnega subjekta k prevzemanju tveganj, in zagotavlja, da se v tem kontekstu upošteva tveganje na področju IKT;

(b) določi jasne vloge in odgovornosti za vse naloge v zvezi z IKT;

(c) določi cilje glede informacijske varnosti in zahteve v zvezi z IKT;

(d) odobri, nadzoruje in redno pregleduje:

(i) razvrstitev informacijskih sredstev finančnega subjekta iz člena 30(1) te uredbe, seznam glavnih identificiranih tveganj ter analizo vpliva na poslovanje in s tem povezane politike;

(ii) načrte neprekinjenega poslovanja finančnega subjekta ter ukrepe za odzivanje in okrevanje iz člena 16(1), točka (f), Uredbe (EU) 2022/2554;

(e) dodeli in vsaj enkrat letno pregleda proračun, ki je potreben, da lahko finančni subjekt izpolnjuje potrebe po digitalni operativni odpornosti v zvezi z vsemi vrstami virov, vključno z ustreznimi programi ozaveščanja o varnosti IKT in usposabljanjem o digitalni operativni odpornosti ter spretnostmi na področju IKT za vse zaposlene;

(f) določi in izvaja politike in ukrepe iz poglavij I, II in III tega naslova za identifikacijo, oceno in obvladovanje tveganja na področju IKT, ki mu je izpostavljen finančni subjekt;

(g) opredeli in izvaja postopke, protokole in orodja IKT, ki so potrebni za zaščito vseh informacijskih sredstev in sredstev IKT;

(h) zagotovi, da zaposleni v finančnem subjektu obnavljajo zadostno znanje in spretnosti, da lahko razumejo in ocenijo tveganje na področju IKT ter njegov učinek na poslovanje finančnega subjekta, in sicer sorazmerno s tveganjem na področju IKT, ki se obvladuje;

(i) določi ureditve poročanja, vključno s pogostostjo, obliko in vsebino poročanja upravljalnemu organu o informacijski varnosti in digitalni operativni odpornosti.

3. Finančni subjekti iz odstavka 1 lahko v skladu s sektorskim pravom Unije in nacionalnim sektorskim pravom naloge preverjanja skladnosti z zahtevami glede obvladovanja tveganj na področju IKT oddajo v zunanje izvajanje ponudnikom storitev IKT znotraj skupine ali tretjim ponudnikom storitev IKT. V primerih tovrstnega zunanjega izvajanja finančni subjekti ostanejo v celoti odgovorni za preverjanje skladnosti z zahtevami glede obvladovanja tveganj na področju IKT.

4. Finančni subjekti iz odstavka 1 zagotovijo ustrezno ločevanje in neodvisnost nadzornih funkcij in funkcij notranje revizije.

5. Finančni subjekti iz odstavka 1 zagotovijo, da revizorji opravijo notranjo revizijo njihovega poenostavljenega okvira za obvladovanje tveganj na področju IKT, in sicer v skladu z revizijskim načrtom finančnih subjektov. Revizorji imajo zadostno znanje, spretnosti in strokovno znanje v zvezi s tveganji na področju IKT ter so neodvisni. Pogostost in osredotočenost revizij na področju IKT sta sorazmerni s tveganjem na področju IKT, s katerim se sooča finančni subjekt.

6. Finančni subjekti iz odstavka 1 na podlagi rezultatov revizije iz odstavka 5 zagotovijo pravočasno preverjanje in sanacijo na podlagi ključnih ugotovitev revizije na področju IKT.

Člen 29

Politika in ukrepi informacijske varnosti

1. Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo politiko informacijske varnosti v kontekstu poenostavljenega okvira za obvladovanje tveganj na področju IKT. Ta politika informacijske varnosti določa načela in pravila na visoki ravni za zaščito zaupnosti, celovitosti, razpoložljivosti in avtentičnosti podatkov in storitev, ki jih zagotavljajo ti finančni subjekti.

