PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

NIS 2: Revízia európskej kyberbezpečnosti

doc. JUDr. Jozef Andraško, PhD.

Obsah

- Prečo smernica NIS 2?
- Predmet úpravy
- Pôsobnosť
- Pojmy
- Riadenie kybernetickobezpečnostných rizík
- Dohľad a presadzovanie práva

Prečo smernica NIS 2?

Prieskum smernice NIS

1. Nedostatočná prepojenosť požiadaviek smernice NIS pre jednotlivé sektory;
2. Nejasné vymedzenie pôsobnosti smernice a nejasné vymedzenie kompetencií národných dozorných autorít;
3. Odlišné bezpečnostné a notifikačné povinnosti naprieč členskými štátmi;
4. Nedostatočne efektívny dohľad a vymáhanie;
5. Neporovnateľné prerozdelenie financií pri otázkach kybernetickej bezpečnosti naprieč členskými štátmi;
6. Limitované zdieľanie informácií medzi členskými štátmi.

Dôvody revízie smernice NIS

1. nízka úroveň kybernetickej odolnosti podnikov pôsobiacich v EÚ;
2. nejednotná úroveň odolnosti v jednotlivých členských štátoch a odvetviach; a
3. nízka úroveň spoločnej situačnej informovanosti a nedostatočná spoločná reakcia na krízu.

Predmet úpravy

Predmet úpravy (čl. 1)

- stanovuje opatrenia na **zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti** v rámci EÚ,

- zároveň sa zameriava na **zlepšenie fungovania vnútorného trhu.**

činnosti potrebné na ochranu sietí a informačných systémov, ***užívateľov*** *takýchto systémov a* ***iných osôb dotknutých*** *kybernetickými hrozbami (CS Act)*

Predmet úpravy (čl. 1)

- ukladá **povinnosti členským štátom** prijať národné stratégie kybernetickej bezpečnosti, určiť príslušné vnútroštátne orgány, jednotné kontaktné miesta a jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT) (čl. 5 – 11 návrhu smernice NIS 2),

- stanovuje **povinnosti riadenia kybernetickobezpečnostných rizík a oznamovania pre subjekty** typu uvedených v prílohách I a II (čl. 17 až 20 návrhu smernice NIS 2),

- stanovujú **pravidlá** a **povinnosti týkajúce sa zdieľania informácií** o kybernetickej bezpečnosti (čl. 26 a 27 Návrhu smernice NIS 2),

- stanovuje **povinnosti dohľadu a presadzovania práva** pre členské štáty.

Pôsobnosť

Pôsobnosť (čl. 2)

- zásadná zmena v otázke rozsahu **(osobnej) pôsobnosti**

1. verejné a súkromné **kľúčové a dôležité subjekty**,
2. **typu** uvedeného v **prílohe I a prílohe II**,
3. poskytujú svoje **služby alebo vykonávajú svoje činnosti** v rámci EÚ a
4. **spĺňajú alebo prekračujú** prahové kritériá pre **stredné podniky** podľa odporúčania Komisie 2003/361/ES.

- *podniky, ktoré zamestnávajú **menej ako 250** osôb a ktoré majú buď ročný obrat nepresahujúci **50 miliónov eur**, alebo ročnú **bilančnú sumu neprevyšujúcu 43 miliónov eur.***

Kľúčové subjekty
(essential entities)
Dôležité subjekty
(important entities)

Nové sektory a podsektory

Pravidlo obmedzenia veľkosti
Stredné a veľké podniky

Pôsobnosť (čl. 2)

Príloha I – Sectors of high criticality

- energetika,
- doprava,
- bankovníctvo,
- infraštruktúry finančných trhov,
- zdravotníctvo,
- pitná voda,
- odpadová voda,
- digitálna infraštruktúra,
- **riadenie IKT služieb (B2B)**
- **subjekty** verejnej správy **okrem súdnictva, parlamentov a centrálnych bánk**
- vesmír.

Pôvodný návrh smernice NIS 2 – Odvetvia pre kľúčové subjekty

Pôsobnosť (čl. 2)

Príloha II – Other critical sectors

- poštové a kuriérske služby,
- odpadové hospodárstvo,
- získavanie, výroba a distribúcia chemických látok,
- výroba, spracovanie a distribúcia potravín,
- výroba,
- poskytovatelia digitálnych služieb a
- **výskum**.

