(nový) Zákon o kybernetické bezpečnosti

-

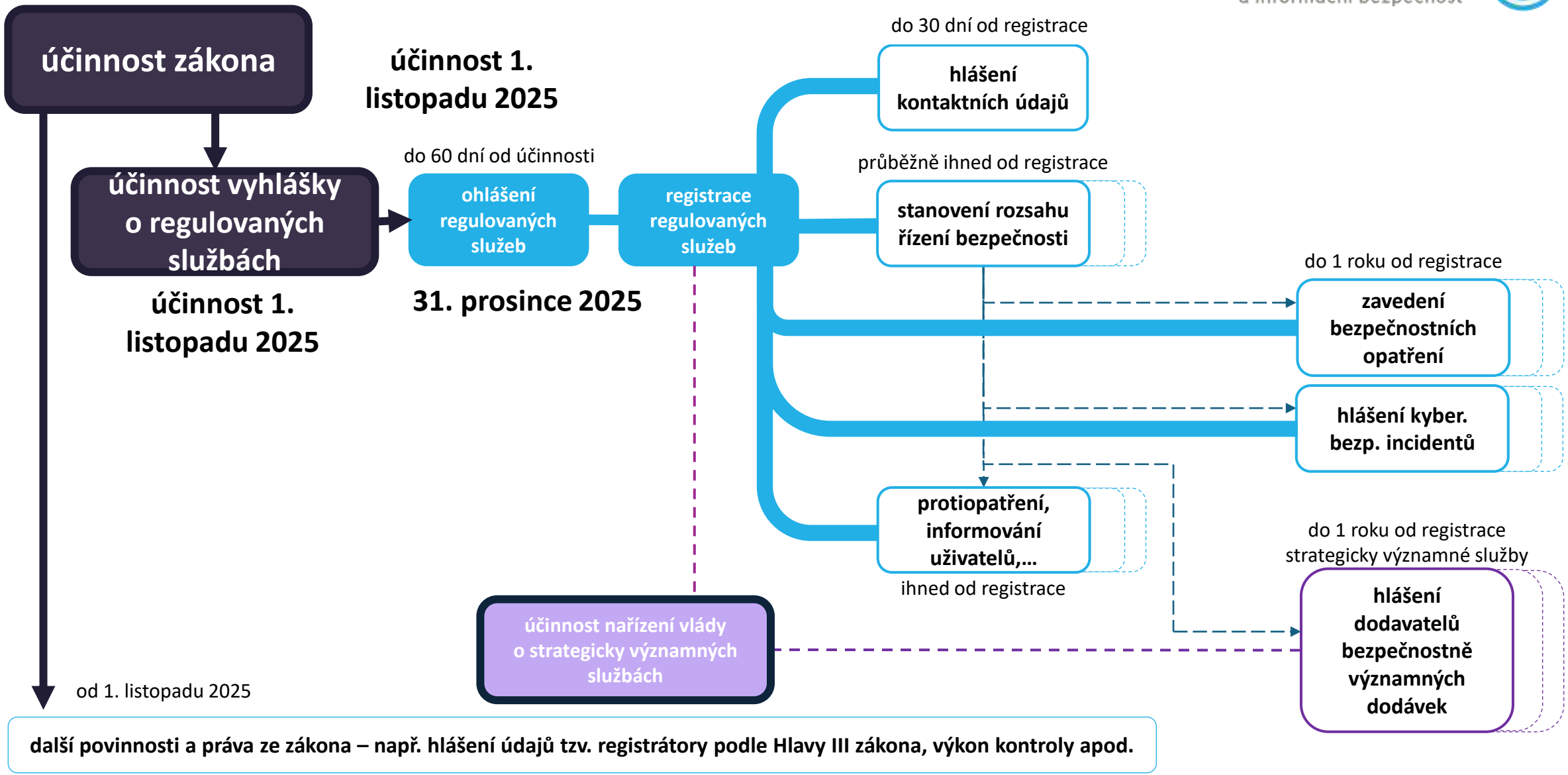
jak vypadá implementace

Tomáš Krejčí
náměstek ředitele NÚKIB

Adam Kučínský
ředitel odboru regulace

ISSS
19.5.2026

Národní úřad pro kybernetickou a informační bezpečnost



Co nový ZKB přinesl

- Hodně starostí

- Společný EU rámec kybernetické bezpečnosti
- Standardizace bezpečnostních opatření
- Odpovědnost vrcholového vedení za KB je legislativně ukotvena
- Konkrétní lhůty na hlášení incidentů

