2024/2690

18.10.2024.

PROVEDBENA UREDBA KOMISIJE (EU) 2024/2690

od 17. listopada 2024.

o utvrđivanju pravila za primjenu Direktive (EU) 2022/2555 u pogledu tehničkih i metodoloških zahtjeva za mjere upravljanja kibernetičkosigurnosnim rizicima te dodatnih specifikacija slučajeva u kojima se incident smatra značajnim za pružatelje usluga DNS-a, registre naziva vršnih domena, pružatelje usluga računalstva u oblaku, pružatelje usluga podatkovnog centra, pružatelje mreža za isporuku sadržaja, pružatelje upravljanih usluga, pružatelje upravljanih sigurnosnih usluga, pružatelje internetskih tržišta, internetskih tražilica i platformi za usluge društvenih mreža te pružatelje usluga povjerenja

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) [1], a posebno njezin članak 21. stavak 5. prvi podstavak i članak 23. stavak 11. drugi podstavak,

budući da:

(1) Svrha je ove Uredbe utvrditi tehničke i metodološke zahtjeve za mjere iz članka 21. stavka 2. Direktive (EU) 2022/2555 i dodatno specificirati slučajeve iz članka 23. stavka 3. Direktive (EU) 2022/2555 u kojima bi se incident trebao smatrati značajnim za pružatelje usluga DNS-a, registre naziva vršnih domena, pružatelje usluga računalstva u oblaku, pružatelje usluga podatkovnog centra, pružatelje mreža za isporuku sadržaja, pružatelje upravljanih usluga, pružatelje upravljanih sigurnosnih usluga, pružatelje internetskih tržišta, internetskih tražilica i platformi za usluge društvenih mreža te pružatelje usluga povjerenja kako su obuhvaćeni člankom 3. Direktive (EU) 2022/2555 (relevantni subjekti).

(2) S obzirom na prekograničnu prirodu aktivnosti pružatelja usluga povjerenja i kako bi se za njih uspostavio dosljedan okvir, ovom bi Uredbom, uz to što će se utvrditi tehnički i metodološki zahtjevi za mjere upravljanja kibernetičkosigurnosnim rizicima, trebalo dodatno specificirati slučajeve u kojima se incident smatra značajnim.

(3) U skladu s člankom 21. stavkom 5. trećim podstavkom Direktive (EU) 2022/2555 tehnički i metodološki zahtjevi za mjere upravljanja kibernetičkosigurnosnim rizicima utvrđeni u Prilogu ovoj Uredbi temelje se na europskim i međunarodnim normama, kao što su ISO/IEC 27001, ISO/IEC 27002 i ETSI EN 319401, i tehničkim specifikacijama, kao što je CEN/TS 18026:2024, koje su bitne za sigurnost mrežnih i informacijskih sustava.

(4) Kad je riječ o provedbi i primjeni tehničkih i metodoloških zahtjeva za mjere upravljanja kibernetičkosigurnosnim rizicima iz Priloga ovoj Uredbi, pri njihovu bi ispunjavanju, u skladu s načelom proporcionalnosti, u obzir bi trebalo uzeti razlike u izloženosti relevantnih subjekata riziku, kao što su kritičnost relevantnog subjekta, rizici kojima je izložen, veličina i struktura relevantnog subjekta te vjerojatnost pojave incidenata i njihova ozbiljnost, uključujući njihove društvene i gospodarske posljedice.

[1] SL L 333, 27.12.2022., str. 80., ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(5) U skladu s načelom proporcionalnosti, ako relevantni subjekti zbog svoje veličine ne mogu provesti neke tehničke i metodološke zahtjeve za mjere upravljanja kibernetičkosigurnosnim rizicima, trebali bi moći poduzeti druge, nadomjesne mjere koje su prikladne za ostvarenje svrhe tih zahtjeva. Primjerice, pri definiranju uloga, odgovornosti i ovlasti za sigurnost mrežnih i informacijskih sustava unutar relevantnog subjekta mikrosubjektima bi moglo biti teško razdvojiti proturječne dužnosti i proturječna područja odgovornosti. Takvi bi subjekti trebali moći razmotriti nadomjesne mjere kao što su ciljani nadzor koji provodi uprava subjekta ili pojačano praćenje i evidentiranje.

(6) Relevantni subjekti određene bi tehničke i metodološke zahtjeve iz Priloga ovoj Uredbi trebali ispunjavati prema potrebi, ako su primjenjivi ili u mjeri u kojoj je to izvedivo. Ako relevantni subjekt smatra da određene tehničke i metodološke zahtjeve iz Priloga ovoj Uredbi nema potrebe ispunjavati, da to nije izvedivo ili da se ti zahtjevi na njega ne primjenjuju, trebao bi jasno dokumentirati svoje razloge za to. Nacionalna nadležna tijela mogu pri obavljanju nadzora uzeti u obzir odgovarajuće vrijeme koje je relevantnim subjektima potrebno za ispunjavanje tehničkih i metodoloških zahtjeva mjera upravljanja kibernetičkosigurnosnim rizicima.

(7) ENISA ili nacionalna nadležna tijela na temelju Direktive (EU) 2022/2555 mogu dati smjernice kako bi pomogli relevantnim subjektima da utvrde, analiziraju i procijene rizike za potrebe provedbe tehničkih i metodoloških zahtjeva koji se odnose na uspostavu i održavanje odgovarajućeg okvira za upravljanje rizicima. Takve smjernice mogu sadržavati nacionalne i sektorske procjene rizika te procjene rizika koje su specifične za određenu vrstu subjekta. Mogu sadržavati i alate ili predloške za izradu okvira za upravljanje rizicima na razini relevantnih subjekata. Okviri, smjernice ili drugi mehanizmi predviđeni nacionalnim pravom država članica i relevantne europske i međunarodne norme mogu državama članicama pomoći i u dokazivanju usklađenosti s ovom Uredbom. Nadalje, ENISA ili nacionalna nadležna tijela na temelju Direktive (EU) 2022/2555 mogu pomoći relevantnim subjektima da utvrde i primijene odgovarajuća rješenja za postupanje s rizicima utvrđenima u takvim procjenama rizika. Takvim smjernicama ne bi se trebala dovoditi u pitanje obveza relevantnih subjekata da utvrde i dokumentiraju rizike za sigurnost mrežnih i informacijskih sustava ni obveza relevantnih subjekata da tehničke i metodološke zahtjeve za mjere upravljanja kibernetičkosigurnosnim rizicima iz Priloga ovoj Uredbi provode u skladu sa svojim potrebama i mogućnostima.

(8) Mjere za sigurnost mreže koje se odnose na i. prelazak na komunikacijske protokole mrežnog sloja najnovije generacije, ii. uvođenje međunarodno dogovorenih i interoperabilnih modernih komunikacijskih standarda e-pošte i iii. primjenu provjereno dobrih postupaka za sigurnost DNS-a i za sigurnost i higijenu usmjeravanja na internetu sa sobom donose specifične izazove u vezi s utvrđivanjem najboljih dostupnih standarda i tehnika uvođenja. Kako bi se što prije postigla visoka zajednička razina kibernetičke sigurnosti svih mreža, Komisija bi, uz pomoć Agencije Europske unije za kibersigurnost (ENISA) i u suradnji s nadležnim tijelima, industrijom, uključujući telekomunikacijski sektor, i drugim dionicima, trebala poduprijeti razvoj višedioničkog foruma čija bi zadaća bila utvrditi najbolje dostupne standarde i tehnike uvođenja. Takve višedioničke smjernice ne bi trebale dovoditi u pitanje obvezu relevantnih subjekata da provode tehničke i metodološke zahtjeve za mjere upravljanja kibernetičkosigurnosnim rizicima iz Priloga ovoj Uredbi.

(9) Prema članku 21. stavku 2. točki (a) Direktive (EU) 2022/2555 ključni i važni subjekti trebali bi, uz politike analize rizika, imati politike sigurnosti informacijskih sustava. Radi toga bi relevantni subjekti trebali uspostaviti politiku sigurnosti mrežnih i informacijskih sustava te tematske politike, kao što su politike kontrole pristupa, koje bi trebale biti usklađene s politikom sigurnosti mrežnih i informacijskih sustava. Politika sigurnosti mrežnih i informacijskih sustava trebala bi biti krovni dokument u kojem se utvrđuje opći pristup relevantnih subjekata sigurnosti njihovih mrežnih i informacijskih sustava i trebala bi je odobriti upravljačka tijela relevantnih subjekata. Tematske politike trebala bi odobriti odgovarajuća rukovodeća razina. U takvim bi politikama trebalo utvrditi pokazatelje i mjere za praćenje njezine provedbe i trenutačne zrelosti mrežne i informacijske sigurnosti relevantnih subjekata, prije svega kako bi se olakšao nadzor provedbe mjera upravljanja kibernetičkosigurnosnim rizicima preko upravljačkih tijela.

(10) Za potrebe tehničkih i metodoloških zahtjeva utvrđenih u Prilogu ovoj Uredbi pojam „korisnik” trebao bi obuhvaćati sve pravne i fizičke osobe koje imaju pristup mrežnim i informacijskim sustavima subjekta.

(11) Relevantni subjekti trebali bi uspostaviti, primjenjivati i revidirati odgovarajući okvir za upravljanje rizicima u svrhu prepoznavanja i suzbijanja rizika za sigurnost mrežnih i informacijskih sustava. Kao dio tog okvira za upravljanje rizicima trebali bi uspostaviti, provoditi i pratiti plan postupanja s rizicima. U tom planu mogu utvrditi mogućnosti i mjere za postupanje s rizicima i njihov prioritet. Neke od mogućnosti postupanja s rizicima su, prije svega, izbjegavanje, smanjenje ili, u iznimnim slučajevima, prihvaćanje rizika. Relevantni subjekti trebali bi odabrati mogućnosti postupanja s rizicima uzimajući u obzir rezultate svoje procjene rizika i u skladu sa svojom politikom sigurnosti mrežnih i informacijskih sustava. Da bi odabrane mogućnosti postupanja s rizicima primijenili u praksi, trebali bi poduzeti odgovarajuće mjere za postupanje s rizicima.

(12) Relevantni subjekti trebali bi pratiti svoje mrežne i informacijske sustave kako bi otkrili događaje, izbjegnute incidente i incidente te poduzimati korake da evaluiraju događaje, izbjegnute incidente i incidente. Te bi mjere trebale omogućivati da se na vrijeme otkriju mrežni napadi na temelju abnormalnih obrazaca ulaznog ili izlaznog prometa i napadi uskraćivanjem usluga.

(13) Relevantni subjekti potiču se da uz analizu učinka na poslovanje provedu i sveobuhvatnu analizu kojom se, prema potrebi, utvrđuju najdulje prihvatljivo trajanje prekida rada, ciljana vremena oporavka, ciljane točke oporavka i ciljane razine usluge.

(14) Za ublažavanje rizika koji proizlaze iz lanaca opskrbe relevantnih subjekata i njihovih odnosa s dobavljačima relevantni subjekti trebali bi uspostaviti politiku sigurnosti lanca opskrbe kojom će se voditi u odnosima sa svojim izravnim dobavljačima i pružateljima usluga. Ti bi subjekti u ugovore s izravnim dobavljačima ili pružateljima usluga trebali uvrstiti odgovarajuće sigurnosne klauzule u kojima bi se, primjerice, zahtijevale mjere upravljanja kibernetičkosigurnosnim rizicima navedene u članku 21. stavku 2. Direktive (EU) 2022/2555 ili drugim sličnim pravnim aktima.

(15) Relevantni subjekti trebali bi redovito provoditi sigurnosne testove u skladu s namjenskom politikom i postupcima kako bi provjerili jesu li mjere upravljanja kibernetičkosigurnosnim rizicima uvedene i funkcioniraju li pravilno. Sigurnosni testovi mogu se provoditi na pojedinim mrežnim i informacijskim sustavima ili na cijelom relevantnom subjektu i mogu obuhvaćati automatizirane ili ručne testove, penetracijske testove, provjeru ranjivosti, statičke i dinamičke sigurnosne testove aplikacija, konfiguracijske testove ili revizije sigurnosti. Relevantni subjekti mogu provoditi sigurnosna testiranja svojih mrežnih i informacijskih sustava kad ih postavljaju, nakon poboljšanja ili izmjena infrastrukture ili aplikacija koje smatraju bitnima ili nakon održavanja. Rezultati sigurnosnih testova trebali bi biti podloga za politike i postupke relevantnih subjekata za procjenu djelotvornosti mjera upravljanja kibernetičkosigurnosnim rizicima te za neovisne revizije njihovih politika mrežne i informacijske sigurnosti.

(16) Kako bi se izbjegli znatni poremećaji i šteta uslijed iskorištavanja neispravljenih ranjivosti u mrežnim i informacijskim sustavima, relevantni subjekti trebali bi utvrditi i primjenjivati odgovarajuće postupke upravljanja sigurnosnim zakrpama koji su usklađeni s njihovim postupcima za upravljanje promjenama, ranjivostima i rizicima te drugim relevantnim postupcima. Trebali bi poduzeti mjere razmjerne svojim mogućnostima kako sigurnosne zakrpe ne bi stvorile dodatne ranjivosti ili nestabilnosti. Relevantni subjekti potiču se da na primjeren način unaprijed obavješćuju korisnike o planiranim nedostupnostima usluge zbog primjene sigurnosnih zakrpa.

(17) Relevantni subjekti trebali bi upravljati rizicima koji proizlaze iz nabave IKT proizvoda ili usluga od dobavljača ili pružatelja usluga i trebali bi dobiti jamstvo da IKT proizvodi ili usluge koje nabavljaju postižu određene razine zaštite kibernetičke sigurnosti, na primjer u obliku europskih certifikata kibernetičke sigurnosti i EU izjave o sukladnosti za IKT proizvode ili usluge izdane u okviru europskog programa kibernetičkosigurnosne certifikacije donesenog u skladu s člankom 49. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća ([2]). Kad relevantni subjekti utvrđuju sigurnosne zahtjeve za IKT proizvode koje nabavljaju, trebali bi uzeti u obzir bitne zahtjeve za kibernetičku sigurnost utvrđene u Uredbi Europskog parlamenta i Vijeća o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima.

(18) Radi zaštite od kibernetičkih prijetnji i potpore sprečavanju i zaustavljanju povreda podataka, relevantni subjekti trebali bi uvesti rješenja za sigurnost mreže. Uobičajena rješenja za sigurnost mreže obuhvaćaju upotrebu vatrozidova za zaštitu unutarnjih mreža relevantnih subjekata, ograničavanje spajanja i pristupa uslugama na nužna spajanja i pristupe te korištenje virtualnih privatnih mreža za daljinski pristup i dopuštanje spajanja pružateljima usluga tek na zahtjev za odobrenje i na određeno razdoblje, npr. dok traje održavanje.

