Prováděcí nařízení komise (EU) 2024/2690
Regulace poskytovatelů digitálních služeb

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Online přednáška portal.nukib.gov.cz

Jiří Bakala
Petr Hrachy
odbor kontroly

Informace na úvod

Tento materiál slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů.
Tento materiál se primárně zaměřuje na oblast bezpečnostních opatření pro poskytovatele digitálních služeb.

Shrnutí situace

Zákon o kybernetické bezpečnosti byl 4. srpna 2025 publikován ve Sbírce zákonů jako zákon č. 264/2025 Sb., a účinnosti nabyde 1. listopadu 2025

- Prováděcí nařízení komise 2024/2690 platné od 7.11.2024, stanoví pravidla pro uplatňování požadavků zejména **čl. 21 odst. 2 čl. 23 odst. 3 NIS2**
- Dokud však nebude účinný nový zákon o kybernetické bezpečnosti, není pro nikoho závazné
- Požadavky se **v mnohém shodují s požadavky vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (PRS-V)**
- Prováděcí nařízení je v této prezentaci porovnáno k **PRS-V**
- **Poskytovatelé digitálních služeb budou zavádět pouze vhodná a přiměřená bezpečnostní opatření** (výběr vhodných a přiměřených opatření se provede na základě výsledků hodnocení rizik)
- Prováděcí nařízení používá pojem **technické a metodické požadavky**
- PRS – V používá **bezpečnostní opatření**
- K prováděcímu nařízení je vydán **Technical Implementation Guidance,** který je dostupný na stránkách ENISA v anglickém znění

Poskytovatelé digitálních služeb

- 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**
- Poskytovatele služeb **vytvářejících důvěru**

Struktura bezpečnostních opatření nařízení komise 2024/2690

- Politika bezpečnosti sítí a informačních systémů
- Politika řízení rizik
- Řešení incidentů
- Kontinuita podnikání a krizové řízení
- Bezpečnost dodavatelského řetězce
- Zabezpečení pořizování, vývoje a údržby sítí a informačních systémů
- Politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik
- Základní postupy v oblasti kybernetické hygieny a bezpečnostní školení
- Kryptografie
- Bezpečnost lidských zdrojů
- Kontrola přístupu
- Správa aktiv
- Environmentální a fyzická bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost, TLP:CLEAR

Zdroj obr.: ENISA

Figure 1: Technical and methodological requirements of the cybersecurity risk-management measures (Annex to Commission Implementing Regulation 2024/2690)

Politika bezpečnosti sítí a informačních systémů

- Politika bezpečnosti sítí a informačních systémů
  - Jiný pojem, ale pořád se jedná o obecné stanovení systému řízení bezpečnosti informací
  - Závazek k neustálému zlepšování a zajištění dostupných zdrojů
  - Stanovení **seznamu dokumentace a politik**
  - Pravidelný přezkum bezpečnostní politiky
  - Výsledky přezkumů se musí **dokumentovat**
- Úkoly, odpovědnosti a pravomoci
  - **Nejsou přímo stanoveny bezpečnostní role**, ale minimálně podřízena jedna osoba řídícím orgánům
  - Dodržování bezpečnostní politiky od zaměstnanců a třetích stran

- Systém řízení bezpečnosti informací (SŘBI)
- Požadavky na vrcholné vedení
  - Zajištění potřebných zdrojů
- Řízení bezpečnostní politiky a bezpečnostní dokumentace
  - Stanovení bezpečnostní politiky a vedení relevantní bezpečnostní politiky a bezpečnostní dokumentace k opatřením v § 4 až 28
  - Pravidelný přezkum bezpečnostní politiky a bezpečnostní dokumentace
- Bezpečnosti lidských zdrojů
- Stanovení bezpečnostních rolí

Politika řízení rizik I.

