Směrnice NIS2 a dopad její transpozice do právního řádu ČR

Vladimír Karas
Security Consultant

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER

Směrnice NIS2 a její transpozice do právního řádu ČR

- **Plné znění: „Směrnice Evropského parlamentu a Rady (EU) o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v EU“**
- **Ze dne 14. prosince 2022, zveřejněná ve věstníku 27. prosince 2022, plné znění na www.nukib.cz**
  - platnost 20. den po zveřejnění, tj. 16. ledna 2023
  - 21 měsíců na promítnutí do právního řádu
  - 144 odstavců recitálu
  - 46 článků
  - 3 přílohy
  - vyžaduje transpozici do národní legislativy
- **Ruší směrnici č. 2016/1148 ze dne 6. července 2016 (NIS)**

Proč je tu NIS2?

- **Rozdíly v implementaci NIS v jednotlivých členských státech EU**
- **Sjednocení přístupu ke kybernetické bezpečnosti v celé EU**
- **Důraz je položen na:**
  - řízení pomocí rizik (ISO 31000)
  - kontinuitu činností (ISO 22301)
  - bezpečnost dodavatelského řetězce
  - řízení kybernetické bezpečnosti např. dle norem řady ISO 27000 (recitál, čl. 79)
- **Důsledek – návrh nového zákona o kybernetické bezpečnosti a jeho doprovodných vyhlášek**

Nový zákon o kybernetické bezpečnosti

- **Garant: NÚKIB**
- **26. ledna 2023 předložen k odborné diskuzi, do 12. března 2023**
- **Nyní předložen k meziresortnímu připomínkovému řízení, do PSP v prvním pololetí 2024**
- **Úplně nová struktura**
  - zákon
  - 8 doprovodných vyhlášek
  - nové resp. rozšířené povinnosti odpovědných osob
  - odpovědnost statutárního orgánu
    - zákaz činnosti
    - trestní odpovědnost
  - vyšší pokuty – horní hranice 250 mil. Kč nebo 2% celosvětového obratu

Struktura nové legislativy

- **Nový zákon o kybernetické bezpečnosti**
- **Doprovodné vyhlášky**
  - 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
  - Vyhláška o kritériích rizikovosti dodavatele
  - Vyhláška o autorizovaných inspektorech
  - Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy

Které jsou regulované služby – odvětví

- Veřejná správa
- Energetika – Elektřina
- Energetika – Ropa a ropné produkty
- Energetika – Plynárenství
- Energetika – Teplárenství
- Energetika – Vodík
- Výrobní průmysl
- Potravinářský průmysl
- Chemický průmysl
- Vodní hospodářství
- Odpadové hospodářství
- Letecká doprava
- Drážní doprava
- Vodní doprava
- Silniční doprava
- Digitální infrastruktura a služby
- Finanční trh
- Zdravotnictví
- Vojenský průmysl
- Vesmírný průmysl

Nový zákon o kybernetické bezpečnosti – I.

- **Sdružuje dosavadní úpravu několika typů povinných osob do jedné - poskytovatele regulované služby**
- **Poskytovatel regulované služby musí naplňovat kritéria daná Vyhláškou o regulovaných službách**
- **Poskytovateli regulované služby zákon a vyhláška následně na základě služeb přiděluje tzv. režim povinností**
  - režim vyšších povinností
  - režim nižších povinností
- **Každý poskytovatel regulované služby má ve výsledku jen jeden režim a ten stanovuje, jaké povinnosti mu ze zákona plynou**

Nový zákon o kybernetické bezpečnosti – II.

- **Povinnosti poskytovatele regulované služby:**
  - hlásit údaje - souvisí s Vyhláškou o Portálu NÚKIB
  - stanovit rozsah řízení kybernetické bezpečnosti
  - zavádět bezpečnostní opatření – souvisí s Vyhláškou o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností a Vyhláškou o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností
  - hlásit kybernetické bezpečnostní incidenty
  - informovat zákazníky o incidentech a hrozbách
  - provádět protiopatření
  - uplatnit pravidla lokalizace dat v případě poskytovatelů regulované služby v režimu vyšších povinností
  - řídit bezpečnost dodavatelského řetězce (vyšší povinnosti)
  - podřídit se kontrole inspektorem (nižší povinnosti), souvisí s Vyhláškou o inspektorech

Co může v této oblasti udělat NOVICOM?

- **Studie zajištění kybernetické bezpečnosti organizace**
  - Posouzení, zda je organizace povinným subjektem (poskytovatelem regulovaných služeb) a stanovení úrovně povinností (nižší úroveň/vyšší úroveň)
  - Analýza současného stavu zajištění kybernetické bezpečnosti v organizaci
  - Analýza dodavatelského řetězce
  - Zpracování rozdílové analýzy vzhledem k úrovni povinností
  - Definice jednotlivých projektů a odhad jejich časové a finanční náročnosti
- **Spolupráce při realizaci projektů (organizační/technická)**
- **Spolupráce při provozu systému (outsourcing týmu kybernetické bezpečnosti)**

novicom

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER