NIS2 a nZKB: Prověřování rizik u dodavatelů & Hlášení incidentů

ZKB 2024: Revoluce v kybernetické bezpečnosti od 18. 10. 2024

Michael Bátrla | 18. 04. 2024

Whoami

Michael Bátrla

Head of Security | Rossum.ai

- Dříve konzultant kybernetické bezpečnosti pro Strategii KB | GRC | Cloud Security

Odborný pracovník | Ústava práva a technologií

Právnická fakulta Masarykovy Univerzity

Kontakty:

michael.batrla@rossum.ai | michael.batrla@law.muni.cz

michael.batrla@protonmail.com

/in/mbtr

Témata

- **Úvod k regulovaným službám**
- **Blok 1: Prověřování rizik u dodavatelů**
  - Aktuální stav
  - Záměr NIS2
  - Kontext v ČR
  - Znění před LRV
- **Blok 2: Hlášení kybernetických bezpečnostních incidentů podle ZKB**
  - Definice, událost vs. incident
  - Vyšší vs. nižší režim a významné incidenty
  - Prvotní hlášení a další postup
  - Sankce
  - Vztah k ostatním předpisům (GDPR)

Aktuální stav materiálu k 22. ledna 2024. V rámci legislativního procesu pravděpodobně dojde ke změnám (např. LRV 04. 04. 2024).

NIS2 a nZKB: Regulované služby

ZKB 2024: Revoluce v kybernetické bezpečnosti od 18. 10. 2024

Michael Bátrla | 18. 04. 2024

Regulovaná služba

- Zjednodušení současné taxonomie povinných osob (pZS, K(I)I, pVIS...) na *Regulované služby (dále RS)*, resp. *Poskytovatele regulované služby (dále pRS)*
- § 2, odst. 1 písm. e): *"služba, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva"*

Kritéria pro identifikaci regulované služby

Tvořeno **kritériem služby** a **kritériem poskytovatele** regulované služby:

- § 4 Odst. 1 písm. a) kritérium služby:
  1. odvětví, pododvětví a druh subjektu dle NIS2 přílohy I, II a
  2. významnost služeb v jednotlivých odvětvích dle NIS2 příloha III
- písm. b) kritérium poskytovatele regulované služby:
  1. Velikost podniku
  2. ekonomickou, společenskou a bezpečnostní významnost poskytovatele regulované služby pro Českou republiku

Specifické případy: **§ 5 Kritéria pro určení regulované služby**

- Rozhodnutím Úřadu
- Vždy ve vyšším režimu povinností
- *odst. 1 písm. c):* její narušení může způsobit **závažný zásah do schopnosti poskytovat jinou regulovanou službu** stejného nebo jiného poskytovatele regulované služby v režimu **vyšších povinností**

Odvětví a RS

a) veřejná správa,
b) energetika,
c) výrobní průmysl,
d) potravinářský průmysl,
e) chemický průmysl,
f) vodní hospodářství,
g) odpadové hospodářství,
h) doprava,
i) digitální infrastruktura a služby,
j) finanční trh,
k) zdravotnictví,
l) věda, výzkum a vzdělávání,
m) poštovní a kurýrní služby,
n) vojenský průmysl,
o) vesmírný průmysl

TLP: CLEAR

NÚKIB

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, řídící 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.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

Subjekty shromažďující a udržující přesnou a úplnou registraci názvu domén.

verze 1.0, platná ke dni 16.08.2022

Vyšší a nižší režim povinností I.