2. Finančni subjekti iz odstavka 1 na podlagi svoje politike informacijske varnosti iz odstavka 1 vzpostavijo in izvajajo varnostne ukrepe na področju IKT za zmanjšanje svoje izpostavljenosti tveganju na področju IKT, vključno z blažilnimi ukrepi, ki jih izvajajo tretji ponudniki storitev IKT.

Varnostni ukrepi na področju IKT vključujejo vse ukrepe iz členov 30 do 38.

Člen 30

Razvrstitev informacijskih sredstev in sredstev IKT

1. Kot del poenostavljenega okvira za obvladovanje tveganj na področju IKT iz člena 16(1), točka (a), Uredbe (EU) 2022/2554 finančni subjekti iz odstavka 1 navedenega člena identificirajo, razvrstijo in dokumentirajo vse kritične ali pomembne funkcije, informacijska sredstva in sredstva IKT, ki jih podpirajo, ter njihove soodvisnosti. Finančni subjekti po potrebi pregledajo to identifikacijo in razvrstitev.

2. Finančni subjekti iz odstavka 1 identificirajo vse kritične ali pomembne funkcije, ki jih podpirajo tretji ponudniki storitev IKT.

Člen 31

Obvladovanje tveganj na področju IKT

1. Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 v svoj poenostavljen okvir za obvladovanje tveganj na področju IKT vključijo vse naslednje:

(a) določitev tolerančnih ravni tveganja za tveganje na področju IKT v skladu z nagnjenostjo finančnega subjekta k prevzemanju tveganj;

(b) identifikacijo in oceno tveganj na področju IKT, ki jim je finančni subjekt izpostavljen;

(c) specifikacijo blažilnih strategij vsaj za tveganja na področju IKT, ki niso v mejah tolerančnih ravni tveganja finančnega subjekta;

(d) spremljanje učinkovitosti blažilnih strategij iz točke (c);

(e) identifikacijo in oceno vseh tveganj za varnost IKT in informacijsko varnost, ki so posledica kakršne koli večje spremembe sistema IKT ali storitev, procesov ali postopkov IKT ter rezultatov testiranja varnosti IKT, in po vsakem večjem incidentu, povezanem z IKT.

2. Finančni subjekti iz odstavka 1 redno opravljajo in dokumentirajo oceno tveganja na področju IKT, in sicer sorazmerno s profilom tveganja finančnih subjektov na področju IKT.

3. Finančni subjekti iz odstavka 1 stalno spremljajo grožnje in ranljivosti, ki so pomembne za njihove kritične ali pomembne funkcije ter informacijska sredstva in sredstva IKT, ter redno pregledujejo scenarije tveganja, ki vplivajo na te kritične ali pomembne funkcije.

4. Finančni subjekti iz odstavka 1 določijo mejne vrednosti opozarjanja in merila za sprožitev in začetek izvajanja postopkov odzivanja na incidente, povezane z IKT.

Člen 32

Fizična varnost in varnost okolja

1. Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 opredelijo in izvajajo ukrepe fizične varnosti, oblikovane na podlagi okolja groženj in v skladu z razvrstitvijo iz člena 30(1) te uredbe, splošnim profilom tveganja sredstev IKT in dostopnimi informacijskimi sredstvi.

2. Ukrepi iz odstavka 1 ščitijo prostore finančnih subjektov in, kadar je ustrezno, podatkovne centre finančnih subjektov, kjer so nameščena sredstva IKT in informacijska sredstva, pred nepooblaščenim dostopom, napadi in nesrečami ter pred okoljskimi grožnjami in nevarnostmi.

3. Zaščita pred okoljskimi grožnjami in nevarnostmi je sorazmerna s pomembnostjo zadevnih prostorov in, kadar je ustrezno, podatkovnih centrov ter kritičnostjo operacij ali sistemov IKT, ki se nahajajo v njih.