Pôvodný návrh smernice NIS 2 – Odvetvia pre dôležité subjekty

Pôsobnosť (čl. 2) – výnimky z POV

2. Táto smernica sa však bez ohľadu na ich veľkosť uplatňuje aj na subjekty uvedené v prílohe I a II, keď:

2. ▌Regardless of their size, this Directive also applies to ***essential and important*** entities▌, where:

- kľúčové a dôležité subjekty **bez ohľadu na veľkosť**, kedy:

služby sú poskytované:

- poskytovateľmi **verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb** uvedené v bode 8 prílohy I;
- poskytovateľmi **dôveryhodných služieb** uvedených v bode 8 prílohy I;
- **správcami mien domény najvyššej úrovne a poskytovateľmi služby systému doménových mien (DNS)** uvedených v bode 8 prílohy I;

Pôsobnosť (čl. 2) – výnimky z POV

- subjekt je **jediným poskytovateľom služby**, ktorá má **zásadný význam** z hľadiska zachovania kľúčových spoločenských alebo hospodárskych činností;

- **narušenie služby** poskytovanej subjektom by mohlo mať **závažný vplyv na ochranu verejnosti, verejnú bezpečnosť alebo verejné zdravie**;

- **narušenie služby** poskytovanej subjektom by mohlo **vyvolať závažné systémové riziká**, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;

Pôsobnosť (čl. 2) – výnimky z POV

- **subjekt** je vzhľadom na svoj osobitný význam na regionálnej alebo celoštátnej úrovni **kritický pre konkrétne odvetvie** alebo typ služby alebo pre iné previazané odvetvia v členskom štáte;

- subjekt je **identifikovaný ako kritický subjekt** podľa Návrhu smernice Európskeho parlamentu a Rady **o odolnosti kritických subjektov** alebo ako subjekt rovnocenný s kritickým subjektom podľa článku 7 uvedenej smernice.

Identifikácia kritických subjektov.
3 kumulatívne kritériá podobne ako v smernici NIS

2. Pri identifikácii kritických subjektov podľa odseku 1 členské štáty zohľadňujú výsledky posúdenia rizika podľa článku 4 a uplatňujú tieto kritériá:

a) subjekt poskytuje jednu alebo viac základných služieb;

b) poskytovanie tejto služby závisí od infraštruktúry nachádzajúcej sa v členskom štáte a

c) incident by mal závažný rušivý vplyv na poskytovanie služby alebo iných základných služieb v odvetviach uvedených v prílohe, ktoré závisia od služby.

„základná služba“ je služba, ktorá má zásadný význam z hľadiska zachovania životne dôležitých spoločenských alebo hospodárskych činností;

Pôsobnosť (čl. 2) – výnimky z POV

- **Subjekty verejnej správy** (ústredná štátna správa, na regionálnej úrovni)

2a. Regardless of their size, this Directive also applies to:

– *public administration entities of central governments recognised as such in a Member State in accordance with national law and referred to in point 9 of Annex I;*

– *public administration entities at regional level referred to in point 9 of Annex I as defined by Member States, in accordance with national law, which following a risk based assessment, provide services the disruption of which could have a significant impact on critical economic or societal activities.*

Member States may establish that this Directive also applies to public administration entities at local level.

Pôsobnosť (čl. 2) – výnimky z POV

- **Subjekty verejnej správy** (ústredná štátna správa, na regionálnej úrovni)

9. Public administration ***entities excluding the judiciary, parliaments and central banks***		— Public administration entities of central governments ***as defined by a Member State in accordance with national law***
		— Public administration entities ***at regional*** level ***as defined by a Member State in accordance with national law***

Pôsobnosť (čl. 2) – SVS

- uznaný ako taký v členskom štáte v súlade s vnútroštátnym právom, ktorý spĺňa tieto (4 kumulatívne) kritériá:

1. je zriadený na účely **plnenia potrieb všeobecného záujmu** a nemá priemyselný ani komerčný charakter,
2. má **právnu subjektivitu** alebo je zo zákona oprávnený konať v mene iného subjektu s správnou subjektivitou,
3. je z väčšej časti financovaný štátnymi, regionálnymi alebo inými verejnoprávnymi inštitúciami; alebo jeho riadenie podlieha dohľadu týchto orgánov alebo inštitúcií; alebo má správnu, riadiacu alebo dozornú radu, v ktorej viac ako polovicu členov menujú štátne, regionálne alebo iné verejnoprávne inštitúcie;
4. má **právomoc vydávať pre fyzické alebo právnické osoby správne alebo regulačné rozhodnutia**, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovaru, služieb alebo kapitálu.

