

POVINNOSTI VYPLÝVAJÍCÍ Z NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

*„Kybernetická a informační bezpečnost
není otázkou zákonů,
je otázkou pudu sebezáchovy.“*

Aleš Špidla (2014)

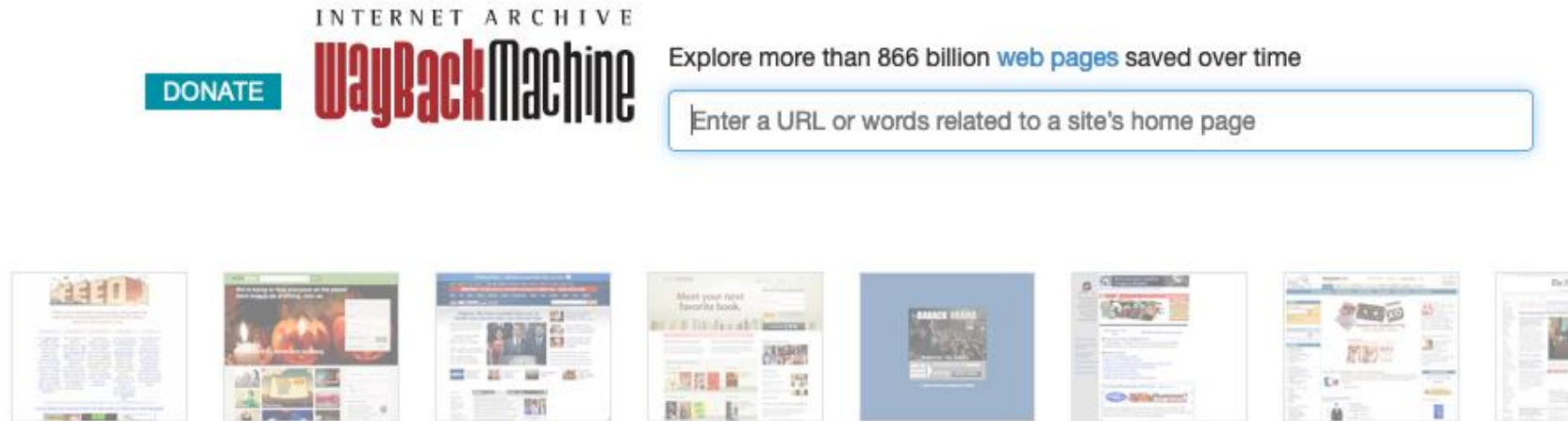
Co se vlastně snažíme chránit?

