Novela NIS2 alebo čo nám prichádza z EÚ do Kyberzákona?

Peter Bíro

Základný rámec NIS2

§

- Smernica EÚ č. 2022/2555 **o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii** (tzv. NIS2)
  - účinná 14. decembra 2022 – **transpozícia do 17. októbra 2024** – do zákona o kybernetickej bezpečnosti (69/2018 Z. z.)
  - Regulačný orgán = Národný bezpečnostný úrad [https://www.nbu.gov.sk/]
- ENISA – vedie eur. databázu zraniteľností (najmä pre CSIRTy) [čl. 12], register (regulovaných) subjektov... [čl. 27] - ČŠ do 17. apríla 2025 zoznam:
  - názov, kontaktné údaje (najmä adresa (hlavnej prevádzkarne), tel, **rozsahy IP adries**), odvetvie +- zoznam ČŠ kde poskytujú služby – do 2týž ohlasovanie každej zmeny (!) – NBÚ niečo z toho nahlasuje EK
- Právomoc ČŠ pri DNS podľa hlavnej prevádzkarne (nie nutne sídla) = presah aj mimo EÚ [čl. 26]

Výrazné rozšírenie subjektov

- Pôvodne poskytovatelia základných služieb a poskytovatelia digi. služieb **podľa (prahových) kritérií**
- Aktuálne - vzťahuje sa na **(bez ohľadu na ich veľkosť)** [čl. 3]
  - posk. verejných e-komunikačných sietí alebo verejne dostupných e-komunikačných služieb
  - poskytovateľov dôveryhodných služieb (podľa eIDAS)
  - registre názvov domén najvyššej úrovne a posk. služieb systému názvov domén
  - jediných posk. služby, kt. je kľúčovou pre zachovanie krit. spol. alebo hosp. činností
  - posk. služby, kt. narušenie by mohlo mať významný vplyv na ver. poriadok / bezp. / zdravie
  - narušenie služby posk. subjektom by mohlo vyvolať významné syst. riziko, najmä v odvetviach, v kt. by takéto narušenie mohlo mať cezhraničný vplyv
  - subjekt, kt. je vzhľadom na svoj osobitný význam na vnútroštátnej alebo reg. úrovni krit. pre konkrétne odvetvie alebo typ služby alebo pre iné vzájomne závislé odvetvia v ČŠ
  - subjekt je subjektom VS v ústrednej ŠS alebo na reg. úrovni, kt. po posúdení rizík poskytuje služby, kt. narušenie by mohlo mať významný vplyv na krit. spol. alebo hosp. činnosti … +

Rozšírenie povinností (1/2)

- **Povinné odborné školenia** pre členov riad. výborov [čl. 20 (2)] (+ možnosť brať takéto FO na zodpovednosť) [čl. 32 (6)] a vítané pre zamestnancov
- **Povinné oznamovanie** významných incidentov CSIRTu / NBÚ [čl. 23]
  - do 24h od zistenia včasné varovanie, do 72h aktualizácia a posúdenie, do 1mes záv. správa
  - v prípade potreby aj príjemcom služieb (aj opatrenia a nápravné kroky, kt. majú príjemcovia prijať)
- Incident je významný, ak: [čl. 23 (3)]
  - zasiahol alebo má schopnosť zasiahnuť iné FO alebo PO tým, že im spôsobí značnú majetkovú alebo nemajetkovú ujmu
  - spôsobil alebo má schopnosť spôsobiť dotknutému subjektu závažné prevádzkové narušenie služieb alebo finančnú stratu

Rozšírenie povinností (2/2)

- Riadiace orgány kľúčových subjektov musia schváliť (vhodné a primerané technické, operačné a organizačné) **opatrenia na riadenie kyber. rizík** [čl. 20 (1), čl. 21 (1)]
- Minimálne:
  - a) analýza kyb. rizík a bezp. IS + f) posudzovanie účinnosti opatrení na riadenie rizík
  - b) riešenie incidentov
  - c) kontinuita činností = riadenie zálohovania a obnova systému po havárii, krízové riadenie
  - d) bezp. dodávateľského reťazca vrátane bezp. aspektov pre vzťahy medzi subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb
  - e) bezp. pri nadobúdaní, vývoji a údržbe siete a IS vrátane riešenia zraniteľností a zverejňovania info o zraniteľnostiach
  - g) kyb. hygiena a odborná príprava v oblasti kyb. bezp.
  - h) kryptografia, prípadne šifrovanie
  - i) bezp. ľudských zdrojov, zásady kontroly prístupu a správu aktív
  - j) ak treba používanie viacstupňovej al. kontinuálnej autentifikácie, zabezpečenej kom.

Ďalšie novinky

§

- Špecifické povinnosti pre subjekty v **DNS infraštruktúre** [čl. 28]
- Rámce pre **kybernetickú krízu** + európska sieť styčných organizácií pre kybernetické krízy **(EU-CyCLONe)** [čl. 16]
- ČŠ môžu vyžadovať používanie **konkrétnych certifikovaných** IKT produktov, služieb alebo procesov [čl. 24]

- EK ***do 17. októbra 2024*** vykonávacie akty (technické a metodické požiadavky na bezp. opatrenia, pre významnosť incidentu...)

- **Sankcie** – max. 10 mil. EUR alebo 2% celosvetového ročného obratu [čl. 34], zastavenie činnosti riadiacej osoby [čl. 32]

OTÁZKY ?

Peter Bíro (gen. riaditeľ)
SK-NIC (správca domény .sk)
akademia@sk-nic.sk

Ďakujem za pozornosť!

Peter Bíro (gen. riaditeľ)

SK-NIC (správca domény .sk)

akademia@sk-nic.sk