2024/2690

18.10.2024

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2024/2690

ze dne 17. října 2024,

kterým se stanoví pravidla pro uplatňování směrnice (EU) 2022/2555, pokud jde o technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik a bližší upřesnění případů, v nichž se incident považuje za významný, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) ([1]), a zejména čl. 21 odst. 5 první pododstavec a čl. 23 odst. 11 druhý pododstavec této směrnice,

vzhledem k těmto důvodům:

(1) Pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru, na které se vztahuje článek 3 směrnice (EU) 2022/2555 (dále jen „příslušné subjekty“), cílem tohoto nařízení je stanovit technické a metodické požadavky na opatření uvedená v čl. 21 odst. 2 směrnice (EU) 2022/2555 a dále upřesnit případy, v nichž se incident považuje za významný, jak je uvedeno v čl. 23 odst. 3 směrnice (EU) 2022/2555.

(2) S ohledem na přeshraniční povahu jejich činností a v zájmu zajištění soudržného rámce pro poskytovatele služeb vytvářejících důvěru by toto nařízení mělo s ohledem na poskytovatele služeb vytvářejících důvěru kromě stanovení technických a metodických požadavků na opatření k řízení kybernetických bezpečnostních rizik dále upřesnit případy, v nichž se incident považuje za významný.

(3) V návaznosti na čl. 21 odst. 5 třetí pododstavec směrnice (EU) 2022/2555 vycházejí technické a metodické požadavky na opatření pro řízení kybernetických bezpečnostních rizik stanovené v příloze tohoto nařízení z evropských a mezinárodních norem, jako jsou ISO/IEC 27001, ISO/IEC 27002 a ETSI EN 319401, a technických specifikací, jako je CEN/TS 18026:2024, které se týkají bezpečnosti sítí a informačních systémů.

(4) Pokud jde o provádění a uplatňování technických a metodických požadavků na opatření k řízení kybernetických bezpečnostních rizik stanovených v příloze tohoto nařízení, v souladu se zásadou proporcionality by se měla při plnění technických a metodických požadavků na opatření k řízení kybernetických bezpečnostních rizik stanovených v příloze tohoto nařízení náležitě zohlednit rozdílná expozice příslušných subjektů rizikům, jako je kritičnost příslušného subjektu, rizika, jimž je vystaven, velikost příslušného subjektu a pravděpodobnost výskytu incidentů a jejich závažnost, včetně jejich společenského a ekonomického dopadu.

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

(5) V souladu se zásadou proporcionality by měly mít příslušné subjekty v případech, kdy nemohou z důvodu své velikosti splnit některé technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik, možnost přijmout jiná kompenzační opatření, která jsou vhodná k dosažení účelu těchto požadavků. Například subjekty velmi malé velikosti mohou mít při určování rolí, odpovědností a pravomocí v oblasti bezpečnosti sítí a informačních systémů v rámci příslušného subjektu potíže s oddělením kolidujících povinností a protichůdných oblastí odpovědnosti. Tyto subjekty by měly mít možnost zvážit kompenzační opatření, jako je cílený dohled ze strany vedení subjektu nebo zvýšené monitorování a vedení protokolů.

(6) Příslušné subjekty by měly požadavky stanovené v příloze tohoto nařízení uplatňovat tam, kde je to vhodné, použitelné nebo proveditelné. Pokud se příslušný subjekt domnívá, že není vhodné, použitelné nebo proveditelné, aby uplatnil určité technické a metodické požadavky stanovené v příloze tohoto nařízení, měl by za tímto účelem srozumitelně zdokumentovat své odůvodnění. Příslušné vnitrostátní orgány mohou při výkonu dohledu zohlednit přiměřenou dobu, kterou příslušné subjekty potřebují k provedení technických a metodických požadavků opatření k řízení kybernetických bezpečnostních rizik.

(7) Agentura ENISA nebo příslušné vnitrostátní orgány podle směrnice (EU) 2022/2555 mohou vydat pokyny s cílem podpořit příslušné subjekty při identifikaci, analýze a posuzování rizik za účelem provádění technických a metodických požadavků týkajících se zavedení a udržování vhodného rámce řízení rizik. Tyto pokyny mohou zahrnovat zejména vnitrostátní a odvětvová posouzení rizik, ale i posouzení rizik specifická pro určitý typ subjektu. Pokyny mohou rovněž obsahovat nástroje nebo šablony pro vytvoření rámce řízení rizik na úrovni příslušných subjektů. Příslušné subjekty mohou při prokazování souladu s tímto nařízením rovněž podpořit rámce, pokyny nebo jiné mechanismy stanovené vnitrostátními právními předpisy členských států, jakož i příslušné evropské a mezinárodní normy. Agentura ENISA nebo příslušné vnitrostátní orgány podle směrnice (EU) 2022/2555 mohou navíc podporovat příslušné subjekty při určování a zavádění vhodných řešení na řešení rizik zjištěných v těchto posouzeních rizik. Těmito pokyny by neměla být dotčena povinnost příslušných subjektů identifikovat a dokumentovat rizika pro bezpečnost sítí a informačních systémů a povinnost příslušných subjektů provádět technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik stanovená v příloze tohoto nařízení podle svých potřeb a zdrojů.

(8) Opatření v oblasti bezpečnosti sítí, která se týkají: i) přechodu na komunikační protokoly síťové vrstvy nejnovější generace; ii) zavedení mezinárodně dohodnutých a interoperabilních moderních standardů pro e-mailovou komunikaci a iii) uplatňování osvědčených postupů pro zabezpečení DNS a pro bezpečnost a hygienu směrování na internetu, s sebou nesou specifické problémy, pokud jde o určení nejlepších dostupných standardů a technik zavádění. V zájmu co nejrychlejšího dosažení vysoké společné úrovně kybernetické bezpečnosti ve všech sítích by Komise měla s pomocí Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) a ve spolupráci s příslušnými orgány, průmyslem (včetně telekomunikačního průmyslu) a dalšími zúčastněnými stranami podpořit vytvoření fóra mnoha zúčastněných stran, jehož úkolem bude určit tyto nejlepší dostupné normy a techniky zavádění. Těmito pokyny zahrnujícími mnoho zúčastněných stran by neměla být dotčena povinnost příslušných subjektů provádět technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik stanovené v příloze tohoto nařízení.

(9) Podle čl. 21 odst. 2 písm. a) směrnice (EU) 2022/2555 by základní a důležité subjekty měly mít kromě politiky analýzy rizik také politiku bezpečnosti informačních systémů. Za tímto účelem by příslušné subjekty měly vytvořit politiku bezpečnosti sítí a informačních systémů a také tematicky zaměřené politiky, jako jsou postupy kontroly přístupu, které by měly být v souladu s politikou bezpečnosti sítí a informačních systémů. Politika bezpečnosti sítí a informačních systémů by měla být dokumentem nejvyšší úrovně, který stanoví celkový přístup příslušných subjektů k bezpečnosti jejich sítí a informačních systémů, a měla by být schválena řídícími orgány příslušných subjektů. Tematicky zaměřené politiky by měly být schváleny odpovídající úrovní vedení. Politika by měla stanovit ukazatele a opatření pro sledování jejího provádění a aktuálního stavu, pokud jde o úroveň vyspělosti v oblasti bezpečnosti sítí a informací příslušných subjektů, zejména s cílem usnadnit dohled nad prováděním opatření k řízení kybernetických bezpečnostních rizik prostřednictvím řídících orgánů.

(10) Pro účely technických a metodických požadavků stanovených v příloze tohoto nařízení by měl pojem „uživatel“ zahrnovat všechny právnické a fyzické osoby, které mají přístup do sítě a informačních systémů subjektu.

(11) Aby bylo možné určit a řešit rizika ohrožující bezpečnost sítí a informačních systémů, měly by příslušné subjekty zavést a udržovat vhodný rámec řízení rizik. Jako součást rámce řízení rizik by příslušné subjekty měly zavést, realizovat a sledovat plán ošetření rizik. Příslušné subjekty mohou plán ošetření rizik použít k určení možností a opatření k ošetření rizik a ke stanovení pořadí jejich důležitosti. Možnosti ošetření rizik zahrnují zejména zamezení, omezení nebo ve výjimečných případech přijetí rizika. Volba možností ošetření rizik by měla zohledňovat výsledky posouzení rizik provedeného příslušným subjektem a měla by být v souladu s politikou příslušného subjektu týkající se bezpečnosti sítí a informačních systémů. Za účelem provedení zvolených možností ošetření rizik by příslušné subjekty měly přijmout vhodná opatření k ošetření rizik.

(12) Aby mohly odhalit příhody, významné události a incidenty, měly by příslušné subjekty monitorovat své sítě a informační systémy a přijmout opatření k vyhodnocení příhod, významných událostí a incidentů. Tato opatření by měla dokázat včas odhalit síťové útoky založené na anomálních vzorcích příchozího nebo odchozího provozu a útoky odmítnutím služby.

(13) Pokud příslušné subjekty provádějí analýzu obchodního dopadu, doporučuje se, aby provedly komplexní analýzu, která případně stanoví maximální přípustnou dobu výpadku, cíle doby potřebné k obnovení provozu, cíle bodu obnovy a cíle poskytování služeb.

(14) Za účelem zmírnění rizik vyplývajících z dodavatelského řetězce příslušného subjektu a jeho vztahů s dodavateli by příslušné subjekty měly zavést bezpečnostní politiku dodavatelského řetězce, která upravuje jejich vztahy s přímými dodavateli a poskytovateli služeb. Tyto subjekty by měly ve smlouvách se svými přímými dodavateli nebo poskytovateli služeb stanovit odpovídající doložky o bezpečnosti, například tím, že budou v případě potřeby vyžadovat opatření k řízení kybernetických bezpečnostních rizik podle čl. 21 odst. 2 směrnice (EU) 2022/2555 nebo jiné podobné právní požadavky.

(15) Příslušné subjekty by měly pravidelně provádět bezpečnostní testy na základě specifické politiky a specifických postupů, aby ověřily, zda jsou opatření k řízení kybernetických bezpečnostních rizik zavedena a řádně fungují. Bezpečnostní testy mohou být prováděny na konkrétních sítích a informačních systémech nebo na příslušném subjektu jako celku a mohou zahrnovat automatické nebo manuální testy, penetrační testy, skenování zranitelnosti, statické a dynamické testy bezpečnosti aplikací, testy konfigurace nebo bezpečnostní audity. Příslušné subjekty mohou provádět bezpečnostní testy svých sítí a informačních systémů při jejich nastavení, po modernizaci nebo úpravách infrastruktury nebo aplikace, které považují za významné, nebo po údržbě. Závěry bezpečnostních testů by měly být podkladem pro politiky a postupy příslušných subjektů k posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik, ale i pro nezávislé přezkumy jejich politik bezpečnosti sítí a informací.

(16) Aby se zabránilo významnému narušení a škodám způsobeným zneužitím neopravených zranitelností v sítích a informačních systémech, měly by příslušné subjekty stanovit a uplatňovat vhodné postupy správy bezpečnostních záplat, které jsou v souladu s postupy příslušných subjektů v oblasti řízení změn, řízení zranitelností, řízení rizik a dalšími příslušnými postupy. Příslušné subjekty by měly přijmout opatření přiměřená svým zdrojům, aby zajistily, že bezpečnostní záplaty neodhalí další zranitelnosti nebo nestabilitu. V případě plánované nedostupnosti služby způsobené instalací bezpečnostních záplat se příslušným subjektům doporučuje, aby zákazníky předem náležitě informovaly.

(17) Příslušné subjekty by měly řídit rizika plynoucí z pořízení produktů IKT nebo služeb IKT od dodavatelů nebo poskytovatelů služeb a měly by získat jistotu, že pořizované produkty IKT nebo služby IKT dosahují určitých úrovní kybernetické bezpečnosti, například prostřednictvím evropských certifikátů kybernetické bezpečnosti a prohlášení EU o shodě pro produkty IKT nebo služby IKT vydaných v rámci evropského systému certifikace kybernetické bezpečnosti přijatého podle článku 49 nařízení Evropského parlamentu a Rady (EU) 2019/881 ([2]). Pokud příslušné subjekty stanoví bezpečnostní požadavky, které se mají uplatnit na pořizované produkty IKT, měly by zohlednit základní požadavky na kybernetickou bezpečnost stanovené v nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky.

(18) Za účelem ochrany před kybernetickými hrozbami a podpory prevence a zamezení šíření úniků dat by příslušné subjekty měly zavést řešení v oblasti bezpečnosti sítí. Typická řešení pro bezpečnost sítě zahrnují používání firewallů k ochraně vnitřních sítí příslušných subjektů, omezení připojení a přístupu ke službám na případy, kdy jsou připojení a přístup nezbytně nutné, a využívání virtuálních soukromých sítí pro dálkový přístup a umožnění připojení poskytovatelů služeb pouze na základě žádosti o povolení a po stanovenou dobu, jako je doba trvání údržby.

(19) Za účelem ochrany sítí příslušných subjektů a jejich informačních systémů před škodlivým a neoprávněným softwarem by tyto subjekty měly zavést kontroly, které zabrání používání neoprávněného softwaru nebo jej odhalí, a v příslušných případech by měly používat software pro detekci a reakci. Příslušné subjekty by rovněž měly zvážit prováděcí opatření k minimalizaci plochy útoku, snížení zranitelností, které mohou útočníci využít, kontrolu provádění aplikací na koncových bodech a zavedení e-mailových a internetových aplikačních filtrů, aby se snížilo vystavení škodlivému obsahu.

