

Návrh nového zákona o kybernetické bezpečnosti ve vztahu k obcím

Petr Hrachy
Odbor Kontroly

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

Jan Hénik
Odbor Regulace

9. listopadu 2023

TLP: CLEAR



Prezentace má informační a osvětových charakter a informace v ní obsažené se mohou se v čase změnit.

Základem změn je nově přicházející **směrnice NIS2** (= viz dále), ale také potřeba zákon o kybernetické bezpečnosti aktualizovat.

Do návrhu zákona jsou promítnuty také vnitrostátní instituty a požadavky.

Směrnice obecně je legislativní akt Evropské unie, který není* sám o sobě aplikovatelný (**= musí nejdříve vzniknout národní úprava**).

Národní úřad pro kybernetickou a informační bezpečnost **připravil návrh nového zákona o kybernetické bezpečnosti**.

Návrh zákona je v meziresortním připomínkovém řízení.

Nová pravidla by měla platit v druhé polovině roku 2024 (do 17. října 2024 podle požadavku směrnice NIS2).

*zpravidla



Mezirezortní připomínkové řízení (MPŘ) – červenec až září 2023

- stále probíhá

Legislativní rada vlády – říjen až prosinec 2023

Poslanecká sněmovna, Senát, prezident – začátek roku 2024

Vydání zákona říjen 2024 (konec transpoziční lhůty)

**Vyhlášky budou mít samostatný legislativní proces, který bude spuštěn v
Q1 2024**



- Spuštěn web – dostupný zde: nis2.nukib.cz

Nová směrnice EU o kybernetické bezpečnosti

„NIS2“

Tematické okruhy

1. Obecné informace o směrnici NIS2

▶ Co se zde dozvím?

Otevřít okruh

2. Koho se nové povinnosti týkají

▶ Co se zde dozvím?

Otevřít okruh



- Regulace se netýká každého v daném odvětví – musí být splněna kritéria:
 - Organizace poskytuje alespoň jednu službu uvedenou v přílohách směrnice, a zároveň
 - Je středním nebo velkým podnikem
- Počítání **velikosti** podniku – nutno zohlednit i majetkově propojené společnosti
- Vybrané služby – **všechny organizace neohledě na jejich velikost** (ISPs, poskytovatelé služeb vytvářejících důvěru, DNS, veřejná správa)
- **Dodatečná kritéria** pro subjekty působící v regulovaných odvětvích bez ohledu na jejich velikost (jediný poskytovatel, narušení služby by mohlo mít významný dopad na veřejnou bezpečnost nebo zdraví osob nebo by mohlo vyvolat významné riziko, zejména s přeshraničním dopadem)
- Propojení směrnice NIS2 s tzv. směrnicí CER – **povinná osoba podle CER** (neznámá množina) → povinná osoba podle NIS2



Směrnice NIS1:

7 odvětví

Kritéria dopadu incidentu

⇒ cca 400 povinných osob

Směrnice NIS2:

18 odvětví

Kritérium velikosti subjektu

⇒ minimálně 6 000 povinných osob

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential“.

ENERGETIKA



Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.



Subjekty poskytující službu dálkového vytápění nebo chlazení.



Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.



Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.



Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA



Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.



Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.



Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.



Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ



Sektor bankovníctví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ



Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ



Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA



Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA



Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA



Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů.

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB



Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA



Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR



V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik“ a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik“ a „střední podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important“ (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY



Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelé kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ



Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL



Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ



Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA



Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB



Poskytovatelé on-line tržišť, internetových vyhledávačů, platform služeb sociálních sítí.

VÝZKUM



Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

NIS2 – velikost podniku

Doporučení Komise 2003/361/ES z 6. května 2003



Kategorie

Počet zaměstnanců: roční

Roční obrat



Bilanční suma roční

TLP: CLEAR

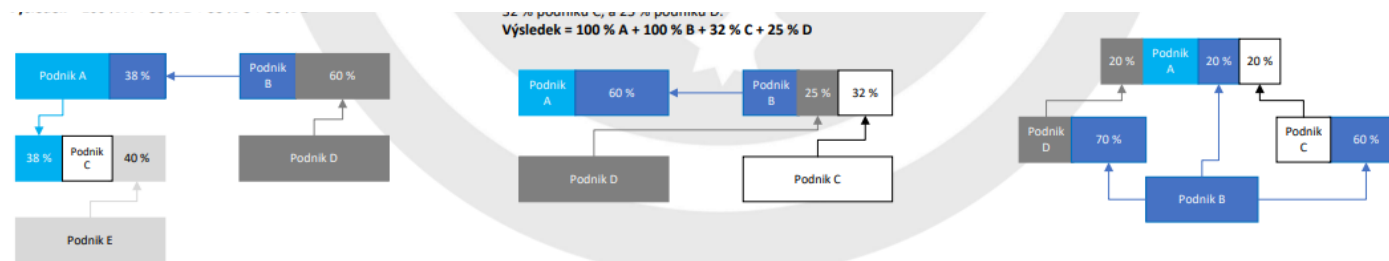


Počítání velikosti propojených organizací u obcí*

NÚKIB přistupuje k výkladu Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků v kontextu směrnice NIS2 tím způsobem, že se počet zaměstnanců, roční obrat nebo bilanční suma roční rozvahy obce nebo dobrovolného svazku obcí nezohledňují při počítání velikosti podniků zřizovaných touto obcí nebo dobrovolným svazkem obcí.

Například subjekt zajišťující odpadové hospodářství bude svou velikost počítat bez ohledu na to, že je zřizován obcí. **Nebude tedy docházet ke sčítání výše uvedených ukazatelů určujících velikost organizace dle uvedeného doporučení.**

Dostupné z: [Uživatelská příručka k definici malých a středních podniků \(nukib.cz\), 2022-11-14](https://nukib.cz/2022-11-14_Pocitani-velikosti-podniku_Zjednodusene_v1.0_final.pdf) [Pocitani-velikosti-podniku_Zjednodusene_v1.0_final.pdf \(nukib.cz\)](https://nukib.cz/2022-11-14_Pocitani-velikosti-podniku_Zjednodusene_v1.0_final.pdf)



Národní úřad pro kybernetickou a informační bezpečnost, TLP: CLEAR

Podrobnější výpočty a informace o tom, co vše započítat do velikosti zkoumaného podniku lze nalézt v uživatelské příručce k definici malých a středních podniků: https://osveta.nukib.cz/pluginfile.php/58365/mod_page/content/311/Priloha-4_U%C5%BElivatelsk%C3%A11%20p%C5%99%C3%ADru%C4%8Dka%20k%20definici%20mal%C3%BDch%20a%20st%C5%99edn%C3%ADch%20podnik%C5%AF.pdf



- Směrnice NIS2 ([EUR-Lex - 32022L2555 - CS - EUR-Lex \(europa.eu\)](#)) stanovuje široce povinné osoby, dělí je do dvou skupin (základní a významné), přiřazuje jim různé povinnosti (bezpečnostní opatření, hlášení incidentů,...)
 - = **stanovuje minimum**, co musí český zákon obsahovat (český zákonodárce může mít nad toto minimum další požadavky)
- Je potřeba mít na paměti, že z požadavku směrnice:
 - musí být regulovány všechny subjekty velikosti středního a velkého podniku (+ některé další) v daných odvětvích
 - musí zavádět bezpečnostní opatření podle čl. 20 a 21 směrnice apod.

Ve výsledku je ale podstatné především to, jak je směrnice převedena (transponována) do národního práva. Její samotný obsah má menší význam.

Útoky proti samosprávám

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost



NÚKIB v letech 2020-2023 eviduje 38 incidentů přímo hlášených samosprávami, konkrétněji obcemi nebo kraji:

- Obce - 27
- Kraje - 11

Dle stupnice závažnosti:

- 10 incidentů - méně významné
- 11 incidentů - významné
- 6 incidentů hlášeno před vyhodnocováním stupně závažnosti

Klasifikace dle ENISA:

- průnik: 7; škodlivý kód: 7; dostupnost: 6; informační bezpečnost: 4; podvod/phishing: 2; pokus o průnik: 1

Jedním z nejčastějších a zároveň nejzávažnějších typů incidentů byly **ransomwarové útoky**. Dále zneužívání zranitelností (např. MS Exchange Server), DDoS útoky, phishing či nepřístupnost elektronické pošty a spisové služby.

Je třeba dodat, že **obce nemají povinnost incidenty NÚKIB hlásit**, protože se nejedná o povinné osoby dle ZKB, jedná se tedy o statistiku z dobrovolných hlášení, skutečné počty se tak mohou lišit.

Rovněž organizace, které systematicky neřídí kybernetickou bezpečnost, **často mohou incidenty nedetekovat**.



Příklady známých dopadů různých incidentů podrobených rozboru NÚKIB:

- Nedostupnost monitorovacího software na jednotky hodin kvůli reinstalaci serveru
- Zařazení veřejné IP adresy obce na blacklisty = poškození reputace obce
- Nedostupnost e-mailových služeb
- Potenciál či potvrzená exfiltrace dat účastníkem
 - Dlouhodobá exfiltrace dat s potenciálem na následné použití těchto dat pro poškozování zájmů ČR
 - Potvrzená exfiltrace významného množství interních dat
- Zašifrování dat = nedostupnost dat = ztížené fungování úřadu pro občany obce, nedostupnost služeb
- Nefunkčnost webových stránek obce



Možný rozsah regulované služby „Výkon svěřených pravomocí“ v obcích



Přenesená působnost obcí

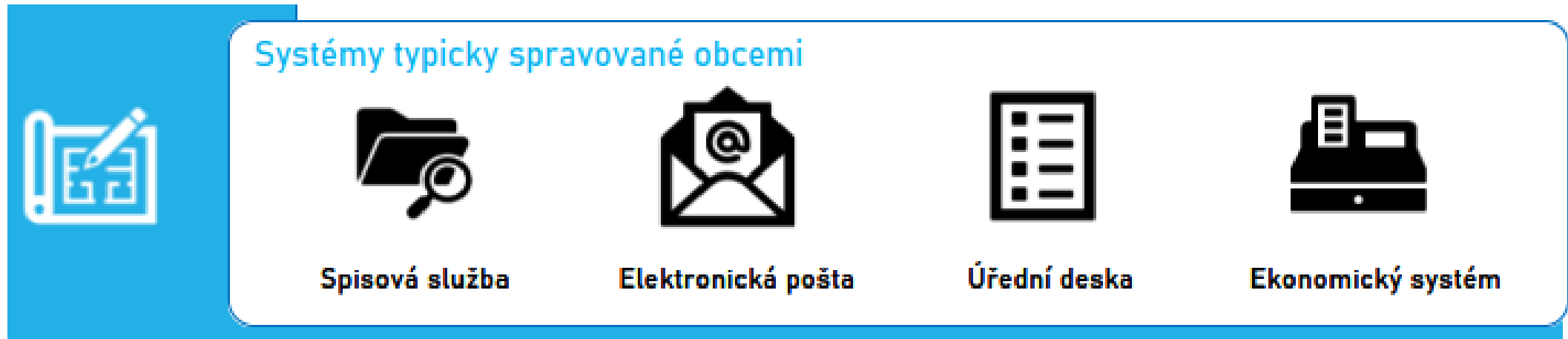
- Evidence obyvatel
- Matrika
- Vidimace a legalizace
- Poskytování informace
- Stavební a silniční správní úřad
- Dopravní agenda
- Životní prostředí
- Přestupky
- Místní poplatky
- Právo shromažďování
- Sociální agenda
- Krizové řízení

