NIS2
Nový zákon o kybernetické bezpečnosti

Novinky a aktuální stav

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

4. října 2023
TLP: CLEAR

Petra Lompejová
oddělení regulace soukromého sektoru

Shrnutí situace

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

Stav směrnice NIS2

- Směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii
- Publikována 27. prosince 2022
- Gestor problematiky (předkladatel návrhu transpozičního zákona) = NÚKIB
- Transpozice, tj. provedení obsahu směrnice do českého práva je potřeba provést do 17. října 2024.

NIS2 – regulované služby

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 bankovnictví 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 provozovatelů 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, platforem 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.

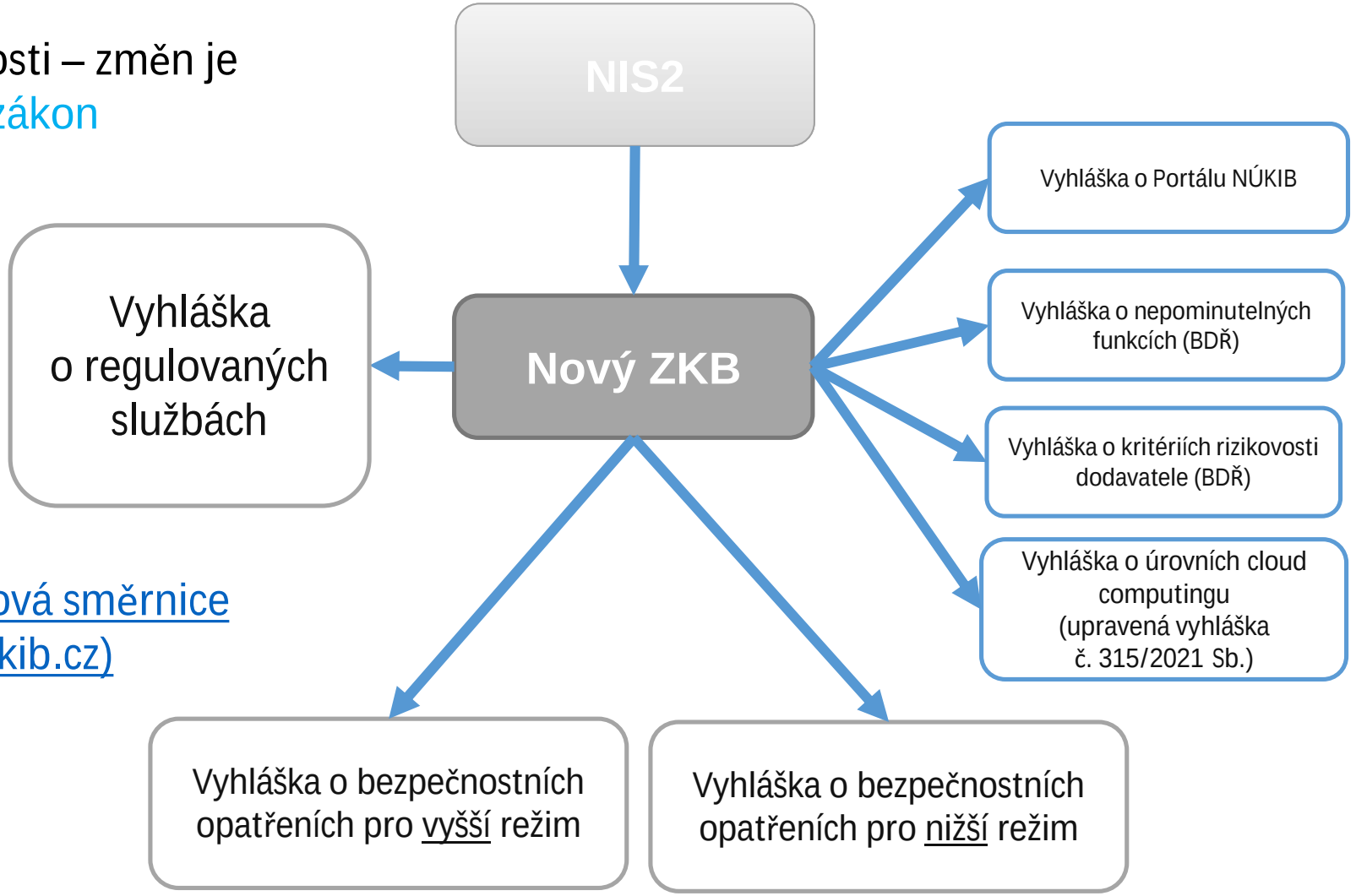
Nový zákon o kybernetické bezpečnosti v MPŘ

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

= zcela nová úprava – cca 70 paragrafů

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

Celý návrh zveřejněn zde: Course: Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)



Nový ZKB – hlavní body

Nový zákon dopadne na minimálně 6 000 organizací

- jde téměř výhradně o požadavek směrnice
- reguluje přes 105 služeb v 18 odvětvích (energetika, zdravotnictví, bankovnictví, 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 – nevybírají 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,…

Regulovaná služba a její režim

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).

Velikost podniku

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

Kategorie podniku	Počet zaměstnanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

TLP: CLEAR

ŘEDNÍHO PODNIKU

edního podniku (MSP) je nutné posuzovat i vztah k tzv. propojeným podnikům. Při výpočtech tak záleží na výši vlastnického pod
k. Pro stanovení celkového počtu zaměstnanců, ročního obratu či bilanční sumy roční rozvahy zkoumaného podniku se tak započítá

I PODNIKŮ

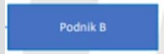
ž 25 % základního kapitálu nebo . **Údaje za tento podnik se**

2. PARTNERSKÝ PODNIK
Každý podnik, který vlastní 25 % - 50 % základního kapitálu nebo hlasovacích práv jiného podniku. **Údaje za tento podnik se přičítají ve výši procentuálního vlastnického podílu.**

3. SPOJENÝ
Každý podni
má právo u
tento podni
vlastnický p

ilý, a nemít tudíž žádné partnerské podniky, i tehdy, je-li 25% práh dosažen nebo překročen některým z investorů uvedených v doporučení Komise 2003/361/ES ze dne 6. května 2003 o edních podniků.

40 % podnikem B. K údajům za
stnanců a 40 % ročního obratu a

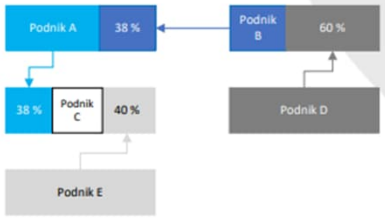


PŘÍKLAD 2
Posuzovaný podnik A je vlastněn ze 40 % podnikem B. Podnik B je navíc vlastněn podnikem C ze 70 %. Jelikož je mezi podnikem B a C spojenecký vztah, musíme k údajům za podnik A přičíst nejen 40 % zaměstnanců a 40 % ročního obratu a aktiv podniku B, ale rovněž podniku C.
Výsledek = 100 % A + 40 % B + 40 % C

PŘÍKLAD 3
Posuzovaný podnik A vlastní z 51 % podnik B. K údajům za podnik A tedy přičítáme 100 % zaměstnanců a 100 % ročního obratu a aktiv podniku B.
Výsledek = 100 % A + 100 % B

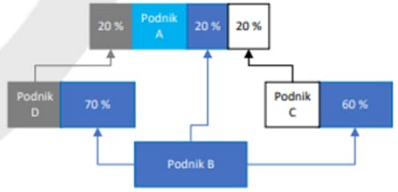
8 % podnikem B. Zároveň podnik
e vlastněn podnikem D z 60 %, a
výši 40 %. K údajům za podnik A
a 38 % ročního obratu a aktiv
u C. Jelikož je podnik D ve
usíme přičíst i 38 % z podniku D
B v posuzovaném podniku A.
protože se jedná o partnerský

Výsledek = 100 % A + 38 % B + 38 % C + 38 % D



PŘÍKLAD 5
Posuzovaný podnik A je vlastněn z 60 % podnikem B. Podnik B má dva partnery, a to podnik C, který vlastní 32 % podniku B, a podnik D, který vlastní 25 % podniku B. K údajům za podnik A tedy přičítáme 100 % zaměstnanců a 100 % ročního obratu a aktiv podniku B, dále 32 % podniku C, a 25 % podniku D.
Výsledek = 100 % A + 100 % B + 32 % C + 25 % D

PŘÍKLAD 6
Posuzovaný podnik A je vlastněn podniky B, C a D, jejichž podíl je u každého roven 20 %. Při letmém posouzení našeho vztahu k podnikům by se mohlo zdát, že se jedná o samostatný podnik, jelikož jednotlivé podíly nepřekračují hranici 25 %. Jelikož jsou ale podniky B, C a D vzájemnými spojenci, musíme jejich podíly na našem podniku A sečíst. Tím se dostáváme přes hranici 50% podílu na vlastnictví a všechny tři podniky se stávají našimi spojenci. Z toho vyplývá, že při výpočtu musíme přičíst údaje za celou skupinu.
Výsledek = 100 % A + 100 % B + 100 % C + 100 % D



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%BEivatelsk%C3%A1%20p%C5%99%C3%ADru%C4%8Dka%20k%20definici%20mal%C3%BDch%20a%20st%C5%99edn%C3%ADch%20podnik%C5%AF.pdf**

verze 1.0, platná ke dni 14.11.2022

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

Shrnutí povinností

Hlavní povinnosti

- hlásit kontaktní a další údaje
- stanovit rozsah řízení kybernetické bezpečnosti – definuje rozsah regulace v organizaci
- zavádět bezpečnosti opatření – podle režimu v kterém je služba určena (vyšší/nižší)
- hlásit kybernetické bezpečnostní incidenty – podle režimu v kterém je služba určena (vyšší/nižší)
- 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