- Odlišná míra uložených povinností
- Definován **Vyhláškou o regulovaných službách**:
  - Míra obecnosti: "velký podnik - vyšší režim, střední - nižší režim„
  - Detaily a výjimky dle odvětví (někteří bez ohledu na velikost), např. →→→
- Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků
  - Včetně vlastnické struktury (**partnerské a propojené organizace**)

16.8. Poskytování služby sítě pro doručování obsahu (CDN)	Poskytovatel služby sítě pro doručování obsahu (CDN) je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je velkým podnikem, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.
16.9. Správa kvalifikovaného systému elektronické identifikace	Kvalifikovaný správce systému elektronické identifikace podle zákona o elektronické identifikaci je poskytovatel regulované služby v režimu vyšších povinností.
16.10. Poskytování služby vytvářející důvěru	Poskytovatel služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie je poskytovatel regulované služby v režimu vyšších povinností.
16.11. Poskytování řízené služby (MSP)	Poskytovatel řízené služby, který v rámci podnikatelských vztahů poskytuje vzdáleně nebo přímo u zákazníka řízenou službu související s instalací, správou, provozem nebo údržbou technických nebo programových prostředků, je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je velkým podnikem, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.

Kategorie podniku	Počet zaměstnanců (roční prac. j., RPJ)	Roční obrat | bilanční suma roční rozvahy
Velký	≥ 250	> 50 mil. EUR | > 43 mil. EUR
Střední	≥ 50	> 10 mil. EUR | > 10 mil. EUR

Vyšší a nižší režim povinností II. - některé rozdíly

- **Bezpečnostní opatření, např. řízení dodavatelů**
- **Hlášení KB incidentů**
- Zvláštní ustanovení o povinnostech např. někteří poskytovatelé digitální infrastruktury a služeb (§ 19)

Režim povinností	**Počet org./tech. bezp. opatření**
Vyšší režim	25 (14 org. + 11 tech.)
Nižší režim	13 (org. + tech.)

Blok 1:
Prověřování rizik u dodavatele

ZKB 2024: Revoluce v kybernetické bezpečnosti od 18. 10. 2024

Michael Bátrla | 18. 04. 2024

Témata

- **Blok 1: Prověřování rizik u dodavatelů**
  - Aktuální stav
  - Záměr NIS2
  - Kontext v ČR
  - Znění před LRV
- **Blok 2: Hlášení kybernetických bezpečnostních incidentů podle ZKB**
  - Definice, událost vs. incident
  - Vyšší vs. nižší režim a významné incidenty
  - Prvotní hlášení a další postup
  - Sankce
  - Vztah k ostatním předpisům (GDPR)

Aktuální stav materiálu k 22. ledna 2024. V rámci legislativního procesu pravděpodobně dojde ke změnám (např. LRV 04. 04. 2024).

Prověřování rizik u dodavatele | Dvě oblasti

Povinnosti RS u řízení dodavatelů a bezpečnostní opatření pro smluvní vztahy

Mechanismus prověřování rizikových dodavatelů

- Doposud nejkontroverznější bod nZKB
- Aktuální verze primárně specifikovala sektor telekomunikací, očekávat lze dopady do energetiky, teplárenství a distribuční soustavy
- Dlouhodobě kritizována centralizace rozhodování na Úřad a nejasně definovaná kritéria (prováděcím předpisem)
- LRV (04. 04. 2024) k Mechanismu údajně zkonstatovala *„velmi široce definované kompetence úřadu“*

Co v úpravě nebude chybět:

Bezpečnost dodavatelského řetězce dle NIS2

Recitál, zejm. odst. 85-86, 88, 90-91, a čl. 22

- **(85)** Reakce na počet incidentů využitím zranitelností v produktech a službách třetích stran

(…) *„posoudit a zohlednit **celkovou kvalitu a odolnost produktů a služeb**, **opatření v oblasti kybernetické bezpečnosti**, která zahrnují, a postupů kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, **včetně** jejich **postupů k zajištění bezpečného vývoje**“* (…)

  - Začlenit opatření do **smluvních ujednání**
  - Přihlížet k rizikům jež mají původ u dodavatelů a poskytovatelů služeb **dalších úrovní**

- **(86)** Zvláštní pozornost – poskytovatelé řízených bezpečnostních služeb (MSSP)