(19) Radi zaštite svojih mreža i informacijskih sustava od zlonamjernog i neovlaštenog softvera, relevantni subjekti trebali bi provoditi kontrole kojima se sprečava ili otkriva korištenje neovlaštenog softvera te bi, prema potrebi, trebali koristiti softver za detekciju i odgovor. Trebali bi razmisliti i o uvođenju mjera za minimiziranje površine napada, smanjenje ranjivosti koje napadači mogu iskoristiti i kontrolu izvođenja aplikacija na krajnjim točkama te upotrebljavati filtre e-pošte i internetskih aplikacija kako bi se smanjila izloženost zlonamjernom sadržaju.

(20) Prema članku 21. stavku 2. točki (g) Direktive (EU) 2022/2555 države članice dužne su osigurati da ključni i važni subjekti primjenjuju osnovne prakse kibernetičke higijene i provode osposobljavanja o kibernetičkoj sigurnosti. Osnovne prakse kibernetičke higijene mogu uključivati načela nulte stope povjerenja, ažuriranja softvera, konfiguraciju uređaja, segmentaciju mreže, upravljanje identitetom i pristupom ili informiranje korisnika, organizaciju osposobljavanja za vlastito osoblje i informiranje o kibernetičkim prijetnjama, *phishingu* ili tehnikama socijalnog inženjeringa. Prakse kibernetičke higijene uključene su u razne tehničke i metodološke zahtjeve za mjere upravljanja kibernetičkosigurnosnim rizicima iz Priloga ovoj Uredbi. Kad je riječ o osnovnim praksama kibernetičke higijene za korisnike, relevantni subjekti trebali bi razmisliti o praksama kao što su politika čistog stola i ekrana, upotreba višestruke provjere i drugih autentifikacijskih sredstava, sigurno korištenje e-pošte i pretraživanje interneta, zaštita od *phishinga* i socijalnog inženjeringa te sigurni načini rada na daljinu.

(21) Kako bi spriječili neovlašten pristup imovini, relevantni subjekti trebali bi uspostaviti i provoditi tematsku politiku koja uređuje pristup osoba te mrežnih i informacijskih sustava, kao što su aplikacije.

(22) Kako bi izbjegli da zaposlenici mogu zloupotrijebiti, primjerice, prava pristupa unutar relevantnog subjekta da naude ili uzrokuju štetu, relevantni subjekti trebali bi razmisliti o uvođenju odgovarajućih mjera upravljanja sigurnošću zaposlenika i informirati osoblje o takvim rizicima. Relevantni subjekti trebali bi uspostaviti, obznaniti i dosljedno primjenjivati disciplinski postupak za kršenje svojih politika sigurnosti mrežnih i informacijskih sustava; on može biti dio drugih disciplinskih postupaka koje su uspostavili. Provjera zaposlenika i, ako je to primjenjivo, izravnih dobavljača i pružatelja usluga relevantnih subjekata trebala bi doprinositi cilju sigurnosti ljudskih resursa subjekata i može obuhvaćati korake kao što su provjere kaznene evidencije ili prethodnih profesionalnih dužnosti osobe, ovisno o njezinim dužnostima u relevantnom subjektu i subjektovoj politici sigurnosti mrežnih i informacijskih sustava.

([2]) Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) Višestruka autentifikacija može povećati kibernetičku sigurnost subjekata, pa bi oni trebali razmisliti o njezinu korištenju, i to osobito kad korisnici pristupaju mrežnim i informacijskim sustavima s udaljenih lokacija ili kad pristupaju osjetljivim informacijama ili povlaštenim računima i računima za administraciju sustava. Višestruka autentifikacija može se kombinirati s drugim tehnikama tako da se u posebnim okolnostima, npr. kod pristupa s neuobičajene lokacije, s neuobičajenog uređaja ili u neuobičajeno vrijeme, zahtijevaju dodatni načini provjere identiteta koji se temelje na unaprijed definiranim pravilima i uzorcima.

(24) Imovinom koja im je vrijedna relevantni subjekti trebali bi upravljati i štititi je dobrim upravljanjem, koje bi također trebalo služiti kao osnova za analizu rizika i upravljanje kontinuitetom poslovanja. Trebali bi upravljati materijalnom i nematerijalnom imovinom, sastaviti popis imovine, povezati je s definiranom klasifikacijskom razinom, rukovati njome i pratiti je te poduzimati korake za zaštitu imovine tijekom njezina životnog ciklusa.

(25) Upravljanje imovinom trebalo bi obuhvaćati klasificiranje imovine prema vrsti, osjetljivosti, razini rizika i sigurnosnim zahtjevima te primjenu odgovarajućih mjera i kontrola kako bi se osigurala njezina dostupnost, cjelovitost, povjerljivost i autentičnost. Klasificiranje imovine prema razini rizika trebalo bi relevantnim subjektima omogućiti da primjenjuju odgovarajuće sigurnosne mjere i kontrole za zaštitu imovine kao što su šifriranje, kontrola pristupa, uključujući nadzor okoline i fizičku i logičku kontrolu pristupa, sigurnosne kopije, evidentiranje i praćenje, zadržavanje i uklanjanje. Pri analizi učinka na poslovanje relevantni subjekti mogu odrediti klasifikacijsku razinu na temelju posljedica koje bi na njih imao poremećaj funkcioniranja imovine. Svi zaposlenici subjekata koji upravljaju imovinom trebali bi biti upućeni u politike i upute za postupanje s njom.

(26) Detaljnost popisa imovine trebala bi biti primjerena potrebama relevantnih subjekata. Cjelovit popis mogao bi za svaku imovinu sadržavati barem jedinstvenu identifikacijsku oznaku, vlasnika imovine, opis imovine, lokaciju imovine, vrstu imovine, vrstu i klasifikaciju informacija koje se obrađuju imovinom, datum posljednjeg poboljšanja, ažuriranja ili zakrpe imovine, klasifikaciju imovine na temelju procjene rizika i kraj životnog vijeka imovine. Pri utvrđivanju vlasnika određene imovine relevantni subjekti trebali bi utvrditi i osobu odgovornu za njezinu zaštitu.

(27) Raspodjelom i organizacijom uloga, odgovornosti i ovlasti za kibernetičku sigurnost trebala bi se uspostaviti usklađena struktura za vođenje i implementaciju kibernetičke sigurnosti u relevantnim subjektima i trebala bi se osigurati učinkovita komunikacija u slučaju incidenata. Pri definiranju i dodjeli odgovornosti za određene uloge relevantni subjekti trebali bi razmotriti uloge kao što su voditelj informacijske sigurnosti, stručnjak za informacijsku sigurnost, stručnjak za postupanje s incidentima i revizor ili usporedive ekvivalente. Relevantni subjekti mogu uloge i odgovornosti dodijeliti vanjskim suradnicima, primjerice vanjskim pružateljima IKT usluga.

(28) Prema članku 21. stavku 2. Direktive (EU) 2022/2555 mjere upravljanja kibernetičkosigurnosnim rizicima trebale bi se temeljiti na pristupu kojim se uzimaju u obzir sve opasnosti i čiji je cilj zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od događaja kao što su krađa, požar, poplava, prekid u telekomunikacijama ili prekid opskrbe električnom energijom ili od neovlaštenog fizičkog pristupa te oštećenja i ometanja podataka i objekata za obradu podataka ključnog ili važnog subjekta koji bi mogli ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koji se nude ili kojima se pristupa putem mrežnih i informacijskih sustava. Tehnički i metodološki zahtjevi za mjere upravljanja kibernetičkosigurnosnim rizicima stoga bi se trebali odnositi i na fizičku i okolišnu sigurnost mrežnih i informacijskih sustava i to tako da obuhvate mjere za zaštitu tih sustava od kvarova sustava, ljudske pogreške, zlonamjernih radnji ili prirodnih pojava. Još neki primjeri fizičkih i okolišnih prijetnji su potresi, eksplozije, sabotaže, unutarnje prijetnje, građanski nemiri, toksični otpad i emisije iz okoliša. Sprečavanje gubitka, oštećenja ili ugrožavanja mrežnih i informacijskih sustava ili prekida njihova rada zbog kvara i poremećaja u radu potpornih komunalnih usluga trebalo bi doprinijeti ostvarenju cilja kontinuiteta poslovanja relevantnih subjekata. Uz to, zaštita od fizičkih i okolišnih prijetnji trebala bi doprinijeti sigurnosti održavanja mrežnih i informacijskih sustava relevantnih subjekata.

(29) Relevantni subjekti trebali bi osmisliti i primjenjivati mjere zaštite od fizičkih i okolišnih prijetnji i odrediti minimalne i maksimalne kontrolne pragove za te prijetnje te pratiti okolišne parametre. Trebali bi, primjerice, razmotriti ugradnju sustava za rano otkrivanje poplava u prostorima u kojima su smješteni mrežni i informacijski sustavi. Kad je riječ o opasnosti od požara, trebali bi razmisliti o izradi zasebnog požarnog odjeljka za podatkovni centar, upotrebi vatrootpornih materijala i senzora za praćenje temperature i vlažnosti, povezivanju zgrade s požarnim alarmnim sustavom s automatskim obavješćivanjem lokalne vatrogasne službe te sustavima za rano otkrivanje i gašenje požara. Relevantni subjekti također bi trebali provoditi redovite protupožarne vježbe i inspekcije protupožarne zaštite. Nadalje, kako bi osigurali izvor napajanja, relevantni subjekti trebali bi razmisliti o upotrebi prenaponske zaštite i odgovarajućeg izvora napajanja za slučaj nužde u skladu s relevantnim normama. Povrh toga, budući da je pregrijavanje rizik za dostupnost mrežnih i informacijskih sustava, relevantni subjekti, osobito pružatelji usluga podatkovnog centra, mogli bi razmotriti upotrebu odgovarajućih redundantnih klimatizacijskih sustava namijenjenih za neprekidan rad.

(30) Ovom se Uredbom žele pobliže specificirati slučajevi u kojima bi se incident trebao smatrati značajnim za potrebe članka 23. stavka 3. Direktive (EU) 2022/2555. Kriteriji bi trebali biti takvi da relevantni subjekti mogu procijeniti je li incident značajan kako bi ga prijavili u skladu s Direktivom (EU) 2022/2555. Nadalje, kriterije utvrđene u ovoj Uredbi trebalo bi smatrati iscrpnima, ne dovodeći u pitanje članak 5. Direktive (EU) 2022/2555. U ovoj se Uredbi slučajevi u kojima bi se incident trebao smatrati značajnim specificiraju tako što se navode univerzalni slučajevi i slučajevi koji su specifični za određene subjekte.

(31) Prema članku 23. stavku 4. Direktive (EU) 2022/2555 relevantni subjekti trebali bi biti dužni dojaviti značajni incident u rokovima utvrđenima tom odredbom. Ti rokovi za dojavu počinju teći od trenutka kad subjekt sazna za takve značajne incidente. Relevantni subjekt dužan je, dakle, javljati o incidentima koji bi, prema njegovoj početnoj procjeni, mogli uzrokovati ozbiljne poremećaje u funkcioniranju usluga ili financijske gubitke za taj subjekt ili utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete. Prema tome, ako je relevantni subjekt otkrio sumnjiv događaj ili ako ga je treća strana, npr. neka osoba, klijent, subjekt, tijelo, medijska organizacija ili drugi izvor, upozorila na potencijalni incident, on bi trebao pravodobno procijeniti sumnjivi događaj da ustanovi je li riječ o incidentu i, ako jest, da utvrdi njegovu prirodu i ozbiljnost. Stoga se smatra da je relevantni subjekt „saznao” za značajni incident ako na temelju takve početne procjene može s razumnim stupnjem sigurnosti reći da se značajni incident dogodio.

(32) Kad žele utvrditi je li neki incident značajan, relevantni subjekti trebali bi, prema potrebi, izračunati broj korisnika zahvaćenih incidentom, uzimajući pritom u obzir poslovne i krajnje klijente s kojima imaju ugovorni odnos te fizičke i pravne osobe koje su povezane s poslovnim klijentima. Ako relevantni subjekt ne može izračunati broj zahvaćenih korisnika, za potrebe izračuna ukupnog broja korisnika zahvaćenih incidentom trebalo bi uzeti u obzir njegovu procjenu mogućeg maksimalnog broja zahvaćenih korisnika. Značajnost incidenta koji uključuje uslugu povjerenja ne bi se trebala određivati samo prema broju korisnika nego i prema broju pouzdajućih strana jer njima takav incident može jednako poremetiti rad i nanijeti materijalnu ili nematerijalnu štetu. Dakle, kad utvrđuju značajnost incidenta, pružatelji usluga povjerenja trebali bi, ako je to primjenjivo, uzeti u obzir i broj pouzdajućih strana. U tu svrhu pouzdajuće strane trebalo bi tumačiti kao fizičke ili pravne osobe koje se pouzdaju u uslugu povjerenja.

(33) Postupke održavanja koji uzrokuju ograničenu dostupnost ili nedostupnost usluge ne bi trebalo smatrati značajnim incidentima ako ograničena dostupnost ili nedostupnost usluge nastupi u skladu s planiranim postupkom održavanja. Nadalje, ako je usluga nedostupna zbog planiranih prekida kao što su prekidi ili nedostupnost na temelju unaprijed utvrđenog ugovornog sporazuma, to ne se bi trebalo smatrati značajnim incidentom.

(34) Trajanje incidenta koji utječe na dostupnost usluge trebalo bi mjeriti od prekida normalnog pružanja te usluge do trenutka oporavka. Ako relevantni subjekt ne može ustanoviti trenutak početka poremećaja, trajanje incidenta trebalo bi mjeriti od trenutka otkrivanja incidenta ili od trenutka kad je incident zabilježen u evidenciji mrežnih ili sistemskih događaja ili u drugim izvorima podataka, ovisno o tome što nastupi prije.

(35) Potpunu nedostupnost usluge trebalo bi mjeriti od trenutka kad usluga postane potpuno nedostupna korisnicima do trenutka ponovne uspostave redovitih aktivnosti ili operacija na razini usluge prije incidenta. Ako relevantni subjekt ne može ustanoviti kad je nastupila potpuna nedostupnost usluge, nedostupnost bi se trebala mjeriti od trenutka kad ju je taj subjekt otkrio.

