NGSS
Next Generation
Security Solutions

„Kybernetická bezpečnost a zavedení směrnice EU NIS2 “

07.06.2024

Směrnice NIS 2

- NIS2 již nehledá systémy důležité pro společnost, ale definuje **celé služby důležité pro její fungování**
- NIS2 přináší nově dva režimy, ve kterých se regulovaný subjekt může nacházet - „**essential / základní**“ a „**important / důležité**“ (přísnější požadavky jsou na „essential“)
- Transpoziční lhůta (tj. lhůta, ve které musí členské státy směrnici promítnout do národního práva) je stanovena na **21 měsíců (říjen 2024)**

Finální znění směrnice NIS2
27. prosince 2022

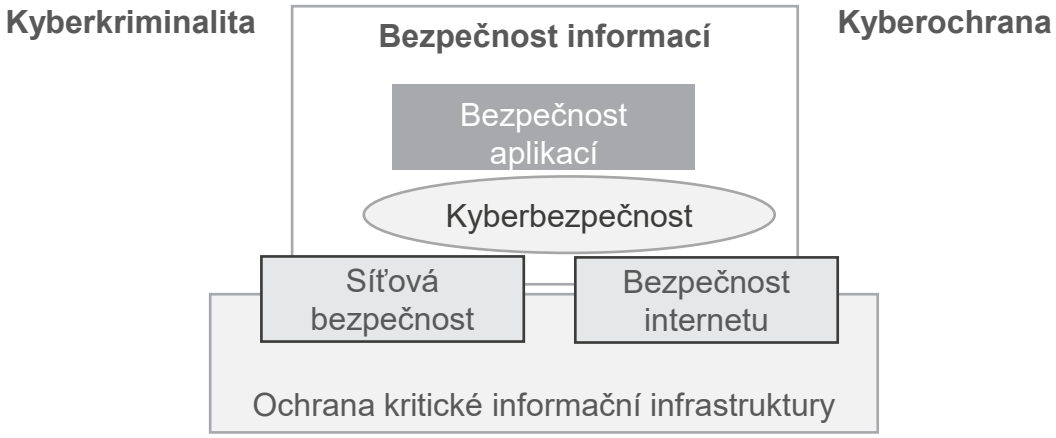
→

Změny zákona a nové povinnosti v ČR
od konce roku 2024?

- **březen 2023 -** veřejná konzultace odborné veřejnosti (**1144** unikátních připomínek, podnětů a komentářů)
- **červenec 2023** - mezirezortní připomínkové řízení (**864** připomínek k zákonu)
- **22. ledna 2024** – NÚKIB vypořádal připomínky a předal zákon do legislativní rady vlády (LRV)
- **4. duben 2024** – zákon vrácen NÚKIB k úpravě
- **29. květen 2024** – zákon znovu předložen LRV (přes 2000 změn)

ISMS - kybernetická bezpečnost

- Kybernetická bezpečnost zahrnuje především **činnosti v kybernetickém prostoru** a její rozsah se předpokládá **užší** než má informační bezpečnost
- Vztah mezi kybernetickou bezpečností a ostatními bezpečnostními doménami:



- **Současné pojetí více slučuje kybernetickou bezpečnost s informační bezpečností** – záleží na rozsahu, který si určíme

NIS 2 – důraz na služby

- NIS2 již nehledá systémy důležité pro společnost, ale definuje **celé služby důležité pro její fungování** (uvedeny v přílohách)
- Jedná se o více než 60 služeb roztříděných do 18 odvětví:
    - organizace poskytuje **alespoň jednu službu** uvedenou v přílohách směrnice, a zároveň
    - je středním nebo velkým podnikem (**50 / 250 a více zaměstnanců**), nebo dosahuje **ročního obratu** nebo bilanční sumy roční rozvahy alespoň **10 milionů EUR** (zhruba 250 milionů CZK)
- NIS2 přináší nově dva režimy, ve kterých se regulovaný subjekt může nacházet - „**essential / základní**“ a „**important / důležité**“ (přísnější požadavky jsou na „essential“)
- NÚKIB upravil výše uvedené režimy na:
    - poskytovatel regulované služby v **režimu vyšších povinností**
    - poskytovatel regulované služby v **režimu nižších povinností**

Odvětví regulovaných služeb

1. veřejná správa a výkon veřejné moci
2. energetika
3. výrobní průmysl
4. potravinářský průmysl
5. chemický průmysl
6. vodní hospodářství
7. odpadové hospodářství
8. doprava

9. digitální infrastruktura a služby
10. finanční trh
11. zdravotnictví
12. věda, výzkum a vzdělávání
13. poštovní a kurýrní služby
14. obranný průmysl
15. vesmírný průmysl

NGSS
Next Generation
Security Solutions

Regulovaná služba ve výrobě

7. Výrobní průmysl

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
7.1. Výroba počítačů, elektronických a optických přístrojů a zařízení	Výrobce počítačů, elektronických a optických přístrojů a zařízení ve smyslu oddílu 26 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.
7.2. Výroba elektrických zařízení	Výrobce elektrických zařízení ve smyslu oddílu 27 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.
7.3. Výroba strojů a zařízení nezařazená pod jiné oddíly klasifikace CZ-NACE	Jinde nezařazený výrobce strojů a zařízení ve smyslu oddílu 28 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.
7.4. Výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů	Výrobce motorových vozidel, přívěsů a návěsů ve smyslu oddílu 29 klasifikace CZ-NACE je I. poskytovatel regulované služby v režimu vyšších povinností v případě, že sériově vyrábí osobní motorová vozidla, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým nebo středním podnikem.
7.5. Výroba ostatních dopravních prostředků a zařízení	Výrobce ostatních dopravních prostředků a zařízení ve smyslu oddílu 30 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.

Firma, s.r.o. **ARES**

CZ-NACE **26200**	Výroba počítačů a periferních zařízení
CZ-NACE **27900**	Výroba ostatních elektrických zařízení

Hlášení a registrace regulované služby

Životní cyklus poskytovatele regulované služby je následující:

1. Naplnění **Podmínek pro registraci** regulované služby
2. **Ohlášení regulované služby** (poskytovatelem) nejpozději **do 60 dnů** ode dne, kdy ke splnění podmínek došlo / **Rozhodnutí o registraci regulované služby** vydané z moci úřední (úřadem)
3. **Registrace regulované služby** (úřadem)

---

4. **Ohlášení změn regulované služby** (poskytovatelem) nejpozději **do 60 dnů** ode dne, kdy ke změně došlo

---

5. **Zrušení registrace regulované služby** pokud služba již nesplňuje podmínky pro registraci regulované služby (úřadem na základě žádosti poskytovatele)

NGSS
Next Generation
Security Solutions

NIS 2 - požadavky

Směrnice stanovuje okruhy bezpečnostních opatření, které mají členské státy rozpracovat ve svých právních předpisech a uložit je budoucím povinným osobám:

- **Analýza rizik** a **politiky bezpečnosti informací**
- Zvládání **incidentů**
- **Kontinuita činností** včetně zálohování, zotavení (disaster recovery) a krizového řízení
- Bezpečnost v rámci **dodavatelského řetězce**
- Bezpečnost v rámci **pořízení, vývoje a údržby systémů**
- Politiky a postupy pro **hodnocení účinnosti bezpečnostních opatření** (tj. audit)
- Praktiky **základní počítačové hygieny a vzdělávání** v oblasti kybernetické bezpečnosti
- Politiky a postupy týkající se **využívání kryptografie**
- **Bezpečnost lidských zdrojů**, **řízení přístupů** a **aktiv**
- Využívání **vícefaktorového ověření identity**, bezpečných komunikačních nástrojů a nástrojů pro nouzovou komunikaci

NIS 2 v ČR

NÚKIB reagoval na zavedení směrnice NIS2 zveřejněním návrhů nového zákona a navazujících směrnic zveřejněných koncem ledna 2023 a v lednu 2024 před předáním legislativní radě vlády dále upravil návrh legislativních norem takto:

- Nový zákon o kybernetické bezpečnosti
- Vyhláška o regulovaných službách
- Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
- Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
- Vyhláška o portálu NÚKIB
- Vyhláška o nepominutelných funkcích stanoveného rozsahu

Bezpečnostní opatření – vyšší povinnosti

Organizační opatření:

1. systém řízení bezpečnosti informací
2. požadavky na vrcholné vedení
3. stanovení bezpečnostních rolí
4. řízení bezpečnostní politiky a bezpečnostní dokumentace
5. řízení aktiv
6. řízení rizik
7. řízení dodavatelů
8. bezpečnost lidských zdrojů
9. řízení změn,
10. akvizice, vývoj a údržba
11. řízení přístupu
12. zvládání kybernetických bezpečnostních událostí a incidentů
13. řízení kontinuity činností a
14. provádění auditu kybernetické bezpečnosti

Technická opatření:

1. fyzická bezpečnost
2. bezpečnost komunikačních sítí
3. správa a ověřování identit
4. řízení přístupových práv a oprávnění
5. detekce kybernetických bezpečnostních událostí
6. zaznamenávání událostí
7. vyhodnocování kybernetických bezpečnostních událostí
8. aplikační bezpečnost
9. kryptografické algoritmy
10. zajišťování dostupnosti regulované služby a
11. zabezpečení průmyslových, řídících a obdobných specifických technických aktiv

NGSS
Next Generation
Security Solutions

Bezpečnostní opatření - nižší povinnosti

Organizační a technická opatření:

1. systém zajišťování minimální kybernetické bezpečnosti
2. požadavky na vrcholné vedení
3. řízení aktiv
4. řízení rizik
5. bezpečnost lidských zdrojů
6. řízení kontinuity činností
7. řízení přístupu
8. řízení identit a jejich oprávnění
9. detekce a zaznamenávání kybernetických bezpečnostních událostí
10. řešení kybernetických bezpečnostních incidentů
11. bezpečnost komunikačních sítí
12. aplikační bezpečnost a
13. kryptografické algoritmy

Bezpečnostní role při zavedení NIS2

Režim vyšších povinností:

- Vrcholové vedení organizace
- Výbor pro řízení kybernetické bezpečnosti
- Manažer kybernetické bezpečnosti
- Architekt kybernetické bezpečnosti
- Garant aktiva
- Auditor kybernetické bezpečnosti

Režim nižších povinností:

- Vrcholové vedení organizace
- Osoba odpovědná za kybernetickou bezpečnost
- Garant aktiva

Politiky dle NIS2 pro vyšší povinnosti

- Politika systému řízení bezpečnosti informací
- Politika organizační bezpečnosti
- Politika řízení bezpečnostní politiky a dokumentace
- Politika řízení aktiv
- Politika řízení rizik
- Politika řízení dodavatelů
- Politika bezpečnosti lidských zdrojů
- Politika bezpečného chování uživatelů, administrátorů a osob zastávajících bezpečnostní role
- Politika bezpečného používání mobilních zařízení
- Politika řízení změn
- Politika akvizice, vývoje a údržby
- Politika řízení přístupu
- Politika zvládání kybernetických bezpečnostních událostí a incidentů
- Politika řízení kontinuity činností
- Politika fyzické bezpečnosti
- Politika bezpečnosti komunikační sítě
- Politika pro zaznamenávání událostí
- Politika nasazení, používání a údržby nástrojů pro detekci kybernetických Opatření pro ochranu přístupu k záznamům o těchto událostech.
- Politika řízení zranitelností a patch management
- Politika používání kryptografie
- Politika dlouhodobého ukládání, zálohování a obnovy

Dokumentace pro vyšší povinnosti

- Metodika pro identifikaci a hodnocení aktiv
- Zpráva o hodnocení aktiv a rizik
- Prohlášení o aplikovatelnosti
- Plán zvládání rizik
- Plán provádění auditu kybernetické bezpečnosti.
- Zpráva z auditu kybernetické bezpečnosti
- Zpráva z přezkoumání systému řízení bezpečnosti informací
- Plán rozvoje bezpečnostního povědomí
- **Metodika pro provedení analýzy dopadů**
- Plány kontinuity činností
- Plány obnovy
- Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

- **Evidence technických aktiv, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována**
- **Evidence technických aktiv, účtů a autentizačních mechanismů, které nesplňují požadavek na vícefaktorovou autentizaci**
- Další **doporučená dokumentace**
  - Topologie infrastruktury
  - Segmentace infrastruktury
  - **Přehled technických aktiv** v rozsahu systému řízení bezpečnosti informací, zejména síťových zařízení, aktivních prvků, koncových zařízení a serverů
  - Spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory

Politiky a dokumentace pro nižší povinnosti

Politiky (7):

- Politika zajišťování minimální úrovně kybernetické bezpečnosti
- Politika bezpečnosti lidských zdrojů
- Politika řízení kontinuity činností
- Politika řízení přístupu
- Politika detekce kybernetických bezpečnostních událostí a řešení kybernetických bezpečnostních incidentů
- Politika bezpečnosti komunikační sítě
- Politika aplikační bezpečnosti