(20) Podle čl. 21 odst. 2 písm. g) směrnice (EU) 2022/2555 mají členské státy zajistit, aby základní a důležité subjekty uplatňovaly základní postupy kybernetické hygieny a školení o kybernetické bezpečnosti. K základním postupům v oblasti kybernetické hygieny může patřit architektura nulové důvěry, aktualizace softwaru, konfigurace zařízení, segmentace sítě, řízení identity a přístupu nebo povědomí uživatelů, měly by pořádat školení pro své zaměstnance a zvyšovat povědomí o kybernetických hrozbách, phishingu či technikách sociálního inženýrství. Postupy v oblasti kybernetické hygieny jsou součástí různých technických a metodických požadavků na opatření k řízení kybernetických bezpečnostních rizik stanovená v příloze tohoto nařízení. Pokud jde o základní postupy v oblasti kybernetické hygieny pro uživatele, příslušné subjekty by měly zvážit postupy, jako jsou zásady čistého pracovního stolu a obrazovky, používání vícefaktorových a jiných autentizačních prostředků, bezpečné používání e-mailů a prohlížení internetových stránek, ochrana před phishingem a sociálním inženýrstvím, bezpečné postupy práce na dálku.

(21) Aby se zabránilo neoprávněnému přístupu k aktivům příslušných subjektů, měly by příslušné subjekty zavést a uplatňovat tematicky zaměřenou politiku zabývající se přístupem pro osoby a pro sítě a informační systémy, jako jsou aplikace.

(22) Aby se předešlo tomu, že zaměstnanci mohou zneužít například přístupová práva v rámci příslušného subjektu, a způsobit tak újmu a škodu, měly by příslušné subjekty zvážit odpovídající opatření k řízení bezpečnosti zaměstnanců a zvýšit povědomí zaměstnanců o těchto rizicích. Příslušné subjekty by měly zavést, sdělit a udržovat disciplinární postup pro řešení porušení zásad bezpečnosti sítí a informačních systémů příslušných subjektů, který může být začleněn do jiných disciplinárních postupů zavedených příslušnými subjekty. Ověřování spolehlivosti zaměstnanců a případně přímých dodavatelů a poskytovatelů služeb příslušných subjektů by mělo přispět k dosažení cíle bezpečnosti lidských zdrojů v příslušných subjektech a může zahrnovat opatření, jako je ověření rejstříku trestů nebo dřívějších profesních povinností dané osoby, a to v návaznosti na povinnosti dané osoby v rámci příslušného subjektu a v souladu s politikou příslušného subjektu týkající se bezpečnosti sítí a informačních systémů.

([2]) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) Kybernetickou bezpečnost subjektů může posílit vícefaktorová autentizace, přičemž subjekty by její zavedení měly zvážit zejména tehdy, když uživatelé mají přístup k sítím a informačním systémům ze vzdálených míst nebo mají přístup k citlivým informacím nebo privilegovaným účtům a účtům pro správu systému. Vícefaktorovou autentizaci lze kombinovat s dalšími technikami, a vyžadovat tak za určitých okolností existenci dalších faktorů, a to na základě předem definovaných pravidel a vzorců, jako je přístup z neobvyklého místa, z neobvyklého zařízení nebo v neobvyklém čase.

(24) Příslušné subjekty by měly spravovat a chránit aktiva, která pro ně mají hodnotu, prostřednictvím řádné správy aktiv, která by měla rovněž sloužit jako základ pro analýzu rizik a řízení kontinuity činností. Příslušné subjekty by měly hospodařit s hmotnými i nehmotnými aktivy a měly by vytvořit soupis aktiv, přiřadit aktivům vymezené úrovně klasifikace, nakládat s aktivy a sledovat je a přijímat opatření na ochranu aktiv po celou dobu jejich životnosti.

(25) Správa aktiv by měla zahrnovat klasifikaci aktiv podle jejich typu, citlivosti, úrovně rizika a bezpečnostních požadavků a použití vhodných opatření a kontrol k zajištění jejich dostupnosti, integrity, důvěrnosti a autenticity. Tím, že klasifikují aktiva podle úrovně rizika, by příslušné subjekty měly být schopny uplatňovat vhodná bezpečnostní opatření a kontroly na ochranu aktiv, jako je šifrování, kontrola přístupu včetně kontroly vnějšího a fyzického a logického přístupu, zálohování, vedení protokolů a monitorování, uchovávání a likvidace. Při provádění analýzy obchodního dopadu mohou příslušné subjekty určit úroveň klasifikace na základě důsledků narušení aktiv pro tyto subjekty. Všichni zaměstnanci subjektů, které nakládají s aktivy, by měli být seznámeni se zásadami a pokyny pro nakládání s aktivy.

(26) Podrobnost soupisu aktiv by měla odpovídat potřebám příslušných subjektů. Úplný soupis aktiv by mohl s ohledem na jednotlivá aktiva uvádět přinejmenším jedinečný identifikátor, vlastníka aktiva, popis aktiva, umístění aktiva, druh aktiva, typ a klasifikaci informací zpracovávaných v rámci aktiva, datum poslední aktualizace nebo opravy aktiva, klasifikaci aktiva podle posouzení rizik a konec životnosti aktiva. Při určování vlastníka aktiva by příslušné subjekty měly rovněž určit osobu odpovědnou za zajišťování ochrany uvedeného aktiva.

(27) Rozdělení a organizace úkolů, odpovědnosti a pravomocí v oblasti kybernetické bezpečnosti by měly vytvořit konzistentní strukturu pro řízení a provádění kybernetické bezpečnosti v rámci příslušných subjektů a měly by zajistit účinnou komunikaci v případě incidentů. Při definování a přidělování odpovědností za určité úkoly by příslušné subjekty měly vzít v potaz funkce, jako je vedoucí pracovník pro bezpečnost informací, pracovník pro bezpečnost informací, pracovník pro řešení incidentů, auditor nebo podobné rovnocenné role. Příslušné subjekty mohou přidělit úkoly a odpovědnost externím stranám, například externím poskytovatelům služeb IKT.

(28) V souladu s čl. 21 odst. 2 směrnice (EU) 2022/2555 mají být opatření k řízení kybernetických bezpečnostních rizik založena na přístupu zohledňujícím všechny druhy rizik, jehož cílem je chránit sítě a informační systémy a jejich fyzické prostředí před událostmi, jako jsou krádež, požár, povodeň, výpadky telekomunikací nebo elektrického proudu, nebo před neoprávněným fyzickým přístupem k informacím a zařízením pro zpracování informací základního nebo důležitého subjektu a jejich poškozením a zásahům do nich, jež by mohly narušit dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné. Technické a metodické požadavky opatření k řízení kybernetických bezpečnostních rizik by proto měly rovněž řešit fyzickou a environmentální bezpečnost sítí a informačních systémů tím, že zahrnou opatření na ochranu těchto systémů před selháním systému, lidskou chybou, zlovolným jednáním nebo přírodními jevy. Mezi další příklady fyzických a environmentálních hrozeb mohou patřit zemětřesení, výbuchy, sabotáž, vnitřní hrozba, občanské nepokoje, toxický odpad a emise z životního prostředí. Předcházení ztrátám, poškození nebo ohrožení sítí a informačních systémů nebo přerušení jejich provozu v důsledku selhání a narušení podpůrných služeb by mělo v příslušných subjektech přispět k cíli kontinuity činnosti. Ochrana před fyzickými a environmentálními hrozbami by navíc měla v příslušných subjektech přispět k bezpečnosti údržby sítí a informačních systémů.

(29) Příslušné subjekty by měly navrhnout a provádět ochranná opatření proti fyzickým a environmentálním hrozbám a stanovit minimální a maximální prahové kontrolní hodnoty pro fyzické a environmentální hrozby a sledovat environmentální parametry. Měly by například zvážit instalaci systémů, které včas odhalí zaplavení prostor, v nichž jsou umístěny síťové a informační systémy. Pokud jde o nebezpečí požáru, příslušné subjekty by měly zvážit zřízení samostatného požárního úseku pro datové centrum, použití ohnivzdorných materiálů, čidel pro sledování teploty a vlhkosti, napojení budovy na požární poplachový systém s automatickým hlášením místnímu hasičskému sboru a systémy včasné detekce a hašení požáru. Příslušné subjekty by měly rovněž provádět pravidelná požární cvičení a požární kontroly. Kromě toho by příslušné subjekty měly v zájmu zajištění dodávky elektrické energie zvážit ochranu před přepětím a odpovídající nouzové napájení, a to v souladu s příslušnými normami. Vzhledem k tomu, že přehřátí představuje riziko pro dostupnost sítí a informačních systémů, mohly by příslušné subjekty, zejména poskytovatelé služeb datových center, zvážit odpovídající, nepřetržité záložní klimatizační systémy.

(30) Toto nařízení má dále upřesnit případy, kdy by se měl incident považovat za významný pro účely čl. 23 odst. 3 směrnice (EU) 2022/2555. Kritéria by měla být taková, aby příslušné subjekty byly schopny posoudit, zda je incident významný, a mohly tak incident oznámit v souladu se směrnicí (EU) 2022/2555. Kritéria stanovená v tomto nařízení by navíc měla být považována za vyčerpávající, aniž je dotčen článek 5 směrnice (EU) 2022/2555. Toto nařízení vymezuje případy, kdy by incident měl být považován za významný, tím, že stanoví horizontální případy i případy specifické pro jednotlivé druhy subjektů.

(31) Podle čl. 23 odst. 4 směrnice (EU) 2022/2555 by příslušné subjekty měly být povinny oznamovat významné incidenty ve lhůtách stanovených uvedeným ustanovením. Tyto lhůty pro oznámení běží od okamžiku, kdy se subjekt o těchto významných incidentech dozví. Příslušný subjekt je tudíž povinen oznamovat incidenty, které by na základě jeho prvotního posouzení mohly uvedenému subjektu způsobit závažné provozní narušení služeb nebo finanční ztrátu nebo postihnout jiné fyzické nebo právnické osoby tím, že by jim způsobily značnou hmotnou nebo nehmotnou újmu. Pokud tedy příslušný subjekt zjistí podezřelou událost nebo poté, co jej na potenciální incident upozorní třetí strana, například fyzická osoba, zákazník, subjekt, orgán, mediální organizace nebo jiný zdroj, měl by příslušný subjekt podezřelou událost včas posoudit a určit, zda se jedná o incident, a pokud ano, určit jeho povahu a závažnost. Proto se má za to, že se příslušný subjekt o významném incidentu „dozvěděl“, pokud má po tomto prvotním posouzení rozumnou míru jistoty, že k významnému incidentu došlo.

(32) Aby bylo možné zjistit, zda je incident významný, by příslušné subjekty měly v příslušných případech spočítat počet uživatelů, na které měl incident dopad, přičemž by měly vzít v úvahu obchodní a koncové zákazníky, s nimiž mají příslušné subjekty smluvní vztah, ale i fyzické a právnické osoby, které jsou spojeny s obchodními zákazníky. Pokud příslušný subjekt není schopen vypočítat počet zasažených uživatelů, měl by se pro účely výpočtu celkového počtu uživatelů zasažených incidentem vzít v úvahu odhad příslušného subjektu ohledně možného maximálního počtu zasažených uživatelů. Významnost incidentu zahrnujícího službu vytvářející důvěru by se neměla určovat pouze podle počtu uživatelů, ale také podle počtu spoléhajících se stran, jelikož tyto strany mohou být významným incidentem zahrnujícím službu vytvářející důvěru rovněž dotčeny, pokud jde o provozní narušení a hmotnou nebo nehmotnou újmu. Poskytovatelé služeb vytvářejících důvěru by proto měli při zjišťování, zda je incident významný, případně zohlednit také počet spoléhajících se stran. Za tímto účelem by se spoléhajícími se stranami měly rozumět fyzické nebo právnické osoby, které se spoléhají na službu vytvářející důvěru.

(33) Operace údržby, které mají za následek omezenou dostupnost nebo nedostupnost služeb, by neměly být za významné incidenty považovány v případě, že k omezené dostupnosti nebo nedostupnosti služby dojde v souladu s plánovanou údržbou. Kromě toho by se za významný incident neměly považovat případy, kdy je služba nedostupná z důvodu plánovaného přerušení, jako je přerušení nebo nedostupnost na základě předem stanoveného smluvního ujednání.

(34) Doba trvání incidentu, který ovlivňuje dostupnost služby, by se měla měřit od přerušení řádného poskytování této služby až do doby obnovy. Pokud příslušný subjekt není schopen určit okamžik, kdy narušení začalo, měla by se doba trvání incidentu měřit od okamžiku, kdy byl incident zjištěn, nebo od okamžiku, kdy byl incident zaznamenán v síťových nebo systémových protokolech nebo jiných zdrojích dat, podle toho, co nastane dříve.

(35) Úplná nedostupnost služby by se měla měřit od okamžiku, kdy je služba uživatelům plně nedostupná, do okamžiku, kdy jsou běžné činnosti nebo provoz obnoveny na úroveň služby, která byla poskytována před incidentem. Pokud příslušný subjekt není schopen určit, kdy úplná nedostupnost služby začala, měla by se nedostupnost měřit od okamžiku, kdy ji tento subjekt zjistil.

(36) Pro účely stanovení přímých finančních ztrát v důsledku incidentu by příslušné subjekty měly vzít v úvahu všechny finanční ztráty, které jim v důsledku incidentu vznikly, jako jsou náklady na výměnu nebo přemístění softwaru, hardwaru nebo infrastruktury, náklady na zaměstnance, včetně nákladů spojených s výměnou nebo přemístěním zaměstnanců, nábor dalších zaměstnanců, odměny za přesčasy a obnovu ztracených nebo zhoršených dovedností, poplatky v důsledku nedodržení smluvních závazků, náklady na nápravu a kompenzace zákazníkům, ztráty v důsledku ušlých příjmů, náklady spojené s interní a externí komunikací, náklady na poradenství, včetně nákladů spojených s právním poradenstvím, forenzními službami a službami souvisejícími se zajišťováním nápravy a další náklady spojené s incidentem. Za finanční ztráty v důsledku incidentu by však neměly být považovány správní pokuty ani náklady, které jsou nezbytné pro každodenní provoz podniku, včetně nákladů na obecnou údržbu infrastruktury, zařízení, hardwaru a softwaru, udržování dovedností zaměstnanců na aktuální úrovni, interních nebo externích nákladů na podporu obchodní činnosti po incidentu, včetně modernizací, zlepšování a iniciativ k posuzování rizik, a pojistného. Příslušné subjekty by měly vypočítat výši finančních ztrát na základě dostupných údajů, a pokud nelze určit skutečnou výši finančních ztrát, měly by tyto částky odhadnout.

