(Nový) zákon č. 264/2025 Sb., o kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

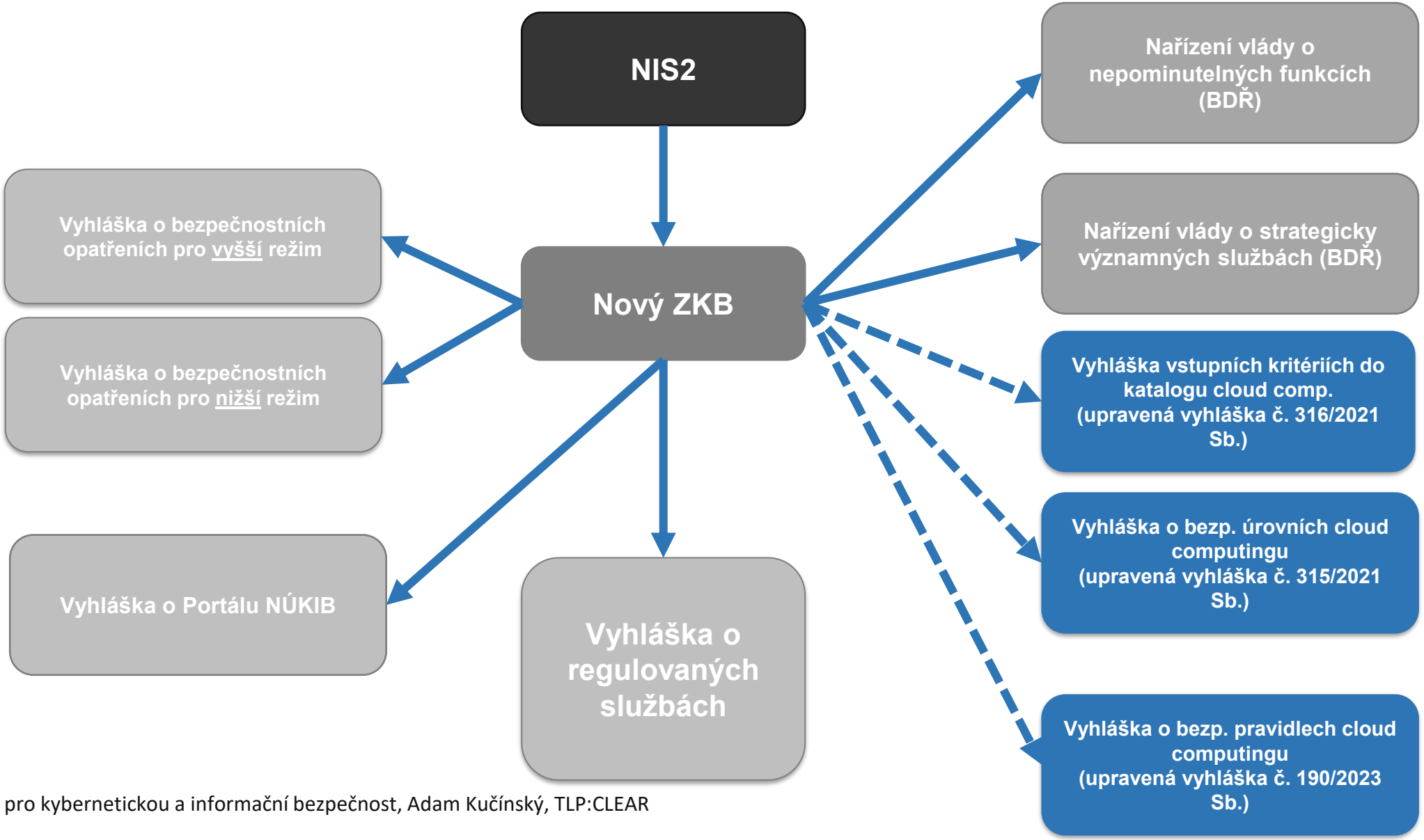
Virtuální konference:
Jak splnit nový zákon o kybernetické bezpečnosti?
23. září 2025
TLP: CLEAR

Adam Kučínský
ředitel
odbor regulace

Hlavní změny v novém zákoně o kybernetické bezpečnosti

- **rozšíření počtu povinných osob,** a to jak rozšířením regulovaných odvětví, tak rozšířením stávajících regulovaných odvětví o nové regulované služby,
- **změna způsobu identifikace povinných osob,**
- doplnění **nových požadavků na zavádění bezpečnostních opatření,**
- doplnění **nových požadavků na proces hlášení kybernetických bezpečnostních incidentů,**
- **větší odpovědnost vrcholného vedení** za zajišťování kybernetické bezpečnosti,
- **větší důraz na sdílení informací,**
- **prohloubení spolupráce** nejen mezi Úřadem a regulovanými osobami, ale i mezi Úřadem a dalšími orgány veřejné moci,
- **zvýšení pokut** a nové formy správního trestání,
- **nové požadavky na řešení problematiky bezpečnosti dodavatelského řetězce.**

Ekosystém NZKB – prováděcí předpisy



Koho se regulace týká?