(36) Kad utvrđuju izravne financijske gubitke zbog incidenta, relevantni subjekti trebali bi uzeti u obzir sve financijske gubitke koje su pretrpjeli zbog incidenta, npr. troškove zamjene ili premještanja softvera, hardvera ili infrastrukture, troškove osoblja, uključujući troškove zamjene ili premještanja osoblja, zapošljavanja dodatnog osoblja, naknade za prekovremeni rad i povrat izgubljenih ili umanjenih vještina, naknade zbog neispunjavanja ugovornih obveza, troškove pravne zaštite i naknada klijentima, gubitke zbog izgubljenih prihoda, troškove unutarnje i vanjske komunikacije, troškove savjetovanja, uključujući troškove povezane s pravnim savjetovanjem, forenzičkim uslugama i uslugama sanacije te druge troškove povezane s incidentom. No novčane kazne i troškovi koji su nužni za svakodnevno poslovanje ne bi se trebali smatrati financijskim gubicima zbog incidenta; to obuhvaća, među ostalim, troškove općeg održavanja infrastrukture, opreme, hardvera i softvera, kontinuiranog unapređivanja vještina osoblja, unutarnje ili vanjske troškove unapređenja poslovanja nakon incidenta, uključujući ažuriranja, poboljšanja i inicijative za procjenu rizika, te premije osiguranja. Relevantni subjekti bi iznose financijskih gubitaka trebali izračunati iz dostupnih podataka, a ako se stvarni iznosi financijskih gubitaka ne mogu utvrditi, subjekti bi ih trebali procijeniti.

(37) Relevantni subjekti također bi trebali biti dužni prijaviti incidente koji su uzrokovali ili mogu uzrokovati smrt osoba ili znatnu štetu zdravlju osoba jer takvi incidenti spadaju u posebno ozbiljne slučajeve sa znatnom materijalnom ili nematerijalnom štetom. Primjerice, incident koji utječe na relevantni subjekt mogao bi uzrokovati nedostupnost zdravstvenih ili hitnih službi ili gubitak povjerljivosti ili cjelovitosti podataka s učinkom na zdravlje pojedinaca. Kad utvrđuju je li incident uzrokovao ili može uzrokovati znatnu štetu zdravlju osobe, relevantni subjekti trebali bi razmotriti je li incident uzrokovao ili može uzrokovati teške ozljede i loše zdravlje. U tu svrhu ne bi trebali biti obvezni prikupljati dodatne informacije kojima nemaju pristup.

(38) Trebalo bi smatrati da je nastupila ograničena dostupnost osobito u slučaju kad je vrijeme odgovora usluge relevantnog subjekta znatno dulje od prosječnog ili kad nisu dostupne sve funkcionalnosti usluge. Kad god je moguće, pri procjeni kašnjenja u vremenu odgovora trebalo bi primjenjivati objektivne kriterije koji se temelje na prosječnom vremenu odgovora u uslugama relevantnih subjekata. Funkcionalnost usluge može, naprimjer, biti funkcionalnost razgovora ili pretraživanja slika.

(39) Uspješan, pretpostavljeno zlonamjeran i neovlašten pristup mrežnim i informacijskim sustavima relevantnog subjekta trebao bi se smatrati značajnim incidentom ako može uzrokovati ozbiljne poremećaje u radu. Primjerice, incident bi se trebao smatrati značajnim kad se akter kibernetičke prijetnje unaprijed pozicionira u mrežnim i informacijskim sustavima relevantnog subjekta s namjerom da uzrokuje poremećaj u pružanju usluga u budućnosti.

(40) Incidenti koji se ponavljaju i povezuje ih isti očiti temeljni uzrok, ali pojedinačno ne ispunjavaju kriterije značajnog incidenta, trebali bi se skupno smatrati značajnim incidentom ako skupno ispunjavaju kriterij financijskog gubitka i dogodili su se najmanje dvaput u šest mjeseci. Takvi incidenti koji se ponavljaju mogu ukazivati na znatne nedostatke i slabosti u postupcima upravljanja kibernetičkosigurnosnim rizicima relevantnog subjekta i njihovoj kibernetičkosigurnosnoj zrelosti. Uz to, takvi incidenti koji se ponavljaju mogu relevantnom subjektu nanijeti znatan financijski gubitak.

(41) U skladu s člankom 21. stavkom 5. i člankom 23. stavkom 11. Direktive (EU) 2022/2555 Komisija je pri izradi nacrta provedbenog akta razmijenila savjete i surađivala sa Skupinom za suradnju i ENISA-om.

(42) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([3]) te je on dao mišljenje 1. rujna 2024.

(43) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem odbora osnovanog člankom 39. Direktive (EU) 2022/2555,

DONIJELA JE OVU UREDBU:

Članak 1.

Predmet

Ovom se Uredbom utvrđuju tehnički i metodološki zahtjevi za mjere iz članka 21. stavka 2. Direktive (EU) 2022/2555 i dodatno specificiraju slučajevi iz članka 23. stavka 3. Direktive (EU) 2022/2555 u kojima se incident smatra značajnim za pružatelje usluga DNS-a, registre naziva vršnih domena, pružatelje usluga računalstva u oblaku, pružatelje usluga podatkovnog centra, pružatelje mreža za isporuku sadržaja, pružatelje upravljanih usluga, pružatelje upravljanih sigurnosnih usluga, pružatelje internetskih tržišta, internetskih tražilica i platformi za usluge društvenih mreža te pružatelje usluga povjerenja (relevantni subjekti).

Članak 2.

Tehnički i metodološki zahtjevi

1. Tehnički i metodološki zahtjevi za mjere upravljanja kibernetičkosigurnosnim rizicima iz članka 21. stavka 2. točaka od (a) do (j) Direktive (EU) 2022/2555 koji se odnose na relevantne subjekte utvrđeni su u Prilogu ovoj Uredbi.

2. Pri provedbi i primjeni tehničkih i metodoloških zahtjeva za mjere upravljanja kibernetičkosigurnosnim rizicima iz Priloga ovoj Uredbi relevantni subjekti osiguravaju razinu sigurnosti mrežnih i informacijskih sustava koja je primjerena rizicima. U tu svrhu pri ispunjavanju tehničkih i metodoloških zahtjeva za mjere upravljanja kibernetičkosigurnosnim rizicima iz Priloga ovoj Uredbi uzimaju u obzir stupanj svoje izloženosti rizicima, svoju veličinu, vjerojatnost pojave incidenata i njihovu ozbiljnost, uključujući njihove društvene i gospodarske posljedice.

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

Ako je u Prilogu ovoj Uredbi uređeno da se određeni tehnički ili metodološki zahtjev neke mjere upravljanja kibernetičkosigurnosnim rizicima ispunjava „prema potrebi”, „ako je to primjenjivo” ili „u mjeri u kojoj je to izvedivo” i ako relevantni subjekt smatra da određene tehničke i metodološke zahtjeve iz Priloga ovoj Uredbi nema potrebe ispunjavati, da to nije izvedivo ili da se oni na njega ne primjenjuju, relevantni subjekt dužan je jasno dokumentirati svoje razloge za to.

Članak 3.

Značajni incidenti

1. Kad je riječ o relevantnim subjektima, incident se smatra značajnim za potrebe članka 23. stavka 3. Direktive (EU) 2022/2555 ako je ispunjen barem jedan od sljedećih kriterija:

(a) incident je relevantnom subjektu uzrokovao ili može uzrokovati izravni financijski gubitak veći od 500 000 EUR ili 5 % ukupnog godišnjeg prometa relevantnog subjekta u prethodnoj financijskoj godini, ovisno koji je iznos niži;

(b) incident je uzrokovao ili može uzrokovati izvlačenje poslovnih tajni relevantnog subjekta kako su definirane u članku 2. točki 1. Direktive (EU) 2016/943;

(c) incident je uzrokovao ili može uzrokovati smrt osobe;

(d) incident je uzrokovao ili može uzrokovati znatno narušeno zdravlje osobe;

(e) došlo je do uspješnog, pretpostavljeno zlonamjernog i neovlaštenog pristupa mrežnim i informacijskim sustavima koji može uzrokovati ozbiljan poremećaj u radu;

(f) incident ispunjava kriterije iz članka 4.;

(g) incident ispunjava barem jedan od kriterija iz članaka od 5. do 14.

2. Planirani prekidi usluge i planirane posljedice planiranih radova održavanja koje obavljaju relevantni subjekti ili se obavljaju u njihovo ime ne smatraju se značajnim incidentima.

3. Pri izračunu broja korisnika zahvaćenih incidentom za potrebe članka 7. i članaka od 9. do 14. relevantni subjekti uzimaju u obzir sve navedeno:

(a) broj klijenata koji s relevantnim subjektom imaju ugovor koji im dopušta pristup mrežnim i informacijskim sustavima relevantnog subjekta ili uslugama koje se nude ili kojima se može pristupiti putem tih mrežnih i informacijskih sustava;

(b) broj fizičkih i pravnih osoba povezanih s poslovnim klijentima koji koriste mrežne i informacijske sustave relevantnog subjekta ili usluge koje se nude ili kojima se može pristupiti putem tih mrežnih i informacijskih sustava.

Članak 4.

Incidenti koji se ponavljaju

Incidenti koji se pojedinačno ne smatraju značajnim incidentom u smislu članka 3. skupno se smatraju jednim značajnim incidentom ako ispunjavaju sve sljedeće kriterije:

(a) dogodili su se najmanje dvaput u šest mjeseci;

(b) imaju isti očiti temeljni uzrok;

(c) skupno ispunjavaju kriterije iz članka 3. stavka 1. točke (a).

Članak 5.

Značajni incidenti za pružatelje usluga DNS-a

Kad je riječ o pružateljima usluga DNS-a, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neka rekurzivna ili autoritativna DNS usluga potpuno je nedostupna dulje od 30 minuta;

(b) u razdoblju duljem od jednog sata prosječno vrijeme odgovora neke rekurzivne ili autoritativne DNS usluge na DNS upite dulje je od 10 sekundi;

(c) ugrožena je cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem usluga DNS-a, osim u slučajevima kad podaci manje od 1 000 naziva domena kojima upravlja pružatelj usluga DNS-a, a koji čine najviše 1 % naziva domena kojima upravlja pružatelj usluga DNS-a, nisu točni zbog pogrešne konfiguracije.

Članak 6.

Značajni incidenti za registre naziva vršnih domena

Kad je riječ o registrima naziva vršnih domena, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neka autoritativna DNS usluga potpuno je nedostupna;

(b) u razdoblju duljem od jednog sata prosječno vrijeme odgovora neke autoritativne DNS usluge na DNS upite dulje je od 10 sekundi;

(c) ugrožena je cjelovitost, povjerljivost ili vjerodostojnost pohranjenih, prenesenih ili obrađenih podataka povezanih s tehničkim funkcioniranjem vršne domene.

Članak 7.

Značajni incidenti za pružatelje usluga računalstva u oblaku

Kad je riječ o pružateljima usluga računalstva u oblaku, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neka pružana usluga računalstva u oblaku potpuno je nedostupna dulje od 30 minuta;

(b) dostupnost neke pružateljeve usluge računalstva u oblaku ograničena je za više od 5 % korisnika te usluge računalstva u oblaku u Uniji ili za više od 1 milijun korisnika te usluge računalstva u oblaku u Uniji, ovisno o tome koji je broj manji, u trajanju duljem od jednog sata;

(c) zbog pretpostavljeno zlonamjerne radnje ugrožena je cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke usluge računalstva u oblaku;

(d) cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem usluge računalstva u oblaku ugrožena je tako da to utječe na više od 5 % korisnika te usluge računalstva u oblaku u Uniji ili na više od 1 milijun korisnika te usluge računalstva u oblaku u Uniji, ovisno o tome koji je broj manji.

Članak 8.

Značajni incidenti za pružatelje usluga podatkovnog centra

Kad je riječ o pružateljima usluga podatkovnog centra, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neka usluga podatkovnog centra koju pruža podatkovni centar kojim upravlja pružatelj potpuno je nedostupna;

(b) dostupnost neke usluge podatkovnog centra koju pruža podatkovni centar kojim upravlja pružatelj ograničena je u trajanju duljem od jednog sata;

(c) zbog pretpostavljeno zlonamjerne radnje ugrožena je cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke usluge podatkovnog centra;

(d) ugrožen je fizički pristup nekom podatkovnom centru kojim upravlja pružatelj.

Članak 9.

Značajni incidenti za pružatelje mreža za isporuku sadržaja

Kad je riječ o pružateljima mreža za isporuku sadržaja, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neka mreža za isporuku sadržaja potpuno je nedostupna dulje od 30 minuta;

(b) dostupnost neke mreže za pružanje sadržaja ograničena je za više od 5 % korisnika te mreže za pružanje sadržaja u Uniji ili za više od 1 milijun korisnika te mreže za pružanje sadržaja u Uniji, ovisno o tome koji je broj manji, u trajanju duljem od jednog sata;

(c) zbog pretpostavljeno zlonamjerne radnje ugrožena je cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke mreže za pružanje sadržaja;

(d) cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke mreže za pružanje sadržaja ugrožena je tako da to utječe na više od 5 % korisnika te mreže za pružanje sadržaja u Uniji ili na više od 1 milijun korisnika te mreže za pružanje sadržaja u Uniji, ovisno o tome koji je broj manji.

Članak 10.

Značajni incidenti za pružatelje upravljanih usluga i pružatelje upravljanih sigurnosnih usluga

Kad je riječ o pružateljima upravljanih usluga i pružateljima upravljanih sigurnosnih usluga, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neka upravljana usluga ili upravljana sigurnosna usluga potpuno je nedostupna dulje od 30 minuta;

(b) dostupnost neke upravljane usluge ili upravljane sigurnosne usluge ograničena je za više od 5 % korisnika te usluge u Uniji ili za više od 1 milijun korisnika te usluge u Uniji, ovisno o tome koji je broj manji, u trajanju duljem od jednog sata;

(c) zbog pretpostavljeno zlonamjerne radnje ugrožena je cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke upravljane usluge ili upravljane sigurnosne usluge;

(d) cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke upravljane usluge ili upravljane sigurnosne usluge ugrožena je tako da to utječe na više od 5 % korisnika te upravljane usluge ili te upravljane sigurnosne usluge u Uniji ili na više od 1 milijun korisnika te usluge u Uniji, ovisno o tome koji je broj manji.

Članak 11.

Značajni incidenti za pružatelje internetskih tržišta

Kad je riječ o pružateljima internetskih tržišta, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neko internetsko tržište potpuno je nedostupno za više od 5 % korisnika tog internetskog tržišta u Uniji ili za više od 1 milijun korisnika tog internetskog tržišta u Uniji, ovisno o tome koji je broj manji;

(b) ograničena dostupnost nekog internetskog tržišta utječe na više od 5 % korisnika tog internetskog tržišta u Uniji ili na više od 1 milijun korisnika tog internetskog tržišta u Uniji, ovisno o tome koji je broj manji;

(c) zbog pretpostavljeno zlonamjerne radnje ugrožena je cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem nekog internetskog tržišta;

(d) cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem nekog internetskog tržišta ugrožena je tako da to utječe na više od 5 % korisnika tog internetskog tržišta u Uniji ili na više od 1 milijun korisnika tog internetskog tržišta u Uniji, ovisno o tome koji je broj manji.

Članak 12.