- Rámec pro řízení rizik
  - Určení vhodného rámce pro vhodnou identifikaci rizik (určení postupů pro identifikaci, analýzu, posouzení a ošetření rizik)
  - **Plán ošetření rizik** - obsahující zavedené i nezavedené opatření
  - **Zbytková rizika** schvalují odpovědné osoby, ty vypracují zprávu ve které informují své řídící orgány
  - Poskytovatel regulované služby:
  - **Postupuje dle metodiky pro řízení rizik**; stanový úrovně tolerance zbytkového rizika s ohledem na risk apetite; určuje kritéria rizik (určování hodnocení, vazby, akceptovatelnost)
  - **Zohledňuje výsledky posouzení rizik**, výsledky postupů pro zhodnocení účinnosti opatření, náklady na provedení ve vztahu k očekávánému přínosu.
  - Posouzení rizik a plán ošetření rizik je **dle potřeby přezkoumáván**.

- Řízení aktiv
  - stanoví metodiku pro určování a hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik
  - Určuje a eviduje vazby mezi aktivy,
  - Provádí hodnocení rizik alespoň 1 ročně (z pohledu hrozeb a zranitelností) a zpracuje zprávu z hodnocení rizik
  - V souladu se stanovenými kritérii pro akceptovatelnost rizik zpracuje plán zvládání rizik
  - Zpracuje prohlášení o aplikovatelnosti
  - v souladu s plánem zvládání rizik zavádí bezpečnostní opatření.

Politika řízení rizik II.

- Sledování souladu
  - Pravidelný přezkum politik, informování vedení o stavu KB IS
  - Přezkum politik v pravidelných intervalech nebo po významných incidentech, nebo při v. změnách
- Zajištění nezávislého přezkumu KB
  - Osobou s odbornou kvalifikací pro audit
  - Zajistí nezávislý přezkum přístupu k řízení KB (z pohledu lidí, procesů, technologií)
  - Veškeré výsledky přezkumů či měření se prezentují vrcholnému vedení, včetně výsledků sledování souladu
  - Na jejich základě se následně přijmou nápravná opatření nebo se akceptují zbytková rizika dle Vámi určených kritérií pro akceptovatelnost zbytkových rizik.

- Systém řízení bezpečnosti informací
  - Pravidelné vyhodnocuje ISMS alespoň jednou ročně
  - Na jeho základě zpracuje zprávu z přezkumu ISMS
- Požadavky na vrcholové vedení
  - Seznamuje se se zprávou o přezkumu ISMS
- Řízení aktiv
  - Provádí hodnocení rizik v pravidelných intervalech
  - Zpracuje zprávu o hodnocení rizik
- Provádí audit kybernetické bezpečnosti
  - Výsledky auditu zohlední v AR a na jejím základě stanoví nápravná opatření

Řešení incidentů

- Politika řešení incidentů
  - Musí být v souladu s plánem kontinuity provozu a plánem pro obnovu po havárii
- Monitorování a vedení protokolů
  - Jedná se o klasickou detekci a zaznamenávání/logování činností
  - **Protokoly = logy**
- Oznamování událostí
- Hodnocení a klasifikace událostí
  - Posoudit podezřelé události, aby určily, zda se jedná o incidenty, a pokud ano, určí jejich povahu a závažnost
- Reakce na incident
  - Reagovat na incidenty včas a v souladu se zdokumentovanými postupy
- Přezkumy po incidentu

- Zvládání kybernetických bezpečnostních událostí a incidentů
  - Zavedení procesů, pravidel a postupů pro koordinaci a zvládání KBI
- Řízení kontinuity činností
- Detekce kybernetických bezpečnostních událostí
  - Využití nástroje pro KBU
- Zaznamenávání událostí
- Vyhodnocování kybernetických bezpečnostních událostí
  - Využití nástroje pro nepřetržité vyhodnocování KBU a jejich vyhodnocování s cílem identifikace KBI

