

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

JUDr. Štefan Pilár



8. marca 2023

OBSAH

Kybernetická bezpečnosť v reáliách SR

Čo je to Smernica NIS II a čo so sebou prináša?

Identifikácia subjektov (pôsobnosť NIS II)

Komparácia požiadaviek ZoKB a NIS II

Smernica NIS II (ostatné)

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

Kybernetická bezpečnosť v reáliách SR

Smernica NIS II

SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555

o opatreniach na zabezpečenie vysokej spoločnej úrovne
kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie
(EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica
(EÚ) 2016/1148 (smernica NIS 2)

~~Smernica NIS~~

~~SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/1148~~

~~zo 6. júla 2016~~

~~o opatreniach na zabezpečenie vysokej spoločnej úrovne
bezpečnosti sietí a informačných systémov v Únii~~

od 18. októbra 2024

ZoKB

zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a
doplnení niektorých zákonov v platnom znení

(zákon č. 231/2022 Z. z.)

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

SMERNICA NIS II

čo to je?

čo so sebou prináša?

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

Čo je Smernica NIS II?

právny predpis záväzný pre členské štáty, nie jednotlivcov

prednosť pred vnútroštátnou úpravou

aplikácia eurokonformného výkladu v zmysle zásady nepriameho účinku

minimálna harmonizácia

povinnosť transpozície do 18. októbra 2024

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

Čo Smernica NIS II so sebou prináša?

Zmeny v kontexte iných predpisov

zrušenie Smernice NIS

vypustenie „bezpečnosti“ z eIDAS

vypustenie „bezpečnosti“ z Kódexu EK

Potreba zmien na národnej úrovni

(*nová*) kategorizácia subjektov

(*nová*) terminológia

povinnosť vypracovať zoznam (týchto) subjektov + povinnosť ich
nahlásenia (I2 mesiacov od nadobudnutia účinnosti)

Potreba zmien na národnej úrovni

(*nová*) zodpovednosť za riešenie incidentov na strane CSIRT

(„*nové*“) požiadavky na bezpečnostné opatrenia

(*nové*) koordinované posúdenia rizika kritických dodávateľských reťazcov na úrovni EÚ

Potreba zmien na národnej úrovni

zmienka o certifikácii

„*ne bis in idem*“ pri porušení ochrany osobných údajov a KB

(*nové - vyššie*) sankcie /...do 10M alebo 2% celkového svetového ročného obratu/

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

SUBJEKTY

Pôsobnosť

stredné podniky

+

podniky bez ohľadu na „veľkosť“

Podniky bez ohľadu na „veľkosť“

- poskytovatelia EK sietí a služieb
- poskytovatelia dôveryhodných služieb
- registre domén najvyššej úrovne
- jediní poskytovatelia kľúčových služieb
- tí, u ktorých narušenie = významný vplyv
- tí, u ktorých narušenie = významné systémové riziko
- subjekt s osobitným kritickým významom
- subjekty verejnej správy

...

klúčové subjekty

„subjekt typu označeného ako klúčový subjekt v prílohe I“

dôležité subjekty

„subjekt typu označeného ako dôležitý subjekt v prílohe II“

- upustenie od názvoslovía „prevádzkovateľ základnej služby“
 - *?zjednodušenie identifikácie povinných osôb?*
 - PDS = dôležitý subjekt
- poskytovateľ cloudových služieb ≠ PDS, ale kľúčový subjekt
 - size-cap rule¹ vs. možnosť národného riešenia
 - rovnocenné požiadavky na bezpečnosť
- rozdielny rozsah oprávnení dozorných orgánov pri kľúčových a dôležitých subjektoch (napr. pozastavenie certifikácie)

¹ *aspoň stredný podnik: menej než 250 zamestnancov a ročný obrat, ktorý nepresahuje 50 miliónov EUR alebo ročnú bilančnú sumu nepresahujúcu 43 miliónov EUR*

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

(nové) Kľúčové subjekty

...v rámci

ODVETVIE	Pododvetvie / Typ subjektu
Energetika	Diaľkové vykurovanie a chladenie; Vodík
Odpadová voda	Podniky zaoberajúce sa zberom, likvidáciou alebo úpravou komunálnych odpadových vôd, odpadových vôd z domácností a priemyselných odpadových vôd
Vesmír	Prevádzkovatelia pozemnej infraštruktúry, ktorú vlastní, spravujú alebo prevádzkujú členské štáty alebo súkromné subjekty, ktorí prispievajú k poskytovaniu vesmírnych služieb

ODVETVIE	Pododvetvie / Typ subjektu
Zdravotníctvo	Subjekty vyrábajúce základné farmaceutické výrobky a farmaceutické prípravky; Subjekty vyrábajúce zdravotnícke pomôcky považované za kritické počas mimoriadnej situácie v oblasti verejného zdravia
Digitálna infraštruktúra	poskytovatelia služieb dátového centra

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

(nové) Dôležité subjekty

...v rámci

ODVETVIE	Pododvetvie / Typ subjektu
Poštové a kuriérske služby	poskytovatelia kuriérskych služieb
Odpadové hospodárstvo	Podniky vykonávajúce činnosti nakladania s odpadom (okrem tých, pre ktoré to nie je hlavná činnosť)
Výroba, spracovanie a distribúcia potravín	Potravinárske podniky

