Nová směrnice EU o kybernetické bezpečnosti „NIS2“

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

27. dubna 2023

TLP: GREEN

Petra Lompejová
oddělení regulace soukromého sektoru

iDNES.cz / ZPRAVODAJSTVÍ Domácí Zahraničí Krimi Kraje Volby Ekonomika Kultura Finance

Domácí Volby Názory MediaHub Koronavirus NATO Speciály

Kyberbezpečnost se firmám příští rok prodraží. Hrozí mnohamilionové pokuty

iROZHLAS

Česko se připravuje na přijetí evropské směrnice o kybernetické bezpečnosti, dotkne se asi 6000 subjektů

Novinky.cz

Hlavní stránka Stalo se Domácí Volby Zahraniční Válka na Ukrajině Krimi Kultura Ekonomika Finan

Komentáře Internet a PC AutoMoto Muži Věda a školy Bydlení Cestování Historie Podcasty Speciá

VÁLKA NA UKRAJINĚ ZBYTEČNÁ VÁLKA ENERGIE: SROVNÁNÍ

Novinky.cz » Internet a PC » Bezpečnost » Kyberbezpečnost budou muset povinně zajistit tisíce českých firem

Kyberbezpečnost budou muset povinně zajistit tisíce českých firem

3. 9. 2022, 21:20 – Praha
ČTK

Co potřebujeme vědět na začátku

- Kybernetická bezpečnost v České republice **je již nyní regulována** (= je z čeho vycházet)
- Základem změn je nově přicházející **směrnice NIS2** (= viz dále), ale také potřeba zákon o kybernetické bezpečnosti aktualizovat
- 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** (= zveřejněn k zasílání podnětů, aktuálně ukončeno)
- Návrh zákona a prováděcích právních předpisů bude **předložen do legislativního procesu v první polovině roku 2023.**
- **Nová pravidla by měla platit v polovině roku 2024** (do 17. října 2024 v souladu se směrnicí NIS2)

*zpravidla

Stav směrnice NIS2

- Směrnice byla 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.**

Regulované služby (směrnice NIS2)

Směrnice NIS1:

30 služeb v 7 odvětvích

Kritéria dopadu incidentu

⇒ **cca 400 povinných osob**

„Kybernetickou bezpečnost musí řešit pouze ti s nejvyšší mírou dopadu na společnost.“

Směrnice NIS2:

60 služeb v 18 odvětvích

Kritérium velikosti subjektu

⇒ **minimálně 6 000 povinných osob**

„Kybernetickou bezpečnost musí řešit každý, kdo na ni má finance.“

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 ZKB – povinné osoby

- **Povinné osoby budou určovány primárně na základě velikosti** (střední a velké podniky)

  a poskytované služby

- **Typ povinné osoby = tzv. Poskytovatel regulované služby**
  - poskytuje regulovanou službu = služba splňující kritéria stanovená vyhláškou
- **Režim poskytovatele regulované služby**
  - Stanovuje míru povinností – vyšší režim / nižší režim (vyšší cca 1 000 povinných osob, nižší cca 5 000)
  - Ke každému režimu bude vyhláška, která bude definovat bezpečnostní opatření
- **Naplnění kritérií je povinen hlásit poskytovatel služby = každý si musí vyhodnotit kritéria sám**
  - Do 30 dnů od doby, kdy naplnění zjistí, nejpozději do 90 kdy k naplnění došlo
- NÚKIB může zaregistrovat i sám dozví-li se o naplnění kritérií

Nový ZKB – povinnosti

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/nižší)**
- **Hlásit kybernetické bezpečnostní incidenty**
- **Informovat zákazníky o incidentech a hrozbách**
- **Provádět protiopatření**
- **Plnit povinnosti z Mechanismu řízení bezpečnosti dodavatelského řetězce u vybraných služeb**
- **Zajistit dostupnost 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