POGLAVJE II

DODATNI ELEMENTI SISTEMOV, PROTOKOLOV IN ORODIJ ZA ZMANJŠANJE UČINKA TVEGANJA NA PODROČJU IKT NA NAJNIŽJO MOŽNO RAVEN

Člen 33

Nadzor dostopa

Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo postopke za nadzor logičnega in fizičnega dostopa ter te postopke izvršujejo, spremljajo in redno pregledujejo. Ti postopki vsebujejo naslednje elemente nadzora logičnega in fizičnega dostopa:

(a) pravice dostopa do informacijskih sredstev, sredstev IKT in njihovih podprtih funkcij ter do kritičnih lokacij delovanja finančnega subjekta se upravljajo na podlagi potrebe po seznanitvi, potrebe po uporabi in delovanja ob najmanjših privilegijih, vključno za oddaljeni dostop in dostop v sili;

(b) sledljivost aktivnosti uporabniškega računa, ki zagotavlja, da je za dejanja, ki se izvajajo v sistemih IKT, mogoče prepoznati uporabnike;

(c) postopke za upravljanje računov za podelitev, spremembo ali preklic pravic dostopa za uporabniške in generične račune, tudi za generične skrbniške račune:

(d) metode avtentikacije, ki so sorazmerne z razvrstitvijo iz člena 30(1) in splošnim profilom tveganja sredstev IKT ter temeljijo na vodilnih praksah;

(e) pravice dostopa se redno pregledujejo in odvzamejo, ko niso več potrebne.

Za namene točke (c) finančni subjekt dodeli prednostni, nujni in skrbniški dostop za vse sisteme IKT na podlagi potrebe po uporabi ali na priložnostni podlagi, kar se beleži v dnevnike v skladu s členom 34, prvi odstavek, točka (f).

Za namene točke (d) finančni subjekti za oddaljeni dostop do omrežja finančnih subjektov, za prednostni dostop in za dostop do sredstev IKT, ki podpirajo kritične ali pomembne funkcije, ki so javno dostopne, uporabljajo metode močne avtentikacije, ki temeljijo na vodilnih praksah.

Člen 34

Varnost delovanja IKT

Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 v okviru svojih sistemov, protokolov in orodij ter za vsa sredstva IKT:

(a) spremljajo in upravljajo življenjski cikel vseh sredstev IKT;

(b) spremljajo, ali sredstva IKT podpirajo tretji ponudniki storitev IKT finančnih subjektov, kadar je ustrezno;

(c) opredelijo zahteve glede zmogljivostih svojih sredstev IKT in ukrepe za ohranjanje in izboljšanje razpoložljivosti in učinkovitosti sistemov IKT ter preprečevanje pomanjkanja zmogljivosti IKT, preden se pojavi;

(d) izvajajo avtomatizirano pregledovanje in ocenjevanje ranljivosti sredstev IKT, in sicer sorazmerno z njihovo razvrstitvijo iz člena 30(1) in splošnim profilom tveganja sredstva IKT, ter uvedejo popravke za odpravo prepoznanih ranljivosti;

(e) obvladujejo tveganja, povezana z zastarelimi, nepodprtimi ali obstoječimi sredstvi IKT;

(f) beležijo dogodke, povezane z nadzorom logičnega in fizičnega dostopa, delovanjem IKT, v dnevnike, vključno z dejavnostmi v zvezi s sistemom in omrežnim prometom, ter upravljanjem sprememb na področju IKT;

(g) opredelijo in izvajajo ukrepe za spremljanje in analizo informacij o neobičajnem ravnanju in vedenju za kritično ali pomembno delovanje IKT;

(h) izvajajo ukrepe za spremljanje relevantnih in najnovejših informacij o kibernetskih grožnjah;

(i) izvajajo ukrepe za identifikacijo morebitnih uhajanj informacij, zlonamernih kod in drugih varnostnih groženj ter javno znanih ranljivosti v programski in strojni opremi ter preverjajo, ali obstajajo ustrezne nove varnostne posodobitve.

Za namene točke (f) finančni subjekti uskladijo raven podrobnosti dnevnikov z njihovim namenom in uporabo sredstev IKT, ki te dnevnike proizvajajo.

