Úradný vestník
Európskej únie

SK
Séria L

2024/2690

18.10.2024

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2024/2690

zo 17. októbra 2024,

ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík a o bližšie určenie prípadov, v ktorých sa incident považuje za významný, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľom dôveryhodných služieb

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) ([1]), a najmä na jej článok 21 ods. 5 prvý pododsek a článok 23 ods. 11 druhý pododsek,

keďže:

(1) Cieľom tohto nariadenia je stanoviť technické a metodické požiadavky na opatrenia uvedené v článku 21 ods. 2 smernice (EÚ) 2022/2555 a bližšie určiť prípady, v ktorých by sa mal incident považovať za významný, ako sa uvádza v článku 23 ods. 3 smernice (EÚ) 2022/2555, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí a poskytovateľom dôveryhodných služieb, na ktorých sa vzťahuje článok 3 smernice (EÚ) 2022/2555 (ďalej len „príslušné subjekty“).

(2) Vzhľadom na cezhraničnú povahu ich činností a s cieľom zabezpečiť jednotný rámec pre poskytovateľov dôveryhodných služieb by sa v tomto nariadení vo vzťahu k poskytovateľom dôveryhodných služieb mali bližšie určiť prípady, v ktorých sa incident má považovať za významný, ako aj stanoviť technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík.

(3) Podľa článku 21 ods. 5 tretieho pododseku smernice (EÚ) 2022/2555 sú technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík, ktoré sa stanovujú v prílohe k tomuto nariadeniu, založené na európskych a medzinárodných normách, ako sú normy ISO/IEC 27001, ISO/IEC 27002 a ETSI EN 319401, a technických špecifikáciách, ako je norma CEN/TS 18026:2024, týkajúcich sa bezpečnosti sietí a informačných systémov.

(4) Pokiaľ ide o vykonávanie a uplatňovanie technických a metodických požiadaviek na opatrenia na riadenie kybernetických rizík stanovených v prílohe k tomuto nariadeniu v súlade so zásadou proporcionality, pri dodržiavaní technických a metodických požiadaviek na opatrenia na riadenie kybernetických rizík stanovených v prílohe k tomuto nariadeniu by sa mala náležite zohľadniť odlišná expozícia príslušných subjektov voči rizikám, napríklad kritickosť príslušného subjektu, riziká, ktorým je vystavený, jeho veľkosť a štruktúra, ako aj pravdepodobnosť výskytu incidentov a ich závažnosť vrátane ich spoločenského a hospodárskeho vplyvu.

([1]) Ú. v. EÚ L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(5) V prípade, keď príslušné subjekty z dôvodu svojej veľkosti nemôžu vykonávať niektoré z technických a metodických požiadaviek na opatrenia na riadenie kybernetických rizík, v súlade so zásadou proporcionality by tieto subjekty mali mať možnosť prijať iné kompenzačné opatrenia vhodné na dosiahnutie účelu týchto požiadaviek. Napríklad pri vymedzovaní úloh, povinností a právomocí pre bezpečnosť sietí a informačných systémov v rámci príslušného subjektu by pre mikrosubjekty mohlo byť náročné oddeliť úlohy a oblasti právomocí, ktoré sa navzájom vylučujú. Tieto subjekty by mali mať možnosť zvážiť kompenzačné opatrenia, ako sú cielený dohľad vykonávaný vedením subjektu alebo zvýšené monitorovanie a logovanie.

(6) Určité technické a metodické požiadavky stanovené v prílohe k tomuto nariadeniu by príslušné subjekty mali uplatňovať v prípade potreby, v náležitých prípadoch alebo pokiaľ to je možné. Ak príslušný subjekt nepovažuje za potrebné, náležité ani možné, aby uplatňoval určité technické a metodické požiadavky stanovené v prílohe k tomuto nariadeniu, mal by zrozumiteľným spôsobom zaznamenať svoje odôvodnenie v tejto súvislosti. Príslušné vnútroštátne orgány môžu pri výkone dohľadu zohľadniť primeraný čas, ktorý príslušné subjekty potrebujú na splnenie technických a metodických požiadaviek na opatrenia na riadenie kybernetických rizík.

(7) Agentúra Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) alebo príslušné vnútroštátne orgány podľa smernice (EÚ) 2022/2555 môžu poskytovať usmernenia na podporu príslušných subjektov pri rozpoznávaní, analyzovaní a posudzovaní rizík na účely vykonávania technických a metodických požiadaviek týkajúcich sa vytvorenia a udržiavania vhodného rámca pre riadenie rizík. Tieto usmernenia môžu zahŕňať najmä vnútroštátne a odvetvové posúdenia rizík, ako aj posúdenia rizík špecifických pre určitý typ subjektu. Usmernenia môžu zahŕňať aj nástroje alebo vzory na vytvorenie rámca pre riadenie rizík na úrovni príslušných subjektov. Rámce, usmernenia alebo iné mechanizmy stanovené vo vnútroštátnom práve členských štátov, ako aj príslušné európske a medzinárodné normy takisto môžu podporovať príslušné subjekty pri preukazovaní súladu s týmto vykonávacím nariadením. Agentúra ENISA alebo príslušné vnútroštátne orgány podľa smernice (EÚ) 2022/2555 okrem toho môžu poskytovať podporu príslušným subjektom pri určovaní a vykonávaní vhodných riešení na ošetrenie rizík zistených pri takomto posudzovaní rizík. Týmito usmerneniami by nemali byť dotknuté povinnosti príslušných subjektov týkajúce sa určovania a zaznamenávania rizík pre bezpečnosť sietí a informačných systémov a povinnosť príslušných subjektov plniť technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík stanovené v prílohe k tomuto nariadeniu podľa ich potrieb a zdrojov.

(8) Opatrenia na zaistenie bezpečnosti siete týkajúce sa: i) prechodu na najnovšiu generáciu komunikačných protokolov sieťovej vrstvy; ii) zavedenia medzinárodne schválených a interoperabilných moderných noriem e-mailovej komunikácie a iii) uplatňovania najlepších postupov bezpečnosti systému názvov domén (DNS) a bezpečnosti a hygieny smerovania internetu prinášajú osobitné problémy pri určovaní najlepších dostupných noriem a techník zavádzania. Komisia s pomocou agentúry ENISA a v spolupráci s príslušnými orgánmi, odvetvím – vrátane telekomunikačného odvetvia – a ďalšími zainteresovanými stranami by v záujme čo najrýchlejšieho dosiahnutia vysokej spoločnej úrovne kybernetickej bezpečnosti vo všetkých sieťach mala podporiť vznik multilaterálneho fóra, ktorého úlohou bude určiť tieto najlepšie dostupné normy a techniky zavádzania. Týmito usmerneniami pre viaceré zainteresované strany by nemala byť dotknutá povinnosť príslušných subjektov plniť technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík stanovené v prílohe k tomuto nariadeniu.

(9) Podľa článku 21 ods. 2 písm. a) smernice (EÚ) 2022/2555 by kľúčové a dôležité subjekty mali mať okrem zásad analýzy rizík aj zásady bezpečnosti informačných systémov. Na tento účel by príslušné subjekty mali stanoviť zásady bezpečnosti sietí a informačných systémov, ako aj tematické zásady, ako sú zásady kontroly prístupu, ktoré by mali byť v súlade so zásadami bezpečnosti sietí a informačných systémov. Zásady bezpečnosti sietí a informačných systémov by mali predstavovať dokument najvyššej úrovne, v ktorom sa stanoví celkový prístup príslušných subjektov k bezpečnosti ich sietí a informačných systémov, a mali by ich schváliť riadiace orgány príslušných subjektov. Tematické zásady by sa mali schvaľovať na vhodnej úrovni riadenia. V rámci zásad by sa mali stanoviť ukazovatele a opatrenia na monitorovanie ich vykonávania a aktuálneho stavu úrovne vyspelosti sieťovej a informačnej bezpečnosti príslušných subjektov, najmä s cieľom uľahčiť dohľad riadiacich orgánov nad vykonávaním opatrení na riadenie kybernetických rizík.

(10) Na účely technických a metodických požiadaviek uvedených v prílohe k tomuto nariadeniu by sa pojem „používateľ“ mal vzťahovať na všetky právnické a fyzické osoby, ktoré majú prístup k sieťam a informačným systémom subjektu.

(11) Na určenie a riešenie rizík pre bezpečnosť sietí a informačných systémov by príslušné subjekty mali vytvoriť a udržiavať vhodný rámec riadenia rizík. Príslušné subjekty by ako súčasť rámca riadenia rizík mali stanoviť, vykonať a monitorovať plán ošetrenia rizika. Príslušné subjekty môžu využiť plán ošetrenia rizika na určenie možností a opatrení na ošetrenie rizika a stanovenie ich priorít. Možnosti na ošetrenie rizika zahŕňajú najmä predchádzanie riziku, jeho znižovanie alebo vo výnimočných prípadoch akceptáciu rizika. Vo výbere možností na ošetrenie rizika by sa mali zohľadniť výsledky posúdenia rizík, ktoré vykonal príslušný subjekt, pričom by tento výber mal byť v súlade so zásadami bezpečnosti sietí a informačných systémov príslušného subjektu. Na uplatnenie zvolených možností na ošetrenie rizík by príslušné subjekty mali prijať vhodné opatrenia na ošetrenie rizika.

(12) Na účely odhaľovania udalostí, udalostí odvrátených v poslednej chvíli a incidentov by príslušné subjekty mali monitorovať svoje siete a informačné systémy a prijať opatrenia na vyhodnocovanie udalostí, udalostí odvrátených v poslednej chvíli a incidentov. Tieto opatrenia by mali dokázať umožniť včas odhaľovať sieťové útoky na základe nezvyčajnej štruktúry prichádzajúcej a odchádzajúcej prevádzky a útoky na vyradenie služby.

(13) Keď príslušné subjekty analyzujú vplyv na obchodnú činnosť, odporúča sa, aby vykonali komplexnú analýzu, pri ktorej podľa potreby určia maximálnu prípustnú dĺžku výpadku, časové ciele obnovy, ciele bodu obnovy a ciele poskytovania služieb.

(14) S cieľom zmierniť riziká vyplývajúce z dodávateľského reťazca príslušného subjektu a z jeho vzťahu s dodávateľmi by príslušné subjekty mali zaviesť zásady bezpečnosti dodávateľského reťazca, ktorými by sa riadili ich vzťahy s priamymi dodávateľmi a poskytovateľmi služieb. Tieto subjekty by mali v zmluvách s priamymi dodávateľmi alebo poskytovateľmi služieb stanoviť náležité bezpečnostné doložky, napríklad by sa v nich mali v prípade potreby požadovať opatrenia na riadenie kybernetických rizík podľa článku 21 ods. 2 smernice (EÚ) 2022/2555 alebo podľa iných podobných právnych požiadaviek.

(15) Príslušné subjekty by mali pravidelne vykonávať testy zabezpečenia založené na vyhradených zásadách a postupoch, aby sa overilo vykonanie a riadne fungovanie opatrení na riadenie kybernetických rizík. Testy zabezpečenia sa môžu vykonávať v prípade konkrétnych sietí a informačných systémov alebo príslušných subjektov ako celku a môžu zahŕňať automatizované alebo manuálne testy, penetračné testy, skenovanie zraniteľnosti, statické a dynamické testy zabezpečenia aplikácií, testy konfigurácie alebo bezpečnostné audity. Príslušné subjekty môžu vykonávať testy zabezpečenia na svojich sieťach a informačných systémoch pri ich nastavovaní, po modernizácii alebo zmenách infraštruktúry alebo aplikácie, ktoré považujú za významné, alebo po údržbe. Zistenia z testov zabezpečenia by mali poslúžiť ako podklady pre zásady a postupy príslušných subjektov s cieľom posúdiť účinnosť opatrení na riadenie kybernetických rizík, ako aj pre nezávislé preskúmania ich zásad v oblasti sieťovej a informačnej bezpečnosti.

(16) S cieľom predísť značným narušeniam a škodám spôsobeným využitím neopravených zraniteľností v sieťach a informačných systémoch by príslušné subjekty mali stanoviť a uplatňovať vhodné postupy riadenia bezpečnostných záplat, ktoré budú v súlade s postupmi riadenia zmien, riadenia zraniteľnosti, riadenia rizík a iných relevantných postupov príslušných subjektov. Príslušné subjekty by mali prijať opatrenia primerané svojim zdrojom s cieľom zabezpečiť, že sa bezpečnostnými záplatami nezavedú ďalšie zraniteľnosti alebo nestability. V prípade plánovanej nedostupnosti služby spôsobenej inštaláciou bezpečnostných záplat sa príslušným subjektom odporúča, aby vopred riadne informovali zákazníkov.

(17) Príslušné subjekty by mali riadiť riziká vyplývajúce z nadobudnutia produktov alebo služieb IKT od dodávateľov alebo poskytovateľov služieb a mali byť získať uistenie, že produkty alebo služby IKT, ktoré sa nadobúdajú, dosahujú určité úrovne ochrany kybernetickej bezpečnosti, napríklad prostredníctvom európskych certifikátov kybernetickej bezpečnosti a EÚ vyhlásení o zhode pre produkty alebo služby IKT vydaných v rámci európskeho systému certifikácie kybernetickej bezpečnosti prijatého podľa článku 49 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 ([2]). Keď príslušné subjekty stanovia bezpečnostné požiadavky, ktoré sa majú vzťahovať na nadobúdané produkty IKT, mali by zohľadniť základné požiadavky kybernetickej bezpečnosti stanovené v nariadení Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami.

(18) V záujme ochrany pred kybernetickými hrozbami a podpory predchádzania porušeniam ochrany údajov a zamedzenia ich šírenia by príslušné subjekty mali zaviesť riešenia týkajúce sa bezpečnosti siete. Medzi typické riešenia týkajúce sa bezpečnosti siete patrí používanie firewallov na ochranu interných sietí príslušných subjektov, obmedzenie spojení a prístupu k službám na prípady, keď sú spojenia a prístup absolútne nevyhnutné, používanie virtuálnych neverejných sietí na vzdialený prístup a umožnenie spojení poskytovateľov služieb len na základe žiadosti o autorizáciu a len na stanovený čas, ako je trvanie činnosti údržby.

(19) V záujme ochrany sietí príslušných subjektov a ich informačných systémov pred škodlivým a neautorizovaným softvérom by tieto subjekty mali vykonávať kontroly, ktorými sa zabráni používaniu neautorizovaného softvéru alebo sa odhalí jeho používanie, a v prípade potreby by mali používať softvér na detekciu a reakciu. Príslušné subjekty by takisto mali zvážiť vykonávacie opatrenia na minimalizáciu plochy útoku, na zmenšenie množstva zraniteľností, ktoré by mohli využiť útočníci, na kontrolu spúšťania aplikácií v koncových bodoch a na nasadenie e-mailových filtrov a filtrov pre webové aplikácie na zníženie expozície škodlivému obsahu.