Pôsobnosť (čl. 2) – Výskum

2b. Member States may decide to apply this Directive to education institutions in particular when carrying out critical research activities.

(26f) 'research organisation': means an entity, excluding education institutions, which has as its primary goal to conduct applied research, or experimental development in view of the exploitation of the results of that research for commercial purpose.

Pôsobnosť (čl. 2) – Výskum

(45a) Research activities play a key role in the development of new products and processes. Many of these activities are carried out by entities that share, disseminate or exploit the results of their research, for commercial purposes. These entities can therefore be important players in value chains, which makes the security of their network and information systems an integral part of the overall cybersecurity of the internal market. Research organisations should be understood to encompass those entities focus the essential part of their activities on the conduct of applied research or experimental development, within the meaning of 2015 Guidelines for Collecting and Reporting Data on Research and Experimental Development (Frascati Manual) of the Organisation for Economic Cooperation and Development (OECD), in view of the results being used for commercial exploitation, such as the manufacturing and marketing of a product, process or the provision of a service.

Výsledky na komerčné účely

Pôsobnosť (čl. 2) – negatívna

- **subjekty verejnej správy**, ktoré vykonávajú svoju činnosť v oblasti **obrany, národnej bezpečnosti, verejnej bezpečnosti alebo presadzovania práva** vrátane vyšetrovania, odhaľovania a stíhania trestných činov.

Kľúčové a dôležité subjekty, ktoré vykonávajú činnosti v týchto oblastiach?

- Nie sú povinné plniť povinnosti podľa **čl. 18** (opatrenia na riadenie kybernetickobezpečnostných rizík) **alebo čl. 20** (oznamovacie povinnosti) vo vzťahu k týmto činnostiam alebo službám.
- Ak výlučne vykonávajú tieto činnosti alebo poskytujú tieto služby - nemusia plniť notifikačné povinnosti podľa článku 2a a článku 25.

Kľúčové subjekty (čl. 2a)

1. *For the purposes of this Directive, essential entities shall be considered all entities of the type listed in Annex I which exceed the ceilings for medium-sized enterprises as well as the following entities:*

   (a) *qualified trust service providers and top-level domain name registries as well as DNS service providers regardless of their size;*

   (b) *providers of public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I meeting the ceiling for medium-sized enterprises;*

   (c) *public administration entities referred to in Article 2(2a), first subparagraph;*

   (d) *any other entities of the types listed in Annex I and Annex II established by a Member State on the basis of national risk assessments following the criteria laid down in Article 2(2)(c) to (f);*

Kľúčové subjekty (čl. 2a)

(e) entities identified as a critical entity pursuant to Directive (EU) X/X of the European Parliament and of the Council [Resilience of Critical Entities Directive], referred to in Article 2(2)(g);

(f) if established by the Member States, entities which the Member States identified before the entry into force of this Directive as operators of essential services in accordance with Directive (EU) 2016/1148 or national law.

Dôležité subjekty (čl. 2a)

2. *For the purpose of this Directive, all entities of the type listed in Annexes I and II which do not qualify as essential pursuant to paragraph 1 shall be considered important entities. This includes entities designated by Member States on the basis of Article 2(2)(c) to (f).*

K a D subjekty

- ČS majú povinnosť vytvoriť **zoznam** KaD subjektov (6 mes. po termíne transpozície)
- KaD subjekty sú **povinné** zaslať tieto **informácie**:

a) názov subjektu;
b) adresa a aktuálne kontaktné údaje vrátane e-mailových adries, rozsahov IP, telefónnych čísel;
c) príslušné sektory a podsektory uvedené v prílohách I a II; a
d) prípadne zoznam členských štátov, v ktorých poskytujú služby podliehajúce tejto smernici.