Samostatná působnost obcí

- Správa vlastního majetku
- Místní referenda
- Vyřizování petic a stížností
- Poskytování dotací
- Odpadové hospodářství
- Poskytování informací
- Zřizování příspěvkových organizací a obecní policie
- Vydávání obecně závazných vyhlášek



- Obce často vykonávají agendy v přenesené působnosti prostřednictvím přístupu do systémů řízených centrálně -> za jejich zajištění by měl být zodpovědný ÚOSS
- **Obce by měly zabezpečovat ty systémy, kterými disponují -> užší rozsah aktiv, na která budou zaváděna opatření**



Nový zákon o kybernetické bezpečnosti

Aktuální stav

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

9. listopadu 2023

TLP:CLEAR



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

Mechanismus BDŘ

Úkol
z usnesení Bezpečnostní rady
státu č. 41 ze dne 21. června
2022 k Bezpečnosti
dodavatelských řetězců
strategické infrastruktury státu,
č. j. 28261/2022-UVCR

Zlepšení a zkušenosti

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

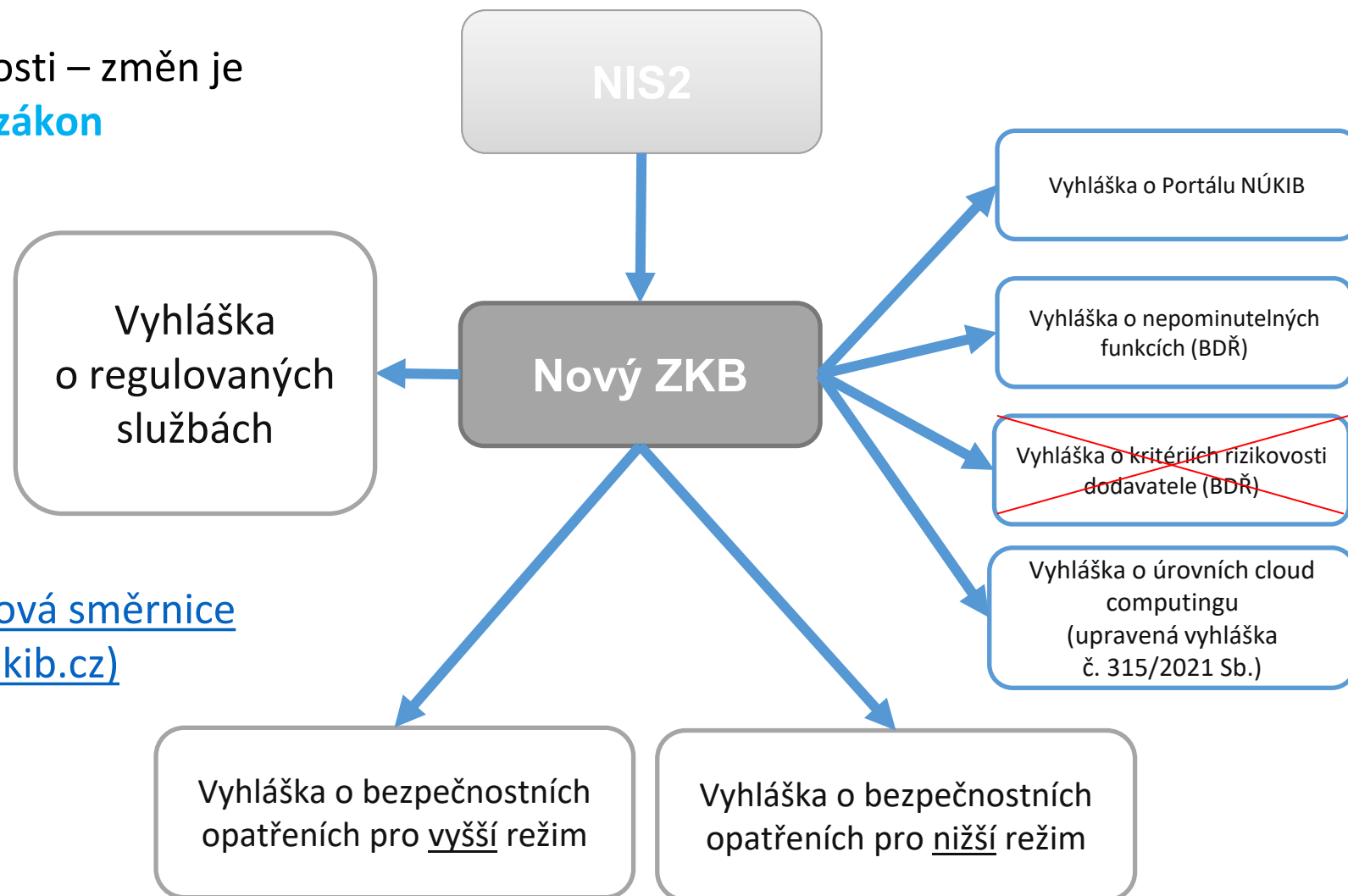
Nový zákon o kybernetické bezpečnosti v MPŘ



Nový zákon o kybernetické bezpečnosti – změna je tolik, že bylo **potřeba vytvořit nový zákon**
= zcela nová úprava – cca 70 paragrafů

Verze po mez. připomínkovém řízení má aktuálně navíc **6 vyhlášek.**

Celý návrh zveřejněn zde: [Course: Nová směrnice EU o bezpečnosti sítí a informací \(nukib.cz\)](https://www.nukib.cz/course/nova-smernice-eu-o-bezpecnosti-siti-a-informaci)



Vyhláška o regulovaných službách

Kritéria pro identifikaci regulované služby v odvětvích

- veřejná správa
- energetika
- výrobní průmysl
- potravinářský průmysl
- chemický průmysl
- vodní hospodářství
- odpadové hospodářství
- doprava
- digitální infrastruktura a služby
- finanční trh
- zdravotnictví
- věda, výzkum a vzdělávání
- poštovní a kurýrní služby
- vojenský průmysl
- vesmírný průmysl

Nový ZKB

Pravidla pro identifikaci a určení poskytovatelů regulovaných služeb

Povinnosti poskytovatelů regulovaných služeb

Bezpečnost dodavatelského řetězce

Oprávnění Úřadu, dozor

Vyhlášky o bezpečnostních opatřeních

Technická a organizační bezpečnostní opatření

Stanovení významnosti dopadu kybernetického bezpečnostního incidentu

Podrobnosti k likvidaci dat



Nový zákon dopadne na minimálně 6 000 organizací

- jde téměř výhradně o požadavek směrnice
- reguluje přes **105 služeb v 18 odvětvích** (energetika, zdravotnictví, bankovníctví, doprava, veřejná správa, digitální infrastruktura,...)
- hlavním kritériem pro zahrnutí do regulace je **velikost subjektu** (daná počtem zaměstnanců nebo jeho finanční situací)
- mění se také přístup k rozsahu regulace – **nevýbírají se konkrétní systémy, ale celé služby**
- do regulace se nově navrhuje **zařadit obce (ORP)**

Regulované organizace zákon nově označuje jako **tzv. poskytovatele regulované služby** a rozděluje je do **dvou režimů – nižších povinností a vyšších povinností**

- podle režimu mají stanovené povinnosti

Vznikají úplně nové instituty

- zajištění dostupnosti regulované služby nebo mechanismus prověřování bezpečnosti dodavatelského řetězce

Mění se některé stávající instituty

- stav kybernetického nebezpečí, (proti)opatření, konkrétní lhůty pro hlášení incidentů, sankce,...

Jedna jediná povinná osoba*:

Poskytovatel regulované služby



Provozovatelé
základní služby

Kritická
(nejen informační)
infrastruktura

Významné
informační systémy

Všechny subjekty
z NIS2

*Pro primární sadu některých povinností spojených s prevencí – zavádění bezpečnostních opatření, hlášení incidentů, apod.



Režim vyšších povinností



Režim nižších povinností





Regulovanou službou je služba

- **naplňující** alespoň jedno **kritérium pro identifikaci** regulované služby **podle vyhlášky o regulovaných službách (objektivní naplnění kritérií)**
- nebo
- **určená rozhodnutím NÚKIBu** na základě **kritéria pro určení** regulované služby

Režim poskytovatele regulované služby stanovuje **míru jemu uložených povinností** (tzn. dvojrychlostní kybernetická bezpečnost).

Režim poskytovatele regulované služby je stanoven vyhláškou o regulovaných službách, s výjimkou služeb určených NÚKIBem, pak je režim jejího poskytovatele vždy režimem vyšších povinností.

Každý poskytovatel regulované služby má pro všechny poskytované regulované služby stanoven jen jeden režim. Poskytovatel regulované služby, kterému je stanoven režim vyšších povinností pro alespoň jednu jím poskytovanou regulovanou službu, má stanoven režim vyšších povinností pro všechny jím poskytované regulované služby (jednotnost).



1. Veřejná správa

1.1. Výkonná pravomocí		<p>Nový zákon o kybernetické bezpečnosti dopadá na obce s rozšířenou působností. ORP (obce s rozšířenou působností) jsou tzv. poskytovateli regulovaných služeb v režimu nižších povinností.</p> <p>Obce I. a II. typu pouze přiměřeně zabezpečují jimi spravované informační systémy veřejné správy, žádné další povinnosti uvedené níže nemají.</p>	povinností, orgánem
		<p>S novým zákonem o kybernetické bezpečnosti se mění rovněž zákon o informačních systémech veřejné správy (ZoISVS).</p> <p>Správci přiměřeně zabezpečují jimi spravované informační systémy veřejné správy (ISVS) a to zaváděním bezpečnostních opatření, jež jsou uvedeny ve vyhlášce pro poskytovatele regulované služby v režimu nižších povinností.</p> <p>Nejedná se však o poskytovatele regulovaných služeb podle zákona o kybernetické bezpečnosti.</p>	q) krajem, nebo r) hlavním městem Praha,

ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy,
c) Kanceláří prezidenta republiky,
d) Kanceláří Senátu,
e) Kanceláří Poslanecké sněmovny.

c) vysokou školou,
d) Akademií věd České republiky, nebo
e) obcí s rozšířenou působností.



10. Vodní hospodářství

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
10.1. Provozování vodovodu	Provozovatel vodovodu podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) zásobuje pitnou vodou alespoň 50 000 obyvatel, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.
10.2. Provozování kanalizace	Provozovatel kanalizace podle zákona o vodovodech a kanalizacích je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, nebo b) poskytuje služby odvádění nebo čištění odpadních vod alespoň 50 000 obyvatelům, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

18. Zdravotnictví

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
18.1. Poskytování zdravotní péče	Poskytovatel zdravotní péče podle zákona o zdravotních službách je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, b) disponuje počtem lůžek akutní péče nejméně 270, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

11. Odpadové hospodářství

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
11.1. Provoz zařízení určeného pro nakládání s odpady	Provozovatel zařízení určeného pro nakládání s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.2. Obchodování s odpadem	Obchodník s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.3. Zprostředkování nakládání s odpadem	Zprostředkovatel nakládání s odpady podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.
11.4. Přeprava odpadu	Dopravce odpadu podle zákona o odpadech, který je středním nebo velkým podnikem, je poskytovatel regulované služby v režimu nižších povinností.