Značajni incidenti za pružatelje internetskih tražilica

Kad je riječ o pružateljima internetskih tražilica, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neka internetska tražilica potpuno je nedostupna za više od 5 % korisnika te internetske tražilice u Uniji ili za više od 1 milijun korisnika te internetske tražilice u Uniji, ovisno o tome koji je broj manji;

(b) ograničena dostupnost neke internetske tražilice utječe na više od 5 % korisnika te internetske tražilice u Uniji ili na više od 1 milijun korisnika te internetske tražilice u Uniji, ovisno o tome koji je broj manji;

(c) zbog pretpostavljeno zlonamjerne radnje ugrožena je cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke internetske tražilice;

(d) cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke internetske tražilice ugrožena je tako da to utječe na više od 5 % korisnika te internetske tražilice u Uniji ili na više od 1 milijun korisnika te internetske tražilice u Uniji, ovisno o tome koji je broj manji.

Članak 13.

Značajni incidenti za pružatelje platformi za usluge društvenih mreža

Kad je riječ o pružateljima platformi za usluge društvenih mreža, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neka platforma za usluge društvenih mreža potpuno je nedostupna za više od 5 % korisnika te platforme za usluge društvenih mreža u Uniji ili za više od 1 milijun korisnika te platforme za usluge društvenih mreža u Uniji, ovisno o tome koji je broj manji;

(b) ograničena dostupnost neke platforme za usluge društvenih mreža utječe na više od 5 % korisnika te platforme za usluge društvenih mreža u Uniji ili na više od 1 milijun korisnika te platforme za usluge društvenih mreža u Uniji, ovisno o tome koji je broj manji;

(c) zbog pretpostavljeno zlonamjerne radnje ugrožena je cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke platforme za usluge društvenih mreža;

(d) cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke platforme za usluge društvenih mreža ugrožena je tako da to utječe na više od 5 % korisnika te platforme za usluge društvenih mreža u Uniji ili na više od 1 milijun korisnika usluga te platforme za usluge društvenih mreža u Uniji, ovisno o tome koji je broj manji.

Članak 14.

Značajni incidenti za pružatelje usluga povjerenja

Kad je riječ o pružateljima usluga povjerenja, incident se smatra značajnim na temelju članka 3. stavka 1. točke (g) ako ispunjava barem jedan od sljedećih kriterija:

(a) neka usluga povjerenja potpuno je nedostupna dulje od 20 minuta;

(b) neka usluga povjerenja nije dostupna korisnicima ili pouzdajućim stranama dulje od jednog sata u kalendarskom tjednu;

(c) ograničena dostupnost neke usluge povjerenja utječe na više od 1 % korisnika ili pouzdajućih strana u Uniji ili na više od 200 000 korisnika ili pouzdajućih strana u Uniji, ovisno o tome koji je broj manji;

(d) ugrožen je fizički pristup prostoru u kojem se nalaze mrežni i informacijski sustavi i kojem pristup ima samo pouzdano osoblje pružatelja usluga povjerenja ili je ugrožena zaštita takvog fizičkog pristupa;

(e) cjelovitost, povjerljivost ili autentičnost pohranjenih, prenesenih ili obrađenih podataka povezanih s pružanjem neke usluge povjerenja ugrožena je tako da to utječe na 0,1 % korisnika ili pouzdajućih strana ili na više od 100 korisnika ili pouzdajućih strana usluge povjerenja u Uniji, ovisno o tome koji je broj manji.

Članak 15.

Stavljanje izvan snage

Provedbena uredba Komisije (EU) 2018/151 ([4]) stavlja se izvan snage.

Članak 16.

Stupanje na snagu i primjena

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

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

Sastavljeno u Bruxellesu 17. listopada 2024.

Za Komisiju
Ursula VON DER LEYEN
Predsjednica

([4]) Provedbena uredba Komisije (EU) 2018/151 od 30. siječnja 2018. o utvrđivanju pravila za primjenu Direktive (EU) 2016/1148 Europskog parlamenta i Vijeća u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident znatan učinak (SL L 26, 31.1.2018., str. 48., ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

PRILOG

Tehnički i metodološki zahtjevi iz članka 2. ove Uredbe

1. **Politika sigurnosti mrežnih i informacijskih sustava (članak 21. stavak 2. točka (a) Direktive (EU) 2022/2555)**

1.1. *Politika sigurnosti mrežnih i informacijskih sustava*

1.1.1. Za potrebe članka 21. stavka 2. točke (a) Direktive (EU) 2022/2555 politika sigurnosti mrežnih i informacijskih sustava mora:

(a) definirati kako relevantni subjekti pristupaju sigurnosti svojih mrežnih i informacijskih sustava;

(b) odgovarati i biti komplementarna poslovnoj strategiji i ciljevima relevantnih subjekata;

(c) definirati ciljeve mrežne i informacijske sigurnosti;

(d) sadržavati obvezu kontinuiranog poboljšavanja sigurnosti mrežnih i informacijskih sustava;

(e) sadržavati obvezu osiguravanja odgovarajućih sredstava potrebnih za njezinu provedbu, uključujući potrebno osoblje, financijska sredstva, postupke, alate i tehnologije;

(f) biti priopćena relevantnim zaposlenicima i relevantnim zainteresiranim vanjskim stranama, koji moraju potvrditi da je prihvaćaju;

(g) definirati uloge i odgovornosti u skladu s točkom 1.2.;

(h) sadržavati popis dokumentacije koju treba čuvati i koliko dugo;

(i) sadržavati popis tematskih politika;

(j) definirati pokazatelje i mjere za praćenje njezine provedbe i razine zrelosti mrežne i informacijske sigurnosti relevantnih subjekata;

(k) sadržavati datum na koji su je službeno odobrila upravljačka tijela relevantnih subjekata („upravljačka tijela”).

1.1.2. Upravljačka tijela politiku sigurnosti mrežnih i informacijskih sustava preispituju i, prema potrebi, ažuriraju najmanje jednom godišnje i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima. Rezultati preispitivanja moraju se dokumentirati.

1.2. *Uloge, odgovornosti i ovlasti*

1.2.1. U okviru svoje politike sigurnosti mrežnih i informacijskih sustava iz točke 1.1. relevantni subjekti utvrđuju odgovornosti i ovlasti za sigurnost mrežnih i informacijskih sustava, povezuju ih s ulogama, raspodjeljuju ih u skladu s potrebama relevantnih subjekata te o njima obavješćuju upravljačka tijela.

1.2.2. Relevantni subjekti zahtijevaju od svih zaposlenika i trećih strana da štite sigurnost mrežnih i informacijskih sustava u skladu s uspostavljenom politikom mrežne i informacijske sigurnosti, tematskim politikama i postupcima relevantnih subjekata.

1.2.3. Najmanje jedna osoba mora izravno odgovarati upravljačkom tijelu kad je riječ o pitanjima sigurnosti mrežnih i informacijskih sustava.

1.2.4. Ovisno o veličini relevantnih subjekata, za sigurnost mrežnih i informacijskih sustava određuju se posebne uloge ili dužnosti koje se izvršavaju uz postojeće uloge.

1.2.5. Ako je to primjenjivo, proturječne dužnosti i proturječna područja odgovornosti moraju se razdvojiti.

1.2.6. Upravljačka tijela preispituju uloge, odgovornosti i ovlasti te ih, prema potrebi, ažuriraju u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

2. **Politika upravljanja rizicima (članak 21. stavak 2. točka (a) Direktive (EU) 2022/2555)**

2.1. *Okvir za upravljanje rizicima*

2.1.1. Za potrebe članka 21. stavka 2. točke (a) Direktive (EU) 2022/2555 relevantni subjekti uspostavljaju i primjenjuju odgovarajući okvir za upravljanje rizicima radi utvrđivanja i suzbijanja rizika za sigurnost mrežnih i informacijskih sustava. Provode i dokumentiraju procjene rizika i na temelju njihovih rezultata izrađuju, provode i prate plan postupanja s rizicima. Rezultate procjene rizika i preostale rizike moraju prihvatiti upravljačka tijela ili, ako je to primjenjivo, osobe koje su odgovorne i ovlaštene za upravljanje rizicima, pod uvjetom da relevantni subjekti o tome na odgovarajući način izvijeste upravljačka tijela.

2.1.2. Za potrebe točke 2.1.1. relevantni subjekti uspostavljaju procedure za utvrđivanje, analizu, procjenu i postupanje s rizicima („postupak upravljanja kibernetičkosigurnosnim rizicima”). Postupak upravljanja kibernetičkosigurnosnim rizicima, ako je to primjenjivo, čini sastavni dio cjelokupnog postupka upravljanja rizicima relevantnih subjekata. U okviru postupka upravljanja kibernetičkosigurnosnim rizicima relevantni subjekti dužni su:

(a) primjenjivati metodologiju upravljanja rizicima;

(b) utvrditi razinu tolerancije na rizik u skladu sa svojom sklonošću preuzimanju rizika;

(c) utvrditi i revidirati relevantne kriterije rizika;

(d) u skladu s pristupom kojim se u obzir uzimaju sve opasnosti utvrditi i dokumentirati rizike za sigurnost mrežnih i informacijskih sustava, posebno u vezi s trećim stranama, i rizike koji bi mogli izazvati poremećaje u dostupnosti, cjelovitosti, autentičnosti i povjerljivosti mrežnih i informacijskih sustava, uključujući utvrđivanje jedinstvenih točaka kvara;

(e) analizirati rizike za sigurnost mrežnih i informacijskih sustava, uključujući prijetnje, vjerojatnost, učinak i razinu rizika, uzimajući pritom u obzir saznanja o kibernetičkim prijetnjama i ranjivostima;

(f) evaluirati utvrđene rizike na temelju kriterija rizika;

(g) utvrditi odgovarajuće mogućnosti i mjere za postupanje s rizicima i odrediti njihov prioritet;

(h) kontinuirano pratiti provedbu mjera za postupanje s rizicima;

(i) utvrditi tko je odgovoran za provedbu mjera za postupanje s rizicima i kada ih treba provesti;

(j) u planu postupanja s rizicima na razumljiv način potkrijepiti odabrane mjere za postupanje s rizicima i razloge za prihvaćanje preostalih rizika.

2.1.3. Pri utvrđivanju i određivanju prioriteta odgovarajućih mogućnosti i mjera za postupanje s rizicima relevantni subjekti uzimaju u obzir rezultate procjene rizika, rezultate postupka za procjenu učinkovitosti mjera upravljanja kibernetičkosigurnosnim rizicima, trošak provedbe u odnosu na očekivanu korist, klasifikaciju imovine iz točke 12.1. i analizu učinka na poslovanje iz točke 4.1.3.

2.1.4. Relevantni subjekti preispituju i prema potrebi ažuriraju rezultate procjene rizika i plan postupanja s rizicima u planiranim intervalima, a najmanje jednom godišnje, i kad se dogode znatne promjene u poslovanju ili rizicima ili značajni incidenti.

2.2. *Praćenje usklađenosti*

2.2.1. Relevantni subjekti redovito preispituju pridržavaju li se svojih politika o sigurnosti mrežnih i informacijskih sustava te tematskih politika, pravila i normi. Upravljačka tijela moraju dobivati redovita izvješća o stanju mrežne i informacijske sigurnosti koja se temelje na preispitivanjima usklađenosti.

2.2.2. Relevantni subjekti uspostavljaju djelotvoran sustav izvješćivanja o usklađenosti koji je primjeren njihovim strukturama, operativnim okruženjima i prijetnjama. Sustav za izvješćivanje o usklađenosti mora biti takav da upravljačkim tijelima može pružiti utemeljeni pregled trenutačnog stanja upravljanja rizicima relevantnih subjekata.

2.2.3. Relevantni subjekti usklađenost prate u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

2.3. *Neovisna revizija informacijske i mrežne sigurnosti*

2.3.1. Relevantni subjekti provode neovisnu reviziju svojeg pristupa upravljanju sigurnošću mrežnih i informacijskih sustava i njegove provedbe, uključujući osobe, postupke i tehnologije.

2.3.2. Relevantni subjekti uspostavljaju, primjenjuju i revidiraju postupke za provedbu neovisnih revizija koje moraju provoditi osobe s odgovarajućim revizijskim kompetencijama. Ako neovisnu reviziju provode članovi osoblja relevantnog subjekta, osobe koje provode reviziju ne smiju biti u hijerarhijskom odnosu s osobljem odgovornim za područje koje se revidira. Ako veličina relevantnih subjekata ne dopušta takvo razdvajanje ovlasti, relevantni subjekti dužni su uvesti alternativne mjere da zajamče nepristranost revizije.

2.3.3. O rezultatima neovisnih revizija, uključujući rezultate praćenja usklađenosti u skladu s točkom 2.2. te praćenja i mjerenja u skladu s točkom 7., izvješćuju se upravljačka tijela. Ovisno o kriterijima prihvatljivosti rizika relevantnih subjekata poduzimaju se korektivne mjere ili se prihvaća preostali rizik.

2.3.4. Relevantni subjekti provode neovisne revizije u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

3. **Postupanje s incidentima (članak 21. stavak 2. točka (b) Direktive (EU) 2022/2555)**

3.1. *Politika postupanja s incidentima*

3.1.1. Za potrebe članka 21. stavka 2. točke (b) Direktive (EU) 2022/2555 relevantni subjekti uspostavljaju i provode politiku postupanja s incidentima u okviru koje utvrđuju uloge, odgovornosti i postupke za pravodobno otkrivanje i analizu incidenata, ograničavanje ili odgovaranje na njih, oporavak od incidenata te njihovo dokumentiranje i izvješćivanje o njima.

3.1.2. Politika iz točke 3.1.1. mora biti usklađena s planom kontinuiteta poslovanja i oporavka od katastrofe iz točke 4.1. Ta politika mora sadržavati:

(a) sustav kategorizacije incidenata koji je u skladu s procjenom i klasifikacijom događaja koje se provode u skladu s točkom 3.4.1.;

(b) djelotvorne komunikacijske planove, među ostalim za upućivanje na više razine i izvješćivanje;

(c) raspodjelu uloga u otkrivanju i prikladnom odgovoru na incidente kompetentnim zaposlenicima;

(d) dokumente za upotrebu pri otkrivanju i odgovaranju na incidente, kao što su priručnici za odgovaranje na incidente, dijagrami za upućivanje na više razine, popisi kontakata i predlošci.

3.1.3. Uloge, odgovornosti i postupci utvrđeni u toj politici testiraju se i revidiraju te se, prema potrebi, ažuriraju u planiranim intervalima i nakon značajnih incidenata ili znatnih promjena u poslovanju ili rizicima.

3.2. *Praćenje i evidentiranje*

3.2.1. Relevantni subjekti utvrđuju postupke i koriste alate za praćenje i evidentiranje aktivnosti u svojim mrežnim i informacijskim sustavima radi otkrivanja događaja koji bi se mogli smatrati incidentima i prikladnog odgovora u cilju ublažavanja njihovih posljedica.