Nový ZKB

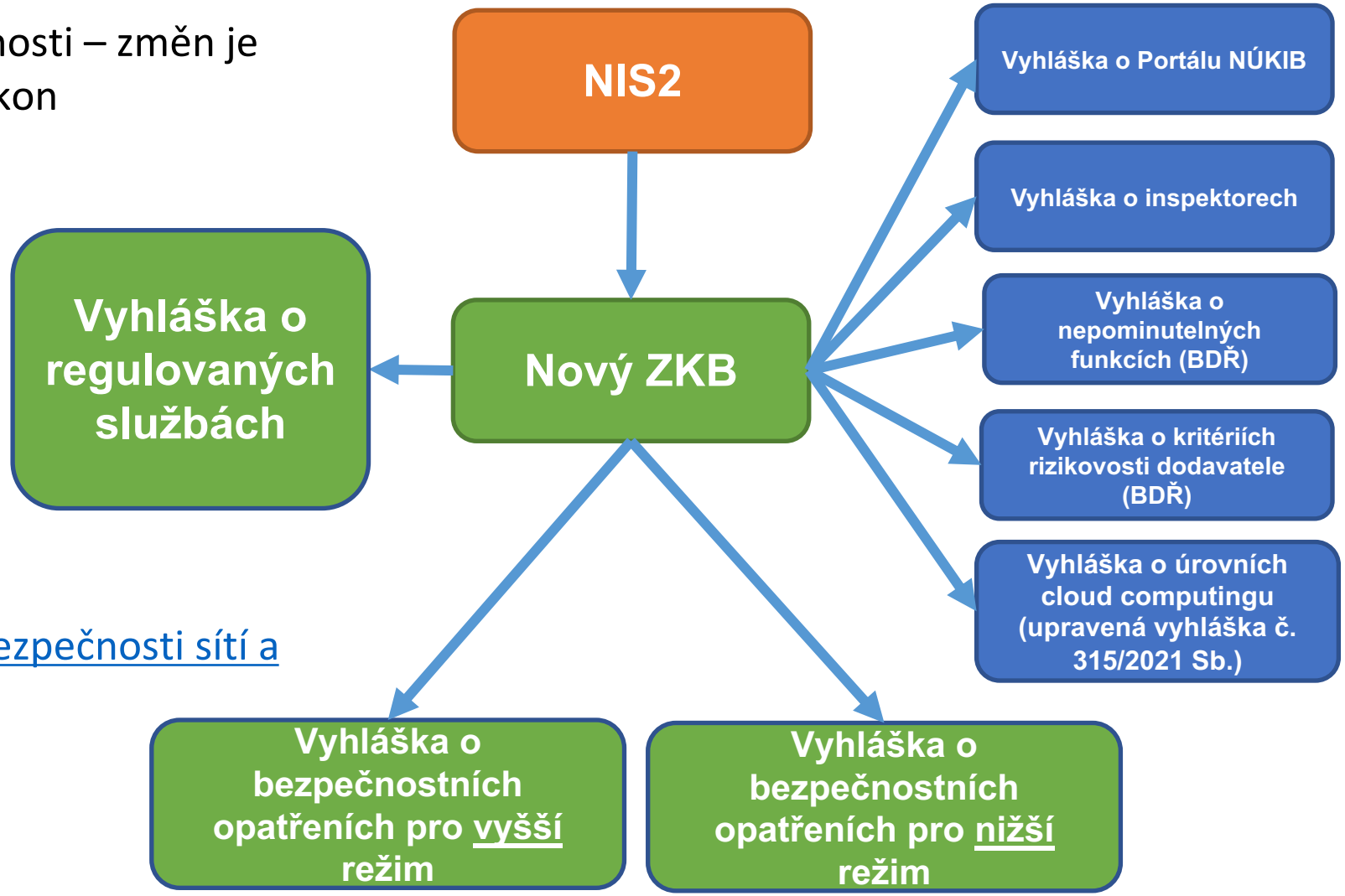
Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo třeba vytvořit nový zákon

zcela nová úprava – cca 60 paragrafů

Zveřejněný návrh má aktuálně navíc 8 vyhlášek

(nicméně stále dochází k úpravám)