(20) Členské štáty majú podľa článku 21 ods. 2 písm. g) smernice (EÚ) 2022/2555 zabezpečiť, aby kľúčové a dôležité subjekty uplatňovali základné postupy kybernetickej hygieny a odbornú prípravu v oblasti kybernetickej bezpečnosti. Základné postupy kybernetickej hygieny môžu zahŕňať zásady nulovej dôvery, aktualizácie softvéru, konfiguráciu zariadení, segmentáciu siete, správu identít a prístupu alebo informovanosť používateľov, organizovanie odbornej prípravy pre zamestnancov a zvyšovanie informovanosti o kybernetických hrozbách, phishingu alebo technikách sociálneho inžinierstva. Postupy kybernetickej hygieny tvoria súčasť jednotlivých technických a metodických požiadaviek na opatrenia na riadenie kybernetických rizík stanovených v prílohe k tomuto nariadeniu. Pokiaľ ide o základné postupy kybernetickej hygieny pre používateľov, príslušné subjekty by mali zvážiť postupy, ako sú zásada čistého stola a obrazovky, používanie viacstupňovej autentifikácie a iných prostriedkov autentifikácie, bezpečné používanie e-mailu a prehľadávanie webu, ochrana pred phishingom a sociálnym inžinierstvom a bezpečné postupy práce na diaľku.

(21) Príslušné subjekty by s cieľom zabrániť neoprávnenému prístupu k svojim aktívam mali stanoviť a vykonať tematické zásady zaoberajúce sa prístupom osôb a sietí a informačných systémov, ako sú aplikácie.

(22) S cieľom zabrániť tomu, aby zamestnanci mohli zneužívať napríklad prístupové práva v rámci príslušného subjektu na poškodenie a spôsobenie škody, by príslušné subjekty mali zvážiť vhodné opatrenia na riadenie bezpečnosti zamestnancov a zvyšovanie informovanosti zamestnancov o uvedených rizikách. Príslušné subjekty by mali stanoviť, oznámiť a udržiavať disciplinárny postup na riešenie porušení zásad príslušných subjektov v oblasti bezpečnosti sietí a informačných systémov, ktorý môže byť začlenený v ďalších disciplinárnych postupoch stanovených príslušnými subjektmi. Overenie spoľahlivosti zamestnancov a v náležitých prípadoch priamych dodávateľov a poskytovateľov služieb príslušných subjektov by malo prispievať k cieľu bezpečnosti ľudských zdrojov v príslušných subjektoch a môže zahŕňať opatrenia, ako sú kontroly výpisu z registra trestov danej osoby alebo overenie jej služobných povinností v minulosti, a to primerane podľa povinností tejto osoby v príslušnom subjekte a v súlade so zásadami bezpečnosti sietí a informačných systémov príslušného subjektu.

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) Viacstupňová autentifikácia môže zvýšiť kybernetickú bezpečnosť subjektov a subjekty by jej použitie mali zvážiť najmä v prípadoch, keď používatelia využívajú vzdialený prístup k sieťam a informačným systémom alebo keď pristupujú k citlivým informáciám alebo privilegovaným účtom a k účtom na správu systému. Viacstupňovú autentifikáciu možno kombinovať s inými technikami s cieľom vyžadovať v konkrétnych situáciách dodatočné prvky na základe vopred stanovených pravidiel a vzorcov, ako sú prístup z nezvyčajného miesta, z nezvyčajného zariadenia alebo v nezvyčajnom čase.

(24) Príslušné subjekty by mali spravovať a ochraňovať aktíva, ktoré sú pre ne cenné, prostredníctvom spoľahlivej správy aktív, ktorá by mala okrem toho slúžiť ako základ pre analýzu rizík a riadenie kontinuity činností. Príslušné subjekty by mali spravovať hmotné aj nehmotné aktíva a mali by vytvoriť inventár aktív, priradiť aktívu vymedzenú úroveň klasifikácie, zaobchádzať s aktívami a sledovať ich a prijať opatrenia na ochranu aktív počas celého ich životného cyklu.

(25) Správa aktív by mala zahŕňať klasifikáciu aktív podľa ich typu, citlivosti, úrovne rizika a požiadaviek na bezpečnosť a uplatnenie vhodných opatrení a kontrol s cieľom zabezpečiť ich dostupnosť, integritu, dôvernosť a pravosť. Na základe klasifikácie aktív podľa úrovne rizika by príslušné subjekty mali byť schopné uplatňovať vhodné bezpečnostné opatrenia a kontroly na ochranu aktív, ako sú šifrovanie, kontrola prístupu vrátane bezpečnostnej zóny a kontroly fyzického a logického prístupu, zálohovanie, logovanie a monitorovanie, uchovávanie a likvidácia. Príslušné subjekty môžu pri vykonávaní analýzy vplyvu na obchodnú činnosť určiť úroveň klasifikácie na základe následkov narušenia aktív pre subjekty. Všetci zamestnanci subjektov, ktorí zaobchádzajú s aktívami, by sa mali oboznámiť so zásadami zaobchádzania s aktívami a so súvisiacimi pokynmi.

(26) Podrobnosť inventára aktív by mala byť primeraná potrebám príslušných subjektov. Komplexný inventár aktív by pre každé aktívum mohol zahŕňať aspoň jedinečný identifikátor, vlastníka aktíva, opis aktíva, umiestnenie aktíva, druh aktíva, druh a klasifikáciu informácií spracúvaných v aktíve, dátum poslednej aktualizácie alebo bezpečnostnej záplaty aktíva, klasifikáciu aktíva podľa posúdenia rizika a skončenie životnosti aktíva. Pri určovaní vlastníka aktíva by príslušné subjekty mali určiť aj osobu, ktorá zodpovedá za ochranu uvedeného aktíva.

(27) Priraďovaním a organizáciou úloh, povinností a právomocí v oblasti kybernetickej bezpečnosti by sa mala stanoviť konzistentná štruktúra správy a vykonávania kybernetickej bezpečnosti v rámci príslušných subjektov a mala by sa nimi zabezpečiť účinná komunikácia v prípade incidentov. Pri vymedzovaní a prideľovaní povinností určitým úlohám by príslušné subjekty mali zohľadňovať úlohy, ako sú hlavný pracovník pre bezpečnosť informácií, pracovník pre bezpečnosť informácií, pracovník pre riešenie incidentov, audítor alebo porovnateľné ekvivalentné úlohy. Príslušné subjekty môžu prideľovať úlohy a povinnosti externým stranám, ako sú externí poskytovatelia IKT služieb.

(28) V súlade s článkom 21 ods. 2 smernice (EÚ) 2022/2555 majú byť opatrenia na riadenie kybernetických rizík založené na prístupe zohľadňujúcom všetky riziká, ktorého cieľom je chrániť siete a informačné systémy a fyzické prostredie uvedených systémov pred udalosťami, ako je krádež, požiar, povodeň, výpadok telekomunikácie alebo elektrickej energie, alebo pred neoprávneným fyzickým prístupom, poškodením alebo zásahom v súvislosti s informáciami kľúčového alebo dôležitého subjektu a jeho zariadeniami na spracovanie informácií, čo by mohlo ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov. Technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík by sa preto mali zaoberať aj fyzickou a environmentálnou bezpečnosťou sietí a informačných systémov tým, že budú zahŕňať opatrenia na ochranu takýchto systémov pred systémovými zlyhaniami, ľudskými chybami, zlomyseľným konaním alebo prírodnými javmi. Medzi ďalšie príklady fyzických a environmentálnych hrozieb môžu patriť zemetrasenia, výbuchy, sabotáž, vnútorné hrozby, občianske nepokoje, toxický odpad a emisie do životného prostredia. Prevencia straty, poškodenia alebo ohrozenia sietí a informačných systémov alebo prerušenia ich prevádzky z dôvodu zlyhania a narušenia podporných verejných služieb by mala prispieť k cieľu kontinuity činností v príslušných subjektoch. Okrem toho by ochrana proti fyzickým a environmentálnym hrozbám mala prispievať k bezpečnosti pri údržbe sietí a informačných systémov v príslušných subjektoch.

(29) Príslušné subjekty by mali navrhovať a vykonávať opatrenia na ochranu pred fyzickými a environmentálnymi hrozbami, určovať minimálne a maximálne kontrolné prahové hodnoty pre fyzické a environmentálne hrozby a monitorovať environmentálne parametre. Mali by napríklad zvážiť inštaláciu systémov na detekciu zaplavenia oblastí, v ktorých sa nachádzajú siete a informačné systémy, vo včasnej fáze. Pokiaľ ide o riziko požiaru, mali by zvážiť vytvorenie samostatného uzavretého požiarneho úseku pre dátové centrum, používanie ohňovzdorných materiálov, senzory na monitorovanie teploty a vlhkosti, pripojenie budovy k požiarnemu poplachovému systému s automatickým upozornením miestnej hasičskej jednotky a systémy včasnej detekcie požiaru a hasiace systémy. Príslušné subjekty by tiež mali vykonávať pravidelné požiarne cvičenia a protipožiarne kontroly. Okrem toho by príslušné subjekty na zabezpečenie zdroja napájania mali zvážiť ochranu proti prepätiu a zodpovedajúci núdzový zdroj napájania v súlade s príslušnými normami. Navyše, keďže prehrievanie predstavuje riziko pre dostupnosť sietí a informačných systémov, príslušné subjekty, a najmä poskytovatelia služieb dátového centra, by mohli zvážiť primerané, kontinuálne a redundantné klimatizačné systémy.

(30) Cieľom tohto nariadenia je bližšie určiť prípady, v ktorých by sa mal incident považovať za významný v zmysle článku 23 ods. 3 smernice (EÚ) 2022/2555. Kritériá by sa mali stanoviť tak, aby príslušné subjekty boli schopné posúdiť, či je incident významný, aby ho mohli oznámiť v súlade so smernicou (EÚ) 2022/2555. Okrem toho by sa kritériá stanovené v tomto nariadení mali považovať za úplné bez toho, aby bol dotknutý článok 5 smernice (EÚ) 2022/2555. Prípady, v ktorých by sa mal incident považovať za významný, sa v tomto nariadení určujú stanovením horizontálnych prípadov, ako aj prípadov špecifických pre daný typ subjektu.

(31) Podľa článku 23 ods. 4 smernice (EÚ) 2022/2555 by príslušné subjekty mali mať povinnosť oznamovať významné incidenty v lehotách stanovených uvedeným ustanovením. Tieto lehoty na oznamovanie začínajú plynúť od chvíle, keď subjekt zistí takýto významný incident. Príslušný subjekt preto musí oznamovať incidenty, pri ktorých by sa na základe prvotného posúdenia mohlo predpokladať, že by mohli viesť k vážnemu narušeniu prevádzky služieb alebo finančným stratám uvedeného subjektu alebo by mohli zasiahnuť iné fyzické alebo právnické osoby tým, že by im spôsobili značnú majetkovú alebo nemajetkovú ujmu. Preto v prípadoch, keď príslušný subjekt zistí podozrivú udalosť alebo keď ho na potenciálny incident upozorní tretia strana, ako sú napríklad osoba, zákazník, subjekt, orgán, mediálna organizácia alebo iný zdroj, príslušný subjekt by mal podozrivú udalosť včas posúdiť s cieľom určiť, či predstavuje incident, a ak áno, mal by určiť jeho povahu a závažnosť. Príslušný subjekt by sa preto mal považovať za subjekt, ktorý „zistil“ významný incident, vtedy, keď po takomto prvotnom posúdení nadobudne primeranú mieru istoty, že k významnému incidentu došlo.

(32) S cieľom určiť, či je incident významný, by príslušné subjekty v relevantných prípadoch mali spočítať používateľov dotknutých incidentom, pričom by mali vziať do úvahy komerčných a koncových zákazníkov, s ktorými majú zmluvné vzťahy, ako aj fyzické a právnické osoby, ktoré sú pridružené ku komerčným zákazníkom. Ak príslušný subjekt nie je schopný vypočítať počet dotknutých používateľov, na účely výpočtu celkového počtu používateľov zasiahnutých incidentom by sa mal zvážiť odhad možného maximálneho počtu zasiahnutých používateľov vypracovaný príslušným subjektom. Významnosť incidentu týkajúceho sa dôveryhodnej služby by sa nemala určovať len na základe počtu používateľov, ale aj podľa počtu spoliehajúcich sa strán, keďže tie môžu byť takisto dotknuté významným incidentom týkajúcim sa dôveryhodnej služby, pokiaľ ide o narušenie prevádzky a majetkovú alebo nemajetkovú ujmu. Poskytovatelia dôveryhodných služieb by preto pri určovaní, či je incident významný, mali v náležitých prípadoch zohľadniť aj počet spoliehajúcich sa strán. Na tento účel by sa za spoliehajúce sa strany mali považovať fyzické alebo právnické osoby, ktoré sa spoliehajú na dôveryhodnú službu.

(33) Činnosti údržby, ktorých výsledkom je obmedzená dostupnosť alebo nedostupnosť služieb, by sa nemali považovať za významné incidenty, ak k obmedzeniu dostupnosti alebo k nedostupnosti služby dôjde na základe plánovaných činností údržby. Okrem toho by sa nedostupnosť služby nemala považovať za významný incident, ak sú dôvodom nedostupnosti plánované prerušenia, ako sú prerušenia alebo nedostupnosť založené na vopred stanovenej zmluvnej dohode.

(34) Dĺžka trvania incidentu, ktorý má vplyv na dostupnosť služby, by sa mala merať od narušenia riadneho poskytovania tejto služby až po obnovenie jej poskytovania. Ak príslušný subjekt nie je schopný určiť čas, keď sa narušenie začalo, dĺžka trvania incidentu by sa mala merať od odhalenia incidentu alebo odvtedy, keď bol incident zaznamenaný v sieťových alebo systémových logoch alebo v iných zdrojov údajov, podľa toho, čo nastane skôr.

(35) Úplná nedostupnosť služby by sa mala merať od chvíle, keď používatelia úplne prídu o službu, až do obnovenia pravidelných činností alebo prevádzky na úroveň služby, ktorá bola poskytovaná pred incidentom. Ak príslušný subjekt nie je schopný určiť, odkedy je služba úplne nedostupná, nedostupnosť by sa mala merať od chvíle, keď ju tento subjekt odhalil.

(36) Na účely určenia priamych finančných strát vyplývajúcich z incidentu by príslušné subjekty mali zohľadniť všetky finančné straty, ktoré im vznikli v dôsledku incidentu, ako sú náklady na výmenu alebo premiestnenie softvéru, hardvéru alebo infraštruktúry, náklady na zamestnancov vrátane nákladov spojených s nahradením alebo premiestnením zamestnancov, prijímaním ďalších zamestnancov, odmenami za nadčasy a obnovením stratených alebo zhoršených zručností, poplatky z dôvodu nedodržania zmluvných záväzkov, náklady na nápravu a odškodnenie zákazníkov, straty v dôsledku ušlých príjmov, náklady spojené s vnútornou a vonkajšou komunikáciou, náklady na poradenstvo vrátane nákladov spojených s právnym poradenstvom, forenznými službami a sanačnými službami a iné náklady spojené s incidentom. Za finančné straty vyplývajúce z incidentu by sa však nemali považovať správne pokuty ani náklady, ktoré sú potrebné na každodennú prevádzku podniku, vrátane nákladov na všeobecnú údržbu infraštruktúry, vybavenia, hardvéru a softvéru, nákladov na aktualizáciu zručností zamestnancov, interných alebo externých nákladov, ktorých cieľom je zlepšiť obchodné činnosti po incidente vrátane modernizácie, zlepšení, iniciatív na posúdenie rizika a poistného. Príslušné subjekty by mali vypočítať výšku finančných strát na základe dostupných údajov a v prípade, keď skutočnú výšku finančných strát nemožno určiť, príslušné subjekty by túto sumu mali odhadnúť.