3.2.2. U mjeri u kojoj je to izvedivo, praćenje se automatizira i provodi kontinuirano ili periodično, ovisno o poslovnim kapacitetima. Relevantni subjekti svoje aktivnosti praćenja provode tako da se lažno pozitivni i lažno negativni rezultati svedu na najmanju moguću mjeru.

3.2.3. Relevantni subjekti vode, dokumentiraju i pregledavaju evidenciju na temelju postupaka iz točke 3.2.1. Relevantni subjekti na temelju rezultata procjene rizika provedene u skladu s točkom 2.1. sastavljaju popis imovine koju treba evidentirati. Prema potrebi se evidentiraju:

(a) relevantni odlazni i dolazni mrežni promet;

(b) izrada, izmjena ili brisanje korisnika mrežnih i informacijskih sustava relevantnih subjekata i proširenje odobrenja;

(c) pristup sustavima i aplikacijama;

(d) događaji povezani s autentifikacijom;

(e) svaki povlašteni pristup sustavima i aplikacijama te aktivnosti koje obavljaju administrativni računi;

(f) pristup ključnim konfiguracijskim datotekama i sigurnosnim kopijama ili njihove izmjene;

(g) evidencije događaja i evidencije iz sigurnosnih alata, kao što su antivirusni programi, sustavi za otkrivanje neovlaštenog ulaska ili vatrozidovi;

(h) korištenje resursa sustava i njihove performanse;

(i) fizički pristup objektima;

(j) pristup njihovoj mrežnoj opremi i uređajima te njihova upotreba;

(k) vrijeme početka, kraja i privremenog prekida vođenja raznih evidencija;

(l) događaji u okolišu.

3.2.4. Evidencije se redovito pregledavaju kako bi se utvrdili eventualni neuobičajeni ili neželjeni trendovi. Relevantni subjekti prema potrebi utvrđuju primjerene vrijednosti za alarmne pragove. Ako se vrijednosti alarmnih pragova prekorače, alarm se, prema potrebi, aktivira automatski. Relevantni subjekti dužni su pobrinuti se da u slučaju alarma na vrijeme započne stručan i prikladan odgovor.

3.2.5. Relevantni subjekti vode evidencije i čuvaju njihove sigurnosne kopije tijekom unaprijed utvrđenog razdoblja te ih štite od neovlaštenog pristupa ili izmjena.

3.2.6. U mjeri u kojoj je to izvedivo, relevantni subjekti dužni su pobrinuti se da vremenski izvori svih sustava budu sinkronizirani kako bi se radi procjene događaja mogle uspostaviti korelacije između evidencija raznih sustava. Relevantni subjekti sastavljaju i vode popis sve imovine koja se evidentira te vode računa o tome da su sustavi praćenja i evidentiranja redundantni. Raspoloživost sustava za praćenje i evidentiranje prati se odvojeno od sustava koje ti sustavi prate.

3.2.7. Postupci i popis imovine koja se evidentira preispituju se i, prema potrebi, ažuriraju u redovitim intervalima i nakon značajnih incidenata.

3.3. *Prijavljivanje događaja*

3.3.1. Relevantni subjekti uspostavljaju jednostavan mehanizam koji njihovim zaposlenicima, dobavljačima i kupcima omogućuje prijavljivanje sumnjivih događaja.

3.3.2. Relevantni subjekti prema potrebi obavješćuju svoje dobavljače i kupce o mehanizmu za prijavljivanje događaja i redovito obučavaju svoje zaposlenike za njegovu upotrebu.

3.4. *Procjena i klasifikacija događaja*

3.4.1. Relevantni subjekti procjenjuju sumnjive događaje kako bi utvrdili jesu li oni incidenti i, ako jesu, koje su prirode i koliko su ozbiljni.

3.4.2. Za potrebe točke 3.4.1. relevantni subjekti postupaju na sljedeći način:

(a) provode procjenu na temelju unaprijed utvrđenih kriterija i trijaže kako bi odredili prioritete radi ograničavanja i iskorjenjivanja incidenata;

(b) svaka tri mjeseca procjenjuju pojavu incidenata koji se ponavljaju kako su opisani u članku 4. ove Uredbe;

(c) pregledavaju odgovarajuće evidencije za potrebe procjene i klasifikacije događaja;

(d) uspostavljaju postupak za korelaciju i analizu evidencija;

(e) ponovno procjenjuju i reklasificiraju događaje ako postanu dostupne nove informacije ili nakon analize već dostupnih informacija.

3.5. *Odgovor na incidente*

3.5.1. Relevantni subjekti na incidente odgovaraju pravodobno i u skladu s dokumentiranim postupcima.

3.5.2. Postupci odgovora na incidente moraju uključivati sljedeće faze:

(a) ograničavanje incidenta kako bi se spriječilo širenje njegovih posljedica;

(b) iskorjenjivanje, kako bi se spriječio nastavak ili ponovna pojava incidenta;

(c) prema potrebi, oporavak od incidenta.

3.5.3. Relevantni subjekti izrađuju komunikacijske planove i uspostavljaju postupke:

(a) za obavješćivanje o incidentima, i to u suradnji s timovima za odgovor na računalne sigurnosne incidente (CSIRT-ovi) ili, ako je to primjenjivo, s nadležnim tijelima;

(b) za komunikaciju među članovima osoblja relevantnog subjekta i komunikaciju s relevantnim dionicima izvan relevantnog subjekta.

3.5.4. Relevantni subjekti evidentiraju aktivnosti odgovora na incidente u skladu s postupcima iz točke 3.2.1. i pohranjuju dokaze.

3.5.5. Relevantni subjekti svoje postupke odgovora na incidente testiraju u planiranim intervalima.

3.6. *Pregledi nakon incidenta*

3.6.1. Relevantni subjekti nakon oporavka od incidenta prema potrebi provode preglede nakon incidenta. Pregledima nakon incidenta utvrđuje se, ako je to moguće, temeljni uzrok incidenta i dokumentiraju se stečena iskustva kako bi se smanjile učestalost i posljedice budućih incidenata.

3.6.2. Relevantni subjekti dužni su pobrinuti se da pregledi nakon incidenta doprinesu poboljšanju njihova pristupa mrežnoj i informacijskoj sigurnosti, mjera za postupanje s rizicima te postupaka rješavanja incidenata, otkrivanja i odgovora na incidente.

3.6.3. Relevantni subjekti u planiranim intervalima provjeravaju jesu li incidenti rezultirali pregledima nakon incidenta.

4. **Kontinuitet poslovanja i upravljanje rizicima (članak 21. stavak 2. točka (c) Direktive (EU) 2022/2555)**

4.1. *Plan kontinuiteta poslovanja i oporavka od katastrofe*

4.1.1. Za potrebe članka 21. stavka 2. točke (c) Direktive (EU) 2022/2555 relevantni subjekti utvrđuju i provode plan kontinuiteta poslovanja i oporavka od katastrofe koji se primjenjuje u slučaju incidenata.

4.1.2. Poslovne aktivnosti relevantnih subjekata ponovno se uspostavljaju u skladu s planom kontinuiteta poslovanja i oporavka od katastrofe. Plan se temelji na rezultatima procjene rizika provedene u skladu s točkom 2.1. te mora, prema potrebi, sadržavati:

(a) svrhu, opseg i osobe kojima je namijenjen;

(b) uloge i odgovornosti;

(c) ključne kontakte i (unutarnje i vanjske) komunikacijske kanale;

(d) uvjete za aktivaciju i deaktivaciju plana;

(e) redoslijed oporavka poslovnih aktivnosti;

(f) planove oporavka za specifične poslovne aktivnosti, uključujući ciljeve oporavka;

(g) potrebna sredstva, uključujući sigurnosne kopije i redundancije;

(h) pojedinosti o ponovnoj uspostavi i nastavku aktivnosti nakon privremenih mjera.

4.1.3. Relevantni subjekti provode analizu učinka kako bi procijenili mogući učinak ozbiljnih poremećaja na svoje poslovne aktivnosti i na temelju rezultata te analize utvrđuju zahtjeve u pogledu kontinuiteta koji se primjenjuju na mrežne i informacijske sustave.

4.1.4. Plan kontinuiteta poslovanja i oporavka od katastrofe testira se, preispituje i, prema potrebi, ažurira u planiranim intervalima i nakon značajnih incidenata ili znatnih promjena u poslovanju ili rizicima. Relevantni subjekti dužni su se pobrinuti da se saznanja dobivena iz takvih testiranja uvrste u planove.

4.2. *Upravljanje sigurnosnim kopijama i redundancijama*

4.2.1. Relevantni subjekti izrađuju sigurnosne kopije podataka i osiguravaju dovoljno raspoloživih resursa, uključujući objekte, mrežne i informacijske sustave i osoblje, da se postigne odgovarajuća razina redundancije.

4.2.2. Na temelju rezultata procjene rizika provedene u skladu s točkom 2.1. i plana kontinuiteta poslovanja relevantni subjekti izrađuju planove za sigurnosne kopije koji moraju obuhvaćati:

(a) vremena oporavka;

(b) jamstvo da su sigurnosne kopije potpune i točne, uključujući konfiguracijske podatke i podatke pohranjene u okruženju usluga računalstva u oblaku;

(c) pohranjivanje sigurnosnih kopija (na internetu ili izvan njega) na sigurnoj lokaciji ili lokacijama koje nisu u istoj mreži kao i sustav te su dovoljno udaljene da se izbjegne bilo kakva šteta od katastrofe na glavnoj lokaciji;

(d) odgovarajuću fizičku i logičku kontrolu pristupa sigurnosnim kopijama, u skladu s klasifikacijskom razinom resursa;

(e) oporavak podataka iz sigurnosnih kopija;

(f) rokove čuvanja na temelju poslovnih i regulatornih zahtjeva.

4.2.3. Relevantni subjekti dužni su redovito provjeravati cjelovitost sigurnosnih kopija.

4.2.4. Na temelju rezultata procjene rizika provedene u skladu s točkom 2.1. i plana kontinuiteta poslovanja relevantni subjekti osiguravaju dovoljno raspoloživih resursa barem djelomičnom redundancijom sljedećih elemenata:

(a) mrežnih i informacijskih sustava;

(b) imovine, uključujući objekte, opremu i zalihe;

(c) osoblja s primjerenom razinom odgovornosti, ovlasti i stručnosti;

(d) odgovarajućih komunikacijskih kanala.

4.2.5. Relevantni subjekti prema potrebi vode računa o tome da se zahtjevi za izradu sigurnosnih kopija i redundanciju primjereno uzimaju u obzir u praćenju i prilagodbi resursa, uključujući objekte, sustave i osoblje.

4.2.6. Relevantni subjekti redovito testiraju oporavak sigurnosnih kopija i redundancije kako bi osigurali njihovu pouzdanost u uvjetima oporavka i da obuhvaćaju kopije, postupke i znanje potrebne za uspješan oporavak. Relevantni subjekti dokumentiraju rezultate testiranja i, prema potrebi, poduzimaju korektivne mjere.

4.3. *Upravljanje krizama*

4.3.1. Relevantni subjekti uspostavljaju postupak za upravljanje krizama.

4.3.2. Relevantni subjekti osiguravaju da postupak za upravljanje krizama obuhvaća barem sljedeće elemente:

(a) uloge i odgovornosti osoblja i, prema potrebi, dobavljača i pružatelja usluga, uz navođenje raspodjele uloga u kriznim situacijama, uključujući konkretne korake koje treba poduzeti;

(b) odgovarajuća sredstva komunikacije između relevantnih subjekata i relevantnih nadležnih tijela;

(c) primjenu odgovarajućih mjera za održavanje sigurnosti mrežnih i informacijskih sustava u kriznim situacijama.

Za potrebe točke (b) protok informacija između relevantnih subjekata i relevantnih nadležnih tijela obuhvaća obveznu komunikaciju, kao što su izvješća o incidentima i pripadajuće rokove, i neobveznu komunikaciju.

4.3.3. Relevantni subjekti uspostavljaju postupak za upravljanje i korištenje informacijama o incidentima, ranjivostima, prijetnjama ili mogućim mjerama ublažavanja koje prime od CSIRT-ova ili, ako je to primjenjivo, nadležnih tijela.

4.3.4. Relevantni subjekti redovito ili nakon značajnih incidenata ili znatnih promjena u poslovanju ili rizicima testiraju, preispituju i prema potrebi ažuriraju plan upravljanja krizama.

5. **Sigurnost lanca opskrbe (članak 21. stavak 2. točka (d) Direktive (EU) 2022/2555)**

5.1. *Politika sigurnosti lanca opskrbe*

5.1.1. Za potrebe članka 21. stavka 2. točke (d) Direktive (EU) 2022/2555 relevantni subjekti utvrđuju, uvode i provode politiku sigurnosti lanca opskrbe kojom se uređuju odnosi s njihovim izravnim dobavljačima i pružateljima usluga kako bi se ublažili utvrđeni rizici za sigurnost mrežnih i informacijskih sustava. Politikom sigurnosti lanca opskrbe relevantni subjekti utvrđuju svoju ulogu u lancu opskrbe i o njoj obavješćuju svoje izravne dobavljače i pružatelje usluga.

5.1.2. U okviru politike sigurnosti lanca opskrbe iz točke 5.1.1. relevantni subjekti utvrđuju kriterije za odabir i sklapanje ugovora s dobavljačima i pružateljima usluga. Ti kriteriji moraju obuhvaćati:

(a) kibernetičkosigurnosne prakse dobavljača i pružatelja usluga, uključujući sigurne postupke njihova razvoja;

(b) sposobnost dobavljača i pružatelja usluga da ispune kibernetičkosigurnosne specifikacije koje utvrde relevantni subjekti;

(c) opću kvalitetu i otpornost IKT proizvoda i usluga te mjere upravljanja kibernetičkosigurnosnim rizicima koje su u njih ugrađene, uključujući rizike i klasifikacijsku razinu IKT proizvoda i usluga;

(d) sposobnost relevantnih subjekata da diversificiraju izvore opskrbe i ograniče ovisnost o jednom dobavljaču, ako je to primjenjivo.

5.1.3. Pri uspostavi politike sigurnosti lanca opskrbe relevantni subjekti dužni su, ako je to primjenjivo, u obzir uzeti rezultate relevantnih koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe provedenih u skladu s člankom 22. stavkom 1. Direktive (EU) 2022/2555.