(37) Příslušné subjekty by měly mít rovněž povinnost hlásit incidenty, které způsobily nebo mohou způsobit úmrtí fyzických osob nebo značnou újmu na zdraví fyzických osob, neboť tyto incidenty jsou zvlášť závažnými případy způsobení značné hmotné nebo nehmotné újmy. Incident, který příslušný subjekt postihne, může například způsobit nedostupnost zdravotní péče nebo záchranných služeb nebo ztrátu důvěrnosti či integrity údajů s dopadem na zdraví fyzických osob. Pro účely určení, zda incident způsobil nebo může způsobit značnou újmu na zdraví fyzické osoby, by příslušné subjekty měly vzít v úvahu, zda incident způsobil nebo může způsobit vážná zranění a špatný zdravotní stav. Za tímto účelem by příslušné subjekty neměly být povinny shromažďovat další informace, ke kterým nemají přístup.

(38) Za omezenou dostupnost je třeba považovat zejména případy, kdy je služba poskytovaná příslušným subjektem výrazně pomalejší než průměrná doba odezvy nebo kdy nejsou k dispozici všechny funkce služby. Pokud je to možné, měla by být pro posouzení zpoždění v době odezvy použita objektivní kritéria založená na průměrných dobách odezvy u služeb poskytovaných příslušnými subjekty. Funkcí služby může být například funkce chatu nebo funkce vyhledávání obrázků.

(39) Úspěšný podezřele zlovolný a neoprávněný přístup do sítě a informačních systémů příslušného subjektu by měl být považován za významný incident, pokud je takový přístup schopen způsobit vážné narušení provozu. Například pokud se aktér kybernetické hrozby předem umístí do sítě a informačních systémů příslušného subjektu s cílem způsobit narušení služeb v budoucnu, měl by být incident považován za významný.

(40) Opakující se incidenty, které jsou spojeny stejnou hlavní příčinou a které jednotlivě nesplňují kritéria významného incidentu, by měly být společně považovány za významný incident za předpokladu, že společně splňují kritérium finanční ztráty a že k nim došlo alespoň dvakrát během šesti měsíců. Takové opakující se incidenty mohou poukazovat na významné nedostatky a slabiny v postupech řízení kybernetických bezpečnostních rizik příslušného subjektu a v úrovni jeho vyspělosti v oblasti kybernetické bezpečnosti. Takové opakující se incidenty navíc mohou příslušnému subjektu způsobit značné finanční ztráty.

(41) Komise si v souladu s čl. 21 odst. 5 a čl. 23 odst. 11 směrnice (EU) 2022/2555 poskytuje se skupinou pro spolupráci a agenturou ENISA vzájemné poradenství a spolupracuje s nimi, pokud jde o návrhy prováděcích aktů.

(42) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 (ES) ([3]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 1. září 2024.

(43) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného podle článku 39 směrnice (EU) 2022/2555,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Předmět

Toto nařízení, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru (dále jen „příslušné subjekty“), stanovuje technické a metodické požadavky na opatření uvedená v čl. 21 odst. 2 směrnice (EU) 2022/2555 a dále upřesňuje případy, v nichž se incident považuje za významný, jak je uvedeno v čl. 23 odst. 3 směrnice (EU) 2022/2555.

Článek 2

Technické a metodické požadavky

1. Technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik uvedené v čl. 21 odst. 2 písm. a) až j) směrnice (EU) 2022/2555 jsou pro příslušné subjekty stanoveny v příloze tohoto nařízení.

2. Příslušné subjekty při provádění a uplatňování technických a metodických požadavků opatření k řízení kybernetických bezpečnostních rizik stanovených v příloze tohoto nařízení zajistí úroveň bezpečnosti sítí a informačních systémů odpovídající existujícím rizikům. Za tímto účelem při plnění technických a metodických požadavků opatření k řízení kybernetických bezpečnostních rizik stanovených v příloze tohoto nařízení náležitě zohlední míru své expozice rizikům, svou velikost a pravděpodobnost výskytu incidentů a jejich závažnost, včetně jejich společenského a hospodářského dopadu.

([3]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Pokud příloha tohoto nařízení stanoví, že technický nebo metodický požadavek opatření k řízení kybernetických bezpečnostních rizik se použije, „v případě potřeby“, „v příslušných případech“ nebo „v proveditelném rozsahu“ a pokud se příslušný subjekt domnívá, že pro něj není vhodné, použitelné nebo proveditelné použít takové určité technické a metodické požadavky, příslušný subjekt srozumitelným způsobem zdokumentuje své odůvodnění v tomto smyslu.

Článek 3

Významné incidenty

1. Incident se považuje za významný pro účely čl. 23 odst. 3 směrnice (EU) 2022/2555, pokud jde o příslušné subjekty, je-li splněno jedno nebo více z těchto kritérií:

a) incident způsobil nebo může způsobit příslušnému subjektu přímou finanční ztrátu, která přesahuje 500 000 EUR nebo 5 % celkového ročního obratu příslušného subjektu za předchozí účetní období, podle toho, která částka je nižší;

b) incident způsobil nebo může způsobit únik obchodního tajemství příslušného subjektu podle čl. 2 bodu 1 směrnice (EU) 2016/943;

c) incident způsobil nebo může způsobit úmrtí fyzické osoby;

d) incident způsobil nebo může způsobit značnou újmu na zdraví fyzické osoby;

e) došlo k úspěšnému podezřelému zlovolnému a neoprávněnému přístupu do sítě a informačních systémů, který může způsobit vážné narušení provozu;

f) incident splňuje kritéria stanovená v článku 4;

g) incident splňuje jedno nebo více kritérií uvedených v článcích 5 až 14.

2) Za významné incidenty se nepovažují plánovaná přerušení provozu a plánované důsledky plánovaných operací údržby prováděných příslušnými subjekty nebo jejich jménem.

3) Při stanovení počtu uživatelů dotčených incidentem pro účely článku 7 a článků 9 až 14 příslušné subjekty zohlední všechny tyto položky:

a) počet zákazníků, kteří mají s příslušným subjektem uzavřenou smlouvu, která jim umožňuje přístup k síti a informačním systémům příslušného subjektu nebo ke službám, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné;

b) počet fyzických a právnických osob spojených s podnikovými zákazníky, kteří využívají sítě a informační systémy subjektů nebo služby, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné.

Článek 4

Opakující se incidenty

Incidenty, které nejsou jednotlivě považovány za významný incident ve smyslu článku 3, se považují společně za jeden významný incident, pokud splňují všechna tato kritéria:

a) došlo k nim nejméně dvakrát během šesti měsíců;

b) mají stejnou příčinu;

c) společně splňují kritéria stanovená v čl. 3 odst. 1 písm. a).

Článek 5

Významné incidenty související s provozovateli DNS

V souvislosti s provozovateli DNS se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) rekurzivní nebo autoritativní služba pro překlad doménových jmen je zcela nedostupná po dobu delší než 30 minut;

b) průměrná doba odezvy rekurzivní nebo autoritativní služby pro překlad doménových jmen na požadavky DNS je déle než jednu hodinu delší než 10 sekund;

c) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služby DNS, s výjimkou případů, kdy z důvodu chybné konfigurace nejsou správné údaje méně než 1 000 doménových jmen spravovaných provozovatelem DNS, které představují nejvýše 1 % doménových jmen spravovaných provozovatelem DNS.

Článek 6

Významné incidenty související s registry domén nejvyšší úrovně

V souvislosti s registry domén nejvyšší úrovně se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) autoritativní služba pro překlad doménových jmen je zcela nedostupná;

b) průměrná doba odezvy autoritativní služby pro překlad doménových jmen na požadavky DNS je déle než jednu hodinu delší než 10 sekund;

c) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s doménou nejvyšší úrovně.

Článek 7

Významné incidenty související s poskytovateli služeb cloud computingu

V souvislosti s poskytovateli služeb cloud computingu se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) služba cloud computingu je zcela nedostupná po dobu delší než 30 minut;

b) déle než jednu hodinu je omezena dostupnost služby cloud computingu poskytovatele pro více než 5 % uživatelů dané služby cloud computingu v Unii nebo pro více než 1 milion uživatelů dané služby cloud computingu v Unii, podle toho, který počet je nižší;

c) v důsledku podezřelého zlovolného jednání je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služeb cloud computingu;

d) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služby cloud computingu a toto narušení má dopad na více než 5 % uživatelů dané služby cloud computingu v Unii nebo na více než 1 milion uživatelů dané služby cloud computingu v Unii, podle toho, který počet je nižší.

Článek 8

Významné incidenty související s poskytovateli služeb datových center

V souvislosti s poskytovateli služeb datových center se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) služba datového centra provozovaného poskytovatelem je zcela nedostupná;

b) dostupnost služby datového centra provozovaného poskytovatelem je déle než jednu hodinu omezena;

c) v důsledku podezřelého zlovolného jednání je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služby datového centra;

d) je ohrožen fyzický přístup k datovému centru provozovanému poskytovatelem.

Článek 9

Významné incidenty související s poskytovateli sítí pro doručování obsahu

V souvislosti s poskytovateli sítí pro doručování obsahu se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) síť pro doručování obsahu je zcela nedostupná po dobu delší než 30 minut;

b) déle než jednu hodinu je omezena dostupnost sítě pro doručování obsahu poskytovatele pro více než 5 % uživatelů dané sítě pro doručování obsahu v Unii nebo pro více než 1 milion uživatelů dané sítě pro doručování obsahu v Unii, podle toho, který počet je nižší;

c) v důsledku podezřelého zlovolného jednání je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním sítě pro doručování obsahu;

d) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním sítě pro doručování obsahu a toto narušení má dopad na více než 5 % uživatelů dané sítě pro doručování obsahu v Unii nebo na více než 1 milion uživatelů dané sítě pro doručování obsahu v Unii, podle toho, který počet je nižší.

Článek 10

Významné incidenty související s poskytovateli řízených služeb a poskytovatelů řízených bezpečnostních služeb

V souvislosti s poskytovateli řízených služeb a poskytovateli řízených bezpečnostních služeb se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) řízená služba nebo řízená bezpečnostní služba je zcela nedostupná po dobu delší než 30 minut;

b) déle než jednu hodinu je omezena dostupnost řízené služby nebo řízené bezpečnostní služby pro více než 5 % uživatelů dané služby v Unii nebo pro více než 1 milion uživatelů dané služby v Unii, podle toho, který počet je nižší;

c) v důsledku podezřelého zlovolného jednání je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním řízené služby nebo řízené bezpečnostní služby;

d) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním řízené služby nebo řízené bezpečnostní služby a toto narušení má dopad na více než 5 % uživatelů dané řízené služby nebo řízené bezpečnostní služby v Unii nebo na více než 1 milion uživatelů dané služby v Unii, podle toho, který počet je nižší.

Článek 11

Významné incidenty související s poskytovateli on-line tržišť

V souvislosti s poskytovateli on-line tržišť se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) on-line tržiště je zcela nedostupné pro více než 5 % uživatelů on-line tržiště v Unii nebo pro více než 1 milion uživatelů on-line tržiště v Unii, podle toho, který počet je nižší;

b) omezenou dostupností on-line tržiště je dotčeno více než 5 % uživatelů on-line tržiště v Unii nebo více než 1 milion uživatelů on-line tržiště v Unii, podle toho, který počet je nižší;

c) v důsledku podezřelého zlovolného jednání je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním on-line tržiště;

d) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných údajů souvisejících s poskytováním on-line tržiště a toto narušení má dopad na více než 5 % uživatelů daného on-line tržiště v Unii nebo na více než 1 milion uživatelů daného on-line tržiště v Unii, podle toho, který počet je nižší.

Článek 12

Významné incidenty související s poskytovateli internetových vyhledávačů

V souvislosti s poskytovateli internetových vyhledávačů se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) internetový vyhledávač je zcela nedostupný pro více než 5 % uživatelů daného internetového vyhledávače v Unii nebo pro více než 1 milion uživatelů daného internetového vyhledávače v Unii, podle toho, který počet je nižší;

b) omezenou dostupností internetového vyhledávače je dotčeno více než 5 % uživatelů internetového vyhledávače v Unii nebo více než 1 milion uživatelů daného internetového vyhledávače v Unii, podle toho, který počet je nižší;

c) v důsledku podezřelého zlovolného jednání je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním internetového vyhledávače;

d) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných údajů souvisejících s poskytováním internetového vyhledávače a toto narušení má dopad na více než 5 % uživatelů daného internetového vyhledávače v Unii nebo na více než 1 milion uživatelů daného internetového vyhledávače v Unii, podle toho, který počet je nižší.

Článek 13

Významné incidenty související s poskytovateli platforem sociálních sítí

V souvislosti s poskytovateli služeb platforem sociálních sítí se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) platforma sociální sítě je zcela nedostupná pro více než 5 % uživatelů dané platformy sociálních sítích v Unii nebo pro více než 1 milion uživatelů platformy sociálních sítí v Unii, podle toho, které číslo je nižší;

b) omezenou dostupností platformy sociálních sítí je dotčeno více než 5 % uživatelů platformy sociálních sítí v Unii nebo více než 1 milion uživatelů dané platformy sociálních sítí v Unii, podle toho, který počet je nižší;

c) v důsledku podezřelého zlovolného jednání je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním platformy sociálních sítí;

d) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných údajů souvisejících s poskytováním platformy sociálních sítí a toto narušení má dopad na více než 5 % uživatelů dané platformy sociálních sítí v Unii nebo na více než 1 milion uživatelů dané platformy sociálních sítí v Unii, podle toho, který počet je nižší.