(37) Príslušné subjekty by takisto mali mať povinnosť oznamovať incidenty, ktoré spôsobili alebo môžu spôsobiť smrť alebo značné poškodenie zdravia fyzických osôb, keďže tieto incidenty predstavujú obzvlášť závažné prípady incidentov spôsobujúcich značnú majetkovú alebo nemajetkovú ujmu. Napríklad incident, ktorý ovplyvňuje príslušný subjekt, by mohol zapríčiniť nedostupnosť zdravotnej starostlivosti alebo záchranných služieb alebo stratu dôvernosti či integrity údajov s vplyvom na zdravie fyzických osôb. Na účely určenia toho, či incident spôsobil alebo môže spôsobiť značné poškodenie zdravia fyzickej osoby, by príslušné subjekty mali zohľadniť, či incident spôsobil alebo potenciálne môže spôsobiť ťažké zranenia a zlý zdravotný stav. Na tento účel by sa od príslušných subjektov nemalo vyžadovať, aby zhromažďovali ďalšie informácie, ku ktorým nemajú prístup.

(38) Za obmedzenú dostupnosť by sa mali považovať najmä prípady, keď je služba, ktorú poskytuje príslušný subjekt, výrazne pomalšia než priemerný čas odozvy alebo keď nie sú k dispozícii všetky funkcie služby. Ak je to možné, na posúdenie omeškaní času odozvy by sa mali používať objektívne kritériá založené na priemerných časoch odozvy služieb poskytovaných príslušnými subjektmi. Funkciou služby môže byť napríklad funkcia chatu alebo funkcia vyhľadávania obrázkov.

(39) Úspešný, domnelo zlomyseľný a neoprávnený prístup do sietí a informačných systémov príslušného subjektu by sa mal považovať za významný incident, ak by takýto prístup mohol spôsobiť vážne narušenie prevádzky. Napríklad v prípade, keď sa aktér kybernetickej hrozby predbežne nastaví v sieťach a informačných systémoch príslušného subjektu s cieľom narúšať služby v budúcnosti, incident by sa mal považovať za významný.

(40) Opakujúce sa incidenty, ktoré sú prepojené rovnakou zjavnou hlavnou príčinou a ktoré jednotlivo nespĺňajú kritériá významného incidentu, by sa kolektívne mali považovať za významný incident za predpokladu, že spoločne spĺňajú kritérium finančnej straty a že k nim došlo aspoň dvakrát za šesť mesiacov. Takéto opakujúce sa incidenty môžu poukazovať na závažné nedostatky a slabé miesta v postupoch riadenia kybernetických rizík príslušného subjektu a v jeho úrovni vyspelosti v oblasti kybernetickej bezpečnosti. Takéto opakujúce sa incidenty navyše môžu príslušnému subjektu spôsobiť značnú finančnú stratu.

(41) Pokiaľ ide o návrh vykonávacieho aktu, Komisia sa v súlade s článkom 21 ods. 5 a článkom 23 ods. 11 smernice (EÚ) 2022/2555 radila so skupinou pre spoluprácu a s agentúrou ENISA a spolupracovala s nimi.

(42) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([3]) sa viedli konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal svoje stanovisko 1. septembra 2024.

(43) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru zriadeného v súlade s článkom 39 smernice (EÚ) 2022/2555,

PRIJALA TOTO NARIADENIE:

Článok 1

Predmet úpravy

Týmto nariadením sa stanovujú technické a metodické požiadavky na opatrenia uvedené v článku 21 ods. 2 smernice (EÚ) 2022/2555 a bližšie sa určujú prípady, v ktorých by sa mal incident považovať za významný, ako sa uvádza v článku 23 ods. 3 smernice (EÚ) 2022/2555, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí a poskytovateľom dôveryhodných služieb (ďalej len „príslušné subjekty“).

Článok 2

Technické a metodické požiadavky

1. Technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík uvedené v článku 21 ods. 2 písm. a) až j) smernice (EÚ) 2022/2555 sa pre príslušné subjekty stanovujú v prílohe k tomuto nariadeniu.

2. Príslušné subjekty pri vykonávaní a uplatňovaní technických a metodických požiadaviek na opatrenia na riadenie kybernetických rizík stanovených v prílohe k tomuto nariadeniu zabezpečia úroveň bezpečnosti sietí a informačných systémov zodpovedajúcu rizikám. Na tento účel pri dodržiavaní technických a metodických požiadaviek na opatrenia na riadenie kybernetických rizík stanovených v prílohe k tomuto nariadeniu náležite zohľadnia svoj stupeň vystavenia rizikám, svoju veľkosť a pravdepodobnosť výskytu incidentov a ich závažnosť vrátane ich spoločenského a hospodárskeho vplyvu.

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Ak sa v prílohe k tomuto nariadeniu stanovuje, že technická alebo metodická požiadavka na opatrenie na riadenie kybernetických rizík sa má uplatňovať „v prípade potreby“, „v náležitých prípadoch“ alebo „pokiaľ to je možné“, a ak príslušný subjekt nepovažuje za potrebné, náležité ani možné, aby uplatňoval určité technické a metodické požiadavky, svoje odôvodnenie v tejto súvislosti zrozumiteľným spôsobom zaznamená.

Článok 3

Významné incidenty

1. Vo vzťahu k príslušným subjektom sa incident na účely článku 23 ods. 3 smernice (EÚ) 2022/2555 považuje za významný vtedy, ak je splnené aspoň jedno z týchto kritérií:

a) incident príslušnému subjektu spôsobil alebo môže spôsobiť priamu finančnú stratu, ktorá prevyšuje 500 000 EUR alebo 5 % celkového ročného obratu príslušného subjektu za predchádzajúci finančný rok, podľa toho, ktorá suma je nižšia;

b) incident spôsobil alebo môže spôsobiť únik obchodných tajomstiev príslušného subjektu, ako sú vymedzené v článku 2 bode 1 smernice (EÚ) 2016/943;

c) incident spôsobil alebo môže spôsobiť smrť fyzickej osoby;

d) incident spôsobil alebo môže spôsobiť značné poškodenie zdravia fyzickej osoby;

e) došlo k úspešnému, domnelo zlomyseľnému a neoprávnenému prístupu do sietí a informačných systémov, ktorý by mohol spôsobiť vážne narušenie prevádzky;

f) incident spĺňa kritériá uvedené v článku 4;

g) incident spĺňa aspoň jedno z kritérií uvedených v článkoch 5 až 14.

2. Plánované prerušenia služby a zamýšľané následky činností plánovanej údržby, ktoré vykonávajú príslušné subjekty alebo ktoré sa vykonávajú v ich mene, sa nepovažujú za významné incidenty.

3. Pri výpočte počtu používateľov dotknutých incidentom na účely článku 7 a článkov 9 až 14 príslušné subjekty zohľadnia všetky tieto údaje:

a) počet zákazníkov, ktorí uzatvorili zmluvu s príslušným subjektom, ktorý im poskytuje prístup k svojim sieťam a informačným systémom alebo k službám poskytovaným alebo prístupným prostredníctvom týchto sietí a informačných systémov;

b) počet fyzických a právnických osôb spojených s komerčnými zákazníkmi, ktorí používajú siete a informačné systémy alebo služby poskytované alebo prístupné prostredníctvom týchto sietí a informačných systémov.

Článok 4

Opakujúce sa incidenty

Incidenty, ktoré sa jednotlivo nepovažujú za významný incident v zmysle článku 3, sa spoločne považujú za jeden významný incident, ak spĺňajú všetky tieto kritériá:

a) vyskytli sa aspoň dvakrát za šesť mesiacov;

b) majú rovnakú zjavnú hlavnú príčinu;

c) spoločne spĺňajú kritériá uvedené v článku 3 ods. 1 písm. a).

Článok 5

Významné incidenty, pokiaľ ide o poskytovateľov služieb DNS

V prípade poskytovateľov služieb DNS sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) služba rekurzívneho alebo autoritatívneho rozlišovania názvov domén je úplne nedostupná dlhšie ako 30 minút;

b) počas viac ako jednej hodiny je priemerný čas odozvy služby rekurzívneho alebo autoritatívneho rozlišovania názvov domén na požiadavky DNS viac ako 10 sekúnd;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním služby autoritatívneho rozlišovania názvov domén je ohrozená, okrem prípadov, keď z dôvodu nesprávnej konfigurácie sú nesprávne údaje menej než 1 000 názvov domén spravovaných poskytovateľom služieb DNS predstavujúcich najviac 1 % názvov domén spravovaných poskytovateľom služieb DNS.

Článok 6

Významné incidenty, pokiaľ ide o správcov názvov TLD

V prípade správcov názvov TLD sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) služba autoritatívneho rozlišovania názvov domén je úplne nedostupná;

b) počas viac ako jednej hodiny je priemerný čas odozvy služby autoritatívneho rozlišovania názvov domén na požiadavky DNS viac ako 10 sekúnd;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s technickou prevádzkou TLD je ohrozená.

Článok 7

Významné incidenty, pokiaľ ide o poskytovateľov služieb cloud computingu

V prípade poskytovateľov služieb cloud computingu sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) poskytovaná služba cloud computingu je úplne nedostupná dlhšie ako 30 minút;

b) dostupnosť služby cloud computingu poskytovateľa je počas viac ako jednej hodiny obmedzená pre viac ako 5 % používateľov služby cloud computingu v Únii alebo pre viac ako 1 milión používateľov služby cloud computingu v Únii, podľa toho, ktorý údaj je nižší;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním služby cloud computingu je ohrozená v dôsledku domnelo zlomyseľného konania;

d) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním služby cloud computingu je ohrozená s dosahom na viac ako 5 % používateľov tejto služby cloud computingu v Únii alebo na viac ako 1 milión používateľov tejto služby cloud computingu v Únii, podľa toho, ktorý údaj je nižší.

Článok 8

Významné incidenty, pokiaľ ide o poskytovateľov služieb dátového centra

V prípade poskytovateľov služieb dátového centra sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) služba dátového centra prevádzkovaného poskytovateľom je úplne nedostupná;

b) dostupnosť služby dátového centra prevádzkovaného poskytovateľom je obmedzená počas viac ako jednej hodiny;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním služby dátového centra je ohrozená v dôsledku domnelo zlomyseľného konania;

d) fyzický prístup k dátovému centru prevádzkovanému poskytovateľom je ohrozený.

Článok 9

Významné incidenty, pokiaľ ide o poskytovateľov sietí na sprístupňovanie obsahu

V prípade poskytovateľov sietí na sprístupňovanie obsahu sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) sieť na sprístupňovanie obsahu je úplne nedostupná dlhšie ako 30 minút;

b) dostupnosť siete na sprístupňovanie obsahu je počas viac ako jednej hodiny obmedzená pre viac ako 5 % používateľov siete na sprístupňovanie obsahu v Únii alebo pre viac ako 1 milión používateľov siete na sprístupňovanie obsahu v Únii, podľa toho, ktorý údaj je nižší;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním siete na sprístupňovanie obsahu je ohrozená v dôsledku domnelo zlomyseľného konania;

d) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním siete na sprístupňovanie obsahu je ohrozená s dosahom na viac ako 5 % používateľov tejto siete na sprístupňovanie obsahu v Únii alebo na viac ako 1 milión používateľov tejto siete na sprístupňovanie obsahu v Únii, podľa toho, ktorý údaj je nižší.

Článok 10

Významné incidenty, pokiaľ ide o poskytovateľov riadených služieb a poskytovateľov riadených bezpečnostných služieb

V prípade poskytovateľov riadených služieb a poskytovateľov riadených bezpečnostných služieb sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) riadená služba alebo riadená bezpečnostná služba sú úplne nedostupné dlhšie ako 30 minút;

b) dostupnosť riadenej služby alebo riadenej bezpečnostnej služby je počas viac ako jednej hodiny obmedzená pre viac ako 5 % používateľov služby v Únii alebo pre viac ako 1 milión používateľov služby v Únii, podľa toho, ktorý údaj je nižší;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním riadenej služby alebo riadenej bezpečnostnej služby je ohrozená v dôsledku domnelo zlomyseľného konania;

d) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním riadenej služby alebo riadenej bezpečnostnej služby je ohrozená s dosahom na viac ako 5 % používateľov tejto riadenej služby alebo riadenej bezpečnostnej služby v Únii alebo na viac ako 1 milión používateľov tejto riadenej služby alebo riadenej bezpečnostnej služby v Únii, podľa toho, ktorý údaj je nižší.

Článok 11

Významné incidenty, pokiaľ ide o poskytovateľov online trhov

V prípade poskytovateľov online trhov sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) online trh je úplne nedostupný pre viac ako 5 % používateľov online trhu v Únii alebo pre viac ako 1 milión používateľov online trhu v Únii, podľa toho, ktorý údaj je nižší;

b) viac ako 5 % používateľov online trhu v Únii alebo viac ako 1 milión používateľov online trhu v Únii, podľa toho, ktorý údaj je nižší, je dotknutých obmedzenou dostupnosťou tohto online trhu;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním online trhu je ohrozená v dôsledku domnelo zlomyseľného konania;

d) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním online trhu je ohrozená s dosahom na viac ako 5 % používateľov tohto online trhu v Únii alebo na viac ako 1 milión používateľov tohto online trhu v Únii, podľa toho, ktorý údaj je nižší.

Článok 12

Významné incidenty, pokiaľ ide o poskytovateľov internetových vyhľadávačov

V prípade poskytovateľov internetových vyhľadávačov sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) internetový vyhľadávač je úplne nedostupný pre viac ako 5 % používateľov tohto internetového vyhľadávača v Únii alebo pre viac ako 1 milión používateľov tohto internetového vyhľadávača v Únii, podľa toho, ktorý údaj je nižší;

b) viac ako 5 % používateľov internetového vyhľadávača v Únii alebo viac ako 1 milión používateľov internetového vyhľadávača v Únii, podľa toho, ktorý údaj je nižší, je dotknutých obmedzenou dostupnosťou tohto internetového vyhľadávača;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním internetového vyhľadávača je ohrozená v dôsledku domnelo zlomyseľného konania;

d) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním internetového vyhľadávača je ohrozená s dosahom na viac ako 5 % používateľov tohto internetového vyhľadávača v Únii alebo na viac ako 1 milión používateľov tohto internetového vyhľadávača v Únii, podľa toho, ktorý údaj je nižší.