Regulovanou službou je

- služba naplňující podmínky pro registraci (podle § 4) = alespoň jedno **„kritérium pro identifikaci“ regulované služby podle vyhlášky o regulovaných službách**

  = **Samoidentifikace**

nebo

- služba naplňující podmínky pro registraci (podle § 5) = **služba stanovená rozhodnutím** Národního úřadu pro kybernetickou a informační bezpečnost na základě kritéria pro určení regulované služby.

  = **určení regulátorem**

Samoidentifikace

- Střední nebo velký podnik
  - Pro posouzení velikosti subjektu musí být naplněn zaměstnanecký nebo finanční ukazatel – počet zaměstnanců nebo rozvaha nebo obrat
  - Střední podnik (nad 50 zaměstnanců/10 mil. EUR rozvaha/10 mil. EUR obrat)
  - Velký podnik (nad 250 zaměstnanců/43 mil. EUR rozvaha/50 mil. EUR obrat)
  - Partnerské podniky (25-50% účasti) / Propojené podniky (nad 50% účasti) **se z pohledu velikosti sčítají**

- Poskytuje regulovanou službu
  - Viz vyhláška o regulovaných službách - vychází z příloh směrnice NIS2

- Typicky velké podniky ve vybraných odvětvích vyšší režim, střední podniky nižší režim
  - Výjimky
    - DNS, registr internetových domén nejvyšší úrovně, veřejná správa, případně dle národní implementace
    - **ISP padají do regulace všichni** – jejich velikost má vliv na režim

Zvláštní ustanovení o určování velikosti podniku

nZKB § 7 Zvláštní ustanovení o určování velikosti podniku

Odchylně od pravidel doporučení Komise 2003/361/ES pro účely tohoto zákona platí, že

a) čl. 3 odst. 4 doporučení Komise 2003/361/ES se neuplatní, */nesčítají se veřejné subjekty – obce, kraje/*

b) za podnik se nepovažují organizační složky státu, územní samosprávné celky a Česká národní banka,

c) za partnerský nebo propojený podnik se nepovažují osoby, jejichž technická aktiva jsou zcela oddělena od technických aktiv, která používá posuzovaná osoba při poskytování regulované služby, a

d) pro určování velikosti poskytovatele regulované služby v odvětví věda, výzkum a vzdělávání, který není podnikem, se pravidla pro určování velikosti podniku podle doporučení Komise 2003/361/ES, včetně speciálních pravidel upravených tímto zákonem, použijí obdobně.

Vyhláška o regulovaných službách - samoidentifikace

16. Digitální infrastruktura a služby

Regulovaná služba	
Služba	**Podmínky významnosti poskytovatele regulované služby a jeho režim**
16.1 Poskytování veřejně dostupné služby elektronických komunikací podle zákona o elektronických komunikacích[33)]	Osoba poskytující veřejně dostupnou službu elektronických komunikací podle zákona o elektronických komunikacích je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) velkým nebo středním podnikem, b) poskytovatelem veřejně dostupné služby elektronických komunikací prostřednictvím nejméně 350 000 aktivních mobilních SIM karet na území České republiky, nebo c) poskytovatelem nejméně 100 000 aktivních pevných internetových přípojek na území České republiky, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je malým podnikem, nebo mikropodnikem podle doporučení Komise 2003/361/ES o definici mikropodniků a malých a středních podniků.
16.2 Zajišťování veřejné komunikační sítě podle zákona o elektronických komunikacích	Osoba zajišťující veřejnou komunikační síť podle zákona o elektronických komunikacích je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) velkým nebo středním podnikem, b) poskytovatelem veřejně dostupné služby elektronických komunikací prostřednictvím nejméně 350 000 aktivních mobilních SIM karet na území České republiky, nebo c) poskytovatelem nejméně 100 000 aktivních pevných internetových přípojek na území České republiky, nebo