Digitální identita



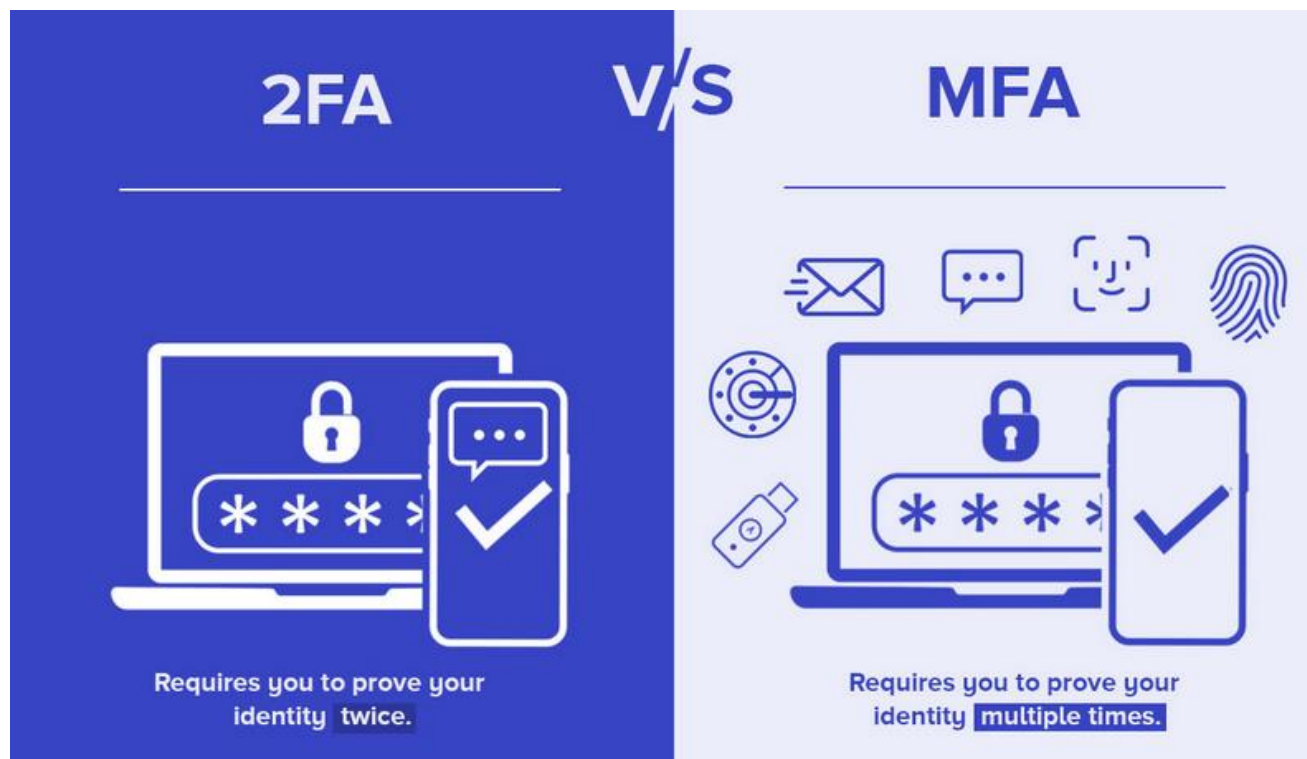
- ekvivalent člověka v digitálním světě
 - informace a data, která identifikují jednotlivce v digitálním světě
- bankovní identita (silné ověření)
 - kvalifikovaný digitální podpis (silné ověření)
 - zaměstnanecký / uživatelský účet v podnikové aplikaci
 - uživatelský účet Google
 - uživatelský účet AppleID
- Mobilní klíč eGovernmentu
 - eObčanka
 - I.CA identita
 - MojID

Digitální stopa



- Internet nemá klávesu “Delete”
- jakákoliv informace, která se na internetu objeví, už nikdy nezmizí
- stránka archive.org vám umožní „cestovat časem“
- aktivní a pasivní digitální stopa

MFA – vícefaktorová autentizace



Autentizace

postup, pomocí kterého dochází k ověření identity osoby

Multifaktorová autentizace

pro ověření totožnosti nestačí pouhé zadání přihlašovacího jména a hesla, ale je zapotřebí totožnost potvrdit nějakým dalším způsobem

Bezpečné chování v on-line světě



1. Chraňte si své osobní údaje
2. Věnujte čas nastavení soukromí
3. Surfujte bezpečně
4. Používejte bezpečné připojení
5. Nezanedbávejte hesla
6. Stahujte opatrně
7. Platě obezřetně
8. Hlídejte si posty
9. Buďte opatrní při setkávání
10. Hlídejte si antivirus