Článek 14

Významné incidenty související s poskytovateli služeb vytvářejících důvěru

V souvislosti s poskytovateli služeb vytvářejících důvěru se incident považuje za významný podle čl. 3 odst. 1 písm. g), pokud splňuje jedno nebo více z těchto kritérií:

a) služba vytvářející důvěru je zcela nedostupná po dobu delší než 20 minut;

b) služba vytvářející důvěru je pro uživatele nebo spoléhající se strany nedostupná déle než jednu hodinu, počítanou na základě kalendářního týdne;

c) omezenou dostupností služby vytvářející důvěru je dotčeno více než 1 % uživatelů nebo spoléhajících se stran v Unii nebo více než 200 000 uživatelů nebo spoléhajících se stran v Unii, podle toho, který počet je nižší;

d) je narušen fyzický přístup do oblasti, kde jsou umístěny sítě a informační systémy a kam mají přístup pouze důvěryhodní pracovníci poskytovatele služby vytvářející důvěru, nebo je narušena ochrana takového fyzického přístupu;

e) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služby vytvářející důvěru a toto narušení má dopad na více než 0,1 % uživatelů dané služby vytvářející důvěru nebo spoléhajících se stran v Unii nebo na více než 100 uživatelů dané služby vytvářející důvěru nebo spoléhajících se stran v Unii, podle toho, který počet je nižší.

Článek 15

Zrušení

Prováděcí nařízení Komise (EU) 2018/151 ([4]) se zrušuje.

Článek 16

Vstup v platnost a použitelnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 17. října 2024.

Za Komisi
Ursula VON DER LEYEN
předsedkyně

([4]) Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný (Úř. věst. L 26, 31.1.2018, s. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

PŘÍLOHA

Technické a metodické požadavky uvedené v článku 2 tohoto nařízení

1. **Politika bezpečnosti sítí a informačních systémů (čl. 21 odst. 2 písm. a) směrnice (EU) 2022/2555)**

1.1. *Politika bezpečnosti sítí a informačních systémů*

1.1.1. Pro účely čl. 21 odst. 2 písm. a) směrnice (EU) 2022/2555 politika bezpečnosti sítí a informačních systémů:

a) stanoví přístup příslušných subjektů k řízení bezpečnosti jejich sítí a informačních systémů;

b) odpovídá obchodní strategii a cílům příslušných subjektů a doplňuje je;

c) stanoví cíle bezpečnosti sítí a informací;

d) obsahuje závazek k neustálému zlepšování bezpečnosti sítí a informačních systémů;

e) obsahuje závazek poskytnout odpovídající zdroje potřebné pro její provedení, včetně potřebných zaměstnanců, finančních zdrojů, postupů, nástrojů a technologií;

f) je sdělena příslušným zaměstnancům a dotčeným zúčastněným externím stranám a je jimi uznána;

g) stanoví role a odpovědnosti podle bodu 1.2.;

h) uvádí seznam dokumentace, která má být uchovávána, a dobu jejího uchovávání;

i) uvádí seznam politik specifických pro toto téma;

j) stanoví ukazatele a opatření ke sledování jejího provádění a aktuálního stavu úrovně vyspělosti bezpečnosti sítí a informací příslušných subjektů;

k) uvádí datum formálního schválení řídícími orgány příslušných subjektů (dále jen „řídící orgány“).

1.1.2. Bezpečnostní politiku v oblasti sítí a informačních systémů řídící orgány přezkoumávají a v případě potřeby aktualizují nejméně každý rok a vždy v případě výskytu významných incidentů nebo významných změn operací či rizik. Výsledky přezkumů se zdokumentují.

1.2. *Úkoly, odpovědnosti a pravomoci*

1.2.1. Příslušné subjekty v rámci své politiky bezpečnosti sítí a informačních systémů uvedené v bodě 1.1 stanoví odpovědnosti a pravomoci v oblasti bezpečnosti sítí a informačních systémů, přidělí je k úkolům, rozdělí je podle potřeb příslušných subjektů a sdělí je řídícím orgánům.

1.2.2. Příslušné subjekty vyžadují, aby všichni zaměstnanci a třetí strany uplatňovali bezpečnost sítí a informačních systémů v souladu se zavedenou politikou bezpečnosti sítí a informací, tematicky zaměřenými politikami a postupy příslušných subjektů.

1.2.3. Řídícím orgánům je v otázkách bezpečnosti sítí a informačních systémů přímo podřízena alespoň jedna osoba.

1.2.4. V závislosti na velikosti příslušných subjektů spadá bezpečnost sítí a informačních systémů pod specializované úkoly nebo povinnosti, které jsou vykonávány nad rámec stávajících úkolů.

1.2.5. Kolidující povinnosti a protichůdné oblasti odpovědnosti budou v příslušných případech odděleny.

1.2.6. Řídící orgány úkoly, odpovědnosti a pravomoci přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při výskytu významných incidentů nebo významných změn operací či rizik.

2. **Politika řízení rizik (čl. 21 odst. 2 bod a) směrnice (EU) 2022/2555)**

2.1. *Rámec pro řízení rizik*

2.1.1. Pro účely čl. 21 odst. 2 písm. a) směrnice (EU) 2022/2555 příslušné subjekty zřídí a spravují vhodný rámec řízení rizik, aby identifikovaly a řešily rizika pro bezpečnost sítí a informačních systémů. Příslušné subjekty provedou a zdokumentují posouzení rizik a na základě výsledků vypracují, zavedou a sledují plán ošetření rizik. Výsledky posouzení rizik a zbytková rizika přijímají řídící orgány nebo v příslušných případech osoby, které jsou odpovědné a mají pravomoc řídit rizika, za předpokladu, že příslušné subjekty zajistí odpovídající podávání zpráv řídícím orgánům.

2.1.2. Pro účely bodu 2.1.1 příslušné subjekty stanoví postupy pro identifikaci, analýzu, posouzení a ošetření rizik (dále jen „proces řízení rizik v oblasti kybernetické bezpečnosti“). Proces řízení rizik v oblasti kybernetické bezpečnosti musí být v příslušných případech nedílnou součástí celkového procesu řízení rizik příslušných subjektů. V rámci procesu řízení rizik v oblasti kybernetické bezpečnosti příslušné subjekty:

a) dodržují metodiku řízení rizik;

b) stanoví úroveň tolerance rizika v souladu s ochotou příslušných subjektů riskovat;

c) stanoví a spravují příslušná kritéria rizik;

d) v souladu s přístupem zohledňujícím všechny druhy rizik identifikují a dokumentují rizika pro bezpečnost sítí a informačních systémů, zejména ve vztahu ke třetím stranám, a rizika, která by mohla vést k narušení dostupnosti, integrity, autenticity a důvěrnosti sítí a informačních systémů, včetně identifikace kritického místa (tzv. single point of failures);

e) analyzují rizika pro bezpečnost sítí a informačních systémů, včetně hrozby, pravděpodobnosti, dopadu a úrovně rizika, s přihlédnutím k informacím o kybernetických hrozbách a zranitelnostech;

f) vyhodnotí identifikovaná rizika na základě kritérií rizik;

g) identifikují vhodné možnosti a opatření k ošetření rizik a stanoví pořadí jejich důležitosti;

h) průběžně sledují provádění opatření k ošetření rizik;

i) určí, kdo je odpovědný za provádění opatření k ošetření rizik a kdy by tato opatření měla být provedena;

j) komplexně zdokumentují zvolená opatření k ošetření rizik v plánu ošetření rizik a důvody, které vedly k akceptaci zbytkových rizik.

2.1.3. Při identifikování vhodných možností a opatření k ošetření rizik a stanovení pořadí jejich důležitosti příslušné subjekty zohlední výsledky posouzení rizik, výsledky postupu pro zhodnocení účinnosti opatření k řízení kybernetických bezpečnostních rizik, náklady na provedení ve vztahu k očekávanému přínosu, klasifikaci aktiv uvedenou v bodě 12.1 a analýzu obchodního dopadu uvedenou v bodě 4.1.3.

2.1.4. Příslušné subjekty výsledky posouzení rizik a plán ošetření rizik přezkoumají a v případě potřeby aktualizují v plánovaných intervalech alespoň jednou ročně a při výskytu významných incidentů nebo významných změn operací či rizik.

2.2. *Sledování souladu*

2.2.1. Příslušné subjekty pravidelně přezkoumávají dodržování svých politik bezpečnosti sítí a informačních systémů, tematicky zaměřených politik, pravidel a norem. Řídící orgány jsou informovány o stavu bezpečnosti sítí a informací na základě přezkumů dodržování souladu prostřednictvím pravidelných zpráv.

2.2.2. Příslušné subjekty zavedou účinný systém podávání zpráv o dodržování souladu, který bude odpovídat jejich struktuře, provoznímu prostředí a prostředí hrozeb. Systém podávání zpráv o dodržování souladu musí být schopen poskytovat řídicím orgánům informovaný přehled o aktuálním stavu řízení rizik příslušnými subjekty.

2.2.3. Příslušné subjekty provádějí sledování souladu v plánovaných intervalech a při výskytu významných incidentů nebo významných změn operací či rizik.

2.3. *Nezávislý přezkum bezpečnosti informací a sítí*

2.3.1. Příslušné subjekty nezávisle přezkoumávají svůj přístup k řízení bezpečnosti sítí a informačních systémů a jeho provádění, včetně lidí, procesů a technologií.

2.3.2. Příslušné subjekty vypracovávají a spravují postupy pro provádění nezávislých přezkumů, které vykonávají osoby s patřičnou kvalifikací pro audit. Pokud nezávislý přezkum vykonávají zaměstnanci příslušného subjektu, nesmí být osoby provádějící přezkumy podřízeny zaměstnancům přezkoumávané oblasti. V případě, že velikost příslušných subjektů neumožňuje takové oddělení pravomocí, zavedou příslušné subjekty alternativní opatření, která zaručí nestrannost přezkumů.

2.3.3. Výsledky nezávislých přezkumů, včetně výsledků sledování souladu podle bodu 2.2 a monitorování a měření podle bodu 7, se oznamují řídícím orgánům. Přijmou se nápravná opatření nebo se akceptuje zbytkové riziko podle kritérií, které si příslušné subjekty stanovily pro přijatelnost rizika.

2.3.4. Nezávislé přezkumy se provádějí v plánovaných intervalech a při výskytu významných incidentů nebo významných změn operací či rizik.

3. **Řešení incidentů (čl. 21 odst. 2 písm. b) směrnice (EU) 2022/2555)**

3.1. *Politika řešení incidentů*

3.1.1. Pro účely čl. 21 odst. 2 písm. b) směrnice (EU) 2022/2555 příslušné subjekty vypracují a zavedou politiku řešení incidentů, která stanoví úkoly, odpovědnosti a postupy pro včasné odhalování, analýzu a omezování incidentů nebo reagování na ně, obnovu po incidentech, dokumentování a oznamování incidentů.

3.1.2. Politika uvedená v bodě 3.1.1 musí být v souladu s plánem kontinuity provozu a plánem pro obnovu po havárii uvedeným v bodě 4.1. Politika obsahuje:

a) systém klasifikace incidentů, který je v souladu s hodnocením a klasifikací událostí provedenými podle bodu 3.4.1;

b) účinné komunikační plány, včetně plánů pro eskalaci a podávání zpráv;

c) přidělení úkolů týkajících se odhalování incidentů a vhodné reakce na ně kompetentním zaměstnancům;

d) dokumenty, které se používají při odhalování incidentů a reakci na ně, jako jsou příručky pro reakci na incidenty, eskalační matice, seznamy kontaktů a šablony.

3.1.3. Úkoly, odpovědnosti a postupy stanovené v politice se testují, přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a po významných incidentech nebo významných změnách operací či rizik.

3.2. *Monitorování a vedení protokolů*

3.2.1. Příslušné subjekty stanoví postupy a používají nástroje pro činnosti v rámci monitorování a vedení protokolů ve svých sítích a informačních systémech s cílem odhalit události, které by mohly být považovány za incidenty, a odpovídajícím způsobem na ně reagovat, aby bylo možné zmírnit dopad.

3.2.2. Monitorování musí být v proveditelném rozsahu automatizované a v závislosti na kapacitách podniku prováděné buď nepřetržitě, nebo v pravidelných intervalech. Příslušné subjekty provádějí své monitorovací činnosti způsobem, který minimalizuje falešně pozitivní a falešně negativní výsledky.

3.2.3. Na základě postupů uvedených v bodě 3.2.1 příslušné subjekty vedou, dokumentují a přezkoumávají protokoly. Příslušné subjekty sestaví seznam aktiv, o kterých mají být vedeny protokoly, na základě výsledků posouzení rizik provedeného podle bodu 2.1. Protokoly musí případně obsahovat:

a) příslušný odchozí a příchozí síťový provoz;

b) vytváření, změny nebo odstraňování uživatelů sítí a informačních systémů příslušných subjektů a rozšiřování oprávnění;

c) přístup k systémům a aplikacím;

d) události související s autentizací;

e) veškerý administrátorský přístup k systémům a aplikacím a činnosti prováděné prostřednictvím účtů správce;

f) přístup k důležitým konfiguračním a záložním souborům nebo jejich změny;

g) protokoly událostí a protokoly z bezpečnostních nástrojů, jako jsou antivirové programy, systémy detekce narušení nebo brány firewall;

h) využití systémových prostředků a jejich výkonnost;

i) fyzický přístup k zařízením;

j) přístup k jejich síťovému vybavení a zařízením a jejich používání;

k) aktivace, zastavení a pozastavení různých protokolů;

l) environmentální události.