Bezpečnost dodavatelského řetězce dle NIS2 | 2

Netechnické rizikové faktory:

- **(88)** Rovněž rizika v rámci interakcí **v širším ekosystému**, vč. **boje proti průmyslové špionáži a ochrany obchodního tajemství**
  - Patří např. i výzkumné instituce, poskytovatelé služeb transformace a zpracování dat – k odst. 85 ukládání a zpracování dat

- **(90) Koordinovaná posouzení bezpečnostních rizik**
  - **Podobně jako u sítí 5G -** Doporučení EK 2019/534 (CELEX:32019H0534)
  - (…) *„Potenciální **netechnické rizikové faktory**, jako je nepatřičný vliv třetí země na dodavatele a poskytovatele služeb, zejména v případě alternativních modelů správy, zahrnují **skryté zranitelnosti nebo „zadní vrátka“ a možné systémové narušení dodávek, zejména v případě technologické závislosti nebo závislosti na poskytovateli**.“*

Bezpečnost dodavatelského řetězce dle NIS2 | 3

- **(91) bližší specifikace odst. 90:**
  - K určení dodavatelských řetězců pro koordinované posouzení bezp. rizik, následující kritéria:
    - **i) rozsah využití** konkrétních *kritických služeb, systémů a produktů IKT* subjekty a jejich **závislost** na nich**, ii) relevantnost** pro plnění kritických nebo citlivých funkcí, **iii) dostupnost alternativních** služeb, **iv) odolnost řetězce** během celého životního cyklu vůči narušení a **v)** budoucí význam pro činnost (u vznikajících služeb)
  - Zvláštní důraz je třeba dále klást na služby IKT, systémy IKT nebo produkty IKT, které podléhají **specifickým požadavkům ze třetích zemí.**

- **Čl. 22 - Koordinované posouzení bezpečnostních rizik kritických dodavatelských řetězců na unijní úrovni**
  - EK, ENISA, NIS Cooperation group
  - koordinované posouzení bezp. rizik dodavatelských řetězců u specifických služeb, systémů nebo produktů IKT, přičemž zohlední **technické, případně netechnické** rizikové faktory

Kontext úpravy v nZKB

§ 25 Řízení dodavatelů a vztah k zadávání veřejných zakázek

§ 25 přejat a mírně formulačně upraven ze (současného) ZKB:

- Povinnost zohledňovat bezpečnostní požadavky při výběru dodavatele
- Povinnosti mít bezpečnostní požadavky kladené na dodavatele součástí smluv (podrobněji v přílohách odpovídajících vyhlášek)
  - Pro režim vyšších povinností dále bezpečnostní opatření Řízení dodavatelů v § 10

Usnesení Bezpečnostní rady státu z 21. 6. 2022: NÚKIB připraví návrh zákona k navýšení bezpečnosti dodavatelských řetězců strategické infrastruktury státu v oblasti IKT

§ 29 nZKB zavádí pravomoc Úřadu provádět prověřování rizik spojených s dodavatelem, jako "stěžejní část mechanismu prověřování bezpečnosti dodavatelského řetězce"

- **Kritika a očekáváné změny (rozhodnutí vlády, kontrasignace)**

Vyšší režim | Řízení dodavatelů

Řízení dodavatelů | Org. opatření | Prováděcí předpis:

- **Pravidla pro dodavatele**, včetně dokumentace **Politika řízení dodavatelů**, a seznamuje s nimi
- Identifikuje a eviduje **významné dodavatele**
- **Prokazatelně informuje** dodavatele o jeho zařazení do evidence (písemně s náležitostmi)
- **Řídí rizika** s nimi spojená a zajistí odpovídající **smluvní ujednání** *(plný text – vyhláška/backup prezentace)*

Významní dodavatelé:

