

BEZPEČNOSTNÍ OPATŘENÍ DLE nZKB

Vyhlášky o kybernetické bezpečnosti – nižší povinnosti v kontextu obcí

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

3. prosince 2024, Ostrava

TLP:CLEAR

Pavel Mazánek
Odbor kontroly



UPOZORNĚNÍ:

Transpozice NIS2 do českého právního řádu není finalizována.
Informace obsažené v této prezentaci se mohou změnit v rámci legislativního procesu.

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



- Představení
- Východiska obsahu návrhu vyhlášek
- Změny spojené s transpozicí evropské směrnice NIS2
- Režim nižších povinností
- Specifika obcí
- Prostor pro dotazy



- Vedoucí oddělení kontroly II – technický specialista
- Provádění auditů a kontrol
- Metodická podpora – zejména výklad VKB
- Transpozice NIS2 – bezpečnostní opatření pro vyšší a nižší režim (vyhlášky)



Směrnice NIS 2.0

Transpozice
směrnice 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

Zlepšení a zkušenosti

Reflexe poznatků a
dosavadních zkušeností,
odstranění současných
nedostatků, zohlednění
podnětů
a připomínek a další doplňující
úpravy

Mezinárodní standardy a normy

Mezinárodní standardy a
normy zejména z řady norem
ISO/IEC 27000, NIST atd.

Povinnosti nZKB

Povinnosti plynoucí ze znění
nového zákona o kybernetické
bezpečnosti



- 2 režimy (nižší, vyšší) → 2 vyhlášky o kybernetické bezpečnosti
- Nižší režim povinností
 - Zaměřeno na nejstěžejnější oblasti řízení KB
 - Snížení personální, administrativní a technické zátěže
 - Princip přiměřenosti
 - Stěžejní dokument
- Vyšší režim povinností
 - Obdobné jako stávající VKB
- Povinnosti vrcholného vedení (větší důraz)



Režim nižších povinností



1. Obec s rozšířenou působností = nově povinná osoba dle nZKB = povinnost „Zaregistrovat se“ na portálu NÚKIB
 - už teď doporučuji seznámit se s prostředím portálu a podpůrnými materiály na něm
2. Určení rozsahu dle instrukcí v nZKB
 - vzniká podpůrný materiál **přímo pro obce** „jak na určení rozsahu a dál“
3. Plnění dalších dílčích povinností z nZKB a jeho prováděcích vyhlášek (v určeném rozsahu dle bodu 2)
 - v této prezentaci si projdeme stěžejní povinnosti specifické pro nižší režim, zejména ty „neopominutelné“
 - vzniká podpůrný materiál pro nižší režim „jak na zavádění bezpečnostních opatření v nižším režimu“

§ 4 Systém zajišťování minimální kybernetické bezpečnosti

(1) Povinná osoba v rámci zajišťování kybernetické bezpečnosti

- a) zavede a provádí přiměřená bezpečnostní opatření zohledňující bezpečnostní potřeby organizace.
- b) vždy zavede a provádí **alespoň bezpečnostní opatření podle § 4 odstavce 2 až odstavce 7, § 5, § 6, § 7 a § 11.**

(2) Povinná osoba

- a) zpracuje **přehled bezpečnostních opatření** požadovaných touto vyhláškou podle přílohy č. 1, který obsahuje alespoň
 - 1. přehled všech bezpečnostních opatření, která byla povinnou osobou zavedena, včetně popisu jejich zavedení,
 - 2. přehled všech bezpečnostních opatření, která budou povinnou osobou zavedena, včetně termínů pro jejich zavedení, priority jejich zavedení, určení osoby odpovědné za jejich zavedení a
 - 3. přehled všech bezpečnostních opatření, která nebyla zavedena, včetně odůvodnění jejich nezavedení,
- b) **alespoň jednou ročně** provede a dokumentuje vyhodnocení účinnosti zavedených bezpečnostních opatření, včetně aktualizace přehledu bezpečnostních opatření,
- c) **uchovává** jednotlivé přehledy bezpečnostních opatření, alespoň **po dobu 4 let.**

Přehled bezpečnostních opatření



Vyhodnocení účinnosti zajišťování kybernetické bezpečnosti					2023
Bezpečnostní opatření dle vyhlášky	Stav bezpečnostního opatření	Popis bezpečnostního opatření	Termín zavedení bezpečnostního opatření	Priorita zavedení bezpečnostního opatření	Odpovědnost za bezpečnostní opatření
§ 6 písm. a)	zavedeno	Politika bezpečného chování uživatelů je v dokumentu Bezp_lidskych_zdroju v kapitole „1 - Politika bezpečného chování uživatelů“ a jsou v ní zohledněna relevantní témata z přílohy č. 4	-	-	-
§ 6 písm. b)	zavedeno	Pravidla rozvoje bezpečnostního povědomí v dokumentu Bezp_lidskych_zdroju v kapitole „2 - Rozvoj bezpečnostního povědomí“, kde jsou také pravidla pro tvorbu hesel v podkapitole „2.1. Pravidla pro tvorbu hesel“	-	-	-
§ 9 odst. 2	v procesu	V současnosti společnost zavádí vícefaktorovou autentizaci.	Q3 2024	1	Petr Horák (IT oddělení)