- Meziroční nárůst povinných osob pod ZKB o více než 1000%

Vývoj počtu povinných osob pod ZKB

Rok	Počet subjektů (KII, VIS, PZS, od roku 2026 PRS)	Procentuální nárůst subjektů oproti předchozímu roku	Poznámka
2015	50	není předchozí rok	účinnost první generace ZKB
2016	96	92%	
2017	101	5%	transpozice NIS1 a zřízení NÚKIB
2018	104	3%	
2019	154	48%	Odbor regulace měl 8 lidí celkem
2020	170	10%	
2021	265	56%	
2022	344	30%	
2023	421	22%	
2024	420	0%	
2025	458	9%	od 1.11.2025 účinnost nZKB (NIS2)
2026	**5437**	**1087%**	**stav k 30.3.2026** (na odboru regulace se tomu věnuje 18 lidí)
2027	5981	10%	PREDIKCE
2028	6579	10%	PREDIKCE
2029	7237	10%	PREDIKCE
2030	7960	10%	PREDIKCE
2031	8756	10%	PREDIKCE

Pár zajímavých momentů z přípravy

- Schválení v PSP
  - Přítomno: 166 (2014) x 165 (2025) – z toho pro návrh: 161 (2014) x 159 (2025), proti návrhu: 0 (2014) x 0 (2025)
  - Nepřihlášen, omluven, zdržel se: 39 (2014) x 41 (2025)
- Zákon v Poslanecké sněmovně strávil celkem 9 měsíců (od 25. července 2024 do 13. května 2025).
- Senát schválil zákon 66 hlasy pro, 1 proti
- Zákon prošel 5 legislativními informačními systémy (eKlep Úřadu vlády, Informační systém PSP, systém na Senátní tisky, proces ve Sbírce zákonů, E-sbírka)
- Byl na stole návrh, aby všechny vyhlášky vydávala vláda jako nařízení
- Byl na stole návrh, aby vyhlášky byly vydávány ve spolugesci s 11 dalšími ministerstvy
- Připomínky k zákonu i vyhláškám byly v některých případech stejné od některých úřadů a soukromého sektoru (vč. překlepů☺)
- U vyhlášek uděleny výjimky z RIA, následně pak nebyly uznány
- NÚKIB navrhoval do vyhlášky o regulovaných službách např. výjimku pro charity poskytující zdravotnické služby
- Neprošla novela správního řádu – není umožněno automatizované podepisování rozhodnutí – pečetit (se pak těžko digitalizuje) – komplikace přípravy nových systémů
- Výjimku na „soláry“ kterou jsme navrhovali již v roce 2022 EK teď navrhuje v rámci revize NIS2 ☺ ☺

nZKB – jak jsme museli připravit NÚKIB

Situace – z 450 „zákazníků“ jdete na 6.000 – hned, bez navýšení lidí a peněz – super úřad což?

Řešení

- Co jde to automatizovat
- Vytvořit portál – jednotnou platformu, přes kterou se bude vše dělat
- Přenastavit všechny procesy (všechno co jste měli doteď už neplatí)
- Vše musí fungovat podle stejných pravidel – žádné výjimky
- Na všechno musí být postup a návod – aby bylo standardizované – škálovatelnost
- Stovky dotazů – trackovací systém
- Procesy musíte řešit tak jak přicházejí, velmi tvrdá prioritizace

Nevýhody

- Nelze individuální přístup
- Málo času na „edge cases“
- Vysoká zátěž pro lidi
- Hodně změn – nutno uřídit
- Není čas na rozvoj jiných aktivit

