

NIS

Network Information Security

CESNET, z. s. p. o.



NIS

- Směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.
 - První evropský právní předpis zabývající se problematikou kybernetické bezpečnosti.
 - Jejím cílem je dosažení vysoké společné úrovně bezpečnosti sítí a informačních systémů napříč členskými státy EU.
-
- *sjednotit úroveň v oblasti bezpečnosti na úrovni sítí a informačních systémů v zemích EU*
 - *dosáhnout zřízení vrcholových CERT/CSIRT týmů*

NIS

- Srpen 2016 – publikace a nabytí platnosti směrnice NIS.
- Směrnice NIS stanoví pro transpozici lhůtu 21 měsíců od nabytí platnosti, tj. květen 2018.
- Dále ještě uvádí lhůtu dalších 6 měsíců od uplynutí transpoziční lhůty pro identifikaci provozovatelů základních služeb.
- NBÚ chce stihnout transpozici směrnice NIS ještě před volbami do Poslanecké sněmovny PČR (říjen 2017).
- Transpozice v ČR
 - novelizace ZKB
 - prováděcí právní předpisy (dopadová a oblastní kritéria)
 - *připravované materiály jsou diskutovány se zástupci ostatních resortů i odborné veřejnosti v rámci zřízených pracovních skupin*

Hlavní pilíře NIS

- Organizační a legislativní charakter
- Povinnosti vztahující se na okruhy povinných subjektů
 - provozovatelé základních služeb
 - poskytovatelé digitálních služeb
- Členské státy jsou povinny:
 - Vytvořit národní rámce bezpečnosti sítí a informačních systémů, tj. strategii pro bezpečnost sítí a informačních systémů
 - Zřídit tým/týmy CSIRT na národní úrovni
 - Zřízení centrálního orgánu (ústřední kontaktní místo na úrovni Unie)
 - Účastnit se unijních kooperačních struktur – skupina pro spolupráci a síť CSIRT (CSIRT Network)
 - Zajistit, aby povinné subjekty přijaly nezbytná bezpečnostní opatření a hlásily incidenty.
 - Kontrolovat a vymáhat plnění povinností povinnými subjekty.

Povinné osoby

- 2 skupiny povinných osob
 - provozovatelé základních služeb
 - poskytovatelé digitálních služeb

Provozovatelé základních služeb

- Subjekty klíčové pro fungování základních společenských a ekonomických činností.
- Budou určováni NBÚ v sektorech – **energetika, doprava, bankovníctví, infrastruktura finančních trhů, zdravotnictví, dodávky a rozvody pitné vody a digitální infrastruktura...**
- Digitální infrastruktura:
 - internetové uzly (IXP)
 - poskytovatelé služeb systému doménových jmen (DNS)
 - rejstříky internetových domén nejvyšší úrovně
- Podléhají principu **minimální harmonizace**.
- Dopadová a oblastní kritéria budou stanovena v prováděcím právním předpise (směrnice uvádí pouze obecné znění, které musí členské státy specifikovat).

Poskytovatelé digitálních služeb

- Jsou omezeni na tři konkrétní druhy – **online tržiště, internetové vyhledávače a poskytovatele cloud computingu.**
- Regulace nepadá na podniky naplňující kritéria pro mikropodniky a malé podniky.
- Jejich povinnosti budou mírnější, aby nedošlo k přílišnému omezení rozvoje tohoto trhu.
- Podléhají principu **maximální harmonizace.**
- Prováděcí akty Evropské komise stanoví doporučení ohledně bezpečnostních opatření, parametrů pro určování významnosti dopadů incidentů a způsobu hlášení incidentů.
- Budou se určovat sami, na základě definic poskytnutých ve směrnici NIS.

Transpozice v ČR

- NBÚ je správním úřadem odpovědným za výkon státní správy v oblasti kybernetické bezpečnosti (§ 22 odst. 1 zákona o kybernetické bezpečnosti)
- NBÚ bude plnit roli centrálního orgánu (ústřední kontaktní místo na úrovni Unie)
- Dále bude fungovat jako jednotné kontaktní místo.
- **Bude určovat provozovatele základních služeb.**
- **Bude kontrolovat plnění povinností povinnými subjekty.**

Role CERT/CSIRT

- Směrnice ukládá členským státům zřídit bezpečnostní tým/týmy typu CSIRT, které budou splňovat určité požadavky.
- CSIRT Network
- V ČR je nastaven systém vládního a národního CERT, který bude ponechán.
 - GovCERT.CZ – vládní, provozován NBÚ
 - CSIRT.CZ – národní, provozován CZ.NIC
- Obě pracoviště budou plnit stejné úkoly jako doposud, rozšíří se však jejich pole působnosti a povinnosti:
 - GovCERT.CZ (vládní) – v rámci jeho působnosti budou zařazeni **provozovatelé základních služeb**
 - CSIRT.CZ (národní) – jeho působnost bude rozšířena o **poskytovatele digitálních služeb**

Povinné osoby § 3 ZKB

- Orgány a osoby, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti:
 - a) poskytovatel služby elektronických komunikací a subjekt zajišťující **síť elektronických komunikací**, pokud není orgánem nebo osobou podle písmene b),
 - b) orgán nebo osoba zajišťující **významnou síť**, pokud nejsou správcem komunikačního systému podle písmene d),
 - c) správce informačního systému kritické informační infrastruktury,
 - d) správce komunikačního systému kritické informační infrastruktury a
 - e) správce významného informačního systému.

Novelizace ZKB

- **Základní služba** = služba, jejíž poskytování je závislé na sítích nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení činností v některém z těchto odvětví – *energetika, doprava, bankovníctví, infra finančních trhů, vodní hospodářství, chemický průmysl, digitální infrastruktura*
- **Informační systém základní služby** = systém, na jehož fungování je závislé poskytování základní služby
- **Provozovatel základní služby** = orgán nebo osoba odpovědná za poskytování základní služby a určená NBÚ

Novelizace ZKB

- **Digitální služba** = služba informační společnosti, která spočívá v poskytování služby
 - **on-line tržiště**, jež spotřebitelům umožňuje on-line uzavírat s prodávajícím kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, jenž využívá službu poskytovanou on-line tržištěm,
 - **internetového vyhledávače** nebo
 - **cloud computingu**, jež umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, jež je možno sdílet
- **Poskytovatelem digitální služby** právnická osoba, která poskytuje digitální službu a která není mikropodnikem nebo malým podnikem

Novelizace ZKB

- **Kritéria pro PZS by podle NIS měly zahrnovat alespoň následující hlediska:**
 - počet uživatelů, kteří jsou závislí na službě poskytované daným subjektem;
 - závislost dalších odvětví na službě poskytované daným subjektem;
 - možný dopad incidentů, pokud jde o intenzitu a trvání, na činnosti hospodářství a společnosti nebo na veřejnou bezpečnost;
 - podíl daného subjektu na trhu;
 - zeměpisný rozsah oblasti, která by mohla být incidentem dotčena;
 - důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativních způsobů zajištění této služby.

Transpozice NIS

- Srpen 2016 – publikace a nabytí platnosti směrnice NIS
- Květen 2018 – směrnice vstupuje v plnou účinnost
- Květen 2018 + 6 měsíců – musí být určení provozovatelé základních služeb
- Říjen 2017 – transpozice NIS novelizací ZKB
- Transpozice probíhá
 - novelizace ZKB
 - prováděcí právní předpisy (dopadová a oblastní kritéria)
 - připravované materiály jsou diskutovány se zástupci ostatních resortů i odborné veřejnosti v rámci zřízených pracovních skupin

Děkuji za pozornost.