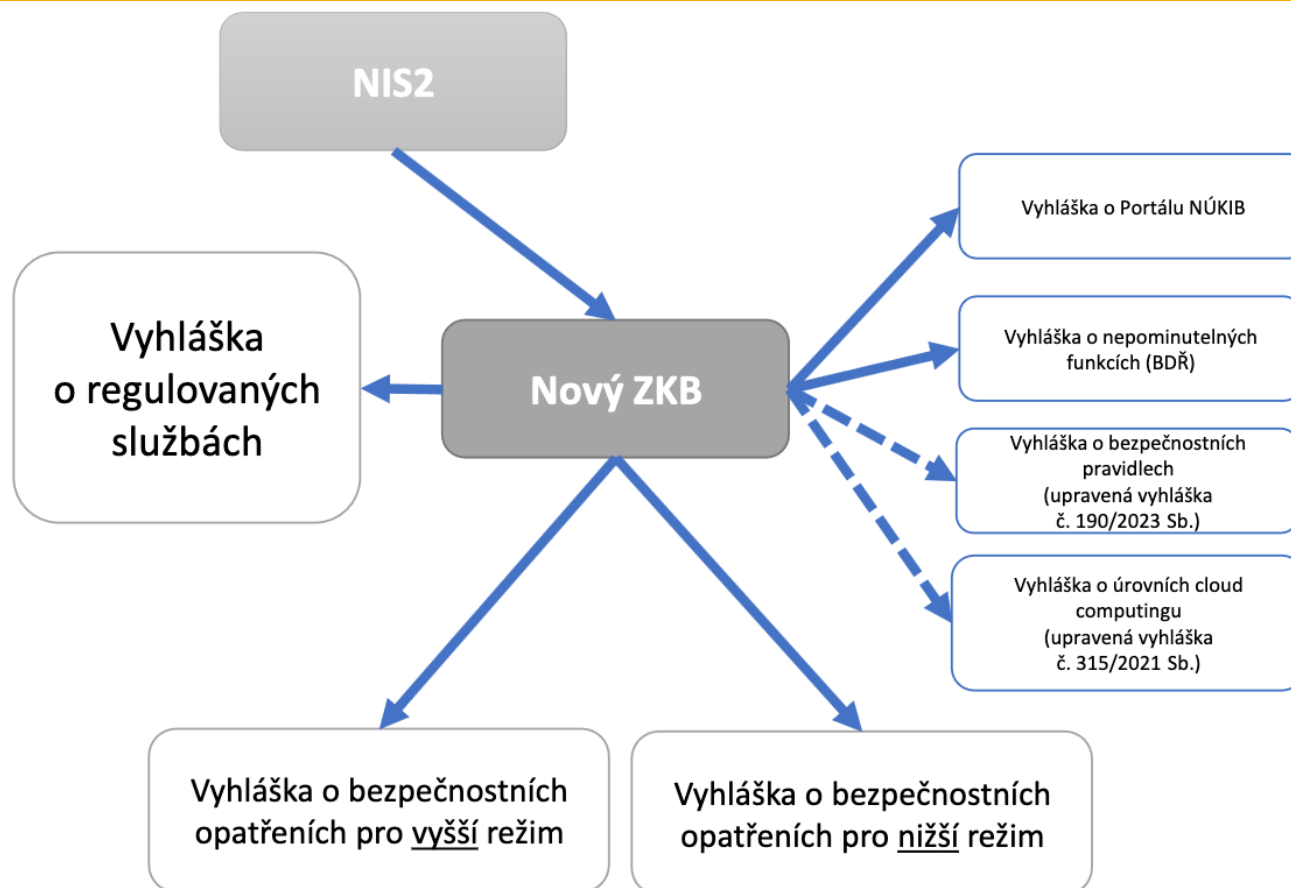
Struktura právních předpisů nZKB

Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo **potřeba vytvořit nový zákon**