Problémy při tvorbě Portálu NÚKIB

- Legislativní problémy
  - **Správní řád z Rakouska-Uherska**
  - generická „jednoduchá“ rozhodnutí musí mít také **kvalifikovaný el. podpis**
  - obecně se tlačí na digitalizaci a automatizaci, ale správní řád na to nereaguje
  - **Krátký čas na přípravu - legislativní proces** – parametry, pojmy a procesy se mění pod rukama

- Finanční problémy
  - Mezirezort: „*MF požaduje, aby **rozpočtové dopady** připravovaného zákona byly zabezpečeny v rámci schválených finančních limitů kapitoly NÚKIB a v rámci schválených finančních limitů příslušných dotčených kapitol státního rozpočtu **bez požadavku na jejich navýšení**.*“
  - Interní vývoj

- eGov problémy
  - Portál musí být napojen na XY dalších systémů (spisová služba, datovky, registry, NIA…)
  - Každý systém funguje trošku jinak, má jiné nároky, možnosti, odstávky a limity.
  - Nastavení a automatizace procesů je pak dost komplikované + se tyto systémy neustále vyvíjí
  - Aktualizace a změny funkcionalit sytémů

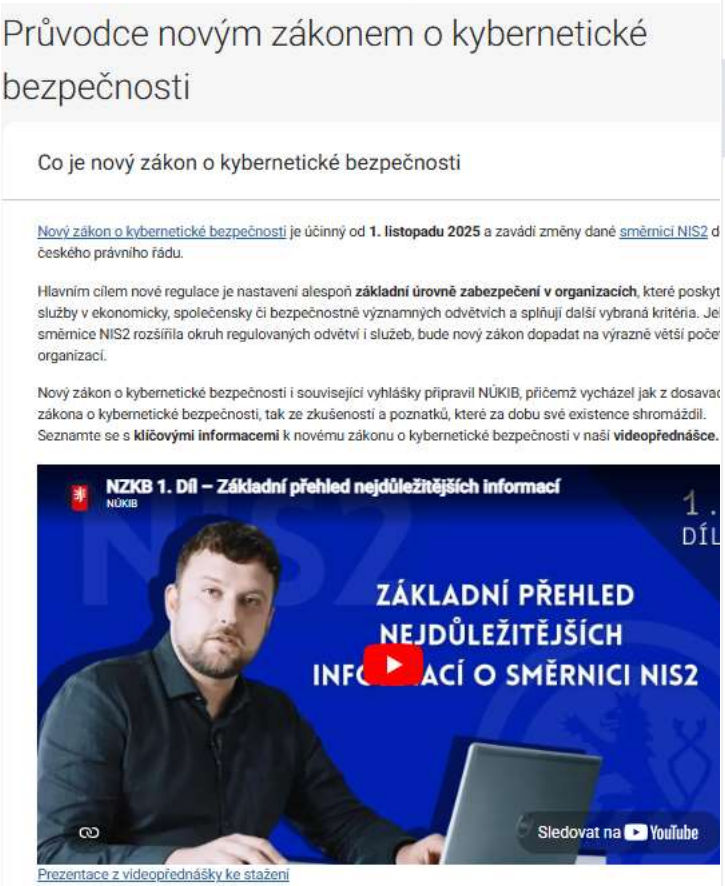
nZKB aktuálně

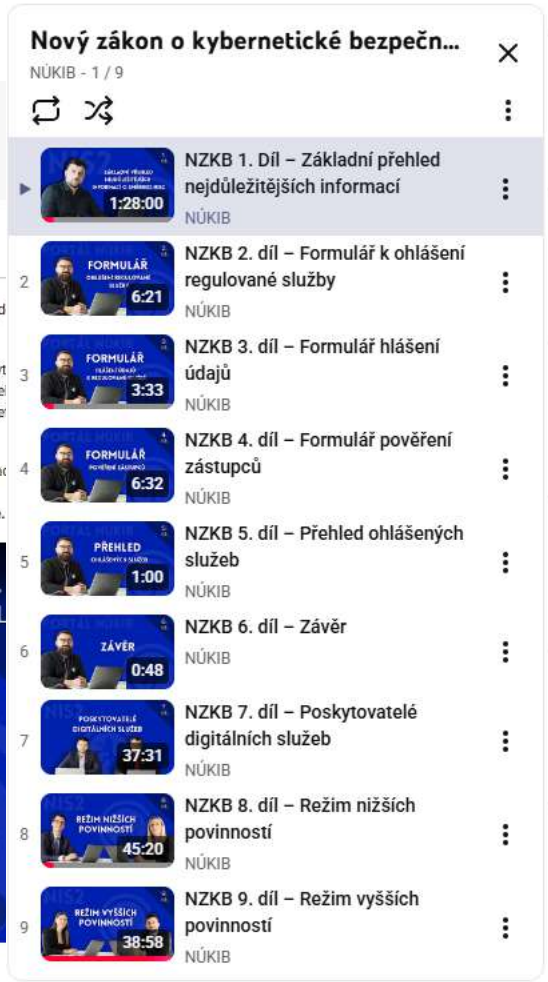
- Aktuální statistiky
  - Ohlášených poskytovatelů = 5700+ (aktuální přírůstek v desítkách týdně)
  - Registrovaných regulovaných služeb = 8000+
  - Nejvíc denních registrací 18. prosince 2025 – 409 (štědrý den 9, silvestr 175, nový rok 7)
  - Návštěvnost portálu = týdně cca 7k návštěv, cca 5k jedinečných návštěvníků
  - Počet dotazů k zákonu = prosinec 2026 - 300, nyní 391 od začátku roku (RT OREG)

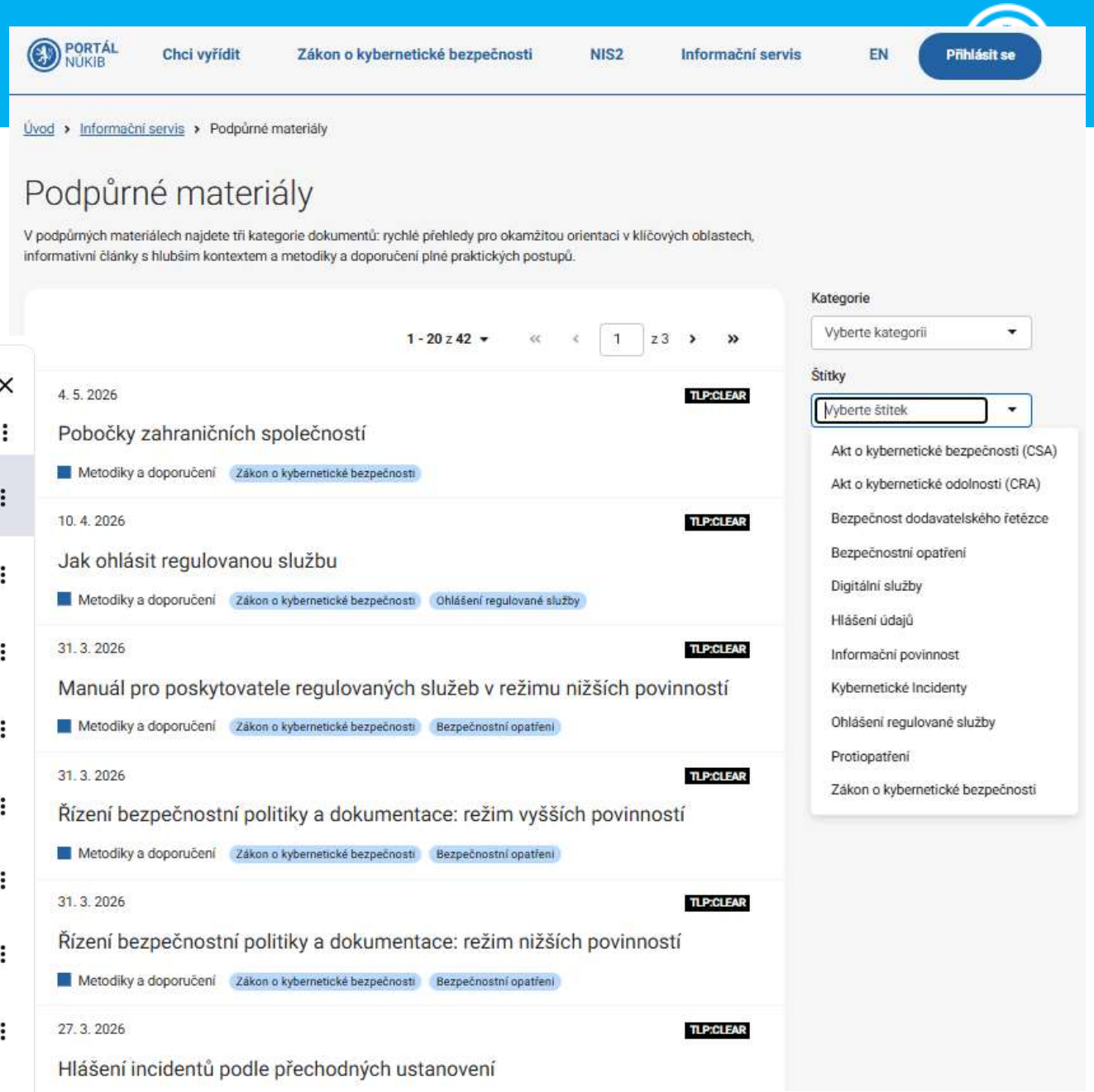
- Co nyní je/bude:
  1. Připomenutí – neadresná komunikační kampaň – proběhlo
  2. Oslovení těch co měli přijít a nepřišli – probíhá
  3. Prověření těch, co na 2 nereagovali, nebo tvrdí, že nesplňují kritéria - chystáme
  4. Určení těch co splňují kritéria – zaregistrování ex offo - chystáme
  5. Předání 4 k přestupkovému řízení
  6. Přestupkové řízení
  7. Sankce

Nové podpůrné materiály

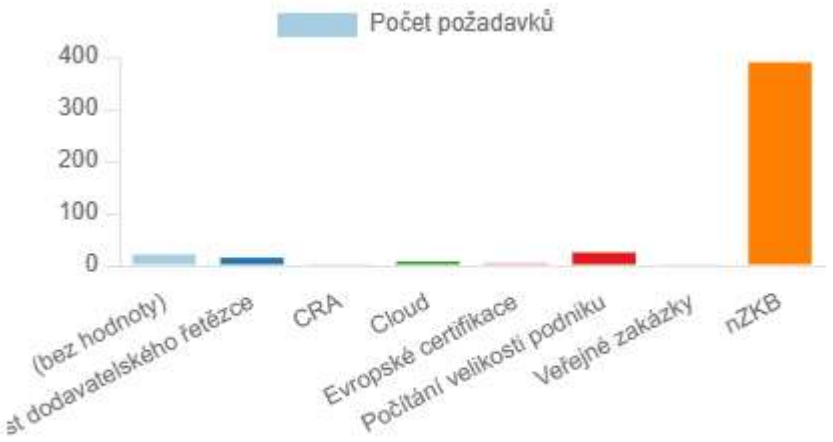
- Nové podpůrné materiály
  - vydáno 29 nových podpůrných materiálů
  - 13 v přípravě
- Videonávody



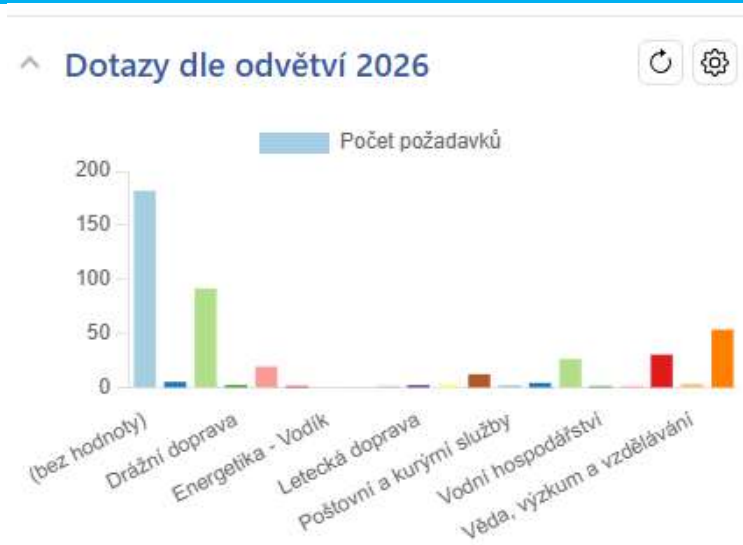




Kdo se ptá a na co…



Custom field Specifikace dotazu	Počet požadavků
(bez hodnoty)	21
Bezpečnost dodavatelského řetězce	15
CRA	3
Cloud	8
Evropské certifikace	5
Počítání velikosti podniku	25
Veřejné zakázky	1
nZKB	390



Data k 29. 4. 2026

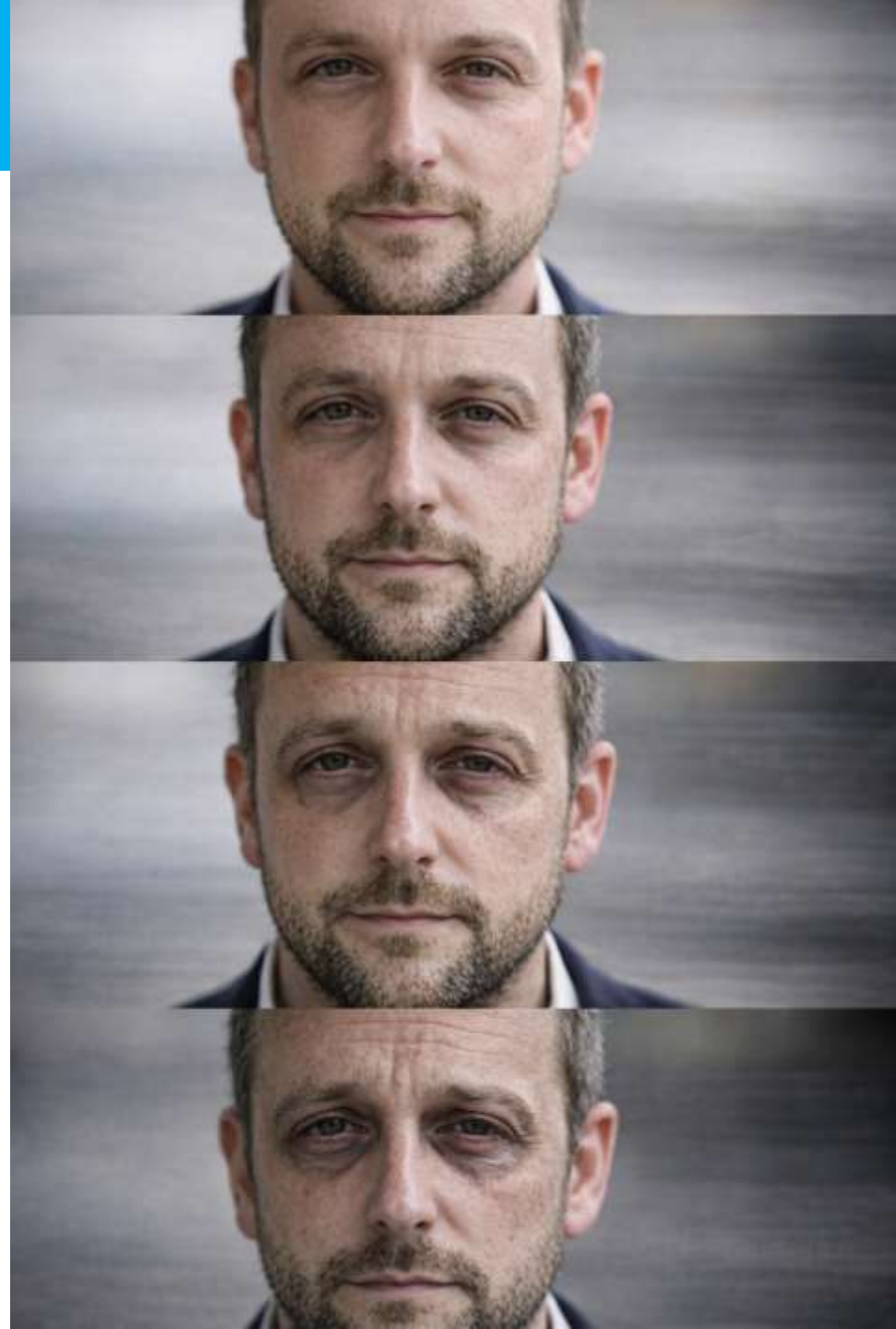
Custom field Odvětví	Počet požadavků
(bez hodnoty)	182
Chemický průmysl	6
Digitální infrastruktra a služby	92
Drážní doprava	3
Energetika - Elektřina	20
Energetika - Plynárenství	2
Energetika - Vodík	1
Energetika- Ropa a ropné produkty	1
Finanční trh	2
Letecká doprava	3
Odpadové hospodářství	4
Potravinářský průmysl	13
Poštovní a kurýrní služby	3
Silniční doprava	5
Veřejná správa a výkon veřejné moci	27
Vodní hospodářství	2
Vojenský průmysl	2
Výrobní průmysl	31
Věda, výzkum a vzdělávání	4
Zdravotnictví	54

Časté otázky

- Počítání velikosti podniku?
- My nejsme důležití!?
- Jaké ip adresy/rozsahy nehlásit?
- Kam v organizaci zařadit manažera kybernetické bezpečnosti?
- Jak sladit požadavky na digitální regulované služby a nedigitální regulované služby?
- Jak probíhá kontrola v přechodném období – co se kontroluje?
- Co když nějaké opatření zavést nejde?
- Co když nestíhám zavést bezpečnostní opatření v přechodné době?
- Dostanu pokutu, když se zaregistruju pozdě?
- …

nZKB – F*CK UPY

- Myslíte si, že lidi si přečtou, co jim píšete
  - Když vám na výzvu dojde 600 dotazů
- Myslíte si, že firmy zareagují na výzvu
  - Z 2,6 K obeslaných jich 1 K nereagovalo
- Myslíte si, že 1 a 1 jsou 2 a o tom se nediskutuje
  - I když je jasné naplnění kritérií, stejně se někdo hádá
- ~~Myslíte si~~ Doufáte, že stát má data správně
  - Nemá
- ~~Myslíte si~~ Doufáte, že pojmy v sektorových zákonech jsou jasné a je k nim výklad
  - Nejsou a není
- 70 telefonátů denně
- Vymyslíte evidenci a změní vám informační systém
- …



Jak zákon zavést?

Přehled v organizaci

- Mé agendy/služby, co poskytuji
- Co pro to potřebuji?
- Z toho vyplývá rozsah, ve kterém KB řeším.

Aktuální stav KB

- Mám již zavedena některá opatření?
- Zdokumentuji aktuální stav zavedených a nezavedených opatření.

Určení priorit

- Jaké mám kapacity?
- Co je má prioritní služba?
- Provedu analýzy, stanovím plán se zohledněním kapacit a priorit.

Zavádění opatření

- Určím odpovědné osoby.
- Priorita je vzdělávání zaměstnanců včetně vedení.
- Pokračuji dle plánu.

Zásada přiměřenosti:

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

- Nechci všechno najednou, postupně se zlepšuji.