Kontinuita podnikání a krizové řízení

- Plán kontinuity provozu a obnovy provozu po havárii
  - Stanoví a udržuje **Plán kontinuity provozu a obnovy po havárii** pro případy incidentů
  - Plán obnovy je vytvořen v souvislosti s výsledky posouzení rizik
  - Plán musí obsahovat specifické požadavky (úkoly, povinnosti, kontaktní osoby, podmínky aktivace a deaktivace plánu. Požadované zdroje, **postup záloh, redundance** apod.)
- Je nutné mít také **analýzu obchodního dopadu** (potencionálního) a na základě jejího výsledku stanovit požadavky na zachování provozu.
- Plány se testují a výsledku reflektují v **postupech krizového řízení**
- S ohledem na výstupy provedené AR zajistí dostatečnou dostupnost / redundanci těchto zdrojů: sítí a inf. systémů, aktiv (zařízení, vybavení), zaměstnanců s potřebnou odpovědností…

- Řízení kontinuity činností
  - Stanovení metodiky pro provedení analýzy dopadů
  - Z pohledu možných dopadů na poskytování reg. Služby
  - Stanovení přijatelné minimální úrovně poskytovaných služeb (SLA) a stanovení přiměřené doby obnovy chodu
  - Stanoví politiku řízení konítinuity činnosti
  - uvedené provádí na základě výstupů analýzy dopadů a hodnocení rizik
  - Aktualizuje a testuje jednotlivé postupy.

Bezpečnost dodavatelského řetězce

- Politika bezpečnosti dodavatelského řetězce
  - **Žádný významný dodavatel – aplikace nutná na všechny dodavatele**
  - Stanoví **kritéria pro výběr dodavatelů a poskytovatelů** služeb a uzavírání smluv s nimi
  - Při vytváření politiky bezpečnosti dodavatelského řetězce v příslušných případech **zohlední výsledky koordinovaného posouzení bezpečnostních rizik** kritických dodavatelských řetězců
  - Detailní popis co mají obsahovat smlouvy s dodavateli a poskytovateli služeb
- Seznam dodavatelů a poskytovatelů služeb
  - Vést a průběžně aktualizovat registr svých přímých dodavatelů a poskytovatelů služeb

- Řízení dodavatelů
  - Stanoví pravidla pro dodavatele zohledňující SŘBI
  - Seznámení dodavatelů s pravidly SŘBI
  - Řídí rizika spojená s dodavateli

Zabezpečení pořizování, vývoje a údržby sítí a informačních systémů I.

- Zabezpečení pořizování služeb IKT nebo produktů IKT
  - Stanoví procesy řízení rizik **kritických** pro zajištění **CIA IKT**
  - Stanoví **bezpečností požadavky** vztahující se **k pořizování IKT** a k zajištění aktualizací v průběhu životního cyklu
  - Zavede metody při kterých ověří zda dodané IKT splňují stanovené bezpečnostní požadavky
- Životní cyklus bezpečného vývoje
  - Stanoví bez. požadavky **pro vývoj sítí a informačních systémů**
  - Stanovení bezp. požadavků pro **životní cyklus vývoje** včetně jeho průběžného testování
- Správa konfigurace
  - Opatření vedoucí k vytvoření, zavedení a monitorování konfigurací, včetně jejich vynucování
  - Přezkum aktualizace (při významné změně nebo incidentu)

- Akvizice vývoj, údržba
  - Řídí rizika, řídí významné změny, zahrnuje bez. požadavky do akvizice, vývoje a údržby.
  - Dostupnost aktualizací po dobu životního cyklu IKT.
- Řízení dodavatelů
  - Stanoví pravidla pro dodavatele zohledňující SŘBI
- Zajišťování dostupnosti regulované služby
  - Ochranu ukládaných záloh a dat v nich obsažených před narušením jejich dostupnosti
  - Zajistí bezpečnou správu konfigurací a nastavení technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik

Zabezpečení pořizování, vývoje a údržby sítí a informačních systémů II.