Článok 13

Významné incidenty, pokiaľ ide o poskytovateľov platforiem služieb sociálnej siete

V prípade poskytovateľov platforiem služieb sociálnej siete sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) platforma služieb sociálnej siete je úplne nedostupná pre viac ako 5 % používateľov tejto platformy služieb sociálnej siete v Únii alebo pre viac ako 1 milión používateľov tejto platformy služieb sociálnej siete v Únii, podľa toho, ktorý údaj je nižší;

b) viac ako 5 % používateľov platformy služieb sociálnej siete v Únii alebo viac ako 1 milión používateľov platformy služieb sociálnej siete v Únii, podľa toho, ktorý údaj je nižší, je dotknutých obmedzenou dostupnosťou tejto platformy služieb sociálnej siete;

c) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním platformy služieb sociálnej siete je ohrozená v dôsledku domnelo zlomyseľného konania;

d) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním platformy služieb sociálnej siete je ohrozená s dosahom na viac ako 5 % používateľov tejto platformy služieb sociálnej siete v Únii alebo na viac ako 1 milión používateľov tejto platformy služieb sociálnej siete v Únii, podľa toho, ktorý údaj je nižší.

Článok 14

Významné incidenty, pokiaľ ide o poskytovateľov dôveryhodných služieb

V prípade poskytovateľov dôveryhodných služieb sa incident považuje za významný v zmysle článku 3 ods. 1 písm. g), ak spĺňa aspoň jedno z týchto kritérií:

a) dôveryhodná služba je úplne nedostupná dlhšie ako 20 minút;

b) dôveryhodná služba je používateľom alebo spoliehajúcim sa stranám nedostupná dlhšie ako jednu hodinu za kalendárny týždeň;

c) viac ako 1 % používateľov alebo spoliehajúcich sa strán v Únii alebo viac ako 200 000 používateľov alebo spoliehajúcich sa strán v Únii, podľa toho, ktorý údaj je nižší, je dotknutých obmedzenou dostupnosťou dôveryhodnej služby;

d) fyzický prístup do oblasti, kde sa nachádzajú siete a informačné systémy a do ktorej je prístup obmedzený len pre dôveryhodný personál poskytovateľa dôveryhodných služieb, alebo ochrana takéhoto fyzického prístupu sú ohrozené;

e) integrita, dôvernosť alebo pravosť uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním dôveryhodnej služby je ohrozená s dosahom na viac ako 0,1 % používateľov alebo spoliehajúcich sa strán alebo na viac ako 100 používateľov alebo spoliehajúcich sa strán využívajúcich dôveryhodnú službu v Únii, podľa toho, ktorý údaj je nižší.

Článok 15

Zrušenie

Vykonávacie nariadenie Komisie (EÚ) 2018/151 ([4]) sa zrušuje.

Článok 16

Nadobudnutie účinnosti a uplatňovanie

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 17. októbra 2024

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

([4]) Vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie toho, či má incident závažný vplyv (Ú. v. EÚ L 26, 31.1.2018, s. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

PRÍLOHA

Technické a metodické požiadavky uvedené v článku 2 tohto nariadenia

1. **Zásady bezpečnosti sietí a informačných systémov [článok 21 ods. 2 písm. a) smernice (EÚ) 2022/2555]**

1.1. *Zásady bezpečnosti sietí a informačných systémov*

1.1.1. Na účely článku 21 ods. 2 písm. a) smernice (EÚ) 2022/2555 zásady bezpečnosti sietí a informačných systémov:

a) stanovia prístup príslušných subjektov k riadeniu bezpečnosti ich sietí a informačných systémov;

b) sú primerané obchodnej stratégii a cieľom príslušných subjektov a dopĺňajú ich;

c) stanovia ciele v oblasti sieťovej a informačnej bezpečnosti;

d) zahŕňajú záväzok sústavne zlepšovať bezpečnosť sietí a informačných systémov;

e) zahŕňajú záväzok poskytovať primerané zdroje potrebné na ich vykonávanie vrátane nevyhnutného personálu, finančných zdrojov, procesov, nástrojov a technológií;

f) oznámia sa príslušným zamestnancom a príslušným zainteresovaným externým stranám, ktorí ich vezmú na vedomie;

g) stanovia úlohy a povinnosti podľa bodu 1.2;

h) stanovia zoznam dokumentov, ktoré sa majú uchovávať, a trvanie ich uchovávania;

i) stanovia zoznam tematických zásad;

j) stanovia ukazovatele a opatrenia na monitorovanie ich vykonávania a aktuálneho stavu úrovne vyspelosti sieťovej a informačnej bezpečnosti príslušných subjektov;

k) stanovia dátum formálneho schválenia riadiacimi orgánmi príslušných subjektov (ďalej len „riadiace orgány“).

1.1.2. Riadiace orgány preskúmajú a v prípade potreby aktualizujú zásady bezpečnosti sietí a informačných systémov aspoň raz za rok a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík. Výsledky preskúmania sa zaznamenajú.

1.2. *Úlohy, povinnosti a právomoci*

1.2.1. Príslušné subjekty v rámci svojich zásad bezpečnosti sietí a informačných systémov uvedených v bode 1.1 stanovia povinnosti a právomoci týkajúce sa bezpečnosti sietí a informačných systémov, priradia ich k úlohám, pridelia ich podľa potrieb príslušných subjektov a oznámia ich riadiacim orgánom.

1.2.2. Príslušné subjekty vyžadujú od všetkých zamestnancov a tretích strán, aby uplatňovali bezpečnosť sietí a informačných systémov v súlade so stanovenými zásadami sieťovej a informačnej bezpečnosti, s tematickými zásadami a postupmi príslušných subjektov.

1.2.3. Správy riadiacemu orgánu o otázkach bezpečnosti sietí a informačných systémov podáva priamo aspoň jedna osoba.

1.2.4. V závislosti od veľkosti príslušných subjektov sa na bezpečnosť sietí a informačných systémov vzťahujú osobitné úlohy alebo povinnosti vykonávané popri existujúcich úlohách.

1.2.5. Povinnosti a oblasti právomocí, ktoré sa navzájom vylučujú, sa od seba v náležitých prípadoch oddelia.

1.2.6. Úlohy, povinnosti a právomoci preskúmavajú a v prípade potreby aktualizujú riadiace orgány v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

2. **Zásady riadenia rizík [článok 21 ods. 2 písm. a) smernice (EÚ) 2022/2555]**

2.1. *Rámec riadenia rizík*

2.1.1. Na účely článku 21 ods. 2 písm. a) smernice (EÚ) 2022/2555 príslušné subjekty vytvoria a udržiavajú vhodný rámec riadenia rizík s cieľom určiť a riešiť riziká pre bezpečnosť sietí a informačných systémov. Príslušné subjekty vykonajú a zaznamenajú posúdenia rizík a na základe výsledkov stanovia, vykonajú a monitorujú plán ošetrenia rizík. Riadiace orgány alebo v náležitých prípadoch osoby, ktoré nesú zodpovednosť a majú právomoc riadiť riziká, prijmú výsledky posúdenia rizík a akceptujú zvyškové IKT riziká, a to za predpokladu, že príslušné subjekty zabezpečia primerané podávanie správ riadiacim orgánom.

2.1.2. Príslušné subjekty na účely bodu 2.1.1 stanovia postupy na určenie, analýzu, posúdenie a ošetrenie rizík (ďalej len „proces riadenia kybernetických rizík“). V náležitých prípadoch proces riadenia kybernetických rizík tvorí neoddeliteľnú súčasť celkového procesu riadenia rizík príslušných subjektov. Príslušné subjekty v rámci procesu riadenia kybernetických rizík:

a) dodržiavajú metodiku riadenia rizík;

b) stanovia úroveň tolerancie rizika v súlade s ochotou príslušných subjektov podstupovať riziká;

c) stanovia a udržiavajú príslušné kritériá v oblasti rizík;

d) v súlade s prístupom zohľadňujúcim všetky riziká určia a zaznamenajú riziká pre bezpečnosť sietí a informačných systémov, a to najmä v súvislosti s tretími stranami a rizikami, ktoré by mohli viesť k narušeniam dostupnosti, integrity, pravosti a dôvernosti sietí a informačných systémov vrátane určenia jediných bodov zlyhania;

e) analyzujú riziká pre bezpečnosť sietí a informačných systémov vrátane hrozby, pravdepodobnosti, vplyvu a úrovne rizika, pričom zohľadnia spravodajské informácie o kybernetických hrozbách a zraniteľnosti;

f) vyhodnocujú zistené riziká na základe kritérií v oblasti rizík;

g) určia vhodné možnosti ošetrenia rizík a opatrenia na ošetrenie rizík a stanovia ich priority;

h) nepretržite monitorujú vykonávanie opatrení na ošetrenie rizík;

i) určia osobu zodpovednú za vykonávanie opatrení na ošetrenie rizík a to, kedy by sa tieto opatrenia mali vykonať;

j) zrozumiteľne zaznamenajú zvolené opatrenia na ošetrenie rizík a dôvody opodstatňujúce akceptáciu zvyškových IKT rizík v pláne ošetrenia rizík.

2.1.3. Pri určovaní vhodných možností ošetrenia rizík a opatrení na ošetrenie rizík a stanovovaní ich priorít príslušné subjekty zohľadnia výsledky posúdenia rizík, výsledky postupu posudzovania účinnosti opatrení na riadenie kybernetických rizík, náklady na vykonávanie vo vzťahu k očakávanému prínosu, klasifikáciu aktív uvedenú v bode 12.1 a analýzu vplyvu na obchodnú činnosť uvedenú v bode 4.1.3.

2.1.4. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú výsledky posúdenia rizík a plán ošetrenia rizík v plánovaných intervaloch a najmenej raz ročne, ako aj v prípade výskytu významných zmien operácií alebo rizík alebo významných incidentov.

2.2. *Monitorovanie súladu*

2.2.1. Príslušné subjekty pravidelne preskúmavajú súlad so svojimi zásadami bezpečnosti sietí a informačných systémov, tematickými zásadami, pravidlami a normami. Riadiacim orgánom sa v pravidelných správach na základe preskúmaní súladu poskytujú informácie o stave sieťovej a informačnej bezpečnosti.

2.2.2. Príslušné subjekty zavedú účinný systém podávania správ o súlade primeraný ich štruktúram, prevádzkovým prostrediam a panoráme hrozieb. Systém podávania správ o súlade dokáže riadiacim orgánom poskytovať informovaný pohľad na aktuálny stav riadenia rizík príslušnými subjektmi.

2.2.3. Príslušné subjekty vykonávajú monitorovanie súladu v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

2.3. *Nezávislé preskúmanie informačnej a sieťovej bezpečnosti*

2.3.1. Príslušné subjekty vykonajú nezávisle preskúmanie svojho prístupu k riadeniu bezpečnosti sietí a informačných systémov a jeho vykonávania vrátane osôb, procesov a technológií.

2.3.2. Príslušné subjekty vypracujú a udržiavajú procesy na vykonávanie nezávislých preskúmaní, ktoré uskutočňujú osoby s primeranou audítorskou kvalifikáciou. Ak nezávislé preskúmanie vykonávajú zamestnanci príslušného subjektu, tieto osoby nesmú byť v hierarchickom vzťahu voči personálu oblasti, ktorá je predmetom preskúmania. Ak veľkosť príslušných subjektov neumožňuje takéto oddelenie línie hierarchie, príslušné subjekty zavedú alternatívne opatrenia s cieľom zaručiť nestrannosť preskúmaní.

2.3.3. Výsledky nezávislých preskúmaní vrátane výsledkov monitorovania súladu podľa bodu 2.2 a monitorovania a merania podľa bodu 7 sa oznámia riadiacim orgánom. Prijmú sa nápravné opatrenia alebo sa akceptujú zvyškové IKT riziká, a to v súlade s kritériami akceptácie rizika príslušných subjektov.

2.3.4. Nezávislé preskúmania sa vykonávajú v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

3. **Riešenie incidentov [článok 21 ods. 2 písm. b) smernice (EÚ) 2022/2555]**

3.1. *Zásady riešenia incidentov*

3.1.1. Na účely článku 21 ods. 2 písm. b) smernice (EÚ) 2022/2555 príslušné subjekty stanovia a vykonávajú zásady riešenia incidentov, ktorými sa stanovujú úlohy, povinnosti a postupy na včasné odhaľovanie incidentov, ich analýzu, zamedzenie ich šíreniu alebo reagovanie na ne, zotavenie sa z nich, ich zaznamenávanie a oznamovanie.

3.1.2. Zásady uvedené v bode 3.1.1 sú v súlade s plánom na zabezpečenie kontinuity činností a plánom obnovy systému po havárii uvedenými v bode 4.1. Tieto zásady zahŕňajú:

a) systém kategorizácie incidentov, ktorý je v súlade s posúdením a klasifikáciou udalosti vykonanými podľa bodu 3.4.1;

b) plány účinnej komunikácie vrátane plánov na postúpenie a podávanie správ;

c) pridelenie úloh týkajúcich sa odhaľovania incidentov a primeraného reagovania na ne kvalifikovaným zamestnancom;

d) dokumenty, ktoré sa majú používať v priebehu odhaľovania incidentov a reagovania na ne, ako sú príručky reakcie na incidenty, diagramy postúpenia incidentov, zoznamy kontaktov a vzory.

3.1.3. Úlohy, povinnosti a postupy stanovené v zásadách sa testujú a preskúmavajú a v prípade potreby aktualizujú v plánovaných intervaloch a po významných incidentoch alebo po významných zmenách operácií alebo rizík.

3.2. *Monitorovanie a logovanie*

3.2.1. Príslušné subjekty stanovia postupy a používajú nástroje na monitorovanie a logovanie činností vo svojich sieťach a informačných systémoch s cieľom odhaľovať udalosti, ktoré by sa mohli považovať za incidenty, a primerane na ne reagovať v záujme zmiernenia ich dosahu.

3.2.2. Pokiaľ je to možné, monitorovanie je automatizované a vykonáva sa buď nepretržite, alebo v pravidelných intervaloch, a to podľa schopností podniku. Príslušné subjekty vykonávajú činnosti v oblasti monitorovania spôsobom, ktorým sa minimalizujú falošne pozitívne a falošne negatívne výsledky.

3.2.3. Na základe postupov uvedených v bode 3.2.1 príslušné subjekty vedú, zaznamenávajú a preskúmavajú logy. Príslušné subjekty vypracujú zoznam aktív podliehajúcich logovaniu na základe výsledkov posúdenia rizík vykonaného podľa bodu 2.1. V prípade potreby logy obsahujú údaje o:

a) relevantnej odchádzajúcej a prichádzajúcej sieťovej prevádzke;

b) vytvorení, zmene alebo vymazaní používateľov sietí a informačných systémov príslušných subjektov a o rozšírení povolení;

c) prístupe k systémom a aplikáciám;

d) udalostiach súvisiacich s autentifikáciou;

e) všetkých privilegovaných prístupoch k systémom a aplikáciám a o činnostiach vykonávaných v rámci správcovských účtov;

f) prístupe ku kriticky významným konfiguračným a záložným súborom alebo o zmenách týchto súborov;

g) logoch udalostí a logoch z bezpečnostných nástrojov, ako sú antivírusový softvér, systémy detekcie prienikov alebo firewally;

h) používaní systémových prostriedkov, ako aj o ich výkone;

i) fyzickom prístupe k zariadeniam;

j) prístupe k ich sieťovému vybaveniu a zariadeniam a o ich používaní;

k) aktivácii, zastavení a pozastavení rozličných logov;

l) environmentálnych udalostiach.