§ 4 Systém zajišťování minimální kybernetické bezpečnosti

(3) Povinná osoba určí osobu odpovědnou za kybernetickou bezpečnost, která v oblasti kybernetické bezpečnosti odpovídá za řízení a rozvoj kybernetické bezpečnosti, dohled nad stavem kybernetické bezpečnosti a komunikaci s vrcholným vedením, přičemž pověřena může být osoba, která pro tuto činnost

- a) bez zbytečného odkladu absolvuje odborné školení podle § 6 písm. g) nebo
- b) prokáže odbornou způsobilost v oblasti kybernetické bezpečnosti.

(4) Povinná osoba v rámci zajišťování kybernetické bezpečnosti řídí bezpečnostní politiku a bezpečnostní dokumentaci

- a) vytvoří a schválí relevantní bezpečnostní politiku a vede relevantní bezpečnostní dokumentaci k opatřením uvedeným v § 4 až 14.
- b) pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci a zajišťuje jejich aktuálnost.
- c) dodržuje a vynucuje dodržování pravidel a postupů stanovených v bezpečnostní politice a bezpečnostní dokumentaci podle odst. 4 písm. a).

§ 4 Systém zajišťování minimální kybernetické bezpečnosti

(5) Povinná osoba v návaznosti na stanovení rozsahu řízení kybernetické bezpečnosti podle § 13 zákona, dále v rámci řízení aktiv stanoví a **zavádí pravidla ochrany a přípustné způsoby používání aktiv**.

- Povinnost určení primárních aktiv vyplývá z § 12 odst. 2 nZKB

(6) Povinná osoba při uzavírání **smlouvy s dodavateli** zajistí, aby smlouvy s těmito dodavateli obsahovaly relevantní oblasti uvedené v **příloze č. 2 k této vyhlášce**.

(7) Povinná osoba v souvislosti s plánovanou **akvizicí, vývojem a údržbou** technických aktiv stanoví **bezpečnostní požadavky v oblasti kybernetické bezpečnosti** a vymáhá jejich dodržování, přičemž vychází zejména z požadavků na bezpečnostní opatření podle této vyhlášky.



Vrcholné vedení s ohledem na zajišťování kybernetické bezpečnosti

- a) je **prokazatelně poučeno** o jeho **povinnostech** a rozsahu **odpovědností**,
- b) prokazatelně **absolvuje školení** podle § 6 písm. c),
- c) zajistí **dostupnost zdrojů potřebných** pro zajišťování kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření a
- d) se **prokazatelně seznamuje se** stavem plnění bezpečnostních opatření podle **přehledu bezpečnostních opatření** podle § 4 odst. 2 písm. a).



Povinná osoba v rámci bezpečnosti lidských zdrojů

- a) stanoví **politiku bezpečného chování uživatelů**, v rámci které zohledňuje relevantní témata uvedená v **příloze č. 3** této vyhlášky,
- b) stanoví pravidla rozvoje bezpečnostního povědomí uživatelů, administrátorů a osoby odpovědné za kybernetickou bezpečnost, včetně **pravidel pro tvorbu hesel dle § 9**,
- c) zajistí **poučení vrcholného vedení o jeho povinnostech, o bezpečnostní politice** zejména v oblasti zajišťování kybernetické bezpečnosti formou **vstupních a pravidelných školení**,
- d) v souladu s pravidly rozvoje bezpečnostního povědomí provádí **vstupní školení v oblasti kybernetické bezpečnosti**,
- e) v souladu s pravidly rozvoje bezpečnostního povědomí provádí **pravidelná školení v oblasti kybernetické bezpečnosti**,
- f) vede **přehledy o školeních a vede seznamy** osob podle písm. c) a d), které školení absolvovaly,
- g) zajistí potřebná **odborná teoretická i praktická školení administrátorů a osoby odpovědné za kybernetickou bezpečnost** v souladu s jejich pracovní náplní,
- h) zajistí **kontrolu dodržování bezpečnostní politiky** ze strany uživatelů, administrátorů a osoby odpovědné za kybernetickou bezpečnost a
- i) stanoví **pravidla a postupy pro řešení případů porušení bezpečnostní politiky**.



Povinná osoba v rámci řízení kontinuity činností

- a) u primárních aktiv stanoví jejich prioritu, pořadí a postupy jejich obnovy,
- b) stanoví dílčí odpovědnosti a povinnosti při obnově podle písm. a) a
- c) vytváří pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.