- **Hodnocení rizik** před výběrovým řízením a před uzavřením smlouvy
- Ve **smluvních vztazích**:
  - způsoby a úrovně realizace bezpečnostních opatření,
  - obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu BO
- **Pravidelné hodnocení rizik a kontrolu zavedených BO** (vlastní zdroje nebo 3. strana)
- **Řešení nedostatků**

Nižší režim | Smluvní opatření a specifické body

- Zejména **opatření při uzavírání smluv s dodavateli** | ustanovení (o):
  - a) **zajišťující bezpečnosti informací** (požadavek na zajištění důvěrnosti, integrity a dostupnosti),
  - b) o **auditu** dodavatele,
  - c) **řetězení** dodavatelů,
  - d) upravující **podmínky ukončení smluvního vztahu z pohledu bezpečnosti**,
  - e) **sankcích** za porušení smluvních povinností,
  - f) **oprávnění užívat data**,
  - g) **autorství** programového kódu, případně o programových **licencích**,
  - h) **důvěrnosti smluvního vztahu**,
  - i) upravující **povinnost dodržovat pravidla pro dodavatele**, se kterými byli relevantní pracovníci dodavatele prokazatelně seznámeni,
  - j) **řízení změn**,
  - k) **kybernetických bezpečnostních incidentech** souvisejících s plněním smlouvy,
  - l) upravující zajištění řízení **kontinuity činností**,
  - m) náležitosti **smlouvy o úrovni služeb (SLA)** a způsobu a úrovni realizace bezpečnostních opatření.

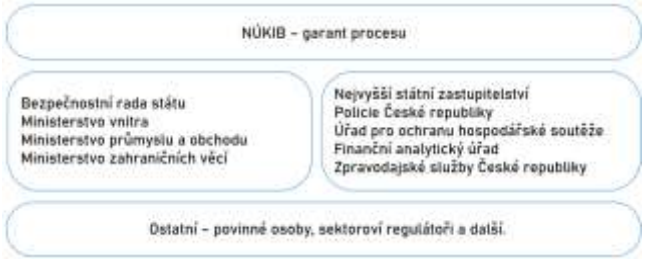
- Dále definovat:
  - Pravidla vzdáleného přístupu dodavatelů
  - (Aplikační bezpečnost) Aktiva bez podpory výrobce / dodavatele

Prověřování rizik u dodavatele – stav před LRV

Prověřování rizik spojených s dodavatelem (§ 29):

NÚKIB ve spolupráci s ministerstvy, zpravodajskými službami a jinými orgány státu mající relevantní informace pro posouzení důvěryhodnosti dodavatele.

Základem procesu jsou informace o dodavatelích od poskytovatelů strategicky významných služeb



Kritická část / Nepominutelné funkce SVS

Pouze u strategicky **významné služby (cca 150 subjektů)**

▪**- Část systému, kterou poskytovatel sám určí jako kritickou** (aktiva s kritickým nebo vysokým dopadem na službu)

- Rozsahem vždy alespoň aktiva SVS, která zajišťují **nepominutelné funkce** systému (NÚKIB)

Nepominutelné funkce definované vyhláškou:

1) ve **veřejné komunikační síti** související s *řízením síťových zdrojů, se směrováním a jinou kontrolou nebo řízením provozu* (…) mohou mít **významný dopad na síťový provoz** a

2) v **sítích 4. a 5. generace**

§ 31 Omezení rizik spojených s dodavatelem:

Úřad vydá **opatření obecné povahy,** kterým **stanoví podmínky nebo zakáže využití** plnění dodavatele *bezpečnostně významné dodávky* **v kritické části** stanoveného rozsahu

- **Přihlédnutí k životnímu cyklu technologií, zohlednění dopadů**
- **Přezkum proveden minimálně jednou za 4 roky**

Děkuji za pozornost

michael.batrla@rossum.ai
michael.batrla@law.muni.cz
michael.batrla@protonmail.com
linkedin.com/in/mbtr