3.2.4. Protokoly se pravidelně přezkoumávají, zda se v nich neobjevují neobvyklé nebo nežádoucí trendy. Příslušné subjekty v případě potřeby stanoví vhodné hodnoty výstražných prahů. Pokud jsou překročeny stanovené hodnoty výstražných prahů, spustí se v případě potřeby automaticky alarm. Příslušné subjekty zajistí, aby v případě spuštění alarmu byla včas zahájena kvalifikovaná a vhodná reakce.

3.2.5. Příslušné subjekty uchovávají a zálohují protokoly po předem stanovenou dobu a chrání je před neoprávněným přístupem nebo změnami.

3.2.6. Příslušné subjekty v proveditelném rozsahu zajistí, aby všechny systémy měly synchronizované zdroje času, a aby tak bylo možné propojovat protokoly mezi systémy za účelem vyhodnocení události. Příslušné subjekty vytvářejí a vedou seznam všech aktiv, o kterých mají být vedeny protokoly, a zajistí, aby systémy monitorování a vedení protokolů byly redundantní. Dostupnost systémů monitorování a vedení protokolů se sleduje nezávisle na systémech, které monitorují.

3.2.7. Postupy i seznam aktiv, o kterých mají být vedeny protokoly, se přezkoumávají a v případě potřeby aktualizují pravidelně a po významných incidentech.

3.3. *Oznamování událostí*

3.3.1. Příslušné subjekty zavedou jednoduchý mechanismus, který umožní jejich zaměstnancům, dodavatelům a zákazníkům oznamovat podezřelé události.

3.3.2. Příslušné subjekty v případě potřeby informují své dodavatele a zákazníky o mechanismu pro oznamování událostí a pravidelně školí své zaměstnance, jak tento mechanismus používat.

3.4. *Hodnocení a klasifikace událostí*

3.4.1. Příslušné subjekty posoudí podezřelé události, aby určily, zda se jedná o incidenty, a pokud ano, určí jejich povahu a závažnost.

3.4.2. Pro účely bodu 3.4.1 postupují příslušné subjekty takto:

a) provedení hodnocení na základě předem stanovených kritérií a na základě roztřídění s cílem určit priority, pokud jde o zamezení šíření incidentu a jeho odstranění;

b) zhodnocení existence opakujících se incidentů podle článku 4 tohoto nařízení jednou za čtvrtletí;

c) přezkoumání příslušných protokolů pro účely hodnocení a klasifikace událostí;

d) zavedení postupu pro propojení a analýzu protokolů a

e) přehodnocení a překlasifikování událostí v případě, že se objeví nové informace, nebo po analýze dříve dostupných informací.

3.5. *Reakce na incident*

3.5.1. Příslušné subjekty reagují na incidenty včas a v souladu se zdokumentovanými postupy.

3.5.2. Postupy reakce na incident zahrnují tyto fáze:

a) zamezení šíření incidentu s cílem předejít důsledkům incidentu způsobeným jeho rozšířením;

b) odstranění incidentu, aby se zabránilo jeho pokračování nebo opětovnému výskytu;

c) případně obnova po incidentu.

3.5.3. Příslušné subjekty stanoví komunikační plány a postupy:

a) s týmy pro reakce na počítačové bezpečnostní incidenty (CSIRT) nebo v příslušných případech s příslušnými orgány v souvislosti s oznamováním incidentů;

b) pro komunikaci mezi zaměstnanci příslušného subjektu a pro komunikaci s příslušnými zúčastněnými stranami mimo subjekt.

3.5.4. Příslušné subjekty vedou protokoly o činnostech v rámce reakce na incident v souladu s postupy uvedenými v bodě 3.2.1 a zaznamenávají důkazy.

3.5.5. Příslušné subjekty v plánovaných intervalech testují své postupy reakce na incidenty.

3.6. *Přezkumy po incidentu*

3.6.1. V případě potřeby příslušné subjekty provádějí po obnově přezkumy po incidentu. Přezkumy po incidentu musí pokud možno identifikovat hlavní příčinu incidentu a vést ke zdokumentování získaných zkušeností s cílem omezit výskyt a následky incidentů v budoucnu.

3.6.2. Příslušné subjekty zajistí, aby přezkumy po incidentu přispěly ke zlepšení jejich přístupu k bezpečnosti sítí a informací, k opatřením pro ošetření rizik a k postupům pro řešení a odhalování incidentů a reakci na ně.

3.6.3. Příslušné subjekty v plánovaných intervalech přezkoumávají, zda incidenty vedly k přezkumu po incidentu.

4. **Kontinuita podnikání a krizové řízení (čl. 21 odst. 2 písm. c) směrnice (EU) 2022/2555)**

4.1. *Plán kontinuity provozu a obnovy provozu po havárii*

4.1.1. Pro účely čl. 21 odst. 2 písm. c) směrnice (EU) 2022/2555 příslušné subjekty stanoví a udržují plán kontinuity provozu a obnovy provozu po havárii, který se použije v případě incidentů.

4.1.2. Provoz příslušných subjektů se obnoví v souladu s plánem kontinuity provozu a obnovy provozu po havárii. Plán se zakládá na výsledcích posouzení rizik provedeného podle bodu 2.1 a obsahuje v případě potřeby tyto údaje:

a) účel, oblast působnosti a cílová skupina;

b) úkoly a povinnosti;

c) hlavní kontaktní osoby a (interní a externí) komunikační kanály;

d) podmínky pro aktivaci a deaktivaci plánu;

e) postup obnovy pro operace;

f) plány obnovy pro konkrétní operace, včetně cílů obnovy;

g) požadované zdroje, včetně záloh a redundancí;

h) obnovení činností po dočasných opatřeních a pokračování v těchto činnostech.

4.1.3. Příslušné subjekty provedou analýzu obchodního dopadu, aby posoudily potenciální dopady závažných narušení na jejich obchodní operace, a na základě výsledků analýzy obchodního dopadu stanoví požadavky na zachování provozu pro sítě a informační systémy.

4.1.4. Plán kontinuity provozu a obnovy provozu po havárii se testuje, přezkoumává a v případě potřeby aktualizuje v plánovaných intervalech a po významných incidentech nebo významných změnách operací nebo rizik. Příslušné subjekty zajistí, aby plány zohledňovaly poznatky získané z těchto testů.

4.2. *Správa zálohování a redundance*

4.2.1. Příslušné subjekty uchovávají záložní kopie údajů a poskytují dostatečné dostupné zdroje, včetně zařízení, sítí a informačních systémů a zaměstnanců, aby zajistily odpovídající úroveň redundance.

4.2.2. Na základě výsledků posouzení rizik provedeného podle bodu 2.1 a plánu kontinuity provozu stanoví příslušné subjekty plány zálohování, které obsahují tyto skutečnosti:

a) doby obnovy;

b) ujištění, že záložní kopie jsou úplné a správné, včetně konfiguračních dat a údajů uložených v prostředí služby cloud computingu;

c) uložení záložních kopií (online nebo offline) na bezpečném místě nebo místech, která nejsou ve stejné síti jako systém a jsou v dostatečné vzdálenosti, aby nedošlo k poškození v případě havárie v hlavní provozovně;

d) vhodné kontroly fyzického a logického přístupu k záložním kopiím v souladu se stupněm utajení dat;

e) obnovení údajů ze záložních kopií;

f) doby uchovávání na základě obchodních a regulačních požadavků.

4.2.3. Příslušné subjekty provádějí pravidelné kontroly integrity záložních kopií.

4.2.4. Na základě výsledků posouzení rizik provedeného podle bodu 2.1 a plánu kontinuity provozu zajistí příslušné subjekty dostatečnou dostupnost zdrojů alespoň částečnou redundancí těchto zdrojů:

a) sítě a informační systémy;

b) aktiva, včetně zařízení, vybavení a zásob;

c) pracovníci s potřebnou odpovědností, pravomocemi a kompetencemi;

d) vhodné komunikační kanály.

4.2.5. Příslušné subjekty v případě potřeby zajistí, aby sledování a přizpůsobení zdrojů, včetně zařízení, systémů a zaměstnanců, byly řádně podloženy požadavky na zálohování a redundanci.

4.2.6. Příslušné subjekty provádějí pravidelné testování obnovy záložních kopií a redundancí, aby bylo zajištěno, že se na ně lze v podmínkách obnovy spoléhat a že zahrnují kopie, postupy a znalosti k provedení účinné obnovy. Příslušné subjekty zdokumentují výsledky testů a v případě potřeby přijmou nápravná opatření.

4.3. *Krizové řízení*

4.3.1. Příslušné subjekty zavedou postup pro krizové řízení.

4.3.2. Příslušné subjekty zajistí, aby postup krizových řízení zahrnoval alespoň tyto prvky:

a) úlohy a odpovědnost zaměstnanců a v případě potřeby dodavatelů a poskytovatelů služeb s uvedením rozdělení úkolů v krizových situacích, včetně konkrétních kroků, které je třeba dodržovat;

b) vhodné komunikační prostředky mezi příslušnými subjekty a příslušnými orgány;

c) uplatňování vhodných opatření k zajištění zachování bezpečnosti sítí a informačních systémů v krizových situacích.

Pro účely písmene b) zahrnuje tok informací mezi příslušnými subjekty a příslušnými orgány jak povinná sdělení, jako jsou oznámení o incidentech a související časové plány, tak nepovinná sdělení.

4.3.3. Příslušné subjekty zavedou postup pro správu a využívání informací obdržených od týmů CSIRT nebo v příslušných případech od příslušných orgánů, které se týkají incidentů, zranitelností, hrozeb nebo možných zmírňujících opatření.

4.3.4. Příslušné subjekty plán krizového řízení pravidelně nebo po významných incidentech nebo významných změnách operací či rizik testují, přezkoumávají a v případě potřeby aktualizují.

5. **Bezpečnost dodavatelského řetězce (čl. 21 odst. 2 písm. d) směrnice (EU) 2022/2555)**

5.1. *Politika bezpečnosti dodavatelského řetězce*

5.1.1. Pro účely čl. 21 odst. 2 písm. d) směrnice (EU) 2022/2555 příslušné subjekty stanoví, zavedou a uplatňují politiku bezpečnosti dodavatelského řetězce, která upravuje vztahy s jejich přímými dodavateli a poskytovateli služeb s cílem zmírnit zjištěná rizika pro bezpečnost sítí a informačních systémů. V politice bezpečnosti dodavatelského řetězce příslušné subjekty určí svou úlohu v dodavatelském řetězci a sdělí ji svým přímým dodavatelům a poskytovatelům služeb.

5.1.2. V rámci politiky bezpečnosti dodavatelského řetězce uvedené v bodě 5.1.1 stanoví příslušné subjekty kritéria pro výběr dodavatelů a poskytovatelů služeb a uzavírání smluv s nimi. Tato kritéria zahrnují:

a) postupy kybernetické bezpečnosti dodavatelů a poskytovatelů služeb, včetně jejich postupů k zajištění bezpečného vývoje;

b) schopnost dodavatelů a poskytovatelů služeb splňovat specifikace v oblasti kybernetické bezpečnosti stanovené příslušnými subjekty;

c) celkovou kvalitu a odolnost produktů a služeb IKT a v nich obsažených opatření pro řízení kybernetických bezpečnostních rizik, včetně rizik a úrovně klasifikace produktů IKT a služeb IKT;

d) schopnost příslušných subjektů diverzifikovat zdroje dodávek a v příslušných případech omezit závislost na dodavateli.

5.1.3. Při vytváření své politiky bezpečnosti dodavatelského řetězce příslušné subjekty v příslušných případech zohlední výsledky koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců provedeného v souladu s čl. 22 odst. 1 směrnice (EU) 2022/2555.

5.1.4. Na základě politiky bezpečnosti dodavatelského řetězce a s přihlédnutím k výsledkům posouzení rizik provedeného podle bodu 2.1 této přílohy příslušné subjekty zajistí, aby jejich smlouvy s dodavateli a poskytovateli služeb, a to v případě potřeby prostřednictvím dohod o úrovni služeb, stanovovaly:

a) požadavky na kybernetickou bezpečnost pro dodavatele nebo poskytovatele služeb, včetně požadavků na bezpečnost při pořizování služeb IKT nebo produktů IKT uvedených v bodě 6.1;

b) požadavky na informovanost, dovednosti a školení a v případě potřeby osvědčení, která se vyžadují od zaměstnanců dodavatelů nebo poskytovatelů služeb;

c) požadavky na ověřování spolehlivosti zaměstnanců dodavatelů a poskytovatelů služeb;

d) povinnost dodavatelů a poskytovatelů služeb bez zbytečného odkladu informovat příslušné subjekty o incidentech, které představují riziko pro bezpečnost sítě a informačních systémů těchto subjektů;

e) právo provést audit nebo právo obdržet auditní zprávy;

f) povinnost dodavatelů a poskytovatelů služeb řešit zranitelnosti, které představují riziko pro bezpečnost sítí a informačních systémů příslušných subjektů;

g) požadavky týkající se subdodávek, a pokud příslušné subjekty subdodávky umožňují, požadavky na kybernetickou bezpečnost subdodavatelů v souladu s požadavky na kybernetickou bezpečnost uvedenými v písmenu a);

h) povinnosti dodavatelů a poskytovatelů služeb při ukončení smlouvy, jako je vyhledání a zničení informací, které dodavatelé a poskytovatelé služeb získali při plnění svých úkolů.

5.1.5. Příslušné subjekty zohlední prvky uvedené v bodech 5.1.2 a 5.1.3 v rámci procesu výběru nových dodavatelů a poskytovatelů služeb, ale i v rámci procesu zadávání zakázek uvedeného v bodě 6.1.