ODVETVIE	Pododvetvie / Typ subjektu
Výroba	Subjekty vyrábajúce zdravotnícke pomôcky; Výroba počítačových, elektronických a optických výrobkov; Výroba elektrických zariadení; Výroba strojov a zariadení; Výroba motorových vozidiel, návesov a prívesov; Výroba ostatných dopravných prostriedkov
Poskytovatelia digitálnych služieb	poskytovatelia platforiem služieb sociálnej siete

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

KOMPARÁCIA POŽIADAVIEK NIS II a ZoKB

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

Bezpečnostné opatrenia

*„Členské štáty zabezpečia, aby **klúčové a dôležité subjekty** prijali vhodné a primerané technické a organizačné opatrenia na **riadenie rizík** súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú pri poskytovaní svojich služieb. S ohľadom na najnovší technický vývoj tieto opatrenia zabezpečujú takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá **miere daného rizika**.“*

NIS II	ZoKB (Vyhláška č. 362/2018 Z. z.)
analýza rizika a bezpečnostné politiky informačného systému	§ 6 + § 2 a 3
riešenie incidentov (predchádzanie incidentom, ich odhaľovanie a reakcia na ne)	§ I4
kontinuita činností a krízové riadenie	§ I7
bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom a jeho dodávateľmi alebo poskytovateľmi služieb, ako sú napríklad poskytovatelia služieb	§ 8

ukladania a spracúvania dát alebo riadených bezpečnostných služieb	
bezpečnosť pri nadobúdaní, vývoji a údržbe sietí a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach	§ 8
politiky a postupy (testovanie a audit) na posúdenie účinnosti opatrení na riadenie kybernetickobezpečnostných rizík	§ I5
používanie kryptografie a šifrovania	§ I3

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

SMERNICA NIS II (ostatné)

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

Lehoty

- účinnosť od **I6. januára 2023**

- transpozičná lehota NLT **I7. októbra 2024**

- vykonávacie akty Komisie (bezpečnostné opatrenia) pre:
*poskytovatelia služieb DNS, správcovia názvov TLD, poskytovatelia služieb
cloud computingu, dátového centra, poskytovatelia sietí na
sprístupňovanie obsahu, poskytovatelia riadených služieb, riadených
bezpečnostných služieb, poskytovatelia online trhov, internetových
vyhľadávačov a platforiem služieb sociálnej siete a poskytovatelia
dôveryhodných služieb*
do **I7. októbra 2024**

- opatrenia sa uplatňujú od I8. októbra 2024
- vytvorenie zoznamu kľúčových a dôležitých subjektov ČS
do I7. apríla 2025
- účinnosť novelizovaného znenia ZoKB (*prechodné ustanovenia?*)

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

Sankcie

IOM / 2% z celosvetového obratu za porušenie

- **čl. 18 bezpečnostné opatrenia**
- **čl. 20 oznamovanie (závažných) incidentov**

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

Budúce zmeny?

- **rozšírenie súčasných povinných osôb v zmysle ZoKB (nové thresholdy?)**
- **doplnenie novej povinnosti popri kybernetických bezpečnostných incidentoch hlásiť aj závažné kybernetické hrozby**

- doplnenie lehôt v rámci riešenia kybernetických bezpečnostných incidentov (**do 24 hodín od zistenia** incidentu poskytnúť prvotné oznámenie; **do 72 hodín** prvotné posúdenie a **najneskôr jeden mesiac** po uskutočnení prvotného oznámenia predložiť konečnú správu o riešení incidentu)
- možnosť dohody s príslušnými orgánmi (napr. jednotkou CSIRT) na **predĺžení lehôt** pre hlásenie incidentu a predloženie konečnej správy o riešení incidentu

- poskytnutie odpovede k prvotnému oznámeniu o incidente vrátane počiatočnej spätnej väzby k incidentu zo strany prijímateľa oznámenia
- povinnosť v určitých prípadoch informovať o incidente aj príjemcov služieb

- povinnosť a zodpovednosť riadiacich orgánov povinných osôb schvaľovať opatrenia a dohliadať na ich uplatňovanie
- **na požiadanie** oznamovateľa incidentu **získanie usmernenia** k vykonávaniu možných zmierňujúcich opatrení k hlásenému incidentu

- oprávnenie dozorného orgánu po uplynutí lehoty určenej k náprave nedostatkov alebo splneniu iných požiadaviek uložiť do doby splnenia povinnosti **dočasný zákaz výkonu riadiacich funkcií fyzickej osobe alebo dočasné pozastavenie certifikácie** (*zodpovednosť manažmentu*)
- (potenciálne) zmena obsahu kategorizácie KBI (*významné incidenty*)

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

A čo bezpečnosť?

súčasn~~e~~é znenie ZoKB pokrýva bezpečnostné požiadavky NIS 2

ALE

národný prístup otázky

ALE

veľa nového už nevymyslíme

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

...aktuálne?

O (r)evolúcii, ktorú prinesie nová Smernica NIS II

<https://www.bch.sk/nis-2>

Ďakujem za pozornosť

spilar@bch.sk

JUDr. Štefan Pilár

právník a certifikovaný audítor kybernetickej bezpečnosti