Nejčastější zjištění z kontrol

- Chybějící podpora vedení
- Bezpečnostní role neustanoveny / nemají přiděleny dostatečné kompetence a odpovědnosti
- Nezpracované/neúplné/neschválené/neřízené/nedodržované bezpečnostní politiky
- Chybějící metodiky pro řízení aktiv a rizik
- Nejednotný proces řízení rizik v rámci organizace
- Chybějící prohlášení o aplikovatelnosti a plán zvládání rizik
- Neprováděny bezpečnostní testy zranitelnosti aplikací přístupných z vnějšku
- Smlouvy nerespektují zákonné požadavky (tím spíš požadavky best practice)
- Řízení přístupových oprávnění dodavatelů ke službám
- Správa privilegovaných účtů
- Plán kontinuity/havarijní plán neexistuje, je neúplný, není otestován

Kde najít další informace?

Portál NÚKIB

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

Hlavní komunikační platforma týkající se nového ZKB

- Formulářová podání
- Podpůrné materiály (sekce **Informační servis**)
- Aktuality
- Otázky & odpovědi

O čem je taky dobré vědět

Cyber Resilience Act – co to je a co přináší

- **Akt o kybernetické odolnosti (Cyber Resilience Act, CRA) byl v listopadu 2024 publikován ve Věstníku EU, je platný a stane se plně účinným ke konci roku 2027 -** Regulation - 2024/2847 - EN - EUR-Lex
- **přelomová unijní legislativa týkající se kybernetické bezpečnosti široké škály produktů s digitálními prvky.**
- Nařízení – přímo účinné – bude ale adaptační zákon, který rozdělí kompetence – je půjde do legislativní procesu
- Týká se produktů s digitálními prvky – HW i SW – budou muset splňovat požadavky na kybernetickou bezpečnost

- Jednoduše - vstup produktů na vnitřní trh EU bude podmíněn splněním bezpečnostních požadavků, např.:
  - neexistence známých zneužitelných zranitelností,
  - bezpečnostní aktualizace,
  - posouzení kyberbezpečnostních rizik
  - Bude k nim muset být připojeno prohlášení o shodě, důležité a kritické produkty budou muset projít nezávislým posouzením - certifikací

Cyber Security Act

- Nařízení EU – **platné** – upravuje mimo jiné Evropské certifikace KB, vydáno v červnu 2019
- Cílem je zajištění důvěry v bezpečnost produktů, procesů a služeb
- Zavedení a sjednocení **certifikace ICT produktů, procesů a služeb** v EU
- Sjednocení roztříštěné certifikační rámce v Evropě
- Vznikají certifikační schémata, které nahradí národní certifikace a budou uznatelné v celé EU
  - Aktuálně vydáno jediné schéma – EUCC, v přípravě jsou/byly peněženky, 5G, Cloud
  - Dokud není schéma není jsou certifikáty
- **Nepovinné** – pokud to nebude stát vyžadovat
- Tři úrovně certifikace
  - LOW - Samoposouzení
  - SUBSTANTIONAL – posouzení v akreditované laboratoři (CAB-conformity assesment body)
  - HIGH – Národní autoritou (NÚKIB), která k tomu může pověřit CAB
- European Cybersecurity Certification - All you need to know - YouTube

Jak to má celé fungovat

Návrh revize CSA – CSA2

Návrh CSA2 - shrnutí

- EK předložila návrh revize CSA – tzv. CSA2
- Jde o **návrh revize** – bude se o něm jednat – **spíše roky než měsíce**
- Nyní k návrhu státy dávají „rámcové pozice“ – deklarují co si o tom myslí a jaké připomínky budou mít
- Bude probíhat vyjednávání a pak celý legislativní proces
- **Nepanikařit**, nenaskakovat na katastrofické scénáře, řídit se tím co je nyní platné
- Návrh přichází se změnami ve 4 oblastech
  - Mandát ENISA
  - Reforma certifikačního rámce
  - Bezpečnost ICT dodavatelích řetězců
  - Revize NIS2

Děkujeme za pozornost !