5.1.6. Příslušné subjekty politiku bezpečnosti dodavatelského řetězce přezkoumávají, sledují a vyhodnocují v plánovaných intervalech a v případě, že dojde k významným změnám operací nebo rizik nebo k významným incidentům souvisejícím s poskytováním služeb IKT nebo majícím dopad na bezpečnost produktů IKT od dodavatelů a poskytovatelů služeb, a v případě potřeby jednají v návaznosti na změny postupů kybernetické bezpečnosti dodavatelů a poskytovatelů služeb.

5.1.7. Pro účely bodu 5.1.6 příslušné subjekty:

a) v příslušných případech pravidelně monitorují zprávy o provádění dohod o úrovni služeb;

b) přezkoumávají incidenty týkající se produktů IKT a služeb ICT od dodavatelů a poskytovatelů služeb;

c) posuzují potřebu neplánovaných přezkumů a komplexně dokumentují zjištění;

d) analyzují rizika, která představují změny související s produkty IKT a službami IKT od dodavatelů a poskytovatelů služeb, a v případě potřeby včas přijímají zmírňující opatření.

5.2. *Seznam dodavatelů a poskytovatelů služeb*

Příslušné subjekty vedou a průběžně aktualizují registr svých přímých dodavatelů a poskytovatelů služeb, který obsahuje:

a) kontaktní místa pro každého přímého dodavatele a poskytovatele služeb;

b) seznam produktů IKT, služeb IKT a procesů IKT poskytovaných přímým dodavatelem nebo poskytovatelem služeb příslušným subjektům.

6. **Zabezpečení pořizování, vývoje a údržby sítí a informačních systémů (čl. 21 odst. 2 písm. e) směrnice (EU) 2022/2555)**

6.1. *Zabezpečení pořizování služeb IKT nebo produktů IKT*

6.1.1. Pro účely čl. 21 odst. 2 písm. e) směrnice (EU) 2022/2555 příslušné subjekty stanoví a zavedou procesy řízení rizik vyplývajících z pořizování služeb IKT nebo produktů IKT pro komponenty, které jsou kritické pro bezpečnost sítí a informačních systémů příslušných subjektů a které pocházejí od dodavatelů nebo poskytovatelů služeb, po celou dobu jejich životnosti na základě posouzení rizik provedeného podle bodu 2.1.

6.1.2. Pro účely bodu 6.1.1 procesy uvedené v bodě 6.1.1 zahrnují:

a) bezpečnostní požadavky, které se mají vztahovat na pořizované služby IKT nebo produkty IKT;

b) požadavky týkající se bezpečnostních aktualizací po celou dobu životnosti služeb IKT nebo produktů IKT nebo nahrazení po skončení doby podpory;

c) informace popisující hardwarové a softwarové komponenty používané ve službách IKT nebo produktech IKT;

d) informace popisující zavedené funkce kybernetické bezpečnosti ve službách IKT nebo produktech ICT a konfiguraci potřebnou pro jejich bezpečný provoz;

e) ujištění, že služby IKT nebo produkty IKT splňují bezpečnostní požadavky podle písmene a);

f) metody ověřování, zda dodané služby IKT nebo produkty IKT splňují stanovené bezpečnostní požadavky, a zdokumentování výsledků ověřování.

6.1.3. Příslušné subjekty procesy přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při výskytu významných incidentů.

6.2. *Životní cyklus bezpečného vývoje*

6.2.1. Před vývojem sítě a informačního systému, včetně softwaru, stanoví příslušné subjekty pravidla pro bezpečný vývoj sítí a informačních systémů a uplatňují je při vývoji sítí a informačních systémů v rámci podniku nebo při zadávání vývoje sítí a informačních systémů externím dodavatelům. Pravidla se vztahují na všechny fáze vývoje, včetně specifikace, návrhu, vývoje, implementace a testování.

6.2.2. Pro účely bodu 6.2.1 příslušné subjekty:

a) provádějí analýzu bezpečnostních požadavků ve fázích specifikace a návrhu jakéhokoli projektu vývoje nebo pořízení realizovaného příslušnými subjekty nebo jejich jménem;

b) uplatňují zásady pro inženýring bezpečných systémů a zásady bezpečného kódování na všechny činnosti spojené s vývojem informačních systémů, jako je podpora kybernetické bezpečnosti již od návrhu a architektury nulové důvěry;

c) stanoví bezpečnostní požadavky týkající se prostředí vývoje;

d) zavádějí a implementují procesy testování bezpečnosti během životního cyklu vývoje;

e) vhodným způsobem vybírají, chrání a spravují údajů o bezpečnostních testech;

f) opravují a anonymizují údaje o testování podle posouzení rizik provedeného podle bodu 2.1.

6.2.3. Při externě zajišťovaném vývoji sítí a informačních systémů příslušné subjekty uplatňují rovněž zásady a postupy uvedené v bodech 5 a 6.1.

6.2.4. Příslušné subjekty v plánovaných intervalech přezkoumají a, je-li to nutné, aktualizují svá pravidla bezpečného vývoje.

6.3. *Správa konfigurace*

6.3.1. Příslušné subjekty přijmou vhodná opatření k vytvoření, zdokumentování, zavedení a monitorování konfigurací, včetně bezpečnostních konfigurací hardwaru, softwaru, služeb a sítí.

6.3.2. Pro účely bodu 6.3.1 příslušné subjekty:

a) stanoví a zajistí bezpečnost konfigurací pro svůj hardware, software, služby a sítě;

b) stanoví a zavedou procesy a nástroje pro vynucování stanovených bezpečných konfigurací pro hardware, software, služby a sítě, pro nově instalované systémy i pro systémy v provozu, a to po celou dobu jejich životnosti.

6.3.3. Příslušné subjekty konfigurace přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech nebo při výskytu významných incidentů nebo významných změn operací či rizik.

6.4. *Řízení změn, opravy a údržba*

6.4.1. Při řízení změn v sítích a informačních systémech příslušné subjekty uplatňují postupy řízení změn. V příslušných případech musí být takové postupy v souladu s obecnými politikami řízení změn příslušných subjektů.

6.4.2. Postupy uvedené v bodě 6.4.1. se uplatní na vydání, úpravy a mimořádné změny jakéhokoli softwaru a hardwaru při provozu a změnách konfigurace. Postupy zajistí, aby tyto změny byly zdokumentovány a na základě posouzení rizik provedeného podle bodu 2.1 byly před provedením testovány a posouzeny z hlediska možného dopadu.

6.4.3. V případě, že nebylo možné dodržet standardní postupy řízení změn z důvodu mimořádné události, příslušné subjekty zdokumentují výsledek změny a vysvětlení, proč nebylo možné postupy dodržet.

6.4.4. Příslušné subjekty postupy přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při významných incidentech nebo významných změnách operací či rizik.

6.5. *Testování bezpečnosti*

6.5.1. Příslušné subjekty stanoví, zavedou a uplatňují politiku a postupy pro testování bezpečnosti.

6.5.2. Příslušné subjekty:

a) na základě posouzení rizik provedeného podle bodu 2.1 stanoví potřebu, rozsah, četnost a typ bezpečnostních testů;

b) provádějí bezpečnostní testy podle zdokumentované metodiky testování, která se vztahuje na složky identifikované v analýze rizik jako důležité pro bezpečný provoz;

c) dokumentují typ, rozsah, čas a výsledky testů, včetně posouzení kritičnosti a zmírňujících opatření pro každé zjištění;

d) v případě kritických zjištění uplatní zmírňující opatření.

6.5.3. Příslušné subjekty své politiky testování bezpečnosti přezkoumají a v případě potřeby aktualizují v plánovaných intervalech.

6.6. *Řízení bezpečnostních záplat*

6.6.1. Příslušné subjekty stanoví a uplatňují postupy, které jsou v souladu s postupy řízení změn uvedenými v bodě 6.4.1, jakož i s postupy řízení zranitelností, řízení rizik a dalšími příslušnými postupy., a to s cílem zajistit, že:

a) bezpečnostní záplaty se použijí v přiměřené době poté, co začaly být k dispozici;

b) bezpečnostní záplaty se před použitím v produkčních systémech otestují;

c) bezpečnostní záplaty pocházejí z důvěryhodných zdrojů a jejich integrita je kontrolována;

d) v případech, kdy záplata není k dispozici nebo kdy není nepoužita podle bodu 6.6.2, jsou zavedena další opatření a akceptována zbytková rizika.

6.6.2. Odchylně od bodu 6.6.1 písm. a) se příslušné subjekty mohou rozhodnout bezpečnostní záplaty nepoužít, pokud nevýhody použití bezpečnostních záplat převažují nad přínosy pro kybernetickou bezpečnost. Příslušné subjekty každé takové rozhodnutí řádně zdokumentují a zdůvodní.

6.7. *Bezpečnost sítí*

6.7.1. Příslušné subjekty přijmou vhodná opatření na ochranu svých sítí a informačních systémů před kybernetickými hrozbami.

6.7.2. Pro účely bodu 6.7.1 příslušné subjekty:

a) v komplexní a aktuální podobě zdokumentují architekturu sítě;

b) určí a uplatní kontrolní mechanismy na ochranu vnitřních síťových domén příslušných subjektů před neoprávněným přístupem;

c) nakonfigurují kontroly, které zabrání přístupům a síťové komunikaci, jež nejsou nutné pro provoz příslušných subjektů;

d) určí a uplatní kontroly vzdáleného přístupu k sítím a informačním systémům, včetně přístupu ze strany poskytovatelů služeb;

e) nevyužijí systémy používané pro správu provádění zásad zabezpečení k jiným účelům;

f) výslovně zakážou nebo deaktivují nepotřebná připojení a služby;

g) v případě potřeby umožní přístup k sítím a informačním systémům příslušných subjektů výhradně prostřednictvím zařízení, která jsou těmito subjekty autorizována;

h) povolí připojení poskytovatelů služeb pouze na základě žádosti o povolení a po stanovenou dobu, například po dobu trvání údržby;

i) zavedou spojení mezi různými systémy pouze prostřednictvím důvěryhodných kanálů, které jsou logicky, kryptograficky nebo fyzicky odděleny od ostatních komunikačních kanálů a zajišťují zaručenou identifikaci jejich koncových bodů a ochranu dat kanálu před modifikací nebo vyzrazením;

j) přijmou prováděcí plán pro úplný přechod na nejnovější generaci komunikačních protokolů síťové vrstvy bezpečným, vhodným a postupným způsobem a zavedou opatření k urychlení tohoto přechodu;

k) přijmou prováděcí plán pro zavedení mezinárodně dohodnutých a interoperabilních moderních standardů pro e-mailovou komunikaci, aby se zabezpečila e-mailová komunikace a zmírnila zranitelnost spojená s hrozbami souvisejícími s elektronickou poštou, a zavedou opatření k urychlení tohoto zavádění;

l) uplatňují osvědčené postupy pro zabezpečení DNS a pro zabezpečení směrování na internetu a hygienu směrování provozu vycházejícího ze sítě a směřujícího do sítě.

6.7.3. Příslušné subjekty tato opatření přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při výskytu významných incidentů nebo významných změn operací či rizik.

6.8. *Segmentace sítě*

6.8.1. Příslušné subjekty rozdělí systémy na sítě nebo zóny v souladu s výsledky posouzení rizik podle bodu 2.1. Oddělí své systémy a sítě od systémů a sítí třetích stran.

6.8.2. Za tímto účelem příslušné subjekty:

a) zohlední funkční, logické a fyzické vztahy mezi důvěryhodnými systémy a službami, včetně jejich umístění;

b) udělí přístup do sítě nebo zóny na základě posouzení jejich bezpečnostních požadavků;

c) uchovávají systémy, které jsou kritické pro provoz příslušných subjektů nebo pro bezpečnost, v zabezpečených zónách;

d) zavedou ve svých komunikačních sítích demilitarizovanou zónu, která zajistí bezpečnou komunikaci vycházející z jejich sítí nebo směřující do jejich sítí;

e) omezí přístup a komunikaci mezi zónami a uvnitř zón na ty, které jsou nezbytné pro provoz příslušných subjektů nebo pro bezpečnost;

f) oddělí specializovanou síť pro správu sítí a informačních systémů od provozní sítě příslušných subjektů;

g) oddělí kanály pro správu sítě od ostatního provozu v síti;

h) oddělí produkční systémy pro útvary příslušných subjektů od systémů používaných pro vývoj a testování, včetně záloh.

6.8.3. Příslušné subjekty segmentaci sítě přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při významných incidentech nebo významných změnách operací či rizik.

6.9. *Ochrana před škodlivým a neautorizovaným softwarem*

6.9.1. Příslušné subjekty chrání své sítě a informační systémy před škodlivým a neautorizovaným softwarem.

6.9.2. Za tímto účelem příslušné subjekty zejména zavedou opatření, která odhalí nebo zabrání používání škodlivého nebo neoprávněného softwaru. Příslušné subjekty v případě potřeby zajistí, aby jejich sítě a informační systémy byly vybaveny softwarem pro detekci a reakci, který je pravidelně aktualizován v souladu s posouzením rizik provedeným podle bodu 2.1 a se smluvními ujednáními s poskytovateli.

6.10. *Řešení a zveřejňování zranitelností*

6.10.1. Příslušné subjekty získají informace o technických zranitelnostech svých sítí a informačních systémů, vyhodnotí, zda jsou těmto zranitelnostem vystaveny, a přijmou vhodná opatření k řízení těchto zranitelností.