(1) Povinná osoba řídí přístup k aktivům, v rámci řízení přístupu

- a) přidělí každému **uživateli a administrátorovi přístupujícímu k aktivům přístupová práva a oprávnění na úroveň nezbytně nutnou k výkonu práce**, a **jedinečný identifikátor** daného typu účtu, přičemž **odděluje uživatelské a administrátorské účty jedné osoby**,
- b) **řídí identifikátory, přístupová práva a oprávnění účtů** technických aktiv,
- c) zavádí bezpečnostní opatření potřebná pro **bezpečné používání mobilních zařízení a jiných technických aktiv**, popřípadě i bezpečnostní opatření spojená s využitím technických aktiv, která povinná osoba nemá ve své správě,
- d) provádí **pravidelné přezkoumání nastavení** veškerých **přístupových práv a oprávnění**,
- e) zajistí **bezodkladné odebrání nebo změnu** přístupových práv a oprávnění **při změně pozice** nebo zařazení uživatelů nebo administrátorů,
- f) zajistí **deaktivaci účtu a bezodkladné odebrání nebo změnu** přístupových práv a oprávnění **při ukončení nebo změně smluvního vztahu** a
- g) stanoví **pravidla pro tvorbu hesel** podle § 9.

(2) Povinná osoba v rámci **fyzické bezpečnosti zamezí neoprávněnému přístupu** ke svým aktivům a předchází poškození, krádeži, neoprávněným zásahům, zneužití aktiv a přerušování poskytování regulované služby.



(1) Povinná osoba pro řízení identit, přístupových práv a oprávnění používá **nástroj**, který zajišťuje

- a) řízení počtu možných neúspěšných pokusů o přihlášení,
- b) opětovné ověření identity po stanovené době nečinnosti,
- c) odolnost uložených a přenášených autentizačních údajů a
- d) řízení přístupových práv, oprávnění pro čtení a zápis informací a dat a změnu oprávnění.

(2) Povinná osoba pro **ověření identity administrátorů a uživatelů využívá autentizační mechanismus**, který je založený na vícefaktorové autentizaci s nejméně **dvěma různými typy faktorů**.

(3) Povinná osoba **do doby využívání** autentizačního mechanismu založeného na **vícefaktorové autentizaci** podle odstavce 2, využívá **autentizaci pomocí kryptografických klíčů nebo certifikátů**.



(4) Povinná osoba **do doby využívání autentizačního mechanismu pomocí kryptografických klíčů nebo certifikátů** podle odstavce 3, využívá nástroj založený na autentizaci pomocí identifikátoru účtu a hesla a stanoví pravidla, která vynucují

a) délky hesla alespoň

1. **12** znaků pro účty **uživatelů**,
2. **17** znaků pro účty **administrátorů**,
3. **22** znaků pro účty **technických aktiv**,

b) **bezodkladnou změnu výchozího hesla** pro ověření identity technických aktiv, přičemž nové heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků,

c) neomezující použití malých a velkých písmen, číslic a speciálních znaků,

d) povinnou změnu hesla v intervalu maximálně po 18 měsících,

e) neumožňující uživatelům a administrátorům

1. zvolit si jednoduchá a často používaná hesla,
2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a
3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.



(5) Povinná osoba dále v rámci řízení identit zajistí

- a) důvěrnost při vytváření výchozích autentizačních údajů a při obnově přístupu,
- b) změnu výchozího hesla nebo hesla sloužícího k obnově přístupu po jeho prvním použití,
- c) zneplatnění hesla nebo identifikátoru sloužícího k obnově přístupu nejpozději do 24 hodin od jeho vytvoření,
- d) bezodkladnou změnu přístupového hesla v případě důvodného podezření na jeho kompromitaci a
- e) zabezpečení administrátorských účtů technických aktiv určených zejména pro případ obnovy po kybernetickém bezpečnostním incidentu a využívá tyto účty pouze v nezbytně nutných případech.



(1) Povinná osoba v rámci detekce kybernetických bezpečnostních událostí zajistí

- a) **ověření a kontrolu přenášených dat** na perimetru komunikační sítě, včetně **blokování nežádoucí komunikace**,
- b) nástroje pro **nepřetržitou a automatickou ochranu před škodlivým kódem** na relevantních technických aktivech, zejména na
 - 1. **serverech**,
 - 2. **koncových stanicích**,
- c) **řízení automatického spouštění obsahu**, zejména u vyměnitelných zařízení a datových nosičů,
- d) **nepřetržité poskytování informací** o relevantních detekovaných **kybernetických bezpečnostních událostech** a včasné varování relevantních osob a
- e) **pravidelnou a bezodkladnou aktualizaci nástrojů** pro nepřetržitou a automatickou **ochranu před škodlivým kódem** a dalších detekčních nástrojů a jejich **pravidel**.