Blok 2:
Hlášení kybernetických bezpečnostních incidentů podle ZKB

ZKB 2024: Revoluce v kybernetické bezpečnosti od 18. 10. 2024

Michael Bátrla | 18. 04. 2024

Témata

- **Blok 1: Prověřování rizik u dodavatelů**
  - Aktuální stav
  - Záměr NIS2
  - Kontext v ČR
  - Znění před LRV
- **Blok 2: Hlášení kybernetických bezpečnostních incidentů podle ZKB**
  - Definice, událost vs. incident
  - Vyšší vs. nižší režim a významné incidenty
  - Prvotní hlášení a další postup
  - Sankce
  - Vztah k ostatním předpisům (GDPR)

Aktuální stav materiálu k 22. ledna 2024. V rámci legislativního procesu pravděpodobně dojde ke změnám (např. LRV 04. 04. 2024).

Úvod

NIS2 | čl. 6 odst. 6

„Událost narušující bezpečnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které jsou nabízeny prostřednictvím informačních sítí a informačních systémů nebo které jsou jejich prostřednictvím dostupné.“

nZKB | § 2, odst. 1 písm. f)

„kybernetickým bezpečnostním incidentem ***narušení bezpečnosti informací v rámci aktiv“***

Kybernetická bezp. událost vs. incident

- Rozdíl mezi **událostí**, **incidentem (nZKB) | významným incidentem** a **rozsáhlým KB incidentem (NIS2)**
  - **Událost (nZKB) -** může nebo mohla vyústit v kybernetický bezpečnostní incident
  - **Významný incident (NIS2)** – závažné provozní narušení služby nebo finanční ztráty, anebo třetí osoby postihl značnou hmotnou nebo nehmotnou újmou
  - **Rozsáhlý (NIS2)** – škodlivost (na území dvou a více ČS)

Pozn.:

- **NIS2** oproti NIS1 příměji definované požadavky u incidentů:
  - Podoba hlášení incidentů i kontaktní údaje
  - Důraz na automatizaci, jednotný postup
  - Ale **hlášení pouze významných** (nZKB u vyššího režimu přísnější)

- **Zvládáním KBI** úkony vedoucí k zajištění prevence, detekce, analýzy, omezení dopadů incidentu, reakce na incident a následné obnovy

Povinnost hlášení

- **Portál NÚKIB (dříve „Neweb“)**
  - Cílem je platforma pro veškerou komunikaci NÚKIB-RS
  - Důraz automatizovat úkony (vs. API možná ve v2025)
  - Nelze-li: datová schránka, příslušná adresa el. pošty

- **Vyšší režim**
  - Povinnost hlásit **všechny** kybernetické bezpečnostní incidenty **Úřadu**
    - mají původ v kybernetickém prostoru
    - a nelze u nich do **24 hodin** (lhůta podle § 17 odst. 1) vyloučit úmyslné zavinění

- **Nižší režim**
  - Povinnost hlásit **Národnímu CERT** všechny KBI, které
    - mají **významný dopad na poskytování RS,**
    - mají původ v kybernetickém prostoru,
    - a nelze u nich do **24 hodin** vyloučit úmyslné zavinění