6.10.2. Pro účely bodu 6.10.1 příslušné subjekty:

a) sledují informace o zranitelnostech prostřednictvím vhodných kanálů, jako jsou oznámení týmů CSIRT, příslušných orgánů nebo informace poskytované dodavateli či poskytovateli služeb;

b) v případě potřeby provádějí v plánovaných intervalech kontroly zranitelnosti a zaznamenávají důkazy o výsledcích těchto kontrol;

c) bez zbytečného odkladu řeší zranitelnosti, které příslušné subjekty označily za kritické pro své operace;

d) zajistí, aby jejich postupy pro řešení zranitelností byly v souladu s jejich postupy pro řízení změn, řízení bezpečnostních oprav, řízení rizik a řízení incidentů;

e) stanoví postup pro zveřejňování zranitelností v souladu s platnou vnitrostátní koordinovanou politikou zveřejňování zranitelností.

6.10.3. Pokud je to odůvodněno potenciálním dopadem zranitelnosti, příslušné subjekty vypracují a zavedou plán na její zmírnění. V ostatních případech příslušné subjekty zdokumentují a zdůvodní, proč zranitelnost nevyžaduje nápravu.

6.10.4. Příslušné subjekty přezkoumají a v případě potřeby v plánovaných intervalech aktualizují kanály, které používají pro sledování informací o zranitelnosti.

7. **Politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik (čl. 21 odst. 2 písm. f) směrnice (EU) 2022/2555)**

7.1. Pro účely čl. 21 odst. 2 písm. f) směrnice (EU) 2022/2555 příslušné subjekty stanoví, zavedou a uplatňují politiku a postupy za účelem posouzení, zda jsou opatření k řízení kybernetických bezpečnostních rizik přijatá příslušným subjektem účinně prováděna a udržována.

7.2. Politika a postupy uvedené v bodě 7.1. zohledňují výsledky posouzení rizik podle bodu 2.1. a minulé významné incidenty. Příslušné subjekty určí:

a) jaká opatření pro řízení kybernetických bezpečnostních rizik mají být sledována a měřena, včetně procesů a kontrol;

b) případně metody monitorování, měření, analyzování a hodnocení, s cílem zajistit platné výsledky;

c) kdy se má provádět monitorování a měření;

d) kdo je odpovědný za monitorování a měření účinnosti opatření k řízení kybernetických bezpečnostních rizik;

e) kdy se mají výsledky monitorování a měření analyzovat a vyhodnocovat;

f) kdo musí tyto výsledky analyzovat a vyhodnotit.

7.3. Příslušné subjekty politiku a postupy přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při významných incidentech nebo významných změnách operací či rizik.

8. **Základní postupy v oblasti kybernetické hygieny a bezpečnostní školení (čl. 21 odst. 2 písm. g) směrnice (EU) 2022/2555)**

8.1. *Zvyšování povědomí a základní postupy v oblasti kybernetické hygieny*

8.1.1. Pro účely čl. 21 odst. 2 písm. g) směrnice (EU) 2022/2555 příslušné subjekty zajistí, aby si jejich zaměstnanci, včetně členů řídících orgánů, ale i přímí dodavatelé a poskytovatelé služeb byli vědomi rizik, byli informováni o významu kybernetické bezpečnosti a uplatňovali postupy v oblasti kybernetické hygieny.

8.1.2. Pro účely bodu 8.1.1 poskytnou příslušné subjekty svým zaměstnancům, včetně členů řídících orgánů, a v případě potřeby přímým dodavatelům a poskytovatelům služeb v souladu s bodem 5.1.4. program zvyšování informovanosti, který:

a) je naplánován v čase tak, aby se činnosti opakovaly a zahrnovaly nové zaměstnance;

b) bude vytvořen v souladu s politikou bezpečnosti sítí a informací, tematicky zaměřenými politikami a příslušnými postupy bezpečnosti sítí a informací;

c) zahrnuje relevantní kybernetické hrozby, zavedená opatření k řízení kybernetických bezpečnostních rizik, kontaktní místa a zdroje pro další informace a poradenství v otázkách kybernetické bezpečnosti a rovněž postupy v oblasti kybernetické hygieny pro uživatele.

8.1.3. Program zvyšování povědomí se v případě potřeby testuje z hlediska účinnosti. Program zvyšování informovanosti se v plánovaných intervalech aktualizuje a nabízí, a to s přihlédnutím ke změnám postupů v oblasti kybernetické hygieny a k aktuálním hrozbám a rizikům pro příslušné subjekty.

8.2. *Bezpečnostní školení*

8.2.1. Příslušné subjekty určí zaměstnance, jejichž funkce vyžadují dovednosti a odborné znalosti v oblasti bezpečnosti, a zajistí, aby pravidelně absolvovali školení v oblasti bezpečnosti sítí a informačních systémů.

8.2.2. Příslušné subjekty vytvoří, zavedou a použijí program školení v souladu s politikou bezpečnosti sítí a informací, tematicky zaměřenými politikami a dalšími příslušnými postupy v oblasti bezpečnosti sítí a informací, který na základě kritérií stanoví potřeby školení pro určité funkce a pozice.

8.2.3. Školení uvedené v bodě 8.2.1 musí být relevantní pro pracovní funkci zaměstnance a musí být posouzena jeho účinnost. Školení by mělo zohledňovat zavedená bezpečnostní opatření a zahrnovat:

a) pokyny týkající se bezpečné konfigurace a provozu sítí a informačních systémů, včetně mobilních zařízení;

b) informování o známých kybernetických hrozbách;

c) školení týkající se chování v případě výskytu bezpečnostních událostí.

8.2.4. Příslušné subjekty vztáhnou školení na zaměstnance, kteří přecházejí na nové pozice nebo funkce vyžadující dovednosti a odborné znalosti v oblasti bezpečnosti.

8.2.5. Program je pravidelně aktualizován a prováděn s přihlédnutím k platným politikám a pravidlům, přiděleným úkolům a odpovědnostem, ale i ke známým kybernetickým hrozbám a technologickému vývoji.

9. **Kryptografie (čl. 21 odst. 2 písm. h) směrnice (EU) 2022/2555)**

9.1. Pro účely čl. 21 odst. 2 písm. h) směrnice (EU) 2022/2555 příslušné subjekty stanoví, zavedou a uplatňují politiku a postupy týkající se kryptografie s cílem zajistit přiměřené a účinné používání kryptografie k ochraně důvěrnosti, autenticity a integrity informací v souladu s klasifikací aktiv příslušných subjektů a výsledky posouzení rizik provedeného podle bodu 2.1.

9.2. Politika a postupy uvedené v bodě 9.1 stanoví:

a) v souladu s klasifikací aktiv příslušných subjektů typ, sílu a kvalitu kryptografických opatření potřebných k ochraně aktiv příslušných subjektů, včetně údajů, které jsou uloženy a předávány;

b) na základě písmene a) protokoly nebo rodiny protokolů, které mají být přijaty, a dále kryptografické algoritmy, úroveň šifrování, kryptografická řešení a postupy používání, které mají být schváleny a jejichž použití v příslušných subjektech se požaduje, případně v souladu s přístupem založeným na kryptografické agilitě;

c) přístup příslušných subjektů k řízení klíčů, včetně případných metod pro:

i) generování různých klíčů pro kryptografické systémy a aplikace;

ii) vydávání a získávání certifikátů veřejných klíčů;

iii) distribuci klíčů určeným subjektům, včetně způsobu aktivace klíčů po jejich obdržení;

iv) ukládání klíčů, včetně způsobu, jakým oprávnění uživatelé získávají přístup ke klíčům;

v) změnu nebo aktualizaci klíčů, včetně pravidel, kdy a jak klíče měnit;

vi) nakládání s napadenými klíči;

vii) zrušení klíčů včetně způsobu jejich odebrání nebo deaktivace;

viii) obnovení ztracených nebo poškozených klíčů;

ix) zálohování nebo archivaci klíčů;

x) ničení klíčů;

xi) vedení protokolů a provádění auditu klíčových činností souvisejících s řízením;

xii) nastavení dat pro aktivaci a deaktivaci klíčů, aby se zajistilo, že klíče lze používat pouze po stanovenou dobu v souladu s pravidly organizace pro správu klíčů.

9.3. Příslušné subjekty v plánovaných intervalech přezkoumávají a v případě potřeby aktualizují své zásady a postupy s ohledem na nejnovější poznatky v oblasti kryptografie.

10. **Bezpečnost lidských zdrojů (čl. 21 odst. 2 písm. i) směrnice (EU) 2022/2555)**

10.1. *Bezpečnost lidských zdrojů*

10.1.1. Pro účely čl. 21 odst. 2 písm. i) směrnice (EU) 2022/2555 příslušné subjekty zajistí, aby jejich zaměstnanci a případně přímí dodavatelé a poskytovatelé služeb porozuměli svým povinnostem týkajícím se bezpečnosti a aby se k jejich dodržování zavázali, a to v návaznosti na poskytované služby a pracovní místa a v souladu s politikou příslušných subjektů v oblasti bezpečnosti sítí a informačních systémů.

10.1.2. Požadavek uvedený v bodě 10.1.1 musí zahrnovat:

a) mechanismy, které zajistí, aby všichni zaměstnanci, případně přímí dodavatelé a poskytovatelé služeb porozuměli standardním postupům v oblasti kybernetické hygieny, které příslušné subjekty uplatňují podle bodu 8.1, a aby je dodržovali;

b) mechanismy, které zajistí, aby si všichni uživatelé s administrátorským nebo privilegovaným přístupem byli vědomi svých úkolů, odpovědností a pravomocí a jednali v souladu s nimi;

c) mechanismy, které zajistí, aby členové řídících orgánů porozuměli svým úkolům, odpovědnostem a pravomocím v oblasti bezpečnosti sítí a informačních systémů a aby jednali v souladu s nimi;

d) mechanismy pro nábor pracovníků majících kvalifikaci pro příslušné funkce, jako jsou ověření referencí, postupy prověřování, ověřování certifikátů nebo písemné testy.

10.1.3. Příslušné subjekty v plánovaných intervalech, nejméně však jednou ročně, přezkoumají zařazení pracovníků na konkrétní funkce uvedené v bodě 1.2 a vyčlenění lidských zdrojů v tomto ohledu. V případě potřeby zařazení aktualizují.

10.2. *Ověření spolehlivosti*

10.2.1. Příslušné subjekty v proveditelném rozsahu zajistí, aby se u jejich zaměstnanců a v příslušných případech u přímých dodavatelů a poskytovatelů služeb provádělo ověřování spolehlivosti v souladu s bodem 5.1.4, pokud to vyžadují jejich úkoly, povinnosti a oprávnění.

10.2.2. Pro účely bodu 10.2.1 příslušné subjekty:

a) zavedou kritéria, která stanoví, které úkoly, odpovědnosti a pravomoci mohou vykonávat pouze osoby, jejichž spolehlivost byla ověřena;

b) zajistí, aby ověření spolehlivosti těchto osob uvedené v bodě 10.2.1, které vezme v potaz platné zákony, předpisy a etické zásady úměrně k obchodním požadavkům, ke klasifikaci aktiv podle bodu 12.1, k sítím a informačním systémům, k nimž mají mít přístup, a vnímaným rizikům bylo provedeno před tím, než tyto osoby začnou vykonávat dané úkoly, odpovědnosti a pravomoci.

10.2.3. Příslušné subjekty tuto politiku v plánovaných intervalech přezkoumávají a v případě potřeby aktualizují a v případě potřeby ji aktualizují.

10.3. *Postup při ukončení nebo změně pracovního poměru*

10.3.1. Příslušné subjekty zajistí, aby byly smluvně vymezeny a vymáhány odpovědnosti a povinnosti v oblasti bezpečnosti sítí a informačních systémů, které zůstávají v platnosti i po ukončení nebo změně pracovního poměru jejich zaměstnanců.

10.3.2. Pro účely bodu 10.3.1 příslušné subjekty začlení do pracovních podmínek, smlouvy nebo dohody fyzické osoby odpovědnosti a povinnosti, které zůstávají v platnosti i po ukončení pracovního poměru nebo smlouvy, například ustanovení o důvěrnosti.

10.4. *Disciplinární řízení*

10.4.1. Příslušné subjekty zavedou, sdělí a udržují disciplinární postup pro řešení porušení politik bezpečnosti sítí a informačních systémů. Tento postup zohledňuje příslušné právní, zákonné, smluvní a obchodní požadavky.

10.4.2. Příslušné subjekty v plánovaných intervalech a v případě potřeby v důsledku právních změn nebo významných změn operací či rizik disciplinární postup přezkoumávají a v případě potřeby aktualizují.

11. **Kontrola přístupu (čl. 21 odst. 2 písm. i) a j) směrnice (EU) 2022/2555)**

11.1. *Postup kontroly přístupu*

11.1.1. Pro účely čl. 21 odst. 2 písm. i) směrnice (EU) 2022/2555 příslušné subjekty stanoví, zdokumentují a zavedou politiky řízení logického a fyzického přístupu k jejich sítím a informačním systémům na základě obchodních požadavků a požadavků na bezpečnost sítí a informačního systému.

11.1.2. Politiky uvedené v bodě 11.1.1:

a) řeší přístup ze strany osob, včetně zaměstnanců, návštěvníků a externích subjektů, jako jsou dodavatelé a poskytovatelé služeb;

b) řeší přístup prostřednictvím sítí a informačních systémů;

c) zajistí, aby byl přístup udělen pouze uživatelům, kteří byli řádně ověřeni.

11.1.3. Příslušné subjekty tyto politiky přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při výskytu významných incidentů nebo významných změn operací či rizik.

11.2. *Správa přístupových práv*

11.2.1. Příslušné subjekty poskytují, upravují, odebírají a dokumentují přístupová práva k sítím a informačním systémům v souladu s politikou řízení přístupu uvedenou v bodě 11.1.