5.1.4. Na temelju politike sigurnosti lanca opskrbe i uzimajući u obzir rezultate procjene rizika provedene u skladu s točkom 2.1. ovog Priloga relevantni subjekti dužni su u svojim ugovorima s dobavljačima i pružateljima usluga, prema potrebi putem sporazuma o razini usluga, navesti sljedeće:

(a) kibernetičkosigurnosne zahtjeve za dobavljače ili pružatelje usluga, uključujući sigurnosne zahtjeve za nabavu IKT usluga ili proizvoda iz točke 6.1.;

(b) zahtjeve u pogledu informiranosti, vještina i osposobljavanja te, prema potrebi, certifikata koje moraju imati zaposlenici dobavljača ili pružatelja usluga;

(c) zahtjeve u pogledu provjera zaposlenika dobavljača i pružatelja usluga;

(d) obvezu dobavljača i pružatelja usluga da bez nepotrebne odgode obavijeste relevantne subjekte o incidentima koji predstavljaju rizik za sigurnost mrežnih i informacijskih sustava tih subjekata;

(e) pravo na reviziju ili pravo na primanje revizorskih izvješća;

(f) obvezu dobavljača i pružatelja usluga da otklanjaju ranjivosti koje predstavljaju rizik za sigurnost mrežnih i informacijskih sustava relevantnih subjekata;

(g) zahtjeve u pogledu podugovaranja i, ako relevantni subjekti dopuštaju podugovaranje, kibernetičkosigurnosne zahtjeve za podugovaratelje u skladu s kibernetičkosigurnosnim zahtjevima iz točke (a);

(h) obveze dobavljača i pružatelja usluga kod prestanka ugovora, kao što su dohvaćanje i uklanjanje informacija koje su dobavljači i pružatelji usluga dobili tijekom izvršavanja svojih zadaća.

5.1.5. U postupcima odabira novih dobavljača i pružatelja usluga i u postupku nabave iz točke 6.1. relevantni subjekti uzimaju u obzir elemente iz točaka 5.1.2. i 5.1.3.

5.1.6. Relevantni subjekti preispituju politiku sigurnosti lanca opskrbe te prate, ocjenjuju i, prema potrebi, reagiraju na promjene u kibernetičkosigurnosnim praksama dobavljača i pružatelja usluga, i to u planiranim intervalima i kad se dogode znatne promjene u poslovanju ili rizicima ili značajni incidenti koji su povezani s pružanjem IKT usluga ili utječu na sigurnost IKT proizvoda koje nude dobavljači i pružatelji usluga.

5.1.7. Za potrebe točke 5.1.6. relevantni subjekti:

(a) ako je to primjenjivo, redovito prate izvješća o provedbi sporazuma o razini usluga;

(b) provjeravaju incidente povezane s IKT proizvodima i uslugama dobavljača i pružatelja usluga;

(c) procjenjuju potrebu za neplaniranim provjerama i dokumentiraju nalaze na razumljiv način;

(d) analiziraju rizike od promjena povezanih s IKT proizvodima i uslugama dobavljača i pružatelja usluga te, prema potrebi, pravodobno poduzimaju mjere ublažavanja.

5.2. *Registar dobavljača i pružatelja usluga*

Relevantni subjekti vode i ažuriraju registar svojih izravnih dobavljača i pružatelja usluga, uključujući:

(a) kontaktne točke za svakog izravnog dobavljača i pružatelja usluga;

(b) popis IKT proizvoda, usluga i procesa koje relevantnim subjektima pruža izravni dobavljač ili pružatelj usluga.

6. **Sigurnost nabave, razvoja i održavanja mrežnih i informacijskih sustava (članak 21. stavak 2. točka (e) Direktive (EU) 2022/2555)**

6.1. *Sigurnost nabave IKT usluga ili proizvoda*

6.1.1. Za potrebe članka 21. stavka 2. točke (e) Direktive (EU) 2022/2555 relevantni subjekti na temelju procjene rizika provedene u skladu s točkom 2.1. utvrđuju i provode postupke za upravljanje rizicima koji proizlaze iz IKT usluga ili proizvoda koje od dobavljača ili pružatelja usluga nabavljaju za komponente ključne za sigurnost mrežnih i informacijskih sustava relevantnih subjekata tijekom cijelog njihova životnog ciklusa.

6.1.2. Za potrebe točke 6.1.1. postupci navedeni u toj točki obuhvaćaju:

(a) sigurnosne zahtjeve koji se primjenjuju na IKT usluge ili proizvode koji se nabavljaju;

(b) zahtjeve u pogledu sigurnosnih ažuriranja tijekom cijelog životnog vijeka IKT usluga ili proizvoda ili u pogledu zamjene nakon isteka razdoblja podrške;

(c) informacije o hardverskim i softverskim komponentama koje se koriste u IKT uslugama ili proizvodima;

(d) informacije o implementiranim kibernetičkosigurnosnim funkcijama IKT usluga ili proizvoda i konfiguraciji potrebnoj za njihov siguran rad;

(e) jamstvo da su IKT usluge ili proizvodi sukladni sa sigurnosnim zahtjevima iz točke (a);

(f) metode za validaciju sukladnosti isporučenih IKT usluga ili proizvoda s navedenim sigurnosnim zahtjevima i dokumentaciju o rezultatima validacije.

6.1.3. Relevantni subjekti preispituju i prema potrebi ažuriraju te postupke u planiranim intervalima i kad se dogode značajni incidenti.

6.2. *Siguran razvojni ciklus*

6.2.1. Prije razvoja mrežnog i informacijskog sustava, što uključuje i softver, relevantni subjekti utvrđuju pravila za siguran razvoj mrežnih i informacijskih sustava, koja primjenjuju kad samostalno razvijaju mrežne i informacijske sustave ili kad njihov razvoj prepuste vanjskom dobavljaču. Ta pravila moraju obuhvaćati sve faze razvoja, uključujući specifikaciju, projektiranje, razvoj, implementaciju i testiranje.

6.2.2. Za potrebe točke 6.2.1. relevantni subjekti:

(a) analiziraju sigurnosne zahtjeve u fazama specifikacije i projektiranja svakog projekta razvoja ili nabave koji provode oni sami ili se on provodi u njihovo ime;

(b) u svim aktivnostima razvoja informacijskih sustava primjenjuju načela za izradu sigurnih sustava i načela sigurnog programiranja, kao što su integrirana kibernetička sigurnost i arhitektura nultog povjerenja;

(c) utvrđuju sigurnosne zahtjeve za razvojna okruženja;

(d) uspostavljaju i provode postupke testiranja sigurnosti u razvojnom ciklusu;

(e) na odgovarajući način odabiru, štite i upravljaju podacima o testiranju sigurnosti;

(f) sigurno uništavaju i anonimiziraju podatke o testiranju u skladu s procjenom rizika provedenom u skladu s točkom 2.1.

6.2.3. Relevantni subjekti politike i postupke iz točaka 5. i 6.1. primjenjuju i ako su za razvoj mrežnih i informacijskih sustava angažirali vanjskog dobavljača.

6.2.4. Relevantni subjekti preispituju i prema potrebi ažuriraju pravila za siguran razvoj u planiranim intervalima.

6.3. *Upravljanje konfiguracijama*

6.3.1. Relevantni subjekti poduzimaju odgovarajuće mjere za uspostavu, dokumentiranje, primjenu i praćenje konfiguracija, uključujući sigurnosne konfiguracije hardvera, softvera, usluga i mreža.

6.3.2. Za potrebe točke 6.3.1. relevantni subjekti:

(a) utvrđuju i jamče sigurnost za konfiguracije svojeg hardvera, softvera, usluga i mreža;

(b) utvrđuju i primjenjuju postupke i alate kojima se osigurava primjena utvrđenih sigurnih konfiguracija hardvera, softvera, usluga i mreža tijekom cijelog životnog vijeka novoinstaliranih sustava i sustava koji su već u upotrebi.

6.3.3. Relevantni subjekti preispituju i prema potrebi poboljšavaju konfiguracije u planiranim intervalima ili kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

6.4. *Upravljanje promjenama, popravci i održavanje*

6.4.1. Kako bi imali kontrolu nad promjenama u mrežnim i informacijskim sustavima, relevantni subjekti primjenjuju postupke upravljanja promjenama. Ako je to primjenjivo, ti postupci moraju biti u skladu s općim politikama relevantnih subjekata koje se odnose na upravljanje promjenama.

6.4.2. Postupci iz točke 6.4.1. primjenjuju se na izdanja, izmjene i hitne promjene bilo kojeg softvera i hardvera u upotrebi te na promjene konfiguracije. Tim se postupcima mora osigurati da se promjene dokumentiraju i, na temelju procjene rizika provedene u skladu s točkom 2.1., prije uvođenja testiraju i procijene s obzirom na mogući učinak.

6.4.3. Ako zbog izvanrednog stanja nije moguće slijediti redovne postupke upravljanja promjenama, relevantni subjekti dokumentiraju rezultat promjene i navode objašnjenje zašto se postupci nisu mogli slijediti.

6.4.4. Relevantni subjekti preispituju i prema potrebi ažuriraju te postupke u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

6.5. *Sigurnosno testiranje*

6.5.1. Relevantni subjekti utvrđuju, uvode i provode politiku i postupke za sigurnosno testiranje.

6.5.2. Relevantni subjekti:

(a) utvrđuju, na temelju procjene rizika provedene u skladu s točkom 2.1., potrebu, opseg, učestalost i vrstu sigurnosnih testova;

(b) provode sigurnosne testove u skladu s dokumentiranom metodologijom testiranja, i to na komponentama za koje je analizom rizika utvrđeno da su važne za siguran rad;

(c) dokumentiraju vrstu, opseg, vrijeme i rezultate testova, uključujući procjenu kritičnosti i mjere ublažavanja za svaki nalaz;

(d) primjenjuju mjere ublažavanja u slučaju kritičnih nalaza.

6.5.3. Relevantni subjekti preispituju i prema potrebi ažuriraju politiku sigurnosnog testiranja u planiranim intervalima.

6.6. *Upravljanje sigurnosnim zakrpama*

6.6.1. Relevantni subjekti utvrđuju i primjenjuju postupke, usklađene s postupcima upravljanja promjenama iz točke 6.4.1., postupcima upravljanja ranjivostima i rizicima te drugim relevantnim postupcima upravljanja, kako bi osigurali:

(a) da se sigurnosne zakrpe primijene u razumnom roku nakon što postanu dostupne;

(b) da se sigurnosne zakrpe testiraju prije primjene u proizvodnim sustavima;

(c) da sigurnosne zakrpe dolaze iz pouzdanih izvora i da im se provjerava cjelovitost;

(d) da se provode dodatne mjere i da se preostali rizici prihvaćaju ako zakrpa nije dostupna ili nije primijenjena u skladu s točkom 6.6.2.

6.6.2. Odstupajući od točke 6.6.1. podtočke (a) relevantni subjekti mogu odlučiti da neće primjenjivati sigurnosne zakrpe ako su nedostaci njihove primjene veći od koristi za kibernetičku sigurnost. Relevantni subjekti dužni su propisno dokumentirati i obrazložiti svaku takvu odluku.

6.7. *Sigurnost mreža*

6.7.1. Relevantni subjekti poduzimaju odgovarajuće mjere za zaštitu svojih mrežnih i informacijskih sustava od kibernetičkih prijetnji.

6.7.2. Za potrebe točke 6.7.1. relevantni subjekti:

(a) dokumentiraju arhitekturu mreže na jasan i aktualan način;

(b) određuju i provode kontrole za zaštitu svoje unutarnje mrežne domene od neovlaštenog pristupa;

(c) konfiguriraju kontrole za onemogućivanje pristupa i mrežne komunikacije koji im nisu nužni za funkcioniranje;

(d) određuju i provode kontrole daljinskog pristupa mrežnim i informacijskim sustavima, uključujući pristup pružatelja usluga;

(e) sustave koji služe za upravljanje provedbom sigurnosne politike ne koriste u druge svrhe;

(f) izričito zabranjuju ili deaktiviraju nepotrebne veze i usluge;

(g) prema potrebi, pristup svojim mrežnim i informacijskim sustavima dopuštaju isključivo uređajima kojima su dali odobrenje;

(h) pružateljima usluga dopuštaju spajanje tek na zahtjev za odobrenje i na određeno razdoblje, npr. dok traje održavanje;

(i) komunikaciju između zasebnih sustava uspostavljaju samo pouzdanim kanalima koji su logički, kriptografski ili fizički izolirani od drugih komunikacijskih kanala i omogućuju pouzdanu identifikaciju njihovih krajnjih točaka i zaštitu podataka iz kanala od izmjene ili otkrivanja;

(j) donose provedbeni plan za potpun prelazak na komunikacijske protokole mrežnog sloja najnovije generacije na siguran, prikladan i postupan način i uspostavljaju mjere za ubrzavanje takvog prelaska;

(k) donose provedbeni plan za uvođenje međunarodno dogovorenih i interoperabilnih modernih komunikacijskih standarda e-pošte da zaštite komunikaciju e-poštom i tako smanje slabe točke osjetljive na prijetnje povezane s e-poštom te uspostavljaju mjere za ubrzavanje tog uvođenja;

(l) primjenjuju provjereno dobre postupke za sigurnost DNS-a i za sigurnost i higijenu internetskog usmjeravanja odlaznog i dolaznog mrežnog prometa.

6.7.3. Relevantni subjekti preispituju i prema potrebi ažuriraju te mjere u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

6.8. *Segmentacija mreže*

6.8.1. Relevantni subjekti segmentiraju sustave u mreže ili zone u skladu s rezultatima procjene rizika iz točke 2.1. Segmentiranjem odvajaju svoje sustave i mreže od sustava i mreža trećih strana.

6.8.2. U tu svrhu relevantni subjekti:

(a) u obzir uzimaju funkcionalni, logički i fizički odnos pouzdanih sustava i usluga, uključujući njihovu lokaciju;

(b) odobravaju pristup mreži ili zoni na temelju procjene njezinih sigurnosnih zahtjeva;

(c) sustave koji su ključni za rad relevantnih subjekata ili sigurnost smještaju u zaštićene zone;

(d) uvode demilitariziranu zonu u svojim komunikacijskim mrežama kako bi zaštitili dolaznu i odlaznu komunikaciju iz svojih mreža;

(e) ograničavaju pristup i komunikaciju između i unutar zona na ono što je potrebno za poslovanje relevantnih subjekata ili za sigurnost;

(f) namjensku mrežu za upravljanje mrežnim i informacijskim sustavima odvajaju od svoje operativne mreže;

(g) kanale za upravljanje mrežom odvajaju od ostalog mrežnog prometa;

(h) proizvodne sustave za svoje usluge odvajaju od sustava koji se koriste za razvoj i testiranje, uključujući sigurnosne kopije.

6.8.3. Relevantni subjekti preispituju i prema potrebi ažuriraju segmentaciju mreže u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

6.9. *Zaštita od zlonamjernog i neovlaštenog softvera*

6.9.1. Relevantni subjekti štite svoje mrežne i informacijske sustave od zlonamjernog i neovlaštenog softvera.

6.9.2. U tu svrhu relevantni subjekti prije svega provode mjere za otkrivanje ili sprečavanje korištenja zlonamjernog ili neovlaštenog softvera. Relevantni subjekti prema potrebi osiguravaju da su njihovi mrežni i informacijski sustavi opremljeni softverom za otkrivanje i odgovor te da se on redovito ažurira u skladu s procjenom rizika provedenom na temelju točke 2.1. i ugovornim sporazumima s pružateljima.