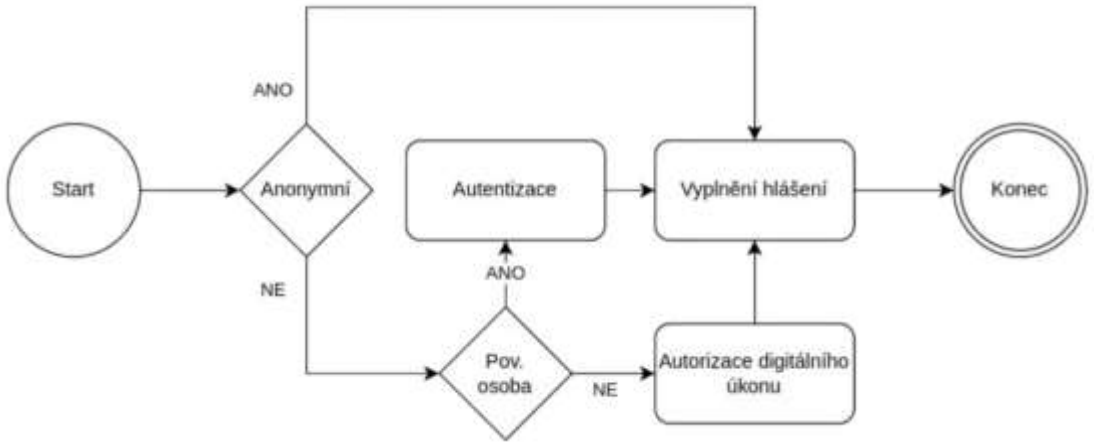
Identita občana

CAAIS

Prvotní hlášení

- Do **24 hodin**
- Identifikační údaje
- Základní údaje o KBI
- Domněnka, zda je způsoben nezákonným zásahem či možnost přeshraničního dopadu

- **NÚKIB (pro vyšší povinnosti):**
  - Informuje, zda KBI **významný dopad** na kybernetický prostor státu
  - Dle dopadu na RS, sektoru, aktuálního stavu KP státu
  - Do 24 hodin po nahlášení



Významný dopad | Další postup oznamování

- Do 72* hodin **| Oznámení s aktualizovanými informacemi**
  - Prvotní posouzení, dopad a indikátory kompromitace (IoC)

- Kdykoli na výzvu NÚKIB/N-CERT nebo nevyřešený > 30 dní | **Průběžná zprávu o podstatných změnách stavu zvládání KBI**
  - Informace o doposud učiněných krocích a o případných nových skutečnostech
  - Nevyřešený > 30 dní| navíc **plánované kroky k vyřešení incidentu** a **vysvětlení, proč doposud nedošlo k vyřešení incidentu**

- Nejpozději do 30 dnů od oznámení nebo poslední zprávy| **Závěrečná zprávu o vyřešení KBI**
  - **podrobný popis incidentu** vč. závažnosti a dopadu
  - druh hrozby nebo pravděpodobnou příčinu
  - učiněná a probíhající opatření ke zmírnění následků,
  - a případně přeshraniční dopad incidentu.

* Poskytovatel RS vytvářejících důvěru do 24 hodin

Vyšší režim | Opatření k detekci KBU

- **Vyhláška o bezpečnostních opatřeních**
- **Org. opatření 12. | Zvládání KB událostí a incidentů:**
  - Procesy, pravidla a postupy pro 1) detekci, zaznamenávání a vyhodnocení KBU a 2) zvládání KBI
  - Přidělí odpovědnosti pro obě oblasti a zajištění oznamování
  - Využívá nástroje pro detekci, zaznamenávání a vyhodnocování KBU:
    - Ověření a kontrolu síťového provozu a perimetru,
    - Centrálně spravovaný nástroj pro ochranu před škodlivým kódem, oprávnění spouštění kódu, datové nosiče...,
    - Sběr, vyhledávání a seskupování souvisejících záznamů, včasné varování
  - Bezpečnostní opatření pro odvrácení nebo zmírnění dopadů
  - Prošetření, určení příčin, vyhodnocení účinnosti řešení a bezpečnostních opatření

Nižší režim

- Incidenty mající **významný dopad** na poskytování regulované služby Národnímu CERT (CSIRT.CZ, provozovaný CZ.NIC)
- **Samostatná úvaha subjektu o významném dopadu** dle vyhlášky
  - Překročení **únosné míry újmy a zároveň významného dopadu:**

1) Únosná míra újmy

- souhrn nejvyšší škody, kde ještě nejsou ohroženy životy či zdraví osob nebo schopnost poskytovatele dostát svým závazkům

2) Oblasti pro posouzení významnosti dopadu:

- Provozní dopad,
- množství zasažených osob (zaměstnanci, uživatelé),
- čas a zdroje k obnově,
- citlivost dat,
- lokaci (významnost zasažených aktiv) a příčinu incidentu (chyba, závada, úmysl)

Sankce za nedodržení povinností

Režim povinností	Maximální částka nebo	celosvětového ročního obratu
Vyšší režim	Až 250 milionů Kč	2 %
Nižší režim	Až 175 milionů Kč	1,4 %

Mimo jiné:

- **neohlásí** kybernetický bezpečnostní incident
- nepředloží **prvotní hlášení** o incidentu
- **nedoplní některý z údajů o incidentu**
- **neposkytne informace nebo součinnost při zvládání incidentu** podle

- **nezohlední požadavky** vyplývající z bezpečnostních opatření **při výběru dodavatele nebo ve smlouvě s dodavatelem**
- **SVS** také: **nezjišťuje, neeviduje a neohlásí informace o dodavateli bezpečnostně významné dodávky**

Hlášení dle nZKB a další předpisy

- *„Není dotčena informační povinnost podle jiného právního předpisu nebo přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů“*
  - **GDPR**: Zásada – osobní údaje **technicky a organizačně zabezpečené** adekvátně jejich důležitosti
  - **NIS2: Konkrétní požadavky** ochrany dat

- **Incidenty s únikem osobních údajů |** Ohlašování na **dvou místech (!):**
  - NÚKIB jako úřad odpovědný za prošetření kybernetické bezpečnostní události
  - Úřad pro ochranu osobních údajů (ÚOOÚ) jako dohled nad dodržováním GDPR

- **Následné kroky | Dle okolností (např. následky incidentu) a dohoda Úřadů**
  - *Ne bis in idem* (ne dvakrát ve stejné věci)

Děkuji za pozornost

michael.batrla@rossum.ai
michael.batrla@law.muni.cz
michael.batrla@protonmail.com
linkedin.com/in/mbtr

Řízení dodavatelů (VR) | BO pro smluvní vztahy

Obsah smlouvy s významnými dodavateli | ustanovení (o):

- a) **bezpečnosti informací** (z pohledu důvěrnosti, integrity a dostupnosti),
- b) oprávnění **užívat data**,
- c) **autorství** programového kódu, popřípadě o programových **licencích,**
- d) **kontrole a auditu** dodavatele (pravidla zákaznického auditu),
- e) upravující **řetězení dodavatelů**, přičemž musí být zajištěno, že **poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem** a nebudou v rozporu s požadavky povinné osoby na dodavatele,
- f) povinnosti dodavatele **dodržovat bezpečnostní politiky** povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele (nebo odsouhlasení pro dodavatelský vztah relevantních částí bezpečnostních politik) povinnou osobou,
- g) **řízení změn,**
- h) **souladu smluv** s obecně závaznými právními předpisy,
- i) **povinnosti dodavatele informovat** povinnou osobu o:
  - 1. KBI souv. s plněním smlouvy,
  - 2.způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,
  - 3. významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy s povinnou osobou,
  - 4. žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána.
- j) **specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy**, tzv. exit strategie (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),
- k) specifikace podmínek pro **řízení kontinuity činností** v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),
- l) specifikace **podmínek pro formát předání dat, provozních údajů a informací** po vyžádání povinnou osobou,
- m) pravidla pro **likvidaci dat,**
- n) **právu jednostranně odstoupit od smlouvy nebo smlouvu vypovědět bez výpovědní doby v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy** využívanými dodavatelem k plnění podle smlouvy,
- o) sankcích **za porušení povinností** a
- p) **zpřístupnění nebo předání dat na základě žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu**
  - 1. až po provedení přezkoumání zákonnosti žádosti,
  - 2. až po vynaložení úsilí o zabránění zpřístupnění nebo předání dat v rámci možností daných právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána
  - 3. pouze v nezbytném rozsahu.