- Řízení změn, opravy a údržba
  - Příslušné subjekty uplatňují postupy řízení změn
  - Pokud nebylo možné dodržet standardní **postupy řízení změn z důvodu mimořádné události, příslušné subjekty zdokumentují výsledek změny a vysvětlení, proč nebylo možné postupy dodržet.**
  - Postupy zajistí, aby změny byly zdokumentovány a na základě posouzení rizik byly před provedením testovány a posouzeny z hlediska možného dopadu.
- Testování bezpečnosti (s ohledem na AR)
- Řízení bezpečnostních záplat (testování jen u kritických aktiv)
- Bezpečnost sítí
- Segmentace sítě
- Ochrana před škodlivým a neautorizovaným softwarem
- Řešení zveřejňování zranitelností

- Řízení změn
- Aplikační bezpečnost
  - Užívá technická aktiva, která jsou výrobcem, dodavatelem nebo jinou osobou podporována a zajistí bezodkladné aplikování schválených bezpečnostních aktualizací vydaných pro tato aktiva .
  - Provádí pravidelné skenování zranitelnosti technických aktiv regulované služby a penetrační testování technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik
- Bezpečnost komunikačních sítí
  - Zajistí a dokumentuje segmentaci komunikační sítě, včetně oddělení provozního, zálohovacího, vývojového, testovacího, administrátorského a jiného specifického prostředí
  - Dokumentuje topologii sítě a infrastruktury
  - zajistí řízení vzdálené správy technických aktiv a vzdáleného přístupu ke komunikační síti
- Detekce KBU

Politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik

- Přezkum a vyhodnocování účinnosti zavedeného SŘBI
- 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
- Politika a postupy zohledňují výsledky posouzení rizik a minulé významné incidenty
  - Následuje detailní výčet co je potřeba určit
- Politiku a postupy přezkoumávají a v případě potřeby aktualizovat v plánovaných intervalech a při významných incidentech nebo významných změnách operací či rizik

- Systém řízení bezpečnosti informací
  - Vyhodnocení účinnosti SŘBI
- Řízení bezpečnostní politiky a bezpečnostní dokumentace
  - Pravidelný přezkum bezpečnostní politiky a bezpečnostní dokumentace

Základní postupy v oblasti kybernetické hygieny a bezpečnostní školení

- Zvyšování povědomí a základní postupy kyb. hygieny
  - Všichni zaměstnanci, dodavatelé, řídící orgány mají povinnost absolvovat školení
  - Vypracuji tzv. **program zvyšování informativnosti**:
    - Plánovaní
    - Vytvořen v souladu s **politikou informační bezpečnosti** a se schválenými postupy bezpečnosti sítí a informací
    - Zahrnuje relevantní kyber. hrozby
    - Testuje je se jeho účinnost / aktuálnost.
- Bezpečnostní školení
  - **Program školení je použitý v souladu s politikou bezpečnosti sítí a informací**.
  - Informování o hrozbách
  - Jak postupovat v případě bezpečnostní události

- Bezpečnost lidských zdrojů
  - Plán rozvoje bezpečnostního povědomí
  - Poučení uživatelů, administrátorů a bezpečnostních rolí
  - Potřebná teoretická i praktická školení
  - Pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní
  - Určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role

Kryptografie

- 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
- Politika a postupy stanoví přístup k řízení klíčů:
  - Přístup k řízení klíčů, včetně případných metod je více detailní

- Kryptografické algoritmy
  - Použití pouze aktuálně odolných kryptografických algoritmů
  - Prosazování bezpečného nakládání s kryptografickými algoritmy
- Řízení bezpečnostní politiky a bezpečnostní dokumentace
  - Pravidelný přezkum bezpečnostní politiky a bezpečnostní dokumentace

Bezpečnost lidských zdrojů I.