Člen 35

Varnost podatkov, sistemov in omrežij

Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 v okviru svojih sistemov, protokolov in orodij razvijejo in izvajajo zaščitne ukrepe, ki zagotavljajo varnost omrežij pred vdori in zlorabo podatkov ter ohranjajo razpoložljivost, avtentičnost, celovitost in zaupnost podatkov. Finančni subjekti ob upoštevanju razvrstitve iz člena 30(1) te uredbe zlasti določijo vse naslednje:

(a) opredelitev in izvajanje ukrepov za varstvo podatkov v uporabi, med prenosom in v mirovanju;

(b) opredelitev in izvajanje varnostnih ukrepov glede uporabe programske opreme, naprav za shranjevanje podatkov, sistemov in končnih naprav, s katerimi se prenašajo in shranjujejo podatki finančnega subjekta;

(c) opredelitev in izvajanje ukrepov za preprečevanje in odkrivanje nepooblaščenih povezav z omrežjem finančnega subjekta ter za zaščito omrežnega prometa med notranjimi omrežji finančnega subjekta ter internetom in drugimi zunanjimi povezavami;

(d) opredelitev in izvajanje ukrepov, ki zagotavljajo razpoložljivost, avtentičnost, celovitost in zaupnost podatkov med prenosi v omrežju;

(e) postopek za varno brisanje podatkov v prostorih ali tistih, ki se hranijo zunaj njih, ki jih finančnemu subjektu ni več treba zbirati ali hraniti;

(f) postopek za varno odstranitev ali razgradnjo naprav za shranjevanje podatkov v prostorih ali naprav za shranjevanje podatkov, ki se hranijo zunaj njih, ki vsebujejo zaupne informacije;

(g) opredelitev in izvajanje ukrepov za zagotovitev, da delo na daljavo in uporaba zasebnih končnih naprav ne vplivata negativno na zmožnost finančnega subjekta, da ustrezno, pravočasno in varno izvaja svoje kritične dejavnosti.

Člen 36

Testiranje varnosti IKT

1. Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 določijo in izvajajo načrt testiranja varnosti IKT za potrditev učinkovitosti svojih varnostnih ukrepov na področju IKT, pripravljenih v skladu s členi 33, 34 in 35 ter členoma 37 in 38 te uredbe. Finančni subjekti zagotovijo, da se v tem načrtu upoštevajo grožnje in ranljivosti, prepoznane kot del poenostavljenega okvira za obvladovanje tveganj na področju IKT iz člena 31 te uredbe.

2. Finančni subjekti iz odstavka 1 pregledajo, ocenijo in testirajo varnostne ukrepe na področju IKT ob upoštevanju splošnega profila tveganja sredstev IKT finančnega subjekta.

3. Finančni subjekti iz odstavka 1 spremljajo in ocenjujejo rezultate testiranj varnosti ter brez nepotrebnega odlašanja ustrezno posodobijo svoje varnostne ukrepe v primeru sistemov IKT, ki podpirajo kritične ali pomembne funkcije.

Člen 37

Pridobitev, razvoj in vzdrževanje sistemov IKT

Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 oblikujejo in izvajajo, kadar je primerno, postopek, ki ureja pridobitev, razvoj in vzdrževanje sistemov IKT v skladu s pristopom, ki temelji na tveganju. S tem postopkom se:

(a) zagotovi, da zadevna poslovna funkcija pred kakršno koli pridobitvijo ali razvojem sistemov IKT jasno določi in odobri funkcionalne in nefunkcionalne zahteve, vključno z zahtevami glede informacijske varnosti;

(b) zagotovi testiranje in odobritev sistemov IKT pred njihovo prvo uporabo in pred uvedbo sprememb v produkcijsko okolje;

(c) opredeli ukrepe za zmanjšanje tveganja nenamerne spremembe ali namerne manipulacije sistemov IKT med razvojem in izvajanjem v produkcijskem okolju.