(2) Povinná osoba **zaznamenává bezpečnostní a relevantní provozní události** v souladu s odstavcem 1 a u těchto událostí zaznamenává zejména následující

- a) datum a čas včetně specifikace časového pásma,
- b) typ činnosti,
- c) jednoznačnou identifikaci technického aktiva a identifikaci účtu původce a
- d) úspěšnost nebo neúspěšnost činnosti.



(1) Povinná osoba v rámci řešení kybernetických bezpečnostních událostí a incidentů

- a) zajistí, že uživatelé, administrátoři, osoby odpovědné za kybernetickou bezpečnost, další zaměstnanci a dodavatelé budou **oznamovat neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti**,
- b) vytvoří **metodikou pro posuzování kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů**, včetně **posuzování významnosti dopadu** kybernetického bezpečnostního incidentu v souladu s § 15,
- c) zajistí **posuzování** kybernetických bezpečnostních **událostí** a kybernetických bezpečnostních **incidentů v souladu s metodikou** podle písmene b),
- d) zajistí **detekci** kybernetických bezpečnostních **událostí** a dále při jejich detekci používá nástroje podle § 10,
- e) zajistí **řešení** kybernetických bezpečnostních **incidentů**,
- f) zajistí **hlášení** kybernetického bezpečnostního **incidentu s významným dopadem** podle § 16 zákona,
- g) zajistí **vytvoření závěrečné zprávy o vyřešení** kybernetického bezpečnostního **incidentu s významným dopadem** podle § 17 zákona, včetně **popisu příčiny vzniku** kybernetické bezpečnostního incidentu s významným dopadem, pokud je známa.



Povinná osoba pro ochranu bezpečnosti komunikační sítě, a to zejména jejího síťového perimetru

- a) zajistí **segmentaci komunikační sítě**, včetně **oddělení provozního a zálohovacího prostředí**,
- b) omezí odchozí a příchozí komunikaci na **perimetru komunikační sítě** na nezbytnou pro řádné zajištění poskytování regulované služby,
- c) užívá **aktuálně odolné a bezpečné síťové protokoly**,
- d) v případě užití **vzdáleného připojení** do interní komunikační sítě nebo **vzdálené správy** technických aktiv regulované služby
 1. **omezí** tato připojení na nezbytně nutná,
 2. zavede bezpečnostní opatření, která zajistí důvěrnost a integritu těchto vzdálených připojení a vzdálené správy a
 3. má **přehled** o uživateli a administrátorech, kteří tato vzdálená připojení nebo vzdálenou správu užívají.



Povinná osoba v rámci zajištění **aplikační bezpečnosti** regulované služby

- a) zajistí **bezodkladné aplikování schválených bezpečnostních aktualizací vydaných** pro technická aktiva,
- b) u technických aktiv, která již **nejsou** výrobcem, dodavatelem nebo jinou osobou **podporována**
 1. vede jejich **evidenci**,
 2. zavede **bezpečnostní opatření**, která zaručí obdobnou nebo vyšší úroveň bezpečnosti a
 3. omezí jejich komunikaci v komunikační síti na nezbytně nutnou,
- c) provádí **pravidelné skenování zranitelností** relevantních technických aktiv a aplikuje přiměřená bezpečnostní opatření na základě **zjištěných výsledků**.



- (1) Povinná osoba v rámci zajištění bezpečnosti technických aktiv a jejich komunikace
 - a) používá **aktuálně odolné kryptografické algoritmy**,
 - b) prosazuje **bezpečné nakládání s kryptografickými algoritmy** a
 - c) **zohledňuje doporučení a metodiky** v oblasti kryptografických algoritmů vydané Úřadem, zveřejněné na jeho internetových stránkách.

- (2) Povinná osoba zajišťuje bezpečnou
 - a) **hlasovou, audiovizuální a textovou komunikaci**, a to včetně e-mailové komunikace, a
 - b) **nouzovou komunikaci** v rámci organizace.



- Již dlouhodobě regulovány podle legislativy spojené s Informačními systémy veřejné správy (ISVS)
 - Již předchozí legislativa řeší kybernetickou bezpečnost obecně a povrchově
- Obdobné organizační struktury a fungování z pohledu veřejnosti
 - Starosta/ka, rada, zastupitelstvo, úředníci, agendy určené legislativou
- Obdobné informační systémy (spisová služba, webové stránky, úřední deska, MP, e-maily,...)
 - Obdobné problémy, které lze řešit obdobně
 - Určení rozsahu bude obdobné (registr práv a povinností)



Prostor pro dotazy

Děkuji za pozornost

Pavel Mazánek

Oddělení kontroly II
Odbor kontroly

pavel.mazanek@nukib.gov.cz