- vytvorenie mechanizmu na **samo-registráciu** (ČŠ)

Zmenu v údajoch nahlásiť do 2 týždňov od kedy nastala zmena.

Lex specialis/ lex generalis (čl. 2b)

- právne akty EÚ **špecifické pre určité odvetvie**

- prijali **opatrenia** na riadenie kybernetickobezpečnostných rizík, alebo aby **oznamovali incidenty,**
- ak majú tieto požiadavky **aspoň rovnocenný účinok** ako povinnosti stanovené v tejto smernici,

- príslušné ustanovenia tejto smernice vrátane ustanovení o dohľade a presadzovaní práva v kapitole VI sa **neuplatňujú**.

Rovnocenný účinok (čl. 2b)

2. *The requirements referred in paragraph 1 of this Article shall be considered equivalent in effect to the obligations laid down in this Directive if:*

(a) *cybersecurity risk management measures, are at least equivalent in effect to those laid down in Article 18(1) and (2) of this Directive; or*

(b) *the sector specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the designated CSIRTs, the competent authorities under this Directive or the single point of contact and if requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 20(1) to (6).*

Lex specialis/ lex generalis (čl. 2b)

3. The Commission shall within six months after the entry into force of this Directive, issue guidelines clarifying the application of paragraphs 1 and 2. The Commission shall review the guidelines on a regular basis. When preparing those guidelines, the Commission shall take into account the views of the Cooperation Group and ENISA.

Princíp minimálnej harmonizácie (čl. 3)

This Directive shall not preclude Member States ***from adopting or maintaining*** provisions ensuring a higher level of cybersecurity***, provided that such provisions are consistent with their obligations under Union law***.

Article 3
Minimum harmonisation

Without prejudice to their other obligations under Union law, Member States may, in accordance with this Directive, adopt or maintain provisions ensuring a higher level of cybersecurity.

Pojmy

Nové pojmy

(4a) 'near miss' means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but was successfully prevented from transpiring or did not materialise;

(5a) 'large-scale cybersecurity incident' means an incident whose disruption exceeds a Member State's capacity to respond to it or with a significant impact on at least two Member States;

(7a) 'significant cyber threat' means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to severely impact the network and information systems of an entity or its users by causing considerable material or non-material losses;

(nové) pojmy

(5) ‘incident’ means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the [redacted] services offered by, or accessible via, network and information systems;

Bezpečnosť SIS

Kybernetická bezpečnosť

(Network security)

Riadenie kybernetickobezpečnostných rizík

Riadenie (čl. 17)

- **riadiace orgány** kľúčových a dôležitých subjektov majú schváliť **opatrenia** na riadenie kybernetickobezpečnostných rizík,
- opatrenia prijaté s cieľom dosiahnuť súlad s článkom 18,
- dohliadať na vykonávanie,
- môžu byť **zodpovední** sa za to, ak subjekty nedodržiavajú povinnosti podľa tohto článku.

Riadenie (čl. 17)

2. Member States shall ensure that ***the*** members of the management body ***of essential and important entities are required to*** follow ***training***, ***and shall encourage essential and important entities to offer similar training to all employees*** on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the ***services provided by*** the entity.

Opatrenia (čl. 18)

a) **analýzu rizika a bezpečnostné politiky** informačného systému;
b) **riešenie incidentov** (predchádzanie incidentom, ich odhaľovanie a reakcia na ne);
c) **kontinuita činností a krízové riadenie**;
d) **bezpečnosť dodávateľského reťazca** vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom a jeho dodávateľmi alebo poskytovateľmi služieb, ako sú napríklad poskytovatelia služieb ukladania a spracúvania dát alebo riadených bezpečnostných služieb;
e) **bezpečnosť pri nadobúdaní, vývoji a údržbe** sietí a informačných systémov vrátane **riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach**;
f) **politiky a postupy** (testovanie a audit) na posúdenie účinnosti opatrení na riadenie kybernetickobezpečnostných rizík;
g) používanie **kryptografie a šifrovania**.