Určení ze strany NÚKIB

§ 5 nZKB

Podmínky pro registraci regulované služby jsou dále splněny v případě, že

a) jde o službu podle § 4 odst. 1 písm. a) a
   1. její poskytovatel je jediným poskytovatelem této služby v České republice a tato služba je zásadní pro zabezpečení důležitých společenských nebo ekonomických činností nebo pro bezpečnost v České republice,
   2. narušení této služby by mohlo mít významný dopad na bezpečnost České republiky, vnitřní pořádek nebo život a zdraví,
   3. narušení této služby by mohlo vyvolat významná systémová rizika, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad, nebo
   4. její poskytovatel je kvůli svému specifickému významu na regionální nebo celostátní úrovni zásadní pro konkrétní odvětví, ve kterém působí, nebo typ služby, kterou poskytuje anebo pro jiná vzájemně propojená odvětví v České republice,
b) jde o službu, jejíž narušení může způsobit závažný zásah do života více než 125 000 osob, a to prostřednictvím ohrožení bezpečnosti České republiky, vnitřního pořádku, života a zdraví, majetkové hodnoty nebo životního prostředí,
c) jde o službu, jejíž narušení může způsobit závažný zásah do schopnosti poskytovat jinou regulovanou službu poskytovatele v režimu vyšších povinností, nebo
d) jde o službu, jejíž poskytovatel je subjektem kritické infrastruktury podle právního předpisu upravujícího krizové řízení a kritickou infrastrukturu; v takovém případě je regulovanou službou služba odpovídající prvku kritické infrastruktury určenému u tohoto subjektu.

Režim poskytovatele regulované služby

Režim poskytovatele regulované služby stanovuje míru jemu uložených povinností.

Režim poskytovatele regulované služby je:

- **režim vyšších povinností,**

nebo

- **režim nižších 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.

Strategicky významná služba – specialita vyššího režimu

Nařízení vlády o strategicky významných službách

Regulované služby splňující podmínky strategicky významné služby

(1) Strategicky významnou službou v odvětví veřejná správa je
   a) výkon svěřených pravomocí vykonávaný orgánem nebo osobou uvedenou v příloze k této vyhlášce v odvětví 1. Veřejná správa, služby 1.1. Výkon svěřených pravomocí, bod I. písm. a) až k).

(2) Strategicky významnou službou v odvětví energetika je
   a) výroba elektřiny v rámci výrobny s celkovým instalovaným elektrickým výkonem nejméně 100 MW vykonávaná držitelem licence na výrobu elektřiny podle energetického zákona,
   b) provoz přenosové soustavy elektřiny vykonávaný držitelem licence na přenos elektřiny podle energetického zákon,
   c) provoz distribuční soustavy elektřiny v rámci celé distribuční soustavy elektřiny s přenosovou kapacitou nejméně 220 MW vykonávaný držitelem licence na distribuci elektřiny podle energetického zákona,

- ….

Pro tyto služby platí ještě **mechanismus bezpečnosti dodavatelského řetězce** a **zajištění dostupnosti**

Nebudou definovány ve vyhlášce ale v nařízení vlády

Povinnosti poskytovatele regulované služby

Hlavní povinnosti vyplývající z návrhu zákona

V případě **všech poskytovatelů regulované služby**

0. Ohlásit regulovanou službu
I. Hlásit kontaktní údaje
II. Stanovit rozsah řízení kybernetické bezpečnosti
III. Zavádět bezpečnostní opatření
IV. Hlásit kybernetické bezpečnostní incidenty
V. Informovat uživatele o incidentech a hrozbách
VI. Zavádět protiopatření vydaná Národním úřadem pro kybernetickou a informační bezpečnost

V případě těch, kteří jsou zároveň tzv. poskytovateli **strategicky významné služby navíc**

VII. Mechanismus prověřování bezpečnosti dodavatelského řetězce
VIII. Zajištění dostupnosti strategicky významné služby

Do kdy co plnit?

I. Hlášení kontaktních údajů

- Cílem je
  - **zpřehlednění vztahu mezi úřadem a povinnou osobou** (regulované služby, režim,…)
  - **nastavení přímé komunikační linky** mezi úřadem a povinnou osobou

- Hlášení má probíhat skrze **Portál NÚKIB** (Portál NÚKIB (gov.cz))
- Co se hlásí upraveno vyhláškou o portálu NÚKIB
  - Upravuje jak se přes systém bude řešit
    - Registrace poskytovatele regulované služby a související změny
    - Pověřování osob aby mohly jednat s NÚKIB
    - Hlášení kontaktních a dalších údajů
    - Hlášení incidentů
    - Hlášení provedení protiopatření
    - Hlášení provedení nápravných opatření
    - Výmaz regulované osoby z registru
    - Hlášení informací o dodavatelích (BDŘ)

II. Stanovení rozsahu řízení kybernetické bezpečnosti

Obecně vždy platí – pokud chcete něco skutečně řídit, musíte vědět, že to máte!