Hlavní povinnosti

- **hlásit kontaktní a další údaje**
- **stanovit rozsah řízení kybernetické bezpečnosti** – definuje rozsah regulace v organizaci
- **zavádět bezpečnostní opatření** – podle režimu v kterém je služba určena (vyšší/nížší)
- **hlásit kybernetické bezpečnostní incidenty** – podle režimu v kterém je služba určena (vyšší/nížší)
- **informovat zákazníky** o incidentech a hrozbách
- **provádět protiopatření**
- **plnit povinnosti z tzv. Mechanismu bezpečnosti dodavatelského řetězce** u vybraných (strategicky významných) služeb
- **zajistit dostupnost z České republiky** u vybraných (strategicky významných) služeb

Zákon dále upravuje další oblasti nezbytné pro fungování regulatorního rámce

- specifické situace – poskytování informací, stav kybernetického nebezpečí
- úprava institucí – NÚKIB, CERT a jejich pravomoci, součinnost dalších orgánů státu
- sankce – přestupky, úprava horních limitů sankcí



Hlášení údajů

- Registrační údaje – info o organizaci
- Kontaktní údaje – info o zástupci, měl by být zastupitelný
- Doplnující údaje – IP rozsahy a další
- Potřeba hlásit i změny (těch údajů, které nelze dohledat v rejstřících)
- Náležitosti – vyhláška o Portálu NÚKIB

Stanovení rozsahu řízení bezpečnosti

- Identifikace primárních aktiv v rámci celé organizace
- Určí, která primární aktiva souvisí s poskytováním regulované služby
- Určí organizační části a podpůrná aktiva, která souvisí s poskytováním regulované služby
- **Ta aktiva a organizační části, která takto určí spadají do rozsahu regulace**
- Dokud/pokud to neudělá = rozsah celá organizace



Bezpečnostní opatření

- Zavádí se v rámci stanoveného rozsahu
- Začínají se plnit nejpozději do jednoho roku od registrace služby
- V rámci vyššího/nížšího režimu:

organizační opatření – vyšší režim

1. systém řízení bezpečnosti informací,
2. povinnosti pro vrcholné vedení,
3. bezpečnostní role,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení rizik,
7. řízení dodavatelů,
8. bezpečnost lidských zdrojů,
9. řízení změn,
10. akvizice, vývoj a údržba,
11. řízení přístupu,
12. zvládání kybernetických bezpečnostních událostí a incidentů,
13. řízení kontinuity činností a
14. audit kybernetické bezpečnosti.

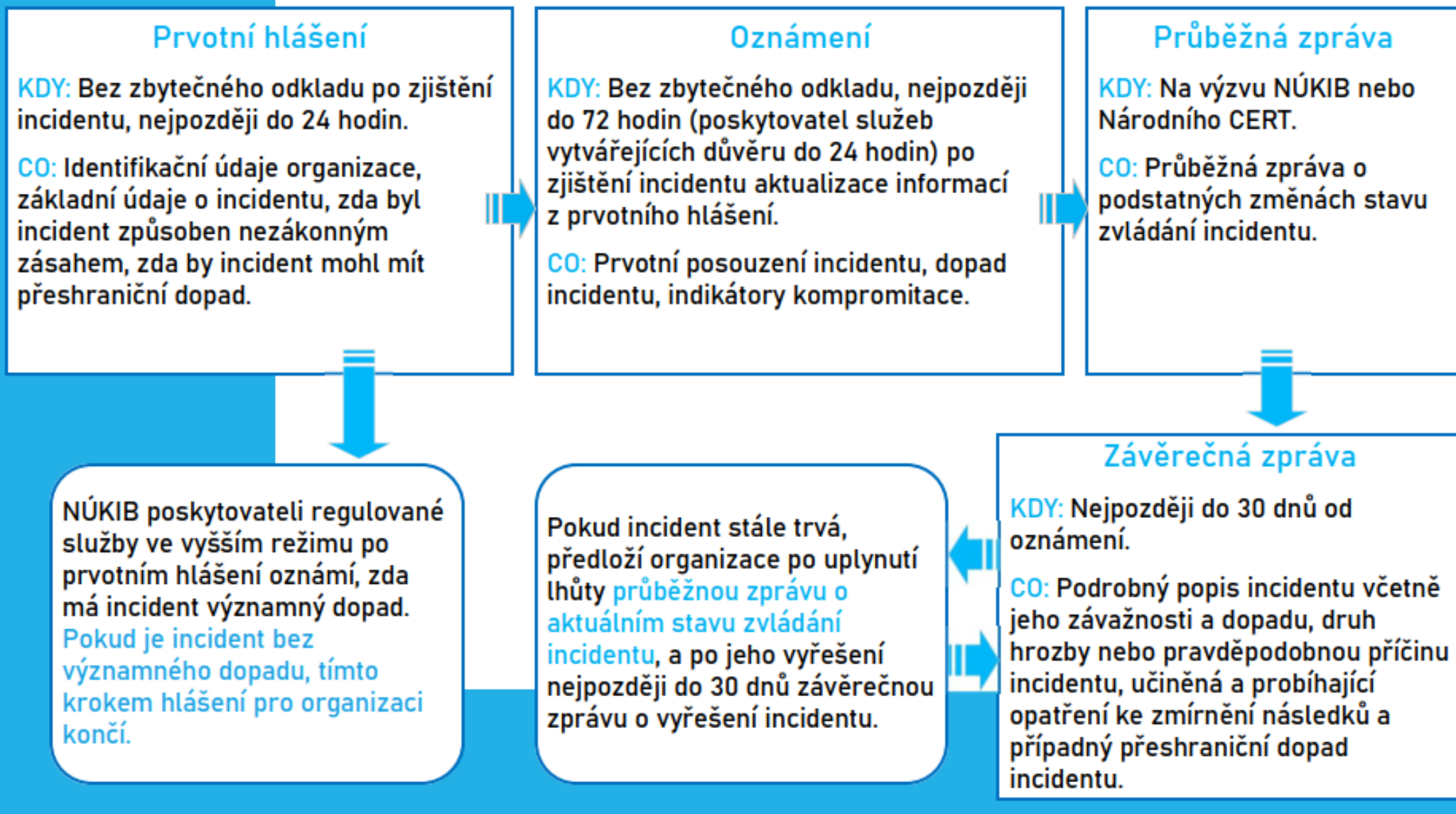
organizační opatření – nižší režim

1. zajišťování minimální úrovně kybernetické bezpečnosti,
2. povinnosti vrcholného vedení
3. bezpečnostní role
4. bezpečnostní politika a dokumentace,
5. řízení aktiv,
6. řízení dodavatelů,
7. bezpečnost lidských zdrojů,
8. řízení změn, akvizice, vývoje a údržby,
9. řízení přístupů,
10. zvládání kybernetických bezpečnostních událostí a incidentů,
11. řízení kontinuity činností.

technická opatření – vyšší režim (nižší režim mimo tučně vyznačené)

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
- 7. vyhodnocování kybernetických bezpečnostních událostí,**
8. aplikační bezpečnost,
9. kryptografické algoritmy,
10. zajišťování dostupnosti regulované služby,
11. zabezpečení průmyslových, řídicí a obdobných specifických aktiv.

KDY A CO PŘESNĚ HLÁSIT?



uššího



Opatření (nově Protiopatření)

- K podstatným změnám v logice opatření nedochází, mění se textace a některé detaily
- Staronový institut – **Výstraha**
 - Jde o upozornění, které je veřejné, nezávazné
 - Vydává se z důvodu ochrany, pořádku, bezpečnosti, života a zdraví nebo ekonomiky
 - Muže být vydáno jako info o incidentu nebo o porušování ZKB
- **Varování** – o hrozbě nebo zranitelnosti – veřejné i neveřejné, musí se promítnout do analýzy rizik u vyššího režimu
- **Reaktivní protiopatření** – k řešení incidentu, zabezpečení před incidentem, ke zvýšení ochrany aktiv
 - Konkrétní úkony, technická opatření či postupy – pro adresáty povinné
 - Rozhodnutí – adresné (konkrétní adresát, konkrétní povinnost)
 - Opatření obecné povahy – neadresné (nekonkrétní adresát, konkrétní povinnost)



Registrovat regulovanou službu

→ Do 30, resp. 90 dnů od naplnění identifikačních kritérií

Hlásit kontaktní a další údaje

→ Do 30 dnů (nové), resp. 15 dnů (změny)

Stanovit rozsah řízení kybernetické bezpečnosti

→ Kdykoli (ALE do doby stanovení je rozsahem celá organizace)

Zavádět bezpečnosti opatření

- Vyšší režim
- Nižší režim

→ Do 1 roku od vyrozumění o zařazení do evidence

Hlášení kybernetických bezpečnostních incidentů

- Vyšší režim
- Nižší režim

→ Do 1 roku od vyrozumění o zařazení do evidence

→ Ihned (lhůty v protiopatření)

Informační povinnost poskytovatele regulované služby

Pokud to poskytovatel regulované služby považuje za vhodné, **oznámí** bez zbytečného odkladu **uživatelům** regulované služby **kybernetický bezpečnostní incident s významným dopadem, který by mohl negativně ovlivnit poskytování této služby.**

Úřad je oprávněn poskytovateli regulované služby uložit povinnost informovat uživatele regulované služby o tomto incidentu.

Poskytovatel regulované služby je **povinen** bez zbytečného odkladu vhodným a srozumitelným způsobem **informovat uživatele regulované služby, který může být ovlivněn významnou hrozbou, o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší.**

→ Ihned (ALE vychází z bezpečnostních opatření a hlášení incidentů)



Mechanismus prověřování dodavatelského řetězce

- Cíl = stát musí mít mechanismus jak řešit závislost na nedůvěryhodných dodavatelích (projev národní suverenity)
- platí pouze pro vybrané organizace v režimu vyšších povinností (a to nikoli všech)
- budou prověřováni dodavatelé do kritické části systému = aktiva s hodnotou 3 a 4 (vysoká/kritická), kteří dodávají bezpečnostně významnou dodávku = má výpočetní kapacitu
- stát prověří to, zda dodavatel není hrozbou pro bezpečnost ČR, zájmy ČR, vnitřní a veřejnou bezpečnost
- NÚKIB může vydat zákaz dodavatele použít nebo upozornění na riziko (je řešitelné bezpečnostním opatřením) + lze udělit výjimku (např. pokud to nikdo jiný nevyrobí, ohrozilo by to službu apod.) + přechodné lhůty

→ Do 1 roku od vyrozumění o označení služby jako strategické

Zajištění dostupnosti strategicky významných služeb

- Cíl = kritické služby musíme být schopni zajistit alespoň omezeně z České republiky, abychom byli připraveni na mimořádné situace v zahraničí
- poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v nezbytném rozsahu ve stanoveném čase a kvalitě z území České republiky + pravidelné ověřování schopnosti zajištění

→ Do 1 roku od vyrozumění o označení služby jako strategické (+ 1x za 2 roky prověřovat)



Základní povinnosti obce s rozšířenou působností:



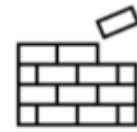
Registrace



Bezpečnostní opatření



Hlášení incidentů



Provedení protiopatření



Bezpečnostní opatření není potřeba zavést všechna hned, jde o postupný proces.