11.2.2. Příslušné subjekty:

a) přidělují a odebírají přístupová práva podle zásady „potřeba vědět“, zásady minimálních práv a zásady oddělení funkcí;

b) zajistí, aby byla přístupová práva při ukončení nebo změně pracovního poměru odpovídajícím způsobem upravena;

c) zajistí, aby přístup k sítím a informačním systémům byl autorizován příslušnými osobami;

d) zajistí, aby přístupová práva vhodně řešila přístup třetích stran, jako jsou návštěvníci, dodavatelé a poskytovatelé služeb, zejména omezením rozsahu a doby trvání přístupových práv;

e) vedou registr udělených přístupových práv;

f) používají vedení protokolů pro správu přístupových práv.

11.2.3. Příslušné subjekty v plánovaných intervalech přezkoumávají přístupová práva a upravují je na základě organizačních změn. Příslušné subjekty zdokumentují výsledky přezkumu včetně nezbytných změn přístupových práv.

11.3. *Administrátorské účty a účty pro správu systému*

11.3.1. Příslušné subjekty udržují politiky pro správu administrátorských účtů a účtů pro správu systému jako součást politiky řízení přístupu uvedenou v bodě 11.1.

11.3.2. Politiky uvedené v bodě 11.3.1:

a) zavádějí silnou identifikaci, autentizaci, jako je např. vícefaktorová autentizace, a postupy schvalování pro administrátorské účty a účty pro správu systému;

b) zřizují specifické účty, které se budou používat výhradně pro operace správy systému, jako je instalace, konfigurace, správa nebo údržba;

c) v maximální možné míře individualizují a omezují oprávnění pro správu systému;

d) zajistí, aby se účty pro správu systému používaly pouze pro připojení k systémům pro správu systému.

11.3.3. Příslušné subjekty v plánovaných intervalech přezkoumávají přístupová práva administrátorských účtů a účtů pro správu systému, která upravují na základě organizačních změn, a výsledky přezkumu, včetně nezbytných změn přístupových práv, dokumentují.

11.4. *Systémy správy*

11.4.1. Příslušné subjekty omezí a řídí používání systémů pro správu systému v souladu s politikou řízení přístupu uvedenou v bodě 11.1.

11.4.2. Za tímto účelem příslušné subjekty:

a) používají systémy pro správu systému pouze pro účely správy systému, a nikoli pro jiné operace;

b) logicky oddělí tyto systémy od aplikačního softwaru, který se nepoužívá pro účely správy systému,

c) chrání přístup k systémům správy pomocí ověřování a šifrování.

11.5. *Identifikace*

11.5.1. Příslušné subjekty řídí celý životní cyklus identit sítí a informačních systémů a jejich uživatelů.

11.5.2. Za tímto účelem příslušné subjekty:

a) nastaví jedinečné identity pro sítě a informační systémy a jejich uživatele;

b) spojí identitu uživatelů s jedinou osobou;

c) zajistí dohled nad identitami sítí a informačních systémů;

d) použijí vedení protokolů pro řízení identit.

11.5.3. Příslušné subjekty povolí identitu přidělenou více osobám, například sdílenou identitu, pouze v případě, že je to nezbytné z obchodních nebo provozních důvodů a že jsou tyto případy podrobeny postupu a zdokumentování udělení výslovného souhlasu. Příslušné subjekty zohlední identity přidělené více osobám v rámci řízení rizik v oblasti kybernetické bezpečnosti uvedeném v bodě 2.1.

11.5.4. Příslušné subjekty pravidelně přezkoumávají identity sítí a informačních systémů a jejich uživatelů, a pokud již nejsou potřebné, neprodleně je deaktivují.

11.6. *Ověření*

11.6.1. Příslušné subjekty zavedou bezpečné ověřovací postupy a technologie založené na omezení přístupu a politice řízení přístupu.

11.6.2. Za tímto účelem příslušné subjekty:

a) zajistí, aby úroveň ověření odpovídala klasifikaci aktiva, k němuž má být poskytnut přístup;

b) kontrolují přidělování tajných ověřovacích údajů uživatelům a jejich správu postupem, který zajišťuje důvěrnost údajů, což zahrnuje i poskytování poradenství pracovníkům ohledně vhodného zacházení s ověřovacími údaji;

c) vyžadují změnu ověřovacích údajů na počátku, v předem stanovených intervalech a v případě podezření, že tyto údaje byly ohroženy;

d) vyžadují obnovení ověřovacích údajů a zablokování uživatelů po předem stanoveném počtu neúspěšných pokusů o přihlášení;

e) ukončí neaktivní relace po uplynutí předem stanovené doby nečinnosti a

f) vyžadují zvláštní ověřovací údaje pro přístup k administrátorskému přístupu nebo k účtu pro správu systému.

11.6.3. Příslušné subjekty v proveditelném rozsahu používají nejmodernější metody ověřování, a to v souladu se souvisejícím posouzeným rizikem a klasifikací aktiva, k němuž má být poskytnut přístup, a jedinečné ověřovací informace.

11.6.4. Příslušné subjekty v plánovaných intervalech přezkoumávají postupy a technologie ověřování.

11.7. *Vícefaktorová autentizace*

11.7.1. Příslušné subjekty zajistí, aby uživatelé byli při přístupu do sítě a informačních systémů subjektů ověřováni pomocí více autentizačních faktorů nebo mechanismů trvalé autentizace, případně v souladu s klasifikací aktiva, k němuž mají mít přístup.

11.7.2. Příslušné subjekty zajistí, aby úroveň ověření odpovídala klasifikaci aktiva, k němuž má být poskytnut přístup.

12. **Správa aktiv (čl. 21 odst. 2 písm. i) směrnice (EU) 2022/2555)**

12.1. *Klasifikace aktiv*

12.1.1. Pro účely čl. 21 odst. 2 písm. i) směrnice (EU) 2022/2555 příslušné subjekty stanoví stupně utajení všech aktiv, včetně informací, v oblasti působnosti svých sítí a informačních systémů pro požadovanou úroveň ochrany.

12.1.2. Pro účely bodu 12.1.1 příslušné subjekty:

a) stanoví systém stupňů utajení aktiv;

b) přiřadí všem aktivům stupeň utajení, a to na základě požadavků na důvěrnost, integritu, autenticitu a dostupnost, s cílem určit požadovanou ochranu podle jejich citlivosti, kritičnosti, rizika a obchodní hodnoty;

c) uvedou do souladu požadavky na dostupnost aktiv a cíle v oblasti poskytování a obnovy stanovené v jejich plánu kontinuity a obnovy provozu po havárii.

12.1.3. Příslušné subjekty provádějí pravidelné přezkumy stupňů utajení aktiv a v případě potřeby je aktualizují.

12.2. *Zacházení s aktivy*

12.2.1. Příslušné subjekty vytvoří, zavedou a uplatňují politiku správného zacházení s aktivy, včetně informací, která je v souladu s jejich politikou bezpečnosti sítí a informací, a sdělí politiku správného nakládání s aktivy všem, kteří aktiva používají nebo s nimi nakládají.

12.2.2. Tato politika:

a) pokrývá celý životní cyklus aktiv, včetně pořízení, používání, uchovávání, přepravy a likvidace;

b) poskytuje pravidla bezpečného používání, bezpečné skladování, bezpečnou přepravu a nevratné vymazání a zničení aktiv.

c) stanoví, že převod se uskuteční bezpečným způsobem v souladu s typem převáděného aktiva.

12.2.3. Příslušné subjekty tuto politiku přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při výskytu významných incidentů nebo významných změn operací či rizik.

12.3. *Politika týkající se vyměnitelných médií*

12.3.1. Příslušné subjekty stanoví, zavedou a uplatňují politiku správy vyměnitelných paměťových médií a sdělí ji svým zaměstnancům a třetím stranám, které s vyměnitelnými paměťovými médii nakládají v prostorách příslušných subjektů nebo na jiných místech, kde jsou vyměnitelná média připojena k sítím a informačním systémům příslušných subjektů.

12.3.2. Tato politika:

a) stanoví technický zákaz připojení vyměnitelných médií, pokud pro použití neexistují organizační důvody;

b) zajistí, aby bylo zakázáno samospouštění z takových médií a aby byla média před jejich použitím v systémech příslušných subjektů prověřována na přítomnost škodlivého kódu;

c) poskytuje opatření pro zajištění kontroly a ochrany přenosných paměťových zařízení obsahujících data při přepravě a skladování;

d) v případě potřeby stanoví opatření pro použití kryptografických technik s cílem chránit údaje na vyměnitelných paměťových médiích.

12.3.3. Příslušné subjekty tuto politiku přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při výskytu významných incidentů nebo významných změn operací či rizik.

12.4. *Soupis aktiv*

12.4.1. Příslušné subjekty vypracují a udržují úplný, přesný, aktuální a ucelený soupis svých aktiv. Dohledatelným způsobem zaznamenávají změny položek v soupisu.

12.4.2. Podrobnost soupisu aktiv by měla být na úrovni odpovídající potřebám příslušných subjektů. Soupis obsahuje:

a) seznam operací a služeb a jejich popis;

b) seznam sítí a informačních systémů a dalších souvisejících aktiv podporujících operace a služby příslušných subjektů.

12.4.3. Příslušné subjekty pravidelně přezkoumávají a aktualizují soupis a svá aktiva a dokumentují historii změn.

12.5. *Uložení, vrácení nebo smazání aktiv po ukončení pracovního poměru*

Příslušné subjekty stanoví, zavedou a uplatňují postupy, které zajistí, aby jejich aktiva, která mají zaměstnanci v úschově, byla po skončení pracovního poměru uložena, vrácena nebo smazána, a zdokumentují uložení, vrácení a smazání těchto aktiv. Pokud uložení, vrácení nebo vymazání aktiv není možné, příslušné subjekty zajistí, aby aktiva již neměla přístup do sítě a informačních systémů příslušných subjektů v souladu s bodem 12.2.2.

13. **Environmentální a fyzická bezpečnost (čl. 21 odst. 2 písm. c), e) a i) směrnice (EU) 2022/2555)**

13.1. *Podpůrné služby*

13.1.1. Pro účely čl. 21 odst. 2 písm. c) směrnice (EU) 2022/2555 příslušné subjekty zabrání ztrátě, poškození nebo ohrožení sítí a informačních systémů nebo přerušení jejich provozu v důsledku selhání a narušení podpůrných služeb.

13.1.2. Za tímto účelem příslušné subjekty v případě potřeby:

a) chrání zařízení před výpadky napájení a dalšími narušeními způsobenými výpadky podpůrných služeb, jako jsou elektřina, telekomunikace, dodávky vody, plynu, kanalizace, ventilace a klimatizace;

b) zváží využití redundance v oblasti veřejných služeb;

c) chrání služby v oblasti elektřiny a telekomunikací, které přenášejí data nebo zásobují sítě a informační systémy, proti přerušení a poškození;

d) sleduje služby uvedené v písmenu c) a oznamuje příslušným interním nebo externím pracovníkům události, které překračují minimální a maximální prahové hodnoty kontroly uvedené v bodě 13.2.2 písm. b) a které ovlivňují tyto služby;

e) uzavírají smlouvy na nouzové dodávky s odpovídajícími službami, například pokud jde o pohonné hmoty pro nouzové zásobování elektřinou;

f) zajišťují trvalou účinnost, sledují, udržují a testují dodávky pro sítě a informační systémy nezbytné pro provoz nabízené služby, zejména v oblasti elektrické energie, regulace teploty a vlhkosti, telekomunikací a internetového připojení.

13.1.3. Příslušné subjekty pravidelně nebo po významných incidentech nebo významných změnách operací či rizik tato ochranná opatření testují, přezkoumávají a v případě potřeby aktualizují.

13.2. *Ochrana před fyzickými a environmentálními hrozbami*

13.2.1. Pro účely čl. 21 odst. 2 písm. e) směrnice (EU) 2022/2555 příslušné subjekty na základě výsledků posouzení rizik provedeného podle bodu 2.1 předcházejí následkům událostí, které mají původ ve fyzických a environmentálních hrozbách, jako jsou přírodní katastrofy a jiné úmyslné nebo neúmyslné hrozby, nebo následky těchto událostí omezují.

13.2.2. Za tímto účelem příslušné subjekty v případě potřeby:

a) navrhují a provádějí ochranná opatření proti fyzickým a environmentálním hrozbám;

b) stanoví minimální a maximální prahové hodnoty kontrol pro fyzické a environmentální hrozby;

c) sledují parametry prostředí a oznamují příslušným interním nebo externím pracovníkům události, kdy jsou překračovány minimální a maximální prahové hodnoty kontrol uvedené v písmenu b).

13.2.3. Příslušné subjekty pravidelně nebo po významných incidentech nebo významných změnách operací nebo rizik testují, přezkoumávají a v případě potřeby aktualizují ochranná opatření proti fyzickým a environmentálním hrozbám.

13.3. *Kontrola vnějšího a fyzického přístupu*

13.3.1. Pro účely čl. 21 odst. 2 písm. i) směrnice (EU) 2022/2555 příslušné subjekty předcházejí neoprávněnému fyzickému přístupu k sítím a informačním systémům, jejich poškození a zásahům do nich a předešle uvedené sledují.

13.3.2. Za tímto účelem příslušné subjekty:

a) na základě posouzení rizik provedeného podle bodu 2.1 stanoví a používají bezpečnostní zóny s cílem chránit oblasti, kde se nacházejí sítě a informační systémy a další související aktiva;

b) chrání oblasti uvedené v písmenu a) vhodnými kontrolami vstupu a přístupovými body;

c) navrhují a provádějí fyzické zabezpečení kanceláří, místností a zařízení;

d) průběžně monitorují své prostory, zda v nich nedochází k neoprávněnému fyzickému přístupu.

13.3.3. Příslušné subjekty opatření ke kontrole fyzického přístupu testují, přezkoumávají a v případě potřeby aktualizují pravidelně nebo po významných incidentech nebo významných změnách operací nebo rizik.