Člen 38

Vodenje projektov IKT in upravljanje sprememb na področju IKT

1. Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 razvijejo, dokumentirajo in izvajajo postopek vodenja projektov IKT ter določijo vloge in odgovornosti za njegovo izvajanje. Ta postopek zajema vse faze projektov IKT od njihovega začetka do njihovega zaključka.

2. Finančni subjekti iz odstavka 1 razvijejo, dokumentirajo in izvajajo postopek upravljanja sprememb na področju IKT za zagotovitev, da se vse spremembe sistemov IKT evidentirajo, testirajo, ocenijo, odobrijo, izvajajo in preverjajo na nadzorovan način in z ustreznimi zaščitnimi ukrepi, da se ohrani digitalna operativna odpornost finančnega subjekta.

POGLAVJE III

UPRAVLJANJE NEPREKINJENEGA POSLOVANJA NA PODROČJU IKT

Člen 39

Komponente načrta neprekinjenega poslovanja na področju IKT

1. Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 pripravijo svoje načrte neprekinjenega poslovanja na področju IKT ob upoštevanju rezultatov analize svojih izpostavljenosti resnim motnjam poslovanja in njihovega morebitnega učinka ter scenarijev, ki bi jim lahko bila izpostavljena njihova sredstva IKT, ki podpirajo kritične ali pomembne funkcije, vključno s scenarijem kibernetskega napada.

2. Načrti neprekinjenega poslovanja na področju IKT iz odstavka 1:

(a) se odobrijo s strani upravljalnega organa finančnega subjekta;

(b) so dokumentirani in zlahka dostopni v primeru izrednih ali kriznih razmer;

(c) dodelijo zadostna sredstva za njihovo izvajanje;

(d) določijo načrtovane ravni obnovitve in časovne okvire za obnovitev in ponovno vzpostavitev funkcij ter ključnih notranjih in zunanjih odvisnosti, vključno s tretjimi ponudniki storitev IKT;

(e) opredelijo pogoje, ki lahko spodbudijo aktivacijo načrtov neprekinjenega poslovanja na področju IKT, in katere ukrepe je treba sprejeti za zagotovitev razpoložljivosti, neprekinjenosti in okrevanja sredstev IKT finančnih subjektov, ki podpirajo kritične ali pomembne funkcije;

(f) opredelijo ukrepe za obnovitev in okrevanje kritičnih ali pomembnih poslovnih funkcij, podpornih procesov, informacijskih sredstev in njihovih soodvisnosti, da se preprečijo škodljivi učinki na delovanje finančnih subjektov;

(g) opredelijo politike in postopke varnostnega kopiranja, ki določajo obseg podatkov za varnostno kopiranje in najmanjšo pogostost varnostnega kopiranja na podlagi kritičnosti funkcije, ki uporablja te podatke;

(h) preučijo alternativne možnosti, kadar okrevanje kratkoročno morda ni izvedljivo zaradi stroškov, tveganj, logistike ali nepredvidenih okoliščin;

(i) določijo ureditev notranje in zunanje komunikacije, vključno z načrti za prenos na višjo raven;

(j) se posodobijo v skladu z izkušnjami, pridobljenimi pri identificiranih incidentih, testih, novih tveganjih in grožnjah, spremenjenimi cilji obnovitve ter večjimi spremembami organizacije finančnega subjekta in sredstev IKT, ki podpirajo kritične ali poslovne funkcije.

Za namene točke (f) ukrepi iz navedene točke zagotavljajo blaženje prenehanja delovanja ključnih tretjih ponudnikov.

Člen 40

Testiranje načrtov neprekinjenega poslovanja

1. Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 testirajo svoje načrte neprekinjenega poslovanja iz člena 39 te uredbe, vključno s scenariji iz navedenega člena, vsaj enkrat letno za postopke varnostnega kopiranja in obnovitve ali ob vsaki večji spremembi načrta neprekinjenega poslovanja.