6.10. *Postupanje s ranjivostima i njihovo otkrivanje*

6.10.1. Relevantni subjekti pribavljaju informacije o tehničkim ranjivostima u svojim mrežnim i informacijskim sustavima, ocjenjuju svoju izloženost takvim ranjivostima i poduzimaju odgovarajuće mjere za upravljanje njima.

6.10.2. Za potrebe točke 6.10.1. relevantni subjekti:

(a) prate informacije o ranjivostima putem odgovarajućih kanala, kao što su objave CSIRT-ova ili nadležnih tijela ili informacije od dobavljača ili pružatelja usluga;

(b) prema potrebi u planiranim intervalima obavljaju provjere ranjivosti i bilježe dokaze rezultata tih provjera;

(c) bez nepotrebne odgode otklanjaju ranjivosti za koje su utvrdili da su kritične za njihovo poslovanje;

(d) vode računa o tome da s ranjivostima postupaju u skladu sa svojim postupcima upravljanja promjenama, sigurnosnim zakrpama, rizicima i incidentima;

(e) uspostavljaju postupak za otkrivanje ranjivosti u skladu s primjenjivom nacionalnom politikom koordiniranog otkrivanja ranjivosti.

6.10.3. Ako je to opravdano zbog potencijalnog učinka ranjivosti, relevantni subjekti izrađuju i provode plan za njezino ublažavanje. U suprotnom dokumentiraju i obrazlažu zašto ranjivost nije potrebno otkloniti.

6.10.4. Relevantni subjekti preispituju i prema potrebi u planiranim intervalima ažuriraju kanale koje koriste za praćenje informacija o ranjivostima.

7. **Politike i postupci za procjenu djelotvornosti mjera upravljanja kibernetičkosigurnosnim rizicima (članak 21. stavak 2. točka (f) Direktive (EU) 2022/2555)**

7.1. Za potrebe članka 21. stavka 2. točke (f) Direktive (EU) 2022/2555 relevantni subjekti utvrđuju, uvode i provode politiku i postupke čija je svrha procijeniti djelotvornost uvođenja i primjene mjera upravljanja kibernetičkosigurnosnim rizicima koje su odlučili poduzeti.

7.2. U politikama i postupcima iz točke 7.1. u obzir se uzimaju rezultati procjene rizika provedene u skladu s točkom 2.1. i prethodni značajni incidenti. Relevantni subjekti utvrđuju:

(a) koje mjere upravljanja kibernetičkosigurnosnim rizicima treba pratiti i mjeriti, uključujući procese i kontrole;

(b) metode praćenja, mjerenja, analize i vrednovanja, ovisno o slučaju, potrebne da bi se dobili valjani rezultati;

(c) kada treba izvršiti praćenje i mjerenje;

(d) tko je odgovoran za praćenje i mjerenje djelotvornosti mjera upravljanja kibernetičkosigurnosnim rizicima;

(e) kada treba analizirati i vrednovati rezultate praćenja i mjerenja;

(f) tko treba analizirati i vrednovati te rezultate.

7.3. Relevantni subjekti preispituju i prema potrebi ažuriraju tu politiku i postupke u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

8. **Osnovne prakse kibernetičke higijene i sigurnosno osposobljavanje (članak 21. stavak 2. točka (g) Direktive (EU) 2022/2555)**

8.1. *Informiranje i osnovne prakse kibernetičke higijene*

8.1.1. Za potrebe članka 21. stavka 2. točke (g) Direktive (EU) 2022/2555 relevantni subjekti osiguravaju da su njihovi zaposlenici, uključujući članove upravljačkih tijela, kao i izravni dobavljači i pružatelji usluga svjesni rizika, da su informirani o važnosti kibernetičke sigurnosti i da primjenjuju prakse kibernetičke higijene.

8.1.2. Za potrebe točke 8.1.1. relevantni subjekti za svoje zaposlenike, uključujući članove upravljačkih tijela, te, prema potrebi, za dobavljače i pružatelje usluga u skladu s točkom 5.1.4. nude program informiranja koji:

(a) se vremenski planira tako da se aktivnosti ponavljaju kako bi u njima sudjelovali novi zaposlenici;

(b) se uspostavlja u skladu s politikom mrežne i informacijske sigurnosti, tematskim politikama i relevantnim postupcima za mrežnu i informacijsku sigurnost;

(c) obrađuje relevantne kibernetičke prijetnje, uvedene mjere upravljanja kibernetičkosigurnosnim rizicima, kontaktne točke i resurse za dodatne informacije i savjete o pitanjima kibernetičke sigurnosti te prakse kibernetičke higijene za korisnike.

8.1.3. Djelotvornost programa informiranja provjerava se prema potrebi. Program informiranja ažurira se i provodi u planiranim intervalima, uzimajući u obzir promjene u praksama kibernetičke higijene i trenutačne prijetnje i rizike za relevantne subjekte.

8.2. *Sigurnosno osposobljavanje*

8.2.1. Relevantni subjekti utvrđuju koji zaposlenici imaju uloge koje zahtijevaju vještine i stručno znanje relevantne za sigurnost te vode računa da se oni redovito osposobljavaju o sigurnosti mrežnih i informacijskih sustava.

8.2.2. Relevantni subjekti izrađuju, uvode i provode program osposobljavanja u skladu s politikom mrežne i informacijske sigurnosti, tematskim politikama i drugim relevantnim postupcima za mrežnu i informacijsku sigurnost. U tom programu na temelju kriterija utvrđuju potrebe za osposobljavanjem za određene uloge i položaje.

8.2.3. Osposobljavanje iz točke 8.2.1. mora biti relevantno za radno mjesto zaposlenika i mora se ocijeniti njegova djelotvornost. U osposobljavanju se u obzir uzimaju postojeće sigurnosne mjere te ono obuhvaća:

(a) upute o sigurnoj konfiguraciji i radu mrežnih i informacijskih sustava, uključujući mobilne uređaje;

(b) izvješćivanje o poznatim kibernetičkim prijetnjama;

(c) osposobljavanje o postupanju u slučaju događaja bitnih za sigurnost.

8.2.4. Relevantni subjekti provode osposobljavanje za članove osoblja koji se premještaju na nova radna mjesta ili preuzimaju uloge za koje su potrebne vještine i stručno znanje relevantni za sigurnost.

8.2.5. Program se ažurira i provodi periodično uzimajući u obzir važeće politike i pravila, dodijeljene uloge i odgovornosti te poznate kibernetičke prijetnje i tehnološki razvoj.

9. **Kriptografija (članak 21. stavak 2. točka (h) Direktive (EU) 2022/2555)**

9.1. Za potrebe članka 21. stavka 2. točke (h) Direktive (EU) 2022/2555 relevantni subjekti utvrđuju, uvode i provode politiku i postupke za kriptografiju kako bi se ona primjereno i djelotvorno koristila za zaštitu povjerljivosti, vjerodostojnosti i cjelovitosti podataka u skladu s klasifikacijom resursa relevantnih subjekata i rezultatima procjene rizika provedene u skladu s točkom 2.1.

9.2. Politikom i postupcima iz točke 9.1. utvrđuju se:

(a) u skladu s klasifikacijom imovine relevantnih subjekata, vrsta, jačina i kvaliteta kriptografskih mjera potrebnih za zaštitu te imovine, uključujući podatke u mirovanju i podatke u tranzitu;

(b) na temelju točke (a), protokoli ili porodice protokola koje treba primijeniti, kao i kriptografski algoritmi, jačina šifre, kriptografska rješenja i praktični postupci koje treba odobriti i čija će se upotreba zahtijevati u relevantnim subjektima, primjenjujući, prema potrebi, pristup kriptografske prilagodljivosti;

(c) pristup relevantnih subjekata upravljanju ključevima, uključujući, prema potrebi, metode za:

i. generiranje raznih ključeva za kriptografske sustave i aplikacije;

ii. izdavanje i pribavljanje certifikata javnog ključa;

iii. distribuciju ključeva subjektima kojima su namijenjeni, uključujući način aktivacije ključeva po primitku;

iv. pohranu ključeva, uključujući način na koji ovlašteni korisnici dobivaju pristup ključevima;

v. promjenu ili ažuriranje ključeva, uključujući pravila o tome kada se i kako ključevi mijenjaju;

vi. postupanje s probijenim ključevima;

vii. opoziv ključeva, uključujući način povlačenja ili deaktivacije ključeva;

viii. obnavljanje izgubljenih ili oštećenih ključeva;

ix. izradu sigurnosnih kopija ili arhiviranje ključeva;

x. uništavanje ključeva;

xi. evidenciju i reviziju aktivnosti povezanih s upravljanjem ključevima;

xii. određivanje datuma aktivacije i deaktivacije ključeva kako bi se ključevi mogli upotrebljavati samo u određenom razdoblju, u skladu s pravilima dotične organizacije o upravljanju ključevima.

9.3. Relevantni subjekti preispituju i prema potrebi ažuriraju svoju politiku i postupke u planiranim intervalima, uzimajući pritom u obzir najnovija dostignuća u području kriptografije.

10. **Sigurnost ljudskih resursa (članak 21. stavak 2. točka (i) Direktive (EU) 2022/2555)**

10.1. *Sigurnost ljudskih resursa*

10.1.1. Za potrebe članka 21. stavka 2. točke (i) Direktive (EU) 2022/2555 relevantni subjekti dužni su se pobrinuti da njihovi zaposlenici i izravni dobavljači i pružatelji usluga, kad god je to primjenjivo, razumiju i prihvate svoje odgovornosti u pogledu sigurnosti, kako je primjereno za ponuđene usluge i radno mjesto te u skladu s politikom relevantnih subjekata o sigurnosti mrežnih i informacijskih sustava.

10.1.2. Zahtjev iz točke 10.1.1. mora obuhvaćati:

(a) mehanizme kojima se osigurava da svi zaposlenici, izravni dobavljači i pružatelji usluga, kad god je to primjenjivo, razumiju i provode standardne prakse kibernetičke higijene koje relevantni subjekti primjenjuju u skladu s točkom 8.1.;

(b) mehanizme kojima se osigurava da su svi korisnici s administrativnim ili povlaštenim pristupom upoznati sa svojim ulogama, odgovornostima i ovlastima te da postupaju u skladu s njima;

(c) mehanizme kojima se osigurava da članovi upravljačkih tijela razumiju i postupaju u skladu sa svojom ulogom, odgovornostima i ovlastima u pogledu sigurnosti mrežnih i informacijskih sustava;

(d) mehanizme za zapošljavanje osoblja kvalificiranog za uloge koje su im namijenjene, kao što su provjeravanje preporuka, postupci provjere, potvrđivanje diploma ili pismeni testovi.

10.1.3. Relevantni subjekti u planiranim intervalima, a najmanje jednom godišnje, preispituju kako je osoblje raspoređeno na određene uloge u skladu s točkom 1.2. te koliko je ljudskih resursa izdvojeno za te poslove. Raspoređivanje zaposlenika ažurira se prema potrebi.

10.2. *Provjera osoblja*

10.2.1. Relevantni subjekti dužni su se pobrinuti, u mjeri u kojoj je to izvedivo, da se za njihove zaposlenike i, ako je to primjenjivo, za izravne dobavljače i pružatelje usluga provode provjere u skladu s točkom 5.1.4., ako je to potrebno zbog njihovih uloga, odgovornosti i ovlasti.

10.2.2. Za potrebe točke 10.2.1. relevantni subjekti:

(a) utvrđuju kriterije na temelju kojih se određuje koje se uloge, odgovornosti i ovlasti mogu dodijeliti samo onim osobama koje su prošle provjeru;

(b) vode računa o tome da se provjera iz točke 10.2.1. na tim osobama obavi prije nego što one preuzmu te uloge, odgovornosti i ovlasti, i da se pritom u obzir uzmu važeći zakoni, propisi i etičke norme razmjerno poslovnim zahtjevima, klasifikaciji resursa iz točke 12.1. i mrežnim i informacijskim sustavima kojima se pristupa te percipirani rizici.

10.2.3. Relevantni subjekti preispituju i prema potrebi ažuriraju tu politiku u planiranim intervalima.

10.3. *Postupci u slučaju prestanka ili promjene radnog odnosa*

10.3.1. Relevantni subjekti osiguravaju da se odgovornosti i dužnosti povezane sa sigurnošću mrežnih i informacijskih sustava koje ostaju važiti nakon prestanka ili promjene radnog odnosa njihovih zaposlenika ugovorno definiraju i izvršavaju.

10.3.2. Za potrebe točke 10.3.1. relevantni subjekti u uvjetima zaposlenja, ugovoru ili sporazumu pojedinačnog zaposlenika navode odgovornosti i dužnosti koje ostaju važiti i nakon prestanka radnog odnosa ili ugovora, kao što su klauzule o povjerljivosti.

10.4. *Disciplinski postupak*

10.4.1. Relevantni subjekti uspostavljaju, obznanjuju i dosljedno primjenjuju disciplinski postupak za kršenje politika sigurnosti mrežnih i informacijskih sustava. U postupku se uzimaju u obzir relevantni pravni, zakonski, ugovorni i poslovni uvjeti.

10.4.2. Relevantni subjekti preispituju i prema potrebi ažuriraju disciplinski postupak u planiranim intervalima i ako je to potrebno zbog pravnih izmjena ili znatnih promjena u poslovanju ili rizicima.

11. **Kontrola pristupa (članak 21. stavak 2. točke (i) i (j) Direktive (EU) 2022/2555)**

11.1. *Politika kontrole pristupa*

11.1.1. Za potrebe članka 21. stavka 2. točke (i) Direktive (EU) 2022/2555 relevantni subjekti uspostavljaju, dokumentiraju i provode politike logičke i fizičke kontrole pristupa svojim mrežnim i informacijskim sustavima na temelju poslovnih zahtjeva te sigurnosnih zahtjeva mrežnih i informacijskih sustava.

11.1.2. Politikama iz točke 11.1.1.:

(a) uređuje se pristup osoba, uključujući osoblje, posjetitelje i vanjske subjekte kao što su dobavljači i pružatelji usluga;

(b) uređuje se pristup mrežnih i informacijskih sustava;

(c) osigurava se da se pristup odobrava samo korisnicima koji su autentificirani na odgovarajući način.

11.1.3. Relevantni subjekti preispituju i prema potrebi ažuriraju te politike u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

11.2. *Upravljanje pravima pristupa*

11.2.1. Relevantni subjekti dodjeljuju, mijenjaju, oduzimaju i dokumentiraju prava pristupa mrežnim i informacijskim sustavima u skladu s politikom kontrole pristupa iz točke 11.1.