= zcela nová úprava – 74 paragrafů

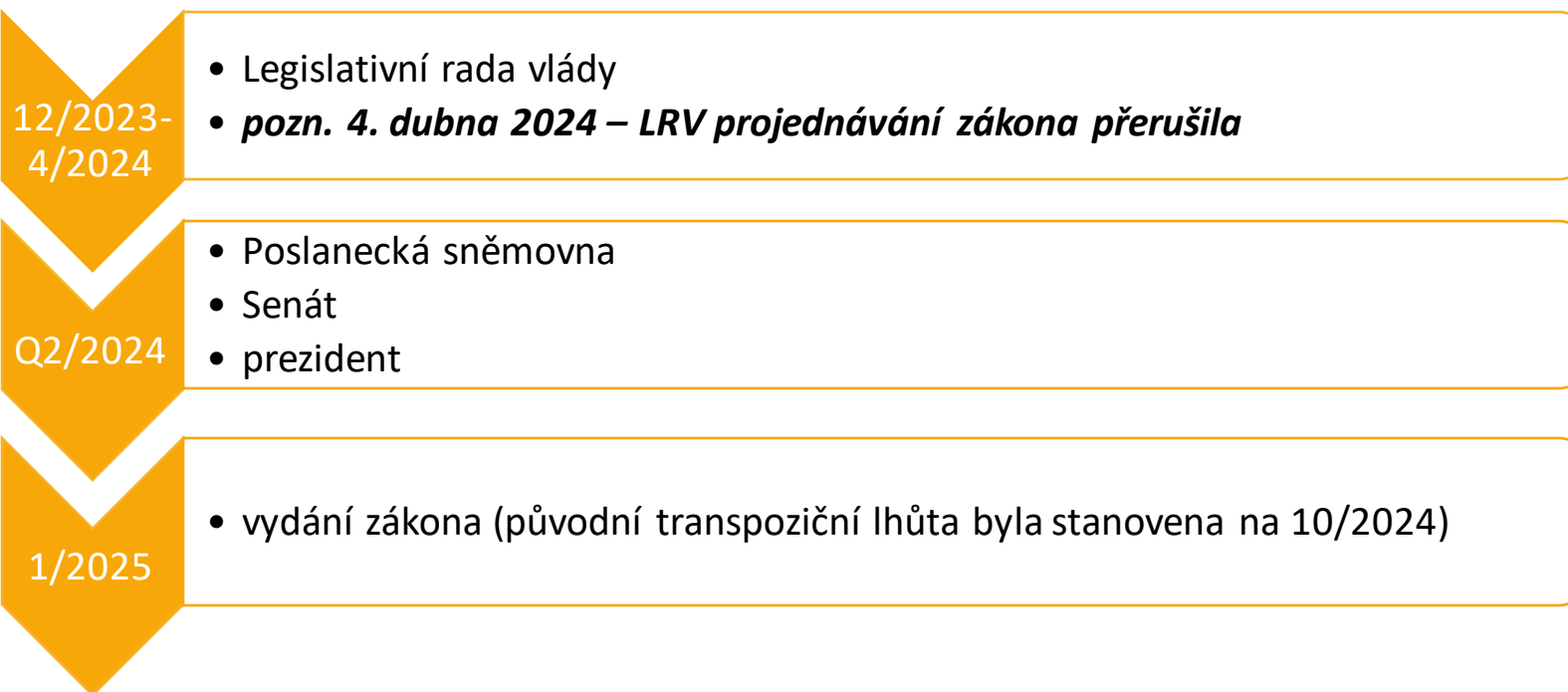
Verze v mez. připomínkovém řízení má aktuálně navíc **7 vyhlášek**

Celý návrh zveřejněn na webu nis2.nukib.cz



Harmonogram legislativního procesu

Mezirezortní připomínkové řízení (MPŘ) – skončeno



Vyhlášky budou mít samostatný legislativní proces

Základní povinnosti dle nového ZKB

- stanovení rozsahu řízení bezpečnosti informací
- samoidentifikace – zápis na portál NÚKIB
- zavedení bezpečnostních opatření (organizační + technická)
- hlášení kybernetických bezpečnostních incidentů
- řízení bezpečnosti dodavatelského řetězce
- reakce na opatření a výstrahy dle NÚKIB
- informování uživatelů služeb o kybernetických bezpečnostních incidentech
- řízení významných dodavatelů

Vyhláška o regulovaných službách

- a) kritéria pro identifikaci regulovaných služeb
- b) stanovení režimů poskytovatele regulované služby
- c) kritéria pro identifikaci strategicky významné služby (§ 27 odst. 1 zákona)

NZKB při identifikaci kombinuje

- kritérium služby
- kritérium poskytovatele

Vyhláška o regulovaných službách

| Služba | Kritérium poskytovatele regulované služby a jeho režim pro tuto službu |
|--|--|
| 2.1. Výroba elektřiny | <p>Držitel licence na výrobu elektřiny podle energetického zákona je</p> <p>I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že</p> <p>a) je velkým podnikem, nebo</p> <p>b) disponuje výrobnou s celkovým instalovaným elektrickým výkonem nejméně 100 MW,</p> <p>II. poskytovatel regulované služby v režimu nižších povinností, v případě, že</p> <p>a) je středním podnikem, nebo</p> <p>b) disponuje výrobnou s celkovým instalovaným elektrickým výkonem nejméně 50 MW, avšak méně než 100 MW.</p> |
| 2.2. Provoz přenosové soustavy elektřiny | <p>Držitel licence na přenos elektřiny podle energetického zákona je poskytovatel regulované služby v režimu vyšších povinností.</p> |