Opatrenia (čl. 18)

2. The measures referred to in paragraph 1 ***shall be based on an all-hazards approach aiming to protect network and information systems and their physical environment from incidents, and*** shall include at least the following:

(a) risk analysis and information system security policies;

(b) incident handling ▌;

(c) business continuity, ***such as backup management and disaster recovery,*** and crisis management;

Opatrenia (čl. 18)

(40a) ***As threats to the security of network and information systems can have different origins, this Directive applies an "all-hazard" approach that includes the protection of network and information systems and their physical environment from any event such as theft, fire, flood, telecommunications or power failures or from any unauthorised physical access and damage to and interference with the entity's information and information processing facilities that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. The risk management measures should therefore also address the physical and environmental security by including measures to protect the entity's network and information systems from system failures, human error, malicious actions or natural phenomena in line with European or internationally recognised standards, such as those included in the ISO 27000 series. In this regard, entities should, as part of their risk management measures, also address human resources security and have in place appropriate access control policies. Those measures should be coherent with Directive XXXX [CER Directive].***

Opatrenia (čl. 18)

(d) supply chain security including security-related aspects concerning the relationships between each entity and its ***direct*** suppliers or service providers ▌;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures ▌ to assess the effectiveness of cybersecurity risk management measures;

(fa) basic computer hygiene practices and cybersecurity training;

(g) ***policies and procedures regarding*** the use of cryptography and***, where appropriate,*** encryption***;***

(ga) human resources security, access control policies and asset management;

(gb) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate.

Vykonávacie akty s cieľom stanoviť technické a metodické špecifikácie prvkov (21 mesiacov po účinnosti)

Opatrenia (čl. 18)

(26a) ***Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data on which entities rely upon. Cyber hygiene policies comprising a common baseline set of practices including, but not limited to, software and hardware updates, password changes, management of new installs, limitation of administrator-level access accounts, and backing up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or threats. ENISA should monitor and analyse Member States' cyber hygiene policies.***

(45b) ***Entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, and organise training for their staff, and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine learning systems to enhance their capabilities and the protection of networks.***

- V rámci národnej stratégie kybernetickej bezpečnosti členské štáty prijmú najmä tieto politiky:

(e) a policy on promoting and developing cybersecurity ***education and training,*** skills, awareness raising and research and development initiatives***, as well as guidance on good cyber hygiene prevention practices and controls, aimed at citizens, stakeholders and businesses***;

Oznamovacie povinnosti

Oznamovacie povinnosti (čl. 20)

- **Kto?**
- **Čo?**
- **Komu?**
- **V akej lehote?**
- Výnimky?

Oznamovacie povinnosti (čl. 20)

- **incident so závažným vplyvom** na poskytovanie ich služieb
- **jednotke CSIRT** alebo v prípade potreby príslušnému orgánu
- **oznámiť príjemcom svojich služieb** incidenty, ktoré by mohli nepriaznivo ovplyvniť ich poskytovanie (v prípade potreby)
- informácie v oznámení – **cezhraničný vplyv**
- ak oznámenie nie je urobené jednotke CSIRT, tak príslušný orgán postúpi oznámenie jednotke CSIRT

Oznamovacie povinnosti (čl. 20)

- **incident so závažným vplyvom:**

3. An incident shall be considered significant if:

(a) the incident has caused or ***is capable of causing severe*** operational disruption ***of the service*** or financial losses for the entity concerned;

(b) the incident has affected or ***is capable of affecting*** other natural or legal persons by causing considerable material or non-material losses.

Oznamovacie povinnosti (čl. 20)

Druh	Lehota	Obsahové náležitosti (v prípade potreby)
skoré varovanie (early warning)	bez zbytočného odkladu najneskôr do 24 hodín od zistenia incidentu	či závažný incident pravdepodobne spôsobilo nezákonné alebo zlomyseľné konanie alebo či má cezhraničný vplyv
incident	bez zbytočného odkladu najneskôr do 72 hodín od zistenia incidentu	• aktualizovanie informácií zo skorého varovania, • uvedie počiatočné posúdenie incidentu, jeho závažnosť a dosah, ako aj ukazovatele kompromitácie, ak sú k dispozícii;
priebežná správa o relevantných aktualizáciách daného stavu	(na základe požiadania jednotky CSIRT alebo príslušného orgánu)	

Oznamovacie povinnosti (čl. 20)