3.2.4. Logy podliehajú pravidelnému preskúmaniu s cieľom odhaliť akékoľvek nezvyčajné alebo nežiaduce trendy. V prípade potreby príslušné subjekty stanovia vhodné prahové hodnoty pre poplach. V prípade prekročenia stanovených prahových hodnôt pre poplach sa v prípade potreby automaticky spustí poplach. Príslušné subjekty zabezpečia, že v prípade poplachu sa včas spustí kvalifikovaná a primeraná reakcia.

3.2.5. Príslušné subjekty vedú a zálohujú logy počas vopred stanoveného obdobia a chránia ich pred neoprávneným prístupom alebo zmenami.

3.2.6. Pokiaľ je to možné, príslušné subjekty zabezpečia, že všetky systémy majú synchronizované zdroje času, aby mohli zharmonizovať logy medzi systémami na účely posúdenia udalosti. Príslušné subjekty vypracujú a vedú zoznam všetkých aktív, ktoré sa zaznamenávajú v logoch, a zabezpečia, aby systémy monitorovania a logovania boli redundantné. Dostupnosť systémov monitorovania a logovania sa monitoruje nezávisle od systémov, ktoré monitorujú.

3.2.7. Postupy, ako aj zoznam aktív, ktoré sú predmetom logovania, sa preskúmavajú a v prípade potreby aktualizujú v plánovaných intervaloch a po významných incidentoch.

3.3. *Oznamovanie udalostí*

3.3.1. Príslušné subjekty zavedú jednoduchý mechanizmus, ktorý ich zamestnancom, dodávateľom a zákazníkom umožňuje oznamovať podozrivé udalosti.

3.3.2. Príslušné subjekty svojich dodávateľov a zákazníkov v prípade potreby informujú o mechanizme oznamovania udalostí a svojim zamestnancom poskytujú pravidelnú odbornú prípravu týkajúcu sa toho, ako sa mechanizmus používa.

3.4. *Posúdenie a klasifikácia udalosti*

3.4.1. Príslušné subjekty posudzujú podozrivé udalosti s cieľom určiť, či predstavujú incidenty, a ak áno, určia ich povahu a závažnosť.

3.4.2. Príslušné subjekty na účely bodu 3.4.1 konajú takto:

a) vykonávajú posúdenie založené na vopred vymedzených kritériách a na triedení s cieľom určiť priority pri zamedzovaní šírenia a odstraňovaní incidentov;

b) raz za štvrťrok posudzujú existenciu opakujúcich sa incidentov uvedených v článku 4 tohto nariadenia;

c) preskúmavajú príslušné logy na účely posúdenia a klasifikácie udalosti;

d) zavedú postup na koreláciu a analýzu logov a

e) prehodnocujú a znovu klasifikujú udalosti v prípade nových informácií alebo po analýze v minulosti dostupných informácií.

3.5. *Reakcia na incident*

3.5.1. Príslušné subjekty včas reagujú na incidenty, a to v súlade so zdokumentovanými postupmi.

3.5.2. Postupy reakcie na incidenty majú tieto fázy:

a) zamedzenie šíreniu incidentu s cieľom zabrániť šíreniu jeho následkov;

b) odstránenie incidentu s cieľom zabrániť jeho pokračovaniu alebo opätovnému výskytu;

c) v prípade potreby zotavenie sa z incidentu.

3.5.3. Príslušné subjekty stanovia plány a postupy komunikácie:

a) s jednotkami pre riešenie počítačových bezpečnostných incidentov (ďalej len „jednotky CSIRT“) alebo v náležitých prípadoch s príslušnými orgánmi, pokiaľ ide o oznamovanie incidentov;

b) na účely komunikácie medzi zamestnancami príslušného subjektu a komunikácie s príslušnými zainteresovanými stranami mimo príslušného subjektu.

3.5.4. Príslušné subjekty v logoch zaznamenávajú činnosti reakcie na incidenty v súlade s postupmi uvedenými v bode 3.2.1 a zaznamenávajú dôkazy.

3.5.5. Príslušné subjekty testujú postupy reakcie na incidenty v plánovaných intervaloch.

3.6. *Preskúmania po incidentoch*

3.6.1. V prípade potreby príslušné subjekty po zotavení sa z incidentov vykonajú preskúmania po incidentoch. Pokiaľ je to možné, v preskúmaniach po incidentoch sa určí hlavná príčina incidentu, pričom výsledkom týchto preskúmaní sú zdokumentované získané poznatky na zníženie výskytu a následkov budúcich incidentov.

3.6.2. Príslušné subjekty zabezpečia, aby preskúmania po incidentoch prispievali k zlepšeniu prístupu príslušných subjektov k sieťovej a informačnej bezpečnosti, k opatreniam na ošetrenie rizík a k postupom riešenia a odhaľovania incidentov, ako aj k postupom reakcie na incidenty.

3.6.3. Príslušné subjekty v plánovaných intervaloch preskúmajú, či incidenty viedli k preskúmaniam po incidentoch.

4. **Kontinuita činností a krízové riadenie [článok 21 ods. 2 písm. c) smernice (EÚ) 2022/2555]**

4.1. *Plán na zabezpečenie kontinuity činností a plán obnovy systému po havárii*

4.1.1. Na účely článku 21 ods. 2 písm. c) smernice (EÚ) 2022/2555 príslušné subjekty stanovia a vedú plán na zabezpečenie kontinuity činností a plán obnovy systému po havárii, ktorý uplatňujú v prípade incidentov.

4.1.2. Operácie príslušných subjektov sa obnovia podľa plánu na zabezpečenie kontinuity činností a plánu obnovy systému po havárii. Plán vychádza z výsledkov posúdenia rizík vykonaného podľa bodu 2.1 a v prípade potreby obsahuje:

a) účel, rozsah pôsobnosti a cieľovú skupinu;

b) úlohy a povinnosti;

c) hlavné kontaktné osoby a (interné a externé) komunikačné kanály;

d) podmienky aktivácie a deaktivácie plánu;

e) poradie obnovovania operácií;

f) plány obnovy konkrétnych operácií vrátane cieľov obnovy;

g) požadované zdroje vrátane záloh a redundantných kapacít;

h) obnovenie činností a pokračovanie v nich po dočasných opatreniach.

4.1.3. Príslušné subjekty vykonajú analýzu vplyvu na obchodnú činnosť s cieľom posúdiť potenciálny vplyv závažných narušení ich obchodných operácií a na základe tejto analýzy vplyvu na obchodnú činnosť stanovia požiadavky na kontinuitu týkajúce sa sietí a informačných systémov.

4.1.4. Plán na zabezpečenie kontinuity činností a plán obnovy systému po havárii podliehajú testovaniu, preskúmaniu a v prípade potreby aktualizácii, a to v plánovaných intervaloch a po významných incidentoch alebo po významných zmenách operácií alebo rizík. Príslušné subjekty zabezpečia, že sa v plánoch zohľadnia poznatky získané z takýchto testov.

4.2. *Riadenie zálohovania a redundantných kapacít*

4.2.1. Príslušné subjekty uchovávajú záložné kópie údajov a poskytujú dostatočné dostupné zdroje vrátane zariadení, sietí a informačných systémov a zamestnancov s cieľom zabezpečiť primeranú úroveň redundancie.

4.2.2. Na základe výsledkov posúdenia rizík vykonaného podľa bodu 2.1, ako aj na základe plánu na zabezpečenie kontinuity činností príslušné subjekty stanovia plány zálohovania, ktoré zahŕňajú:

a) časy obnovy;

b) uistenie, že záložné kópie sú úplné a presné, vrátane konfiguračných údajov a údajov uložených v prostredí služieb cloud computingu;

c) uloženie záložných kópií (online alebo offline) na bezpečnom mieste alebo miestach, ktoré nie sú v rámci tej istej siete ako systém a nachádzajú sa v dostatočnej vzdialenosti, aby unikli poškodeniu po havárii v hlavnom mieste;

d) vhodné kontroly fyzického a logického prístupu k záložným kópiám v súlade s úrovňou klasifikácie aktív;

e) obnovu údajov zo záložných kópií;

f) obdobia uchovávania založené na obchodných a regulačných požiadavkách.

4.2.3. Príslušné subjekty vykonávajú pravidelné kontroly integrity záložných kópií.

4.2.4. Na základe výsledkov posúdenia rizík vykonaného podľa bodu 2.1, ako aj na základe plánu na zabezpečenie kontinuity činností príslušné subjekty zabezpečia dostatočnú dostupnosť zdrojov prostredníctvom aspoň čiastočnej redundancie týchto prvkov:

a) siete a informačné systémy;

b) aktíva vrátane zariadení, vybavenia a zásob;

c) personál s potrebnou zodpovednosťou, právomocami a spôsobilosťou;

d) vhodné komunikačné kanály.

4.2.5. V prípade potreby príslušné subjekty zabezpečia, aby sa pri monitorovaní a úprave zdrojov vrátane zariadení, systémov a personálu riadne zohľadnili požiadavky na zálohovanie a redundantné kapacity.

4.2.6. Príslušné subjekty vykonávajú pravidelné testovanie obnovy záložných kópií a redundantných kapacít s cieľom zabezpečiť, aby sa na ne mohli spoľahnúť v podmienkach obnovovania a aby zahŕňali kópie, procesy a vedomosti na vykonanie účinnej obnovy. Príslušné subjekty zaznamenajú výsledky testov a v prípade potreby prijmú nápravné opatrenia.

4.3. *Krízové riadenie*

4.3.1. Príslušné subjekty zavedú proces krízového riadenia.

4.3.2. Príslušné subjekty zabezpečia, aby bol proces krízového riadenia zameraný aspoň na tieto prvky:

a) úlohy a povinnosti pre personál a v prípade potreby pre dodávateľov a poskytovateľov služieb, pričom sa stanoví rozdelenie úloh v krízových situáciách vrátane konkrétnych krokov, ktoré sa majú dodržať;

b) vhodné prostriedky komunikácie medzi príslušnými subjektmi a relevantnými príslušnými orgánmi;

c) uplatňovanie primeraných opatrení na zabezpečenie zachovania bezpečnosti sietí a informačných systémov v krízových situáciách.

Súčasťou toku informácií medzi príslušnými subjektmi a relevantnými príslušnými orgánmi na účely písmena b) sú povinné oznámenia, ako sú správy o incidentoch a súvisiace harmonogramy, aj nepovinné oznámenia.

4.3.3. Príslušné subjekty vykonajú proces týkajúci sa riadenia a využívania informácií získaných od jednotiek CSIRT alebo v náležitých prípadoch od príslušných orgánov, pokiaľ ide o incidenty, zraniteľnosti, hrozby alebo prípadné zmierňujúce opatrenia.

4.3.4. Príslušné subjekty testujú, preskúmavajú a v prípade potreby aktualizujú plán krízového riadenia v pravidelných intervaloch alebo po významných incidentoch či po významných zmenách operácií alebo rizík.

5. **Bezpečnosť dodávateľského reťazca [článok 21 ods. 2 písm. d) smernice (EÚ) 2022/2555]**

5.1. *Zásady bezpečnosti dodávateľského reťazca*

5.1.1. Na účely článku 21 ods. 2 písm. d) smernice (EÚ) 2022/2555 príslušné subjekty stanovia, vykonajú a uplatňujú zásady bezpečnosti dodávateľského reťazca, ktorými sa upravujú vzťahy s ich priamymi dodávateľmi a poskytovateľmi služieb, s cieľom zmierniť zistené riziká pre bezpečnosť sietí a informačných systémov. Príslušné subjekty v rámci zásad bezpečnosti dodávateľského reťazca určia svoju úlohu v dodávateľskom reťazci a oznámia ju svojim priamym dodávateľom a poskytovateľom služieb.

5.1.2. Príslušné subjekty v rámci zásad bezpečnosti dodávateľského reťazca uvedenej v bode 5.1.1 stanovia kritériá na výber dodávateľov a poskytovateľov služieb a uzatváranie zmlúv s nimi. Tieto kritériá zahŕňajú:

a) postupy dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich bezpečných vývojových postupov;

b) schopnosť dodávateľov a poskytovateľov služieb dodržiavať špecifikácie kybernetickej bezpečnosti stanovené príslušnými subjektmi;

c) celkovú kvalitu a odolnosť produktov a služieb IKT a opatrenia na riadenie kybernetických rizík, ktoré zahŕňajú, vrátane rizík a úrovne klasifikácie produktov a služieb IKT;

d) schopnosť príslušných subjektov diverzifikovať zdroje dodávok a v náležitých prípadoch obmedziť odkázanosť na určitého dodávateľa.

5.1.3. Príslušné subjekty pri stanovovaní svojich zásad bezpečnosti dodávateľského reťazca v náležitých prípadoch zohľadnia výsledky koordinovaných posúdení bezpečnostných rizík kritických dodávateľských reťazcov vykonaných v súlade s článkom 22 ods. 1 smernice (EÚ) 2022/2555.

5.1.4. Na základe zásad bezpečnosti dodávateľského reťazca, ako aj s ohľadom na výsledky posúdenia rizík vykonaného podľa bodu 2.1 tejto prílohy príslušné subjekty v prípade potreby zabezpečia, aby sa v ich zmluvách s dodávateľmi a poskytovateľmi služieb stanovili, v prípade potreby aj na základe dohôd o úrovni poskytovaných služieb, tieto prvky:

a) požiadavky na kybernetickú bezpečnosť dodávateľov alebo poskytovateľov služieb vrátane požiadaviek týkajúcich sa bezpečnosti pri nadobúdaní služieb alebo produktov IKT uvedených v bode 6.1;

b) požiadavky týkajúce sa informovanosti, zručností a odbornej prípravy a v prípade potreby aj certifikácií, ktoré sa vyžadujú od zamestnancov dodávateľov alebo poskytovateľov služieb;

c) požiadavky týkajúce sa overenia spoľahlivosti zamestnancov dodávateľov a poskytovateľov služieb;

d) povinnosť dodávateľov a poskytovateľov služieb bezodkladne oznamovať príslušným subjektom incidenty, ktoré predstavujú riziko pre bezpečnosť sietí a informačných systémov týchto subjektov;

e) právo na audit alebo právo dostávať audítorské správy;

f) povinnosť dodávateľov a poskytovateľov služieb riešiť zraniteľnosti, ktoré predstavujú riziko pre bezpečnosť sietí a informačných systémov príslušných subjektov;

g) požiadavky týkajúce sa subdodávateľských vzťahov a v prípade, keď príslušné subjekty povolia využívanie subdodávateľov, požiadavky na kybernetickú bezpečnosť subdodávateľov v súlade s požiadavkami na kybernetickú bezpečnosť uvedenými v písmene a);

h) povinnosti dodávateľov a poskytovateľov služieb pri ukončení zmluvy, ako sú získanie a likvidácia informácií, ktoré dodávatelia a poskytovatelia služieb získali pri výkone svojich úloh.