- Bezpečnost lidských zdrojů
  - **Cílí na vytvoření mechanismů** aby členové vrcholného vedení, zaměstnanci, přímý dodavatelé, administrátoři s privilegovaným přístupem **porozuměli** a **dodržovali stanovené postupy kybernetické hygieny a aby vrcholné vedení a privilegování administrátoři znali své úkoly, pravomoci a odpovědnosti v oblasti bezpečnosti IKT**
- Ověření spolehlivosti
  - Zavedou kritéria, která stanoví, které úkoly, odpovědnosti a pravomoci mohou vykonávat pouze osoby, jejichž spolehlivost byla ověřena (vytvoření politik)
  - **Při ověření spolehlivosti osob, se zohledňují platné zákony a etické zásady úměrně k obchodním požadavkům**, ke klasifikaci aktiv, 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

- Bezpečnost lidských zdrojů
  - s ohledem na stav a potřeby systému řízení bezpečnosti informací stanoví plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí včetně formy, obsahu a rozsahu poučení a školení
  - zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role,
- Řízení přístupů
  - Provádí pravidelné přezkoumání veškerých přístupových práv a oprávnění
    včetně rozdělení do
    skupin a rolí

Bezpečnost lidských zdrojů II.

- Postup při ukončení nebo změně pracovního poměru
  - 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.
- Disciplinární řízení
  - **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 – přezkum postupů

- Vrcholné vedení
  - Zajistí, aby byla zachována mlčenlivost u všech relevantních osob (zejména administrátorů, osob zastávajících bezpečnostní role a dodavatelů)
- Řízení bezpečnostní politiky a bezpečnostní dokumentace
  - Pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci, zajistí jejich aktuálnost a zohlednění jejich relevantních oblastí v provozních pravidlech a postupech a další dokumentaci.
- Bezpečnost lidských zdrojů
  - určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role

Kontrola přístupu

- Postup kontroly přístupu
  - Jiný pojem, ale jedná se o **řízení přístupu**
- Správa přístupových práv
- Administrátorské účty a účty pro správu systému
- Systémy správy
  - Logicky oddělí tyto systémy od aplikačního softwaru, který se nepoužívá pro účely správy systému
- Identifikace
  - Použijí vedení protokolů pro řízení identit
  - Sdílená identita
- Ověření = **autentizace**
  - Zajistí, aby úroveň ověření odpovídala klasifikaci aktiva, k němuž má být poskytnut přístup;
- Vícefaktorová autentizace

- Řízení přístupu
  - Na základě bezpečnostních a provozních potřeb řídí přístup k aktivům a přijímá bezpečnostní opatření
- Bezpečnost komunikačních sítí
- Správa a ověřování identit
  - Vícefaktorová autentizace
- Zaznamenávání událostí
  - Na základě hodnocení aktiv a bezpečnostních potřeb určí technická aktiva, u kterých je zaznamenávání bezpečnostních a relevantních provozních událostí prováděno
- Řízení bezpečnostní politiky a bezpečnostní dokumentace

Správa aktiv I.

- Klasifikace aktiv
  - Stanoví **stupně utajení** aktiv
- Zacházení s aktivy
  - **Zavedou a uplatňují politiku správného zacházení s aktivy**, včetně informací, v souladu s jejich politikou bezpečnosti sítí a informací, **a sdělí politiku správného nakládání s aktivy všem, kteří aktiva používají nebo s nimi nakládají**
- Politika týkající se vyměnitelných medií
  - Uplatňují politiku správy vyměnitelných paměťových médií a sdělí ji svým zaměstnancům a třetím stranám, které s vyměnitelnými paměťovými médii nakládají
  - V **případě potřeby stanoví opatření pro použití kryptografických technik** s cílem chránit údaje na vyměnitelných paměťových médiích

- Řízení aktiv
  - Pro úrovně aktiv stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jejich důvěrnosti, integrity a dostupnosti, která obsahují zejména:
    - přípustné způsoby používání aktiv, pravidla pro jejich manipulaci, klasifikaci informací a označování aktiv, pro bezpečné elektronické sdílení, pravidla správy výměnných medií
- Řízení bezpečnostní politiky a bezpečnostní dokumentace
  - Povinná osoba stanoví bezpečnostní politiku ve vztahu k řízení kybernetické bezpečnosti a vede relevantní bezpečnostní politiku a bezpečnostní dokumentaci k opatřením uvedeným v § 4 až 28
- Detekce kybernetických bezpečnostních událostí
- Řízení a sledování používání vyměnitelných zařízení a datových nosičů,

Správa aktiv II.