11.2.2. Relevantni subjekti:

(a) dodjeljuju i oduzimaju prava pristupa na temelju načela nužnosti pristupa, načela minimalnih potrebnih ovlasti i načela razdvajanja dužnosti;

(b) na odgovarajući način mijenjaju prava pristupa nakon prestanka ili promjene radnog odnosa;

(c) vode računa o tome da pristup mrežnim i informacijskim sustavima odobravaju relevantne osobe;

(d) osiguravaju da se prava pristupa na odgovarajući način primjenjuju na pristup trećih strana, kao što su posjetitelji, dobavljači i pružatelji usluga, prije svega ograničavanjem njihova opsega i trajanja;

(e) vode registar dodijeljenih prava pristupa;

(f) vode evidenciju o upravljanju pravima pristupa.

11.2.3. Relevantni subjekti preispituju prava pristupa u planiranim intervalima i mijenjaju ih u skladu s organizacijskim promjenama. Relevantni subjekti dužni su dokumentirati rezultate preispitivanja, uključujući potrebne izmjene prava pristupa.

11.3. *Povlašteni računi i računi za administraciju sustava*

11.3.1. Relevantni subjekti provode politike za upravljanje povlaštenim računima i računima za administraciju sustava u okviru politike kontrole pristupa iz točke 11.1.

11.3.2. Politikama iz točke 11.3.1.:

(a) uspostavljaju se postupci za pouzdanu identifikaciju, za autentifikaciju kao što je višestruka autentifikacija i za izdavanje odobrenja za povlaštene račune i račune za administraciju sustava;

(b) uspostavljaju se posebni računi namijenjeni isključivo za radnje administriranja sustava, kao što su instalacija, konfiguracija, upravljanje ili održavanje;

(c) prava administratora sustava definiraju se tako da budu maksimalno individualizirana i ograničena;

(d) osigurava se da se računi za administraciju sustava koriste samo za povezivanje sa sustavima za administraciju sustava.

11.3.3. Relevantni subjekti preispituju prava pristupa povlaštenim računima i računima za administraciju sustava u planiranim intervalima i mijenjaju ih u skladu s organizacijskim promjenama te dokumentiraju rezultate preispitivanja, uključujući potrebne izmjene prava pristupa.

11.4. *Sustavi za administraciju*

11.4.1. Relevantni subjekti ograničavaju i kontroliraju korištenje sustava za administraciju sustava u skladu s politikom kontrole pristupa iz točke 11.1.

11.4.2. U tu svrhu relevantni subjekti:

(a) sustave za administraciju sustava koriste isključivo za potrebe administracije sustava i ni za koje druge radnje;

(b) logički odvajaju takve sustave od aplikacijskog softvera koji se ne koristi za administriranje sustava;

(c) štite pristup sustavima za administraciju sustava autentifikacijom i šifriranjem.

11.5. *Identifikacija*

11.5.1. Relevantni subjekti upravljaju cijelim životnim ciklusom identiteta mrežnih i informacijskih sustava i njihovih korisnika.

11.5.2. U tu svrhu relevantni subjekti:

(a) uspostavljaju jedinstvene identitete za mrežne i informacijske sustave i njihove korisnike;

(b) povezuju identitet korisnika s jednom osobom;

(c) osiguravaju nadzor identiteta mrežnih i informacijskih sustava;

(d) vode evidenciju o upravljanju identitetima.

11.5.3. Relevantni subjekti dopuštaju upotrebu identiteta koji se dodjeljuju većem broju osoba, kao što su zajednički identiteti, samo ako su oni potrebni iz poslovnih ili operativnih razloga i pod uvjetom da se moraju izričito odobriti i dokumentirati. Relevantni subjekti dužni su identitete koji se dodjeljuju većem broju osoba uzeti u obzir u okviru upravljanja kibernetičkosigurnosnim rizicima iz točke 2.1.

11.5.4. Relevantni subjekti redovito preispituju identitete mrežnih i informacijskih sustava i njihovih korisnika te ih, ako više nisu potrebni, bez odgode deaktiviraju.

11.6. *Autentifikacija*

11.6.1. Relevantni subjekti primjenjuju sigurne postupke i tehnologije autentifikacije koji se temelje na ograničenjima pristupa i politici kontrole pristupa.

11.6.2. U tu svrhu relevantni subjekti:

(a) osiguravaju da je jačina autentifikacije primjerena klasifikaciji resursa kojem se pristupa;

(b) kontroliraju dodjelu tajnih autentifikacijskih podataka korisnicima i upravljanje njima postupkom kojim se jamči povjerljivost tih podataka, uključujući savjetovanje osoblja o primjerenom postupanju s njima;

(c) zahtijevaju promjenu autentifikacijskih vjerodajnica na samom početku, u unaprijed određenim intervalima i ako postoji sumnja da su ugrožene i probijene;

(d) zahtijevaju ponovno izdavanje autentifikacijskih vjerodajnica i blokiranje korisnika nakon unaprijed određenog broja neuspješnih pokušaja prijave;

(e) prekidaju neaktivne sesije nakon unaprijed određenog razdoblja neaktivnosti; i

(f) zahtijevaju zasebne vjerodajnice za pristup povlaštenim ili administrativnim računima.

11.6.3. Relevantni subjekti koriste, u mjeri u kojoj je to izvedivo, najsuvremenije metode autentifikacije, u skladu s povezanim procijenjenim rizikom i klasifikacijom resursa kojem se pristupa, te jedinstvene autentifikacijske podatke.

11.6.4. Relevantni subjekti preispituju autentifikacijske postupke i tehnologije u planiranim intervalima.

11.7. *Višestruka autentifikacija*

11.7.1. Relevantni subjekti osiguravaju da se korisnici za potrebe pristupa njihovim mrežnim i informacijskim sustavima, prema potrebi, autentificiraju pomoću višestruke autentifikacije ili mehanizama kontinuirane autentifikacije u skladu s klasifikacijom resursa kojem se pristupa.

11.7.2. Relevantni subjekti vode računa o tome da je jačina autentifikacije primjerena klasifikaciji resursa kojem se pristupa.

12. **Upravljanje resursima (članak 21. stavak 2. točka (i) Direktive (EU) 2022/2555)**

12.1. *Klasifikacija resursa*

12.1.1. Za potrebe članka 21. stavka 2. točke (i) Direktive (EU) 2022/2555 relevantni subjekti utvrđuju klasifikacijske razine za svu imovinu, uključujući informacije, u okviru svojih mrežnih i informacijskih sustava kako bi se utvrdila potrebna razina zaštite.

12.1.2. Za potrebe točke 12.1.1. relevantni subjekti:

(a) uspostavljaju sustav klasifikacijskih razina za imovinu;

(b) svoj imovini dodjeljuju klasifikacijsku razinu na temelju zahtjeva u pogledu povjerljivosti, cjelovitosti, autentičnosti i dostupnosti kako bi naznačili kakva joj je zaštita potrebna s obzirom na njezinu osjetljivost, kritičnost, rizik i poslovnu vrijednost;

(c) usklađuju zahtjeve za dostupnost imovine s ciljevima isporuke i oporavka utvrđenima u svojim planovima kontinuiteta poslovanja i oporavka od katastrofe.

12.1.3. Relevantni subjekti periodično provjeravaju klasifikacijske razine imovine te ih ažuriraju prema potrebi.

12.2. *Postupanje s imovinom*

12.2.1. Relevantni subjekti utvrđuju, uvode i provode politiku za pravilno postupanje s imovinom, uključujući informacije, u skladu sa svojom politikom mrežne i informacijske sigurnosti te o toj politici obavješćuju sve osobe koje se imovinom služe ili rukuju.

12.2.2. Ta politika mora:

(a) obuhvaćati cijeli životni ciklus imovine, uključujući nabavu, upotrebu, skladištenje, prijevoz i uklanjanje;

(b) sadržavati pravila za sigurnu upotrebu, sigurnu pohranu, siguran prijevoz i nepovratno brisanje i uništavanje imovine;

(c) osigurati da se prijenos odvija na siguran način, u skladu s vrstom resursa koji se prenosi.

12.2.3. Relevantni subjekti preispituju i prema potrebi ažuriraju tu politiku u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

12.3. *Politika o prenosivim medijima*

12.3.1. Relevantni subjekti utvrđuju, uvode i provode politiku upravljanja prenosivim medijima za pohranu te o njoj obavješćuju svoje zaposlenike i treće strane koje rukuju prenosivim medijima za pohranu u prostorima relevantnih subjekata ili na drugim lokacijama na kojima su prenosivi mediji povezani s mrežnim i informacijskim sustavima relevantnih subjekata.

12.3.2. Tom se politikom mora:

(a) propisati tehnička zabrana priključivanja prenosivih medija, osim ako postoji organizacijski razlog za njihovo korištenje;

(b) propisati onemogućivanje samostalnog pokretanja datoteka s takvih medija i provjeru da mediji ne sadržavaju zlonamjerni kod prije njihova korištenja u sustavima relevantnih subjekata;

(c) uspostaviti mjere za kontrolu i zaštitu prijenosnih uređaja za pohranu koji sadržavaju podatke dok se prenose i dok su spremljeni;

(d) prema potrebi uspostaviti mjere za upotrebu kriptografskih tehnika za zaštitu podataka na prenosivim medijima za pohranu.

12.3.3. Relevantni subjekti preispituju i prema potrebi ažuriraju tu politiku u planiranim intervalima i kad se dogode značajni incidenti ili znatne promjene u poslovanju ili rizicima.

12.4. *Popis resursa*

12.4.1. Relevantni subjekti izrađuju i vode potpun, točan, aktualan i dosljedan popis svoje imovine. Izmjene unosa na popisu dužni su evidentirati na sljediv način.

12.4.2. Granularnost popisa imovine mora biti primjerena potrebama relevantnih subjekata. Popis mora obuhvaćati:

(a) popis poslovnih aktivnosti i usluga i njihov opis;

(b) popis mrežnih i informacijskih sustava i druge povezane imovine koja se koristi u poslovanju relevantnih subjekata i uslugama koje oni pružaju.

12.4.3. Relevantni subjekti redovito pregledavaju i ažuriraju popis i imovinu te dokumentiraju povijest izmjena.

12.5. *Predaja, vraćanje ili brisanje imovine nakon prestanka radnog odnosa*

Relevantni subjekti utvrđuju, uvode i provode postupke kojima osiguravaju da zaposlenici nakon prestanka radnog odnosa predaju, vrate ili izbrišu imovinu koju su im povjerili te dokumentiraju njezinu predaju, vraćanje ili brisanje. Ako se imovina ne može predati, vratiti ili izbrisati, relevantni subjekti dužni su pobrinuti se, u skladu s točkom 12.2.2., da ta imovina više nema pristup njihovim mrežnim i informacijskim sustavima.

13. **Okolišna i fizička sigurnost (članak 21. stavak 2. točke (c), (e) i (i) Direktive (EU) 2022/2555)**

13.1. *Potporne javne službe*

13.1.1. Za potrebe članka 21. stavka 2. točke (c) Direktive (EU) 2022/2555 relevantni subjekti sprečavaju gubitak, oštećenje ili ugrožavanje mrežnih i informacijskih sustava ili prekid njihova rada zbog kvara i poremećaja u radu potpornih komunalnih službi.

13.1.2. U tu svrhu relevantni subjekti prema potrebi:

(a) štite objekte od nestanka električne energije i drugih poremećaja uzrokovanih prekidima pružanja usluga javnih službi kao što su opskrba električnom energijom, telekomunikacije, vodoopskrba, plinoopskrba, kanalizacija, ventilacija i klimatizacija;

(b) razmatraju korištenje redundantnih sustava kad je riječ o uslugama javnih službi;

(c) od presretanja i oštećenja štite usluge javnih službi kojima dobivaju električnu energiju i telekomunikacije za prijenos podataka za njihove mrežne i informacijske sustave;

(d) prate usluge javnih službi iz točke (c) i izvješćuju nadležno unutarnje ili vanjsko osoblje o događajima koji su izvan minimalnih i maksimalnih pragova kontrole iz točke 13.2.2. podtočke (b) i koji utječu na komunalne usluge;

(e) s odgovarajućim službama sklapaju ugovore za opskrbu u hitnim slučajevima, na primjer gorivom za izvor napajanja za slučaj nužde;

(f) vode računa o tome da opskrba mrežnih i informacijskih sustava potrebnih za pružanje ponuđene usluge bude kontinuirano djelotvorna te da se prati, održava i testira, a to se prije svega odnosi na opskrbu električnom energijom, regulaciju temperature i vlažnosti, telekomunikacije i internetsku vezu.

13.1.3. Relevantni subjekti redovito ili nakon značajnih incidenata ili znatnih promjena u poslovanju ili rizicima testiraju, preispituju i prema potrebi ažuriraju te zaštitne mjere.

13.2. *Zaštita od fizičkih i okolišnih prijetnji*

13.2.1. Za potrebe članka 21. stavka 2. točke (e) Direktive (EU) 2022/2555 relevantni subjekti na temelju rezultata procjene rizika provedene u skladu s točkom 2.1. sprečavaju ili smanjuju posljedice događaja proizišlih iz fizičkih i okolišnih prijetnji, kao što su prirodne katastrofe i druge namjerne ili nenamjerne prijetnje.

13.2.2. U tu svrhu relevantni subjekti prema potrebi:

(a) osmišljavaju i uvode mjere zaštite od fizičkih i okolišnih prijetnji;

(b) utvrđuju minimalne i maksimalne kontrolne pragove za fizičke i okolišne prijetnje;

(c) prate okolišne parametre i izvješćuju nadležno unutarnje ili vanjsko osoblje o događajima izvan minimalnih i maksimalnih kontrolnih pragova iz točke (b).

13.2.3. Relevantni subjekti redovito ili nakon značajnih incidenata ili znatnih promjena u poslovanju ili rizicima testiraju, preispituju i prema potrebi ažuriraju zaštitne mjere protiv fizičkih i okolišnih prijetnji.

13.3. *Nadzor okoline i fizičkog pristupa*

13.3.1. Za potrebe članka 21. stavka 2. točke (i) Direktive (EU) 2022/2555 relevantni subjekti sprečavaju i prate neovlašteni fizički pristup svojim mrežnim i informacijskim sustavima te njihovo oštećivanje i ometanje.

13.3.2. U tu svrhu relevantni subjekti:

(a) na temelju procjene rizika u skladu s točkom 2.1. uspostavljaju i koriste sigurnosne zone za zaštitu prostora u kojima su smješteni mrežni i informacijski sustavi i druga povezana imovina;

(b) štite prostore iz točke (a) primjenom odgovarajućih ulaznih kontrola i pristupnih točaka;

(c) osmišljavaju i provode mjere fizičke sigurnosti za urede, prostorije i objekte,

(d) kontinuirano nadziru svoje prostore radi otkrivanja neovlaštenog fizičkog pristupa.

13.3.3. Relevantni subjekti redovito ili nakon značajnih incidenata ili znatnih promjena u poslovanju ili rizicima testiraju, preispituju i prema potrebi ažuriraju te mjere kontrole fizičkog pristupa.