5.1.5. Príslušné subjekty zohľadnia prvky uvedené v bodoch 5.1.2 a 5.1.3 v rámci procesu výberu nových dodávateľov a poskytovateľov služieb, ako aj v rámci procesu obstarávania uvedeného v bode 6.1.

5.1.6. Príslušné subjekty preskúmavajú zásady bezpečnosti dodávateľského reťazca a monitorujú zmeny postupov dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti, hodnotia tieto zmeny a v prípade potreby na ich základe konajú, a to v plánovaných intervaloch a v prípade výskytu významných zmien operácií alebo rizík alebo významných incidentov, ktoré súvisia s poskytovaním služieb IKT alebo ktoré majú vplyv na bezpečnosť produktov IKT od dodávateľov a poskytovateľov služieb.

5.1.7. Príslušné subjekty na účely bodu 5.1.6:

a) pravidelne monitorujú správy o vykonávaní dohôd o úrovni poskytovaných služieb, v náležitých prípadoch;

b) preskúmavajú incidenty súvisiace s produktmi a službami IKT od dodávateľov a poskytovateľov služieb;

c) posudzujú potrebu neplánovaných preskúmaní a zistenia zrozumiteľným spôsobom zaznamenajú;

d) analyzujú riziká, ktoré predstavujú zmeny súvisiace s produktmi a službami IKT od dodávateľov a poskytovateľov služieb, a v prípade potreby včas prijmú zmierňujúce opatrenia.

5.2. *Zoznam dodávateľov a poskytovateľov služieb*

Príslušné subjekty vedú a pravidelne aktualizujú zoznam svojich priamych dodávateľov a poskytovateľov služieb, ktorý obsahuje:

a) kontaktné miesta v prípade každého priameho dodávateľa a poskytovateľa služieb;

b) zoznam produktov IKT, služieb IKT a procesov IKT, ktoré priamy dodávateľ alebo poskytovateľ služieb poskytuje príslušným subjektom.

6. **Bezpečnosť pri nadobúdaní, vývoji a údržbe sietí a informačných systémov [článok 21 ods. 2 písm. e) smernice (EÚ) 2022/2555]**

6.1. *Bezpečnosť pri nadobúdaní služieb alebo produktov IKT*

6.1.1. Na účely článku 21 ods. 2 písm. e) smernice (EÚ) 2022/2555 príslušné subjekty na základe posúdenia rizík vykonaného podľa bodu 2.1 stanovia a vykonávajú procesy na riadenie rizík vyplývajúcich z nadobúdania služieb alebo produktov IKT od dodávateľov alebo poskytovateľov služieb v súvislosti s komponentmi, ktoré sú kľúčové pre bezpečnosť sietí a informačných systémov príslušných subjektov, a to počas celého životného cyklu týchto komponentov.

6.1.2. Na účely bodu 6.1.1 procesy uvedené v bode 6.1.1 zahŕňajú:

a) požiadavky na bezpečnosť, ktoré sa majú uplatniť na nadobúdané služby alebo produkty IKT;

b) požiadavky týkajúce sa aktualizácií zabezpečenia počas celej životnosti služieb alebo produktov IKT alebo ich výmeny po uplynutí obdobia podpory;

c) informácie opisujúce hardvérové a softvérové komponenty použité v službách alebo produktoch IKT;

d) informácie opisujúce implementované funkcie kybernetickej bezpečnosti služieb alebo produktov IKT a konfiguráciu potrebnú na ich bezpečnú operáciu;

e) uistenie, že služby alebo produkty IKT spĺňajú požiadavky na bezpečnosť podľa písmena a);

f) metódy validácie toho, že poskytnuté služby IKT alebo dodané produkty IKT spĺňajú stanovené požiadavky na bezpečnosť, ako aj dokumentáciu o výsledkoch validácie.

6.1.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú procesy v plánovaných intervaloch a v prípade výskytu významných incidentov.

6.2. *Životný cyklus bezpečného vývoja*

6.2.1. Pred vývojom siete a informačného systému vrátane softvéru príslušné subjekty stanovia pravidlá bezpečného vývoja sietí a informačných systémov a uplatnia ich pri internom vývoji sietí a informačných systémov alebo pri externom obstaraní vývoja sietí a informačných systémov. Pravidlá sa vzťahujú na všetky vývojové fázy vrátane špecifikácie, návrhu, vývoja, realizácie a testovania.

6.2.2. Príslušné subjekty na účely bodu 6.2.1:

a) vykonajú analýzu požiadaviek na bezpečnosť vo fáze špecifikácie a návrhu akéhokoľvek vývojárskeho projektu alebo projektu nadobúdania, ktorý vykonávajú príslušné subjekty alebo ktorý sa vykonáva v ich mene;

b) pri každej činnosti vývoja informačných systémov uplatnia zásady navrhovania bezpečných systémov a zásady bezpečného kódovania softvéru, ako sú podpora kybernetickej bezpečnosti už od návrhu a architektúry nulovej dôvery;

c) stanovia požiadavky na bezpečnosť týkajúce sa vývojových prostredí;

d) stanovia a vykonávajú procesy testovania bezpečnosti vo vývojovom životnom cykle;

e) primerane vyberú, chránia a spravujú údaje o testovaní bezpečnosti;

f) sanitizujú a anonymizujú testovacie údaje podľa posúdenia rizík vykonaného podľa bodu 2.1.

6.2.3. V prípade externe obstarávaného vývoja sietí a informačných systémov príslušné subjekty uplatňujú aj zásady a postupy uvedené v bodoch 5 a 6.1.

6.2.4. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú pravidlá bezpečného vývoja v plánovaných intervaloch.

6.3. *Správa konfigurácie*

6.3.1. Príslušné subjekty prijmú vhodné opatrenia na vytvorenie, zaznamenanie, vykonanie a monitorovanie konfigurácií vrátane bezpečnostných konfigurácií hardvéru, softvéru, služieb a sietí.

6.3.2. Príslušné subjekty na účely bodu 6.3.1:

a) stanovia a zaistia bezpečnosť v rámci konfigurácií svojho hardvéru, softvéru, služieb a sietí;

b) stanovia a zavedú procesy a nástroje na presadzovanie stanovených bezpečných konfigurácií hardvéru, softvéru, služieb a sietí v prípade nových inštalovaných systémov, ako aj v prípade systémov v prevádzke počas ich životnosti.

6.3.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú konfigurácie v plánovaných intervaloch alebo v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

6.4. *Riadenie zmien, opravy a údržba*

6.4.1. Príslušné subjekty uplatňujú postupy riadenia zmien na kontrolu zmien sietí a informačných systémov. V náležitých prípadoch sú postupy v súlade so všeobecnými zásadami príslušných subjektov týkajúcimi sa riadenia zmien.

6.4.2. Postupy uvedené v bode 6.4.1 sa uplatňujú na vydania, úpravy a núdzové zmeny akéhokoľvek softvéru a hardvéru v prevádzke a na zmeny konfigurácie. Postupmi sa zabezpečí, že tieto zmeny sa pred vykonaním zaznamenajú a na základe posúdenia rizík vykonaného podľa bodu 2.1 sa otestujú a posúdia z hľadiska potenciálneho vplyvu.

6.4.3. V prípade, že z dôvodu núdzovej situácie nebolo možné dodržať riadne postupy riadenia zmien, príslušné subjekty zaznamenajú výsledok zmeny a vysvetlenie, prečo riadne postupy nebolo možné dodržať.

6.4.4. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú postupy v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

6.5. *Testovanie bezpečnosti*

6.5.1. Príslušné subjekty stanovia, vykonajú a uplatňujú zásady a postupy testovania bezpečnosti.

6.5.2. Príslušné subjekty:

a) na základe posúdenia rizík vykonaného podľa bodu 2.1 určia potrebu, rozsah, frekvenciu a typ testov bezpečnosti;

b) vykonávajú testy bezpečnosti podľa zdokumentovanej metodiky testovania, v rámci ktorých sa testujú komponenty určené v analýze rizík ako dôležité pre bezpečnú prevádzku;

c) zaznamenajú typ, rozsah, čas a výsledky testov vrátane posúdenia kritickosti a zmierňujúcich opatrení pri každom zistení;

d) v prípade kritických zistení uplatňujú zmierňujúce opatrenia.

6.5.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú svoje zásady testovania bezpečnosti v plánovaných intervaloch.

6.6. *Riadenie bezpečnostných záplat*

6.6.1. Príslušné subjekty presne stanovia a uplatňujú postupy, ktoré sú v súlade s postupmi riadenia zmien uvedenými v bode 6.4.1, ako aj s postupmi riadenia zraniteľnosti, riadenia rizík a inými relevantnými postupmi, s cieľom zabezpečiť, že:

a) bezpečnostné záplaty sa uplatnia v primeranej lehote po sprístupnení;

b) bezpečnostné záplaty sa testujú pred uplatnením v produkčných systémoch;

c) bezpečnostné záplaty pochádzajú z dôveryhodných zdrojov a kontroluje sa ich integrita;

d) v prípadoch, keď bezpečnostná záplata nie je k dispozícii alebo sa podľa bodu 6.6.2 neuplatňuje, vykonajú sa dodatočné opatrenia a akceptujú sa zvyškové IKT riziká.

6.6.2. Odchylne od bodu 6.6.1 písm. a) sa príslušné subjekty môžu rozhodnúť, že neuplatnia bezpečnostné záplaty v prípade, keď nevýhody uplatnenia bezpečnostných záplat prevyšujú prínosy z hľadiska kybernetickej bezpečnosti. Príslušné subjekty riadne zaznamenajú a podložia dôvody každého takéhoto rozhodnutia.

6.7. *Bezpečnosť siete*

6.7.1. Príslušné subjekty prijmú vhodné opatrenia na ochranu svojich sietí a informačných systémov pred kybernetickými hrozbami.

6.7.2. Príslušné subjekty na účely bodu 6.7.1:

a) zrozumiteľným spôsobom zaznamenajú aktuálnu podobu architektúry siete;

b) určia a uplatnia kontroly na ochranu interných sieťových domén príslušných subjektov pred neoprávneným prístupom;

c) konfigurujú kontroly na zabránenie prístupom a sieťovej komunikácii, ktoré nie sú potrebné v rámci prevádzky príslušných subjektov;

d) určia a uplatnia kontroly vzdialeného prístupu k sieťam a informačným systémom vrátane prístupu poskytovateľov služieb;

e) nesmú používať systémy používané na správu vykonávania zásad bezpečnosti na iné účely;

f) výslovne zakážu alebo deaktivujú nepotrebné spojenia a služby;

g) v prípade potreby povolia prístup k sieťam a informačným systémom príslušných subjektov výlučne prostredníctvom zariadení autorizovaných týmito subjektmi;

h) umožnia spojenia poskytovateľov služieb len na základe žiadosti o autorizáciu a len na stanovený čas, ako je trvanie činnosti údržby;

i) vytvoria prepojenie medzi odlišnými systémami len prostredníctvom dôveryhodných kanálov, ktoré sú od seba oddelené, s použitím logického, kryptografického alebo fyzického oddelenia od iných komunikačných kanálov a poskytnú zaručenú identifikáciu svojich koncových bodov a ochranu údajov o kanáli pred úpravami alebo zverejnením;

j) prijmú plán vykonávania úplného prechodu na najnovšiu generáciu komunikačných protokolov sieťovej vrstvy bezpečným, primeraným a postupným spôsobom a stanovia opatrenia na urýchlenie tohto prechodu;

k) prijmú plán vykonávania na zavedenie medzinárodne schválených a interoperabilných moderných noriem e-mailovej komunikácie na bezpečnú e-mailovú komunikáciu s cieľom zmierniť zraniteľnosti spojené s e-mailovými hrozbami a stanovia opatrenia na urýchlenie tohto zavádzania;

l) uplatňujú najlepšie postupy bezpečnosti DNS a bezpečnosti smerovania internetu a hygieny smerovania prevádzky pochádzajúcej zo siete a smerujúcej do siete.

6.7.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú tieto opatrenia v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

6.8. *Segmentácia siete*

6.8.1. Príslušné subjekty segmentujú systémy na siete alebo zóny v súlade s výsledkami posúdenia rizík uvedeného v bode 2.1. Svoje systémy a siete segmentujú od systémov a sietí tretích strán.

6.8.2. Príslušné subjekty na tieto účely:

a) posudzujú funkčný, logický a fyzický vzťah, vrátane umiestnenia, medzi dôveryhodnými systémami a službami;

b) udeľujú prístup k sieti alebo zóne na základe posúdenia ich požiadaviek na bezpečnosť;

c) udržujú systémy, ktoré sú kriticky dôležité pre prevádzku príslušných subjektov alebo pre bezpečnosť, v bezpečných zónach;

d) zavedú v rámci svojich komunikačných sietí demilitarizovanú zónu s cieľom zaistiť bezpečnú komunikáciu odchádzajúcu z ich sietí alebo smerujúcu do ich sietí;

e) obmedzia prístup a komunikáciu medzi zónami a v rámci nich na prístup a komunikáciu potrebné pre prevádzku príslušných subjektov alebo pre bezpečnosť;

f) oddelia vyhradenú sieť na správu sietí a informačných systémov od prevádzkovej siete príslušných subjektov;

g) oddelia kanály na správu sietí od ostatnej sieťovej prevádzky;

h) oddelia produkčné systémy pre služby príslušných subjektov od systémov používaných pri vývoji a testovaní vrátane záloh.

6.8.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú segmentáciu siete v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

6.9. *Ochrana pred škodlivým a neautorizovaným softvérom*

6.9.1. Príslušné subjekty chránia svoje siete a informačné systémy pred škodlivým a neautorizovaným softvérom.

6.9.2. Na tento účel príslušné subjekty predovšetkým vykonávajú opatrenia na detekciu alebo prevenciu používania škodlivého alebo neautorizovaného softvéru. Príslušné subjekty v prípade potreby zabezpečia, aby ich siete a informačné systémy boli vybavené softvérom na detekciu a reakciu, pravidelne aktualizovaným v súlade s posúdením rizík vykonaným podľa bodu 2.1 a so zmluvnými dohodami s poskytovateľmi.

6.10. *Riešenie zraniteľností a zverejňovanie informácií o nich*

6.10.1. Príslušné subjekty získavajú informácie o technických zraniteľnostiach vo svojich sieťach a informačných systémoch, vyhodnocujú vystavenie sietí a informačných systémov týmto zraniteľnostiam a prijímajú vhodné opatrenia na riadenie zraniteľností.