2. S testiranjem načrtov neprekinjenega poslovanja iz odstavka 1 se dokaže, da so finančni subjekti iz navedenega odstavka sposobni ohraniti uspešnost svojega poslovanja, dokler se ponovno ne vzpostavijo kritične dejavnosti, in prepoznajo morebitne pomanjkljivosti v teh načrtih.

3. Finančni subjekti iz odstavka 1 dokumentirajo rezultate testiranja načrtov neprekinjenega poslovanja, vse pomanjkljivosti, ugotovljene pri tem testiranju, pa se analizirajo, odpravijo in sporočijo upravljalnemu organu.

POGLAVJE IV

POROČILO O PREGLEDU POENOSTAVLJENEGA OKVIRA ZA OBVLADOVANJE TVEGANJ NA PODROČJU IKT

Člen 41

Oblika in vsebina poročila o pregledu poenostavljenega okvira za obvladovanje tveganj na področju IKT

1. Finančni subjekti iz člena 16(1) Uredbe (EU) 2022/2554 predložijo poročilo o pregledu okvira za obvladovanje tveganj na področju IKT iz odstavka 2 navedenega člena v elektronski obliki, ki omogoča iskanje.

2. Poročilo iz odstavka 1 vsebuje vse naslednje informacije:

(a) uvodni del, ki vsebuje:

(i) opis konteksta poročila v smislu narave, obsega in kompleksnosti storitev, dejavnosti in poslovanja finančnega subjekta, njegove organizacije, identificiranih kritičnih funkcij, strategije, velikih tekočih projektov ali dejavnosti in odnosov ter njegove odvisnosti od notranjih in zunanjih storitev in sistemov IKT ali posledic, ki bi jih imela popolna izguba ali resna degradacija takih sistemov na kritične ali pomembne funkcije in učinkovitost trga;

(ii) povzetek identificiranih trenutnih in kratkoročnih tveganj na področju IKT, okolja groženj, ocenjene učinkovitosti njegovih kontrol in varnostnega stanja finančnega subjekta;

(iii) informacije o področju, o katerem se poroča;

(iv) povzetek večjih sprememb okvira za obvladovanje tveganj na področju IKT od prejšnjega poročila;

(v) povzetek in opis vpliva večjih sprememb poenostavljenega okvira za obvladovanje tveganj na področju IKT od prejšnjega poročila;

(b) kadar je primerno, datum, ko je upravljalni organ finančnega subjekta odobril poročilo;

(c) opis razlogov za pregled, vključno z:

(i) kadar se je pregled začel po nadzorniških navodilih, dokazili o takih navodilih;

(ii) kadar se je pregled začel po pojavu incidentov, povezanih z IKT, seznamom vseh teh incidentov, povezanih z IKT, skupaj z analizo temeljnih vzrokov incidentov;

(d) začetni in končni datum obdobja pregleda;

(e) osebo, odgovorno za pregled;

(f) povzetek ugotovitev in samooceno resnosti slabosti, pomanjkljivosti in vrzeli, identificiranih v okviru za obvladovanje tveganj na področju IKT za obdobje pregleda, vključno s podrobno analizo navedenega;

(g) popravne ukrepe, opredeljene za odpravo slabosti, pomanjkljivosti in vrzeli v poenostavljenem okviru za obvladovanje tveganj na področju IKT, ter pričakovani datum za izvedbo teh ukrepov, vključno z nadaljnjim ukrepanjem v zvezi s slabostmi, pomanjkljivostmi in vrzelmi, identificiranimi v prejšnjih poročilih, kadar te slabosti, pomanjkljivosti in vrzeli še niso bile odpravljene;

(h) splošne sklepe o pregledu poenostavljenega okvira za obvladovanje tveganj na področju IKT, vključno z morebitnimi nadaljnjimi načrtovanimi spremembami.

NASLOV IV

KONČNE DOLOČBE

Člen 42

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 13. marca 2024

Za Komisijo
predsednica
Ursula VON DER LEYEN