Vyhláška stanovuje 13 bezpečnostních opatření, pouze 4 opatření musí být splněny vždy.

Ostatní opatření se zavádějí vždy přiměřeně s ohledem na bezpečnostní potřeby uvnitř organizace.



Přehled v organizaci

Jaké vykonávám agendy a poskytuji služby?

Co potřebuji k výkonu těchto agend a služeb?

Stanovím si rozsah v němž řeším kybernetickou bezpečnost.

Aktuální stav KB

Mám již některá bezpečnostní opatření zavedena?

Zdokumentuji aktuální stav, vytvořím přehled zavedených a nezavedených opatření.

Určení priorit

Jaké mám finanční a personální kapacity?

Stanovím plán zavádění bezpečnostních opatření, odůvodním případné nezavedení nepovinných opatření.

Zavádění opatření

Určím osobu odpovědnou za KB.

Prioritní je školení zaměstnanců i vedení.

Vytvořím bezpečnostní politiku a dokumentaci.

Pokračuji dle plánu.



Zajišťování kyberbezpečnosti (KB)

- Přehled bezpečnostních opatření + roční vyhodnocení účinnost + uchování přehledů po dobu 4 let
- Určení osoby odpovědné za KB
- Vytvoření a schválení bezpečnostní politiky a dokumentace
- Dodržování pravidel a postupů

Povinnosti vrcholového vedení

- Vrcholové vedení je poučeno o povinnostech a odpovědnosti
- Zajistí dostupnost zdrojů pro zajišťování kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření
- Prokazatelně se seznamuje s plněním přehledu bezpečnostních opatření



Rozsah bezpečnostní politiky a dokumentace

- Politika zajišťování minimální úrovně KB
- Politika bezpečnosti lidských zdrojů
- Politika řízení kontinuity činností
- Politika řízení přístupu
- Politika detekce KB události a řešení KB incidentů
- Politika bezpečnosti komunikační sítě
- Politika aplikační bezpečnosti
- Evidence aktiv
- Přehled bezpečnostních opatření
- Plán obnovy
- Závěrečná zpráva o KB incidentu
- Evidence nepodporovaných aktiv

klé
ezření

tí a



školení v oblasti KB

- Školení administrátorů a osob odpovědných za KB v organizaci
- Kontrola dodržování bezpečnostní politiky
- Pravidla a postupy pro řešení případů porušení stanovených pravidel

incidentu

- Řešení KB incidentů (proces)
- Hlášení KB incidentů s významným dopadem na NÚKIB
- Závěrečná zpráva o KB incidentu s významným dopadem
- Detekce KB událostí

- Připravujeme tzv. Portál NÚKIB
- Portál bude rozhraní sloužící administraci povinností, poskytování služeb a sdílení informací
 - Registrace organizace
 - Hlášení kontaktních údajů
 - Hlášení incidentů
 - Další hlášení (provádění opatření apod.)
 - Přístup k registru zranitelností
- Provázáno s vyhláškou o Portálu NÚKIB
- Vystavěn na platformě Neveřejného webu
- Tvoříme interním vývojem

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST
PORTÁL NÚKIB

PORTÁL INFORMAČNÍ SERVIS DOKUMENTACE PODPORA

Upozornění na probíhající DDoS útoky

Aplikace

 PORTÁL Portál je web určený k publikování informací určených pro povinné subjekty. Obsahuje také informace o platformě Neveřejný web.	 MISP MISP je nástroj pro informování o indikátorech kompromisů vyskytujících se v Česku nebo v síti organizace.	 NEXTCLOUD Nextcloud je nástroj pro sdílení souborů a zároveň slouží jako platforma umožňující se-line kolaboraci nad dokumenty.
 MATRIX Matrix je komunikační nástroj (chat) s podporou video konferencí (VTC).	 DATOR DATOR je služba určená k předávání dat směrem k NÚKIB a částečně v této oblasti nahrazuje aplikaci Nextcloud.	 GITLAB Gitlab je pro správu zdrojových kódů. S jeho pomocí s vámi můžeme lépe spolupracovat.



Dozorový orgán – NÚKIB

Oprávnění:

- **Kontrola**
- **Nápravná opatření**
- **Zvláštní sankce**
 - Pozastavení platnosti certifikace (NÚKIB)
 - Pozastavení výkonu řídicí funkce (soud)
- **Pokuta za přešupek**
 - Odstupňováno podle režimu a povahy pochybení
 - Až 250 mil. Kč nebo 2 % z celosvětového obratu
 - GDPR – *ne bis in idem*



V srpnu 2022 spuštěn **informační web věnovaný směrnici NIS2 a nové regulaci**

[Nová směrnice EU o bezpečnosti sítí a informací \(nukib.cz\)](https://www.nukib.cz)*

Představení problematiky na desítkách konferencí a bilaterálních jednání se zástupci úřadů a soukromého sektoru

Osloveno a komunikováno **s více než 28 svazy, oborovými sdruženími a komorami**

Provedena veřejná konzultace a připomínkování návrhů ze strany veřejnosti

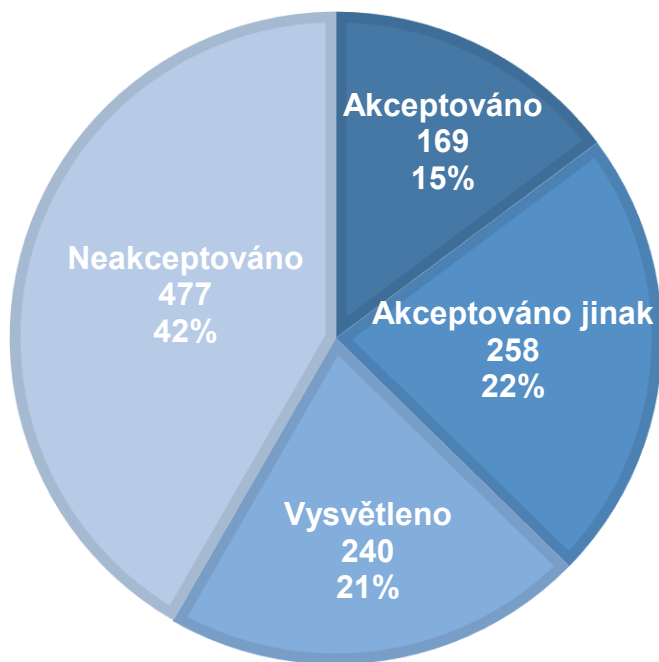
- veřejná konzultace a zveřejnění prvotních návrhů ZKB pro podněty veřejnosti bylo zahájeno 26. ledna 2023 a ukončeno 12. března 2023
- NÚKIB obdržel **podněty od 117 jednotlivých míst** (toho bylo 27 obsahově stejných)

* na webu je přes 270 000 přístupů

V rámci veřejných konzultací bylo od 26. ledna do 12. března **zasláno 1144 podnětů od odborné veřejnosti, soukromého sektoru i veřejné správy**

ANALÝZA VYPOŘÁDÁNÍ PODNĚTŮ

■ Akceptováno ■ Akceptováno jinak ■ Vysvětleno ■ Neakceptováno



- **Akceptováno** – podnět byl zapracován do návrhu zákona či doprovodných dokumentů (RIA, důvodová zpráva, návrhy vyhlášek);
- **Akceptováno jinak** – podnět byl v návrhu zákona či doprovodných dokumentech zohledněn jinak;
- **Vysvětleno** – podnět byl shledán spíše jako dotaz nebo konstatování, tudíž byl vysvětlen či okomentován;
- **Neakceptováno** – podnět nebylo možné zapracovat do návrhu zákona či doprovodných materiálů.



- Formulační změny, zpřehlednění a zpřesnění textu
- Nastavení inspektorů → **zrušení institutu inspektorů**
- Obsah vyhlášky o bezpečnostních opatřeních pro režim nižších povinností
→ **zeštíhlení, zjednodušení – do MPŘ byla následně předložena zcela přepracovaná verze**
- Lokalizace informací a dat při zpracování v zahraničí → **zcela přepracováno, nově zajištění dostupnosti strategicky významných služeb z České republiky**
- Určovací a identifikační kritéria ve vyhlášce → **přesun určovacích kritérií, určení změny režimu do zákona a výčet odvětví pro identifikaci přímo v zákoně**
- Zákon rozdělen na dva → **hlavní zákon a změnový zákon (měnící jiné předpisy)**
- Dílčí změny v mechanismu prověřování bezpečnosti dodavatelského řetězce
- Stav kybernetického nebezpečí → **koncepční změny, provázání s krizovým řízením**

Oficiální meziresortní připomínkové řízení bylo zahájeno 19. června 2023 a ukončeno 26. července 2023 (téměř 6 týdnů)

NÚKIB obdržel vyšší stovky připomínek

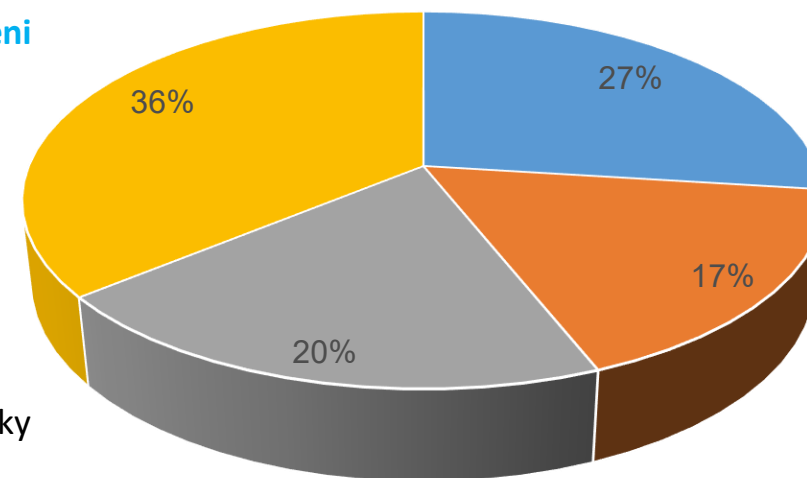
- o připomínky zaslalo **41 řádných připomínkových míst**
- o dalších **11 organizací zaslalo své připomínky i bez toho, aby byli osloveni** (ale jejich připomínky byly také přijaty a řešeny)

Písemné návrhy vypořádání připomínek byly rozeslány 11. 9. 2023

Nejčastější připomínkované oblasti

- o legislativně-technické úpravy, obsah doprovodných materiálů, definice apod.
- o mechanismus bezpečnosti dodavatelského řetězce a zajištění dostupnosti strategicky významné služby
- o nastavení vztahu zákon – vyhlášky
- o pravomoci Úřadu a Národního CERT
- o stav kybernetického nebezpečí

Způsob vypořádání



■ Akceptováno ■ Akceptováno jinak
■ Vysvětleno ■ Neakceptováno

Bezpečnostní opatření

(režim nižších povinností)