6.10.2. Príslušné subjekty na účely bodu 6.10.1:

a) monitorujú informácie o zraniteľnostiach prostredníctvom vhodných kanálov, ako sú oznámenia jednotiek CSIRT, príslušné orgány alebo informácie poskytované dodávateľmi alebo poskytovateľmi služieb;

b) v prípade potreby v plánovaných intervaloch vykonávajú skenovanie zraniteľnosti a zaznamenávajú dôkazy o výsledkoch skenovania;

c) bez zbytočného odkladu riešia zraniteľnosti, ktoré príslušné subjekty označili ako kritické pre ich operácie;

d) zabezpečia, že ich riešenie zraniteľnosti bude zlučiteľné s ich postupmi riadenia zmien, riadenia bezpečnostných záplat, riadenia rizík a riadenia incidentov;

e) stanovia postup na zverejňovanie informácií o zraniteľnostiach v súlade s platnou vnútroštátnou politikou koordinovaného zverejňovania informácií o zraniteľnostiach.

6.10.3. V prípadoch odôvodnených možným vplyvom zraniteľnosti príslušné subjekty vytvoria a realizujú plán na zmiernenie tejto zraniteľnosti. V ostatných prípadoch príslušné subjekty zaznamenajú a podložia dôvod, pre ktorý sa v súvislosti so zraniteľnosťou nevyžaduje náprava.

6.10.4. Príslušné subjekty v plánovaných intervaloch preskúmavajú a v prípade potreby aktualizujú kanály, ktoré používajú na monitorovanie informácií o zraniteľnostiach.

7. **Zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík [článok 21 ods. 2 písm. f) smernice (EÚ) 2022/2555]**

7.1. Na účely článku 21 ods. 2 písm. f) smernice (EÚ) 2022/2555 príslušné subjekty stanovia, vykonajú a uplatňujú zásady a postupy posudzovania účinného vykonávania a udržiavania opatrení na riadenie kybernetických rizík prijatých príslušným subjektom.

7.2. V zásadách a postupoch uvedených v bode 7.1 sa zohľadnia výsledky posúdenia rizík podľa bodu 2.1 a minulé významné incidenty. Príslušné subjekty určia:

a) ktoré opatrenia na riadenie kybernetických rizík sa budú monitorovať a merať vrátane procesov a kontrol;

b) metódy na monitorovanie, meranie, analyzovanie a hodnotenie, podľa potreby, s cieľom zabezpečiť platné výsledky;

c) kedy sa musí vykonať monitorovanie a meranie;

d) kto zodpovedá za monitorovanie a meranie účinnosti opatrení na riadenie kybernetických rizík;

e) kedy sa musia analyzovať a vyhodnotiť výsledky z monitorovania a merania;

f) kto musí analyzovať a vyhodnotiť tieto výsledky.

7.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú zásady a postupy v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

8. **Základné postupy kybernetickej hygieny a odborná príprava v oblasti kybernetickej bezpečnosti [článok 21 ods. 2 písm. g) smernice (EÚ) 2022/2555]**

8.1. *Zvyšovanie informovanosti a základné postupy kybernetickej hygieny*

8.1.1. Na účely článku 21 ods. 2 písm. g) smernice (EÚ) 2022/2555 príslušné subjekty zabezpečia, aby si ich zamestnanci vrátane členov riadiacich orgánov, ako aj priami dodávatelia a poskytovatelia služieb uvedomovali riziká, boli informovaní o dôležitosti kybernetickej bezpečnosti a uplatňovali postupy kybernetickej hygieny.

8.1.2. Na účely bodu 8.1.1 príslušné subjekty poskytnú svojim zamestnancom vrátane členov riadiacich orgánov, ako aj priamym dodávateľom a poskytovateľom služieb v prípade potreby v súlade s bodom 5.1.4 program na zvyšovanie informovanosti, ktorý:

a) bude naplánovaný v priebehu času tak, aby sa činnosti opakovali a zahŕňali nových zamestnancov;

b) bude stanovený v súlade so zásadami sieťovej a informačnej bezpečnosti, s tematickými zásadami a príslušnými postupmi v oblasti sieťovej a informačnej bezpečnosti;

c) bude zahŕňať relevantné kybernetické hrozby, zavedené opatrenia na riadenie kybernetických rizík, kontaktné miesta a zdroje doplňujúcich informácií a odporúčaní v otázkach kybernetickej bezpečnosti, ako aj postupy kybernetickej hygieny pre používateľov.

8.1.3. Program na zvyšovanie informovanosti sa v prípade potreby otestuje z hľadiska účinnosti. Program na zvyšovanie informovanosti sa aktualizuje a poskytuje v plánovaných intervaloch, pričom sa zohľadnia zmeny postupov kybernetickej hygieny a aktuálna panoráma hrozieb i riziká pre príslušné subjekty.

8.2. *Odborná príprava v oblasti kybernetickej bezpečnosti*

8.2.1. Príslušné subjekty určia zamestnancov, ktorých úlohy si vyžadujú súbor zručností a odbornosť v oblasti bezpečnosti, a zabezpečia, aby absolvovali pravidelnú odbornú prípravu v oblasti bezpečnosti sietí a informačných systémov.

8.2.2. Príslušné subjekty stanovia, vykonajú a uplatňujú program odbornej prípravy v súlade so zásadami sieťovej a informačnej bezpečnosti, s tematickými zásadami a inými príslušnými postupmi v oblasti sieťovej a informačnej bezpečnosti, pričom v ňom stanovia potreby v oblasti odbornej prípravy pre určité úlohy a pracovné pozície na základe kritérií.

8.2.3. Odborná príprava uvedená v bode 8.2.1 je relevantná pre pracovnú úlohu zamestnanca a účinnosť tejto prípravy sa posudzuje. Odborná príprava zohľadňuje zavedené bezpečnostné opatrenia a týka sa týchto oblastí:

a) pokyny týkajúce sa bezpečnej konfigurácie a prevádzky sietí a informačných systémov vrátane mobilných zariadení;

b) informovanie o známych kybernetických hrozbách;

c) nácvik správania v prípade výskytu udalostí súvisiacich s bezpečnosťou.

8.2.4. Príslušné subjekty uplatňujú odbornú prípravu v prípade zamestnancov, ktorí sa presúvajú na nové pozície alebo úlohy, ktoré si vyžadujú súbor zručností a odbornosť týkajúce sa bezpečnosti.

8.2.5. Program sa pravidelne aktualizuje a realizuje, pričom sa zohľadňujú platné zásady a pravidlá, priradené úlohy a povinnosti, ako aj známe kybernetické hrozby a technologický vývoj.

9. **Kryptografia [článok 21 ods. 2 písm. h) smernice (EÚ) 2022/2555]**

9.1. Na účely článku 21 ods. 2 písm. h) smernice (EÚ) 2022/2555 príslušné subjekty stanovia, vykonajú a uplatňujú zásady a postupy týkajúce sa kryptografie s cieľom zabezpečiť dostatočné a účinné používanie kryptografie na ochranu dôvernosti, pravosti a integrity údajov v súlade s klasifikáciou aktív príslušných subjektov a s výsledkami posúdenia rizík vykonaného podľa bodu 2.1.

9.2. V zásadách a postupoch uvedených v bode 9.1 sa stanovia:

a) typ, sila a kvalita kryptografických opatrení požadovaných na ochranu aktív príslušných subjektov vrátane údajov v pokoji a pri prenose v súlade s klasifikáciou aktív príslušných subjektov;

b) na základe písmena a) protokoly alebo rady protokolov, ktoré sa majú prijať, ako aj kryptografické algoritmy, sila šifrovania, kryptografické riešenia a postupy používania kryptografie, ktoré sa majú schváliť a ktorých používanie v príslušných subjektoch sa vyžaduje, v prípade potreby s dodržaním prístupu kryptografickej pružnosti;

c) prístup príslušných subjektov k správe kľúčov, v prípade potreby vrátane metód týkajúcich sa:

i) vytvorenia jednotlivých kľúčov pre kryptografické systémy a aplikácie;

ii) vydávania a získavania certifikátov verejného kľúča;

iii) distribúcie kľúčov plánovaným subjektom vrátane spôsobu, ako aktivovať kľúče po prijatí;

iv) uchovávania kľúčov vrátane spôsobu, ako oprávnení používatelia získavajú prístup ku kľúčom;

v) zmeny alebo aktualizácie kľúčov vrátane pravidiel upravujúcich čas a spôsob zmeny kľúčov;

vi) zaobchádzania so zneužitými kľúčmi;

vii) zrušenia kľúčov vrátane spôsobu odobratia alebo deaktivácie kľúča;

viii) obnovy stratených alebo poškodených kľúčov;

ix) zálohovania alebo archivácie kľúčov;

x) zničenia kľúčov;

xi) logovania a auditu činností súvisiacich so správou kľúčov;

xii) stanovenia dátumov aktivácie a deaktivácie kľúčov s cieľom zabezpečiť, že kľúče možno používať len stanovený čas v súlade s pravidlami danej organizácie upravujúcimi správu kľúčov.

9.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú svoje zásady a postupy v plánovaných intervaloch, pričom zohľadňujú najnovší vývoj v oblasti kryptografie.

10. **Bezpečnosť ľudských zdrojov [článok 21 ods. 2 písm. i) smernice (EÚ) 2022/2555]**

10.1. *Bezpečnosť ľudských zdrojov*

10.1.1. Na účely článku 21 ods. 2 písm. i) smernice (EÚ) 2022/2555 príslušné subjekty zabezpečia, aby ich zamestnanci a priami dodávatelia a poskytovatelia služieb vždy, keď je to potrebné, chápali svoje povinnosti v oblasti bezpečnosti a aby sa zaviazali ich plniť s ohľadom na ponúkané služby a pracovné miesto a v súlade so zásadami príslušných subjektov týkajúcimi sa bezpečnosti sietí a informačných systémov.

10.1.2. Požiadavka uvedená v bode 10.1.1 zahŕňa:

a) mechanizmy, ktorými sa zabezpečí, aby všetci zamestnanci, priami dodávatelia a poskytovatelia služieb vždy, keď je to potrebné, chápali a dodržiavali štandardné postupy kybernetickej hygieny, ktoré príslušné subjekty uplatňujú podľa bodu 8.1;

b) mechanizmy, ktorými sa zabezpečí, aby si všetci používatelia so správcovským alebo s privilegovaným prístupom boli vedomí svojich úloh, povinností a právomocí a konali v súlade s nimi;

c) mechanizmy, ktorými sa zabezpečí, aby členovia riadiacich orgánov chápali svoje úlohy, povinnosti a právomoci v súvislosti s bezpečnosťou sietí a informačných systémov a konali v súlade s nimi;

d) mechanizmy prijímania zamestnancov kvalifikovaných na príslušné úlohy, ako sú overovanie odporúčaní, preverovacie postupy, overovanie certifikácií alebo písomné skúšky.

10.1.3. Príslušné subjekty v plánovaných intervaloch a aspoň raz za rok preskúmavajú priradenie zamestnancov na konkrétne úlohy, ako sa uvádza v bode 1.2, ako aj svoju potrebu ľudských zdrojov v tejto súvislosti. V prípade potreby priradenie na úlohy aktualizujú.

10.2. *Overenie spoľahlivosti*

10.2.1. Pokiaľ je to možné, príslušné subjekty zabezpečia overenie spoľahlivosti svojich zamestnancov a v náležitých prípadoch priamych dodávateľov a poskytovateľov služieb v súlade s bodom 5.1.4, ak je to potrebné pre ich úlohu, povinnosti a právomoci.

10.2.2. Príslušné subjekty na účely bodu 10.2.1:

a) zavedú kritériá stanovujúce, ktoré úlohy, povinnosti a právomoci môžu vykonávať len osoby, ktorých spoľahlivosť bola overená;

b) zabezpečia, že overenie spoľahlivosti týchto osôb podľa bodu 10.2.1 sa vykoná pred tým, než začnú vykonávať tieto úlohy, povinnosti a právomoci, pričom sa pri ňom zohľadnia platné právne predpisy, nariadenia a etické zásady primerané obchodným požiadavkám, klasifikácii aktív podľa bodu 12.1 a sieťam a informačným systémom, ktoré sa sprístupňujú, ako aj vnímaným rizikám.

10.2.3. Príslušné subjekty v plánovaných intervaloch preskúmavajú a v prípade potreby aktualizujú tieto zásady a podľa potreby ich aktualizujú.

10.3. *Postupy súvisiace s ukončením alebo zmenou zamestnania*

10.3.1. Príslušné subjekty zabezpečia, aby sa zmluvne vymedzili a presadzovali povinnosti a úlohy v oblasti bezpečnosti sietí a informačných systémov, ktoré zostávajú v platnosti po ukončení alebo zmene pracovného pomeru zamestnancov.

10.3.2. Na účely bodu 10.3.1 príslušné subjekty do pracovných podmienok, zmluvy alebo dohody jednotlivca zahrnú povinnosti a úlohy, ktoré zostávajú v platnosti aj po ukončení pracovného pomeru alebo pracovnej zmluvy, ako sú doložky o dôvernosti.

10.4. *Disciplinárny postup*

10.4.1. Príslušné subjekty stanovia, oznámia a udržiavajú disciplinárny postup na riešenie porušení zásad bezpečnosti sietí a informačných systémov. V rámci postupu sa zohľadňujú príslušné právne, zákonné, zmluvné a obchodné požiadavky.

10.4.2. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú disciplinárny postup v plánovaných intervaloch a v prípade, že je to nevyhnutné z dôvodu právnych zmien alebo významných zmien operácií alebo rizík.

11. **Kontrola prístupu [článok 21 ods. 2 písm. i) a j) smernice (EÚ) 2022/2555]**

11.1. *Zásady kontroly prístupu*

11.1.1. Na účely článku 21 ods. 2 písm. i) smernice (EÚ) 2022/2555 príslušné subjekty stanovia, zaznamenajú a vykonajú zásady kontroly logického a fyzického prístupu týkajúce sa prístupu do ich sietí a informačných systémov na základe obchodných požiadaviek, ako aj na základe požiadaviek na bezpečnosť sietí a informačných systémov.

11.1.2. V zásadách uvedených v bode 11.1.1:

a) sa rieši prístup zo strany osôb vrátane zamestnancov, návštevníkov a externých subjektov, ako sú dodávatelia a poskytovatelia služieb;

b) sa rieši prístup sietí a informačných systémov;

c) sa zabezpečuje, že prístup sa udelí len používateľom, ktorí sa dostatočne autentifikovali.

11.1.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú tieto zásady v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

11.2. *Správa prístupových práv*

11.2.1. Príslušné subjekty zabezpečujú, upravujú, odstraňujú a zaznamenávajú prístupové práva do sietí a informačných systémov v súlade so zásadami kontroly prístupu uvedenými v bode 11.1.