Lhůty pro plnění povinností

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 od zařazení do evidence

Hlášení kybernetických bezpečnostních incidentů

- Vyšší režim
- Nižší režim

→ Do 1 roku od vyrozumění od zařazení do evidence

Protiopatření

- Výstraha, varování, reaktivní opatření

→ 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)

Povinnosti vyplývající z národních potřeb

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 nevyrábí, ohrozilo by to službu apod.) + přechodné lhůty

→ Do 1 roku od vyrozumění o označení služby jako strategické

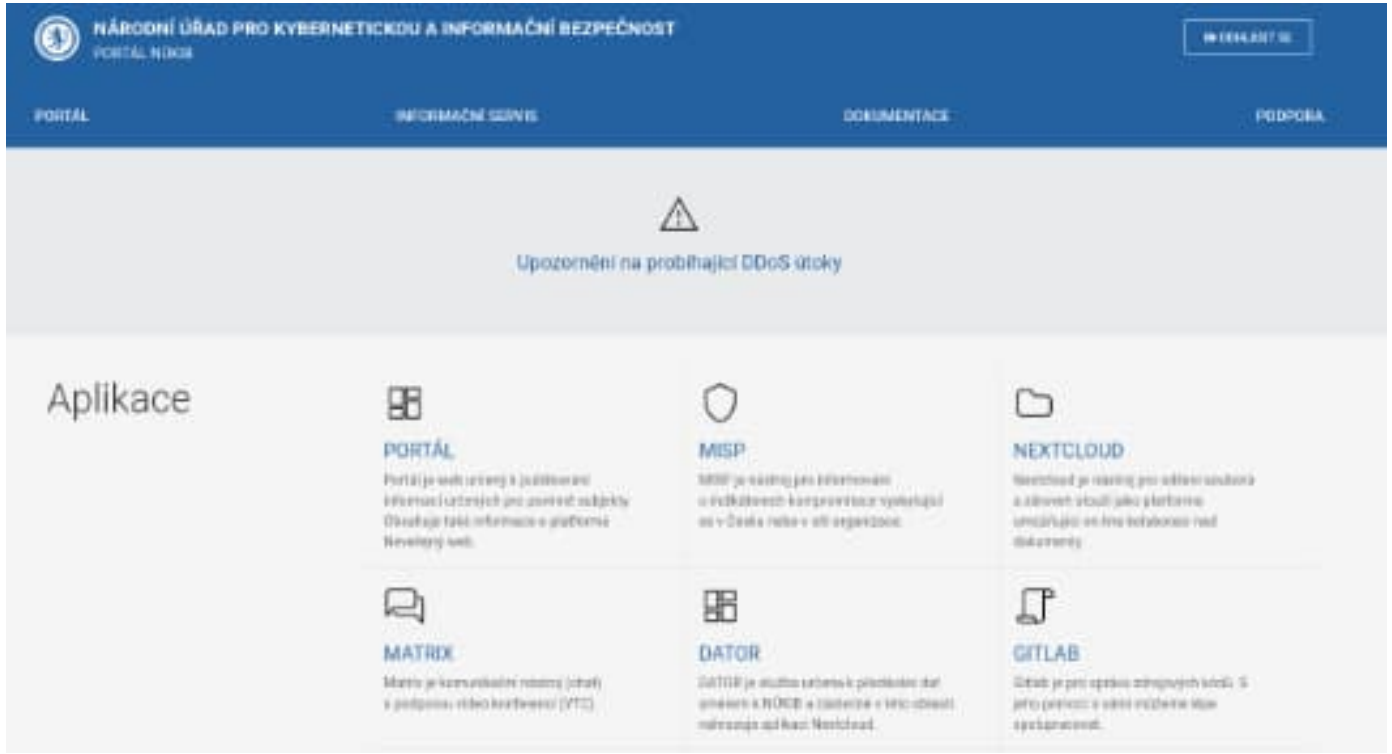
Zajištění dostupnosti strategicky významných služeb

- 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)

Portál NÚKIB

- 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



Dozor nad dodržováním zákona

Dozorový orgán – NÚKIB

Oprávnění:

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

Komunikace návrhů a zapojení veřejnosti

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

Nová směrnice EU o bezpečnosti sítí a informací (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

Veřejné konzultace – hlavní změny

- 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

Mezirezortní připomínkové řízení

Oficiální mezirezortní připomínkové řízení bylo zahájeno 19. června 2023 a ukončeno 26. července 2023
(původní lhůta na připomínky stanovená do 19. července byla prodloužena)

NÚKIB obdržel vyšší stovky připomínek

- připomínky zaslalo 41 řádných připomínkových míst
- dalších 11 organizací zaslalo své připomínky i bez toho, aby byly osloveny (ale jejich připomínky byly také přijaty a řešeny)
- připomínky vypořádány písemně + další jednání

Nejčastější připomínkované oblasti

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

Nový ZKB – další předpokládané kroky

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 roce 2024

Děkuji za pozornost.

Nis2.nukib.cz

regulace@nukib.cz