- Soupis aktiv
  - Vypracují a udržují úplný, přesný, aktuální a ucelený soupis svých aktiv. Dohledatelným způsobem zaznamenávají změny položek v soupisu.
  - Soupis obsahuje:
    - seznam operací a služeb a jejich popis
    - seznam sítí a informačních systémů a dalších souvisejících aktiv podporujících operace a služby
- Uložení, vrácení, smazání aktiv po ukončení pracovního poměru
  - 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.

- Stanovení rozsahu řízení kybernetické bezpečnosti (§ 12 nZKB)
  - Určení aktiv souviseních s poskytováním regulované služby
    - a) určí všechna svá primární aktiva
    - b) posoudí zda primární aktiva souvisí s poskytováním regulované služby
    - U primárních aktiv podle písm. b) určí podpůrná aktiva
  - Eviduje aktiva, která jsou součástí stanoveného rozsahu, a primární aktiva, která byla ze stanoveného rozsahu vyjmuta, včetně důvodů jejich vyjmutí.
  - Stanovený rozsah je poskytovatel regulované služby povinen pravidelně přezkoumávat a aktualizovat.

Environmentální a fyzická bezpečnost

- Podpůrné služby
  - Zabrání **ztrátě, poškození nebo ohrožení sítí a informačních systémů nebo přerušení** jejich provozu v důsledku selhání a narušení podpůrných služeb
  - Pravidelně nebo po významných incidentech nebo významných změnách operací či rizik tato ochranná opatření testují, přezkoumávají a v případě potřeby aktualizují
- Ochrana před fyzickými a environmentálními hrozbami
  - Na **základě výsledků posouzení rizik** 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
- Kontrola vnějšího a fyzického přístupu

- Fyzická bezpečnost
  - Předchází poškození, krádeži, neoprávněným zásahům a zneužití aktiv
- Zvládání kybernetických bezpečnostních událostí a incidentů
- Řízení kontinuity činností
- Zajišťování dostupnosti regulované služby
  - Vůči hrozbám a zranitelnostem, které by mohly snížit její dostupnost
- Řízení rizik
  - Určuje relevantní hrozby a zranitelnosti

Závěrem

- V případech, kdy poskytovatele digitálních služeb z důvodu **své velikosti nemohou splnit některé technické a metodické požadavky** na opatření k řízení kybernetických bezpečnostních rizik **mají možnost přijmout jiná kompenzační opatření, která jsou vhodná k dosažení účelu těchto požadavků**

- **BO stanovené nařízením se uplatňují tam, kde je to vhodné, použitelné a proveditelné**, v opačných případech, kdy tomu tak není, a nedojde k jejich uplatnění, je nutné tuto skutečnost srozumitelně odůvodnit a zdokumentovat

- Poskytovatelé digitálních služeb **při provádění a uplatňování BO zajistí úroveň bezpečnosti sítí a informačních systémů odpovídající existujícím rizikům**, proto mají náležitě zohlednit míru svého vystavení rizikům, svoji velikost a pravděpodobnost výskytu incidentů, jejich možnou závažnost, včetně možného společenského a hospodářského dopadu

- *Požadavky na opatření k řízení kybernetických bezpečnostních rizik jsou pro příslušné subjekty stanoveny v příloze prováděcího nařízení*

Děkujeme za pozornost

https://portal.nukib.gov.cz/

regulace@nukib.gov.cz