Bezpečnostní dokumentace:

- Evidence aktiv
- **Přehled bezpečnostních opatření**
- Plány obnovy
- Závěrečná zpráva o kybernetickém bezpečnostním incidentu
- **Evidence nepodporovaných technických akt**iv
- Další **doporučená dokumentace**:
  - Topologie infrastruktury
  - Segmentace infrastruktury
  - Přehled technických aktiv zejména síťových zařízení, aktivních prvků, koncových zařízení a serverů
  - Kontakty na osoby pověřené technickou a systémovou podporou

Vybraná opatření

- **Stanoveny požadavky na vrcholové vedení organizace (školení, účast na testech…).** NÚKIB může navrhnout **pozastavení výkonu řídící funkce členovi statutárního orgánu**
- Definována **Strategicky významná služba** v odvětvích **veřejná správa, energetika, doprava a digitální infrastruktura**
- **Všichni hodnotí aktiva** (součástí rozsahu), jen ti kdo mají **vyšší povinnosti hodnotí rizika**
- NÚKIB může až **zakázat využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu** (na základě vyhodnocení rizikovosti dodavatele významné ohrožení bezpečnosti ČR nebo vnitřního pořádku)
- Povinnost provádět **protiopatření** (výstraha, varování a reaktivní protiopatření)
- Možnost vyhlášení **stavu kybernetického nebezpečí (**při značném ohrožení nebo narušení BI v kybernetickém prostoru)
- Poskytovatel regulované služby **hlásí KBI**, které, mají původ v kybernetickém prostoru (nižší jen ty, které mají významný dopad na poskytování regulované služby) a nelze u nich … vyloučit úmyslné zavinění (**do 24 hodin**) – nutno rozlišit událost a incident
- V kontinuitě činností se provádí **analýza dopadů (vyšší)** a stanovuje **RTO, RPO** a **minimální úroveň poskytovaných služeb**
- **MFA** jako **základ,** jsou stanoveny **požadavky na hesla** (uživatel **12 znaků,** Admin **17 znaků a** technická aktiva **22 znaků)**
- **Použití** předepsaných **technických nástrojů** (zejména vyšší povinnosti)

Jak na to – zavést/aktualizovat ISMS/SŘBI

- Bezpečnost informací má za cíl zajistit ochranu zpracovávaných a uchovávaných informací

- Bezpečnost informací se řídí a prosazuje s využitím **Systému řízení bezpečnosti informací** ve zkratce **ISMS** nebo zajišťování **Systému minimální kybernetické bezpečnosti**

Zjednodušeně lze říci, že **ISMS:**

- má za cíl **ochránit zpracovávané informace** a
- k dosažení cíle **zavádí sadu bezpečnostních opatření**
- vybraných na základě **ohodnocení rizik**

Schéma zavedení ISMS

Jedná o **zavedení a provoz ISMS** s:

- vymezeným rozsahem
- výběrem opatření na základě hodnocení rizik
- který má zavedené role a opatření
- je pravidelně auditován a hodnocen

Zavádění SŘBI - etapy

1. Provedení **srovnávací analýzy současného stavu kybernetické bezpečnosti** vůči požadavkům vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen Vyhláška).
2. Provedení **hodnocení aktiv a rizik a přijetí bezpečnostních opatření** k určení možných rizik a návrhu jejich pokrytí.
3. **Implementace vybraných bezpečnostních opatření** zahrnuje návrh postupů, jejich popis v bezpečnostní dokumentaci a rozpracování do návrhu záznamů systému řízení bezpečnosti informací.
4. Provedení **interního auditu** a **přezkoumání systému řízení bezpečnosti informací** uzavírá celý cyklus zavedení systému řízení bezpečnosti informací. Audit bude proveden jako vzorový.

Na co si dát pozor

- Navázat na to co již bylo v oblasti bezpečnosti zavedeno
- Připravit si **plán zavedení – definovat rozsah**
- Počítat s časovou a projektovou náročností, vyčlenění zdrojů
- S posouzením stavu a hodnocením rizik mohu začít hned
- Jednotný systém řízení bezpečnosti informací
- Neopakovat chyby spojené s GDPR

Děkuji za pozornost

Antonín Šefčík

asefcik@ngss.cz

+ 420 601 307 992