Součástí rozsahu řízení kybernetické bezpečnosti jsou **aktiva související s poskytováním regulované služby.**

= stanovený rozsah

Postup:

Za účelem vymezení stanoveného rozsahu poskytovatel regulované služby

a) **určí všechna svá primární aktiva,**

b) **posoudí, zda** primární aktiva **souvisí s poskytováním regulované služby**, **a**

c) u primárních aktiv podle písmene b) **určí podpůrná aktiva.**

V rámci stanoveného rozsahu se jsou pak plněny povinnosti ze zákon.

Fikce stanovení rozsahu = Pokud/dokud rozsah není stanoven má se za to, že je rozsahem celá organizace.

Aktivum = fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováváním informací a dat v elektronické podobě
Primární aktivům = aktivum v podobě zpracovávané informace nebo poskytované služby

III. Organizační a technická bezpečnostní opatření

Pro poskytovatele regulované služby v režimu <u>vyšších</u> povinností jsou

Organizační opatření

a) systém řízení bezpečnosti informací,
b) povinnosti vrcholného vedení,
c) bezpečnostní role,
d) řízení bezpečnostní politiky a bezpečnostní dokumentace,
e) řízení aktiv,
f) řízení rizik,
g) řízení dodavatelů,
h) bezpečnost lidských zdrojů,
i) řízení změn,
j) akvizice, vývoj a údržba,
k) řízení přístupu,
l) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
m) řízení kontinuity činností a
n) audit kybernetické bezpečnosti

Technickými opatření

a) fyzická bezpečnost,
b) bezpečnost komunikačních sítí,
c) správa a ověřování identit,
d) řízení přístupových oprávnění,
e) detekce kybernetických bezpečnostních událostí,
f) zaznamenávání bezpečnostních a relevantních provozních událostí,
g) vyhodnocování kybernetických bezpečnostních událostí,
h) aplikační bezpečnost,
i) kryptografické algoritmy,
j) zajišťování dostupnosti regulované služby a
k) zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.

Pro poskytovatele regulované služby v režimu <u>nižších</u> povinností jsou bezpečnostními opatřeními

Organizační a technická opatření

a) systém zajišťování minimální kybernetické bezpečnosti,
b) požadavky na vrcholné vedení,
c) řízení aktiv,
d) řízení rizik,
e) bezpečnost lidských zdrojů,
f) řízení kontinuity činností,
g) řízení přístupu,
h) řízení identit a jejich oprávnění,
i) detekce a zaznamenávání kybernetických bezpečnostních událostí,
j) řešení kybernetických bezpečnostních incidentů,
k) bezpečnost komunikačních sítí,
l) aplikační bezpečnost a
m) kryptografické algoritmy

*„na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a řízení rizik **zavede přiměřená bezpečnostní opatření …**“*

IV. Hlášení kybernetických bezpečnostních incidentů

Poskytovatel regulované služby **v režimu vyšších povinností** je povinen:

- v rámci stanoveného rozsahu
- hlásit Úřadu
- všechny kybernetické bezpečnostní incidenty, které
  - **mají původ v kybernetickém prostoru a**
  - nelze u nich do maximálně 24 hodin vyloučit úmyslné zavinění
- významný dopad – do 24 hodin vyhodnotí NÚKIB

Pokud významný dopad

- Do 72 hodin další hlášení
- Na výzvu průběžná zpráva o řešení
- Do 30 dnů závěrečná zpráva (do 60 pokud incident trvá)

Poskytovatel regulované služby **v režimu nižších povinností** je povinen:

- v rámci stanoveného rozsahu
- hlásit Národnímu CERT
- všechny kybernetické bezpečnostní incidenty, které
  - mají původ v kybernetickém prostoru,
  - nelze u nich do maximálně 24 hodin vyloučit úmyslné zavinění
  - **mají významný dopad na poskytování regulované služby**
- významný dopad - vyhodnotí sám podle vyhlášky

Digitálové – specifická úprava

Z důvodu speciálního nastavení ve směrnici NIS 2 **existuje množina subjektů, které mají jiná pravidla pro bezpečnostní opatření a hlášení incidentů.**

Pravidla se použijí na ty subjekty, které poskytují

- **službu systému překladu jmen domén,**
- **služby správy a provozu registru domény nejvyšší úrovně,**
- **služby cloud computingu,**
- **služby datového centra,**
- **služby sítě pro doručování obsahu,**
- **služby on-line tržiště,**
- **služby internetového vyhledávače,**
- **služby platformy sociální sítě,**
- **řízené služby nebo**
- **řízené bezpečnostní služby**.