NÚKIB

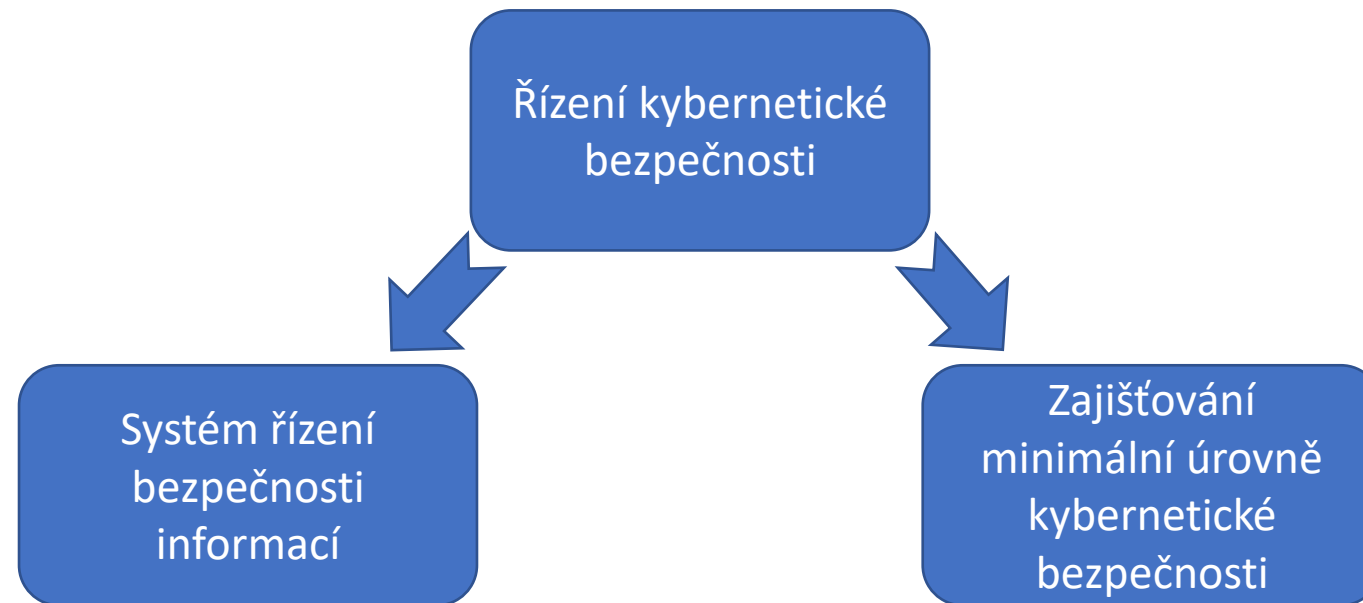


Národní úřad
pro kybernetickou
a informační
bezpečnost

Důležité změny oproti současně platné legislativě



- Nový pojem **řízení kybernetické bezpečnosti** na úrovni zákona
- Již známý pojem **systém řízení bezpečnosti informací** v prováděcím předpise pro režim vyšších povinností
- Nový pojem **zajišťování minimální úrovně kybernetické bezpečnosti** v prováděcím předpise pro režim nižších povinností





- **Řízení kybernetické bezpečnosti** - činnost poskytovatele regulované služby podle tohoto zákona směřující k zajištění kybernetické bezpečnosti regulované služby
- **System řízení bezpečnosti informací** - část systému řízení povinné osoby založená na přístupu k rizikům aktiv, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat
- **Zajišťování minimální úrovně kybernetické bezpečnosti** - zajištění minimální úrovně kybernetické bezpečnosti aktiv povinné osoby založené na zavedení bezpečnostních opatření



- Okruhy bezpečnostních opatření:
 - **Analýza rizik a politiky bezpečnosti informací**
 - **Zvládání incidentů**
 - **Kontinuita činností**, rozvedená např. o správu zálohování a obnovu provozu po havárii, a krizové řízení
 - **Bezpečnost dodavatelského řetězce**
 - Bezpečnost v rámci **pořizování, vývoje a údržby** systémů
 - Politiky a postupy pro **posouzení účinnosti bezpečnostních opatření**
 - Prakticky **kybernetické hygieny a školení v oblasti kybernetické bezpečnosti**
 - Politiky a postupy využívání **kryptografie a případně šifrování**
 - **Bezpečnost lidských zdrojů, řízení přístupů a aktiv**
 - **Využívání vícefaktorových autentizačních mechanismů**, bezpečných komunikačních nástrojů a nástrojů pro nouzovou komunikaci



- Určení toho, kde všude je žádoucí zavádět bezpečnostní opatření
- Směrnice NIS2 přináší pohled na celou organizaci
- Stanovení rozsahu **v návrhu ZKB je v porovnání s aktuálně platnou legislativou zpřesněno** a přináší **presumpci, že pokud poskytovatel regulované služby stanovení rozsahu řízení kybernetické bezpečnosti neprovede, má povinnost zavádět bezpečnostní opatření na celou organizaci**
- **Při stanovení rozsahu řízení KB podle návrhu zákona subjekt pohlíží na organizaci jako na celek a následně se rozhoduje, jaká aktiva lze z rozsahu vyjmout (vyjmutí je třeba řádně zdůvodnit)**



- Nově upraven samostatným paragrafem v nZKb.

(1) Poskytovatel regulované služby

- identifikuje všechna primární aktiva v rámci celé organizace,
- určí, která primární aktiva identifikovaná podle písmene a) souvisejí s poskytováním regulované služby, a
- u primárních aktiv určených podle písmene b) identifikuje a určí související organizační části organizace a podpůrná aktiva.

Postup pro určení rozsahu řízení kybernetické bezpečnosti

O provedení identifikace a určení organizačních částí a aktiv podle odstavce 1 vede poskytovatel regulované služby dokumentovaný záznam, a to včetně evidence primárních aktiv, která byla ze stanoveného rozsahu vyjmuta, a odůvodnění jejich vyjmutí.

Určený rozsah

- Dokumentovat
- Přezkoumávat
- Aktualizovat

Stanovený rozsah podle odstavce 1 je poskytovatel regulované služby povinen pravidelně přezkoumávat a aktualizovat.

Ve stanoveném rozsahu řízení kybernetické bezpečnosti se následně zavádí bezpečnostní opatření dle jednotlivých prováděcích předpisů



- **Pokud poskytovatel regulované služby stanovení rozsahu řízení kybernetické bezpečnosti neprovede, má povinnost zavádět bezpečnostní opatření na celou organizaci**
- Určuje rozsah řízení kybernetické bezpečnosti do doby, než dojde k jeho stanovení postupem podle odst. 1

Do doby splnění povinností podle odstavců 1 a 3 se má za to, že stanovený rozsah je tvořen regulovanou službou a podpůrnými aktivy jsou všechna podpůrná aktiva organizace a další podpůrná aktiva související s poskytováním regulované služby. Má se za to, že aktiva, která ještě nebyla identifikována a určena podle odstavce 1 jsou součástí stanoveného rozsahu, dokud nejsou zahrnuta v procesu identifikace a určování organizačních částí a aktiv tvořících stanovený rozsah podle odstavce 1 a není o nich veden dokumentovaný záznam podle odstavce 3.

- Nově pořízená aktiva jsou automaticky součástí stanoveného rozsahu, dokud organizace dokumentovaným způsobem nerozhodne o tom, že do rozsahu nepatří.

Má se za to, že aktiva, která ještě nebyla identifikována a určena podle odstavce 1 jsou součástí stanoveného rozsahu, dokud nejsou zahrnuta v procesu identifikace a určování organizačních částí a aktiv tvořících stanovený rozsah podle odstavce 1 a není o nich veden dokumentovaný záznam podle odstavce 3.



Režim vyšších povinností:

- Registruje se a hlásí kontaktní údaje
- Hlásí většinu incidentů
- Provádí veškerá protiopatření

- Na některé se aplikují povinnosti týkající se bezpečnosti dodavatelského řetězce a zajišťování dostupnosti služby

Režim nižších povinností:

- Registruje se a hlásí kontaktní údaje
- Hlásí jen významné incidenty
- Neprovádí varování, jen reaktivní protiopatření

Bezpečnostní opatření a rozdíly v nich vizte dále.

Bezpečnostní opatření - prováděcí vyhlášky



- Z pohledu oblastí bezpečnostních opatření jsou **obě prováděcí vyhlášky** téměř totožné, nicméně **zásadně se liší v rozsahu jednotlivých bezpečnostních opatření**

Organizační opatření	
Vyhláška pro režim vyšších povinností	Vyhláška pro režim nižších povinností
Systém řízení bezpečnosti informací	Zajišťování minimální úrovně kybernetické bezpečnosti
Povinnosti vrcholového vedení	Povinnosti vrcholového vedení
Bezpečnostní role	Bezpečnostní role
Řízení bezpečnostní politiky a dokumentace	Řízení bezpečnostní politiky a dokumentace
Řízení aktiv	Řízení aktiv
Řízení rizik	Řízení rizik
Řízení dodavatelů	Řízení dodavatelů
Bezpečnost lidských zdrojů	Bezpečnost lidských zdrojů
Řízení změn	Řízení změn, akvizice, vývoje a údržby
Akvizice, vývoj a údržba	
Řízení přístupu	Řízení přístupu
Zvládání kybernetických bezpečnostních událostí a incidentů	Zvládání kybernetických bezpečnostních událostí a incidentů
Řízení kontinuity činností	Řízení kontinuity činností
Audit kybernetické bezpečnosti	

Technická opatření	
Vyhláška pro režim vyšších povinností	Vyhláška pro režim nižších povinností
Fyzická bezpečnost	Fyzická bezpečnost
Bezpečnost komunikačních sítí	Bezpečnost komunikačních sítí
Správa a ověřování identit	Správa a ověřování identit
Řízení přístupových oprávnění	Řízení přístupových oprávnění
Detekce kybernetických bezpečnostních událostí	Detekce kybernetických bezpečnostních událostí
Zaznamenávání bezpečnostních a relevantních provozních událostí	Zaznamenávání bezpečnostních a relevantních provozních událostí
Vyhodnocování kybernetických bezpečnostních událostí	
Aplikační bezpečnost	Aplikační bezpečnost
Kryptografické algoritmy	Kryptografické algoritmy
Zajišťování dostupnosti regulované služby	Zajišťování dostupnosti regulované služby
Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv	Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv



NIŽŠÍ REŽIM

§ 7

Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

1. v rámci primárních aktiv stanoví jejich prioritu a pořadí a postupy jejich obnovy,
2. stanoví odpovědnosti a povinnosti při obnově podle písm. a),
3. vytváří pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

VYŠŠÍ REŽIM

§ 16

Řízení kontinuity činností

1. Povinná osoba v rámci řízení kontinuity činností
2. stanoví metodiku pro provedení analýzy dopadů,
3. pomocí analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik podle § 9, v rámci kterého posoudí možná rizika související s ohrožením kontinuity činností,
4. na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) stanoví cíle řízení kontinuity činností formou určení
 5. minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby,
 6. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby a
 7. bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
8. stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c) a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
9. vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby a
10. realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 27.
11. Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § X [Zajištění dostupnosti strategicky významné služby] zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod ii) tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bod i) tohoto ustanovení.