Druh oznámenia	Lehota	Obsahové náležitosti
konečná správa	najneskôr jeden mesiac po predložení oznámenia incidentu	• podrobný opis incidentu, jeho závažnosť a vplyv; • druh hrozby alebo základnú príčinu, ktorá pravdepodobne incident spôsobila; • uplatnené a prebiehajúce zmierňujúce opatrenia; • prípadne cezhraničný vplyv incidentu;
správa o pokroku (progress report) – prebiehajúce incidenty	• v čase keď mali podať konečnú správu • záverečnú správu do jedného mesiaca po vyriešení incidentu	

Povinnosti po oznámení (čl. 20)

- **Jednotka CSIRT/príslušný orgán**

Druh	Lehota	Poznámka
odpoveď oznamovateľovi	bez zbytočného odkladu a ak je to možné do 24 hodín od prijatia skorého varovania	• vrátane **počiatočnej spätnej väzby** k incidentu a na žiadosť subjektu usmernenia, operatívne poradenstvo k vykonávaniu možných zmierňujúcich opatrení. • jednotka CSIRT poskytne **doplňujúcu technickú podporu**, ak o to príslušný subjekt požiada. • ak existuje podozrenie, že incident má trestnoprávnu povahu, príslušné vnútroštátne orgány alebo jednotka CSIRT poskytnú aj usmernenia týkajúce sa oznamovania incidentu orgánom presadzovania práva.

Oznamovacie povinnosti (čl. 20)

- **2 a viac ČS –** informovať iné dotknuté ČŠ + ENISA bez zbytočného odkladu

- **informovanie verejnosti -** podmienky

Oznamovacie povinnosti (čl. 20)

- **Závažné kybernetické hrozby**

2. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili príslušným orgánom alebo jednotke CSIRT každú závažnú kybernetickú hrozbu, ktorú tieto subjekty zistia a ktorá by mohla potenciálne viesť k závažnému incidentu.

2. ***Where applicable,*** Member States shall ensure that essential and important entities ***are required to communicate***, without undue delay, the ***recipients of their services that are potentially affected by a*** significant cyber threat ***any measures or remedies*** that those ***recipients are able to take in response to that threat***. ***Where appropriate, the entities shall also inform those recipients of the threat itself.***

Dobrovoľné oznámenie relevantných informácií (čl. 27)

Member States shall ensure that ▌ notifications ***may be submitted to the CSIRTs or where relevant competent authorities***, on a voluntary basis, ***by:***

(a) ***essential and important entities with regard to*** cyber threats**,** near misses ***and relevant incidents which do not meet the criteria pursuant to Article 20(3);***

(b) ***entities falling outside the scope of this Directive, with regard to significant incidents, cyber threats or near misses.***

Dohľad a presadzovanie práva

Dohľad a presadzovanie práva

- **Čl. 29 – kľúčové subjekty**
- plnohodnotný režim dohľadu (ex ante a ex post)

- **Čl. 30 – dôležité subjekty**
- zjednodušený režim dohľadu (ex post),
- by nemali systematicky dokumentovať súlad s požiadavkami na riadenie kybernetickobezpečnostných rizík,
- príslušné orgány by nemali mať všeobecnú povinnosť vykonávať nad týmito subjektmi dohľad.

Dohľad a presadzovanie práva

- pri vykonávaní svojich právomocí na presadzovanie práva v súvislosti s kľúčovými subjektmi mali právomoc:
  - Vydávať varovania,
  - Vydávať záväzné pokyny.....

- opatrenia na presadzovanie práva **neúčinné**?
- KS - prijať potrebné opatrenia na nápravu nedostatkov alebo splniť požiadavky týchto orgánov v stanovenej lehote
- opatrenia sa v **lehote neprijali**?
- **dočasné pozastavenie alebo zákaz**

Dohľad a presadzovanie práva

(a) ***temporarily*** suspend or request a certification or authorisation body ***or courts according to national laws*** to ***temporarily*** suspend a certification or authorisation concerning part or all ***relevant*** services or activities provided by an essential entity;

(b) ▌request the imposition by the relevant bodies or courts ***in accordance with*** national ***law*** of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, ▌from exercising managerial functions in that entity.

Uložiť dočasný zákaz- pôvodný návrh

akejkoľvek inej fyzickej osobe zodpovednej za porušenie- pôvoný návrh

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

ďakujem za pozornosť

doc. JUDr. Jozef Andraško, PhD.
jozef.andrasko@flaw.uniba.sk