Vyhláška o regulovaných službách

Kritérium služby

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

Vyhláška o regulovaných službách

Kritérium poskytovatele

- ZKB pracuje s definicí středních a velkých podniků
- doporučení Komise 2003/361/ES ze dne 6. května 2003
- uživatelská příručka k definici malých a středních podniků

| Kategorie podniku | Počet zaměstnanců: Roční pracovní jednotka (RPJ) | Roční obrát | nebo | Roční bilanční suma |
|-------------------|---|---|------|---|
| střední | < 250 | ≤ 50 milionů € (v roce 1996 40 milionů €) | nebo | ≤ 43 milionů € (v roce 1996 27 milionů €) |
| malý | < 50 | ≤ 10 milionů € (v roce 1996 7 milionů €) | nebo | ≤ 10 milionů € (v roce 1996 5 milionů €) |
| mikropodnik | < 10 | ≤ 2 miliony € (dříve nedefinováno) | nebo | ≤ 2 miliony € (dříve nedefinováno) |

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

Organizační opatření

- systém řízení bezpečnosti informací
- povinnosti vrcholného vedení
- bezpečnostní role
- řízení bezpečnostní politiky a bezpečnostní dokumentace
- řízení aktiv
- řízení rizik
- řízení dodavatelů
- bezpečnost lidských zdrojů
- řízení změn
- akvizice, vývoj a údržba
- řízení přístupu
- zvládání kybernetických bezpečnostních událostí a incidentů
- řízení kontinuity činností
- audit kybernetické bezpečnosti

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

Technická opatření

- fyzická bezpečnost
- bezpečnost komunikačních sítí
- správa a ověřování identit
- řízení přístupových oprávnění
- detekce kybernetických bezpečnostních událostí
- zaznamenávání událostí
- vyhodnocování kybernetických bezpečnostních událostí
- aplikační bezpečnost
- kryptografické algoritmy
- zajišťování dostupnosti regulované služby
- zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

Nezbytný rozsah dostupnosti strategicky významné služby

Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v nezbytném rozsahu, který je stanoven v příloze č. 9 této Vyhlášky

b) Odvětví 2. Energetika - Elektřina, služba 2.1. Výroba elektřiny, bod I. písm. b),

Nezbytným rozsahem je výroba ve zdroji s celkovým instalovaným elektrickým výkonem nejméně 100 MW.

c) Odvětví 2. Energetika - Elektřina, služba 2.2. Provoz přenosové soustavy elektřiny,

Nezbytným rozsahem je provoz přenosové soustavy elektřiny.

d) Odvětví 2. Energetika - Elektřina, služba 2.3. Provoz distribuční soustavy elektřiny, bod I. písm. b),

Nezbytným rozsahem je provoz distribuční soustavy elektřiny jejíž přenosová kapacita je nejméně 220 MW.

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

Přílohy

1. Identifikace a hodnocení aktiv
2. Hodnocení rizik
3. Zranitelnosti a hrozby
4. Likvidace dat
5. Obsah bezpečnostní politiky a bezpečnostní dokumentace
6. Výbor pro řízení kybernetické bezpečnosti a bezpečnostní role
7. Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy
8. Doporučená témata pro rozvoj bezpečnostního povědomí
9. Stanovení nezbytného rozsahu dostupnosti strategicky významných služeb

Jak přistoupit k zavádění bezpečnosti?

Přehled v organizaci

- Jaké poskytují služby?
- Co pro poskytování služeb potřebují?
- Z toho vyplývá rozsah, ve kterém KB řeším.

Aktuální stav KB

- Mám již zavedena některá opatření?
- Zdokumentuji aktuální stav zavedených a nezavedených opatření (audit KB).

Určení priorit

- Jaké mám finanční a personální kapacity?
- Co je má prioritní služba?
- Stanovím plán zavádění bezpečnostních opatření, odůvodním případné nezavedení nepovinných.

Zavádění opatření

- Určím osobu/výbor odpovědný za KB.
- Priorita vzdělávání zaměstnanců vč. vedení.
- Vytvořím bezpečnostní politiku, kterou lze fakticky používat.
- Pokračuji dle plánu.

Zásada přiměřenosti:

Náklady na zaváděné opatření by neměly převyšovat náklady na případnou realizaci kybernetického incidentu.

Nechci všechno najednou, postupně se zlepšuji.

Praktická použitelnost:

Šablonovitá dokumentace nikdy nebude používána a nebude sedět mé organizaci

Příliš složitý systém nebudu mít kapacitu udržovat