- Veřejná konzultace přinesla významnou redukci úrovně vyhlášky o bezpečnostních opatřeních pro nižší režim

PŮVODNÍ NIŽŠÍ REŽIM

organizační opatření – nižší režim před konzultací

1. Zajišťování minimální úrovně kybernetické bezpečnosti
2. Povinnosti pro vrcholové vedení,
3. bezpečnostní role,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení dodavatelů,
7. bezpečnost lidských zdrojů,
8. řízení změn, akvizice, vývoj a údržba,
9. řízení přístupu,
10. zvládání kybernetických bezpečnostních událostí a incidentů,
11. řízení kontinuity činností a

technická opatření – nižší režim před konzultací

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
7. aplikační bezpečnost,
8. kryptografické algoritmy,
9. zajišťování dostupnosti regulované služby,
10. zabezpečení průmyslových, řídicí a obdobná specifických aktiv

SOUČASNÝ NIŽŠÍ REŽIM

bezpečnostní opatření – nižší režim po konzultaci

1. povinnosti vrcholového vedení
2. bezpečnost lidských zdrojů
3. řízení kontinuity činností
4. řízení přístupu
5. řízení identit a jejich oprávnění
6. detekce a zaznamenávání kybernetických bezpečnostních událostí
7. řešení kybernetických bezpečnostních incidentů
8. bezpečnost komunikačních sítí
9. aplikační bezpečnost
10. kryptografické algoritmy



NIŽŠÍ REŽIM PO KONZULTACÍCH

§ 7

Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

1. v rámci primárních aktiv stanoví jejich prioritu a pořadí a postupy jejich obnovy,
2. stanoví odpovědnosti a povinnosti při obnově podle písm. a),
3. vytváří pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

NIŽŠÍ REŽIM PŘED KONZULTACEMI

§ 14

Řízení kontinuity činností

- 1) Povinná osoba v rámci řízení kontinuity činností
 - a) stanoví metodiku pro provedení analýzy dopadů,
 - b) pomocí analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů,
 - c) stanoví práva a povinnosti administrátorů a osob zodpovědných za kybernetickou bezpečnost podílejících se na zajištění poskytování regulované služby,
 - d) na základě výsledků analýzy dopadů dle písmene b) vypracuje, aktualizuje a testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby,
 - e) stanoví pravidla a postupy k provádění pravidelného zálohování,
 - f) stanoví pravidla a postupy kontroly použitelnosti provedených záloh,
 - g) provádí pravidelné zálohování a kontrolu použitelnosti záloh podle § 23 a
 - h) realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 23.
- 2) Povinná osoba při tvorbě plánů kontinuity činností může využít vzor z přílohy č. 5 k této vyhlášce.



- Zcela nový legislativní předpis
- Většina oblastí bezpečnostních opatření shodná s režimem vyšším, avšak liší se jak počtem opatření, tak z pohledu obsahu a rozsahu bezpečnostních opatření
- Subjekt neprovádí hodnocení rizik ve smyslu současného znění VKB
- Obsahuje přehled bezpečnostních opatření, které subjekt má povinnost zavést, pokud některé nemůže zavést – řádně zdůvodní a přijme jiné vhodné bezpečnostní opatření
- Vybrané dokumenty/bezpečnostní role jsou pojmenovány jinak, než v režimu vyšších povinností
- Vhodné technické nástroje/prostředky – doména, firewall, detekce škodlivého kódu a zálohy



- **§ 4 Zajišťování kybernetické bezpečnosti:**

- Sumarizační §, který definuje proces zavádění bezpečnostních opatření a kontinuálního zlepšování
- Princip přiměřenosti (zavádí se přiměřená opatření se zohledněním bezpečnostních potřeb organizace)
- Ústřední dokument: Přehled bezpečnostních opatření (zavedená/nezavedená/kdy budou zavedená + odůvodnění, 1x ročně vyhodnocení, archivace)
- Určení osoby zodpovědné za KB
- Vytvoření a schválení bezpečnostní politiky, vedení bezpečnostní dokumentace, povinnost dodržování
- Stanovení pravidel ochrany (řízení) aktiv a přípustné způsoby jejich používání, na hodnocení aktiv, příp. vazby mezi nimi, jsou následně vázána vybraná technická opatření
- Zohlednění požadavků na dodavatele ve smluvním vztahu
- Stanoví bezpečnostní požadavky v souvislosti s akvizicí, vývojem a údržbou



- S ohledem na zjednodušenou AR pro režim nižších povinností § 4 nově přistupuje k některým bezpečnostním opatřením jako k tzv. *obligatorním*, tedy bez možnosti je (typicky prostřednictvím prohlášení o aplikovatelnosti) vyloučit, i když se na první pohled může tento krok jevit jako zpřísnění úpravy oproti režimu vyšších povinností, není tomu tak, jelikož v režimu nižších povinností jsou obsahové náležitosti BO maximálně zredukovány.
- Kromě **modrého** v předchozím snímku se jedná také o:
 - § 5 (vrcholné vedení)
 - § 6 (bezpečnost lidských zdrojů)
 - § 11 (řešení kybernetických bezpečnostních incidentů)



- **§ 5 Povinnosti vrcholového vedení:**
 - Zapojit se do oblasti kybernetické bezpečnosti a jejího řízení
 - Vedení zná své povinnosti a odpovědnosti
 - Zajišťuje potřebné zdroje
 - Seznamuje se s plněním přehledu bezpečnostních opatření



- **§ 6 Bezpečnost lidských zdrojů**
 - Politika bezpečného chování uživatelů
 - Pravidla rozvoje bezpečnostního povědomí (školení zaměstnanců)
- **§ 7 Řízení kontinuity činností**
 - Prioritizace primárních aktiv pro obnovu a postup obnovy včetně odpovědných osob
 - Zálohování
- **§ 8 Řízení přístupů**
 - Zajištění řízenosti přístupů a pravidel pro privilegované účty – nezbytně nutné
 - přidělování/změna/odebírání oprávnění
 - Bezpečnost mobilních zařízení
- **§ 9 Řízení identit a jejich oprávnění**
 - Disponovat nástrojem pro řízení identit a jejich oprávnění
 - Vícefaktorová autentizace (+ délky hesel do doby zavedení vícefaktorové autentizace)
 - Pravidla pro tvorbu a nakládání s hesly



- **§ 10 Detekce a zaznamenávání kybernetických bezpečnostních událostí**
 - Detekce událostí na perimetru + vedení záznamů o nich
 - Nástroj pro nepřetržitou a automatickou ochranu před škodlivým kódem na relevantních aktivech
- **§ 11 Řešení kybernetických bezpečnostních incidentů**
 - Zavede postupy pro oznamování podezření na incidenty/události
 - Metodika pro posuzování incidentů a událostí + posouzení těch významných, které jsou hlášeny
 - Zajistit řešení incidentů
 - Další postupy v souladu s požadavky na hlášení incidentů dle ZKB
- **§ 12 Bezpečnost komunikačních**
 - Segmentace (zálohy vs. provozní prostředí)
 - Omezení příchozí a odchozí komunikace na perimetru na nutnou
 - Užívání aktuálně odolných a bezpečných síťových protokolů
 - Zajišťuje bezpečnost vzdálených připojení a vzdálené správy technických aktiv



- **§ 13 Aplikační bezpečnost**
 - Bezodkladné aplikování bezpečnostních aktualizací
 - Řídí bezpečnost technických aktiv, která již nemají podporu (vede evidenci, zavádí dodatečná bezpečnostní opatření)
 - Skenování zranitelností relevantních technických aktiv
- **§ 14 Kryptografické algoritmy**
 - Používá šifrování pomocí aktuálně odolných kryptografických algoritmů, kde je to vhodné
 - Zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Úřadem
 - Zajišťuje bezpečnou hlasovou, textovou a audiovizuální komunikaci (vč. e-mailů a nouzové komunikace)
- **§ 15 Stanovení významnosti dopadu kybernetického bezpečnostního incidentu**
 - Obsahuje pravidla pro stanovení významnosti dopadu incidentů a tedy pro jeho hlášení



- **Příloha č. 1 – Přehled bezpečnostních opatření**
 - Přehled o tom co je zavedeno a co nezavedeno
- **Příloha č. 2 – Bezpečnostní politika a bezpečnostní dokumentace**
 - Doporučená struktura a obsah bezpečnostní dokumentace
- **Příloha č. 3 – Požadavky na smluvní ujednání s dodavateli**
 - Smluvní standard
- **Příloha č. 4 - Doporučená témata pro rozvoj bezpečnostního povědomí**

Vyhláška má celkem 12 stran vč. příloh

Kontrola v oblasti KB

(režim nižších povinností)

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

9. listopadu 2023

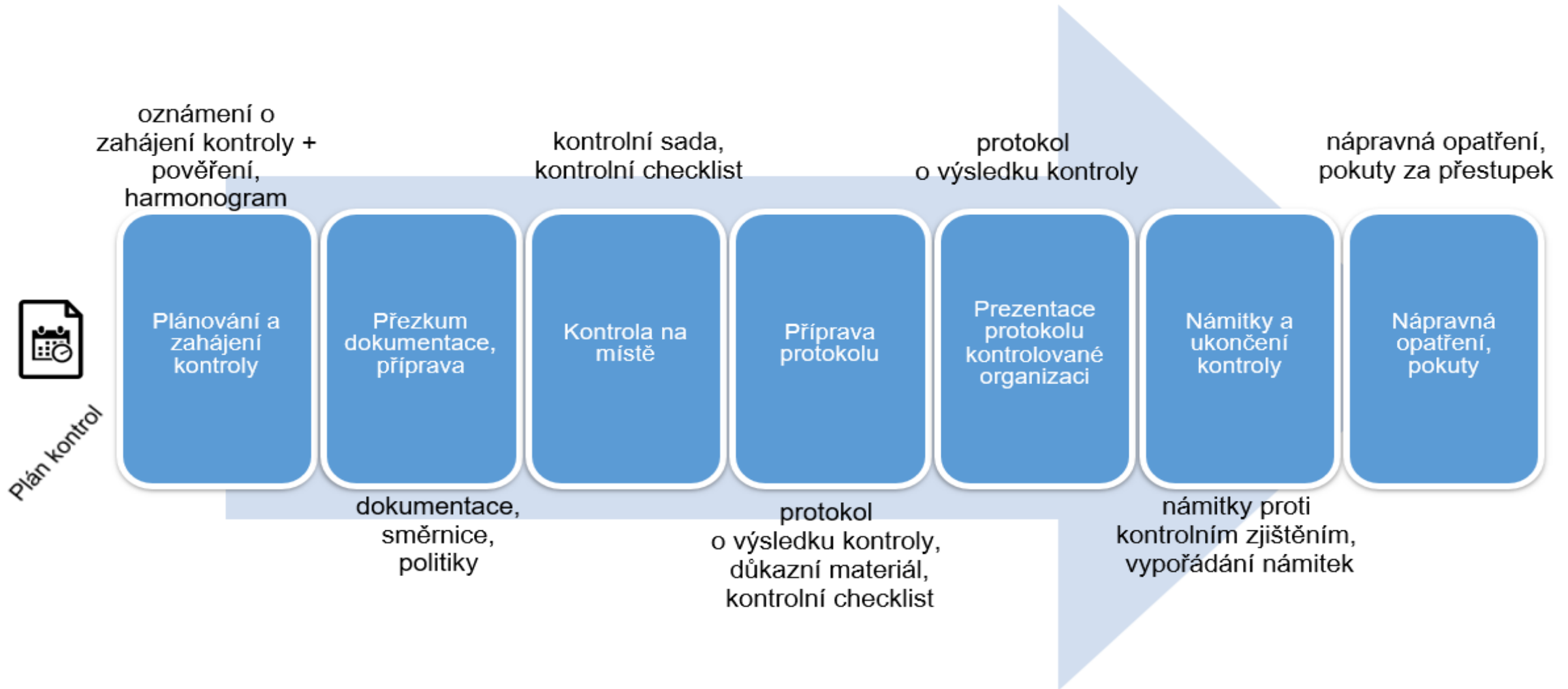
TLP:GREEN



- Kontrola plnění povinností vyplývajících ze ZKB, resp. VKB; zmocnění NÚKIB v ZKB
Prováděna podle kontrolního řádu a v souladu se správním řádem
- Při zjištění nesouladu se ZKB/VKB ukládána nápravná opatření, příp. pokuty za přestupek proti ZKB
- Charakteristiky kontroly:
 - roční plán kontrolní činnosti
 - rámcově 150 kontrolních bodů (vycházející ze ZKB a VKB)
 - délka kontroly cca 7 – 10 týdnů



- Pozorování
- Provádění interview
 - Otevřené otázky
 - Ujasnění, že kontrolující správně chápe vyjádření respondenta
- Přezkum dokumentace / záznamů dat
 - Před / v průběhu kontroly na místě
- Testování / simulace
 - Ukázky nastavení v praxi (např. pravidla na firewallu, práce se SIEM)
- Sběr důkazů
 - Fotografie, nahrávky dokumentace
 - Export nastavených politik
 - Atp.
- Vzorkování
 - Důležité vysvětlit i vrcholnému vedení povinné osoby



Klasifikace zjištění



Klasifikace/typ zjištění	Popis
Neshoda	Nesplnění požadavku podle stanovených kritérií nebo odchýlení praxe od dokumentovaných postupů v organizaci (nesoulad).
Shoda	Splnění požadavků podle stanovených kritérií (soulad).
Potenciální riziko	Typ zjištění, kdy kontrolující upozorňuje na nevhodné plnění požadavku stanovených kritérií, které může v budoucnu vést k neshodě. Může se také jednat o typ zjištění, kdy je plnění požadavku podmíněno předchozím splněním jiného požadavku.
Příležitost ke zlepšení	Příležitost ke zlepšení je typ zjištění, které má charakter doporučení a vychází ze zkušeností kontrolujícího.
Pozoruhodné úsilí	Nadstandardní hodnocení dané oblasti.



- **Organizační opatření**

- Systém řízení bezpečnosti informací
- Řízení aktiv
- Řízení rizik
- Organizační bezpečnost
- Bezpečnostní role
- Řízení dodavatelů
- Bezpečnost lidských zdrojů
- Řízení provozu a komunikací
- Řízení změn
- Řízení přístupu
- Akvizice, vývoj a údržba
- Zvládání kybernetických bezpečnostních událostí a incidentů
- Řízení kontinuity činností
- Audit kybernetické bezpečnosti
- Bezpečnostní politika a bezpečnostní dokumentace



- **Technická opatření**

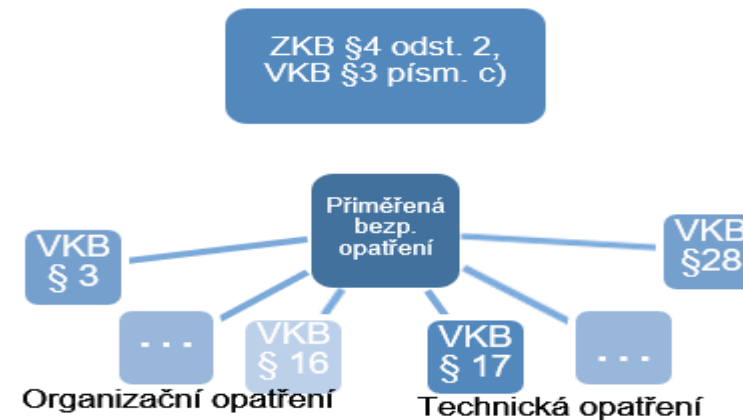
- Fyzická bezpečnost
 - Bezpečnost komunikačních sítí
 - Správa a ověřování identit
 - Řízení přístupových oprávnění
 - Ochrana před škodlivým kódem
 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů – logování
 - Detekce kybernetických bezpečnostních událostí - monitoring
- Sběr a vyhodnocování kybernetických bezpečnostních událostí - SIEM
 - Aplikační bezpečnost
 - Kryptografické prostředky
 - Zajišťování úrovně dostupnosti informací
 - Průmyslové, řídicí a obdobné specifické systémy



- Nedostatečná podpora KB vrcholovým vedením organizace
 - Neoprávněné výjimky pro top management
- Nedostatek zdrojů (lidských, finančních, ...) v oblasti KB
 - Může být rovněž znakem nedostatečné podpory vrcholovým vedení
- Neúplná, nevhodná, neschválená bezpečnostní politika a dokumentace



- Nepochopení základního principu VKB
 - Povinná osoba v rámci ISMS v souladu s:
 - VKB § 3 písm. a) - stanoví s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah systému řízení bezpečnosti informací, ve kterém určí organizační části a aktiva, jichž se systém řízení bezpečnosti informací týká
 - VKB § 3 písm. b) – stanoví cíle ISMS
 - VKB § 3 písm. c) - pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření

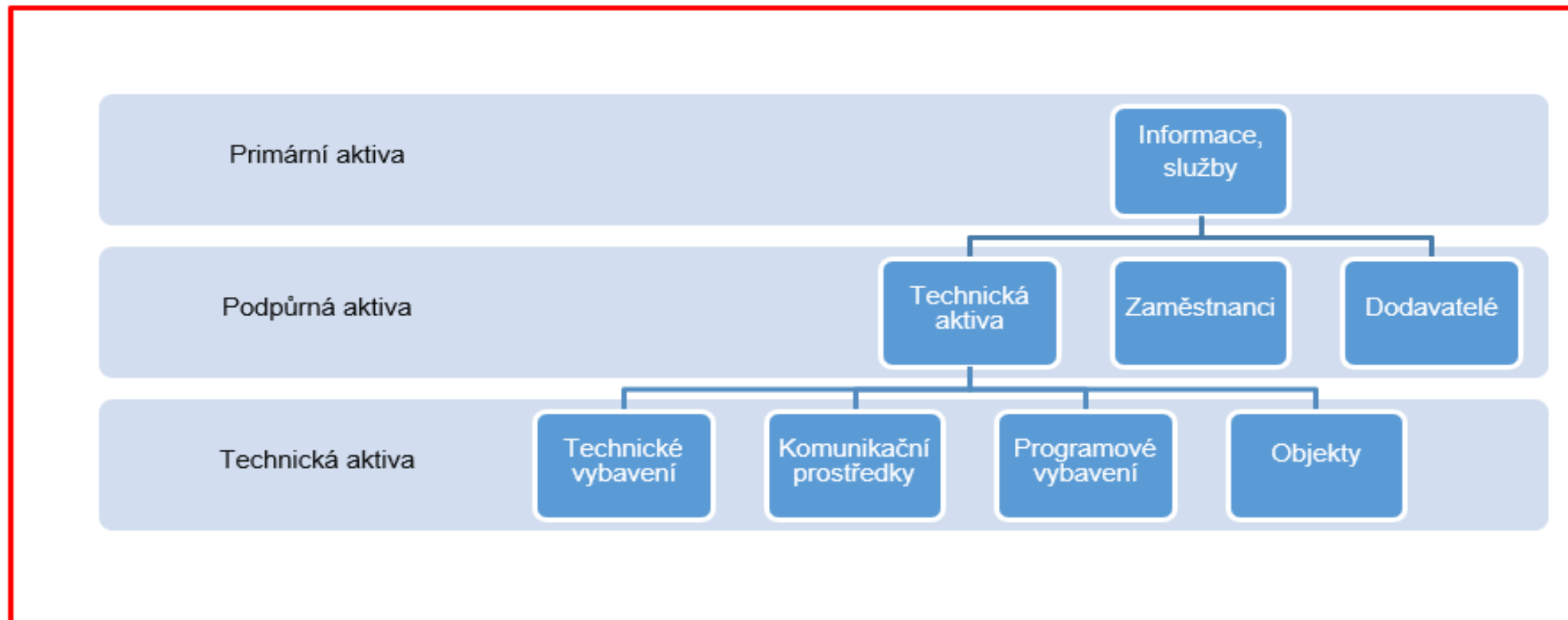


Nejčastější organizační nedostatky



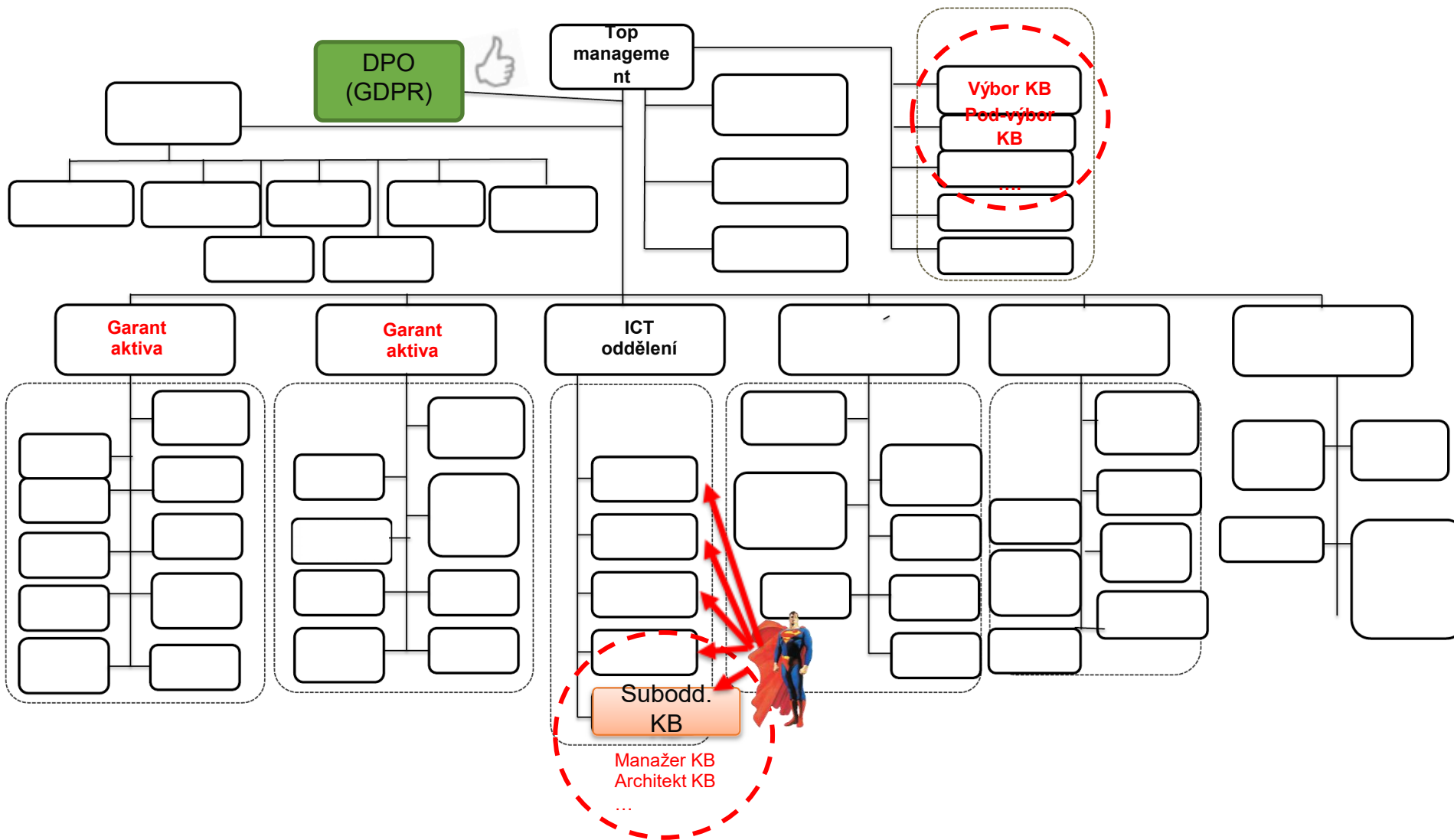
- Nevhodný rozsah ISMS
 - Bezpečnostní opatření tak nejsou zaváděna všude tam, kde by měla být

Rozsah ISMS





- KB a organizační struktura
 - Zbytečné složitosti – výbor, podvýbor, výbor z výboru atp.
 - Nevhodné organizační zařazení celku řešícího KB
 - Platové ohodnocení, oddělení rolí od provozu, výkon rolí externisty





- **Nedostatečné řízení aktiv a rizik**
 - Hodnocení rizik je často jen záležitostí IT
 - Hodnocení rizik je vytvořeno externí organizací pouze za účelem shody se ZKB, kontrolovaná osoba s jeho výsledky nikterak nepracuje a nerozumí jim
- **Prohlášení o aplikovatelnosti**
 - Neexistence
 - Obsahuje neaktuální / nepravdivé informace
 - Obsahuje pouze vybraná bezpečnostní opatření, nikoliv všechna z VKB
- **Plán zvládání rizik**
 - Neexistence
 - Nereflektuje výsledky hodnocení rizik

Nejčastější organizační nedostatky



- Bezpečnostní povědomí v oblasti KB
 - Často používaná fráze „uživatel je mnohdy nejslabší článek“, i přesto je v praxi vzdělávání uživatelů v oblasti KB podceňované a často je nedostatečné
- Závislost na dodavatelích
 - Snaha vše neřízeně outsourcovat
 - Smlouvy neřeší oblast kybernetické bezpečnosti

	SW KII	DC	Správa sítě	Servery a OS	Správa virtualizace	Správa dat	Internet	Konzultační služby	Koordinace
Správce KII									?
Dodavatel A	X								
Dodavatel B		X							
Dodavatel C			X						
Dodavatel D	X			X		X			
Dodavatel E					X				
Dodavatel F							X		
Konzultant (1 ... N)								X	?



- Řízení změn
 - Neurčování významných změn dle VKB
 - Neprovádění přezkumu možných dopadů změn
 - Nezohledňování vlivu na kybernetickou bezpečnost
- Řízení kontinuity činností
 - Nestanovení cílů řízení kontinuity činností
 - Není provedena analýza dopadů
 - Neexistují plány kontinuity činností a havarijní plány případně neprobíhá jejich testování
 - Dokumentace k řízení kontinuity činností není vypracována, případně není aktuální a neodpovídá potřebám organizace
 - SLA neodpovídají požadavkům na dostupnost, které organizace stanovila v rámci hodnocení aktiv nebo analýzy dopadů
 - Požadavky na dostupnost stanovuje IT samostatně, bez konzultace s garanty primárních aktiv, příp. vedením organizace



- **Nedostatečná zpětná vazba a přezkum**
 - Nепrovádění interního auditu v oblasti kybernetické bezpečnosti
 - Nevyhodnocování účinnosti ISMS
- **Kybernetické bezpečnostní incidenty**
 - Je využívána vlastní definice KBI
 - Nedochozí k bezodkladnému hlášení KBI NÚKIB
 - Nevedení evidence KBI a jejich zvládnání
- **Audit kybernetické bezpečnosti**
 - Nепrobíhá v adekvátním intervalu
 - Nevhodná míra detailu
 - Nепředávání výsledků auditu správcům IS



- Špatně stanovený rozsah ISMS
- Řízení aktiv neprobíhá v souladu s požadavky
- Řízení rizik neprobíhá dostatečně
- Není vytvořeno prohlášení o aplikovatelnosti
- Bezpečnostní role nemají stanovenou zastupitelnost
- Významní dodavatelé/provozovatelé nejsou informováni
- Neprobíhá řízení rizik u dodavatelů
- Nejsou určovány významné změny
- Subjekty s ISO certifikací nezohledňují dostatečně požadavky vyhlášky.

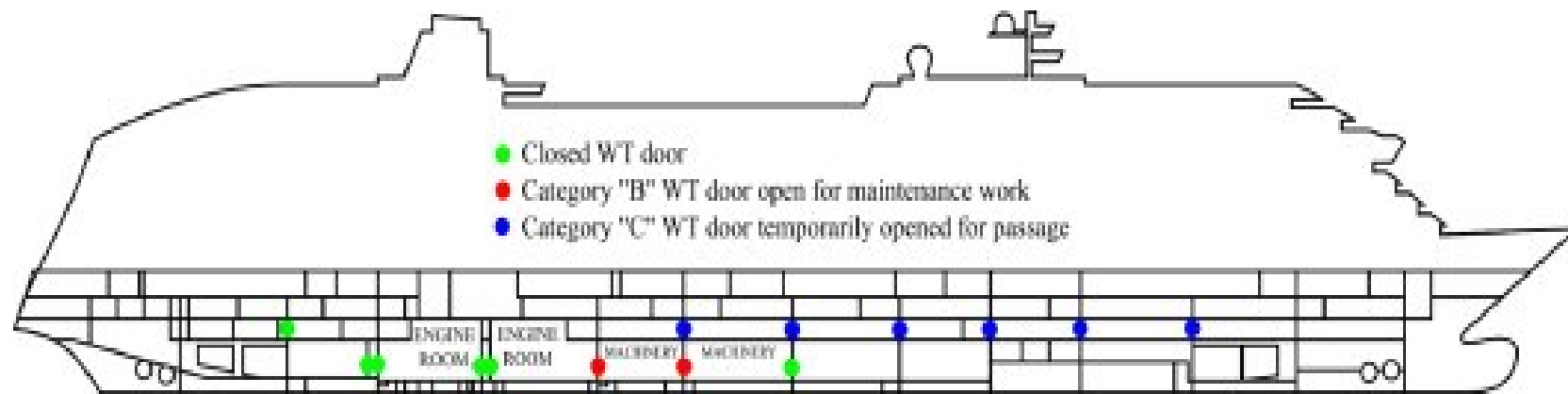
- Fyzická bezpečnost
 - Nezamezení neoprávněného přístupu do vymezených prostor
 - Nezamezení možného poškození a zásahů ve vymezených prostorech
 - Absence preventivních opatření (bezpečnostní a požární alarmy, dvojitá podlaha - pro odvod vody nebo klimatizace, KAMEROVÝ SYSTÉM, MFA se záznamem přístupu
 - V serverovně se nachází hořlavý materiál





- Bezpečnost komunikačních sítí
 - Segmentace komunikační sítě není dostatečná, nebo není komunikace dostatečně řízena
 - Není zajištěna důvěrnost a integrita dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě prostřednictvím bezdrátových sítí.
zajištění důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do
 - Nedostatečně oddělená provozní část komunikační sítě od kontrolovaných systémů
 - nedostatečné aktivní blokování nežádoucí komunikace
 - Existence nezabezpečených ethernetových přístupů

- Bezpečnost komunikačních sítí
 - Granularita segmentů
 - Příliš velká - vyšší riziko
 - Příliš malá - nároky na údržbu





- Správa a ověřování identit
 - Požadavky na Hesla neodpovídají VKB
 - Neochota k zavádění 2FA
 - Neřízení oprávnění pro čtení zápis a změnu dat

Ochrana před škodlivým kódem

- Absence whitelisting
- Mobilní telefony nemají nasazeno MDM
- Ochrana před škodlivým kódem není nasazena na všech serverech
- Není řízení automatické spuštění obsahu výměnných datových nosičů





- Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
 - Neuchovávání záznamů o událostí dle požadavku VKB / absence nástroje
 - Nejednoznačná identifikace účtu, pod kterým byla činnost provedena
- Aplikační bezpečnost
 - Penetrační testy nejsou prováděny dle požadavků VKB § 25 odst. 1 (na důležitých aktivech před jejich uvedením do provozu)
 - Nedostatečná nebo pozdní mitigace již odhalených nedostatků



- Při stanovení úrovně zabezpečení a výběru konkrétních bezpečnostních opatření je potřeba v souladu se zákonem a vyhláškami **zohlednit specifika organizace a důležitost jednotlivých systémů a služeb** (není smyslem zavádět nesmyslná a nákladná řešení tam, kde to pro vaši organizaci nemá význam).
- Pokud vaše organizace kybernetickou bezpečnost do této chvíle systematicky neřešila, lze doporučit jako výchozí krok především **zmapování aktuálního stavu organizace** (tzn. audit aktuálního stavu kybernetické bezpečnosti a potenciálních slabých míst) a vypracováním **business impact analýzy** (zejm. jaké by byly dopady narušení řádného fungování jednotlivých systémů na vaši organizaci; nejde přitom jen o nedostupnost používaných informačních systémů, ale i o narušení důvěrnosti nebo integrity shromažďovaných dat).
- Již v této fázi je dobré se zaměřit na **školení relevantních osob** v organizaci – základní školení pro všechny uživatele, odborné školení pro osoby, které v organizaci řeší/budou řešit kybernetickou bezpečnost, nezapomínat přitom i na vrcholný management (management si musí být vědom důležitosti řízení kybernetické bezpečnosti v organizaci).
- **Rozhodně nedoporučujeme nakupovat služby typu „posoudíme soulad vaší organizace s NIS2“ nebo „zavedeme vám v organizaci NIS2“.** Nenechte se napálit „vševědoucími“ implementátory NIS2 na klíč. Směrnice NIS2 žádné konkrétní požadavky neupravuje, vše bude obsaženo až v novém zákoně o kybernetické bezpečnosti, který je teprve připravován a bude platit až od poloviny roku 2024 a bude mít implementační lhůtu 1 rok.
- Z technických opatření lze obecně doporučit nasadit **firewally** (zejména perimetrové), **antiviry** (zejména sofistikovanější EDR), a **zálohovací řešení**. Společně s prováděním **aktualizací** (tam kde je to možné) se jedná o věci, které by měly být dávno běžnou součástí chodu každé organizace a výše zmiňovanou osvětu a školení.



Díky za pozornost!

regulace@nukib.cz