11.2.2. Príslušné subjekty:

a) prideľujú a odoberajú prístupové práva na základe zásad potreby poznať, minimálneho privilégia a oddelenia úloh;

b) zabezpečia, aby sa prístupové práva pri ukončení alebo zmene pracovného pomeru zodpovedajúcim spôsobom upravili;

c) zabezpečia, aby oprávnenie na prístup do sietí a informačných systémov udeľovali príslušné osoby;

d) zabezpečia, aby sa prístupovými právami vhodne riešil prístup tretích strán, ako sú návštevníci, dodávatelia a poskytovatelia služieb, a to najmä obmedzením rozsahu a skrátením trvania prístupových práv;

e) vedú zoznam udelených prístupových práv;

f) uplatňujú logovanie na správu prístupových práv.

11.2.3. Príslušné subjekty v plánovaných intervaloch preskúmavajú prístupové práva a upravujú ich na základe organizačných zmien. Príslušné subjekty zaznamenajú výsledky preskúmania vrátane nevyhnutných zmien prístupových práv.

11.3. *Privilegované účty a účty na správu systému*

11.3.1. Príslušné subjekty ako súčasť zásad kontroly prístupu uvedených v bode 11.1 udržiavajú zásady riadenia privilegovaných účtov a účtov na správu systému.

11.3.2. Zásadami uvedenými v bode 11.3.1 sa:

a) stanovujú postupy silnej identifikácie, autentifikácie, napríklad viacstupňová autentifikácia, a autorizácie pre privilegované účty a účty na správu systému;

b) vytvárajú osobitné účty, ktoré sa majú používať výlučne na operácie správy systému, ako sú inštalovanie, konfigurovanie, správa alebo údržba;

c) v čo najvyššej miere individualizujú a obmedzujú privilégia na správu systému;

d) stanovuje, že účty na správu systému sa používajú len na pripojenie k systémom na správu systému.

11.3.3. Príslušné subjekty v plánovaných intervaloch preskúmavajú prístupové práva privilegovaných účtov a účtov na správu systému a upravujú ich na základe organizačných zmien a zároveň zaznamenávajú výsledky preskúmania vrátane nevyhnutných zmien prístupových práv.

11.4. *Správcovské systémy*

11.4.1. Príslušné subjekty obmedzia a kontrolujú používanie systémov na správu systému v súlade so zásadami kontroly prístupu uvedenými v bode 11.1.

11.4.2. Príslušné subjekty na tieto účely:

a) používajú systémy na správu systému len na účely správy systému, a nie na iné operácie;

b) logicky oddelia takéto systémy od aplikačného softvéru, ktorý sa nepoužíva na účely správy systému;

c) chránia prístup do systémov na správu systému prostredníctvom autentifikácie a šifrovania.

11.5. *Identifikácia*

11.5.1. Príslušné subjekty spravujú celý životný cyklus identít sietí a informačných systémov a ich používateľov.

11.5.2. Príslušné subjekty na tieto účely:

a) vytvárajú jedinečné identity sietí a informačných systémov a ich používateľov;

b) prepájajú identitu používateľov s jedinou osobou;

c) zabezpečujú dohľad nad identitami sietí a informačných systémov;

d) uplatňujú logovanie na správu identít.

11.5.3. Príslušné subjekty povolia identity priradené k viacerým osobám, ako sú spoločné identity, len keď sú nevyhnutné z obchodných alebo prevádzkových dôvodov a podliehajú procesu výslovného súhlasu a zaznamenávaniu. Príslušné subjekty zohľadnia identity priradené viacerým osobám v rámci riadenia kybernetických rizík uvedenom v bode 2.1.

11.5.4. Príslušné subjekty pravidelne preskúmavajú identity sietí a informačných systémov a ich používateľov, a ak už nie sú potrebné, bezodkladne ich deaktivujú.

11.6. *Autentifikácia*

11.6.1. Príslušné subjekty zavedú postupy a technológie zabezpečenej autentifikácie založené na obmedzení prístupu a zásadách kontroly prístupu.

11.6.2. Príslušné subjekty na tieto účely:

a) zabezpečia, aby sila autentifikácie bola primeraná klasifikácii aktíva, ktoré sa sprístupňuje;

b) kontrolujú prideľovanie tajných autentifikačných informácií používateľom a ich riadenie prostredníctvom procesu, ktorým sa zabezpečuje dôvernosť informácií, vrátane poučenia zamestnancov o vhodnom zaobchádzaní s autentifikačnými informáciami;

c) vyžadujú, aby sa autentifikačné prihlasovacie údaje zmenili na začiatku, vo vopred stanovených intervaloch a pri podozrení, že boli ohrozené;

d) vyžadujú obnovenie autentifikačných prihlasovacích údajov a zablokovanie prístupu používateľov po určitom počte neúspešných pokusov o prihlásenie;

e) ukončia neaktívne relácie po stanovenom období nečinnosti a

f) vyžadujú samostatné prihlasovacie údaje na prístup do privilegovaných účtov alebo správcovských účtov.

11.6.3. Pokiaľ je to možné, príslušné subjekty používajú najmodernejšie metódy autentifikácie v súlade so súvisiacim vyhodnoteným rizikom a s klasifikáciou aktíva, ktoré sa sprístupňuje, a jedinečné autentifikačné informácie.

11.6.4. Príslušné subjekty v plánovaných intervaloch preskúmavajú postupy a technológie autentifikácie.

11.7. *Viacstupňová autentifikácia*

11.7.1. Príslušné subjekty zabezpečia, že sa používatelia budú v prípade potreby overovať prostredníctvom viacerých stupňov autentifikácie alebo prostredníctvom mechanizmov kontinuálnej autentifikácie na účely prístupu do sietí a informačných systémov príslušných subjektov v súlade s klasifikáciou aktíva, ktoré sa sprístupňuje.

11.7.2. Príslušné subjekty zabezpečia, aby sila autentifikácie bola primeraná klasifikácii aktíva, ktoré sa sprístupňuje.

12. **Správa aktív [článok 21 ods. 2 písm. i) smernice (EÚ) 2022/2555]**

12.1. *Klasifikácia aktív*

12.1.1. Na účely článku 21 ods. 2 písm. i) smernice (EÚ) 2022/2555 príslušné subjekty stanovia úrovne klasifikácie všetkých aktív vrátane informácií v rámci ich sietí a informačných systémov podľa požadovanej úrovne ochrany.

12.1.2. Príslušné subjekty na účely bodu 12.1.1:

a) stanovia systém úrovní klasifikácie týkajúci sa aktív;

b) zaradia všetky aktíva do niektorej z úrovní klasifikácie na základe požiadaviek na dôvernosť, integritu, pravosť a dostupnosť s cieľom určiť požadovanú ochranu podľa ich citlivosti, kritickosti, rizika a obchodnej hodnoty;

c) zosúladia požiadavky na dostupnosť aktív s cieľmi poskytovania služieb a obnovy stanovenými v ich pláne na zabezpečenie kontinuity činností a pláne obnovy systému po havárii.

12.1.3. Príslušné subjekty vykonávajú pravidelné preskúmania úrovní klasifikácie aktív a v prípade potreby ich aktualizujú.

12.2. *Zaobchádzanie s aktívami*

12.2.1. Príslušné subjekty stanovia, vykonajú a uplatňujú zásady riadneho zaobchádzania s aktívami vrátane informácií v súlade so svojimi zásadami sieťovej a informačnej bezpečnosti a tieto zásady riadneho zaobchádzania s aktívami oznámia každej osobe, ktorá aktíva používa alebo s nimi zaobchádza.

12.2.2. V zásadách:

a) je zahrnutý celý životný cyklus aktív vrátane ich nadobúdania, používania, uchovávania, prepravy a likvidácie;

b) stanovujú sa pravidlá o bezpečnom používaní, bezpečnom uchovávaní, bezpečnej preprave a nenávratnom vymazaní a zničení aktív;

c) stanovuje sa, že prenos sa uskutoční zabezpečeným spôsobom v súlade s typom aktíva, ktoré sa prenáša.

12.2.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú tieto zásady v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

12.3. *Zásady týkajúce sa vymeniteľných médií*

12.3.1. Príslušné subjekty stanovia, vykonajú a uplatňujú zásady správy vymeniteľných pamäťových médií a oznámia ich svojim zamestnancom a tretím stranám, ktoré zaobchádzajú s vymeniteľnými pamäťovými médiami v priestoroch príslušných subjektov a na iných miestach, kde sa vymeniteľné médiá pripájajú k sieťam a informačným systémom príslušných subjektov.

12.3.2. V zásadách sa:

a) stanovuje technický zákaz pripojenia vymeniteľných médií, ak neexistuje organizačný dôvod na ich použitie;

b) stanovuje vypnutie automatického spúšťania z týchto médií a kontrola médií z hľadiska prítomnosti škodlivého kódu pred ich použitím v systémoch príslušných subjektov;

c) stanovujú opatrenia na kontrolu a ochranu prenosných pamäťových zariadení obsahujúcich údaje počas prenosu a uchovávania;

d) v prípade potreby stanovujú opatrenia na použitie kryptografických techník na ochranu údajov na vymeniteľných pamäťových médiách.

12.3.3. Príslušné subjekty preskúmavajú a v prípade potreby aktualizujú tieto zásady v plánovaných intervaloch a v prípade výskytu významných incidentov alebo významných zmien operácií alebo rizík.

12.4. *Inventár aktív*

12.4.1. Príslušné subjekty vypracujú a vedú úplný, presný, aktuálny a konzistentný inventár svojich aktív. Záznamy o zmenách položiek v inventári vedú tak, aby ich bolo možné vysledovať.

12.4.2. Podrobnosť inventára aktív je na úrovni primeranej potrebám príslušných subjektov. Inventár obsahuje:

a) zoznam operácií a služieb a ich opis;

b) zoznam sietí a informačných systémov a ďalších súvisiacich aktív podporujúcich operácie a služby príslušných subjektov.

12.4.3. Príslušné subjekty pravidelne preskúmavajú a aktualizujú inventár a svoje aktíva a zaznamenávajú históriu zmien.

12.5. *Uloženie, vrátenie alebo vymazanie aktív pri ukončení pracovného pomeru*

Príslušné subjekty stanovia, vykonajú a uplatňujú postupy, ktorými sa pri ukončení pracovného pomeru zabezpečí uloženie, vrátenie alebo vymazanie ich aktív, ktoré majú v úschove zamestnanci, a uloženie, vrátenie a vymazanie týchto aktív zaznamenajú. Ak aktíva nie je možné uložiť, vrátiť ani vymazať, príslušné subjekty zabezpečia, že aktíva už nebudú mať prístup do sietí a informačných systémov príslušných subjektov, v súlade s bodom 12.2.2.

13. **Environmentálna a fyzická bezpečnosť [článok 21 ods. 2 písm. c), e) a i) smernice (EÚ) 2022/2555]**

13.1. *Podporné verejné služby*

13.1.1. Na účely článku 21 ods. 2 písm. c) smernice (EÚ) 2022/2555 príslušné subjekty predchádzajú strate, poškodeniu alebo ohrozeniu sietí a informačných systémov alebo prerušeniu ich prevádzky z dôvodu zlyhania a narušenia podporných verejných služieb.

13.1.2. Príslušné subjekty na tento účel v prípade potreby:

a) ochraňujú zariadenia pred výpadkom elektrickej energie a inými narušeniami spôsobenými zlyhaniami v podporných verejných službách, ako sú elektrická energia, telekomunikácie, zásobovanie vodou, plynom, odpadová voda, vetranie a klimatizácia;

b) zvažujú použitie redundantných kapacít vo verejných službách;

c) chránia verejné služby v oblasti elektrickej energie a telekomunikácií, ktorými sa prenášajú údaje alebo zásobujú siete a informačné systémy, pred zachytávaním údajov a poškodením;

d) monitorujú verejné služby uvedené v písmene c) a príslušnému internému alebo externému personálu oznamujú udalosti prekračujúce minimálne a maximálne kontrolné prahové hodnoty uvedené v bode 13.2.2 písm. b), ktoré ovplyvňujú verejné služby;

e) uzatvárajú zmluvy o núdzových dodávkach s príslušnými službami, napríklad pokiaľ ide o palivo pre núdzový zdroj napájania;

f) zabezpečia nepretržitú účinnosť, monitorujú, udržiavajú a testujú dodávky pre siete a informačné systémy potrebné na prevádzku ponúkaných služieb, najmä pokiaľ ide o elektrickú energiu, kontrolu teploty a vlhkosti, telekomunikácie a internetové pripojenie.

13.1.3. Príslušné subjekty testujú, preskúmavajú a v prípade potreby aktualizujú ochranné opatrenia v pravidelných intervaloch alebo po významných incidentoch či po významných zmenách operácií alebo rizík.

13.2. *Ochrana proti fyzickým a environmentálnym hrozbám*

13.2.1. Na účely článku 21 ods. 2 písm. e) smernice (EÚ) 2022/2555 príslušné subjekty predchádzajú následkom udalostí vyplývajúcim z fyzických a environmentálnych hrozieb, ako sú prírodné katastrofy a iné úmyselné alebo neúmyselné hrozby, alebo tieto následky zmierňujú, a to na základe výsledkov posúdenia rizík vykonaného podľa bodu 2.1.

13.2.2. Príslušné subjekty na tento účel v prípade potreby:

a) navrhnú a vykonajú opatrenia na ochranu proti fyzickým a environmentálnym hrozbám;

b) určia minimálne a maximálne kontrolné prahové hodnoty týkajúce sa fyzických a environmentálnych hrozieb;

c) monitorujú environmentálne parametre a príslušnému internému alebo externému personálu oznamujú udalosti prekračujúce minimálne a maximálne kontrolné prahové hodnoty uvedené v písmene b).

13.2.3. Príslušné subjekty testujú, preskúmavajú a v prípade potreby aktualizujú opatrenia na ochranu proti fyzickým a environmentálnym hrozbám v pravidelných intervaloch alebo po významných incidentoch či po významných zmenách operácií alebo rizík.

13.3. *Perimeter a kontrola fyzického prístupu*

13.3.1. Na účely článku 21 ods. 2 písm. i) smernice (EÚ) 2022/2555 príslušné subjekty predchádzajú neoprávnenému fyzickému prístupu ku svojim sieťam a informačným systémom, ich poškodeniu alebo zásahom do nich a monitorujú takýto prístup, poškodenie a zasahovanie.

13.3.2. Príslušné subjekty na tieto účely:

a) na základe posúdenia rizík vykonaného podľa bodu 2.1 stanovia a používajú bezpečnostné perimetre na ochranu oblastí, v ktorých sa nachádzajú siete a informačné systémy a iné súvisiace aktíva;

b) ochraňujú oblasti uvedené v písmene a) primeranými kontrolami vstupu a prostredníctvom prístupových bodov;

c) navrhnú a zavedú opatrenia fyzickej bezpečnosti pre kancelárie, miestnosti a zariadenia;

d) nepretržite monitorujú svoje priestory s cieľom zabrániť neoprávnenému fyzickému prístupu.

13.3.3. Príslušné subjekty testujú, preskúmavajú a v prípade potreby aktualizujú opatrenia kontroly fyzického prístupu v pravidelných intervaloch alebo po významných incidentoch či po významných zmenách operácií alebo rizík.