Celý návrh zveřejněn zde: [Course: Nová směrnice EU o bezpečnosti sítí a informací (nukib.cz)](nis2.nukib.cz) (nis2.nukib.cz)



Nový ZKB – hlavní dopady na organizace

Nové povinné osoby

- Primárně **v režimu nižších povinností**:
  - ⇒ Povinnost zaregistrovat se a nahlásit kontaktní údaje NÚKIB
  - ⇒ Základní úroveň bezpečnostních opatření
  - ⇒ Hlášení významných kybernetických incidentů
  - ⇒ Řízení se protiopatřeními vydanými NÚKIB

Původní subjekty dle ZKB

- Primárně **v režimu vyšších povinností:**
  - ⇒ Bezpečnostní opatření jsou vymezeny službou – může dojít k rozšíření okruhu, na který budou bezpečnost zavádět, ale konkrétní opatření se pro vyšší režim mění pouze minimálně
  - ⇒ NIS2 stanovuje vyšší sankce za porušení – blíže GDPR
  - ⇒ Povinnost samoidentifikace spíše než kontaktování ze strany NÚKIB

Aktuální harmonogram transpozice

Veřejná konzultace a zveřejnění prvotních návrhů ZKB pro podněty veřejnosti bylo zahájeno 26. ledna 2023 a ukončeno 12. března 2023. NÚKIB obdržel a vypořádal podněty od více než sta jednotlivých míst, počet jednotlivých podnětů se blíží tisícovce.

Další předpokládané kroky

- Polovina května – start Mezirezortního připomínkového řízení (MPŘ) – 2Q 2023
  - Oficiální zahájení legislativního procesu
  - Zveřejnění došlých podnětů veřejnosti vč. vypořádání a zveřejnění návrhů předložených do MPŘ
- Legislativní rada vlády – 3/4Q 2023
- Poslanecká sněmovna – konec 2023
- Vydání zákona říjen 2024 (konec transpoziční lhůty)

Nejčastější dosavadní zjištění...

NAJČASTEJŠIE NÁLEZY AUDITU

Riadenie bezpečnosti (Security governance):

- Neexistujúca stratégia KB a nedostatočná podpora najvyššieho vedenia
- Neurčený Manažér KB, prípadne neformálna rola,
- Nedostatočná, alebo chýbajúca bezpečnostná dokumentácia (aj pri PZS s certifikátmi SO27001)
- Dokumentácia často tvorená len dodávateľmi konkrétneho projektu
- Nezávislosť riadenia bezpečnosti od riadenia IT
- Neexistencia vzdelávania v oblasti informačnej bezpečnosti
- Závislosť na dodávateľoch (vendor lock)
- Neexistujúce riadenie aktív, hrozieb a rizík
- Chýbajúci vlastníci rizík a ich zodpovednosti
- Neformálne riadenie prevádzky

Výkon bezpečnosti (Security operations):

- Chýbajúci bezpečnostný monitoring
- Chýbajúce logovanie
- Nesystematické riešenie incidentov
- Nedostatky v riadení bezpečnosti sietí
- Chýbajúca topológia, segmentácia, zoznamy portov
- Nezabezpečenie a nedostatočná vybavenosť „serverovní" (často plných kvalitného ale nevyužitého HW)

Slovenské Cyber Security Competence and Certification Centre, dostupné zde: https://www.linkedin.com/posts/cybercompetence_naj%C4%8Dastej%C5%A1ie-n%C3%A1lezy-auditov-kybernetickej-activity-6950447432744759296-XChs?utm_source=share&utm_medium=member_desktop

...aneb kde začít

- 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 **zmapováním 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 vrcholový 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.
- 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.

Děkuji za pozornost

Dotazy je možné zasílat na:

regulace@nukib.cz