V případě **služby vytvářející důvěru** se pravidla použijí jen pro bezpečnostní opatření.

Digitálové mají bezpečnostní opatření a hlášení incidentů stanoveno prováděcím nařízení komise:

- **https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L_202402690**
- **Vysvětlení zde: https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti/okruh-regulace-poskytovatelu-digitalnich-sluzeb**

V případě ostatních dalších služeb takového poskytovatele se však prováděcí nařízení Komise nepoužije!

V. Informační povinnost – incident a hrozba

Informační povinnost – kybernetický bezpečnostní **incident**

- 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 může poskytovateli regulované služby uložit povinnost nebo zákaz informovat uživatele regulované služby o tomto incidentu.

Informační povinnost – významná **hrozba**

- Poskytovatel regulované služby je **povinen informovat uživatele** regulované služby, který může být ovlivněn významnou hrozbou o této **hrozbě a o krocích k minimalizaci dopadu** hrozby.
- Významnou hrozbou **hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál závažně ovlivnit aktiva poskytovatele regulované služby nebo uživatele regulované služby natolik, že způsobí značnou újmu.**

VI. Protiopatření

Podstatou je v mimořádných případech možnost státu zasáhnout k ochraně aktiv – existují 3 druhy

Výstraha

- Vydává NÚKIB.
- **Informování veřejnosti** o kybernetickém bezpečnostním **incidentu či o porušování povinností** daných tímto zákonem.
- Možno uložit, aby to poskytovatel udělal sám.

Varování

- Úřad vydá varování, dozví-li se o **závažné hrozbě nebo zranitelnosti** v oblasti kybernetické bezpečnosti.
- Varování Úřad oznámí dotčeným poskytovatelům regulované služby prostřednictvím Portálu Úřadu a zveřejní jej na úřední desce Úřadu.
- Nově může být varování i neveřejné.

Reaktivní protiopatření

- Rozhodnutí, ve kterém **uloží poskytovateli regulované služby povinnost** provést reaktivní protiopatření.
- k řešení incidentu, k zabezpečení aktiv před incidentem, ke zvýšení bezpečnosti na základě incidentu

VII. Bezpečnost dodavatelského řetězce

- Nová oblast, nevyplývá ze směrnice NIS2 ale z národního rozhodnutí
- Platí pouze pro strategicky významné služby
- Organizace v rámci této povinnosti musí nahlásit dodavatele
- Budou prověřování dodavatelé do kritické části systému = aktiva s hodnotou 4 (kritická), kteří dodávají bezpečnostně významnou dodávku = má výpočetní kapacitu
- Stát prověří
  - NÚKIB k tomu vyžaduje informace a součinnost řady orgánů (PČR, SLUŽBY, FAU, NSZ, MPO, MV, NBÚ, ÚOHS…)
- Vláda může vydat zákaz dodavatele použít nebo upozornění na riziko (je řešitelné bezp. opatřením)
- Lze udělit výjimku (např. pokud to nikdo jiný nevyrábí, ohrozilo by to službu apod.)
  - K vyřazení již dodaných technologií nemusí dojí hned – počítá se s přechodnými lhůtami
- Hlášení dodavatelů do 1 roku od určení poskytovatele regulované služby

- Detail koho přesně se to týká - nařízení vlády o strategicky významných službách
- Jakých aktiv se to týká - Nařízení vlády o nepominutelných částech a těch s hodnocením kritická

VIII. Zajištění dostupnosti strategicky významných regulovaných služeb

- Východiska:
  - zajištění dostupnosti **směruje na službu**, nikoli nutně na její dílčí aktiva (a už vůbec ne na všechna),
  - zajištění dostupnosti služby je **možné i mimo kyberprostor,**
  - kvalita služby může být snížena – míru snížení si definuje sám poskytovatel v BCM,
  - úroveň služby může být snížena – míru snížení si definuje sám poskytovatel v BCM,
  - rozsah služby může je dle připomínek subjektů nutno omezit/definovat, aby byla právní jistota.

- Cíl:
  - kritické služby musíme být schopni zajistit alespoň omezeně z České republiky, abychom byli připraveni na mimořádné situace v zahraničí.

- Prakticky to tedy znamená, že:
  - je potřeba být schopen službu poskytovat z území ČR, tedy bez zajištění služeb ze zahraničí,
  - zjištění služby může být i mimo ICT, např. náhradním postupem fyzicky - pokud to splní stanovený rozsah a kvalitu.

Děkuji za pozornost

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

regulace@nukib.gov.cz